Journal of Information Technology and Computer Science (INTECOMS)
Volume 9 Nomor 1, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

ANALISIS KEAMANAN JARINGAN WIFI DAN CCTV MENGGUNAKAN ZENMAP SEBAGAI NETWORK VULNERABILITY SCANNER

WIFI AND CCTV NETWORK SECURITY ANALYSIS USING ZENMAP NETWORK VULNERABILITY SCANNER AS A

Helena Dorthea Fiay[1], Magdalena A. Ineke Pakereng M[2]
Universitas Kristen Satya Wacana[1,2]
6720219271@student.uksw.edu[1]

ABSTRACT

This study analyzes the security of WiFi networks and IP-based CCTV systems using Zenmap as the graphical interface of Nmap. The research is motivated by the increasing adoption of Internet of Things (IoT) devices, which often suffer from weak security configurations such as default passwords, outdated firmware, and insufficient encryption. By applying vulnerability assessment methods, the study conducted network scanning to identify active hosts, open ports, running services, and potential vulnerabilities in WiFi and CCTV devices at S-Code Programming Studio, Salatiga. The scanning results revealed several exposed ports and services that could be exploited by unauthorized parties. The analysis was carried out using a descriptive-qualitative approach, assessing risk levels and providing mitigation recommendations including firmware updates, replacement of default credentials, WPA3 implementation, and network segmentation. This research is expected to serve as a practical reference for network administrators and organizations in strengthening IoT-based infrastructure security.

Keywords*: Network Security, WiFi, CCTV/IP Camera, Zenmap / Nmap, Vulnerability Assessment*

ABSTRAK

Penelitian ini membahas analisis keamanan jaringan WiFi dan sistem CCTV berbasis IP dengan memanfaatkan Zenmap sebagai antarmuka grafis dari Nmap. Latar belakang penelitian berangkat dari meningkatnya penggunaan perangkat Internet of Things (IoT) yang sering kali memiliki konfigurasi keamanan lemah, seperti penggunaan kata sandi bawaan, enkripsi rendah, serta firmware yang tidak diperbarui. Melalui metode vulnerability assessment, penelitian ini melakukan pemindaian jaringan untuk mengidentifikasi host aktif, port terbuka, layanan yang berjalan, serta potensi kerentanan pada perangkat WiFi dan CCTV di Studio Pemrograman S-Code Salatiga. Hasil pemindaian menunjukkan adanya port berisiko yang terbuka serta layanan yang rentan terhadap eksploitasi. Analisis dilakukan secara deskriptif- kualitatif dengan menilai tingkat risiko dan memberikan rekomendasi mitigasi, seperti pembaruan firmware, penggantian kredensial default, penerapan WPA3, serta segmentasi jaringan. Penelitian ini diharapkan dapat menjadi acuan praktis bagi administrator jaringan maupun organisasi lain dalam meningkatkan keamanan infrastruktur berbasis IoT.

Kata Kunci: Keamanan Jaringan, WiFi, CCTV/IP Camera, Zenmap / Nmap, Vulnerability Assessment

PENDAHULUAN

Di era digital saat ini, kebutuhan akan konektivitas internet telah menjadi aspek yang tidak terpisahkan dari aktivitas individu, organisasi, maupun industri, terutama dengan semakin meluasnya penggunaan Internet of Things (IoT) yang mendorong hadirnya berbagai perangkat pintar seperti jaringan nirkabel (WiFi) dan sistem pengawasan berbasis IP (CCTV/IP Camera). WiFi memberikan fleksibilitas dalam akses jaringan, sementara kamera IP memungkinkan pemantauan keamanan secara real-time dari jarak jauh; kedua teknologi ini bekerja dalam ekosistem IoT yang memungkinkan perangkat saling terhubung untuk bertukar data dan berinteraksi, sehingga menciptakan efisiensi pada berbagai aspek manajemen dan pengawasan keamanan (Olaniyi et al., 2023). Namun, kemudahan tersebut juga dibarengi meningkatnya ancaman keamanan jaringan karena banyak pengguna atau administrator masih mengabaikan konfigurasi keamanan dasar seperti penggunaan kata sandi bawaan pabrik, enkripsi yang lemah seperti WPA2-PSK sederhana, serta pembaruan firmware

yang jarang dilakukan, sehingga membuka celah bagi serangan seperti botnet Mirai yang diketahui memanfaatkan perangkat dengan kredensial default (Ryan & Rozier, 2024). Martinez et al. Farraj & Hammad (2024) turut menegaskan bahwa kerentanan pada perangkat IoT sangat signifikan karena lemahnya penerapan kontrol keamanan yang mestinya menjadi standar, terutama terkait penggunaan password yang kuat dan unik. Dalam kondisi seperti itu, jaringan menjadi sangat rentan terhadap teknik serangan seperti packet sniffing, dictionary attack, maupun Man-in-the-Middle (MITM) yang dapat mengakibatkan penyadapan dan manipulasi data sensitif yang dikirimkan melalui WiFi. Risiko serupa bahkan lebih tinggi pada sistem CCTV berbasis IP yang sering kali menggunakan konfigurasi keamanan lemah, sehingga menjadi sasaran mudah bagi penyerang untuk mendapatkan akses tidak sah; kamera IP sendiri kerap mengandung banyak celah yang dapat dieksploitasi melalui pemindaian jaringan, termasuk kelemahan pada protokol RTSP maupun ONVIF yang memungkinkan pengambilalihan kendali perangkat (Zhao et al., 2023), yang pada akhirnya bukan hanya mengancam privasi tetapi juga membahayakan keamanan fisik individu maupun aset organisasi (Hamada & Kuzminykh, 2023). Situasi tersebut menunjukkan pentingnya pendekatan proaktif dalam menjaga keamanan jaringan melalui penilaian kerentanan (vulnerability assessment), yaitu proses terstruktur untuk mengidentifikasi, menganalisis, dan memprioritaskan risiko pada aset informasi sehingga dapat dirumuskan strategi mitigasi yang tepat (Bellamkonda, 2022). Salah satu perangkat yang sering digunakan dalam audit keamanan jaringan adalah Nmap dengan antarmuka grafis resminya, Zenmap, yang membantu proses pemindaian untuk mengetahui host aktif, port terbuka, layanan berjalan, serta mendeteksi potensi celah keamanan melalui pemanfaatan Nmap Scripting Engine (NSE) (Heverin et al., 2023). Berangkat dari kondisi tersebut, penelitian ini dilakukan untuk menganalisis tingkat keamanan jaringan WiFi dan sistem CCTV yang terhubung di Studio Pemrograman S-Code Salatiga dengan memanfaatkan Zenmap, guna memperoleh gambaran nyata mengenai postur keamanan jaringan dan memberikan rekomendasi mitigasi yang relevan. Penelitian ini memfokuskan diri pada identifikasi host aktif, port terbuka, serta layanan yang berjalan pada perangkat WiFi dan CCTV, mengungkap kerentanan konfigurasi jaringan seperti protokol enkripsi, default credentials, dan firmware usang; serta merumuskan rekomendasi keamanan berdasarkan hasil pemindaian. Tujuan penelitian ini mencakup pemetaan perangkat aktif dalam jaringan mulai dari access pointWiFi, router Palapa Net, hingga perangkat CCTV/IP Camera analisis kerentanan berdasarkan hasil pemindaian Zenmap, identifikasi titik rawan serangan yang dapat dimanfaatkan pihak tidak berwenang, serta pemberian rekomendasi teknis untuk memperkuat keamanan jaringan. Secara teoretis, penelitian ini berkontribusi pada pengembangan literatur di bidang keamanan siber praktis, khususnya terkait metodologi penilaian kerentanan pada perangkat IoT serta pemanfaatan tools open-source seperti Zenmap dalam audit keamanan jaringan; sedangkan secara praktis penelitian ini memberikan manfaat bagi S-Code Studio Salatiga dalam meningkatkan keamanan konfigurasi WiFi dan CCTV, membantu administrator jaringan dalam melakukan evaluasi keamanan melalui laporan audit, menjadi rujukan bagi industri atau organisasi lain dengan infrastruktur serupa, dan menambah wawasan praktisi maupun akademisi terkait penerapan Zenmap dalam pemindaian kerentanan jaringan. Ruang lingkup penelitian dibatasi pada pemanfaatan Zenmap sebagai antarmuka grafis Nmap dengan fokus pada aktivitas vulnerability assessment tanpa melakukan penetration testing atau eksploitasi aktif, objek penelitian terbatas pada jaringan

WiFi Studio 1 Pemrograman S-Code dan perangkat CCTV berbasis IP yang terhubung di dalamnya, termasuk access pointatau router Palapa Net serta kamera IP yang diasumsikan berfungsi normal selama pengujian; dan analisis hanya mencakup konfigurasi jaringan serta layanan yang terdeteksi melalui pemindaian port tanpa menyentuh aspek keamanan fisik perangkat. Seluruh proses pemindaian dilakukan dengan izin eksplisit dari pengelola jaringan dalam rentang waktu maksimal 14 hari agar tidak mengganggu operasional sistem yang sedang berjalan.

Keamanan jaringan merupakan serangkaian upaya untuk melindungi integritas, kerahasiaan, dan ketersediaan data pada sistem jaringan komputer (CIA Triad). Tujuan utama dari keamanan jaringan adalah mencegah akses tidak sah, modifikasi, ataupun perusakan data dan sumber daya jaringan. Pendekatan keamanan melibatkan kombinasi kebijakan, konfigurasi perangkat keras maupun perangkat lunak, serta penerapan kontrol akses dan enkripsi yang tepat. Proses penguatan sistem dan kebijakan autentikasi yang kuat adalah salah satu cara untuk meningkatkan keamanan jaringan. Berbagai jenis autentikasi dapat meningkatkan keamanan dan manajemen operasional jaringan, menurut Datta et al. (Datta et al., 2023). Selain itu, Satria menunjukkan bahwa pengembangan solusi jaringan yang inovatif dan efisien juga perlu didukung oleh pemahaman yang mendalam tentang kinerja dan keamanan jaringan modern (Satria, 2024). Wireless Local Area Network (WLAN) menggunakan gelombang radio berdasarkan standar IEEE 802.11 untuk menghubungkan perangkat tanpa kabel. Keamanan WiFi telah berkembang dari WEP (Wired Equivalent Privacy) yang lemah, menuju WPA dan WPA2, hingga versi terbaru WPA3 yang lebih aman. Namun, jaringan WiFi tetap rentan terhadap serangan seperti packet sniffing, deauthentication attack, brute force, dan dictionary attack, terutama jika menggunakan passphrase lemah. Studi menunjukkan bahwa WPA2-PSK masih dapat diretas menggunakan alat seperti Aircrack-ng bila kata sandi tidak kuat (Abdallah et al., 2023). Oleh karena itu, penggunaan WPA3 dan penerapan audit keamanan jaringan secara berkala menjadi langkah penting untuk mencegah eksploitasi. Sistem CCTV modern berbasis Internet Protocol (IP) memungkinkan akses video secara real-time melalui jaringan. Berbagai fitur canggih, seperti analisis video dan deteksi perilaku mencurigakan, termasuk dalam sistem CCTV berbasis IP. Studi Sonavane et al. (2025) menemukan bahwa algoritma berbasis kecerdasan buatan yang digunakan oleh CCTV kontemporer dapat mendeteksi aktivitas kriminal dan anomali dalam waktu nyata. Algoritma ini mencakup deteksi objek, analisis gerakan, dan pengenalan wajah, dan bertujuan untuk meningkatkan kemampuan sistem untuk mencegah kejahatan. Kamera IP menggunakan protokol umum seperti RTSP untuk streaming dan ONVIF untuk konfigurasi perangkat. Namun, penggunaan protokol terbuka ini juga membuka peluang serangan. Kerentanan umum pada CCTV meliputi penggunaan kredensial default (seperti admin/admin) yang mudah ditebak, Port terbuka seperti HTTP (80), HTTPS (443), dan RTSP (554) yang terekspos ke jaringan public, Firmware yang tidak diperbarui, sehingga mengandung celah keamanan (CVE) yang dapat dieksploitasi. Analisis port scanning menggunakan Nmap dapat membantu mengidentifikasi layanan yang berjalan dan menilai potensi kerentanan pada perangkat kamera. Vulnerability Assessment merupakan proses sistematis untuk mengidentifikasi, mengukur, dan memprioritaskan kerentanan dalam suatu sistem jaringan. Hasil penilaian kelemahan membantu organisasi mengambil tindakan yang tepat untuk meningkatkan keamanan dan melindungi sistem mereka dari ancaman (Muharrom & Saktiansyah, 2023). Dengan menggunakan pendekatan sistematis,

organisasi dapat meningkatkan keamanan dan melindungi sistem mereka dari ancaman yang mungkin terjadi. Tujuannya adalah memberikan 2 pemahaman tentang kelemahan keamanan yang ada sebelum dieksploitasi oleh pihak tidak berwenang. Hasil VA digunakan sebagai dasar dalam perencanaan mitigasi atau perbaikan sistem keamanan. Zenmap merupakan antarmuka grafis resmi dari Nmap yang memudahkan pengguna, baik pemula maupun profesional, dalam melakukan pemindaian dan analisis jaringan. Zenmap menyediakan fitur penyimpanan profil pemindaian, perbandingan hasil, serta visualisasi topologi jaringan secara grafis. Keunggulan utama Zenmap adalah kemudahan penggunaan dan dokumentasi hasil yang lebih terstruktur, menjadikannya alat yang efektif untuk melakukan penilaian keamanan jaringan. Penggunaan Zenmap sebagai bagian dari tahap analisis dan pelaporan penilaian kerentanan dapat menghasilkan dokumentasi yang lebih sistematis dan terorganisir dan meningkatkan pemahaman pengguna tentang hasil pemindaian (Priambodo et al., 2023). Berbagai penelitian telah dilakukan terkait keamanan jaringan, pemindaian kerentanan, serta keamanan perangkat IoT. Penelitian sebelumnya melakukan audit keamanan jaringan di institusi pendidikan menggunakan Nmap. Hasil penelitian menunjukkan banyak port server internal yang terbuka karena kurangnya konfigurasi firewall yang tepat, meskipun fokus penelitian masih pada server, bukan perangkat IoT (Pidlisnyi, 2025). Patel dan Gupta (2023) menganalisis keamanan perangkat IoT di lingkungan smart home dan menemukan bahwa sekitar 80% perangkat, termasuk IP Camera, rentan terhadap serangan karena penggunaan kredensial bawaan. Namun, penelitian ini tidak berfokus pada penggunaan Zenmap sebagai alat analisis utama. Putra (2023) meneliti kelemahan protokol WPA2-PSK pada jaringan WiFi publik. Dengan menggunakan teknik packet sniffing dan dictionary attack, penelitian ini membuktikan bahwa kunci WPA2 dapat diretas jika passphrase yang digunakan lemah. Lee dkk. (2024) membandingkan performa beberapa alat pemindai kerentanan open-source seperti Nmap, OpenVAS, dan Nessus Essentials. Hasilnya menunjukkan bahwa Nmap memiliki keunggulan dari segi kecepatan dan akurasi dalam mendeteksi layanan. Cybersecurity Research Group (2024) melaporkan peningkatan serangan botnet (seperti Mirai) yang menargetkan port Telnet dan SSH pada perangkat IoT, termasuk NVR/DVR CCTV, menegaskan perlunya pemindaian proaktif terhadap port berisiko tinggi. Rahman dkk. (2025) mensimulasikan serangan port scanning di jaringan WiFi lokal menggunakan Nmap/Zenmap dan memonitor hasilnya menggunakan Wireshark serta Snort. Hasilnya menunjukkan bahwa aktivitas pemindaian dapat terdeteksi dan dimitigasi dengan konfigurasi IDS yang tepat. Alghamdi dkk. (2022) melakukan studi komparatif terhadap berbagai tool pemindai keamanan seperti Nmap, Zenmap, Nessus, dan OpenVAS. Mereka menyimpulkan bahwa Zenmap unggul dalam kemudahan penggunaan, dokumentasi hasil, serta kemampuan visualisasi topologi jaringan secara grafis. Penelitian-penelitian tersebut menunjukkan bahwa penggunaan alat pemindaian open- source seperti Nmap dan Zenmap sangat efektif untuk mengidentifikasi kerentanan jaringan. Namun, sebagian besar penelitian sebelumnya hanya berfokus pada satu jenis perangkat atau infrastruktur tertentu. Penelitian ini dilakukan untuk mengisi celah tersebut dengan menggabungkan dua komponen penting sekaligus WiFi dan CCTV dalam satu kerangka analisis terpadu menggunakan Zenmap. Dengan demikian, penelitian ini menawarkan pendekatan yang lebih aplikatif, terstruktur, dan dapat direplikasi oleh administrator jaringan dalam konteks nyata.

METODE

Gambar 1. Tahapan Penelitian
Sumber : sumber pribadi menggunakan draw io

1. Jenis Penelitian dan Pendekatan

Penelitian ini bersifat eksperimental-deskriptif dengan pendekatan studi kasus. Secara eksperimental dilakukan aktivitas vulnerability scanning (pemindaian kerentanan) pada infrastruktur jaringan nyata, sementara pendekatan deskriptif-kualitatif digunakan untuk menggambarkan dan menganalisis temuan secara sistematis dalam konteks lokasi penelitian.

2. Lokasi, Waktu, dan Izin

Lokasi penelitian di Studio Pemrograman S-Code Salatiga, dengan fokus pada segmen jaringan WiFi yang dikelola oleh router penyedia layanan Palapa Net serta perangkat CCTV/IP Camera yang terhubung. Waktu: Pelaksanaan penelitian dilakukan pada periode yang telah disepakati dengan pihak pengelola (jadwal lapangan dicatat dalam lampiran). Izin: Semua kegiatan pemindaian dilaksanakan setelah memperoleh izin tertulis dari manajemen/penanggung jawab jaringan untuk memastikan kepatuhan terhadap etika dan operasional.

3. Objek Penelitian

Objek penelitian mencakup: Perangkat keras: access point/router WiFi (Palapa Net), IP Camera, dan/atau NVR/DVR yang berada dalam satu segmen jaringan studi kasus. Perangkat lunak: Zenmap (GUI Nmap) dan skrip Nmap Scripting Engine (NSE) yang digunakan untuk pemindaian serta (opsional) alat verifikasi lalu lintas seperti Wireshark/Snort.

4. Alat dan Bahan

Penelitian yang dilakukan membutuhkan Workstation (laptop/PC) dengan sistem operasi Windows dan instalasi Zenmap, koneksi ke jaringan target (akses fisik/on-site) dan dokumen konfigurasi awal yang diizinkan pihak pengelola (SSID, jenis enkripsi, firmware router, dsb.), perlengkapan dokumentasi: notasi lapangan, catatan wawancara, dan media penyimpanan hasil pemindaian.

5. Prosedur Pengumpulan Data

Penelitian ini dilaksanakan melalui alur kerja terstruktur yang memprioritaskan etika dan minimalisasi gangguan operasional, diawali dengan tahap persiapan yang mencakup studi literatur, pengurusan izin resmi, serta instalasi workstation, diikuti dokumentasi awal terhadap konfigurasi jaringan dan inventarisasi perangkat fisik. Proses teknis berlanjut ke identifikasi jaringan (network discovery) untuk memetakan IP aktif, yang kemudian diperdalam melalui pemindaian kerentanan (vulnerability scanning) intensif menggunakan konfigurasi dan skrip khusus guna mendeteksi status port serta layanan. Validitas data dipastikan melalui tahap verifikasi menggunakan analisis lalu lintas jaringan atau uji silang non-eksploitasi, sebelum akhirnya seluruh temuan dan log dikonsolidasikan ke dalam dokumentasi hasil yang komprehensif untuk keperluan analisis lebih lanjut.

6. Teknik Analisis Data

Analisis dalam penelitian ini dilakukan dengan pendekatan deskriptif-kualitatif melalui rangkaian langkah yang terstruktur. Tahap awal mencakup identifikasi dan 4 klasifikasi seluruh temuan guna mengelompokkannya ke dalam jenis kerentanan yang relevan, seperti penggunaan kredensial bawaan, kesalahan konfigurasi layanan, keterbukaan port yang tidak perlu, ataupun pemanfaatan firmware usang. Selanjutnya, setiap temuan dinilai tingkat risikonya kritis, tinggi, sedang, atau rendah berdasarkan potensi dampaknya terhadap aspek kerahasiaan,

integritas, dan ketersediaan; bila data memungkinkan, penilaian tersebut turut dipetakan ke skor CVSS untuk memperoleh gambaran objektif mengenai tingkat keparahan. Tahap berikutnya berfokus pada analisis akar masalah dengan menelaah faktor penyebab munculnya kerentanan, baik yang bersumber dari konfigurasi sistem, kebijakan pembaruan, maupun kelemahan prosedural dalam pengelolaan perangkat. Pada tahap akhir, seluruh temuan disintesiskan menjadi rekomendasi yang dapat ditindaklanjuti, mencakup langkah teknis maupun prosedural, seperti menonaktifkan protokol yang tidak aman (misalnya Telnet), memperbarui firmware, mengganti kredensial bawaan, mengaktifkan WPA3 atau menerapkan passphrase yang kuat, melakukan segmentasi jaringan, serta mengimplementasikan mekanisme pemantauan atau IDS untuk meningkatkan kesiapan deteksi dan respons.

7. Etika Penelitian dan Batasan Operasional

Seluruh kegiatan pemindaian dilakukan secara terkendali pada jaringan dan perangkat yang telah memperoleh izin eksplisit, tanpa upaya eksploitasi maupun pengambilan kredensial nyata. Pelaksanaannya dijadwalkan pada waktu yang tidak mengganggu operasional, sesuai kesepakatan dengan pihak terkait. Temuan pemindaian dilaporkan hanya kepada pihak berwenang dan disimpan dengan mekanisme pengamanan yang memadai. Penelitian ini dibatasi pada aktivitas vulnerability assessment menggunakan Zenmap/NSE tanpa melakukan penetration testing yang bersifat agresif, tidak mencakup jaringan di luar ruang lingkup studi, serta tidak menilai aspek keamanan fisik perangkat.

8. Output yang Diharapkan

Luaran dari penelitian ini disajikan dalam bentuk laporan audit komprehensif yang memuat peta topologi perangkat, rincian port terbuka beserta layanannya, serta klasifikasi kerentanan berbasis risiko yang disertai rekomendasi mitigasi teknis maupun kebijakan. Laporan tersebut diperkuat oleh lampiran data teknis berupa file log hasil pemindaian dalam format terstruktur (XML/gnmap/normal), yang berfungsi sebagai bukti dokumentasi otentik guna memfasilitasi proses verifikasi dan replikasi temuan di masa mendatang.

HASIL DAN PEMBAHASAN

1. Instalasi dan Konfigurasi Zenmap

Zenmap dapat diunduh dan diinstal di berbagai sistem operasi utama. Situs resmi Nmap menyertakan paket instalasi Zenmap (yang seringkali dibundel dengan Nmap) dalam format biner untuk Linux (RPM), Windows (installer NSIS), dan macOS (.dmg). Pengguna Windows dapat menjalankan installer grafis untuk menginstal Zenmap, sedangkan pada Linux dapat menggunakan manajer paket (misalnya apt atau yum) sesuai distribusi. Beberapa distribusi Linux security (misalnya Kali Linux) bahkan telah menyertakan Zenmap secara default. Setelah instalasi, Zenmap siap digunakan melalui antarmuka grafis, cukup jalankan aplikasi Zenmap dan pastikan koneksi jaringan komputer berfungsi normal. Inventarisasi awal dilakukan untuk mengetahui kondisi jaringan sebelum pemindaian.

Tabel 1. Baseline Configuration

Perangkat	Jumlah	IP/Subnet	Enkripsi	Catatan
Router/AP	1	192.167.1.1	WPA2-PSK	Sertifikat HTTPS self-signed
IP Camera	2	192.168.1.10–192.168.1.12	HTTP	Salah satu membuka Telnet
Pengguna	2	DHCP	-	Laptop/PC
Subnet	-	192.168.1.0/24	-	Single segment

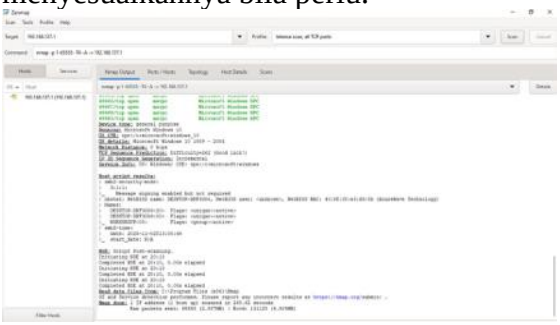
Sumber : data hasil observasi pribadi

2. Profil dan Metode Pemindaian

Zenmap menyediakan berbagai profil pemindaian bawaan yang memudahkan proses audit jaringan. Pengguna dapat memilih profil ini dari menu Profile, atau memasukkan perintah Nmap kustom. Beberapa profil utama di antaranya:

- Intense Scan (nmap -T4 -A -v): melakukan pemindaian port TCP umum (1.000 port teratas) dengan deteksi OS dan versi layanan secara agresif.
- Intense Scan, all TCP Ports (nmap -p1-65535 -T4 -A -v): sama seperti Intense Scan namun meliputi seluruh port TCP (1–65535).
- Intense Scan, no ping (nmap -T4 -A -v -Pn): melakukan Intense Scan tanpa ping (berguna jika host tidak merespons ping).
- Ping Scan (nmap -sn): hanya mendeteksi host aktif (ping sweep) tanpa memeriksa port.
- Quick Scan (nmap -T4 -F): memindai 100 port TCP teratas untuk proses yang lebih cepat.
- Quick Scan Plus (nmap -sV -T4 -O -F --version-light): seperti Quick Scan namun juga mendeteksi versi layanan dan sistem operasi.
- Quick Traceroute (nmap -sn --traceroute): mem-ping target dan menunjukkan jalur jaringan (traceroute).
- Regular Scan (nmap <target>): pemindaian default (SYN scan pada port umum).

Setelah memilih profil, antarmuka Zenmap secara otomatis menampilkan perintah Nmap lengkap yang akan dijalankan. Hal ini memudahkan pengguna memahami opsi yang digunakan dan menyesuaikannya bila perlu.



Gambar 2. Layar tab Nmap Output Zenmap yang menampilkan hasil pemindaian jaringan

Sumber : sumber pribadi

Penelitian ini menunjukkan bahwa pemindaian jaringan WiFi dan CCTV menggunakan Zenmap dapat mengungkap kerentanan-kerentanan penting. Zenmap sebagai antarmuka Nmap mempermudah proses pemindaian melalui profil bawaan dan tampilan grafis yang informatif. Hasil pemindaian mengidentifikasi perangkat aktif, port terbuka, dan layanan yang berjalan, sehingga memudahkan peneliti mengetahui titik rawan (misalnya layanan HTTP/Telnet aktif pada kamera CCTV). Temuan ini konsisten dengan

3. Pelaksanaan Pemindaian Jaringan

Pelaksanaan pemindaian menggunakan Zenmap terdiri dari langkah-langkah sebagai berikut:

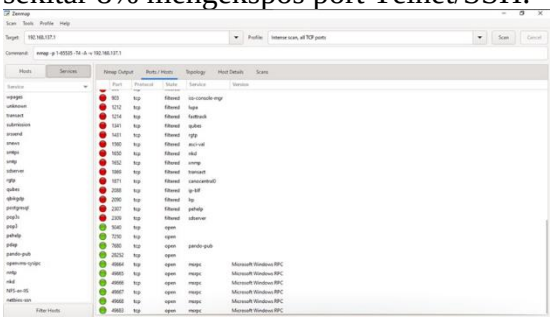
- Menjalankan Zenmap. Buka aplikasi Zenmap melalui menu program atau terminal.
- Memasukkan target. Ketik alamat IP atau rentang jaringan yang akan dipindai pada kolom Target. Zenmap mendukung spesifikasi subnet seperti 192.168.1.0/24 ataupun rentang dengan wildcard (misalnya 10.0.0-5.).
- Memilih profil scan. Dari menu Profile, pilih profil pemindaian yang diinginkan (misalnya Intense Scan atau Quick Scan).
- Menjalankan pemindaian. Klik tombol Scan untuk memulai proses. Zenmap kemudian menjalankan Nmap sesuai profil yang dipilih. Hasil keluaran Nmap (daftar host dan port) ditampilkan pada tab Nmap Output segera setelah pemindaian selesai.

Dalam konteks studi kasus, pemindaian dimulai dengan identifikasi perangkat aktif (Ping Scan) untuk memetakan host dalam jaringan WiFi dan jaringan CCTV. Selanjutnya dilakukan pemindaian mendalam (misalnya dengan Intense Scan) untuk menentukan port terbuka, layanan yang berjalan, serta sistem operasi. Hasil pemindaian kemudian disimpan (misalnya dalam format XML) dan digunakan untuk analisis kerentanan lebih lanjut

4. Temuan Pemindaian Jaringan

Analisis hasil pemindaian mengungkap beberapa perangkat aktif

dalam jaringan WiFi dan CCTV. Misalnya, ditemukan sebuah Access pointWiFi (IP 192.168.1.1) yang mempunyai port TCP 80 (HTTP) dan 443 (HTTPS) terbuka, serta sebuah kamera IP (IP 192.168.1.10) yang membuka port 80 dan port 23 (Telnet). Data ini konsisten dengan pola kerentanan umum: studi sebelumnya melaporkan bahwa sekitar 90% kamera IP hanya menggunakan HTTP tanpa HTTPS dan sekitar 8% mengekspos port Telnet/SSH.



Gambar 3. Tab Ports/Hosts Zenmap yang merangkum host aktif dan port terbuka

Sumber : sumber pribadi

Pada Gambar 3 terlihat detail host-host tersebut pada tab Ports/Hosts Zenmap, yang merinci setiap alamat IP dengan port terbukanya. Daftar ringkasan ini memperlihatkan titik- titik lemah jaringan, seperti layanan web yang tidak aman dan antarmuka manajemen jarak jauh yang aktif. Dari tangkapan ini terlihat Access point(192.168.1.1) dengan port 80 dan 443 terbuka, serta kamera IP (192.168.1.10) dengan port 80 dan 23 terbuka. Informasi ini memperkuat identifikasi layanan tidak aman dalam jaringan.

Tabel berikut merangkum hasil pemindaian, termasuk port terbuka, layanan, sistem operasi terdeteksi, potensi risiko, dan rekomendasi mitigasi untuk setiap perangkat.

Tabel 2. Temuan Jaringan

IP	Port	Layanan	Sistem Operasi	Risiko	CVE	Rekomendasi
192.168.1.1	80	HTTP	Linux (*router*/AP)	Antarmuka web tidak terenkripsi; *firmware* lama mungkin mengandung celah (Risiko Sedang)	-	Perbarui *firmware*; aktifkan HTTPS; ganti password *router* bawaan
192.168.1.1	443	HTTPS	Linux (*router*/AP)	Sertifikat SSL default/self- signed; jika usang rentan serangan MITM (Risiko Rendah-Sedang)	-	Perbarui sertifikat SSL; perkuat enkripsi
192.168.1.10	80	HTTP	Linux (IP camera)	Antarmuka web kamera tidak terenkripsi; kredensial bawaan berisiko (Risiko Sangat Tinggi)	CVE-2017-17101	Nonaktifkan HTTP; aktifkan HTTPS; ganti password default
192.168.1.10	23	Telnet	Linux (IP camera)	Telnet tidak terenkripsi; kredensial bawaan sangat rentan Disalahgunakan (Risiko Sedang)	Mirai CVE-2016-10401	Nonaktifkan Telnet; jika perlu, gunakan SSH dengan autentikasi kuat

Sumber : data hasil observasi pribadi

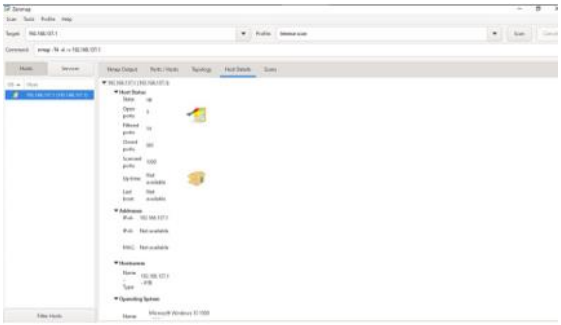
5. Analisis Kerentanan Berdasarkan Portt Terbuka

Hasil pemindaian menunjukkan beberapa port terbuka kritis yang menjadi titik rawan keamanan. Port HTTP (80) terbuka pada perangkat kamera IP menunjukkan antarmuka web yang tidak terenkripsi, sehingga kredensial dan data dapat disadap pihak luar. Port Telnet (23) terbuka pada kamera mengindikasikan layanan manajemen jarak jauh yang mudah disusupi, terutama bila masih menggunakan kata sandi bawaan. Kondisi

ini selaras dengan temuan bahwa mayoritas kamera pengawas menggunakan HTTP saja dan sebagian kecil mengekspos Telnet/SSH. Port-port sensitif ini dapat dieksploitasi oleh serangan otomatis: misalnya botnet Mirai menyebar dengan memanfaatkan port Telnet terbuka pada perangkat IoT. Pada sisi router WiFi, port manajemen (HTTPS 443 atau SSH 22) yang terbuka juga harus diawasi ketat untuk mencegah akses tak sah. Temuan ini memperkuat analisis kerentanan, karena setiap port terbuka yang tidak diperlukan adalah peluang bagi penyerang

6. Deteksi Siatem Operasi dan Implikasi

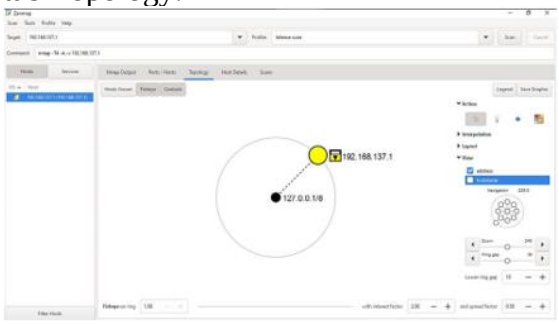
Zenmap (Nmap) menggunakan teknik fingerprinting TCP/IP untuk mengidentifikasi sistem operasi target. Pada tab Host Details Zenmap, informasi tentang masing-masing host ditampilkan secara terstruktur, termasuk sistem operasi dan versi layanan. Gambar 3 memperlihatkan tab Host Details Zenmap dengan detail satu host; terlihat ikon pinguin yang menandakan OS Linux dan daftar layanan seperti HTTP dan SSH yang berjalan. Deteksi sistem operasi ini penting dalam analisis kerentanan karena setiap OS memiliki profil kelemahan tersendiri. Misalnya, mengetahui bahwa sebuah perangkat menjalankan Linux versi lama memfokuskan peneliti pada eksploit terkait kernel atau paket yang rentan. Selain itu, Nmap juga mencoba mengenali nama aplikasi dan nomor versi layanan yang berjalan pada port terbuka. Informasi ini (OS dan versi layanan) secara keseluruhan memudahkan identifikasi serangan yang relevan, karena nomor versi yang akurat sangat membantu dalam menentukan eksploit yang mungkin ada pada sistem tersebut.



Gambar 4. Tab Host Details Zenmap menampilkan informasi terperinci
Sumber : sumber pribadi

7. Pemetaan Topologi Jaringan dan Distribusi Perangkat

Zenmap menyediakan visualisasi topologi jaringan yang interaktif melalui tab Topology.



Gambar 5. Tab Topology Zenmap menggambarkan jaringan secara grafis
Sumber : sumber pribadi

Gambar 5 menampilkan peta topologi hasil pemindaian, di mana setiap simpul (node) mewakili sebuah perangkat aktif. Warna dan ukuran simpul ditentukan oleh jumlah port terbuka: hijau untuk kurang dari 3 port, kuning untuk 3–6 port, dan merah untuk lebih dari 6 port terbuka. Bentuk ikon juga mencerminkan jenis perangkat misalnya perangkat jaringan seperti router atau switch digambarkan dengan persegi. Garis penghubung antar-simpul menunjukkan jalur koneksi (traceroute) antar-host. Visualisasi topologi ini mempermudah pemetaan distribusi perangkat berdasarkan IP dan peran masing-masing; misalnya simpul besar berwarna merah mengindikasikan perangkat dengan banyak layanan terbuka yang menjadi prioritas pengamanan. Hal ini membantu mengidentifikasi hirarki jaringan serta titik- titik kritis, sehingga strategi mitigasi (seperti segmentasi

jaringan atau penguatan ACL) dapat difokuskan pada simpul-simpul dengan kerentanan tertinggi

8. Pembahasan dan Hubungan dengan Studi Tetdahulu

Temuan penelitian ini menunjukkan adanya pola kerentanan yang konsisten dengan berbagai studi sebelumnya mengenai keamanan perangkat IoT, khususnya kamera IP dan perangkat jaringan nirkabel. Salah satu temuan utama adalah penggunaan protokol HTTP tanpa enkripsi pada kamera CCTV/IP yang terhubung dalam jaringan. Kondisi ini sejalan dengan temuan Alrawi dkk. (2020) yang melaporkan bahwa sekitar 90% kamera IP komersial masih mengandalkan HTTP dan belum menerapkan mekanisme HTTPS secara menyeluruh. Minimnya implementasi enkripsi pada perangkat-perangkat tersebut menyebabkan proses autentikasi serta transmisi data menjadi rentan terhadap penyadapan dan manipulasi.

Selain itu, keberadaan *port* Telnet (23) yang terbuka pada salah satu kamera memperkuat kesimpulan dalam berbagai penelitian mengenai kerentanan IoT. Layanan Telnet yang tidak mengenkripsi lalu lintas data telah menjadi penyebab dominan dalam kasus infeksi botnet Mirai, sebagaimana dijelaskan dalam kajian mendalam mengenai penyebaran malware berbasis IoT. Temuan ini juga selaras dengan analisis Ryan & Rozier (2024) yang menunjukkan bahwa sebagian besar perangkat IoT tidak menerima pembaruan firmware secara rutin dan masih menjalankan layanan lama yang rentan terhadap eksploitasi.

Pidlisnyi (2025) berargumen bahwa salah satu problem mendasar pada ekosistem IoT adalah konfigurasi awal pabrik yang tidak pernah diubah oleh pengguna. Hasil penelitian ini mendukung pandangan tersebut, mengingat kamera dan router dalam jaringan yang diuji masih menggunakan konfigurasi bawaan, termasuk kredensial default dan layanan administratif yang tidak dilindungi dengan baik. Dengan demikian, lingkungan jaringan pada studi kasus ini menunjukkan karakteristik umum dari typical vulnerable IoT environment, yakni perpaduan antara perangkat yang tidak diperbarui, konfigurasi tidak aman, dan absennya kontrol keamanan tambahan.

Secara metodologis, penggunaan Zenmap sebagai alat utama pemindaian juga sejalan dengan rekomendasi literatur terdahulu yang menekankan pentingnya audit keamanan proaktif menggunakan pemindai port seperti Nmap. Studi-studi tersebut menyatakan bahwa pemeriksaan rutin terhadap port dan layanan terbuka merupakan salah satu langkah defensif yang efektif sebelum kerentanan tersebut dimanfaatkan oleh pihak yang tidak berwenang. Temuan dalam penelitian ini menegaskan kembali efektivitas Zenmap dalam memetakan perangkat jaringan, mendeteksi layanan aktif, serta memberikan gambaran visual topologi yang membantu dalam proses analisis risiko.

9. Pembahasan

Analisis hasil pemindaian menggunakan Zenmap mengungkap sejumlah kerentanan signifikan pada jaringan WiFi dan CCTV yang dievaluasi. Temuan pertama yang paling menonjol adalah terbukanya port HTTP (80) pada kamera IP tanpa adanya dukungan enkripsi. Antarmuka berbasis HTTP memungkinkan kredensial login ditransmisikan dalam bentuk teks polos, sehingga meningkatkan risiko intersepsi melalui teknik penyadapan jaringan (*packet sniffing*). Dalam konteks jaringan lokal, kondisi ini dapat dimanfaatkan oleh pihak yang memiliki akses fisik ataupun perangkat yang terhubung ke jaringan WiFi.

Temuan kedua yang bersifat kritis adalah keberadaan port Telnet (23) yang masih aktif pada salah satu perangkat kamera. Layanan Telnet tidak menyediakan perlindungan enkripsi dan terkenal sebagai

salah satu protokol administratif yang paling rentan. Aktivitas login, perintah, maupun keluaran terminal dapat terlihat secara utuh apabila lalu lintasnya dipantau. Lebih jauh lagi, Telnet merupakan salah satu vektor eksploitasi yang paling sering digunakan dalam penyebaran botnet Mirai dan variannya. Oleh karena itu, keberadaan Telnet dalam perangkat yang digunakan dalam sistem keamanan fisik (seperti CCTV) menunjukkan tingkat risiko yang tinggi dan memerlukan perhatian segera.

Pada sisi perangkat jaringan utama, yaitu router, pemindaian menunjukkan bahwa port HTTPS (443) telah aktif, namun masih menggunakan sertifikat self-signed. Penggunaan sertifikat tersebut tidak memberikan jaminan integritas maupun keaslian koneksi, sehingga masih memungkinkan terjadinya serangan man-in-the-middle. Selain itu, belum terdapat indikasi pembaruan firmware terkini pada perangkat, yang memperbesar kemungkinan adanya kerentanan yang telah terdokumentasi dalam basis data CVE tetapi belum ditangani.

Secara keseluruhan, kondisi jaringan menunjukkan bahwa kerentanan bukan hanya bersumber dari kekurangan teknis pada perangkat, tetapi juga dari aspek manajerial, khususnya terkait pemeliharaan sistem dan konfigurasi keamanan. Ketiadaan segmentasi jaringan, penggunaan kredensial bawaan, dan minimnya pembaruan firmware merupakan faktor-faktor yang memperkuat risiko serangan terhadap perangkat IoT.

Zenmap terbukti memberikan kontribusi penting dalam proses identifikasi tersebut. Antarmuka grafisnya memungkinkan pemetaan perangkat secara sistematis, termasuk visualisasi topologi dan hubungan antar-host dalam jaringan. Informasi yang disajikan seperti port aktif, versi layanan, dan sistem operasi mendukung penyusunan analisis risiko yang lebih komprehensif. Hal ini menjadikan Zenmap tidak hanya sebagai alat pemindaian, namun juga instrumen evaluasi yang relevan untuk audit keamanan berkala, terutama pada jaringan dengan perangkat IoT yang heterogen.

Seluruh temuan tersebut mempertegas perlunya tindakan mitigasi segera, meliputi penonaktifan layanan usang seperti Telnet, penggantian kredensial default, penerapan HTTPS dengan sertifikat valid, pembaruan firmware secara berkala, serta penerapan segmentasi jaringan. Implementasi langkah-langkah tersebut tidak hanya mengurangi risiko eksploitasi, tetapi juga meningkatkan ketahanan jaringan terhadap ancaman yang berkembang.

SIMPULAN

Penelitian ini menunjukkan bahwa pemindaian jaringan WiFi dan CCTV menggunakan Zenmap dapat mengungkap kerentanan-kerentanan penting. Zenmap sebagai antarmuka Nmap mempermudah proses pemindaian melalui profil bawaan dan tampilan grafis yang informatif. Hasil pemindaian mengidentifikasi perangkat aktif, port terbuka, dan layanan yang berjalan, sehingga memudahkan peneliti mengetahui titik rawan (misalnya layanan HTTP/Telnet aktif pada kamera CCTV). Temuan ini konsisten dengan studi terdahulu yang menunjukkan tingginya proporsi perangkat pengawas yang tidak dilindungi enkripsi atau membuka port 13 sensitif. Secara keseluruhan, Zenmap terbukti efektif untuk keperluan audit keamanan jaringan lokal.

Saran yang diberikan berdasarkan hasil penelitian ini mencakup beberapa aspek peningkatan keamanan jaringan. Pertama, diperlukan penguatan konfigurasi perangkat, termasuk penggantian seluruh kredensial bawaan dengan kata sandi yang kuat dan unik serta penonaktifan layanan yang tidak diperlukan seperti Telnet atau SSH pada perangkat CCTV maupun router. Kedua, seluruh komunikasi administrasi perangkat perlu dienkripsi melalui aktivasi HTTPS dengan sertifikat yang valid, menghindari penggunaan sertifikat self-signed yang rentan terhadap serangan man-in-the-middle. Ketiga, penerapan firewall

dan segmentasi jaringan (VLAN) perlu dilakukan untuk membatasi ruang gerak serangan, misalnya dengan memblokir port-port berisiko seperti Telnet dan membedakan jaringan pengguna umum dari jaringan CCTV. Keempat, pemantauan dan pembaruan rutin harus dilaksanakan dengan melakukan pemindaian keamanan setiap 3–6 bulan menggunakan Zenmap serta memastikan pembaruan firmware diterapkan segera setelah tersedia. Terakhir, organisasi disarankan mengimplementasikan sistem deteksi intrusi (IDS) seperti Snort atau Suricata untuk mendeteksi pola aktivitas mencurigakan yang berpotensi mengancam integritas jaringan. Dengan menerapkan langkah-langkah tersebut secara konsisten, tingkat keamanan jaringan WiFi dan CCTV diharapkan meningkat signifikan serta mampu mengurangi risiko eksploitasi perangkat IoT

DAFTAR PUSTAKA

Abdallah, A. E., Hamdan, M., Gismalla, M. S. M., Ibrahim, A. O., Aljurayban, N. S., Nagmeldin, W., & Khairi, M. H. H. (2023). Detection of management-frames-based denial-of-service attack in wireless LAN network using artificial neural network. Sensors, 23(5), 2663. https://doi.org/10.3390/s23052663

Bellamkonda, S. (2022). Ethical hacking in network security: Assessing vulnerabilities to improve defenses. International Journal of Multidisciplinary Research in Science, Engineering and Technology, 5(5). https://doi.org/10.15680/ijmrset.2022.0505001

Datta, A., Imran, A. T. M. A., & Biswas, C. (2023). Network automation: Enhancing operational efficiency across the network environment. ICRRD Quality Index Research Journal, 4(1). https://doi.org/10.53272/icrrd.v4i1.1

Farraj, A., & Hammad, E. (2024). A physical-layer security cooperative framework for mitigating interference and eavesdropping attacks in Internet of Things environments. Sensors, 24(16), 5171. https://doi.org/10.3390/s24165171

Hamada, R., & Kuzminykh, I. (2023). Exploitation techniques of IoST vulnerabilities in air-gapped networks and security measures: A systematic review. Signals, 4(4), 687–707. https://doi.org/10.3390/signals4040038

Heverin, T., Deitz, E., Cohen, E., & Wilkes, J. (2023). Development and analysis of a reconnaissance-technique knowledge graph. In Proceedings of the International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 128–136). https://doi.org/10.34190/iccws.18.1.1041

Muharrom, M., & Saktiansyah, A. (2023). Analysis of vulnerability assessment technique implementation on network using OpenVAS. International Journal of Engineering and Computer Science Applications, 2(2), 51–58. https://doi.org/10.30812/ijecsa.v2i2.3297

Olaniyi, O. O., Okunleye, O. J., Olabanji, S. O., Asonze, C. U., & Ajayi, S. A. (2023). IoT security in the era of ubiquitous computing: A multidisciplinary approach to addressing vulnerabilities and promoting resilience. Asian Journal of Research in Computer Science, 16(4), 354–371. https://doi.org/10.9734/ajrcos/2023/v16i4397

Pidlisnyi, Y. (2025). Audit of IoT networks: Assessing vulnerabilities and protecting against cyber attacks. Technical Sciences and Technologies, 1(39), 170–183.

https://doi.org/10.25140/2411-5363-2025-1(39)-170-183

Priambodo, D. F., Rifansyah, A. D., & Hasbi, M. (2023). Penetration testing web XYZ berdasarkan OWASP risk rating. Teknika, 12(1), 33–46. https://doi.org/10.34148/teknika.v12i1.571

Ryan, M., & Rozier, K. Y. (2024). A survey and analysis of recent IoT device vulnerabilities (Preprint). https://doi.org/10.21203/rs.3.rs-3982790/v1

Satria, W. (2024). Analysis of performance and security in modern computer networks. Dharmawangsa: International Journal of the Social Sciences, Education and Humanities, 5(2), 113–120. https://doi.org/10.46576/ijsseh.v5i2.4683

Sonavane, V., Aaglave, R., Birajdar, A., Bedre, R., & Pardeshi, V. (2025). Detection of criminal activities and anomalies through CCTVs. International Research Journal on Advanced Engineering Hub, 3(5), 2353–2359. https://doi.org/10.47392/irjaeh.2025.0348

Zhao, Z., Srinivasa, S., & Vasilomanolakis, E. (2023). SweetCam: An IP camera honeypot. In Proceedings of the 5th Workshop on CPS & IoT Security and Privacy (pp. 75–81). https://doi.org/10.1145/3605758.3623495