Universitas Bina Darma ISO 9001 : 2000	PROSEDUR MUTU Pengelolaan Jurnal Ilmiah Terpadu	Nomor Dok : PM/PPMM/01 Nomor Revisi : 00 Tgl. Berlaku : 1 Juli 2007 Klausa ISO : 7.1

FORMULIR PENERIMAAN ARTIKEL JURNAL ILMIAH TERPADU
UNIVERSITAS BINA DARMA

Nama Penulis : Rasmila & Ari Muzakir
Institusi : Universitas Bina Darma
Judul Artikel : Celah Keamanan Sniffing Website Menggunakan Aplikasi SSLSTRIP

Tipe Artikel : ✓ Field Research ○ Library Research

Nama Jurnal : ✓ MATRIK ○ MBiA ○ TEKNO ○ Bina EDUKASI ○ Bina BAHASA ○ INOVASI ○ PSYCE

Daftar Kelengkapan Artikel :	ada	tidak	Keterangan
Hardcopy 2 rangkap & Softcopy (file.doc)	✓		
Biodata penulis			
Judul (Indonesia max 14 kata & Inggris 10 kata)	✓		
Abstrak : Indonesia dan Inggris (100-150 kata)	✓		
Keywords	✓		
Pendahuluan	✓		
Metodologi Penelitian (Field Research)	✓		
Pembahasan	✓		
Kesimpulan	✓		
Daftar Rujukan (T-5)	✓		
Lampiran (optional)			

Catatan : Keaslian materi artikel bukan tanggung jawab tim penyunting.

Waktu Proses

Deskripsi	Waktu	Keterangan
Penyerahan artikel	22 Juli 2014	
Pengeditan format artikel oleh pengelola (selesai)	22 Juli 2014	
Pengeditan format artikel oleh penulis (selesai)		
Pembagian artikel oleh Ketua Penyunting		
Pengeditan isi (content) artikel oleh Penyuting (Editor)		
Pengeditan isi (content) artikel oleh Penulis (jika ada)		

Palembang, 22 Juli 2014

Yang Menerima
Pengelola Jurnal Ilmiah Terpadu

Ch. Desi K.

Penulis,

Rasmila Ari Muzakir

Universitas Bina Darma Jurnal Ilmiah Terpadu (JIT - UBD)

Voucher Rp. 100.000 (seratus ribu rupiah)
Diberikan kepada : Arie Muzakie
Tanggal pemberian : 22 Juli 2014
Yang memberikan :

Ch. Desi K.

Universitas Bina Darma Jurnal Ilmiah Terpadu (JIT - UBD)

Jl. Jend. A. Yani No.12 Palembang 30264 Indonesia Telp. (0711) 515679, 515581, 515582
Fax. (0711) 515581, 515582 website : www.binadarma.ac.id Email : universitas@mail.binadarma.ac.id

CELAH KEAMANAN SNIFFING WEBSITE MENGGUNAKAN APLIKASI SSLSTRIP

Rasmila [1], Ari Muzakir [2]
Universitas Bina Darma1 (1)
Jalan Jendral A.Yani No.12 Plaju Palembang 30264
E-mail : rasmila@mail.binadarma.ac.id [1], arimuzakir@mail.binadarma.ac.id[2]

Abstrak

Dengan perkembangan teknologi yang pesat, penggunaan internet saat ini tidak harus mengguakan kabel LAN (UTP) untuk mengakses internet karena harus mencari kabel yang dapat tersambung ke internet. Sebagai pengembangannya, internet dapat diakses mengguakan wireless yaitu akses yang dapat dilakukan tanpa menggunakan kabel. Dengan begitu pengguna akan mudah mengakses internet dengan perangkat yang terdapat wirelessnya. Perkembangan internet juga sangat berkembang saat ini. Banyak sekali website yang tersedia saat ini dan dapat diakses pengguna dengan mudah. Pengguna biasanya mengakses langsung dengan mengetikan www pada browser di komputer atau laptopnya. Tapi pengguna yang awam tersebut tidak tahu bahwa terdapat protokol HTTP (Hypertext Transfer Protocol) yang menjadi gerbang antara pengguna internet dan website. Protokol HTTP sekarang berkembang dengan adanya protokol HTTPS (Hypertext Transfer Protocol Secure) yang dapat mengamankan data pengguna karena terdapat sertifikat digital yang dapat mengetahui pengguna kalau website tersebut benar dan aman dari serangan internet (hacking). Tapi beberapa website masih ada yang mengarahkan protokol HTTP tersebut ke HTTPS sehingga website tersebut rentan dari serangan internet dan dapat mengambil data pengguna baik itu username dan password yang mengakses ke website tersebut. Serangan tersebut dapat dilakukan melalui teknk sniffing dengan menggunakan aplikasi SSLStrip. Aplikasi SSLStrip merupakan aplikasi yang dapat mencari celah keamanan website yang menggunakan HTTPS dan dapat merekam kegiatan pengguna sehingga username dan password dapat dengan mudah didapatkan. Sebagai pengguna internet, harus tetap waspada terhadap serangan yang terjadi dengan tidak mengakses website perbankan atau transaksi (belanja internet) melalui wireless yang digunakan secara bersama-sama (publik) dan dapat mengaksesnya melalui modem.

Kata kunci:sniffing, HTTP, HTTPS, sslstrip

1. PENDAHULUAN

Wireless merupakan teknologi yang dapat digunakan untuk bekomunikasi baik itu mengakses internet dan mengakses perangkat lain sehingga dapat mempermudah pengguna karena wireless dapat menjalankan aktifitas (internet, mengakses perangkat) tanpa kabel. Protokol HTTP yang kita kenal sebagai pengakses halaman website di internet perkembangannya sangat bagus dalam hal keamanan data pengguna, dengan mengeluarkan protokol HTTP over SSL (HTTPS). HTTPS menggunakan sertifikat yaitu private key dan public key untuk mengautentikasi apakah website tersebut mendapatkan sertifikat yang dikeluarkan oleh CA (certificate

authority) yaitu lembaga yang mengatur sertifikat digital HTTPS, sehingga pengguna dapat mengakses website tersebut dengan aman. Pengguna internet yang awam tidak memahami apa itu HTTP dan HTTPS karena pengguna mengunjungi website dengan mengetikkan www.

Dengan perkembangan teknologi internet saat ini, banyak website yang telah mengubah protokol HTTP ke HTTPS karena terjamin keamanan data pengguna. Tapi mengakses protokol HTTPS langsung dapat memperlambat akses website dibandingkan dengan HTTP sehingga kebanyakan website hanya mengarahkan protokol HTTPS melalui HTTP. Jadi terdapat celah keamanan dalam penggunaan HTTPS di beberapa website yang masih mengarahkan HTTPS melalui protokol HTTP. Jurnal ini dibuat untuk mencari celah keamanan di setiap website, contohnya Yahoo Mail, Google Mail (Gmail), Facebook dan Twitter.

2. LANDASAN TEORI

2.1 SNIFFING

Network Sniffing adalah suatu aktifitas menyadap yang dilakukan dalam jaringan internet, dengan adanya penyerang (hacker) yang menyadap data pengguna pengakses internet untuk mendapatkan informasi yang berguna seperti data kartu kredit, username dan password.

2.2 HTTP

HTTP singkatan dari Hypertext Transfer Protocol merupakan protokol jaringan yang digunakan website-website internetyang menyediakan komunikasi antar jaringan, yaitu komunikasi antara jaringan komputer client dengan web server. Pada dasarnya kita mengetikan www pada browser internet, terdapat protokol HTTP untuk menghubungkan pengguna internet ke web server di website tersebut.

2.3 HTTPS

HTTPS singkatan dari Hypertext Transfer Protocol Secure merupakan pengembangan dari HTTP dengan tingkat kemananinternet tinggi dengan ditambahkan sertifikat digital yang dikelola oleh setiap CA (certificate authority) untuk digunakan pada website.

2.4 SSLSTRIP

SSLStrip adalah sebuah aplikasi yang dibuat oleh Moxie Marlinspike untuk melakukan serangan internet terhadap pengguna internet mengakses website yang dilindungi dengan protokol HTTPS dengan mencari celah

kemanan website yang mengarahkan HTTPS melaluiHTTP sehingga penyerang (hacker) mendapatkan informasi pengguna tersebut.

3. PENGUJIAN WEBSITE

Website yang diuji adalah Yahoo Mail, Google Mail (Gmail), Facebook dan Twitter yang menggunakan protokol HTTPS. Cara kerja dari SSLStrip adalah sebagai berikut:

a. SSLStrip akan mengubah link berawalan https menjadi HTTP sehingga yang muncul di browser pengguna bukan website ke HTTPS melainkan webiste ke HTTP.
b. Memberikan response redirect ke website HTTPS. SSLStrip akan mengubah header location dari website berawalan HTTPS menjadi HTTP.
c. Menggunakan META tag auto refresh ke website HTTPS: SSLStrip akan mengubah wesite HTTPS menjadi HTTP.
d. Menggunakan javascript untuk membuka website HTTPS: SSLStrip akan mengubah website HTTPS menjadi HTTP.

Hardware dan software yang digunakan adalah sebagai berikut:

1. Laptop processor Intel Atom (sebagai komputer target)
   Sistem operasi Windows XP SP2
   Aplikasi Mozilla Firefox untuk mengakses website Yahoo Mail, Google Mail (Gmail), Facebook dan Twitter.
2. Laptop processor Intel Core i5 (sebagai komputer attacker)
   Sistem operasi BackTrack 5 R3
   Aplikasi SSLStrip untuk mengambil data komputer target yang mengakses ke-4 website diatas.

Di komputer attacker, perintah yang diketik di Terminal adalah:

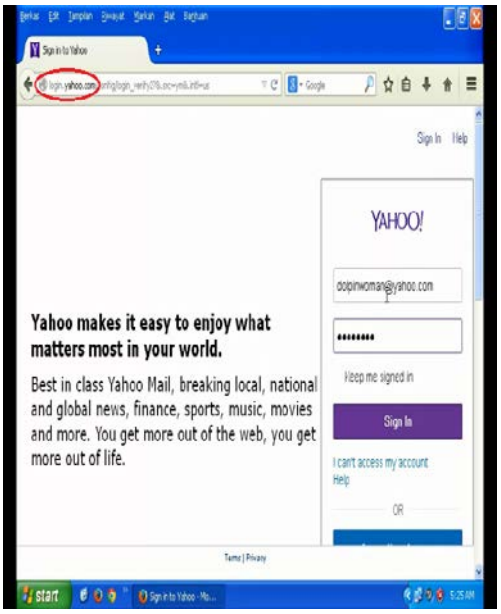
1. `nano /etc/etter.conf`
   untuk mengedit konfigurasi di bagian redir_command dengan mehilangkan tanda pagar di bagian iptables agar aplikasi SSLStrip mengaktifkan fungsi redir_command..

```
# if you use iptables:
redir_command_on          =
“iptables   -t   nat   -A
PREROUTING -i %iface -p tcp
–dport $
redir_command_off         =
“iptables   -t   nat   -D
PREROUTING -i %iface -p tcp
–dport$
```

2. `echo 1 > /proc/sys/net/ipv4/ip_forward`
   menginputkan angka 1 di file ip_forward.
3. `iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000`
   untuk mengubah iptables ke port 10000 agar dilisten aplikasi SSLStrip.
4. `nmap –sP –T4 192.168.243.1/24`
   untuk mencari ip komputer target di ip gateway.
5. `arpspoof -i eth0 -t 192.168.243.101 192.168.243.1`
   untuk memberikan broadcast arp ke ip komputer target. (192.168.1.101) adalah ip komputer target sedangkan (192.168.1.1) adalah ip gateway. Setelah itu buka terminal baru, dan ketik perintah:
6. `cd /pentest/web/sslstrip`
   untuk masuk ke dalam direktori sslstrip.
7. `python ./sslstrip.py -w hasilbaru.txt -a -l 10000`
   untuk membuka aplikasi SSLStrip dengan menambahkan port 10000 yang telah diinputkan di perintah iptables untuk dilisten aplikasi SSLStrip dan mengoutputkan file log hasil tangkapan website yang diakses oleh komputer target.
8. `tail –f hasil.txt`
   untuk menampilkan file hasil.txt di Terminal, berisi file log dari pengaksesan website komputer target.

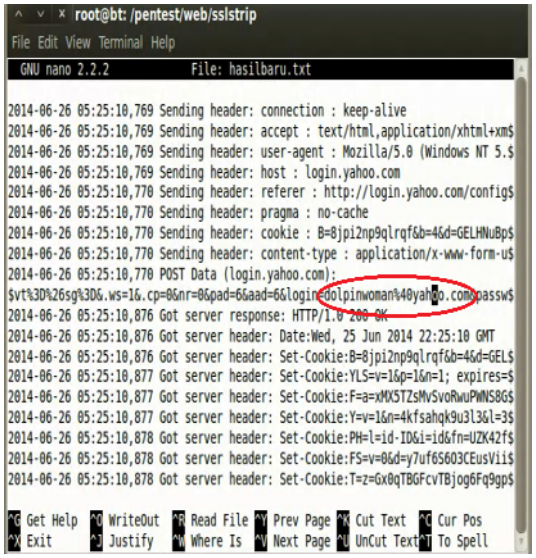
3.1 HASIL PENGUJIAN

Dari keempat website yang diuji, hanya website Yahoo Mail yang terdapat celah kelemahan, mengarahkan protokol HTTP ke HTTPS seperti gambar dibawah ini:

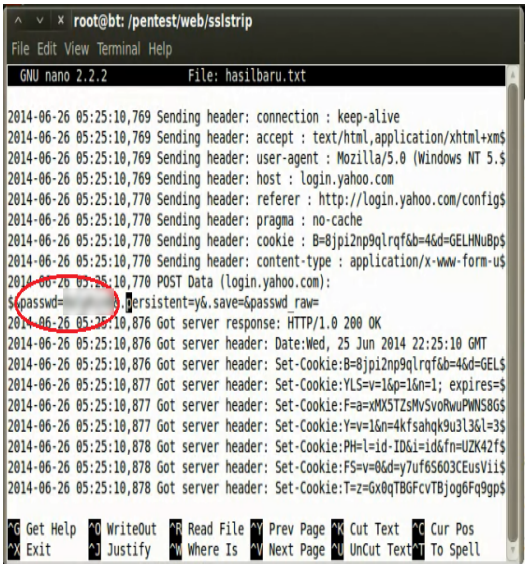


Gambar 1: Komputer target mengakses Yahoo Mail dan yang dilingkaran merah tidak terdapat protokol HTTPS.

Pada gambar diatas, tidak terdapat protokol HTTPS, maka komputer attacker dapat merekam username dan password di website email Yahoo Mail tersebut seperti gambar di bawah ini:

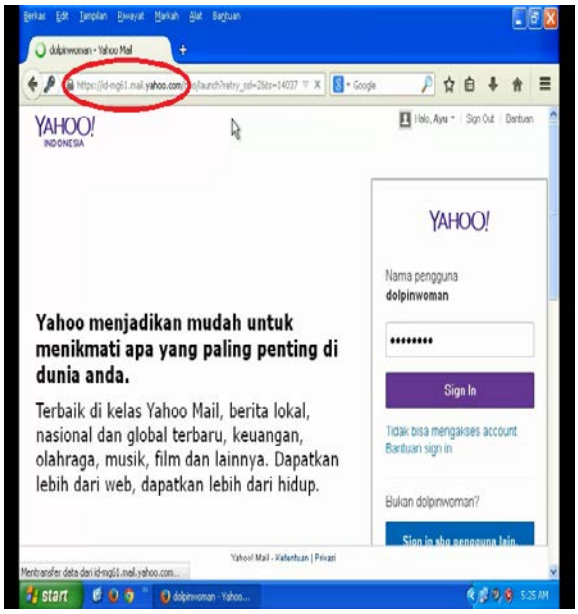


Gambar 2: Tampilan log dari file hasilbaru.txt yang menangkap username Yahoo Mail



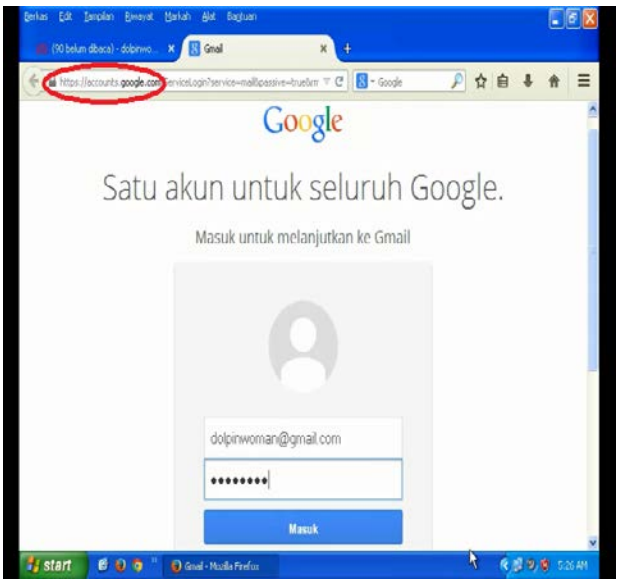
Gambar 3: Tampilan log dari file hasilbaru.txt yang menangkap password Yahoo Mail

Di komputer target, website Yahoo Mail tampil di menu login seperti Gambar 1 dan protokol website berubah menjadi HTTPS.



Gambar 4: Website Yahoo Mail yang menampilkan halaman username dan password.

Beberapa gambar dibawah ini adalah tampilan dari website Gmail, Facebook dan Twitter yang langsung mengarahkan ke protokol HTTPS.



Gambar 5: Tampilan website Gmail, Facebook dan Twitter yang merahkan langsung ke protokol HTTPS tanpa melalui protokol HTTP seperti pada website Yahoo Mail

4. KESIMPULAN DAN SARAN

Kesimpulannya adalah keamanan dari HTTPS dapat mudah dieksploitasi karena dari website yang tidak sigap dengan mengelola dengan tidak mengarahkan protokol HTTPS melalui HTTP sehingga celah keamanan dapat diminimalisir.Dengan aplikasi SSLStrip ini dapat dilakukan pemanfaataan pengguna yang mengakses website di protokol HTTPS yang sebenarnya diarahkan melalui HTTP. Padahal saat pengguna menggunakan protokol HTTP itulah berpotensi terkena serangan internet. Jika pengguna langsung menggunakan HTTPS, maka pengguna akan aman dan terbebas dari serangan internet.

Sarannya adalah berhati-hati menggunakan wireless publik seperti di mall, café yang banyak orang menggunakan wireless tersebut untuk mengakses website yang dianggap datanya sangat sensitif, seperti contoh website perbankan untuk transaksi online sehingga dapat muncul kejahatan dari penggunaan internet. Gunakanlah akses website perbankan tersebut dengan akses yang aman seperti di bank atau melalui modem internet. Untuk pengguna internet yang sudah mengerti dengan penggunaan komputer dan internet dapat

menggunakan SSH tunneling untuk mengakses internet. Jika pengguna mempunyai account SSH tunneling di internet (misalnya sistem linux-host), pengguna dapat mengguanakan account tersebut dan dapat menggunakannya melalui aplikasi seperti contoh Bitvise SSH Client dan Proxifier. Lalu lintas internet dengan penggunaan SSH tunneling tersebut sangat aman karena data akan dienkripsi.

DAFTAR RUJUKAN

Suryayusra. (2014) Ssltrip Sniffing Selection. *http://blog.binadarma.ac.id/suryayusra/wp-content/uploads/2014/04/ETHICAL-HACKING-SSLTRIP-SNIFFING-SELECTION-10.pptx* diunduh pada 30 April 2014.

Wicaksono, R. (2009) MITM Attack on Mandiri Internet Banking using SSLStrip. *http://www.ilmuhacking.com/web-security/mitm-attack-mandiri-internet-banking-using-sslstrip/* diunduh pada 26 Juni 2014.