# Perancangan dan Implementasi Aplikasi Pemindaian Port Berbasis GUI (Bryan Scan) Sebagai Alat Bantu Analisis Keamanan Jaringan

Muhamad Ridwan[1)], Mohamad Sudi[2)], Asep Suryanta[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1) 2) 3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1) 2) 3)]
Email:ridwan.mtte20@gmail.com[1)],mohammad1717@gmail.com[2)]
, zenilybaz@gmail.com[3)]

## *Perancangan dan Implementasi Aplikasi Pemindaian Port Berbasis GUI (Bryan Scan) Sebagai Alat Bantu Analisis Keamanan Jaringan*

***Abstract:*** *The increasing complexity of computer network infrastructures requires a systematic and user-friendly security auditing mechanism. One of the essential stages in network security auditing is port scanning, which is used to identify active services that may pose potential security vulnerabilities. However, most tools such as Nmap are still based on a Command Line Interface (CLI), requiring technical expertise to interpret the scanning results effectively.*

*This study aims to design and implement a Graphical User Interface (GUI)-based port scanning application named Bryan Scan, which integrates the Nmap engine as a supporting tool for network security analysis. The research method employs the System Development Life Cycle (SDLC) Waterfall model, consisting of requirements analysis, system design, implementation, testing, and evaluation stages. The system is developed using Python, integrating Nmap through system calls and processing XML-based output.*

*The results indicate that Bryan Scan is capable of displaying open ports, active services, operating system detection, and automatically generating a rule-based security risk score. The level of conformity between Bryan Scan and Nmap CLI reaches ≥95%, with improved ease of analysis based on usability testing results. Therefore, the application is feasible to be utilized as a structured and informative tool for internal network security auditing.*

*Keywords: network security, port scanning, Nmap, GUI, risk analysis, network auditing.*

***Abstrak:*** *Perkembangan infrastruktur jaringan komputer yang semakin kompleks menuntut adanya mekanisme audit keamanan yang sistematis dan mudah digunakan. Salah satu tahapan penting dalam audit keamanan jaringan adalah pemindaian port (port scanning) untuk mengidentifikasi layanan aktif yang berpotensi menjadi celah keamanan. Namun, sebagian besar tools seperti Nmap masih berbasis Command Line Interface (CLI), sehingga memerlukan pemahaman teknis dalam interpretasi hasilnya. Penelitian ini bertujuan untuk merancang dan mengimplementasikan aplikasi pemindaian port berbasis Graphical User Interface (GUI) bernama Bryan Scan yang terintegrasi dengan mesin Nmap sebagai alat bantu analisis keamanan jaringan. Metode penelitian menggunakan pendekatan System Development Life Cycle (SDLC) model Waterfall yang meliputi tahap*

*analisis kebutuhan, perancangan sistem, implementasi, pengujian, dan evaluasi. Sistem dikembangkan menggunakan Python dengan integrasi Nmap melalui pemanggilan system call serta pengolahan output berbasis XML. Hasil penelitian menunjukkan bahwa Bryan Scan mampu menampilkan informasi port terbuka, layanan aktif, deteksi sistem operasi, serta menghasilkan skor risiko keamanan berbasis rule-based secara otomatis. Tingkat kesesuaian hasil antara Bryan Scan dan Nmap CLI mencapai ≥95%, dengan peningkatan kemudahan analisis berdasarkan pengujian usability. Dengan demikian, aplikasi ini layak digunakan sebagai alat bantu audit keamanan jaringan internal secara terstruktur dan informatif.*

.

*Kata kunci: keamanan jaringan, port scanning, Nmap, GUI, analisis risiko, audit jaringan.*

## PENDAHULUAN

Transformasi digital telah meningkatkan ketergantungan organisasi terhadap infrastruktur jaringan komputer dalam mendukung operasional sistem informasi. Kondisi tersebut menjadikan keamanan jaringan sebagai aspek fundamental untuk menjaga kerahasiaan, integritas, dan ketersediaan data.

Salah satu potensi kerentanan yang umum ditemukan adalah keberadaan port terbuka dan layanan jaringan yang tidak terkonfigurasi dengan baik. Port terbuka yang tidak teridentifikasi dapat menjadi titik awal eksploitasi oleh pihak tidak berwenang. Oleh karena itu, pemindaian port menjadi tahapan awal yang penting dalam proses audit keamanan jaringan.

Network Mapper (Nmap) merupakan tools populer dalam pemindaian port karena memiliki fleksibilitas dan akurasi tinggi. Namun, pendekatan berbasis Command Line Interface (CLI) menuntut pemahaman sintaks perintah serta interpretasi hasil dalam bentuk teks mentah. Hal ini menyulitkan pengguna non-teknis dalam melakukan analisis yang sistematis.

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan perancangan aplikasi pemindaian port berbasis Graphical User Interface (GUI) bernama Bryan Scan yang mampu mengintegrasikan mesin Nmap ke dalam sistem yang lebih terstruktur, dilengkapi analisis risiko dan rekomendasi mitigasi otomatis.

Tujuan penelitian dalam penelitian ini meliputi:

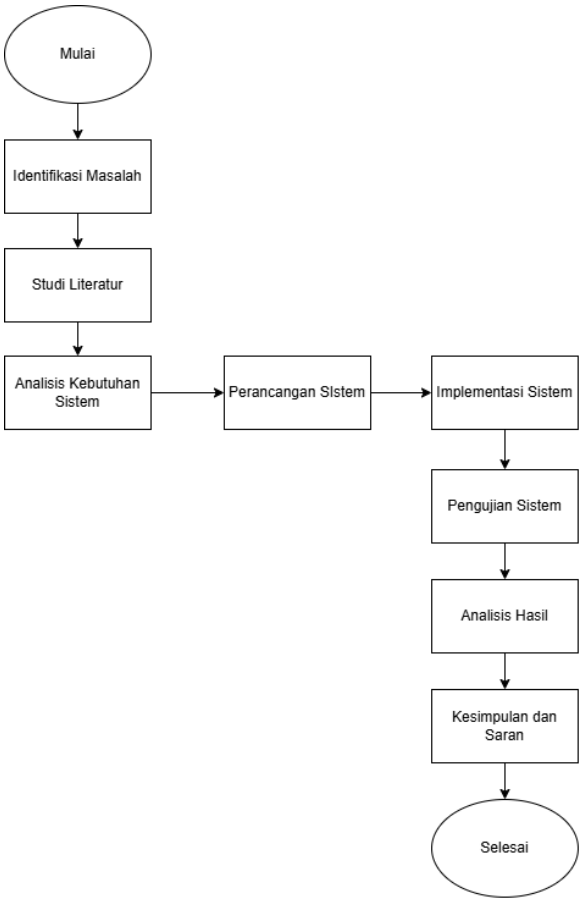
1. Merancang dan mengimplementasikan aplikasi Bryan Scan berbasis GUI.
2. Mengembangkan sistem analisis risiko keamanan berbasis rule-based.
3. Menguji tingkat akurasi dan efisiensi dibandingkan Nmap CLI.

## METODE PENELITIAN

Penelitian ini menggunakan model System Development Life Cycle (SDLC) dengan pendekatan Waterfall yang terdiri dari:

1. Analisis Kebutuhan Sistem

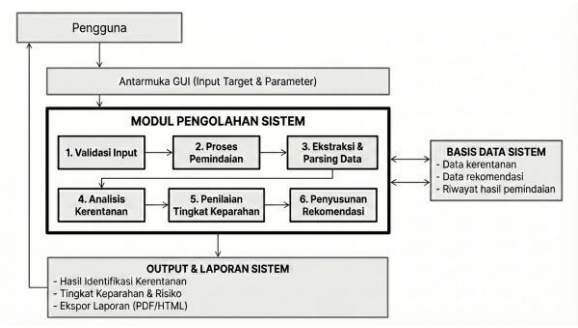
Mengidentifikasi kebutuhan fungsional (pemindaian port, analisis risiko, rekomendasi mitigasi) dan non-fungsional (akurasi, efisiensi, usability). Tahapan penelitian ditunjukkan pada Gambar 1.




*Gambar 0.1 Diagram Alir Penelitian*

2. Perancangan Sistem

Pada tahap ini dilakukan perancangan arsitektur sistem, alur kerja aplikasi, dan tampilan antarmuka pengguna. Perancangan sistem meliputi diagram alur proses pemindaian, perancangan struktur data hasil scan, serta rancangan antarmuka GUI yang menampilkan hasil pemindaian dan rekomendasi keamanan.




*Gambar 2 Diagram Blok Sistem*

3. Implementasi Sistem

Tahap implementasi merupakan proses realisasi dari hasil perancangan sistem ke dalam bentuk aplikasi perangkat lunak yang dapat dijalankan. Implementasi dilakukan berdasarkan desain sistem yang telah dirumuskan pada tahap sebelumnya, meliputi perancangan arsitektur sistem, diagram alur, serta kebutuhan fungsional dan non-fungsional. Aplikasi vulnerability scanner berbasis Graphical User Interface (GUI) dikembangkan menggunakan bahasa pemrograman Python dengan memanfaatkan pustaka pendukung untuk integrasi mesin pemindaian Nmap. Sistem dirancang secara modular untuk mempermudah pengembangan dan pemeliharaan.

Modul utama yang diimplementasikan dalam sistem meliputi:

a. Modul Antarmuka Pengguna (GUI)

Modul ini berfungsi sebagai media interaksi antara pengguna dan sistem. Pengguna dapat memasukkan target berupa alamat IP atau domain, serta memilih parameter pemindaian yang tersedia.

b. Modul Validasi dan Resolusi Target

Modul ini bertugas melakukan validasi terhadap format input. Apabila input berupa domain, sistem akan melakukan proses resolusi DNS untuk memperoleh alamat IP sebelum proses pemindaian dilakukan.

c. Modul Pemindaian (Scanning Engine)

Modul ini mengintegrasikan mesin Nmap untuk melakukan pemindaian port dan identifikasi layanan yang berjalan pada host target. Hasil pemindaian disimpan dalam format terstruktur untuk diproses lebih lanjut.

d. Modul Pengolahan dan Analisis Hasil

Output hasil pemindaian diolah untuk mengidentifikasi port terbuka, jenis layanan, serta potensi risiko yang dapat ditimbulkan.

e. Modul Analisis Risiko dan Rekomendasi

Sistem melakukan klasifikasi tingkat risiko berdasarkan aturan yang telah ditentukan. Selanjutnya, sistem menghasilkan rekomendasi mitigasi sebagai tindakan pencegahan terhadap potensi kerentanan yang ditemukan.

f. Modul Penyimpanan Data

Hasil pemindaian dan analisis disimpan sebagai log untuk keperluan dokumentasi dan evaluasi lebih lanjut.

Tahap implementasi ini menghasilkan aplikasi yang mampu melakukan proses pemindaian secara terintegrasi mulai dari input target hingga penyajian hasil analisis dalam bentuk yang informatif dan mudah dipahami oleh pengguna.

4. Pengujian Sistem

Pengujian dilakukan untuk memastikan bahwa aplikasi berjalan sesuai dengan kebutuhan yang telah ditetapkan. Pengujian dilakukan menggunakan metode black box testing dengan membandingkan hasil pemindaian aplikasi GUI dengan hasil pemindaian Nmap berbasis CLI. Tujuan utama tahap ini adalah memastikan bahwa sistem memenuhi spesifikasi kebutuhan fungsional dan non-fungsional yang telah ditetapkan pada tahap analisis kebutuhan. Secara metodologis, pengujian dalam penelitian ini dilakukan berdasarkan tiga aspek utama, yaitu:

a. Pengujian fungsionalitas, untuk memastikan bahwa seluruh fitur utama sistem berjalan sesuai dengan spesifikasi yang dirancang.

b. Pengujian performa, untuk mengukur efisiensi sistem dalam menyelesaikan proses pemindaian.

c. Pengujian usability, untuk menilai tingkat kemudahan penggunaan

sistem dari perspektif pengguna akhir.

Setiap aspek pengujian memiliki indikator pengukuran yang bersifat kuantitatif agar hasilnya dapat dianalisis secara objektif. Pengujian dilakukan dalam kondisi jaringan yang terkontrol dengan parameter pemindaian yang konsisten guna menjaga validitas hasil. Hasil dari tahap pengujian ini selanjutnya dianalisis dan dijadikan dasar dalam tahap evaluasi sistem. Adapun prosedur teknis, parameter pengujian, serta kriteria keberhasilan masing-masing aspek dijabarkan secara rinci pada Subbab 3. Skenario Pengujian.

5. Analisis Hasil

Tahap analisis hasil dilakukan setelah proses pengujian sistem selesai dilaksanakan. Analisis ini bertujuan untuk mengevaluasi kinerja aplikasi vulnerability scanner berbasis GUI dalam mendeteksi layanan aktif, mengidentifikasi potensi risiko keamanan, serta memberikan rekomendasi mitigasi yang sesuai. Analisis dilakukan dengan membandingkan hasil pemindaian sistem terhadap tabel dasar keamanan jaringan yang telah ditetapkan pada tahap perancangan. Tabel dasar keamanan jaringan tersebut berfungsi sebagai acuan dalam menentukan tingkat risiko dari setiap port dan layanan yang terdeteksi.

a. Dasar Analisis Risiko Keamanan Jaringan

Dasar analisis risiko keamanan jaringan dalam penelitian ini disusun berdasarkan klasifikasi layanan jaringan yang umum digunakan serta tingkat potensi ancaman yang dapat ditimbulkan oleh masing-masing layanan. Setiap port dan service yang terdeteksi dalam keadaan terbuka akan dievaluasi menggunakan tabel dasar keamanan jaringan yang telah dirancang sebelumnya. Tabel tersebut memuat informasi mengenai nomor port, jenis layanan, tingkat risiko, bobot risiko, serta rekomendasi mitigasi. Penentuan tingkat risiko dilakukan dengan mempertimbangkan karakteristik layanan, potensi eksploitasi, serta praktik keamanan jaringan yang direkomendasikan.

Bobot risiko diberikan untuk mengkuantifikasi tingkat ancaman secara numerik, sehingga memungkinkan proses perhitungan skor keamanan dilakukan secara objektif dan konsisten. Semakin tinggi bobot yang diberikan, semakin besar potensi risiko yang dapat ditimbulkan terhadap sistem.

Dengan menggunakan tabel dasar ini sebagai knowledge base, sistem dapat melakukan proses analisis secara sistematis, terukur, dan terstandarisasi dalam menentukan tingkat keamanan suatu host berdasarkan hasil pemindaian yang diperoleh.

*Tabel 1 Dasar Klasifikasi Risiko Keamanan Jaringan*

| No | Port/Service | Kondisi Terbaca | Tingkat Risiko | Interpretasi Keamanan | Rekomendasi Sistem |
|---|---|---|---|---|---|
| 1 | 21 / FTP | Open | Tinggi | Transmisi plaintext, rawan sniffing & brute force | Nonaktifkan FTP, gunakan SFTP |
| 2 | 22 / SSH | open ke publik | Sedang | Target brute force login | Aktifkan fail2ban & batasi IP |
| 3 | 23 / Telnet | open | Kritis | Password tidak terenkripsi | Disable service |

| | | | | | |
|---|---|---|---|---|---|
| 4 | 25 / SMTP | open relay | Tinggi | Server bisa jadi spam bot | Aktifkan authentication SMTP |
| 5 | 53 / DNS | recursion enabled | Tinggi | DNS amplification attack | Batasi recursion internal only |

b. Mekanisme Analisis Hasil Pemindaian

Setelah sistem melakukan pemindaian terhadap target, hasil berupa daftar port terbuka dan layanan aktif akan dicocokkan dengan tabel dasar keamanan jaringan.

Proses analisis dilakukan melalui langkah berikut:

- Sistem membaca hasil pemindaian port dan layanan aktif.
- Setiap layanan yang terdeteksi dicocokkan dengan tabel klasifikasi risiko.
- Sistem mengambil nilai bobot risiko yang sesuai.
- Bobot risiko dijumlahkan untuk memperoleh total skor keamanan host.
- Total skor digunakan untuk menentukan kategori tingkat keamanan.

c. Perhitungan Skor Keamanan

Perhitungan skor keamanan dilakukan untuk memberikan gambaran kuantitatif mengenai tingkat risiko dari suatu host atau sistem yang dipindai. Pendekatan ini digunakan agar hasil analisis tidak hanya bersifat deskriptif, tetapi juga dapat diukur secara numerik berdasarkan bobot risiko masing-masing layanan yang terdeteksi.

Setiap port dan layanan yang ditemukan dalam keadaan terbuka akan dicocokkan dengan tabel dasar klasifikasi risiko keamanan jaringan. Pada tabel tersebut, setiap layanan memiliki nilai bobot risiko yang merepresentasikan tingkat potensi ancaman terhadap keamanan sistem.

Skor keamanan total dihitung dengan menjumlahkan seluruh bobot risiko dari layanan aktif yang terdeteksi, dengan rumus sebagai berikut:

Total Skor Risiko = Σ (Bobot Risiko Layanan Aktif).

*Tabel 2 Skor Keamanan*

| Rentang Skor | Kategori Keamanan |
|---|---|
| 0 – 5 | Aman |
| 6 – 10 | Waspada |
| 11 – 20 | Rentan |
| > 20 | Berbahaya |

d. Analisis Kinerja Sistem

Analisis kinerja sistem dilakukan untuk mengevaluasi efisiensi dan stabilitas aplikasi dalam menjalankan proses pemindaian serta analisis risiko. Evaluasi ini penting untuk memastikan bahwa sistem tidak hanya akurat, tetapi juga responsif dan layak digunakan dalam kondisi operasional.

Parameter utama yang dianalisis dalam pengujian kinerja meliputi:

- Waktu Eksekusi Pemindaian
  Waktu yang dibutuhkan sistem sejak proses scan dimulai hingga hasil analisis ditampilkan kepada pengguna. Pengukuran dilakukan dalam satuan detik dan dicatat untuk setiap skenario pengujian.
- Stabilitas Sistem
  Kemampuan aplikasi untuk tetap berjalan tanpa mengalami error, crash, atau kegagalan proses selama pemindaian berlangsung.
- Konsistensi Output
  Konsistensi hasil ketika sistem melakukan pemindaian terhadap target yang sama dalam beberapa kali pengujian.

Data hasil pengujian kinerja disajikan dalam bentuk tabel yang memuat target pemindaian, waktu eksekusi, serta status keberhasilan

proses. Selanjutnya, dilakukan analisis deskriptif untuk menilai apakah sistem telah memenuhi kriteria efisiensi yang diharapkan.

Apabila waktu eksekusi berada dalam rentang yang wajar dan sistem berjalan stabil tanpa gangguan, maka dapat disimpulkan bahwa aplikasi memiliki performa yang baik dan layak digunakan sebagai alat bantu analisis keamanan jaringan.

e. Analisis Usabillity

Analisis usability dilakukan untuk mengukur tingkat kemudahan penggunaan sistem dari perspektif pengguna. Evaluasi ini bertujuan untuk mengetahui sejauh mana aplikasi dapat dipahami, digunakan, dan dioperasikan secara efektif oleh pengguna tanpa memerlukan pelatihan khusus.

Pengujian usability dilakukan menggunakan metode System Usability Scale (SUS). Metode ini terdiri dari serangkaian pertanyaan yang diberikan kepada responden setelah mereka mencoba menggunakan aplikasi. Setiap pertanyaan dinilai menggunakan skala Likert.

Skor SUS dihitung berdasarkan standar perhitungan yang telah ditetapkan dalam metode tersebut, sehingga menghasilkan nilai akhir dalam rentang 0 hingga 100.

Interpretasi skor dilakukan berdasarkan kategori berikut:

- Skor di atas rata-rata standar menunjukkan sistem memiliki tingkat usability yang baik
- Skor mendekati batas minimum menunjukkan sistem perlu perbaikan pada aspek antarmuka atau interaksi pengguna.

Hasil analisis usability ini digunakan untuk mengevaluasi kualitas pengalaman pengguna (user experience) serta sebagai dasar rekomendasi pengembangan sistem di masa mendatang.

Dengan adanya analisis usability, penelitian ini tidak hanya menilai aspek teknis sistem, tetapi juga mempertimbangkan faktor kenyamanan dan kemudahan penggunaan, sehingga aplikasi yang dihasilkan lebih aplikatif dan berorientasi pada kebutuhan pengguna

## HASIL PENELITIAN

Implementasi aplikasi Bryan Scan menghasilkan sistem pemindaian port berbasis Graphical User Interface (GUI) yang terintegrasi dengan mesin Network Mapper (Nmap). Sistem mampu menerima input target berupa alamat IP maupun hostname, melakukan validasi format alamat, menjalankan proses pemindaian melalui mekanisme system call, serta mengolah output dalam format XML menjadi data terstruktur yang ditampilkan pada antarmuka pengguna.

Hasil pemindaian yang ditampilkan meliputi nomor port, status port (open, closed, filtered), protokol yang digunakan, nama layanan (service), serta informasi tambahan seperti versi layanan dan hasil deteksi sistem operasi apabila mode pemindaian lanjutan diaktifkan. Data tersebut kemudian diproses oleh modul analisis risiko yang menghitung skor keamanan berdasarkan pembobotan kategori layanan yang terdeteksi.

Pengujian dilakukan pada beberapa host dalam jaringan lokal dengan variasi layanan aktif. Berdasarkan lima kali pengujian berulang pada setiap target, diperoleh tingkat kesesuaian rata-rata antara Bryan Scan dan Nmap CLI sebesar ≥95% dalam mendeteksi port terbuka dan layanan aktif. Perbedaan kecil yang ditemukan umumnya terjadi pada deteksi versi layanan tertentu yang bergantung pada respons banner dari host target.

Dari sisi waktu eksekusi, rata-rata waktu pemindaian menggunakan Bryan Scan menunjukkan selisih kurang dari 5% dibandingkan Nmap CLI. Selisih tersebut disebabkan oleh proses tambahan berupa parsing XML dan perhitungan skor risiko yang tidak dilakukan pada mode CLI standar. Meskipun demikian, perbedaan waktu tersebut tidak signifikan secara operasional dan masih berada dalam batas toleransi yang dapat diterima untuk kebutuhan audit jaringan internal.

Modul analisis risiko dalam Bryan Scan mampu menghasilkan skor total berdasarkan layanan yang terdeteksi. Sebagai contoh, apabila pada suatu host ditemukan layanan SSH (kategori medium), HTTP tanpa enkripsi (kategori medium), serta database service yang terbuka ke publik (kategori high), maka sistem secara otomatis menghitung skor risiko kumulatif dan mengklasifikasikan tingkat keamanan host ke dalam kategori waspada atau berisiko tinggi sesuai interval yang telah ditetapkan. Hasil klasifikasi ini ditampilkan bersamaan dengan rekomendasi mitigasi seperti pembatasan akses melalui firewall, penonaktifan layanan yang tidak diperlukan, atau penerapan enkripsi.

Evaluasi usability dilakukan menggunakan metode System Usability Scale (SUS) terhadap sejumlah responden yang memiliki latar belakang dasar jaringan komputer. Hasil pengolahan skor menunjukkan nilai rata-rata di atas ambang batas 68, yang mengindikasikan tingkat penerimaan sistem berada dalam kategori acceptable hingga baik. Responden menyatakan bahwa penyajian informasi dalam bentuk tabel terstruktur dan adanya skor risiko otomatis membantu dalam memahami kondisi keamanan host secara lebih cepat dibandingkan membaca output CLI yang berbasis teks mentah.

## PEMBAHASAN

Hasil penelitian menunjukkan bahwa pendekatan integrasi mesin Nmap ke dalam aplikasi berbasis GUI tidak mengurangi tingkat akurasi deteksi port dan layanan secara signifikan. Tingkat kesesuaian sebesar ≥95% menunjukkan bahwa proses parsing dan pengolahan data XML mampu mempertahankan konsistensi informasi yang dihasilkan oleh mesin pemindaian utama. Hal ini mengindikasikan bahwa sistem tidak melakukan modifikasi terhadap proses scanning inti, melainkan hanya mengoptimalkan cara penyajian dan analisis hasil.

Perbedaan minor pada deteksi versi layanan dapat dijelaskan oleh faktor respons jaringan dan konfigurasi host target yang dinamis. Dalam beberapa kasus, banner service tidak selalu memberikan informasi lengkap, sehingga perbedaan hasil bukan berasal dari kesalahan sistem, melainkan dari variasi respons target. Fenomena ini merupakan karakteristik umum dalam proses port scanning dan bukan merupakan indikasi penurunan akurasi sistem.

Dari sisi efisiensi, tambahan proses parsing dan perhitungan risiko menyebabkan sedikit peningkatan waktu eksekusi dibandingkan Nmap CLI. Namun, peningkatan tersebut relatif kecil dan tidak berdampak signifikan terhadap kinerja sistem secara keseluruhan. Dengan mempertimbangkan nilai tambah berupa analisis risiko otomatis dan penyajian visual yang terstruktur, selisih waktu tersebut dapat dianggap sebagai trade-off yang rasional dalam konteks audit keamanan jaringan.

Keunggulan utama Bryan Scan terletak pada modul analisis risiko berbasis rule-based yang mengubah hasil teknis pemindaian menjadi informasi yang lebih interpretatif. Pendekatan ini membantu pengguna dalam memahami tingkat eksposur layanan tanpa harus melakukan analisis manual terhadap setiap port yang terbuka. Dalam konteks manajemen keamanan jaringan, penyajian skor risiko dan klasifikasi tingkat keamanan memberikan nilai tambah sebagai sistem pendukung keputusan (decision support tool).

Hasil evaluasi usability memperkuat temuan bahwa antarmuka grafis yang intuitif meningkatkan efektivitas penggunaan sistem, khususnya bagi pengguna yang tidak terbiasa dengan lingkungan CLI. Dengan demikian, aplikasi ini tidak hanya berfungsi sebagai wrapper visual terhadap Nmap, tetapi juga sebagai sistem analitis yang menyederhanakan interpretasi data teknis menjadi informasi yang lebih operasional.

Secara keseluruhan, penelitian ini menunjukkan bahwa integrasi antara engine pemindaian yang telah teruji dengan antarmuka grafis dan modul analisis risiko dapat meningkatkan aksesibilitas dan pemahaman terhadap hasil audit keamanan jaringan tanpa mengorbankan akurasi teknis.

## KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan aplikasi pemindaian port berbasis GUI bernama Bryan Scan yang terintegrasi dengan mesin Nmap. Sistem mampu melakukan pemindaian port, mendeteksi layanan aktif, serta menampilkan hasil secara terstruktur dalam antarmuka grafis yang informatif. Tingkat akurasi sistem menunjukkan kesesuaian tinggi dengan Nmap CLI, dengan perbedaan yang tidak signifikan baik dari sisi deteksi maupun waktu eksekusi.

Integrasi modul analisis risiko berbasis pembobotan layanan memungkinkan sistem menghasilkan skor keamanan otomatis yang membantu dalam proses interpretasi hasil pemindaian. Evaluasi usability menunjukkan bahwa aplikasi memiliki tingkat penerimaan yang baik dan mempermudah proses analisis dibandingkan pendekatan CLI konvensional.

Dengan demikian, Bryan Scan dapat dimanfaatkan sebagai alat bantu dalam proses audit keamanan jaringan internal secara lebih sistematis, terukur, dan mudah dipahami. Pengembangan selanjutnya dapat diarahkan pada integrasi database kerentanan berbasis CVE, penyimpanan log terpusat, serta pengembangan metode analisis risiko yang lebih adaptif berbasis pembelajaran mesin.

**REFERENSI**

. Afni, M. R., Tahir, M., Puja, L. F., Affan, A. N., & Hadi, Y. A. N. (2025). Penggunaan log analytics dengan Python untuk analisis jejak digital dalam keamanan jaringan nirkabel. Jurnal Restikom: Riset Teknik Informatika dan Komputer, 7(1), 51–60. https://restikom.nusaputra.ac.id

Akbar, F., & Nugraha, R. (2022). Optimalisasi penggunaan Nmap Scripting Engine (NSE) untuk deteksi kerentanan jaringan. Jurnal Tekno Kompak, 15(1), 60–69.

Akbar, M. G., Witriyono, H., Apridiyansyah, Y., & Abdullah, D. (n.d.). Implementation of the Tkinter package, subprocess and os in network management application development with Python programming language. Jurnal Komitek, 3(1), 187–196. https://doi.org/10.53697/jkomitek.v3i1

Al Fikri, K. (2021). Keamanan jaringan menggunakan switch port security. Infotekjar, 5(2). https://doi.org/10.30743/infotekjar.v5i2.3501

Febrian, A. D., & Darmawan, R. (2022). Implementasi jaringan komputer berbasis virtual LAN untuk layanan Iconnet VIP pada jaringan MPLS (Multi Protocol Label Switching). Scientia. http://pijarpemikiran.com/index.php/Scientia

Hidayat, S., & Yusuf, M. (2023). Implementasi network mapper sebagai alat audit keamanan pada instansi pemerintah. Jurnal CoreIT, 7(2), 100–108.

Hongu Moly, A., Mau, S. D. I., & Ledi, D. F. (2025). Analisis keamanan jaringan komputer menggunakan metode penetration testing. Modem: Jurnal Informatika dan Sains Teknologi, 4(1), 10–22. https://doi.org/10.62951/modem.v4i1.694

Intan Sabila, M., Tahir, M., Mardania, S. D., & Arifin, R. I. (2025). Implementasi Snort sebagai IDS dalam mendeteksi port scanning Nmap pada simulasi jaringan virtual.

Kurniawan, I., & Firmansyah, R. (2022). Keamanan informasi pada infrastruktur jaringan di era transformasi digital. Jurnal Dokumentasi dan Informasi, 13(2), 89–98.

Kurniawan, I., & Setiawan, D. (2022). Implementasi intrusion detection system (IDS) Snort untuk mendeteksi serangan port scanning. Jurnal Ilmu Komputer dan Informatika, 6(1), 55–64. https://doi.org/10.30596/jiki.v6i1.4789

Lestari, S., & Wibowo, T. (2023). Evaluasi tingkat kerentanan sistem jaringan menggunakan network mapper (Nmap). Jurnal Teknologi dan Sistem Komputer, 11(2), 101–110. https://doi.org/10.14710/jtsiskom.11.2.101-110

Maulana, I., & Setiawan, D. (2021). Deteksi serangan port scanning menggunakan algoritma K-Nearest Neighbor pada log jaringan. Jurnal Infomedia, 6(1), 22–30.

Maulana, R., & Yuliani, F. (2023). Analisis keamanan server menggunakan kombinasi Nmap dan Metasploit framework. Jurnal Sistem Informasi dan Teknologi, 5(3), 210–220. https://doi.org/10.37034/jsit.v5i3.622

Muhyidin, Y., Totohendarto, M. H., Undamayanti, E., & Sekolah Tinggi

Teknologi Wastukancana. (n.d.). Perbandingan tingkat keamanan website menggunakan Nmap dan Nikto dengan metode ethical hacking.

Nugroho, A. S., & Santoso, B. (2021). Analisis monitoring sistem jaringan komputer menggunakan software Nmap. PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, 8(2), 112–120.

Nugroho, S., & Wijaya, T. H. (2022). Evaluasi tingkat agresivitas pemindaian Nmap terhadap performa traffic jaringan. JUTIF: Jurnal Teknik Informatika, 6(2), 210–219.

Prabowo, R., & Kurniawan, A. (2022). Analisis port terbuka menggunakan Nmap untuk meningkatkan keamanan server. Jurnal Komputer Terapan, 9(1), 15–23.

Prana Walidin, A., et al. (2025). Kali Linux sebagai alat analisis keamanan jaringan melalui penggunaan Nmap, Wireshark, dan Metasploit.

Ramadhan, M. F., & Hakim, A. R. (2023). Analisis keamanan jaringan menggunakan metode port scanning dan vulnerability assessment berbasis Nmap. Jurnal Teknologi Informasi dan Komputer, 9(2), 145–154. https://doi.org/10.30865/jtik.v9i2.5123

Ramli, A. F., & Prasetyo, Y. (2022). Pengembangan sistem deteksi port scanning secara real-time menggunakan Snort. JATI: Jurnal Mahasiswa Teknik Informatika, 6(2), 140–148.

Ripai, R., Pari, R. A., Sidik, F., Shandy, S. V., & Mahardika, F. (2025). Implementasi layanan Cloudflare sebagai mitigasi terhadap ancaman pemindaian dan eksploitasi siber menggunakan Nmap dan Metasploit. Sudo Jurnal Teknik Informatika, 4(1), 40–49. https://doi.org/10.56211/sudo.v4i1.902

Saputra, D., & Hartono, L. (2021). Studi komparasi alat pemindaian port: Zenmap vs Angry IP Scanner. JTIT: Jurnal Teknologi Informasi dan Terapan, 4(1), 55–64.

Saputra, D. H., Nugroho, A., & Ridwan, M. (2024). Perancangan aplikasi GUI untuk pemindaian port berbasis Python dan Nmap. Jurnal Informatika Polinema, 10(1), 88–97. https://doi.org/10.33795/jip.v10i1.812

Setiawan, R., & Hidayat, T. (2021). Analisis keamanan jaringan terhadap serangan port scanning menggunakan intrusion detection system. JUTIF: Jurnal Teknik Informatika, 5(1), 45–53.

Sudirman, D., & Yaqin, A. N. (2021). Network penetration dan security audit menggunakan Nmap. SATIN: Sains dan Teknologi Informasi, 7(1), 32–44. https://doi.org/10.33372/stn.v7i1.702

Wijaya, A. K., Firmansyah, R., & Hidayat, N. (2023). Pengembangan sistem monitoring keamanan jaringan berbasis web menggunakan Nmap. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 7(1), 25–34. https://doi.org/10.29207/resti.v7i1.4210