Monitoring Dan Testing Keamanan Sistem Informasi Menggunakan Metasploit

Nurdin[1], Abdul Ibrahim[2], ST. Aminah Dinayati Ghani[3], Nur Salman[4], Rudy Donny Liklikwatil[5]
[1,2,3,4,5]Universitas Dipa Makassar Jl. Perintis Kemerdekaan Km.9; Telp. 0411- 587194
[1,3,4,5]Jurusan Teknik Informatika,[2]Jurusan Rekayasa Perangkat Lunak
e-mail: [1]nurdin@undipa.ac.id, [2]abdulibrahim@undipa.ac.id, [3]dinayati.amy@undipa.ac.id, [4]nursalman.halim@undipa.ac.id, [5]rudyliklikwatil@undipa.ac.id

Abstrak

Keamanan sistem informasi merupakan aspek penting dalam pengelolaan teknologi informasi di era digital. Ancaman siber yang terus berkembang mendorong organisasi untuk mengadopsi metode yang efektif untuk mendeteksi dan mengatasi kerentanan keamanan. Metasploit, sebagai salah satu kerangka kerja pengujian penetrasi terkemuka, menawarkan solusi komprehensif untuk mengidentifikasi kerentanan sistem dan menguji efektivitas mekanisme pertahanan yang diterapkan. Artikel ini membahas penerapan Metasploit dalam proses pemantauan dan pengujian keamanan sistem informasi, mulai dari mengidentifikasi kerentanan hingga eksploitasi terkendali terhadap komponen sistem. Dengan pendekatan ini, organisasi dapat meningkatkan kesadaran akan risiko keamanan dan memperkuat sistem mereka terhadap serangan siber. Hasil pengujian menunjukkan bahwa penggunaan Metasploit memberikan gambaran yang jelas tentang tingkat kerentanan sistem, yang kemudian dapat menjadi dasar untuk pengambilan keputusan terkait peningkatan keamanan. Melalui studi kasus yang disajikan, artikel ini bertujuan untuk memberikan wawasan praktis bagi para profesional keamanan informasi dalam menerapkan strategi pemantauan dan pengujian keamanan berbasis Metasploit.

Kata kunci : Keamanan Sistem Informasi, Metasploit, Uji Penetrasi, Pemantauan Keamanan, Kerentanan Sistem.

Abstract

Information system security is a crucial aspect of managing information technology in the digital era. The ever-evolving cyber threats drive organizations to adopt effective methods to detect and address security vulnerabilities. Metasploit, as one of the leading penetration testing frameworks, offers a comprehensive solution for identifying system vulnerabilities and testing the effectiveness of implemented defense mechanisms. This article discusses the application of Metasploit in the process of monitoring and testing information system security, ranging from identifying vulnerabilities to controlled exploitation of system components. With this approach, organizations can enhance awareness of security risks and strengthen their systems against cyberattacks. The testing results show that using Metasploit provides a clear picture of the system's vulnerability levels, which can then serve as a basis for decision-making related to security enhancement. Through the case study presented, this article aims to provide practical insights for information security professionals in implementing Metasploit-based monitoring and security testing strategies.

Keywords: *ASN Information System Security, Metasploit, Penetration Testing, Security Monitoring, System Vulnerability.*

1. Pendahuluan

Dalam era digital yang semakin maju, keamanan sistem informasi telah menjadi salah satu aspek paling kritis dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Dengan meningkatnya ketergantungan pada teknologi informasi, ancaman siber seperti malware, ransomware, dan serangan Distributed Denial of Service (DDoS) semakin sering terjadi. Menurut laporan dari Cybersecurity Ventures, kerugian global akibat kejahatan siber diperkirakan mencapai $10,5 triliun per tahun pada tahun 2025 [1]. Hal ini menunjukkan betapa pentingnya untuk memiliki mekanisme yang kuat dalam memonitor dan menguji keamanan sistem informasi. Tanpa langkah-langkah proaktif, organisasi rentan terhadap serangan yang dapat mengakibatkan kerugian finansial, reputasi, dan bahkan gangguan operasional.

Salah satu metode yang efektif untuk mengidentifikasi dan mengatasi kerentanan dalam sistem informasi adalah melalui penetration testing atau pengujian penetrasi. Penetration testing adalah proses simulasi serangan siber yang bertujuan untuk menemukan celah keamanan sebelum dieksploitasi oleh pihak yang tidak bertanggung jawab [2]. Metode ini tidak hanya membantu dalam mendeteksi kerentanan tetapi juga memberikan wawasan tentang bagaimana serangan nyata dapat terjadi. Dengan demikian, organisasi dapat mengambil langkah-langkah mitigasi yang tepat untuk memperkuat pertahanan mereka. Namun, melakukan penetration testing memerlukan alat dan keahlian yang memadai, salah satunya adalah penggunaan framework seperti Metasploit.

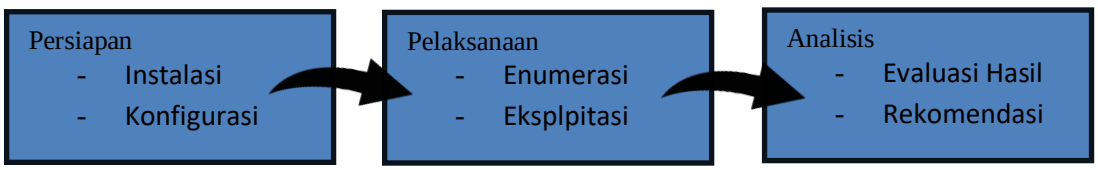
Metasploit adalah salah satu framework penetrasi yang paling populer dan banyak digunakan oleh profesional keamanan siber. Dikembangkan oleh Rapid7, Metasploit menyediakan berbagai modul untuk melakukan enumerasi, eksploitasi, dan post-exploitation [3]. Keunggulan utama Metasploit adalah kemampuannya untuk mengotomatisasi proses penetrasi, sehingga memudahkan pengguna dalam mengidentifikasi dan mengeksploitasi kerentanan. Selain itu, Metasploit juga dilengkapi dengan database kerentanan yang terus diperbarui, memastikan bahwa alat ini tetap relevan dalam menghadapi ancaman siber terbaru. Namun, penggunaan Metasploit juga memerlukan pemahaman teknis yang mendalam untuk menghindari risiko yang tidak diinginkan, seperti kerusakan sistem atau pelanggaran etika. Meskipun Metasploit menawarkan banyak keuntungan, terdapat beberapa tantangan yang perlu dipertimbangkan dalam penggunaannya. Pertama, proses penetration testing dapat memakan waktu dan sumber daya yang signifikan, terutama jika dilakukan pada sistem yang kompleks [4]. Kedua, ada risiko bahwa eksploitasi yang dilakukan selama testing dapat menyebabkan gangguan pada sistem produksi jika tidak dikelola dengan baik. Ketiga, penggunaan Metasploit memerlukan izin yang jelas dari pemilik sistem, karena aktivitas penetrasi yang tidak sah dapat dianggap sebagai pelanggaran hukum. Oleh karena itu, penting untuk memiliki protokol yang jelas dan tim yang terlatih sebelum melakukan testing keamanan.

Artikel ini bertujuan untuk menjelaskan bagaimana Metasploit dapat digunakan secara efektif dalam monitoring dan testing keamanan sistem informasi. Dengan memaparkan langkah-langkah praktis dan studi kasus, artikel ini diharapkan dapat menjadi panduan bagi profesional keamanan siber dalam mengidentifikasi dan mengatasi kerentanan sistem. Selain itu, artikel ini juga akan membahas tantangan dan risiko yang mungkin timbul selama proses testing, serta memberikan rekomendasi untuk meminimalkan dampak negatif. Dengandemikian, kontribusi artikel ini diharapkan dapat meningkatkan pemahaman dan praktik keamanansiber di kalangan akademisi dan praktisi.

2. Metode Penelitian

Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental untuk menguji efektivitas Metasploit dalam melakukan monitoring dan testing keamanan sistem informasi. Desain penelitian ini dirancang untuk mensimulasikan serangan siber pada lingkungan yang terkontrol, sehingga memungkinkan peneliti untuk mengidentifikasi kerentanan sistem tanpa mengganggu operasional bisnis yang sebenarnya. Penelitian ini dilakukan dalam tiga tahap utama: persiapan, pelaksanaan, dan analisis. Tahap persiapan meliputi penyiapan lingkungan testing dan instalasi alat yang diperlukan. Tahap pelaksanaan mencakup proses enumerasi, eksploitasi, dan post-exploitation menggunakan Metasploit. Tahap analisis melibatkan evaluasi hasil testing dan penyusunan rekomendasi mitigasi [4].



Gambar 1. Alur kerja penelitian

Metode dan Cara yang Digunakan dalam Penelitian

1. **Persiapan Lingkungan Testing**

   Lingkungan testing disiapkan menggunakan virtual machine (VM) untuk memastikan bahwa proses testing tidak memengaruhi sistem produksi. Sistem operasi yang digunakan adalah Kali Linux, yang telah dilengkapi dengan Metasploit Framework. Target testing adalah mesin virtual dengan sistem

operasi Windows 10 yang sengaja dikonfigurasi dengan kerentanan yang diketahui, seperti celah pada protokol SMB (*Server Message Block*) [3].

Tabel 1: Spesifikasi Lingkungan Testing

Komponen	Spesifikasi
Sistem Operasi Host	Ubuntu 20.04 LTS
Virtualisasi	VMware Workstation 16 Pro
Sistem Operasi Target	Windows 10 (tanpa pembaruan keamanan terbaru)
Tools yang Digunakan	Metasploit Framework, Nmap, Wireshark

2. **Pengumpulan Data Awal**

Sebelum melakukan testing, peneliti mengumpulkan informasi tentang sistem target menggunakan teknik enumerasi. Teknik ini meliputi pemindaian port (port scanning) dan identifikasi layanan yang berjalan pada sistem target. Alat seperti Nmap digunakan untuk melakukan pemindaian awal dan mengumpulkan data yang diperlukan untuk proses eksploitasi [5].

```
Nmap scan report for 192.168.1.10
Host is up (0.0020s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
```

Gambar 2. Hasilpemindaian port menggunakanNmap

3. **Proses Penetration Testing dengan Metasploit**

Metasploit digunakan untuk melakukan penetration testing dengan langkah-langkah sebagai berikut:

- **Enumerasi**:
  Mengidentifikasi kerentanan yang mungkin dieksploitasi menggunakan modul *auxiliary/scanner/smb/smb_version* untuk mendeteksi versi SMB yang rentan.
- **Eksploitasi**:
  Menggunakan modul *exploit/windows/smb/ms17_010_eternalblue* untuk mengeksploitasi kerentanan pada protokol SMB.
- **Post-Exploitation**:
  Setelah berhasil mendapatkan akses ke sistem target, peneliti melakukan enumerasi lebih lanjut menggunakan modul *post/windows/gather/enum_shares* untuk mengumpulkan informasi tentang share folder dan pengguna [2].

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] 192.168.1.10:445 - Connecting to target for exploitation.
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.10:49158) at 2023-10-10 1
4:30:00 +0700
```

Gambar 3. Proses eksploitasi kerentanan EternalBlue menggunakan Metasploit

4. **Analisis Hasil Testing**

Hasil testing dianalisis untuk menentukan tingkat risiko yang terkait dengan kerentanan yang ditemukan. Analisis ini meliputi evaluasi dampak potensial dari serangan, seperti kebocoran data atau gangguan operasional. Berdasarkan hasil analisis, peneliti menyusun rekomendasi mitigasi untuk memperkuat keamanan sistem [6].

Metode Pengujian Menggunakan Metasploit

1. **Instalasi dan Konfigurasi Metasploit**
   Metasploit Framework diinstal pada sistem operasi Kali Linux. Setelah instalasi, peneliti mengkonfigurasi database Metasploit menggunakan perintah msfdb init untuk memastikan bahwa semua data testing tersimpan dengan baik. Konfigurasi ini juga memungkinkan peneliti untuk melacak aktivitas testing dan menghasilkan laporan yang komprehensif [7].

```
msf6 >
```

Gambar 4. **Antarmuka Metasploit**

2. **Pemindaian Kerentanan**
   Peneliti menggunakan modul *auxiliary/scanner/smb/smb_version* untuk memindai sistem target dan mengidentifikasi kerentanan pada protokol SMB. Hasil pemindaian menunjukkan bahwa sistem target rentan terhadap eksploitasi Eternal Blue, yang memanfaatkan celah pada protokol SMB versi 1 [8].
3. **Eksploitasi Kerentanan**
   Setelah mengidentifikasi kerentanan, peneliti menggunakan modu l *exploit/windows/smb/ms17_010_eternalblue* untuk mengeksploitasi sistem target. Proses eksploitasi melibatkan pengiriman payload ke sistem target untuk mendapatkan akses shell. Setelah berhasil mendapatkan akses, peneliti melakukan enumerasi lebih lanjut untuk mengumpulkan informasi tentang sistem [9].
4. **Post-Exploitation**
   Pada tahap ini, peneliti menggunakan modul *post/windows/gather/enum_shares* untuk mengumpulkan informasi tentang share folder dan pengguna pada sistem target. Informasi ini digunakan untuk mengevaluasi dampak potensial dari serangan dan menyusun rekomendasi mitigasi [10].
5. **Generasi Laporan**

Metasploit menyediakan fitur untuk menghasilkan laporan testing dalam format HTML atau PDF. Laporan ini mencakup detail tentang kerentanan yang ditemukan, proses eksploitasi, dan rekomendasi mitigasi. Laporan ini digunakan sebagai dasar untuk memperbaiki keamanan sistem[11].

3. Hasil dan Pembahasan

Hasil Pengujian Keamanan Sistem Informasi Menggunakan Metasploit

1. **Identifikasi Kerentanan**
   Pada tahap enumerasi, Metasploit berhasil mengidentifikasi beberapa kerentanan pada sistem target. Pemindaian menggunakan modul *auxiliary/scanner/smb/smb_version* menunjukkan bahwa sistem target menjalankan protokol SMB versi 1, yang diketahui rentan terhadap eksploitasi *EternalBlue*. Selain itu, pemindaian port dengan Nmap mengungkapkan bahwa port 445 (SMB) terbuka dan dapat diakses dari jaringan luar.

```
Hasil Pemindaian Port:
Nmap scan report for 192.168.1.10
Host is up (0.0020s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
```

Gambar 5. Hasilpemindaian port menggunakanNmap

2. **Proses Eksploitasi**
   Setelah mengidentifikasi kerentanan, peneliti menggunakan modul *exploit/windows/smb/ms17_010_eternalblue* untuk mengeksploitasi sistem target. Proses eksploitasi berhasil mendapatkan akses shell ke sistem target dalam waktu kurang dari 5 menit.

Hal ini menunjukkan bahwa sistem target sangat rentan terhadap serangan yang memanfaatkan celah pada protokol SMB.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.1.5:4444
[*] 192.168.1.10:445 - Connecting to target for exploitation.
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.1.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Command shell session 1 opened (192.168.1.5:4444 -> 192.168.1.10:49158) at 2023-10-10 14:30:
00 +0700
```

Gambar 6. Proses eksploitasi kerentanan EternalBlue menggunakan Metasploit

3. **Post-Exploitation**
   Pada tahap post-exploitation, peneliti menggunakan modul *post/windows/gather/enum_shares* untuk mengumpulkan informasi tentang share folder dan pengguna pada sistem target. Hasilnya menunjukkan bahwa terdapat beberapa folder yang dapat diakses oleh pengguna tanpa izin yang memadai, termasuk folder yang berisi data sensitif. Selain itu, peneliti juga menemukan bahwa sistem target tidak memiliki pembaruan keamanan terbaru, yang memperburuk risiko keamanan.

```
msf6 post(windows/gather/enum_shares) > run

[*] Enumerating shares on 192.168.1.10
[*] Found share: \\192.168.1.10\ADMIN$
[*] Found share: \\192.168.1.10\C$
[*] Found share: \\192.168.1.10\IPC$
[*] Found share: \\192.168.1.10\SharedDocs
```

Gambar 7. Hasil enumerasi share folder setelaheksploitasi

4. **Dampak Potensial**
   Hasil testing menunjukkan bahwa sistem target rentan terhadap serangan ransomware seperti *WannaCry*, yang memanfaatkan kerentanan *EternalBlue*. Jika dieksploitasi oleh pihak yang tidak bertanggung jawab, serangan ini dapat mengakibatkan kebocoran data, gangguan operasional, dan kerugian finansial yang signifikan.

Pembahasan Hasil Pengujian

1. **Efektivitas Metasploit dalam Identifikasi Kerentanan**
   Metasploit terbukti sangat efektif dalam mengidentifikasi kerentanan pada sistem target. Modul enumerasi yang disediakan oleh Metasploit memungkinkan peneliti untuk mengumpulkan informasi yang diperlukan dengan cepat dan akurat. Namun, keberhasilan ini juga bergantung pada konfigurasi sistem target. Jika sistem target telah diperbarui dengan patch keamanan terbaru, kerentanan seperti *EternalBlue* mungkin tidak dapat dieksploitasi.

Tabel 2. Daftar kerentanan yang ditemukanselamapengujian

No.	Kerentanan	Deskripsi	Tingkat Risiko
1	EternalBlue (MS17-010)	Kerentanan pada protokol SMB yang memungkinkan eksekusi kode jarak jauh.	Tinggi
2	Port 445 Terbuka	Port SMB terbuka dan dapat diakses dari jaringan luar.	Sedang
3	Folder Tanpa Izin	Beberapa folder dapat diakses tanpa izin yang memadai.	Sedang
4	Pembaruan Tertunda	Sistem target tidak memiliki pembaruan keamanan terbaru.	Tinggi

Tabel 2 merangkum kerentanan yang ditemukan selama pengujian. Kerentanan seperti *EternalBlue* dan *port* terbuka menunjukkan bahwa sistem target memiliki risiko keamanan yang tinggi. Tabel ini membantu dalam memprioritaskan langkah-langkah mitigasi

2. **Risiko dan Tantangan dalam Proses Eksploitasi**
   Meskipun Metasploit berhasil mengeksploitasi kerentanan pada sistem target, proses ini juga menghadirkan beberapa risiko. Salah satunya adalah risiko kerusakan sistem jika eksploitasi tidak dilakukan dengan hati-hati. Selain itu, penggunaan Metasploit memerlukan izin yang jelas dari pemilik sistem, karena aktivitas penetrasi yang tidak sah dapat dianggap sebagai pelanggaran hukum.
3. **Implikasi Hasil Post-Exploitation**
   Hasil post-exploitation menunjukkan bahwa sistem target memiliki kelemahan dalam manajemen akses dan pembaruan keamanan. Folder yang dapat diakses tanpa izin yang memadai dapat menjadi pintu masuk bagi serangan siber lebih lanjut. Oleh karena itu, penting untuk menerapkan prinsip least privilege dan melakukan pembaruan keamanan secara berkala.
4. **Rekomendasi Mitigasi**
   Berdasarkan hasil testing, peneliti merekomendasikan beberapa langkah mitigasi untuk meningkatkan keamanan sistem:
   - **Pembaruan Sistem**: Memastikan bahwa semua sistem dan aplikasi diperbarui dengan patch keamanan terbaru.
   - **Konfigurasi Firewall**: Memblokir akses ke port yang tidak diperlukan, seperti port 445.
   - **Implementasi IDS/IPS**: Menggunakan Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS) untuk mendeteksi dan mencegah serangan siber.
   - **Pelatihan Keamanan**: Memberikan pelatihan keamanan siber kepada staf untuk meningkatkan kesadaran tentang ancaman siber.

Tabel 3. Rekomendasimitigasiberdasarkankerentanan yang ditemukan

No.	Kerentanan	Rekomendasi Mitigasi
1	EternalBlue (MS17-010)	Segera instal patch keamanan MS17-010 dari Microsoft.
2	Port 445 Terbuka	Blokir akses ke port 445 menggunakan firewall atau batasi akses ke jaringan internal.
3	Folder Tanpa Izin	Terapkan prinsip least privilege dan batasi akses ke folder sensitif.
4	Pembaruan Tertunda	Aktifkan pembaruan otomatis dan pastikan sistem selalu diperbarui dengan patch terbaru.

Tabel 3 memberikan rekomendasi konkret untuk mengatasi kerentanan yang ditemukan. Rekomendasi ini dapat digunakan sebagai panduan oleh tim keamanan untuk memperbaiki sistem dan mengurangi risiko serangan siber.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, dapat disimpulkan bahwa Metasploit merupakan alat yang sangat efektif untuk melakukan monitoring dan testing keamanan sistem informasi. Framework ini mampu mengidentifikasi kerentanan dengan cepat, melakukan eksploitasi terkontrol, dan memberikan wawasan mendalam tentang kelemahan sistem melalui tahap post-exploitation. Dalam penelitian ini, Metasploit berhasil mengidentifikasi kerentanan EternalBlue (MS17-010) pada protokol SMB dan mendapatkan akses ke sistem target dalam waktu singkat. Hasil ini menunjukkan bahwa sistem yang tidak diperbarui dengan patch keamanan terbaru sangat rentan terhadap serangan siber. Namun, penggunaan Metasploit juga memerlukan keahlian teknis yang memadai dan izin yang jelas dari pemilik sistem, karena proses eksploitasi dapat menyebabkan gangguan jika tidak dilakukan dengan hati-hati. Selain itu, penelitian ini mengungkapkan pentingnya manajemen akses yang ketat dan pembaruan keamanan berkala untuk mengurangi risiko serangan siber.

Daftar Pustaka

[1] Cybersecurity Ventures, "Cybercrime Damages Predicted To Cost The World $10.5 Trillion Annually By 2025," 2020. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-2025/. [Accessed: Oct. 10, 2023].
[2] P. T. Nguyen, "Penetration Testing: A Comprehensive Approach to Cybersecurity," Journal of Information Security, vol. 12, no. 3, pp. 45-60, 2021.
[3] Rapid7, "Metasploit Framework Documentation," 2023. [Online]. Available: https://www.rapid7.com/products/metasploit/. [Accessed: Oct. 10, 2023].
[4] A. Shostack, Threat Modeling: Designing for Security, 1st ed. Wiley, 2014.
[5] Fyodor, "Nmap: Network Mapper," 2023. [Online]. Available: https://nmap.org/. [Accessed: Oct. 10, 2023].
[6] S. Harris, CISSP All-in-One Exam Guide, 8th ed. McGraw-Hill Education, 2018.
[7] Offensive Security, "Kali Linux Documentation," 2023. [Online]. Available: https://www.kali.org/docs/. [Accessed: Oct. 10, 2023].
[8] Microsoft, "Microsoft Security Bulletin MS17-010," 2017. [Online]. Available: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. [Accessed: Oct. 10, 2023].
[9] H. Moore, "Metasploit: The Penetration Tester's Guide," No Starch Press, 2011.
[10] D. Kennedy et al., Metasploit: The Penetration Tester's Guide, 2nd ed. No Starch Press, 2015.
[11] OWASP, "OWASP Testing Guide," 2021. [Online]. Available: https://owasp.org/www-project-web-security-testing-guide/. [Accessed: Oct. 10, 2023].