EVALUASI KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN NETWORK MAPPING

Rakhmadi Rahman[1], Indah Amelya Aprilia[2], Zulkifli[3]
rakhmadi.rahman@ith.ac.id[1], indahamelyaaprilia.s.241031040@mahasiswa.ith.ac.id[2], zulkifli.241031053@mahasiswa.ith.ac.id[3]
Instutit Teknologi Bacharuddin Jusuf Habibie

ABSTRAK

Keamanan infrastruktur jaringan memainkan peran penting dalam memastikan keamanan dan integritas data organisasi. Namun, visibilitas terbatas ke dalam aset jaringan sering menciptakan kerentanan yang dapat dieksploitasi oleh aktor jahat. Studi ini berupaya menilai tingkat keamanan lingkungan Local Area Network (LAN) dengan menggunakan teknik pemetaan jaringan. Pendekatannya deskriptif dan evaluatif, mengandalkan alat keamanan seperti Nmap, Zenmap, dan Wireshark. Proses evaluasi melibatkan beberapa langkah, termasuk mengidentifikasi rentang IP, menemukan host aktif, melakukan pemindaian port terperinci, mendeteksi layanan, dan menentukan sistem operasi yang digunakan. Temuan mengungkapkan 15 perangkat aktif, salah satunya adalah perangkat tidak sah yang terhubung tanpa izin. Selain itu, 65 pelabuhan terbuka diidentifikasi, dengan 45 di antaranya merupakan layanan non-kritis yang meningkatkan potensi serangan. Penilaian kerentanan juga mengungkap penggunaan Apache 2.4.49, yang rentan terhadap serangan traversal jalur. Studi ini menyimpulkan bahwa melakukan pemetaan jaringan secara teratur merupakan praktik penting untuk mengidentifikasi aktivitas yang tidak biasa dan meningkatkan keamanan infrastruktur jaringan yang berfokus pada data melalui audit aktual.
Kata Kunci: Keamanan Jaringan, Network Mapping, Nmap, Port Scanning, Kerentanan Sistem.

ABSTRACT

Network infrastructure security plays a vital role in ensuring the safety and integrity of an organization's data. However, limited visibility into network assets often creates vulnerabilities that can be exploited by malicious actors. This study seeks to assess the security level of Local Area Network (LAN) environments using a network mapping technique. The approach is descriptive and evaluative, relying on security tools such as Nmap, Zenmap, and Wireshark. The evaluation process involves several steps, including identifying the IP range, discovering active hosts, performing detailed port scanning, detecting services, and determining the operating system in use. The findings revealed 15 active devices, one of which was an unauthorized device connected without permission. Additionally, 65 open ports were identified, with 45 of them being non-critical services that increase the potential for attacks. A vulnerability assessment also uncovered the use of Apache 2.4.49, which is susceptible to path traversal attacks. The study concludes that regularly conducting network mapping is an essential practice for identifying unusual activities and improving the security of data-focused network infrastructures through actual audits.
***Keywords**: Network Security, Network Mapping, Nmap, Port Scanning, System Vulnerability.*

PENDAHULUAN

Dalam lingkungan digital yang kompleks saat ini, jaringan komputer sering ditargetkan oleh berbagai jenis ancaman cyber, seperti akses tidak sah dan pencurian data penting. Tantangan utama bagi administrator jaringan adalah kurangnya kesadaran tentang semua perangkat yang terhubung ke infrastruktur jaringan mereka. Tanpa pemahaman yang jelas tentang tata letak jaringan, perangkat yang tidak terpakai atau tidak dikelola, serta layanan yang ketinggalan jaman, dapat menciptakan peluang bagi penyerang untuk memasuki sistem.

Pemetaan jaringan lebih dari sekadar membuat diagram visual; ini adalah metode aktif untuk memeriksa dan menganalisis jaringan untuk memahami bagaimana data

bergerak dan di mana kelemahan mungkin ada.

Melalui pemetaan jaringan, administrator dapat menentukan port mana yang harus diamankan atau ditutup, dan memastikan bahwa tidak ada perangkat yang tidak sah atau tidak dikenal yang terhubung ke jaringan. Studi ini menguraikan proses penggunaan teknik-teknik ini untuk menilai keamanan jaringan dan menawarkan pandangan yang jelas tentang potensi risiko dalam jaringan lokal.

METODOLOGI

Penelitian ini menggunakan pendekatan deskriptif-evaluatif, mengumpulkan data dengan mengamati langsung subjek penelitian menggunakan metode teknis. Tahapan penelitian disusun secara sistematis sebagai berikut:

1. Tahap Identifikasi: Proses mengidentifikasi cakupan jaringan dan subnet yang akan dinilai.
2. Tahap pemindaian: Melibatkan penggunaan alat Nmap untuk mengidentifikasi host aktif dengan menggunakan protokol pemindaian ICMP dan TCP/UDP.
3. Tahap Enumerasi: Fase ini melibatkan pemeriksaan menyeluruh setiap host untuk mengidentifikasi layanan yang sedang aktif, seperti HTTP yang beroperasi pada port 80 atau SSH pada port 22, bersama dengan versi spesifik dari perangkat lunak yang digunakan.
4. Tahap Analisis Kerentanan: Melibatkan perbandingan versi layanan yang diidentifikasi dengan database kerentanan komprehensif, seperti CVE, untuk menilai tingkat risiko yang ditimbulkannya.

HASIL DAN PEMBAHASAN

A. Analisis Perangkat dan Visabilitas Aset

Berdasarkan temuan dari proses penemuan host, sistem mampu mengidentifikasi dan memetakan 15 node aktif. Pengamatan yang memprihatinkan adalah identifikasi satu perangkat yang memiliki alamat MAC yang tidak dikenali dalam catatan organisasi. Kehadiran perangkat tidak sah ini menunjukkan potensi kelemahan dalam kebijakan kontrol akses fisik atau protokol keamanan nirkabel seperti WPA atau WPA2, yang mungkin rentan terhadap eksploitasi.

B. Audit Port dan Analisis Surface Attack

Memindai seluruh 65.535 port menghasilkan data yang menunjukkan 65 port terbuka. Dari jumlah tersebut, 69% (yaitu 45 port) merupakan layanan yang tidak mendukung fungsi operasional penting namun tetap aktif secara default. Setiap port terbuka mewakili titik masuk yang mungkin bagi malware atau peretas untuk mendapatkan akses.

C. Identifikasi Layanan Kritis dan Sistem Operasi

Analisis deteksi layanan menemukan bahwa server web Apache versi 2.4.49 sedang digunakan. Versi ini memiliki masalah keamanan teknis yang memungkinkan penyerang mengakses file sistem yang biasanya dilindungi dengan menavigasi jalur file. Selain itu, deteksi sistem operasi menunjukkan bahwa beberapa perangkat lama tidak lagi menerima pembaruan keamanan, sehingga sangat rentan untuk dieksploitasi secara otomatis.

D. Analisis Topologi dan Segmentasi

Hasil pemetaan menunjukkan bahwa topologi bintang sedang digunakan, dengan satu saklar utama di tengahnya, dan tidak ada segmentasi VLAN di tempatnya. Karena tidak ada segmentasi VLAN, seluruh jaringan beroperasi dalam satu domain siaran. Akibatnya, jika satu perangkat disusupi, serangan seperti mengendus paket atau penyebaran ransomware di seluruh jaringan menjadi jauh lebih mudah.

KESIMPULAN

Studi ini menunjukkan bahwa metode pemetaan jaringan dapat mengungkap informasi teknis yang tersembunyi, namun juga berdampak signifikan terhadap keamanan. Hasilnya, termasuk identifikasi perangkat yang tidak sah dan sejumlah port yang tidak perlu, menunjukkan bahwa memiliki visibilitas yang jelas sangat penting untuk memastikan keamanan.

DAFTAR PUSTAKA

M. Al-Saud and B. J. Mohd, "Network mapping and vulnerability assessment for improving network security," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 6, 2020.

G. F. Lyon, Nmap Network Scanning: The Official Nmap Project Guide. Insecure.org, 2023.

S. Choudhary and A. Gupta, "Network security assessment using Nmap scanning techniques," J. Netw. Inf. Secur., vol. 9, no. 2, 2021.

R. Muslim, et al., "Evaluasi keamanan jaringan menggunakan metode pemindaian aktif," Jurnal Sistem Informasi, vol. 10, no. 1, 2021.

W. Stallings, Network Security Essentials: Applications and Standards, 7th ed. Pearson, 2021.