SANTIKA *Seminar Nasional Informatika Bela Negara (SANTIKA)*
ISSN (Online) 2747-0563
Volume 2 Tahun 2021

Analisa Keamanan Website Menggunakan Metode Footprinting dan Vulnerability Scanning pada Website Kampus

Muhammad Fatkhurozzi[1]
[1]Fakultas Teknik, Universitas Pancasila, Depok, Indonesia
[1]fatkhurozzi16@gmail.com
*Corresponding author email: fatkhurozzi16@gmail.com

Abstrak—Website adalah sebuah halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama aktivitas internet pada suatu device tersambung , keamanan informasi informasi pada sutau website adalah hal terpenting saat ini, tidak terkecuali pada website institute perguruan tinggi yang menyajikan informasi penting tentang suatu institute . masalah tersebut penting karena jika informasi diakes oleh orang yang tidak bertanggung jawab.

Metode penelitian yang digunakan dalam penelitian ini adalah metode Ethical Hacking yang menitikberatkan pada teknik footprinting dan vulnerability scanning dengan hanya menguji serangan pasif. Hasil penelitian ini telah menemukan informasi terkait website target (website lembaga pendidikan di salah satu kota di Indonesia) dan beberapa peringatan kerentanan setelah dilakukan pengujian pemindaian kerentanan dengan tingkat risiko tinggi hingga rendah sehingga peneliti merekomendasikan perbaikan kerentanan untuk meminimalkan. lubang keamanan yang dimanfaatkan oleh para peretas.

Kata Kunci— ***Website, Keamanan, Network Security Footprinting, Vulnerability***

I. PENDAHULUAN

Seiring semakin berkembang nya teknologi system informasi dikalangan masyarakat, berkembang pula system yang dapat memudahkan masyarakat untuk mengakses dan mencari suatu informasi dalam bentuk sebuah website. Teknologi informadi menjadi salah satu peran penting dalam suatu aktivitas perusahaan, organisasi untuk mendukung kinerja dan aktivitas . namun dalam pengelolaan IT keamanan suatu website dalah hal yang sangat penting.

Resiko keamanan menjadi salah satu hal yang berada pada urutann terakhir dalam hal – hal yang dianggap penting. Dan apabilla menggangu performa seringkali di kurangi . hal itu berbanding terbalik dengan semakin banyak nya celah yang keamanan dari website tersebut. [4]

II. TEORI PENDUKUNG

1. Keamanan Jaringan

Keamanan jaringan tidak ada yang benar benar aman karena sifat jaringan yang melakukan sebuah komunikasi. Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaan dan mengantisipasi ketika jaringan dapat ditembus. [2]

2. Hacking

Hacking komputer melibatkan beberapa tingkat pelanggaran atas sebuah privasi dan melanggar keamanan jaringan. Dampak dari sebuah kegiatan hacking tersebut bervariasi dari yang sekadar ingin tahu sampai pada kegiatan ilegal yang dapat merusak dan bahkan sampai menghilangkan sebuah file , webste ataupun perangkat lunak . Namun, cukup banyak perusahaan besar seringkali menyewa tim hacker untuk menyelidiki celah keamanan jaringan yang dimiliki pada sutau instansi . [2]

3. Footprintig

Teknik footprinting adalah Footprinting adalah kegiatan mengumpulkan data – data atau informasi yang ada pada terkait dari target yang akan di lihat. Pada permasalahan disini aplikasi yang akan di gunakan adalah CMD (Command prompt), Zenmap, dan whois domain

4. Vulnerability Scanning

Vulnerability scanning adalah kegiatan proses memperoleh informasi vulnerability network dengan memanfaatkan berbagai tools network scanning dan vulnerability scanner, seperti port yang terbuka , bugs aplikasi dan mengetahui serangan - serangan yang akan terjadi terhadap kerentaan website yang ada, yang akan berdampak cukup buruk apabila terjadi.

Tipe untuk melakukan suatu vulnerability testing ada 2 macam [2]. Kedua macam itu antara lain:

A. External Testing.

External Testing adalah testing dengan melakukan analisa terhadap informasi public yang tersedia, network enumeration phase, dan analisa keamanan devices yang digunakan. [2]

ISSN (Online) 2747-0563
Volume 2 Tahun 2021

B. Internal Testing.

Internal Testing adalah testing yang akan menampilkan jumlah network access points yang mewakili beberapa logical dan physical segment.[2]

Ada beberapa metode untuk melakukan Vulnerability testing yang bisa digunakan [2], antara lain:

- Passive Vulnerability testing.

  Dalam hal ini yang dilakukan adalah melakukan pemetaan dan pengujian terhadap kontrol yang ada didalam web application, login, dan konfigurasinya, sehingga dapat memetakan target sistem. [2]
- Active Vulnerability testing.

  Active Vulnerability testing merupakan melakukan kegiatan aktif dalam pengujian terhadap keamanan sistem dengan melakukan manipulasi input, pengambilan hak akses, dan melakukan pengujian terhadap vulnerability yang sudah ada. [2]
- Aggressive Vulnerability testing.

  Aggressive Vulnerability testing adalah melakukan eksploitasi terhadap vulnerability, melakukan reverse enginering terhadap software dan system, menanamkan backdoor, mengunduh code, dan mencoba mengambil alih finansial dan informasi yang ada di server. [2]

III. METEDOLOGI PENELITIAN

Penelitian ini akan dilakukan melakukan metode ethical hacking dimana nantinya akan di fokus kan pada tahapan footprinting dan vulnerability scanning . adapun objek / target yang akan menjadi bahan penelitian adalah website Siak Universitas pancasila.

Adapun skenario pengujian dan analisis sistem sebagai berikut :

1. Penentuan batasan penelitian

   Batasan penelitian dibutuhkan supaya vulnerabilty assessment tidak terlalu luas, sehingga tidak melibatkan hal – hal yang tidak diperlukan. [5]

2. Footprinting

   Pada tahap ini akan dilkakukan kegiatan mengumpulkan data – data atau informasi yang ada pada terkait dari target yang akan di lihat.

3. Vulnerability scanning

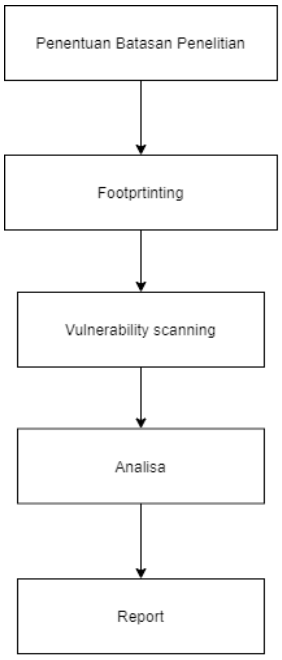
   Pada tahapan proses ini akan dilakukan pengumpulan informasi vulnerability network dengan memanfaatkan berbagai tools network scanning dan vulnerability scanner, seperti port yang terbuka , bugs aplikasi dan mengetahui serangan - serangan yang akan terjadi terhadap kerentaan website yang ada, yang akan berdampak cukup buruk apabila terjadi.

4. Analisa

   Pada tahapan akan melakukan proses analisa terhadap informasi–informasi vulnerability yang ditemukan setelah melakukan scanning terhadap target dengan beberapa tools serta memberi rekomendasi bagaimana memperbaiki dan menutupi vulnerability yang ditemukan pada proses scanning.

5. Report

   Pada tahapan ini dilakukan tahap dokumentasi terhadap analisa yang telah dilakukan.



Gbr. 1 Skenario Pengujian dan Analisis Sistem

IV. PEMBAHASAN DAN HASIL PENGUJIAN

Pada tahap ini dilakukan pengujian website dengan menggunakan 2 teknik yaitu dengan metode footprinting dan vulnerability scanning

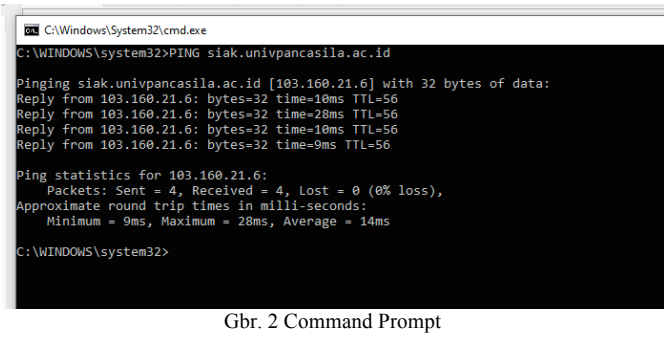
1. Hasil pengujian dengan metode teknik footprinting

   Teknik footprinting adalah Footprinting adalah kegiatan mengumpulkan data – data atau informasi yang ada pada terkait dari target yang akan di lihat. Pada permasalahan disini aplikasi yang akan di gunakan adalah CMD (Command prompt), Zenmap, dan whois domain

   a. CMD (Command prompt)

      Tahap ini melakukan PING pada cmd untuk mengetahui IP Server Dari website tersebut

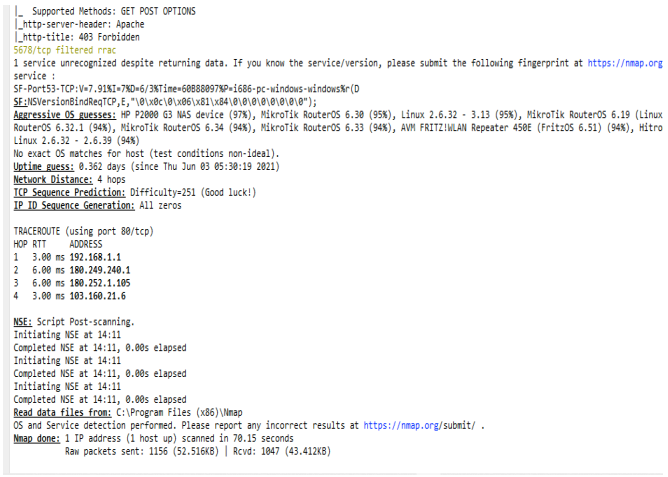
ISSN (Online) 2747-0563
Volume 2 Tahun 2021



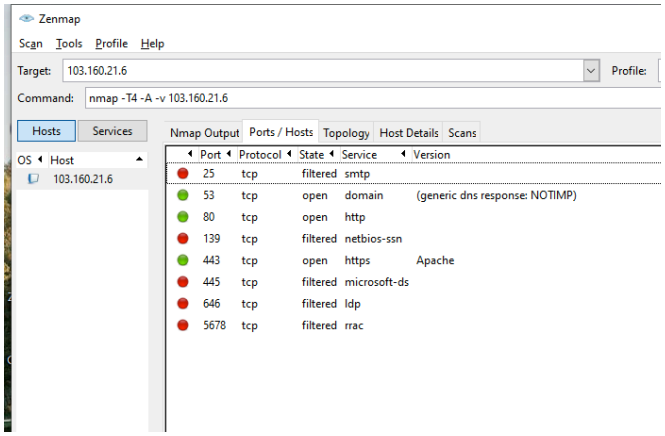
Gbr. 2 Command Prompt

Dari hasil gambar diatas pada CMD , dengan perintah PING siak.univpancasila.ac.id menemukan IP Sever yaitu (103.160.21.6)

b. Zenmap



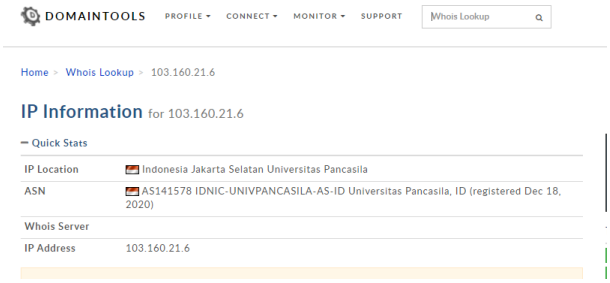
Gbr. 3 Zenmap



Gbr. 4 Zenmap

Dari hasil gambar di atas pada zenmap , dengan command perintah -T4 -A -v 103.160.21.6 , aplikasi zenmap dapat menemukan beberapa informasi webstie tersebut , yaitu antara lain operating system , tracetoute, dan bebrapa port yang terbuka

c. Whois domain



Gbr. 5 Whois Domoin

Dari hasil gambar di atas website whois.domain , dapat menemukan beberapa informasi , yaitu nama dan lokasi website tersebut.

TABEL I
HASIL PENGUJIAN TEKNIK FOOTPRINTING.

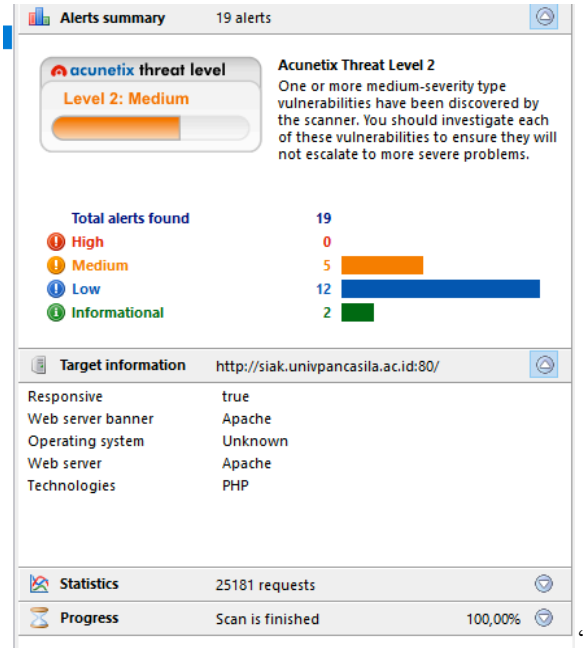
NO	Tools Footprinting & Information Gathering	Informasi yang ditemukan target
1	CMD (Ping)	IP Server
2	Zenmap	Operating system (OS) version
		Port - port yang terbuka
		Traceroute
3	Whois	Nama domain
		Alamat IP
		Lokasi server

2. Hasil Pengujian dengan metode vulnerability scanning

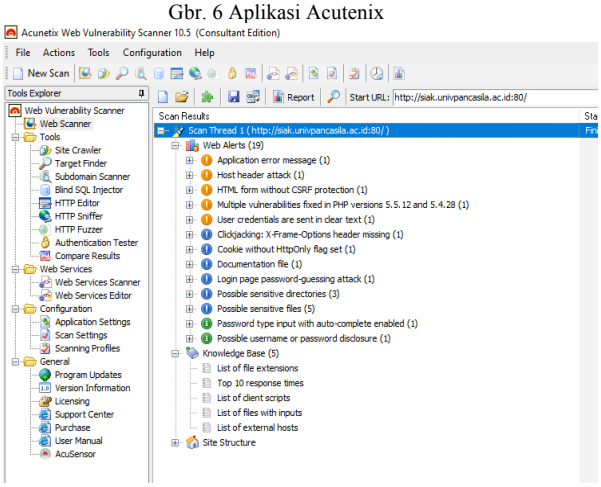
Vulnerability scanning adalah kegiatan proses memperoleh informasi vulnerability network dengan memanfaatkan berbagai tools network scanning dan vulnerability scanner, seperti port yang terbuka , bugs aplikasi dan mengetahui serangan - serangan yang akan terjadi terhadap kerentaan website yang ada, yang akan berdampak cukup buruk apabila terjadi. Pada tahap ini menggunakan aplikasi acutenix

ISSN (Online) 2747-0563
Volume 2 Tahun 2021

Hail pengujian dengan aplikasi acutenix:



Gbr. 6 Aplikasi Acutenix



Gbr. 7 Aplikasi Acutenix

Dari hasil gambar di atas pada aplikasi web vulnerabilty terdapat 3 kategori high risk alert sebagai acuan dalam menentukan terget maksimum pada resiko untuk hacking dan pencurian data . adapun rincian vulnerability yang ditemukan yaitu 5 medium risk level dan 12 low risk level.

TABEL II
HASIL PENGUJIAN VULNERABILITY SCANNING

NO	Vulnerability Scanner	Alert	Risk Level
1	Acutenix	Application error message	Medium
		Host header attack	Medium
		HTML form without CSRF protection	Medium
		Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28	Medium
		User credentials are sent in clear text	Medium
		Clickjacking: X-Frame-Options header missing	Low
		Cookie without HttpOnly flag set	Low
		Documentation file	Low
		Login page password-guessing attack	Low
		Possible sensitive directories	Low
		Possible sensitive file	Low

V. KESIMPULAN

Pada website target ditemukan celah keamanan dengan alert risk level medum hingga low yaitu , Application error message (Medium), Host header attack (Medium), HTML form without CSRF protection (Medium), Multiple vulnerabilities fixed in PHP (Medium), User credentials are sent in clear text (Medium), Clickjacking: X-Frame-Options header missing (Low), Cookie without HttpOnly flag set (Low), Documentation file (Low), Login page password-guessing attack (Low), Possible sensitive directories (Low), Possible sensitive files (Low)

Dengan ditemukan beberapa celah maka sebaiknya dilakukan perbaikan pada website sehingga tidak ditemukan lagi celah – celah yang akan merugikan website.

REFERENSI

[1] Angi, D. C., Noertjahyana, A., & Andjarwirawan, J. (2016). Vulnerability Mapping pada Jaringan Komputer Di Universitas X. *Jurnal Ilmiah Vol 3, No 2*, 1-7.

[2] Harjowinoto, D., A. N., & Andjarwirawan, J. (2016). Vulnerability Testing pada Sistem Administrasi Rumah Sakit X. *JURNAL INFRA VOL 1 NO 4*, 1-6.

[3] Riadi, I., Yudhana, A., & Yunanri.W. (2018). ANALISIS KEAMANAN WEBSITE OPEN JOURNAL SYSTEM MENGGUNAKAN METODE VULNERABILITY ASSESSMENT. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) Vol. 7 No. 4*, 853-860.

[4] Suryayusra, Solikin, I., & Ulfa, M. (2017). PENERAPAN SISTEM KEAMANAN JARINGAN SMK NEGERI 1. *MATRIK Vol.19 No.3*, 197-206.

[5] Wibowo, F., Harjono, & Wicaksono, A. P. (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. *JURNAL INFORMATIKA, Vol.6 No. 2*, 212-21