VULNERABILITY ASSESMENT UNTUK MENINGKATKAN KUALITAS KEMANAN *WEB*

Mira Orisa [1], Michael Ardita [2]
[1] Teknik Infomatika, Institut Teknologi Nasional Malang
[2] Teknik Elektro, Institut Teknologi Nasional Malang
mir4orisa@gmail.com

ABSTRAK

Aplikasi *web* sangat rentan terhadap serangan seperti sql injection, denial of service, dan berbagai macam bentuk malware lainnya. Kerentanan terjadi karena Banyak aplikasi *web* dirancang dari awal tanpa memperhitungkan masalah keamanan. Biasanya, aplikasi dirancang oleh orang yang tidak berpengalaman dalam bidang keamanan *web*. Sehingga memungkinkan banyak celah keamanan dalam *web*site mereka. Metode vulnerability *assessment* ini adalah cara terbaik saat ini untuk membantu pihak-pihak tertentu dalam menjaga keamanan aplikasi *web* mereka. Dengan melakukan vulneribility *assessment* dapat mengidentifikasi macam-macam celah yang memungkinkan masuknya serangan. Metode ini dapat membantu pihak-pihak tertentu untuk mengambil tindakan pencegahan terhadap serangan atau suatu kerusakan akibat kejahatan dunia maya. *Network mapping* atau dikenal dengan Nmap dapat membantu para master *web* untuk melakukan *vulnerability assessment*. Pada penelitian ini menggunakan OS kali Linux untuk menjalankan Nmap. *Host* target yang di uji mendukung metode *POST, OPTIONS, GET, HEAD.* Hasil pengujian VA dengan nmap juga menunjukkan bahwa target tersebut terdeteksi sebagai HTTP open proxy. Kemudian target yabg diuji tidak terdeteksi *cross site scripting.* Dan *hos*t target juga tidak terdeteksi *sql injection.*

Keyword : *assessment*,keamanan,vulnerability,*web*, Nmap.

1. PENDAHULUAN

Perkembangan teknologi internet dan sistem informasi saat ini telah meningkatkan jumlah pengguna aplikasi *web*. Setiap kali seseorang terkoneksi dengan internet maka saat itu juga mereka terkoneksi pada sebuah *website*. Banyak sekali dijumpai kerentanan pada aplikasi *web*. Kerentanan atau biasa disebut *vulneribily* mengundang para *attacker* untuk melakukan serangan dengan tujuan illegal. Serangan yang diluncurkan biasanya menyerang bagian *syntax* dan semantic dari aplikasi *web*. Berbagai macam cara dilakukan oleh *attacker* seperti menggunakan media sosial atau panggilan telepon untuk menipu orang agar mendapatkan akses ke informasi sensitive seseorang.

Untuk Mengantisifasi serangan tersebut para pengembang *web* harus melakukan *vulnerability assessment*. *Vulnerability assessment* dapat mendefinisikan, mengidentifikasi, mengelompokkan dan memprioritaskan kerentanan dalam sistem *web*. *Vulnerability* pada aplikasi *web* dapat di deteksi menggunakan *tool* atau *software* tertentu. Menurut referensi [1], scanning pada aplikasi *web* bertindak sebagai pelengkap dan menguji kinerja serangan pada target. Contohnya *Payment Card Industry Data Security Standart (PCI DSS) versi 2.0,* sekarang mewajibkan semua pedagang yang menerima kartu pembayaran untuk lulus pemindaian untuk *vulnerability* pada aplikasi *web*.

Ashikali Hasan dan Divyakant Meva pada tahun 2018 melakukan penelitian untuk menghilangkan berbagai jenis ancaman keamanan pada aplikasi *web* dengan metode *vulnerability assessment* dan penetration *testing*. Sehingga ancaman seperti *SQL injection, cross site scripting, local file inclusion* and *remote file inclusion* dapat di hilangkan menggunakan sebuah *tool* yaitu proses VAPT [2]. Dalam Penelitian Hilal Afrih Juhad dan kawan-kawan, pengguna sebuah *website* harus memiliki kesadaran akan pentingnnya perlindungan terhadap informasi yang ada dalam *website* seperti menentukan hak akses, mengidentifikasi penggunjung *website*. Karena jika tidak maka seorang *attacker* akan mengambil keuntungan dari *vulnerability* yang ada. Ari marta tania dan kawan-kawan pada tahun 2018 menggunakan sebuah *tool* bernama CVSS (*Common Vulnerability Scoring System*) versi 2 untuk mengkomunikasikan karakteristik dan dampak yang ditimbulkan *vulnerability* [3].

Pengetahuan tentang aspek keamanan sangat penting diketahui oleh seorang master *web*. Dengan metode *vulnerability assessment* dapat membantu mendeteksi kerentanan dalam sebuah aplikasi *web*. Hasil dari *assessment* tersebut menjadi pertimbangan bagi master *web* untuk mengambil tindakan pencegahan serta mengetahui kinerja serangan saat melakukan serangan.

2. TINJAUAN PUSTAKA

2.1. Penelitian Terkait

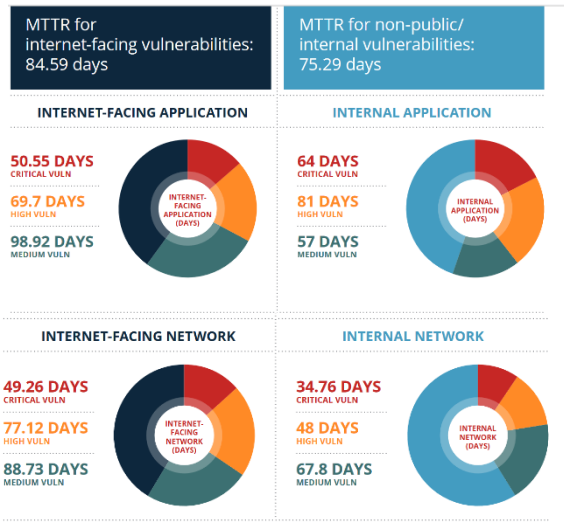
Ari Marta Tania dan kawan-kawan mendeteksi beberapa sserangan seperti *brute force attack* dan *denial of service*, *sniffing* dengan menggunakan beberapa *tool* diantaranya *Wpscan, exploit, metasploit-Framework dan THC-Hydra, slowlori,*

webscarab [4]. Imam Riadi dan kawan-kawan menggunakan *tool owasp* untuk menganalisis keamanan *website open journal system* (OJS) versi 2.4.7 Hasil dari *assessment* menyatakan bahwa OJS versi 2.4.7 memiliki banyak *vulnerability* [5]. Selain itu tool yang dapat melakukan penetrasi diantaranya W3af, Havij, Fimap, Metasploit, Kali linux, Acunetix, dan Nexpose [2]. Pada penelitian yang dilakukan oleh Said F. Aboelfotoh dan Noha A. Hikal menggunakan tool nmap sebagai tool untuk assessment jaringan [6].

2.2. B. Vulnerability Assessment

Vulnerability assessment digunakan untuk melakukan pengujian pada *point-point* yang berpotensial masuknya serangan. Selain itu juga mengidentifikasi masa berlakunya versi sebuah *software*, mengidentifikasi port-port yang terbuka, dan dapat juga mengidentifikasi aplikasi apa saja yang sedang berjalan. *Vulnerability assessment* digunakan untuk mendeteksi kelemahan dalam jaringan [6].

MTTR (*mean time to remediate*) merupakan total rata-rata di seluruh aplikasi *web* dan kerentanan infrastruktur, ditunjukkan pada Gambar 1 [7]



Gambar 1. Mean time to remediate
(Eoin Keary. Rdgescan" Fullstack Vulnerability Management")

Besar risiko kritis Internet dalam menghadapi kerentanan aplikasi *web* hampir sama dengan besar risiko kritis Internet dalam menghadapi kerentanan jaringan yaitu masing-masing 50,55 hari dan 49,26 hari.

2.3. C. Network Mapper

Network Mapper atau dikenal dengan nmap. Namap lebih optimal bekerja di system operasi Linux dari pada windows. Nmap merupakan *tool* yang biasa digunakan untuk melakukan audit keamanan jaringan dan melakukan eksplorasi jaringan. Namap merupakan tool yang bersifat *open source*. Aplikasi bawaan dari nmap seperti: [8]

1. Zenmap yang merupakan nmap versi GUI
2. Ndiff merupakan *tool* yang diperuntukkan untuk membandingkan hasil scanning
3. Nping merupakan *tool* untuk analisis paket data
4. Ncrak merupakan *tool* yang digunakan untuk melakukan *brute-force*
5. Ncat merupakan *tool* untuk *read* dan *write* data pada jaringan
6. NSE merupakan fitur dimana anda dapat menulis *script* sendiri untuk melakukan scanning.

Namap dapat ampuh menemukan *vulnerability* dalam sebuah jaringan dan selain itu nmap juga merupakan *tool* yang bisa melakukan pengelolaan server. Namap bisa melakukan scanning jaringan dengan teknik [8]:

1. Port scanning
   Teknik port scanning ini bertujuan memindai port host tetentu apakah sedang terbuka. Jika port suatu aplikasi dalam jaringan computer terbuka, maka siapaun akan bisa masuk dan dapat mengakses aplikasi tersebut. Selain dapat melihat status terbuka atau tertutup sebuah port dalam jaringan, Nmap juga bisa melihat status lainnya seperti: filtered, unfiltered, open/filtered, dan closed/filtered.
2. Ping scanning
   Teknik ping scanning berfungsi untuk mengetahui apakah host sedang aktif atau tidak di jaringan. Teknik ini diantaranya [8]:
3. Ping scanning TCP SYN
   Ketika ada firewall yang memblokir permintaan pin scan yang ber flag –sp untuk meminta respons dari host yang ada didalam jaringan, sehingga Nmap tidak bisa melihat host aktif maka digunakan pin scan TCP SYN.
4. Ping scan TCP ACK
   Ping scan TCP ACK digunakan jika teknik ping scan TCP SYN diblokir oleh firewall.
5. Ping scan UDP
   Teknik ini bisa digunakan jika dua teknik diatas diblokir oleh firewall.ini merupakan teknik alternative.
6. Ping scan ICMP
   Penggunaan teknik ini saat pada hak akses root. Teknik ping scan ICMP juga masih bisa di blokir oleh firewall.
7. Ping scan IP
   Pada teknik ini Nmap membutuhkan hak akses root. Adapun protocol IP yang dimaksud adalah IGMP, IP-in-IP dan ICMP. Tabel 2 menunjukkan daftar nomer pada protocol pin scan IP

Tabel 2. Daftar nomer protocol ping scan IP

Nomor	Protokol
1	ICMP
17	UDP
6	TCP
2	IGMP
4	IP-in-IP
132	SCTP

(sumber: Abdullah,2016)

Adapun celah vulnerability atau kerentanan *web* yang sering dimanfaatkan oleh para hacker untuk mengencarkan serangan, diantaranya [9]:

1. HTTP Header
   HTTP header bisa menjadi celah kerentanan karena dia dikirim oleh client yang tidak sepenuhnya bisa dipercaya.
2. HTML Injection
   Injeksi HTML bisa menjadi jalan masuknya serangan dari hacker
3. Pengunaan metode GET
   Ada dua metode pengiriman yaitu POST dan GET. Jika master *web* menggunkan metode GET maka data yang dikirim akan terlihat di URL. Para hacker tentu akan memanfaatkan celah ini dengan merubah halaman atau membuat *script* tertentu untuk keuntungan dirinya.
4. Cookie
   Hacker biasanya memanfaatkan cookie untuk masuk kehalaman target tanpa melalui login terlebih dahulu. Creaker bisa mencuri *username* dan *password* pengguna resmi.
5. Shell injection
   Para hacker menjalankan perintah system operasi pada *web*. seperti perintah “ping & dir c:”
6. Hacking perintah include
   Perintah include dalam pemprograman php terkadang bisa menjadi celah masuknya serangan hacker. Hacker bisa saja membuka file.inc

Sebagian orang akan selalu mengaitkan antara penetration testing dengan vulnerability *assessment*. Adahal ada perbedaannya antara penetration testing dan vulnerability *assessment*, seperti ditunjukkan pada Tabel 1[10].

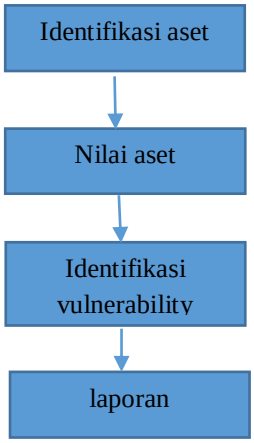
Tabel 1. Perbedaan antara penetration testing dan vulnerability *assessment*

Penetration testing	Vulnerability *assessment*
Identifikasi beberapa celah keamanan	Identifikasi semua celah keamanan
Pendekatan risiko IT	Pendekatan bisnis dan risiko IT
Pembuktian secara teknis	Pembuktian secara teori

(sumber: Girindro pringgo Digdo,2017)

3. METODELOGI

Metode penelitian terdiri dari beberapa tahap yaitu mengidentifikasi asset, menilai asset, menidentifikasi kerentannan, melaporkannya. Seperti terlihat pada Gambar 2.

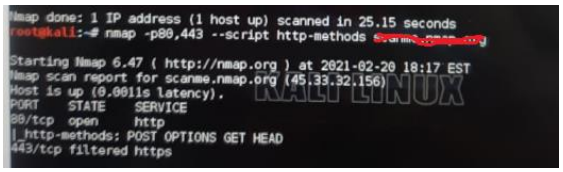


Gambar 2. Metode vulnerability assessment [4]

Vulnerablity *assessment* dilakukan dengan menggunakan *Nmap Scripting Engine (NSE)*. Seperti yang ditunjukkan pada Gambar 2, dimana akan dilakukan pengecekkan terhadap *malware/web phising* dan *sql injection*. Kategori di *Nmap Scripting Engine (NSE)* ini memiliki fungsi nya masing-masing. *Nmap Scripting Engine (NSE)* dapat dipergunakan oleh master *web* sebagai tool untuk vulnerability *assessment*.

4. HASIL DAN PEMBAHASAN

Hasil pengujian *web server scanning* antara lain: mendeteksi metode pada protocol HTTP dengan perintah $nmap –p80,443 –script http-methods <target>. Pada host target tersebut mendukung metode *POST, OPTIONS, GET, HEAD*.

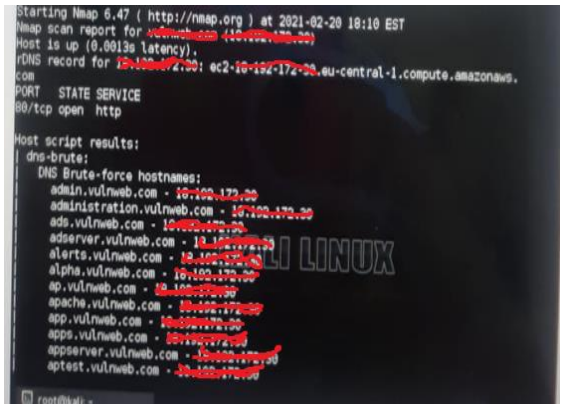


Gambar 3. Deteksi metode protocol HTTP

Hasil untuk kategori script NSE nmap $nmap –p8080 –script http-open-proxy <target>, menunjukkan bahwa target tersebut terdeteksi sebagai HTTP open proxy.

Gambar 4. Scanning open proxy HTTP

Hasil untuk kategori script NSE nmap $ nmap –p 80 –script dns-brute.nse.nse <target>, untuk menemukan dns yang valid.

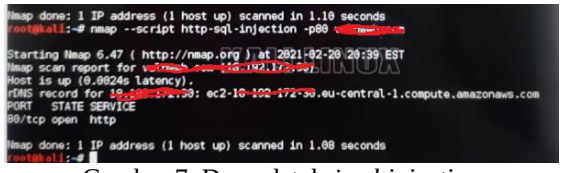


Gambar 5. Dns Brute

Hasil untuk kategori script NSE nmap $ nmap –script http-unsafe-output-escaping –p80 <target>. Saat dilakukan scanning tersebut pada host target tidak terdeteksi *cross site scripting*.

Gambar 6. Dmendeteksi *cross site scripting*

Hasil untuk kategori script NSE nmap $ nmap –script http-aql-injection –p80 <target>. Saat dilakukan scanning tersebut pada host target tidak terdeteksi *sql injection.*



Gambar 7. Dmendeteksi *sql injection*

5. SIMPULAN

Network mapping atau Nmap merupakan tool yang mampu melalukan vulnerability *assessment* untuk melakukan pengecekan masalah *malware/web phising*, dapat melakukan pengecekan terhadap serangan denial of service, dapat menemukan vulnerability xss pada file php, dan dapat menemukan vulnerability terhadap serangan sql-injection. Pada penelitian ini, *host* target yang di uji mendukung metode *POST, OPTIONS, GET, HEAD.* Menunjukkan bahwa target tersebut terdeteksi sebagai HTTP open proxy. Tidak terdeteksi *cross site scripting.* Pada host target tidak terdeteksi *sql injection.*

DAFTAR PUSTAKA

[1] Shema.M.2011.*Web* Application Security for Dummies.A john wiley and Sons, Ltd, Publication

[2] Hasan.A, $ D. Meva. 2018. *Web* application Safety Penetration Testing.Special Issue based on proceeding of 4th International Conference on Cyber Security (ICCS).

[3] Juhad. H. A, R. Isnanto, E. D. 2016.Widianto. Analisis Keamanan pada Aplikasi Her-registrasi Online Mahasiswa Universitas Diponegoro.Jurnal Teknologi dan Sistem Komputer. 4(3). 2016. 479-484. DOI:10.1470/jtsiskom.4.3.2016.479-484

[4] Tania. A. M., D. Setiyadi, & F. N. Khasanah. 2018. Keamanan *Web*site Menggunakan Vulnerability *Assessment*. Informatics for Educator and Professionals. vol.2.no.2. 2018. E_ISSN: 2548-3412

[5] Riadi. I, A. Yudhana, & Yunanri. 2018. Analisis Keamanan *Web*site Open Journal System Menggunakan Metode Vulnerability *Assessment*. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK). vol.7.no.4. 2020. 853-860. E-ISSN: 2528-6579

[6] Aboelfotoh. S. F, & N. A. Hikal. A. 2020. Review of Cyber-Security Measuring and *Assessment* Methods for Modern Enterprise. International Journal on Informatics Visualization. vol.3.no.2. 2019. E-ISSN: 2549-9904. ISSN: 2549-9610

[7] Keary. E. 2020. Rdgescan," Fullstack Vulnerability Management".

[8] Abdullah.2016. Kung Fu Hacking dengan Nmap. Penerbit: ANDI. Yogyakarta.

[9] S'to. 2009. *Web* Hacking: Scenario & Demo.Penerbit: jasakom. Edisi revisi dari buku best seller SIH Recoded.

[10] Pringgo. D. G. 2017. panduan audit keamanan computer bagi pemula. penerbit PT.elex media komputindo.