TRANSMISI : JURNAL ILMIAH TEKNIK ELEKTRO, 24, (3), JULI 2022
p-ISSN 1411-0814 e-ISSN 2407-6422

ANALISIS KEAMANAN JARINGAN SISTEM INFORMASI SEKOLAH MENGGUNAKAN *PENETRATION TEST* DAN *ISSAF*

Esi Putri Silmina[*)], Arizona Firdonsyah, Rovalia Adhella Attya Amanda

Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta
Jl. Siliwangi No. 63, Mlangi, Nogotirto, Gamping, Sleman, Yogyakarta, 55292, Indonesia

[*)]*E-mail:esiputrisilmina@unisayogya.ac.id, arizona@unisayogya.ac.id*

Abstrak

Perkembangan teknologi di era industri 4.0 telah berkembang pesat, salah satunya Sistem Informasi Sekolah. Pada MTsN 8 Bantul, telah dibuat Sistem Informasi Sekolah untuk memudahkan pengolahan data sekolah. Sistem ini masih belum diluncurkan karena belum melalui proses pencarian celah keamanan jaringan. Tujuan penelitian ini untuk mencari celah keamanan dan mengetahui tingkat keamanan jaringan untuk menghindari adanya tindakan yang tidak diinginkan seperti pencurian data atau penyalahgunaan hak akses. Metode yang digunakan pada penelitian ini adalah *Information System Security Assessment Framework (ISSAF). ISSAF* digunakan untuk mengkategorikan penilaian keamanan sistem informasi. *Penetration Test* juga digunakan untuk pengujian keamanan dengan menggunakan *tool* yang sudah ditentukan yaitu *Kali linux, Nmap,* dan *WireShark.* Hasil dari penetrasi menggunakan 3 *tool* menunjukkan bahwa *tool Kali linux* tidak mengeluarkan hasil yang diharapkan, *WireShark* tidak *support* untuk *capturing* pada *Localhost,* dan *Nmap* yang menampilkan 11 data pada setiap percobaan sebanyak 10 kali. Hasil dari penetrasi pada *Nmap* dihitung langsung menggunakan Algoritma *Naive Bayes* yang menghasilkan nilai akurasi 72,72% dan telah memenuhi *Threshold Limit Value* sebesar 70%. Hasil akurasi ini menunjukkan bahwa Sistem Informasi Sekolah MTsN 8 Bantul aman dari celah keamanan.

Kata kunci: ISSAF, Naive Bayes, Penetration Test, Sistem Informasi Sekolah

Abstract

Technological developments in the industrial era 4.0 have developed rapidly, one of which is the School Information System. MTsN 8 Bantul has created School Information System to make it easier to process data in schools. This system has not yet been launched because it has not gone through the process of finding network security holes. The purpose of this search for security holes is to determine the level of network security to avoid unwanted actions such as data theft, abuse of access rights, and so on. The method used in this research is ISSAF. ISSAF is used to categorize information system security assessments. Penetration Test is also used for security testing using predefined tools, namely Kali linux, Nmap, and WireShark. The results of the penetration using 3 tools show that the Kali linux tool does not produce the expected results, WireShark does not support capturing on Localhost, and Nmap which displays 11 data in each experiment 10 times. The results of the penetration on Nmap are calculated directly using the Naive Bayes Algorithm which produces an accuracy value of 72.72% and has met the Threshold Limit Value of 70%. The results indicate that the School Information System is safe from security holes.

Keywords: ISSAF, Naive Bayes, Penetration Test, School Information System

1. Pendahuluan

Masyarakat kini sudah mulai mengikuti perkembangan jaman terutama di era serba digital pada saat ini. Perkembangan digital di era Industri 4.0 dimana ada digitalisasi yang mempengaruhi seluruh bidang yang ada, salah satunya sekolah yang kini mulai menggunakan sistem informasi. Sistem informasi adalah kombinasi dari informasi dan kegiatan orang yang menggunakan teknologi untuk mendukung operasi dan manajemen [1]. Sistem Informasi Sekolah sendiri merupakan sistem yang mengatur administrasi untuk sekolah dalam basis internet. Sistem informasi dapat diakses dari berbagai kalangan baik guru wali kelas, pegawai sekolah, siswa, dan orang tua atau wali seperti Sistem Informasi yang ada di MTsN 8 Bantul Penelitian ini merupakan tahap lanjutan dari studi kasus yang diambil yaitu Sistem Informasi MTsN 8 Bantul dimana Sistem Informasi Sekolah ini sudah pernah menjadi subjek kegiatan Merdeka Belajar Kampus Merdeka (MBKM) Bentuk Kegiatan Pembelajaran (BKP) Magang Industri dengan menganalisis keamanan jaringan dimana keamanan jaringan sendiri memiliki arti cara untuk mencegah dan mengontrol akses tidak sah ke jaringan atau sistem yaitu Sistem Informasi Sekolah MTsN 8 Bantul

sebelum diluncurkan untuk mengetahui apakah sistem sudah aman dan siap untuk digunakan [2].
Pencarian celah keamanan Sistem Informasi Sekolah MTsN 8 Bantul ini menggunakan *Penetration Test* dan *Information System Security Assessment Framework (ISSAF)*. *Penetration Test* adalah mengetahui seberapa baik sistem dalam menangani masalah yang diberikan. *Penetration Test* juga kerap digunakan untuk mendeteksi dan melakukan serangan [3] *ISSAF*. *ISSAF* dipilih karena sesuai dengan tujuanpenelitian dan bersifat *open source*, sehingga bebas digunakan oleh siapa saja. Selain itu *ISSAF* memiliki kerangka terstruktur yang mengkategorikan penilaian keamanan sistem informasi dalam berbagai domain dan rincian kriteria evaluasi atau pengujian khusus untuk masing-masing domain [4]. *ISSAF* juga memiliki standar pengujian penetrasi untuk menguji ketahanan dari serangan yang diberikan [5]. Adapun metod lain yang kerap disandingkan dengan *ISSAF* yaitu *OWASP* seperti penelitian yang dibuat oleh Raden Teduh Dirgahayu, dkk (2015) dari Universitas Islam Indonesia yang membahas mengenai penggunaan Metode ISSAF dan OWASP untuk penetrasi penyerangan pada Web Server IKIP PGRI Madiun. Tujuan dari penelitian untuk mengetahui apakah Web Server IKIP PGRI Madiun aman atau tidak aman dari serangan. Web server ini sudah digunakan sejak 2010 hingga sekarang. Hasil dari penelitian ini yaitu Web Server IKIP PGRI Madiun ternyata masih bisa dibobol dari akses administrator menggunakan Metode ISSAF. Sedangkan hasil untuk OWASP versi 4 hanya menunjukkan otorisasi dan manajemen yang belum diimplementasikan dengan baik [6].

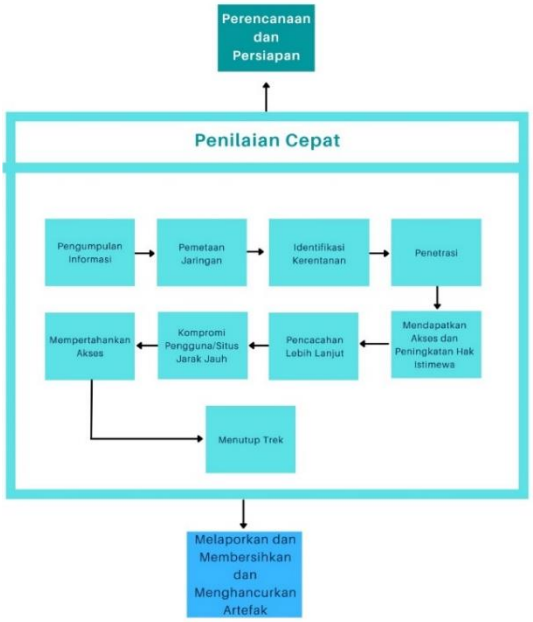
Implementasi *Penetration Test* membutuhkan alat untuk menjalankan serangan yang ada pada Sistem Informasi Sekolah. *Tool* yang akan digunakan antara lain *Kali linux*, *WireShark*, dan *Nmap*. *Kali linux* dipilih karena Pemaketan/*packaging* jangka panjang & sering memberikan *update* paket terbaru dan perbaikan keamanan yang tersedia [7]. *WireShark* dipilih karena dapat menangkap paket informasi yang berjalan pada suatu jaringan [8]. *Network Mapper* atau *Nmap* dipilih karena dapat digunakan untuk *port scanning*, mengaudit jaringan yang ada, dan mengetahui host yang aktif atau *port* yang terbuka [9].

Hasil dari *Penetration Test* yang sudah dilakukan menggunakan 3 *tool* yaitu *Kali linux*, *WireShark*, dan *Nmap* yang akan dihitung akurasinya menggunakan *Naive Bayes*.

2. Metode

2.1. *Information System Security Assessment Framework (ISSAF)*

ISSAF memiliki 3 fase utama yang akan digunakan pada penelitian ini yaitu Fase *Planning and Preparation*, Fase *Assessment*, Fase *Clean Up and Destroy Artefacts* [10]. Tahapan yang akan dilakukan pada penelitian ini dapat dilihat seperti Gambar 1 [11].



Gambar 1. Fase Kerangka *ISSAF*

A. Fase *Planning and Preparation*

Mempersiapkan Sistem Informasi Sekolah MTsN 8 Bantul yang akan menjadi sasaran penelitian ini. Setelah mempersiapkan sistem informasi sekolah yang ada dilakukan penyusunan rencana untuk pengujian dari sistem informasi tersebut.

B. Fase *Assessment*

Fase *Assessment* adalah fase yang digunakan untuk menguji coba sistem informasi yang sudah disepakati pada Fase *Planning and Preparation.* Fase *Assessment* sendiri dapat dikembangkan menjadi 9 fase yaitu:

a. Pengumpulan Informasi (*Information Gathering*)
   Pengumpulan informasi umum yang terjadi di tempat tujuan. Informasi yang dikumpulkan meliputi informasi tentang IP tujuan, informasi tentang pendaftar dan administrator, informasi tentang *reverse* DNS dan pencarian IP, dan informasi umum lainnya.
b. Pemetaan Jaringan (*Network Mapping* Fase)
   Pemetaan Jaringan adalah fase di mana informasi dikumpulkan secara khusus tentang jaringan di tempat tujuan. Salah satu informasi yang dikumpulkan pada fase ini mencakup informasi tentang *port* TCP dan UDP pada sistem target.
c. Identifikasi Keterangan (*Vulnerability Identification* Fase)
   Fase berfungsi dimana *web* target dipindai untuk menemukan kerentanan keamanan yang ada.
d. Penetrasi (*Penetration* Fase)

Penetrasi adalah fase simulasi serangan pada *web target* dengan tujuan untuk menemukan celah dalam keamanan sistem.

e. Mendapatkan Akses dan Peningkatan Hak Istimewa (*Gaining Access and Privilege Escalation* Fase)
Fase ini adalah fase pengujian selama upaya untuk mengakses sistem target. Jenis akses yang dilakukan pada penelitian ini adalah akses ke sistem pengguna administrator dan akses ke sistem.

f. Perencanaan Lebih Lanjut (*Enumerating Further* Fase)
Fase ini adalah fase pengujian dalam melakukan pemulihan dan menyelesaikan semua informasi terkait dengan kata sandi yang diperoleh dari web.

g. Kompromi Pengguna/Situs Jarak Jauh (*Compromise Remote User/Sites* Fase)
Fase ini adalah fase pengujian di mana mengeksploitasi akses pengguna root melalui koneksi jarak jauh ke *web*.

h. Mempertahankan Akses (*Maintaining Access*)
Dengan memakai sesuatu misalnya *Backdoor*, penguji bisa balik ke pada sebuah sistem, bahkan bila sistem yg diuji telah tidak ada lagi ada. *Backdoor* bisa dibentuk menggunakan beberapa cara, baik menggunakan *root-kit*, dengan mengizinkan sistem sasaran terkoneksi menggunakan *server* penguji dan lain-lain.

i. *Covering Tracks*
Pada tahapan ini, penguji akan menghapus jejak-jejak yang ada dengan cara menyembunyikan *file*, dan juga menghapus *log files* dilakukan dalam fase sebelumnya.

Penetration Test yang akan dilakukan pada fase ini untuk melakukan *security assessment*, dengan menggunakan 3 *tool*, yaitu:

a. *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*.

b. *WireShark*
Penggunaan *WireShark* untuk mengetahui lalulintas sistem, apakah ada *error* yang muncul dari penyerangan.

c. *Network Mapper (Nmap)*
Nmap memiliki tujuan untuk mengetahui *port* yang terbuka dengan status yang sudah ada yaitu terbuka (*open*), di-*filter* (*filtered*), tertutup (*closed*), atau tidak di-*filter* (*unfiltered*)

C. Fase *Clean Up and Destroy Artifacts*

Fase ini merupakan fase terakhir dimana penghapusan sistem informasi yang telah digunakan untuk penelitian. Hal ini ditujukan untuk menghindari adanya penyalahgunaan di luar penelitian dan persetujuan pada Fase *Planning and Preparation*. Fase *Clean Up and Destroy Artefacts* dapat dibagi menjadi 2 fase yaitu:

a. *Reporting*
Pada tahap ini, penguji akan melakukan penulisan laporan yang mendeskripsikan hasil pengujian dengan rekomendasi dan penyelesaiannya.

b. Clean Up and Destroy Artifacts
Setiap informasi yang dibuat atau dimasukkan ke dalam sistem harus dihapus pada tahap ini. Jika ini tidak memungkinkan pada sistem jarak jauh, pihak yang diuji harus diberi tahu sehingga staf TI dapat menghapus informasi ini setelah menerima laporan.

2.2. *Naive Bayes*

Algoritma *Naive Bayes* adalah salah satu algoritma dari teknik klasifikasi. Sedangkan pengertian secara matematis *Naive Bayes* adalah klasifikasi yang diusulkan oleh ilmuwan Inggris *Thomas Bayes* menggunakan Metode Probabilitas dan Statistik, yang memprediksi peluang masa depan berdasarkan pengalaman sebelumnya untuk apa yang disebut Teorema *Bayes* adalah dengan gabungan *Naive*, dengan asumsi bahwa kondisi antar atribut adalah independen. Klasifikasi *Naive Bayes* mengasumsikan bahwa ada tidaknya karakteristik tertentu dari satu kelas tidak ada hubungannya dengan karakteristik kelas lainnya [12].

2.3. Perhitungan Akurasi

Perhitungan ini dilakukan berdasarkan hasil pengujian menggunakan 3 *tool Kali linux, WireShark*, dan *Nmap*. Pengujian akan dilakukan sebanyak 10 kali pada setiap *tool*, percobaan ini ditentukan dari perbandingan penelitian yang serupa dengan beragam jumlah percobaan baik dari 5 kali, 10 kali, dan 76 kali. Maka pada penelitian ini penulis memutuskan mengambil jumlah percobaan 10 kali dimana tidak terlalu sedikit dan tidak terlalu banyak [13], [14]. Untuk mendapatkan perhitungan rata-rata akurasi menggunakan persamaan (1) [13].

Rata-rata akurasi:

$$Akurasi = \frac{prediksi\ yang\ benar}{Total\ percobaan} x100\% \quad (1)$$

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 [15]. Penelitian ini sudah menentukan *Threshold Limit Value* sebesar 70% [15]. Penentuan nilai *Threshold Limit Value* dari referensi yang diambil sesuai dengan gambaran dari penelitian yang akan diangkat. *Threshold Limit Value* tersebut didapatkan dari perbandingan antara penelitian lain yang menentukan *Threshold Limit Value* 30%, 70%, dan 87,5% [15]{Formatting Citation}. 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.

3. Hasil dan Analisis

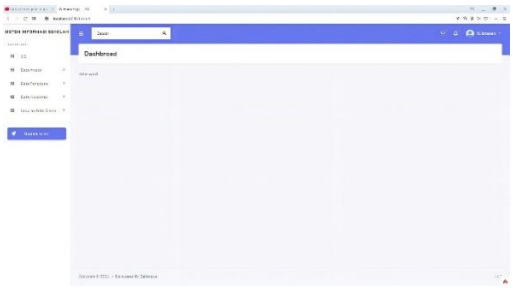
3.1. Fase *Planning and Preparation*

Fase *Planning and Preparation* merupakan fase awal untuk menentukan kesepakatan pemilik sistem informasi dimana saat ini Sistem Informasi Sekolah MTsN 8 Bantul masih dipegang oleh PT. Solusi 247. Instansi ini merupakan tempat yang pernah digunakan untuk kegiatan Merdeka Belajar Kampus Merdeka (MBKM) Bentuk Kegiatan Pembelajaran (BKP) Magang Industri dimana pembuatan Sistem Informasi Sekolah MTsN 8 Bantul dibuat.

Proses persetujuan tersebut dilakukan dengan pemberian surat izin pengambilan data Sistem Informasi Sekolah MTsN 8 Bantul untuk kegiatan penelitian yang diberikan dari Fakultas Universitas ‘Aisyiyah Yogyakarta. Surat tersebut dibuat sebagai prosedur resmi dari pihak universitas yang bertujuan untuk menghindari penyalahgunaan sistem yang akan digunakan

3.2. 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 Sistem Informasi Sekolah MTsN 8 Bantul yang berbasiskan *Localhost* dimana dapat diakses melalui localhost:8080/SIS. Sistem ini berbasiskan *Localhost* maka hanya dapat diakses melalui *server* lokal saja. Sistem Informasi Sekolah MTsN 8 Bantul berperan sebagai *guest* dengan tampilan dari Sistem Sistem Informasi Sekolah MTsN 8 Bantul seperti Gambar 2.



Gambar 2. Sistem Informasi Sekolah MTsN 8 Bantul

Gambar 3. IP Gateway

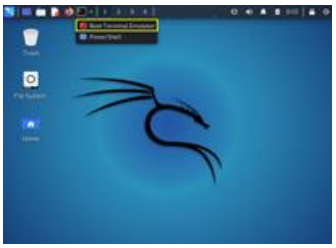
Sistem Informasi Sekolah MTSN 8 Bantul masih berbasis *Localhost*, sehingga pengujian sistem informasi ini dilakukan dengan menggunakan *IP Getaway* dari *host* yaitu 192.168.56.1 dan *IP Localhost* yaitu 127.0.0.1 [18] seperti Gambar 3

IP tersebut merupakan kepemilikan dari *Localhost* yang dapat digunakan untuk mencari tahu informasi dari tampilan komputer, selain itu *Localhost* juga dapat digunakan untuk mengecek fungsional dari *website* maupun *web* yang sudah terinstal di komputer (Sinaga, 2009). Fase ini adalah fase inti dari penelitian dimana proses dari *Penetration Test* akan dilakukan pada fase ini. Metodologi Penelitian sudah dipaparkan mengenai 3 *tool* yang akan digunakan untuk *Penetration Test* untuk mengetahui kerentanan dari Sistem Informasi Sekolah MTsN 8 Bantul.

a. *Kali linux*

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 [19]. Sedangkan *Nmap* memiliki fungsi untuk melakukan *port scanning* [20]. Proses instalasi *Virtual Machines Kali linux* pada *Virtualbox* sudah selesai. Langkah selanjutnya adalah pengimplementasian *Metasploit* pada *Kali linux* yang dilakukan sebagai berikut:

1. Langkah pertama buka *Root Terminal Emulator* seperti Gambar 4.



Gambar 4. Tampilan *Kali linux*

2. Langkah selanjutnya adalah mengaktifkan *console msf* atau *Metasploit* dengan memberikan perintah “*msfconsole*” di *Root Terminal Emulator* yang telah dibuka seperti Gambar 5.

Gambar 5.* Pengaktifan *Metasploit

3. Langkah selanjutnya berikan perintah "*search* vsftpd" pada *Root Terminal Emulator*,seperti Gambar 6.

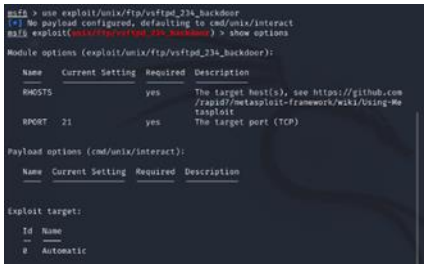
Gambar 6. *Search* vsftpd

Syntax ini memiliki fungsi untuk mengetahui detail dari *vsft* atau *FTP Server* yang ada pada *exploit* beserta dengan *rank* indikasi tingkat keberhasilan *exploit* yaitu *excellent*. Hasil dari detail *vsft* dapat di-*Copy* sebagai berikut "*exploit/unix/ftp/vsftpd_234_backdoor*".

4. *Copy* detail *vsft*, *paste* dan tambahkan *use* sebelum *syntax* dari detail *vsft*. *use "exploit/unix/ftp/vsftpd_234_backdoor*". *Syntax* ini bertujuan agar *exploit* dapat terbuka ke dalam *msf*, seperti Gambar 7.

Gambar 7. Use Exploit

5. Langkah selanjutnya masukkan *syntax "show options"* pada *Root Terminal Emulator* untuk menampilkan konfigurasi yang mengatur *exploit* seperti Gambar 8.

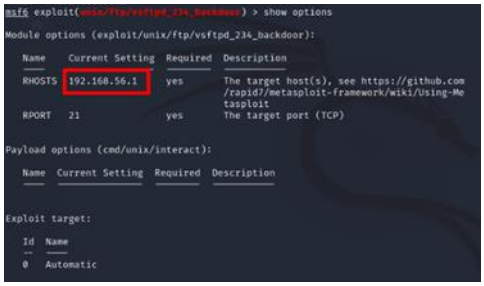


Gambar 8. *Show Options*

6. Langkah selanjutnya pada *RHOSTS* target belum dimasukkan. Target dapat dimasukkan dengan cara memberikan *IP* dengan *syntax* "*set RHOST"* 192.168.56.1 seperti Gambar 9.

Gambar 9. *RHOSTS*

7. Langkah selanjutnya memasukkan target pada *RHOSTS*, masukkan kembali *syntax "show options"* pada *Root Terminal Emulator* untuk memastikan bahwa target sudah berhasil dimasukkan seperti Gambar 10.



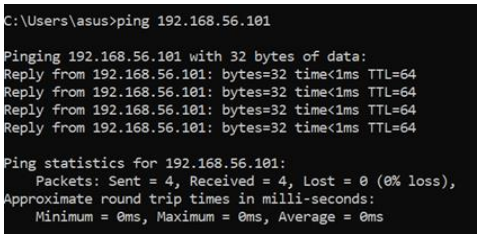
Gambar 10. Show Options

8. Langkah selanjutnya yaitu ketikkan "*run"* pada *Root Terminal Emulator* untuk mengeksekusi target. Percobaan yang dilakukan sebanyak 10 kali.

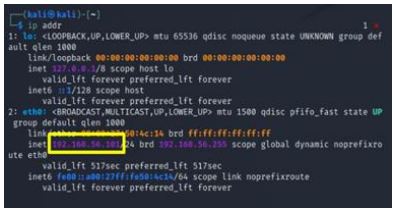
Hasil yang didapatkan dari 10 kali percobaan *Penetration Test* adalah *Exploit failed [unreachable]*.
Proses implementasi *Metasploit* pada *Kali linux* sudah selesai. Langkah selanjutnya adalah pengimplementasian *Nmap* pada *Kali linux.*

1. Langkah pertama adalah buka buka *Root Terminal Emulator* seperti Gambar 4.
2. Langkah selanjutnya masukkan perintah "*nmap* -v -A -sV 192.168.56.1." Percobaan yang dilakukan sebanyak 10 kali.

Fungsi dari "*nmap* -v -A -sV 192.168.56.1" adalah untuk menjalankan *Nmap* pada *Kali linux*. 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 11.

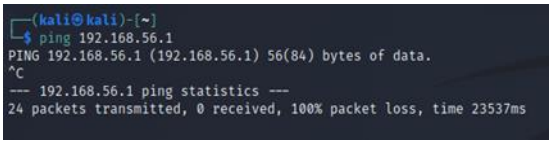


Gambar 11. *Ping* pada Windows



Gambar 12. Pengecekan IP pada *Kali linux*

Gambar 11 menunjukkan hasil "ping 192.168.56.101" berhasil dilakukan dengan keterangan *Lost* 0%. Hal ini berarti *Network* dari *Windows* ke *Kali linux* berhasil terhubung. *IP* 192.168.56.101 untuk melakukan *ping* pada *Kali linux* didapatkan dari pengecekan *IP* di *Kali linux* menggunakan *"ip addr*" pada *Terminal Kali linux* seperti Gambar 12.
Langkah selanjutnya lakukan *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 13.



Gambar 13. Ping pada *Kali linux*

Hasil yang didapatkan adalah ping dari *Kali linux* ke *Windows* adalah gagal. Hal ini dapat berarti bahwa *Network Kali linux* ke *Windows* gagal dengan keterangan *loss 100%* seperti Gambar 13.

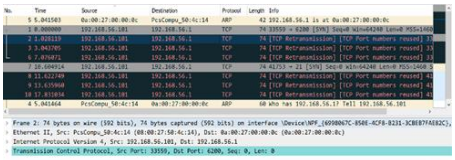
b. *WireShark*

WireShark digunakan untuk *Tool Penetration Test* pada Sistem Informasi Sekolah MTsN 8 Bantul dengan membutuhkan *Local Area Conection* dimana sistem yang akan diteliti ini masih dalam *Localhost.*
Langkah implementasi *Penetration Test seperti berikut:*

1. Akses *website* resmi dari *WireShark* https://www.*WireShark*.org/download.html
2. tampilan dari *WireShark* seperti Gambar 14.

Gambar 14. Tampilan *WireShark*

3. Karena *interface* untuk mengakses langsung sistem tidak tersedia maka pilih *Interface VirtualBox Host-Only Network.* Tujuannya untuk mencari tahu arus lalu lintas yang terjadi pada *VirtualBox* ketika dilakukan *Penetration Test* menggunakan *Metasploit* dan *Nmap* seperti Gambar 15.



Gambar 15. Hasil Lalu Lintas pada *Kali linux*

Pastikan *Interface VirtualBox Host-Only Network* sudah berjalan ketika proses penyerangan pada *Kali linux* berlangsung. Hasil yang muncul seperti Gambar 15 terdapat *TCP Retransmission* yang ada pada *Port TCP 33559* berjumlah 7.

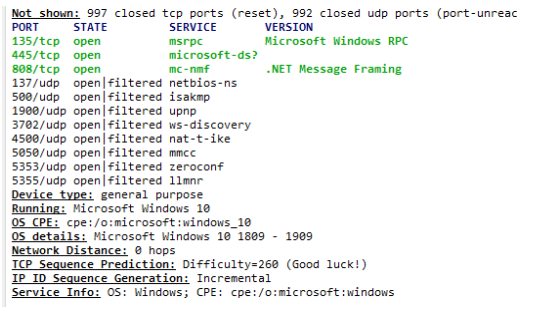
c. *Network Mapper (Nmap)*

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. Masukkan *IP Localhost* seperti Gambar 16.

Gambar 16. *Scan Zenmap*

2. Hasil dari *scan IP* dengan percobaan yang dilakukan sebanyak 10 kali menggunakan *ZeNmap* didapatkan hasil yang konsisten yaitu ada 3 *port tcp* yang terbuka. 3 *Port* yang terbuka terdiri dari *port* 135, 445, dan 808. 8 *port udp* juga ditemukan dengan status *open* namun ter-*filter* yaitu 137, 500, 1900, 3702, 4500, 5050, 5353, dan 5355, seperti Gambar 17 dam 18.



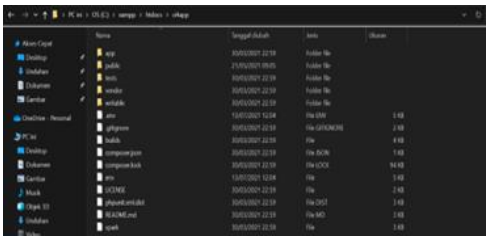
Gambar 17. Hasil scan IP

```
Not shown: 997 closed tcp ports (reset), 992 closed udp ports (port-unreac
PORT     STATE         SERVICE       VERSION
135/tcp  open          msrpc         Microsoft Windows RPC
445/tcp  open          microsoft-ds?
808/tcp  open          mc-nmf        .NET Message Framing
137/udp  open|filtered netbios-ns
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 1909
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Gambar 18. Hasil scan IP 2

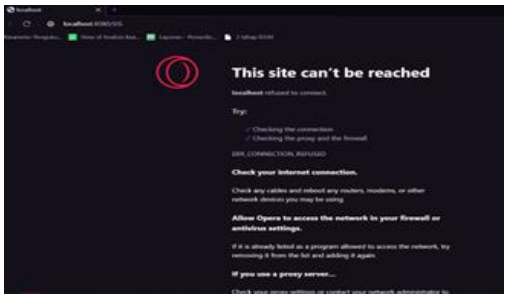
3.3. Fase *Reporting* dan *Clean Up and Destroy Artifacts*

Fase ini merupakan fase akhir kelanjutan dari Fase *Assessment* dengan melaporkan serta menghancurkan semua jejak/bukti aktivitas penetrasi. Fase *Reporting* dan *Clean Up and Destroy Artefacts* dilakukan pelaporan terhadap pihak PT. Solusi 247 bahwa sistem sudah berhasil diserang dan disampaikan bahwa sistem dikatakan aman berdasarkan *Penetration Test* pada *Nmap.* Selain itu proses penghapusan seluruh hal yang berkaitan dengan target yaitu Sistem Informasi Sekolah MTsN 8 Bantul seperti Gambar 19 hingga Gambar 21.



Gambar 19. File Sistem Informasi Sekolah sebelum Dihapus

Gambar 20. File Sistem Informasi Sekolah setelah Dihapus



Gambar 21. Pengecekan Akses Sistem

Pengecekan mengenai keberadaan Sistem Informasi Sekolah MTsN 8 Bantul seperti Gambar 14 yang dilaporkan kepada pihak PT. Solusi 247. Proses ini dilakukan untuk membuktikan secara langsung mengenai hilangnya akses untuk Sistem Informasi Sekolah MTsN 8 Bantul dan fase ini merupakan fase terakhir pada proses penelitian yang dilakukan menggunakan *ISSAF*.

3.4. Perhitungan Akurasi

Hasil *Penetration Test* dari 3 *tool* yang telah diuji, menampilkan hasil *Nmap* pada *Windows* saja yang dapat menghasilkan keluaran yang dapat dihitung akurasinya menggunakan *Naive Bayes*. Perhitungan akurasi pada *Nmap* menggunakan rumus Persamaan yang dapat diimplementasikan di setiap percobaan pada *Nmap* dengan memasukkan angka 8 yang berasal dari jumlah *port TCP open-filter* dan 11 dari total jumlah data yang muncul baik *open* maupun *open-filter.*

Rata-rata akurasi dari semua percobaan akan dihitung menggunakan Persamaan 2.

$$rata - rata = \frac{\sum_{p=1}^{n} p}{n} \quad (2)$$

Keterangan:
P = Hasil perhitungan setiap percobaan
N = Banyaknya percobaan

Hasil perhitungan dari 10 kali percobaan dengan *Nmap* dimasukan ke Persamaan 1 seperti Tabel 1.

Tabel 1. Perhitungan Akurasi Seluruh Percobaan

Percobaan	Perhitungan
1	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
2	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
3	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
4	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
5	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
6	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
7	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
8	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
9	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$
10	$\frac{8}{11} = 0.7272\ x\ 100 = 72{,}72\%$

Maka diperoleh nilai rata-rata akurasi menggunakan perhitungan dari *Penetration Test* menggunakan *Nmap* pada Window adalah sebesar 72,72%. Hasil akurasi yang didapatkan melebihi dari *Threshold Limit Value* yang

sudah ditentukan yaitu sebesar 70%, maka Sistem Informasi Sekolah MTsN 8 Bantul dikatakan aman dari serangan yang dilakukan menggunakan *Tool Nmap* pada *Windows*. Pada penelitian sebelumnya didapatkan perhitungan menggunakan *Threshold Limit Value* dari *Tool WireShark* menggunakan *IPSEC* [17]. *Tool* ini digunakan untuk *Tools* yang digunakan untuk *analysis traffic* dan *sniffing* dengan *Threshold Limit Value* sebesar 30%. Penelitian pula yanng dijadikan acuan penentuan besaran *Threshold Limit Value* seperti yang sudah dijelaskan pada subab 2.2. Sedangkan pada *Tool* lainnya terdapat hasil seperti Tabel 2.

Tabel 2 membahas tentang persentase akurasi yang berhasil dari pengujian *Penetration Test* menggunakan 4 *Tool* yaitu *Kali linux, Nmap* pada *Kali linux*, dan *WireShark* dimana tidak memunculkan hasil yang diinginkan. Hasil *Penetration Test* dari 3 *Tool* tersebut gagal karena sistem informasi masih berbasis *Localhost* sehingga *Penetration Test* yang yang dilakukan terhalang oleh *firewall* yang ada pada komputer dan *Localhost*. Sedangkan *Nmap* pada Windows berhasil memunculkan hasil yang diinginkan dengan hasil akurasi 72,72% sesuai dengan perhitungan pada Tabel 1.

Tabel 2. Perbandingan *Tool Penetration Test*

Tool	Pengimplementasian	Hasil Penetration Test	Akurasi
Kali linux	Kali linux	✗	0%
Nmap	Kali linux	✗	0%
WireShark	WireShark	✗	0%
Nmap	Zenmap	✓	72,72%

4. Kesimpulan

Pengujian yang dilakukan dengan *Kali linux* dengan *Metasploit* sebagai implementor mendapatkan hasil *Loss* 100% atau tidak ada celah yang terdeteksi, hal ini menunjukkan bahwa *Kali linux* tidak memiliki fitur untuk memunculkan *port* yang terbuka. Hasil pengujian dengan *WireShark* menunjukkan *WireShark* tidak dapat melakukan *Penetration Test* karena tidak memiliki *support* untuk melakukan *capturing* pada *Localhost*. Pengujian yang dilakukan menggunakan *Nmap* dengan menggunakan aplikasi *Zenmap* menemukan celah keamanan sebanyak 3 *port tcp* yang terbuka terdiri dari *port* 135, 445, dan 808. Hasil pengujian juga menunjukkan terdapat 8 *port* yang terbuka namun memiliki *filter*. Pengujian dilakukan sebanyak 10x dan mendapatkan hasil yang sama, hasil tersebut kemudian dihitung menggunakan *Naive Bayes* untuk mengetahui akurasi dari *Tool* yang digunakan.

Hasil yang didapatkan dari perhitungan akurasi tersebut sebesar 72,72% dimana nilai ini melampaui ambang batas atau *Threshold Limit Value* sebesar 70%. Hasil Efektifitas *tool* juga dapat dilihat dengan hasil yang didapatkan yaitu hanya terdapat 1 *tool* yang menampilkan hasil yang diinginkan yaitu *tool Nmap* pada *Windows*. Hasil ini mengindikasikan Sistem Informasi Sekolah MTsN 8 Bantul aman dari proses *Penetration Test* sehingga Sistem Informasi Sekolah MTsN 8 Bantul dinyatakan siap diluncurkan.

Referensi

[1] F. Magaline, B. N. Mahamudu, and E. Ho, "Konsep Dasar Aristektur Dan Klasifikasi Sistem Informasi," *Sist. Inf.*, pp. 1–7, 2019.

[2] N. Hayaty, "Buku Ajar : Sistem Keamanan," p. 99, 2020.

[3] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[4] T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *J. Ilm. NERO*, vol. 1, no. 3, pp. 190–197, 2015, [Online]. Available: http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27.

[5] R. L. B. Yudiana, Anggi Elanda, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada Stmik Rosma Dengan Menggunakan Owasp Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, pp. 37–43, 2021.

[6] T. Dirgahayu, Y. Prayudi, and A. Fajaryanto, "Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server," *Jurnal Ilmiah NERO*, vol. 1, no. 3. pp. 190–197, 2015, [Online]. Available: http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27.

[7] R. S. Nugraha, "Sistem Informasi Sekolah Surakarta Berbasis Website," *Appl. Microbiol. Biotechnol.*, vol. 85, no. 1, pp. 2071–2079, 2016.

[8] B. D. Permana, T. M. Fauzi, and M. Faiz, "Implementasi Sniffing Pada Jaringan HTTP Menggunakan Wireshark," no. December, 2021.

[9] D. Bayu Rendro and W. Nugroho Aji, "Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software Nmap (Studi Kasus Di Smk Negeri 1 Kota Serang)," *PROSISKO J. Pengemb. Ris. dan Obs. Sist. Komput.*, vol. 7, no. 2, pp. 108–115, 2020, [Online]. Available: https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/2522.

[10] I. G. A. S. Sanjaya, G. M. A. Sasmita, and D. M. S. Arsa, "Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF," *J. Ilm. Merpati*, vol. 8, no. 2, pp. 113–124, 2020.

[11] T. Syarif Revolino and D. Jatmiko Andri, "Analisis Perbandingan Metode Web Security Ptes , Issaf Dan Owasp Di Dinas Komunikasi Dan Informasi Kota Bandung," p. 8, 2019, [Online]. Available: https://elibrary.unikom.ac.id/880/13/21.10112427_TIO REVOLINO SYARIF_JURNAL BAHASA INDONESIA.pdf.

[12] Y. Adani, P. Studi, S. Informasi, and A. N. Baye, "Penerapan Algoritma Naive Bayes Untuk Memprediksi," pp. 13–24.

[13] J. Chandra, H. Hermanto, and A. Rahman, "Deteksi Serangan Port Scanning Menggunakan Algoritma Naive

Bayes," *Core.Ac.Uk*, no. x, pp. 1–12, 2012, [Online]. Available: https://core.ac.uk/download/pdf/153523864.pdf.

[14] S. R. Niko Suwaryo, Ismasari Nawangsih, "Deteksi Serangan pada Intrusion Detection System (IDS) untuk Klasifikasi Serangan dengan Algoritma Naïve Bayes, C.45 dan K-NN dalam Meminimalisasi Resiko Terhadap Pengguna," *Angew. Chemie Int. Ed. 6(11), 951–952.*, pp. 2013–2015, 2021.

[15] I. Iskandar, E. Resdifa Jurusan Teknik Informatika, F. Sains dan Teknologi, U. H. Sultan Syarif Kasim Riau Jl Soebrantas No, and S. Baru, "Penerapan Metode Radial Basis Function Dengan Jumlah Center Dinamis Untuk Klasifikasi Serangan Jaringan Komputer," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 5, no. 2, pp. 78–85, 2020, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/coreit/article/view/8193.

[16] I. G. N. A. Sucipta, I. M. W. Wirawan, and A. Muliantara, "Analisis Kinerja Anomaly-Based Intrusion Detection System (IDS) Dalam Mendeteksi Serangan Dos (Denial of Services) Pada Jaringan Komputer," *Anal. Kinerja Anomaly-Base Intrusion Syst.*, vol. 1, no. 2, pp. 8–13, 2013.

[17] N. A. Reza Arlan1, Rendy Munadi2, "Implementasi dan Analisis Sistem Keamanan IP Security (Ipsec) di dalam Multi Protocol Label Switching-Virtual Private Network (MPLS-VPN) pada Layanan Berbasis IP Multimedia Subsystem (IMS) Implementation," vol. 3, no. July, pp. 1–23, 2016.

[18] A. Lincoln, "Lab 4 : Metasploit Framework."

[19] Offensive Security, "Penetration Testing with Kali Linux v1.0.1," *Penetration Test.*, p. 361, 2014.

[20] M. Marsoni, T. U. Kalsum, and A. Kurniawan, "Analisa Implementasi Teknik Reconnaissance Pada Webserver (Studi Kasus: Upt Puskom Universitas Dehasen)," *J. Media Infotama*, vol. 12, no. 1, pp. 11–20, 2016, doi: 10.37676/jmi.v12i1.268.