Analisis Keamanan *Website* BAZMA Pertamina RU III Plaju Palembang

Muhammad Iqbal [1,] Yesi Novaria Kunang, S.T., M.Kom[2]., Usman Ependi, M.Kom[3].
[1)] Mahasiswa Teknik Informatika Universitas Bina Darma
[2)] Dosen Ilmu Komputer [3)] Dosen Ilmu Komputer. Jl Jend A.Yani No.12 Plaju, Palembang 30264

Email: muhammadiqbal12142045@gmail.com[1)]
yesi_kunang@mail.binadarma.ac.id[2)], usmanependi@mail.binadarma.ac.id[3)]

Abstrak. Keamanan informasi sebuah *website* sangatlah diutamakan pada saat ini, seiring semakin meningkatnya kejahatan di dunia maya sesuai dengan data ID-SIRTI sepanjang tahun 2014 terjadi serangan keamanan *cyber* berbagai macam bentuk. Tujuan dibuatnya penelitian ini yaitu mengevaluasi *control* keamanan *internal* sistem dengan mengidentifikasi ancaman yang dapat menimbulkan masalah serius terhadap aset organisasi dengan menerapkan metode penelitian *Action Resarch* yang mana tahap awalnya melakukan identifikasi masalah seperti pencurian paket data dan lain sebagainya, kemudian merencanakan hal-hal untuk penetrasi yang akan dilakukan diantaranya menggunakan tools-tools seperti *Acunetix web vulnerability scanner 9, Net tools, DoSHTTP 2.5, Digiblast 2, SynAttack, Sql map, Cross Site Scripting (XSS)* dan *Arp Spoofing*. Selanjutnya menerapkan perencanaan yang telah dibuat sebelumnya, lalu tahap mengevaluasi hasil dari penerapan dan yang terakhir yaitu mempelajari kriteria dalam prinsip pembelajaran. Hasil dari penetrasi akan dijadikan bahan pertimbangan seorang *administrator* jaringan untuk memperbaiki celah keamanan website yang terbuka.

1. Pendahuluan

1.1 Latar Belakang

Pertamina RU III Plaju suatu perusahaan BUMN yang bergerak di bidang eksplorasi dan pengolahan minyak serta gas bumi menjadi berbagai jenis bahan bakar dan petrokimia. Salah satu badan pendukung di Pertamina RU III yang membantu menyalurkan dana bantuan kepada kaum dhuafa dan sabilillah adalah Bazma. Bazma didirikan atas SK Menteri Agama No. 313 tanggal 24 Mei 2004. Saat ini, Bazma RU III Plaju Palembang mempunyai website sendiri dan web servernya berada di kantor *Information Technology* (IT) Area Pertamina RU III Plaju Palembang.

Pada website Bazma menyediakan informasi dalam sebuah tampilan *website*, baik informasi untuk pengenalan maupun informasi yang berkaitan tentang

penyaluran dana kepada kaum dhuafa dan sabilillah yang berada di sekitar Perusahaan. Adapun alamat URL Bazma Pertamina RU III Plaju Palembang adalah 10.53.1.12/webfungsi/bazma. Website Bazma menggunakan jaringan intranet atau *private network* untuk membagi informasi aktivitas Bazma setiap bulan. Namun sistem *private network* membuat masyarakat sekitar kesulitan untuk mengenal Bazma secara detail sehingga kurangnya informasi mengenai aktifitas bazma. Lemahnya keamanan website bazma membuat peneliti tertarik untuk melakukan penelitian terhadap web Bazma dengan tujuan untuk mengetahui informasi error, kemudian melakukan evaluasi terhadap celah keamanan website Bazma. Sehingga kedepannya *web* Bazma bisa online dan lebih dikenal lagi oleh masyarakat luas.

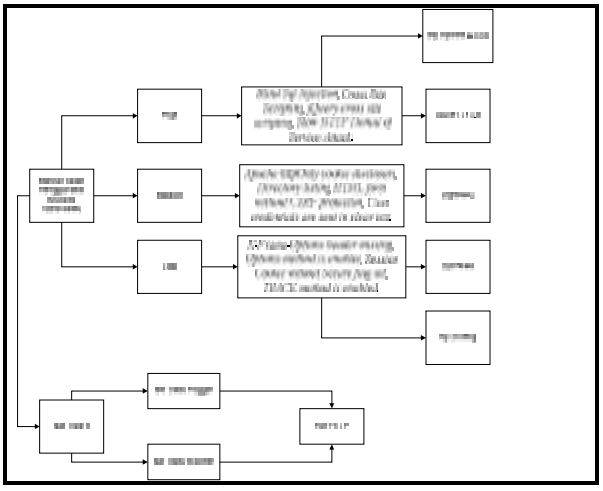
Demi menjaga fasilitas yang sangat diperlukan oleh para pekerja pertamina dari orang yang tidak bertanggung jawab yang menemukan pintu masuk atau celah ke *web server* bazma, akan lebih baik penelitian ini dilakukan. Dan jika menemukan pintu masuk atau celah keamanan akan dilaporkan ke bagian admin *web server* bazma serta melakukan perbaikan (*patching*) secepatnya. adapun batasan permasalahan dalam penelitian ini adalah untuk mengetahui informasi error dengan menggunakan *acunetix vulnerability,* kemudian melakukan evaluasi terhadap celah keamanan website Bazma dan hanya sebatas pengujian saja.

2. Metode dan Perancangan

2.1 Metode

Metode yang digunakan dalam penelitian ini adalah *action research*.

3.2 Perancangan Penetrasi



Gambar 1 Perancangan Penetrasi

Dari gambar diatas dapat dilihat bahwa awalnya mencari celah yang terbuka menggunakan *Acunetix Web Vulnerability*, penetrasi *ping* menggunakan *Net tools*, penetrasi menggunakan *DoSHTTTP 2.5* melakukan *flooding* pada website, penetrasi menggunakan *Digiblast 2* dengan mengirimkan paket data, penetrasi menggunakan *SynAttack flooding* pada *web server*, penetrasi menggunakan *Sql injection*, penetrasi menggunakan *Cross Site Scripting (XSS)*, dan penetrasi menggunakan *Arp Spoofing* melakukan pencegatan pengiriman data.

4 Hasil dan Pembahasan

4.1 Hasil

Setelah tahap demi tahap peneliti melakukan analisa dan uji coba yang dimulai dari tanggal 15 desember 2015 sampai dengan 23 desember 2016, dengan beberapa tools yaitu *Acunetix Web Vulnerability Scanner 9* yang digunakan untuk mencari informasi celah menunjukkan bahwa website bazma dalam level kerentanan *Low*, hal ini ditunjukkan dengan ditemukannya *web alerts* dengan kategori *Low* dan *informational* berdasarkan beberapa tingkatan *high*, *medium* dan *low* menghasilkan tingkatan celah keamanan yang tinggi. Dari hasil *Acunetix Web Vulnerability Scanner 9* ditemukan celah yang terdiri dari beberapa tingkatan diantaranya :

1. Tingkatan high dengan total nilai 17 celah yaitu terdiri dari diantaranya *Blind Sql Injection, Cross Site Scripting, jQuery cross site scripting, Slow HTTP Denial of Service Attack*.
2. Tingkatan medium dengan total nilai 22 celah yaitu *Apache httpOnly cookie disclosure, Directory listing, HTML form without CSRF protection, User credentials are sent in clear text.*
3. Tingkatan low dengan total nilai 16 celah yaitu *X-Frame-Options header missing, Options method is enabled, Session Cookie without Secure flag set, TRACE method is enabled.*

4.1.1 Ujicoba *Acunetix Web Vulnerability Scanner 9*

Buka program *Acunetix Web Vulnerability Scanner 9*, kemudian pada *menu start* – buka *Acunetix Web Vulnerability Scanner 9*, Masukkan alamat *website URL* http://10.53.1.12/webfungsi/bazma lalu *Scan single* website merupakan memindai satu website lanjutkan proses scanning port pada website Bazma, berikut ini tampilan hasil scanning port yang menampilkan lubang website Bazma sangat rentan.

Gambar 2 Hasil *Scaning Acunetix Web Vulnerability Scanner 9*

4.1.2 Ujicoba *Net Tools pinger*

Buka program *Net tools*, kemudian pada *menu start – network tools – ping*, lalu isi berapa kali ping contoh 1.000 kali, packet 64 lalu klik ping.

Gambar 3 Hasil *penetrasi* menggunakan *Net tools*

4.1.3 Ujicoba *DoSHTTP 2.5*

Buka program *DosHTTP*, tentukan *target URL* misal 10.53.1.12, tentukan *socket* 500, *request* 2500, lalu *start flood*.

Gambar 4 Hasil *Penetrasi* Menggunakan *DoSHTTP 2.5*

4.1.4 Ujicoba *DigiBlast 2*

Buka program *digiblaster*, tentukan *ip address* contoh 10.53.1.12, tentukan *port* 80, *time left* 100000, *delay* 100, *flood mode* pilih *TCP*, lalu pilih *flood*, lalu hasilnya target sukses di *flooding*.

Gambar 5 Hasil *Penetrasi* Menggunakan *DigiBlast 2*

4.1.5 Ujicoba *SynAttack*

Buka program *SynAttack*, isi target IP missal 10.53.1.12 pilih port 80

Gambar 6 Hasil *Penetrasi* Menggunakan *SynAttack*

4.1.6 Ujicoba *SQL Injection*

Sqlmap merupakan tools scanning teknik *SQL Injection* secara otomatis tergantung dari perintah si *attacker*. -u adalah perintah untuk membaca alamat target yang peneliti masukkan. *--dbms=mysql* merupakan perintah untuk melakukan *scanning* dengan aplikasi *database* pada target yaitu *mysql*.

Gambar 7 Output Dari Sqlmap

4.1.7 Ujicoba *Cross-Site Scripting (XSS)*

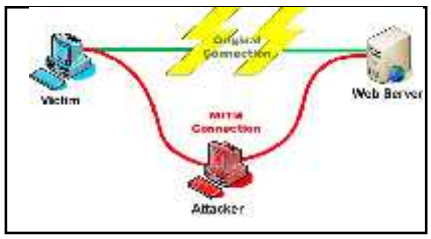
XSS digunakan dengan cara memasukkan kode HTML atau *client script code* lainnya ke *web*. Akibat serangan ini penyerang dapat mem-*bypass* keamanan di sisi klien, mendapatkan informasi sensitif, dan menyimpan aplikasi berbahaya. Skripnya <script>alert(“tes xss”);</script>

Gambar 8 *Form* di *inject* dengan *XSS*

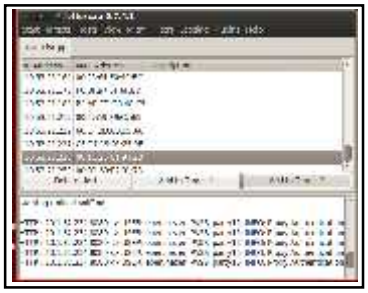
4.2 Hasil

4.2.1 Pengujian *Arp Spoofing*

Arp Spoofing adalah suatu teknik menyerang pada jaringan komputer lokal baik dengan media kabel atau *wireless*, yang memungkinkan penyerang bisa mengetahui *frames data* pada jaringan lokal atau melakukan modifikasi *traffic* atau bahkan menghentikan *traffic*.



Gambar 9 Ilustrasi *sniffing password* dengan *ettercap*



Gambar 9 Tampilan *username* dan *password* dari *proxy authentication*

5 Kesimpulan

Berdasarkan hasil penelitian maka dapat disimpulkan Bahwa keamanan website Bazma belum dapat dikatakan aman, hal ini di tunjukkan dengan masih adanya tingkat keamanan yang berada pada *level High* dengan ditemukannya *web alerts* berbahaya pada beberapa website Bazma Pertamina dan *level Medium* yang mengandung informasi sensitif, dan sehingga keamanan website Bazma Pertamina berhasil dapat penetrasi dan *server down*, dari sisi keamanan klien berhasil diserang bahkan penyusup berhasil masuk melalui admin dengan menyerang keamanan klien. Sehingga mendapatkan informasi-informasi sensitif website Bazma Pertamina tersebut.

.

Referensi

1. Siagian, H.P. 2014. Vulnerability Assesment Pada Web Server www.binadarma.ac.id Journal.
2. Metasari, dkk. 2014. *Analisis Keamanan Website di Universitas Muhammadiyah Surakarta*. Jurnal.