Buat paper ttg perlindungan dari insiden serangan Web Deface, DDOS, Phising, SQL Injection, atau Malware dari aspek etike.

Kelas B:

- Belpa Yayang Anugrah (Web Deface)
- Caesario Rian Saputra (DDOS)
- Dhea Noranita Putri (Phising)
- Dian Satria Pratama (SQL Injection)
- Hamzah Ramadhan (Malware)
- Masroni Dedi Kiswanto (Web Deface)
- Mezi Puspayani (DDOS)
- Muhammad Syahril (Phising)
- Rahmad Kartolo (SQL Injection)
- Reynaldi (Malware)
- Rio Permata (Web Deface)
- Yeni Gustini (DDOS)
- Yudistira Sira Permana (Phising)
- Dini Rahmadia (SQL Injection)

Kelas A:

- Gian Pratama (Web Deface)
- Arieansyah (DDOS)
- Mefta Eko Saputra (Phising)
- Lily Pebriana (SQL Injection)
- Lailatur Rahmi (Malware)
- Adiktia (Web Deface)
- Armansyah (DDOS)
- Ibnu Fajar (Phising)
- Moh. Rendy Septiyan (SQL Injection)
- Revi Candra (Malware)
- Agus wiranto (Web Deface)
- Agus sumitro (DDOS)
- Moh Fajri Al Amin (Phising)
- Angga (SQL Injection)
- Yudistira (Malware)
- Ekariva Annas (Web Deface)
- Hari febriadi (DDOS)
- Miftahul fallah (Phising)
- Fajar Prayoga (SQL Injection)
- Erwin (Malware)
- Putri Armilia (WEb Deface)
- Putri Eleina (DDOS)
- I Made Phising)
- M. Devian (SQL Injection)
- Herli Septia Fani (Malware)

- Candra Inara (Web Deface)

Struktur Paper: Pendahuluan, Literature Review, Pembahasan, Kesimpulan, Daftar Referensi. Minimum 1500 kata

Nama : Putri Armilia Prayrsy
Nim : 182420125
Kelas : MTI.20 A
Mata Kuliah : Ethical Issues In Electronic information System

I. PENDAHULUAN

Teknologi yang berkembang begitu cepat memang dirasa membuat semuanya menjadi mudah, namun hal itu juga menimbulkan dampak yang cukup banyak bagi kehidupan sendiri. Misalkan saja seperti kejahatan dunia maya yang terus berkembang dari era ke era, bahkan dengan metode yang berbeda-beda

Memiliki website memang suatu keharusan bagi mereka yang ingin menjalani bisnis dengan lebih mudah. Karea rana online saat ini sangat luas dan mudah untuk dilakukan oleh siapa saja. Namun kemudahan dan keleluasaan ini juga memberikan banyak kesempatan bagi orang – orang iseng untuk memberikan kita rasa takut. Mulai dari kehilangan data sampai tidak bisa diaksesnya website karena serangan hacker. Begitu pentingnya sebuah data bagi kita, perlu juga kiranya kita menjaga website dan benar – benar waspada dalam melindungi website dari serangan hacker.

Hacker memiliki motivasi yang berbeda ketika mereka merusak situs web. Motivasi politik adalah satu. Hacker yang menentang pemerintah atau gerakan tertentu dapat memilih untuk menghapus situs web terkait untuk menyiarkan pandangan mereka. Hacker yang melakukan ini dikenal sebagai hacker. Mereka dapat mengubah konten situs web yang dirusak dengan gambar atau pesan pilihan mereka.

Hacker dapat memilih untuk merusak situs web untuk bersenang-senang mengejek pemilik situs dengan menemukan kerentanan situs web dan mengeksploitasi ini untuk merusak situs web. Hacker ini mengejek pemilik situs. Mirip dengan retas, hacker ini merusak situs web dengan gambar atau pesan pilihan mereka.

Selain itu pelaku deface biasanya untuk melakukan deface memulai dengan dorking menggunakan google. Menggunakan query tertentu yang memungkinkan untuk menampilkan website yang memiliki celah keamanan. Celah keamanan yang kira kira bisa melakukan deface website.

Situs web tidak hanya dirusak karena alasan politik, banyak pelaku deface melakukannya hanya untuk kesenangan. Sebagai contoh, ada kontes online di mana hacker diberikan poin karena mengotori sejumlah besar situs web dalam jumlah waktu tertentu .

Perusahaan juga lebih sering ditargetkan daripada situs web lain di World Wide Web dan mereka sering berupaya mengambil tindakan untuk melindungi diri dari perusakan atau hackeran pada umumnya. Situs web mewakili citra perusahaan atau organisasi dan karenanya mengalami kerugian yang signifikan karena perusakan.

Pengunjung mungkin kehilangan kepercayaan pada situs yang tidak dapat menjanjikan keamanan dan akan menjadi waspada dalam melakukan transaksi online. Setelah defraksi, situs harus ditutup untuk perbaikan dan tinjauan keamanan, kadang kadang untuk periode waktu yang lama, menyebabkan biaya dan hilangnya keuntungan dan nilai..

Kejahatan dunia maya tentu saja sifatnya merugikan, tidak hanya bisa mencuri privasi seseorang saja tapi juga dapat mengganggu website milik orang lain; misalnya seperti melakukan **web deface**.

II. LITERATURE RIVIEW

Deface Website adalah tindakan memodifikasi halaman web orang lain, termasuk penambahan, penghapusan, atau perubahan konten yang ada secara tidak sah. Serangan serangan ini biasanya dilakukan oleh hacker, yang mengkompromikan situs web atau server dan mengubah informasi situs web yang dihosting dengan pesan yang mereka buat sendiri.

Deface website merupakan salah satu kejahatan yang tidak asing lagi dalam sistem keamanan website. Deface ini termasuk tindakan yang dilarang karena merugikan berbagai pihak, biasanya deface dilandasi karena tindakan usil, pamer, unjuk kebolehan uji coba ilmu, pamer kemampuan dan tujuan lainnya.

Celah keamanan website yang dibuat oleh developer ini lah yang membuat suatu web menjadi rentan untuk di serang, adapun celah utama seperti rentan terhadap serangan injeksi SQL. Situs web yang tidak dipatch atau tidak terkonfigurasi dengan mudah rentan terhadap alat scanner yang digunakan oleh para pelaku ini, yang dapat mengarah pada akses tidak sah ke situs web.

Deface website sering menyasar pada website-website pemerintahan atau website perusahaan, jarang menyasar pada website pribadi. Tujuan utamanya biasanya untuk menyampaikan pesan kepada instansi terkait. Selain itu ada juga para defacer yang melakukan deface website karena ingin mencari ketenaran saja dengan menyasar sembarang website.

Orang yang melakukan Deface disebut dengan istilah Defacer, Defacer bisa mengubah tampilan website target sesuai dengan keinginan mereka. Salah satu teknik yang sangat terkenal dalam proses Deface ini adalah DDoS atau Denial of Service (mengirimkan request palsu pada server website sehingga server akan menjadi lambat dan down).

III. PEMBAHASAN

Deface website adalah salah satu kegiatan yang tujuan utamanya untuk merubah tampilan website halaman utama, index file atau halaman lainnya. Kegiatan web deface ini bisa terjadi karena adanya celah keamanan yang lemah pada website korban. Ciri-ciri website yang sudah menjadi korban web deface adalah tampilan tiba-tiba berubah dengan isi pesan yang aneh-aneh yang berbeda dari sebelumnya.

A. Jenis-Jenis Web Deface

Adapun untuk jenis jenis deface nya ada beberapa jenis, yaitu;

1. Image Deface => yaitu mendeface website namun hanya merubah gambarnya saja. Misal hanya mendeface pada halaman index saja, atau halaman tertentu yang ingin atau memiliki celah keamanan.
2. Script Deface => yaitu mendeface website namun hanya merubah scriptnya saja.
3. Anchor Deface => yaitu mendeface website namun hanya merubah anchor nya saja.
4. Iframe Deface => yaitu mendeface website namun hanya merubah iframenya saja.
5. Link Deface => yaitu mendeface website namun hanya merubah linknya saja.
6. Text Deface => yaitu mendeface website namun hanya merubah textnya yang tertentu saja.

B. Tujuaan Serangan Deface

Setiap peretas tentu memiliki alasan dan tujuan masing-masing dibalik serangan deface yang mereka lakukan. Misalkan saja karena iseng, karena pelaku tidak suka dengan website bersangkutan, karena ingin balas dendam, ingin dianggap hebat, ingin menguji kemampuan dan lain sebagainya. Alasan-alasan tersebut bisa saja menjadi motivasi utamanya, namun

yang pasti aktivitas deface sendiri tentu merugikan pihak lain dan hal ini sudah bisa dianggap sebagai salah satu kejahatan dunia maya.

C. Penyebab Terjadinya Deface

Faktor-faktor yang menyebabkan terjadinya deface yaitu sebagai berikut :

1. Kurangnya Security Awarness dari web master atau administrator sehingga menyebakan kurangnya kewaspadaan terhadap celah kemanan yang ada di website.
2. Penggunaan Free CMS dan Web App Open Source tanpa adanya perubahan, penggunaan default konfigurasi, ini akan membudahkan defacer yang memang sudah memahami celah keamanan di suatu CMS untuk masuk ke dalam suatu sistem maupun database.
3. Menggunakan Versi CMS lama atau cms tidak di update, ini terbilang cukup rentan karena bug dan security issue terus berkembang dari waktu ke waktu, jadi sebaiknya selalu update versi CMS yang terbaru agar mendapatkan kemanan yang lebih dan juga perbaikan bug.
4. Jarang melakukan update security, sebelum mendeface kebanyakan defacer sudah menemukan bug dan menyisipkan shell backdoor jadi sebelum keduluan di deface web master harus sering melakukan pengecekan terhadap security update.

D. Tool Pendeteksi Deface Web

Berikut ini adalah tool yang digunakan untuk mendeteksi tindakan deface pada website, yaitu:

1. **Fluxguard**
   Fluxguard adalah aplikasi monitoring serangan deface website berbasis cloud, yang mampu merender semua jenis halaman web termasuk dashboard yang dilindungi kata sandi dan tindakan formulir. Bersamaan dengan pemantauan defacement, Fluxguard dapat membantu Anda dengan otomatisasi QA, transaksi sintetis, regresi visual, dan pemantauan kinerja aplikasi.
2. **SUCURI**
   SUCURI menawarkan pemantauan keamanan, perlindungan, pencadangan, dan keuntungan kinerja situs web dalam semua hal. Ia berfungsi dengan situs kapan saja, termasuk WordPress, Joomla, Drupal, Magento, Bulletin, phpBB, dan lain lain.
3. **IPVTec**
   IPVTec adalah tool online layanan pemantauan yang membantu untuk memberi tahu jika situs web menjadi rusak atau berubah. Pengguna dapat mengonfigurasi untuk mendapatkan pemberitahuan melalui email, SMS, atau keduanya. IPVTec juga membantu pengguna untuk mengingatkan dalam skenario berikut.
4. **24×7**
   Web 24 × 7 menyediakan layanan pemantauan ujung ke ujung, dan deteksi defokasi adalah bagian dari Pemantauan Situs Web. Ada banyak kombinasi yang dapat dikonfigurasi untuk mendapatkan peringatan ketika situs website menjadi rusak.
5. **Visualping**
   Tool visualping Ini memungkinkan pengguna untuk memilih area situs web yang ingin di pantau dan mendapat pemberitahuan tentang segala perubahan yang terdeteksi. Ini lebih seperti perbandingan visual untuk memicu peringatan pada perubahan kecil, sedang, atau signifikan pada interval harian, jam, atau mingguan.
6. **OnWebChange**
   OnWebChange membantu pengguna memilih beberapa area dalam halaman web dan memberi tahu jika ada perubahan yang terdeteksi. Bersama dengan halaman web, pengguna juga dapat memonitor file seperti PDF, gambar, video, teks biasa, dan lain

lain. Selain pengguna memiliki opsi untuk mengonfigurasi pengguna ingin diberi tahu melalui email, pushover, teamstinct, atau HTTP callback.

7. **WebOrion**
   Monitor WebOrion menawarkan perubahan visual, konten & pemantauan integritas. pengguna memiliki opsi untuk menerima pemberitahuan melalui email, SMS, atau Webhooks. Layanan monitor WebOrion tersedia di Cloud (SaaS), pada perangkat premis atau perangkat virtual.
8. **Versionista**
   Versionista merayapi seluruh situs untuk memantau perubahan dan memberi tahu melalui email atau slack. Bukan hanya HTML, tetapi Versionista mampu melacak perubahan dalam PDF, teks, dan konten dinamis juga.
9. **Monitis**
   Salah satu platform pemantauan situs berbasis cloud yang populer menawarkan daftar hitam dan pemantauan defokasi. Monitis melakukan pengecekan setiap 12 jam dan memberi tahu segala kemungkinan suatu situs dirusak atau masuk daftar hitam.
10. **Wachete**
    Monitor area tertentu atau seluruh situs setiap 24 jam GRATIS. Dan, jika pengguna perlu meningkatkan frekuensi, maka tingkatkan untuk memeriksa setiap jam dari $ 4,90 per bulan. Wachete mampu memonitor halaman yang dilindungi kata sandi, halaman dinamis, dan terintegrasi dengan baik dengan produk pihak ketiga. Wachete mendapatkan aplikasi selulernya untuk Android, Windows, dan iOS untuk melacak perubahan dan menerima pemberitahuan push.

E. Cara Mencegah Web Deface

Berikut ini adalah cara mencegah terjadinya deface di website, yaitu;

1. Melakukan Audit Dan Penetration Testing

Yaitu melakukan pemeriksaan atau audit dan percobaan penerobosan terhadap sistem sendiri. Hacker mengeksploitasi kerentanan yang belum ditonton. Mereka menggunakan port terbuka untuk mencoba menghubungkan server tanpa masuk dan menjalankan kode berbahaya melalui koneksi yang sah. Audit reguler dan pengujian penetrasi sangat membantu dalam mengevaluasi keamanan infrastruktur TI (sistem operasi, layanan dan kelemahan aplikasi, konfigurasi yang tidak tepat, atau perilaku pengguna akhir yang berisiko) dan melindungi sistem dengan lebih baik.

2. Hati Hati Dengan SQL Injection

Yaitu membuat pertahanan dalam coding yang berfungsi untuk mencegahnya serangan deface website. Banyak aplikasi web menerima input pengguna dari formulir dan input pengguna dimasukkan langsung ke query SQL dalam aplikasi web. Contoh:
$result=$mysql >query (‘select email, userid FROM members Where email= “$email”’);
Melakukan pertahanan ini bisa menggunakan variabel terikat, namun lebih baik untuk menghindari penggunaan SQL yang dihasilkan secara dinamis dengan menggunakan prosedur tersimpan atau kalengan.
Sebagai tambahan yaitu dengan;
• Batasi input hanya untuk karakter yang diterima,
• White list. Penggunaan biasa, daftar set nilai yang mungkin jika ada,
• melakukan pemeriksaan panjang. Periksa panjang input terhadap panjang bidang.

3. Hati Hati Dengan Cross Site Scripting

Yaitu membuat pertahanan coding untuk melawan serangan Cross Site Scripting (XSS). Serangan Cross Site Scripting memungkinkan hacker untuk menyematkan kode skrip ke dalam halaman web yang dapat melakukan berbagai tindakan tidak sah. Ini mungkin

termasuk mengubah tampilan halaman web, mencuri cookie sesi dari pengguna situs web lain, atau bahkan sebagai cara untuk membentuk serangan XSS lain di situs web lain.
Sebagian besar bidang biasanya hanya membutuhkan karakter alfanumerik jadi hati hati dengan karakter khusus seperti <, > and =. Ini juga merupakan praktik yang baik untuk menggunakan web Application firewall (WAF).

4. **Menggunakan Tool Pendeteksi Deface Website**

Yaitu menggunakan perangkat lunak pendeteksi deface wwebsite. Serangan zero day membuat kita memiliki waktu yang sangat singkat untuk bereaksi dan membentuk kontrol kerusakan setelah insiden. Alat pemantauan dan pendeteksian defraksi adalah solusi terbaik untuk mendeteksi setiap defokasi atau perubahan tidak sah di situs web.Banff Cyber's WebOrion, Site24x7 dan Nagios merupakan perangkat lunak yang dapat digunakan untuk menjalankan tugas ini.

5. **Membuat Rencana Jika Terjadi Deface Website**

Yaitu membuat perencanaan ketika terjadi insiden deface website. Alat deteksi yang baik hanya memberi tahu kita ketika situs web kita telah dirusak tetapi bukan tindakan yang harus diambil. Karena itu, sangat penting untuk mengambil tindakan untuk menanggapi insiden semacam itu, memastikan bahwa personel yang tepat ada di tim tanggapan. Mungkin juga penting untuk memiliki komunikasi perusahaan dan menyiapkan pidato publik.

6. **Mengelola Pesan Eror**

Yaitu mengelola pesan error yang muncul dari website. Hati hati dengan jumlah informasi yang disediakan dalam pesan kesalahan. Pesan kesalahan terperinci harus dicatat secara lokal dan hanya pesan kesalahan sederhana yang harus ditampilkan kepada pengguna, karena memberikan pesan terperinci dapat membocorkan rahasia kelemahan yang ada pada sistem pengguna dan membuat serangan jauh lebih mudah.

7. **Pastikan Validasi Dari Sisi Server Dan Client**

Validasi harus dilakukan di kedua sisi server dan klien untuk memberikan keamanan tambahan. Misalnya. hanya izinkan angka dalam bidang angka dan berikan validasi lebih dalam pada server jika hal ini mungkin dilewati.

8. **Hati Hati dengan Fitur File upload**

Yaitu memberikan konfigurasi hanya file tertentu yang bisa diupload. hanya Banyak file yang diunggah mungkin berisi kode yang dapat dieksekusi oleh server. Mengubah izin file yang sedang diunggah dengan menghapus izin yang dapat dieksekusi akan mencegah server dari mencoba untuk mengeksekusinya.

9. **Menggunakan Protokol HTTPS**

Yaitu menggunakan layanan HTTPS. HTTPS memungkinkan komunikasi yang aman antar perangkat. Ketika https digunakan di seluruh situs web, data yang dikirimkan dari satu perangkat ke perangkat lainnya dienkripsi, membuatnya tidak dapat dibaca. Itu dienkripsi di satu ujung dan didekripsi di ujung lainnya.

10. **Buat Direktori Admin Yang Unik**

Cara cerdik yang digunakan hacker untuk mengakses situs web adalah dengan langsung dan meretas direktori admin web. Mereka menggunakan skrip untuk nama giveaway seperti admin dan login dan memfokuskan energi mereka pada memasukkan folder ini untuk berkompromi. Memilih nama unik dapat sangat mengurangi kemungkinan pelanggaran potensial.

11. **Gunakan Alamat Admin Yang Unik**

Pastikan bahwa email admin yang digunakan untuk masuk ke situs web aman berbeda dari alamat apa pun yang tercantum pada info kontak situs website. Menjaga alamat ini tetap pribadi akan mencegah scammers mengirimi pengguna email phishing. Untuk mengetahui phishing lebih detail baca artikel tentang teknik phishing, metode, dan toolnya ini ya.

12. Ubah Prefix Database

Dengan mengubah awalan basis data default atau prefix basis data akan mempersulit hacker untuk mendapatkan data dari basis data.

13. Batasi Level Akses Website

Jika lebih dari satu orang masuk ke situs web untuk membuat perubahan pada konten, batasi jenis akses yang dimiliki setiap individu tambahan. Memiliki banyak administrator di situs web Anda membuka peluang bagi kejahatan dunia maya untuk mendapatkan akses tidak sah melalui halaman login Anda. Membatasi akses penuh ke konten dapat mencegah perusakan situs web yang disebabkan oleh kesalahan manusia (misalkan Kata sandi yang lemah).

14. Scan Coding Website

Jika memiliki latar belakang teknis atau anggota staf yang mengerti teknologi, maka dapat memeriksa malware secara manual celah kemanan di situs Anda. Anda juga harus memiliki akses ke pengelola file yang disediakan oleh host domain atau protokol transfer file, yang keduanya dapat digunakan untuk memeriksa situs Anda terhadap malware. Cari atribut skrip dan <iframe>, dan pindai URL yang mengikuti atribut ini untuk memastikan Anda mengenalinya. Jika Anda tidak melakukannya, mereka mungkin telah disuntik dengan konten jahat.

F. Contoh Serangan Web Deface

Beberapa Contoh Website Milik Negara yang Pernah Terkena Serangan dari Deface:

1. Website KPU

Pada tanggal 17 April 2004 silam, seorang hacker bernama Dani Hermansyah pernah melakukan serangan deface terhadap website KPU dan mengubah nama-nama partai menjadi nama buah-buahan dalam situs tersebut, yaitu www.kpu.go.id.

Kejadian itu akhirnya membuat kepercayaan website KPU berkurang di mata masyarakat, dan kredibiltasnya pun patut dipertanyakan. Masyarakat hanya risau kejadian itu mengakibatkan angka-angka jumlah pemilih yang sudah masuk di sana menjadi tidak aman dan berpotensi diubah begitu saja.

2. Website Kepolisan Republik Indonesia

Pada tahun 2011 lalu, website milik Kepolisan Republik Indonesia yang beralamatkan www.pori.go.id juga sempat menjadi salah satu korban dibalik serangan deface. Padahal kejadian waktu itu bertepatan pada proses penangkapan teroris di Jawa Tengah. Hal ini akhirnya membuat masyarakat berspekulasi bahwa serangan website tersebut dilakukan oleh sekelompok teroris yang bekerja di bidang internet. Tidak habis sampai disana, akibat serangan yang terjadi pada website Kepolisia Republik Indonesia ternyata juga berimbas terhadap website milik negeri lainnya, bahkan salah satunya adalah website milik Kementrian Komunikasi dan Informatika yang merupakan tonggak IT Indonesia juga tak luput dari serangan deface.

IV. KESIMPULAN

Deface website merupakan teknik hacking yang merubah tampilan tertentu pada website orang lain secara tidak sah. Tekniknya adalah dengan membaca source codenya agar tidak menjadi korban deface website maka perlu melakukan tindak pencegahan seperti memonitoring perubahan coding, dan menggunakan perangkat keamanan teknologi informasi. Selain itu perlu juga membuat rencana jika terjadi insiden deface website.

V. DAFTAR REFERENSI

https://www.google.com/amp/s/aliyhafiz.com/deface-website-pengertian-jenis-mencegah/amp/
https://www.google.com/amp/s/www.indoworx.com/web-deface/amp/
https://qwords.com/blog/apa-itu-deface-website/
https://www.indoworx.com/web-deface/

Keamanan Terhadap Serangan SQL Injection

Rahmad Kartolo
Magister Teknik Informatika
Universitas Bina Darma Palembang
Rahmadcart87@gmail.com

ABSTRAK- Keamanan merupakan faktor penting dalam membantu pembangunan website. Banyaknya layanan bisnis berupa toko online berbasis web dan sebagainya menjadikan keamanan sebagai faktor terpenting untuk dijaga dengan baik. Aplikasi yang bersifat terbuka dan dapat diakses dengan mudah oleh siapa saja dapat membuat keamanan terancam. Salah santu ancaman serangan tersebut yaitu SQL injection yang merupakan serangan hacker untuk website untuk memasuki dan mendapatkan akses ke basis data. Metode yang digunakan SQL injection biasnya menggunakan form yang terdapat di dalam website yang tidak dilindungi dengan script khusus.
Kata kunci : SQL Injeksi, Web

PENDAHULUAN

Salah satu gangguan atau bentuk kejahatan di internet adalah dalambentuk mengganggu sistem jaringan dan database. Salah satu teknik dalammengganggu sistem database jaringan adalah dengan menggunakan SQL injection.SQL injection atau dikenal juga dengan SQL insertion yaitu sebuah teknik yangdigunakan untuk mengeksploitasi database pada suatu websites dengan memaksakeluarnya error page situs itu yang ada error pages itu terdapat info tentangs truktur database website yang dieksploitasi.
Serangan *SQL Injection* merupakan jenis eksploitasi keamanan halaman web, dimana penyerangan menyisipkan kode-kode SQL melalui formulir/*form* kemudian memanipulasi URL berdasarkan pada parameter sql. Serangan *SQL Injection* adalah serangan yang berupa menginjeksi perintah SQL malaui *form input data*, yang kemudian di teruskan menuju *database* untuk dieksekusi, dengan tujuan mengakses data sensitive seperti *database*.

Teknik SQL Injection memungkinkan seseorang dapat login kedalam sistem dabase tanpa harus memiliki account dengan cara mengisi default setting SQL. Default setting SQL yang paling berbahaya (kosong / tidak diisi). Jika default settingnya belum dirubah maka ketika ada sebuah direktori pada website yang memiliki form untuk login admin, para hacker dapat masuk kedalam dengan hanya (kosong / tidak diisi). Bentuk lain untuk masuk kedalam adalah dengan menggunakan string ' OR 1-1- - pada halaman yang memilikii user dan password. Jika kita memasukan string ' OR 1=1-- di input box user dan memasukan password = foobar di input box password, sehingga menagkibatkan SQL Query menjadi bingung. SQL Query akan membacanya sebagai: SELECT * from users where User =" or 1=1-- and Password='foobar' yang memiliki arti bahwa sql akan men-SELET semua - - (tanda adalah mark dari SQL).

Literatur Review

Tinjauan Pustaka Pada penelitian ini digunakan empat buah tinjauan pustaka, yang pertama ditulis oleh Feri Setiyawan. Web server pada penelitian ini menggunakan nginx yang dilengkapi dengan naxsi sebagai web application firewall. Pembahasan mengenai perbandingan antara sebelum dan sesudah implementasi naxsi terhadap serangan SQL injection (Feri Setiyawan, 2014). Pustaka kedua ditulis oleh Albi Alamsyah mengenai pengujian keamanan setelah implementasi ModSecurity terhadap empat jenis serangan yaitu SQL Injection, Cross Site Scripting (XSS), Local File Inclusion (LFI) dan Remote File Inclusion (RFI) (Albi Alamsyah, 2016). Pustaka ketiga

ditulis oleh Gilang Ramadhan, web server yang digunakan adalah nginx yang dilengkapi dengan naxsi dan apache yang dilengkapi dengan modsecurity. Pembahasan mengenai studi kasus pada sebuah instansi yang membandingan instalasi nginx yang dilengkapi naxsi dengan apache yang dilengkapi dengan ModSecurity (Gilang Ramadhan, 2014).

Pustaka keempat ditulis oleh Aditya, web server yang digunakan adalah apache yang dilengkapi dengan ModSecurity. Pembahasan mengenai pembacaan log oleh aplikasi jwall auditconsole untuk dijadikan alat pelapor adanya insiden (Aditya Noor Sandy, 2014).

Detail dari tinjauan pustaka disajikan dalam bentuk tabel yang terlihat pada tabel 2.1 Tabel Perbandingan

Tabel 2 1 Tabel Perbandingan

Parameter / Penulis	Objek	Metode/Alat	Bahasa Pemrograman	Interface
Feri Setiyawan (UIN SUKA) tahun 2014	Pencegah *SQL Injection*	Naxsi, Nginx	PHP (Joomla)	-
Albi Alamsyah (Universitas Muhammadiyah Jember) tahun 2016	Pengujian keamanan terhadap *SQL Injection, Cross Site Scripting (XSS), Local File Inclusion (LFI) dan Remote File Inclusion (RFI)*	ModSecurity , Apache	PHP (DVWA)	-
Gilang Ramadhan (Unikom) tahun 2014	Perbandingan keamanan dua jenis *Web Application Firewall (WAF)*	Naxsi, Nginx, ModSecurity , Apache	PHP (website XecureIT)	-
Aditya Noor Sandy (UPN Veteran Jawa Timur) tahun 2014	Pelaporan dugaan tindakan intrusi pada website	ModSecurity , Apache	PHP	Jwall Auditconsole
Usulan	Pengembangan filter *ModSecurity* untuk *File Upload, PHP Code Injection* dan *PHP Object Injection*	ModSecurity , Apache	PHP (Wordpress dan Joomla)	-

METODELOGI PENELITIAN

Metode Penelitian yang dilakukan dalan penulisan makalah ini adalah bersifat literature. SQL Injection merupakan kegiatan yang dilakukan untuk perintah SQL ditujukan statment SQL yang ada pada aplikasi yang sedang berjalan. Adapun teknik untuk mengeksploitassikan web ini di dalam SQL injection yang memiliki database sebagai tempat penyimpanan data. SQL Injection terjadi karena kurangnya keamanan pada website tersebut untuk menghandle suatu inputan pada form login yang umumnya terletak pada username dan password

Pembahasan

Beberapa jenis serangan yang digunakan pada penelitian ini diuraikan seperti berikut.

1. File Upload File yang diunggah mewakili risiko yang signifikan terhadap aplikasi. Langkah pertama serangan pada umumnya adalah mendapatkan beberapa kode pada sistem yang akan diserang. Kemudian serangan hanya perlu mencari jalan untuk mendapatkan kode yang dieksekusi. Menggunakan upload file membantu penyerang menyelesaikan langkah pertama. Konsekuensi dari upload file yang tidak terbatas dapat bervariasi, termasuk pengambilalihan sistem yang lengkap, sistem berkas atau database yang kelebihan beban, serangan penerusan ke sistem back-end, serangan sisi klien, atau penghindaran sederhana. Itu tergantung pada apa aplikasi yang dilakukan dengan file upload dan terutama di tempat penyimpanannya.
2. Code Injection
   Code Injection adalah istilah umum untuk jenis serangan dengan mengirim kode program kemudian dieksekusi oleh aplikasi. Jenis serangan ini memanfaatkan penanganan data yang tidak sempurna. Jenis serangan ini biasanya dimungkinkan karena kurangnya validasi data input / output yang tepat, misalnya: karakter yang diizinkan, format data dan jumlah data yang diharapkan. Code Injection berbeda dengan Command Injection karena penyerang hanya dibatasi oleh fungsi bahasa pemrograman yang digunakan.
3. PHP Object Injection PHP Object Injection adalah tingkat kerentanan aplikasi yang memungkinkan penyerang melakukan berbagai jenis serangan berbahaya, seperti Code Injection, SQL Injection, Path Traversal dan Denial of Service, tergantung pada konteksnya. Kerentanan terjadi ketika masukan yang diberikan pengguna tidak disterilkan dengan baik sebelum dikirim ke fungsi PHP unserialize(). Karena PHP memungkinkan serialisasi objek, penyerang bisa melewati string serial ke panggilan unserialize() yang rentan, sehingga menghasilkan sembarang objek PHP ke dalam lingkup aplikasi

Dari uraian tiga buah ancaman pada aplikasi web di atas, terdapat perbedaan metode yang dilakukan oleh penyerang dalam memanfaatkannya. Berikut ini merupakan tabel beberapa metode penyerangan yang biasa digunakan pada masing – masing jenis kelemahan.

Tabel 2 2 Metode Penyerangan

Kelemahan	Metode
File Upload	Pengiriman file php secara langsung
	Pengiriman file php dengan ekstensi ganda
PHP Code Injection	Manipulasi parameter untuk bypass seleksi
	Penyisipan kode ke dalam database
PHP Object Injection	Pengiriman serialisasi objek secara langsung
	Pengiriman serialisasi objek dengan enkripsi

Beberapa aplikasi website yang memiliki kelemahan seperti yang telah diuraikan dan akan diteliti ditampilkan dalam bentuk tabel berikut ini.

Tabel 2 3 Informasi Kelemahan

Nama	Kelemahan	Jenis Kelemahan
Wordpress Plugin Mac Photo Gallery 2.7	Tidak terdapat verifikasi terhadap file yang dikirimkan.	*File Upload*
Wordpress Plugin Asset Manager 0.2	Tidak terdapat verifikasi terhadap file yang dikirimkan.	
Wordpress Plugin AllWebMenus < 1.1.9	Fitur update dengan menggunakan file kompresi zip dapat dieksekusi oleh siapa saja.	
Wordpress Plugin LearnDash 2.5.3	Fitur upload melakukan pemotongan string ekstensi file yang bisa dimanfaatkan dengan ekstensi ganda.	
Wordpress Plugin Insert PHP < 3.3.1	Program gagal melakukan validasi terhadap hak pengguna terhadap id posting.	*PHP Code Injection*
Wordpress Plugin W3 Total Cache 0.9.2.3	Tag khusus dengan nama "mfunc" mempunyai fungsi spesial untuk penambahan kode php.	
Joomla Component com_civicrm 4.2.2	Pembuatan file dengan fungsi *fwrite* yang bisa dieksekusi siapa saja.	
Wordpress Plugin Ultimate Product Catalog <= 4.2.24	Fungsi *unserialize* langsung diberi parameter nilai cookie tanpa validasi.	*PHP Object Injection*
Joomla! 1.5 < 3.4.5 'x-forwarded-for'	Tidak terdapat verifikasi terhadap data browser yang dimasukkan ke	

1. Web Application Firewall

Web Application Firewall (WAF) adalah firewall untuk aplikasi HTTP. Menerapkan seperangkat aturan terhadap permintaan atau keluaran HTTP. Umumnya, aturan ini mencakup serangan umum seperti cross-site scripting (XSS) dan SQL injection. Sementara proxy umumnya melindungi klien, WAFs melindungi server. WAF digunakan untuk melindungi aplikasi web atau kumpulan aplikasi web tertentu. WAF bisa dianggap sebagai reverse proxy. WAF bisa berbentuk alat, plugin server, atau filter, dan mungkin disesuaikan dengan aplikasi. Upaya untuk melakukan kustomisasi dapat menjadi signifikan dan perlu dipertahankan menyesuaikan dengan perubahan yang dilakukan pada aplikasi.

2. ModSecurity

ModSecurity adalah open source, cross platform web application firewall (WAF) yang dikembangkan oleh Trustwave's SpiderLabs. ModSecurity memiliki bahasa pemrograman berbasis event yang kuat yang memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP, logging dan analisis secara real-time. Dengan lebih dari 10.000 penyebaran di seluruh dunia, ModSecurity adalah WAF yang paling banyak digunakan Skenario paling penting penggunaan ModSecurity adalah :

- ✓ **Real-time application security monitoring and access control**, ModSecurity memberi akses ke arus lalu lintas HTTP secara real-time, beserta kemampuan untuk memeriksanya. Dengan tambahan mekanisme penyimpanan permanen ModSecurity, dapat dilakukan pelacakan elemen sistem dari waktu ke waktu dan melakukan korelasi peristiwa. Karena ModSecurity menggunakan permintaan dan penyangga respons penuh, maka dapat dilakukan pemblokiran
- ✓ **Full HTTP traffic logging Web server**, secara tradisional menyimpan sangat sedikit log yang mengandung informasi untuk keamanan dan bahkan dengan melakukan konfigurasi khusus tidak bisa didapatkan semua informasi yang dibutuhkan. ModSecurity menyediakan kemampuan untuk mencatat apapun yang dibutuhkan, termasuk data transaksi mentah, yang penting untuk forensik. Selain itu, bisa dipilih transaksi yang akan disimpan, bagian mana dari transaksi yang masuk, dan komponen mana yang disterilkan.
- ✓ **Continuous passive security assessment,** Penilaian keamanan aktif sebagian besar merupakan kegiatan yang terjadwal, di mana tim independen bersumber untuk mencoba melakukan serangan simulasi. Penilaian keamanan pasif terus menerus adalah variasi pemantauan real-time, di mana berfokus pada perilaku pihak eksternal, dengan mengamati

perilaku sistem itu sendiri. Hal ini adalah sistem peringatan dini yang bisa mendeteksi jejak kelainan perilaku sistem dan kelemahan keamanan sebelum dieksploitasi

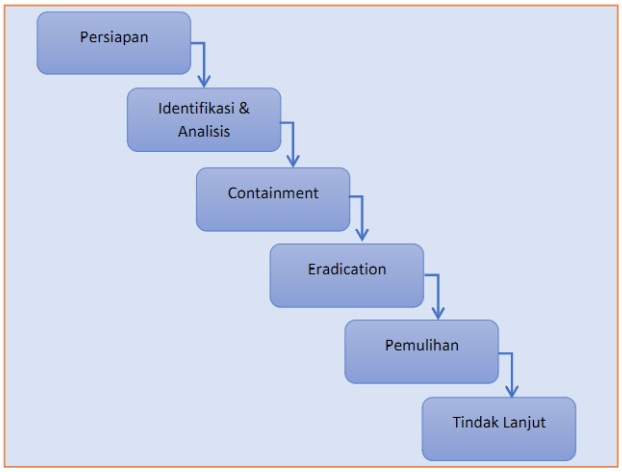
- ✓ **Web application hardening** Salah satu kegunaan ModSecurity adalah digunakan untuk mempersempit data HTTP yang diterima, misalnya metode, header, jenis konten dan lain – lain. Dengan ModSecurity mungkin juga dilakukan perbaikan masalah manajemen sesi, serta kerentanan pemalsuan data pada lalu lintas situs.

PROSEDUR PENANGANAN SERANGAN SQL INJECTION

Penanganan serangan SQL Injectionditujukan utuk mencapai hal-hal sebagai berikut:

a.Mengumpulkan informasi sebanyak mungkin tentangserangan SQL Injection;
b.Menghalangi atau mencegah eskalasi kerusakan yang disebabkan olehserangantersebut;
c.Mengumpulkan bukti terkait serangan SQL Injection;
d.Mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya serangan SQL Injectiondi masa depan.

Supaya tujuan diatas dapat terlaksana dengan baik, maka penanganan terhadap serangan SQL Injectiondilakukan dalam beberapa tahapsebagai berikut:



Gambar 1. Tahap Penanganan Serangan *SQL Injection*

Dalam melakukan penanganan serangan SQL Injection, perlu adanya tahap persiapan dengan prosedur sebagai berikut :

a)Pembentukan tim respon. Timdapat berasal dari institusi yang mengalami serangan(internal) atau juga bisaberasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang SQL Injectiondan memiliki kemampuan penanganannya;
b)Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan SQL Injection.Dokumen ini antara lain adalah :-Panduan penanganan insiden serangan siber;-Formulir penanganan insiden serangan siber;-Diagram yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun website (web server, aplikasi web, daftar user, diagram network).c)Menyiapkan tool dan media yang dibutuhkan untuk penanganan.MMisalnya Notepad ++ untuk membaca log, IDS/IPS, SQL Map, Accunetix /Nessus

Pada tahap identifikasi dan Analisis dilakukan proses identifikasi untuk memastikan telah terjadi serangan SQL Injectiondan mendeteksi sumbernya.Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain:

a.Memeriksaalertdan anomaliesdari perangkat IDS atau IPS;
b.Melakukan error checking melalui form atau url dengan memberikan karakter atau sebuah simbol. Misalnya:
•Melalui form login, memasukan pada username dan password berupa karakter-karakter yang digunakan SQL Injection, seperti:OR 1=1 – OR 1=2 --OR 'a'='a'
•Melalui url, menambahkan karakter-karakter yang digunakan SQL Injection, seperti single quote, double minus.
c.Memeriksa semua log (error log, access log, database log, firewall log).Lokasi log file secara default berada pada var/log, log tersebut menyimpan seluruh aktivitas yang terjadi pada sistem;
d.Memeriksa adanya command line, string-string yang digunakan untuk menyerang;
e.Memeriksa isi database untuk mencari script yang berbahaya, dan mengecek apakah ada penambahan user secara tidak sah;
f.Memeriksa apakah ada file atau script berbahaya (trojan, malicious file, backdoor) yang ditanamkan pada web server;
g.Menggunakan tool untuk memeriksa kerentanan. Tool yang dapat digunakan diantaranya Acunetix, SQLMap, SQL Injectiontools.

Mengukur dampak dari terjadinya SQL Injectionadalah a.Terhadap kelangsungan proses bisnis, indikatornya adalah seberapa besar dari fungsi-fungsi bisnis yang terdapat pada websitemengalami gangguan;b.Terhadapsistem dan informasi, apakah penyerang melakukan distribusi malware, membuat backdooratau melakukan web defacement. Selain itu, apakah ada data daninformasi yang berubah atau terhapus.

Tahap Eradication pada penanganan serangan SQL Injectionadalah untuk menghapus file /script serta menutup sumber serangan. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut:a.Memeriksa apakah terdapat malicious file, backdoor, rootkit atau kode-kode berbahaya lainnya yang berhasil ditanamkan pada server dan segera menghapusnya;b.Jika terdapat kode SQL yang mengakses IP tertentu maka perlu melakukan block /menutup sumber serangan(block IP dan Port).

Tahap Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Prosedur yang dapat dilakukan sebagai berikut:

a.Mengubah kredential password pengguna. Hal iniuntuk mengantisipasi apabila password pengguna telah diketahuioleh penyerang;
b.Melakukan recovery database pada aplikasi web;
c.JikaSQL Injection menyebabkanweb defacement, gunakan panduan penanganan insiden web defacement;
d.Jika SQL Injection menyebabkan insiden malware, gunakan panduan penanganan insiden malware;
e.Menutup semua kerentananyang telah diketahui;
f.Membatasi akses root langsung ke database;
g.Melakukan filter terhadap input yang dimasukkan oleh pengguna;
h.Mematikan atau menyembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan;
i.Patching terhadap aplikasi yang rentan, melakukan upgrade terhadap aplikasiwebyang masih memiliki kerentanan;
j.Melakukan penetration testing untuk mengetahui celah-celah keamanan yang mungkin masih terdapatpada website

Kesimpulan

Tenik hacking dari SQL Injection merupakan teknik yang cukup popoler pada website dengan prinsip untuk melewati perintah dari statment SQL yang di eksekusi oleh database backend. Apabila inputan user tidak disaring dengan sempurna maka akan sangat mudah untuk hacker menerobos masuk kedalam. Keamanan perlu ditingkatkan dengan cara selalu mengecek code program yang dibuat, kesalahan dalam statment SQL dapat memicu terjadinya web tersebut akan mudah diterbos masuk. Kepekaan kita harus ditingkatkan bila ingin melindungi web yang sedang diolah agar kenyamanan web dan privasi web terjamin dengan sempurna dan juga selalu mengikuti dan menerapkan Prosedur Penanganan Serangan Sql Injection.

Referensi:

https://cloud.bssn.go.id/s/Ho2B9xdfPjB89Kq#pdfviewer
https://eprints.akakom.ac.id/8085/3/3_175410054_BAB_II.pdf

Ancaman dan Bahaya Malware pada Organisasi

Reynaldi
Jurusan Magister Tehnik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma
Palembang, Indonesia
scarlettorey@gmail.com

Abstrak- Dizaman yang serba teknologi ini Internet sudah menjadi kebutuhan penting bagi masyarakat dunia, dan tentunya bagi organisasi juga. Pengunaan internet dapat memudahkan dalam menjalankan kegiatan organisasional. Namu dari segala kemudahan yang diberikan itu terdapat ancaman dan bahaya dari program-program yang sengaja di buat untuk merusak dan juga mengganggu proses berjalannya kegiatan operasional. Program-program tersebut adalah malware yang sengaja di buat bertujuan untuk merusak dan mengganggu kerja sistem operasi sebuah perangkat komputer.

Oleh karna itu, penulis ingin memberikan edukasi terhadap akan bahayanya malware pada yang tidak hanya berbahaya bagi perangkat komputer tingkat individual namun juga berbahaya bagi tingkat organisasi.

Kata Kunci : *Malware, Organisasi, Threat and danger*

I. Pendahuluan

Hampi seluruh aspek kehidupan manusia saat ini tidak dapat lepas dari kemajuan teknologi di zaman sekarang, khususnya teknologi computer, hal ini dapat dilihat dari penggunaan computer yang semakin meluas, kemajuan teknologi informasi dan komunikasi mempunyai pengaruh pada perkembangan pengolahan data, data dari satu tempat dapat dikirim ke tempat lain dengan alat telekomunikasi. Begitu pula cara kerja pengiriman data suatu organisasi untuk menjalankan proses kegiatan perkantoran .

Jaringan internet merupakan media atau teknologi yang sangat berguna pada masa ini, hampir semua orang yang menggunakan alat elektronik yang dapat tehubung kedalam jaringan internet. Dengan adanya aringan internet ini, orang-orang dapat mengakses dunia maya dengan mudah, baik dalam melakukan browsing ataupun streaming.

Tetapi banyak orang-orang yang tidak menyadari akan bahaya dan ancaman dari penggunaan jaringan internet itu sendiri dan bahkan terkesan menyepelehkan ancaman yang dapat terjadi ini, padahal ancaman dan bahaya dari malware ini dapat menyebabkan kerugian yang sangat besar untuk struktur organisasional jika tidak di tangani dengan baik.

II. Tinjauan Pustaka

Untuk melengkapi pengetahuan penulis mengenai latar belakang tentang Malware, penulis melakukan tinjauan literatur. Studi literatur bersumber dari artikel di internet, materi kuliah yang mendukung, buku–buku yang berkaitan.

A. Malware

Malicious Software atau seting disebut dengan *malware* .merupakan suatu program yang bertujuan untuk merusak, mengambil atau mengubah data-data yang dimiliki orang lain dengan tujuan tertentu, agat informasi-informasi yang didapat dimanfaatkan untuk kejahatan (Arifanto, 2009:1)

Malware memiliki beberapa klasiikasi umum, contohnya seperti: Virus, Worm dan Trojan. Sedangkan jenis lainnya sepertiL Backdoor, Adware, Keyloger dan lainnya, masuk ke dalam sub jenis dari Virus, worm dan trojan.

Pada awalkemunculan *Malware* (virus, worm, dan trojan) dalam jaringan telah berevolusi melalui serangkaian inovasi yang berkelanjutan, sehingga menyebakan penyraran semaik luas.

B. Jenis-jenis *Malware*

Virus

Inilah istilah yang sering dipakai untuk seluruh jenis perangkat lunak yang mengganggu komputer. Bisa jadi karena inilah tipe malware pertama yang muncul. Birus bisa bersarang dibanyak tipe file. Tapi ole dibilang, target utama virus adalah file yang bisa dijalankan seperti EXE COM dan VBS, yang menjadi bagian dari suatu perangkat lunak. Boot sectorjuga bisa diadikan sarang oleh virus. Penyebaran ke komputer lain dapat dilakukan dengan bantuan pengguna komputer, saat file yang terinfeksi dijalankan di komputer lain itu akan terinfeksi pula. Virus mencari file lain yang bisa diserangnya dan kemudian ersarang disana. Bisa juga virus menyebar melalui jaringan peer-to-peer yang sudah tak asing figunakan untuk berbagi file.

Worm

Worm alias cacing, begitu sebutanya. Kalau virus bersarang pada suatu program atau dokumen, cacing-cacing ini tidak demikian. Cacing adalah sebuah program yang berdiri sendiri dan tidak membutuhkan sarang untuk menyearkan dairi. Hebatnya lagi, melalui jaringan, cacing bisa "bertelur" di komputer-komputer yang terhubung dalam suatu kerapuhan (vulnerability) dari suatu sistem, biasanya sistem operasi. Setelah masuk kedalam suaru komputer, wormmemodifikasi beberapa pengaturan di sistem operasi agar tetap hidup. Minimal, ia memasukkan diri dalam proses boot suatu komputer. Lainnya mungkin mematikan akses ke situs antivirus, menonaktfkan fitur keamanan di sistem dan tindakan lain.

Trojan Horse

Kuda Troya adlaah malware yang seolah-olah merupakan yang erguna, menghibur dan menyelamatkan, padahal dibalik itu, ia merusak. Kuda ini bisa ditunggangi oleh malware lain seperti virus, worm, spyware. Kuda troya dpat digunakan untuk menyebarkan atau mengaktifkan mereka.

III. Hasil dan Pembahasan

Malware adalah program yang dirancang dengan tujuan untuk masuk dan menyusup ke sebuah sistem komputer, yang akan merusak sistem komputer tersebut. Malware dapat masuk kebanyak komputer melalui jaringan internet seperti email, download dari internet, atau melalui program yang terinfeksi, malware bisa menyebabkan kerusakan pada sistem komputer, data dan kemungkinan juga terjadi pencuarian data/informasi. Hal ini yang umum penyebab malware adalah mendownload software dari situs ilegal yang disisipkan malware. Malware mencakup virus, worm trojan horse, sebagian besar rootkit, spyware, ransomware, dan lain-lain.

Ada beberapa tanda-tanda adanya kehadiran Malware pada komputer yang dapat kita lihat sendiri:

1. PC selalu Crash :
   Kesalah sistem berefek sama uruknya dengan virus karena dapat memaksa windows mogok kerj. Akiatnya muncul laporan file-file yang hilang atau rusak, sistem hang, ahkan PC yang merestart sendiri. Masalah diatas bisa disebabkan malware yang diprogram buruk sehingga menimbulkan konflik dalam sistem file.
2. Anomali lalu lintas internet :
   Adanya lalu lintas data aktif via jaringan atau koneks internet yang dilihat melalui "windows task manager I Network" bisa menjadi indikasi adanya malware. Sekarang ini semakin jarang malware yang hanya merusak system file. Lebih banyak yang mengirim data pengguna ke pembuat virus, mendownload malware lain dari internet atau mengirim spam dari PC anda.
3. PC menjadi lumpuh :
   Fenomena ini mungkin sering dualami banyak pengguna windows. Seiting waktu, PC menjadi semakin lambat. Oot berlangsung lebih lama, setelah start, windows meload semakin banyak me-load data/ memang, setiap malware juga menghabiskan resources dan membebani system. Namun sejak pertam kali digunakan, PC pun mengumpulkan banyak program penghambat PC yang memenuhi registry, folde autorun, dan mem-fragmentasi hard disk.
4. Browser Berperilaku Aneh :
   Browser mendadak membuka sebuah halaman start lain, toolbars baru muncul dalam iconbar, dan pop up windows iklan yang selalu muncul dengan cara-cara itu malware berusaha memancing pengguna ke wabsite yang telah dipersiapkan untuk mencuri data login atau menyusupkan malware lain ke pc.

Selain tanda-tanda adanya kehadiran Malware adapula bagaiman cara penanggulangan Malware

1. Tidak mengupload lagi file-file website yang telah terinfeksi malware, dan tidak melakukan pembersihan script, sebaiknya tidak di upload ulang, karena hal tersebut masih akan terdeteksi virus dan website anda di blokir oleh google lagi.
2. Gunakan dan selalu update driver antivrus dengan adanya antivirus yang terupdate, malware baru dapat dikenali. Semakun tahun berganti, Trojan dan variannya semakin berkembang dan semakin intens dalam penyebarannya. Karena itu sebaiknya lengkapi PC/Laptop anda dengan update info-info terkini. Tidak perlu tahu terlalu detail, cukup mengena; scara general dan mengerti trend penyebaran.
3. Ubah password, malware mungkin sudah mengetahu passwrd anda sebaikna password siubah secara berkala. Password tersbut meliputi password akun window, password email, FTP, Administator website, Cpanel dan lain-lain.
4. Update perangkat lunak, dan sistem operasi, akan mentup celah ekamanan, celah yang tadinya bisa funakan amlware untuk masuk bisa ditutupi, pada saat ini kebanyakan sistem operasi dan perangkat lunak telah menyediakan fasilitas update secara automatis.
5. Melalkukan filter atas infromasi dan data yang diterima, dunia internet yang amat luas memungkinkan informasi mengalir demikian cepat. Melompati batas-batas negara dan perundangan. Tapi tidak semua informasi dan data dipercaya. Gunakan sellau akal sehat, ratio dan pemikiran yang

matang ketika melakukan justifikasi. Kumpulkan data sebnyak munkin lalu bandingkan seobjektif mungkin

6. Gunakan antispyware, spyware merupakan turunan dari adware, yang memantau kebiasaan pengguna dalam melakukan perjalanan atau penejelajahan internet dan pada umumnya bisa erupa virus.
7. Backup file, backup file ke media lain seperti CD, DVD, atau hard disk eksternl sehingga data tak akan terganggu meskiun komputer terserang malware.

VI. Daftar Pustaka

[1] Agus Tedyyana danSupria, 2018,Perancangan Sistem Pendeteksi dan Pencegahan Malware melalui SMS Gateway, RIAU, Teknik Infromatika, Politeknik Negeri Bengkalis;

[2] Harjono, 2013,Deteksi Malware dalam jarinan menggunakan DIONAEA, Puwokerto,Universitas Muhammadiyah Purwokerto;

[3] Ismail dkk, 2015,Tugas Besar Etika Profesi , Surabaya, Institut Bisini dan Infromasi STIKOM;

Undang-Undang ITE Sebagai Perlindungan Dari Serangan Web Deface Serta Cara Pencegahannya

Rio Permata
Magister Teknik Informatika
Universitas Bina Darma Palembang
riopermata@gmail.com

Abstrak

Cybercrime atau kejahatan dunia maya tercipta akibat penyalahgunaan teknologi. Perkembangan teknologi yang semakin berkembang tentu bertujuan memberikan kemudahan dalam membantu manusia dalam aktifitas sehari-hari. Meskipun demikian, sebagian orang memanfaatkan untuk tujuan yang negatif. Banyak sekali macam cybercrime, dan salah satunya adalah defacing. Defacing merupakan kejahatan yang mengubah tampilan website orang lain tanpa izin baik sebagian ataupun menyeluruh dengan menerobos sistem orang lain terlebih dahulu. Menurut Undang- undang No.19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (UU ITE) defacing merupakan perbuatan dilarang yaitu pada Pasal 30 dalam aktifitas menerobos sistem orang lain tanpa izin dan Pasal 32 ayat (1) pada aktifitas memodifikasi website tanpa hak. Pada tulisan kali ini akan dibahas peran UU ITE sebagai perlindungan dari serangan web deface serta bagaimana cara pencegahannya agar terhindar dari serangan tersebut

Kata Kunci:
Web Deface , UU ITE, Etika IT

1. Pendahuluan

Kemajuan teknologi merupakan sesuatu yang tidak bisa kita hindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan peradaban, teknologi dan ilmu pengetahuan. Internet dengan kelebihan-kelebihannya mempunyai sisi kelemahan dan memiliki dampak buruk jika dipergunakan orang yang tidak bertanggungjawab. Adanya *cyberspace* memberi peluang terjadinya kejahatan atau lebih dikenal dengan *cybercrime* (kejahatan dunia maya), banyak sekali jenis *cybercrime* salah satunya adalah *defacing*.

Defacing yang merupakan salah satu kejahatan dunia maya yaitu kegiatan merubah tampilan suatu *website* orang lain tanpa izin baik halaman utama atau *index file*nya ataupun halaman lain yang masih terkait dalam satu *URL* dengan *website* tersebut (bisa di *folder* atau di *file*). *Defacing* terdiri dari dua tahap, yaitu mula-mula menerobos system orang lain atau kedalam *web server* dan tahap kedua adalah mengganti halaman *website (web page)*.

Telah banyak kasus *defacing* yang telah terjadi di luar negeri dan dalam negeri. Contoh kasus yang terjadi di Indonesia seperti yang dilakukan oleh Dani Hermansyah pada tanggal 17 April 2004, pada waktu itu UU ITE belum di buat dan disahkan. Nama- nama partai diubah dengan nama-nama buah dalam *website* www.kpu.go.id yang mengakibatkan berkurangnya kepercayaan masyarakat terhadap pemilu yang sedang berlangsung pada saat itu.

Contoh lain yang cukup menghebohkan, seperti pada tanggal 26 maret 2008 situs Depkominfo telah dibobol, Pembobolan tersebut di duga berkaitan dengan pengesahan RUU tentang Informasi dan Transaksi Elektronik (ITE) sebagai Undang-undang oleh DPR. Selain terdapat pula *defacing* situs resmi mantan presiden SBY,*defacing* pada *website* TV One, *defacing* situs resmi kepolisian yang beralamat http://www/polri.go.id dan lain sebagainya.

Sebagaimana gambaran dan contoh kasus *defacing* di atas maka agar hal tersebut tidak terjadi lagi, diperlukan perangkat hukum yang mengatur hal itu. Oleh karena itu, dengan dibentuknya Undang-undang Nomor 11 Tahun 2008 jo Undang- undang Nomor 19 tahun 2016 tentang Informasi dan Transaksi Elektronik oleh pemerintah yang disahkan pada tanggal 28 April 2008 dan perubahannya pada tanggal 25 November 2016, diharapkan agar semua kejahatan mayantara dapat terakomodir oleh Undang-undang tersebut, termasuk *defacing* yang telah diatur di dalamnya.

2. Tinjauan Pustaka

2.1. Pengertian *Cyber Crime*

Pada dasarnya *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai sarana atau media yang didukung oleh sistem telekomunikasi, baik menggunakan telepon atau *wireles system* yang menggunakan antena khusus yang nirkabel. Hal inilah yang disebut "telematika" yaitu konvergensi antar teknologi telekomunikasi, media dan informatika yang semula masing-masing berkembang secara terpisah.

Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut dengan *cyber crime*. Dari pengertian ini tampak bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif aplikasi internet.

2.2. *Defacing*

Menurut istilah, *defacing* adalah teknik mengganti atau menyisipkan file pada server. Teknik ini dapat dilakukan karena terdapat lubang pada sistem *security* yang ada didalam sebuah aplikasi atau *website*. Hal ini bertujuan untuk melakukan perubahan tampilan pada website korban dengan tampilan yang dimiliki oleh si *defacer*. *Defacing* terdiri dari dua tahap, yaitu mula-mula menerobos system orang lain atau kedalam *web server* dan tahap kedua adalah mengganti halaman *website (web page)*.

Serangan dengan tujuan utama merubah tampilah sebuah *website*, baik halaman utama maupun halaman lain terkait dengannya, diistilahkan sebagai "*Web Defacement*". Hal ini biasa dilakukan oleh para "attacker" atau penyerang karena merasa tidak puas atau tidak suka kepada individu, kelompok, atau entitas tertentu sehingga *website* yang terkait dengannya menjadi sasaran utama.

2.3. Jenis-Jenis *Defacing*

Defacing dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait:

1. *Full of page*

   Artinya mendeface satu halaman penuh tampilan depan alias *file index* atau *file* lainnya yang akan diubah secara utuh, artinya untuk melakukan ini biasanya seorang '*defacer*' umumnya harus berhubungan secara 'langsung' dengan *box* (mesin) atau usaha mendapatkan *priveleged* terhadap mesin, baik itu *root account* atau sebagainya yang memungkinkan *defacer* dapat secara Interaktif mengendalikan file indek dan lainnya secara utuh. Umumnya dengan memanfaatkan kelemahan kelemahan pada *services-services* yang berjalan di mesin, sehingga dapat melakukan pengaksesan ke mesin.

2. Sebagian atau hanya menambahi

   Artinya, *defacer* mendeface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan *script-script* yang mengganggu, hal ini umumnya hanya akan memperlihatkan tampilan *file* yang di *deface* menjadi kacau dan umumnya cukup mengganggu, *defacer* biasanya mencari celah baik dari kelemahan *scripting* yang digunakan dengan *XSS injection*, bisa dengan *SQL* atau *database injection* dan juga beberapa *vulnerabilities* yang seringkali ditemukan pada situs-situs yang dibangun dengan menggunakan *CMS* (*Content Manajemen System*)

3. Pembahasan

3.1. Tindak Pidana *Defacing* Menurut Undang-Undang No. 19 Tahun 2016

Berdasarkan kasus-kasus *Cyber Crime* yang kian marak pemerintah mengambil tindakan hukum di Indonesia dengan membuat Undang-Undang Informasi transaksi (UU ITE) dengan maksud agar membuat para pelaku tindak kejahatan di dunia maya (*Cyber Crime*), dengan membuat rasa nyaman dan aman untuk para pengguna internet.

Adapun dalam UU No.19 Tahun 2016 berkaitan dengan tindak pidana *Defacing* merupakan perbuatan dilarang yang telah diatur pada Pasal 30 dalam hal *illegal acces* dan pada Pasal 32 ayat (1) dalam hal *data interference* mengingat langkah awal dalam *defacing* adalah melakukan *hacking* kemudian memodifikasi dari *website* tersebut. Mengenai Perundangan dunia maya (*defacing*) yang masuk ranah tindak kejahatan dunia maya (*cyber crime*) diatur dalam BAB VII mengenai PERBUATAN YANG DILARANG dalam UU No.11 Tahun 2008 jo UU No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. Maka para pelaku akan di jerat dalam pasal sebagai berikut:

Pasal 30 yang berbunyi :

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau Sistem Elektronik milik orang lain dengan cara apapun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses computer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh informasi Elektronik dan/atau Dokumen Elektronik.

(3) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengkases computer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol system pengaman.

Pasal 32 ayat (1) yang berbunyi:

(2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambahkan, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.

3.2. Sanksi Tindak Pidana *Defacing* Menurut Undang- Undang No. 19 Tahun 2016

Adapun ketentuan pidana dari pasal-pasal tersebut diatas mengenai tindak kejahatan Perundangan dunia maya (*Defacing*) diatur dalam BAB XI KETENTUAN PIDANA dalam UU N0.11 Tahun 2008 jo UU No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik yaitu:

Pasal 46 ayat (1) yang berbunyi:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp.600.000.000,00 (enam ratus juta rupiah).

(2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/ atau denda paling banyak Rp.700.000.000,00 (tujuh ratus juta rupiah).

(3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp.800.000.000,00 (delapan ratus juta rupiah).

Pasal 46 ayat (1) yang berbunyi:

(1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/ atau denda paling banyak Rp.2.000.000.000,00 (dua miliar rupiah).

Defacing menurut UU ITE merupakan perbuatan dilarang yang telah diatur pada Pasal 30 dalam hal *illegal acces* dan pada Pasal 32 ayat (1) dalam hal *data interfence* mengingat langkah awal dalam *defacing* adalah melakukan *hacking* kemudian memodifikasi dari *website* tersebut. Sanksi hukum *defacing* di Indonesia sudah jelas diatur pada Pasal 46 dan Pasal 48 ayat (1) UU ITE.

Dengan adanya Undang-Undang yang mengatur mengenai *cyber crime* khusus nya *defacing* akan membuat pengguna internet menjadi terlindungi serta memberikan rasa aman dan kepastian hukum.

3.3. Pencegahan Dari Serangan *Web Deface*

Untuk mencegah agar terhindar dari serangan *web deface* ada beberapa cara yang dapat dilakukan yaitu :

1. Gunakan firewall untuk menjaga dari akses orang yang tidak bertanggung jawab. Firewall bekerja dengan mengamati IP yang masuk, sehingga jika ada IP yang mencurigakan bisa dicegah sedari awal.
2. Lakukan backup website secara berkala agar aman saat terjadi suatu hal yang tidak diinginkan.
3. Lakukan update software serta aplikasi ke versi yang paling terbaru.
4. Jangan menggunakan default konfigurasi saat membuat username, password dan keperluan website lainnya.
5. Gunakan plugin keamanan tambahan untuk mencegah website defacing pada website. Contoh plugin WordPress seperti Sucuri, Wordfence, iThemes Security, AIO WP Security.
6. Gunakan tool penetration test untuk mengetahui seberapa amankah website. Contoh tool yang bisa gunakan seperti Nexus, Acunetix dan lain sebagainnya.

4. Kesimpulan dan Saran

Berdasarkan pembahasan diatas dapat ditarik kesimpulan sebagai berikut :

1. *Defacing* menurut UU ITE merupakan perbuatan dilarang yang telah diatur pada Pasal 30 dalam hal *illegal acces* dan pada Pasal 32 ayat (1) dalam hal *data interfence* mengingat langkah awal dalam *defacing* adalah melakukan *hacking* kemudian memodifikasi dari *website* tersebut. Sanksi hukum *defacing* di Indonesia sudah jelas diatur pada Pasal 46 dan Pasal 48 ayat (1) UU ITE.
2. Pencegahan terhadap serangan *Web Defacing* dapat dilakukan dengan beberapa cara.

Dari pembahasan diatas juga dapat diambil beberapa poin sebagai bahan evaluasi dan saran yaitu :

1. Bagi Pengguna Internet
   Hendaknya pengguna internet mematuhi norma dan etika di dunia maya dan tidak melanggar Undang-undang yang berlaku karena jika melanggar Undang-undang maka dapat dikategorikan sebagai tindak kejahatan yang terdapat sanksi hukum bagi yang melanggar.
2. Bagi Pemerintah
   a. Hendaknya pemerintah lebih menyempurnakan lagi UU ITE.
   b. Hendaknya pemerintah meningkatkan sistem pengamanan jaringan komputer nasional dan meningkatkan pemahaman serta keahlian aparatur Negara mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan kejahatan dunia maya
   c. Hendaknya pemerintah meningkatkan kesadaran warga Negara mengenai kejahatan dunia maya serta pentingnya mencegah kejahatan tersebut dan meningkatkan kerjasama antar negara dalam upaya penanganan kejahatan mayantara

Daftar Pustaka

[1] M. Ade Chairuddin Najib.(2018). “Sanksi Terhadap Tindak Pidana Defacing Dalam Undang-Undang No.19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik Dengan Perspektif Hukum Islam”. Skripsi. Palembang : UIN Raden Fatah.

[2] Budi Agus Riswandi, Hukum Internet di Indonesia, (Yogyakarta: UII Press, 2003

[3] Dikdik M.Arief Mansur dan Elisatris Gultom, Cyberlaw Aspek Hukum Teknologi Informasi, cet. II (Bandung: Refika Aditama, 2009)

[4] Sutan Remi Syahdeini, Kejahatan dan Tindak Pidana Komputer, (Jakarta: Pustaka Utama Grafiti, 2009)

[5] Budi Surhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime), (Jakarta: Raja Grafindo Persada, 2013)

[6] Maskun, Kejahatan Siber (Cyber Crime) Suatu Pengantar, (Jakarta: Kharisma Putra Utama, 2013)

[7] Qwords.(2020).”Apa itu Deface Website, Jenis dan Cara Mengatasinya” https://qwords.com/blog/apa-itu-deface-website/ (Diakses tanggal 25 Mei 2020)

Nama : Yudistira Sira Permana
NIM : 182420104
Kelas : MTI 20A

MALWARE

Malware adalah singkatan dari malicious software. **Malware sendiri adalah sebuah software yang dirancang dengan tujuan untuk membahayakan, menyusup, atau merusak sebuah komputer.** Malware juga biasa didefinisikan sebagai kode berbahaya. Software ini bisa melumpuhkan atau mengganggu operasi sebuah sistem, memungkinkan hacker untuk mendapat akses ke informasi rahasia dan sensitif serta memata-matai komputer serta pemilik komputer itu sendiri.

Malware dibuat secara khusus agar tersembunyi sehingga mereka bisa tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut. Biasanya, mereka menyamarkan diri menjadi program yang bersih.

Efek dari malicious software biasa jauh lebih berbahaya bagi corporates dibanding untuk personal user. Jika malware menyerang jaringan sistem Anda, mereka bisa menyebabkan kerusakan dan gangguan yang meluas, yang memerlukan upaya pemulihan ekstensif di dalam organisasi.

Malware dapat menginfeksi komputer dengan masuk melalui email, hasil download internet, dan program-program yang sudah terinfeksi.

Kebanyakan kejahatan komputer yang sering terjadi adalah pencurian informasi personal atau pembentukan sebuah backdoor ke komputer Anda dimana seseorang bisa mendapatkan akses ke komputer Anda tanpa sepengetahuan dan izin Anda. Software yang membantu orang-orang untuk melakukan hal-hal ini tanpa seizin Anda bisa dianggap sebagai malware.

Malware juga memiliki beberapa nama lain seperti badware dan di dokumen legal, malware lebih sering disebut sebagai computer contamination (kontaminasi sistem komputer). Sehingga apabila Anda melihat kata itu, itu hanyalah cara lain untuk menyebut malware.

Jenis-Jenis Malware

Menemukan kata yang dimulai dengan mal adalah tanda bahwa ada sesuatu yang buruk. Seperti yang sudah disebutkan di atas, kebanyakan ahli melihat istilah malware sebagai kontraksi dua kata – malicious software (perangkat lunak berbahaya). Kata itu memiliki konotasi buruk dengan konstruksi yang disengaja, namun psikologi sebenarnya dari malware sedikit kurang jelas.

Itu karena ada berbagai macam software berbahaya yang dapat Anda temukan dan hadapi, dengan jenis dan kategori ancaman baru muncul, apalagi di saat dunia bergerak menuju masa depan digital.

Sebuah penelitian menemukan bahwa **jenis malware yang paling umum sekarang adalah Trojans dan worms,** dengan virus mengalami penurunan dalam jumlah. Sementara itu di tahun ini, malware juga ditemukan sudah menargetkan mobile devices seperti smartphones dan tablets. Bahkan, ada malware yang sudah di pre-install di devicenya sendiri.

Lalu apa saja jenis-jenis Malware dan bagaimana mereka diklasifikasikan? Berikut adalah beberapa jenis malware.

1. **VIRUS**

   Virus sudah ada sejak lama. John von Neumann adalah orang pertama yang melakukan penelitian akademik mengenai teori replikasi diri program komputer pada tahun 1949. Contoh pertama virus, atau apa yang bisa diklasifikasikan sebagai virus, sudah dideteksi sejak tahun 70-an.

Karakteristik utama yang dimiliki sebuah software untuk memenuhi syarat sebagai virus adalah software yang mendorong untuk mereproduksi program di dalamanya. **Ini berarti jenis malware ini akan mendistribusikan salinan programnya sendiri dengan cara apapun untuk menyebar.**Ciri lain yang umum terjadi adalah mereka selalu tersembunyi di dalam sistem sehingga sulit untuk mendeteksi eksistensinya tanpa program keamanan khusus yang disebut antivirus.

Pada dasarnya, mereka datang tanpa diundang, bersembunyi di dalam sebuah sistem dan biasanya bekerja tanpa jejak yang jelas. Inilah yang membuat mereka sangat mematikan.

Mereka bersembunyi di dalam file komputer, dan komputer harus menjalankan file itu dengan kata lain, menjalankan kode itu, agar virus melakukan pekerjaan kotornya. Pada intinya, virus tidak lain hanyalah kode atau program menular yang menempel pada software lain dan biasanya memerlukan interaksi manusia untuk diperbanyak. Ini adalah bagaimana virus diklasifikasikan lebih lanjut, tergantung pada apakah mereka berada dalam binary executables, file data, atau di boot sector dari hard drive sistem tertentu.

2. WORMS

Ini adalah jenis malware yang menular. **Worm adalah sebuah software mandiri yang bereplikasi tanpa menargetkan dan menginfeksi file tertentu yang sudah ada di komputer.** Worms adalah sebuah program kecil yang mereplikasikan diri di dalam komputer untuk menghancurkan data-data yang ada di dalamnya. Mereka biasanya menargetkan file sistem operasi dan bekerja sampai drive mereka menjadi kosong.

Yang membedakan worms dari virus adalah cara kerjanya. Virus memasukkan diri mereka ke dalam file yang sudah ada sementara worms hanya masuk ke dalam komputernya.

Worms biasa muncul melalui email dan instant messages, dan mereka membatasi aktivitasnya dengan apa yang dapat mereka capai di dalam aplikasi yang membantu mereka bergerak. Mereka menggunakan jaringan komputer untuk menyebar, bergantung pada kegagalan keamanan di komputer target untuk mengaksesnya, dan menghapus data.

Banyak worms yang dirancang untuk menyebar dan tidak berusaha untuk mengubah sistem yang mereka lewati. Tetapi bahkan cara ini memiliki kemungkinan untuk menyebabkan gangguan besar dengan meningkatkan lalu lintas jaringan.

Contoh Worms adalah Melissa, Morris, Mydoom, Sasser, Blaster, and Myife.

3. TROJAN HORSES

Trojan adalah sebuah program jahat yang menyamar menjadi sebuah program yang berguna bagi komputer Anda.**Trojan disebarkan dengan menyamar menjadi software rutin yang membujuk user untuk menginstal program tersebut di PC mereka.** Istilah ini sendiri berasal dari cerita Yunani kuno tentang sebuah kuda kayu yang digunakan untuk menyerang kota Troy secara diam-diam. Trojan horses di komputer juga menggunakan cara yang sama untuk menyerang komputer Anda.

Payload bisa apa saja, tapi biasanya berupa backdoor yang memungkinkan penyerang memiliki akses ilegal ke komputer yang terkena serangan. Trojan juga memberi penjahat cyber akses ke informasi personal pemilik komputer seperti IP address, password, dan detail akun bank. Mereka bisa digunakan untuk menginstal keyloggers yang bisa dengan mudah mengambil nama akun dan password atau data kartu kredit dan memberikannya kepada penjahat cyber. Kebanyakan serangan ransomware juga dilakukan

menggunakan Trojan horse, dengan menjadi rumah bagi kode-kode berbahaya di dalam data yang sebenanya aman.

Trojans sekarang dianggap sebagai malware paling berbahaya, terutama trojans yang dirancang untuk mencuri informasi finansial pemilik komputer tersebut. Beberapa jenis Trojan yang berbahaya biasa memperkenalkan softwarenya sebagai antivirus, padahal software mereka malah membawa masalah ke komputer Anda.

Beberapa contoh Trojan horses adalah Magic Lantern, FinFisher, WARRIOR PRIDE, Netbus, Beast, Blackhole exploit kit, Gh0st RAT, Tiny Banker Trojan, Clickbot.A, dan Zeus. Selain itu, di tahun 2015, ditemukan sebuah malware untuk Android bernama Shedun yang memang menargetkan mobile devices.

4. ROOTKITS

Rootkit adalah sebuah koleksi software yang dirancang khusus untuk memperbolehkan malware untuk mengumpulkan informasi. Jenis malware ini bekerja di balik layar sehingga pengguna komputer tidak akan curiga.

Software ini bekerja seperti backdoor untuk malware agar mereka bisa masuk dan mengganggu sistem komputer Anda. Rootkit banyak digunakan oleh hackers untuk menginfeksi sebuah sistem. Ini bisa diinstal secara otomatis atau diinstal oleh penyerang saat mereka mendapat hak administrator.

Cara mendeteksi rootkit tidaklah mudah karena jenis malware ini biasanya sering bisa menumbangkan software yang menempatkannya. Menghapus rootkit juga sama rumitnya dan dalam beberapa kasus hampir tidak mungkin, apalagi jika rootkit tinggal di dalam kernel sebuah sistem operasi. Menginstal ulang OS terkadang menjadi satu-satunya solusi untuk benar-benar menyingkirkan rootkit yang sudah advance.

5. RANSOMWARE

Ransomware diidentifikasi sebagai jenis software berbahaya yang paling menghancurkan. Ransomware adalah salah satu malware yang paling advance dan terus meningkat akhir-akhir ini. **Ransomware memblokir akses ke data korban, agar bisa mengancam untuk mempublikasikannya atau menghapusnya sampai uang tebusan dibayar.** Lebih buruk lagi, tidak ada jaminan bahwa membayar uang tebusan akan mengembalikan akses ke data, atau mencegah penghapusan.

Jenis malware ini pada dasarnya menginfeksi sistem dari dalam, mengunci komputer dan membuatnya tidak berguna. Ransomware yang lebih sederhana dapat mengunci sistem yang mungkin sulit dibalikkan bagi kebanyakan orang, sementara ransomware yang lebih maju mengenkripsi file korban, membuat mereka tidak dapat diakses, dan menuntut pembayaran tebusan untuk mendekripsi file.

Serangan ransomware awalnya mendapat popularitas di Rusia, namun jenis penipuan ini sekarang semakin populer di dunia internasional. Mereka biasanya dilakukan dengan menggunakan Trojan yang dilengkapi dengan muatan yang disamarkan sebagai file yang sah.

Meskipun cara pemerasan digital ini telah digunakan sejak akhir 80-an, ini kembali menonjol pada akhir tahun 2013 dengan munculnya mata uang digital yang digunakan untuk mengumpulkan uang tebusan. Banyak vendor keamanan mengklasifikasikan ransomware menjadi ancaman cyber paling berbahaya – pendeteksian dan penghapusannya adalah proses yang rumit. Meskipun tersebar luas di platform PC, ransomware yang menargetkan sistem operasi mobile juga telah mengalami peningkatan.

Uang tebusan utama seperti Reveton, CryptoLocker, CryptoWall, dan baru-baru ini, serangan WannaCry 2017, tidak menyebabkan kehancuran kecil. Sementara Fusob,

salah satu keluarga ransomware mobile yang paling banyak digunakan, telah menggunakan taktik menakut-nakuti untuk memeras orang untuk membayar uang tebusan.

6. KEYLOGGERS

Keyloggers adalah software yang menyimpan semua informasi yang diketik dengan menggunakan keyboard. Keyloggers biasanya tidak memiliki kemampuan untuk menyimpan informasi yang dimasukkan dengan keyboard virtual dan device input lainnya, tetapi keyboard fisik memiliki resiko yang lebih besar akan malware jenis ini.

Keyloggers mengumpulkan informasi dan kemudian mengirimnya kepada penyerang. Penyerang kemudian akan mengeluarkan informasi sensitif seperti username dan password serta detail kartu kredit dari data-data yang dikumpulkan keyloggers.

7. GRAYWARE

Grayware adalah sebuah istilah yang pertama kali muncul di tahun 2004. Istilah ini digunakan untuk mendeskripsikan **aplikasi dan files yang tidak diinginkan, tetapi tidak diklasifikasikan sebagai malware, dapat memperburuk kinerja sebuah komputer dan menyebabkan risiko keamanan.** Program-program ini berperilaku menyebalkan atau tidak diinginkan, dan paling buruk, mereka memantau sistem dan memberi tahu rumah melalui telepon.

Dua jenis grayware adalah adware dan spyware. Hampir semua software antivirus komersial yang tersedia bisa mendeteksi program-program yang kemungkinan besar tidak diinginkan. Mereka juga menawarkan mode terpisah untuk mendeteksi, mengkarantina, dan menghapus malware yang menampilkan advertisements atau iklan.

- **Adware**

Meskipun software yang didukung iklan sekarang jauh lebih umum, dan dikenal sebagai adware di beberapa kalangan, kata tersebut telah dikaitkan dengan malware untuk beberapa lama. Meskipun adware bisa merujuk ke program apa saja yang didukung oleh iklan, biasanya malware tersebut menampilkan iklan dalam bentuk popup dan windows yang tidak bisa ditutup.

Ini mungkin adalah malware yang paling menguntungkan dan paling tidak berbahaya, dirancang dengan tujuan khusus menampilkan iklan di komputer Anda. Penggunaan adware semakin meningkat di ponsel, khususnya, dengan beberapa perusahaan China melakukan bundling dalam adware secara default di smartphone berbiaya rendah tertentu.

- **Spyware**

Spyware, seperti namanya, adalah software yang selalu memata-matai Anda. Tujuan utamanya adalah untuk melacak aktivitas Internet Anda agar bisa mengirim adware. Spyware juga digunakan untuk mengumpulkan informasi tentang organisasi tanpa sepengetahuan mereka, dan mengirimkan informasi tersebut ke entitas lain, tanpa persetujuan dari pemilik data.

8. BACKDOORS

Sebuah backdoor di software atau sistem komputer pada umumnya merupakan portal yang tidak terdokumentasi yang memungkinkan administrator masuk ke sistem untuk melakukan troubleshoot atau melakukan perawatan. Tapi itu juga mengacu pada portal rahasia yang digunakan hacker dan agen intelijen untuk mendapatkan akses ilegal.

Sebuah backdoor memiliki banyak arti. Ini bisa merujuk pada sebuah titik akses yang sah yang tertanam dalam sistem atau program software untuk administrasi jarak jauh.

Umumnya backdoor jenis ini tidak terdokumentasi dan digunakan untuk pemeliharaan software atau sistem. Beberapa backdoors administratif dilindungi dengan username dan password hardcoded yang tidak dapat diubah; meskipun beberapa menggunakan kredensial yang bisa diubah. Seringkali, keberadaan backdoor tidak diketahui oleh pemilik sistem dan hanya diketahui oleh pembuat software. Built-in backdoorsadministrasi membuat kerentanan pada software atau sistem yang dapat digunakan penyusup untuk mendapatkan akses ke sistem atau data.

Penyerang juga bisa memasang backdoor sendiri pada sistem yang ditargetkan. Dengan melakukan itu, mereka bisa datang dan pergi sesuka mereka dan memberi mereka akses jarak jauh ke sistem. Malware yang terpasang pada sistem untuk tujuan ini sering disebut Trojan akses jarak jauh, atau RAT (remote access Trojan), dan dapat digunakan untuk menginstal malware lain di sistem atau mengekstrak data.

9. ROGUE SECURITY SOFTWARE

Rogue Security Software, atau juga sering disebut sebagai rogue antimalware, adalah sebuah software yang terlihat seperti software bermanfaat dari perspektif keamanan, padahal tidak. Rogue Security Software menyamar sebagai software asli dan menyesatkan Anda untuk ikut serta dalam transaksi yang tidak benar. Dengan kata sederhana, **tujuan Rogue Security Software adalah menipu Anda agar percaya bahwa komputer Anda terinfeksi dengan beberapa ancaman serius, dan kemudian menipu Anda untuk menginstal / membeli software keamanan palsu.**

Program ini akan mengklaim untuk membantu komputer Anda menyingkirkan malware, sebenarnya justru sebaliknya. Mereka akan tetap berada dalam sistem dan terus-menerus mengganggu Anda tentang terinfeksi dan memaksa Anda untuk membeli solusinya (misalnya, menyarankan Anda untuk meningkatkan versi gratis program tersebut ke versi berbayar). Salah satu karakteristik penting dari software ini adalah adalah

mengaitkan dirinya jauh ke dalam sistem dan tidak dapat dengan mudah dihapus atau dihapus.

10. BROWSER HIJACKER

Browser hijacker didefinisikan sebagai sebuah software yang tidak diinginkan yang mengubah pengaturan browser web tanpa izin pengguna. Malware ini menyebabkan penempatan iklan yang tidak diinginkan ke browser dan mungkin perubahan homepage atau search page menjadi halaman hijacker. Pada dasarnya malware ini membuat pengguna mengunjungi website tertentu, tidak peduli apakah mereka mau atau tidak agar hijacker mendapat profit yang lebih besar dari iklan. Browser hijackers juga mungkin mengandung spyware untuk mendapatkan informasi bank dan data sensitif lainnya.

Nama : Adiktia
NIM : 182420101
Kelas : MTI.20.A
Mata Kuliah : Ethical Issues in Electronic Information Systems

WEB DEFACE

1. PENDAHULUAN

Penetrasi pengguna internet di Indonesia meningkat dari tahun ke tahun. Sejak 10 tahun yang lalu pengguna selalu naik minimal + 10.000.000 pengguna setiap tahunnya. Pada tahun 2018 mengalami peningkatan + 27.900.000 pengguna dibandingkan tahun 2017 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2019). Tindak kejahatan melalui media digital atau teknologi informasi dan komunikasi pun selaras dengan pertumbuhan pengguna internet, selalu mengalami peningkatan penerimaan barang bukti elektronik dan/atau digital di Kepolisian (Hariyadi, Winarno, & Luthfi, 2016).

Tindak kejahatan berupa serangan siber sepanjang tahun 2018 dengan objek pantau situs web sebanyak 16.939 serangan. Situs web dengan domain .go.id mendapat serangan terbanyak dibanding *Country Code Top Level Domain* (ccTLD) .id lainnya. Tabel 1 menunjukan persentase pemantauan insiden situs web pada tahun 2018 dengan ccTLD .id. Bentuk insiden yang terjadi pada situs web adalah *web defacement* (Indonesia Security Incident Response Team on Infrastructure / Coordination Center, 2019). Pada penelitian sebelumnya serangan *web defacement* pada situs web milik pemerintah juga pada urutan pertama berdasarkan observasi pada bulan Januari sampai dengan Juli 2014 (Mantra, 2015).

Tabel 1. Pemantauan Insiden Situs Web Tahun 2018

No	ccTLD	Persentase
1	.go.id	30.75 %
2	.ac.id	28.38 %
3.	.sch.id	12.58 %
4.	.co.id	10.92 %
5.	.id	8.25 %
6.	.or.id	2.96 %
7.	.desa.id	2.76 %
8.	.web.id	2.56 %
9.	.my.id	0.53 %
10.	.mil.id	0.11 %
11.	.biz.id	0.08 %
12.	.net.id	0.08 %
13.	.ponpes.id	0.03 %

Defacement pada situs web atau *web defacement* dapat diartikan tindakan mengubah tampilan halaman situs yang tidak semestinya oleh orang yang tidak memiliki otoritas (Romagna & Hout, 2017). Masih menurut Rogmana dan Hout serangan *web defacement* merupakan serangan yang berpotensi karena memerlukan biaya untuk memperbaikinya. Penelitian ini fokus pada pemantauan serangan *web defacement* dengan studi kasus situs web pemerintah yaitu yang memiliki domain .go.id supaya pihak pemerintah memperhatikan pembiayaan setelah pengembangan sebuah sistem berbasis web.

2. LITERATURE REVIEW

2.1.TOP-LEVEL *DOMAIN*

Domain Name System (DNS) Merupakan sistem yang berfungsi mengkoversi nama domain yang mudah diingat ke dalam bentuk IP Address dengan melakukan permintaan informasi ke sistem yang memiliki hierarki dan tersebar. Adanya DNS maka memudahkan menghubungkan sumber daya komputasi baik melalui internet maupun jaringan internal (Mockapetris, 1987). Sistem hierarki DNS tertinggi yang disebut *Root* yang melakukan pendelegasian tanggung jawab ke *Top-Level Domain (TLD)*. Contoh *Top-Level Domain* diantaranya: .com, .net, .org, .info, .online, dan .id. Organisasi nirlaba yang mengelola DNS dan IP adalah Internet Corporation for Assigned Names and Numbers (ICANN). Adapun daftar basis data *Root Zone* yang

beralamat di ftp://ftp.rs.internic.net/domain/root.zone dikelola Internet Assigned Numbers Authority (IANA), sebuah departemen di bawah ICANN (Wang, Zhang, & Xu, 2018). Berdasarkan surat Dirjen APTEL Kementerian Komunikasi dan Informatika Nomor BA–343/DJAT/MKOMINFO/6/2007 pengelolaan *Top-Level Domain* .id diserahkan dari Dirjen APTEL ke Pengelola Nama Domain Internet Indonesia (Pandi). Pandi tidak hanya mengelola *Top-Level Domain* .id, sub domain dua tingkat dibawahnya juga dikelola oleh Pandi. Adapun daftar sub domain dua tingkat yang dikelola oleh Pandi diantaranya .co.id, .ac.id, .or.id, .go.id, .my.id, .web.id, .biz.id, .net.id, .mil.id, .sch.id, .desa.id, dan .ponpes.id (Pengelola Nama Domain Internet Indonesia, n.d.).

2.2.WEB SCRAPING

Web scraping merupakan kode yang memanfaatkan teknik untuk melakukan ekstraksi informasi dengan sumber suatu halaman situs web. Informasi yang didapatkan dapat disimpan pada suatu berkas dengan format, open document spreadsheet, Microsoft Excel, Comma Separated Value, Structured Query Language, Extensible Markup Language, atau berkas teks. Kode tersebut maka disebut *web scraper* yang dibuat menggunakan bahasa pemrograman tertentu (Mishra & Pujari, 2011). Pada penelitian ini bahasa yang digunakan untuk melakukan *scraping* situs web adalah Python. Istilah lain dari *web scraping* juga dikenal sebagai *screen scraping*, *web data extraction* atau *web harvesting* (Jain & Kasbe, 2018).

2.3.PUSTAKA PYTHON

Dipilihnya bahasa pemrograman Python pada penelitian ini karena ketersediaan pustaka yang mendukung untuk proses *web scraping*. Adapun pustaka Python yang digunakan dalam penelitian ini sebagai berikut:

a. *Requests*, pustaka yang penggunaan mudah dan sederhana dalam pemanfaatan *HTTP Persistent Connection.* Hal ini memudahkan dalam berkomunikasi dengan *web service* dengan berbagai metode yang digunakan dalam penelitian ini, yaitu GET untuk mengambil data dari halaman web (Mehak, Zafar, Aslam, & Bhatti, 2019).
b. CSV, pustaka manipulasi data yang dikhususkan pada berkas berformat CSV. Berkas berformat CSV merupakan dokumen bertipe MIME Text sesuai standar

RFC 4180. Dipilih berkas format CSV untuk memudahkan pengolahan data (Nastiti, Hariyadi, & Fazlurrahman, 2019).

c. *Argparse*, pustaka yang berfungsi melakukan parsing argumen suatu masukan, perintah tambahan dan pilihan suatu perintah yang berbasis *Command Language Interpreter*.
d. *BeatifulSoup*, fungsi dari pustaka ini mengambil informasi pada halaman situs web baik dalam bentuk HTML ataupun XML. Proses pengambilan informasi menggunakan pendekatan pohon dari Document Object Model (DOM) (Mehak et al., 2019).
e. Datetime, hasil dari *web scraping* berupa berkas CSV yang memanfaatkan pustaka CSV yang dikombinasikan dengan pustaka ini untuk penamaan berkas berdasarkan waktu pengambilan atau *scraping*.
f. Cookie, untuk meminimalisir mengubah kode web scraping dengan memanfaatkan pustaka ini untuk memisahkan berkas yang berisi informasi dari Cookie situs web.

2.4.ELK STACK

ELK Stack yang merupakan kependekan dari Elasticsearch, Logstash, Kibana sebagai satu kesatuan sebuah sistem dengan fungsi melakukan sebuah analisis dengan visualisasi untuk mempermudah pengguna. Sesuai kependekannya ELK Stack terdiri dari tiga komponen yaitu (Prakash, Kakkar, & Patel, 2016):

a. Elasticsearch merupakan pengindeks konten dari sebuah mesin pencarian situs web yang pencariannya dan daftar informasinya memanfaatkan arsitektur RESTful sebagai JSON diatas protokol HTTP. Proyek pengembangan Elasticsearch dibawah naungan Apache's Lucene Project dengan lisensi Apache License versi 2 yang mudah untuk diadaptasi tanpa biaya tinggi.
b. Logstash merupakan alat pengelola sebuah catatan berupa log atau berkas teks lainnya yang selanjutnya untuk diolah oleh Elasticsearch.
c. Kibana berfungsi untuk mengolah informasi dari Logstash berdasarkan dari pengindeksan dari Elasticsearch dalam bentuk visualisasi yang mempermudah.

3. PEMBAHASAN

Beberapa serangan *web defacement* dilaporkan oleh penyerang ke situs web www.zone-h.org. Serangan berasal dari berbagai negera sehingga untuk memisahkan serangan *web defacement* ke pemerintah menggunakan sub-domain dari TLD, yaitu .go.id. Untuk menarik informasi serangan *web defacement* pada www.zone-h.org terlebih dahulu menelusuri pola dari *Uniform Resource Locator* (URL) dengan kata kunci situs web pemerintah Indonesia. Adapun URL yang digunakan untuk mendapatkan serangan *web defacement* pada situs wes pemerintah di Indonesia adalah http://www.zone-h.org/archive/filter=1/special=1/domain=go.id/fulltext=1/. Selain mencatat URL yang diperlukan dalam penelitian ini adalah *Cookies* saat mengakses URL tersebut.

Makaboro merupakan *Web scraper* yang dikembangkan menggunakan bahasa pemrograman Python membutuhkan beberapa pustaka. Oleh sebab itu sebelum menjalankan aplikasi *web scraper* terlebih dahulu installasi pustaka-pustaka yang diperlukan. Berdasarkan penelusuran kata kunci .go.id didapatkan daftar situs-situs web pemerintah Indonesia yang ter-*deface* dengan penyajian per halaman web dua puluh lima situs web pemerintah Indonesia. Oleh sebab itu proses *scraping* diperlukan juga nomor lembar halaman situs web. Penggunaan aplikasi *web scraper* menggunakan perintah *python makaboro.py –start [Nomor Halaman Terdepan] --stop [Nomor Halaman Terakhir] –output [Penanda Berkas]*. Dari perintah tersebut akan mendapatkan berkas berformat *zoneH-Tahun-Bulan-Tanggal-Penanda.csv*. *Tahun-Bulan-Tanggal* merupakan waktu pengambilan data. Penanda berfungsi sebagai pemberian versi pengambilan data secara manual (Fazlurrahman, 2018).

1. Berkas .csv yang didapatkan tidak dapat langsung dilakukan analisis. Berkas tersebut perlu dilakukan penyesuaian, diantaranya memastikan bahwa setiap kolom terisi dengan informasi yang benar dan mengisi kolom Institusi yang belum bisa didapatkan saat *scraping*. Tabel 2 sebagian contoh hasil *web scraping* dalam bentuk berkas .csv. Informasi yang didapatkan diantaranya Halaman Terdeface, Attacker, Tebas Index, Kejadian, Arsip. Sedangkan nama institusi pemerintah belum bisa didapatkan.

Tabel 2: Hasil Scraping

Institusi	Halaman Terdeface	*Attacker*	Tebas Index	Kejadian	Arsip
	perpustakaan.pn-medankota.go.i...	Vijune15	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252173
	wondamakab.go.id/galau.htm	Astra	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252807
	www.blh.badungkab.go.id/k.htm	Mr.Yagami	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252501
	takalarkab.go.id/lol.php	MR.5T1Y0	T	2019-03-06 00:00:00	www.zone-h.org/mirror/id/32251085
	oku.sumsel.polri.go.id/readme....	KURD ELECTRONIC TEAM	T	2019-03-05 00:00:00	www.zone-h.org/mirror/id/32248515
	pa-taliwang.go.id	by_dadaş	Y	2019-03-05 00:00:00	www.zone-h.org/mirror/id/32248369

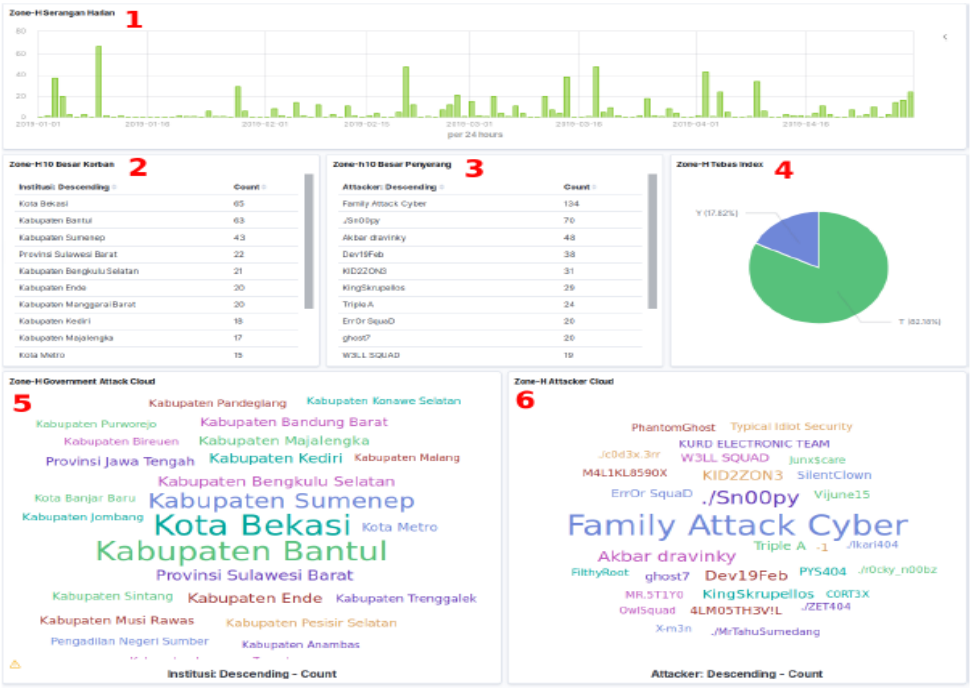
Setelah berkas .csv sudah ter-*scrap* proses selanjutnya adalah melakukan penyesuaian berkas .csv. Terlihat pada Tabel 2 kolom Insitusi masih kosong. Oleh sebab itu kolom Institusi diisi manual berdasarkan kaidah nama institusi pemerintah. Tabel 3 menunjukan proses dari hasil penyesuaian bekars pada kolom institusi.

Tabel 3. Hasil Penyesuaian Berkas

Institusi	Halaman Terdeface	*Attacker*	Tebas Index	Kejadian	Arsip
Pengadilan Negeri Kota Meda	perpustakaan.pn-medankota.go.i...	Vijune15	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252173
Kota Wondaman	wondamakab.go.id/galau.htm	Astra	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252807
Kabupaten Badung	www.blh.badungkab.go.id/k.htm	Mr.Yagami	T	2019-03-07 00:00:00	www.zone-h.org/mirror/id/32252501
Kabupaten Takalar	takalarkab.go.id/lol.php	MR.5T1Y0	T	2019-03-06 00:00:00	www.zone-h.org/mirror/id/32251085
Kepolisian	oku.sumsel.polri.go.id/readme....	KURD ELECTRONIC TEAM	T	2019-03-05 00:00:00	www.zone-h.org/mirror/id/32248515
Pengadilan Agama Taliwang	pa-taliwang.go.id	by_dadaş	Y	2019-03-05 00:00:00	www.zone-h.org/mirror/id/32248369

Berkas yang telah disesuaikan diunggah ke mesin ELK Stack untuk diolah menggunakan Logstash dan Elasticsearch yang selanjutnya ditampilkan dalam bentuk *Dashboard* menggunakan Kibana. Pada *Dashboard* yang tampak pada Gambar 2 terdiri dari enam bagian, yaitu grafik serangan harian *web defacement* (1), sepuluh besar institusi pemerintah yang menjadi korban *web defacement* (2),

sepuluh besar penyerang (3), grafik yang menunjuk persentase dampak serangan tebas index (4), visualisasi cloud situs web pemerintah yang terkena dampak (5), dan visualisasi *cloud* penyerang situs web pemerintah (6).



Gambar 2. Dashboard Serangan Web Defacement

Analisis dan visualisasi pada Gambar 2 menggunakan ELK Stack dengan sumber data yang diambil dari 1 Januari 2019 sampai dengan 30 April 2019. Serangan web defacement tidak selalu dilaporkan setiap hari oleh penyerang. Dalam hal ini penyerang ada dalam bentuk kelompok ataupun individu. Pada situs www.zone-h.org tidak mengklasifikasikan peretas menjadi kelompok atau individu. Dalam rentang 1 Januari 2019 sampai dengan 30 April 2019 institusi pemerintah yang lebih banyak diserang adalah Kota Bekas sedangkan pelaku yang paling sering melakukan penyerangan adalah grup Family Attack Cyber.

Tabel 4. Sepuluh Besar Institusi Terdampak Web Defacement

No	Institusi Terdampak	Jumlah Serangan
1	Kota Bekas	65
2	Kabupaten Bantul	63
3	Kabupaten Sumenep	43
4	Provinsi Sulawesi Barat	22
5	Kabupaten Bengkulu Selatan	21
6	Kabupaten Ende	20
7	Kabupaten Manggarai Barat	20

Tabel 5. Sepuluh Besar Penyerang

No	Penyerang	Kategori penyerang	Jumlah Serangan
1	Family Attack Cyber	Grup	134
2	./Sn00py	Individu	70
3	Akbar dravinky	Individu	48
4	Dev19Feb	Individu	38
5	KID2ZON3	Individu	31
6	KingSkrupellos	Grup	29
7	Triple A	Individu	24
8	ErrOr SquaD	Grup	20
9	ghost7	Grup	20
10	W3LL SQUAD	Grup	19

Dampak serangan *web defacement* terbagi menjadi dua, yaitu Tebas Index dan Serangan Sub Halaman Web. Tebas Index merupakan istilah yang sering digunakan oleh para penyerang dengan dampak serangan halaman depan terganti dengan halaman yang tidak semestinya. Tentu halaman tersebut telah dipersiapkan oleh penyerang dengan berbagai pesan.

4. KESIMPULAN

Makaboro yang dapat diunduh di alamat https://github.com/orangmiliter/makaboro berfungsi sebagai web scraper pada OSINT Source www.zone-h.org yang dikhususkan serangan defacement pada situs web pemerintah Indonesia. Hasil dari Makaboro perlu disesuaikan kembali untuk pengolahan lebih lanjut, yaitu pada kolom institusi. Harapannya penelitian selanjutnya OSINT Source lebih dari satu penyedia. Hal ini disebabkan ada beberapa peretas yang melaporkan tindakan defacement selain di www.zone-h.org.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2019). *Penetrasi dan Perilaku Pengguna Internet Indonesia 2018*. Jakarta.

Fazlurrahman. (2018). Makaboro. Retrieved December 20, 2018, from https://github.com/orangmiliter/makaboro

Hariyadi, D., Winarno, W. W., & Luthfi, A. (2016). Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger. *Teknomatika STMIK Jenderal Achmad Yani Yogyakarta*, *9*(1), 81–89. Retrieved from http://teknomatika.stmikayani.ac.id/teknomatika-9-1/ Indonesia Security Incident Response Team on Infrastructure / Coordination Center. (2019). *Indonesia Cyber Security Monitoring Report 2018*. Jakarta.

Jain, A., & Kasbe, A. (2018). Fake News Detection. *2018 IEEE International Students' Conference on Electrical, Electronics and Computer Science, SCEECS 2018*, 1–5. https://doi.org/10.1109/SCEECS.2018.8546944

Mantra, I. (2015). Indonesia Web Defacement Attacks Analysis for Anti Web Defacement. *Jurnal TICOM*, *3*(3).

Mehak, S., Zafar, R., Aslam, S., & Bhatti, S. M. (2019). Exploiting Filtering Approach with Web Scrapping for Smart Online Shopping. *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies, ICoMET 2019*, 1–5. https://doi.org/10.1109/ICOMET.2019.8673399

Mishra, D., & Pujari, N. (2011). Cross-domain query answering: Using Web scrapper and data integration. *2011 2nd International Conference on Computer and Communication Technology, ICCCT-2011*, 27–32. https://doi.org/10.1109/ICCCT.2011.6075193

Mockapetris, P. V. (1987). *RFC 1035: Domain Names - Implementation and Specification*.

Nastiti, F. E., Hariyadi, D., & Fazlurrahman. (2019). TelegramBot : Crawling Data Serangan Malware dengan Telegram. *Journal of Computer Engineering System and Science*, *4*(1). https://doi.org/10.24114/cess.v4i1.11436

Pengelola Nama Domain Internet Indonesia. (n.d.). Tentang PANDI. Retrieved February 1, 2019, from https://pandi.id/profil/tentang-pandi/

Prakash, T., Kakkar, M., & Patel, K. (2016). Geo-Identification of Web Users through Logs using ELK Stack. In *Proceedings of the 2016 6th International Conference - Cloud System and Big Data Engineering, Confluence 2016* (pp. 606–610). https://doi.org/10.1109/CONFLUENCE.2016.7508191

Romagna, M., & Hout, N. J. Van Den. (2017). Hacktivism and website defacement : Motivations, capabilities and potential threats. *27th Virus Bulletin International Conference*, (October).

Wang, M., Zhang, Z., & Xu, H. (2018). DNS Configurations and Its Security Analyzing via Resource Records of the Top-Level Domains. In *Proceedings of the International Conference on Anti-Counterfeiting, Security and Identification, ASID* (Vol. 2017-Octob, pp. 21–25). https://doi.org/10.1109/ICASID.2017.8285736

TUGAS SISTEM MATA KULIAH

ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS

" DDOS "

DISUSUN OLEH :
Agus Sumitro– 182420126

DOSEN :
M. Izman Herdiansyah , S.T., M.M., Ph.D.

MAGISTER TEKNIK INFORMATIKA
UNIVERSITAS BINADARMA
Jl. Jenderal A. Yani No. 3 Palembang Sumatera Selatan
Email : universitas@binadarma.ac.id
https://www.binadarma.ac.id/

BAB I
PENDAHULUAN

1. Latar Belakang

Perkembangan teknologi informasi pada masa sekarang ini telah mempengaruhi banyak aspek dari kehidupan. Hampir seluruh pekerjaan manusia berhubungan dengan teknologi informasi baik sisi positif dan sisi negatifnya semua dapat mengakibatkan sesuatu hasil dari teknologi informasi tersebut merugikan dan menguntungkan manusia.

Dengan menggunakan bantuan teknologi informasi dan komunikasi tersebut. Adanya alat-alat itu dapat mengubah pikiran manusia, mengubah cara kerja dan cara hidupnya ,kejadian ini dapat diidentifikasikan sebagai kemajuan ilmu pengetahuan teknologi, informasi dan komunikasi.

Sejak tahun 1970 teknologi informasi dan komunikasi di Negara Indonesia berkembang pesat, perkembangan tersebut berjalan secara bertahap perkembangan teknologi informasi dan komunikasi yang ada di Indonesia dengan adanya internet.

Dalam internet terdapat banyak variasi program atau layanan internet yang sangat membantu masyarakat dalam hal sarana informasi maupun edukasi. Internet identik dengan media sosial yang terdapat banyak variasi program di dalamnya salah satunya yaitu konten.

Dengan adanya internet tak dapat dihindari lagi akan serangan terhadap keamanan internet itu sendiri. Dari berbagai macam serangan yang melalui jaringan internet diantaranya adalah DDOS (Distributed Denial of Service).

Keamanan merupakan hal yang sangat penting dalam dunia teknologi informasi. Di era teknologi informasi saat ini, pelayanan kepada konsumen menjadi hal yang mutlak untuk bertahan dalam persaingan. Banyak sekali cara yang ditempuh untuk menghalangi seseorang / instansi / perusahaan guna memberikan pelayanan tersebut. Hal ini menjadi sangat mungkin bila pelayanan yang diberikan melalui jalur yang dapat dikatakan kurang aman (internet) yang terkoneksikan melalui jaringan. Beberapa serangan kepada server sebagai penyedia layanan kerap dilakukan, walaupun tidak semua tujuan yang dilakukan berlandaskan pada politik,atau bisnis belaka. Namun beberapa diantaranya juga merupakan unjuk gigi guna memperoleh prestise tertentu di sebuah komunitas atau perkumpulan. Serangan DOS (Denial Of Service) dan DDOS (Distributed Denial Of Service) adalah serangan yang mungkin bisa sering kita jumpai diantara serangan serangan lainnya

LITERATURE REVIEW

Siapa yang tak pernah mendengar istilah internet sekarang ini? Hampir semua orang mulai dari anak-anak hingga orang dewasa atau bahkan lansia sekalipun sudah tak asing lagi dengan istilah tersebut. Pengertian internet itu sendiri mungkin juga sudah bisa Anda rumuskan secara sekilas.

Bahkan kini, hampir semua aspek pekerjaan dalam kehidupan kita sehari-hari telah mengandalkan internet. Sudah bukan trik rahasia lagi untuk mencari segala solusi dan jawaban di internet. Ketika Anda mencari resep makanan, ketika Anda mencari berita, bahkan ketika Anda memesan barang atau produk tertentu.

Tak jarang pula, teknologi canggih yang satu ini memisahkan kita dari orang-orang sekitar kita. Pada restoran-restoran misalnya, pelanggan yang datang dan makan cenderung menanyakan password WiFi ke pramusaji sebelum mereka memesan makanan. Setelah selesai menyantap makanan yang dihidangkan pun, satu keluarga yang tadinya makan semeja jadi sibuk dengan perangkat mobile masing-masing untuk mengakses internet.

Internet adalah suatu jaringan komunikasi yang menghubungkan satu media elektonik dengan media yang lainnya. Standar teknologi pendukung yang dipakai secara global adalah Transmission Control Protocol atau Internet Protocol Suite (disingkat sebagai istilah TCP/IP). TCP/IP ini merupakan protokol pertukaran paket (dalam istilah asingnya Switching Communication Protocol) yang bisa digunakan untuk miliaran lebih pengguna yang ada di dunia. Sementara itu, istilah “internetworking” berarti cara/prosesnya dalam menghubungkan rangkaian internet beserta penerapan aturannya yang telah disebutkan sebelumnya.

Dengan berkembangnya teknologi keamanan jaringan ternyata tidak bisa menjamin sepenuhnya untuk melindungi sistem anda dari serangan attacker. Berbagai cara akan dilakukan attacker untuk dapat mengganggu sistem anda, seperti dengan cara membanjiri trafik pada jaringan sehingga dapat menghabiskan resource pada server anda dan server anda tidak bisa menjalankan fungsinya dengan baik.

Berikut adalah jenis-jenis serangan pada jaringan komputer yang biasa dilakukan oleh attacker

1. Spoofing

Teknik serangan yang dilakukan attacker dengan cara memalsukan data sehingga attacker dapat terlihat seperti host yang dapat dipercaya. Terdapat 3 jenis spoofing

- **IP spoofing** adalah teknik yang digunakan dengan cara memalsukan source IP address sehingga ip address aslinya tidak dapat dilacak ketika pengiriman paket
- **DNS Spoofing** adalah teknik yang digunakan untuk mengambil alih DNS server sehingga DNS dan IP address sebuah situs akan dialihkan ke server sang pelaku
- **Identity Spoofing** adalah teknik penyusupan menggunakan identitas secara resmi untuk mengakses segala sesuatu dalam jaringan secara illegal

2. DDoS (Distributed Denial of Service)

Merupakan jenis serangan terhadap server pada suatu jaringan dengan metode menghabiskan resource yang dimiliki server sampai server tersebut tidak dapat menjalankan fungsinya untuk memberikan akses layananya. Ada beberapa cara yang biasanya dilakukan attacker yaitu

- Dengan cara membanjiri trafik dengan banyak data sehingga data dari host yang terdaftar tidak dapat masuk kedalam sistem
- Dengan cara membanjiri trafik dengan banyaknya request terhadap server sehingga request dari host yang terdaftar tidak dapat dilayani oleh server
- Mengganggu komunikasi antara server dengan host yang terdaftar dengan berbagai cara seperti salah satunya bisa dengan mengubah informasi konfigurasi sistem

DDOS (Distributed Denial of Service)
merupakan jenis serangan DOS yang menggunakan banyak host sekaligus untuk menyerang satu server sehingga dapat mengakibatkan server tidak dapat berfungsi bagi klien.

3. Packet Sniffing

Paket Sniffing merupakan teknik pencurian data dengan cara memonitoring dan menganalisis setiap paket data yang ditransmisikan dari klien ke server. biasanya attacker melakukan serangan ini menggunakan tools wireshark dan netcut untuk mencuri password dan pengambilan data-data penting lainya. Berikut merupakan tahap-tahap cara kerja paket sniffing

- **Collecting** -> merubah interface yang digunakan menjadi promicius code dan kemudian mengelompokan paket data yang lewat melalui jaringan dalam bentuk raw binary
- **Conversion** -> mengkonveriskan data binary kedalam data yang mudah dibaca/dipahami
- **Analysis** -> setelah itu data diklasifikasikan kedalam blok protokol sesuai dengan sumber data tersebut
- **Pencurian Data**-> Setelah data dikasifikasikan, maka attacker dapat mencuri datanya

4. DNS Poisoning

Merupakan Jenis serangan dengan cara memberikan informasi IP address yang palsu untuk mengalihkan trafik pada paket data dari tujuan yang sebenarnya. biasanya cara ini dipakai attacker untuk menyerang situs-situs ecommerce dan banking. attacker juga dapat membuat server palsu yang memiliki tampilan yang sama dengan situ yg sebenarnya. oleh karena itu diperlukan adanya digital certificate untuk mengamankanya agar server palsu tersebut dapat dibedakan dengan server aslinya yang memiliki digital certificate

5. Trojan Horse

Merupakan salah satu jenis Malicious software/malware yang dapat merusak sebuah sistem. Trojan ini dapat digunakan untuk memperoleh informasi dari target seperti password, system log dll, dan dapat memperoleh hak akses dari target. Trojan merupakan software yang berbeda

dengan virus atau worm karena trojan ini bersifat stealth dalam beroperasi dan seolah-olah seperti program biasa yang tidak mencurigakan dan trojan juga bisa dikendalikan dari komputer lain (attacker). ada beberapa jenis trojan dan 3 diantaranya yaitu:

- **Pencuri Password** -> jenis trojan ini dapat mencuri password yang disimpan didalam sistem dengan cara membuat tampilan seolah-olah tampilan login dengan menunggu host memasukan passwordnya pada saat login kemudian password tersebut akan dikirimkan ke attacker
- **Keylogger** -> Jenis Trojan akan merekam semua yang diketikan oleh host dan mengirimkanya ke attacker.
- **RAT (Remote Administration Tools)**-> Jenis trojan ini mampu mengambil alih kontrol secara penuh terhadap sistem dan dapat melakukan apapun yang attacker mau dari jarak jauh seperti memformat hardisk, mengedit dan menghapus data dll

6. SQL Injection

Sebuah Teknik serangan yang memanfaatkan celah keamanan dimana website mengijinkan user untuk menginput data tetapi tanpa adanya filter terhadap malicious character sehingga attacker bisa mendapatkan akses kedalam basis data sebuah aplikasi. inputan tersebut biasanya dimasukan kedalam bagian-bagian tertentu pada website yang berhubungan dengan database dari situs tersebut. attacker biasanya memasukan data link yang mengarahkan korban menuju website yang digunakan attacker untuk mengambil informasi/data pribadi dari korban.

BAB II

PEMBAHASAN

1. **Definisi DDOS**

Distributed Denial of Service atau lebih dikenal dengan nama DDoS adalah sebuah percobaan penyerangan dari beberapa sistem komputer yang menargetkan sebuah server agar jumlah traffic menjadi terlalu tinggi sampai server tidak bisa menghandle requestnya.

DDoS biasa dilakukan dengan menggunakan beberapa sistem komputer yang digunakan sebagai sumber serangan. Jadi mereka melakukan serangan ke satu server melalui beberapa komputer agar jumlah traffic juga bisa lebih tinggi. Serangan DDoS bisa dibilang seperti kemacetan lalu lintas yang menghalangi pengemudi untuk mencapai tujuan yang diinginkan dengan tepat waktu.

Lalu bagaimana sebenarnya **cara kerja serangan DDoS** ini?

Untuk melakukan DDoS attack, penyerang memerlukan kontrol ke jaringan sebuah mesin online. Ini bisa berupa komputer atau device Internet of Things lainnya yang memiliki malware. Ini dilakukan agar setiap komputer atau device ini menjadi bot atau zombie. Kumpulan dari bot atau zombie ini disebut dengan istilah botnet.

Setelah botnet berhasil dibuat, penyerang juga bisa mengatur mesin-mesin ini dengan mengirimkan instruksi ke setiap bot melalui metode remote control. Setelah botnet menargetkan IP Address korban, setiap bot akan mengirimkan request ke target sampai server target tidak bisa menghandle requestnya. Ini akan mengakibatkan denial of service atau penolakan layanan ke traffic normal. Karena setiap bot yang digunakan adalah device internet yang masuk akal, memisahkan mana yang traffic biasa dan mana yang traffic serangan memang tidak mudah.

Jenis-Jenis DDOS Attack

DDoS attack sendiri terdiri dari beberapa jenis. Berikut ini adalah beberapa jenis serangan DDoS yang paling sering terjadi:

UDP Flood

UDP atau User Diagram Protocol adalah jaringan protocol tanpa session, yang membanjiri port sebuah remote host secara acak. Dengan begitu, host server perlu melakukan pemeriksaan di port-port ini dan me-report balik dengan menggunakan paket ICMP. Proses ini sebenarnya akan menghancurkan resource milik host dan menyebabkan website tidak bisa diakses.

ICMP (Ping) Flood

Pada serangan ICMP flood, resource target akan dibanjiri dengan request ICMP secara cepat tanpa menunggu respon dari Anda. Jenis serangan seperti ini semua bandwidth masuk maupun keluar terkena dampaknya dan ini mengakibatkan kelambatan sistem pada server milik korban.

SYN Flood

Pada serangan SYN flood, pesan sinkronisasi (SYN) diterima di mesin host untuk memulai dengan "jabat tangan". Permintaan ini diakui oleh server dengan mengirimkan tanda pengesahan (ACK) ke host awal dan menunggu koneksi ditutup. Koneksi akan selesai ketika mesin yang meminta akan menutup koneksi. Dalam serangan SYN flood, permintaan palsu dikirim dan server merespon dengan paket ACK untuk menyelesaikan koneksi TCP tetapi sambungan diarahkan kee timeout, daripada menutupnya. Oleh karena itu, sumber daya server menjadi lelah dan server pun akhirnya offline.

Ping of Death

Serangan ping of death ("POD") adalah serangan dimana penyerang mengirimkan beberapa ping yang salah atau berbahaya ke komputer. Panjang paket maksimum dari paket IP (termasuk header) adalah 65.535 byte. Namun, Layer Data Link biasanya menimbulkan batasan untuk ukuran frame maksimum – misalnya 1500 byte melalui jaringan Ethernet. Dalam hal ini, paket IP yang besar dibagi di beberapa paket IP (dikenal sebagai fragmen), dan host penerima merakit kembali fragmen IP ke dalam paket lengkap. Dalam skenario Ping of Death, setelah manipulasi berbahaya dari konten fragmen, penerima berakhir dengan paket IP yang lebih besar dari 65.535 byte ketika dipasang kembali. Ini dapat membanjiri buffer memori yang dialokasikan untuk paket, menyebabkan penolakan layanan untuk paket yang sah.

Lindungi Website dan Server Anda dari DDoS Attack

Web app Anda terdiri dari beberapa layers dan untuk melindungi diri dari berbagai DDoS Attack, Anda perlu memastikan bahwa tujuh layer web app Anda sudah terlindungi. Untuk melindungi website dari serangan ini, Anda bisa menggunakan beberapa layanan yang memang disediakan dengan tujuan untuk melindungi website Anda.

Cloudflare

Cloudflare adalah salah satu layanan keamanan website yang paling popular. Bahkan jika Anda menggunakan versi gratisnya, Anda tetap akan terlindungi dari DDoS. Jika Anda memerlukan perlindungan yang lebih tinggi, mungkin Anda memerlukan akun bisnis. Untuk menggunakan Cloudflare, Anda hanya perlu membayar tiap bulan dan biayanya selalu sama; tidak peduli berapa banyak serangan yang mereka hadapi atau seberapa kuat serangannya. Jaringan Cloudflare sudah tersebar ke lebih dari 102 data centers dan bisa menghandle lebih dari 10 TBps serta menghadapi serangan apapun. Cloudflare juga menyediakan layanan emergency 24 jam yang bisa Anda gunakan saat sedang terjadi serangan. Kalau ada dari Anda yang ingin tahu lebih banyak tentang Cloudflare, Anda bisa membaca Panduan Dasar Cloudflare dari kami.

Dewaguard

Dewaguard adalah tool anti malware berkualitas tinggi dari Dewaweb. Dengan Dewaguard, website Anda akan terlindungi. Mulai dari WordPress sampai Magento, Dewaguard bisa melindungi semuanya. Perlindungan dari DDoS sudah disertakan di paket antivirus dan firewall. Dewaguard sendiri bisa menghilangkan malware yang menginfeksi website Anda dan memberi notifikasi kepada webmaster jika ada potensi ancaman. Selain itu, Dewaguards juga melakukan backup secara rutin dan otomatis jadi Anda tidak perlu khawatir soal data yang hilang. Jika Anda ingin informasi lebih lanjut, Anda bisa mengunjungi halaman produk Dewaguard.

Akamai

Akamai adalah salah satu pemimpin di bidang cybersecurity dan CDN. Berdasarkan administrasi Akamai, layanan ini bisa mengatasi sampai dengan serangan 1.3 TBps. Serangan terbesar yang pernah mereka atasi adalah 620 Gbps dan mereka berhasil mengatasinya dengan cepat. Akamai memiliki layanan perlindungan DDoS yang disebut Kona DDoS Defender yang memang dibangun di platform intelijen Akamai. Selain itu, mereka juga menyediakan support 24/7. Layanan ini bisa menghentikan serangan sebelum serangannya mencapai web applications. Perlindungan DDoS Akamai terdiri dari sekitar 1300 node jaringan yang terletak di lebih dari 100 negara di seluruh dunia.

Bagaimana Mencegah Serangan DDoS

Anda tidak dapat mencegah penyerang jahat mengirimkan gelombang lalu lintas tidak otentik ke server Anda, tetapi Anda dapat mempersiapkan diri sebelumnya untuk menangani beban.

1. Tangkap Lebih Awal dengan Memantau Lalu Lintas

Penting untuk memahami dengan baik tentang apa yang termasuk lalu lintas normal, rendah, dan volume tinggi bagi perusahaan Anda, menurut Amazon Web Services.

Jika Anda tahu apa yang mungkin terjadi ketika lalu lintas data mencapai batas maksimalnya, Anda dapat menetapkan pembatasan laju. Artinya, server hanya akan menerima permintaan sebanyak yang dapat ditanganinya.

Dengan memiliki pengetahuan terkini tentang tren lalu lintas, Anda akan mampu mengidentifikasi masalah dengan cepat.

Anda pun harus siap menghadapi lonjakan lalu lintas terkait sesuatu yang bersifat musiman, kampanye pemasaran, dan lain-lain. Banyak lalu lintas yang otentik (dari tautan media sosial yang viral, misalnya) yang punya dampak serupa dalam membuat server crash. Dan meskipun berasal dari sumber yang sah, downtime tetap berdampak buruk bagi bisnis Anda.

2. Dapatkan Bandwidth yang Lebih Banyak

Setelah Anda tahu pasti kapasitas server yang dibutuhkan, berdasarkan tingkat lalu lintas rata-rata dan tinggi, Anda harus mendapatkannya *plus tambahan*. Mendapatkan bandwidth server yang lebih banyak dari jumlah yang dibutuhkan disebut “overprovisioning.”

Dengan cara ini, Anda punya waktu lebih banyak seandainya terjadi serangan DDoS sebelum situs web, server, atau aplikasi Anda benar-benar kelebihan beban.

3. Gunakan Jaringan Distribusi Konten (Content Distribution Network – CDN)

Tujuan dari DDoS adalah untuk membebani server hosting Anda. Maka, salah satu solusinya adalah dengan menyimpan data Anda di beberapa server di seluruh dunia.

Itulah yang dilakukan Jaringan Distribusi Konten (CDN).

CDN melayani situs web atau data Anda untuk pengguna dari server yang dekat dengannya untuk kinerja yang lebih cepat. Namun, dengan menggunakan CDN, Anda pun tidak terlalu rentan terhadap serangan karena apabila satu server kelebihan beban, banyak server lainnya yang masih operasional untuk Anda gunakan.

BAB III
KESIMPULAN

Server manapun bisa terkena serangan ini. DDoS dilakukan oleh seorang penyerang, artinya serangan ini memang sengaja dilakukan oleh pihak-pihak tertentu. DDoS punya beberapa dampak seperti melambatnya trafik server hingga matinya jaringan atau null-route. Seorang administrator harus sudah mengimplementasikan lapisan anti-DDoS sebagai langkah mitigasi. Mitigasi tersebut mampu menjaga server dari ancaman-ancaman DDoS, sehingga server yang ada tetap dapat diakses ketika terjadi serangan.

Solusi terbaiknya adalah dengan mencegah risiko serangan DDoS sejak awal, dengan menginstal **antivirus yang layak** untuk melindungi Anda dari malware. Menggunakan CDN dan mengatur pembatasan laju berdasarkan lalu lintas normal merupakan langkah pencegahan lainnya yang bagus.

Mencegah lebih baik daripada mengobati, karena begitu serangan DDoS berjalan, dan server Anda offline, memulihkannya dapat berbiaya mahal — downtime situs web dapat berdampak pada penjualan dan reputasi bisnis Anda. Jadi, pastikan agar bisnis Anda siap menghadapi beraneka macam serangan kapan saja.

Dari aspek etika , orang atau organisasi yang membuat dan melakukan DDOS adalah orang yang melanggar hukum karena dengan perbuatanya tersebut akan sangat merugikan bagi korbanya dengan resiko yang mungkin akan berefek pada kegiatan dalam usaha atau organisasinya.

Dengan demikian harus di lakukan penindakan hukum yang tepat bagi pelaku penyerangan dengan DDOS sehingga tidak ada kerugian lagi dalam suatu sistem.

BAB IV
DAFTAR PUSTAKA

https://www.dewaweb.com/blog/ddos-attack-pengertian-dan-solusinya/;
ANALISIS KONSEP DAN CARA KERJA SERANGAN KOMPUTER DISTRIBUTED DENIAL OF SERVICE (DDOS) RUDI HERMAWAN Program Studi Teknik Informatika Fakultas Teknik, Matematika dan Ilmu Pengetahuan Alam Universitas Indraprasta PGRI;
Network security – The internal threat By Steven F. Delahunty

AGUS WIRANTO

182420102 ➢ MTI2A1 ➢ Ethical Issues in Electronic

➢ Web Deface

1. Pendahuluan

Perkembangan Ilmu Pengetahuan dan Teknologi (IPTEK) yang cukup pesat sekarang ini sudah menjadi realita sehari-hari bahkan merupakan tuntutan masyarakat yang tidak dapat ditawar lagi. Tujuan utama perkembangan iptek adalah perubahan kehidupan masa depan manusia yang lebih baik, mudah, murah, cepat dan aman. Perkembangan iptek, terutama teknologi informasi *(Information Technology*) seperti internet sangat menunjang setiap orang mencapai tujuan hidupnya dalam waktu singkat, baik legal maupun illegal dengan menghalalkan segala cara karena ingin memperoleh keuntungan secara "potong kompas". Dampak buruk dari perkembangan "dunia maya" ini tidak dapat dihindarkan dalam kehidupan masyarakat modern saat ini dan masa depan.

Kemajuan teknologi yang merupakan hasil budaya manusia disamping membawa dampak positif, dalam arti dapat didaya gunakan untuk kepentingan umat manusia juga membawa dampak negative terhadap perkembangan manusia dan peradabannya. Dampak negative yang dimaksud adalah yang berkaitan dengan dunia kejahatan. J.E. Sahetapy telah menyatakan dalam tulisannya, bahwa kejahatan erat kaitannya dan bahka menjadi sebagian dari hasil budaya itu sendiri ini berarti semakin tinggi tingkat budaya dan semakin modern suatu bangsa, maka akan semakin modern pula kejahatan itu dalam bentuk, sifat dan cara pelaksanaannya.

Tindak kejahatan berupa serangan siber sepanjang tahun 2018 dengan objek pantau situs web sebanyak 16.939 serangan. Situs web dengan domain .go.id mendapat serangan terbanyak dibanding Country Code Top Level Domain (ccTLD) .id lainnya. Tabel 1 menunjukan persentase pemantauan insiden situs web pada tahun 2018 dengan ccTLD .id. Bentuk insiden yang terjadi pada situs web adalah web defacement (Indonesia Security Incident Response Team on Infrastructure / Coordination Center, 2019). Pada penelitian sebelumnya serangan web defacement pada situs web milik pemerintah juga pada urutan pertama berdasarkan observasi pada bulan Januari sampai dengan Juli 2014 (Mantra, 2015).

Tabel 1 Pemantauan Insiden Situs Web Tahun 2018

No	ccTLD	Persentase
1	.go.id	30.75 %
2	.ac.id	28.38 %
3.	.sch.id	12.58 %
4.	.co.id	10.92 %
5.	.id	8.25 %
6.	.or.id	2.96 %
7.	.desa.id	2.76 %
8.	.web.id	2.56 %
9.	.my.id	0.53 %
10.	.mil.id	0.11 %
11.	.biz.id	0.08 %
12.	.net.id	0.08 %
13.	.ponpes.id	0.03 %

Defacement pada situs web atau web defacement dapat diartikan tindakan mengubah tampilan halaman situs yang tidak semestinya oleh orang yang tidak memiliki otoritas (Romagna & Hout, 2017). Masih menurut Rogmana dan Hout serangan web defacement merupakan serangan yang berpotensi karena memerlukan biaya untuk memperbaikinya. Penelitian ini fokus pada pemantauan serangan web defacement dengan studi kasus situs web pemerintah yaitu yang memiliki domain .go.id supaya pihak pemerintah memperhatikan pembiayaan setelah pengembangan sebuah sistem berbasis web

2. Landasan Teori

2.1. Cyber Crime

2.1.1 Definisi Cybercrime

Cybercrime adalah tindakan pidana kriminal yang dilakukan pada teknologi internet (cyberspace), baik yang menyerang fasilitas umum di dalam cyberspace ataupun kepemilikan pribadi. Secara teknik tindak pidana tersebut dapat dibedakan menjadi off-line crime, semi on-line crime, dan cybercrime. Masing-masing memiliki karakteristik tersendiri, namun

perbedaan utama antara ketiganya adalah keterhubungan dengan jaringan informasi publik (internet).

Cybercrime dapat didefinisikan sebagai perbuatan melawan hukum yang dilakukan dengan menggunakan internet yang berbasis pada kecanggihan teknologi komputer dan telekomunikasi. The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba pada tahun 1999 dan di Wina, Austria tahun 2000, menyebutkan ada 2 istilah yang dikenal:

- Cybercrime dalam arti sempit (Cyber crime in a narrow sense) disebut computer crime, yaitu prilaku ilegal/ melanggar yang secara langsung menyerang sistem keamanan komputer dan/atau data yang diproses oleh komputer.
- Cybercrime dalam arti luas (Cyber crime in a broader sense) disebut computer related crime, yaitu prilaku ilegal/ melanggar yang berkaitan dengan sistem komputer atau jaringan.

Dari beberapa pengertian di atas, cybercrime dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai sarana/ alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

2.1.2 Karakteristik Cybercrime

Berdasarkan beberapa literatur serta praktiknya, cybercrime memiliki beberapa karakteristik, yaitu :

1. Perbuatan yang dilakukan secara ilegal, tanpa hak atau tidak etik tersebut terjadi dalam ruang/wilayah siber/cyber (cyberspace), sehingga tidak dapat dipastikan yurisdiksi negara mana yang berlaku terhadapnya.
2. Perbuatan tersebut dilakukan dengan menggunakan peralatan apapun yang terhubung dengan internet.
3. Perbuatan yang mengakibatkan kerugian materiil maupun immateriil (waktu, nilai, jasa, uang, barang, harga diri, martabat, kerahasian informasi) yang cenderung lebih besar dibandingkan dengan kejahatan konvensional.
4. Pelakunya adalah orang yang menguasai penggunaan internet beserta aplikasinya
5. Perbuatan tersebut sering dilakukan secara transnasional/melintasi batas negara.

2.1.3 Faktor Penyebab Munculnya Cybercrime

Jika dipandang dari sudut pandang yang lebih luas, latar belakang terjadinya kejahatan di dunia maya ini terbagi menjadi dua faktor penting, yaitu :

1. **Faktor Teknis**

   Dengan adanya teknologi internet akan menghilangkan batas wilayah negara yang menjadikan dunia ini menjadi begitu dekat dan sempit. Saling terhubungnya antara jaringan yang satu dengan yang lain memudahkan pelaku kejahatan untuk melakukan aksinya. Kemudian, tidak meratanya penyebaran teknologi menjadikan pihak yang satu lebih kuat daripada yang lain.

2. **Faktor Sosial ekonomi**

   Cybercrime dapat dipandang sebagai produk ekonomi. Isu global yang kemudian dihubungkan dengan kejahatan tersebut adalah keamanan jaringan. Keamanan jaringan merupakan isu global yang muncul bersamaan dengan internet. Sebagai komoditi ekonomi, banyak negara yang tentunya sangat membutuhkan perangkat keamanan jaringan. Melihat kenyataan seperti itu, Cybercrime berada dalam skenario besar dari kegiatan ekonomi dunia.

2.1.4 Jenis-jenis Cybercrime

1. **a) Berdasarkan jenis aktifitas yang dilakukannya**

- **Unauthorized Access**

  Merupakan kejahatan yang terjadi ketika seseorang memasuki atau menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin, atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. *Probing* dan *port* merupakan contoh kejahatan ini.

- **Illegal Contents**

  Merupakan kejahatan yang dilakukan dengan memasukkan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau menggangu ketertiban umum, contohnya adalah penyebaran pornografi.

- **Penyebaran virus secara sengaja**

  Penyebaran virus pada umumnya dilakukan dengan menggunakan email. Sering kali orang yang sistem emailnya terkena virus tidak menyadari hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya.
- **Data Forgery**

  Kejahatan jenis ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database.
- **Cyber Espionage, Sabotage, and Extortion**

  Cyber Espionage merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Sabotage and Extortion merupakan jenis kejahatan yang dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
- **Cyberstalking**

  Kejahatan jenis ini dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya menggunakan e-mail dan dilakukan berulang-ulang. Kejahatan tersebut menyerupai teror yang ditujukan kepada seseorang dengan memanfaatkan media internet. Hal itu bisa terjadi karena kemudahan dalam membuat email dengan alamat tertentu tanpa harus menyertakan identitas diri yang sebenarnya.
- **Carding**

  Carding merupakan kejahatan yang dilakukan untuk mencuri nomor kartu kredit milik orang lain dan digunakan dalam transaksi perdagangan di internet.
- **Hacking dan Cracker**

  Istilah *hacker* biasanya mengacu pada seseorang yang punya minat besar untuk mempelajari sistem komputer secara detail dan bagaimana meningkatkan kapabilitasnya. Adapun mereka yang sering melakukan aksi-aksi perusakan di internet lazimnya disebut *cracker*. Boleh dibilang cracker ini sebenarnya adalah hacker yang yang memanfaatkan kemampuannya untuk hal-hal yang negatif. Aktivitas cracking di internet memiliki lingkup yang sangat luas, mulai dari pembajakan account milik orang lain, pembajakan situs web, probing, menyebarkan virus, hingga pelumpuhan target sasaran. Tindakan yang terakhir

disebut sebagai DoS (Denial Of Service). Dos attack merupakan serangan yang bertujuan melumpuhkan target (hang, crash) sehingga tidak dapat memberikan layanan.

- **Cybersquatting and Typosquatting**

  Cybersquatting merupakan kejahatan yang dilakukan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya kepada perusahaan tersebut dengan harga yang lebih mahal. Adapun typosquatting adalah kejahatan dengan membuat domain plesetan yaitu domain yang mirip dengan nama domain orang lain. Nama tersebut merupakan nama domain saingan perusahaan.

- **Hijacking**

  Hijacking merupakan kejahatan melakukan pembajakan hasil karya orang lain. Yang paling sering terjadi adalah Software Piracy (pembajakan perangkat lunak).

- **Cyber Terorism**

  Suatu tindakan cybercrime termasuk cyber terorism jika mengancam pemerintah atau warganegara, termasuk cracking ke situs pemerintah atau militer.

1. **b) Berdasarkan motif kegiatan yang dilakukannya**

- **Cybercrime sebagai tindakan murni criminal**

  Kejahatan yang murni merupakan tindak kriminal merupakan kejahatan yang dilakukan karena motif kriminalitas. Kejahatan jenis ini biasanya menggunakan internet hanya sebagai sarana kejahatan. Contoh kejahatan semacam ini adalah Carding, yaitu pencurian nomor kartu kredit milik orang lain untuk digunakan dalam transaksi perdagangan di internet. Juga pemanfaatan media internet (webserver, mailing list) untuk menyebarkan material bajakan. Pengirim e-mail anonim yang berisi promosi (spamming) juga dapat dimasukkan dalam contoh kejahatan yang menggunakan internet sebagai sarana. Di beberapa negara maju, pelaku spamming dapat dituntut dengan tuduhan pelanggaran privasi.

- **Cybercrime sebagai kejahatan ”abu-abu”**

  Pada jenis kejahatan di internet yang masuk dalam wilayah ”abu-abu”, cukup sulit menentukan apakah itu merupakan tindak kriminal atau bukan mengingat motif kegiatannya terkadang bukan untuk kejahatan. Salah satu contohnya adalah probing atau portscanning. Ini adalah sebutan untuk semacam tindakan pengintaian terhadap sistem

milik orang lain dengan mengumpulkan informasi sebanyak-banyaknya dari sistem yang diintai, termasuk sistem operasi yang digunakan, port-port yang ada, baik yang terbuka maupun tertutup, dan sebagainya.

1. c) **Berdasarkan Sasaran Kejahatan**

- **Cybercrime yang menyerang individu (Against Person)**

  Jenis kejahatan ini, sasaran serangannya ditujukan kepada perorangan atau individu yang memiliki sifat atau kriteria tertentu sesuai tujuan penyerangan tersebut. Beberapa contoh kejahatan ini antara lain :

  a. **Pornografi**

     Kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan, dan menyebarkan material yang berbau pornografi, cabul, serta mengekspos hal-hal yang tidak pantas.

  b. **Cyberstalking**

     Kegiatan yang dilakukan untuk mengganggu atau melecehkan seseorang dengan memanfaatkan komputer, misalnya dengan menggunakan e-mail yang dilakukan secara berulang-ulang seperti halnya teror di dunia cyber. Gangguan tersebut bisa saja berbau seksual, religius, dan lain sebagainya.

  c. **Cyber-Tresspass**

     Kegiatan yang dilakukan melanggar area privasi orang lain seperti misalnya Web Hacking. Breaking ke PC, Probing, Port Scanning dan lain sebagainya.

- **Cybercrime menyerang hak milik (Againts Property)**

  Cybercrime yang dilakukan untuk menggangu atau menyerang hak milik orang lain. Beberapa contoh kejahatan jenis ini misalnya pengaksesan komputer secara tidak sah melalui dunia cyber, pemilikan informasi elektronik secara tidak sah/pencurian informasi, carding, cybersquating, hijacking, data forgery dan segala kegiatan yang bersifat merugikan hak milik orang lain.

- **Cybercrime menyerang pemerintah (Againts Government)**

  Cybercrime Againts Government dilakukan dengan tujuan khusus penyerangan terhadap pemerintah. Kegiatan tersebut misalnya *cyber terorism* sebagai tindakan yang mengancam pemerintah termasuk juga cracking ke situs resmi pemerintah atau situs militer.

5. **Contoh Cybercrime Di Indonesia**

- **Pencurian Account User Internet**

  Merupakan salah satu dari kategori Identity Theft and fraud (pencurian identitas dan penipuan), hal ini dapat terjadi karena pemilik user kurang aware terhadap keamanan di dunia maya, dengan membuat user dan password yang identik atau gampang ditebak memudahkan para pelaku kejahatan dunia maya ini melakukan aksinya.

- **Deface (Membajak situs web)**

  Metode kejahatan deface adalah mengubah tampilan website menjadi sesuai keinginan pelaku kejahatan. Bisa menampilkan tulisan-tulisan provokative atau gambar-gambar lucu. Merupakan salah satu jenis kejahatan dunia maya yang paling favorit karena hasil kejahatan dapat dilihat secara langsung oleh masyarakat.

- **Probing dan Port Scanning**

  Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan "port scanning" atau "probing" untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya.

- **Virus dan Trojan**

  Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Trojan adalah sebuah bentuk perangkat lunak yang mencurigakan (malicious software) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

- **Denial of Service (DoS) attack**

  Denial of Service (DoS) attack adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh

komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

2.2 Cyber Law

2.2.1 Definisi Cyberlaw

Cyberlaw adalah hukum yang digunakan di dunia cyber (dunia maya) yang umumnya diasosiasikan dengan internet. Cyberlaw merupakan aspek hukum yang ruang lingkupnya meliputi setiap aspek yang berhubungan dengan orang perorangan atau subyek hukum yang menggunakan dan memanfaatkan teknologi internet yang dimulai pada saat mulai online dan memasuki dunia cyber atau maya.

Cyberlaw merupakan seperangkat aturan yang dibuat oleh suatu negara tertentu, dan peraturan yang dibuat itu hanya berlaku kepada masyarakat negara tersebut. Jadi,setiap negara mempunyai cyberlaw tersendiri.

2.2.2 Ruang Lingkup Cyberlaw

Jonathan Rosenoer dalam Cyber law, the law of internet mengingatkan tentang ruang lingkup dari cyber law diantaranya :

- Hak Cipta (Copy Right)
- Hak Merk (Trademark)
- Pencemaran nama baik (Defamation)
- Fitnah, Penistaan, Penghinaan (Hate Speech)
- Serangan terhadap fasilitas komputer (Hacking, Viruses, Illegal Access)
- Pengaturan sumber daya internet seperti IP Address, domain name
- Kenyamanan Individu (Privacy)
- Prinsip kehati-hatian (Duty care)
- Tindakan kriminal biasa yang menggunakan TI sebagai alat
- Isu prosedural seperti yuridiksi, pembuktian, penyelidikan dll
- Kontrak / transaksi elektronik dan tanda tangan digital
- Pornografi
- Pencurian melalui Internet
- Perlindungan Konsumen

- Pemanfaatan internet dalam aktivitas keseharian seperti ecommerce, e-government, e-education dll

2.2.3 Perangkat Hukum Cyber Law

Agar pembentukan perangkat perundangan tentang teknologi informasi mampu mengarahkan segala aktivitas dan transaksi didunia cyber sesuai dengan standar etik dan hukum yang disepakati maka proses pembuatannya diupayakan sebagai berikut:

1. Menetapkan prinsip – prinsip dan pengembangan teknologi informasi antara lain :

- Melibatkan unsur yang terkait (pemerintah, swasta, profesional).
- Menggunakan pendekatan moderat untuk mensintesiskan prinsip hukum konvensional dan norma hukum baru yang akan terbentuk
- Memperhatikan keunikan dari dunia maya
- Mendorong adanya kerjasama internasional mengingat sifat internet yang global
- Menempatkan sektor swasta sebagai leader dalam persoalan yang menyangkut industri dan perdagangan.
- Pemerintah harus mengambil peran dan tanggung jawab yang jelas untuk persoalan yang menyangkut, kepentingan publik
- Aturan hukum yang akan dibentuk tidak bersifat restriktif melainkan harus direktif dan futuristik

1. Melakukan pengkajian terhadap perundangan nasional yang memiliki kaitan langsung maupun tidak langsung dengan munculnya persoalan hukum akibat transaksi di internet seperti:

UU hak cipta, UU merk, UU perlindungan konsumen, UU Penyiaran dan Telekomunikasi, UU Perseroan Terbatas, UU Penanaman Modal Asing, UU Perpajakan, Hukum Kontrak, Hukum Pidana dll

2.2.4 Undang-undang Informasi dan Transaksi Elektronik

Undang-undang Informasi dan Transaksi Elektronik adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia.

Secara umum, materi Undang-Undang Informasi dan Transaksi Elektronik (UUITE) dibagi menjadi dua bagian besar, yaitu pengaturan mengenai informasi dan transaksi elektronik dan pengaturan mengenai perbuatan yang dilarang.

1. a) Pengaturan mengenai informasi dan transaksi elektronik

Pengaturan mengenai informasi dan transaksi elektronik mengacu pada beberapa instrumen internasional, seperti UNCITRAL Model Law on eCommerce dan UNCITRAL Model Law on eSignature. Bagian ini dimaksudkan untuk mengakomodir kebutuhan para pelaku bisnis di internet dan masyarakat umumnya guna mendapatkan kepastian hukum dalam melakukan transaksi elektronik. Beberapa materi yang diatur, antara lain:

- pengakuan informasi/dokumen elektronik sebagai alat bukti hukum yang sah (Pasal 5 & Pasal 6 UU ITE)
- tanda tangan elektronik (Pasal 11 & Pasal 12 UU ITE)
- penyelenggaraan sertifikasi elektronik (certification authority, Pasal 13 & Pasal 14 UU ITE)
- penyelenggaraan sistem elektronik (Pasal 15 & Pasal 16 UU ITE);

1. b) pengaturan mengenai perbuatan yang dilarang

Beberapa materi perbuatan yang dilarang (cybercrimes) yang diatur dalam UU ITE, antara lain:

- konten ilegal, yang terdiri dari, antara lain: kesusilaan, perjudian, penghinaan/pencemaran nama baik, pengancaman dan pemerasan (Pasal 27, Pasal 28, dan Pasal 29 UU ITE)
- akses ilegal (Pasal 30)
- intersepsi ilegal (Pasal 31)
- gangguan terhadap data (data interference, Pasal 32 UU ITE)
- gangguan terhadap sistem (system interference, Pasal 33 UU ITE)
- penyalahgunaan alat dan perangkat (misuse of device, Pasal 34 UU ITE)

3. Pembahasan

3.1 Website / Situs Web

3.1.1 Definisi Website

Situs web (*Web Site*) atau sering disingkat dengan istilah situs adalah sejumlah halaman web yang memiliki topik saling terkait, terkadang disertai pula dengan berkas-berkas gambar, video, atau jenis-jenis berkas lainnya. Sebuah situs web biasanya ditempatkan setidaknya pada

sebuah server web yang dapat diakses melalui jaringan seperti internet, ataupun jaringan wilayah lokal (LAN) melalui alamat internet yang dikenali sebagai URL. Meskipun setidaknya halaman beranda situs internet umumnya dapat diakses publik secara bebas, pada prakteknya tidak semua situs memberikan kebebasan bagi publik untuk mengaksesnya, beberapa situs web mewajibkan pengunjung untuk melakukan pendaftaran sebagai anggota, atau bahkan meminta pembayaran untuk dapat menjadi anggota untuk dapat mengakses isi yang terdapat dalam situs web tersebut, misalnya situs-situs yang menampilkan pornografi, situs-situs berita, layanan surel (*e-mail*), dan lain-lain. Pembatasan-pembatasan ini umumnya dilakukan karena alasan keamanan, menghormati privasi, atau karena tujuan komersil tertentu.

Sebuah halaman web merupakan berkas yang ditulis sebagai berkas teks biasa (plain text) yang diatur dan dikombinasikan sedemikian rupa dengan instruksi-instruksi berbasis HTML, atau XHTML, kadang-kadang pula disisipi dengan sekelumit bahasa skrip. Berkas tersebut kemudian diterjemahkan oleh peramban web dan ditampilkan seperti layaknya sebuah halaman pada monitor komputer.

3.1.2 Jenis-Jenis Website

1. Berdasarkan **fungsi** & **kegunaan web**
    - **Web Perorangan**, yaitu situs yang digunakan untuk menceritakan tentang biografi diri, pengalaman pribadi, dsb (contoh : Blog Pribadi)
    - **Web Komersial** (Company Profile / Online Shop Website, biasa menggunakan .com, .co.id, dsb), yaitu situs yang dipakai untuk menunjukkan produk dan jasa suatu perusahaan, atau juga dapat melakukan transaksi penjualan online (dengan sistem shopping cart system)
    - **Web Pemerintahan** (di Indonesia menggunakan .gov.id), situs jenis ini hanya boleh dipakai untuk keperluan website pemerintahan yang resmi.
    - **Web Non-Profit** (biasanya menggunakan .org, .edu, dll), **website** jenis-jenis ini biasanya digunakan hanya untuk **yayasan, sekolahan**, dsb.
    -

1. Berdasarkan keberadaan *content management system* (**CMS**) yang ada padanya :
    - **Web Statik** (*Static Website*)

Yaitu situs web yang langsung ditulis dalam bentuk HTML dan berbentuk sederhana seperti web design classic, desain website 5 (lima) halaman, website brosur produk dan jasa.

- **Web Dinamis** (*Dynamic Website*)

  Yaitu situs web yang ditulis dalam bentuk bahasa pemrograman dan database, seperti PHP, ASP, Javascript, Ajax, jQuery, MySQL. Dalam perkembangannya web dinamis menggunakan CMS sebagai back-end untuk administrator web tersebut. Salah satu yang paling terkenal karena sangat *SEO Friendly* adalah *WordPress*. **Web WordPress** sangat handal sekali untuk dipakai sebagai website dinamis karena kecepatan dan struktur front end yang Google Friendly. Membuat web dengan wordpress sangat mudah dan cepat untuk dipelajari. Adapun CMS lain adalah **Joomla**, **Drupal**, dll

  .

3.2 Deface

3.2.1 Pengertian Deface

Deface yang berdasarkan kamus UMUM berarti merusakkan; mencemarkan; menggoresi; menghapuskan tetapi arti kata deface disini yang sangat lekat adalah sebagai salah satu kegiatan merubah tampilan suatu website baik halaman utama atau index filenya ataupun halaman lain yang masih terkait dalam satu url dengan website tersebut (bisa di folder atau di file).

Deface adalah teknik mengganti atau menyisipkan file pada server, teknik ini dapat dilakukan karena terdapat lubang pada sistem security yang ada di dalam sebuah aplikasi. Hal ini bertujuan untuk melakukan perubahan tampilan pada website korban dengan tampilan yang dimiliki oleh si defacer. Deface merupakan sebuah serangan yang dilakukan untuk mengganti visual dari sebuah website. Para hacker biasanya meninggalkan pesan dan nickname mereka agar hasil kerjanya diketahui oleh khalayak hacker.

3.2.2 Jenis-Jenis pen-Deface-an

Deface dapat dibagi menjadi dua jenis berdasarkan dampak pada halaman situs yang terkena serangan terkait.

1. Full of page

Artinya mendeface satu halaman penuh tampilan depan alias file index atau file lainnya yang akan diubah secara utuh, artinya untuk melakukan ini biasanya seorang ‘defacer’ umumnya harus berhubungan secara ‘langsung’ dengan box (mesin) atau usaha mendapatkan priveleged terhadap mesin, baik itu root account atau sebagainya yang memungkinkan defacer dapat secara Interaktif mengendalikan file indek dan lainnya secara utuh. Umumnya dengan memanfaatkan kelemahan kelemahan pada services-services yang berjalan di mesin, sehingga dapat melakukan pengaksesan ke mesin.

1. Sebagian atau hanya menambahi

Artinya, defacer mendeface suatu situs tidak secara penuh, bisa hanya dengan menampilkan beberapa kata, gambar atau penambahan script-script yang mengganggu, hal ini umumnya hanya akan memperlihatkan tampilan file yang di deface menjadi kacau dan umumnya cukup mengganggu, defacer biasanya mencari celah baik dari kelemahan scripting yang digunakan dengan XSS injection, bisa dengan SQL atau database injection dan juga beberapa vulnerabilities yang seringkali ditemukan pada situs-situs yang dibangun dengan menggunakan CMS (Content Manajemen System).

3.2.3 Penyebab terjadinya Deface

1. Penggunaan free CMS dan open source tanpa adanya modification. Keseluruhan konfigurasi menggunanakan default konfigurasi, akan memudahkan para defacer untuk menemukan informasi file, directory, source, database, user, connection, dsb. Bagi para blogger apalagi yang masih newbie melakukan modifikasi konfigurasi engine blog bukanlah merupakan hal yang mudah. Namun tak ada salahnya kita meluangkan waktu mencari berbagai pedoman dan mungkin bisa juga dengan melakukan instalasi plugin untuk keamanan wordpress seperti wp firewall, login lock down, stealth login, dan plugin lainnya untuk keamanan blog.
2. Tidak updatenya source atau tidak menggunakan versi terakhir dari CMS. Hal ini sangat ini rentan, karena security issue terus berkembang seiring masuknya laporan dan bugtrack terhadap source, kebanyakan hal inilah yang menjadi sebab website mudah dideface. Oleh karena hal itu diputuskan untuk melakukan upgrade pada blog ini.

3. Tidak adanya ada research yang mendalam dan detail mengenai CMS sebelum digunakan & diimplementasikan. Sehingga pemahaman dan pengetahuan dari webmaster hanya dari sisi administrasinya saja, tidak sampai ke level pemahaman sourcecode.
4. Tidak adanya audit trail atau log yang memberikan informasi lengkap mengenai penambahan, pengurangan, perubahan, yang terjadi di website baik source, file, directory, dsb. Sehingga kesulitan untuk menemukan, memperbaiki dan menghapus backdoor yang sudah masuk di website.
5. Jarang melakukan pengecekan terhadap security update, jarang mengunjungi dan mengikuti perkembangan yang ada di situs-situs security jagad maya. Sehingga website sudah keduluan di deface oleh sebelum dilakukan update dan patch oleh webmaster.
6. Kurangnya security awareness dari masing-masing personel webmaster & administrator. Sehingga kewaspadaan terhadap celah-celah keamanan cukup minim, kadangkala setelah website terinstall dibiarkan begitu saja. Kurangnya training dan kesadaraan akan keamanan website seperti ini akan menjadikan website layaknya sebuah istana yang tak punya benteng.

3.2.4 Contoh Kasus Deface di Indonesia

a. Situs presiden SBY (*http://www.presidensby.info*)

b. Situs **TV One (**www.tvonenews.tv**)**

3.2.5 Undang-undang ITE mengenai tindak kejahatan deface

Kejahatan tentang Informasi Teknologi dan Elektronik khususnya mengenai kejahatan deface diatur dalam UUD ITE BAB VII MENGENAI PERBUATAN YANG DILARANG, diantaranya :

1. Pasal 30
   - Ayat 1

     Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun.
   - Ayat 2

     Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik.
   - Ayat 3

     Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

2. Pasal 32
    - Ayat 1

      Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik.
    - Ayat 3

      Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.

3. Pasal 35

   Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik
   dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
   Adapun ketentuan pidana yang mengatur tindak pidana tentang kejahatan Informasi Teknologi dan Elektronik, khususnya mengenai kejahatan deface yang disebutkan diatas diatur dalam UUD ITE BAB XI KETENTUAN PIDANA diantaranya :
4. Pasal 46
    - Ayat 1

      Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
    - Ayat 2

      Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).

- Ayat 3

  Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

5. Pasal 48
   - Ayat 1

     Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah).
   - Ayat 3

     Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah).
6. Pasal 51
   - Ayat 1

     Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)

3.2.6 Cara mengatasi website/blog yang terkena deface

1. Download source & database yang ada diwebsite untuk backup. Hal ini berjaga-jaga apabila langkah yang kita lakukan gagal, tetapi apabila konfigurasi & lengkap dijamin 100% berhasil, terkecuali ada sesuatu yang terlewatkan.
2. Download source CMS versi terbaru dari website penyedia CMS, misalkan : http://www.drupal.org, http://www.joomla.org, http://www.wordpress.org, dsb.
3. Lakukanlah perbaikan database secara lokal, berjaga-jaga apabila backdoor ada di database. Biasanya didalam database ada acces user tidak dikenal yang akses levelnya sama dengan Administrator.

4. Install CMS yang tadi sudah didownload diweb hosting. Kemudian lakukanlah konfigurasi : database, file permission, directory permission. Jangan menggunakan default configuration, modifikasilah konfigurasi-konfigurasi yang ada agar lebih powerfull.
5. Kemudian instalasi component: Themes, Plugin, Component, dsb. Gunakanlah yang paling update, atau source baru dari komponen yang akan diinstall(Fresh Install Component).
6. Kemudian update database, dengan login ke Database Control Panel(phpmyadmin, DB Admin, cPanel Database, dsb). Setelah melakukan login, maka importlah database.
7. Gantilah username Administrator & Password menggunakan nama yang lebih Unik, jangan menggunakan user (admin, administrator, adm1n, dsb) gunakanlah yang lebih powerfull dan susah untuk ditebak untuk menghindari bruteforce, gunakanlah alias untuk menampilkan username administrator di web content.

3.2.7 Cara untuk menanggulangi kasus deface

1. Penggunaan Firewall. Tujuan utama dari firewall adalah untuk menjaga agar akses dari orang tidak berwenang tidak dapat dilakukan. Program ini merupakan perangkat yang diletakkan antara internet dengan jaringan internal. Informasi yang keluar dan masuk harus melalui atau melewati firewall. Firewall bekerja dengan mengamati paker *Intenet Protocol* (IP) yang melewatinya
2. Wajib untuk mengikuti perkembangan source dari source website yang digunakan, backuplah website dan database sebelum dilakukan update.
3. Kebanyakan defacer telah memasang backdoor ketika telah berhasil melakukan deface website, hal ini dimungkinkan agar dapat melakukan deface ulang terhadap website. Wajib untuk memeriksa perubahan folder, file, database dan source terakhir dari website
4. Pelajarilah lebih dalam mengenai dasar-dasar hacking dan antisipasinya, contoh hacking yaitu SQL Injection.
5. Sering-seringlah berdiskusi di forum dan milist yang berkaitan dengan perangkat serta aplikasi yang mensupport website, baik dari sisi operating system, tempat hosting, bugtrack milist, developer milist, dsb.
6. Hardening website dan source wajib dilakukan, misalkan jangan menggunakan ”default configuration”, aturlah sedemikian rupa ”configuration website” dengan memperhatikan:

permission, acces level, indexiding, database configuration, password dan user management.

7. Gunakanlah tambahan plugin / component yang tepat, sehingga dapat meminimalisasi terjadinya kegiatan defacing dari thirdparty. Pastikan hasil review & ranking plugin bereputasi baik dan sudah diverified oleh penyedia CMS yang bersangkutan.
8. Lakukanlah penetration testing terhadap website, baik secara lokal maupun langsung di website. Banyak tools penetration testing yang bisa digunakan: Nexus, Acunetix, dsb.

4 Kesimpulan

Berdasarkan pembahasan di atas dapat disimpulkan bahwa semakin maju peradaban dunia dan teknologi dunia maka semakin besar juga tingkat kejahatan yang muncul. Seiring berkembangnya kehidupan dunia maya semakin berkembang pula tingkat kejahatan dunia maya (defacing). Penyerangan dengan cara defacing merupakan suatu tindak kejahatan yang dilakukan untuk merusak suatu tampilan dan konfigurasi fisik dari web. Untuk menanggulanginya dapat menggunakan beberapa cara diantaranya yaitu penggunaan firewall, penggunaan SSL (Secure Socket Layer), menutup service yang tidak digunakan, back up secara rutin, pemantau integritas sistem, adanya cyber law dan adanya dukungan lembaga khusus. Tetapi karena hukum tentang kasus kejahatan cybercrime di dunia kususnya di indonesia yang tidak tegas sehingga menyebabkan pelaku deface tidak jera untuk melakukan ke “jahil” an di dunia maya,justru semakin marak dan bertambah pelaku-pelaku kejahatan di dunia maya.

Referensi:

http://inet.detik.com/read/2013/01/31/135610/2157633/398/menyoal-kasus-hacking-situs-presiden-sby

http://indonesiaindonesia.com/f/98161-website-tv-one-terkena-deface/

https://timsatu.wordpress.com/2015/05/20/makalah-deface-website/

PAPER

Perlindungan dan Pencegahan Serangan

”Distributed Denial of Services (DDoS)”

DISUSUN OLEH :

Nama : Arie Ansyah

Nim : 182420117

PROGRAM PASCASARJANA

MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

2020

DAFTAR ISI

BAB I
PENDAHULUAN

a. Latar Belakang

Apabila bicara masalah keamanan sebuah jaringan, amat sangat rentan terhadap serangan dari berbagai pihak. Alasan dari serangan tersebut tentu saja beragam. Diantaranya yaitu alasan untuk merusak, balas dendam, politik, atau cuma iseng – iseng saja untuk unjuk gigi. Status subkultural dalam dunia hacker, adalah sebuah unjuk gigi atau lebih tepat kita sebut sebagai pencarian jati diri.

Dibutuhkan keamanan yang sangat kuat agar pelaku tidak bisa merusak data-data pada komputer kita. Sering terjadi kasus, dimana resource komputer tiba-tiba penuh diakses oleh banyak pengguna. Serangan seperti itu bisa di lakukan dengan satu host dan banyak host, lalu serangan ini dinamakan "DDos". Dikarenakan ada beberapa penggunaan media komputer dan internet sebagai media untuk melakukan aksi kejahatan pada umumnya dikenal dengan istilah "cryber crime" (kejahatan dunia maya) (Antoni, 2018). *Cyber-crime* juga dapat didefinisikan sebagai perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer yang memiliki basis pada kecanggihan teknologi internet (Antoni, 2018)

DDOS Attack merupakan hal paling sering digunakan oleh para peretas untuk melumpuhkan suatu sistem, banyak sekali berita-berita di berbagai media yang menginformasikan serangan DDOS pada situs-situs yang terkena serang DDOS. Dikutip dari laporan Kaspersky pada Selasa (13/5/2020), serangan DDoS (distributed denial-of-service) mengalami peningkatan signifikan selama tiga bulan pertama 2020. Hal ini disebabkan, pelaku di belakangan serangan DDoS mengambil kesempatan ketika hampir semua kegiatan-baik itu belajar, bekerja, atau bersantai-bergeser ke dalam bentuk online. Peningkatan ini dimanfaatkan pelaku kejahatan siber, yang melakukan serangan terhadap layanan digital paling vital atau yang semakin populer.

Beberapa diantaranya, termasuk Departemen Kesehatan dan Layanan Kemanusiaan pemerintah Amerika Serikat, sejumlah rumah sakit di Paris, dan server gim online adalah beberapa contoh target serangan DDoS pada bulan Februari dan Maret.

b. Tujuan

Maksud penulisan makalah ini adalah :

1. Untuk memberikan pengetahuan kepada pembaca tentang kejahatan yang terjadi di dunia maya.
2. Menjelaskan contoh kasus *cybercrime* yaitu DDos.
3. Menjelaskan perundang-undangan yang berlaku dan berkaitan dengan *cybercrime* serta hukuman yang berlaku atas tindakan illegal tersebut.
4. Memberikan info bagaimana cara menanggulangi masalah kejahatan DDos

BAB II
LANDASAN TEORI

DDos merupakan kependekan dari *Distributed Denial of Service* atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi (NIAGAHOSTER, 2018)**.** DDos adalah jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan. Umumnya serangan ini dilakukan menggunakan beberapakan komputer host penyerang sampai dengan komputer target tidak bisa diakses (NIAGAHOSTER, 2018).

DDos merupakan serangan yang sangat populer digunakan oleh hacker. Selain mempunyai banyak jenis, DDos memiliki konsep yang sangat sederhana, yaitu membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari user lain (*overload)* (NIAGAHOSTER, 2018). Salah satu cara dengan mengirimkan *request* ke server secara terus menerus dengan transaksi data yang besar.

Cara penanggulangannya pun menarik untuk di bahas dan kita tidak akan tau apakah kita akan menjadi target selanjutnya. Sedangkan, dunia maya sendiri merupakan dunia yang sulit di tebak, kita tidak tau dengan benar dan tepat siapa yang kita ajak komunikasi. Maka ingatkan suatu kutipan "*Don't trust anyone in cyber, be paranoid"*.Sebelum pembahasan lebih lanjut, ada baiknya kita terlebih dahulu mengetahui apa itu serangan Denial of Service(DoS). **Denial of Service** atau yang mungkin lebih sering kita dengar dengan nama **DoS** merupakan suatu aktifitas yang menghambat laju kerja dari sebuah layanan atau malah mematikannya sehingga yang dapat menyebabkan pengguna yang asli/sah/memiliki hak akses tidak dapat menggunakan layanan. Dimana pada akhirnya, serangan ini mengakibatkan terhambatnya aktifitas yang akan dilakukan oleh korban yang akibatnya boleh dibilang sangat fatal.

DoS merupakan serangan yang cukup menakutkan di dunia internet karena akibat dari serangan ini server akan mati dan tidak dapat beroperasi lagi sehingga otomatis tidak dapat meberikan pelayanan lagi. DoS memiliki beberapa jenis serangan, diantaranya adalah

1. Ping of Death
2. Teardrop
3. SYN Attack

4. Land Attack
5. Smurf Attack
6. UDP Flood

Selain itu, agar komputer atau mesin yang diserang lumpuh total karena kehabisan resource dan pada akhirnya komputer akan menjadi hang, maka dibutuhkan resource yang cukup besar untuk seorang penyerang dalam melakukan aksi penyerangannya terhadapa sasaran. Berikut ini merupakan beberapa resource yang dihabiskan :

1. **SwapSpace**.Swap spase biasanya digunakan untuk mem-forked child proses.
2. **Bandwidth.**Dalam serangan DoS, bukan hal yang aneh bila bandwith yang dipakai oleh korban akan dimakan habis.
3. **Kernel Tables**.Serangan pada kernel tables, bisa berakibat sangat buruk pada sistem. Alokasi memori kepada kernel juga merupakan target serangan yang sensitif. Kernel memiliki kernelmap limit, jika sistem mencapai posisi ini, maka sistem tidak bisa lagi mengalokasikan memory untuk kernel dan sistem harus di re-boot.
4. **RAM.** Serangan Denial of Service banyak menghabiskan RAM sehingga sistem mau-tidak mau harus di re-boot.
5. **Disk.** Serangan klasik banyak dilakukan dengan memenuhi Disk.

data diatas merupakan beberapa bagian dari resource yang dihabiskan oleh serangan DoS. Ada beberapa hal yang harus di perhatikan sebelum melakukan penyerangan DoS:

- Serangan membutuhkan Shell Linux (Unix/Comp)
- Mendapatkan exploits di: http://packetstormsecurity.nl (gunakan fungsi search agar lebih mudah)
- Menggunakan/membutuhkan GCC (Gnu C Compiler)

Alasan Penyerangan

Banyak sekali motf yang melandasi penyerangan yang menggunakan denial of service ini. Seperti yang dijelas kan oleh **"**Hans Husman" (t95hhu@student.tdb.uu.se) serangan ini dapat terjadi baik karena alasan politik, balas dendam, alasan ekonomi, maupun memang untuk aksi kejahatan.

BAB III
PEMBAHASAN

a. Serangan DDos

Bukan suatu hal yang mustahil bagi siapa saja yang ingin melakukan serangan DoS. DoS merupakan jenis serangan yang menyerang layanan publik. Dan cara yang paling gampang yang sebenarnya bisa kita lakukan dengan cara menutup layanan publik tersebut. Tapi itu hal yang tidak mungkin karena bukan atas dasar iseng saja orang menghubungkan ke jaringan luas, akan tetapi memang adanya keperluan-keperluan. yang mengharuskan hal tersebut terjadi.

Seperti yang sudah dibahas pada bab sebelumnya, behwa serangan DoS merupakan serangan yang melumpuhkan kinerja server bahkan sampai menyebabkan server crass. Beberapa hal yang akan dilakukan dalam sistem penyerangan DoS yaitu diantaranya :

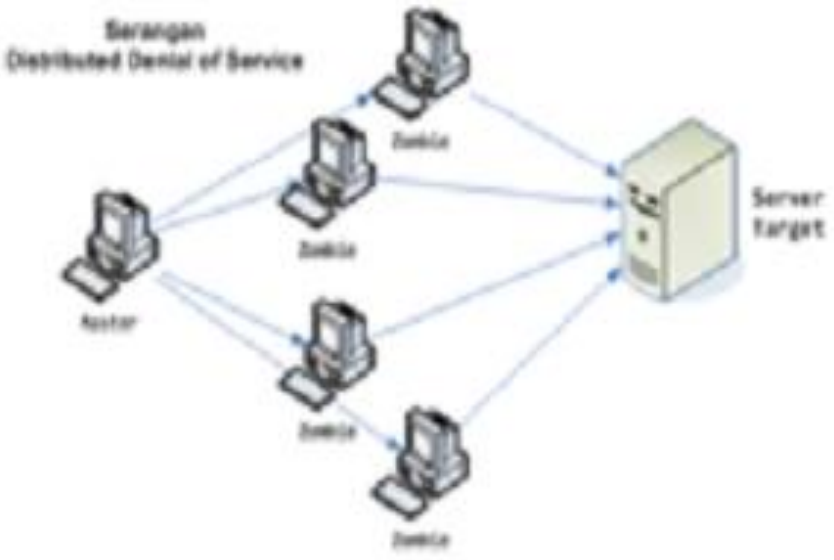
1. Aktifitas 'flooding' terhadap suatu server.
2. Memutuskan koneksi antara 2 mesin.
3. Mencegah korban untuk dapat menggunakan layanan
4. Merusak sistem agar korban tidak dapat menggunakan layanan.

Pada dunia maya terdapat dua istilah yang sudah sangat sering kita dengar, yaitu ”hacker” dan ”krecker”. Hacker merupakan orang yang biasanya melakukan penetrasi/scaning terhadap sebuah situs untuk mencari kelemahan-kelemahan dari situs tersebut. Akan tetapi seorang hacker tidak pernah melakukan pengrusakan ataupun mengubah data. Melainkan mereka akan memberitahukan pada admin bahwa terdapat cela yang harus diperbaiki untuk penjegahan agar tidak terjadi hal-hal yang merugukan. Sementara cracker kebalikan dari hacker, seorang crecker akan melakukan pengrusakan, pengubahan data,penyalah gunaan hak akses dan sebagainya(tindakan kejahatan). Banyak hal yang melatar belakangi seorang crecker berbuat jahat, baik motif balas dendam, mengeruk keuntungan berupa uang, dan sebagainya. Dalam dunia hack, juga terdapat istilah hacker topi putih, yaitu merupakan sebutan bagi seorang crecker yang sudah tobat, tidak menggunakan keakhliannya untuk hal-hal jahat lagi.

”**Zombie”**

Menurut saya seorang penyerang itu seorang pengecut, kenapa saya beranggapan begitu?? Karena pada saat seorang penyerang melakukan serangan DoS kepada korbannya, biasanya mereka tidak langsung melakukan penyerang melalui jaringan internetnya sendiri (IP addnya sendiri), melainkan merekan akan melakukan peloncatan menggunakan yang namanya ”zombie”. Zombie adalah sebuah komputer (tentunya milik orang lain) yang menjadi di pergunakan untuk proses penyerangan.

Biasanya para penyerang tidak hanya sekali saja melakukan pelompatan, melewati para zombie, melaikan banyak, agar jejak mereka tidak terlacak. Pada umumnya si komputer yang dijadikan alat zombie, mereka tidak tahu kalu mereka sudah dimanfaatkan sebagai batu loncatan dalam penyerangan.



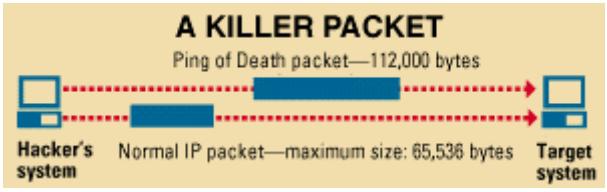
Jenis-jenis serangan Denial of Service (DoS) dan Penanggulangannya

Bagi para penyerang, tidak lah sulit untuk m,elakukan penyerangan, biasanya penyerang akan di bantu dengan program-program, Program-program DoS itu sendiri terdiri dari nestea, teardrop, land, boink,jolt dan vadim. Tidak begitu sulit untuk mendapatkan program-program ini. Berikut ini penjelasan dari macam-macam penyerangan DoS:

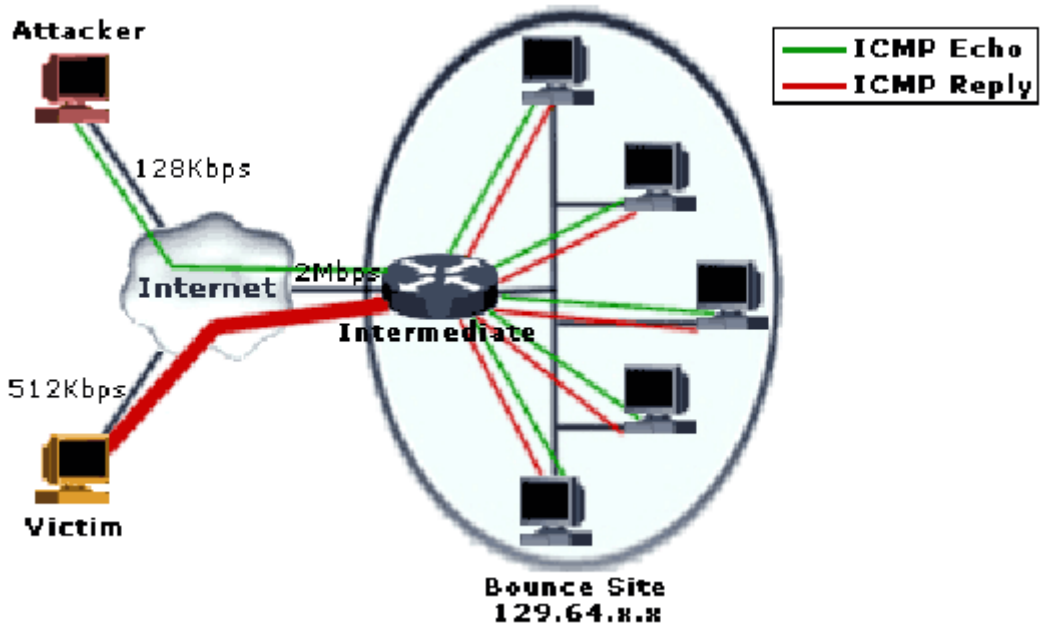
Ping of Death

Ping of Death merupakan jenis serangan yang sudah tidak baru lagi, semua vendor sistem operasi sudah memperbaiki sistemnya. Jenis serangan ini menggunakan utility ping yang ada pada sistem operasi komputer. Ping ini digunakan untuk mengecek waktu yang akan diperlukan untuk mengirim data tertentu dari satu komputer ke komputerlainnya. Panjang

maksimum data menurut TCP protocol IP adalah 65,536 byte.



Selain itu, paket serangan Ping of Death dapat dengan mudah dispoof atau direkayasa sehingga tidak bisa diketahui asal sesungguhnya dari mana, dan penyerang hanya perlu mengetahui alamat IP dari komputer yang ingin diserangnya



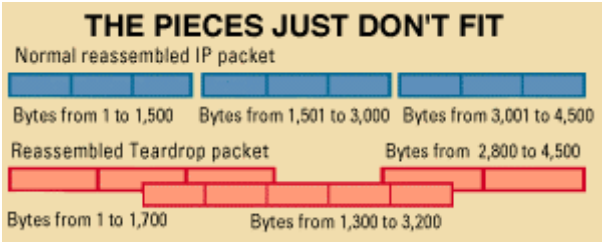
Penyerang dapat mengirimkan berbagai paket ICMP (digunakan untuk melakukan ping) yang terfragmentasi sehingga waktu paket-paket tersebut disatukan kembali, maka ukuran paket seluruhnya melebihi batas 65536 byte.Contoh yang sederhana adalah sebagai berikut: C:\windows>ping -l 65540 Perintah MSDOS di atas melakukan ping atau pengiriman paket ICMP berukuran 65540 byte ke suatu host/server.

Pada jenis serangan ini, data yang akan dikirim melebihi panjang maksimum yang disediakan. Jika sistem tidak siap pada saat penerimaan data, maka sistem akan hang, crash atau reboot.

Teardrop

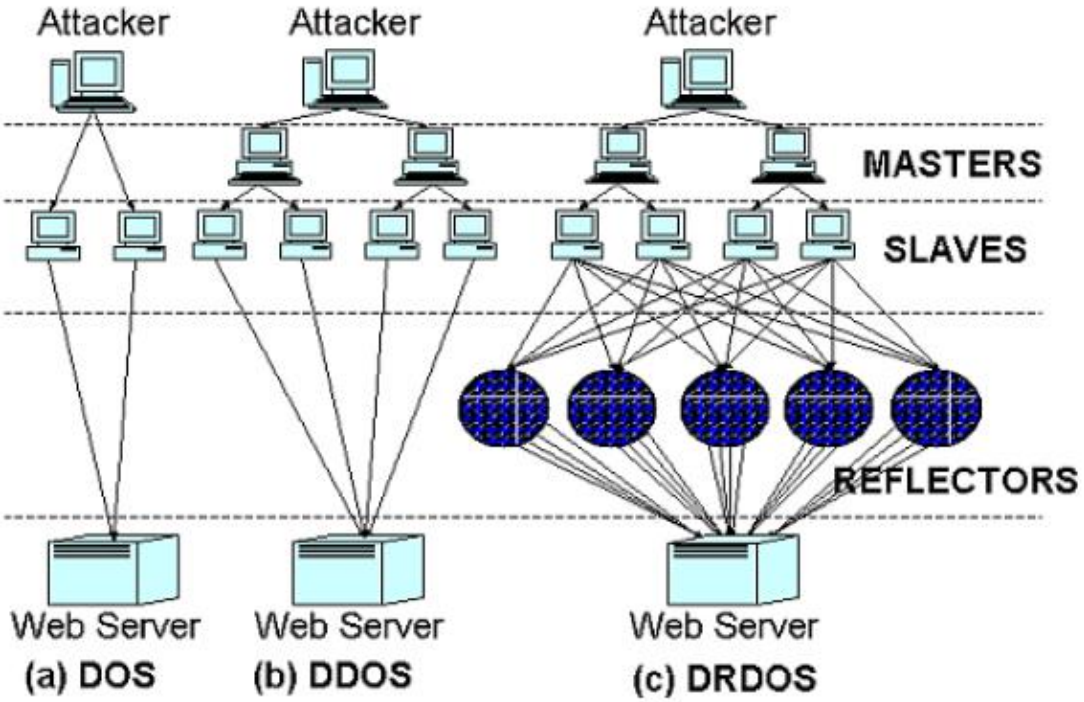
Teardrop attack adalah suatu serangan bertipe Denial of Service (DoS) erhadap suatu server/komputer yang terhubung dalam suatu jaringan.

Teardrop attack ini memanfaatkan fitur yang ada di TCP/IP yaitu packet fragmentation atau pemecahan paket, dan kelemahan yang ada di TCP/IP pada waktu paket-paket yang terfragmentasi tersebut disatukan kembali. Jenis serangan ini. dikembangkan dengan cara mengeksplotasi proses disassembly-reassembly paket data. Dalam jaringan Internet, seringkali data harus di potong kecil-kecil untuk menjamin reliabilitas & proses multiple akses jaringan. Potongan paket data ini, kadang harus dipotong ulang menjadi lebih kecil lagi pada saat di salurkan melalui saluran Wide Area Network (WAN) agar pada saat melalui saluran WAN yang tidak reliable proses pengiriman data menjadi lebih reliable.



Pada proses pemotongan data paket yang normal setiap potongan di berikan informasi offset data yang kira-kira berbunyi “potongan paket ini merupakan potongan 600 byte dari total 800 byte paket yang dikirim”. Program teardrop akan memanipulasi offset potongan data sehingga akhirnya terjadi overlapping antara paket yang diterima di bagian penerima setelah potongan-potongan paket ini di reassembly. Misalnya ada data sebesar 4000 byte yang ingin dikirim dari komputer A ke komputer B. Maka, data tersebut akan dipecah menjadi 3 paket demikian:

Di komputer B, ketiga paket tersebut diurutkan dan disatukan sesua dengan OFFSET yang ada di TCP header dari masing-masing paket. Terlihat di atas bahwa ketiga paket dapat diurutkan dan disatukan kembali menjadi data yang berukuran 4000 byte tanpa masalah.



gap dan overlap pada waktu paket-paket tersebut disatukan kembali. Byte 1501 sampai 1600 tidak ada, dan ada overlap di byte 2501 sampai 3100.

Akibat dari serangan :

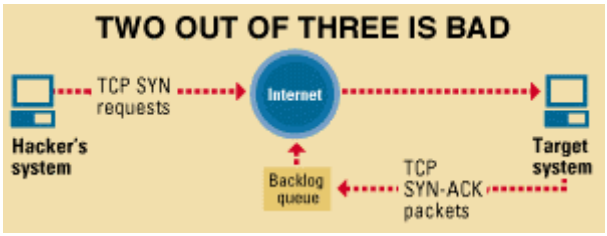
Pada waktu server yang tidak terproteksi menerima paket-paket Seringkali, overlapping ini enimbulkan system yang crash, hang & reboot di ujung sebelah sana.

Penanggulangan :

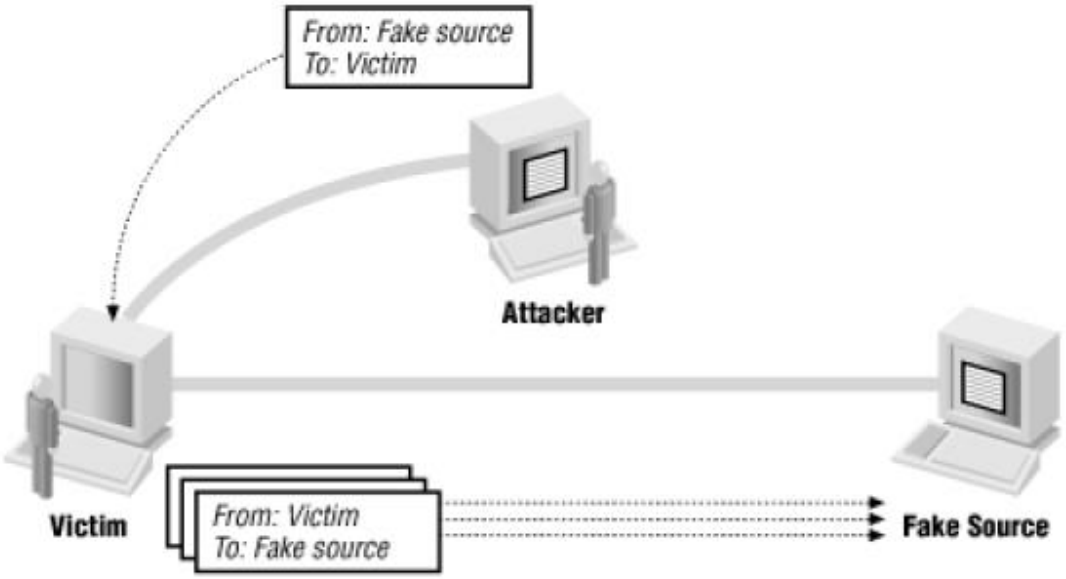
Server bisa diproteksi dari tipe serangan teardrop ini dengan paket filtering melalui firewall yang sudah dikonfigurasi untuk memantau dan memblokir paketpaket yang berbahaya seperti ini.

SYN flood Attack

SYN-Flooding merupakan network Denial ofService yang memanfaatkan 'loophole' pada saat koneksi TCP/IP terbentuk. Kernel Linux terbaru (2.0.30 dan yang lebih baru) telah mempunyai option konfigurasi untuk mencegah Denial of Service dengan mencegah/menolak cracker untuk mengakses sistem.



Pada kondisi normal, client akan mengirimkan paket data berupa SYN (synchronization) untuk mensincrokan pada server. Lalu server akan menerima request dari client dan akan memberikan jawaban ke client berupa ACK (Acknowledgement). Sebagai tanda bahwa transaksi sudah dimulai (pengiriman & penerimaan data), maka client akan mengirimkan kembali sebuah paket yang berupa SYN lagi. Jenis serangan ini akan membajiri server dengan banyak paket SYN. Karena setiap pengiriman paket SYN oleh client, server pasti akan membalasnya dengan mengirim paket SYN ACK ke client. Server akan terus mencatat dan membuat antrian backlog untuk menungu respon ACK dari client yang sudah mengirim paket SYN tadi. Biasanya memori yang disediakan untuk backlog sangat kecil, . Pada saat antrian backlog ini penuh, sistem tidak akan merespond paket TCP SYN lain yang masuk – dalam bahasa sederhana-nya sistem tampak bengong / hang. Sialnya paket TCP SYN ACK yang masuk antrian backlog hanya akan dibuang dari backlog pada saat terjadi time out dari timer TCP yang menandakan tidak ada responds dari pengirim.
Land attack merupakan salah satu jenis serangan SYN, karena menggunakan paket SYN (synchronization) pada saat melakukan 3-way Handshake untuk membentuk suatu hubungan TCP/IP antara client dengan server. Namun jenis serangan ini sudah tidak efektif lagi karena hampir pada setiap sistem sudah di proteksi melalui paket filtering ataupun firewall.



Berikut ini merupakan langkah –langkah yang akan dilakukan dalam melancarkan serangan land :

- pertama-tama client akan mengirimkan sebuah paket pada server/host. Paket yang dikirim yaitu berupa paket SYN.
- Setelah itu server/host akan menjawab permintaan dari client tersebut dengan cara mengirim paket SYN/ACK (Synchronization/Acknowledgement)
- Stelah server mengirimkan balasan atas permintaan dari client, client punt akan kembali menjawab dengan cara mengirimkan sebuah paket ACK kembali pada server. Dengan demikian hubungan antara clien dengan server sudah terjalin, sehingga transfer data bisa dimulai.
- Client yang bertindak sebagai penyerang akan mengirimkan sebauh paket SYN ke server yang sudah di Dispoof (direkayasa). Paket data yang sudah direkayasa tersebut akan berisikan alamat asal (source address) dan port number asal (alamat dan port number dari server). Dimana akan sama persis dengan alamat tujuan (destination source) dan nomor port tujuan (destination port number). Pada saat server/host mengirimkan SYN/ACKK kembali ke pada si client, maka akan terjadi suatu infinite loop. Karena sebenarnya si server bukan mengirimkan paket tersebut ke client melainkan pada dirinya sendir.

Akibat dari serangan :

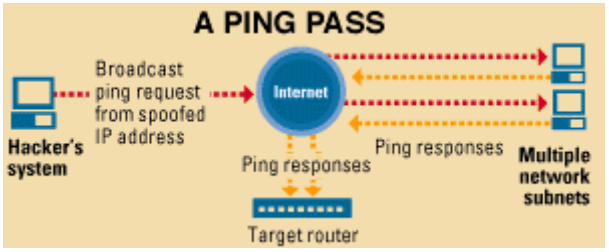
Seandainya server/host tersebut belum terproteksi terhadap jenis serangan ini, server akan crash/ hang.

Penanggulangan :

Cara mencegahnya yaitu dengan cara memproteksi sistem dengan paket filtering atau firewall.

Smurf Attack

Smurf attack adalah serangan secara paksa pada fitur spesifikasi IP yang kita kenal sebagai direct broadcast addressing. Seorang Smurf hacker biasanya membanjiri router kita dengan paket permintaan echo Internet Control Message Protocol (ICMP) yang kita kenal sebagai aplikasi ping.



Karena alamat IP tujuan pada paket yang dikirim adalah alamat broadcast dari jaringan anda, maka router akan mengirimkan permintaan ICMP echo ini ke semua mesin yang ada di jaringan. Kalau ada banyak host di jaringan, maka akan terhadi trafik ICMP echo respons & permintaan dalam jumlah yang sangat besar.

Akibat dari serangan :

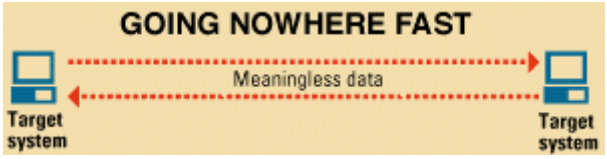
jika si hacker ini memilih untuk men-spoof alamat IP sumber permintaan ICMP tersebut, akibatnya ICMP trafik tidak hanya akan memacetkan jaringan komputer perantara saja, tapi jaringan yang alamat IP-nya di spoof – jaringan ini di kenal sebagai jaringan korban (victim). Untuk menjaga agar jaringan kita tidak menjadi perantara bagi serangan Smurf ini, maka broadcast addressing harus di matikan di router kecuali jika kita sangat membutuhkannya untuk keperluan multicast, yang saat ini belum 100% di definikan. Alternatif lain, dengan cara memfilter permohonan ICMP echo pada firewall.

Penanggulangan :

Untuk menghindari agar jaringan kita tidak menjadi korban Smurf attack, ada baiknya kita mempunyai upstream firewall (di hulu) yang di set untuk memfilter ICMP echo atau membatasi trafik echo agar presentasinya kecil dibandingkan trafik jaringan secara keseluruhan.

UDP Flood

UDP flood merupakan serangan yang bersifat connectionless, yaitu tidak memperhatikan apakah paket yang dikirim diterima atau tidak. flood attack akan menempel pada servis UDP chargen di salah satu mesin, yang untuk keperluan "percobaan" akan mengirimkan sekelompok karakter ke mesin lain, yang di program untuk meng-echo setiap kiriman karakter yang di terima melalui servis chargen. Karena paket UDP tersebut di spoofing antara ke dua mesin tersebut, maka yang terjadi adalah banjir tanpa henti kiriman karakter yang tidak berguna antara ke dua mesin tersebut.



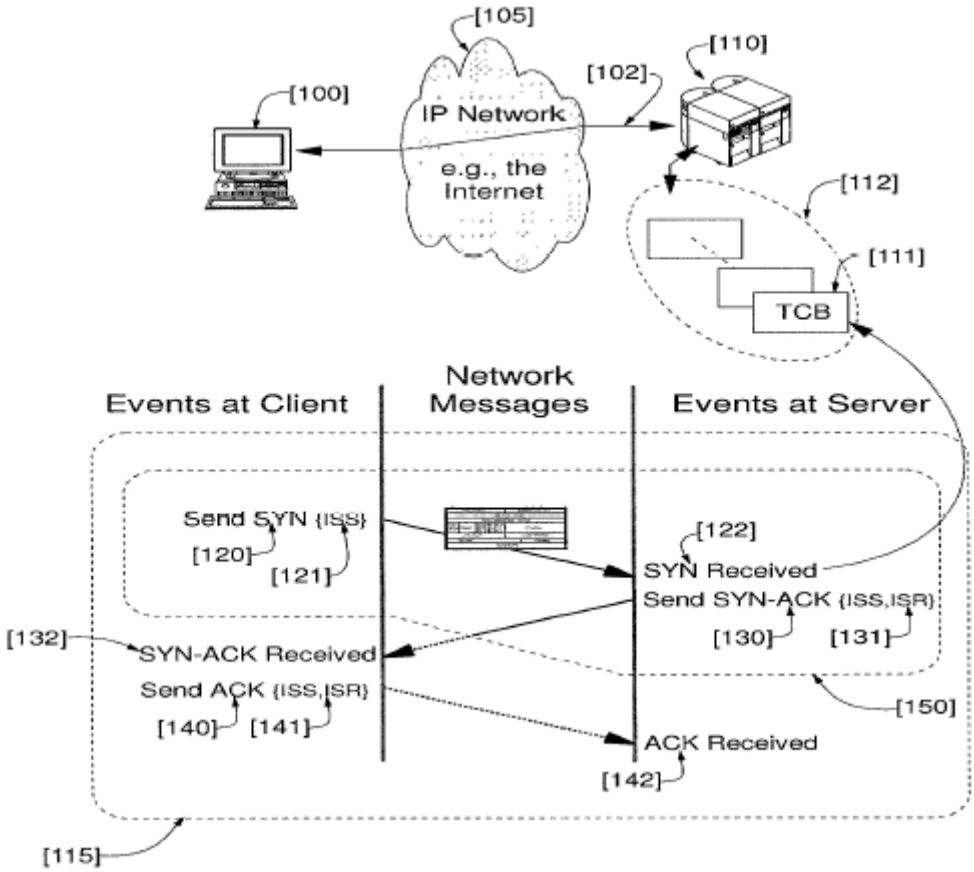
Penanggulangan :

Untuk menanggulangi UDP flood, anda dapat men-disable semua servis UDP di semua mesin di jaringan, atau yang lebih mudah memfilter pada firewall semua servis UDP yang masuk. Karena UDP dirancang untuk diagnostik internal, maka masih aman jika menolak semua paket UDP dari Internet. Tapi jika kita menghilangkan semua trafik UDP, maka beberapa aplikasi yang betul seperti RealAudio, yang menggunakan UDP sebagai mekanisme transportasi, tidak akan jalan. Bisa juag dengan menggunakan IDS dan catat dari log sistem yang biasanya dari port 53, tutp ip address source dan destination.

UDP Bomb Attack

UDP Bomb attack adalah suatu serangan bertipe Denial of Service (DoS)
terhadap suatu server atau komputer yang terhubung dalam suatu jaringan. Untuk melakukanserangan UDP Bomb terhadap suatu server, seorang penyerang mengirim

sebuah paket UDP (User Datagram Protocol) yang telah dispoof atau direkayasa sehingga berisikan nilai-nilai yang tidak valid di field-field tertentu.



Jika server yang tidak terproteksi masih menggunakan sistem operasi (operating system) lama yang tidak dapat menangani paketpaket UDP yang tidak valid ini, maka server akan langsung crash. Contoh sistem operasi yang bisa dijatuhkan oleh UDP bomb attack adalah SunOS versi 4.1.3a1 atau versi sebelumnya.

Penanggulangan :

Kebanyakan sistem operasiakan membuang paket-paket UDP yang tidak valid, sehingga sistem operasi tersebut tidak akan crash. Namun, supaya lebih aman, sebaiknya menggunakan paket filtering melalui firewall untuk memonitor dan memblokir serangan seperti UDP Bomb attack.

b. Tinjauan Pelanggaran

Undang-Undang Nomor 11 Tahun 2008 Tentang Internet dan Transaksi Elektronik (ITE) adalah UU yang mengatur tentang informasi serta transaksi elektronik, atau teknologi informasi secara umum.

Adapun pasal-pasal yang dapat menjerat pelaku serangan DoS dan DDoS adalah sebagai berikut:

a. Pasal 30 ayat (1 dan 3)

Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik orang lain dengan cara apa pun.

Ancaman pidana Pasal 46 ayat (1). Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).

(1) Setiap orang dengan sengaja dan tanpa hak atau melawan hokum mengakses Komputer atau Sistem Elektronik milik orang lain dengan cara apapun.

(2) Setiap orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer atau Sistem Elektronik dengan cara apapun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.

Ancaman pidana Pasal 46 ayat (3) Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun atau denda paling banyak Rp.800.000.000,00 (Delapan Ratus Juta Rupiah).

b. Pasal 33

Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apapun yang berakibat terganggunya Sistem Elektronik atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.

Ancaman pidana Pasal 49, setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun atau denda paling banyak Rp.10.000.000.000,00 (Sepuluh Miliar Rupiah).

BAB IV
KESIMPULAN

a. **Kesimpulan**

Dari hasil penulisan makalah ini serta prmbahasan dari semua bab-bab diatas dapat disimpulkan sebagai berikut :

1. *Cybercrime* adalah kejahatan yang dilakukan secara illegal oleh orang yang tidak bertanggung jawab atas kejahatan yang dilakukannya di dunia maya atau internet, contohnya DDos..
2. *DDos* adalah Sebuah serangan yang dilakukan dengan cara membanjiri atau memenuhi sumber daya atau *resource* komputer agar pengguna tidak dapat mengakses layanan.
3. Terdapat banyak sekali varian dari serangan Denial os Service, diantaranya yang paling sering terjadi yaitu ping of death, teardrop, SYN flood attack, Smurf Attack, UDP boms attack, dan masih banyak lagi

b. **Saran**

Dari penulisan makalah ini serta penjelasan diatas kami dapat membuat saran sebagai berikut :

1. Lakukan sesering mungkin terhadap bug-bug dengan cara melakukan back-up secara berkala.
2. Gunakan *firewall* agar kemungkinan serangan ini tidak melakukan serangan-serangan data terhadap komputer anda.

DAFTAR PUSTAKA

Antoni, A. (2018). Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online. *Nurani: Jurnal Kajian Syari'ah Dan Masyarakat*, *17*(2), 261–274. https://doi.org/10.19109/nurani.v17i2.1192

Geges, S., & Wibisono, W. (2015). Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle. *JUTI: Jurnal Ilmiah Teknologi Informasi*, *13*(1), 53. https://doi.org/10.12962/j24068535.v13i1.a388

https://help.idcloudhost.com/panduan-umum-web-hosting/cara-mengatasi-serangan-ddos-distributed-denial-of-service-attack

https://berbagiilmukomputerbersama.wordpress.com/jenis-jenis-serangan-denial-of-service-attack-dos-attack-dan-cara-mengatasinya/

https://www.niagahoster.co.id/blog/ddos-adalah/

http://group2ddos.blogspot.com/2017/04/uu-ite-yang-dapat-menjerat-ddos.html

DISTRIBUTED DENIAL OF *SERVICE* (DDOS)

A. PENDAHULUAN

Teknologi internet saat ini berkembang dengan pesat, begitu pula dengan jumlah penggunanya yang semakin banyak. Internet tidak lagi hanya digunakan sebagai sarana bertukar informasi, namun mulai digunakan untuk keperluan komersial, misalnya saja sebagai sarana transaksi pembayaran. Hal ini tentu

menyebabkan sejumlah besar data berharga semakin banyak beredar melalui jaringan internet. Namun, dari waktu ke waktu semakin banyak celah keamanan internet yang ditemukan dan disalahgunakan oleh para penjahat elektronik. Lebih spesifik lagi, motif yang melatarbelakangi penyalahgunaan internet belakangan ini sudah berbeda dengan motif tradisional (untuk menyerang *server* atau perangkat lain dalam jaringan), serangan yang dilakukan saat ini dimaksudkan untuk memperoleh keuntungan finansial [6]. Hal ini tentu menjadi ancaman baru yang membahayakan jutaan orang yang menggunakan internet dalam beraktivitas. Contoh serangan yang dapat dilakukan melalui internet antara lain, pencurian informasi pribadi oleh para penjahat elektronik yang dapat menyebabkan kerugian keuangan yang signifikan, internet digunakan untuk mengirim *spam mail*, hingga sebagai sarana meluncurkan serangan *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS).

Sampai saat ini, serangan DoS dan DDoS masih belum memiliki metode pencegahan yang dapat diterapkan pada semua jenis DoS dan DDoS. Hal ini disebabkan karena manajemen dan serangan DoS/DDoS memiliki mekanisme yang bervariasi, para *hacker* juga terus mengembangkan metode serangan yang sudah ada, bahkan menggunakan metode baru untuk melakukan penyerangan. Saat ini, terdapat beberapa pendekatan untuk memerangi serangan DoS/DDoS. Perlindungan terhadap serangan DoS/DDoS yang dapat dilakukan dari sisi *server* adalah dengan menerapkan protokol yang mengatur penggunaan sumber daya *server* dengan tujuan untuk mengurangi eksploitasi sumber daya yang dimiliki *server*.

Dalam penelitian ini, penulis mengemukakan sebuah rancangan protokol untuk melakukan verifikasi *service request* kepada *web service*. Protokol ini memanfaatkan karakteristik utama serangan DDoS (*Network Behavior*) dan mengkombinasikannya dengan metode *Client Puzzle*. Proses verifikasi ini dapat dilakukan diluar *server* sehingga tidak mengurangi kinerja *server* untuk menyediakan layanan.

B. Literature Review

A. Perumusan Masalah

Masalah utama yang menjadi sorotan dalam penelitian ini adalah peluang terjadinya serangan DDoS melalui *service request* dalam jumlah besar sehingga dapat melumpuhkan kinerja *web service*. Untuk menangani masalah ini, penulis mengemukakan sebuah metode pengamanan *web service* dari sisi penyedia layanan. Pendekatan ini dilakukan dengan melakukan filtrasi dan validasi *service request* menggunakan *Network Behavior Analysis* dan *Client Puzzle* sehingga layanan yang dilayani oleh *web service* adalah *service request* yang sah. Dari sini, permasalahan berkembang ke karakreristik jaringan DDoS apa yang yang dapat dijadikan parameter serangan, mekanisme *Client Puzzle* yang dijalankan untuk validasi, serta bagaimana melakukan integrasi *Network Behavior Analysis* dengan *Client Puzzle* sehingga dapat menjaga kemampuan sistem melayani permintaan yang sah.

B. Literatur

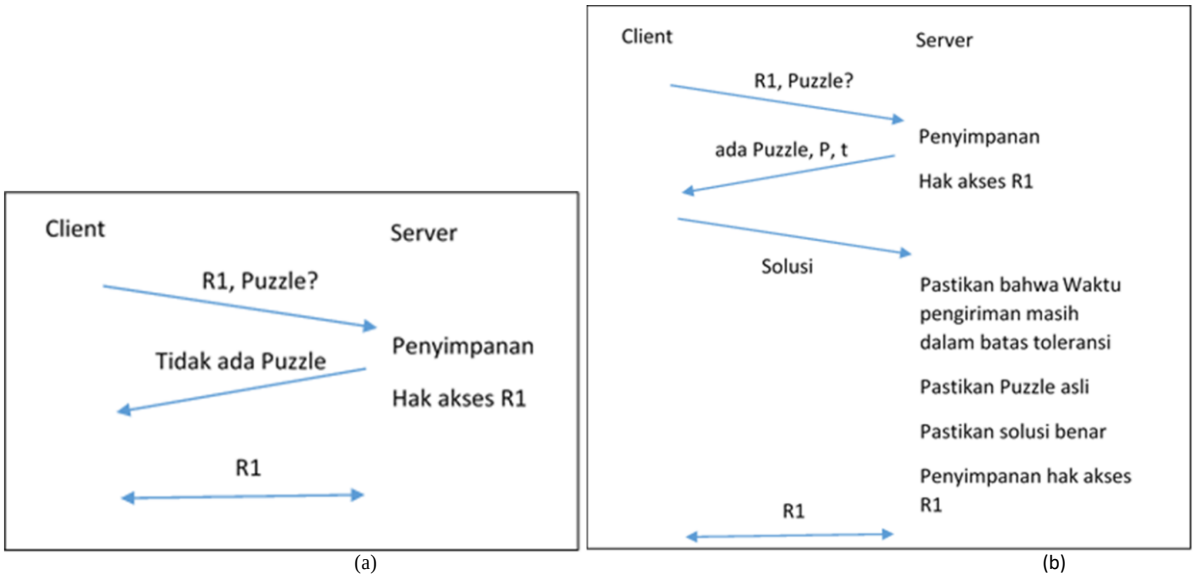
Setelah mengetahui permasalahan yang dihadapi, langkah selanjutnya adalah melakukan pengkajian materi yang berkaitan dengan topik penelitian yang diambil. Pada penelitian ini, referensi yang digunakan adalah jurnal- jurnal yang berkaitan dengan DoS, DDoS, dan Client Puzzle. Selain itu, short paper yang termuat pada prosiding- prosiding, artikel ilmiah yang terkait dan situs-situs penyedia informasi yang terkait. Dari studi literatur yang telah dilakukan maka diperoleh informasi yang berkaitan dengan penelitian yang dilakukan ini, seperti berikut:

a. Tipe serangan DoS dan DDoS, karakteristik dari serangan tersebut dan bagaimana serangan DoS dan DDoS dilancarkan.
b. Penelitian-penelitian terkait dengan pertahanan terhadap serangan DoS dan DDoS.
c. Teknik pengamanan web service yang sudah ada, terutama yang berkaitan dengan pengamanan dari sisi korban/server penyedia layanan.
d. Protokol dan arsitektur yang mendukung pengamanan web service, terutama protokol Client Puzzle.

Dari studi literatur, dapat disimpulkan juga mengenai kondisi pada saat serangan terjadi:

a. DoS: Kalau ada request dari alamat IP yang sama untuk fungsi yang sama dalam jumlah besar dalam rentang waktu yang hampir bersamaan
b. DDoS: Kalau ada request dari sejumlah alamat IP untuk fungsi yang sama dalam jumlah besar dalam rentang waktu tertentu (memperlihatkan aktifitas grup)

Kedua hasil observasi diatas dapat dijadikan sebagai indikator terjadinya serangan DoS/DDoS.



Gambar. Protokol *Client Puzzle* ketika diakses oleh *client* yang berhak (a) dan ketika melakukan validasi *client* (b)

C. Pembahasan

sistem dilakukan dengan dua pendekatan yang disesuaikan dengan tujuan evaluasi sistem. Untuk melakukan uji coba fungsionalitas sistem, pengujian dilakukan secara menyeluruh yaitu mencakup *Network Behavior Analysis* dan dan terus dilanjutkan dengan *Client Puzzle* (Hasil dari metode *Network Behavior Analysis* menjadi masukkan bagi metode *Client Puzzle*). Dengan perlakuan ini, maka dapat terbukti bahwa sistem yang dibangun dapat menyelesaikan permasalahan DDoS dengan baik. Untuk uji coba performa sistem, pengujian dilakukan secara

terpisah sehingga bisa didapatkan performa yang akurat dari masing-masing komponen sistem deteksi DDoS.

1. Hasil uji coba fungsionalitas sistem
   Mekanisme deteksi DDoS diuji dengan melihat melihat kemampuan sistem untuk menyelesaikan mekanisme *Network Behavior Analysis* dan *Client Puzzle* dengan baik. Proses pengujuan dimulai dengan menjalankan program *request logger* yang bertugas menerima permintaan layanan, kemudian menjalankan *puzzle provider* yang bertugas memberikan *puzzle*. Begitu *puzzle provider* sudah berjalan, baru kemudian kita jalankan *client* sebagai *service requeste*r yang meminta layanan. Gambar 8 menunjukkan hasil output dari proses eksekusi protokol deteksi DDoS. Pada pengujian fungsionalitas ini, dijalankan serangan DDoS.
   Serangan DDoS dilancarkan dengan melakukan *request* secara terus-menerus ke satu *service* yaitu penjumlahan. Ketika serangan berlangsung, *client* yang *legitimate* pun mengakses *service* penjumlahan ini. Dari percobaan yang dilakukan, terbukti bahwa walaupun sedang mengalami serangan DDoS, layanan penjumlahan masih dapat diberikan kepada *client* yang *legitimate*.

2. Hasil uji coba performa sistem
   Pada bagian ini, akan diuji performa sistem dalam mendeteksi serangan DDoS. Tujuan awal sistem (*Network Behavior Analysis*) adalah mendeteksi nama *web service* yang diserang DDoS dan mengidentifikasi alamat IP mana saja yang terlibat dalam penyerangan DDoS. Untuk dapat menilai performa dalam melakukan fungsionalitasnya, digunakan pendekatan *recall* dan *precision*. Pada pengujian performa ini, digunakan data uji *log* yang merepresentasikan 9660 *service request*, 10 *web service*, dan pola serangan DDoS (terdapat satu *web service* yang diakses secara serentak dan dalam jumlah permintaan layanan yang banyak). Nilai *threshold* kepadatan yang diujikan berada pada rentang interval 0 <= *threshold* <=1 dengan ketelitian dua angka di belakang koma

   Dari hasil *Network Behavior Analysis*, didapatkan tingkat kepadatan untuk masing-masing *web service*.
   Tingkat kepadatannya dapat dilihat sebagai berikut:
   - 1.ncc.if.its.ac.id memiliki tingkat kepadatan 0,002795031
   - 2.ncc.if.its.ac.id memiliki tingkat kepadatan 0,003312629
   - 3.ncc.if.its.ac.id memiliki tingkat kepadatan 0,008385093
   - 4.ncc.if.its.ac.id memiliki tingkat kepadatan 0,009109731
   - 5.ncc.if.its.ac.id memiliki tingkat kepadatan 0,009730849
   - 6.ncc.if.its.ac.id memiliki tingkat kepadatan 0,010351967
   - 7.ncc.if.its.ac.id memiliki tingkat kepadatan 0,011490683
   - 8.ncc.if.its.ac.id memiliki tingkat kepadatan 0,012732919
   - 9.ncc.if.its.ac.id memiliki tingkat kepadatan 0,02494824
   - 10.ncc.if.its.ac.id (target serangan DDoS) memiliki tingkat kepadatan 0,907142857

Nilai FP = 14 Nilai FN = 10

Pengujian berikutnya yang dilakukan untuk melihat pengaruh sistem *Network Behavior Analysis* terhadap validasi *client puzzle* adalah penambahan jumlah *request web service*. Hasil percobaan dapat dilihat pada Gambar 10. Terlihat bahwa pada awalnya metode yang diusulkan (*Network Behavior Analysis + Client Puzzle*) memerlukan waktu yang lebih lama jika dibandingkan dengan pengujian secara langsung dengan *Client Puzzle* saja. Hal ini disebabkan karena metode *Network Behavior Analysis* memerlukan waktu untuk melakukan *logging* permintaan layanan *web service* serta melakukan analisa dan penyederhanaan *log*. Namun pada saat jumlah *request* layanan diatas 20000, terlihat bahwa metode yang diusulkan memerlukan waktu yang lebih singkat untuk menyelesaikan validasi alamat IP. Terlihat juga ada Gambar 10 bahwa waktu yang diperlukan oleh mekanisme *client puzzle* untuk menyelesaikan validasi alamat IP berbanding lurus dengan jumlah *request* yang ada di *log*. Hal ini dikarenakan seluruh *request* yang ada pada *log* diikutsertakan dalam proses validasi. Sedangkan pada mekanisme yang diusulkan, peningkatan waktu yang terjadi tidak signifikan. Hal ini dikarenakan metode *Network Behavior Analysis* telah melakukan penyederhanaan *log* dan menentukan alamat IP mana saja yang harus diuji dengan metode *Client Puzzle*.

C Kesimpulan

Adapun kesimpulan yang diambil berdasarkan dari hasil penelitian yang telah dilakukan dan analisa metode yang diusulkan adalah sebagai berikut:

1. Deteksi serangan DDoS dapat dilakukan dengan menerapkan metode pengamanan proaktif terhadap serangan yang ditujukan kepada sumber daya jaringan. Hal ini dibuktikan dari keberhasilan mekanisme yang diusulkan untuk mendeteksi serangan DDoS
2. Berdasarkan hasil analisa uji coba, tingkat presisi sistem untuk mendeteksi serangan DDoS sangat baik, mencapai tingkat 86.67% yang berarti sistem dapat mendeteksi dengan tepat *web service* yang diserang, namun mekanisme ini juga memiliki tingkat sensitifitas yang tinggi, yaitu 90.09% yang mendeskripsikan bahwa kemampuan sistem untuk mendeteksi serangan DDoS sangat tergantung pada parameter/*tresholding* yang ditentukan (dalam hal ini adalah tingkat kepadatan jaringan maksimal untuk identifikasi serangan DDoS). Namun hal ini tidak menjadi masalah yang besar karena perbedaan tingkat kepadatan jaringan serangan DDoS dan tingkat kepadatan jaringan *service request* kepada *web service* normal sangat jauh berbeda (tingkat kepadatan jaringan serangan DDoS berkisar antara 0.8 - 0.9, sedangan tingkat kepadatan jaringan *service request* yang normal berkisar antara 0.05 hingga 0.02)
3. Mekanisme *Network Behavior Analysis* menggunakan *network density* (kepadatan jaringan) dalam implementasinya dapat diintegrasikan dengan mekanisme *Client Puzzle*. Pengaruh *Network Behavior Analysis* terhadap sistem validasi secara keseluruhan antara lain:
    - Proses *Network Behavior Analysis* menyebabkan *request web service* yang harus divalidasi oleh mekanisme *Client Puzzle* menjadi lebih sedikit (akibat proses reduksi analitis dari *Network Behavior Analysis*).
    - Dengan berkurangnya jumlah *request web service* yang harus dianalisis, otomatis waktu untuk melakukan validasi secara keseluruhan menjadi lebih singkat.

DAFTAR PUSTAKA

[1] Abliz, Mehmud, and Taieb Znati. "A Guided Tour Puzzle For Denial Of Service Prevention". *2009 Annual Computer Security Applications Confer- ence* (2009): n. pag.

[2] Aura, Tuomas, Pekka Nikander, and Jussipekka Leiwo. "DOS-Resistant Authentication with Client Puzzles". *Lecture Notes in Computer Science*

[3] (2001): 170-177.

[4] Choi, Hyunsang et al. "Botnet Detection By Monitoring Group Activities In DNS Traffic". *7th IEEE International Conference on Computer and Information Technology* (CIT 2007) (2007): n. pag.

[5] Choi, Hyunsang, Heejo Lee, and Hyogon Kim. "BotGAD". *Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE* - COMSWARE "09 (2009): n. pag.

[6] Choi, Hyunsang, and Heejo Lee. "Identifying Botnets By Capturing Group Activities In DNS Traffic". *Computer Networks 56.1* (2012): 20-33.

[7] Falkenberg, Andreas et al. "A New Approach Towards DOS Penetration Testing On Web Services". *2013 IEEE 20th International Conference on Web Services* (2013): n. pag.

[8] Gu, Qijun, and Peng Liu. "Denial Of Service Attacks". *Handbook of Computer Networks* (2007): 454-468.

[9] Imperva,. Denial Of Service Attacks: A Comprehensive Guide To Trends, Techniques, And Technologies. Redwood City: Imperva, 2012. Print. ADC Monthly Web Attacks Analysis.

[10] Juels, Ari, and John Brainard. "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks". *Proceedings of NDSS "99 (Networks and Distributed Security Systems)* (1999): 151-165. Print

SERANGAN DDOS PADA SOFTWARE DEFINED NETWORK

Tugas Caesario Rian Saputra (182420131)

ABSTRAK

Serangan DoS atau DDoS merupakan bentuk serangan yang dilakukan dengan mengirim paket secara terus menerus kepada mesin bahkan jaringan komputer. Serangan ini akan mengakibatkan sumber daya mesin ataupun jaringan tidak bisa diakses atau digunakan oleh pengguna. Serangan DDoS biasanya berasal dari beberapa mesin yang dioperasikan oleh pengguna ataupun oleh bot, sedangkan serangan Dos dilakukan oleh satu orang atau satu sistem. Dalam makalah ini, istilah yang akan digunakan adalah istilah DDoS untuk mewakili serangan DoS ataupun DDoS. Pada dunia jaringan, *Software Defined Network* (SDN) merupakan paradigma yang cukup menjanjikan. SDN memisahkan *control plane* dengan *forwarding plane* untuk meningkatkan *network programmibility* dan manajemen jaringan. Sebagai bagian dari jaringan, maka SDN tidak luput dari serangan DDoS. Maka makalah ini secara umum akan membahas bentuk serangan DDoS yang ditujukan khusus pada SDN.

Keyword: DoS, DDoS, Software Defined Network, Network

DAFTAR ISI

1. PENDAHULUAN

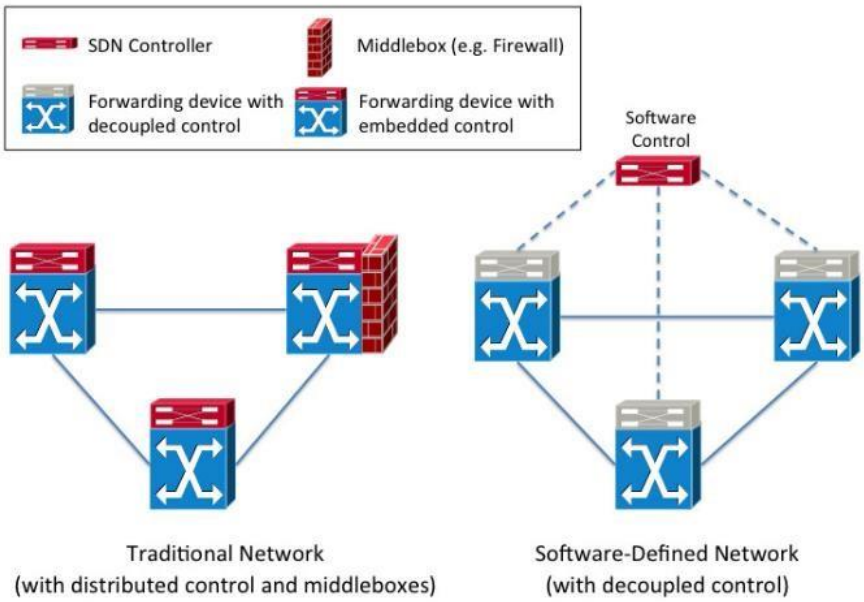
Sejak kemunculannya beberapa tahun lalu, Software Defined Network (SDN) menjadi salah satu isu yang menarik dalam dunia jaringan baik akademisi maupun praktisi. SDN dimunculkan untuk menggantikan jaringan yang sudah ada saat ini. Jaringan saat ini dianggap kaku dan sulit untuk dikembangkan. Pada jaringan saat ini, perangkatperangkat seperti *switch*, router dan perangkat jaringa lainnya, bagian kontrol dan data tergabung secara fisik sehingga tidak fleksibel. Dengan adanya SDN, maka kedua bagian dapat dipisahkan, sehingga secara fisik perangkat yang ada di jaringan adalah bagian data atau *data plane*.

Karakteristik fundamental dari SDN adalah pemisahan antara *control plane* dari *forwarding plane.* SDN secara fungsional terbagi menjadi tiga lapisan yaitu lapisan infrastruktur, lapisan *control* dan lapisan aplikasi seperti yang ditampilkan pada gambar 3. Maka ketiga lapisan tersebut memiliki potensi untuk diserang dengan serangan DDoS. Karena kemungkinan diatas, maka serangan DDoS dibagi menjadi tiga kategori yaitu serangan DDoS pada lapisan aplikasi, serangan DDoS pada lapisan *control* dan serangan DDoS pada lapisan infrastruktur.

Pada makalah ini akan dibahas serangan DDoS pada ketiga lapisan diatas dan beberapa solusi yang pernah diusulkan oleh peneliti untuk mengatasinya. Makalah ini dibagi atas enam bagian yaitu, Pendahuluan, Overview SDN, Tinjauan Keamanan Pada SDN, Serangan DDoS, Serangan DDoS pada SDN dan Simpulan.

2. OVERVIEW SDN

Software Defined Network (SDN) menjadi salah satu agenda pada dunia jaringan yang paling menarik sejak kemunculannya beberapa tahun yang lalu. Karakteristik fundamental dari SDN adalah pemisahan antara *control plane* dari *forwarding plane* berbeda dengan jaringan sebelumnya yang menggabungkan keduanya di semua perangkat, seperti terlihat pada gambar 1. Pada SDN, fungsi dari *control plane* secara logika adalah menjaga keadaan di jaringan dan memberikan instruksi ke *data plane* [1].

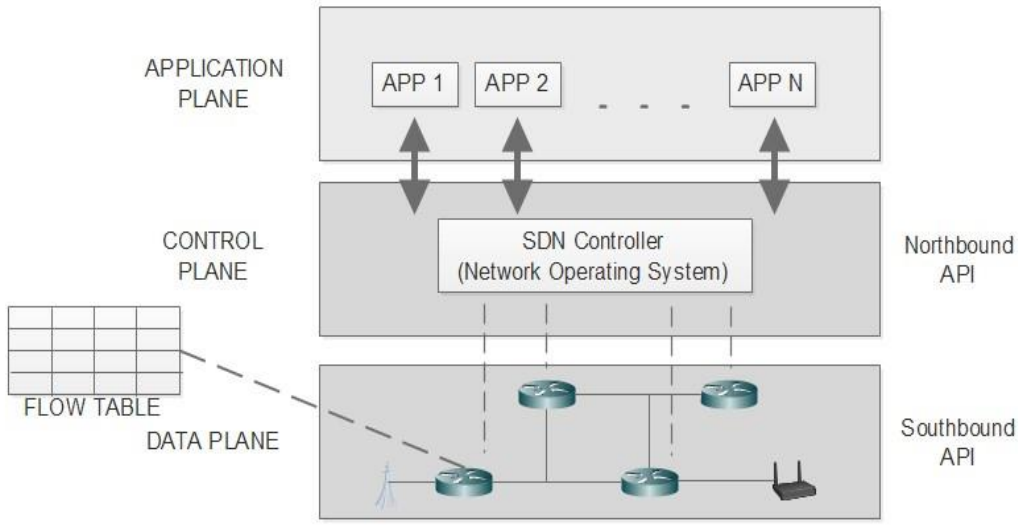


Gambar 1. Jaringan Tradisional dan *Software-Defined Network*[2]

Arsitektur SDN yang terlihat pada gambar 1 memisahkan logika kontrol dari perangkat keras penerusan, dan memungkinkan konsolidasi middlebox, manajemen kebijakan yang lebih sederhana, dan fungsionalitas baru. Garis-garis yang solid menentukan hubungan data-*plane* dan garis putus-putus link-*plane* kontrol. Seiring dengan lahirnya teknologi baru yang diperuntukkan untuk pusat data dan jaringan, yaitu teknologi cloud computing dan virtualisasi, diikuti semakin meningkatkan ketertarikan dunia akademis dan praktisi pada perkembangan SDN.

2.1 Arsitektur SDN

Framework Software-Defined Network memfasilitasi kemampuan program jaringan dan memberikan kemampuan untuk mengelola, mengubah dan mengendalikan perilaku jaringan secara dinamis melalui *open interface*. SDN memungkinkan fitur tambahan seperti alokasi sumber daya sesuai permintaan, penyediaan layanan mandiri, dan jaringan yang benar-benar tervirtualisasi melalui perangkat cerdas dan *provisioning system*. Arsitektur SDN yang dilahirkan oleh Open Networking Foundation (ONF) ditunjukkan pada Gambar 2. Arsitektur tersebut terdiri dari tiga lapisan utama yaitu, Data Plane, Control Plane dan Application Plane. Pada arsitektur tersebut, setiap lapisan memiliki fungsi dan komponen spesifiknya masing-masing pada setiap SDN *deployment* termasuk Southbound API, SDN Controller (atau *Network Operating System/NOS*), Northbound API dan aplikasi jaringan [3].



Gambar 2. Arsitektur SDN

2.1.1 Data Plane

Data *plane* terdiri dari perangkat jaringan seperti router dan *switch* yang memiliki kemampuan untuk meneruskan paket. Perangkat ini hanya melakukan *forwarding* secara sederhana tanpa kemampuan lain seperti melakukan *autonomous decision*. Perangkat-perangkat ini berkomunikasi dengan *controller* melalui standar *interface* OpenFlow. Interface ini memastikan konfigurasi dan kompatibilitas komunikasi serta interoprability antar perangkat.

2.1.2 Southbound API

Southbound API merupakan bagian yang menyebabkan *controller* mampu mengendalikan perilaku jaringan dengan menjaga alur masukan semua perangkat yang terhubung ke *switch*. Oleh karena itu Southbound API menjadi salah satu komponen kritikal pada sistem SDN. Kemampuan ini menjembatani antara perangkat *forwarding* dengan *control plane*. Untuk itu Southbound API menyediakan *interface* yang umum untuk lapisan atas. Sehingga *controller* dapat terhubung menggunakan southbound API yang berbeda-beda misalnya OpenFLow, OpFLex dan OpenState. Southbound API juga memiliki kemampuan untuk menerima plugin bermascam protokol yang berfungsi untuk menngatur perangkat fisik atau virtual yang baru seperti BGP, SNMP dan NetConf.

2.1.3 Northbound API

Northbound API merupakan software ekosistem yang menyediakan *interface* umum untuk membuat aplikasi. Oleh karena itu, bersama dengan southbound API, northbound API menjadi kunci dari abstrasksi SDN. Interface yang disediakan menjadi penghubung atau penerjemah antara instruksi low-level yang digunakan oleh *interface* southbound ke program pada perangkat *forwarding*, termasuk didalamnya otomasi global, manajemen data aplikasi juga routing dan keamanan.

2.1.4 SDN Controller

Komponen ini menjadi otak dari jaringan dengan men-generate konfigurasi jaringan berdasarkan aturan atau *policy* yang didefinisikan oleh operator jaringan. Komponen ini menerjemahkan aturan pada *lower level* sehingga tersedia untuk application *plane* melalui service utama dan API untuk developer.

2.1.5 Application Plane

Komponen ini bertanggung jawab untuk memaksakan aturan atau *policy* yang dimasukkan ke *control plane*. Pelaksanaanya dengan mengimplementasikannya pada perangkat *forwarding* jaringan. Aplikasi SDN yang terpasang pada *controller* terdiri atas SDN App Logic dan A-CPI Driver.

2.2 Perkembangan Terkini Teknologi SDN

OpenFlow secara standard terbatas dan terlalu kaku sehingga ada beberapa peneliti mengusulkan tambahan untuk menambah flexibility. Secara umum ada tiga kategori dari usulan tersebut.

A) Menambah *multiple flow tables* pada perangkat *forwarding*. B) Meningkatkan fleksibilitas *match rule*

C) *Stateful data planes*.

3. TINJAUAN KEAMANAN PADA SDN

Arsitektur SDN yang memisahkan definisi dan penyimpanan *policy* jaringan dari pelaksanaan dan implementasinya maka peneliti [4], mengkategorikan serangan terhadapat kelima komponen utama sesuai dengan dampaknya pada *policy*, *enforcement* dan *implementation*.

3.1 *Implementation Attacks*

Tiga jenis serangan yang ditujukan pada *data plane* diantaranya adalah *Device Attack, Protocol Attack* dan *Side Channel Attack. Device Attack* merupakan serangan yang mengeksploit vulnerabilites pada software maupun hardware *switch* yang memiliki kemampuan SDN untuk menyusupi *data plane*. Penyerang menargetkan bugs pada software ataupun hardware pada perangkat *forwarding*. *Protocol Attack* merupakan serangan yang mengexploit kelemahan pada protokol jaringan pada perangkat *forwarding*. Contoh serangan ini adalah BGP *attack*. *Side Channel Attack* dilakukan dengan menganalisa performa dari perangkat *forwarding*.

Apabila pada *Data Plane* ada tiga jenis serangan, maka pada Southbound API ada empat jenis serangan yang ditargetkan terhadapnya. Serangan tersebut adalah *Interaction, Eavesdrop, Avail- ability* dan *TCP attacks*. *Eavesdrop Attack* merupakan serangan yang bertujuan mempelajari informasi yang terjadi antara *control plane* dengan *data plane* untuk menargetkan serangan yang lebih besar. *Interception Attack* bertujuan untuk merusak kondisi jaringan dengan mengubah informasi atau pesan yang dkirim diantara *control plane* dengan *data plane*. *Availability Attack* sama seperti serangan *Denial of Service (DoS)*. Pada *Availibility attack, Southbound API* di banjiri dengan paket permintaan yang menyebabkan kegagalan implementasi *policy* atau aturan.

3.2 *Enforcement Attacks*

Enforcement attack merupakan serangan yang bertujuan untuk menghalangi SDN dalam menerapkan instruksi secara benar. Serangan ini dapat dengan mengubah waktu, kapan dan bagaimana *policy* seharusnya dijalankan pada jaringan. Target serangan ini adalah pada *Control Plane, Southbound API dan Northbound API*.

3.3*Policy Attacks*

Policy Attack merupakan serangan yang biasanya ditujukan karena kemampuan SDN untuk mendefinisikan dan menyimpan *policy* jaringan secara benar. Penyerang biasanya menargetkan level *policy* untuk mengganggu atau menyusupi *control plane* dan application *plane* SDN. Dengan menyusupi *controller*, maka penyerangan dapat mengubah informasi yang dishare dengan application *plane* terutama tentang jaringan dan keputusan yang akan dibuat. Biasanya serangan ini merupakan bagian dari serangan yang lebih besar untuk menyusupi atau mengganggu jaringan. Serangan ini juga dilakukan untuk menghindari deteksi yang dilakukan oleh instruction

detection system (IDS), sehingga penyerang dapat memiliki akses jaringan secara menyeluruh.

4. SERANGAN DDOS

Serangan DDoS merupakan serangan yang mudah dilakukan namun sulit untuk ditanggulangi. Serangan DDoS biasanya ditujukan pada organisasi atau perusahaan yang terhubung ke Internet. Dalam laporan yang dibuat pada tahun 2017, Akamai menyatakan bahwa 72 persen perusahaan yang menyatakan bahwa perusahaan mereka kurang efektif dalam mencegah serangan DOS[5]. Hal tersebut disebabkan salah satunya karena kurangan sumber daya manusia yang memiliki kualifikasi dalam mencegah serangan tersebut. Dalam beberapa tahun terakhir, paling tidak terjadi sedikitnya lima kali serangan DDoS yang mengakibatkan terjadinya *downtime* pada jaringan mereka rata-rata 8,2 jam. Sedangkan waktu untuk memitigasi serangan tersebut dibutuhkan waktu lebih kurang satu jam.

Serangan DDoS dilakukan terhadap target setidaknya dalam dua bentuk serangan, yaitu:

- Penyerangan menghabiskan semua *bandwidth* atau *resource* dari sistem yang dimiliki oleh target
- Penyerangan menemukan bug atau kelemahan pada implementasi software yang dapat mengganggu layanan.

Sebelum melakukan DdoS, penyerang biasanya akan menyiapkan mesin zombie. Mesin zombie adalah host atau mesin yang berada dalam suatu jaringan yang digunakan sebagai agen untuk melakukan DDoS. Mesin zombie ini didapatkan dari hasil scanning terhadap suatu jaringan, apabila mesin tersebut memiliki *vulnerability*, maka si penyerang akan memasang software didalamnya tanpa diketahui pemilik, sehingga mesin tersebut dapat dikuasai oleh penyerang.

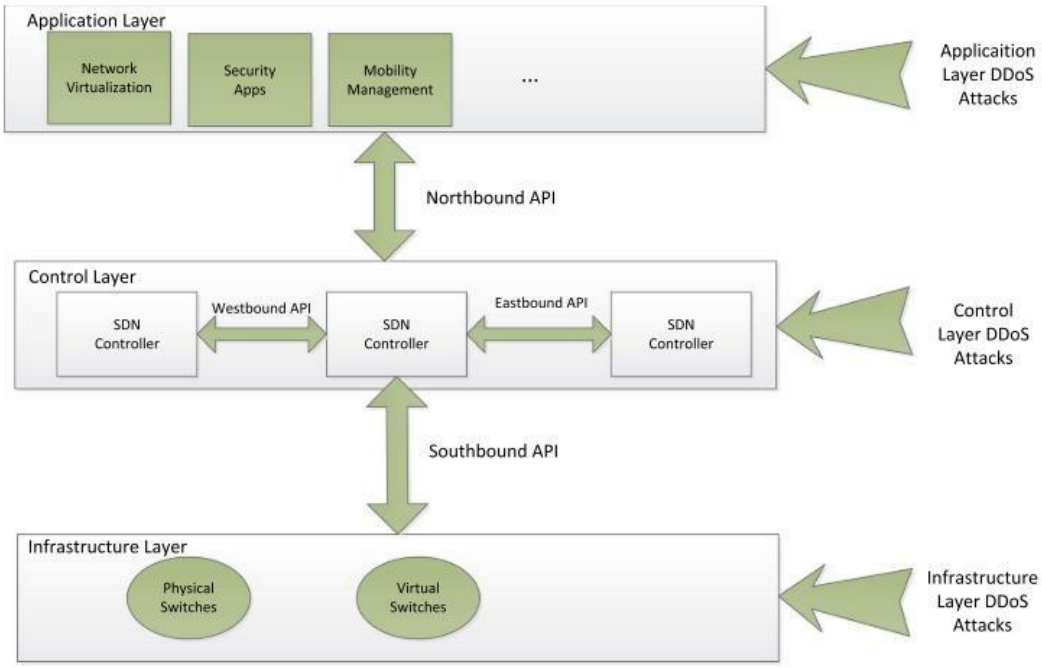
Saat melakukan serangan DDoS, mesin zombie akan dipasang ip spoofing sehingga serangan sulit untuk dilacak. Semakin banyak mesin zombie maka serangan akan semakin berbahaya dan semakin sulit dilacak. Target utama dari serangan DDoS adalah sumber daya seperti *bandwidth*, CPU dan sebagainya. Biasanya sumber daya ini terbatas di dalam jaringan. Meskipun sumber daya tersebut ditingkatkan untuk mengurangi dampak serangan namun tetapi saja akan ada dampak kerugian pada finansial.

Berdasarkan level protokol target, serangan DDoS diklasifikasikan menjadi dua kategori, sebagai berikut [6]:

1) Serangan DDoS pada level network/transport
   Serangan ini biasanya dilakukan menggunakan paket protokol TCP, UDP, ICMP dan DNS. Tujuan utama dari serangan ini adalah mengganggu konektivitas pengguna dengan menghabiskan *bandwidth* target.
2) Serangan DDoS pada level *application*
   Serangan ini bertujuan utama untuk mengganggu layanan pengguna dengan menghabiskan sumber daya server, seperti CPU, memory, *bandwidth disk*, *bandwidth database* dan *bandwidth* I/O.

5. SERANGAN DDOS PADA SDN

Seperti pada jaringan pada umumnya, SDN juga menjadi target serangan DDoS. SDN secara fungsional terbagi menjadi tiga lapisan yaitu lapisan infrastruktur, lapiran *control* dan lapisan aplikasi seperti yang ditampilkan pada gambar 3. Maka ketiga lapisan tersebut memiliki potensi untuk diserang dengan serangan DDoS. Karena kemungkinan diatas, maka serangan DDoS dibagi menjadi tiga kategori yaitu serangan DDoS pada lapisan aplikasi, serangan DDoS pada lapisan *control* dan serangan DDoS pada lapisan infrastruktur, seperti ditampilkan pada gambar 3.

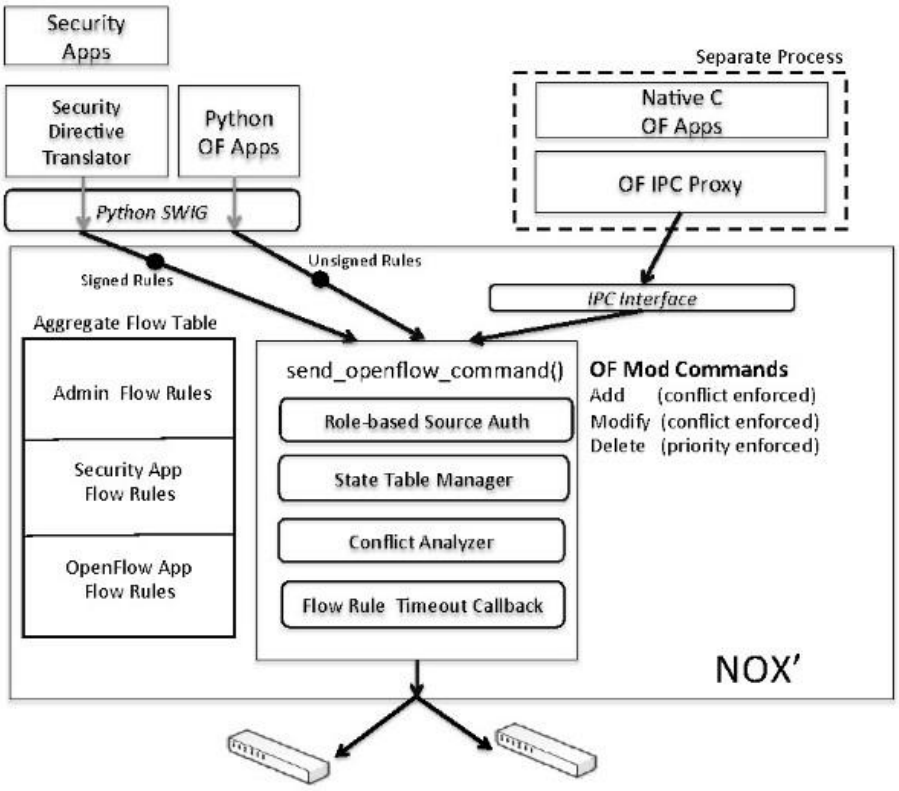


Gambar 3. Serangan DDoS Pada SDN [7]

1. Serangan DDoS pada lapisan aplikasi.

   Metode yang digunakan untuk menjalankan serangan DDoS pada lapisan aplikasi ada dua jenis. Yang pertama adalah menyerang langsung aplikasi dan yang kedua adalah dengan menyerang northbound API. Penyerangan terhadap satu aplikasi pada SDN akan berdampak terhadap aplikasi-aplikasi lainnnya. Karena isolasi antar aplikasi atau resources pada SDN belum dapat diatasi dengan baik.

   Solusi yang dapat digunakan untuk mengatasi masalah ini adalah dengan menggunakan metode FortNOX. FortNOX [8] adalah *policy enforcement* keamanan baru yang dapat dipasang sebagai ekstension atau modul pada NOX OpenFlow *controller*. Metodenya adalah dengan memediasi semua *rule* OpenFlow yang berisi permintaan untuk melakukan penyisipan. FortNOX mengimplementasikan otentikasi berbasis *role* untuk menentukan otorisasi keamanan pada setiap aplikasi yang ada pada OpenFlow. FortNOX juga memberlakukan prinsip *least privilege* untuk memastikan integritas pada saat proses mediasi sehinngga meskipun penyerang mencoba menyisipkan aturan secara strategis, aturan atau *rule* tetap akan melewati proses analisis dan mediasi.



Gambar Implementasi FortNOX [8]

2. Serangan DDoS pada lapisan *control*

   Controller merupakan target yang menarik bagi serangan DDoS pada arsitektur SDN karena memiliki fungsi yang vital di dalam jaringan. Serangan terhadap *control plane* dapat dilakukan dengan menyerang langsung *controller* atau melalui northboundAPI, southboundAPI, westboundAPI serta eastbound API. Sebagai contoh, *flow rules* yang bertentangan pada aplikasi yang berbeda dapat menyebabkan terjadinya serangan DDoS pada lapisan kontrol. *Data plane* pada saat SDN beroperasi, akan bertanya kepada *control plane* ketika adanya paket baru yang tidak dapat diatasi. Apabila ada *flow* baru ketika *flow* tersebut tidak sesuai dengan *flow* tabel, maka untuk mengatasinya ada dua pilihan, yang pertama adalah paket dianggap lengkap atau sebagian header paket dikirimkan ke *controller* untuk menyelesaikan query-nya. Dengan besarnya volume trafik jaringan, pengiriman paket yang lengkap ke *controller* akan memakan *bandwidth* yang besar.

   Solusi yang diusulkan untuk mengatasi ini adalah dengan melakukan deteksi DDoS secara ringan dan cepat berbasiskan *entropy* [9]. Mekanisme ini dapat melindungi *controller* dengan memperhitungkan kemampuan *controller*. Dengan mendeteksi paket diawal antara 250 sampai dengan 500 paket, maka penambahan kode pada *controller* tidak akan meningkatkan beban CPU baik pada saat jaringan normal maupun ketika terjadi serangan. Usulan tersebut diimplementasikan oleh peneliti menggunakan Mininet dan POX Controller.

3. Serangan DDoS pada lapisan infastruktur

   Serangan pada lapirsan infrastruktur dapat dilakukan dengan dua cara, pertama dengan melakukan serangan langsung terhadap *switch-switch* atau menyerang southbound API. Sebagai contoh, jika hanya header informasi yang dikirimkan ke *controller* maka paket tersebut harus disimpan pada node memory sampai *flow table entry* dikembalikan. Hal tersebut menjadi ide bagi penyerang dapat mengirimkan sejumlah *flow* baru dan tidak dikenali sebagai serangan DDoS. Serangan ini akan mnenyebabkan elemen memori pada node mengalami *bottleneck* akibat beban yang tinggi. Akibatnya penyerang mampu membuat memori *switch* menjadi kelebihan beban.

   Solusi yang dapat digunakan untuk mengatasi serangan ini adalah AVANT-GUARD. AVANT-GUARD[10] bertujuan untuk meningkatkan keamanan aplikasi SDN sehingga lebih responsif dan skalabel terhadap ancaman jaringan yang dinamis. AVANT-GUARD terdiri dari dua metode. Metode pertama adalah dengan dengan

menginspeksi sesi TCP pada bagian *forwarding* sebelum melakukan notifikasi pada kontroler sehingga memungkinkan peningkatan ketahanan jaringan SDN. Bagian kedua bertujuan untuk meningkatkan respon sehingga keamanan aplikasi dapat mengakses statistik jaringan secara efisien dalam menanggapi ancaman. Metodenya adalah dengan membuat *actuating trigger* yang mememungkinkan kontroler untuk mendeteksi dan merespon ancaman. Bagian ini direalisasikan melalui pengumpulan statistik jaringan secara efisien yang secara otomatis akan mengatur *flow rules* sesuai statistik jaringan.

Solusi lainnya adalah menggunakan FLOODGUARD. FLOODGUARD [11] menggunakan dua teknik / modul baru, yaitu proactive *flow rule* analyzer dan packet migration. Untuk mempertahankan *policy* enforcement jaringan, proactive *flow rule* analyzer secara dinamis mengambil *rule* aliran proaktif dengan logika runtime *controller* SDN / OpenFlow dan aplikasinya. Teknik yang kedua, yaitu packet migration, digunakan untuk melindungi pengontrol dari kelebihan beban, dengan membuat cache paket flooding secara temporer dan mengirimkannya ke *controller* OpenFlow menggunakan rate limit dan penjadwalan round-robin.

6. SIMPULAN

SDN menjadi topik yang menarik dibidang jaringan, sehingga terus dikembangkan baik oleh praktisi maupun akademisi. Sifatnya yang memisahkan antara control plane dengan data plane menjadi salah satu kelemahan bagi SDN. Salah satu variasi serangan yang dilakukan adalah serangan DDoS. Serangan DDoS dilakukan terhadap tiga lapisan fungsional yang dimiliki oleh SDN. Serangan-serangan tersebut bervariasi pada tiap lapisan, dan dapat dilakukan terhadap lima komponen yang terdapat pada SDN. Serangan tersebut dapat dilakukan secara langsung pada perangkat maupun melalui API yang dimiliki oleh SDN.

Untuk mengatasi serangan DDos tersebut, peneliti mengusulkan beberapa ide. Ide tersebut dapat diimplementasikan pada perangkat secara langsung terutama pada *controller*. Solusi tersebut bisa dilakukan pada saat deteksi awal ketika serangan akan terjadi maupun pada saat serangan telah terjadi.

Daftar Pustaka

[1] S. . A. Scott-Hayward, S.a , Natarajan, S.b , Sezer, "A Survey of Security in Software Defined Networks," *A Surv. Secur. Softw. Defin. Networks*, vol. 18, no. 1, 2016.

[2] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka, and T. Turletti, "A Survey of Software-Defined Networking : Past , Present , and Future of Programmable Networks," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 3, pp. 1617–1634, 2014.

[3] A. Shaghaghi and S. Jha, "Software-Defined Network (SDN) Data Plane Security: Issues, Solutions and Future Directions," 2018.

[4] S. Gao, Z. Li, B. Xiao, and G. Wei, "Security Threats in the Data Plane of Software-Defined Networks," *IEEE Netw.*, vol. 32, no. 4, pp. 108–113, 2018.

[5] A. Technologies, "Cost of Web Application & Denial of Service Attacks," no. October, 2018.

[6] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Commun. Surv. TUTORIALS*, pp. 1–24, 2013.

[7] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys and Tutorials*. 2016.

[8] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, "A Security Enforcement Kernel for OpenFlow Networks," *Proc. first Work. Hot Top. Softw. Defin. networks*, pp. 121–126, 2012.

[9] S. M. Mousavi and P. Affairs, "Early Detection of DDoS Attacks in Software Defined Networks Controller Early Detection of DDoS Attacks in Software Defined Networks Controller," Carleton Univ, 2014.

[10] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD : Scalable and Vigilant Switch Flow Management in Software-Defined Networks Categories and Subject Descriptors," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*, 2013, pp. 413–424.

[11] H. Wang, "FloodGuard : A DoS Attack Prevention Extension in SoftwareDefined Networks," 2015.

Menangkal Serangan SQL Injection dengan Parameterized Query

Dini Rahmadia

Program Studi Magister Teknik Informatika

Fakultas Ilmu Komputer

Universitas Bina Darma Palembang

dinirahmadia@yahoo.co.id

Abstrak- SQL injection merupakan cara yang sangat populer dan sering digunakan untuk melakukan serangan. Semakin meningkat pertumbuhan layanan informasi maka semakin tinggi pula tingkat kerentanan keamanan dari suatu sumber informasi. Melalui tulisan ini disajikan penelitian yang dilakukan secara eksperimen yang membahas tentang kejahatan penyerangan database secara SQL Injection. Penyerangan dilakukan melalui halaman autentikasi dikarenakan halaman ini merupakan pintu pertama akses yang seharusnya memiliki pertahanan yang cukup. Kemudian dilakukan eksperimen terhadap metode Parameterized Query untuk mendapatkan solusi terhadap permasalahan tersebut.

I. PENDAHULUAN

Aplikasi berbasis web berkembang pesat mengikuti pertumbuhan kebutuhan dunia bisnis yang saat ini cenderung mengedepankan layanan berbasis online untuk menjawab kebutuhan customer mendapatkan layanan yang cepat, tepat dan aman. Disisi lain peningkatan tersebut mengakibatkan meningkatnya ide kreatif dari para penyerang (attacker) yang menyalah gunakan kesempatan tersebut untuk mendapatkan segala sesuatu dengan cara illegal. Dampak dari kegiatan tersebut tentu saja menimbulkan kerugian pada kedua stackholder yaitu produsen dan customer. Munculnya kerentanan tersebut dipengaruhi beberapa faktor antara lain kurangnya pengetahuan customer terhadap jenis layanan berbasis web dan kurang siapnya penyelenggara layanan terhadap isu-isu keamanan yang berhubungan dengan bisnis berbasis online atau e-commerce. Dengan demikian diperlukan sebuah metode yang mampu memberikan solusi tepat. Untuk dapat menentukan metode yang tepat maka dianggap perlu mengenal karakter dan cara kerja dari kegiatan penyerangan tersebut. Dalam penelitian ini diperkenalkan jenis penyerangan dengan cara sql injection secara server side scripting untuk kemudian diberikan solusi menghindarinya.

Dalam penelitian ini diangap perlu mengangkat jenis serangan SQL Injection dikarenakan bahwa total serangan terhadap situs-situs yang ada di Indonesia adalah 28.430.843 dan jenis serangan paling besar adalah melalui SQL.

II. TINJAUAN PUSTAKA

Penelitian ini didukung dengan teori-teori sebagai acuan untuk memberikan solusi yang tepat antara lain:

A. SQL Injection

Merupakan sebuah kerentanan yang menyebabkan seorang penyerang memiliki kemampuan untuk mempengaruhi query SQL yang dikirimkan melalui aplikasi ke database. Dengan kemampuan tersebut seorang penyerang dapat mempengaruhi syntax SQL, kekuatan, fleksibilitas dari database pendukung fungsional dan mempengaruhi fungsi sistem operasi yang dialokasikan untuk database. SQL Injection tidak hanya mempengaruhi aplikasi web tapi juga semua program lain yang menggunakan kalimat SQL. Semua program yang menggunakan input dinamis dari luar (untrusted) dapat terserang oleh SQL

B. Bagaimana SQL Injection dapat mengeksploitasi kerentanan?

Beberapa hal yang membuka kesempatan bagi penyerang untuk melakukan SQL Injection antara lain:

1. Memanfaatkan keuntungan dari sebuah sebuah aplikasi yang tidak terlindungi pada fungsi autentikasi pengguna karena tidak adanya validasi.
2. Umumnya seorang penyerang membajak login field yang tidak terlindungi untuk memperoleh akses database.
3. SQL Interpreter tidak dapat membedakan antara perintah yang dimaksud dengan kode yag di-inject oleh penyerang

C. Bahaya SQL Injection

Berikut diberikan beberapa data yang dapat dijadikan acuan tentang bahaya yang pernah terjadi dari tindakan tersebut :

1. Ancaman terbesar terhadap aplikasi web pada tahun 2011, menurut Trustwave terjadi 71 serangan SQL Injection setiap jamnya, menurut Imperva
2. 97% kebocooran data disebabkan oleh SQL Injection, menurut Nationa Fraud Authority, UK.
3. 83% kegiatan hacking situs web yang sukses tahun 2005-2011 menggunakan metode SQL Injection, menurut privacy rights.org
4. Serangan-serangan SQL Injection dengan kerugian terbesar antara lain: Card Systems Solutions (2005, 40 juta kartu data kredit berhasil dicuri), TJX (2006, 94 juta kartu), Heartland Payment Systems (2008, 134 juta kartu), RockYou (2009, 32 juta pengguna), Sony (2011, 77 juta pengguna).
5. Serangan terautomatisasi berhasil menginfeksi 100.000 web: In 2008, SQL attack menjadi terautomatisasi via botnets. Infeksimasi yang pernah terjadi adalah yang melibatkan lebih dari 500 juta pengguna, dilaporkan 500.000 insiden yang dilaporkan tahun 2000

D. Metode Untuk Menghindari SQL Injection

Metode untuk menghindari SQL Injection dapat dilakukan kedalam dua cara yaitu secara client-side dan server-side. Pada metode client-Side yaitu menerima 'Shadow SQL Query' dari server-side dan melakukan pengecekan terhadap deviasi yang terjadi antara shadow query dengan query dinamis yang dibentuk oleh masukan dari pengguna. Jika ditemukan adanya deviasi maka dapat dipastikan bahwa masukannya tidak benar (Malicious)[5]. Sedangkan dalam penelitian ini dikedepankan metode secara server-side. yaitu melalui sejumlah langkah antara lain:

1. Gunakan Prepared Statement atau Parameterized Query. Lebih sederhana dan lebih mudah untuk dimengerti dibanding query dinamis, Parameterized query mengirimkan setiap parameter kedalam lapisan query setelah semua kode SQL telah didefinisikan. Database dapat membedakan antara kode dan data, apapun masukan dari pengguna. Seorang penyerang tidak dapat merubah maksud query, meskipun SQL command telah disusupkan di dalamnya
2. Lakukan validasi masukan. Autentikasi masukan dari pengguna dengan aturan-aturan yang telah didefinisikan seperti panjang, tipe dan filter lain jika diperlukan.
3. Matikan atau sembunyikan pesan-pesan error yang keluar dari server database.

4. Mengunci atau membatasi database anda. Jika aplikasi web Anda tidak memerlukan akses ke tabel tertentu, maka pastikan bahwa mereka semua tidak memiliki izin untuk itu. Jika hanya read-only maka akanmenghasilkan laporan dari tabel hutang account anda maka pastikan anda menonaktifkan insert / update / menghapus akses..

III. HASIL DAN PEMBAHASAN

Halaman autentikasi merupakan pintu pertama pengamanan yang dimiliki oleh sebuah situs, umumnya yang harus dilakukan oleh pengguna layanan adalah mengisi user dan password. Kedua bagian ini mempunyai prinsip kerja dimana harus memiliki nilai keduanya benar maka benar. Hasil tahapan ekperimen berikut memberikan pembuktian tersebut

Tahap 1. Login dengan SQL Injection
Mengetikan kalimat query yang berisi SQL Injection kedalam field password dengan tujuan melakukan login secara illegal
Tahap 2. Membangun logika parameterized query
Tahap 3. Memberikan serangan kedua dengan cara yang sama dengan langkah pertama setelah adanya parameterized query pada listing program. Mengetikan kembali kalimat query yang berisi SQL Injection kedalam field password yang sudah dilakukan pemberian parameterized query dengan tujuan login secara illegal. Dan mendapatkan hasil login salah.
Tahap 4. Menganalisa data hasil eksperimen yang diperoleh kemudian menarik kesimpulan. Ditemukan pembuktian bahwa parameterized query yang digunakan berhasil melakukan fungsinya untuk melakukan pertahanan dari usaha penyerangan secara SQL Injection.

IV. KESIMPULAN

Berdasarkan hasil eksperimen didapat sejumlah kesimpulan antara lain :
1. Halaman autentikasi merupakan pintu pertama keamanan suatu data harus memiliki fasilitas pertahanan yang tinggi yang mampu mengikuti perkembangan teknologi

dengan benar yang bertujuan mengikuti pola berpikir para penyerang yang semakin banyak karakteristik dan cara kerjanya nya.

2. Menganggap suatu metode atau jenis penyerangan yang telah usang atau sederhana merupakan suatu tindakan ceroboh yang dapat merugikan diri sendiri.

3. Menentukan konsep pertahanan pada lapisan awal suatu layanan berbasis web perlu memperhatikan beberapa hal anatara lain : kenyamanan pengguna layanan dan pengaruhnya terhadap kecepatan proses.

REFERENSI

[1] Indonesia Cyber Security Report 2015, Id-SIRTII/CC, 2015

[2] SQL Injection Fact Sheet, Veracode, 2012

[3] Yudantoro, Tri Raharjo, SQL Injection pada sistem keamanan database. Jurnal Teknologi Informasi dan Komunikasi, LPPM STMIK ProVisi: Semarang, 2013, vol 4 No.2.

[4] Hossain Shariar, sarah north, wei-chuen chen, Early Detection of SQL Injection Attcaks, International Journal of Network & Its Application (IJNSA), 2013, vol 5 no

WEB DEFACEMENT ETHICAL PREVENTION

Gian Pratama

Universitas Bina Darma Palembang

Email: gianvenido@gmail.com

Abstrak

Web defacement merupakan hasil dari serangan menggunakan berbagai macam teknik *hacking* yang mengeksploitasi kelemahan sebuah *web*, menyebabkan sebuah tampilan *website* berubah dari yang seharusnya. Penyerang dalam hal ini *hacker* memanfaatkan celah yang ditemukannya dari sebuah *website* untuk berbagai kepentingan, mulai dari uang, ketenaran di dunia maya, memunculkan isu politik ataupun agama, dendam dan sentimen, dan lain sebagainya. Dari sisi *ethical hacking*, artikel ini akan membahas pencegahan dan proteksi yang bisa dilakukan agar terhindar dari serangan *web defacement*.

Kata Kunci: etika, retas, *web deface*

Abstract

Web defacement is the result of attacks using various hacking techniques that exploit the weaknesses of a web, causing a website's appearance changed from what it should. Attackers (hackers) take advantage of vulnerability that founded in a website for various purposes, ranging from money, fame in cyberspace, raising political or religious issues, revenge and sentiment, and many more. In terms of ethical hacking, this article will discuss the prevention and protection that can be done to avoid web defacement attacks.

Keywords: *ethics, hacking, web deface*

1. Pendahuluan

Kebutuhan manusia akan *website* menjadi sangat vital karena semua orang berbelanja, belajar dan mencari ilmu pengetahuan, menonton film, membaca berita dan informasi kini cukup dengan mengakses *website*. Dengan mengetik kata kunci pada mesin pencari (*Google, Yahoo, Bing, DuckDuckGo*). Dalam hitungan detik semua kebutuhan akan tampil dan cepat tersedia untuk dipilih. Maka dari itu, setiap *e-commerce,* situs pendidikan, penjualan jasa, portal berita, semua berlomba-lomba menjadi yang terbaik dan teratas dalam mesin

pencari, dengan memanfaatkan fitur SEO (*Search Engine Optimization*).

Semakin banyak trafik pengunjung, tentunya sebuah *website* akan semakin terkenal. Bila sudah demikian, keamanan *website* pun harus semakin ditingkatkan. Jika tidak, oknum-oknum yang tidak bertanggungjawab akan menyerang dan mampu menembus pertahanan *website* Anda dan mengacaukan semuanya. Mereka disebut *Hacker*.

Beberapa teknik *Hacker* yang digunakan untuk menyerang sebuah *website* antara lain : *malware, phising, SQL Injection, Web Defacement, DdoS,* dan lain sebagainya.

Web Defacement contohnya, merupakan jenis serangan pada *website* yang mampu mengubah halaman *website* menjadi seperti keinginan penyerang. Penyerang dalam hal ini *Hacker* tentu tidak memiliki otorisasi untuk melakukannya, dan kegiatan tersebut termasuk kegiatan ilegal yang melanggar hukum dan etika IT.

Gambar 1.1. Contoh website yang terkena Web Defacement

2. Tinjauan Pustaka

Web Defacement adalah sebuah serangan yang memodifikasi tampilan *website* dengan mencantumkan sebuah tanda atau sebagian pesan, atau membuat *website* menjadi tidak aktif. *Web Defacement* adalah hasil dari kombinasi dan koordinasi dari berbagai bentuk serangan. Berbagai bentuk variasi serangan ini menjadi faktor yang menyebabkan resiko *web defacement* kapan saja dapat terjadi karena sulitnya membangun sebuah pertahanan handal yang bisa menghadapi dan sesuai dengan berbagai macam jenis serangan sekaligus. (Mao & Bagolibe, 2019).

3. Pembahasan

Beragam cara dan teknik dirancang untuk mencegah, menangani, dan

mengidentifikasi secara cepat bila sebuah *website* terkena serangan *web defacement*. Dalam artikel ini akan dibahas tata cara dan panduan dasar pencegahan *web defacement* yang mengacu pada dokumen milik BPPT CSIRT (Badan Pengkajian dan Penerapan Teknologi – Computer Security Incident Response Team) yang dikeluarkan pada tahun 2014 dan dinilai masih relevan hingga saat ini.

1. Memperketat keamanan *web server*

Web server adalah *server* untuk menempatkan *website.* Agar *website* bisa terhindar dari *web defacement*, maka pada *web server* juga harus diterapkan pengamanan yang ketat.

Beberapa pengamanan harus dilakukan pada level sistem operasi dengan cara melakukan *system update* secara berkala, mematikan semua *service* yang tidak terpakai, menutup *port* yang tidak perlu di *publish* ke internet, memonitor *log system*, membuat *backup system*, *access control* ke file-file tertentu, tidak membuka akses *superuser/root server* dari luar, dsb.

Pada level *web server*, dapat dilakukan *patching* dan *security update* secara berkala, mematikan semua layanan yang tidak digunakan (*ftp, tftp*, dsb), menghapus semua file dokumentasi dari *vendor*, mengubah semua akun *default* yang dibuat pada waktu instalasi, mengubah *file permission* untuk file-file tertentu, seperti: *htaccess, index, file admin, config,* dsb.

Pada level sistem aplikasi, bila menggunakan CMS (*Content Management System*), dapat dilakukan perubahan terhadap semua konfigurasi *default* pada CMS, melakukan *update & upgrade,* hanya menggunakan *plugin* yang tepat, bereputasi baik, dan terverifikasi oleh penyedia CMS.

Selanjutnya dapat diakukan teknik *code scanning*, yakni melakukan pemeriksaan dan validasi terhadap kode-kode yang diinputkan ke dalam halaman *web,* aplikasi pada *web,* maupun *database* pendukung *web* dengan menggunakan aturan-aturan yang telah ditetapkan.

Keamanan kode program pembangun *website* seperti *php, asp, javascript* juga perlu diperhatikan mengingat teknik dan aturan yang salah dalam mengimplementasikan kode-kode program tersebut dapat mengakibatkan kerentanan pada aplikasi *web*.

Untuk mengurangi kerentanan pada level sistem *database*, lakukan juga *patching* dari *service pack* teraktual, lakukan *log monitoring* secara rutin, tidak memberikan akses *superuser/root database* pada aplikasi yang membutuhkan *database*, akses *database* yang diberikan hanya kepada alamat IP tertentu, mengubah *port default* yang menjadi koneksi antara aplikasi dan *database*, kemudian gunakan *tools* tertentu dalam melakukan proses pertukaran data, misal *authentication* menggunakan RSA, *encryption* menggunakan AES (128), *message digest algorithm* menggunakan SHA1, dsb.

2. Perlindungan dari *Network Sniffing*.

Network Sniffing adalah kegiatan untuk melakukan mata-mata terhadap jaringan komputer. Tujuan dari kegiatan ini adalah untuk mengambil data-data penting yang sedang lewat pada jaringan. Untuk mencegah terjadinya efek negatif yang dihasilkan dari kegiatan *Network Sniffing*, dapat dilakukan langkah-langkah berikut:

a. Memasang *Network IPS/IDS*

Intrusion Prevention System (IPS) adalah sebuah aplikasi yang bekerja untuk monitoring lalu-lintas jaringan, mendeteksi aktivitas yang mencurigakan, dan melakukan pencegahan dini terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. Bisa jadi karena adanya serangan dari luar, dan sebagainya. Produk IPS sendiri dapat berupa perangkat keras (*hardware*) atau perangkat lunak (*software*).

Network-based Intrusion Prevention System (NIPS) tidak melakukan pantauan secara khusus di satu *host* saja. Tetapi melakukan pantauan dan proteksi dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan *firewall* dan kadang disebut sebagai *In-Line* IDS atau *Gateway Intrusion Detection System* (GIDS). Sistem kerja IPS yang *populer* yaitu pendeteksian berbasis *signature*, pendeteksian berbasis anomali, dan monitoring berkas-berkas pada sistem operasi *host*.

Sedangkan NIDS adalah jenis IDS yang menganalisa lalulintas paket dalam jaringan. Oleh NIDS, paket-paket data yang dikirimkan melalui jaringan akan diperiksa apakah berbahaya untuk keseluruhan jaringan. Apabila ada paket data yang berbahaya atau mencurigakan, NIDS

akan membuat log mengenai paket tersebut, yang disertai informasi-informasi tambahan. Berdasarkan paket yang mencurigakan tadi, NIDS akan memeriksa *database* miliknya mengenai ciri-ciri paket yang merupakan serangan terhadap jaringan. Kemudian NIDS akan memberikan label mengenai tingkat bahaya dari setiap paket yang dicurigai. Apabila tingkat bahaya cukup tinggi, NIDS bisa mengirimkan email peringatan kepada *administrator* agar dilakukan analisa lebih lanjut. NIDS mendapatkan input dari sensor-sensor yang berada di lokasi-lokasi yang strategis dalam sebuah jaringan. Beberapa lokasi strategis yang bisa dipakai untuk menempatkan sensor antara lain *switch*, *router*, *firewall*, atau berada di sebuah *host*.

b. Memasang *Web Application Firewall* (WAF)

Web Application Firewall (WAF) adalah suatu alat pada layer aplikasi, yang bisa berupa *plugin* pada *server* atau *filter* yang berupa seperangkat aturan untuk penanganan HTTP. Umumnya, aturan ini digunakan untuk menangkal serangan seperti *Cross-site Scripting* (XSS) dan *SQL Injection* yang menjadi serangan populer pada kasus *Web Defacement*. Dengan membuat aturan untuk sebuah aplikasi, banyak serangan terhadap aplikasi dapat diidentifikasi dan diblokir.

3. Memasang *Anti Defacement tools/system*.

Salah satu jenis sistem *anti web defacement* bekerja dengan cara membandingkan *hash code* dari halaman web dalam interval waktu tertentu. Dari suatu halaman web yang asli akan dihasilkan sebuah *hash code*, setiap membuka halaman web, akan menghasilkan hash code yang baru, *hash code* inilah yang dibandingkan dengan *hash code* yang asli untuk melihat apakah ada perubahan yang terjadi dari halaman web.

Tools terkenal yang dapat digunakan antara lain *DotDefender, Nagios, dan WebGuard*.

4. Memperketat akses terhadap *web*

Peraturan akses terhadap *web server*, aplikasi-aplikasi pada *web*, dan *database* yang mendukung *web* harus diterapkan dengan ketat. Proses akses terhadap *web* bisa dilakukan dengan beberapa tahap, diantaranya :

a. Keamanan otentikasi dilakukan melalui saluran yang aman, melindungi *password* pengguna dengan menerapkan standar, pembatasan jumlah *login* yang

gagal lalu mengunci penggunanya, memaksimalkan fungsi *hashing kriptografi,* serta menggunakan proses *re-authentication* untuk operasi yang sensitif seperti perubahan *password*.

b. Manajemen sesi (*Session Management*) juga dapat dilakukan seperti fasilitas *logout,* token sesi harus berakhir setelah jangka waktu aktif yang wajar, dsb.

c. *Access Control* yang berhubungan dengan pengendalian akses terhadap *resource* dari suatu sistem, dalam hal ini adalah *server* untuk menempatkan situs *web*. Cara paling umum dalam hal pengendalian akses adalah pemberian otoriasasi kepada *user* untuk mengakses bagian/ *file* tertentu.

5. Melakukan *Security Audit/Penetration Testing* secara berkala

Salah satu proses *ethical hacking* yang sering dilakukan ialah *penetration testing* yakni sebuah proses untuk melakukan pengujian terhadap celah keamanan yang terdapat pada suatu sistem komputer atau jaringan. *Penetration testing* yang khusus ditujukan untuk melakukan pengujian terhadap celah keamanan pada halaman *web* bisaanya disebut dengan *Penetration Testing Web application*. Pada proses *penetration testing*, sebuah *web server* akan dijadikan target serangan dengan melakukan beberapa simulasi serangan.

Terdapat 2 metode untuk melakukan *Web Application Penetration Testing*, yaitu:

a. *Passive Penetration Testing*: Pada mode ini *tester* mencoba untuk mengetahui logika dari aplikasi *web*. Tool yang ada digunakan untuk mengetahui beberapa informasi seperti kontrol yang ada didalam *web application, login* dan konfigurasinya, sehingga kita bisa memetakan target sistem.

b. *Active Penetration Testing*: Yaitu melakukan kegiatan aktif dalam pengujian terhadap keamanan sistem dengan melakukan manipulasi input, pengambilan akses, dan melakukan pengujian terhadap vulnerability-vulnerability yang sudah ada.

Khusus untuk menghindari *web defacement*, *penetration testing* dapat dilakukan pengujian *Configuration Management Testing, Authentication*

Testing, Session Management Testing, Authorization Testing, Data Validation Testing dan *Web Service Testing.*

Kesimpulan

Tidak ada sistem yang benar-benar aman. Selalu akan ada celah, tergantung bagaimana seseorang mengeksploitasi celah tersebut. Bagi sebuah *website*, semua bentuk serangan akan terus menghampiri, terlebih bila *website* tersebut merupakan *website* yang terkenal, atau berpengaruh, atau memiliki trafik kunjungan yang tinggi. Selalu akan ada upaya untuk menjegal dan mengganggu kestabilan sistemnya, salah satunya ialah serangan *web defacement*.

Beberapa teknik yang dapat digunakan untuk mencegah adanya *web defacement* ialah memperkuat keamanan web server, menyiapkan perlinudngan dengan NIPS/NIDS, memasang *anti defacement*, dan memperketat aksesnya. Secara *ethical hacking*, teknik mencegahnya ialah dengan melakukan *penetration testing* secara berkala kepada *website* tersebut, yang dilakukan oleh *administrator* atau tim *web audit* yang ditunjuk dan diberi otoritas melakukannya.

Daftar Referensi

Mao, BM, dkk. 2019. *A contribution to detect and prevent a website defacement.* International Conference of Cyberworlds. IEEE 978-1-7281-2297-7 DOI 10.1109. Diakses tanggal 18 Juni 2020.

Tim Penyusun. 2014. *Panduan Penanganan Insiden Web Defacement.* BPPT CSIRT. https://csirt.bppt.go.id/download-2/. Diakses tanggal 18 Juni 2020.

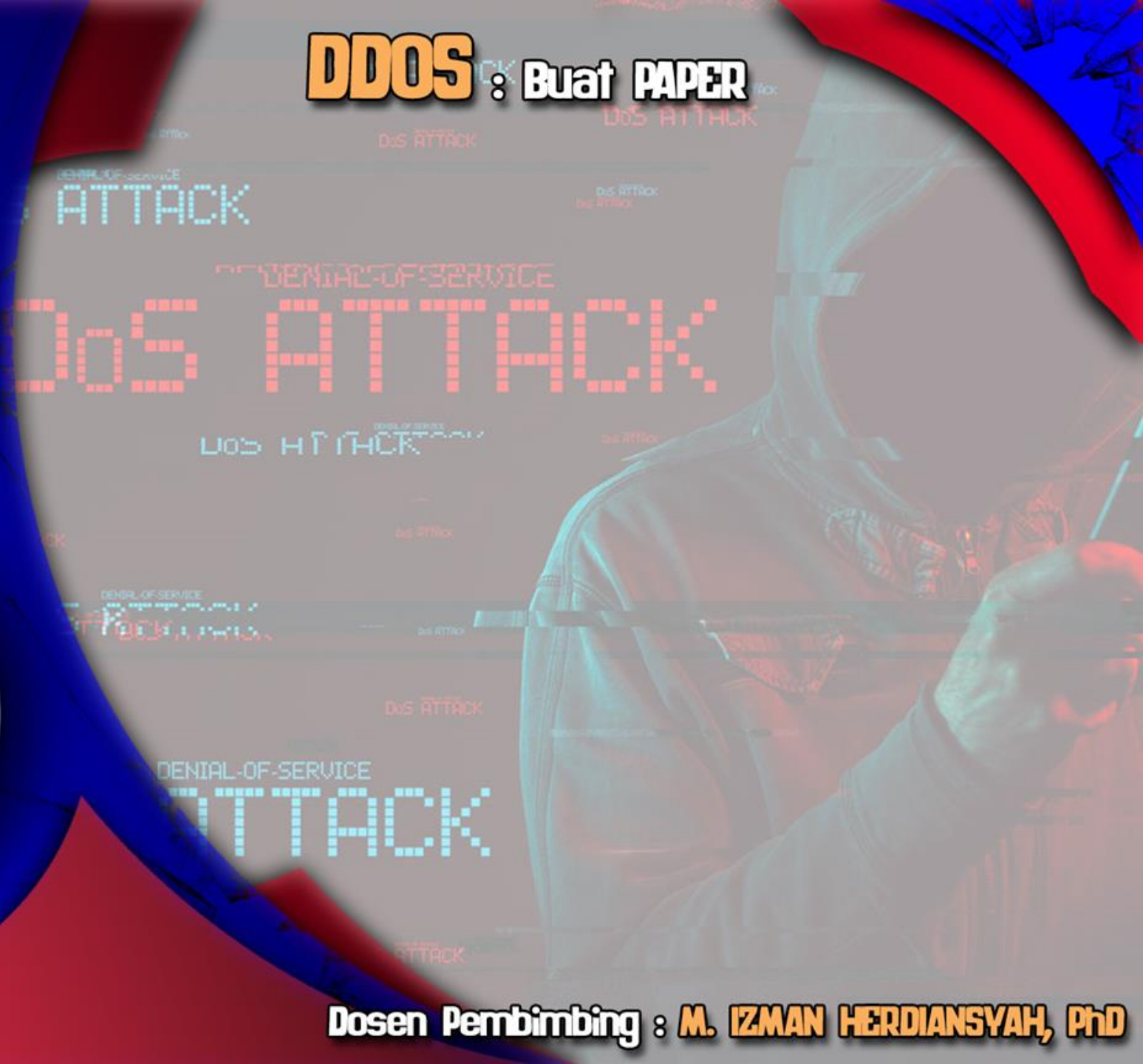
Nama : Hari Febriadi
NIM : 182120127

DDOS

Paper tentang inseden penyerangan

MTI.20A

DDOS : Buat PAPER



ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

❑ PENGERTIAN DDOS DAN CARA MENANGGULANGINYA

- Apa itu DDoS? DDoS merupakan kependekan dari ***Distributed Denial of Service*** atau dalam bahasa Indonesia dapat diartikan sebagai Penolakan Layanan secara Terdistribusi. **DDoS** adalah *jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan*. Umumnya serangan ini dilakukan menggunakan beberapa komputer host penyerang sampai dengan komputer target tidak bisa diakses.

- **DDoS** adalah serangan yang sangat populer digunakan oleh hacker. Selain mempunyai banyak jenis, **DDoS memiliki konsep yang sangat sederhana**, yaitu membuat lalu lintas server berjalan dengan beban yang berat sampai tidak bisa lagi menampung koneksi dari user lain (overload). Salah satu cara dengan mengirimkan request ke server secara terus menerus dengan transaksi data yang besar.

Berhasil atau tidaknya teknik DDoS dipengaruhi oleh kemampuan server menampung seluruh request yang diterima dan juga kinerja firewall saat ada request yang mencurigakan.

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

Daftar isi

1) Serangan Ddos Terbesar
2) Cara Kerja dan Tujuan Ddos
3) Teknik Ddos
4) Ciri website anda Terkena Ddos
5) Cara Mengatasi Ddos

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

❑ Serangan Ddos Terbesar

- Percobaan serangan DDoS setiap tahun selalu meningkat. Penggunanya tidak hanya user yang ingin mencari sensasi, bahkan digunakan dengan alasan politik, atau tindak kejahatan yang ingin mengganggu stabilitas server dan bahkan mencuri data yang ada di dalamnya.

- Serangan ke Spamhaus pada tahun 2013 tercatat sebagai serangan DDoS terbesar sepanjang sejarah. Serangan ini mencapai puncak tertinggi 400 Gbps dan mengakibatkan Github tidak bisa diakses beberapa menit. Di tahun berikutnya terjadi serangan ke salah satu klien Cloudflare dengan kekuatan 33% lebih besar dibandingkan serangan yang dilakukan ke Spamhaus.

- Github mendapatkan serangan DDoS yang mencapai puncak tertinggi transaksi data yang sangat fantastis, yaitu 1.35 Tbps. Serangan tersebut berasal dari ribuan Autonomous System (ASN) di puluhan ribu titik akhir yang unik.

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

❑ Cara Kerja dan Tujuan Ddos

- Konsep sederhana DDoS attack adalah membanjiri lalu lintas jaringan dengan banyak data. Konsep **Denial of Service** bisa dibagi menjadi 3 tipe penggunaan, yakni sebagai berikut :

❑ Request flooding merupakan teknik yang digunakan dengan membanjiri jaringan menggunakan banyak **request**. Akibatnya, pengguna lain yang terdaftar tidak dapat dilayani.

❑ Traffic flooding merupaka teknik yang digunakan dengan membanjiri lalu lintas jaringan dengan banyak **data**. Akibatnya, pengguna lain tidak bisa dilayani.

❑ Mengubah sistem konfigurasi atau bahkan merusak komponen dan server juga termasuk tipe denial of service, tetapi cara ini tidak banyak digunakan karena cukup sulit untuk dilakukan.

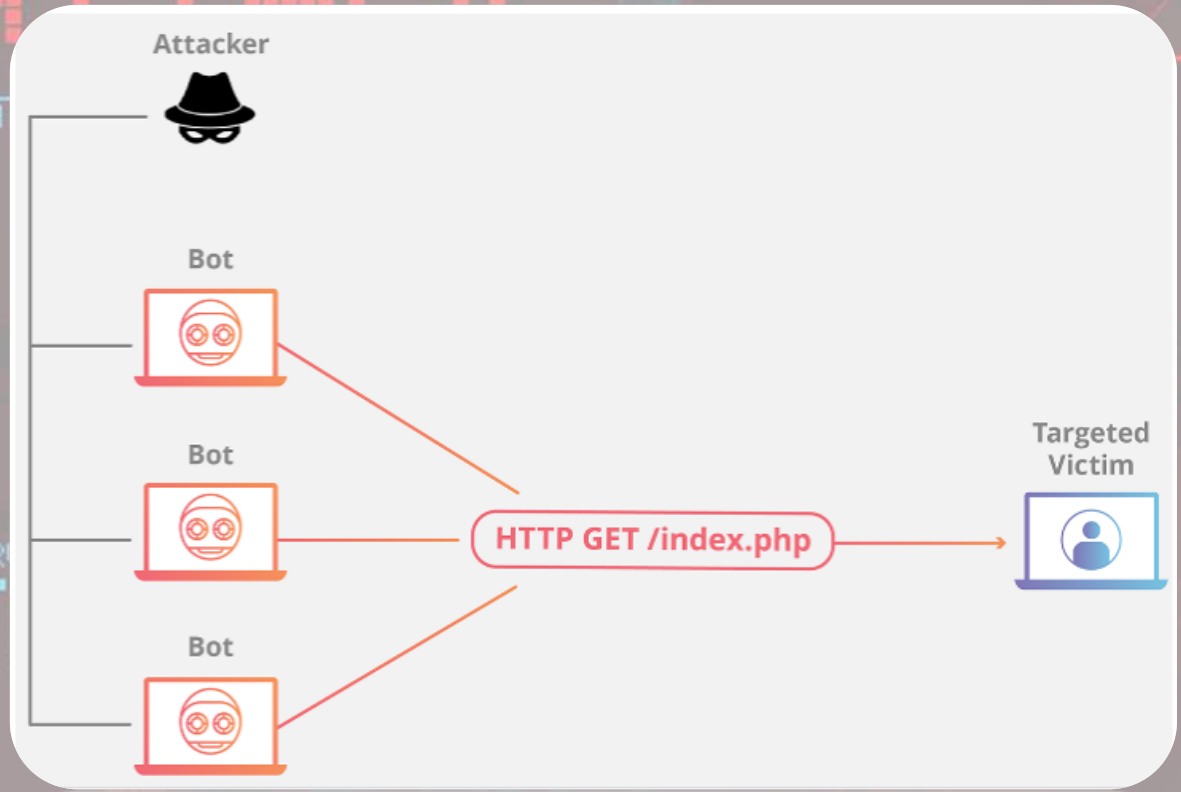
MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

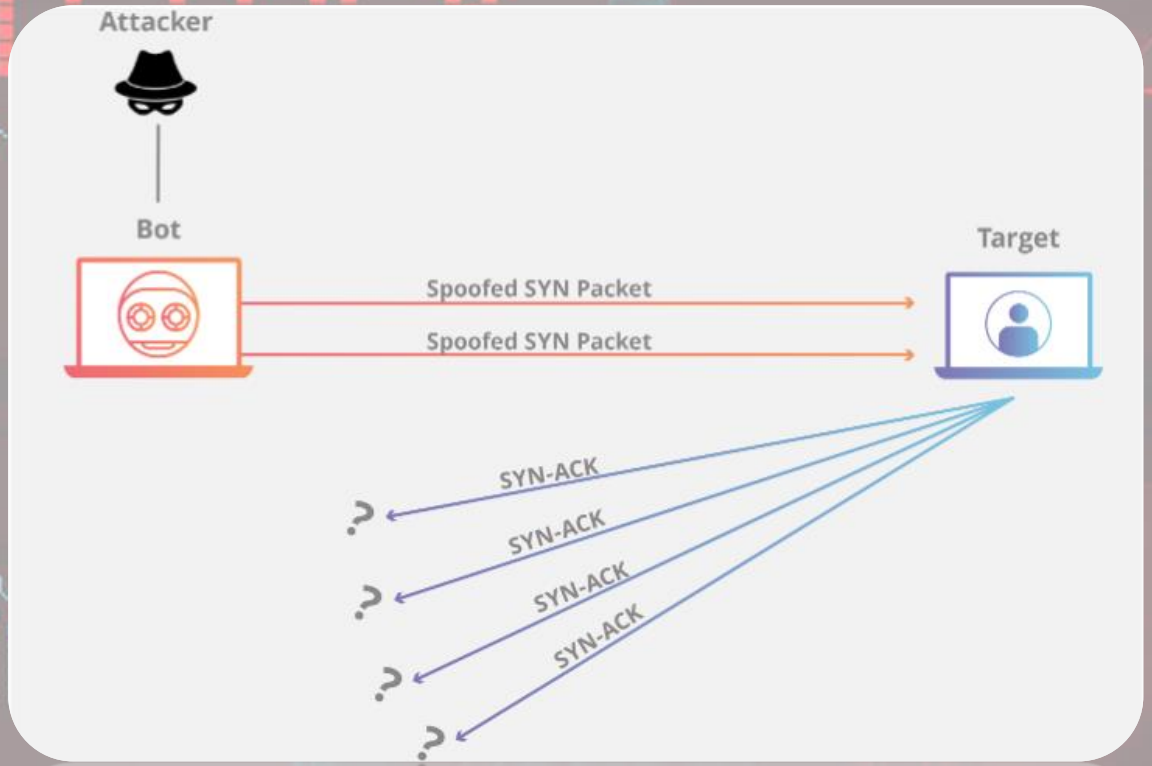
Sedangkan jika kategorikan berdasarkan layer OSI, ada serangan pada layer aplikasi, protokol, dan volumetrik.

- **DDoS Layer Aplikasi**



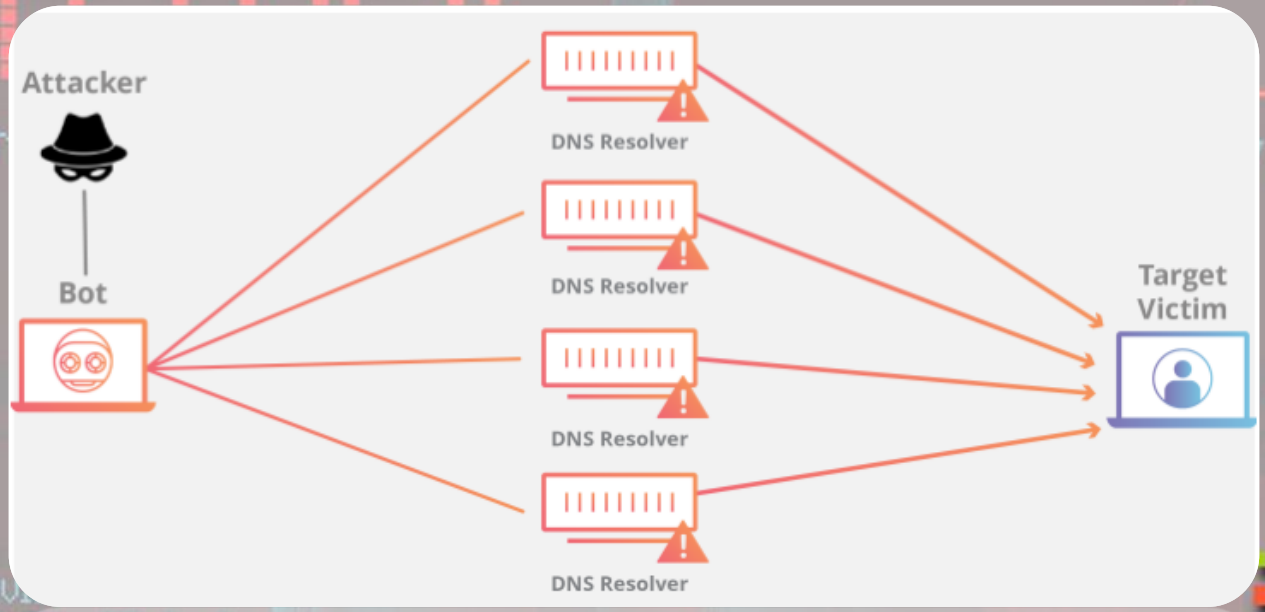
Sedangkan jika kategorikan berdasarkan layer OSI, ada serangan pada layer aplikasi, protokol, dan volumetrik.

- **DDoS Protocol**



Sedangkan jika kategorikan berdasarkan layer OSI, ada serangan pada layer aplikasi, protokol, dan volumetrik.

- **Volumetriks DDoS**



❑ Teknik DDos

❑ Serangan DDoS adalah teknik penyerangan yang mempunyai banyak cara sederhana, seperti menggunakan virus, botnet, dan perangkat lunak yaitu RailGun.

- **Botnet**

  Pada pengembangannya, serangan DDoS dilakukan dengan bantuan kumpulan bot yang dijalankan secarabersama-sama. Bot disisipkan pada malware yang kemudian di tanam ke komputer yang terhubung ke jaringan internet.

  Jumlah komputer ini bisa puluhan sampai dengan jutaan, tergantung banyaknya komputer yang telah terinfeksi malware. Semua komputer ini dinamakan dengan botnet, sedangkan satu komputer yang terinfeksi dinamakan dengan komputer zombie.

  Hanya menggunakan satu perintah saja, botnet langsung menjalankan perintah untuk melakukan DDoS ke komputer target dalam waktu bersamaan.

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

❑ Teknik DDos

- **Virus**

  Di internet, seseorang yang berencana melakukan DDoS adalah dengan menyebarkan virus melalui file yang dibagikan ke berbagai situs yang terhubung dengan internet. Virus sengaja diciptakan salah satunya adalah untuk menjalankan bot melalui script yang berjalan pada sistem operasi. Bahkan beberapa virus dapat mengambil hak akses dari perangkat yang sudah mengunduh script dan dijalankan pada sistem operasi.

❑ Cara Pengatasi DDos

- Ada beberapa cara yang bisa Anda lakukan jika website atau sistem terkena DDoS. Berikut ini beberapa yang bisa Anda coba:
  - ❑ Melakukan Identifikasi Serangan, biasanya jika Anda mempunyai server sendiri, tanda-tanda jika sedang terjadi serangan DDoS akan terlihat. Jika dikethui maka Anda bisa bersiap-siap melakukan penanganan sebelum terjadi serangan DDoS yang lebih serius.
  - ❑ Mempertahankan Parameter Network, ada beberapa langkah teknis yang dapat diambil untuk mengurangi sebagian efek dari serangan, dan beberapa diantaranya cukup sederhana. Misalnya anda dapat:
  - ❑ Memperbesar Bandwidth, jika masih bisa melakukan pelebaran bandwidth, cara ini bisa dicoba untuk memberikan waktu agar sistem tidak sampai down. Jika serangan DDoS terlalu besar maka cara ini mungkin tidak akan berpengaruh banyak untuk penanganan.

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

❑ Kesimpulan

- ❑ **DDoS** adalah teknik penyerangan pada sistem yang sangat populer digunakan. Selain sederhana, dengan modifikasi strategi, DDoS bisa menjadi teknik yang sangat ampuh untuk meenggantu sistem.

- ❑ Ada beberapara cara melakukan DDoS seperti menggunakan request flooding dan traffic flooding. Kedua cara ini mempunyai kesamaan yaitu membanjiri lalu lintas jaringan dengan banyak data atau request. Jika berhasil maka pengguna lain akan kesulitan untuk melakukan akses ke sistem dan bisa jadi mengakibatkan sistem rusak dan tidak bisa diakses.

- ❑ Tetapi ada beberapa cara yang bisa dilakukan untuk mencegah sistem bermasalah saat diserang oleh DDoS. Memperbarui sistem operasi ke versi terbaru adalah cara mencegah DDoS menyerang melalui celah yang ada pada sistem operasi.

MTI.20A

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

Nama : Hari Febriadi
NIM : 182120127

DDOS

Paper tentang inseden penyerangan

MTI.20A

TERIMA KASIH

ETHICAL : Computer And Internet Crime

Dosen Pembimbing : M. IZMAN HERDIANSYAH, PhD

TUGAS INDIVIDU 2

ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEM
DOSEN PENGASUH: M. IZMAN HERDIANSYAH, PhD

Nama : Harli Septia Fani
NIM : 182420122
Kelas : MTI 20A

MALWARE

Pendahuluan

Teknologi sudah menjadi bagian yang tak terpisahkan dalam segala aktifitas hidup manusia, khususnya teknologi informasi dan komunikasi. Kemajuan dalam pengolahan data, kemudahkan komunikasi data dari tempat yang berjauhan adalah sedikit dari banyak kemudahan yang bisa kita dapatkan berkat teknologi informasi. Aktifitas browsing, streaming, media sosial dan lain-lain juga dapat dilakukan kapan saja saja dan dimana saja. Dengan menggunakan jaringan internet yang menghubungkan semua perangkat, semua aktifitas berbasis teknologi akan sangat mudah dilakukan. Melalui jaringan internet juga kemungkinan terjadi serangan malware hampir di setiap aktifitas selancar dunia maya.

Tantangan kemajuan teknologi informasi tersebut memberi dampak positif dan negative. Jika dimanfaatkan dengan baik tentu saja akan memberi dampak yang baik, demikian juga sebaliknya. Pengaruh negative yang seringkali muncul adalah kejahatan computer atau yang dikenal dengan istilah *cybercrime*. Kegiatan *cybercrime* ini seringkali terjadi tanpa disadari oleh pengguna. Pengguna baru menyadari ada yang salah dalam keamanan data dan system mereka setelah mengalami kehilangan data atau bahkan mengalami kegagalan system. Resiko keamanan jaringan tersebut bisa saja terjadi disebabkan oleh *malware* yang disisipkan dalam satu software atau system dan menyebar ke seluruh computer yang terhubung dalam jaringan internet tersebut.

Dalam paper ini, penulis memberikan pemahaman mengenai malware, bagaimana memberikan perlindungan data dari insiden penyerangan malware, cara menanggulangi dan mengurangi resiko kehilangan data dan kerusakan system yang diakibatkan oleh kejahatan malware tersebut.

Literature Review

Malware merupakan program computer yang ditujukan khusus untuk mencari kelemahan software sehingga perangkat tersebut akan terkena virus, dengan cara menyusup ke dalam system dan merusaknya. Malware dapat menyusup melalui aktifitas yang dilakukan menggunakan jaringan internet seperti email, download, copy data, dan sebagainya. Selain menyebabkan kerusakan system dan data, malware mungkin juga bisa menyebabkan terjadinya pencurian data/informasi. Hal ini terjadi jika malware tersebut disisipkan dengan berupa virus, worm, trojan horse, sebagian besar rootkit, spyware, ransomware, adware dan lain-lain. Ini merupakan ancaman serius bagi keamanan system jaringan computer. Kurangnya pengetahuan *user* akan masalah keamanan system menjadi salah satu penyebab timbulnya masalah dalam perangkat computer. Tidak menggunakan anti virus atau tidak update anti virus merupakan salah satu penyebab computer dapat terinfeksi *malware* tanpa disadari oleh pengguna. Jika *malware* sudah menyebar ke computer yang lain dalam jaringan akan sangat merugikan banyak pihak.

Pembahasan

Trojan, virus, worm, spyware, adware, keyloggers. Nama-nama itu hanya beberapa dari sekian banyak *malware* yang berkeliaran dan membahayakan komputer kita. Kerusakan yang ditimbulkannya pun bermacam-macam, dari mulai "hanya" mengubah ekstensi *file* sehingga tidak bisa digunakan sampai melumpuhkan 50 juta komputer hanya dalam waktu 1 hari. Mengingat bahayanya, kami kira penting untuk sekali lagi mengingatkan Anda tentang cara melindungi komputer dari *malware.*

Perangkat apa pun yang kita gunakan ketika mengakses Internet, entah itu laptop, PC, atau *smartphone*, semua itu memiliki risiko yang sama. Ketika mengakses Internet, pernahkah terpikir bahwa informasi pribadi Anda aman dari pencurian? Ketika mengakses Internet, pernahkah Anda terpikir bahwa komputer Anda aman dari berbagai macam program berbahaya?

Barangkali Anda pernah mendengar tentang kegemparan yang dibuat oleh *malware* bernama ILOVEYOU. Pada bulan Mei tahun 2000 silam, *malware* sejenis *worm* ini telah melumpuhkan sedikitnya 50 juta komputer yang terhubung dengan Internet di Amerika sana. Komputer yang diserang bukan hanya milik perusahaan-perusahaan besar, tapi juga milik Pentagon dan CIA.

Beberapa macam bahaya kejahatan internet :

1. Pencurian data seperti data pelanggan, data perbankan, dan lain-lain.
2. Pencurian informasi pribadi seperti *username* dan *password*, nomor kartu kredit dan kartu debit, dan PIN.
3. Penyusupan dan pencurian data kontak seperti alamat surel *(e-mail)* yang kemudian dipergunakan untuk menyebarkan virus lain atau konten-konten seperti pornografi dan konten sensitif lainnya.
4. Memperlambat sistem dengan cara "menumpang" jaringan Internet yang kita gunakan.
5. Mengakes dan menghapus data atau *file* yang ada di komputer kita.
6. Merusak *software* komputer.
7. Mengganti *username* dan *password* sehingga kita tidak bisa mengakses akun yang kita miliki.
8. Mempergunakan komputer dan jaringan kita sebagai "inang" untuk menyebarkan virus berbahaya ke komputer lain.

Sebuah penelitian menemukan bahwa **jenis malware yang paling umum sekarang adalah Trojans dan worms,** dengan virus mengalami penurunan dalam jumlah. Sementara itu di tahun ini, malware juga ditemukan sudah menargetkan mobile devices seperti smartphones dan tablets. Bahkan, ada malware yang sudah di pre-install di devicenya sendiri. Lalu apa saja jenis-jenis Malware dan bagaimana mereka diklasifikasikan? Berikut adalah beberapa jenis malware :

1. Virus

   Karakteristik utama yang dimiliki sebuah software untuk memenuhi syarat sebagai virus adalah software yang mendorong untuk mereproduksi program di dalamanya. **Ini berarti jenis malware ini akan mendistribusikan salinan programnya sendiri dengan cara apapun untuk menyebar.**Ciri lain yang umum terjadi adalah mereka selalu tersembunyi di dalam sistem sehingga sulit untuk mendeteksi eksistensinya tanpa program keamanan khusus yang disebut antivirus. Mereka bersembunyi di dalam file komputer, dan komputer harus menjalankan file itu dengan kata lain, menjalankan kode itu, agar virus melakukan pekerjaan kotornya. Pada intinya, virus tidak lain hanyalah kode atau program menular yang menempel pada software lain dan biasanya memerlukan interaksi manusia untuk diperbanyak. Ini adalah bagaimana virus diklasifikasikan lebih lanjut, tergantung pada apakah mereka berada dalam binary executables, file data, atau di boot sector dari hard drive sistem tertentu.
2. Worms

Ini adalah jenis malware yang menular. **Worm adalah sebuah software mandiri yang bereplikasi tanpa menargetkan dan menginfeksi file tertentu yang sudah ada di komputer.** Worms adalah sebuah program kecil yang mereplikasikan diri di dalam komputer untuk menghancurkan data-data yang ada di dalamnya. Mereka biasanya menargetkan file sistem operasi dan bekerja sampai drive mereka menjadi kosong. Worms biasa muncul melalui email dan instant messages, dan mereka membatasi aktivitasnya dengan apa yang dapat mereka capai di dalam aplikasi yang membantu mereka bergerak. Mereka menggunakan jaringan komputer untuk menyebar, bergantung pada kegagalan keamanan di komputer target untuk mengaksesnya, dan menghapus data. Contoh Worms adalah Melissa, Morris, Mydoom, Sasser, Blaster, and Myife.

3. Trojan Horses

   Trojan adalah sebuah program jahat yang menyamar menjadi sebuah program yang berguna bagi komputer Anda.**Trojan disebarkan dengan menyamar menjadi software rutin yang membujuk user untuk menginstal program tersebut di PC mereka.** Istilah ini sendiri berasal dari cerita Yunani kuno tentang sebuah kuda kayu yang digunakan untuk menyerang kota Troy secara diam-diam. Trojan horses di komputer juga menggunakan cara yang sama untuk menyerang komputer Anda.**_Trojans sekarang dianggap sebagai malware paling berbahaya**, terutama trojans yang dirancang untuk mencuri informasi finansial pemilik komputer tersebut. Beberapa jenis Trojan yang berbahaya biasa memperkenalkan softwarenya sebagai antivirus, padahal software mereka malah membawa masalah ke komputer Anda. Beberapa contoh Trojan horses adalah Magic Lantern, FinFisher, WARRIOR PRIDE, Netbus, Beast, Blackhole exploit kit, Gh0st RAT, Tiny Banker Trojan, Clickbot.A, dan Zeus. Selain itu, di tahun 2015, ditemukan sebuah malware untuk Android bernama Shedun yang memang menargetkan mobile devices.

4. Rootlits

   Software ini bekerja seperti backdoor untuk malware agar mereka bisa masuk dan mengganggu sistem komputer Anda. Rootkit banyak digunakan oleh hackers untuk menginfeksi sebuah sistem. Ini bisa diinstal secara otomatis atau diinstal oleh penyerang saat mereka mendapat hak administrator.

5. Ransomware

Jenis malware ini pada dasarnya menginfeksi sistem dari dalam, mengunci komputer dan membuatnya tidak berguna. Ransomware yang lebih sederhana dapat mengunci sistem yang mungkin sulit dibalikkan bagi kebanyakan orang, sementara ransomware yang lebih maju mengenkripsi file korban, membuat mereka tidak dapat diakses, dan menuntut pembayaran tebusan untuk mendekripsi file.

Karena ancaman malware dalam jaringan yang bisa merusak data dan membuat kerugian yang tidak sedikit, maka sebagai user harus senantiasa melakukan perlindungan dari malware. Secara sederhana, *malware* (*malicious software*) adalah perangkat lunak yang sengaja dibuat sebagai alat untuk melakukan tindak kejahatan. Jenisnya bermacam-macam, virus, *trojan, worm*, adalah yang paling sering kita dengar. Cara infeksinya juga bermacam-macam, *malware* bisa disebarkan melalui lampiran di surel (*phishing*), instalasi *software*, atau menyerang server korban secara langsung. *Flashdisk*, CD, atau kontak fisik apa pun adalah media penyebaran *malware* dari dan ke computer kita. *Malware* yang paling sering disebarkan melalui *flashdisk* adalah *worm*.

Worm memiliki banyak sekali varian. Menurut Microsoft Malware Protection Center, *worm* yang paling banyak menginfeksi pengguna di Indonesia adalah jenis Gamarue dan Bondat. Tergantung kepada variannya, *worm* memiliki karakteristik yang berbeda-beda, begitu juga dengan bahayanya.

Beberapa bahaya umum dan karakteristik *worm* :

- Berbeda dengan virus yang hanya akan aktif dengan "bantuan" pengguna *(double klik* atau *install)*, *worm* dapat menginfeksi berbagai perangkat (komputer, laptop, *smartphone*, *flashdisk*, CD) jika perangkat itu dihubungkan dengan perangkat yang sudah terinfeksi.
- *Worm* juga kerap dijadikan salah satu metode serangan botnet, berisi "payload" yang bertugas untuk mencari kerentanan dalam sebuah server. Komputer dan server yang sudah terinfeksi kemudian digunakan sebagai "zombie" yang dapat dikendalikan oleh si peretas. Untuk mengetahui lebih lanjut tentang serangan botnet dan cara mengamankan server
- Mencuri informasi dari komputer korban.
- Mengunduh *malware* lain.
- Mencegah kita untuk mengakses *file*.
- Menjadi "distributor" yang mengirimkan *malware* ke perangkat, kontak surel, dan jaringan Internet.

- Memakan memori/*bandwith*. Misalnya, kapasitas asli *flashdisk* kita 8GB, *worm* membuat *flashdisk* kita seakan-akan penuh sehingga kita tidak bisa menambahkan *file* lain.

Tanda-tanda computer/flashdisk terkena worm :

- Yang paling umum dari cara kerja *worm* adalah dengan menyembunyikan *file* atau folder asli dan membuat *shortcut* sebagai tiruan. Ekstensi *shortcut* tersebut bisa bermacam-macam, yang paling umum adalah .exe, .dmb, atau ekstensi lain yang mirip *file* biasa.
- *Flashdisk* atau folder tiba-tiba penuh walaupun tidak banyak *file* di dalamnya.
- Beberapa jenis worm menumpang koneksi Internet yang kita gunakan dan memakan kuota.
- Muncul peringatan debug application

Cara mencegah infeksi worm:

- Jangan mengkoneksikan perangkat yang terinfeksi dengan perangkat lain karena cara kerja *worm* yang akan menduplikasi diri tanpa bisa kita cegah.
- Hati-hati ketika menggunakan komputer di tempat umum seperti warnet, tempat *print*, atau ketika menggunakan *flashdisk* milik orang lain.
- Nonaktifkan autorun.
- *Scan flashdisk* dengan anti virus sebelum membuka *file*.
- Aktifkan personal Firewall.

Selain melalui flashdisk, malware dapat menginfeksi computer melalui lampiran surel. Hati-hati terhadap semua lampiran yang masuk ke kotak masuk Anda. Banyak *malware* dilampirkan melalui lampiran surel. Bentuk lampirannya barangkali tidak seperti *file* berbahaya, beberapa bahkan "menyamar" sebagai file Ms. Office biasa. Jenis *malware* yang sering dikirim via lampiran surel adalah *worm, virus, trojan.*

Ada beberapa tips yang bisa diterapkan untuk melindungi perangkat anda dari serangan *malware* via surel :

- Jangan membuka lampiran dari pengirim yang tidak Anda kenal.

- Penyedia layanan surel seperti Gmail menyertakan *Anti-virus scanning attachments* yang akan memindai (*scanning*) setiap lampiran yang datang atau dikirim. Jika Gmail mendeteksi virus dalam lampiran, surel tersebut akan otomatis ditolak.
- Jika Anda menerima notifikasi **"Oops… the virus scanner has a problem right now."** Itu artinya sistem tidak bisa mendeteksi jenis *file* yang diterima karena masalah koneksi atau lainnya, Anda bisa batal mengunduh, mencobanya lain kali, atau mengunduhnya dengan risiko ditanggung sendiri. Tapi kami sangat tidak menyarankan opsi ketiga.
- Lakukan *scan* anti-virus secara berkala di komputer Anda.

Yang berbahaya dari Trojan adalah kemampuannya untuk menyamar menjadi *file* atau program lain yang menurut kita tidak berbahaya. Bisa saja itu berupa foto, video, atau *software* yang mampir begitu saja di kotak masuk kita. Atau bisa saja itu berupa *link* yang di-*tag*-kan oleh teman Facebook kita.

Berbeda dengan *phishing* yang datanya dikumpulkan dari *username* dan *password* yang kita masukkan, *link* berisi *Trojan* bisa aktif hanya dengan SATU KALI klik. Situs *freeware* adalah "markas" penyebaran *Trojan*. Tergantung variannya, *malware* berbahaya ini bisa menyebabkan berbagai macam kerusakan dari yang parah sampai sangat parah. Penyebarannya pun bisa melalui banyak sumber. Yang jelas, sama seperti cara kerja Kuda Troya dalam legenda Yunani, Trojan menyamar sebagai program lain yang kelihatan tidak berbahaya lalu menyusup ke dalam komputer dan server yang kita miliki. Berikut beberapa bahaya Trojan:

- Trojan sering digunakan untuk mencuri data-data transaksi di dalam situs jual beli *online*. Itu sebabnya, ketika melakukan transaksi *online*, pastikan situs tersebut dilindungi oleh SSL Certificates dan perlindungan lainnya.
- Merusak dan melumpuhkan sistem.
- Mencuri dan mengirimkan seluruh data di server atau di komputer kita kepada si pengirim trojan.
- Dipergunakan sebagai bagian dari DDoS *attack*. Menjadikan komputer dan jaringan yang kita gunakan untuk mengirimkan virus atau spam kepada pengguna lain.
- Digunakan sebagai *keyloggers* dan mengintip semua yang kita ketikkan, termasuk *username* dan *password*.
- Menghapus dan menghancurkan *file* di komputer.

Media penyebaran Trojan :

- Kontak fisik. Jika *worm* bisa menduplikasi diri sendiri dan langsung menginfeksi perangkat lain tanpa bisa dicegah, Trojan yang menyamar sebagai program biasa akan menginfeksi komputer lain jika program tersebut dikopi. Aktivasinya bisa dengan beberapa cara, ada yang langsung aktif ketika komputer yang telah terinfeksi terhubung ke Internet, ada yang akan aktif ketika program tersebut dijalankan atau di-*install*, ada pula yang memanfaatkan fitur *autorun* dan langsung aktif ketika di-*double* klik.
- Lampiran dan media di badan surel. Sekilas tampak nyaris sama dengan metode *phishing* berisi *malware* lain. Bedanya, lampiran atau *link* di badan surel berisi trojan biasanya memanfaatkan ketertarikan alami manusia. Misalnya, video yang mengarah ke situs porno dengan *thumbnail* yang "menggoda". Ketika diklik, tab akan terbuka lalu menutup dengan sendirinya. Tanpa Anda sadari, Trojan telah menyusup ke komputer Anda.
- Datang dari orang yang Anda kenal. Serangan Trojan tidak hanya dikirim secara *massal* oleh para peretas di luar sana, trojan bisa saja dikirimkan oleh seseorang yang Anda kenal, baik disengaja oleh si pelaku atau tanpa ia ketahui. Surel berisi Trojan bisa saja tampak seperti ini, *"Hai kamu, sudah lama ya kita tidak bertemu. Eh, tahu nggak? Aku bikin video nih buat kamu, tonton gih."* Begitu diklik, maka, bum! Trojan masuk ke komputer Anda.
- Situs *freeware*. Situs penyedia software gratis adalah "markas" penyebaran Trojan. Untuk lebih lengkapnya, topik ini akan dibahas di poin selanjutnya.

Selain gerbang pertukaran data dan informasi, Internet adalah tempat segala macam barang gratisan berada. Foto, musik, video, *e-book, software, game*, dan lain-lain. Para pengguna yang tidak peka biasanya tidak tahan ketika melihat kata "free" atau "gratis" dan akan mengunduhnya begitu saja. Ini yang dimanfaatkan oleh para peretas. Meskipun misalnya jenis *file* yang kita unduh benar, tapi kita tidak akan pernah tahu *script* atau *malware* macam apa yang ditanamkan di dalamnya. Untuk mencegah hal-hal yang tidak diinginkan, sebaiknya lakukan hal-hal berikut sebelum memutuskan untuk mengunduh *file* apa saja dari Internet :

- Situs penyedia *freeware* atau *software* gratisan sering dimanfaatkan untuk menyebarkan Trojan. Sebelum memutuskan untuk mengunduh atau berkunjung ke sebuah situs, Anda bisa mendeteksinya dengan tools deteksi malware.
- Hindari mengunduh jenis *software* apa pun dari situs yang bukan penyedia aslinya. Misalnya, mengunduh Windows dari situs selain Microsoft.

- Ketika akan mengunduh *file* seperti foto, *e-book,* atau video, pastikan situs tersebut sudah Anda kenal atau kredibel. Bisa dilihat dari sudah berapa lama situsnya berdiri, kontaknya, atau tampilan webnya.
- Sayangnya, kebanyakan situs-situs peretas terlihat seperti situs web profesional. Jadi, pastikan bahwa anti virus Anda aktif.
- Situs berisi Trojan biasanya berisi *pop-up* yang muncul secara bertubi-tubi dan sama sekali tidak berkorelasi dengan *software* yang akan Anda unduh lalu ketika tab ditutup, *browser* akan membuka dengan sendirinya dan membawa Anda ke situs-situs yang tidak Anda kenal. Misalnya, Anda akan mengunduh anti virus dari situs entah apa lalu tiba-tiba muncul *pop-up* berisi ajakan untuk mengklik *link* porno atau undian yang menjanjikan hadiah puluhan juta.

Kesimpulan

Malware dibuat secara khusus agar tersembunyi sehingga mereka bisa tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut. Biasanya, mereka menyamarkan diri menjadi program yang bersih. Efek dari malicious software biasa jauh lebih berbahaya bagi corporates dibanding untuk personal user. Jika malware menyerang jaringan sistem Anda, mereka bisa menyebabkan kerusakan dan gangguan yang meluas, yang memerlukan upaya pemulihan ekstensif di dalam organisasi. Malware dapat menginfeksi komputer dengan masuk melalui email, hasil download internet, dan program-program yang sudah terinfeksi. Sementara itu, virus adalah jenis malware tertentu yang menggandakan sesuatu dan menginfeksi program apapun di komputer Anda. Secara teknis, virus adalah jenis malware yang pada saat dijalankan, menggandakan dirinya sendiri dan mereproduksi source code dirinya sendiri serta menginfeksi program komputer lain yang ada dengan cara memodifikasi cara kerja program tersebut.

Karena perkembangan yang sangat pesat, ada banyak sekali para pengguna internet yang komputernya terinfeksi virus. Maka menjadi masuk akal, bila muncul banyak pula antimalwar yang dikembangkan dan dijual ke pasar. Namun anti-malware pada saat itu lebih awam disebut sebagai antivirus. Hal itu menyebabkan suatu masalah, sebab jika para pengelola berfokus pada antivirus software saja, mereka jadi mengabaikan jenis-jenis malware lain yang potensial.

Anti-malware adalah jenis software yang di-install langsung pada komputer untuk mendeteksi dan menghapus malware dari sistem yang ada secara aktif. Bagaimana cara anti-malware tersebut melakukan identifikasi? Dengan tetap terhubung ke internet, kebanyakan program anti-malware ini dapat menyimpan daftar malware yang terus diperbaharui sehingga ia mampu mengidentifikasinya. Selain itu, anti-malware dapat difungsikan sesuai jadwal untuk melakukan pemindaian berkala. Penjadwalan ini dilakukan untuk mengetahui apakah ada bagian-bagian perangkat Anda yang rusak atau terinfeksi.

Referensi :

https://media.neliti.com/media/publications/256241-perancangan-sistem-pendeteksi-dan-penceg-02992d4e.pdf

https://www.dewaweb.com/blog/cara-melindungi-komputer-dari-malware-dan-bahaya-lainnya/

https://www.dewaweb.com/blog/pengertian-malware-pentingnya-dewaguard/#:~:text=Malware%20adalah%20singkatan%20dari%20malicious,biasa%20didefinisikan%20sebagai%20kode%20berbahaya.

Nama : I Made Harya Wijaya Oka Rafflesia
NIM : 182420129
Matkul : Ethical Issues in Electronic Information Systems

PHISHING

Pendahuluan

Di era modern sekarang, orang-orang tidak bisa lepas dari yang namanya internet dan gadget. Di tambah, saat ini orang-orang berlomba memperbanyak akun jejaring sosial mereka untuk mencari kepopuleran seperti Facebook, Twitter, Instagram, Snapchat, dan masih banyak lagi. Untuk mendapat berita ter-updateorang-orang juga bisa menjumpai berbagai macam artikel baik dalam maupun luar negeri melalui sebuah laman web ataupun di jejaring sosial juga. Pastinya orang-orang membuka web browser dulu agar bisa pergi ke berbagai jejaring sosial semacam itu. Setiap orang pasti memiliki akun jejaring sosial lebih dari satu. Selain itu, sosial media juga digunakan untuk lahan berbisnis misalnya online shop. Kegiatan ini sangat mudah dan menguntungkan karena tidak membutuhkan modal dan hanya tinggal memposting barang jualan. Untuk pembayarannya bisa lewat rekening, COD, market, dll.

Di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya yaitu dengan phishing. Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. *Phishing* termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi *hacker* cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang *hacker*.

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam *phishing*. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh *fake link* pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran *online*.

Untuk pengantisipasian serangan *phishing* semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada *link* yang masuk melalui akun sosial media maupun *email* yang di gunakan untuk akun sosial media. Karena *link* yang tidak di kenal patut di curigai sebagai serangan *phishing* yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain.

Sebenarnya tujuan di buatnya jurnal ini yang pertama yaitu agar orang-orang mulai mengubah pemikirannya terlebih dahulu terhadap serangan *phishing*. Kemudian orang-orang harus mengetahui hal-hal yang mencurigakan pada akun jejaring sosial maupun situs *web*

yang lain. Bila benar ada serangan *phishing*, maka mereka harus meninggalkan laman palsu itu sesegera mungkin. Jangan hanya pergi begitu saja, kita juga harus mencari jalan keluar untuk menyelamatkan akun kita. Tentu kita harus mencari anti*phishing* untuk mencegahnya. Karena sekali kita terkena serangan, maka ancaman *phishing* juga akan menyerang pengguna yang lain. Dan serangan akan terus menyebar dan menyebar ke seluruh penjuru dunia. Bila dalam jejaring sosial pengguna yang terserang tidak tau apa-apa, di pihak lain akan marah-marah karena pengguna yang terserang tadi akan terus mengirim pesan spam pada seluruh akun yang berteman dengannya.

Tidak tau sampai kapan serangan *phishing* akan di lancarkan sebagai kejahatan siber. Karena para *hacker-hacker* itu terus memunculkan ide-ide baru untuk merusak kegiatan di internet.Dan sayangnya di setiap tahunnya kasus seperti ini semakin bertambah banyak dan korban yang terjaring juga tidak bisa hanya di hitung dengan jari. Mereka mencari uang dengan cara yang mudah. Namun tak selamanya mereka melakukan itu karena uang. Biasanya mereka hanya ingin bersenang-senang atau ingin mengintip kegiatan sang pemilik akun. Jika beruntung, mereka juga bisa mendapat uang sekaligus melihat-lihat isi akun pengguna yang mereka serang untuk bersenang-senang. Bila hanya orang biasa yang mereka serang mungkin masalah tidak akan terlalu besar. Bagaimana jika yang mereka serang adalah orang yang penting atau pun orang yang berpengaruh di dunia ini.Kasus itu pasti sudah sering terjadi. Orang-orang yang memiliki kuasa tertinggi beberapa juga melakukan kejahatan tetapi ia hanya menjadi bagian penyuruh untuk sang hacker. Selanjutnya hacker-hacker itu yang melaksanakan perintah untuk menyerang. Hal-hal itu sudah wajar terjadi apalagi saat masa-masa kampanye berpolitik ataupun contohnya pada saat dua perusahaan yang awalnya menjalin hubungan yang baik tiba-tiba salah satu perusahaan merasa kecewa karena saat pembagian hasil tidak memenuhi sepakat yang tercantum sebelumnya. Maka muncul lah ide-ide berbuat kecurangan. Mereka akan memanfaatkan *hacker* sebagai sarana penghancur sang lawan. Mereka menyuruh sang hacker untuk diam-diam mencuri data keuangan perusahaan musuh dan kemudian memanipulasi data tersebut sebaik mungkin. Lalu pada akhirnya semua uang hasil kerja sama mereka menjadi milik perusahaan yang menyewa hacker tadi semua. Pastinya si *hacker* tadi mendapat keuntungan beberapa persen. Untuk itulah masih ada banyak orang baik di dunia ini yang mau menciptakan alat pendeteksi atau aplikasi untuk mencegahnya. Para peneliti maupun pembuat aplikasi itu biasanya merupakan orang-orang yang pernah mengalami serangan *phishing*. Mereka tidak terima dan kemudian memutuskan untuk membalaskan dendamnya dengan sebuah aplikasi anti *phishing*. Maka dari itu orang-orang harus memanfaatkannya sebaik mungkin agar mengurangi resiko terkena serangan *phishing*. Bila enggan melakukan sesuatu yang menurutnya terlalu merepotkan, mereka juga bisa menjaga akunnya sebaik mungkin dengan pengamanan yang tepat. Hanya dengan cara itu akun tidak akan di serang dan pengguna bisa nyaman bersosialisasi di dunia maya tanpa hambatan.

Literature Review

Kata "phishing" berawal pada tahun 1996, kebanyakan orang percaya kata ini berasal sebagai ejaan alternatif dari "fishing" (memancing) seperti halnya "memancing informasi".Phising dikenal juga sebagai “Brand spoofing” atau “Carding” adalah sebuah bentuk layanan yang menipu anda dengan menjanjikan keabsahan dan keamanan transfer data yang anda lakukan. Menurut Felten et al spoofing (1997) dapat didefinisikan sebagai

“Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya”.

Pengertian Phising secara lengkapnya adalah suatu aktivitas penipuan untuk mendapatkan username dan password dari pengguna dengan cara tidak sah. Salah satu cara yang banyak dilakukan oleh para hacker dengan membuat website tiruan yang mirip dengan perusahaan aslinya, tujuannya agar Anda percaya dan kemudian memasukan username serta password, nah inilah yang dicari oleh para hacker Phising adalah singkatan dari Password Harvesting Phising yang artinya adalah tindakan memancing dengan tujuan untuk mengumpulkan password. Bentuk penipuan melalui phising, baik untuk mendapatkan informasi yang sensitif seperti password, nomor kartu kredit dan lain-lain atau menggiring orang untuk melakukan download file palsu yang berisi virus dengan menyamar sebagai orang atau lembaga bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti email atau pesan singkat lainnya. Aksi ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus phising selama Januari 2005 melonjak 42% dari bulan sebelumnya. Anti-Phishing Working Group (APWG) dalam laporan bulanannya, mencatat ada 12.845 e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana phishing. Selain terjadi peningkatan kuantitas, kualitas serangan pun juga mengalami kenaikan. Artinya, situs-situs palsu itu
ditempatkan pada server yang tidak menggunakan protokol standar sehingga terhindar dari pendeteksian.

Komunikasi yang dipakai ini mulai dalam bentuk web site social yang sangat popular di mata masyarakat, site-site auction/ lelang, pengolah transaksi online payment atau dalam bentuk lain yang biasanya user menggunakan site tersebut untuk kepentingan administrasi, seperti email site, site jejaring public, dan lainnya. Bentuk phishing yang lain adalah mengirimkan email official dan instant messaging kepada user yang biasanya menggunakan site-site legitimate dan site-site nama besar perusahaan yang dikenal masyarakat dilengkapi dengan logo perusahaan, header email official sampai dengan cap dan tanda tangan salah satu pimpinan perusahaan tersebut.

Pembahasan

Berikut merupakan cara kerja phishing berdasarkan sumber-sumber ancaman phishing yang telah kami survey dari beberapa jurnal :

A. Email

Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti link URL yang terdapat dalam email tersebut [2]. Pada dasarnya, phishing menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima email [9]. Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut [13]. Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi [15].

B. Website

Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti password dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas [7].Phiser juga menggunakan tool untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu [6]. Selain itu, phiser menciptakan embedding link untuk mendapatkan informasi sensitif milik korban [3].

C. Malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu file yang di kirim oleh phiser sebagai penetralisir malware di komputer nantinya [8].

CARA MENCEGAH PHISHING

Berikut adalah hasil survey kami mengenai cara pencegahan atau antisipasi terhadap serangan phishing melalui website dari beberapaliteratur :

1) Medeteksi dengan toolsdetect

Sekarang ini internet sudah dianggap sebagai makanan sehari-hari, bahkan ada beberapa orang yang berangga-pan tanpa internet mereka tidak bisa hidup. Ada banyak hal yang bisa kita lakukan dengan internet, mulai dari mencari informasi, berbagi informasi, dsb. Namun, pasti kita pernah menjumpai situs-situs yang muncul tanpa kita inginkan dan mengandung informasi berhadiah yang menggiurkan. Tentu saja hal tersebut akan menarik kita untuk mengisinya dengan data penting tanpa tau bahwa itu hanyalah situs phishing. Untuk mencegah hal tersebut kita dapat menggunakan toolsdetect yang mana dapat membedakan mana situs yang asli dan palsu (phishing). Berikut toolsdetect yang dapat digunakan :

a) PhishShield

PhishShield merupakan aplikasi desktop yang berkonsentrasi pada URL dan konten situs web phishing [13]. Cara ker-janya dengan mengambil URL sebagai masukan dan outputnya berupa status yang mengkonfirmasi URL [13] termasuk phishing atau situs asli [13]. Tingkat akurasi yang diperoleh untuk PhishShield adalah 96,57% dan mencakup berbagai situs phishing yang dihasilkan tingkat kepalsuan negatif dan positif [13].

b) LinkGuard Algoritma

LinkGuard Algoritma digunakan untuk menganalisis dua URL dan akhirnya tergantung pada hasil yang dihasilkan oleh algoritma [15]. URL tersebut adalah URL yang melibatkan ekstraksi URL yang sebenarnya dan URL visual (yang dilihat pengguna) [15].

c) PhishDetector

PhishDetector adalah ekstensi browser yang digunakan untuk mendeteksi serangan phishing yang mana menggunakan al-goritma pencocokan string perkiraan untuk menentukan hubungan antara konten dan URL dari suatu halaman web[11].

2) Menggunakan add ons web browser anti tabnabbing

Setiap tahunnya para phisher melancarkan aksi-aksinya dengan membuat serangan-serangan baru. Dan salah satu serangan baru tersebut yaitu bernama tabnabbing. Serangan phishing tersebut dapat menyerang pada web. Dimana cara penyerangannya ketika pengguna membuka banyak tab, phishing tersebut akan terbuka di sela-sela tab yang lain. Saat pengguna lengah, maka tab tersebut akan di buka dan serangan di mulai. Tab palsu itu di samarkan menjadi salah satu tab yang di buka oleh pengguna dan tab asli yang sebelumnya lenyap. Untuk itulah serangan ini di anggap serangan yang pintar karena tidak lagi menggunakan link yang di klik dulu agar pengguna masuk perangkap phisher. Namun sepintar apapun suatu serangan, pasti ada jalan keluar. Beberapa cara pencegahan serangan

tabnabbing: a) Ketika pengguna membuka firefox dan terjadi serangan, pengguna bisa mengatasi serangan dengan account manager. Account manager dapat mengamankan pengguna karena pengguna di sarankan menyimpan login dan saat itu juga pengguna di berikan password acak setiap kali login [14]. b) Tidak hanya pada firefox saja, pada crome juga di berikan pengamanan terhadap phishing tabnabbing. Yaitu menggunakan AgenTab. AgenTab melakukan tindakan ketika pengguna mulai membuka situs web [14]. AgenTab akan menyalakan peringatan ketika serangan terdeteksi. Peringatan tersebut akan muncul ketika tab tiba-tiba berubah tempat [14]. c) Dan yang terakhir dalam pencegahan tabnabbing dapat di lakukan dengan NoTabNab4. Add-on tersebut di usulkan oleh web browser Unlu dan Bicakci, dimana serangan phishing dapat diketahui saat suatu tab palsu meniru tab asli lalu add-on tersebut bekerja dengan cara memperingati dengan memberi tanda warna kuning atau merah sesuai tingkat serangan pada highlightned [14].

3) Menggunakan mekanisme pre-filter

Pencegahan phishingjuga dapat di lakukan dengan penggunaan anti-phishing pre-filter ini. Di dalam pre-filter terdapat tiga bagian pencegahan yakni Site Identifier, Login Form Finder, dan Webpage Feature Generator. Ketiganya tersebut melakukan pencegahan secara berurutan. Site Identifier digunakan untuk mengurangi jumlah perhitungan situs yang tidak perlu dan hanya mendeteksi halaman yang sah [6]. Kemudian Login Form Finder di gunakan untuk menyaring halaman tanpa bentuk login lalu menghentikan mereka dari proses lebih lanjut karena form login merupakan satu-satunya cara untuk menyadarkan pengguna bila informasi pribadinya dicuri oleh phiser [6]. Sistem ini dapat mengurangi kesalahan positif dari sistem tanpa harus mencurigai jumlah kesalahan negatif [6]. Yang terakhir adalah Webpage Feature Generator, dimana fungsinya adalah mengidentifikasi halaman web phishing dengan melacak karakteristik phishing yang di pamerkan dalam halaman tersebut [6]. Seseorang dapat menggunakan cara ini ketika merasa bila halaman webnya sudah terserang phishing.

4) Pendeteksian dengan streaming analytics ‘PhishStrom’

Sekarang ini banyak sekali orang-orang yang berlomba-lomba melakukan penelitian untuk menciptakan suatu alat maupun aplikasi. Namun bukan hanya itu saja. Orang-orang juga mulai melakukan pendeteksian dengan berbagai cara. Dan anti phishing kali ini yaitu melakukan pendeteksian berupa streaming analisa menggunakan PhisStrom. PhisStrom sendiri di gunakan untuk mendeteksi URL yang terserang phishing. Dalam percobaannya, pendeteksian dengan cara ini dapat menghasilkan akurasi klasifikasi 94, 91% dengan tingkat positif palsu yakni 1,44% . Untuk risiko pada pengujian dataset menunjukkan pengidentifikasian 99,22% pada web yang sah dan phishing 83,97%. Untuk selanjutnya, PhisStrom dapat di gunakan sebagai alat add-on pada Mozila Firefox agar mempermudah dalam pendeteksian serangan phishing pada web.

5) Self-efficacy

Untuk mencegah terjadinya phishing tidak hanya membutuhkan suatu aplikasi atau software anti-phishing me-lainkan juga membutuhkan self-efficacy. Self-efficacy adalah keyakinan individu dalam mengambil tindakan pen-gamanan[4]. Dengan memiliki sikap tersebut dapat menunjukkan kepercayaan individu dalam pemecahan masa-lah dan penyelesaian tugas sesuai kemampuan mereka sendiri[17]. Sangat penting bagi kita melatih sikap tersebut dari dini karena di era modern ini kita tidak bisa jauh dari teknologi dan mau tidak mau kita akan menjumpai bahkan terjerat dalam serangan phishing. Caranya adalah

dengan mencari tau tentang phishing mulai dari defini-si, cara kerja, contohnya, dll. Pada beberapa jurnal menunjukkan bahwa peserta yang secara khusus mengikuti studi phishing lebih berhati-hati dalam membedakan web asli dan palsu(phishing) dari pada peserta yang tidak mengikuti studi phishing. Phisher biasanya menyerang perusahan karena untuk mengambil keuntungan (uang) dengan melalui karyawan-karyawannya. Ada dua temuan utama alasan phisher menyerang karyawan pe-rusahaan: a) karyawan mudah tertipu dan rentan menjadi korban pada SNS yang mana unsur-unsur konseptual memberikan pemicu psikologis untuk penyerang; b) organisasi tidak memiliki mekanisme untuk mengontrol ancaman keamanan pada SNS online. Untuk itu sangat perlu pembinaan terhadap karyawan-karyawan tentang phishing guna untuk melindungi informasi perusahaan.

Kesimpulan

Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Sumber-sumber ancaman *phishing* yaitu *email*, *website*, dan *malware*. Berdasarkan hasil *survey* yang telah dilakukan *website* merupakan sumber ancaman *phishing* paling banyak dan cara pencegahan yang sering dilakukan adalah *self-efficacy* (keyakinan individu dalam mengambil suatu tindakan).

Daftar Referensi

Gavahane, M., Sequeira, D., Pandey, A., & Shetty, A. (2015). A nti-Phishing U sing H adoop- F ramework, 4–7.

Rachmawati, D., Studi, P., Komputer, S., Utara, U. S., Crime, C., & Security, C. (1978). Issn : 1978-6603 phising sebagai salah satu bentuk ancaman dalam dunia cyber, 209–216.

Gowtham, R., & Krishnamurthi, I. (2013). ScienceDirect A comprehensive and efficacious architecture for detecting phishing webpages. *Computers & Security*, *40*, 23–37. http://doi.org/10.1016/j.cose.2013.10.004

Hamid, I. R. A., & Abawajy, J. H. (2014). An Approach for Profiling Phishing Activities. *Computers & Security*. http://doi.org/10.1016/j.cose.2014.04.002

Perlindungan dari Insiden Serangan Phising dari Aspek Etiket.

Pendahuluan

Saat ini banyak sekali media online membicarakan tentang kasus pencurian data atau penjualan data pelanggan perusahaan startup di Indonesia. Karena berita ini, para pelanggan dari E-Commerce tersebut khawatir terhadap akun dan datanya yang mungkin bisa disalahgunakan. Berita ini sempat trending di sosial media **Twitter** dan menimbulkan banyak respon yang bermacam-macam dari netizen. Nah oleh karena itu pada kesempatan kali ini saya akan membuat paper yang membahas tentang hal tersebut yang mungkin bisa bermanfaat untuk kita.

Seiring berkembangnya jaman dan juga teknologi, saat ini banyak sekali kasus cybercrime yang terjadi, salah satunya yaitu Phising. Phising adalah suatu metode kejahatan dunia maya di mana target dihubungi melalui email, telepon atau pesan teks oleh seseorang yang menyamar sebagai lembaga yang sah untuk memikat individu agar memberikan data sensitif seperti informasi yang dapat diidentifikasi secara pribadi, rincian kartu kredit dan perbankan, serta kata sandi. Di dalam email tersebut biasanya akan terdapat sebuah tautan ke halaman palsu yang tampilannya dibuat persis seperti website yang asli untuk menjebak seseorang.

Informasi tersebut kemudian digunakan untuk mengakses akun-akun penting dan dapat mengakibatkan pencurian identitas dan kerugian finansial. Gugatan pertama kasus phishing diajukan pada tahun 2004 terhadap seorang remaja California yang menciptakan tiruan dari website “America Online”. Dengan website palsu ini, ia dapat memperoleh informasi sensitif dari pengguna dan mengakses detail kartu kredit untuk menarik uang dari akun bank mereka.

Literature Review

Hakitat *Phising*

Phising adalah suatu metode untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target. Istilah *phising* sendiri berasal dari bahasa slang yaitu *fishing* yang berarti memancing korban untuk terperangkap dijebakannya. Phising bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. Hal ini bisa saja dengan maksud mencari celah untuk beberapa akun yang terhubung dengan akun yang telah didapat. *Hal ini bisa saja dengan maksud mencari celah untuk beberapa akun yang terhubung dengan akun yang telah di dapat.*

Phishing adalah *scammer* berbasis *e-mail* yang pada dasarnya adalah penipuan dengan mengatasnamakan nama kita sendiri, biasanya *phishing* ini berbentu*k e-mail* dengan isi seperti saldo Bank karena kita nasabah dan juga pemberitahuan yang penting mengatasnamakan mereka sendiri, mengatasnamakan mereka sendiri dengan arti adalah mereka ini menipu atau sering juga memakai nama Bank atau Lembaga finansial yang ada di Indonesia seakan-akan E-Mail tersebut resmi sedangkan pada kenyataannya tidak. Lembaga financial di Indonesia bahkan di seluruh dunia menjaga *privacy* dan tidak akan pernah mengirim email tersebut kepada nasabah karena bersifat sangat *privacy*.

Jenis - Jenis *Phising*

Phising terbagi menjadi beberapa jenis dan teknik yang terus menerus dilakukan oleh penjahat cyber, jenis-jenisnya yaitu :

1. Spear Phising

Spear phishing adalah tindakan mengirim email ke target spesifik dan mengaku sebagai pengirim terpercaya. Isi email tersebut biasanya berisi tautan yang mengarahkan

penerima ke situs web palsu yang penuh dengan malware. Upaya ini ditargetkan untuk mencuri informasi sensitif seperti kredensial akun atau informasi keuangan dari korban tertentu. Meskipun sering dimaksudkan untuk mencuri data untuk tujuan jahat, penjahat cyber mungkin juga berniat untuk menginstal malware di komputer pengguna yang ditargetkan. Ini adalah bentuk paling sukses untuk memperoleh informasi rahasia di internet, mencakup 91% serangan.

2. Deceptive Phising

Deceptive Phising adalah jenis penipuan phishing yang paling umum. Penipuan ini terjadi ketika sumber yang dikenal atau perusahaan yang Kita kenal mengirim email kepada Kita untuk mengkompromikan informasi. Biasanya, email-email ini meminta Kita:

- Verifikasi informasi akun
- Masukkan kembali informasi, seperti login atau kata sandi
- Minta kita mengubah kata sandi kita
- Melakukan pembayaran

Setelah informasi ini dimasukkan, peretas akhirnya mendapatkan informasi dan dapat mengakses akun Kita lalu menggunakan informasi sensitif untuk mencuri informasi kartu pembayaran, menjual informasi pribadi Kita atau memanfaatkan informasi sensitif Kita untuk mendapatkan keuntungan.

Ada 2 cara yang bisa dilakukan oleh pelaku untuk melakukan tindakan phising ini, cara pertama yaitu pelaku mengklaim atau menyamar sebagai perwakilan dari sebuah instansi/perusahaan resmi dan meminta korbannya tersebut untuk memberikan informasi tertentu. Etiket kedua, pelaku ini menyisipkan situs berbahaya di tautan yang korban klik.

3. Smishing

Smishing adalah jenis phishing yang melibatkan pesan teks. Sering kali, bentuk phishing ini melibatkan pesan teks dalam SMS atau nomor telepon. Smishing sangat menakutkan karena kadang-kadang orang cenderung lebih mempercayai pesan teks daripada email. Sebagian besar orang menyadari risiko keamanan yang terlibat dengan mengklik tautan di email. Namun lain hal jika melalui pesan teks.

Biasanya pelaku kejahatan menggunakan cara atau trik agar korban mengklik tautan yang diberikan, menelpon nomor yang tertera, atau membalas pesan tersebut dengan informasi yang pelaku butuhkan. Contohnya yang sering ada di Indonesia yaitu menang undian atau hadiah dari perusahaan besar dan mengatasnamakan diri mereka bagian dari perusahaan tersebut. Selain hal tersebut sebenarnya masih banyak lagi modus lainnya. Oleh karena itu hati-hati dan jangan mudah percaya.

4. Whale Phising

Whale phishing adalah istilah yang digunakan untuk menggambarkan serangan phishing yang seEtiket khusus ditujukan untuk individu yang kaya, berkuasa, atau terkemuka. Karena status mereka, jika pengguna seperti itu menjadi korban serangan phishing, ia dapat dianggap sebagai big pish (ikan besar) atau whale (ikan paus). Whale phising ini pelaku menggunakan taktik yang sama seperti spear phising.

Ciri-Ciri Phising

1. URL Singkat di Email

Banyak contoh serangan phishing akan mengundang korban untuk mengklik ke URL yang terlihat resmi. Namun, jika pengguna meluangkan waktu sedetik untuk memeriksa tautan tersebut, maka dapat ditemukan bahwa itu bukan URL yang sah. Pelaku berharap korban tidak akan memeriksa tautan sama sekali dan cukup mengklik. Dalam kasus lain,

pelaku akan mengambil sedikit variasi pada alamat web yang sah dan berharap pengguna tidak menyadarinya.

2. Ejaan atau Tata Bahasa yang Buruk

Pesan resmi dari organisasi besar mana pun tidak mungkin mengandung ejaan atau tata bahasa yang buruk.

3. Alamat Pengirim Yang Tidak Sesuai

Perusahaan resmi biasanya akan menggunakan alamat email resmi yang berasal dari nama domain website-nya. Pastikan terlebih dahulu bahwa email itu memiliki website yang bisa diakses dan merupakan website resmi perusahaan.

4. Tampilan Website Relatif Mirip Asli

Ini menjadi salah satu ciri web phising yaitu tampilan website terlihat relatif mirip dengan yang asli. Jika ada beberapa hal yang tidak sesuai atau merasa berbeda seperti biasanya, Kita harus memastikan terlebih dahulu bahwa itu website yang sah.

5. Alamat Website Typo

Walaupun pelaku bisa membuat website yang mirip dengan website aslinya, namun untuk domain tidak akan bisa menirunya nya. Karena 1 (satu) domain resmi hanya bisa digunakan untuk 1 (satu) website. Jadi untuk mengelabui korban, pelaku menggunakan domain yang sedikit mirip dengan website aslinya contoh www.klikbca.com dibuat web palsu nya dengan domain www.klikkbca.com. Jadi sebelum login pastikan alamat website nya benar.

6. Website Tidak ada HTTPS

Untuk memberikan keamanan pada penggunanya biasanya situs-situs besar atau kredibel menggunakan SSL untuk websitenya. Kita bisa melihat di bagian address bar untuk

mengetahui website tersebut menggunakan HTTPS (SSL) atau tidak. Sebagian besar situs phising tidak memiliki **SSL Certificate**.

7. Login Sering Gagal

Jika Kita sudah menggunakan username dan password yang benar namun masih tidak bisa masuk, Kita perlu curiga mungkin Kita berada di situs phising. Jika Kita sudah terlanjur mengisi data disana, segeralah Kita masuk ke website aslinya dan ganti password Kita.

Pembahasan

Phising biasanya sering digunakan pada email, dimana penyebaran melalui email ini dilakukan untuk memberikan informasi yang mengarah ke halaman palsu untuk maksud menjebak korban. Untuk menghindari phising, pengguna harus lebih berhati-hati dengan memperhatikan beberapa hal keamanan. Sebagai contoh, jika Kita mengakses suatu halaman website, maka pastikan Kita berada di halaman website dengan url domain yang benar. Misalnya, untuk login facebook pastikan Kita mengakses halaman https://facebook.com/ bukan halaman selain itu.

Phising banyak memakan korban di sektor social media, hal itu dikarenakan social media merupakan akun harian yang sering digunakan oleh pengguna, tanpa sadar pengguna memasuki halaman jebakan yang menyebabkan pengguna bisa saja terjebak karena halaman palsu tersebut. Tidak hanya itu, phising juga terkadang bisa terjadi manipulasi dimana komputer yang terinfeksi bisa saja memanipulasi beberapa hal yang membuat halaman itu merupakan halaman aslinya, sehingga perlu diperhatikan untuk komputer Kita tidak terkena virus untuk menghindari kasus ini.

Pada dasarnya *Phising* didefinisikan sebagai penipuan yang memanfaatkan email untuk menguak informasi sensitif korban. Phising memiliki 2 teknik untuk memperdaya korban agar ‘menyerahkan’ informasi mereka. Pertama, dengan menautkan virus

atau *malware* pada *e-mail phising* yang dikirimkan. Pada tahun 2016, *e-mail phising* yang menyasar korban-korbannya, 8,89% melampirkan rojan-downloaderJS.Agent. sebuah program jahat yang mengancam *system komputer* siapapun. Teknik kedua adalah *e-mail phising* akan berisi tautan menuju situs web asli namun palsu sebuah Lembaga atau perusahaan.

Selain teknik ada beberapa tipe *phising* yang kerap dilakukan oleh para pelaku kejahatan di dunia maya. Namun, jenis *phising* yang paling populer dan kerap digunakan biasanya ada dua jenis. Pertama, adalah *clone phishing*. Pada *phising* jenis ini, serangan dilakukan dengan melalui surat elektronik yang terlihat resmi dan mengandung *attachment* di dalamnya. *Attachment* ini kemudian digunakan untuk mengambil data dari si korban untuk kemudian dikirimkan lagi ke tempat yang diinginkan oleh si pelaku. Jenis yang kedua dinamakan *spear phishing*. Tingkat keberhasilan mencuri data pada jenis ini cenderung lebih tinggi karena si pelaku memiliki target yang lebih spesifik dibandingkan jenis *phising* sebelumnya. cara kerjanya, mereka mencari dan mengenali data dari targetnya terlebih dahulu sehingga si korban tidak akan curiga bahwa dirinya sedang diserang.

Para tersangka pembuat *phising*, biasanya akan membuat situs web atau perusahaan semirip mungkin dan terlihat sangat asli dan dijadikan langganan si korban dengan sangat baik, jika korban masuk situs tersebut maka lenyaplah informasi yang dimilikinya. Data yang biasanya diambil bisa berupa *password*, nomor kartu kredit, nomor telepon, hingga nomor rekening bank yang biasanya dicantumkan korban pada layanan-layanan yang tersedia di internet seperti media sosial, *e-commerce*, penyimpanan *cloud*, sampai pinjaman berbasis *online*.

Cara Kerja Phising

Serangan phishing dasar mencoba menipu pengguna untuk memasukkan detail pribadi atau informasi rahasia lainnya, dan email adalah metode paling umum untuk

melakukan serangan ini. Diperkirakan 3,7 miliar orang mengirim sekitar 269 miliar email setiap hari. Para peneliti di Symantec menyatakan bahwa hampir satu dari setiap 2.000 email ini adalah email phishing, yang berarti sekitar 135 juta serangan phishing dicoba setiap hari.

Kebanyakan orang tidak punya waktu untuk menganalisis setiap pesan yang masuk ke kotak masuknya dengan hati-hati dan inilah yang dieksploitasi oleh phisher menggunakan beberapa Etiket. Teknik kampanye phishing yang umum mencakup penawaran hadiah yang dimenangkan dalam kompetisi palsu seperti lotere atau kontes oleh pengecer yang menawarkan ‘voucher pemenang’.

Dalam contoh ini, untuk ‘memenangkan’ hadiah, para korban diminta untuk memasukkan rincian mereka seperti nama, tanggal lahir, alamat dan detail bank untuk mengklaim. Teknik serupa juga digunakan dalam penipuan lain di mana pelaku mengklaim berasal dari bank yang ingin memverifikasi detail pembelian yang tidak ada atau kadang-kadang bahkan lebih parah lagi pelaku akan mengklaim berasal dari perusahaan keamanan teknologi dan mereka memerlukan akses ke informasi untuk menjaga keamanan pelanggan mereka. Penipuan lain yang lebih canggih yaitu ditujukan untuk pengguna bisnis. Di sini pelaku dapat berperan sebagai seseorang dari dalam organisasi yang sama atau salah satu pemasoknya dan akan meminta Kita untuk mengunduh lampiran yang mereka klaim berisi informasi tentang kontrak atau kesepakatan. Dalam banyak kasus file tersebut akan mengeluarkan perangkat lunak berbahaya ke dalam sistem dan akan memanen data pribadi. Namun dalam banyak kasus file itu juga digunakan untuk menyebarkan ransomware.

Etiket Mengantisipasi Phising

Biasanya korban *phising* akan terjebak saat mengklik tautan pada surat elektronik palsu atau laman iklan sehingga mengarahkannya ke tautan yang berbahaya. Saat Kita sudah

mengklik, pelaku dapat mengakses komputer dengan akses penuh tanpa disadari sama sekali. Oleh karena itu, Kita perlu mengenali Etiket mengantisipasi serangan ini.

Etiket pertama yang perlu diperhatikan adalah dengan tidak mengklik tautan seEtiket sembarangan. Perhatikan dengan seksama tautan tersebut karena biasanya memiliki kesalahan dalam struktur penulisannya sehingga sekilas terlihat mirip dengan tautan yang asli. Misalnya, tautan tersebut mengarah ke situs dengan *domain* yang tidak jelas alih-alih ke *domain* resminya.

Etiket kedua adalah dengan mengenali alamat pengirim jika serang dilakukan melalui surat elektronik. Biasanya pelaku akan menggunakan akun dengan *domain* yang terlihat mirip dengan *domain* yang asli. Misalnya menggunakan alamat "updates@gmail-co.com." Etiket mengenalinya cukup mudah, tapi terkadang korban akan terdistraksi terlebih dahulu dengan isi surel yang menarik, misalnya dengan embel-embel korban akan mendapatkan hadiah dengan mengklik sebuah tautan.

Terakhir, jika Kita sudah terlanjur terjebak ke dalamnya langkah pertama yang harus dilakukan adalah jangan panik. Lakukan segera tindakan untuk mengurangi kerugian yang akan dialami. Misalnya dengan melakukan penggantian *password* seluruh akun di dunia digital seperti email, PIN internet banking, sampai media sosial. Ganti *password* dengan kombinasi yang sulit ditebak menggunakan karakter spesial seperti simbol, huruf kapital, tanda seru, dan yang lainnya.

Saat menggunakan internet memang sudah seharusnya Kita meningkatkan kewaspadaan terhadap situs atau tautan yang mencurigakan. Jangan malas atau ragu untuk melakukan riset di dunia maya tentang situs-situs yang akan dituju.

Etiket Menghindari Phising

1. Memeriksa akun secara rutin

2. Buat bookmark untuk halaman login
3. Jangan mengklik apapun di pesan SMS
4. Jangan mengklik tautan di pesan email yang mencurigakan
5. Pastikan ejaan URL website tersebut resmi dan memiliki SSL (HTTPS)
6. Ubah password secara berkala
7. Waspada setiap menerima pesan dari orang yang tidak dikenal
8. Install software untuk keamanan internet dan tetap update antivirus.
9. Waspada terhadap email atau pesan teks mendapat hadiah

Etiket Menjaga Bisnis Kita dari Serangan Phishing

Sebuah perusahaan dapat melakukan yang terbaik untuk menjaga kelangsungan bisnis mereka dari serangan *phishing*. Salah satunya menciptakan kesadaran para karyawan terhadap bahaya serangan *phishing*, dan juga memprioritaskan keamanan dalam kebebasan penggunaan internet. Sebagai tindakan awal membantu bisnis Kita terlindungi dari serangan *phishing*, Kita dapat melakukan pengecekan umum yang mudah untuk dilakukan, seperti mengevaluasi kembali setiap email yang Kita terima.

1. Evaluasi kembali setiap informasi yang Kita terima

Sangat penting untuk Kita mengevaluasi terlebih dahulu email yang Kita terima. Karena *hacker* banyak menjadikan email sebagai objek dalam menjalankan aksinya. Kita dapat memerhatikan penggunaan tata bahasa setiap email yang masuk. Peggunaan tata bahasa yang buruk adalah salah satu ciri dari serangan *phishing*. Selain itu, lakukan pengecekan kembali *link* yang tertera dalam email untuk memastikan *link* tersebut adalah link resmi.

Kita juga perlu memerhatikan setiap permintaan informasi yang berkaitan dengan kepentingan perusahaan, misalnya informasi finansial. Permintaan informasi sensitif tidak akan dilakukan dengan proses yang mudah, terlebih jika itu berkaitan dengan bisnis Kita.

2. Menggunakan solusi isolation untuk mencegah ancaman Phishing

Tahukah Kita jika *phishing* telah menjadi senjata utama para *cybercryminals* untuk menjalankan aksinya? Meskipun beroperasi dengan solusi keamanan email dan saluran media lain seperti *anti-spam*, *anti-virus*, *data security*, dan *encryption*, sebuah perusahaan akan terus menjadi target *phishing* untuk mengambil data kredensial dan eksploitasi *malware*. Oleh karena itu, sebuah perusahaan memerlukan solusi yang lebih terjamin selain solusi yang telah disebutkan, untuk mencegah ancaman *phishing*.

Menlo Security dengan solusi isolation yang akan membantu perusahaan bukan hanya untuk mengurangi, namun menghilangkan resiko serangan *phishing*. Solusi Phishing Isolation dari Menlo Security menghilangkan resiko pencurian kredensial dan eksploitasi *drive-by* yang terjadi melalui serangan email. Solusi ini mengintegrasikan Phishing Isolation berbasis cloud dengan server mail yang sudah ada seperti Exchange, Gmail, dan Office 365. Semua *link* email dapat ditransformasikan agar dapat dijaga oleh Phishing Isolation dari Menlo. Ketika pengguna mengklik *link* yang ada di email, *link* tersebut akan 100% terisolasi dari segala ancaman malware, termasuk ransomware. Situs web juga dapat dirender dalam mode *read-only*, yang dapat mencegah Kita menginput informasi sensitif ke dalam *form web* yang berbahaya.

Dengan kegiatan pengguna yang terisolasi secara aman, administrator dapat memantau statistik perilaku, dan memberikan peringatan yang melatih kesadaran *anti-phishing*. Administrator juga dapat menetapkan kebijakan *workflow* untuk tim atau individu. Dengan tidak adanya ketergantungan pada metode deteksi ancaman seperti *data analytics*, Menlo Security Phishing Isolation menjadi satu-satunya solusi keamanan yang melindungi setiap pengguna dari serangan *phising* pada saat menggunakan email.

Kesimpulan

Saat ini banyak sekali kasus kejahatan phising yang bisa ditemukan, apalagi sekarang jaman sudah berubah sedikit demi sedikit masyarakat menjadi lebih modern dan mempunyai akses digital sehingga potensi cybercrime semakin tinggi. Oleh karena itu kita harus berhati – hati saat menggunakan internet, mengakses website, membuka email dan lain-lain. Berikut Etiket mengantisipasi terjadinya hal *Phising* :

1. Untuk situs social media seperti *Facebook* dan *Instagram*, buatlah *bookmark* untuk halaman *login* atau mengetik URL facebook.com secara langsung di *browser address bar.*
2. Jangan mengklik *link* pada pesan *e-mail* yang terlihat mencurigakan.
3. Hanya mengetik data rahasia pada *website* yang aman.
4. Mengecek akun *bank* kita secara regular dan melaporkan apapun yang mencurigakan kepada *bank*
5. Kenali tanda GiveAway yang ada dalam e-mail phising:
    - Jika hal itu tidak ditujukan secara personal kepada kita.
    - Jika kita bukan satu-satunya penerima e-mail.
    - Jika terdapat kesalahan ejaan, tata bahasa atau sintaks yang buruk kekakuan kata lainnya dalam penggunaan bahasa. Biasanya ini dilakukan penyebar phising untuk mencegah filtering.
6. Menginstall software untuk keamanan internet dan tetap meng-update antivirus.
7. Menginstall patch
8. Waspada terhadap e-mail dan pesan instan yang tidak diminta.
9. Berhati-hati ketika login yang meminta hak Administrator. Cermati alamat URL-nya yang ada di addess bar.
10. Backup data kita

Daftar Referensi:

1. https://www.tirto.id/waspada-pencurian-data-lewat-phising-cnbt
2. https://www.tekno.kompas.com/read/2009/05/27/17001058/10.tips.mencegah.serangan.phising
3. https://www.idcloudhost.com/mengenal-apa-itu-phising-penyebab-dan-mengatasinya/
4. https://www.infokomputer.grid.id/read/121706181/apa-itu-phising-dan-bagaimana-Etiket-ampuh-untuk-menghindarinya?page=all
5. https://www.jojonomic.com/blog/phising/#:~:text=Phising%20adalah%20suatu%20metode%20untuk,akun%20korban%20untuk%20maksud%20tertentu.
6. https://www.blogs.masterweb.com/apa-itu-phising/

MALWARE

Pendahuluan,

Pada zaman sekarang Kejahatan di dunia maya semakin meningkat . itu semua di sebabkan oleh banyaknya kemajuan teknologi yang ada pada saat ini. Kemajuan teknologi yang terjadi saat ini tidak hanya berdampak positf terhadap kehidupan. Ada beberapa oknum yang memanfaatkan kemajuan teknologi untuk tindak kriminal guna mendapatkan keuntungan pribadi.

Berbagai macam alasan tindakan melaggar hukum tersebut dilakukan untuk kepuasan pribadi bahkan untuk mengambil keuntungan dari sebuah sistem yang di rusak nya. Ada banyak cara yang dapat digunakan untuk melakukan tindak kejahtan ini dengan melibatkan teknologi komputer salah satunya adalah dengan memanfaatkan kelemahan sistem jaringan computer dengan cara menyusupkan program yang di gunakan untuk mencari informasi dalam sistem computer tersebut yang d kenal dengan istilah malware.

Malware sendiri dapat di artikan sebagai semua perangkat lunak jahat, program computer jahat, atau perangkat lunak jahat, seperti virus (computer), Trojans, spyware, dan worm. Virus computer berkerja dengan cara menepel pada satu file computer yang biasanya berupa file executable. Trojan bekerja dengan cara melakukan social engineering files berbahaya dengan menampilkannya seperti files yang terlihat tidak berbahaya, spyware adalah perangkat lunak yang disisipi kode untuk mendapatkan informasi penting dari pengguna seperti akun bank, password, dan informasi lainnya yang diinginkan oleh pembuatnya, sedangkan worm adalah perangkat lunak jahat yang dibuat dengan memanfaatkan celah lubang keamanan pada sistem operasi untuk tujuan tertentu.

Pada paper ini penulis akan membahas lebih dalam mengenai perlindungan dari insiden serangan malware dari segi etika.

Literature Review,

Pengertian malware

Malware adalah singkatan dari malicious software. Malware sendiri adalah sebuah software yang dirancang dengan tujuan untuk membahayakan, menyusup, atau merusak sebuah komputer. Malware juga biasa didefinisikan sebagai kode berbahaya. Software ini bisa melumpuhkan atau mengganggu operasi sebuah sistem, memungkinkan hacker untuk mendapat akses ke informasi rahasia dan sensitif serta memata-matai komputer serta pemilik komputer itu sendiri.

Malware dibuat secara khusus agar tersembunyi sehingga mereka bisa tetap berada di dalam sebuah sistem untuk periode waktu tertentu tanpa sepengetahuan pemilik sistem tersebut. Biasanya, mereka menyamarkan diri menjadi program yang bersih.

Efek dari malicious software biasa jauh lebih berbahaya bagi corporates dibanding untuk personal user. Jika malware menyerang jaringan sistem Anda, mereka bisa menyebabkan kerusakan dan gangguan yang meluas, yang memerlukan upaya pemulihan ekstensif di dalam organisasi.

Malware dapat menginfeksi komputer dengan masuk melalui email, hasil download internet, dan program-program yang sudah terinfeksi.

Kebanyakan kejahatan komputer yang sering terjadi adalah pencurian informasi personal atau pembentukan sebuah backdoor ke komputer Anda dimana seseorang bisa mendapatkan akses ke komputer Anda tanpa sepengetahuan dan izin Anda. Software yang membantu orang-orang untuk melakukan hal-hal ini tanpa seizin Anda bisa dianggap sebagai malware.

Malware juga memiliki beberapa nama lain seperti badware dan di dokumen legal, malware lebih sering disebut sebagai computer contamination (kontaminasi sistem komputer). Sehingga apabila Anda melihat kata itu, itu hanyalah cara lain untuk menyebut malware.

Berikut ini berbagai jenis Malware yang dinilai paling dominan menginfeksi komputer [5]

(1). Virus
Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah Malware pertama yang dikenalkan sebagai program yang memiliki kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah Malware sendiri. Biasanya virus berbentuk file eksekusi (executable) yang baru akan beraktivitas bila user mengaktifkannya. Setelah diaktifkan virus akan menyerang file yang juga bertipe executable (.exe) atau juga tipe file lainnya sesuai dengan perintah yang dituliskan pembuatnya.

(2). Worm
Worm yang berarti cacing merupakan Malware yang cukup berbahaya. Worm mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, Worm memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di dalam sistem komputer. Hal yang diakibatkan dari aktivitas Worm adalah merusak data dan memenuhi memory dengan Worm lainnya hasil dari penggandaan

diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan
komputer menjadi hang dapat menjadi gejala awal terdapatnya Worm pada komputer tersebut. Contoh Worm yang populer akhir-akhir ini adalah Conficker.

(3). Trojan Horse
Teknik Malware ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke Hollywood adalah menumpangi file biasa yang bila sudah dieksekusi
dalam film berjudul 'Troy'. Modus dari Trojan Horse inadalah menumpangi file biasa yang bila sudah dieksekusi
akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama file yang ditumpanginya. rojan Horse merupakan Malware berbahaya, lebih dari sekedar keberadaannya tidak diketahui oleh pengguna komputer. Trojan dapat melakukan aktivitas tak terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan file, mencuri data, melihat aktivitas user (spyware), mengetahui apa saja yang diketikkan oleh user termasuk password (keylogger) bahkan menguasai sepenuhnya komputer yang telah terinfeksi Trojan Horse.

(4). Spyware
Spyware merupakan Malware yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan Spyware jelas sangat merugikan user karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya. Aktivitas Spyware terasa sangat berbahaya karena rentan terhadap pencurian password. Dari kegiatan ini juga akhirnya lahir istilah Adware yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. Spam yang muncul secara tak terduga di komputer juga merupakan salah satu dampak aktivitas Spyware yang dirasa sangat menjengkelkan.

(5). Backdoor
Kerja dari Backdoor sangat berkaitan dengan aktivitas hacking. Backdoor merupakan metode yang digunakan untuk melewati autentifikasi normal (login) dan berusaha tidak terdeteksi. Backdoor sendiri sering kali disusupkan bersama dengan Trojan dan Worm. Dapat diartikan secara singkat Backdoor berarti masuk ke sistem komputer melalui jalur pintu belakang secara tidak sah. Dengan metode Backdoor maka akan sangat mudah untuk mengambil alih kendali dari komputer yang telah berhasil disusupi. Setelah berhasil masuk maka aktivitas yang dilakukan oleh Backdoor antara lain adalah mengacaukan lalu lintas jaringan,melakukan brute force attack untuk mengcrack password dan enkripsi dan mendistribusikan serangan Distributed Denial of Service (DDoS).

Pembahasan,

Sederhananya, malware adalah software apa saja yang melakukan tugas tak diinginkan pada komputer Anda. Menyebalkan bukan? Nah, inilah tugas anti-malware. Anti-malware dapat mencegah tindakan berbahaya dari malware yang merepotkan tersebut.

Sementara itu, virus adalah jenis malware tertentu yang menggandakan sesuatu dan menginfeksi program apapun di komputer Anda. Secara teknis, virus adalah jenis malware yang pada saat dijalankan, menggandakan dirinya sendiri dan mereproduksi source code dirinya sendiri serta menginfeksi program komputer lain yang ada dengan cara memodifikasi cara kerja program tersebut. Lalu apa itu anti-virus?

Istilah antivirus muncul dari banyaknya keberadaan malware yang berupa virus. Jadi malware ini muncul dengan berbagai bentuk, maka istilah anti-malware jadi banyak digunakan untuk penanganan virus dari malware ini.

Malware tersebut dapat dikatakan jahat karena dapat menganggu kinerja komputer Anda, hinggga berpotensi mengancam eksistensi file-file yang ada pada komputer Anda. Hal itu mungkin saja terjadi mengingat malware ini dapat melakukan modifikasi terhadap keseluruhan isi dari RAM yang ada di komputer Anda. Ada banyak sekali jenis-jenis malware seperti yang telah kami sebutkan di penjelasan sebelumnya. Baik itu worms, trojans, crypto lockers, dan lain-lain. Semua jenis malware tersebut beraksi sesuai dengan tugas berbeda-beda sesuai dengan tujuan mereka untuk menganggu dan meneror end-users.

Sebenarnya antivirus ini sering dipakai secara bergantian dengan anti-malware. Namun, software dari antivirus secara historis ternyata hanya menargetkan penanganannya pada sub dari kumpulan malware tertentu saja, semacam worm atau trojan versi terdahulu.

Antivirus menjadi istilah populer yang digunakan pada semua software anti-malware di tahun 90-an. Jadi, pada era awal internet digunakan oleh orang-orang, kebijakan keamanan internet tidak dikenal secara luas oleh kebanyakan pengguna baru internet. Sementara itu, malware terus meningkat kuantitas dan kualitasnya. Virus ini terus-menerus berkembang pesat karena sifatnya yang dapat menduplikasi host file dan menginfeksi perangkat apapun tanpa pandang bulu.

Karena perkembangan yang sangat pesat itu pula, ada banyak sekali para pengguna internet yang komputernya terinfeksi virus. Maka menjadi masuk akal, bila muncul banyak pula antimalwar yang dikembangkan dan dijual ke pasar. Namun anti-malware pada saat itu lebih awam disebut sebagai antivirus. Hal itu menyebabkan suatu masalah, sebab jika para pengelola berfokus pada antivirus software saja, mereka jadi mengabaikan jenis-jenis malware lain yang potensial.

Inilah awal mula muncul malware-malware lain yang berbahaya semacam ransomware dan spyware yang menyebar luas. Pengembang antivirus dan anti-malware kemudian melakukan modifikasi terhadap software mereka untuk memasukkan alat pendeteksi baru, sehingga nantinya keduanya baik antivirus maupun anti-malware berkembang ke arah satu jenis perangkat saja yaitu anti-malware. Namun masih banyak kita temukan software-software antivirus yang sebenarnya hanya menangani virus-virus lama ("tua") dan jika Anda hanya mengandalkan ini dampaknya komputer Anda beresiko.

Jadi apa itu anti-malware? Anti-malware adalah jenis software yang di-install langsung pada komputer untuk mendeteksi dan menghapus malware dari sistem yang ada secara aktif.

Setiap saat, data atau file yang ditambahkan ke sistem pada komputer Anda akan dipindai atau di-scan oleh anti-malware yang ada. Kemudian akan dilakukan identifikasi apakah malware yang ada dari file baru tersebut dikenali atau "ramah" terhadap perangkat Anda atau tergolong malware berbahaya.

Bagaimana cara anti-malware tersebut melakukan identifikasi? Dengan tetap terhubung ke internet, kebanyakan program anti-malware ini dapat menyimpan daftar malware yang terus diperbaharui sehingga ia mampu mengidentifikasinya.

Selain itu, anti-malware dapat difungsikan sesuai jadwal untuk melakukan pemindaian berkala. Penjadwalan ini dilakukan untuk mengetahui apakah ada bagian-bagian perangkat Anda yang rusak atau terinfeksi.

Jika anti-malware gagal dalam memutuskan apakah suatu file berbahaya atau tidak, maka software ini akan memasukkannya pada sandbox. Sandbox ini semacam suatu lingkungan yang benar-benar terpisah dari host operating system. Hal ini dilakukan agar program yang ada tak membahayakan host system dan anti-malware dapat menganalisa efek dari file-nya.

Cara Mengatasi Malware

Berikut kami akan memberikan cara penanganan yang dapat Anda lakukan pada jenis-jenis malware yang spesifik, diurutkan sesuai penjelasan kami sebelumnya soal jenis-jenis malware:

- Virus

Setiap sistem yang terhubung dengan internet harus melakukan instalasi software anti-malware dan aktifkan fungsi Firewall-nya. Lalu, lakukan scan secara menyeluruh pada sistem Anda. Jika yang terinfeksi adalah USB atau Flash drive anda, dan anda membutuhkan data-data di

dalamnya, buka USB tersebut di PC dengan sistem informasi Linux/Mac. Selamatkan data-data yang diperlukan, dan format ulang USB anda.

- Worm

Seperti virus, cara terbaik untuk mencegah infeksi dari worm ini adalah dengan menggunakan software antivirus atau anti-malware. Dan seperti biasa, Anda sebagai pengguna internet sebaiknya hanya mengklik link email atau lampiran saat Anda benar-benar yakin apa isinya.

- Trojans

Karena Trojans menggabungkan social trick, sangat penting untuk mendidik pengguna internet atau klien website Anda tentang ancaman tersebut. Pengguna juga harus berhati-hati saat menginstal software baru di sistem mereka atau saat mengklik link maupun membuka attachment email. Selain itu, organisasi dapat mencegah banyak Trojans dengan security software yang memadai, seperti software anti-malware juga firewall.

- Backdoor

Backdoors adalah salah satu jenis ancaman yang paling sulit untuk diatasi. Para ahli di bidangnya mengatakan pertahanan terbaik adalah strategi keamanan multi-cabang yang mencakup software firewall, anti-malware, pemantauan jaringan, pencegahan sekaligus deteksi intrusi, dan perlindungan data

- Spyware

Spyware adalah masalah besar bagi pengguna yang tidak ingin data penting menyebar. Alasan ini cukup untuk membuat penggunanya mengetahui cara mengatasi spyware. Tidak sulit untuk mengatasinya, simak saja ulasan berikut:

1. Pasang anti virus

Langkah terbaik untuk mengatasi spyware adalah memasang anti virus terpercaya supaya terhindar dari spyware. Dengan adanya antivirus tersebut, komputer atau perangkat yang digunakan bisa terhindar dari serangan spyware.

2. Update anti virus

Bagi yang menggunakan antivirus, setidaknya lakukan update pada anti virus tersebut secara berkala. Ya, jika menggunakan antivirus namun jarang update maka hal tersebut tidak akan

berpengaruh pada kinerjanya. Pasalnya, antivirus tidak bisa mengidentifikasi dan mencegah spyware yang masuk ke perangkat.

3. Disable penyimpanan cookie

Selain menggunakan super anti spyware untuk mengatasi spyware Anda harus mendisable penyimpanan cookie juga. Disable adalah mematikan penyimpanan cookie yang biasanya merupakan tempat dimana spyware tersebut muncul. Caranya mudah, tinggal tekan kombinasi tombol Ctrl + Shift + Delete dan kemudian pilih Clear Data.

Dari segi etika tentunya malware merupakan tindakan yang tidak di benarkan . ini semua tidak sesuai dengan etika profesi seorang ahli IT di mana menggunakan kemampuan nya dalam bidang IT untuk melakukan tindakan yang tidak sesuai dengan aturan hukum. Tindakan pemasangan malware ini tentunya akan merugikamn pihak tertentu yang dapat menyebabkan kerusakan sistem atau pun file yang nantinya akan menghambat proses kerja orang atau perusahaan yang terserang malware ini.

Kesimpulan,

Dari paparan yang telah di jelaskan di atas malware merupakan suatu tindakdan kriminal yang melanggar hukum dan etika seorang profesi IT dimana malware dapat merusak sistem atau pun file – file yang pada sistem yang di serang oleh malware.

Untuk menghindari malware ada beberapa cara yang dapat di lakukan tergantung jenis malware itu sendiri seperti pengunaan anti virus dan edukasi pengguna internet untuk tidak malukakan beberapa hal yang dapat menyebabkan malware menyerang sistem.

Daftar Referensi.

Gandotra, B., & Sanjeev, D. Analisis dan klasifikasi mallware. Jurnal internasional. 2014.

devi rizky Septiani, dkk. Investigasi serangan malware njrat PC. Jurnal edukasi dan pendidikan informatika (JEPIN). 2016

https://www.dewaweb.com/blog/pengertian-malware-pentingnya-dewaguard/

https://qwords.com/blog/spyware-adalah/

NAMA	:	LILY PEBRIANA
NIM	:	182420114
KELAS	:	MTI 20.A
MATA KULIAH	:	ETICHAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS
DOSEN PENGAMPUH	:	M. IZMAN HERDIANSYAH, M.M., Ph.D
PROGRAM STUDI	:	PASCASARJANA TEKNIK KOMPUTER

TUGAS INDIVIDU

SQL INJECTION

SQL INJECTION

Abstrak – *paper ini membahas mengenai bagaimana cara mengenai seperti apa itu SQL Injection, bahayanya SQL Injenction, sebab-sebab yang menyebabkan terjadinya SQL Injection, penanganan dan pencegahannya.*

1. PENDAHULUAN

SQL Injection atau Injeksi SQL memiliki makna dan arti yaitu : sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan ke dalam bahasa yang lain. (Wikipedia)

SQL Injection adalah jenis aksi hacking pada keamanan computer dimana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. SQL Injection yaitu serangan yang mirip dengan serangan XSS dalam bahwa penyerang memanfaatkan aplikasi vektordan juga dengan Common dalam serangan XSS.

2. TUJUAN

Adapun beberapa tujuan dalam pembuatan paper ini, yaitu :

1. Mengetahui pengetahuan mengenai SQL Injection.
2. Mengetahui bagaimana cara mencegah dan menangani SQL Injection.

3. DASAR TEORI

3.1. SQL Injection

SQL Injection adalah jenis aksi hacking pada keamanan computer dimana seorang penyerang bisa mendapatkan akses ke basis data di dalam sistem. SQL injection exploits adalah hasil interfacing sebuah bahasa lewat informasi melalui bahasa lain. Dalam hal SQL Injection, sebuah bahasa pemrograman seperti PHP atau Perl mengakses database melalui SQL query. Jika data yang diterima dari pengguna akhir yang dikirim langsung ke data base dan tidak disaring dengan benar, maka yang penyerang dapat menyisipkan perintah SQL nya sebagai bagian dari input.

Setalah dijalankan pada data base, perintah ini dapat mengubah, menghapus atau membeberkan data sensitive. Lebih parah lagi jika sampai ke sistem eksekusi kode akses yaitu mematikan database itu sendiri, sehingga tidak bisa memberikan layanan kepada web server.

4. HASIL DAN PEMBAHASAN

4.1. Pentingnya Keamanan sebuah Password

Ada beberapa yang menyebabkan terjadinya SQL Injection, yaitu :

- ✓ Tidak adanya penanganan terhadap karakter – karakter tanda petik satu ‘ dan juga karakter double minus – yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL.
- ✓ Penggunaan pesan error yang masih bersifat default – mudah untuk melacak query yang digunakan.

4.2. Bahaya SQL Injection

Ada beberapa bahaya yang ditimbulkan oleh SQL Injection, yaitu :

- ✓ Memungkinkan seseorang dapat login ke dalam sistem tanpa harus memiliki account.
- ✓ Memungkinkan seseorang mengubah, menghapus maupun menambahkan data-data yang berada di dalam database.
- ✓ Dapat mematikan data base dari suatu aplikasi, sehingga tidak bisa memberi layanan kepada web server.

4.3. Penyebab Terjadinya SQL Injection

Penyebab terjadinya SQL Injection, yaitu :

- ✓ Tidak adanya penanganan terhadap karakter-karakter tanda petik satu ‘ dan juga karakter double minus – yang menyebabkan suatu aplikasi dapat disisipi dengan perintah SQL.
- ✓ Sehingga seorang Hacker menyisipkan perintah SQL ke dalam suatu parameter maupun suatu form.

4.4. Penanganan SQL Injection

Ada beberapa cara untuk menangani SQL Injection, yaitu :

1. Menggunakan sintaks string ‘ OR ‘’ = ‘’

   $SQL = “select * from login where username = ‘$username’ and password = ‘$password’”;(dari GET atau POST variabel)

   Jika dimasukkan ‘ OR ‘’=’’,maka eksekusi SQL-nya menjadi :

   ‘’select *from login where username = ‘$username’ and password=;pas’ or ‘=’”;’ (dengan SQL ini hasil selection akan selalu TRUE true sehingga user dapat login ke dalam suatu sistem).

2. Menggunakan sintaks string ‘_ pada username

Contoh :

“ SELECT * FROM members WHERE username = ‘saya’ _’ AND password = ‘ayas’”;

Berubah menjadi :

“ SELECT * FROM members WHERE username = ‘saya’ _’ AND password = ‘xxxx’ “ ; password tidak akan dieksekusi karena dianggap sebagi komentar.

3. $SQL = “select * from login where username = ‘$username’ and password = ‘$password’”; , {dari GET atau POST variabel}

4. Isikan password dengan string ’ or “ = ’ Hasilnya maka SQL akan seperti ini =”select * from login where username = ’$username’ and password=’pass’ or ‘=”’;, {dengan SQL ini hasil selection akan selalu TRUE}

Maka kita bisa inject sintax SQL (dalam hal ini OR) kedalam SQL.

4.5. Cara Pencegahan SQL Injection

Untuk mencegah terjadinya SQL Injection adapun beberapa pencegahan yang dapat dilakukan adalah :

- ✓ Membatasi panjang input box (jika memungkinkan), dengan cara membatasinya di kode program, jadi si cracker pemula akan bingung sejenak melihat input box nya tidak bisa diinject dengan perintah yang panjang.
- ✓ Memfilter input yang dimasukan oleh user, terutama penggunaan tanda kutip tunggal (input validation).
- ✓ Mematikan atau menyembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan.
- ✓ Mematikan fasilitas-fasilitas standar seperti Stored Procedures, Extended Stored Procedures jika memungkinkan.
- ✓ Mrngubah “Startup and run SQL Server” menggunakan low privilege user di SQL Server Sequrity tab.

5. KESIMPULAN

SQL Injection terjadi karena kesalahan dari programmer yang tidak mengetahui cara membuat website yang aman. Agar terhindar dari SQL Injection programmer harus memperhatikan logika atau codingan dalam aplikasi yang dibuat, buatlah variasi-variasi codingan yaitu dengan menggunakan beberapa batasan-batasan pada codingan, seperti batasi panjang input box (jika memungkinkan), dengan cara membatasinya dikode

program, sehingga itu nantinya tidak dapat memungkinkan dan seseorang akan sedikit kesulitan dalam menembus dan berniat tidak baik terhadap website atau aplikasi yang telah dibuat.

DAFTAR REFERENSI :

1. Budi Raharjo, "Keamanan Sistem Informasi Berbasis Internet", PT. Insan Indonesia & PT. INDOCISC, Jakarta,2002.
2. http://dekill.blogspot.com/2009/04/seki as-sql-injection.html.
3. SQLinjection, (www.BlackAngels.it).

SQL Injection

Muhammad Angga Oktaharisetia
Universitas Bina Darma Palembang
muhanggaohs@gmail.com

ABSTRAK- Keamanan merupakan faktor penting dalam membantu pembangunan website. Banyaknya layanan bisnis berupa toko online berbasis web dan sebagainya menjadikan keamanan sebagai faktor terpenting untuk dijaga dengan baik. Aplikasi yang bersifat terbuka dan dapat diakses dengan mudah oleh siapa saja dapat membuat keamanan terancam. Salah santu ancaman serangan tersebut yaitu SQL injection yang merupakan serangan hacker untuk website untuk memasuki dan mendapatkan akses ke basis data. Metode yang digunakan SQL injection biasnya menggunakan form yang terdapat di dalam website yang tidak dilindungi dengan script khusus.
Kata kunci : SQL Injeksi, Web

PENDAHULUAN

Salah satu gangguan atau bentuk kejahatan di internet adalah dalambentuk mengganggu sistem jaringan dan database. Salah satu teknik dalammengganggu sistem database jaringan adalah dengan menggunakan SQL injection.SQL injection atau dikenal juga dengan SQL insertion yaitu sebuah teknik yangdigunakan untuk mengeksploitasi database pada suatu websites dengan memaksakeluarnya error page situs itu yang ada error pages itu terdapat info tentangs truktur database website yang dieksploitasi.
Serangan *SQL Injection* merupakan jenis eksploitasi keamanan halaman web, dimana penyerangan menyisipkan kode-kode SQL melalui formulir/*form* kemudian memanipulasi URL berdasarkan pada parameter sql. Serangan *SQL Injection* adalah serangan yang berupa menginjeksi perintah SQL malaui *form input data*, yang kemudian di teruskan menuju *database* untuk dieksekusi, dengan tujuan mengakses data sensitive seperti *database*.

Teknik SQL Injection memungkinkan seseorang dapat login kedalam sistem dabase tanpa harus memiliki account dengan cara mengisi default setting SQL. Default setting SQL yang paling berbahaya (kosong / tidak diisi). Jika default settingnya belum dirubah maka ketika ada sebuah direktori pada website yang memiliki form untuk login admin, para hacker dapat masuk kedalam dengan hanya (kosong / tidak diisi). Bentuk lain untuk masuk kedalam adalah dengan menggunakan string ' OR 1-1- - pada halaman yang memilikii user dan password. Jika kita memasukan string ' OR 1=1-- di input box user dan memasukan password = foobar di input box password, sehingga menagkibatkan SQL Query menjadi bingung. SQL Query akan membacanya sebagai: SELECT * from users where User ='' or 1=1-- and Password='foobar' yang memiliki arti bahwa sql akan men-SELET semua - - (tanda adalah mark dari SQL).

Literatur Review

Tinjauan Pustaka Pada penelitian ini digunakan empat buah tinjauan pustaka, yang pertama ditulis oleh Feri Setiyawan. Web server pada penelitian ini menggunakan nginx yang dilengkapi dengan naxsi sebagai web application firewall. Pembahasan mengenai perbandingan antara sebelum dan sesudah implementasi naxsi terhadap serangan SQL injection (Feri Setiyawan, 2014). Pustaka kedua ditulis oleh Albi Alamsyah mengenai pengujian keamanan setelah implementasi ModSecurity terhadap empat jenis serangan yaitu SQL Injection, Cross Site Scripting (XSS), Local File Inclusion (LFI) dan Remote File Inclusion (RFI) (Albi Alamsyah, 2016). Pustaka ketiga

ditulis oleh Gilang Ramadhan, web server yang digunakan adalah nginx yang dilengkapi dengan naxsi dan apache yang dilengkapi dengan modsecurity. Pembahasan mengenai studi kasus pada sebuah instansi yang membandingan instalasi nginx yang dilengkapi naxsi dengan apache yang dilengkapi dengan ModSecurity (Gilang Ramadhan, 2014).

Pustaka keempat ditulis oleh Aditya, web server yang digunakan adalah apache yang dilengkapi dengan ModSecurity. Pembahasan mengenai pembacaan log oleh aplikasi jwall auditconsole untuk dijadikan alat pelapor adanya insiden (Aditya Noor Sandy, 2014).

Detail dari tinjauan pustaka disajikan dalam bentuk tabel yang terlihat pada tabel 2.1 Tabel Perbandingan

Tabel 2 1 Tabel Perbandingan

Parameter / Penulis	Objek	Metode/Alat	Bahasa Pemrograman	Interface
Feri Setiyawan (UIN SUKA) tahun 2014	Pencegah *SQL Injection*	Naxsi, Nginx	PHP (Joomla)	-
Albi Alamsyah (Universitas Muhammadiyah Jember) tahun 2016	Pengujian keamanan terhadap *SQL Injection, Cross Site Scripting (XSS), Local File Inclusion (LFI) dan Remote File Inclusion (RFI)*	ModSecurity, Apache	PHP (DVWA)	-
Gilang Ramadhan (Unikom) tahun 2014	Perbandingan keamanan dua jenis *Web Application Firewall (WAF)*	Naxsi, Nginx, ModSecurity, Apache	PHP (website XecureIT)	-
Aditya Noor Sandy (UPN Veteran Jawa Timur) tahun 2014	Pelaporan dugaan tindakan intrusi pada website	ModSecurity, Apache	PHP	Jwall Auditconsole
Usulan	Pengembangan filter *ModSecurity* untuk *File Upload, PHP Code Injection* dan *PHP Object Injection*	ModSecurity, Apache	PHP (Wordpress dan Joomla)	-

METODELOGI PENELITIAN

Metode Penelitian yang dilakukan dalan penulisan makalah ini adalah bersifat literature. SQL Injection merupakan kegiatan yang dilakukan untuk perintah SQL ditujukan statment SQL yang ada pada aplikasi yang sedang berjalan. Adapun teknik untuk mengeksploitassikan web ini di dalam SQL injection yang memiliki database sebagai tempat penyimpanan data. SQL Injection terjadi karena kurangnya keamanan pada website tersebut untuk menghandle suatu inputan pada form login yang umumnya terletak pada username dan password

Pembahasan

Beberapa jenis serangan yang digunakan pada penelitian ini diuraikan seperti berikut.

1. File Upload File yang diunggah mewakili risiko yang signifikan terhadap aplikasi. Langkah pertama serangan pada umumnya adalah mendapatkan beberapa kode pada sistem yang akan diserang. Kemudian serangan hanya perlu mencari jalan untuk mendapatkan kode yang dieksekusi. Menggunakan upload file membantu penyerang menyelesaikan langkah pertama. Konsekuensi dari upload file yang tidak terbatas dapat bervariasi, termasuk pengambilalihan sistem yang lengkap, sistem berkas atau database yang kelebihan beban, serangan penerusan ke sistem back-end, serangan sisi klien, atau penghindaran sederhana. Itu tergantung pada apa aplikasi yang dilakukan dengan file upload dan terutama di tempat penyimpanannya.
2. Code Injection
   Code Injection adalah istilah umum untuk jenis serangan dengan mengirim kode program kemudian dieksekusi oleh aplikasi. Jenis serangan ini memanfaatkan penanganan data yang tidak sempurna. Jenis serangan ini biasanya dimungkinkan karena kurangnya validasi data input / output yang tepat, misalnya: karakter yang diizinkan, format data dan jumlah data yang diharapkan. Code Injection berbeda dengan Command Injection karena penyerang hanya dibatasi oleh fungsi bahasa pemrograman yang digunakan.
3. PHP Object Injection PHP Object Injection adalah tingkat kerentanan aplikasi yang memungkinkan penyerang melakukan berbagai jenis serangan berbahaya, seperti Code Injection, SQL Injection, Path Traversal dan Denial of Service, tergantung pada konteksnya. Kerentanan terjadi ketika masukan yang diberikan pengguna tidak disterilkan dengan baik sebelum dikirim ke fungsi PHP unserialize(). Karena PHP memungkinkan serialisasi objek, penyerang bisa melewati string serial ke panggilan unserialize() yang rentan, sehingga menghasilkan sembarang objek PHP ke dalam lingkup aplikasi

Dari uraian tiga buah ancaman pada aplikasi web di atas, terdapat perbedaan metode yang dilakukan oleh penyerang dalam memanfaatkannya. Berikut ini merupakan tabel beberapa metode penyerangan yang biasa digunakan pada masing – masing jenis kelemahan.

Tabel 2 2 Metode Penyerangan

Kelemahan	Metode
File Upload	Pengiriman file php secara langsung
	Pengiriman file php dengan ekstensi ganda
PHP Code Injection	Manipulasi parameter untuk bypass seleksi
	Penyisipan kode ke dalam database
PHP Object Injection	Pengiriman serialisasi objek secara langsung
	Pengiriman serialisasi objek dengan enkripsi

Beberapa aplikasi website yang memiliki kelemahan seperti yang telah diuraikan dan akan diteliti ditampilkan dalam bentuk tabel berikut ini.

Tabel 2 3 Informasi Kelemahan

Nama	Kelemahan	Jenis Kelemahan
Wordpress Plugin Mac Photo Gallery 2.7	Tidak terdapat verifikasi terhadap file yang dikirimkan.	*File Upload*
Wordpress Plugin Asset Manager 0.2	Tidak terdapat verifikasi terhadap file yang dikirimkan.	
Wordpress Plugin AllWebMenus < 1.1.9	Fitur update dengan menggunakan file kompresi zip dapat dieksekusi oleh siapa saja.	
Wordpress Plugin LearnDash 2.5.3	Fitur upload melakukan pemotongan string ekstensi file yang bisa dimanfaatkan dengan ekstensi ganda.	
Wordpress Plugin Insert PHP < 3.3.1	Program gagal melakukan validasi terhadap hak pengguna terhadap id posting.	*PHP Code Injection*
Wordpress Plugin W3 Total Cache 0.9.2.3	Tag khusus dengan nama "mfunc" mempunyai fungsi spesial untuk penambahan kode php.	
Joomla Component com_civicrm 4.2.2	Pembuatan file dengan fungsi *fwrite* yang bisa dieksekusi siapa saja.	
Wordpress Plugin Ultimate Product Catalog <= 4.2.24	Fungsi *unserialize* langsung diberi parameter nilai cookie tanpa validasi.	*PHP Object Injection*
Joomla! 1.5 < 3.4.5 'x-forwarded-for'	Tidak terdapat verifikasi terhadap data browser yang dimasukkan ke	

1. Web Application Firewall

Web Application Firewall (WAF) adalah firewall untuk aplikasi HTTP. Menerapkan seperangkat aturan terhadap permintaan atau keluaran HTTP. Umumnya, aturan ini mencakup serangan umum seperti cross-site scripting (XSS) dan SQL injection. Sementara proxy umumnya melindungi klien, WAFs melindungi server. WAF digunakan untuk melindungi aplikasi web atau kumpulan aplikasi web tertentu. WAF bisa dianggap sebagai reverse proxy. WAF bisa berbentuk alat, plugin server, atau filter, dan mungkin disesuaikan dengan aplikasi. Upaya untuk melakukan kustomisasi dapat menjadi signifikan dan perlu dipertahankan menyesuaikan dengan perubahan yang dilakukan pada aplikasi.

2. ModSecurity

ModSecurity adalah open source, cross platform web application firewall (WAF) yang dikembangkan oleh Trustwave's SpiderLabs. ModSecurity memiliki bahasa pemrograman berbasis event yang kuat yang memberikan perlindungan dari berbagai serangan terhadap aplikasi web dan memungkinkan pemantauan lalu lintas HTTP, logging dan analisis secara real-time. Dengan lebih dari 10.000 penyebaran di seluruh dunia, ModSecurity adalah WAF yang paling banyak digunakan Skenario paling penting penggunaan ModSecurity adalah :

- ✓ **Real-time application security monitoring and access control**, ModSecurity memberi akses ke arus lalu lintas HTTP secara real-time, beserta kemampuan untuk memeriksanya. Dengan tambahan mekanisme penyimpanan permanen ModSecurity, dapat dilakukan pelacakan elemen sistem dari waktu ke waktu dan melakukan korelasi peristiwa. Karena ModSecurity menggunakan permintaan dan penyangga respons penuh, maka dapat dilakukan pemblokiran
- ✓ **Full HTTP traffic logging Web server**, secara tradisional menyimpan sangat sedikit log yang mengandung informasi untuk keamanan dan bahkan dengan melakukan konfigurasi khusus tidak bisa didapatkan semua informasi yang dibutuhkan. ModSecurity menyediakan kemampuan untuk mencatat apapun yang dibutuhkan, termasuk data transaksi mentah, yang penting untuk forensik. Selain itu, bisa dipilih transaksi yang akan disimpan, bagian mana dari transaksi yang masuk, dan komponen mana yang disterilkan.
- ✓ **Continuous passive security assessment,** Penilaian keamanan aktif sebagian besar merupakan kegiatan yang terjadwal, di mana tim independen bersumber untuk mencoba melakukan serangan simulasi. Penilaian keamanan pasif terus menerus adalah variasi pemantauan real-time, di mana berfokus pada perilaku pihak eksternal, dengan mengamati

perilaku sistem itu sendiri. Hal ini adalah sistem peringatan dini yang bisa mendeteksi jejak kelainan perilaku sistem dan kelemahan keamanan sebelum dieksploitasi

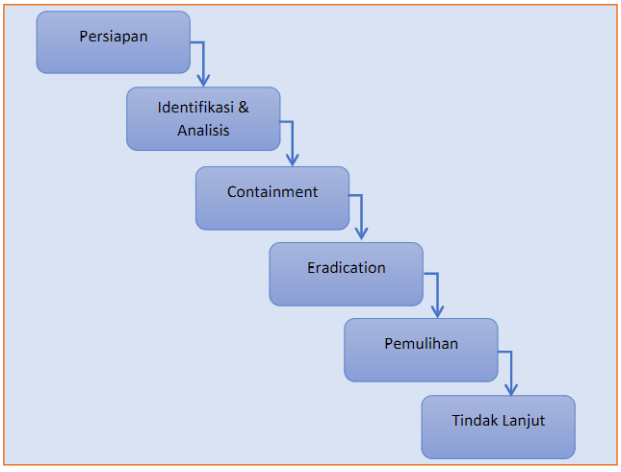
- ✓ **Web application hardening** Salah satu kegunaan ModSecurity adalah digunakan untuk mempersempit data HTTP yang diterima, misalnya metode, header, jenis konten dan lain – lain. Dengan ModSecurity mungkin juga dilakukan perbaikan masalah manajemen sesi, serta kerentanan pemalsuan data pada lalu lintas situs.

PROSEDUR PENANGANAN SERANGAN SQL INJECTION

Penanganan serangan SQL Injectionditujukan utuk mencapai hal-hal sebagai berikut:

a. Mengumpulkan informasi sebanyak mungkin tentangserangan SQL Injection;
b. Menghalangi atau mencegah eskalasi kerusakan yang disebabkan olehserangantersebut;
c. Mengumpulkan bukti terkait serangan SQL Injection;
d. Mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya serangan SQL Injectiondi masa depan.

Supaya tujuan diatas dapat terlaksana dengan baik, maka penanganan terhadap serangan SQL Injectiondilakukan dalam beberapa tahapsebagai berikut:



Gambar 1. Tahap Penanganan Serangan *SQL Injection*

Dalam melakukan penanganan serangan SQL Injection, perlu adanya tahap persiapan dengan prosedur sebagai berikut :

a) Pembentukan tim respon. Timdapat berasal dari institusi yang mengalami serangan(internal) atau juga bisaberasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang SQL Injectiondan memiliki kemampuan penanganannya;
b) Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan SQL Injection.Dokumen ini antara lain adalah :-Panduan penanganan insiden serangan siber;-Formulir penanganan insiden serangan siber;-Diagram yang menggambarkan hubungan antar komponen-komponen aplikasi yang membangun website (web server, aplikasi web, daftar user, diagram network).c)Menyiapkan tool dan media yang dibutuhkan untuk penanganan.MMisalnya Notepad ++ untuk membaca log, IDS/IPS, SQL Map, Accunetix /Nessus

Pada tahap identifikasi dan Analisis dilakukan proses identifikasi untuk memastikan telah terjadi serangan SQL Injectiondan mendeteksi sumbernya.Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain:

a. Memeriksaalertdan anomaliesdari perangkat IDS atau IPS;
b. Melakukan error checking melalui form atau url dengan memberikan karakter atau sebuah simbol. Misalnya:

•Melalui form login, memasukan pada username dan password berupa karakter-karakter yang digunakan SQL Injection, seperti:OR 1=1 – OR 1=2 --OR 'a'='a'

•Melalui url, menambahkan karakter-karakter yang digunakan SQL Injection, seperti single quote, double minus.

c. Memeriksa semua log (error log, access log, database log, firewall log).Lokasi log file secara default berada pada var/log, log tersebut menyimpan seluruh aktivitas yang terjadi pada sistem;
d. Memeriksa adanya command line, string-string yang digunakan untuk menyerang;
e. Memeriksa isi database untuk mencari script yang berbahaya, dan mengecek apakah ada penambahan user secara tidak sah;
f. Memeriksa apakah ada file atau script berbahaya (trojan, malicious file, backdoor) yang ditanamkan pada web server;
g. Menggunakan tool untuk memeriksa kerentanan. Tool yang dapat digunakan diantaranya Acunetix, SQLMap, SQL Injectiontools.

Mengukur dampak dari terjadinya SQL Injectionadalah a.Terhadap kelangsungan proses bisnis, indikatornya adalah seberapa besar dari fungsi-fungsi bisnis yang terdapat pada websitemengalami gangguan;b.Terhadapsistem dan informasi, apakah penyerang melakukan distribusi malware, membuat backdooratau melakukan web defacement. Selain itu, apakah ada data daninformasi yang berubah atau terhapus.

Tahap Eradication pada penanganan serangan SQL Injectionadalah untuk menghapus file /script serta menutup sumber serangan. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut:a.Memeriksa apakah terdapat malicious file, backdoor, rootkit atau kode-kode berbahaya lainnya yang berhasil ditanamkan pada server dan segera menghapusnya;b.Jika terdapat kode SQL yang mengakses IP tertentu maka perlu melakukan block /menutup sumber serangan(block IP dan Port).

Tahap Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Prosedur yang dapat dilakukan sebagai berikut:

a.Mengubah kredential password pengguna. Hal iniuntuk mengantisipasi apabila password pengguna telah diketahuioleh penyerang;
b.Melakukan recovery database pada aplikasi web;
c.JikaSQL Injection menyebabkanweb defacement, gunakan panduan penanganan insiden web defacement;
d.Jika SQL Injection menyebabkan insiden malware, gunakan panduan penanganan insiden malware;
e.Menutup semua kerentananyang telah diketahui;
f.Membatasi akses root langsung ke database;
g.Melakukan filter terhadap input yang dimasukkan oleh pengguna;
h.Mematikan atau menyembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan;
i.Patching terhadap aplikasi yang rentan, melakukan upgrade terhadap aplikasiwebyang masih memiliki kerentanan;
j.Melakukan penetration testing untuk mengetahui celah-celah keamanan yang mungkin masih terdapatpada website

Kesimpulan

Tenik hacking dari SQL Injection merupakan teknik yang cukup popoler pada website dengan prinsip untuk melewati perintah dari statment SQL yang di eksekusi oleh database backend. Apabila inputan user tidak disaring dengan sempurna maka akan sangat mudah untuk hacker menerobos masuk kedalam. Keamanan perlu ditingkatkan dengan cara selalu mengecek code program yang dibuat, kesalahan dalam statment SQL dapat memicu terjadinya web tersebut akan mudah diterbos masuk. Kepekaan kita harus ditingkatkan bila ingin melindungi web yang sedang diolah agar kenyamanan web dan privasi web terjamin dengan sempurna dan juga selalu mengikuti dan menerapkan Prosedur Penanganan Serangan Sql Injection.

Referensi:

https://cloud.bssn.go.id/s/Ho2B9xdfPjB89Kq#pdfviewer
https://eprints.akakom.ac.id/8085/3/3_175410054_BAB_II.pdf

Nama : **Mefta Eko Saputra**

NIM : **182420113**

Kelas : **MTI20A**

Phising

1. PENDAHULUAN

Berbicara mengenai perkembangan teknologi seperti sekarang ini, bisa dilihat di negara Indonesia sangat berkembang dengan pesat dan cepat. Terlepas dari hal itu sekarang sudah banyak yang membicarakan tentang revolusi industry 4.0 yang makin marak menjadi topik utama perbicangan. Revolusi industry ini merupakan perubahan secara besar- besaran yang menyangkut dari segala aspek pokok dalam segala bidang, yang mana aspek tersebut menjadi ukuran berjalannya sebuah sistem. Mau tidak mau kita juga harus bisa mengikuti perkembangan revolusi industry agar tetap selalu bisa bersaing dan bertahan. yang mana segala aspek sudah terubung satu sama lain secara otomatis, maka tidak mungkin kalau tidak melibatkan persoalan data dari segala aspek tersebut. Mengenai data tersebut otomatis juga akan banyak data yang digunakan sehingga dapat terjadi kemungkinan penumpukan data sampai melebihi kapasitas. Dengan kata lain persoalan sebuah data akan menjadi factor utama yang harus diperhatikan dengan baik, karena sebuah system dapat berjalan baik dan benar salah satunya unsur utamanya adalah data.

Maka dalam hal ini kemanan sebuah data menjadi sebuah permasalahan yang sangat penting. Bagaimana data tersebut dapat digunakan dengan baik, bagaimana cara mengatasi sebuah keamanan datanya dan bagaimana cara-cara menangani jika sampai terjadi pencurian sebuah data. Dari sebab itu untuk mengamankan sebuah data perlu dilakukan sebuah penelitian dengan metode naïve bayes classifier untuk menjaga sebuah keamanan data.

a. Website Phising

Phising adalah sebuah tindakan criminal untuk mencuri informasi pribadi orang lain menggunakan entitas electronic, salah satunya adalah website (Susanto Bekti Maryuni, 2016). Informasi ini dicuri dari website yang telah diakses yang mengandung phising atau dengan kata lain masuk ke dalam kategori website phising. Dikatakan website phising jika suatu website tersebut memenuhi kriteria atau karakteristik phising. Karakteristik phising

tersebut digolongkan menjadi empat golongan utama yaitu, Address Bar based Feature, Abnormal based Feature, HTML and Javascript based Features dan Domain based Feature (Mohammad, R., McCluskey, T., & Thabtah, F.A, 2012). Penjelasan dari empat jenis karakteristik tersebut terdapat dalam penjelasan di bawah ini.

1. **Address Bar Based**

   Pada Address Bar Based Feature ini terdapat 12 feature yaitu

   Using the IP Address Sebagai contoh untuk hal ini misal jika sebuah alamat IP Address yang digunakan sebagai alternative nama domain dalam URL seperti http://125.98.3.123/fake.html ini akan mengindikasi bahwa ada upaya seseorang untuk mengambil sebuah informasinya.

   Using URL Shorthening Service "Tiny URL" adalah metode untuk membuat URL menjadi lebih kecil panjangnya akan tetapi tetap mengarah ke alamat yang dituju, misalnya http://portal.hud.ac.uk/ dapat disingkat menjadi "bit.ly/19DXSk4".

   URL's having "@" Symbol Penggunaan symbol @ di dalam URL membuat browser mengabaikan segala sesuatu yang mendahului symbol @ dan alamat aslinya sering mengikuti symbol @**.**

   Redirect using"//" Penggunaan tanda"//" dalam URL berarti pengguna nantinya akan diarahkan ke situs lain.

   Adding Prefix or Suffix Separated by(-) to the Domain Simbol tanda hubung (-) jarang digunakan untuk oenamaan sebuah URL. Untuk tujuan Pisher cenderung akan menambahkan awlan atau sufiks yang dipisahkan oleh (-) ke nama domain sehingga pengguna merasa sudah masuk ke alamat yang benar. Misalnya http://www.Confirme-paypal.com/.

   Long URL to Hide the Suspicious Part Sebagai contoh untuk hal ini phising dapat menggunakan almat URL yang panjang untuk menyembunyikannya seperti *"http://federmacedoadv.com.br/3f/aze/ab51e2e319e51502f416dbe46b773a5e/?cmd =_home&dispatch=11004d58f5b74f8dc1e7c2e8dd4105e811004d58f5b74f8dc 1e7c2e8dd4105e8@ph ishing.website.html"* dari data alamat tersebut akan menghitung berapa panjang URL dan akan menghasilkan panjang rata-rata.

Sub Domain and Multi Sub Domain Terkadang penamaan suatu alamat website ada yang menggunakan sub domain ataupun muti domain. Jadi teknik untuk phising website ini juga memanfaatkan nama sub domain ataupun multi domain sehingga seolah-olah terlihat seperti turunan dari website aslinya.

HTTPS(Hyper Text Transfer Using Protocol with Secure Sockets Layer) Penggunaan HTTPS sangatlah penting dalam URL, dengan begitu legalitas sebuah situs web akan semakin diakui keasliannya.

Domain Registration Length Berapa lama usia domain suatu website ini juga berpengaruh dalam mendeteksi apakah suatu website termasuk website phising atau tidak. Sejauh ini umur website sebagai pelaku phising tidak lebih dari satu tahun.

Favicon adalah gambar grafik (ikon) yang dikaitkan dengan halaman web tertentu. Banyak agen pengguna yang ada seperti browser grafis dan pembaca berita menunjukkan favicon sebagai pengingat visual dari identitas situs web di bilah alamat.

Using Non-Standart Port

Fitur ini berguna dalam memvalidasi jika layanan tertentu naik atau turun di server tertentu. Untuk mengendalikan intrusi, lebih baik membuka port yang Anda butuhkan saja. Beberapa firewall, server Proxy dan Network Address Translation (NAT) akan, secara default, memblokir semua atau sebagian besar port dan hanya membuka yang dipilih.

The Existance of "HTTPS" Token in the Domain Part of thr URL Phisher dapat menambahkan token "HTTPS" ke bagian domain dari URL untuk mengelabui pengguna. Sebagai contoh, http://https-www- paypal-it-webapps-mpp-home.soft-hair.com/.

2. Abnormal Based Features

Pada Based Features ini ada 6 features yang dijelaskan di bawah ini :

Request URL URL Permintaan memeriksa apakah objek eksternal yang terkandung dalam halaman web seperti gambar, video, dan suara dimuat dari

domain lain.

URL of Anchor Fitur ini diperlakukan persis seperti "URL Permintaan.

Links in <Meta>, <Script> and <Link> tags Web yang sah menggunakan tag <Meta> untuk menawarkan metadata tentang dokumen HTML; Tag <Script> untuk membuat skrip sisi klien; dan tag <Link> untuk mengambil sumber daya web lainnya.

Server Form Handler (SFH) SFH yang berisi string kosong atau "about: blank" dianggap meragukan karena tindakan harus diambil atas informasi yang disampaikan.

Submitting Information to Email Formulir web memungkinkan pengguna untuk mengirimkan informasi pribadinya yang diarahkan ke server untuk diproses. Phisher mungkin mengarahkan informasi pengguna ke email pribadinya.

Abnormal URL Fitur ini dapat diekstraksi dari database WHOIS. Untuk situs web yang sah, identitas biasanya merupakan bagian dari URL-nya.

b. Internet Of Things (IoT)

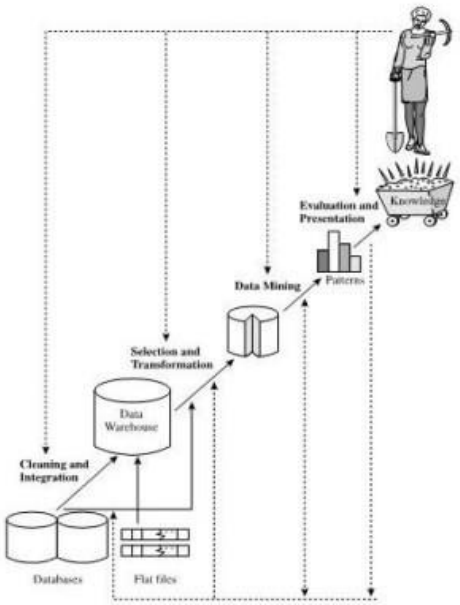
Internet of Things merupakan perkembangan keilmuan yang sangat menjanjikan untuk mengoptimalkan kehidupan berdasarkan sensor cerdas dan peralatan pintar yang bekerjasama melalui jaringan internet **(**Keoh, S. L., Kumar, S., & Tschofenig, H, 2014**)**. Sejak mulai dikenalnya internet pada tahun 1989, mulai banyak hal kegiatan melalui internet, dan pada tahun 1990 John Romkey menciptakan 'perangkat' pemanggang roti yang bisa dinyalakan dan dimatikan melalui Internet. Kemudian WearCam diciptakan pada tahun 1994 oleh Steve Mann dan ada tahun 1997 Paul Saffo memberikan penjelasan singkat pertama tentang sensor dan masa depan **(**Junaidi Apri, 2015). Selain itu juga masih banyak lagi kegunaan internet yang berkaitan dengan IoT.

c. Data Mining

Data Mining adalah proses penemuan keteraturan pola, dan hubungan dalam set data berukuran besar. Data yang dapat dianalisa dengan data mining bisa dari database, data

warehouse, web, repositori informasi atau data yang dapat dialirkan ke dalam sistem secara dinamis (Salim Tomy, Giap Yo Ceng, 2017**)**. Hasil dari pengolahan data dengan metode data mining ini dapat digunakan untuk mengambil keputusan di masa depan. Data mining ini juga dikenal dengan istilah pattern recognition (Sulastri Heni & Gufroni Acep Irham, 2017). Seorang pakar menyebutkan bahwa KDD atau Knowledge Discovery from Data, merupakan proses terstruktur, yaitu sebagai berikut (pei Han, J. Kamber M&Jian, 2011) :

a. Data Cleaning adalah Proses membersihkan data dari data noise dan tidak konsisten.
b. Data Integration adalah Proses untuk menggabungkan data dari beberapa sumber yang berbeda.
c. Data Selection adalah Proses untuk memilih data dari database yang sesuai dengan tujuan analisis.
d. Data Transformation adalah Proses mengubah bentuk data menjadi data yang sesuai untuk proses Mining.
e. Data Mining adalah Proses penting yang menggunakan sebuah metode tertentu untuk memperoleh sebuah pola dari data.
f. Pattern Evaluation adalah Proses mengidentifikasi pola.
g. Knowledge Presentation adalah yang dapat merepresentasikan informasi yang dibutuhkan, proses dimana informasi yang telah didapatkan kemudian digunakan oleh pemilik data.



Gambar 3. Data Mining sebagai dari proses *knowledge discovery*

Gambar 3 menunjukkan proses penjelajahan pengetahuan dimulai dari beberapa database dilakukan proses cleaning dan integration sehingga menghasilkan data warehouse. Dilakukan proses selection dan transformation yang kemudian disebut sebagai data mining hingga menemukan pola dan memperoleh pengetahuan dari data (knowledge). (Haryati Siska, Sudarsono Aji, Suryana Eko, 2015)

d. Naïve Bayyes Classifier

Naive Bayes classifier (NBC) merupakan salah satu metoda pembelajaran mesin yang memanfaatkan perhitungan probabilitas dan statistik yang dikemukakan oleh ilmuwan Inggris Thomas Bayes, yaitu memprediksi probabilitas di masa depan berdasarkan pengalaman di masa sebelumnya. Teori Naive Bayes Classifier bekerja sangat baik dibanding dengan model classifierlainnya. Hal ini dibuktikan oleh Xhemali, Hinde dan Stone dalam jurnalnya "Naïve Bayes vs. Decisi n Trees vs. Neural Networks in the Classification raining Web Pages" mengatakan bahwa "Naïve Bayes Classi ier memiliki tingkat akurasi yang lebih baik disbanding model classifier lainnya. Metode naïve bayes classifier akan mencari beberapa kemungkinan aman atau tidaknya situs web yang kita akses tersebut. Dengan begitu kita bisa menjaga keamanan data kita dengan tidak mengakses web yang sudah terdeteksi sebagai web phising. Metode naïve bayes ini dipilih karena dirasa paling tepat untuk menyelesaikan masalah deteksi website phising. Metode ini mampu menyeleseksi data dengan cara mengklasifikasikan sekumpulan data dengan memanfaatkan probabilitas dan statistic. Dimana probabilitas yang digunakan yaitu dengan menggunakan prediksi probabilitas masa depan dengan dasar-dasar masa sebelumnya. Klasifikasi Naive Bayes diasumsikan bahwa ada atau tidak ciri tertentu dari sebuah kelas tidak ada hubungannya dengan ciri dari kelas lainnya. Persamaan dari teorema Bayes adalah:

Persamaan dari teorema Bayes adalah (Saleh Alfa, 2015) :

$$P(H|X) = \frac{P(X|H) \cdot P(H)}{P(X)} \quad \ldots\ldots\ldots\ldots$$

Dimana :

X : Data dengan class yang belum diketahui

H : Hipotesis data merupakan suatu class spesifik

P(H|X) : Probabilitas hipotesis H berdasarkan kondisi X(posteriori probabilitas)

P(H) : Probabilitas hipotesis H(prior probabilitas)

P(X|H) : Probabilitas X berdasarkan kondisi pada hipotesis H

P(X) : Probabilitas X

Untuk menjelaskan metode naïve bayes, perlu diketahui bahwa proses klasifikasi memerlukan sejumlah petunjuk untuk menentukan kelas apa yang cocok untuk sampel yang sedang dianalisis tersebut. Oleh karena itu metode naïve bayes diatas disesuaikan swbagai berikut :

$$P(C|F1\ldots Fn) = \frac{P(C)P(F1\ldots.Fn|C)}{P(F1\ldots.Fn)} \ldots\ldots\ldots$$

Dimana variable C merepresentasikan kelas, smenetara variable F1…Fn merepresentasikan karakteristik petunjuk yang dibutuhkan untuk melakukan klasifikasi. Maka rumurs tersebut menjelaskan bahwa peluang masuknya sampel karakteristik tertentu dalam kelas C(Posterior) adalah peluang munculnya kelas C(sebelum masuknya sampel tersebut, seringkali disebut prior), dikali dengan peluang kemunculan karakteristik-karakteristik sampel pada kelas C(disebut juga likelihood), dibagi dengan peluang kemunculan karakteristik-karakteristik sampel secara global(disebut juga evidence). Karena itu, rumus diatas dapat pula ditulis secara sederhana sebagai berikut :

$$\text{Posterior} = \frac{\text{Prior x likelihood}}{\text{Evidence}} \ldots\ldots\ldots\ldots$$

Nilai evidence selalu tetap untuk setiap kelas pada satu sampel. Nilai dai posterior tersebut nantinya akan dibandingkan dengan nilai-nilai posterior kelas lainnya untuk menentukan ke kelas apa suatu sampel akan diklasifikasikan. Penjabaran lebih lanjut rumus bayes tersebut dilakukan dengan menjabarkan (C|F1,..Fn) menggunakan aturan perkalian sebagai berikut :

$$\begin{aligned} & P(C|F1, \ldots Fn = P(C)P(F1\ldots.Fn|C) \\ = \; & P(C)P(F1|C)P(F2,\ldots Fn|C,F1) \\ = \; & P(C)P(F1|C)P(F2|C,F1)P(F3,\ldots Fn|C,F1,F2) \\ = \; & (C)P(F1|C)P(F2|C,F1)P(F3|C,F1,F2) \\ & P(F4,\ldots Fn|C,F1,F2,F3) \\ = \; & P(C)P(F1|C)P(F2|C,F1)P(F3|C,F1,F2)\ldots \\ & P(Fn|C,F1,F2,F3\ldots Fn\text{-}1) \ldots. \end{aligned}$$

Dapat dilihat bahwa hasil penjabaran tersebut menyebabkan semakin banyak dan

semakin kompleksnya factor-faktor syarat yang mempengaruhi nilai probabilitas, yang hamper mustahil untuk dianalisa satu persatu. Akibatnya perhitungan tersebut menjadi sulit untuk dilakukan. Disinilah digunakan asumsi independensi yang sangat tinggi(naif), bahwa masing-masing petunjuk (F1,F2..Fn) saling bebas(independent) satu sama lain. Dengan asumsi tersebut maka berlaku satu kesamaan sebaai berikut :

$$P(F_i|F_j) = \frac{P(F_i \cap F_j)}{P(F_j)} = \frac{P(F_i)P(F_j)}{P(F_j)} = P(F_i) \quad (5)$$

Untuk i≠j , sehingga

$$P(F_i|C, F_j) = P(F_i|C) \quad (6)$$

Persamaan ke 5 dan 6 untuk pehitungan naïve bayes

Persamaan diatas merupakan model dari teorema naïve bayes yang selanjutnya akan digunakan dalam proses klasifikasi. Untuk klasifikasi dengan data kontinyu digunakan rumus Densitas Gauss :

$$P(X_i = x_i|Y = y_j) = \frac{1}{\sqrt{2\pi\sigma_{ij}}} e^{-\frac{(x_i-\mu_{ij})^2}{2\sigma^2_{ij}}} \quad (7)$$

Rumus Densitas Gauss

Dimana :

P : Peluang

Xi : Atribut ke i

xi : nilai atribut ke i

Y : kelas yang dicari

yi : Sub kelas Y yang dicari

u : mean, menyatakan rata-rata seluruh atribut

q : Deviasi standar, menyatakan varian dari seluruh atribut

e. Folds Cross Validation

Setelah data telah dibagi menjadi 80% data training dan 20% data testing, maka akan dilakukan 10-fold cross validation pada data training. Cross Validation adalah teknik untuk mengevaluasi model dengan cara mempartisi sampel asli ke dalam training set untuk melatih model, dan test set untuk mengevaluasi model. Dalam k-fold cross validation, sampel asli secara acak dipartisi dalam k equal size subsample. Dari subsample k, satu

subsample akan digunakan sebagai testing data dan sisanya akan menjadi training data. Proses cross validation akan diulang sebanyak k kali (kelipatan), dengan masing – masing dari subsample k digunakan sekali sebagai validation data. (Sandag Green Arther, Leopod Jonathan, Ong Vinky Fransiscus, 2018)

Folds Cross Validation

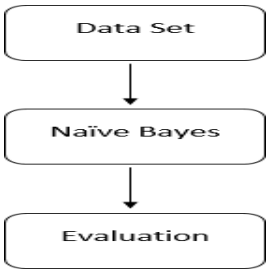
K-fold cross validation merupakan salah satu metode yang digunakan untuk mengetahui rata-rata keberhasilan dari suatu sistem dengan cara melakukan perulangan dengan mengacak atribut masukan sehingga sistem tersebut teruji untuk beberapa atribut input yang acak. K fold cross validation diawali dengan membagi data sejumlah n-fold yang diinginkan. Dalam proses cross validation data akan dibagi dalam n buah partisi dengan ukuran yang sama D1, D2, D3.. Dn selanjutnya proses uji dan latih dilakukan sebanyak n kali. Dalam iterasi ke-i partisi. Di akan menjadi data uji dan sisanya akan menjadi data latih. Untuk penggunaan jumlah fold terbaik untuk uji validitas, dianjurkan menggunakan 10-fold cross validation dalam model (R. Kohavi,1995). Skenario pengujian merupakan tahap penentuan pengujian yang dilakukan. Pengujian dilakukan menggunakan metode k-cross validation dengan nilai k sebanyak 10 fold, pengujian ini bertujuan untuk mengetahui akurasi metode naïve bayes classifier yang diterapkan pada analisis dan diuji dengan data training dan data testing yang berbeda . Penggunaan 10 fold ini dianjurkan karena merupakan jumlah fold terbaik untuk uji validitas (Pitria Pipit, 2016)

Fold	Data	*Subset*
Fold 1	Training Testing	$S_2, S_3, S_4, S_5, S_6, S_7 S_8, S_9, S_{10}$ S_1
Fold 2	Training Testing	$S_1, S_3, S_4, S_5, S_6, S_7 S_8, S_9, S_{10}$ S_2
Fold 3	Training Testing	$S_1 S_2, S_4, S_5, S_6, S_7 S_8, S_9, S_{10}$ S_3
Fold 4	Training Testing	$S_1 S_2, S_3, S_5, S_6, S_7 S_8, S_9, S_{10}$ S_4
Fold 5	Training Testing	$S_1 S_2, S_3, S_4, S_6, S_7 S_8, S_9, S_{10}$ S_5
Fold 6	Training Testing	$S_1 S_2, S_3, S_4, S_5, S_7, S_8, S_9, S_{10}$ S_6
Fold 7	Training Testing	$S_1 S_2, S_3, S_4, S_5, S_6, S_8, S_9, S_{10}$ S_7
Fold 8	Training Testing	$S_1 S_2, S_3, S_4, S_5, S_6, S_7 S_9, S_{10}$ S_8
Fold 9	Training Testing	$S_1 S_2, S_3, S_4, S_5, S_6, S_7, S_{10}$ S_9
Fold 10	Training Testing	$S_1 S_2, S_3, S_4, S_5, S_6, S_7 S_8, S_9$ S_{10}

Gambar tabel scenario stabilitas uji validitas 10-cross validation

2. HASIL DAN PEMBAHASAN

Peranan jaringan internet dalam era revolusi industri 4.0 ini sangat besar, karena hampir semua sistem yang digunakan sudah melibatkan jaringan internet. Dari hal tersebut maka tingkat keamanan data yang digunakan juga sangat berpotensi menjadi sasaran untuk tindak kejahatan. Kejahatan dengan menggunakan internet ini biasanya menggunakan perantara website atau yang sering disebut dengan website phising. Dengan cara seperti itu pelaku kejahatan bisa dengan bebas mencuri data yang menjadi incaran. Dari permasalahan tesebut penelitian ini akan membahas penerapan sebuah algoritma naïve bayes calssifier untuk menanggulangi kejahatan website phising agar kemanan data yang kita gunakan terjaga dengan baik. Penelitian ini adalah penelitian eksperimen dimana penelitian dilakukan dengan menerapkan k-fold cross-validation pada dataset website phising. Data set diambil dari repository UCI Machine Learning. Selanjutnya dari hasil feature reduction, dataset diterapkan pada algoritma machine learning yang popular yaitu naïve bayes untuk diukur tingkat akurasinya. Software yang digunakan pada penlitian ini adalah WEKA, dengan pemodelan alur peneletian seperti di bawah ini (Agus Fatkhurohman, Eli Pujastuti, 2019) :



Gambar 5. Alur Penelitian

Analisis Data Dalam tahapan ini peneliti mengumpulkan beberapa data yang akan diolah dengan sumber data dari UCI Machine Learning. Dengan menggunakan algoritma naïve bayes data tersebut akan diolah untuk mencari hasil dengan tingkat akurasi yang terbaik. Algoritma Naïve Bayes Classifier ini nantinya akan mengidentifikasi sebuah sebuah alamat website yang dicurigai sebagai alamat website phising. Dengan begitu dari sisi pengguna jaringan intenet akan mengetahui bahwa alamat website tersebut aman atau tidak. Dengan menggunakan dataset yang mempunyai jumlah atribut sebanyak 30 atribut yang diambil dari karakteristik phising yang digolongkan dari empat golongan utama yaitu, Address Bar based Feature, Abnormal based Feature, HTML and Javascript based Features dan Domain based Feature. Untuk pengujian Naïve Bayes menggunakan metode k-fold cross-validation untuk mengetahui kinerja algoritma tersebut. Tabel kategorikal atribut dapat dilihat dalam tabel di bawah ini (Agus Fatkhurohman, Eli Pujastuti, 2019) :

TABEL I.
ATRIBUT DAN LABEL

Nilai	Atribut
1 = valid 0 = mencurigakan -1 = phising	having_IP_Address, URL_Length, Shortining_Service, having_At_Symbol, double_slash_redirecting, Prefix_Suffix, having_Sub_Domain, SSLfinal_State, Domain_registeration_length, *Favicon*, *port*, HTTPS_token, Request_URL, URL_of_Anchor, Links_in_tags, SFH, Submitting_to_email, Abnormal_URL *Redirect*, on_mouseover, RightClick, popUpWidnow, *Iframe*, age_of_domain, DNSRecord, web_traffic, Page_Rank, Google_Index, Links_pointing_to_page, Statistical_report, *Result* (*Label*)

Penggunaan k-fold cross-validation ini nantinya akan menggunakan 10 folds dari total dataset yang ada. Dataset yang dipakai disini ada sekitar 11055 data atribut, yang berarti akan terbagi sekitar 1100 data dalam setiap folds. Dari perhitungan tersebut akan menghasilkan detail akurasi yang diambil sampai dengan F-Measure yang digambarkan hasilnya dengan tabel dibawah ini **(**Agus Fatkhurohman, Eli Pujastuti, 2019).

VALIDATION

Hasil 10 Folds Cross Validation							
	1	2	3	4	5	6	7
Weight average	0.93 0	0.07 6	0.93 0	0.93 0	0.93 0	92.9 8	7.01

Keterangan Tabel :
Hasil tersebut diatas adalah dalam hitungan persen %

1. TP Rate
2. FP Rate
3. Precision
4. Recall
5. F-Measure
6. Akurasi
7. Error

Dari perhitungan detail akurasi tersebut akan menemukan hasil cross validation dengan tingkat akurasi yang bisa dibilang sangat akurat karena akan memperoleh nilai sebesar 92.98% dan nilai toleransi error yang kecil sebesar 7.01% (Agus Fatkhurohman, Eli Pujastuti, 2019**).**

3. KESIMPULAN

Algoritma Naïve bayes sangat tepat untuk memperhitungkan klasifikasi website phising. Dari dataset yang telah di dapat ditarik kesimpulan dengan hasil sebagai berikut, Hasil dari pengujian algoritma Naive Bayes diperoleh nilai rata-rata akurasi sebesar 92.98% dengan TP Rate yang diperoleh sebesar 0.930%, FP Rate sebesar 0.076%, Precision sebesar 0.930%, Recall sebesar 0.930% dan F-measure sebesar 0.930%. Dengan demikian hasil penerapan algoritma naive bayes tersebut untuk melindungi data dari website phising dikatakan sangat baik, dan penggunaan algoritma tersebut sudah tepat jika digunakan untuk pencegahan pencurian data dari sebuah ancaman website phising.

REFERENSI

Fatkhurohman, Agus & Eli Pujastuti, 2019, " Penerapan Algoritma Naïve Bayes Classifier Untuk Meningkatkan Keamanan Data Dari Website Phising", Vol. XIV Nomor 2 Juni 2019 – Jurnal Teknologi Informasi

Susanto Bekti Maryuni, 2016, *"Identifikasi Website Phising Dengan Seleksi Atribut Berbasis Korelasi"*, Seminar Nasional Teknologi dan Komunikasi(SENTIKA), 18-19 Maret 2016

Mohammad, R., McCluskey, T., & Thabtah, F. A. 2012. "An Assesment Features Related to Phishing Websites using an Automated Technique. International Conference For Internet Technology And Secure Transaction. Ss 492-497. London:ICITST 2012

Keoh, S. L., Kumar, S., & Tschofenig, H. (2014). Securing the Internet of Things: A Standardization Perspective. *IEEE Internet of Things Journal*, *1*(3), 1–1

Junaidi Apri, 2015, *"Internet Of Things, Sejarah, Teknologi, dan Penerapannya : Review"*. Jurnal Ilmiah Teknologi Informasi Terapan (JITTER), Vol 1 No 3, Agustus, 2015

Salim Tomy, Giap Yo Ceng, 2017, *"Data Mining Identifikasi Website Phising Menggunakan Algoritma C4.5"*, Jurnal TAM(Technology Acceptance Model) Volume 8, Desember 2017, hal. 130-135

Saleh Alfa, 2015, *"Implementasi Metode Klasifikasi Naïve Bayes Dalam Memprediksi Besarnya Penggunaan Listrik Rumah Tangga",* Citec Journal, Vol. 2 No. 3 Mei 2015

Sandag Green Arther, Leopod Jonathan, Ong Vinky Fransiscus, 2018, *"Klasifikasi Malicious Website Menggunakan Algoritma K- NN Berdasarkan Application Layers dan Network Characteristics"*, Cogito Smart Journal, Vol.4 No.1 June

R. Kohavi, *"A study of Cross-Validation and Bootstrap for Accuracy Estimation and Model Selection,"*1995.[Online]

Available:http://frostiebek.free.fr/docs/Machine%20Learning/validation-1.pdf [Accessed 1 Februari 2019]

Pitria Pipit, 2016, *"Analisis Sentimen Pengguna Twitter Pada Akun Resmi Samsung Indonesia Dengan Menggunakan Naïve Bayes",* [Online], https://elib.unikom.ac.id/files/disk1/714/jbptun ikompp-gdl-pipitpitri-35651-7-unikom_p-a.pdf[akses pada 2 Februari 2019]

Sulastri Heni, Gufroni Acep Irham, 2017, "Penerapan Data Mining Dalam Pengel mp kan Penderita halassaemia", Jurnal Nasional Teknologi da Sistem Informasi, Vol. 03 No. 02

Han, J. Kamber M&Jian, Pei, 2011, "Data Mining : Concepts and Techniques, Thrid Edition, America : Morgan Kauffman,San Francisco.

Haryati Siska, Sudarsono Aji, Suryana Eko, 2015, *"Implementasi Data Mining Untuk Memprediksi Masa Studi Mahasiswa Menggunakan Algoritma C4.5 (Studi Kasus: Universitas Dehasen Bengkulu),* Jurnal Media Informatika, Vol. 11 No. 2 September

Nama : **MIFTAHUL FALLAH**
Nim : **182420132**
Kelas : **MTI. 20A**
DosenPengasuh : **M. IZMAN HERDIANSYAH, PhD**
Mata Kuliah : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEM**

TUGAS INDIVIDU 2
PAPER TENTANG PISHING

1. Pendahuluan

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yang senantiasa berubah serta cepatnya perkembangan software, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, data maupun aplikasi. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu sistem informasi. Keamanan komputer adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada komputer. Sasaran keamanan komputer antara lain adalah sebagai perlindungan informasi terhadap pencurian atau korupsi, atau pemeliharaan ketersediaan, seperti dijabarkan dalam kebijakan keamanan. Menurut Howard (1997) dalam bukunya "*An Analysis of security incidents on the internet"* menyatakan bahwa Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab.

Kejahatan dunia maya adalah istilah yang mengacu kepada aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan. Termasuk didalam kejahatan dunia maya antara lain penipuan lelang secara online, pemalsuan cek, penipuan kartu kredit (*carding*), *confidence fraud* dan kasus-kasus yang lainya. Dalam ruang lingkup keamanan komputer, phising adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk menyaru sebagai sebuah entitas yang dapat dipercaya*/ legitimate organization* dan biasanya berkomunikasi secara elektronik. Ada beberapa tipe *phising* yang kerap dilakukan oleh para pelaku kejahatan di dunia maya. Namun, jenis *phising* yang paling populer dan kerap digunakan biasanya ada dua jenis yaitu clone phising dan *spear phishing.*

Ketentuan hukum yang mengatur tentang *phishing* ini, sampai saat ini masih belum ada, tetapi bukanlah berarti perbuatan ini dibiarkan begitu saja. Sejauh ini bila terjadi kasus hukum yang menyangkut dunia maya *(cyber space)* pihak penegak hukum (baik itu polisi maupun jaksa)

akan menggunakan azas-azas hukum yang terdapat di dalam KUHP, dan nantinya bila telah masuk dalam persidangan biasanya hakim juga akan mencoba menggali lagi persoalan ini lebih lanjut dengan mempertimbangan nilai-nilai yang ada dalam masyarakat. Perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar penggunaannya dapat berkembang secara optimal. Ada tiga pendekatan untuk menjaga keamanan di *cyber space*, yaitu pendekatan aspek hukum, aspek teknologi, dan aspek sosial, budaya dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

2. Literature Review

Kata "phishing" berawal pada tahun 1996, kebanyakan orang percaya kata ini berasal sebagai ejaan alternatif dari "fishing" (memancing) seperti halnya "memancing informasi".Phising dikenal juga sebagai “Brand spoofing” atau “Carding” adalah sebuah bentuk layanan yang menipu anda dengan menjanjikan keabsahan dan keamanan transfer data yang anda lakukan. Menurut Felten et al spoofing (1997) dapat didefinisikan sebagai “Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya”.

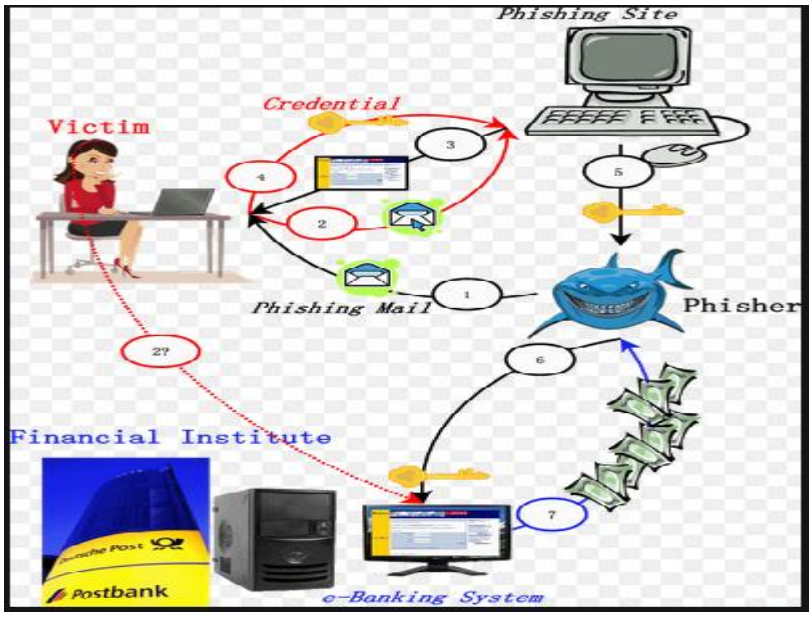
Pengertian Phising secara lengkapnya adalah suatu aktivitas penipuan untuk mendapatkan username dan password dari pengguna dengan cara tidak sah. Salah satu cara yang banyak dilakukan oleh para hacker dengan membuat website tiruan yang mirip dengan perusahaan aslinya, tujuannya agar Anda percaya dan kemudian memasukan username serta password, nah inilah yang dicari oleh para hacker Phising adalah singkatan dari Password Harvesting Phising yang artinya adalah tindakan memancing dengan tujuan untuk mengumpulkan password. Bentuk penipuan melalui phising, baik untuk mendapatkan informasi yang sensitif seperti password, nomor kartu kredit dan lain-lain atau menggiring orang untuk melakukan download file palsu yang berisi virus dengan menyamar sebagai orang atau lembaga bisnis yang terpercaya dalam sebuah komunikasi elektronik resmi, seperti email atau pesan singkat lainnya. Aksi ini semakin marak terjadi. Tercatat secara global, jumlah penipuan bermodus phising selama Januari 2005 melonjak 42% dari bulan sebelumnya. Anti-Phishing

Working Group (APWG) dalam laporan bulanannya, mencatat ada 12.845 e-mail baru dan unik serta 2.560 situs palsu yang digunakan sebagai sarana phishing. Selain terjadi peningkatan kuantitas, kualitas serangan pun juga mengalami kenaikan. Artinya, situs-situs palsu itu ditempatkan pada server yang tidak menggunakan protokol standar sehingga terhindar dari pendeteksian.

Komunikasi yang dipakai ini mulai dalam bentuk web site social yang sangat popular di mata masyarakat, site-site auction/ lelang, pengolah transaksi online payment atau dalam bentuk lain yang biasanya user menggunakan site tersebut untuk kepentingan administrasi, seperti email site, site jejaring public, dan lainnya. Bentuk phishing yang lain adalah mengirimkan email official dan instant messaging kepada user yang biasanya menggunakan site-site legitimate dan site-site nama besar perusahaan yang dikenal masyarakat dilengkapi dengan logo perusahaan, header email official sampai dengan cap dan tanda tangan salah satu pimpinan perusahaan tersebut.

Cara Kerja Phising

Dari definisi phising dapat diketahui cara kerja dari phising tersebut yang dilakukan untuk menjebak korban oleh sang penjebak (phisher). Phising yaitu aktivitas seseorang untuk mendapatkan informasi rahasia user dengan cara menggunakan email dan situs web palsu yang tampilannya menyerupai tampilan asli atau resmi web sebenarnya. Informasi yang didapat atau dicari oleh phiser adalah berupa password account atau nomor kartu kredit korban. Penjebak (phisher) menggunakan email, banner atau pop-up window untuk menjebak user agar mengarahkan ke situs web palsu (fake webpage), dimana user diminta untuk memberikan informasi pribadinya. Disinilah phisher memanfaatkan kecerobohan dan ketidak telitian user dalam web palsu tersebut untuk mendapatkan informasi. Cara kerja phising terlihat pada gambar berikut:



3. Pembahasan

Phising diperkenalkan pertama kali pada tahun 1995. Menurut James (2005) cara pertama yang dilakukan phisher adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Dalam ruang lingkup keamanan komputer, phising adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk menyaru sebagai sebuah entitas yang dapat dipercaya/ legitimate organization dan biasanya berkomunikasi secara elektronik. Berikut ini adalah aspek-aspek ancaman yang ternfeksi oleh phising:

1. Manipulasi Link

   Sebagian teknik phising menggunakan manipulasi link sehingga yang terlihat seperti alamat dari institusi yang asli. URL yang salah ejaannya atau penggunaan subdomain adalah trik umum digunakan oleh phisher, seperti contoh URL dibawah:

   www.micosoft.com

   www.mircosoft.com

   www.verify-microsoft.com dan bukannya

   www.microsoft.com

2. Filter Evasion

Phisher telah menggunakan gambar (bukan teks) sehingga mengecoh pengguna sehingga menyerahkan informasi pribadinya. Ini adalah alasan Gmail atau Yahoo akan mematikan gambar secara default untuk email yang masuk.

Teknik Phising

Dalam memancing korbannya seorang phiser melakukan beberapa teknik antara lain:

1) Email Spoofing

Teknik ini biasa digunakan phiser dengan mengirim email ke jutaan penggunaan dengan menyaru berasal dari institusi resmi. Biasanya email berisi pemintaan nomor kredit, password atau mendownload form tertentu

2) Pengiriman Berbasis Web

Pengiriman berbasis web adalah salah satu teknik Phising yang paling canggih. Juga dikenal sebagai “man-in-themiddle”, hacker terletak diantara situs web asli dan sistem phising.

3) Pesan Instan

Olah pesan cepat adalah metode dimana pengguna menerima pesan dengan link yang mengarahkan mereka ke situs web Phising palsu yang memiliki tampilan yang sama dan merasa sebagai situs yang sah

4) *Trojan Hosts*

Trojan hosts, hacker terlihat mencoba u ntuk login ke *account* pengguna anda untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke phisher.

5) Manipulasi Tautan

Manipulasi link adalah teknik dimana phiser mengirimkan link kesebuah website. Bila penggun menklik pada link tersebut maka akan terbuka website phiser dan bukan website sebenarnya.

6) *Malware phising*

Penipuan phising melibatkan *malware* memerlukan cara untuk dijalankan pada komputer pengguna. *Malware* ini biasanya melekat pada email yang dikirimkan kepada pengguna oleh *phisher.* Setelah korban mengklik pada *link* maka *malware* akan mulai berfungsi. *Malware* tersebut terkadang disertakan pada *file download.*

Cara Melawan Serangan Phising

Cara yang paling populer untuk melawan serangan phishing adalah dengan mengikuti perkembangan situs-situs yang dianggap sebagai situs phishing. Berikut ini adalah beberapa extensions Firefox yang bisa digunakan untuk melawan serangan phishing.

- **PhishTank SiteChecker**

  SiteChecker memblokir semua situs phishing berdasarkan data dari Komunitas PhishTank. Ketika Anda mengunjungi situs yang dianggap situs phishing oleh PhishTank, maka akan muncul halaman blocking.

- **Google Safe Browsing**

  Google Safe Browsing memberikan peringatan kepada Anda jika suatu halaman situs mencoba untuk mengambil data pribadi atau informasi rekening Anda. Dengan menggabungkan kombinasi algoritma dengan data-data tentang situs-situs palsu dari berbagai sumber, maka Google Safe Browsing dapat secara otomatis mengenali jika Anda mengunjungi situs phishing yang mencoba mengelabui seperti layaknya situs asli.

- **WOT**

  WOT membantu Anda mengenali situs-situs phishing dengan memperlihatkan reputasi situs tersebut pada browser Anda. Dengan mengetahui reputasi suatu situs, diharapkan Anda akan semakin mudah menghindari situs-situs phishing. Reputasi suatu situs diambil berdasarkan testimoni dari komunitas WOT.

- **Verisign EV Green Bar**

  Ekstensi ini menambahkan validitasi certificate pada browser Anda. Ketika Anda mengakses situs 'secure', maka address bar akan berubah warna menjadi hijau dan menampilkan pemilik dan otoritas sertifikat. Ekstensi ini berguna untuk mengenali situs-situs palsu.

- **ITrustPage**

  iTrustPage mencegah pengguna internet mengisi form pada suatu situs palsu. Ketika mengunjungi situs yang terdapat halaman form, iTrustPage menghitung nilai dari TrustScore halaman form tersebut, untuk mengetahui apakah situs tersebut dapat dipercaya atau tidak.

- **Finjan Secure Browsing**

Finjan SecureBrowsing meneliti link pada hasil pencarian Anda dan memberi peringatan kepada Anda mengenai link-link yang berpotensi sebagai link phishing. Finjan akan mencoba mendeteksi kode berbahaya dan script-script berbahaya. Setelah itu akan diberi tanda hijau untuk yang aman dan merah untuk link yang berbahaya.

- **FirePhish**

  FirePhish memperingatkan Anda ketika Anda mengunjungi situs yang dianggap situs phishing atau yang terdapat script dan kode yang mencurigakan.

Hukuman dan Undang-Undang yang Mengatur tentang Phishing

Ketentuan hukum yang mengatur tentang phishing saat ini memang belum ada,tetapi tidak berari perbuatan tersebut dapat dibiarkan begitu saja. Perbuatan penipuandengan modus phishing tetap dapat terjerat dengan berbagai peraturan yang ada, diantaradengan UU No. 11 Tahun 2008 tentang Internet & Transaksi Elektronik (ITE) dimana UUini telah disahkan dan diundangkan pada tanggal 21 April 2008.

1) Pasal 28 ayat 1 UU ITE tahun 2008Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong danmenyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.
2) Pasal 35 UU ITE tahun 2008Setiap orang dengan sengaja dan tanpa hak atau melawan hikum melakukanmanipulasi, penciptaan, perubahaan, penghilangan, pengrusakan informasielektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik. (Phshing = penipuan situs).
3) Pasal 45 ayat 2Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 28 ayat 1atau ayat 2 dipidana dengan pindana penjara paling lama 6 (enam) tahun dan/ataudenda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).
4) Pasal 51 ayat 1Setiap orang yang memenuhi unsur sebagimana yang dimaksud dalam pasal 35 dihukum dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

4. Kesimpulan

Phishing adalah tindakan memperoleh informasi pribadi seperti User ID, Password dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah Kebanyakan dari teknik phising adalah melakukan manipulasi sebuah link di dalam yang akan dikirimkan ke korbannya. Dengan adanya , praktek phising terbilang mudah hanya dengan melakukan spam pada dan kemudian menunggu korbannya untuk masuk kedalam tipuannya.

Daftar Referensi

Rachmawati, D., Studi, P., Komputer, S., Utara, U. S., Crime, C., & Security, C. (1978). Issn : 1978-6603 phising sebagai salah satu bentuk ancaman dalam dunia cyber, 209–216.

Radiansyah, I., & Priyadi, Y. (2016). ANALISIS ANCAMAN PHISHING DALAM, *7*(1).

https://ditsti.itb.ac.id/email-phising/

Nama : MOH FAJRI AL AMIN

Nim : 182420121

Kelas : MTI. 20A

DosenPengasuh : M. IZMAN HERDIANSYAH, PhD

Mata Kuliah : ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEM

Tugas Individu 2

Phising

Pendahuluan

Di-era dewasa ini, orang-orang sudah sangatlah erat dengan yang namanya teknologi informasi dan haus akan informasi terbaru. Sebut saya tentang banyaknya orang yang aktf di dalam bersosial media seperti Facebook, Twitter, Whatsapp, Ataupun Instagram. Terlepas dari bersosial media, orang-orang juga dapat mendapatkan informasi dari berbagai website,blog ataupun apabila mereka mau melakukan transaksi barang secara elektronik atau yang biasa disebut online shop,kini sudah bukan hal yang asing lagi. Di saat maraknya pengguna sosial media di seluruh dunia, saat itu juga penjahat-penjahat dunia siber mulai melancarkan aksinya untuk mencari keuntungan dari pengguna sosial media. Salah satunya yaitu dengan phishing. Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung. memberikan semua informasi yang di butuhkan oleh sang penjebak. Phishing termasuk dalam kejahatan siber, dimana sekarang ini marak terjadi tindak kriminal melalui jaringan komputer. Seiring perkembangan zaman, tindak kriminal juga semakin merebak di seluruh dunia. Sehingga ancaman yang banyak terjadi saat ini juga melalui komputer. Bagi hacker cara ini merupakan cari paling mudah untuk di jadikan serangan. Meskipun di anggap mudah dan sepele tapi tetap saja ada pengguna yang masuk ke perangkap sang hacker

Banyak dari pengguna sosial media tidak memikirkan ancaman-ancaman seperti itu. Mereka mengangap hal tersebut sebagai hal yang sepele dan tidak perlu di besar-besarkan. Hingga kini, banyak sekali akun sosial media yang sudah terjebak dalam phishing. Salah satu serangan yang di luncurkan oleh penjahat siber itu adalah dengan menaruh fake link pada akun sosial media dengan ajakan atau iklan sederhana dan menggiurkan. Dengan hal tersebut penyerang dapat mengambil informasi pengguna dan menggunakannya untuk mencari keuntungan misalnya untuk mengambil uang dari rekening pengguna atau menggunakan rekening untuk pembayaran online. Untuk pengantisipasian serangan phishing semacam itu yang paling sederhana yaitu untuk tidak meng-klik jika ada link yang masuk melalui akun sosial media maupun email yang di gunakan untuk akun sosial media. Karena link yang tidak di kenal patut di curigai sebagai serangan phishing yang menjebak akun sosial media untuk menyebar luaskan hal-hal yang tidak baik pada pengguna sosial media yang lain.

Pada dasarnya, ketentuan hukum yang mengatur tentang phishing ini, sampai saat ini masih belum ada, tetapi bukanlah berarti perbuatan ini dibiarkan begitu saja. Sejauh ini bila

terjadi kasus hukum yang menyangkut dunia maya (cyber space) pihak penegak hukum (baik itu polisi maupun jaksa) akan menggunakan azas-azas hukum yang terdapat di dalam KUHP, dan nantinya bila telah masuk dalam persidangan biasanya hakim juga akan mencoba menggali lagi persoalan ini lebih lanjut dengan mempertimbangan nilai-nilai yang ada dalam masyarakat. Perlu diperhatikan sisi keamanan dan kepastian hukum dalam pemanfaatan teknologi informasi, media, dan komunikasi agar penggunaannya dapat berkembang secara optimal. Ada tiga pendekatan untuk menjaga keamanan di cyber space, yaitu pendekatan aspek hukum, aspek teknologi, dan aspek sosial, budaya dan etika. Untuk mengatasi gangguan keamanan dalam penyelenggaraan sistem secara elektronik, pendekatan hukum bersifat mutlak karena tanpa kepastian hukum, persoalan pemanfaatan teknologi informasi menjadi tidak optimal.

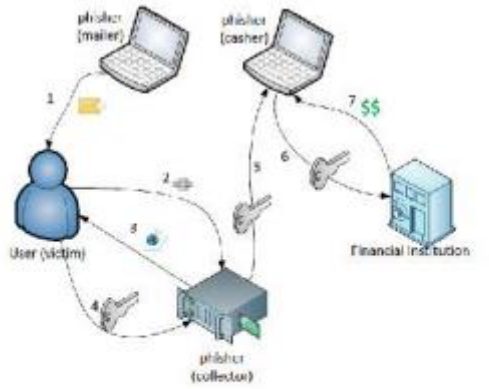
Literature review

Dalam ruang lingkup keamanan komputer, phising adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk menyaru sebagai sebuah entitas yang dapat dipercaya/ legitimate organization dan biasanya berkomunikasi secara elektronik. Phising diperkenalkan pertama kali pada tahun 1995. Menurut James (2005) cara pertama yang dilakukan phisher adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Jumlah kredit acak kartu yang digunakan untuk membuat rekening AOL. Akun tersebut kemudian digunakan untuk spam pengguna lain dan untuk berbagai hal lainnya. Programprogram khusus seperti AOHell digunakan untuk menyederhanakan proses. Praktek ini diakhiri oleh AOL pada tahun 1995, ketika perusahaan membuat langkah-langkah keamanan untuk mencegah keberhasilan penggunaan angka kredit secara acak kartu. Phising dikenal juga sebagai “Brand spoofing” atau “Carding” adalah sebuah bentuk layanan yang menipu anda dengan menjanjikan keabsahan dan keamanan transfer data yang anda lakukan. Menurut Felten et al spoofing (1997) dapat didefinisikan sebagai “Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya”.

Cara kerja Phishing

Dalam ruang lingkup keamanan komputer, phising adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk menyaru sebagai sebuah entitas yang dapat dipercaya/ legitimate organization dan biasanya berkomunikasi secara elektronik. Phising diperkenalkan pertama kali pada tahun 1995. Menurut James (2005) cara pertama yang dilakukan phisher adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Jumlah kredit acak kartu yang digunakan untuk membuat rekening AOL. Akun tersebut kemudian digunakan untuk spam pengguna lain dan untuk berbagai hal lainnya. Programprogram khusus seperti AOHell digunakan untuk menyederhanakan proses. Praktek ini diakhiri oleh AOL pada tahun 1995, ketika perusahaan membuat langkah-langkah keamanan untuk mencegah keberhasilan penggunaan angka kredit secara acak kartu. Phising dikenal juga sebagai “Brand spoofing” atau “Carding” adalah sebuah bentuk layanan yang menipu anda dengan menjanjikan keabsahan dan keamanan transfer data yang anda lakukan. Menurut Felten et al spoofing (1997) dapat didefinisikan sebagai “Teknik yang digunakan untuk memperoleh akses yang

tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya". Berikut lampiran gambar yang mengilustrasikan bagaimana Phising itu bekerja.



Gambar 1 Cara Kerja dan Alur informasi Phising

Berikut merupakan cara kerja phishing berdasarkan sumber-sumber ancaman phishing yang didapat dari beberapa sumber :

A. Email

Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti link URL yang terdapat dalam email tersebut . Pada dasarnya, phishing menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima email . Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut . Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi .

B. Website

Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti password dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas .Phiser juga menggunakan tool untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu . Selain itu, phiser menciptakan embedding link untuk mendapatkan informasi sensitif milik korban.

C. Malware

Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu file yang di kirim oleh phiser sebagai penetralisir malware di komputer nantinya .

Pembahasan

Phising diperkenalkan pertama kali pada tahun 1995. Menurut James (2005) cara pertama yang dilakukan phisher adalah dengan menggunakan algoritma yang membuat nomor kartu kredit secara acak. Dalam ruang lingkup keamanan komputer, phising adalah salah bentuk kejahatan elektronik dalam bentuk penipuan. Dimana proses phising ini bermaksud untuk menangkap informasi yang sangat sensitif seperti username, password dan detil kartu kredit dalam bentuk menyaru sebagai sebuah entitas yang dapat dipercaya/ legitimate organization dan biasanya berkomunikasi secara elektronik. Berikut ini adalah aspek-aspek ancaman yang ternfeksi oleh phising:

1. Manipulasi Link

Sebagian teknik phising menggunakan manipulasi link sehingga yang terlihat seperti alamat dari institusi yang asli. URL yang salah ejaannya atau penggunaan subdomain adalah trik umum digunakan oleh phisher yang dapat mengecoh calon korban dan membuat tampilan web mirip dengan website yang aslinya sehingga calon korban tidak akan sadar bahwa website yang dia akses ternyata adalah jebakan phising, seperti contoh URL dibawah:

www.microsotf.com

www.mircosoft.com

www.verify-microsoft.com dan

bukannya www.microsoft.com

d

2. Filter Evasion

Phisher telah menggunakan gambar (bukan teks) sehingga mengecoh pengguna sehingga menyerahkan informasi pribadinya. Ini adalah alasan Gmail atau Yahoo akan mematikan gambar secara default untuk email yang masuk.

Gambar 2 Email Phising yang dihubungkan ke sebuah halaman web

Teknik Phising

Dalam memancing korbannya seorang phiser melakukan beberapa teknik antara lain:

1) Email Spoofing

Teknik ini biasa digunakan phiser dengan mengirim email ke jutaan penggunaan dengan menyaru berasal dari institusi resmi. Biasanya email berisi pemintaan nomor kredit, password atau mendownload form tertentu

2) Pengiriman Berbasis Web

Pengiriman berbasis web adalah salah satu teknik Phising yang paling canggih. Juga dikenal sebagai “man-in-themiddle”, hacker terletak diantara situs web asli dan sistem phising.

3) Pesan Instan

Olah pesan cepat adalah metode dimana pengguna menerima pesan dengan link yang mengarahkan mereka ke situs web Phising palsu yang memiliki tampilan yang sama dan merasa sebagai situs yang sah

4) Trojan Hosts Trojan hosts, hacker terlihat mencoba u ntuk login ke account pengguna anda untuk mengumpulkan kredensial melalui mesin lokal. Informasi yang diperoleh kemudian dikirim ke phisher.

5) Manipulasi Tautan

Manipulasi link adalah teknik dimana phiser mengirimkan link kesebuah website. Bila penggun menklik pada link tersebut maka akan terbuka website phiser dan bukan website sebenarnya.

6) Malware phising

Penipuan phising melibatkan malware memerlukan cara untuk dijalankan pada komputer pengguna. Malware ini biasanya melekat pada email yang dikirimkan kepada pengguna oleh phisher. Setelah korban mengklik pada link maka malware akan mulai berfungsi. Malware tersebut terkadang disertakan pada file download.

Solusi mencegah terkena phishing

1) Medeteksi dengan toolsdetect

Sekarang ini internet sudah dianggap sebagai makanan sehari-hari, bahkan ada beberapa orang yang beranggapan tanpa internet mereka tidak bisa hidup. Ada banyak hal yang bisa kita lakukan dengan internet, mulai dari mencari informasi, berbagi informasi, dsb. Namun, pasti kita pernah menjumpai situs-situs yang muncul tanpa kita inginkan dan mengandung informasi berhadiah yang menggiurkan. Tentu saja hal tersebut akan menarik kita untuk mengisinya dengan data penting tanpa tau bahwa itu hanyalah situs phishing. Untuk mencegah hal tersebut kita dapat menggunakan toolsdetect yang mana dapat membedakan mana situs yang asli dan palsu (phishing). Berikut toolsdetect yang dapat digunakan :

a) PhishShield PhishShield merupakan aplikasi desktop yang berkonsentrasi pada URL dan konten situs web phishing. Cara kerjanya dengan mengambil URL sebagai masukan dan outputnya berupa status yang mengkonfirmasi URL termasuk phishing atau situs asli . Tingkat

akurasi yang diperoleh untuk PhishShield adalah 96,57% dan mencakup berbagai situs phishing yang dihasilkan tingkat kepalsuan negatif dan positif .

b) LinkGuard Algoritma LinkGuard Algoritma digunakan untuk menganalisis dua URL dan akhirnya tergantung pada hasil yang dihasilkan oleh algoritma . URL tersebut adalah URL yang melibatkan ekstraksi URL yang sebenarnya dan URL visual (yang dilihat pengguna) .

c) PhishDetector PhishDetector adalah ekstensi browser yang digunakan untuk mendeteksi serangan phishing yang mana menggunakan algoritma pencocokan string perkiraan untuk menentukan hubungan antara konten dan URL dari suatu halaman web.

2) Menggunakan add ons

web browser anti tabnabbing Setiap tahunnya para phisher melancarkan aksi-aksinya dengan membuat serangan-serangan baru. Dan salah satu serangan baru tersebut yaitu bernama tabnabbing. Serangan phishing tersebut dapat menyerang pada web. Dimana cara penyerangannya ketika pengguna membuka banyak tab, phishing tersebut akan terbuka di sela-sela tab yang lain. Saat pengguna lengah, maka tab tersebut akan di buka dan serangan di mulai. Tab palsu itu di samarkan menjadi salah satu tab yang di buka oleh pengguna dan tab asli yang sebelumnya lenyap. Untuk itulah serangan ini di anggap serangan yang pintar karena tidak lagi menggunakan link yang di klik dulu agar pengguna masuk perangkap phisher. Namun sepintar apapun suatu serangan, pasti ada jalan keluar. Beberapa cara pencegahan serangan tabnabbing:

a) Ketika pengguna membuka firefox dan terjadi serangan, pengguna bisa mengatasi serangan dengan account manager. Account manager dapat mengamankan pengguna karena pengguna di sarankan menyimpan login dan saat itu juga pengguna di berikan password acak setiap kali login .

b) Tidak hanya pada firefox saja, pada crome juga di berikan pengamanan terhadap phishing tabnabbing. Yaitu menggunakan AgenTab. AgenTab melakukan tindakan ketika pengguna mulai membuka situs web . AgenTab akan menyalakan peringatan ketika serangan terdeteksi. Peringatan tersebut akan muncul ketika tab tiba-tiba berubah tempat.

c) Dan yang terakhir dalam pencegahan tabnabbing dapat di lakukan dengan NoTabNab4. Add-on tersebut di usulkan oleh web browser Unlu dan Bicakci, dimana serangan phishing dapat diketahui saat suatu tab palsu meniru tab asli lalu add-on tersebut bekerja dengan cara memperingati dengan memberi tanda warna kuning atau merah sesuai tingkat serangan pada highlightned.

3) Menggunakan mekanisme pre-filter

Pencegahan phishingjuga dapat di lakukan dengan penggunaan anti-phishing pre-filter ini. Di dalam pre-filter terdapat tiga bagian pencegahan yakni Site Identifier, Login Form Finder, dan Webpage Feature Generator. Ketiganya tersebut melakukan pencegahan secara berurutan. Site Identifier digunakan untuk mengurangi jumlah perhitungan situs yang tidak perlu dan hanya mendeteksi halaman yang sah. Kemudian Login Form Finder di gunakan untuk menyaring halaman tanpa bentuk login lalu menghentikan mereka dari proses lebih lanjut karena form login merupakan satu-satunya cara untuk menyadarkan pengguna bila informasi pribadinya dicuri oleh phiser . Sistem ini dapat mengurangi kesalahan positif dari sistem tanpa harus mencurigai jumlah kesalahan negatif . Yang terakhir adalah Webpage Feature Generator, dimana fungsinya adalah mengidentifikasi halaman web phishing dengan melacak

karakteristik phishing yang di pamerkan dalam halaman tersebut. Seseorang dapat menggunakan cara ini ketika merasa bila halaman webnya sudah terserang phishing.

4) Pendeteksian dengan streaming analytics ‘PhishStrom’

Sekarang ini banyak sekali orang-orang yang berlomba-lomba melakukan penelitian untuk menciptakan suatu alat maupun aplikasi. Namun bukan hanya itu saja. Orang-orang juga mulai melakukan pendeteksian dengan berbagai cara. Dan anti phishing kali ini yaitu melakukan pendeteksian berupa streaming analisa menggunakan PhisStrom. PhisStrom sendiri di gunakan untuk mendeteksi URL yang terserang phishing. Dalam percobaannya, pendeteksian dengan cara ini dapat menghasilkan akurasi klasifikasi 94, 91% dengan tingkat positif palsu yakni 1,44%. Untuk risiko pada pengujian dataset menunjukkan pengidentifikasian 99,22% pada web yang sah dan phishing 83,97%. Untuk selanjutnya, PhisStrom dapat di gunakan sebagai alat add-on pada Mozila Firefox agar mempermudah dalam pendeteksian serangan phishing pada web.

HukumandanUndang-Undang yangMengatur tentangPhishing

Ketentuan hukum yang mengatur tentang phishing saat ini memang belum ada,tetapi tidak berari perbuatan tersebut dapat dibiarkan begitu saja. Perbuatan penipuandengan modus phishing tetap dapat terjerat dengan berbagai peraturan yang ada, diantaradengan UU No. 11 Tahun 2008 tentang Internet & Transaksi Elektronik (ITE) dimana UUini telah disahkan dan diundangkan pada tanggal 21 April 2008.

1) Pasal 28 ayat 1 UU ITE tahun 2008Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong danmenyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik.

2) Pasal 35 UU ITE tahun 2008Setiap orang dengan sengaja dan tanpa hak atau melawan hikum melakukanmanipulasi, penciptaan, perubahaan, penghilangan, pengrusakan informasielektronik dan/atau dokumen elektronik dengan tujuan agar informasi elektronik dan/atau dokumen elektronik tersebut seolah-olah data yang otentik. (Phshing = penipuan situs).

3) Pasal 45 ayat 2Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam pasal 28 ayat 1atau ayat 2 dipidana dengan pindana penjara paling lama 6 (enam) tahun dan/ataudenda paling banyak Rp 1.000.000.000,00 (satu miliar rupiah).

4) Pasal 51 ayat 1Setiap orang yang memenuhi unsur sebagimana yang dimaksud dalam pasal 35 dihukum dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp 12.000.000.000,00 (dua belas miliar rupiah).

Kesimpulan

Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Sumber-sumber ancaman phishing yaitu email, website, dan malware. Berdasarkan hasil survey yang telah dilakukan website merupakan sumber ancaman phishing paling banyak dan cara pencegahan yang sering dilakukan adalah self-efficacy (keyakinan individu dalam mengambil suatu tindakan).

Daftar Referensi

Rachmawati, D., Studi, P., Komputer, S., Utara, U. S., Crime, C., & Security, C. (1978). Issn : 1978-6603 phising sebagai salah satu bentuk ancaman dalam dunia cyber, 209–216.

Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, Technical Report: 540-96.

Howard, J.1997. An Analysis of Security Incidents on the Internet 1989-1995, (PhD thesis). Engineering and Public Policy: Carnegie Mellon University.

http://tekno.kompas.com/read/2009 /05/27/1 7001058/10.Tips.Mencegah.Serangan. Phising

Schneier, Bruce. 1996.Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed, John Wiley & Son Inc: New Jersey.

NAMA : MOH. RENDY SEPTIYAN

NIM : 182420103

KELAS : MTI20A

MATKUL : TUGAS - Ethical Issues in Electronic Information Systems

SQL INJECTION

1. PENDAHULUAN

Aplikasi web ada di mana-mana di Internet. Hampir semua yang Anda lakukan online selesai melalui aplikasi web apakah Anda mengetahuinya atau tidak. Mereka datang dalam bentuk berbasis webmail, forum, papan buletin, pembayaran tagihan, sistem rekrutmen, tunjangan kesehatan dan penggajian sistem. Penting untuk dipahami bahwa semua jenis situs web ini didorong oleh basis data. Database adalah elemen penting dari aplikasi web karena mereka dapat menyimpan pengguna preferensi, informasi pribadi yang dapat diidentifikasi, dan Web informasi pengguna sensitif lainnya aplikasi berinteraksi dengan database untuk secara dinamis membangun konten yang disesuaikan untuk setiap pengguna. Itu aplikasi web berkomunikasi dengan database menggunakan Structured Query Language (SQL). SQL adalah bahasa pemrograman untuk mengelola basis data yang memungkinkan Anda membaca dan memanipulasi data dalam MySQL, SQL Server, Access, Oracle, DB2, dan sistem basis data lainnya. Itu hubungan antara aplikasi web dan database biasanya disalahgunakan oleh penyerang melalui injeksi SQL. Injeksi SQL adalah jenis serangan injeksi di mana perintah SQL berada disediakan dalam variabel input pengguna, seperti bidang entri formulir web, dalam upaya untuk menipu web aplikasi dalam mengeksekusi kode penyerang pada database.

Injeksi SQL adalah salah satu vektor serangan utama yang bertanggung jawab untuk banyak profil tinggi 2011 ini kompromi termasuk Sony Pictures, HBGary, dan PBS. Itu juga bertanggung jawab untuk lebih pelanggaran data Adobe terbaru di mana nama, alamat email, dan hash kata sandi dicuri dari salah satu database pelanggan mereka. Injeksi SQL adalah kerentanan berbahaya yang mudah terdeteksi dan murah untuk diperbaiki. Metode serangan ini telah digunakan oleh hacker selama lebih dari satu sepuluh tahun namun ini masih merupakan vektor serangan paling umum dalam pelanggaran data saat ini.

Injeksi SQL ("Netralisasi Elemen Khusus yang Tidak Digunakan dalam Perintah SQL") ada di bagian atas daftar Kesalahan Perangkat Lunak Paling Berbahaya CWE / SANS terbaru dan harus dianggap serius. [1] Injeksi SQL terjadi ketika data yang dipasok oleh pengguna yang tidak terpercaya dimasukkan ke dalam aplikasi web dan data itu kemudian digunakan secara dinamis untuk membuat kueri SQL yang akan dieksekusi oleh server basis data. Aplikasi web umumnya menggunakan bahasa skrip sisi-server, seperti

ASP, JSP, PHP, dan CGI, untuk membangun kueri string yang diteruskan ke database sebagai pernyataan SQL tunggal. Aplikasi PHP dan ASP cenderung terhubung ke server database menggunakan Application Pemrograman Interface (API) yang lebih lama yang secara alami lebih mudah dieksploitasi sementara Aplikasi J2EE dan ASP.NET tidak mudah dieksploitasi. Jika aplikasi web rentan terhadap injeksi SQL, maka penyerang memiliki kemampuan untuk mempengaruhi SQL yang digunakan untuk berkomunikasi dengan database. Implikasinya sangat besar. Database sering mengandung informasi sensitif; oleh karena itu, seorang penyerang dapat membahayakan kerahasiaan dengan melihat meja. Penyerang juga dapat membahayakan integritas dengan mengubah atau menghapus catatan basis data menggunakan Injeksi SQL. Dengan kata lain, penyerang dapat memodifikasi kueri untuk mengungkapkan, menghancurkan, merusak, atau mengubah data yang mendasarinya. Bahkan mungkin untuk masuk ke aplikasi web sebagai pengguna lain tanpa pengetahuan kata sandi jika digunakan perintah SQL yang tidak divalidasi untuk memverifikasi nama pengguna dan kata sandi. Jika tingkat otorisasi pengguna disimpan dalam database, itu juga dapat diubah melalui injeksi SQL yang memungkinkan mereka mendapatkan lebih banyak izin dari yang seharusnya memiliki. Jika query SQL digunakan untuk otentikasi dan otorisasi, penyerang dapat mengubah logika pertanyaan tersebut dan memintas kontrol keamanan yang diatur oleh admin. Web aplikasi mungkin juga rentan terhadap injeksi SQL urutan kedua. Perintah SQL kedua serangan injeksi terjadi ketika data yang diberikan pengguna pertama kali disimpan dalam database, lalu kemudian diambil dan digunakan sebagai bagian dari kueri SQL yang rentan. Jenis kerentanan injeksi SQL ini lebih sulit untuk menemukan dan mengeksploitasi. Eksploitasi tidak berakhir ketika database dikompromikan, dalam beberapa kasus penyerang mungkin dapat meningkatkan hak istimewa mereka di Internet server database memungkinkan mereka untuk menjalankan perintah sistem operasi.

2. LITERATURE REVIEW

SQL Injection

[2] Injeksi SQL (*Bahaasa Inggris: SQL Injection*) adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan. Ini sebenarnya adalah sebuah contoh dari sebuah kategori celah keamanan yang lebih umum yang dapat terjadi setiap kali sebuah bahasa pemrograman atau skrip diimbuhkan di dalam bahasa yang lain.

3. PEMBAHASAN

a. Attack Skeanrio

Pertimbangkan kerentanan injeksi SQL sederhana. Kode berikut membangun kueri SQL oleh menggabungkan string yang dimasukkan oleh pengguna dengan string kode keras:

String query = "SELECT * FROM items WHERE owner = '" + userName + "'

AND itemName = '"+ ItemName.Text +"' ";

Maksud dari permintaan ini adalah untuk mencari semua item yang cocok dengan nama item yang dimasukkan oleh pengguna. Di contoh di atas, userName adalah pengguna yang diautentikasi saat ini dan ItemName.Text adalah input yang disediakan oleh pengguna. Misalkan pengguna normal dengan nama pengguna smith memasukkan manfaat dalam formulir web. Nilai itu diekstraksi dari formulir dan ditambahkan ke kueri sebagai bagian dari Kondisi SELECT. Query yang dieksekusi kemudian akan terlihat mirip dengan yang berikut:

SELECT * FROM items WHERE owner = 'smith' AND itemName = 'benefit' Namun, karena kueri dibuat secara dinamis dengan menggabungkan string kueri basis konstan dan string yang didukung pengguna, kueri hanya berlaku dengan benar jika itemName tidak mengandung satu kutipan (') karakter. Jika penyerang dengan nama pengguna smith memasuki string:

apapun 'OR' a '=' a

Kueri yang dihasilkan akan:

SELECT * FROM item WHERE pemilik = 'smith' DAN itemName = 'apa pun' ATAU 'a' = 'a' Penambahan kondisi OR 'a' = 'a' menyebabkan klausa WHERE untuk selalu mengevaluasi ke true. Kueri kemudian menjadi setara secara logis dengan kueri yang kurang selektif:

SELECT * FROM item

Query yang disederhanakan memungkinkan penyerang untuk melihat semua entri yang disimpan dalam tabel item, menghilangkan kendala bahwa kueri hanya mengembalikan item yang dimiliki oleh pengguna yang diautentikasi. Pada kasus ini penyerang memiliki kemampuan untuk membaca informasi yang seharusnya tidak dapat dia akses. Sekarang asumsikan bahwa penyerang masuk sebagai berikut:

apa pun'; jatuhkan item tabel— Dalam hal ini, kueri berikut dibuat oleh skrip:

SELECT * FROM items WHERE owner = 'smith' AND itemName = 'anything'; drop table items-- ' Tanda titik koma (;) menunjukkan akhir dari satu permintaan dan awal dari yang lain. Banyak database server memungkinkan beberapa pernyataan SQL yang dipisahkan oleh titik koma untuk dieksekusi bersama. Ini memungkinkan penyerang untuk mengeksekusi perintah sewenang-wenang terhadap database yang mengizinkan banyak pernyataan yang akan dieksekusi dengan satu panggilan. Tanda hubung ganda (-)

menunjukkan bahwa sisa tanda hubung baris saat ini adalah komentar dan harus diabaikan. Jika kode yang dimodifikasi secara sintaksis benar, maka kode itu akan dieksekusi oleh server. Ketika server database memproses dua pertanyaan ini, itu akan pertama-tama pilih semua catatan dalam item yang cocok dengan nilai apa pun yang dimiliki oleh pengguna smith. Kemudian server basis data akan menjatuhkan, atau menghapus, seluruh tabel item.

b. Blind SQL Injection

Bentuk lain dari injeksi SQL disebut injeksi SQL buta. Biasanya, jika penyerang untuk menyuntikkan kode SQL yang menyebabkan aplikasi web membuat kueri SQL yang tidak valid, lalu penyerang harus menerima pesan kesalahan sintaksis dari server database. Namun spesifik kode kesalahan dari database tidak boleh dibagi dengan pengguna akhir suatu aplikasi. Mungkin ungkapkan informasi tentang desain basis data yang dapat membantu penyerang. Dalam upaya untuk mencegah eksploitasi injeksi SQL, beberapa pengembang mengembalikan halaman generik dari pada pesan kesalahan atau informasi lain dari database. Ini membuat pemanfaatan SQL potensial kerentanan injeksi lebih sulit, tetapi bukan tidak mungkin. Seorang penyerang akan tahu apakah atau tidak permintaan valid berdasarkan halaman yang dikembalikan. Jika aplikasi rentan dan kueri valid, halaman tertentu akan dikembalikan. Namun, jika kueri tidak valid, halaman yang berbeda mungkin dikembalikan. Oleh karena itu, seorang penyerang masih bisa mendapatkan informasi dari database dengan meminta serangkaian pertanyaan benar dan salah melalui pernyataan SQL yang disuntikkan. Halaman yang sama harus dikembalikan terlepas dari apakah kueri SQL yang tidak valid dieksekusi.

c. Mitigation

Tiga strategi pertahanan utama terhadap injeksi SQL adalah query parameter, disimpan prosedur, dan validasi input. Opsi pertama adalah penggunaan kueri berparameter. Mereka mengharuskan semua kode SQL didefinisikan terlebih dahulu dan kemudian parameter dilewatkan ke kueri. Mereka lebih mudah untuk menulis daripada permintaan dinamis dan membantu mencegah injeksi SQL dengan membedakannya kode SQL dan data yang disediakan pengguna. Ini mencegah penyerang mengubah desain kueri dengan menyuntikkan kode SQL-nya sendiri. Misalnya, jika seorang penyerang memasukkan sesuatu 'OR '1' = '1 permintaan parameterisasi akan mencari basis data untuk item yang cocok dengan string apa pun 'OR' 1 '=' 1 alih-alih memasukkan OR '1' = '1 ke dalam kueri.

Strategi pertahanan kedua, sebanding dengan yang pertama, adalah penggunaan prosedur tersimpan yang mencegah injeksi SQL selama mereka tidak menyertakan generasi SQL dinamis yang tidak aman. Sekali lagi, kode SQL harus didefinisikan terlebih dahulu dan kemudian parameter dilewatkan.

Perbedaan antara permintaan parameter dan prosedur tersimpan adalah bahwa kode SQL untuk disimpan prosedur didefinisikan dan disimpan dalam database itu sendiri, kemudian dipanggil dari aplikasi. Aplikasi dapat memanggil dan menjalankan prosedur tersimpan menggunakan pernyataan panggilan SQL. Itu sintaks dan kemampuan prosedur yang disimpan bervariasi berdasarkan jenis database. Kode berikut akan membuat prosedur tersimpan yang akan menjalankan permintaan asli tanpa berbahaya menggabungkan input pengguna dengan kode SQL.

```
CREATE PROCEDURE SearchItems
@userName varchar(50),
@userItem varchar(50)
AS
BEGIN
SELECT * FROM items
WHERE owner = @userName
AND itemName = @userItem;
END
GO
```

Struktur kueri sudah ditentukan di server sebelum permintaan dijalankan dan kondisi kueri diteruskan sebagai parameter, oleh karena itu, input yang disediakan pengguna tidak akan keliru sebagai bagian dari permintaan SQL. Seperti dengan permintaan parameter, jika penyerang ingin kirimkan string apa pun 'OR' 1 '=' 1, itu akan diperlakukan sebagai input pengguna, bukan kode SQL. Di lain kata-kata, kueri akan mencari item dengan nama ini alih-alih mengeksekusi kode SQL yang tidak terduga Penting untuk dicatat bahwa prosedur yang disimpan tidak mencegah injeksi SQL dalam dan dari dirinya sendiri.
Jika kueri SQL dibangun dalam prosedur tersimpan dengan menggabungkan nilai parameter, seperti dalam contoh query rentan asli, ini menjalankan risiko yang sama dari injeksi SQL. Keuntungan menggunakan pendekatan ini adalah bahwa semua akun pengguna basis data dapat dibatasi hanya untuk mengakses yang disimpan prosedur dan karenanya tidak akan memiliki wewenang untuk menjalankan kueri dinamis. Tanpa kemampuan untuk menjalankan kueri dinamis, kerentanan injeksi SQL cenderung tidak ada.

Pendekatan ketiga adalah menghindari semua input yang disediakan pengguna sebelum menambahkannya ke kueri. Kapan input yang diterapkan pengguna diloloskan, karakter khusus diganti dengan karakter basis data jangan bingung dengan kode SQL yang ditulis oleh pengembang. Fungsi spesifik yang digunakan untuk menghindari input yang diterapkan pengguna bervariasi berdasarkan

bahasa skrip sisi server. Misalnya, dalam PHP fungsi addlashes () dapat digunakan untuk memasukkan garis miring terbalik sebelum tanda kutip tunggal ('), dobel kutipan ("), dan karakter garis miring terbalik (\) serta sebelum byte NULL. Catatan yang menambahkanlash () seharusnya tidak digunakan pada string yang telah lolos dengan magic_quotes_gpc (diaktifkan secara default sampai dihapus dalam PHP 5.4). Juga sangat disarankan untuk menggunakan basis data spesifik fungsi escape seperti mysqli_real_escape_string () untuk MySQL. Setiap manajemen basis data sistem mendukung satu atau lebih skema pelarian karakter khusus untuk jenis pertanyaan tertentu. Jika semua input yang disediakan pengguna diloloskan menggunakan skema pelolosan yang tepat untuk database, itu tidak akan bingung dengan kode SQL yang ditulis oleh pengembang. Ini akan menghilangkan beberapa kemungkinan SQL kerentanan injeksi, tetapi penyerang yang gigih akan dapat menemukan cara untuk menyuntikkan kode SQL. Teknik ini tidak sekuat yang lain, tetapi dapat dipertimbangkan jika menulis ulang dinamis kueri sebagai kueri parameterisasi atau prosedur tersimpan dapat merusak aplikasi warisan atau miliki dampak negatif yang signifikan terhadap kinerja.

Beberapa perlindungan tambahan terhadap injeksi SQL ditawarkan dengan menggunakan daftar putih untuk input validasi. Validasi input dapat digunakan untuk mendeteksi input yang tidak sah sebelum diproses oleh aplikasi. Pendekatan daftar putih untuk validasi input melibatkan pendefinisian input apa sebenarnya resmi. Semua input lain dianggap tidak sah. Pola validasi yang sangat kaku menggunakan ekspresi reguler harus dibuat untuk bidang yang terstruktur dengan baik seperti nomor telepon, tanggal, nomor jaminan sosial, nomor kartu kredit, alamat email, dll. Jika data yang dimasukkan pengguna tidak cocok dengan pola itu tidak boleh diproses. Jika bidang input memiliki set tetap opsi, seperti daftar drop-down atau tombol radio, maka input dari bidang itu harus tepat cocok dengan salah satu dari nilai-nilai itu. Bidang yang paling menantang untuk divalidasi adalah bidang teks gratis, seperti entri forum. Namun, bahkan bidang ini dapat divalidasi hingga tingkat tertentu. Tidak terduga dan karakter yang tidak perlu harus dihapus dan ukuran maksimum harus ditentukan untuk bidang input. Semua bidang input harus divalidasi menggunakan daftar putih.

Ukuran lain yang dapat digunakan untuk melengkapi strategi pertahanan utama adalah kepala sekolah paling tidak istimewa untuk akun basis data. Untuk membatasi kerusakan yang dilakukan oleh SQL yang sukses serangan injeksi, hak akses administrator tidak boleh diberikan ke akun aplikasi. Setiap pengguna yang diberikan harus memiliki akses ke sumber daya minimum yang diperlukan untuk melakukan tugas bisnis. Ini termasuk hak pengguna dan izin sumber daya seperti CPU dan batas memori, jaringan, dan izin sistem file. Akses hanya diberikan kepada tabel spesifik yang dibutuhkan akun untuk berfungsi dengan benar. Jika prosedur tersimpan digunakan, maka akun aplikasi hanya boleh diizinkan

untuk menjalankan prosedur tersimpan yang mereka gunakan dan mereka seharusnya tidak memiliki akses langsung ke tabel database. Penting untuk membatasi izin bahwa jika penyerang berhasil menyuntikkan kode berbahaya, pengguna basis data aplikasi akun tidak akan memiliki wewenang untuk menjalankan perintah.

Sistem manajemen basis data itu sendiri juga harus memiliki hak minimal pada operasi sistem. Banyak dari sistem ini berjalan dengan akses root atau tingkat sistem secara default dan seharusnya diubah menjadi izin yang lebih terbatas. Ini akan membuat semakin sulit bagi penyerang untuk mendapatkan akses tingkat sistem melalui injeksi SQL

4. KESEMIPULAN

Penting untuk mengetahui bagaimana mengidentifikasi dan memulihkan kerentanan injeksi SQL karena Sebagian besar pelanggaran data disebabkan oleh aplikasi web yang tidak memiliki kode. Kode apa saja itu membangun pernyataan SQL harus ditinjau untuk kerentanan injeksi SQL sejak server basis data akan menjalankan semua kueri yang secara sintaksis valid. Juga, perlu diingat bahwa bahkan data yang telah diparameterisasi dapat dimanipulasi oleh penyerang yang terampil dan gigih. Oleh karena itu, aplikasi web harus dibangun dengan mempertimbangkan keamanan dan secara teratur diuji untuk SQL kerentanan injeksi. Informasi lebih lanjut tentang injeksi SQL dan cara mencegahnya, termasuk contoh spesifik untuk berbagai bahasa skrip, serta pedoman untuk meninjau kode dan uji kerentanan injeksi SQL dapat ditemukan di Proyek Keamanan Aplikasi Web Terbuka (OWASP). [3]

5. DAFTAR REFERENSI

[1] "2011 CWE/SANS Top 25 Most Dangerous Software Errors." mitre.org. Ed. Steve Christey. The MITRE Corporation, 2011. Web. November 8, 2012.

[2] id.wikipedia.org. (2020, 25 Mei). Injeksi SQL. Diakses pada 27 Juni 2020, dari https://id.wikipedia.org/wiki/Injeksi_SQL

[3] The Open Web Application Security Project (OWASP):

- "SQL Injection." owasp.org. The Open Web Application Security Project, July 8, 2012. Web. November 7, 2012.
- "SQL Injection Prevention Cheat Sheet." owasp.org. The Open Web Application Security Project, July 8, 2012. Web. November 8, 2012.
- "Blind SQL Injection." owasp.org. The Open Web Application Security Project, July 8, 2012. Web. November 10, 2012.

Nama : Muhammad Devian Saputra

NIM 182420128

Matkul : Ethical Issues in Electronic Information Systems

SQL Injection

Pendahuluan

Apa Itu SQL Injection

SQL Injection adalah salah satu teknik yang menyalahgunakan celah keamanan yang ada di SQL pada lapisan basis data suatu aplikasi. Celah ini terjadi karena input dari user tidak difilter secara benar dan dalam pembuatannya menggunakan form yang salah. Jadi sampai saat ini SQL Injection masih menjadi favorit hacker untuk melakukan serangan pada website. Apalagi sekarang ini hacking melalui jaringan internet sudah tidak semudah zaman dulu.

Contoh mudah teknik SQL Injection melalui form username harusnya username diisi dengan karakter saja, tetapi form tersebut bisa diisi dengan karakter lain, jadi hacker bisa menyisipkan karakter seperti (:;-,=') sehingga hacker bisa memasukan query SQL Injection, akibatnya yang pasti website Anda sudah bisa ditembus oleh hacker tersebut.

Tujuan SQL Injection

Cara Kerja SQL Injection

SQL Injection yang dilakukan oleh hacker pasti memiliki tujuan, tidak mungkin hanya sebatas iseng saja. Berikut beberapa tujuan SQL Injection yang sering banyak ditemui:

- **Bypass Otentikasi**

Jika berhasil masuk kedalam sistem, hacker akan mudah melakukan bypass tanpa perlu menggunakan username dan password yang benar untuk bisa mendapatkan akses. Cukup dengan memasukan script SQL Injection pada form yang masih terbuka.

- **Pencurian Informasi**

Hacker memungkinkan untuk mengambil semua informasi yang ada pada website terutama informasi yang bersifat sensitif seperti username dan password.

Baca juga : Apa Itu Spoofing dan Bahayanya

- **Delete Data**

SQL Injection memungkinkan untuk hacker menghapus semua data yang tersimpan di database, jika sudah terjadi seperti ini dan tidak ada backup database maka akan sangat berbahaya. Jadi Anda perlu melakukan backup data secara berkala untuk tujuan keamanan data.

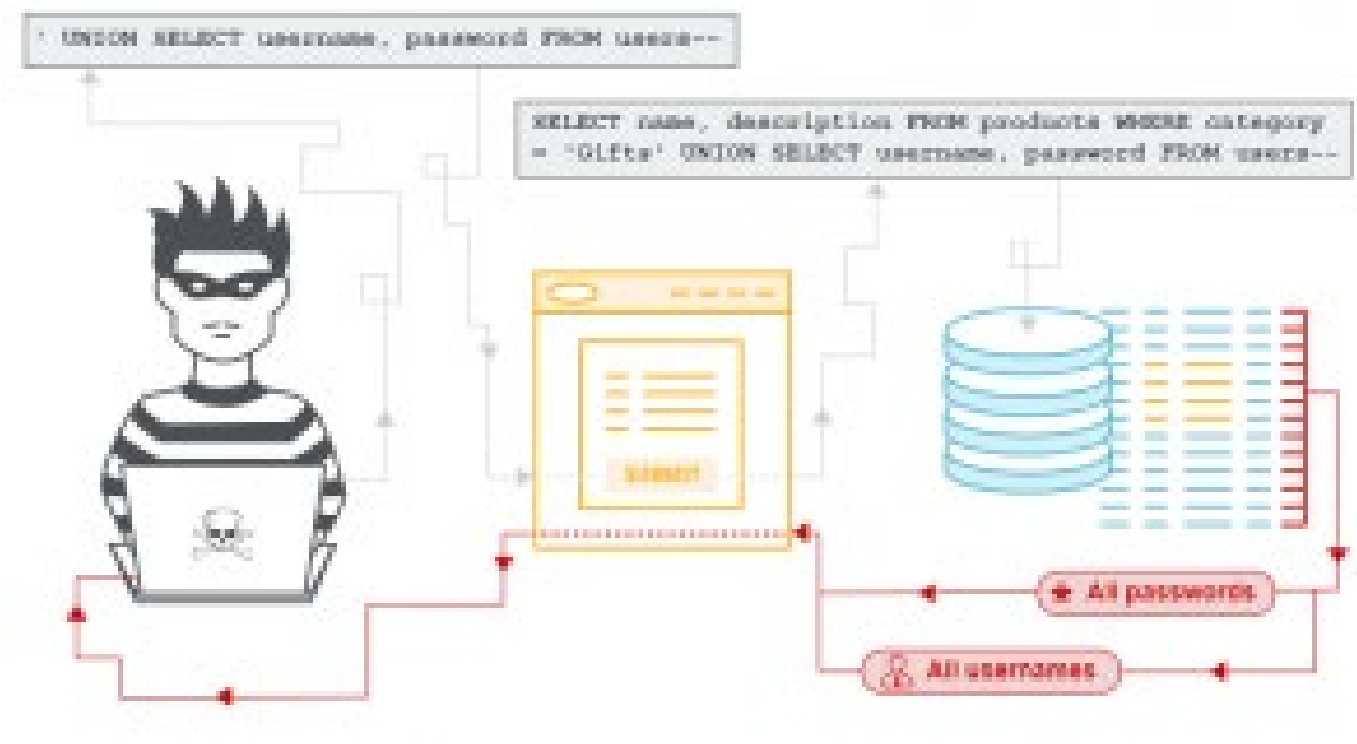
- **Modify Data**

Selain menghapus data, hacker dengan mudah mengubah data yang tersimpan di database sehingga menyebabkan data tidak valid. Jadi Anda perlu memiliki backup data jika sewaktu-waktu data dirubah oleh orang yang tidak bertanggung jawab.

- **Command Execution**

Pada beberapa database, Anda sebagai user bisa mengakses operating system menggunakan server database, kalau sudah seperti ini hacker bisa dengan mudah menyerang semua yang ada pada website Anda.

Cara Mengecegah SQL Injection



Proses SQL Injection

Untuk meminimalisir semua efek yang diakibatkan dari serangan SQL Injection, Anda bisa melakukan beberapa tindakan seperti berikut ini, yaitu:

1. Sesuaikan input box

Jika form input box tujuannya untuk menuliskan nama, maka berikan khusus untuk karakter saja, jika untuk mengisikan nomor telepon maka isilah dengan numbering saja sehingga tindakan SQL Injection bisa dihindarkan.

2. Batasi input box

Untuk lebih amannya dalam setiap box dibatasi jumlah karakternya, contoh saja untuk nama paling tidak diberikan 30 karakter atau disesuaikan sesuai dengan kebutuhan, sehingga jika ada percobaan SQL Injection yang masuk akan terkendala oleh jumlah karakter yang tersedia.

3. Filter user

Melakukan filter kepada inputan setiap user, terutama yang menggunakan karakter kutip tunggal (Validation Input) karena ini menjadi salah satu trik yang dilakukan hacker untuk SQL Injection.

4. Mematikan error handling

Jika terjadi error, Anda perlu mematikan fitur notifikasi pesan error yang keluar dari SQL Server. Jika sampai ada, ini bisa menjadi celah bagi hacker untuk melakukan eksploitasi lebih dalam percobaan SQL Injection.

5. Nonaktifkan fitur standart SQL

Fitur-fitur standart yang ada di SQL seperti *Stored Procedures* dan *Extend Stored Procedures* lebih baik untuk dimatikan saja, karena rawan terkena SQL Injection.

6. Setting Privilege

Silahkan Anda rubah pada bagian *'Stratup and run SQL Server'* dengan setting low privilege user pada menu SQL Server Security tab.

Nah demikian pemabahasan tentang apa itu SQL Injection dan cara mengatasinya. Kesimpulannya jangan sampai memberikan celah sedikitpun kepada hacker untuk melakukan SQL Injection, Anda sebagai pemilik website harus selalu berhati-hati dan waspada pada tindak kejahatan cyber seperti ini.

Untuk Anda yang membutuhkan pengamanan lebih pada website, kami memiliki rekomendasi untuk menggunakan layanan SSL Certificate, cukup dengan harga 150.000/tahun Anda sudah bisa memiliki **SSL Murah** dari brand Sectigo PositiveSSL. Tunggu apalagi segera pesan SSL untuk keamanan website Anda hanya di **GudangSSL.id**.

Teknik ini dapat mempengaruhi website dan aplikasi apa pun yang menggunakan database SQL seperti mySQL, Oracle, SQL Server, dan lainnya. Jika hal ini tidak Anda tangani dengan tepat, hacker dapat melakukan berbagai tindakan kejahatan yang dapat merugikan Anda dengan mengakses data sensitif seperti informasi pelanggan, data pribadi, rahasia bisnis, dan lain-lain. Untuk meminimalisir serangan SQL injection, terdapat beberapa tindakan yang dapat Anda lakukan, yaitu :

1. Jika memungkinkan, Anda dapat membatasi panjang input box. Dengan membatasinya di kode program, maka peretas tidak bisa melakukan injeksi dengan perintah yang panjang.

2. Memfilter input yang dimasukkan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation)

3. Menyembunyikan atau mematikan pesan eror yang muncul dari SQL server yang sedang berjalan.

Layanan Logique Digital Indonesia

Jika Anda belum mengetahui penaganan yang tepat terhadap serangan ini, Anda dapat menghubugi ***Logique Digital Indonesia*** . Kami memiliki ***layanan penetration testing*** yang dapat membantu Anda dalam menemukan celah keamanan serta meningkatkan sistem keamanan yang Anda miliki. Kerugian besar yang dapat ditimbulkan dari tindak peretasan dapat Anda hindari dengan memanfaatkan layanan yang kami berikan. Dengan tenaga profesional, kami akan membantu memberikan solusi terbaik untuk keamanan website dan aplikasi yang Anda miliki. Selain layanan penetration testing, ***Logique*** juga memiliki ***layanan lain*** yaitu pembuatan website, aplikasi, digital marketing, dan lain-lain.

ANCAMAN PHISING TERHADAP LAYANAN *E-COMMERCE* DALAM DUNIA *CYBERCRIME*

Muhammad Syahril
jurusan Magister Teknik Informatika
Fakultas Ilmu Komputer
Universitas Bina Darma
Palembang,Indonesia
msyahril311@gmail.com

Abstrak

Di era globaliasi teknologi yang sangat berkembang pesat *e-commerce* merupakan sebuah kebutuhan yang tidak bias lepas dari kehidupan sehari-hari masyarakat sekarang.dari segala kebutuhan tersebut terdapat ancaman(*cybercrime*) yang tidak di sadari oleh masyarakat salah satunya adalah phising,. Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak

Katakunci:e-commerce,cybercrime,phising

I. Pendahuluan

Peningkatan serangan cybercrime pada organisasi bisnis, infrastruktur pemerintah, dan individu telah menekankan pentingnya keamanan cyber, oleh karena itu analisis terhadap serangan cyber merupakan salah satu hal yang perlu dilakukan. Bentuk cybercrime yang dilakukan oleh para frauder diantaranya phishing. Phishing merupakan kegiatan kriminal dengan menggunakan teknik rekayasa sosial. Phisher (sebutan bagi pelaku kriminal phishing) berupaya menipu untuk mendapatkan informasi sensitif, seperti *username, password* dan rincian kartu kredit, dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik (N. P. Singh, 2007). Pengguna dirugikan dalam hal privasi, penyalahgunaan (eksploitasi) dari tindakan hacking bahkan kerugian finansial.

II. Tinjauan Pustaka

Sebagai penguatan teori penulis mengenai latar belakang ancaman phising terhadap layanan e-commerce penulis melakukan studi literature yang bersumber dari internet dan buku-buku yang berkaitan.

A. E-commerce

Berikut pengertian e-commerce menurut para ahli:

1. Penggunaan jaringan komunikasi dan komputer untuk melaksanakan proses bisnis. Pandangan populer dari e-commerce adalah penggunaan internet dan komputer dengan web browser untuk membeli dan menjual produk.
2. Transaksi bisnis yang terjadi dalam jaringan elektronik, seperti internet. Setiap orang yang mengakses komputer dan terhubung ke internet serta memiliki cara untuk membayar barang-barang atau jasa yang dibeli, dapat berpartisipasi dalam ecommerce.
3. Pembelian, penjualan dan pemasaran barang serta jasa melalui sistem elektronik, seperti : radio, televisi dan jaringan komputer atau internet.

B. *Cybercrime*(kejahatan dunia maya)

Menurut brenda nawawi (2001) kejahatan *cyber* merupakan bentuk fenomena baru dalam tindak kejahatan sebagai dampak langsung dari perkembangan teknologi informasi beberapa sebutan diberikan pada jenis kejahatan baru ini di dalam berbagai tulisan, antara lain: sebagai " kejahatan dunia maya" (cyberspace/virtual-space offence), dimensi baru dari "hi-tech crime", dimensi baru dari "transnational crime", dan dimensi baru dari "white collar crime".

C. Phising

Phishing adalah aktivitas cyber crime yang menggunakan rekayasa sosial dan tipuan teknis untuk mencuri data identitas dan kredensial akun keuangan. Skema rekayasa sosial dilakukan dengan menggunakan email palsu yang mengaku berasal dari institusi bisnis yang sah dan dirancang untuk mengarahkan korban ke situs web palsu yang mengelabui, sehingga korban membocorkan data keuangan seperti : nama dan kata sandi. Skema subterfomen teknis menanam crimeware ke PC untuk mencuri kerahasiaan secara langsung, sering menggunakan sistem untuk mengelabui nama pengguna dan kata sandi akun online dan merusak infrastruktur navigasi lokal untuk menyesatkan konsumen ke situs web palsu (atau situs web asli melalui proxy yang dikendalikan phiser yang digunakan untuk memantau dan intercept pada konsumen).

III. Hasil dan Pembahasan

Dari penjelasan tentang phising di atas kita dapat mengetahui cara kerja dari phising.adapun cara kerjanya:

1. Email

   Serangan ini di mulai dengan mengirimkan email yang terlihat dari sebuah organisasi

yang kenal dengan korban. Kemudian email tersebut akan meminta mereka untuk memperbarui informasi mereka dengan mengikuti link URL yang terdapat dalam email tersebut. Pada dasarnya, phishing menggabungkan rekayasa sosial dan vektor serangan kompleks untuk menciptakan ilusi atau penipuan di mata penerima email. Penyerang akan mengirimkan jutaan email ke jutaan pengguna dan ribuan dari mereka setidaknya akan jatuh pada rekayasa tersebut .Pastinya serangan-serangan tersebut menggunakan email palsu untuk menipu pengguna untuk menipu pengguna agar mau membocorkan data pribadi.

2. Website
   Pada situs web mereka akan diminta untuk memasukkan informasi rahasia pribadi, seperti password dan nomor rekening bank yang pada akhirnya akan digunakan untuk pencurian identitas .Phiser juga menggunakan tool untuk mencuri kode sumber laman web yang sah dan menggantinya dengan web palsu. Selain itu, phiser menciptakan embedding link untuk mendapatkan informasi sensitif milik korban [3].
3. Malware
   Cara penyerangan dengan berpura-pura meminta karyawan untuk mendownload suatu file yang di kirim oleh phiser sebagai penetralisir malware di komputer nantinya

Adapun pencegahan yang dapat dilakukan untuk mengatasi phising sebagai berikut:

1. Medeteksi dengan toolsdetect
   Adapun toolsdetect yang digunakan adalah:
   a. PhishShield
      PhishShield merupakan aplikasi desktop yang berkonsentrasi pada URL dan konten situs web phishing Cara kerjanya dengan mengambil URL sebagai masukan dan outputnya berupa status yang mengkonfirmasi URL termasuk phishing atau situs asli. Tingkat akurasi yang diperoleh untuk PhishShield adalah 96,57% dan mencakup berbagai situs phishing yang dihasilkan tingkat kepalsuan negatif dan positif.

      b. LinkGuard Algoritma
      LinkGuard Algoritma digunakan untuk menganalisis dua URL dan akhirnya tergantung pada hasil yang dihasilkan oleh algoritma. URL tersebut adalah URL yang melibatkan ekstraksi URL yang sebenarnya dan URL visual (yang dilihat pengguna)

      c. PhishDetector

PhishDetector adalah ekstensi browser yang digunakan untuk mendeteksi serangan phishing yang mana menggunakan algoritma pencocokan string perkiraan untuk menentukan hubungan antara konten dan URL dari suatu halaman web

2. Menggunakan add ons web browser anti tabnabbing
3. Menggunakan mekanisme pre-filter
4. Pendeteksian dengan streaming analytics 'PhishStrom'
5. Self-efficacy

IV. Kesimpulan

Phishing merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut. Yaitu dengan menipu seseorang sehingga orang tersebut secara tidak langsung memberikan semua informasi yang di butuhkan oleh sang penjebak. Sumber-sumber ancaman phishing yaitu email, website, dan malware. Berdasarkan hasil survey yang telah dilakukan website merupakan sumber ancaman phishing paling banyak dan cara pencegahan yang sering dilakukan adalah self-efficacy (keyakinan individu dalam mengambil suatu tindakan).

V. Daftar Pustaka

[1]. N. P. Singh, P., 2007. Online Frauds in Banks with Phishing. Journal of Internet Banking and Commerce, p. 4.

[2] P. McLeod, Sistem Informasi Manajemen, Jakarta: Salemba, 2008.

[3] S. C. Thomson, Discovering Computer, Jakarta : Salemba, 2008.

[4] W. Jony, Internet Marketing for Beginner, Jakarta: PT Alex Media Komputindo, 2010.

[5] dspace.uii.ac.id

[6]. APWG, "Phishing Activity Trends Report," Wasington D.C, 2018.

[7]. [2]Abdelhamid, N., Ayesh, A., & Thabtah, F. (2014). Expert Systems with Applications Phishing detection based Associative Classification data mining. Expert Systems With Applications, 41(13), 5948–5959. http://doi.org/10.1016/j.eswa.2014.03.019

[8]. [9]Lacey, D., Salmon, P., & Glancy, P. (2015). Taking the bait : a systems analysis of phishing attacks. Procedia Manufacturing, 3(Ahfe), 1109–1116. http://doi.org/10.1016/j.promfg.2015.07.185

[9]. 5]Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). AN IDEAL APPROACH FOR DETECTION AND PREVENTION OF PHISHING ATTACKS. Procedia - Procedia Computer Science, 49, 82–91. http://doi.org/10.1016/j.procs.2015.04.230

[10].]Gowtham, R., & Krishnamurthi, I. (2013). ScienceDirect A comprehensive and efficacious architecture for detecting phishing webpages. Computers & Security, 40, 23–37. http://doi.org/10.1016/j.cose.2013.10.004

[11]. Hamid, I. R. A., & Abawajy, J. H. (2014). An Approach for Profiling Phishing Activities. Computers & Security. http://doi.org/10.1016/j.cose.2014.04.002