Volume 20 Nomor 2 (2025) 29-36
E – Link P-ISSN 1858-2109 E-ISSN 2656-5676
Jurnal Teknik Elektro dan Informatika

EVALUASI DASAR PENETRATION TESTING MENGGUNAKAN FRAMEWORK MITRE ATT&CK

Vivin Wahyudi[1)], Muhammad Rudyanto Arief, S.T., M.T[2)], Banu Santoso, S.T., M.Eng[3)], Rangga Wahyu Nugroho[4)]
[1,2,3)] Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
Jl. Ring Road Utara, Condong Catur, Sleman, D.I Yogyakarta, Indonesia
E-mail : [1)]vin.udi@students.amikom.ac.id, [2)]rudy@amikom.ac.id, [3)]banu@amikom.ac.id, [4)]rangga52223@students.amikom.ac.id

ABSTRAK

Penetration testing adalah metode untuk menemukan kelemahan keamanan dalam jaringan atau sistem komputer. Dengan tahapan ini, pentester mencoba memanfaatkan celah keamanan dalam sistem dengan memodelkan potensi serangan yang dapat dilakukan oleh penyerang yang sebenarnya. Tujuan dari penetration testing adalah untuk mengevaluasi keamanan sistem komputer atau jaringan. Pendekatan multi-tahap ini, yang mencakup reconnaissance, exploitation, dan post-exploitation, meggunakan framework MITRE ATT&CK. Tools digunakan untuk membantu menemukan dan mengeksploitasi kelemahan keamanan, seperti nmap, netdiscover, metasploit, SSH, dan MySQL. Penelitian ini dapat menurunkan risiko kehilangan data dan gangguan operasional, meningkatkan keahlian dan kesadaran pentester, serta memperkuat keamanan sistem dan jaringan komputer.
Kata kunci : Penetration Testing, MITRE ATT&CK, Jaringan Komputer, Exploitasi.

ABSTRACT

Penetration testing is a method used to identify security vulnerabilities in networks or computer systems. In this process, pentesters attempt to exploit security gaps by simulating potential attacks that could be carried out by an actual attacker. The goal of penetration testing is to evaluate the security of computer systems or networks. This multi-stage approach, which includes reconnaissance, exploitation, and post-exploitation, utilizes the MITRE ATT&CK framework. Tools are used to help identify and exploit security weaknesses, such as nmap, netdiscover, metasploit, SSH, and MySQL. This research can reduce the risk of data loss and operational disruptions, enhance pentesters' skills and awareness, and strengthen the security of computer systems and networks.
Keywords*: Penetration Testing, MITRE ATT&CK, Computer Network, Exploitation.*

1. PENDAHULUAN

Penetration Testing adalah teknik yang digunakan untuk mengidentifikasi kelemahan dalam sistem komputer atau jaringan dengan melakukan simulasi serangan yang persis serangan nyata, namun dengan batasan tertentu. [1], [2], [3], [4] Mengingat meningkatnya ancaman siber saat ini, perusahaan dan organisasi harus memastikan bahwa sistem komputer dan jaringan mereka dilindungi dengan baik agar tidak mengakibatkan kerugian.

Latar belakang masalah yang ingin dipecahkan adalah karena semakin meningkatnya ancaman terhadap sistem komputer dan jaringan yang disebabkan oleh serangan siber yang semakin kompleks dan canggih. Banyak organisasi yang belum sepenuhnya menyadari potensi kerentanannya,

sehingga perlunya pendekatan yang sistematis dan terstruktur untuk mengidentifikasi dan mengatasi kerentanan dalam sebuah sistem. [5], [6]

Rumusan masalah dalam penelitian ini berkaitan dengan penerapan framework MITRE ATT&CK yaitu:

- Bagaimana MITRE ATT&CK diterapkan untuk mengidentifikasi dan mengeksploitasi kerentanan melalui tahapan pengujian? [7]
- Bagaimana tools seperti netdiscover, nmap, metasploit, SSH, dan MySQL mendukung pengujian untuk menemukan celah yang dapat dieksploitasi? [8]

Dengan pendekatan ini, diharapkan dapat ditemukan celah-celah yang sebelumnya tidak terdeteksi dan dapat diexploitasi oleh penyerang. [9]

Penelitian ini bertujuan untuk memecahkan masalah terkait keamanan sistem komputer dan jaringan dengan cara yang lebih efektif dan terfokus, yaitu:

- Meningkatkan deteksi kerentanan sistem dengan framework MITRE ATT&CK dalam penetration testing.
- Mengevaluasi dampak kerentanan pada tahapan penetration testing untuk menilai potensi ancaman.
- Menyarankan perbaikan untuk meningkatkan keamanan sistem yang teridentifikasi kerentanannya.

Penelitian ini diharapkan memberi manfaat untuk meningkatkan keamanan sistem komputer dan jaringan, [10] membantu organisasi memahami strategi penyerang melalui framework MITRE ATT&CK, [11] serta meningkatkan keterampilan dan kesadaran pentester.[12] Hal ini juga diharapkan dapat mengurangi risiko kerugian data dan gangguan operasional akibat serangan siber. [13]

2. METODE PENELITIAN

Penelitian ini menggunakan metode penetration testing dengan framework MITRE ATT&CK untuk mengidentifikasi kerentanan menggunakan alat seperti netdiscover, nmap, dan metasploit. [7], [8] Pengujian dilakukan pada Metasploitable, yaitu sistem yang sengaja dibuat rentan untuk melatih pentester dan menguji efektivitas framework, serta untuk memperbaiki sistem nyata berdasarkan hasil temuan. [12], [16]

2.1 Pengumpulan data

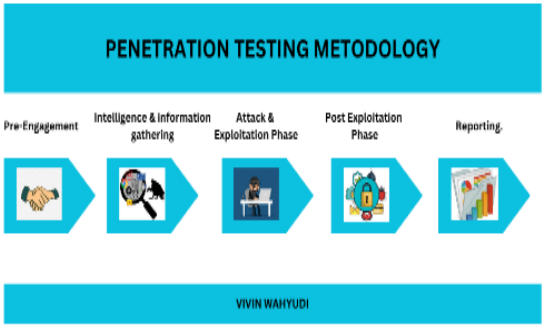
Data yang dikumpulkan berasal dari sumber yang tersedia di internet, yang bersifat sekunder, karena informasi tersebut diperoleh dari publikasi atau materi yang dimiliki oleh pihak lain. Berikut adalah data yang didapat [13]

Gambar 1. Grapik Serangan Sibe

2.2 Skenario Metodologi Penelitian

Penelitian ini menggunakan metodologi dari MITRE ATT&CK adalah sebagai berikut.

- Pre-Engagement
- Intelligence & information gathering
- Attack & Exploitation Phase
- Post Exploitation Phase
- Reporting.



Gambar 2. Desain Metodologi Penelitian

Proses serangan yang dijelaskan di bawah ini mengikuti prosedur dan metodologi penetration testing yang sesuai dengan framework MITRE ATT&CK, [11] di mana setiap tahapan serangan diidentifikasi dan diklasifikasikan berdasarkan teknik-teknik yang tercantum dalam framework tersebut untuk memastikan kesesuaian dengan standar analisis dan deteksi yang diakui secara internasional.

Tabel 1. Tahapan Serangan

Fase	Metode Serangan
Reconnaissance / Intelligence & information gathering	ARP Sniffing
	Ping Sweep
	Port Scanning
	Vulnerability Scanning
	SMB Discovery
Attack & Exploitation	SMB Exploitation
	Establishing Command Interpreter
Post Exploitation	SSH authorized_keys Tampering
	Exfiltrate Local Database Information
	Linux Log Removal
	Bash History Removal

Berikut ini, tahapan-tahapan serangan yang dijelaskan di bawah ini telah diberikan penomoran yang sesuai dengan framework MITRE ATT&CK. Penomoran ini digunakan untuk secara sistematis mengidentifikasi dan mengklasifikasikan berbagai teknik yang diterapkan dalam setiap tahap serangan, sesuai dengan standar yang berlaku dalam framework tersebut, sehingga memudahkan analisis, pemahaman, serta deteksi terhadap aktivitas yang dilakukan oleh penyerang.

Tabel 2. ID teknik framework MITRE ATT&CK

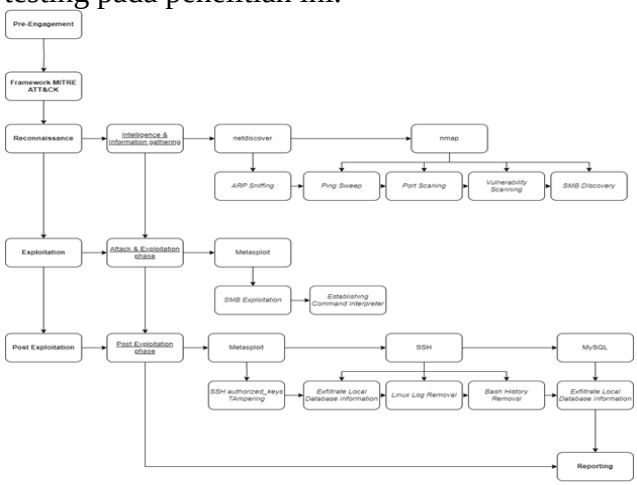
Metode Serangan	MITRE ATT&CK	Tools
ARP Sniffing	T1040	Netdiscover
Ping Sweep	T1018	Nmap
Port Scanning	T1046	Nmap
Vulnerability Scanning	T1595.002	Nmap
SMB Discovery	T1135	Nmap
SMB Exploitation	T1210	Metasploit
Establishing Command Interpreter	T1059.004	Metasploit
SSH authorized_keys Tampering	T1098.004	Metasploit
Exfiltrate Local Database Information	T1041	Ssh & Mysql
Linux Log Removal	T1070.002	Ssh
Bash History Removal	T1070.003	Ssh

3. HASIL DAN DISKUSI

Penelitian ini mengambil contoh kasus yang menerapkan penetration testing untuk mengidentifikasi kerentanan pada sistem komputer dan jaringan yang disimulasi pada Metasploitable [10] Framework MITRE ATT&CK sebagai tahapan kerangka kerja dan tools seperti netdiscover, nmap, metasploit, SSH, dan MySQL yang digunakan untuk membantu proses penelitian. [11]

3.1 Proses Penetration Testing

Penelitian ini terdiri dari beberapa tahapan, seperti Reconnaissance (pencarian dan pengumpulan informasi), Exploitation (pemanfaatan kelemahan), dan Post-Exploitation (tahap lanjutan setalah berhasil masuk). Tahapan tersebut merupakan teknik yang baik untuk mengidentifikasi setiap kerentanan keamanan, karena menggunakan framework MITRE ATT&CK dengan tahapan pertama yaitu reconnaissance T1040 (Pengumpulan Informasi Teknis) dan T1018 (Pengumpulan Informasi Jaringan), exploitation T1210 (Eksploitasi Daftar Kendala) dan T1059.004 (Penggunaan Fungsi Autentikasi), Terakhir tahapan Post Exploitation T1098.004 (Penggunaan Tool Command and Control). [8], [11]
Alur lengkap dari tahapan serangan penetration testing pada penelitian ini.



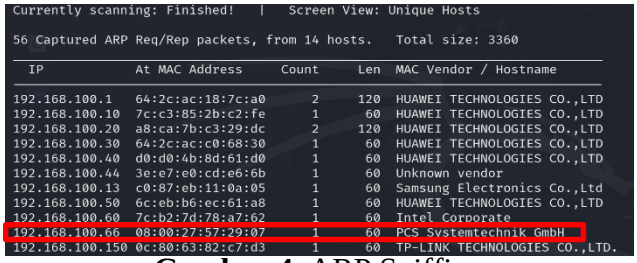
Gambar 3. Tahapan Penetration Testing

3.2 Tools dan Tahap Penetration Testing

Penelitian ini menggunakan berbagai tools seperti Netdiscover, Nmap, Metasploit, SSH, dan MySQL untuk mengidentifikasi kerentanan melalui tahapan reconnaissance, exploitation, dan post-exploitation. Pada tahap reconnaissance, dikumpulkan informasi target seperti perangkat dalam jaringan, port terbuka, dan celah keamanan menggunakan ARP Sniffing, pemindaian port, serta pemindaian kerentanan layanan SMB.

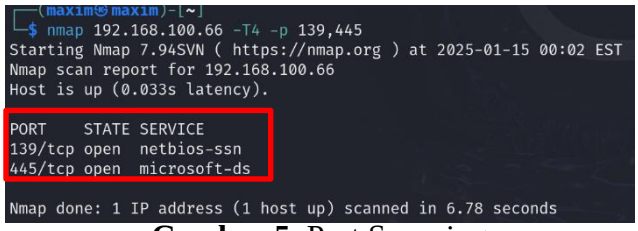
Eksploitasi dilakukan dengan metasploit untuk memperoleh kendali sistem menggunakan listener. Setelah akses diperoleh, langkah-langkah seperti membuat kunci SSH, ekstraksi database MySQL, dan penghapusan log untuk mempertahankan akses dan menghilangkan jejak.

Tahapan Penettration Testing sebegai berikut.



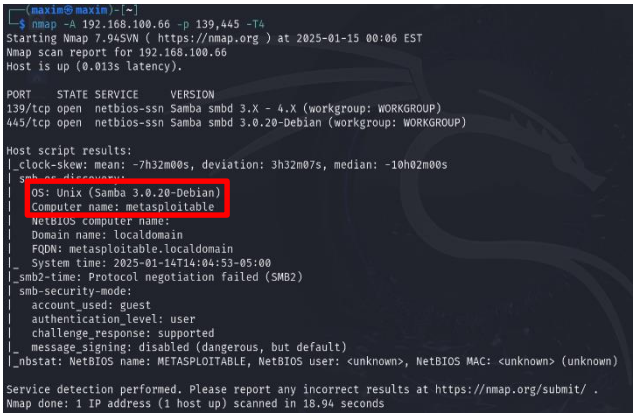
Gambar 4. ARP Sniffing

Gambar 4 menunjukkan tahapan Reconnaissance yaitu, proses ARP Sniffing dengan netdiscover untuk mendeteksi perangkat dalam jaringan.



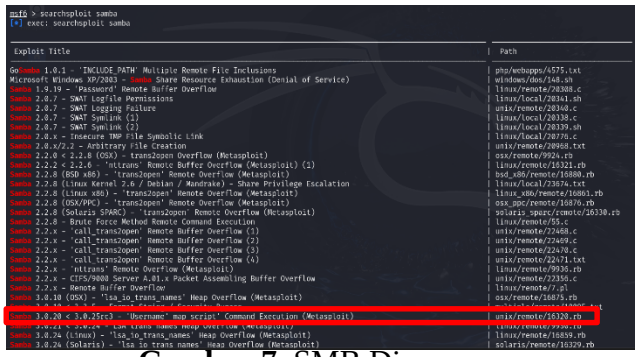
Gambar 5. Port Scanning

Gambar 5 menampilkan proses pemindaian port menggunakan nmap untuk menemukan layanan SMB yang terbuka.



Gambar 6. Vulnerability Scanning

Gambar 6 memperlihatkan proses pemindaian kerentanan menggunakan nmap pada layanan SMB guna menemukan celah keamanan.

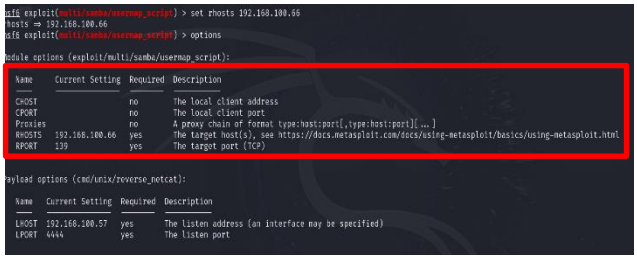


Gambar 7. SMB Discovery

Gambar 7 menunjukkan identifikasi layanan SMB menggunakan metasploit yang rentan terhadap eksploitasi.

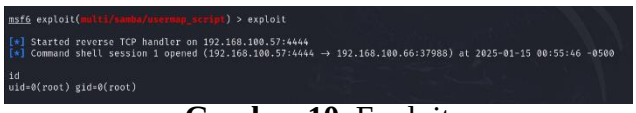
Gambar 8. Set Modul

Gambar 8 merupakan proses pemilihan modul untuk eksploitasi SMB menggunakan metasploit.



Gambar 9. Set Target

Gambar 9 merupakan tahapan exploitasi yaitu, proses konfigurasi modul untuk eksploitasi SMB menggunakan metasploit.



Gambar 10. Exploit

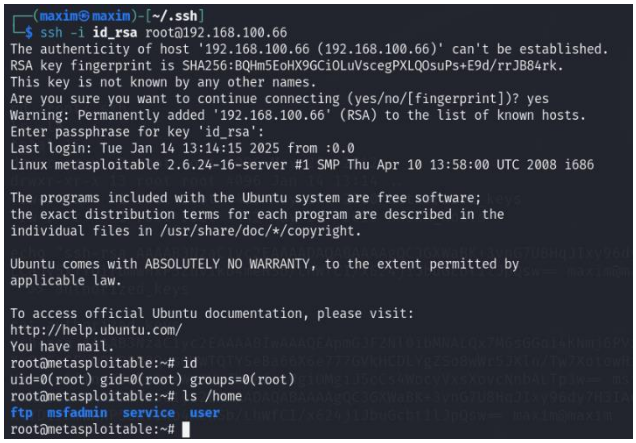
Gambar 10 merupakan proses menjalankan exploit agar mendapatkan akses pada mesin.

Gambar 11. SSH authorized_keys tampering

Gambar 11 menampilkan tahapan post exploitation, membuat kunci SSH untuk akses masuk kembali ke dalam sistem.

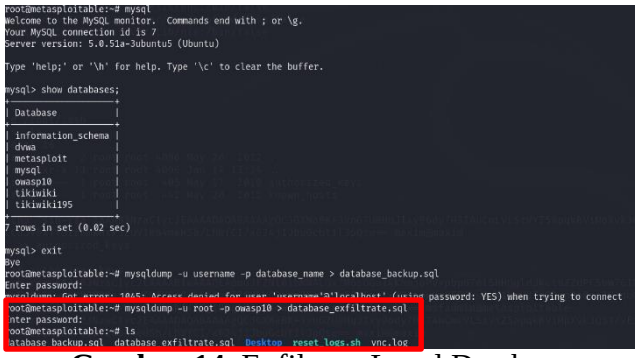
Gambar 12. Memasukan id_rsa.pub

Gambar 12 memperlihatkan proses mengirimkan kunci SSH ke dalam sistem melalui akses listener metasploit sebelumnya.



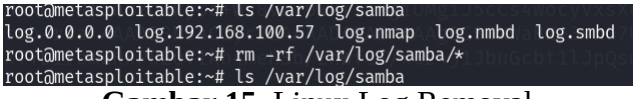
Gambar 13. Akses Ssh

Gambar 13 merupakan proses mengakses mesin menggunakan ssh dengan kunci SSH yang sudah dibuat pada mesin target.



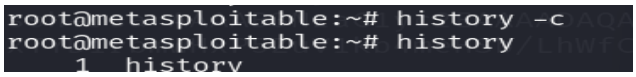
Gambar 14. Exfiltrate Local Database Information

Gambar 14 menunjukkan proses ekstraksi informasi dari database MySQL dalam mesin target.



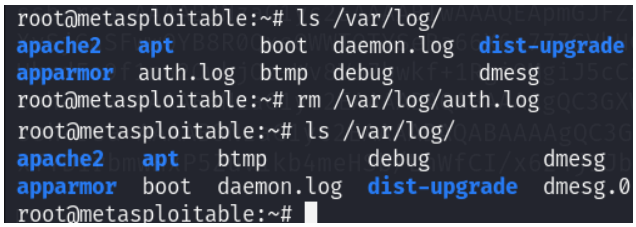
Gambar 15. Linux Log Removal

Gambar 15 merupakan proses penghapusan log sistem untuk menghilangkan jejak pada log SMB.



Gambar 16. Bash History Removal

Gambar 16 merupakan proses penghapusan log history command sistem dengan perintah history -c.



Gambar 17. Auth History Removal

Gambar 17 merupakan proses penghapusan log auntentikasi sistem.

Dengan tahapan tersebut, penetration testing dapat memberikan gambaran menyeluruh mengenai kerantanan yang ada serta teknik yang dapat digunakan sesuai dengan framework MITRE ATT&CK untuk mengamankan sistem dari ancaman serangan. [15]

3.3 Penilaian Kerentanan

Tingkat keamanan sistem bisa dilihat dengan nilai kerentanan yang didapat dari hasil penilaian proses penetration testing. Berikut adalah nilai yang diberikan untuk masing-masing tahap dalam penelitian ini.

Penilaian risiko dengan menggunakan perhitungan CVSS dengan rumus sebagai berikut. [17]

- Exploitability Subscore (ES)= $8.22 \times AV \times AC \times PR \times UI$
- Impact Subscore (ISC) = $1 - ((1-C) \times (1-I) \times (1-A))$
- Impact Scope (IS) = $6.42 \times ISC$
- Base Score (BS) = min(Impact Scope+Exploitability)

Proses perhitungan CVSS dalam setiap tahapan Penetration Testing

1. Reconnaissance (R)
   - AV (Attack Vector) = 0.85
   - AC (Attack Complexity) = 0.77
   - PR (Privilege Required) = 0.00
   - UI (User Interaction) = 0.00
   - C (Confidentiality Impact) = 0.56
   - I (Integrity Impact) = 0.22
   - A (Availability Impact) = 0.00

   ES = $8{,}22 \times 0{,}85 \times 0{,}77 = 5{,}37999$
   ISC = $1 - ((1 - 0.56) \times (1 - 0.00) \times (1 - 0.22)) = 1 - (0.44 \times 1 \times 0.78) = 1 - 0.3432 = 0.6568$
   IS= $6.42 \times 0.6568 = 4.2162$
   BS = min(4.22 + 0) = 4.22

2. Scanning (C)
   - AV (Attack Vector) = 0.85
   - AC (Attack Complexity) = 0.77
   - PR (Privilege Required) = 0.00
   - UI (User Interaction) = 0.00
   - C (Confidentiality Impact) = 0.56
   - I (Integrity Impact) = 0.22
   - A (Availability Impact) = 0.22

   ES = $8.22 \times 0.85 \times 0.77 \times 0.00 \times 0.00 = 0$
   ISC = $1-((1-0.56)\times(1-0.22)\times(1-0.22))=1-(0.44 \times 0.78 \times 0.78)=1-0.269568 = 0.730432$
   IS = $6.42 \times 0.730432 = 4.693$
   BS = min(4.693+0) = 4.69

3. Exploitation (E)
   - AV (Attack Vector) = 0.85
   - AC (Attack Complexity) = 0.77
   - PR (Privilege Required) = 0.85
   - UI (User Interaction) = 0.77
   - C (Confidentiality Impact) = 0.56
   - I (Integrity Impact) = 0.22
   - A (Availability Impact) = 0.22

   ES = $8.22 \times 0.85 \times 0.77 \times 0.85 \times 0.77 = 3.74655425$
   ISC = $1-((1-0.56)\times(1-0.22)\times(1-0.22))=1-(0.44 \times 0.78 \times 0.78) = 0.745056$
   IS = $6.42 \times 0.745056 = 4.78335$
   BS = min(4.78+3.75) = 8.53

4. Post-Exploitation (P)
   - AV (Attack Vector) = 0.85
   - AC (Attack Complexity) = 0.77
   - PR (Privilege Required) = 0.85
   - UI (User Interaction) = 0.85
   - C (Confidentiality Impact) = 0.56

- I (Integrity Impact) = 0.56
- A (Availability Impact) = 0.56

ES = 8.22×0.85×0.77×0.85×0.85 = 3.89
ISC = 1−((1−0.56)×(1−0.56)×(1−0.56)) = 0.91498
IS = 6.42×0.91498 = 5.87
BS = min(5.87+3.89) = 9,76

Total Skor Base Score Paling Tinggi:

$$BaseScoreMax = max[4{,}22 + 4{,}69 + 8{,}53 + 9{,}76] = 9{,}76$$

Dari hasil yang ditunjukan dalam framework MITRE ATT&CK, skor CVSS Base Score tertinggi didapatkan 9,76 pada tahap post-exploitation. Dari nilai-nilai yang didapatkan menunjukkan bahwa sistem rentan pada tahapan berikut

1. Reconnaissance (TA0043)
   Penyerang berhasil mengumpulkan informasi tentang celah.
2. Exploitation (TA0011)
   Celah dieksploitasi untuk mendapatkan akses.
3. Post-Exploitation (TA0003, TA0004)
   Penyerang meningkatkan hak akses dan bertahan dalam sistem.
4. Exfiltration (TA0010)
   Data sensitif dapat dicuri.

Ini menandakan ancaman serius pada tahap exploitation dan post-exploitation.

3.4 Saran Perbaikan Sistem

Rekomendasi perbaikan dari temuan hasil penetration testing berdasarkan framework MITRE ATT&CK mencakup pembatasan informasi pada tahap Reconnaissance (TA0043), pembaruan rutin dan patch pada tahap Exploitation (TA0011), penerapan IDS/IPS serta pengawasan log pada tahap Post-Exploitation (TA0003, TA0004), serta enkripsi data dan pemantauan lalu lintas keluar pada Exfiltration (TA0010). [9], [11] Langkah-langkah ini diharapkan dapat memperkuat sistem dan memitigasi ancaman secara efektif. [14]

4. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penerapan penetration testing dengan framework MITRE ATT&CK berhasil mengidentifikasi kerentanan pada sistem, terutama pada layanan SMB, melalui tahapan reconnaissance, exploitation, dan post-exploitation menggunakan tools seperti Netdiscover, Nmap, dan Metasploit. Nilai keamanan tertinggi yang ditemukan adalah 9,76, mengindikasikan kerentanannya yang tinggi. Oleh karena itu, diperlukan perbaikan segera, seperti pembatasan informasi, pembaruan perangkat lunak, penguatan firewall IDS/IPS, enkripsi data sensitif, dan pemantauan lalu lintas untuk mencegah eksploitasi lebih lanjut dan meningkatkan ketahanan sistem.

5. DAFTAR PUSTAKA

[1] L. Demetrio and B. Biggio, ‘secml-malware: Pentesting Windows Malware Classifiers with Adversarial EXEmples in Python’, Apr. 2021, [Online]. Available: http://arxiv.org/abs/2104.12848

[2] I. Pradeep and G. Sakthivel, ‘Ethical hacking and penetration testing for securing us form Hackers’, in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Mar. 2021. doi: 10.1088/1742-6596/1831/1/012004.

[3] D. Shmaryahu, G. Shani, J. Hoffmann, and M. Steinmetz, ‘Simulated Penetration Testing as Contingent Planning’. [Online]. Available: www.aaai.org

[4] J. Hoffmann, ‘Simulated Penetration Testing: From “Dijkstra” to “Turing Test++”’. [Online]. Available: http://www.coresecurity.com/

[5] H. Holm, ‘Lore a Red Team Emulation Tool’, *IEEE Trans Dependable Secure Comput*, vol. 20, no. 2, pp. 1596–1608, Mar. 2023, doi: 10.1109/TDSC.2022.3160792.

[6] Y. Yang, X. Xie, Z. Fang, F. Zhang, Y. Wang, and D. Zhang, ‘VeMo: Enable Transparent Vehicular Mobility Modeling at Individual Levels With Full Penetration’, *IEEE Trans Mob Comput*, vol. 21, no. 7,

pp. 2637–2651, Jul. 2022, doi: 10.1109/TMC.2020.3044244.

[7] A. S. Sani, D. Yuan, J. Jin, L. Gao, S. Yu, and Z. Y. Dong, 'Cyber security framework for Internet of Things-based Energy Internet', *Future Generation Computer Systems*, vol. 93, pp. 849–859, Apr. 2019, doi: 10.1016/j.future.2018.01.029.

[8] A. Georgiadou, S. Mouzakitis, and D. Askounis, 'Assessing mitre att&ck risk using a cyber-security culture framework', *Sensors*, vol. 21, no. 9, May 2021, doi: 10.3390/s21093267.

[9] T. Caldwell, 'Plugging the cyber-security skills gap', *Computer Fraud and Security*, vol. 2013, no. 7, pp. 5–10, Jul. 2013, doi: 10.1016/S1361-3723(13)70062-9.

[10] M. C. Ghanem and T. M. Chen, 'Reinforcement learning for efficient network penetration testing', *Information (Switzerland)*, vol. 11, no. 1, Jan. 2020, doi: 10.3390/info11010006.

[11] Z. Wang, W. Hu, G. Chen, C. Yuan, R. Gu, and Y. Huang, 'Towards Efficient Distributed Subgraph Enumeration Via Backtracking-Based Framework', *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 12, pp. 2953–2969, Dec. 2021, doi: 10.1109/TPDS.2021.3076246.

[12] S. Mallissery, K.-Y. Chiang, C.-A. Bau, and Y.-S. Wu, 'Pervasive Micro Information Flow Tracking', *IEEE Trans Dependable Secure Comput*, pp. 1–18, Jan. 2023, doi: 10.1109/tdsc.2023.3238547.

[13] Andi Nugroho, 'Serangan Siber ke Indonesia yang Terekam Sensor Honeypot Capai 361,17 Juta'.

[14] H. Berger and A. Jones, 'Cyber security & ethical hacking for SMEs', in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Jul. 2016. doi: 10.1145/2925995.2926016.

[15] J. L. Colorossi, 'Cyber Security', in *Security Supervision and Management: Theory and Practice of Asset Protection*, Elsevier, 2015, pp. 501–525. doi: 10.1016/B978-0-12-800113-4.00038-9.

[16] M. M. Yamin, B. Katt, and M. Nowostawski, 'Serious games as a tool to model attack and defense scenarios for cyber-security exercises', *Comput Secur*, vol. 110, Nov. 2021, doi: 10.1016/j.cose.2021.102450.

[17] M. Aziz, "VULNERABILITY ASSESMENT UNTUK MENCARI CELAH," *Journal of Engineering, Computer Science and Information Technology*, Vols. Vol. 1, No. 1, 2021, 101-109 , p. 8, 2021