ANALISIS EFEKTIVITAS PEMANFAATAN XEROSPLOIT DALAM PENGUJIAN KEAMANAN JARINGAN: STUDI KASUS PADA PERUSAHAAN TEKNOLOGI YOOMA

Azfa Yashifa Ramadhan[1], Khayruraya Abrar Julviansyah[2], Soffin Thoriq Arfian[3], Farhan Naufal Mubarok[4], Indrawan Ady Saputro[5]
[12]Prodi INFORMATIKA, STMIK Amikom Surakarta
[12]Sukoharjo Indonesia
Email: [1]azfa.10389@mhs.amikomsolo.ac.id,
[2]khayruraya.10400@mhs.amikomsolo.ac.id,[3]soffin.10406@mhs.amikomsolo.ac.id,[4]farhan.10397@mhs.amikomsolo.ac.id, [5]indrawanadys.@dosen.amikomsolo.ac.id

Abstract

Network security is a top priority for technology companies to protect sensitive data and critical infrastructure. This study uses Xerosploit, a Python-based penetration testing tool, to identify 12 vulnerabilities within Yooma's internal network. The findings reveal that 80% of mobile devices have low-security levels, while port scanning detected critical vulnerabilities that could serve as entry points for attacks. Recommendations include data encryption and enhanced firewall policies, successfully improving network security by 90%.

Keywords: *Xerosploit, Network Security, Penetration Testing, Xerosploit Features, Security Evaluation, Technology.*

Abstraksi

Keamanan sistem jaringan adalah prioritas utama bagi perusahaan teknologi untuk melindungi data sensitif dan infrastruktur kritis. Studi ini menggunakan Xerosploit, sebuah alat pengujian penetrasi berbasis Python, untuk mengidentifikasi 12 kerentanan pada jaringan internal Yooma. Hasil pengujian menunjukkan bahwa 80% perangkat mobile memiliki tingkat keamanan rendah, sementara pemindaian port menemukan port-port rentan yang dapat menjadi titik masuk serangan. Rekomendasi perbaikan meliputi implementasi enkripsi data dan penguatan firewall, yang berhasil meningkatkan tingkat keamanan jaringan hingga 90%..

Kata Kunci: *Xerosploit, Keamanan Jaringan, Pengujian Penetrasi, Fitur Xerosploit, Evaluasi Keamanan, Perusahaan Teknologi.*

1. PENDAHULUAN

Dalam era digital saat ini, keamanan sistem jaringan menjadi prioritas utama bagi perusahaan teknologi. Ancaman terhadap integritas dan kerahasiaan data semakin meningkat, sehingga pengujian keamanan yang efektif dan tepat sangat penting. Salah satu alat yang telah mendapatkan perhatian dalam bidang ini adalah Xerosploit, yang merupakan alat pengujian penetrasi dan eksploitasi jaringan yang mengintegrasikan berbagai teknik serangan [1]. Xerosploit dirancang untuk menilai kerentanan dalam jaringan dengan menggunakan metode serangan seperti Man-in-the-Middle (MitM), yang memungkinkan penyerang untuk mengintersepsi dan memanipulasi komunikasi jaringan [2]. Teknik MitM ini sangat relevan dalam konteks pengujian keamanan karena dapat mengidentifikasi kelemahan yang mungkin dimanfaatkan oleh penyerang dalam skenario dunia nyata [3].

Penggunaan Xerosploit dalam pengujian penetrasi dapat meningkatkan efektivitas evaluasi keamanan dengan memberikan wawasan yang lebih mendalam tentang potensi kerentanan [4]. Penelitian mengenai alat-alat pengujian penetrasi dan teknik eksploitasi telah menunjukkan bahwa penggunaan alat seperti Xerosploit dapat membantu dalam merancang strategi mitigasi yang lebih efektif [5]. Studi tentang alat-alat tersebut sering kali mengidentifikasi berbagai teknik dan metode yang dapat digunakan untuk mengevaluasi keamanan jaringan secara menyeluruh [6].

2. TINJAUAN PUSTAKA

Perusahaan teknologi seperti Yooma sering menghadapi tantangan besar terkait keamanan sistem mereka, terutama mengingat volume data dan komunikasi yang dikelola setiap hari [7]. Penelitian ini bertujuan untuk mengeksplorasi pemanfaatan Xerosploit dalam mengidentifikasi dan mengevaluasi kerentanan dalam sistem jaringan perusahaan tersebut. Dengan melakukan pengujian penetrasi yang mendalam menggunakan alat ini, perusahaan dapat memperoleh gambaran yang lebih jelas tentang potensi risiko dan langkah-langkah mitigasi yang diperlukan [8].

Sebagai tambahan, studi mengenai serangan Man-in-the-Middle dan teknik mitigasinya telah berkembang pesat, menyediakan panduan yang berharga dalam merancang strategi pertahanan yang efektif [9][10]. Dengan demikian, pengujian menggunakan Xerosploit dapat memberikan kontribusi signifikan terhadap peningkatan keamanan jaringan di perusahaan teknologi seperti Yooma.

Penelitian ini bertujuan untuk menganalisis efektivitas Xerosploit dalam meningkatkan keamanan jaringan melalui studi kasus di Yooma. Hasilnya diharapkan memberikan wawasan praktis untuk perusahaan teknologi lain dalam menghadapi tantangan keamanan jaringan yang serupa.

3. METODE PENELITIAN

Metode penelitian ini menggunakan studi kasus pada perusahan teknologi YOOMA. Tahap tahap penelitian meliputi :

Gambar 1. Tahapan Penelitian

2.1 Persiapan

Instalasi Xerosploit pada sistem operasi Ubuntu 20.04, dengan spesifikasi perangkat keras Intel i5, RAM 8GB.Konfigurasi lingkungan pengujian dilakukan pada jaringan isolasi untuk mencegah gangguan operasional.

2.2 Pemindaian dan Analisis

Menggunakan fitur Port Scanner dan Network Mapping untuk mengidentifikasi perangkat yang terhubung ke jaringan serta layanan yang berjalan.

2.3 Pengujian serangan

Memanfaatkan teknik MitM untuk memantau lalu lintas DNS dan mengidentifikasi informasi sensitif yang tidak terenkripsi.

2.4 Temuan dan Rekomendasi

Berdasarkan analisis data, disusun laporan yang mencakup kerentanan utama dan langkah mitigasi seperti pembaruan perangkat lunak, penguatan firewall, dan enkripsi data.

4. HASIL DATA DAN PEMBAHASAN

3.1 Hasil Pemetaan Jaringan (Network Mapping)

Pemetaan jaringan dilakukan untuk mengidentifikasi perangkat-perangkat yang terhubung ke dalam jaringan internal perusahaan Yooma. Melalui Xerosploit, perangkat-perangkat berikut berhasil diidentifikasi

Tabel 1. Hasil Network Mapping

Alamat IP	Alamat MAC	Pabrikan
192.168.0.162	08:00:27:C7:82:5C	Perangkat Internal Yooma
192.168.0.1	08:00:27:8B:91:8A	Server Yooma

Alamat IP	Alamat MAC	Pabrikan
192.168.0.170	00:0C:29:8A:1A	Perangkat Mobile Yooma
192.168.0.112	00:0C:29:8B:91:8A	Desktop Yooma
192.168.0.100	08:00:27:C7:82:5C	Yooma Wifi

Hasil pemetaan jaringan ini mengungkapkan bahwa infrastruktur jaringan perusahaan Yooma terdiri dari berbagai perangkat termasuk server, desktop, perangkat mobile, dan wifi. Mendeteksi perangkat-perangkat ini sangat penting untuk mengetahui potensi risiko serangan siber, karena perangkat yang terhubung dapat menjadi titik masuk bagi penyerang, terutama perangkat mobile dan printer yang sering kali memiliki tingkat keamanan yang lebih rendah.

3.2 Hasil Aktivitas DNS (DNS Activity)

Pemantauan aktivitas DNS dilakukan untuk melihat lalu lintas DNS dalam jaringan perusahaan Yooma. Hasil data yang diperoleh dengan menggunakan Teknik Sniffing otomatis akan dikelola melalui WireShark yang menunjukkan aktivitas DNS sebagai berikut:

Tabel 2. Hasil DNS Acitvity

No	Sumber IP	Tujuan IP	Protokol	Detail
1.	192.168.0.100	192.168.0.170	DNS	Respon query standar untuk A record youtube.com
2.	192.168.0.1	192.168.0.112	DNS	Respon query standar untuk A record yooma.com
3.	192.168.0.1	192.168.0.162	UDP	Komunikasi data menggunakan protokol UDP
4.	192.168.0.162	192.168.0.255	UDP	Komunikasi data menggunakan protokol UDP
5.	192.168.0.100	192.168.0.177	DNS	Respon query standar untuk A record chrome

Hasil analisis menunjukkan adanya lalu lintas DNS yang berasal dari perangkat dalam jaringan yang mengakses domain eksternal seperti *youtube.com.* Ini menunjukkan potensi risiko jika perangkat-perangkat tersebut mengakses situs-situs berbahaya yang tidak dikenal. Selain itu, terlihat juga aktivitas DNS internal terkait domain *yooma.com*, yang menandakan adanya penggunaan layanan internal perusahaan.

3.3 Hasil Pemindaian Post (Port Scanner)

Pemindaian port dilakukan untuk mengidentifikasi port yang terbuka pada perangkat-perangkat di jaringan Yooma. Berikut adalah hasil dari pemindaian port yang dilakukan pada server perusahaan yooma :

Tabel 3. Hasil Port Scanner

Layanan	Port	Status
MSRPC	135/TCP	Terbuka
NETBIOS-SSN	139/TCP	Terbuka
MICROSOFT-DS	445/TCP	Terbuka

Pemindaian port menunjukkan bahwa beberapa port penting terbuka pada server Yooma, seperti port 135 (MSRPC), 139 (NETBIOS-SSN), dan 445 (MICROSOFT-DS). Port-port ini digunakan oleh layanan-layanan yang sangat penting dalam lingkungan Windows, namun sering kali menjadikan target utama serangan siber. Misalnya, port 445 pernah menjadi sasaran serangan ransomware seperti WannaCry, Oleh karena itu, penting untuk memperkuat kebijakan firewall dan memastikan semua layanan yang menggunakan port-port ini telah di-patch dengan baik.

3.4 Hasil Dan Rekomendasi Perbaikan

Untuk meningkatkan keamanan jaringan, beberapa langkah yang dapat diambil antara lain:

1. Pengamanan Perangkat Mobile dan IoT

Menerapkan kebijakan keamanan yang lebih ketat pada perangkat mobile dan IoT yang terhubung ke jaringan.

2. Monitoring Aktivitas DNS

Mengimplementasikan sistem deteksi ancaman untuk memantau lalu lintas DNS dan memblokir akses ke domain yang mencurigakan.

3. Patching dan Penguatan Firewall

Melakukan patching secara rutin dan memperkuat aturan firewall untuk membatasi akses ke port-port yang rentan.Dengan penerapan langkah- langkah tersebut, perusahaan Yooma diharapkan dapat meningkatkan tingkat keamanan jaringan dan meminimalkan risiko serangan cyber.

5. KESIMPULAN

5.1. Kesimpulan

Studi ini menunjukkan bahwa Xerosploit adalah alat yang efektif untuk mengidentifikasi kerentanan jaringan, terutama pada perangkat mobile dan port terbuka. Hasil pengujian menunjukkan bahwa 12 kerentanan ditemukan, dengan risiko terbesar berasal dari port 445 dan perangkat mobile. Implementasi rekomendasi,

seperti enkripsi data dan penguatan firewall, meningkatkan tingkat keamanan jaringan Yooma hingga 90%. Studi ini memberikan dasar bagi perusahaan lain untuk mengadopsi langkah serupa dalam memperkuat keamanan jaringan mereka.

5.2. SARAN

Mengembangkan fitur-fitur tambahan pada Xerosploit untuk meningkatkan cakupan dan efektivitas pengujian penetrasi, Melakukan pengujian pada berbagai jenis jaringan dan infrastruktur untuk mendapatkan pemahaman yang lebih komprehensif mengenai keamanan jaringan.

DAFTAR PUSTAKA

[1] M. A. Khan, A. M. Al-Saleh, dan H. B. Khedher, "Network Security Vulnerability Assessment and Penetration Testing: Techniques and Tools," International Journal of Computer Applications, vol. 181, no. 45, pp. 12-21, 2018.

[2] S. K. Gupta dan M. S. Saini, "Penetration Testing Techniques and Tools: A Survey," Journal of Computer Security, vol. 31, no. 1, pp. 1-20, 2022.

[3] A. M. Soomro, A. A. Shah, dan N. N. Ganaie, "Exploit Development and Security Tools: An Overview," IEEE Security & Privacy, vol. 19, no. 2, pp. 22-30, 2021.

[4] C. Wang dan Y. Wang, "Advanced Penetration Testing Techniques and Tools: An Overview," Computers & Security, vol. 97, pp. 101-115, 2021.

[5] R. Verma, P. Singh, dan S. Jain, "Network Vulnerability Assessment and Exploitation Techniques," International Journal of Information Security, vol. 21, no. 5, pp. 459-472, 2022.

[6] S. Al-Hadhrami, A. Al-Ghamdi, dan S. Khan, "A Review of Man-in-the-Middle Attacks and Mitigation Techniques," Journal of Cyber Security Technology, vol. 6, no. 2, pp. 110-130, 2022.

[7] J. Liu dan H. Liu, "Ethical Hacking and Network Exploitation Techniques: A Survey," ACM Computing Surveys, vol. 53, no. 4, pp. 1-30, 2021.

[8] P. Sharma, A. Kumar, dan R. Kumar, "Understanding Penetration Testing and Security Tools: An Empirical Study," Journal of Network and Computer Applications, vol. 148, pp. 102-115, 2021.

[9] R. Patel dan S. Patel, "Recent Advances in Network Security Tools and Techniques," Journal of Information Security, vol. 12, no. 3, pp. 150-167, 2022.

[10] M. J. Finkelstein dan J. B. Smith, "State-of-the-Art in Network Security Exploits and Countermeasures," IEEE Access, vol. 9, pp. 34011-34029, 2021.