# BAB V

# KESIMPULAN DAN SARAN

## 5.1. Kesimpulan

Dari hasil uraian pada bab sebelumnya dapat disimpulkan bahwa identifikasi kerentanan pada jaringan menggunakan metode *penetration testing* dengan jenis serangan *ip scanning, port scanning* dan *packet scanning* dapat digunakan untuk mencari kerentanan pada jaringan. Hasil pengujian IP *scanning* dengan alat *advanced* IP *scanner* adalah *attacker* dengan mudah melakukan pemindaian menyeluruh terhadap jaringan komputer perusahaan dengan tujuan menemukan dan mengidentifikasi perangkat yang terkoneksi ke dalamnya. Pengujian kedua yang dilakukan dengan *port scanning* dengan alat NMAP adalah *attacker* menggunakan alat pemindaian *port* dapat mengetahui *port* apa saja yang terbuka pada suatu sistem. Pengujian selanjtnya yaitu *packet scanning* dengan alat *wireshark* berhasil menemukan *packet* yang memiliki kerentanan yaitu pada *protocol* HTTP *port* 80 ketika target melakukan *login via webfig, didapatkan* informasi dari *packet* berupa IP target, *username*, *password*, dan *url* nya. Pengujian selanjutnya yaitu denial of service (DoS) menggunakan slowhttptest pada kali linux. Attacker berhasil melakukan denial of service (DoS) membuat layanan lambat di akses. Pengujian terakhir yaitu DNS Spoofing menggunakan Ettercap pada kali linux. Attacker gagal melakukan DNS Spooning karena kemungkinan server DNS yang aman.

Untuk mengatasi kerentanan yang ditemukan, perusahaan bisa menggunakan rekomendasi perbaikan. Perbaikan yang bisa dilakukan untuk mengatasi IP *scanning* adalah pisahkan jaringan internal menjadi segmen-segmen yang berbeda, konfigurasi *firewall* untuk membatasi akses ke jaringan *internal* hanya dari alamat IP yang terpercaya dan memberikan pelatihan keamanan kepada karyawan untuk meningkatkan kesadaran tentang praktik keamanan jaringan. Perbaikan yang bisa dilakukan untuk mengatasi *port scanning* adalah

menggunakan *Intrusion Detection and Prevention System* (IDPS) pada jaringan komputer, mengubah nama *port* atau *disabled port* yang sedang tidak digunakan, pastikan *firewall* dikonfigurasi dengan benar untuk memblokir lalu lintas yang tidak diinginkan dan aktifkan *logging* pada *firewall, router, dan server* untuk mencatat semua upaya akses dan lalu lintas jaringan. Perbaikan yang bisa dilakukan untuk mengatasi *packet scanning* adalah menerapkan *port knocking*, menggunakan *protocol* HTTPS daripada HTTP, pisahkan jaringan sensitif dari jaringan yang lebih umum atau tidak aman menggunakan VLAN dan edukasi pengguna dan staf TI tentang praktik keamanan jaringan. Perbaikan yang bisa dilakukan untuk mengatasi *denial of service* (DoS*)* adalah gunakan layanan cloud dengan proteksi DDoS (Distributed Denial of Service) yang dapat menangani serangan besar-besaran dengan infrastruktur dan kapasitas yang lebih besar.

## 5.2. Saran

Penelitian selanjutnya dalam melakukan *penetration testing* dapat memperluas metode yang digunakan dengan menambahkan teknik seperti *brute force, ping flooding,* dan pengenalan *malware*. Dengan pendekatan ini, diharapkan dapat mengidentifikasi lebih banyak kerentanan, memberikan gambaran yang lebih komprehensif tentang potensi ancaman yang dihadapi, serta memperkuat langkah-langkah mitigasi yang diperlukan untuk melindungi infrastruktur jaringan.

# DAFTAR PUSTAKA


[1] Y. Citra, mahendra, and N. K. D. Setiawati Arya Pinatih, "Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia," *J. Rev. Pendidik. dan Pengajaran,* vol. 6, no. 4, p. 1941, 2023.

[2] R. Damanik, P. Andika, and Rahmayanti, "Sistem Pengamanan Jaringan Terhadap Serangan Cyber Warfare," *TNI Angkatan Udar.*, vol. 2, no. 2, pp. 63–76, 2023, [Online]. Available: https://e-jurnal.tni-au.mil.id/index.php/jpb/article/download/67/63.

[3] E. Sachlos and D. Auguste, "Jurnal Ilmu Komputer," *Biomaterials*, vol. 29, no. 34, pp. 4471–4480, 2022.

[4] M. A. Ajharie and M. Sulistiyono, "Implementasi Framework Mitm (Man in the Middle Attack) Untuk Memantau Aktifitas Pengguna Dalam Satu Jaringan," *J. Infomedia*, vol. 7, no. 1, p. 45, 2022, doi: 10.30811/jim.v7i1.2966.

[5] L. Adi Saputra, F. Muhammad Akbar, F. Cahyaningtias, M. Puspa Ningrum, and A. Fauzi, "Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan," *J. Pendidik. Siber Nusant.*, vol. 1, no. 2, pp. 58–66, 2023, doi: 10.38035/jpsn.v1i2.48.

[6] K. Khotimah, K. Murti Prabowo, and K. Kunci, "Penerapan Layanan Publik Menggunakan Secure Socket Tunneling Protokol (Sstp)," *Sci. Technol. J.*, vol. 12, no. 2, pp. 28–39, 2022.

[7] S. Informasi, U. Merdeka, M. Jalan, T. Dieng, and N. Klojen, "Implementasi Honeypot Dionaea Sebagai Uji Kerentanan dan Penunjang Keamanan Jaringan," no. September, pp. 3807–3817, 2023.

[8] M. Yaqi, *Vulnerability Assessment dan Penetration Testing (Vapt) Menggunakan Metode Zero Entry Hacking (Zeh) Terhadap Website Studi Kasus: Dinas Penanaman Modal …*. 2023.

[9] Herman, R. Umar, and A. Prasetyo Marsaid, "Analisis Keamanan Jaringan

LAN Terhadap Kerentanan Jaringan Ancaman DDoS Menggunakan Metode Penetration Testing," *J. Ris. Komput.*, vol. 10, no. 1, pp. 2407–389, 2023, doi: 10.30865/jurikom.v10i1.5835.

[10] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," *sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, 2022, doi: 10.56211/sudo.v1i4.160.

[11] A. S. Anggraini, S. Raharjo, and P. Haryani, "Analisis Keamanan Jaringan Router Mikrotik Menggunakan Metode Penetration Testing Man in the Middle ( Mitm )," vol. 10, no. 2, 2022.

[12] T. Yusnanto, M. A. Muin, and S. Wahyudiono, "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux," *J. Educ.*, vol. 4, no. 4, pp. 1470–1476, 2022, doi: 10.31004/joe.v4i4.2175.

[13] A. K. Ibrahim, "Analisis Keamanan Sistem Informasi Dengan Penetration Testing Dan Iso 27001: 2013 (Studi Kasus Sistem Informasi Manajemen Aset …," vol. 2013, 2019, [Online]. Available: https://digilib.uin-suka.ac.id/id/eprint/37042.

[14] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, "Mobile Application Security Penetration Testing Based on OWASP," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 846, no. 1, 2020, doi: 10.1088/1757-899X/846/1/012036.

[15] D. D. Papaceda, A. Mewengkang, and S. Pratasik, "Analisis dan Pengembangan Jaringan Komputer di SMK Negeri 8 Weda Halmahera Tengah," *Edutik J. Pendidik. Teknol. Inf. dan Komun.*, vol. 3, no. 1, pp. 1–13, 2023, doi: 10.53682/edutik.v3i1.6465.

[16] H. Suhendi and H. Gusdevi, "Perancangan Jaringan Komputer Wide Area Network Menggunakan Mpls (Multylayer Protocol Labeling Switching)," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 5, no. 1, pp. 96–103, 2023,

doi: 10.53580/naratif.v5i1.214.

[17] S. Kasus, S. M. K. Kesehatan, B. Kencana, J. F. Fitrian, and H. Sujadi, "IMPLEMENTASI HOTSPOT DENGAN PENGELOLAAN USER MANAGER DAN BANDWIDTH MENGGUNAKAN MIKROTIK RB941-2nd," vol. 1, no. 1, 2023.

[18] M. Wicaksono and J. Pamungkas, "Membuat Web Server Menggunakan Debian 10 Pada Virtual," *J. Informatics Electr. Eng. Univ. Aisyah Pringsewu*, vol. 4, no. 1, pp. 17–26, 2022, [Online]. Available: http://jti.aisyahuniversity.ac.id/index.php/AJIEE.

[19] M. Ibrahim, "Implementasi dan Analisis Profil Sistem Pada Virtualisasi Fortigate Firewall Berdasarkan Metrik Sumber Daya Komputasi Implementation and Analysis of System Profile on Fortigate Firewall Virtualization Based on Computing Resource Metrics," vol. 10, no. 2, pp. 1505–1511, 2023.

[20] D. Rezano Akhiruddin and T. Sutabri, "Analisis Peningkatan Keamanan Pada Simple Network Time Protocol (Sntp) Untuk Mendeteksi Cybercrime Dalam Aktifitas Jaringan Menggunakan Metode Firewall," *Blantika Multidiscip. J.*, vol. 2, no. 1, pp. 21–32, 2023, doi: 10.57096/blantika.v2i1.9.

[21] M. T. Sulistyono *et al.*, "Peningkatan Sumberdaya Panti Asuhan Dalam Pengamankan Aset Informasi Dengan Teknologi Literasi Informasi," *Abdimasku J. Pengabdi. Masy.*, vol. 5, no. 2, p. 295, 2022, doi: 10.33633/ja.v5i2.452.

[22] A. Khaliq and N. Sari, "Pemanfaatan Kerangka Kerja Investigasi Forensik Jaringan Untuk Identifikasi Serangan Jaringan Menggunakan Sistem Deteksi Intrusi (IDS)," *J. Nas. Teknol. Komput.*, vol. 2, no. 3, pp. 150–158, 2022, [Online]. Available: https://publikasi.hawari.id/index.php/jnastek/article/view/52.

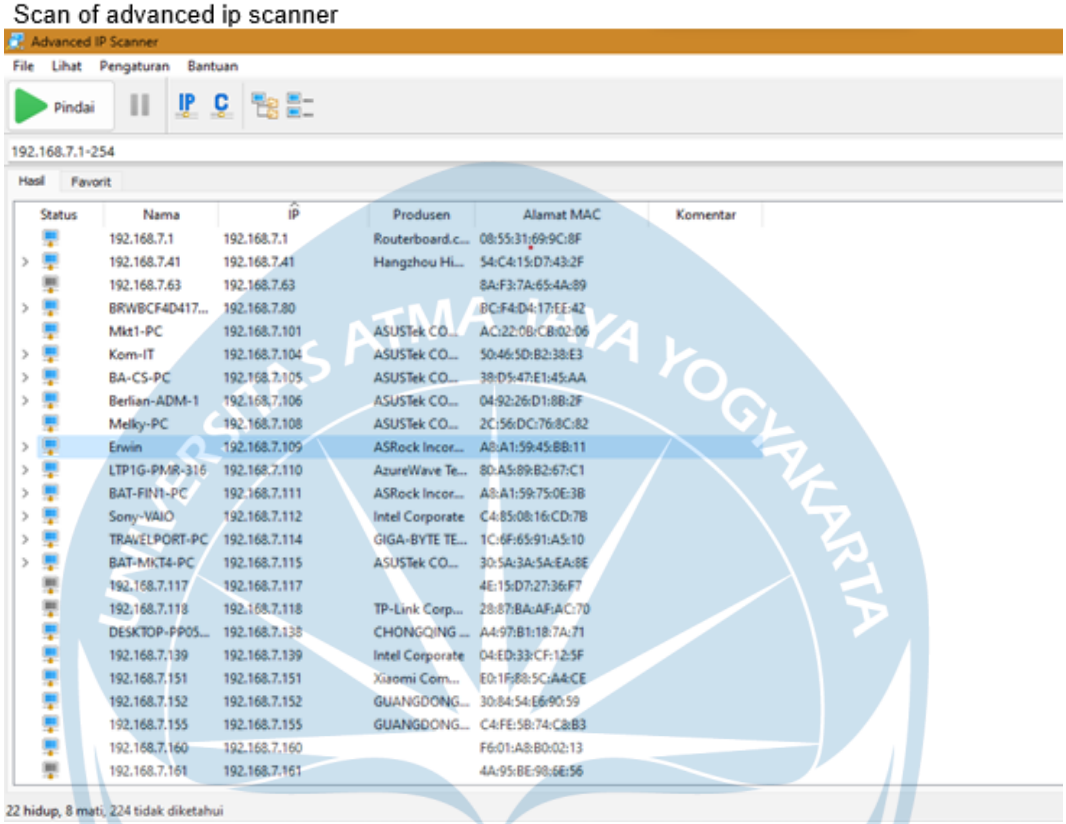
[23] T. Informatika, P. Scan, and J. Komputer, "Journal of Data Science and Information System (DIMIS)," vol. 1, no. 2, pp. 41–49, 2023, [Online]. Available: https://doi.org/10.58602/dimis.v1i2.35.

[24] A. Arini, M. Luthfi Arsalan, and H. Teja Sukmana, “Keamanan Jaringan Wi-Fi Terhadap Serangan Packet Sniffing Menggunakan Firewall Rule (Studi Kasus : Pt. Akurat.Co),” *Cyber Secur. dan Forensik Digit.*, vol. 6, no. 2, pp. 30–38, 2024, doi: 10.14421/csecurity.2023.6.2.4075.

[25] Zahrani Fatni Hapsah and Muhammad Irwan Padli Nasution, “Analisis Tingkat Keamanan Data Perusahaan Yang Rentan Terhadap Serangan Cyber Dalam Sistem Informasi Manajemen,” *J. Manaj. Dan Akunt.* , vol. 1, no. 2, pp. 338–343, 2023.

# Lampiran

Scan of advanced ip scanner




Scan of NMAP