ANASLISIS KERENTANAN TERHADAP ANCAMAN SERANGAN PADA *WEBSITE* PDAM TIRTA MUSI PALEMBANG

Doda Saputra Ahad[1], Muhamad.Akbar[2], Maria Ulfa[3]

[1,2,3] Fakultas Ilmu Komputer Universitas Bina Darma
Jalan Jenderal Ahmad Yani No.12 Palembang
dodasaputra@gmail.com, muhamad.akbar@binadarma.ac.id, maria.ulfa@binadarma.ac.id,

At the moment the website is one of the media information that is growing very fast. In a *website* is not only the design and information that is overlooked but the security aspects as well as the vulnerability gap has an important role in a website. The need to determine the vulnerability of a website is required to protect data from damage and data loss, and of the irresponsible who want to access and change data. Another problem is includes protection from various attacks and interference from outside and inside. The method used in the action research is Action Research. To perform security analysis website, the software used is the website Acunetix vulnerability scanner, Netsparker and Nessus. The author knows a crack susceptibility / vulnerability anything contained

Keyword : Website, kerentanan website, Vulnerability, Acunetix, Netsparker, Nessus.

1. Pendahuluan

1.1 Latar Belakang

Web/Website merupakan sumber daya internet yang sangat populer dan dapat diguakan untuk memperoleh informasi, transaksi pembelian barang, diskusi, ataupun untuk keperluan lainnya. Sedangkan Hacking (Hack) merupakan suatu aktifitas mempelajari, menganalisis, memodifikasi, dan menyusup ke dalam sebuah sistem komputer baik untuk keuntungan maupun dimotivasi oleh tantangan. Jika kedua pengertian tersebut digabungkan, maka bisa ditarik kesimpulan bahwa Web-Hacking adalah suatu aktivitas mempelajari, menganalisis, memodifikasi, ataupun menyusup kedalam sebuah sistem komputer yang menggunakan protocol HTTP, yang mana file-file diletakkan kedalam sebuah kompter yang memiliki protocol tersebut (HTTP) yang disebut dengan istilah web server. Dari hasil wawancara dengan kepala unit bagian PDR (pengolahan data dan rekening) menyebutkan bahwa seringnya terjadi serangan terhadap situs web, dalam hal ini banyak attacker yang mencoba menyerang server

dengan cara menyisipkan file Sql Injection setelah sebelumnya melakukan serangan Ddos (Distributed Denial of Services) agar website tersebut down untuk beberapa waktu. Untuk menjaga situs web www.tirtamusi.com agar tetap berjalan sebagaimana mestinya serta mencegah gangguan dari pihak yang tidak bertanggung jawab, peneliti merasa perlu melakukan analisa pada situs web www.tirtamusi.com, untuk metode penelitian menggunakan metode action research dan dibantu tools analisis celah kerentanan dengan menggunakan Accunetic Web Vulnerability, Netsparker dan Nessus. Oleh karena itu peneliti tertarik untuk melakukan penelitian dengan judul "Analisis Kerentanan Terhadap Ancaman Serangan Pada Website PDAM Tirta Musi Palembang" terhadap sistem keamanan untuk melihat kerentanan atau Vulnerability yang ada.

2 Metodologi dan Perancangan

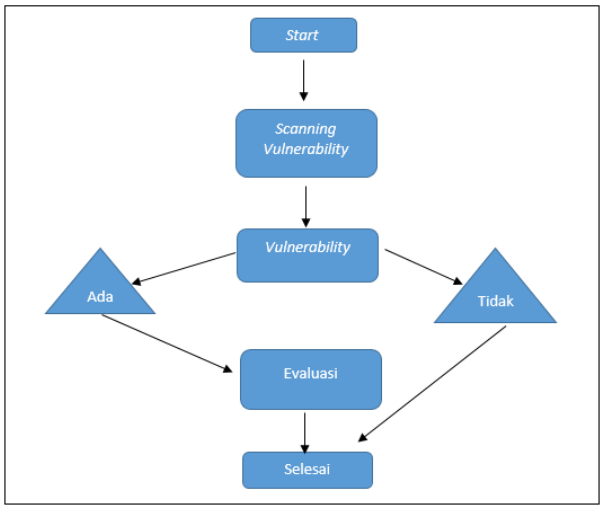
2.1 Metode

Dalam melakukan analisis disini peneliti mrnggunakan metode penelitian tindakan yaitu Action Research Menurut Jean Mcniff dan Jack WhiteHead (1988) ada lima tahapan dalam penelitian yang merupakan siklus dari action research, yaitu : Melakukan diagnosa (Diagnosing), Membuat rencana tindakan (Action Planning), Melakukan tindakan (Action Taking), Melakukan evaluasi (Evaluating), dan Pembelajaran (Learning).

2.2 Perancangan

(Diagnosing) > (Action Planning) > (Action Taking) > (Evaluating) > (Learning).

2.3 Diagram Alur Kerja



3 Hasil dan Pembahasan

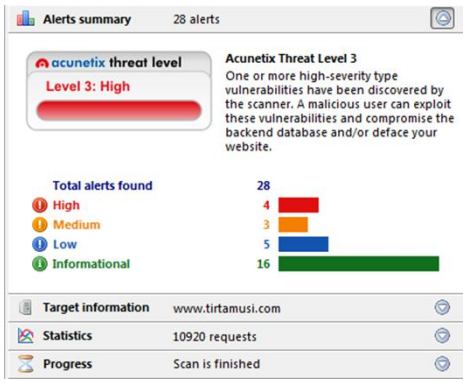
3.1 Hasil

Dari hasil penelitian yang dilakukan pada website PDAM Tirtamusi Palembang menggunakan 3 tools, yang pertama menggunakan Acunetic. Dari hasil scanning tersebut di dapatkanlah hasil bahwa Acunetic menemukan 28 jenis total alert yang terdiri dari 4 dengan jenis yang bertipe high, 3 medium, 5 low dan 16 informasi dengan kategori threat level High. Sedangkan tools yang kedua yaitu menggunakan Netsparker. Scanning yang dilakukan menggunakan tools tersebut maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi. Dan untuk tools ketiga yaitu menggunakan Nessus, dari hasil scanning yang dilakukan maka didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.

3.2 Pembahasan

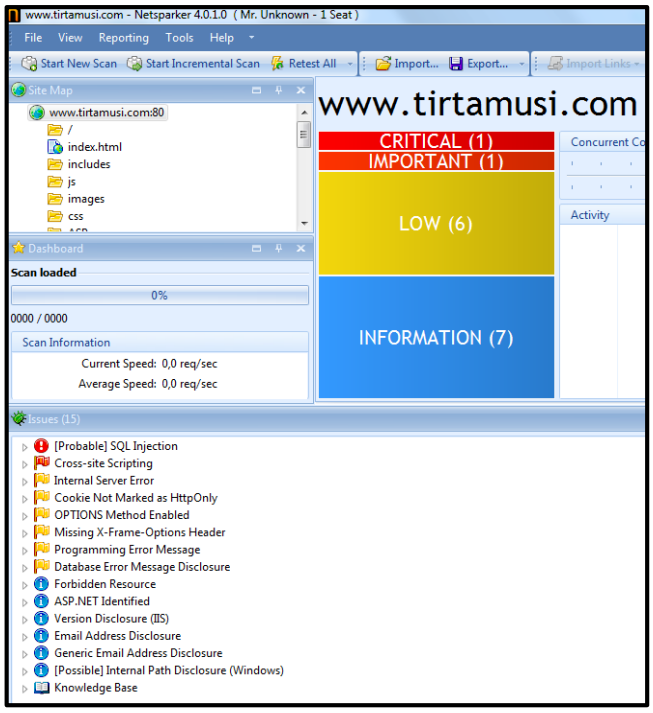
3.2.1 Scanning www.tirtamusi.com Dengan *Acunetic*

Dari hasil *scanning* menggunakan *Acunetic*, didapatkan 28 total *alert* yang terdiri dari 4 dengan jenis yang bertipe *high*, 3 *medium*, 5 *low* dan 16 informasi dengan kategori *threat level High*.



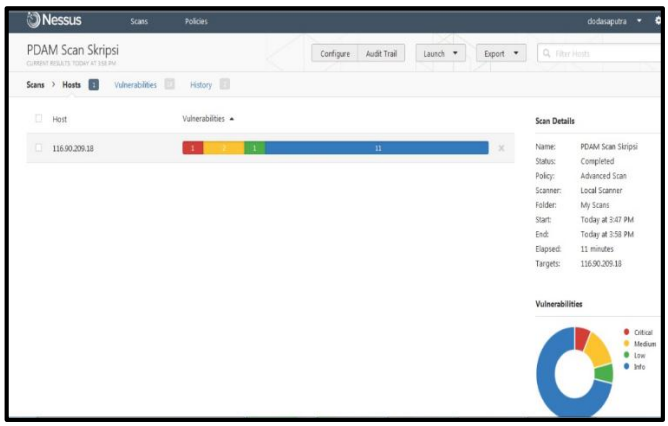
3.2.2 Scanning menggunakan *Netsparker*

Dari hasil scanning menggunakan Netsparker maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi.



3.2.3 Scanning Menggunakan *Nessus*

Dari hasil scanning menggunakan Nessus maka didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.



4 Kesimpulan

hasil simpulan sebagai berikut :

1. Dari hasil scanning yang dilakukan dengan menggunakan tools Acunetic di dapatkanlah hasil bahwa Acunetic menemukan 28 jenis total alert yang terdiri dari 4 dengan jenis yang bertipe high, 3 medium, 5 low dan 16 informasi dengan kategori threat level High.

2. Untuk hasil scanning yang telah dilakukan sebelumya dengan mengguanakan tools kedua yaitu Netsparker maka didapatlah 15 alert yang terdiri dari 1 jenis tipe critical, 1 jenis yang bertipe important, 6 low dan 7 yang bertipe informasi.

3. Sementara untuk tools yang terakhir dengan menggunakan aplikasi Nessus didapatkanlah hasil dengan total 15 alert yang terdiri dari 1 jenis tipe critical, 2 jenis yang bertipe medium, 1 low dan 11 yang berjenis informasi.

4. Hasil penelitian ini menunjukan bahwa masih banyak terdapat celah yang ada pada website www.tirtamusi.com yang bertipe High ataupun Critical yang memerlukan perhatian khusus, sementara untuk kerentanan lainnya dengan kategori low dan informasi juga tidak dapat dikesampingkan karena dapat mempermudah hacker untuk menembus sistem dari server itu sendiri.

Daftar Pustaka

1 Daniel, Muhammad Ilham dkk (2015). Evaluasi Celah Keamanan Web Server pada LPSE Kota Palembang. Diakses 08 November 2015, dari : http://eprints.binadarma.ac.id/2416/1/1508.06069.pdf

2 FAIR-ISO/IEC 27005 COOKBOOK. (2010). Implementing a vulnerability management process. SANS Institute InfoSec Reading Room.

3 Jasman (2015). Panduan Praktis WEB Hacking dari Subkultural Programmer. Yogyakarta : ANDI.

4 Matthew B. Miles & A. Michael Huberman (1994). Qulitative Data Anlysis. : Sage Publication : United Staten of America.

5 McNiff Jean & Jack Whitehead (1988). Action Research : Principles and Practice. London and New York : RoutledgeFalmer.

6 Santoto, Kodrat Iman (2009). Keamanan sistem informsi Berbasis Web Di Fakultas Teknik Universitas Diponegoro. Diakses 27 November 2015, dari : http://eprints.undip.ac.id/5501/1/Analisis_Keamanan_Sistem_Informasi_Akademik_Berbasis_Web_di_Fakultas_Teknik_Universitas_Diponegoro.pdf.

7 Sofana, Iwan (2013). Membangun Jaringan Komputer. Bandung : Informatika Bandung

8 Wikipedia. CVSS (Common Vulnerability Scoring System). Diakses pada 25 November 2015 Dari : https://en.wikipedia.org/wiki/CVSS

9 Wikipedia. Web Bacon. Diakses pada 10 November 2015 dari : https://en.wikipedia.org/wiki/Web_beacon.

10 Wikipedia. Web server. Diakses pada 27 November 2015 Dari : https://id.wikipedia.org/wiki/Server_web

11 Wikipedia. Analysis. Diakses pada 29 November 2015 Dari : https://en.wikipedia.org/wiki/Analysis