Company profile website security analysis using issaf method

Muhammad Nur Kamil Al Mubaroq, Esi Putri Silmina, Arizona Firdonsyah

Program Studi Teknologi Informasi, Fakultas Sains dan Teknologi, Universitas 'Aaisyiyah Yogyakarta
*Email: mpan01421@gmail.com

Abstrak

Website didikninithowok.id menampilkan informasi terkait profil, informasi Sanggar Tari Didik Nini Thowok. Pembuatan *Website* tidak hanya ditinjau dari segi tampilan, desain dan kelengkapan informasi saja, keamanan juga merupakan salah satu hal terpenting untuk diperhatikan dalam membangun situs web. Tujuan dari pencarian celah keamanan ini untuk mengetahui tingkat keamanan *Website* Sanggar Tari Didik Nini Thowok untuk mencegah dan menghindari adanya tindakan yang tidak diinginkan seperti pencurian data, penyalahgunaan hak akses dan sebagainya. Metode yang digunakan pada penelitian ini adalah ISSAF (*Information System Security Assessment Framework*). Proses evaluasi keamanan sistem *Kali Linux* menggunakan metode *Penetration Test*. Aplikasi *Port Scanning* yang digunakan adalah *Metasploit*, *Nmap* dan *Zenmap*. Hasil dari penetrasi menggunakan 3 tool menunjukkan bahwa *tool Kali Linux* tidak mengeluarkan hasil yang diharapkan, *Nmap* tidak mengeluarkan hasil yang diharapkan dan *Zenmap* yang menampilkan 24 data pada setiap percobaan sebanyak 10 kali. Hasil dari penetrasi pada *Zenmap* dihitung langsung menggunakan Algoritma *Naive Bayes* yang menghasilkan nilai akurasi 54,16%% dan belum memenuhi *Threshold Limit Value* sebesar 70%. Hasil akurasi ini menunjukkan bahwa *Website* Sanggar Tari Didik Nini Thowok kurang aman dari celah kerentanan. Hasil penetrasi pada *Kali Linux* (*Metasploit* dan *Nmap*) menghasilkan nilai akurasi sebesar 0%. Perbandingan antara ke 3 tools tersebut adalah 2:1 dengan keterangan 2 tools tidak bisa menembus website dan 1 tool berhasil menembus *website*.

Kata Kunci: *Website*; ISSAF; Kali Linux; Keamanan *Website*

Company profile website security analysis using issaf

Abstract

The didikninithowok.id website displays information related to the profile, information on the Didik Nini Thowok Dance Studio. Website creation is not only viewed in terms of appearance, design and completeness of information, security is also one of the most important things to pay attention to when building a website. The purpose of searching for security gaps is to determine the security level of the Didik Nini Thowok Dance Studio Website to prevent and avoid unwanted actions such as data theft, misuse of access rights and so on. The method used in this research is ISSAF (Information System Security Assessment Framework). The Kali Linux system security evaluation process uses the Penetration Test method. The Port Scanning applications used are Metasploit, Nmap and Zenmap. The results of penetration using 3 tools show that the Kali Linux tool does not produce the expected results, Nmap does not produce the expected results and Zenmap displays 24 data in each experiment 10 times. The results of penetration on Zenmap were calculated directly using the Naive Bayes algorithm which produced an accuracy value of 54.16%% and did not meet the Threshold Limit Value of 70%. These accuracy results indicate that the Didik Nini Thowok Dance Studio website is less secure from vulnerabilities. The penetration results on Kali Linux (Metasploit and Nmap) produce an accuracy value of 0%. The ratio between the 3 tools is 2:1 with the information that 2 tools could not penetrate the website and 1 tool succeeded in penetrating the website, so the final result can be drawn that the website is less secure from vulnerabilities.

Keywords: *Website; ISSAF; Kali Linux; Website Security*

1. Pendahuluan

Mengelola *website* memang tidak selalu mudah. Ada saja halangan seperti kendala atau *error* pada *website* hingga serangan peretas (*hacker*) yang bersumber dari berbagai celah keamanan *Website* yang kurang diperhatikan administrator. Tingkat keamanan *Website* yang rendah menjadikan para hacker dapat dengan mudah mengakses data penting. Semakin canggih teknologi yang tersedia sekarang menjadikan hacker makin pintar dalam melakukan teknik hacking untuk mendapatkan keuntungan pribadi dari pembobolan tersebut, maka penting melakukan *self-pentest* secara teratur untuk menguji kerentanan *Website*. Agar tingkat keamanan *Website* dapat terus di-*update* secara berkala untuk

mencegah terjadinya serangan *hacker*. Terdapat beberapa *framework* yang dapat digunakan dalam melakukan *pentest* seperti Metode *Information Systems Security Assessment Framework* (ISSAF). ISSAF merupakan *framework* yang terstruktur penggunaannya, terdiri dari beberapa tahap dalam pengelompokan informasi dalam rencana, penilaian serta laporan pengujian sistem keamanan ke dalam domain yang diuji dan menganalisa secara jelas (Dirgahayu, 2015).

Website utama Sanggar Tari Didik Nini Thowok tentunya memiliki kelemahan dan celah yang dapat digunakan oleh *hacker* untuk menyusup ke dalam sistem *website*. Proses untuk mengetahui kerentanan celah keamanan dari website utama Sanggar Tari Didik Nini Thowok akan menggunakan Metode ISSAF. Hasil dari pengujian ini akan ditindaklanjuti oleh pihak *administrator* sebagai upaya meningkatkan keamanan *Website* dan mencegah terjadinya serangan *hacker* lainnya (Eko Prasetyo & Hassanah, 2021).

Penelitian ini berfokus pada pengujian kemanan jaringan pada *Website* yang ada di Sanggar Tari Didik Nini Thowok dengan menggunakan metode *Information Systems Security Assessment Framework* (ISSAF). Proses *Penetration Test* akan menggunakan 3 tool yaitu *Kali Linux, Zenmap,* dan *Nmap*.

2. Metode

2.1. *Framework* ISSAF

Tahapan yang dilakukan untuk menyelesaikan penelitian ini berdasarkan *Framework* ISSAF. Tahapan penelitian menggunakan *Framework* ISSAF melalui tahapan-tahapan sebagai berikut :

2.1.1. Fase *Planning and Preparation*

Mempersiapkan *Website* Sanggar Tari Didik Nini Thowok yang akan menjadi sasaran penelitian ini. Setelah mempersiapkan sistem informasi sekolah yang ada dilakukan penyusunan rencana untuk pengujian dari sistem informasi tersebut.

2.1.2. Fase *Assessment*

Fase ini adalah pelaksanaan 8 fase yang sudah dijelaskan seperti pada kajian pustaka, fase tersebut terdiri dari:

1. *Information Gathering*
2. *Network Mapping*
3. *Vulnerability Identification*
4. *Penetration*
5. *Gaining Access and Privilege Escalation*
6. *Enumerating Further*
7. *Compromise Remote User/Sites*
8. *Maintaining Access*
9. *Covering Tracks.*

Penetration Test akan dilakukan pada fase ini dengan menggunakan 3 tool yang telah dijelaskan pada tinjauan pustaka, yaitu:

1. *Kali Linux*
   Kali Linux digunakan pada penelitian ini untuk mengetahui keamanan jaringannya jika dilakukan *Penetration Test* menggunakan Kali Linux sebagai *Tool,* dengan, menggunakan *Metasploit* dan Nmap. *Penetration Test* dilakukan dengan menggunakan CMD pada Kali Linux dengan memasukkan target dengan dan dieksekusi menggunakan *Metasploit* dan *Nmap*.
2. *Zenmap*
   Hasil yang diharapkan dalam *Penetration Test* Sistem informasi Sekolah dalam mencari kerentanan keamanan jaringan dimana mengetahui *port* apa saja yang terbuka menggunakan *Zenmap*.

2.1.3. Fase *Reporting* dan *Clean Up and Destroy Artifacts*

Fase ini adalah fase terakhir untuk memberikan solusi dari permasalahan yang ada. Selain itu dengan adanya *Clean Up and Destroy Artefacts* menghapus seluruh informasi yang telah dilakukan ketika Fase *Assessment* (Syarif Revolino, 2015).

2.2. Perhitungan Akurasi

Perhitungan ini dilakukan berdasarkan hasil pengujian menggunakan 3 *tool Kali Linux, Zenmap,* dan *Nmap*. Pengujian akan dilakukan sebanyak 10 kali pada setiap *tool*. Penelitian ini menggunakan beberapa *tool* salah satunya adalah *Tool Zenmap* yang digunakan untuk melakukan penyerangan sebanyak 10 kali. Penelitian penyerangan lainnya juga melakukan percobaan sebanyak 10 kali dengan metode yang berbeda. Maka dari itu untuk mendapatkan hasil yang imbang pengujian untuk masing-masing tool yakni *Kali Linux, Zenmap*, dan *Nmap* dilakukan sebanyak 10 kali.

Perhitungan akurasi dengan *Naive Bayes* ini menggunakan total percobaan dari setiap *tool*. Perhitungan ini membutuhkan percobaan yang sudah ditentukan untuk mendapatkan hasil yang imbang. Jumlah percobaan yang digunakan sebanyak 10 kali setiap *tool*.

Hasil dari perhitungan akan menentukan persentase akurasi keamanan dari sistem informasi yang diuji. Sistem akan dikatakan aman jika persentase dari hasil perhitungan melebihi *Threshold Limit Value* yang sudah ditentukan sebelumnya. Penelitian ini sudah menentukan *Threshold Limit Value* sebesar 70%. *Threshold Limit Value* tersebut didapatkan dari perbandingan antara penelitian lain yang menentukan *Threshold Limit Value* 30%, 70%, dan 87,5%. Sistem informasi ini belum diluncurkan, maka untuk *Threshold Limit Value* diambil yang tidak terlalu rendah dan tinggi, sehingga didapatkan *Threshold Limit Value* sebesar 70%. Hasil penentuan *Threshold Limit* Value pada penelitian ini diperkuat dengan jurnal yang dijadikan acuan pada penelitian ini (Purnamasari et al., 2000).

3. Hasil dan Pembahasan

3.1. Hasil Pengujian

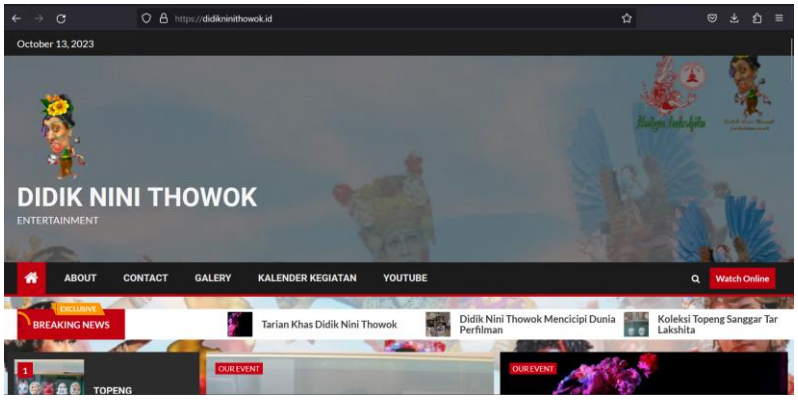
Tahap ini merupakan pemaparan dari hasil proses percobaan *Penetration Test* pada *Website* Sanggar Tari Didik Nini Thowok. Proses *Penetration Test* menggunakan *Kali Linux, Zenmap* dan *Nmap* yang diimplementasikan menggunakan 3 fase yang ada dalam ISSAF yaitu:

3.1.1. Fase *Planning and Preparation*

Fase *Planning and Preparation* merupakan fase awal untuk menentukan kesepakatan pemilik sistem informasi dimana saat ini *Website* Sanggar Tari Didik Nini Thowok sedang dikerjakan oleh mahasiswa MBKM dari UNISA Yogya. Instansi ini merupakan tempat yang pernah digunakan untuk kegiatan Merdeka Belajar Kampus Merdeka (MBKM) Proyek Independent dimana *Website* ini dibuat sebagai topik utama pembelajaran MBKM.

3.1.2. Fase *Assessment*

Fase *Assessment* merupakan fase inti dari ISSAF. Tahap pengumpulan informasi atau *Information Gathering* yang merupakan langkah awal untuk mengetahui informasi mengenai target. Penelitian ini telah memiliki target yang ditentukan yaitu *Website* Sanggar Tari Didik Nini Thowok. *Website* Sanggar Tari Didik Nini Thowok seperti Gambar 1.



Gambar 1. Tampilan *Website* Sanggar Tari Didik Nini Thowok

Website Sanggar Tari Didik Nini Thowok memiliki Alamat IP yaitu 103.119.228.118 seperti Gambar 2.

```
C:\Users\ASUS>ping didikninithowok.id

Pinging didikninithowok.id [103.119.228.118] with 32 bytes of data:
Reply from 103.119.228.118: bytes=32 time=23ms TTL=57
Reply from 103.119.228.118: bytes=32 time=38ms TTL=57
Reply from 103.119.228.118: bytes=32 time=15ms TTL=57
Reply from 103.119.228.118: bytes=32 time=28ms TTL=57

Ping statistics for 103.119.228.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 38ms, Average = 26ms
```

Gambar 2. Alamat IP *Website* Sanggar Tari Didik Nini Thowok

Alamat IP tersebut adalah kepemilikan dari *Website* Sanggar Tari Didik Nini Thowok yang dapat digunakan untuk mencari tahu informasi dari tampilan komputer. Selain itu juga dapat digunakan untuk mengecek fungsional dari *Website* maupun web. Fase ini adalah fase inti dari penelitian dimana proses dari Penetration Test akan dilakukan pada fase ini. Metodologi Penelitian ini sudah dipaparkan mengenai 3 *tools* yang akan digunakan untuk *Penetration Test* untuk mengetahui kerentanan dari *Website* Sanggar Tari Didik Nini Thowok.

3.1.3. Proses Pengujian

Kali Linux pada penelitian ini digunakan sebagai *tool* untuk melakukan *Penetration Test*. Pengimplementasian dari *Penetration Test* pada *Kali Linux* ini membutuhkan peran *Metasploit* dan *Nmap*. *Metasploit* merupakan sebuah program yang digunakan untuk masuk atau meng-eksploit target dengan mengontrol perangkat yang sedang digunakan penguji. *Metasploit* ini digunakan untuk mengetahui kerentanan keamanan dan bukan untuk hacking atau peretasan. Sedangkan *Nmap* memiliki fungsi untuk melakukan *port* scanning. Proses pengimplementasian *Metasploit* pada *Kali Linux* yang dilakukan sebagai berikut:

Tabel 1. Hasil Percobaan *Kali Linux*

Percobaan ke	Hasil

Percobaan 1	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

Percobaan 2	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

Percobaan 3	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

Percobaan 4	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

Percobaan 5	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

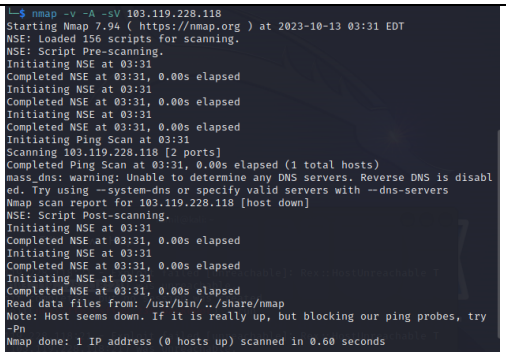
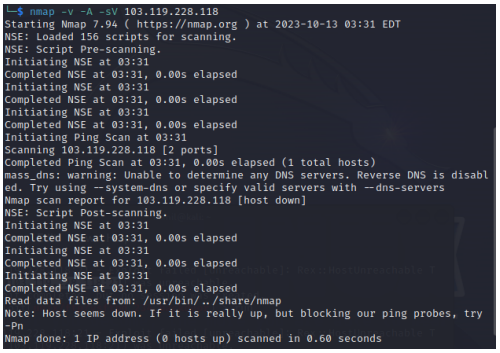
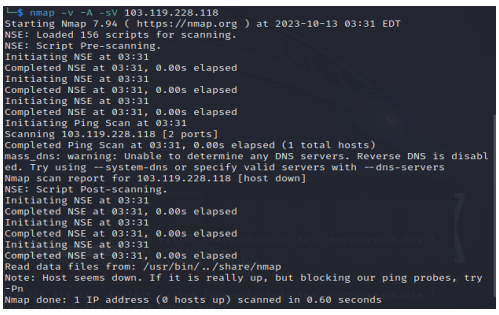
Percobaan 6	`msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run`
	`[-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable.`
	`[*] Exploit completed, but no session was created.`

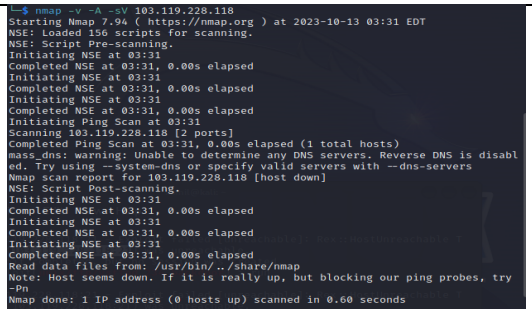
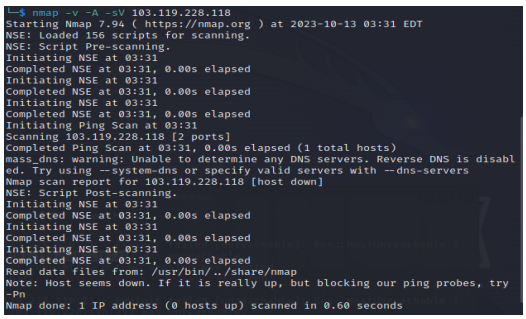
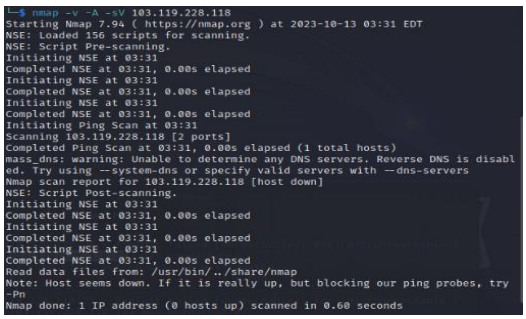
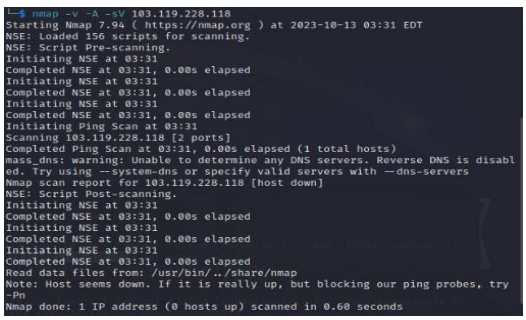
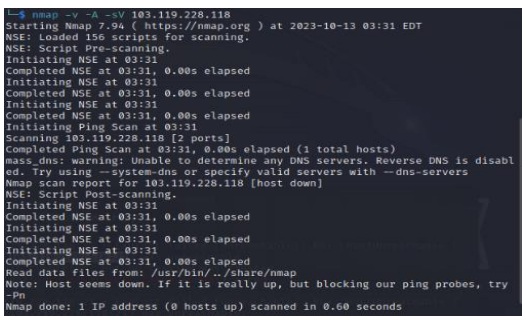
Percobaan 7	msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run [-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable. [*] Exploit completed, but no session was created.
Percobaan 8	msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run [-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable. [*] Exploit completed, but no session was created.
Percobaan 9	msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run [-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable. [*] Exploit completed, but no session was created.
Percobaan 10	msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run [-] 103.119.228.118:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (103.119.228.118:21) was unreachable. [*] Exploit completed, but no session was created.

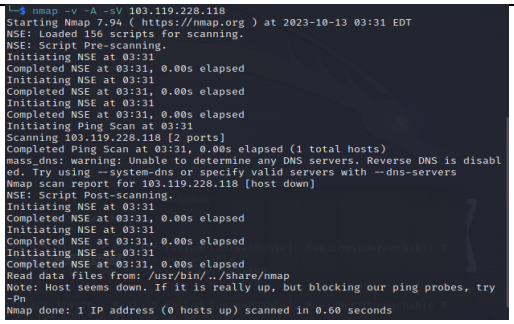
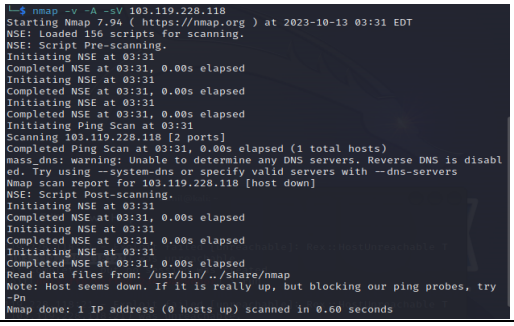
Sumber : Hasil Pengujian Penulis (2024)

Hasil yang didapatkan dari 10 kali percobaan *Penetration Test* adalah *Exploit failed [unreachable]*. Proses implementasi *Metasploit* pada *Kali Linux* sudah selesai. Langkah selanjutnya adalah pengimplementasian *Nmap* pada *Kali Linux*.

Tabel 2. Hasil Percobaan *Nmap*

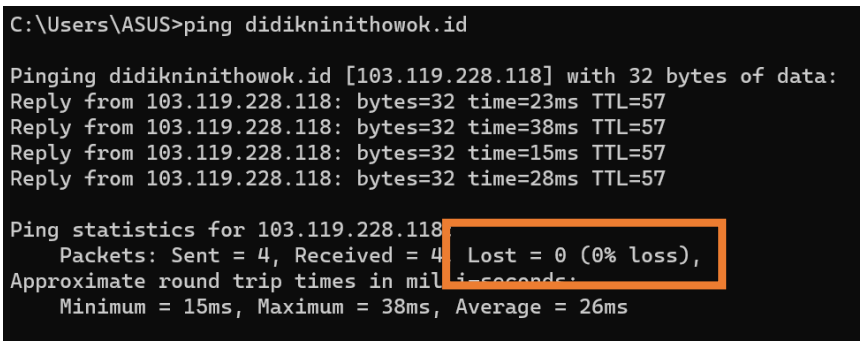
Perobaan	Hasil
Percobaan 1	
Percobaan 2	
Percobaan 3	

Perobaan	Hasil
Percobaan 4	
Percobaan 5	
Percobaan 6	
Percobaan 7	
Percobaan 8	

Perobaan	Hasil
Percobaan 9	
Percobaan 10	

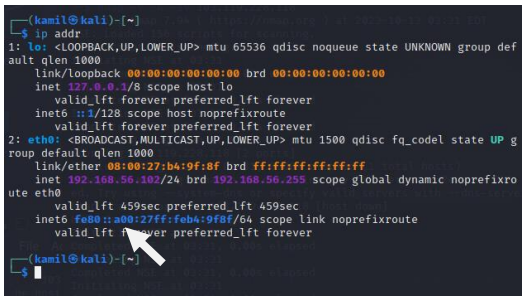
Sumber : Hasil Pengujian Penulis (2024)

"*Nmap* -v -A -sV 103.119.228.118" berfungsi untuk menjalankan *Nmap* pada *Kali Linux*. Tabel 4.2 menampilkan hasil dari *Nmap* pada *Kali Linux* yaitu tidak terdeteksinya *port* yang terbuka. Dibutuhkan proses untuk memastikan hasil dari *Metasploit* dan *Nmap* dari *Sistem* pada Operasi *Kali Linux* dengan melakukan ping kepada *Sistem* Operasi *Windows* ke *Sistem* Operasi *Kali Linux* seperti Gambar 4.3.



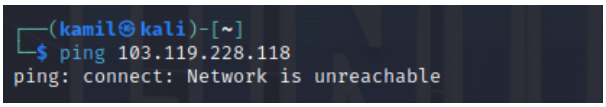
Gambar 3. *ping Windows*

Gambar 3 menunjukkan hasil "ping 103.119.228.118" berhasil dilakukan dengan keterangan *Lost* 0%. Hal ini berarti *Network* dari *Windows* ke *Kali Linux* berhasil terhubung. *IP* 103.119.228.118 untuk melakukan *ping* pada *Kali Linux* didapatkan dari pengecekan *IP* di *Kali Linux* menggunakan *"IP addr*" pada *Terminal Kali Linux* seperti Gambar 4.



Gambar 4. *IP addr*

Ping dari *Kali Linux* ke *Windows* dengan membuka *Terminal Kali Linux*. Masukkan perintah "ping 192.168.56.1" yang merupakan *IP Getaway* dari *Host* atau *Windows* seperti Gambar 5.



Gambar 5. *ping Linux*

Ping dari *Kali Linux* ke *Windows* adalah gagal karena jaringan tidak terbaca. Hal ini dapat berarti bahwa Network *Kali Linux* ke *Windows* gagal dengan keterangan Network is *unreachable*.

Penetration Test menggunakan *Nmap* membutuhkan aplikasi *Zenmap* pada *Windows* dalam pengimplementasiannya. *Penetration Test* membutuhkan *IP* dimana memasukkan *IP* dari *Localhost* yaitu 127.0.0.1. Langkah implementasi *Penetration Test* menggunakan *Nmap* sebagai berikut:

1. Akses *Website Nmap* yaitu https://*Nmap*.org/*Zenmap*/ lalu unduh aplikasi *Zenmap* disesuaikan dengan jenis *bit PC* yang digunakan.
2. Langkah selanjutnya install *Zenmap* yang sudah terunduh
3. Langkah selanjutnya buka Aplikasi *Zenmap* yang sudah terinstall lalu masukkan Alamat *IP*
4. Hasil dari scan *IP* dengan percobaan yang dilakukan sebanyak 10 kali dapat dilihat pada Tabel 3.

Percobaan sebanyak 10 kali menggunakan *Zenmap* didapatkan hasil yaitu 13 *port TCP* yang terbuka dan 11 *port TCP* yang tertutup. 13 *port TCP* yang terbuka terdiri dari *port* 21, ,26, 53, 80, 110, 143, 443, 465, 587, 993, 995, 3306 dan 11 *port TCP* yang tertutup terdiri dari 81, ,8080, 8081, 32768, 49152, 49153, 49154, 49155, 49156, 49157.

Hal yang menyebabkan perbedaan hasil pengujian Zenmap adalah perbedaan alamat IP wifi dan perbedaan koneksi jaringan sehingga berpengaruh terhadap hasil pengujian.

3.2. Perhitungan Akurasi

3.2.1. *Zenmap*

Perhitungan akurasi pada *Zenmap* dapat diimplementasikan di setiap percobaan pada *Zenmap* dengan memasukkan angka 13 yang berasal dari jumlah *port TCP open-filter* dan 24 dari total jumlah data yang muncul baik *open* maupun *open-filter*. Hasil perhitungan dari 10 kali percobaan dengan *Nmap* maka diperoleh nilai rata-rata percobaan:

Rata-rata :

$$\frac{54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%+54{,}16\%}{10} = 54{,}16\%$$

Hasil Rata-rata akurasi menggunakan perhitungan Algoritma *Naive Bayes* dari *Penetration Test* menggunakan *Nmap* didapatkan hasil akurasi sebesar 54,16%. Hasil akurasi yang didapatkan kurang dari *Threshold Limit Value* yaitu sebesar 70%. *Website* Sanggar Tari Didik Nini Thowok dikatakan kurang aman dari serangan yang dilakukan menggunakan *Tool Nmap* pada *Windows*.

3.2.2. *Metasploit*

Perhitungan akurasi pada *Nmap* dapat diimplementasikan di setiap percobaan pada *Metasploit* dengan memasukkan angka 0 yang berasal dari hasil pengujian *metasploit* dan 10 dari total jumlah percobaan. Hasil perhitungan dari 10 kali percobaan dengan *Nmap* diperoleh nilai rata-rata percobaan :

Rata-rata

$$\frac{0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\%}{10} = 0\%$$

Hasil perhitungan rata-rata pada *Tools Metasploit* yaitu sebesar 0%. Solusi agar hasil perhitungan tidak 0% yaitu menggunakan *tools* yang mampu melakukan penetrasi *website* sehingga hasil yang didapatkan sesuai harapan.

3.2.3. *Nmap*

Perhitungan akurasi pada *Nmap* dapat diimplementasikan di setiap percobaan pada *Nmap* dengan memasukkan angka 0 yang berasal dari hasil pengujian *metasploit* dan 10 dari total jumlah percobaan. Hasil perhitungan dari 10 kali percobaan dengan *Nmap* pada **Tabel 4.6** dimasukan ke Persamaan (4.1), maka diperoleh nilai rata-rata percobaan:

Rata-rata :

$$\frac{0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\% + 0\%}{10} = 0\%$$

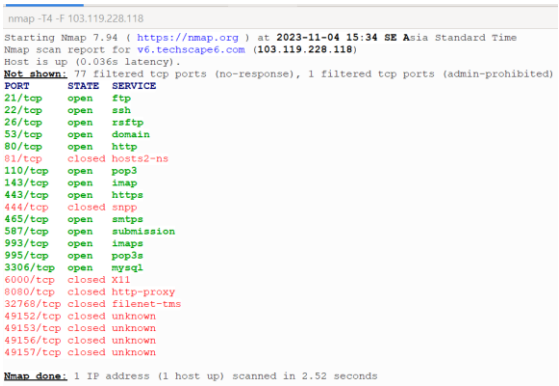
Hasil perhitungan rata-rata pada *Tools Metasploit* yaitu sebesar 0%. Solusi agar hasil perhitungan tidak 0% yaitu menggunakan *tools* yang mampu melakukan penetrasi *website* sehingga hasil yang didapatkan sesuai harapan.

3.3. Pembahasan

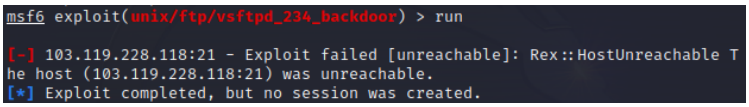
Tool Kali Linux tidak dapat dihitung akurasinya karena hasil yang didapatkan tidak sesuai dengan harapan. Hal ini dikarenakan tidak adanya jenis *port* yang terbuka pada hasil *Penetration Testing* dan hanya menghasilkan keluaran Exploit Failed (*unreachable*) pada setiap percobaan menggunakan *Metasploit* menghasilkan nilai akurasi sebesar 0% dengan nilai rata-rata sebesar 0%.

Percobaan menggunakan *Nmap* juga tidak memunculkan *port* yang terbuka. Hasil tidak sesuai dikarenakan aktifnya firewall public network sehingga proses *Penetration Testing* menggunakan *Metasploit* dan *Nmap* ini gagal. Perhitungan menggunakan *Nmap* menghasilkan nilai akurasi sebesar 0% dan nilai rata-rata sebesar 0%.

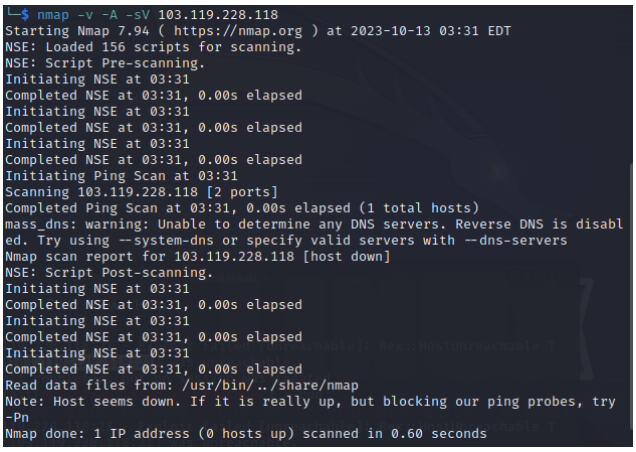
Tool Zenmap adalah *tool* yang dapat menampilkan hasil yang sesuai dengan harapan dimana terdeteksi *port* yang terbuka sejumlah 13 *port* dan 11 *port* yang ter*filter*. Maksud dari *port* yang *open* berarti aplikasi pada mesin target sedang terkoneksi pada *port* target, sedangkan *filter* berarti target memiliki *firewall*, *filter*, atau penghalang jaringan lainnya untuk memblokir *port* sehingga *Nmap* tidak dapat mendeteksi apakah *port* tersebut terbuka atau tertutup. Hasil akurasi dari *Penetration Test* pada *Nmap* juga kurang dari *Threshold Limit Value* yaitu sebesar 54,16%.



Gambar 6. Hasil Pengujian *Zenmap*



Gambar 7. Hasil Pengujian *Metasploit*



Gambar 8. Hasil Pengujian Nmap

Solusi untuk meningkatkan keaman pada *Website* Sanggar Tari Didik Ninik Thowok adalah:

a. Menjaga keamanan sistem operasi dan aplikasi
   Sistem operasi dan aplikasi yang sudah kadaluarsa biasanya memiliki kerentanan yang dapat dimanfaatkan oleh penyerang. Oleh karena itu, penting untuk selalu menjaga keamanan sistem operasi dan aplikasi dengan melakukan pembaruan secara berkala.
b. Melakukan monitoring jaringan secara berkala
   Monitoring jaringan secara berkala dapat membantu untuk mendeteksi adanya ancaman keamanan. Oleh karena itu, penting untuk memiliki sistem monitoring jaringan yang efektif.

4. Kesimpulan

Proses penelitian telah dilakukan dan mendapatkan hasil berupa nilai akurasi dari *Website* Sanggar Tari Didik Nini Thowok. Kesimpulan yang dapat diambil dari penelitian ini yaitu ada beberapa celah keamanan yang ditemukan pada *Penetration Testing* menggunakan tool *Zenmap* pada *Windows* yaitu sebanyak 13 *port* TCP yang terbuka terdiri dari *port* 21, ,26, 53, 80, 110, 143, 443, 465, 587, 993, 995, 3306 dan 11 *port* TCP yang tertutup terdiri dari 81, ,8080, 8081, 32768, 49152, 49153, 49154, 49155, 49156, 49157. Hasil dari *Penetration Testing* menggunakan *Zenmap* dinyatakan bahwa *Website* Sanggar Tari Didik Nini Thowok kurang aman. Hasil tersebut diambil dari perhitungan akurasi sebesar 54,16% dari nilai ambang batas sebesar 70%. Hasil *Penetration Testing Metasploit* dinyatakan bahwa *website* Sanggar Tari Didik Nini Thowok aman. Hasil tersebut diperoleh dari proses *Penetration Testing Metasploit* pada *Kali Linux* tidak bisa menembus *website* Sanggar Tari Didik Nini Thowok dan hasil dari perhitungannya sebesar 0%. Hasil *Penetration Testing Nmap* dinyatakan bahwa *website* Sanggar Tari Didik Nini Thowok aman. Hasil tersebut diperoleh dari proses *Penetration Testing* pada *Kali Linux* gagal menembus *website* Sanggar Tari Didik Nini Thowok dan hasil perhitungannya sebesar 0%. Hasil pengujian menggunakan ke 3 tools menunjukkan hasil perbandingan 2:1 yaitu dengan keterangan 2 *tools* gagal melakukan *penetration testing* dan 1 tool berhasil melakukan *penetration testing* pada *website* maka disimpulkan bahwa *website* Sanggar Tari Didik Nini Thowok aman dari tindakan *Penetration Testing.* Efektifitas *tool* juga dapat dilihat dengan hasil yang didapatkan. Hanya terdapat 1 *tool* yang menampilkan hasil yang diinginkan yaitu *tool Zenmap* pada *Windows*. Pernyataan ini diperkuat dengan adanya nilai akurasi yang belum melebihi *Threshold Limit Value* yaitu sebesar 54,16%. Sedangkan *Tool Kali Linux* hasil yang didapatkan pada penggunaan *Metasploit* dan *Nmap* tidak sesuai dengan apa yang diharapkan dimana tidak ada keterangan *port* mana saja yang terbuka maupun tertutup.

5. Ucapan terimakasih

Suka duka telah penulis lalui dalam menyelesaikan skripsi ini, banyak pihak yang telah memberikan dukungan dan bantuan selama menyelesaikan skripsi atau tugas akhir ini. Sepantasnya saya berterimakasih kepada pihak yang telah menjadi semangat dan tekat untuk menyelesaikan skripsi, penulis berterimakasih sebesar-besarnya kepada Ibu Warsiti, M.Kep., Sp.Mat. selaku Rektor

Universitas 'Aisyiyah Yogyakarta, Ibu Zahra Arwananing Tyas, S.Kom., M.Cs. selaku Kepala Program Studi Teknologi Informasi, Ibu Esi Putri Silmina, S.T., M.Cs. selaku Dosen Pembimbing I dan Bapak Arizona, S.Kom., M.Cs. selaku Dosen Pembimbing II yang telah sabar membimbing dan sabar memberi masukan dan arahan hingga skripsi selesai, Bapak dan Ibu saya yang telah memberikan dukungan finansial maupun moral sehingga penulis sampai dititik ini, kakak kandung yang telah memberikan dukungan mental hingga membuat penulis kembali bersemangat dan tegar, teman-teman seperjuangan yang telah memberikan motivasi dan semangat sehingga ketika ada masalah dalam pengerjaan skripsi ini saya bisa kembali semangat dan bisa menyelesaikan masalah tersebut dan terakhir teman-teman dekat saya yang tidak dapat disebutkan satu persatu yang telah membantu dalam segala hal.

Daftar Pustaka

Andria. (2020). Analisis Celah Keamanan Website Menggunakan *Tools Webpwn3r* di *Kali Linux.* Generation Journal, 70-76.

Dirgahayu, D. R. T. (2015). Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server. 1(3).

Eko Prasetyo, S., & Hassanah, N. (2021). Analisis Keamanan Website Universitas Internasional Batam Menggunakan Metode Issaf. jurnal ilmiah informatika, 9(02), 82–86. https://doi.org/10.33884/jif.v9i02.3758

Guntoro, G., Costaner, L., & Musfawati, M. (2020). Analisis Keamanan *Web Server Open Journal System* (OJS) Menggunakan Metode Issaf dan Owasp (Studi Kasus OJS Universitas Lancang Kuning). JIPI (Jurnal Ilmiah Penulisan dan Pembelajaran Informatika), 5(1), 45. https://doi.org/10.29100/jIPi.v5i1.1565

Marsoni, M., Kalsum, T. U., & Kurniawan, A. (2016). Analisa Implementasi Teknik *Reconnaissance* Pada *Webserver* (Studi Kasus: Upt Puskom Universitas Dehasen). Jurnal Media Infotama, 12(1), 11–20.

Pujiarto, B., Utami, E., & Sudarmawan, S. (2013). Evaluasi Keamanan *Wireless Local Area Network* Menggunakan Metode *Penetration Testing* (Kasus :Universitas Muhammadiyah Magelang). Data Manajemen Dan Teknologi Informasi (DASI), 14(2), 16.

Purnamasari, D., Santoso, I., & Zahra, A. A. (2021). Analisis Kapasitas Kanal Trafik BTS pada Jaringan CDMA 450 untuk Layanan Suara. ResearchGate, 1-10.

Putra, R. D., & Mardianto, I. (2019). Exploitation with Reverse_tcp Method on Android Device using Metasploit. Jurnal Edukasi dan Penelitian Informatika (JEPIN), 5(1), 106. https://doi.org/10.26418/jp.v5i1.26893

Silmina, E. P., Amanda, R. A., & Firdonsyah, A. (2022). Analisis Keamanan Jaringan Sistem Informasi Sekolah Menggunakan *Penetration Test* dan ISSAF. Jurnal Ilmiah Teknik Elektro, 83-91.

Sudirman, D., & Yaqin, A. N. (2021). *Network Penetration* dan *Security Audit* Menggunakan *Nmap*. Satin, 7(1), 32–44.

Suwaryo, N., Nawangsih, I., & Rejeki, S. (2021). Deteksi Serangan pada Intrusion Detection System (IDS) untuk Klasifikasi Serangan dengan Algoritma Naïve Bayes, C.45 dan K-NN dalam Meminimalisasi Resiko Terhadap Pengguna. JSI (Jurnal Sistem Informasi), 171-180.

Syarif Revolino, T. (2015). Analisis Perbandingan Metode *Web Security Pets*, ISSAF, dan OWASP. 17–39.

Wardhana, A. W., & Seta, H. B. (2021). Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. Informatik : Jurnal Ilmu Komputer, 17(3), 226. https://doi.org/10.52958/iftk.v17i3.3653

Wardhana, A. W., & Seta, H. B. (2021). Analisis Keamanan Sistem Pembelajaran Online Menggunakan Metode ISSAF pada Website Universitas XYZ. Informatik : Jurnal Ilmu Komputer, 17(3), 226. https://doi.org/10.52958/iftk.v17i3.3653

WK, W. N., & Adani, Y. (2020). Penerapan Algoritma *Naive Bayes* Untuk Memprediksi Keputusan Calon Nasabah dan Nasabah Tetap Bank BRI Syariah Menerima Penawaran Program Deposito Berjangka. STMIK LPKIA Bandung, 13-24.