Jurnal Penelitian Teknologi Informasi Dan Sains
Volume. 3, Nomor. 1, Tahun 2025
e-ISSN : 2985-7635; dan p-ISSN : 2985-6280; Hal. 82-91
DOI: https://doi.org/10.54066/jptis.v3i1.3119
Available online at: https://jurnal.itbsemarang.ac.id/index.php/JPTIS

Implementasi Pengujian Kerentanan Windows 10 Menggunakan *EternalBlue* dan *Phising*

Muhammad Naufal Hafizh[1*], Isram Rasal[2]
[1,2] Universitas Gunadarma, Indonesia
naufaldexerr@gmail.com[1], isramrasal@staff.gunadarma.ac.id[2]

Alamat: Jalan Margonda Raya Nomor 100, Pondok Cina, Depok, Jawa Barat 16424
*Korespondensi penulis: naufaldexerr@gmail.com**

Abstract. *Attacks on Windows can be carried out in various ways, one of which is exploiting SMBv1 vulnerabilities and phishing. Exploitation is an attack technique that takes advantage of system weaknesses. Windows 10 itself has vulnerabilities that can be exploited for hacking, which may include data theft, user data deletion, credential theft, and even damaging the Windows 10 system itself. A possible solution is to conduct penetration testing on the Windows 10 operating system. The testing is carried out based on the Cyber Kill Chain model, utilizing appropriate tools and following the stages outlined in the model. The test results indicate that Windows 10 vulnerabilities can be exploited, particularly through direct system attacks via SMBv1 with CVE-2017, codenamed EternalBlue, and phishing techniques that allow attackers to gain administrator privileges directly or inject malware into the target Windows 10 system.*

Keywords*: Cybersecurity, Kali linux, Penetration Testing, Windows 10*

Abstrak. Penyerangan terhadap windows dapat dilakukan dengan berbagai cara kerentanan, salah satunya eksploitasi kerentanan SMBv1 dan Phising. Eksploitasi merupakan teknik penyerangan yang memanfaatkan celah yang dimiliki oleh sistem, Windows 10 sendiri mempunyai kerentanan yang menyebabkan dapat dilakukan peretasan, peretasan itu dapat berupa pencurian data, penghapusan data pengguna, pencurian kredensial sampai merusak sistem Windows 10 itu sendiri. Solusi yang dapat dilakukan, yaitu dengan melakukan pengujian penetrasi pada sistem operasi Windows 10. Pengujian dilakukan sesuai dengan metode yang digunakan yaitu dengan model Cyber Kill chain, dengan menggunakan tools-tools yang sesuai dan diikuti dengan tahapan-tahapan yang ada pada model Cyber Kill Chain. Pengujian menyatakan bahwa kerentanan Windows 10 dapat di eksploitasi, terutama melalui penyerang an langsung ke sistem melalui SMBv1 dengan CVE-2017 codename Eternalblue dan dengan teknik pishing yang memungkinkan penyerang mendapatkan hak akses admi nistrator secara langsung atau menyusupkan malware ke dalam Windows 10 target.

Kata kunci: Cybersecurity, Kali linux, Uji Penetrasi, Windows 10

1. LATAR BELAKANG

Keamanan sistem operasi merupakan aspek fundamental dalam teknologi informasi yang berperan penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Windows 10, sebagai salah satu sistem operasi yang paling banyak digunakan secara global, sering menjadi target utama serangan siber. Berbagai metode eksploitasi digunakan oleh peretas untuk menembus sistem ini, termasuk serangan terhadap protokol komunikasi dan metode rekayasa sosial yang memanfaatkan kelalaian pengguna (Kumar & Ramlie, 2021).

Perkembangan *platform digital* telah mengubah berbagai aspek kehidupan, termasuk dalam bidang ekonomi, sosial, dan teknologi (Lestari et al., 2019). Transformasi digital ini memberikan peluang besar bagi kemajuan teknologi, tetapi juga meningkatkan risiko keamanan siber. Seiring dengan meningkatnya ketergantungan terhadap layanan digital, ancaman terhadap sistem operasi dan perangkat lunak juga semakin berkembang.

Received: Februari 13, 2025; Revise:d Februari 21, 2025; Accepted: Maret 01, 2025; Published: Maret 03, 2025

Salah satu eksploitasi yang terkenal adalah serangan SMBv1 EternalBlue, yang telah digunakan dalam berbagai serangan ransomware seperti WannaCry (Gupta, nd.). Serangan ini memanfaatkan celah keamanan dalam protokol komunikasi Server Message Block (SMB) versi 1 untuk mendapatkan akses tidak sah ke sistem (Algarni, 2021). Selain itu, teknik phishing juga menjadi salah satu metode yang sering digunakan dalam eksploitasi sistem operasi Windows, dengan memanipulasi pengguna agar mengunduh dan mengeksekusi perangkat lunak berbahaya (Alkhalil et al., 2021).

Metode Cyber Kill Chain sering digunakan untuk menganalisis tahapan serangan siber, mulai dari rekognisi, weaponization, delivery, exploitation, installation, command and control, hingga action on objectives (Naik et al., 2022). Analisis terhadap metode ini memungkinkan identifikasi titik lemah dalam sistem keamanan Windows 10 serta evaluasi efektivitas fitur pertahanan seperti firewall dan Windows Defender (Andhika, 2021).

Penelitian ini bertujuan untuk menguji tingkat keamanan Windows 10 melalui simulasi serangan menggunakan teknik Cyber Kill Chain. Melalui analisis ini, diharapkan dapat diidentifikasi kelemahan yang masih terdapat dalam sistem serta efektivitas mekanisme pertahanan yang tersedia. Dengan memahami celah keamanan yang ada, penelitian ini juga memberikan rekomendasi untuk meningkatkan sistem keamanan, baik melalui konfigurasi yang lebih optimal maupun integrasi dengan solusi keamanan tambahan (Fermana, nd.).

2. KAJIAN TEORITIS

Sistem Operasi

Sistem operasi (Operating System) adalah perangkat lunak yang bertanggung jawab untuk mengelola perangkat keras komputer dan menyediakan layanan umum untuk program aplikasi.), sistem operasi bertindak sebagai mediator antara pengguna dan perangkat keras, mengelola tugas-tugas seperti pengelolaan memori, penjadwalan proses, dan kontrol input/output (I/O) (Abraham, Greg, & Peter, 2018).

Windows 10

Windows 10 adalah sistem operasi yang dikembangkan oleh Microsoft sebagai bagian dari keluarga sistem operasi Windows NT. Diperkenalkan sebagai penerus dari Windows 8.1, Windows 10 membawa berbagai fitur dan pembaruan signifikan yang dirancang untuk menyatukan pengalaman komputasi di berbagai perangkat, termasuk PC, tablet, smartphone, dan perangkat IoT (Ontko, Reeder & Tanenbaum, 2020).

Penetration Testing

Penetration Testing atau uji penetrasi adalah proses evaluasi keamanan sistem komputer, jaringan, atau aplikasi dengan mensimulasikan serangan dari sumber eksternal dan internal. Tujuan dari penetrasi testing adalah menemukan celah keamanan dalam sistem sebelum dapat dieksploitasi oleh penyerang yang sebenarnya, Menilai seberapa 12 efektif langkah-langkah keamanan saat ini dalam mencegah atau mendeteksi serangan, dan memberikan rekomendasi untuk memperbaiki kelemahan yang ditemukan dan memperkuat sistem terhadap potensi ancaman, serta membantu organisasi memenuhi persyaratan keamanan dari regulasi dan standar industri, seperti PCI-DSS, HIPAA, atau GDPR (Yaacoub et al., 2021).

Server Message Block version 1

SMBv1 (Server Message Block version 1) adalah versi pertama dari protokol Server Message Block yang dikembangkan oleh IBM pada tahun 1983 dan kemudian diadopsi serta dikembangkan lebih lanjut oleh Microsoft. Protokol ini digunakan untuk menyediakan layanan berbagi file, printer, dan komunikasi jaringan lainnya antara node dalam jaringan komputer. SMBv1 memungkinkan komputer Windows untuk berinteraksi dengan perangkat lain dalam jaringan dan adalah fondasi dari banyak jaringan berbasis Windows di masa lalu (Mohammed & Abiodun, nd.).

SMBv1 dirancang untuk memfasilitasi berbagai fungsi jaringan, termasuk:

a. Berbagi File: SMBv1 memungkinkan pengguna untuk berbagi file dan folder di jaringan, sehingga memudahkan akses dan kolaborasi data di antara berbagai perangkat.
b. Berbagi Printer: Protokol ini juga mendukung berbagi printer, memungkink an beberapa pengguna untuk menggunakan printer yang terhubung ke satu komputer dalam jaringan.
c. Navigasi Jaringan: SMBv1 memungkinkan komputer dalam jaringan untuk menemukan satu sama lain dan sumber daya yang tersedia, seperti berbagi f ile dan printer, melalui mekanisme penjelajahan jaringan.
d. Autentikasi dan Keamanan: Meskipun terbatas dibandingkan dengan versi yang lebih baru, SMBv1 menyediakan beberapa mekanisme autentikasi dasar untuk mengamankan komunikasi dan akses ke sumber daya dalam jaringan (Yudha & Prayudi, nd.).

Nmap

Nmap adalah pemeta jaringan yang digunakan sebagai alat pengujian pe netrasi untuk memindai jaringan, melakukan Pemindaian adalah proses mengum pulkan informasi tanpa mengeksploitasi sistem untuk menemukan host, port, dan layanan apa yang sedang berjalan, dan menemukan kerentanan serta juga dapat menemukan versi apa yang sedang dijalankan (Jayasuryapal et al., 2021).

Metasploit

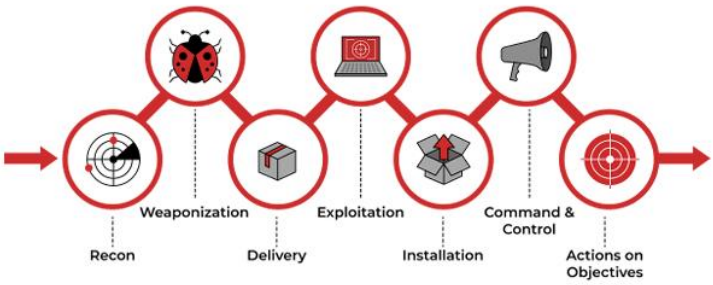
Metasploit adalah platform kuat yang digunakan untuk pengujian penetrasi dan eksploitasi kerentanan dalam keamanan jaringan. Pertama kali dikembangkan oleh H.D. Moore pada tahun 2003 dan sekarang dikelola oleh Rapid7, Metasploit telah berkembang menjadi salah satu alat yang paling penting dalam dunia keamanan siber.

Havoc C2

Havoc C2 adalah sistem Command and Control (C2) yang modern dan open source, dirancang untuk mendukung operasi pengujian penetrasi dan red team dengan alat-alat yang canggih. Platform ini dikembangkan untuk memberikan kontrol komprehensif atas operasi siber dengan menawarkan kemampuan untuk mengelola agen-agen yang disuntikkan ke dalam sistem target, memfasilitasi komunikasi, dan menjalankan payloads berbahaya secara teratur (Desclaux & Claverie, 2022).

3. METODE PENELITIAN

Penelitian ini menggunakan metode **CKC (Cyber Kill Chain)** yang didalamya memiliki tahapan- tahapan serangan siber, dari perencanaan hingga eksekusi. Metode ini membantu dalam memahami dan menganalisis tindakan yang dilakukan oleh penyerang serta memungkinkan implementasi langkah-langkah mitigasi yang efektif.



Sumber: Approach Cyber (2023).

Gambar 1. Metode penyerangan Cyber Kill Chain

Tahapan-tahapan dalam metode ini meliputi:

a. Reconnaissance (Pengintaian)

   Pada tahap ini, dilakukan pengumpulan informasi terkait sistem target, seperti alamat IP, nama domain, topologi jaringan, dan karyawan perusahaan. Informasi ini digunakan untuk merencanakan serangan.

b. Weaponization (Persenjataan)

   Setelah informasi terkumpul, tahap ini penyerang membuat atau memperoleh alat serangan, seperti malware, exploit, atau virus, yang akan digunakan untuk menyerang target.

c. Delivery (Pengiriman)

   Pada tahap ini penyerang mengirimkan alat serangan kepada target melalui berbagai metode, seperti email phishing, lampiran berbahaya, atau media yang terinfeksi.

d. Exploitation (Eksploitasi)

   Setelah alat serangan sampai ke target, penyerang mengeksploitasi kerentanan untuk mendapatkan akses awal ke sistem atau jaringan.

e. Installation (Instalasi)

   Tahap ini penyerang menginstal malware atau backdoor pada sistem target untuk mem pertahankan akses dan memungkinkan kontrol jarak jauh.

f. Command and Control (C2)

   Penyerang membangun jalur komunikasi antara sistem yang telah dikompromikan dan server C2 untuk mengontrol operasi selanjutnya dan mengumpulkan data

g. Actions on Objectives (Aksi pada Sasaran)

   Penyerang mencapai tujuannya, yang bisa berupa pencurian data, penghancuran sistem, atau tindakan lain yang merugikan target.

4. HASIL DAN PEMBAHASAN

Penelitian ini berhasil untuk menguji kerentanan sistem operasi Windows 10 dengan metode Cyber Kill Chain (CKC), yang terdiri dari tujuh tahapan: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, serta Actions on Objectives. Pengujian dilakukan pada dua jenis serangan, yaitu eksploitasi SMBv1 dengan EternalBlue dan serangan phishing. Setiap metode serangan diuji dalam dua skenario, yaitu

dengan sistem keamanan aktif dan tidak aktif, guna mengevaluasi efektivitas pertahanan Windows 10 terhadap serangan siber.

Tabel 1. Skenario Penyerangan

Penyerangan SMBv1		Penyerangan Phising	
Skenario A	Skenario B	Skenario A	Skenario B
Penyerangan dilakukan dengan keadaan dimatikannya firewall.	Penyerangan dilakukan dengan keadaan firewall yang menyala.	Penyerangan dilakukan dengan keadaan dimatikannya Windows Defender.	Penyerangan dilakukan dengan keadaan dinyalakannya Windows Defender.

Analisis Kebutuhan

Dalam penelitian ini, pengujian dirancang menggunakan VirtualBox, dengan Windows 10 sebagai target dan Kali Linux sebagai mesin penyerang. Perangkat keras yang digunakan mencakup laptop ASUS ROG Strix 15 GL503GE dengan prosesor Intel Core i7-8750H, RAM 16 GB DDR3, serta Nvidia GeForce GTX 1050 Ti untuk mendukung pemrosesan eksploitasi. Perangkat lunak yang digunakan meliputi Metasploit Framework, Havoc C2 Framework, dan alat pendukung lainnya seperti Nmap dan MiTEX.

Pengujian CKC dengan Metasploit (Eksploitasi SMBv1 - EternalBlue)

Eksploitasi dilakukan dengan Metasploit Framework, memanfaatkan CVE-2017-0143 (EternalBlue). Pengujian dibagi menjadi dua skenario:

Tabel 2. Report Metasploit

Tahapan metode CKC	Skenario A (Firewall Tidak Aktif)	Skenario B (Firewall Aktif)
Reconnaissance	Menggunakan Nmap untuk memindai jaringan dan mengidentifikasi port yang terbuka, ditemukan bahwa SMBv1 aktif pada port 445	Pemindaian menggunakan Nmap menunjukkan bahwa port 445 tidak dapat diakses karena firewall aktif
Weaponization	Payload eksploitasi dibuat menggunakan Metasploit Framework, dengan modul exploit/windows/smb/ms17-010-eternalblue	Payload eksploitasi tetap dibuat dengan Metasploit, namun tidak dapat dikirimkan ke target
Delivery	Payload dikirim ke sistem target melalui protokol SMBv1 yang rentan	Firewall memblokir eksploitasi EternalBlue sebelum mencapai sistem target
Exploitation	Payload dijalankan di sistem target, memberikan akses administratif ke penyerang	Serangan gagal karena firewall mencegah komunikasi dengan layanan SMBv1

Tahapan metode CKC	Skenario A (Firewall Tidak Aktif)	Skenario B (Firewall Aktif)
Command and Control (C2)	Sistem yang telah dikompromikan dikendalikan melalui Metasploit Meterpreter	Tidak terjadi akses jarak jauh karena eksploitasi tidak berhasil
Actions on Objectives	Penyerang berhasil mencuri data, melakukan eskalasi hak akses, dan menanamkan malware tambahan	Tidak terjadi akses jarak jauh karena eksploitasi tidak berhasil

Tabel 3. Hasil Pengujian Metasploit CKC

Skenario A	Skenario B
Eksploitasi berhasil dilakukan, menunjukkan bahwa tanpa firewall, sistem Windows 10 sangat rentan terhadap serangan berbasis SMBv1 EternalBlue.	Firewall terbukti efektif dalam mencegah eksploitasi EternalBlue, sehingga sistem tidak dapat dikompromikan.

Pengujian CKC dengan Havoc (Serangan Phishing)

Serangan phishing dilakukan dengan metode spear-phishing, menyamar sebagai layanan Microsoft guna menipu pengguna agar menginstal malware yang telah dimodifikasi. Pengujian dibagi menjadi dua skenario:

Tabel 4. Report Havoc

Tahapan metode CKC	Skenario A (Windows Defender Tidak Aktif)	Skenario B (Windows Defender Aktif)
Reconnaissance	Penyerang mengidentifikasi target melalui email pengguna Windows	Identifikasi target tetap dilakukan, tetapi langkah ini tidak berpengaruh pada proteksi sistem
Weaponization	Pembuatan payload berbahaya menggunakan Havoc C2, dikemas dalam file eksekusi palsu yang menyerupai pembaruan Windows Defender	Payload tetap dibuat menggunakan Havoc C2
Delivery	Email phishing dikirim ke target, dengan tautan yang mengarah ke situs palsu atau lampiran berbahaya	Email phishing tetap dikirimkan ke target
Exploitation	Korban mengklik tautan dan menginstal payload, memberi akses ke sistem	Windows Defender mengenali payload sebagai ancaman dan memblokir eksekusi
Installation	Malware berhasil dipasang dan backdoor dibuat untuk akses jangka panjang	Malware tidak dapat dipasang karena sistem keamanan Windows menghapus file berbahaya sebelum dijalankan
Command and Control (C2)	Sistem target dikendalikan melalui Havoc C2 Framework, memungkinkan peretas melakukan perintah dari jarak jauh	Tidak ada koneksi ke server penyerang karena malware gagal dieksekusi

Tahapan metode CKC	Skenario A (Windows Defender Tidak Aktif)	Skenario B (Windows Defender Aktif)
Actions on Objectives	Penyerang mencuri data, mengambil kredensial pengguna, dan melakukan spionase pada aktivitas target	Tidak ada data yang dapat dicuri karena eksploitasi tidak berhasil

Tabel 5. Hasil Pengujian Havoc CKC

Skenario A (Windows Defender Tidak Aktif)	Skenario B (Windows Defender Aktif)
Phishing berhasil dilakukan, menunjukkan bahwa sistem tanpa proteksi Windows Defender rentan terhadap serangan berbasis rekayasa sosial.	Windows Defender terbukti efektif dalam mencegah serangan phishing, mencegah eksekusi malware dan perlindungan terhadap serangan berbasis rekayasa sosial.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil pengujian yang dilakukan terhadap sistem operasi Windows 10 menggunakan metode Cyber Kill Chain (CKC), ditemukan bahwa tingkat keberhasilan eksploitasi sangat bergantung pada kondisi keamanan sistem. Pengujian Metasploit CKC Skenario A menunjukkan bahwa eksploitasi terhadap SMBv1 menggunakan EternalBlue (CVE-2017-0143) berhasil dilakukan ketika firewall dalam kondisi tidak aktif, memungkinkan penyerang memperoleh hak akses administrator secara penuh. Sebaliknya, pada Metasploit CKC Skenario B, eksploitasi gagal dilakukan karena firewall aktif, sehingga lalu lintas jaringan berbahaya berhasil diblokir

Dalam pengujian Havoc CKC Skenario A, teknik phishing terbukti efektif dalam memperoleh hak akses administrator apabila Windows Defender tidak aktif. Hal ini menunjukkan bahwa rekayasa sosial masih menjadi metode serangan yang sangat berbahaya, terutama jika pengguna tidak memiliki kesadaran terhadap ancaman keamanan siber. Namun, pada Havoc CKC Skenario B, serangan phishing gagal dilakukan karena Windows Defender berhasil mendeteksi dan memblokir eksekusi payload yang dikirimkan melalui email berbahaya

Secara keseluruhan, penelitian ini mengonfirmasi bahwa kerentanan Windows 10 sangat bergantung pada pengaturan keamanan sistem. Proteksi seperti firewall dan Windows Defender memainkan peran krusial dalam mencegah eksploitasi. Oleh karena itu, penting bagi pengguna untuk selalu memperbarui sistem operasi, mengaktifkan firewall, serta meningkatkan kesadaran terhadap ancaman berbasis rekayasa sosial guna mengurangi risiko serangan siber

Berdasarkan hasil penelitian ini, terdapat beberapa saran yang dapat diterapkan untuk meningkatkan keamanan Windows 10 terhadap serangan siber. Studi lebih lanjut diperlukan untuk menguji dan meningkatkan efektivitas fitur keamanan bawaan seperti Windows Defender dan firewall, serta mengintegrasikannya dengan solusi keamanan pihak ketiga guna menciptakan lapisan perlindungan yang lebih kuat. Selain itu, penelitian berkelanjutan sangat diperlukan untuk mengidentifikasi ancaman baru dan mengembangkan metode pengujian penetrasi yang lebih inovatif serta responsif terhadap perkembangan serangan siber. Upaya lainnya mencakup pengembangan sistem pemantauan yang lebih canggih dan otomatis untuk mendeteksi aktivitas mencurigakan pada Windows, dengan memanfaatkan teknik pembelajaran mesin guna menganalisis log serta mendeteksi anomali yang berpotensi membahayakan sistem.

DAFTAR REFERENSI

Abraham, S., Greg, G., & Peter Baer, G. (2018). Operating system concepts (10th ed.).

Algarni, S. (2021). Cybersecurity attacks: Analysis of WannaCry attack and proposing methods for reducing or preventing such attacks in the future. In ICT systems and sustainability: Proceedings of ICT4SD 2020, Volume 1 (pp. 763–770). Springer.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Andhika, D. A. (2021). Pengujian penetrasi pada Windows 10 menggunakan Model Penetration Testing Execution Standard (PTES) [Tesis, Universitas Dinamika].

Desclaux, G., & Claverie, B. (2022). C2-command and control: A system of systems to control complexity. American Journal of Management, 22(2).

Fermana, M. F. N. (2022). Analisis kerentanan keamanan sistem pada Windows Server 2022 menggunakan metode Penetration Testing Execution Standard.

Gupta, M. R., Koli, Y. P., Patiyane, V. A., & Wagh, K. P. (2021). EternalBlue vulnerability.

Jayasuryapal, G., Pranay, P., Kaur, H., & Swati. (2021). A survey on network penetration testing. In 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 373–378). IEEE.

Kumar, P. R., & Ramlie, H. R. E. B. H. (2021). Anatomy of ransomware: Attack stages, patterns and handling techniques. In Computational intelligence in information systems: Proceedings of the Computational Intelligence in Information Systems Conference (CIIS 2020) (pp. 205–214). Springer.

Lestari, D. P., Indarti, D., Setiawan, D. E., & Rasal, I. (2019). Platform digital tata kelola sumber daya yang terintegrasi untuk peningkatan kinerja dan daya saing usaha mikro, kecil, dan menengah.

Mohamed, N., & Abiodun, O. (2021). Protect governments and organizations' infrastructure against cyber terrorism: Mitigation and stop of Server Message Block (SMB) remote code execution attack.

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing attack models for IT systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK framework, and Diamond Model. In 2022 IEEE International Symposium on Systems Engineering (ISSE) (pp. 1–7). IEEE.

Ontko, R., Reeder, A., & Tanenbaum, A. (2020). Modern operating systems simulators (MOSS).

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: Issues and challenges.

Yudha, F., & Prayudi, Y. (2021). Teknik eksplorasi bukti digital pada file sharing protokol SMB untuk mendukung forensika digital pada jaringan komputer.