Jejakdigital
JURNAL ILMIAH MULTIDISIPLIN
Available online at https://indojurnal.com/index.php/jejakdigital

eISSN 3089-7734; pISSN 3089-7742
Vol. 1, No. 4b, Tahun 2025
doi.org/10.63822/sht2dr90
Hal. 2127-2137

Pengujian Penetrasi Jaringan Lokal dengan Metasploit Framework

Fadhil Aditya[1], Andi Mahrani[2], Rakhmadi Rahman[3]
Institut Teknologi Bacharuddin Jusuf Habibie Parepare, Indonesia[1,2,3]

*Email Korespodensi: fadhiladitya551@gmail.com

Sejarah Artikel:

Diterima 01-07-2025
Disetujui 07-07-2025
Diterbitkan 09-07-2025

ABSTRACT

Local network security is a vital component in maintaining the integrity and confidentiality of data in information systems. This study aims to identify and evaluate the vulnerability of the Windows 7 operating system through penetration testing using the Metasploit Framework. The method used is an experiment with attack si mulation in a controlled virtual environment. The test target is a Windows 7 system that has not received the MS17-010 security patch and still activates the SMBv1 protocol. The EternalBlue exploit (CVE-2017-0144) is used to exploit the vulnerability. The test results show that the exploitation was successful, marked by the acquisition of Meterpreter shell access to the target system, as well as the ability to retrieve system information and desktop screenshots. These findings confirm that systems that have not been updated are highly vulnerable to remote code execution attacks. This study recommends the application of security patches, disabling SMBv1, and configuring firewalls as crucial mitigation steps. The results of this study are expected to be a reference in the practice of evaluating local network security, especially in infrastructure that still uses old operating systems.

Keywords: *Penetration Testing, Local Network, Metasploit Framework, Network Security, System Exploitation*

Bagaimana Cara Sitasi Artikel ini:

Fadhil Aditya, Andi Mahrani, & Rakhmadi Rahman. (2025). Pengujian Penetrasi Jaringan Lokal dengan Metasploit Framework. Jejak Digital: Jurnal Ilmiah Multidisiplin, 1(4b), 2127-2137. https://doi.org/10.63822/sht2dr90

PENDAHULUAN

Di era digital yang terus berkembang pesat, keamanan jaringan menjadi aspek yang sangat krusial, terutama bagi berbagai jenis organisasi atau instansi. Jika sistem jaringan tidak memiliki perlindungan yang memadai, risiko yang dihadapi cukup besar—mulai dari pencurian data, gangguan sistem, hingga berbagai aksi berbahaya lainnya dari pihak yang tidak bertanggung jawab. Oleh karena itu, pengujian terhadap ketahanan sistem keamanan menjadi langkah penting untuk mengidentifikasi dan menutup potensi celah yang dapat dimanfaatkan oleh penyerang.

Salah satu metode yang umum digunakan untuk menguji keamanan jaringan adalah penetration testing atau uji penetrasi. Teknik ini mensimulasikan serangan terhadap sistem atau jaringan untuk mengungkap titik-titik lemah yang berpotensi dieksploitasi. Hasil dari pengujian ini memungkinkan administrator jaringan untuk mengetahui bagian mana saja yang perlu diperbaiki guna meningkatkan perlindungan sistem secara keseluruhan.

Dalam pelaksanaannya, uji penetrasi seringkali dibantu oleh sebuah alat bernama Metasploit Framework. Ini merupakan platform open-source yang menyediakan beragam modul dan eksploit yang dirancang khusus untuk mengidentifikasi kerentanan dalam sistem. Popularitas Metasploit cukup tinggi di kalangan praktisi keamanan karena kemampuannya dalam melakukan serangan secara terstruktur sekaligus menghasilkan laporan evaluasi yang komprehensif.

Penelitian ini difokuskan pada penerapan uji penetrasi terhadap jaringan lokal dengan memanfaatkan Metasploit Framework. Tujuan utamanya adalah mengevaluasi tingkat keamanan jaringan tersebut serta mengidentifikasi kelemahan yang ada. Diharapkan, hasil pengujian ini dapat memberikan dasar yang kuat untuk melakukan perbaikan dan memperkuat sistem keamanan jaringan lokal yang digunakan.

TINJAUAN PUSTAKA

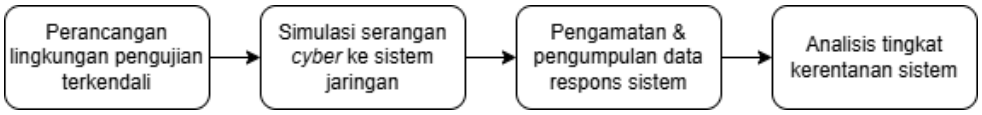
Kali Linux

Kali Linux, merupakan alat untuk *Operating System* yang digunakan dalam virtualisasi menggunakan Virtualbox yang digunakan untuk melakukan hacking. [1]

a. Netdiscover. Netdiscover merupakan sebuah tool yang dapat digunakan untuk proses scanning dalam pencarian IP. [2]
b. Nmap. Nmap merupakan sebuah tool yang dapat digunakan untuk melakukan port scanning.[2]
c. Metasploit *Framework.* Metasploit *framework* adalah platform pengujian penetrasi yang memungkinkan penyerang menemukan, mengeksploitasi, dan memvalidasi kerentanan. Selain itu, menyediakan infrastruktur, konten, dan alat untuk melakukan uji penetrasi dan audit keamanan yang komprehensif. [3]

METODE PENELITIAN

Metode penelitian yang di gunakan dalam pengujian penetrasi jaringan lokal dengan metasploit framework adalah metode eksperimen dengan melakukan pengujian langsung terhadap perangkat jaringan yang digunakan dalam sebuah lingkungan yang telah dirancang secara terkendali. Lingkungan ini memungkikan proses pengujian berjalan secara aman tanpa mengganggu sistem jaringan yang sebenarnya, namun tetap mempresentasikan kondisi nyata dari sebuah jaringan lokal.



Dalam pelaksnaanya, metode ini melibatkan simulasi serangan siber terhadap perangkat-perangkat jaringan guna mengamati respons sistem terhadap berbagai ancaman yang mungkin terjadi. Melalui pendekatan eksperimental ini, diperoleh data yang mendalam mengenai bagaimana sistem bekerja saat mengahadapi upaya eksploitasi atau akses tidak sah. Hasil dari pengujian ini kemudian digunakan untuk mengevaluasi tingkat kerentanan jaringan yang diuji.

HASIL DAN PEMBAHASAN

Melakukan pengujian penetrasi secara langsung terhadap jaringan lokal menggunakan eksploit EternalBlue adalah pendekatan strategis untuk mengevaluasi dan mengungkap kerentanan keamanan sistem operasi lama seperti Windows 7. Berikut langkah-langkah dalam pengujian penetrasi jaringan lokal menggunakan metasploit *framework* dengan target berhasil masuk di windows 7.

langkah pertama yang kita lakukan adalah dengan melakukan scanning pada jaringan lokal saya untuk mendapatkan ip dari target, dapat dilihat pada gambar di atas, target kita pada bagian ini adalah windows 7 yang ip addressnya **192.168.1.18**

Gambar 1 Scanning Ip Address

setelah mendapatkan ip address dari target selanjutnya kita akan melakukan scanning apakah target memiliki celah keamanan pada protokol server message block versi 1 (SMBv1) namun pertama tama yang perlu kita lakukan adalah dengan menjalankan metasploit framework consolenya terlebih dahulu untuk menjalankan metasploit, kita bisa mengetikkan perintah **msfconsole**

Gambar 2 Jalankan Metasploit

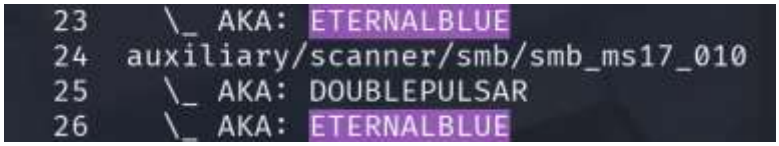
setelah memasukkan perintah di atas, kita akan masuk pada msfconsole

Gambar 3 Tampilan Awal msfconsole

gambar di atas adalah tampilan awal ketika masuk ke **msfconsole**, di sini kita bisa mencari dan menggunakan 2496 module exploit dan 1283 modul tambahan (auxiliary), pada kasus ini kita akan menggunakan modul eternal blue, oleh karena itu langkah selanjutnya adalah mencari modul eternal blue dengan memasukkan perintah seperti pada gambar di bawah.

Gambar 4 Scanning Ip Address

dapat dilihat pada gambar di atas kalau modul EternalBlue ditandai dengan nomor 0, namun sebelum menggunakannya kita akan melakukan scanning terlebih dahulu apakah terdapat celah keamanan pada target, untuk melakukan scanning, kita akan menggunakan module auxiliary/scanner/smb/smb_ms17 yang ditandai dengan nomor 24 pada gambar di bawah.



Gambar 5 Modul EternalBlue

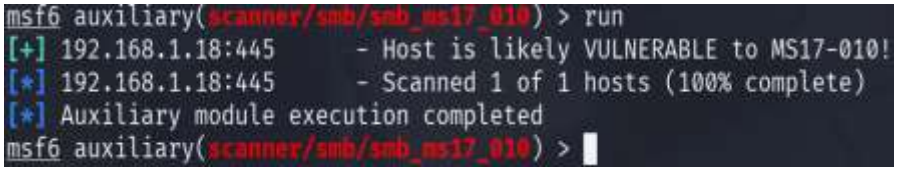
untuk menggunakan modul nya masukkan perintah use 24

Gambar 6 melakukan perintah use 24

secara otomatis kita akan masuk ke modulnya, langkah selanjutnya adalah dengan memasukkan **RHOST** yang merupakan Ip dari target.

Gambar 7 RHOTS

sekarang **RHOST** sudah di set menjadi ip dari target, selanjutnya masukkan perintah run untuk menjalankan scanning

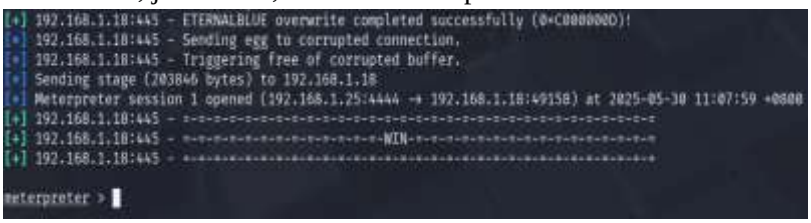


Gambar 8 Run

dapat dilihat pesan pada gambar di atas kalau target kemungkinan besar memiliki celah keamanan terhadap **MS17-010** langkah selanjutnya adalah menggunakan module exploit eternalblue nya dengan memasukkan perintah **use 0**

Gambar 9 module exploit eternalblue

lakukan langkah seperti saat menggunakan module sebelumnya dengan **set RHOSTS** menjadi ip target seperti pada gambar di atas, jika sudah, lalu masukkan perintah run



Gambar 10 berhasil masuk ke komputer target!

exploit successfully! kita telah berhasil masuk ke komputer target! dapat dilihat pada gambar di atas ip kita berubah menjadi ip target dan sekarang kita masuk ke meterpreter dimana kita bisa memasukkan banyak perintah untuk mengambil informasi yang ada pada komputer target mari kita coba dengan memasukkan perintah **sysinfo**

Gambar 11 Informasi dari komputer target

pada gambar di atas menunjukkan informasi dari komputer target yang hanya bisa diakses ketika kita berhasil masuk ke komputer target kita coba 1 lagi perintah untuk mengambil screenshot dengan memasukkan perintah screenshot

```
meterpreter > screenshot
Screenshot saved to: /home/dyl/UyuBUXuU.jpeg
meterpreter >
```

Gambar 12 Screnshot hasil

Gambar 13 Windows 7

ini adalah hasil screenshot windows 7 yang diambil dari kali linux

Hasil

1. Temuan Utama
   a) Berhasil melakukan eksploitasi CVE-2017-0144 (EternalBlue) pada Windows 7 melalui protokol SMBv1
   b) Bukti keberhasilan:
   Akses Meterpreter shell (lihat Gambar 12).

   Berhasil mengambil informasi sistem (sysinfo) dan screenshot (Gambar 13).
   c.) Sistem target tidak memiliki patch MS17-010 dan mengaktifkan SMBv1 secara default.
2. Analisis kerentanan

a) Penyebab:

Protokol SMBv1 yang tidak di-patch memungkinkan eksekusi kode jarak jauh (RCE).

Firewall Windows tidak memblokir port 445 (SMB).

3. Dampak:

Penyerang dapat mengambil alih sistem, mencuri data, atau menginstal malware.

4. Data Pendukung:

Kerentanan	CVE	Dampak	Kondisi Target
EternalBlue (SMBv1)	CVE-2017-014	Remote Code Execution	Windows 7 SP1 tanpa patch

Rekomendasi Keamanan

1. Untuk administrator jaringan

a. Patch management

Instal patch MS17-010 dari Microsoft Update.

Nonaktifkan SMBv1 dengan perintah:

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

b. Konfigurasi Firewall

Blokir port 445 (SMB) kecuali untuk kebutuhan kritis.

Gunakan Network Segmentation untuk isolasi perangkat rentan.

2. Best practice untuk windows 7

a. Upgrade OS: Ganti Windows 7 dengan versi yang masih didukung (Windows 10/11).

b. Minimalkan Eksposur:

Matikan layanan tidak perlu (RDP, SMB) jika tidak digunakan.

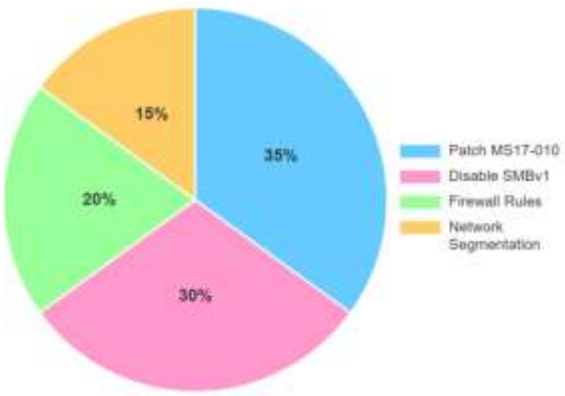
Gunakan Akun dengan Privilege Minimal (non-administrator).

c.Monitoring dan Deteksi:

Gunakan SIEM tools (seperti Wazuh/Splunk) untuk memantau upaya eksploitasi SMB.

Aktifkan Windows Event Logging untuk mencatat aktivitas mencurigakan.

3. Grafik Rekomendasi

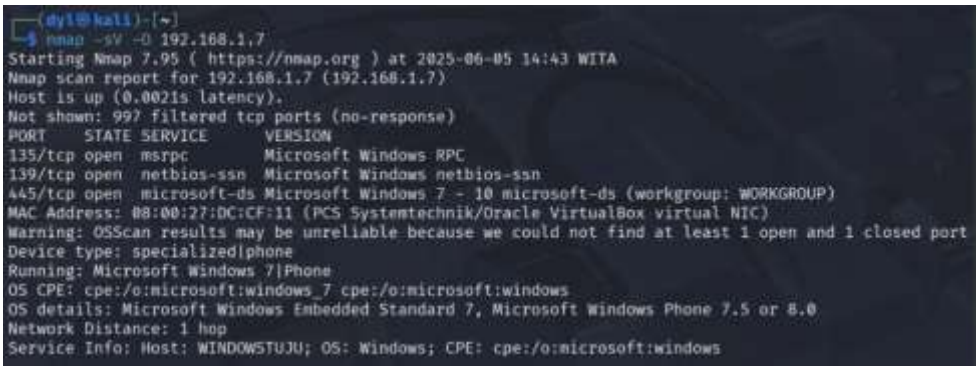


Gambar 14 Grafik Rekomendasi

Setelah melakukan pengujian penetrasi terhadap beberapa perangkat yang terhubung dalam jaringan lokal, ditemukan sejumlah kerentanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk mengakses sistem secara tidak sah. Berdasarkan temuan tersebut, pada bab ini akan disusun rancangan keamanan jaringan yang bertujuan untuk meminimalkan risiko serangan serupa di masa mendatang. Rancangan ini disusun sebagai tindak lanjut dari hasil pengujian sebelumnya:

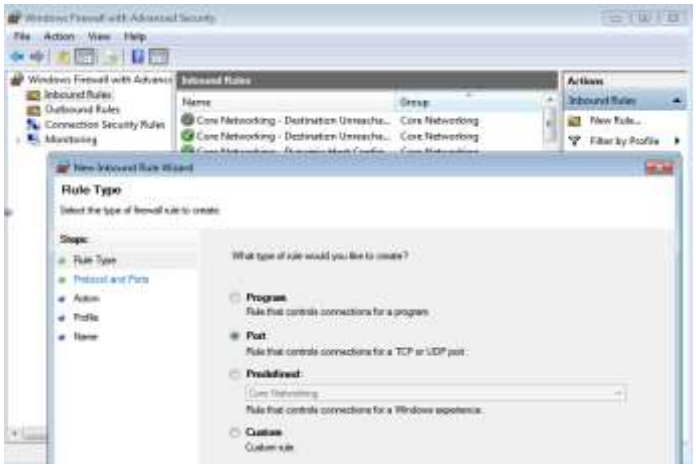
1. Implementasi Keamanan Jaringan pada Windows 7

Sebelumnya ketika kita melakukan scanning pada windows 7, kita mendapati beberapa port yang terbuka seperti port 135, 139 dan 445, dapat dilihat pada gambar di bawah. Terbukanya port ini bisa menjadi celah keamanan pada mesin



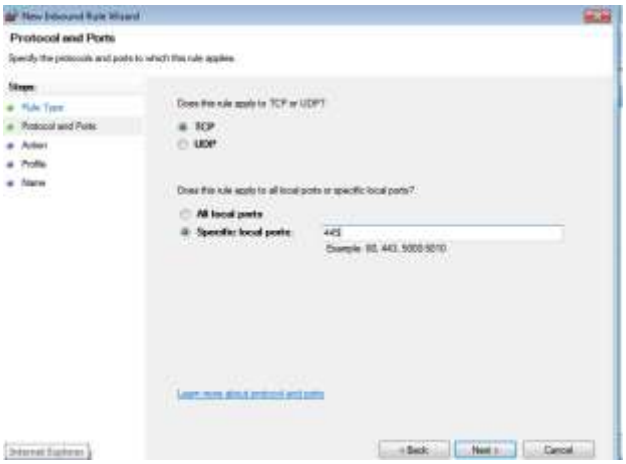
Gambar 15 Port yang terbuka

Untuk mengatasinya kita dapat masuk ke **firewall with advanced security** lalu click **Inbound Rules**, di sebelah kanan klik **New Rule..**, pada opsi **Rule Type** pilih yang **Port** seperti gambar di bawah

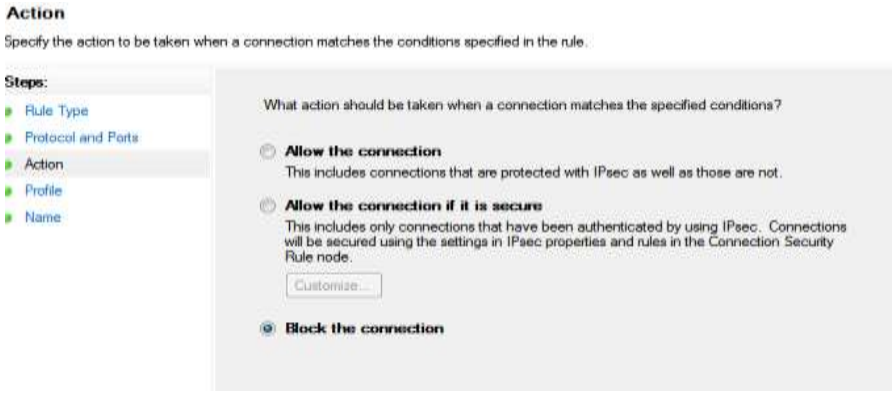


Gambar 16 Rule Type

selanjutnya pada opsi **Protocol and Ports** pilih yang TCP dan masukkan port yang ingin di block, di sini bisa memilih apakah ingin block semua port atau hanya port spesifik saja, pada praktik ini saya memasukkan port yang spesifik yaitu 445, jika sudah tekan **next**

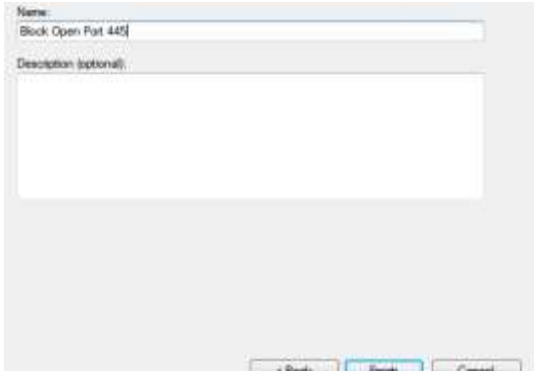


Gambar 17 Protocol and Ports



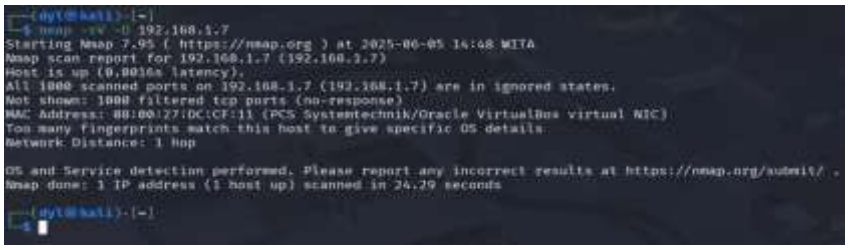
Gambar 18 Action

Pada bagian **Action** pilih opsi **Block the connection** seperti gambar di atas



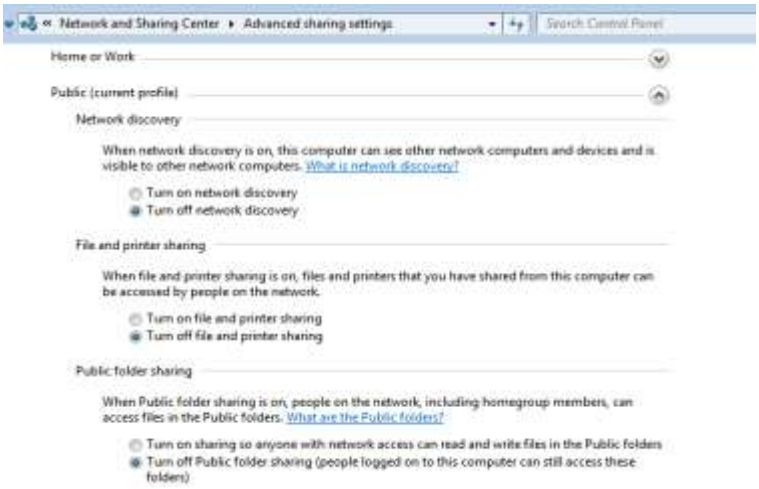
Gambar 19 Action

Lalu berikan nama pada rule ini, untuk pemberian namanya bebas ingin memberikan nama apa



Gambar 20 Hasil

Hasilnya dapat dilihat pada gambar di atas yang tadinya port 135, 139 dan 445 terbuka, sekarang sudah tidak dapat di scan menggunakan NMAP. Namun itu saja belum cukup untuk mengatasi kerentanan ini langkah selanjutnya adalah menonaktifkan layanan SMB pada windows



Gambar 21 Menonaktifkan layanan SMB pada windows

Untuk menonaktifkan layanan SMB masuk ke **Network and Sharing Center > Advanced sharing setting** akan ada 3 opsi yang terlihat, turn off semua opsi yang ada seperti pada gambar di atas. Hasilnya dapat dilihat pada gambar di bawah, sebelum menonaktifkan layanan SMB target mesin terdeteksi **VULNERABLE to MS17-010**

Gambar 22 Hasil

Setelah menonaktifkan layanan SMB dapat dilihat pesan VULNERABLE sudah tidak muncul lagi

Gambar 23 Hasil

KESIMPULAN

Berdasarkan hasil pengujian penetrasi yang dilakukan terhadap jaringan lokal menggunakan Metasploit Framework dengan target sistem operasi Windows 7, dapat disimpulkan bahwa sistem yang tidak mendapatkan pembaruan keamanan secara berkala sangat rentan terhadap eksploitasi. Eksploit EternalBlue (CVE-2017-0144) berhasil dimanfaatkan untuk mendapatkan akses tidak sah ke sistem target melalui celah pada protokol SMBv1.

Pengujian ini menunjukkan bahwa:

- Sistem target belum menginstal patch keamanan MS17-010 dari Microsoft.
- SMBv1 masih diaktifkan secara default, memungkinkan terjadinya eksekusi kode jarak jauh (Remote Code Execution).
- Setelah eksploitasi berhasil, penyerang dapat mengakses sistem target, mengambil informasi, serta melakukan tindakan lanjutan seperti pengambilan screenshot dan pengumpulan data sistem.

Keberhasilan pengujian ini membuktikan bahwa Metasploit Framework merupakan alat yang efektif dalam mendeteksi dan mengevaluasi kerentanan jaringan lokal, khususnya pada perangkat yang belum diperbarui atau dikonfigurasi dengan aman. Oleh karena itu, hasil penelitian ini diharapkan dapat menjadi referensi bagi administrator jaringan untuk segera menerapkan langkah-langkah mitigasi, seperti menonaktifkan SMBv1, memperbarui sistem operasi, serta memperkuat konfigurasi firewall guna meningkatkan keamanan jaringan secara keseluruhan.

DAFTAR PUSTAKA

[1] R. A. Wijayanti *et al.*, “Analisis Perbandingan Penggunaan Kali Linux pada Windows Subsystem for Linux (WSL) dan VirtualBox terhadap OpenSSL Benchmark Testing,” *J. Educ.*, vol. 06, no. 01, pp. 10146–10154, 2023.

[2] M. R. Rusydianto, E. Budiman, and H. J. Setyadi, “Implementasi Teknik Hacking Web Server Dengan Port Scanning Dalam Sistem Operasi Kali Linux,” *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf. e-ISSN*, vol. Vol.2 No, no. 2, 2017.

[3] O. Dwi Prasetyo, P. Hari Trisnawan, and A. Bhawiyuga, “Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos,” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 6, pp. 2686–2692, 2023, [Online]. Available: http://j-ptiik.ub.ac.id