Network Assessment Pada Prama Sanur Beach Hotel Menggunakan Metode Vulnerability Assessment

I Putu Hogi Pradnya Diva [1a], Ricky Aurelius Nurtanto Diaz [2b], I Made Ari Santosa [1c]
[1]Sistem Komputer, Institut Teknologi dan Bisnis STIKOM Bali, Bali, Indonesia
e-mail: [a] Hogipradnyadiva01@gmail.com, [b]ricky@stikom-bali.ac.id, [c]arisantosa@stikom-bali.ac.id

Abstrak

Prama Sanur Beach Hotel memiliki ketergantungan tinggi pada infrastruktur jaringan untuk layanan operasional (reservasi, data tamu, Wi-Fi, POS, dan perangkat jaringan), namun berdasarkan pengamatan awal masih terdapat indikasi pengelolaan keamanan yang belum optimal (pembaruan perangkat, konfigurasi, dan audit berkala). Penelitian ini menerapkan Vulnerability Assessment melalui tahapan evaluasi karakteristik sistem, identifikasi kerentanan, analisis dampak berbasis CIA dan CVSS, serta penyusunan rekomendasi kontrol; pemetaan layanan dilakukan dengan Nmap dan deteksi kerentanan menggunakan Nessus (Basic Network Scan). Hasil menunjukkan terdapat 0 Critical, 1 High, 13 Medium, dan 2 Low. Temuan prioritas mencakup SWEET32/dukungan 3DES pada DNS/DC (High), beberapa isu SSL/TLS (TLS 1.0/1.1, RC4, sertifikat self-signed/tidak dipercaya), SMB signing tidak diwajibkan pada layanan SMB/445, Telnet tanpa enkripsi pada PABX/23, serta potensi penyalahgunaan NTP Mode 6 dan konfigurasi IP forwarding pada PABX. Rekomendasi difokuskan pada hardening layanan (TLS, SMB, RDP), pembatasan akses port manajemen, serta penonaktifan layanan tidak aman agar risiko dapat ditekan tanpa mengganggu operasional hotel.

Kata kunci: *Network Assessment, Vulnerability Assessment, Nmap, Nessus, Keamanan Jaringan.*

1. Pendahuluan

Prama Sanur Beach Hotel merupakan salah satu hotel ternama di kawasan pesisir Sanur, Bali, yang telah beroperasi sejak tahun 1970-an sebagai bagian dari perkembangan pariwisata Bali. Seiring transformasi layanan menuju operasional yang modern, hotel ini semakin bergantung pada teknologi informasi dan komunikasi, khususnya infrastruktur jaringan komputer, untuk mendukung layanan inti seperti sistem reservasi kamar, pengelolaan data tamu, akses *Wi-Fi*, integrasi sistem POS *(Point of Sale)*, hingga perangkat pintar yang terhubung dalam jaringan. Ketergantungan tinggi terhadap jaringan memberi manfaat berupa efisiensi dan peningkatan kualitas layanan, namun pada saat yang sama meningkatkan paparan terhadap risiko keamanan siber[1]. Gangguan pada jaringan tidak hanya berdampak pada penurunan kualitas layanan, tetapi juga berpotensi memengaruhi stabilitas operasional dan reputasi hotel di mata pelanggan[2].

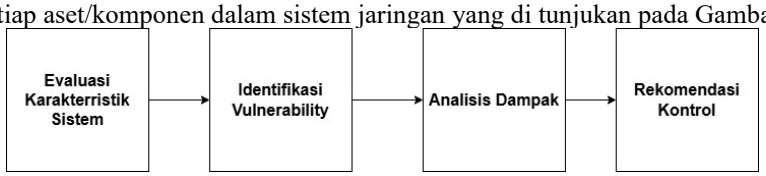
Dalam konteks organisasi yang bergantung pada layanan digital, evaluasi jaringan menjadi kebutuhan strategis untuk memastikan jaringan tetap andal dan aman. *Network Assessment* merupakan proses penilaian kondisi, performa, serta tingkat keamanan jaringan dengan tujuan menemukan potensi masalah dan menyusun rekomendasi perbaikan melalui tahapan inventarisasi aset, pemeriksaan konfigurasi, pengukuran kinerja, hingga analisis keamanan [3]. Namun, berdasarkan pengamatan awal dan wawancara informal dengan perwakilan tim IT Prama Sanur Beach Hotel, ditemukan indikasi bahwa aspek keamanan jaringan belum dikelola secara optimal. Beberapa perangkat belum diperbarui secara rutin, sebagian konfigurasi default masih dipertahankan, serta belum terdapat audit keamanan jaringan yang dilakukan secara berkala. Kondisi tersebut dapat meningkatkan peluang terjadinya insiden seperti penyusupan, pencurian data, maupun serangan terhadap layanan yang berdampak langsung pada operasional hotel.

Sebelumnya telah dilakukan beberapa penelitian terkait dengan topik saat penelitian penulis saat ini. Penelitian berjudul "Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website *Points of Sales*" berfokus pada sistem keamanan *website Points of Sales*[4] . Selanjutnya, penelitian berjudul "Analisis Celah Keamanan E-Learning Perguruan Tinggi Menggunakan *Vulnerability Assessment*" mendeteksi dan menganalisis kerentanan pada sistem E-Learning perguruan tinggi [5]. Penelitian lain dalam karya "*Website Security Analysis Using Vulnerability Assessment Method (Case Study*: Universitas Internasional Batam)" berfokus pada analisis kerentanan sistem *website* universitas[6]. Tidak seperti penelitian sebelumnya yang sebagian besar menitikberatkan pada pengujian keamanan website, penelitian ini difokuskan pada analisis kerentanan sejumlah aset jaringan internal yang dinilai paling vital sesuai rekomendasi pihak IT hotel.

Untuk menjawab permasalahan tersebut, penelitian ini mengajukan pendekatan *Vulnerability Assessment* guna memperoleh gambaran menyeluruh mengenai tingkat keamanan infrastruktur jaringan internal hotel. *Vulnerability Assessment* dipilih karena mampu mengidentifikasi aset dan komponen jaringan yang vital, melakukan pemindaian kerentanan, menganalisis tingkat risiko, serta menghasilkan rekomendasi perbaikan yang terukur . Implementasi dilakukan dengan mengombinasikan dua alat analisis yang saling melengkapi, yaitu Nmap dan Nessus. Nmap digunakan untuk memetakan *host* aktif, port terbuka, dan layanan yang berjalan sehingga memberikan gambaran struktur jaringan dan permukaan serangan (*attack surface*)[7], sedangkan Nessus digunakan untuk mendeteksi kerentanan berbasis basis data yang diperbarui secara berkala sehingga mampu mengidentifikasi potensi ancaman yang lebih spesifik[8]. Kombinasi keduanya diharapkan menghasilkan evaluasi yang lebih komprehensif, sekaligus meminimalkan risiko rekomendasi yang tidak sesuai dengan kondisi operasional hotel.

2. Metode Penelitian

Penelitian ini menerapkan metode vulnerability assessment yang dibagi ke dalam empat tahapan utama. Melalui pendekatan tersebut, dilakukan identifikasi sistematis terhadap celah kerentanan dan potensi ancaman pada setiap aset/komponen dalam sistem jaringan yang di tunjukan pada Gambar 1.



Gambar 1. Alur Vulnerability Assessment

Metode *Vulnerability Assessment* adalah proses penilaian keamanan yang bertujuan untuk menemukan dan mengevaluasi kelemahan (kerentanan) pada sistem teknologi informasi, seperti jaringan, server, aplikasi, maupun perangkat yang terhubung[9]. Melalui assessment ini, organisasi dapat mengetahui celah apa saja yang berpotensi dimanfaatkan penyerang, seberapa besar tingkat risikonya (misalnya dengan acuan skor CVSS), serta tindakan perbaikan yang perlu diprioritaskan. Umumnya, kegiatan ini dilakukan dengan menginventarisasi aset dan layanan yang berjalan, melakukan pemindaian menggunakan tools seperti Nmap dan Nessus, menganalisis hasil temuan berdasarkan tingkat keparahan dan dampaknya, lalu menyusun rekomendasi mitigasi seperti pembaruan sistem, penguatan konfigurasi, pembatasan akses, atau penonaktifan layanan yang tidak diperlukan[10]. Dengan demikian, *Vulnerability Assessment* membantu meningkatkan keamanan sistem secara terukur tanpa harus melakukan eksploitasi seperti pada penetration testing[11].

2.1 Evaluasi Karakteristik Sistem

Pada tahap ini dilakukan kajian pendahuluan terhadap kondisi jaringan di Gedung Departemen IT Prama Sanur Beach Hotel, mencakup inventarisasi dan penilaian terhadap infrastruktur yang digunakan, baik perangkat keras (*hardware*) maupun perangkat lunak (*software*).

2.2 Identifikasi Vulnerability

Tahap ini berfokus pada pemetaan dan penentuan kerentanan setelah gambaran ancaman diperoleh. Tujuannya adalah menemukan kelemahan yang terdapat pada lingkungan jaringan di Gedung Departemen IT Prama Sanur Beach Hotel agar dapat ditindaklanjuti pada tahap berikutnya.

2.3 Analisis Dampak (Impact Analysis)

Analisis dampak dilakukan untuk menilai konsekuensi apabila kerentanan yang ditemukan dieksploitasi. Penilaian mencakup aspek kerahasiaan, keutuhan, dan ketersediaan (CIA), serta pengaruhnya terhadap operasional, kepatuhan/hukum, reputasi, dan biaya. Setiap temuan kemudian dikategorikan (Rendah, Sedang, Tinggi, Sangat Tinggi) dan digabungkan dengan tingkat kemungkinan berdasarkan CVSS guna menentukan prioritas mitigasi dan waktu penanganan.

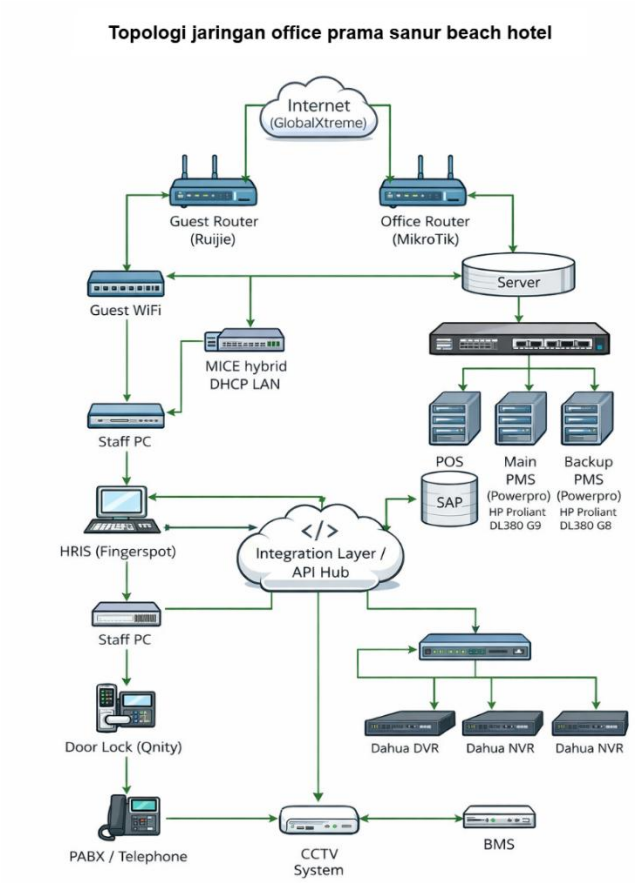
2.4 Rekomendasi Kontrol

Pada tahapan ini akan dibuatkan rekomendasi dari vulnerability system tersebut ditemukan dan Analisa dampak dari vulnerability telah didapatkan.

2.5 Topologi Prama Sanur Beach

Topologi jaringan pada Prama Sanur Beach menggunakan dua gateway utama yang terhubung ke Internet (GlobalXtreme), yaitu Guest Router (Ruijie) untuk jaringan tamu dan Office Router (MikroTik) untuk jaringan operasional hotel. Guest Router mendistribusikan koneksi ke Guest WiFi dan jaringan MICE hybrid DHCP LAN, sedangkan Office Router menghubungkan jaringan internal ke server serta sistem

utama hotel seperti POS (PowerPro), SAP, Main PMS, dan Backup PMS. Seluruh sistem aplikasi dan perangkat operasional diintegrasikan melalui Integration Layer/API Hub yang menghubungkan HRIS (Fingerspot) dengan layanan lain serta mendukung integrasi ke Door Lock, PABX/Telephone, CCTV (DVR/NVR Dahua), dan BMS. Struktur ini memungkinkan pemisahan akses tamu dan internal sekaligus memastikan layanan hotel terintegrasi dan dapat dipantau secara terpusat. Dapat dilihat pada Gambar 2.



Gambar 2. Topologi Jaringan Prama Sanur Beach

3. Hasil dan Pembahasan

3.1 Hasil Pemetaan Layanan (Nmap)

Pemindaian awal menggunakan Nmap dilakukan untuk memetakan host aktif serta port dan layanan yang terbuka pada aset jaringan kritikal. Ringkasan hasil pemetaan ditunjukkan pada Tabel 1. Secara umum, layanan berbasis Windows (RPC/SMB/RDP) dominan pada server dan DNS/Domain Controller, sedangkan pada PABX teridentifikasi layanan manajemen yang berisiko apabila tidak dibatasi (misalnya Telnet/FTP). Selain itu, host kanal/remote (Channel 1) hanya mengekspos satu layanan SSL pada *port* 7070 dan port lainnya terfilter.

Tabel 1. Ringkasan port terbuka dan layanan (hasil Nmap)

Host (IP)	Port terbuka	*Service*	Interpretasi singkat
Server (172.17.22.27)	135, 139, 445	MSRPC; NetBIOS-SSN; SMB	Layanan Windows RPC/SMB aktif (file sharing/remote service).
PowerPro (172.17.22.10)	135, 139, 445, 5985, 7070	MSRPC; NetBIOS-SSN; SMB; HTTPAPI; SSL service	Host aplikasi bisnis dengan layanan Windows/management dan layanan SSL pada 7070.

Host (IP)	Port terbuka	*Service*	Interpretasi singkat
DNS/DC (172.17.22.11)	53, 88, 135, 139, 389, 445, 464, 593, 636, 3268, 3269, 3389	DNS; Kerberos; RPC; SMB; LDAP/GC; RDP	Pola layanan konsisten dengan Domain Controller (AD) dan akses RDP.
PABX (172.17.22.250)	21, 23, 80, 443 (+514 terdeteksi)	FTP; Telnet; HTTP/HTTPS	Antarmuka manajemen/layanan komunikasi; Telnet/FTP berisiko jika tidak dibatasi.
Channel 1 (172.17.22.252)	7070	SSL service (indikasi AnyDesk)	Satu layanan SSL terbuka; port lain terfilter.

3.2 Hasil Vulnerability Assessment (Nessus)

Pemindaian kerentanan menggunakan Tenable Nessus *(Basic Network Scan)* menghasilkan temuan yang mayoritas bersifat informasional, namun terdapat beberapa temuan prioritas *(High/Medium)* yang relevan untuk mitigasi. Seluruh host pada pemindaian ini berstatus non-authenticated *(Auth: Fail)*, sehingga temuan lebih berfokus pada eksposur layanan dan konfigurasi yang dapat dinilai dari sisi jaringan[12] tabel 2. merangkum temuan prioritas beserta *port* terdampak, deskripsi masalah, dan solusi/mitigasi ringkas.

Temuan paling kritikal berada pada DNS/DC, yaitu dukungan cipher lemah (SWEET32/3DES) serta kelemahan konfigurasi TLS dan pengamanan RDP (NLA tidak dipaksakan). Pada sisi server aplikasi dan server umum, temuan dominan berupa konfigurasi SMB signing tidak diwajibkan, yang meningkatkan risiko manipulasi trafik SMB di jaringan internal. Pada PABX, temuan kunci terkait layanan manajemen tidak aman (Telnet tanpa enkripsi), potensi penyalahgunaan NTP Mode 6, serta konfigurasi IP *forwarding* yang perlu dikendalikan. Pada *Channel* 1, isu utama adalah sertifikat SSL yang tidak tepercaya/*self-signed* pada port 7070, sehingga identitas layanan sulit diverifikasi.

Tabel 2. Temuan prioritas hasil Nessus dan rekomendasi perbaikan

Host (IP)	Port terbuka	*Service*	Interpretasi singkat
Server (172.17.22.27)	SMB Signing not required (Medium/5.3)	445/tcp	SMB tidak mewajibkan message signing sehingga trafik SMB lebih rentan dimanipulasi (MITM) pada jaringan.
PowerPro (172.17.22.10)	SMB Signing not required (Medium/5.3)	445/tcp	Kebijakan SMB signing tidak diwajibkan pada host aplikasi, meningkatkan risiko manipulasi trafik SMB.
PowerPro (172.17.22.10)	SMB Protocol Version 1 Enabled (Info)	445/tcp	SMBv1 masih aktif (protokol legacy) dan umumnya tidak direkomendasikan karena risiko keamanan.
DNS/DC (172.17.22.11)	SWEET32 / 3DES supported (High/7.5)	3389/tcp	TLS masih mendukung cipher 3DES sehingga kekuatan enkripsi berkurang.
DNS/DC (172.17.22.11)	TLS 1.0 enabled (Medium)	3389/tcp	TLS 1.0 masih aktif (protokol lama, risiko lebih tinggi).
DNS/DC (172.17.22.11)	TLS 1.1 deprecated (Medium)	3389/tcp	TLS 1.1 masih aktif (sudah deprecated).
DNS/DC (172.17.22.11)	RC4 supported (Medium/5.9)	3389/tcp	Cipher RC4 masih didukung, padahal bersifat usang dan tidak aman.
DNS/DC (172.17.22.11)	SSL self-signed / untrusted cert (Medium/6.5)	3389/tcp	Sertifikat tidak tepercaya/self-signed sehingga identitas layanan sulit diverifikasi dan meningkatkan risiko MITM.
DNS/DC (172.17.22.11)	RDP not NLA-only (Medium/4.0)	3389/tcp	RDP tidak dipaksa NLA-only sehingga permukaan serangan RDP lebih terbuka.
PABX (172.17.22.250)	Unencrypted Telnet Server (Medium/6.5)	23/tcp	Telnet mengirim kredensial tanpa enkripsi sehingga mudah disadap.
PABX (172.17.22.250)	IP Forwarding Enabled (Medium/6.5)	N/A	Host dapat meneruskan paket (routing) sehingga berpotensi disalahgunakan jika tidak diperlukan.
PABX (172.17.22.250)	NTP Mode 6 Scanner (Medium/5.8)	123/udp	NTP merespons query Mode 6 yang berpotensi disalahgunakan (enumerasi/amplification).

Host (IP)	Port terbuka	*Service*	Interpretasi singkat
Channel 1 (172.17.22.252)	SSL cert cannot be trusted (Medium/6.5)	7070/tcp	Sertifikat tidak dipercaya sehingga verifikasi identitas layanan lemah.
Channel 1 (172.17.22.252)	SSL self-signed certificate (Medium/6.5)	7070/tcp	Sertifikat self-signed menyebabkan koneksi tidak dapat dipercaya tanpa trust manual.

Dalam penelitian ini, pemetaan kategori CVSS tersebut membantu menghubungkan hasil pemindaian dengan analisis dampak (CIA) untuk menetapkan urutan tindakan perbaikan yang realistis bagi operasional hotel tabel 3. tingkat keparahan digunakan untuk menerjemahkan skor CVSS v3.x (0–10) menjadi kategori risiko yang mudah dipahami dan dapat langsung dipakai untuk menentukan prioritas mitigasi. Skor *None* (0.0) menunjukkan tidak ada risiko terukur; *Low* (0.1–3.9) umumnya bersifat minor/informasional; *Medium* (4.0–6.9) perlu perbaikan terjadwal; *High* (7.0–8.9) berpotensi dieksploitasi sehingga butuh penanganan cepat; dan *Critical* (9.0–10.0) merupakan prioritas tertinggi karena dampaknya besar[13].

Tabel 3. Tingkat Keparahan

Tingkat Keparahan	Rentang Skor CVSS v3.x	Keterangan
None	0.0	Tidak ada dampak/risiko yang terukur.
Low	0.1 – 3.9	Risiko rendah; umumnya informasi/konfigurasi minor.
Medium	4.0 – 6.9	Risiko sedang; perlu perbaikan terjadwal/prioritas menengah.
High	7.0 – 8.9	Risiko tinggi; berpotensi dieksploitasi, perlu penanganan cepat.
Critical	9.0 – 10.0	Risiko sangat tinggi; dampak besar, prioritas penanganan paling tinggi.

3.3 Rekapitulasi Nessus

Rekapitulasi Nessus menunjukkan komposisi temuan didominasi *Medium* (13), disusul *Low* (2), *High* (1), dan tidak ada *Critical* (0). Artinya, kondisi keamanan jaringan relatif tidak berada pada fase "darurat ekstrem" (karena tidak ada *Critical*), tetapi terdapat satu isu berisiko tinggi yang perlu diprioritaskan (SWEET32/3DES pada DNS/DC), serta banyak isu konfigurasi tingkat menengah yang jika dibiarkan dapat menjadi pintu masuk serangan. Dari sisi sebaran host, DNS/DC menanggung beban temuan paling serius (High + beberapa Medium TLS/RDP), PABX memiliki beberapa Medium terkait layanan/konfigurasi jaringan (Telnet, NTP Mode 6, IP forwarding), sementara Server Hotel dan PowerPro menonjol pada isu SMB signing; *Channel* 1 didominasi isu sertifikat SSL. Karena pemindaian Nessus pada dokumen tercatat non-authenticated (*Auth: Fail*), hasil lebih banyak merefleksikan eksposur layanan dan konfigurasi yang terlihat dari jaringan; *scan* kredensial akan membuat identifikasi *patch*/konfigurasi internal lebih presisi.

Tabel 4. Hasil Temuan Rekapitulasi Nessus

Severity	Jumlah Temuan (minimum)
Critical	0
High	1
Medium	13
Low	2

4. Kesimpulan

Adapun kesimpulan berdasarkan *network assessment* di Departemen IT Prama Sanur Beach Hotel menggunakan Nmap untuk pemetaan host/port/layanan dan Nessus untuk identifikasi kerentanan berbasis CVSS, ditemukan bahwa permukaan layanan jaringan masih cukup terbuka pada beberapa aset kritikal (mis. SMB/RDP pada server Windows dan layanan manajemen pada PABX). Hasil Nessus memperlihatkan 0 *Critical*, 1 *High*, 13 *Medium*, dan 2 *Low*, dengan temuan prioritas tertinggi berada pada DNS/DC terkait dukungan cipher lemah (SWEET32/3DES) serta isu konfigurasi TLS/RDP, sementara temuan *medium* dominan berupa SMB signing yang tidak diwajibkan, sertifikat SSL yang tidak tepercaya/*self-signed*, Telnet tanpa enkripsi, NTP Mode 6, dan IP *forwarding*. Secara umum, temuan menunjukkan kebutuhan utama bukan sekadar menutup port, melainkan hardening konfigurasi layanan dan pembatasan akses administratif agar layanan yang memang dibutuhkan tetap aman dan terkendali. Penelitian ini masih memiliki beberapa keterbatasan. Pertama, pemindaian Nessus yang digunakan bersifat *network-based* dan

pada laporan tercatat *non-authenticated* (*credentialed scan* belum dilakukan), sehingga identifikasi patch level, konfigurasi internal host, serta akurasi beberapa temuan bisa kurang presisi (berpotensi *false positive/false negative*).

Daftar Pustaka

[1] T. Fernandes, J. P. Magalhães, and W. Alves, "Cybersecurity in Smart Railways: Exploring risks, vulnerabilities and mitigation in the data communication services," *Green Energy and Intelligent Transportation*, vol. 4, no. 4, p. 100305, Aug. 2025, doi: 10.1016/j.geits.2025.100305.

[2] S. Abdelkader *et al.*, "Securing modern power systems: Implementing comprehensive strategies to enhance resilience and reliability against cyber-attacks," *Results in Engineering*, vol. 23, p. 102647, Sep. 2024, doi: 10.1016/j.rineng.2024.102647.

[3] Y. Yu, "A network security situation assessment method based on fusion model," *Discover Applied Sciences*, vol. 6, no. 3, p. 97, Feb. 2024, doi: 10.1007/s42452-024-05723-6.

[4] Wahyudin, H. Kuswara, Resti, and S. Dalis, "Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales," *Computer Science (CO-SCIENCE)*, Jan. 2024.

[5] A. Rohim and L. Setiyani, "View of Analisis Celah Keamanan E-Learning Perguruan Tinggi Menggunakan Vulnerability Assessment," *Jurnal Inovasi Pengembangan Aplikasi dan kemanan Informasi Nusantara*, 2023.

[6] Haeruddin, Gautama Wijaya, H. Winata, Sukma Aji, and Muhammad Nur Faiz, "Website Security Analysis Using Vulnerability Assessment Method," *Journal of Innovation Information Technology and Application (JINITA)*, vol. 6, no. 2, pp. 173–180, Dec. 2024, doi: 10.35970/jinita.v6i2.2476.

[7] R. Liu, "Nmap network scan performance optimisation," in *Fourth International Conference on Signal Processing and Computer Science (SPCS 2023)*, H. Kolivand and A. Nayyar, Eds., SPIE, Dec. 2023, p. 200. doi: 10.1117/12.3012568.

[8] Dd Hassel Putra Q, Ilham Ammarul Aziz, Eginna Gresia Br Purba, Dewa Made Wiharta, and I Gusti Ayu Garnita Darmaputri, "Evaluasi Celah Keamanan dengan Metodologi Vulnerability Assessment Sebagai Penilaian Tingkat Kerentanan pada Domain Unud.Ac.Id," *JURAL RISET RUMPUN ILMU TEKNIK*, vol. 4, no. 1, pp. 422–447, Apr. 2025, doi: 10.55606/jurritek.v4i1.5004.

[9] S. Pan, L. Bao, J. Zhou, X. Hu, X. Xia, and S. Li, "Towards More Practical Automation of Vulnerability Assessment," in *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, New York, NY, USA: ACM, Apr. 2024, pp. 1–13. doi: 10.1145/3597503.3639110.

[10] A. M. Sllame, T. E. Tomia, and R. M. Rahuma, "A Holistic Approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb," in *2024 IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA)*, IEEE, May 2024, pp. 68–75. doi: 10.1109/MI-STA61267.2024.10599685.

[11] A. Dabit, Q. A. Al-Haija, and M. Al-Fayoumi, "Identifying Weaknesses: A Guide to Conducting an Effective Network Vulnerability Assessment," in *2023 24th International Arab Conference on Information Technology (ACIT)*, IEEE, Dec. 2023, pp. 1–6. doi: 10.1109/ACIT58888.2023.10453877.

[12] Muhammad Risky Ardiansyah *et al.*, "Analisis Kerentanan Keamanan Website Menggunakan Metode PTES (Penetration Testing Execution And Standart)," *NUANSA INFORMATIKA*, vol. 18, no. 2, pp. 145–153, Jul. 2024, doi: 10.25134/ilkom.v18i2.119.

[13] A. Balsam, M. Nowak, M. Walkowski, J. Oko, and S. Sujecki, "Comprehensive comparison between versions CVSS v2.0, CVSS v3.x and CVSS v4.0 as vulnerability severity measures," in *2024 24th International Conference on Transparent Optical Networks (ICTON)*, IEEE, Jul. 2024, pp. 1–4. doi: 10.1109/ICTON62926.2024.10647452.