Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

Comparison of Port Scanning, Vulnerability Scanning, and Penetration Testing Combinations for Network Vulnerability Detection in GNS3 Testbed

Rusdianto[*1], Raka Yusuf[2]

[1,2]Computer Science, Mercu Buana University, Indonesia

Email: [1]rusdi6219@gmail.com

Received : Jun 19, 2025; Revised : Jul 12, 2025; Accepted : Jul 15, 2025; Published : Oct 21, 2025

Abstract

Network security faces significant challenges due to the increasing number and complexity of system vulnerabilities. This study aims to develop and evaluate a full combination method (ABC) integrating port scanning (Nmap), vulnerability scanning (OpenVAS), and penetration testing (Metasploit), and compare it with partial combinations (AB, BC, AC) for more effective vulnerability detection. Using a quantitative experimental approach within a controlled GNS3 TestBed, three key indicators were analyzed: number of vulnerabilities detected, detection time, and exploit validity. Experimental results show that the ABC method detected 62 potential vulnerabilities, including 11 high and medium severity CVEs, matching the AB method but significantly outperforming AC, which detected none. In terms of detection time, the ABC method achieved a balanced performance at 91 minutes, which is 31.5% faster than AB (133 minutes), while maintaining full exploit validation. Notably, the ABC method successfully validated 100% of critical vulnerabilities using Metasploit, confirming the practical applicability and reliability of the integrated approach compared to dual combinations. Overall, the findings demonstrate that the full combination method (ABC) offers superior accuracy and comprehensiveness in detecting and validating network vulnerabilities. This research contributes to cybersecurity practices by proposing an integrated detection workflow that effectively balances speed and depth of analysis, setting a practical benchmark for vulnerability detection systems applicable to both simulated and real-world network environments.

Keywords : *GNS3, Network Security, Penetration Testing, Port Scanning, Vulnerability Scanning.*

1. PENDAHULUAN

Keamanan jaringan menghadapi tantangan yang semakin kompleks dengan meningkatnya jumlah kerentanan dan serangan siber yang lebih canggih[1]. Serangan siber terutama yang memanfaatkan celah dalam jaringan semakin berkembang menjadi lebih kompleks dan beragam, sehingga keamanan jaringan kini menghadapi tantangan yang semakin rumit karena keterbatasan dalam pengelolaan risiko keamanan[2]. Data yang diperoleh dari laporan Skybox Vulnerability and Threat Trends Report 2024 menunjukkan peningkatan signifikan dalam identifikasi kerentanan, dengan 30.927 CVE baru terdaftar pada tahun 2023, meningkat 17% dibandingkan tahun sebelumnya[3]. Sebanyak 50% dari kerentanan ini diklasifikasikan sebagai berisiko tinggi atau kritis, tetapi lebih dari 25% dieksploitasi pada hari yang sama ketika kerentanan tersebut dipublikasikan[4].

Berbagai pendekatan metode telah dikembangkan untuk mendeteksi kerentanan jaringan, antara lain melalui metode port scanning, vulnerability scanning, dan penetration testing[5], [6]. Namun, dalam praktiknya, pendekatan-pendekatan ini umumnya digunakan secara terpisah, sehingga menghasilkan analisis yang parsial dan kurang menyeluruh[7], [8]. Metode port scanning seperti yang dilakukan menggunakan Nmap efektif dalam mengidentifikasi layanan dan port terbuka pada perangkat jaringan[9], [10], tetapi tidak memberikan informasi mendalam mengenai kerentanannya. Di sisi lain, OpenVAS sebagai alat vulnerability scanning terbukti memiliki akurasi tinggi dalam mendeteksi

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

kerentanan berdasarkan basis data CVE dan skor CVSS [2], namun tidak dapat memastikan apakah kerentanan tersebut benar-benar dapat dieksploitasi. Sementara itu, Metasploit dapat sebagai alat penetration testing mampu melakukan validasi terhadap eksploitasi kerentanan [11], tetapi akan kurang optimal jika tidak diawali dengan proses pemetaan layanan dan analisis kerentanan yang sistematis[12].

Celah utama yang muncul adalah kurangnya pendekatan yang mengkombinasikan ketiga metode tersebut untuk deteksi kerentanan jaringan[13]. Metode yang diterapkan secara terpisah sering kali menghasilkan data yang kurang komprehensif dalam memprioritaskan risiko kerentanan yang harus ditangani, sehingga dapat menyebabkan adanya celah dalam analisis serta pengambilan keputusan keamanan yang tepat[14]. Kondisi ini menjadi semakin kritis seiring meningkatnya jumlah dan kecepatan eksploitasi kerentanan baru yang ditemukan setiap tahun.

Hal ini menjadi celah penelitian (research gap) yang signifikan, dimana terbatasnya penelitian mengenai penerapan kombinasi metode ini dalam lingkungan TestBed GNS3 semakin memperbesar ketidakseimbangan dalam praktik dan pengembangan keamanan jaringan [2], [15]. Sementara sebagian besar penelitian terdahulu hanya menekankan keefektifan masing-masing metode secara individual atau pada kombinasi parsial, penelitian ini fokus pada pendekatan sistematis yang menggunakan metode kombinasi penuh (ABC) dan kombinasi parsial (AB, BC, AC) di lingkungan TestBed GNS3. Hal ini dilakukan untuk menghasilkan deteksi kerentanan yang lebih komprehensif, valid, dan realistis terhadap skenario jaringan sebenarnya. Meskipun penelitian sebelumnya telah mengevaluasi metode individual, penelitian terbatas telah dilakukan untuk membandingkan secara sistematis kombinasi teknik pemindaian dan pengujian dalam lingkungan terkendali.

Penelitian ini dapat mengisi celah tersebut dengan mengembangkan dan mengimplementasikan kombinasi antara metode port scanning, vulnerability scanning, dan penetration testing dalam mendeteksi kerentanan jaringan[16]. Proses ini dilakukan dalam lingkungan TestBed berbasis perangkat lunak GNS3, yang memungkinkan pengujian dilakukan tanpa risiko terhadap infrastruktur jaringan nyata[17]. Alat-alat yang digunakan dalam kombinasi ini meliputi Nmap untuk port scanning, OpenVAS untuk vulnerability scanning, serta Metasploit untuk penetration testing yang digunakan secara bersamaan guna memberikan pendekatan yang lebih komprehensif. Penelitian ini juga akan membandingkan antara metode kombinasi penuh (ABC) dan dengan kombinasi parsial (AB, BC, AC) dalam hal jumlah kerentanan yang terdeteksi, tingkat keparahan kerentanan, waktu deteksi, serta validitas eksploitasi.

Tujuan dari penelitian ini adalah untuk mengembangkan dan mengimplementasikan metode deteksi kerentanan jaringan melalui kombinasi tiga metode utama dalam satu kerangka alur terpadu, serta untuk mengevaluasi metode kombinasi penuh dibandingkan dengan kombinasi parsial dalam lingkungan TestBed. Melalui pendekatan komparatif ini, diharapkan dapat diperoleh pemahaman yang lebih menyeluruh mengenai kemampuan masing-masing kombinasi metode, sekaligus menjadi dasar bagi pengembangan sistem deteksi kerentanan yang lebih efisien dan akurat[18], [19], [20].

Penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan keamanan jaringan melalui beberapa manfaat utama[21], [22]. Pertama, memberikan kontribusi terhadap ilmu pengetahuan dalam deteksi kerentanan jaringan, penelitian ini diharapkan mampu memberikan kontribusi terhadap bidang keamanan jaringan yang lebih baik tentang mengkombinasikan ketiga metode deteksi kerentanan dalam satu kerangka alur terpadu[23]. Kedua, menjadi referensi empiris bagi penelitian selanjutnya, dimana penelitian ini diharapkan dapat menjadi acuan empiris dengan tujuan memberikan manfaat kepada praktisi dalam menentukan kombinasi alat pemindaian kerentanan jaringan yang sesuai dengan kebutuhan dan persyaratan yang spesifik[24]. Penelitian ini diharapkan menjadi salah satu pendekatan yang belum banyak diimplementasikan maupun dikaji secara sistematis pada lingkungan terkendali seperti TestBed GNS3.

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

2. METODOLOGI PENELITIAN

2.1. Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen berbasis TestBed di lingkungan GNS3, sehingga pengujian dapat dilakukan secara aman tanpa risiko terhadap infrastruktur jaringan nyata[25], [26]. Tujuannya adalah mengembangkan dan mengimplementasikan kombinasi metode deteksi kerentanan jaringan, meliputi port scanning (Nmap), vulnerability scanning (OpenVAS), dan penetration testing (Metasploit). Penelitian membandingkan kombinasi penuh (ABC) dengan kombinasi parsial (AB, BC, AC) untuk menjawab perumusan masalah mengenai pengembangan metode kombinasi yang komprehensif dalam deteksi kerentanan jaringan. Pendekatan eksperimen ini dirancang untuk menghasilkan data yang valid dan relevan, sehingga memberikan solusi yang dapat diimplementasikan dalam skenario nyata dengan sistem deteksi kerentanan yang lebih menyeluruh dan akurat.

2.2. Desain Penelitian

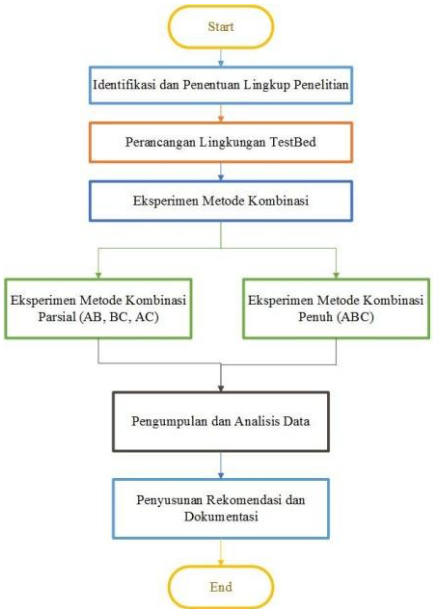
Penelitian ini dirancang untuk mengembangkan, mengimplementasikan, dan membandingkan metode kombinasi penuh (ABC) dengan kombinasi parsial (AB, BC, AC) dalam mendeteksi kerentanan jaringan menggunakan TestBed berbasis GNS3. Desain penelitian dimulai dengan identifikasi dan penentuan lingkup penelitian yang mencakup topologi jaringan, alat yang digunakan (Nmap, OpenVAS, dan Metasploit), serta batasan lingkungan TestBed. Selanjutnya dilakukan perancangan lingkungan TestBed menggunakan perangkat lunak GNS3 dengan topologi yang mencakup perangkat jaringan seperti router dan endpoint untuk mendukung eksperimen keamanan tanpa risiko terhadap jaringan nyata[27]. Setiap kombinasi metode memiliki alur kerja teknis seperti pada tabel 1, sebagai berikut:

Tabel 1. Ringkasan Metode Kombinasi

Metode Kombinasi	Tools Digunakan	Deteksi Port	Deteksi Kerentanan	Validasi Eksploitasi	Output
AB	Nmap + OpenVAS	✓	✓	✗	Jumlah kerentanan & skor CVSS
BC	OpenVAS + Metasploit	✗	✓	✓	Jumlah kerentanan & kerentanan tervalidasi
AC	Nmap + Metasploit	✓	✗	✓	Kerentanan tervalidasi langsung
ABC	Nmap + OpenVAS + Metasploit	✓	✓	✓	Jumlah kerentanan, skor CVSS, validitas eksploitasi

Tahap eksperimen dilakukan pada dua kategori metode, yaitu metode kombinasi parsial yang terdiri dari AB (Port Scanning + Vulnerability Scanning), BC (Vulnerability Scanning + Penetration Testing), dan AC (Port Scanning + Penetration Testing), serta metode kombinasi penuh (ABC) yang mengintegrasikan ketiga metode dalam satu alur kerja terkombinasi. Data yang diperoleh dari kedua kategori metode tersebut kemudian dianalisis secara kuantitatif menggunakan metrik indikator yang telah ditentukan, mencakup perbandingan jumlah kerentanan yang teridentifikasi, waktu deteksi, serta validitas eksploitasi. Alur desain penelitian ini dapat dilihat pada Gambar 1 sebagai berikut.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917



Gambar 1. Desain Alur Penelitian

2.3. Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui eksperimen berbasis kuantitatif di lingkungan TestBed GNS3 dengan mengimplementasi dan membandingkan metode kombinasi penuh (ABC) dengan metode parsial (AB, BC, AC). Data yang dikumpulkan meliputi jumlah kerentanan yang terdeteksi, tingkat keparahan kerentanan, waktu deteksi, dan validitas eksploitasi. Pada tahap awal, pengumpulan data dilakukan secara parsial dimana metode AB menggunakan port yang teridentifikasi Nmap sebagai input OpenVAS untuk mendeteksi kerentanan, metode BC menguji validitas kerentanan OpenVAS melalui Metasploit, dan metode AC menggunakan data port scanning langsung untuk penetration testing. Tahap berikutnya adalah eksperimen metode kombinasi penuh (ABC) dengan alur kerja berurutan yang memungkinkan deteksi lebih komprehensif dan mengurangi pengulangan data. Seluruh data yang dihasilkan dicatat menggunakan catatan manual selama proses pengujian untuk memastikan kelengkapan data empiris yang mendukung perbandingan pendekatan metode kombinasi dengan metode parsial

2.4. Analisis Data Penelitian

Penelitian ini menggunakan analisis data untuk mengembangkan serta membandingkan kombinasi metode penuh (ABC) dan kombinasi parsial (AB, BC, AC) dalam mendeteksi kerentanan jaringan. Data diperoleh melalui eksperimen pada tiga kombinasi parsial yaitu AB (Port Scanning + Vulnerability Scanning), BC (Vulnerability Scanning + Penetration Testing), AC (Port Scanning + Penetration Testing), dan satu kombinasi penuh ABC yang mengintegrasikan ketiga metode secara menyeluruh. Data yang dikumpulkan meliputi jumlah kerentanan yang terdeteksi, tingkat keparahan kerentanan berbasis skor CVSS (rendah, sedang, tinggi, dan kritis), waktu deteksi kerentanan, dan tingkat validitas eksploitasi berdasarkan keberhasilan penetrasi menggunakan Metasploit.

Analisis dilakukan menggunakan pendekatan analisis deskriptif untuk menggambarkan data eksperimen secara kuantitatif dan analisis komparatif untuk membandingkan metode kombinasi penuh dengan kombinasi parsial. Analisis deskriptif menghasilkan gambaran mengenai jumlah kerentanan terdeteksi per metode, distribusi tingkat keparahan kerentanan, dan waktu deteksi pada setiap metode. Sementara itu, analisis komparatif dilakukan dengan membandingkan jumlah kerentanan yang terdeteksi, waktu deteksi, dan persentase keberhasilan eksploitasi kerentanan antar metode.

- Equation (1): Perbandingan Jumlah Kerentanan Terdeteksi

$$P = \frac{Jumlah_{ABC} - Jumlah_{Parsial}}{Jumlah\ Parsial} \times 100\% \quad (1)$$

Equation (1) digunakan untuk menghitung selisih jumlah kerentanan yang terdeteksi antara metode ABC dan kombinasi lainnya.

- Equation (2): Perbandingan Waktu Deteksi Kerentanan

$$W_{eff} = \frac{Waktu_{Parsial} - Waktu_{ABC}}{Waktu\ Parsial} \times 100\% \ (2)$$

Equation (2) digunakan untuk menentukan seberapa cepat metode ABC dibanding metode lain dalam hal waktu deteksi.

- Equation (3): Perbandingan Validitas Eksploitasi Kerentanan

$$Validitas_{Eksploitasi} = \frac{Validitas_{ABC} - Validitas_{Parsial}}{Validitas\ Parsial} \times 100\% \quad (3)$$

Equation (3) menunjukkan persentase validasi eksploitasi terhadap kerentanan yang diuji.

Hasil analisis diharapkan menunjukkan bahwa metode kombinasi penuh (ABC) mampu mendeteksi lebih banyak kerentanan, dan memiliki validitas eksploitasi yang lebih tinggi dibandingkan metode kombinasi parsial. Analisis ini memberikan bukti empiris mengenai keunggulan pendekatan kombinasi dalam menghasilkan hasil deteksi kerentanan yang lebih komprehensif.

3. HASIL DAN PEMBAHASAN

3.1. Gambaran Umum Penelitian

Penelitian ini dilakukan pada sebuah lingkungan simulasi jaringan berbasis GNS3 (Graphical Network Simulator-3), yang dirancang sebagai TestBed untuk mensimulasikan infrastruktur jaringan. Tujuan dari pengujian ini adalah mengkombinasi serta membandingkan metode Port Scanning, Vulnerability Scanning, dan Penetration Testing dalam mendeteksi kerentanan jaringan dengan pendekatan yang komprehensif dan terstruktur. Topologi yang digunakan dirancang terdiri atas beberapa router, segmen jaringan internal, serta dua endpoint utama, yaitu Server Linux Debian dan Kali Linux, yang mewakili target dan penyerang. Topologi jaringan terdiri atas Deskripsi Komponen Utama, yaitu.

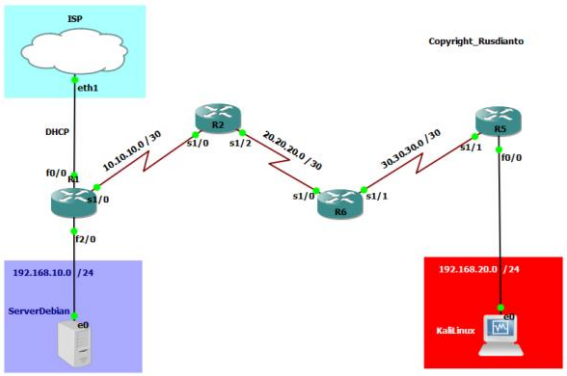
3.1.1. Server Debian (Target Sistem)

Server debian dikonfigurasi sebagai sistem target yang menjalankan berbagai layanan jaringan aktif. Server debian berperan sebagai target dari deteksi kerentanan. Server ini dikonfigurasi dengan berbagai layanan aktif seperti HTTP, FTP, SSH, dan layanan-layanan lainnya yang memungkinkan dilakukannya deteksi kerentanan jaringan sehingga dapat diuji eksploitasi.

3.1.2. Kali Linux (Host Penyerang)

Kali Linux merupakan sistem operasi berbasis Debian yang dirancang khusus untuk keperluan mendeteksi kerentanan jaringan. Sistem ini bertindak sebagai attacker (penyerang) yang menjalankan alat-alat metode deteksi kerentanan seperti Nmap, OpenVAS, dan Metasploit. Mesin ini akan digunakan untuk menjalankan serangkaian metode pemindaian dan pengujian kerentanan terhadap Server Debian.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917



Gambar 2. Topologi Jaringan TestBed GNS-3

Topologi ini dirancang untuk memungkinkan dilakukannya pengujian dengan tiga kombinasi metode, baik secara parsial (AB, BC, AC) maupun kombinasi penuh (ABC), dalam satu alur kerja eksperimen. Penggunaan GNS3 sebagai testbed lingkungan jaringan memberikan fleksibilitas dalam merancang dan memodifikasi topologi untuk dapat mengombinasikan serta membandingkan ketiga metode.

3.2. Hasil Eksperimen Metode Kombinasi Parsial (AB, BC, AC)

Pada bagian ini menguraikan hasil pengujian penelitian dengan pendekatan kombinasi parsial dari tiga metode kombinasi (AB, BC, AC) untuk mendeteksi kerentanan pada sistem target.

3.2.1. Hasil Metode AB (Port Scanning + Vulnerability Scanning)

Pada hasil penelitian tahap ini, dilakukan eksperimen menggunakan metode kombinasi parsial, yaitu AB (Port Scanning + Vulnerability Scanning). Proses ini pertama diawali dengan pemindaian port menggunakan Nmap untuk mengidentifikasi port terbuka dan layanan yang berjalan, yang dimana hasilnya kemudian digunakan sebagai input untuk analisis kerentanan lanjutan menggunakan OpenVAS. Proses ini diawali dengan Nmap yang mengidentifikasi host aktif pada rentang jaringan 192.168.10.0/24 dan selanjutnya melakukan port scanning pada host target 192.168.10.11. Hasil pemindaian Nmap menunjukkan tujuh port TCP terbuka. Nmap juga berhasil mendeteksi sistem operasi target sebagai Linux kernel 4.x/5.x. Gambar 3 menunjukkan hasil pemindaian port menggunakan Nmap.

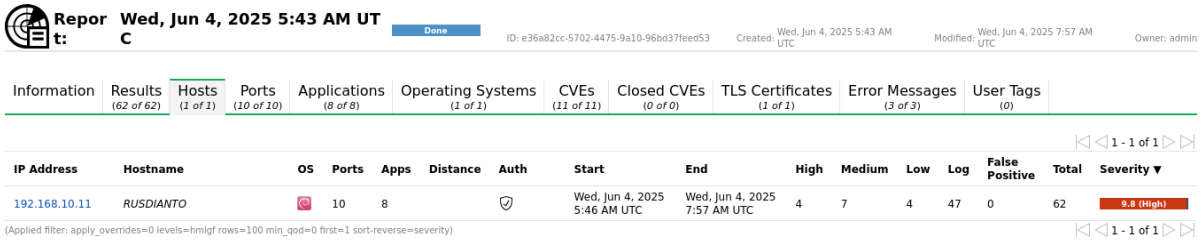
```
Nmap scan report for 192.168.10.11
Host is up (0.091s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
10000/tcp open  snet-sensor-mgmt
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Uptime guess: 35.831 days (since Tue Apr 29 01:31:32 2025)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   14.06 ms 192.168.20.1
2   45.22 ms 30.30.30.1
3   55.52 ms 20.20.20.1
4   75.75 ms 10.10.10.1
5   86.22 ms 192.168.10.11

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.88 seconds
           Raw packets sent: 40 (2.322KB) | Rcvd: 20 (1.530KB)
```

Gambar 3. Hasil Pemindaian Nmap AB

Hasil Nmap kemudian digunakan sebagai input untuk OpenVAS. Pemindaian OpenVAS dilakukan selama 2 jam 13 menit. OpenVAS berhasil mengidentifikasi 62 kerentanan dengan berbagai

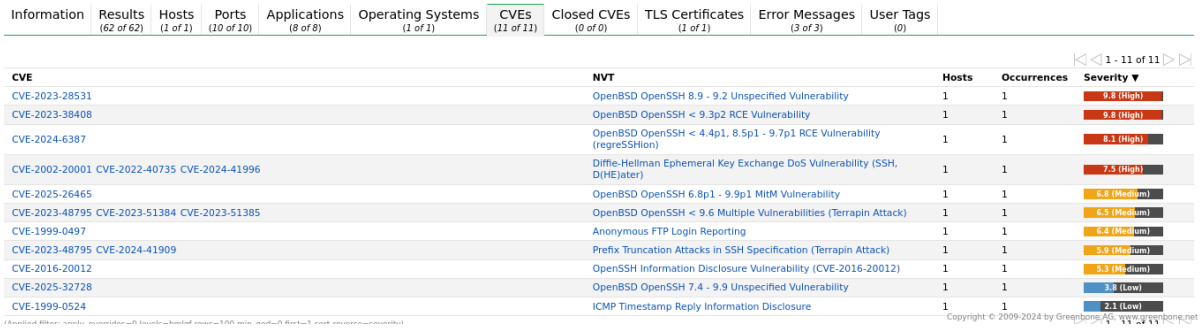
Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

tingkat keparahan. Rincian kerentanan berdasarkan tingkat keparahan adalah sebagai berikut: 4 kerentanan tingkat Tinggi (High), 7 kerentanan tingkat Sedang (Medium), dan 4 kerentanan tingkat Rendah (Low), seperti yang terlihat pada Gambar 4.



Gambar 4. Hasil Scanning Host OpenVas AB

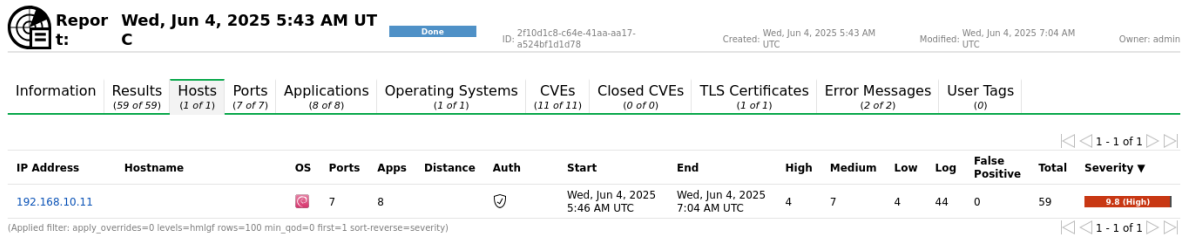
Kerentanan tertinggi teridentifikasi pada port 22/tcp (SSH) dengan skor keparahan 9.8 (High) dan port 21/tcp (FTP) dengan skor 6.4 (Medium). Pada Gambar 5 analisis lebih lanjut menunjukkan kerentanan kritis pada layanan SSH, termasuk dua kerentanan Remote Code Execution (RCE) yang dapat dieksploitasi untuk mendapatkan akses shell. Selain itu, terdeteksi pula kerentanan terkait login anonim pada FTP dan serangan Terrapin pada SSH.



Gambar 5. Hasil CVE OpenVAS AB

3.2.2. Hasil Metode BC (Vulnerability Scanning + Penetration Testing)

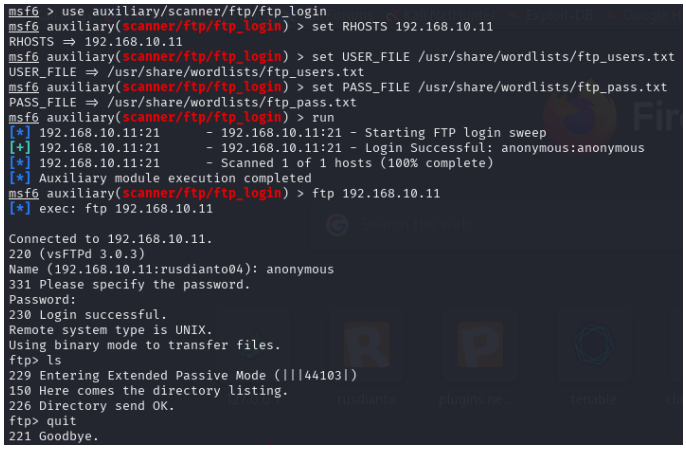
Pada hasil tahap dengan OpenVAS yang memindai host target 192.168.10.11. Pada Gambar 6 menunjukkan hasil pemindaian ini memerlukan waktu 1 jam 20 menit dan berhasil mendeteksi total 59 kerentanan. Fokus validasi eksploitasi diarahkan pada layanan SSH (port 22) skor keparahan 9.8 (High) dan FTP (port 21) skor 6.4 (Medium), karena kerentanan ini dianggap paling kritis dan berpotensi memberikan akses ke sistem.



Gambar 6. Hasil Scanning Host OpenVas BC

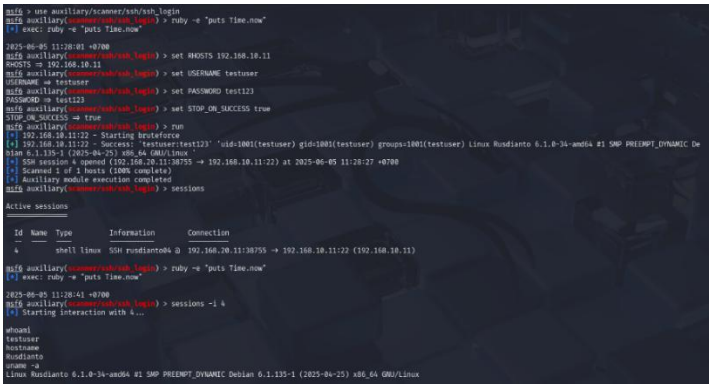
Kerentanan utama yang menjadi target validasi adalah kemungkinan Remote Code Execution (RCE) pada SSH dan login anonim pada FTP. Pengujian eksploitasi menggunakan Metasploit berhasil memvalidasi kerentanan login anonim pada FTP (CVE-1999-0497). Gambar 7 menunjukkan keberhasilan validasi kerentanan FTP.

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917



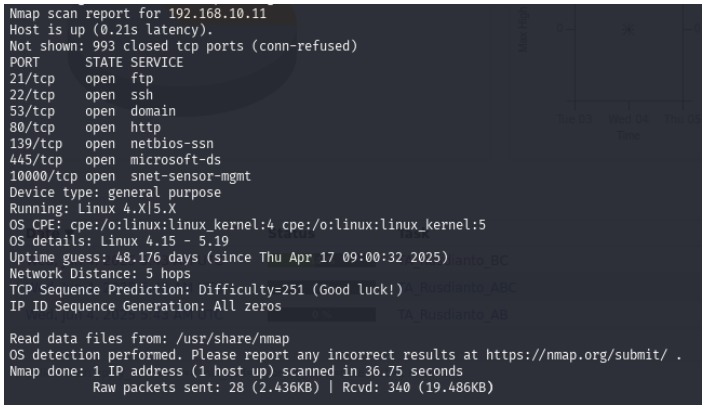
Gambar 7. Hasil Eksploitasi FTP BC

Untuk layanan SSH, serangan brute force menggunakan Metasploit berhasil menembus keamanan sistem dengan kredensial "testuser":"test123" dan mendapatkan sesi shell aktif. Keberhasilan ini mengonfirmasi akses penuh ke sistem target melalui SSH. Gambar 8 menampilkan bukti keberhasilan penetrasi eksploitasi SSH.


Gambar 8. Hasil Eksploitasi SSH BC

3.2.3. Hasil Metode AC (Port Scanning + Penetration Testing)

Pendekatan ini berfokus pada efisiensi dengan melewati pemindaian kerentanan mendalam OpenVAS, langsung menggunakan informasi Nmap untuk eksploitasi dengan metasploit. Pemindaian Nmap selesai dalam 36.75 detik dan berhasil mengidentifikasi tujuh port TCP terbuka pada host target 192.168.10.11 seperti yang ditunjukkan pada Gambar 9. Layanan FTP (port 21) dan SSH (port 22) dipilih sebagai target utama berdasarkan hasil port scanning.



Gambar 9. Hasil Pemindaian Port Scanning Nmap AC

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

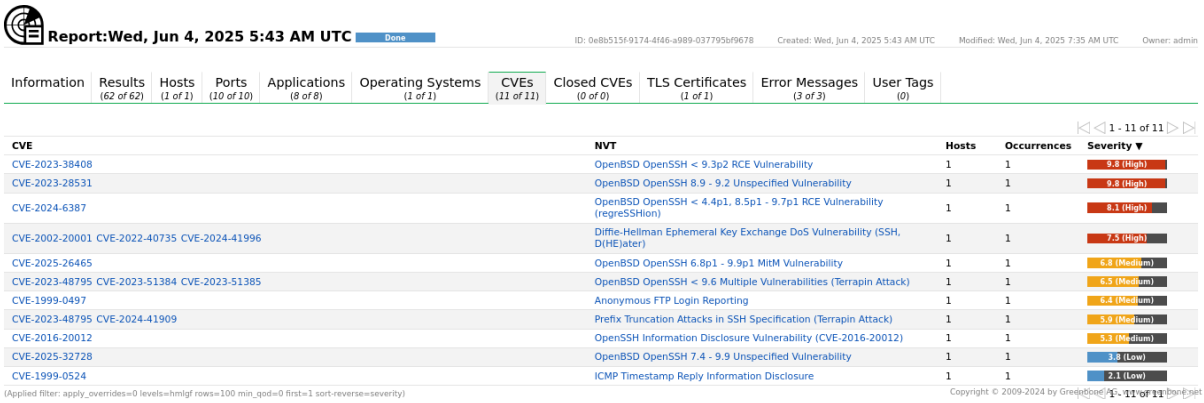
Pengujian Metasploit berhasil mendapatkan akses anonim pada FTP dengan kredensial "anonymous:anonymous", mengkonfirmasi kerentanan konfigurasi. Untuk SSH, serangan brute force menggunakan Metasploit berhasil menembus sistem dengan kredensial "testuser:test123", memberikan kendali penuh atas host Rusdianto melalui sesi shell interaktif. Gambar 10 menunjukkan keberhasilan akses SSH pada metode AC.

Gambar 10. Hasil Eksploitasi SSH AC

3.3. Hasil Eksperimen Metode Kombinasi Penuh (ABC)

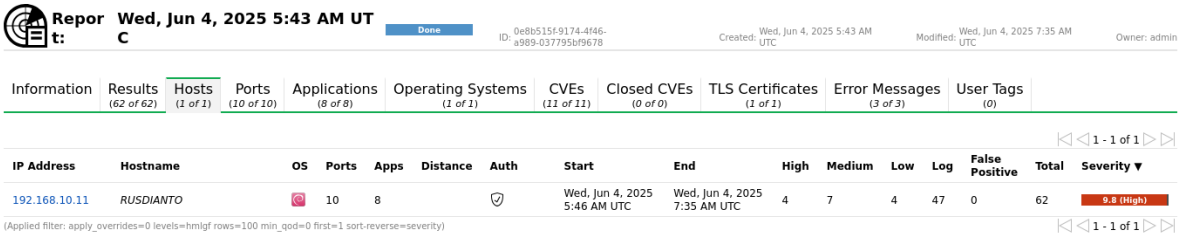
Pada hasil metode kombinasi penuh (ABC) mengkombinasikan ketiga tahapan (Nmap, OpenVAS, dan Metasploit) ke dalam satu alur kerja yang terintegrasi. Tahapan dimulai dengan Nmap untuk identifikasi host aktif dan layanan yang berjalan, dilanjutkan dengan OpenVAS untuk pemindaian kerentanan terfokus berdasarkan hasil Nmap, dan diakhiri dengan Metasploit untuk memvalidasi kerentanan berisiko tinggi yang ditemukan OpenVAS melalui upaya eksploitasi.

Proses deteksi pada host target 192.168.10.11 dimulai dengan Nmap yang memakan waktu 28.08 detik dan dengan 7 port kerentanan yang terdeteksi. Hasil Nmap ini kemudian diteruskan ke OpenVAS. Pemindaian OpenVAS memerlukan waktu 1 jam 31 menit dan mengidentifikasi total 62 temuan kerentanan. Rincian kerentanan ini mencakup 4 kerentanan tingkat Tinggi (High), 7 kerentanan tingkat Sedang (Medium), dan 4 kerentanan tingkat Rendah (Low). Layanan SSH pada port 22/tcp menjadi titik paling tinggi dengan skor keparahan 9.8 (High), mengindikasikan potensi risiko yang signifikan. Gambar 11 menunjukkan hasil scan OpenVAS pada metode ABC, sedangkan Gambar 12 menampilkan dashboard OpenVAS yang merangkum hasil pemindaian.



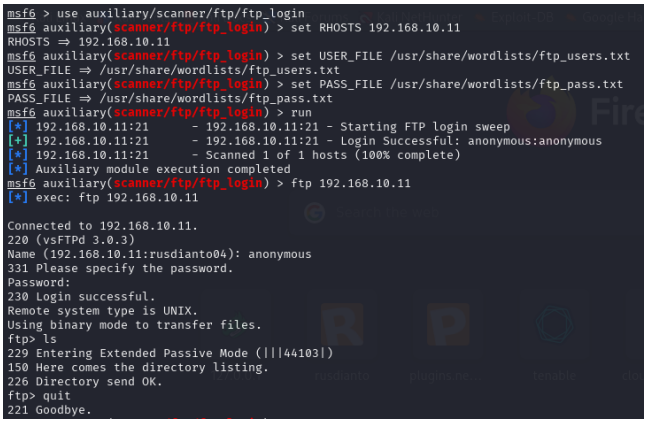
Gambar 11. Hasil Scan OpenVas CVE ABC

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917



Gambar 12. Hasil Scan OpenVas ABC

Validasi eksploitasi menggunakan Metasploit dilakukan terhadap kerentanan yang terdeteksi oleh OpenVAS. Validasi FTP (Port 21): Menggunakan modul auxiliary/scanner/ftp/ftp_login, pengujian berhasil memvalidasi kerentanan login anonim dengan kredensial "anonymous:anonymous". Ini membuktikan bahwa host target memiliki kesalahan konfigurasi yang fatal, memungkinkan akses tidak sah. Gambar 13 menunjukkan keberhasilan validasi eksploitasi kerentanan FTP.



Gambar 13. Hasil Validasi Kerentanan FTP (Login Anonim) ABC

Validasi SSH (Port 22): Menggunakan modul auxiliary/scanner/ssh/ssh_login, pengujian brute force berhasil mendapatkan akses sistem dengan kredensial lemah "testuser:test123". Keberhasilan ini menghasilkan akses shell pada mesin target, mengkonfirmasi kerentanan pada layanan SSH. Gambar 14 menampilkan keberhasilan validasi kerentanan SSH.

Gambar 14. Hasil Validasi Kerentanan SSH (Brute Force) ABC

3.4. Analisis Komparatif Hasil Penelitian

Penelitian ini membandingkan antara metode kombinasi penuh (ABC) dengan kombinasi parsial (AB, BC, AC) berdasarkan tiga indikator utama: jumlah kerentanan yang terdeteksi, waktu deteksi, dan validitas eksploitasi. Analisis dilakukan untuk memberikan gambaran terkait keunggulan pendekatan terintegrasi da-lam mendeteksi kerentanan jaringan secara komprehensif

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

3.4.1. Perbandingan Jumlah Kerentanan Terdeteksi

Analisis perbandingan kuantitatif jumlah deteksi kerentanan yang ditemukan menunjukkan perbedaan antara metode kombinasi penuh (ABC) dengan masing-masing metode kombinasi parsial. Berdasarkan data hasil eksperimen, dapat dilihat pada Tabel 2 bahwa setiap metode memiliki kemampuan deteksi yang berbeda-beda.

Tabel 2. Hasil Perbandingan Jumlah Kerentanan Terdeteksi

Perbandingan	Jumlah ABC	Jumlah Parsial	Selisih	Persentase Perbedaan
ABC vs AB	62	62	0	0%
ABC vs BC	62	59	3	+5.08%
ABC vs AC	62	7	55	+785.71%

1. Perbandingan ABC vs AB

Metode ABC berhasil mendeteksi 62 kerentanan dengan kategorisasi 4 High, 7 Medium, dan 4 Low, sedangkan metode AB mengidentifikasi 62 kerentanan dengan jumlah yang sama. Kesamaan jumlah ini disebabkan karena kedua metode sama-sama menggunakan OpenVAS sebagai komponen utama dalam deteksi kerentanan. Meskipun jumlah total kerentanan yang terdeteksi sama, kualitas analisis pada metode ABC lebih unggul karena adanya tahap validasi eksploitasi yang memberikan konfirmasi empiris terhadap kerentanan yang terdeteksi. Metode ABC memiliki keunggulan dalam menghasilkan actionable results melalui validasi yang sistematis

2. Perbandingan ABC vs BC

Metode ABC mendeteksi 62 kerentanan, sementara metode BC mendeteksi 59 kerentanan. Perbedaan ini menunjukkan bahwa tahap awal port scanning (A) dalam metode ABC memberikan kontribusi penting dalam pemetaan komprehensif layanan target, yang kemudian memungkinkan OpenVAS melakukan pemindaian yang lebih terfokus dan menyeluruh

3. Perbandingan ABC vs AC

Metode ABC menunjukkan keunggulan dengan berhasil mendeteksi 62 kerentanan keamanan, dibandingkan dengan pendekatan AC yang terbatas pada validasi eksploitasi layanan spesifik. Meskipun metode AC menunjukkan untuk proses eksploitasi langsung, pendekatan ini memiliki keterbatasan dalam mengidentifikasi kerentanan yang memerlukan analisis mendalam melalui vulnerability scanning komprehensif. Pendekatan AC tidak berhasil mendeteksi satu pun Common Vulnerabilities and Exposures (CVE) karena metode yang diimplementasikan tidak melibatkan vulnerability scanner OpenVas.

3.4.2. Perbandingan Waktu Deteksi Kerentanan

Analisis perbandingan waktu yang diperlukan oleh setiap metode menunjukkan variasi waktu. Data waktu deteksi menunjukkan karakteristik yang berbeda untuk setiap pendekatan metode seperti yang ditunjukkan pada Tabel 3, sebagai berikut.

Tabel 3. Hasil Perbandingan Waktu Deteksi Kerentanan

Perbandingan	Waktu ABC (Menit)	Waktu Parsial (Menit)	Selisih (Menit)	Persentase Waktu
ABC vs AB	91	133	42	+31.58% lebih cepat
ABC vs BC	91	80	-11	-13.75% lebih lambat
ABC vs AC	91	0.6125	-90.39	-14758% jauh lebih lambat

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

1. Perbandingan ABC vs AB

Metode kombinasi penuh (ABC) lebih unggul dibandingkan metode parsial AB. Meskipun keduanya menggunakan alat yang sama (Nmap dan OpenVAS), alur kerja terkombinasi pada metode ABC, di mana hasil Nmap menjadi acuan bagi OpenVAS untuk tujuan validasi kerentanan, membuktikan mampu mengoptimalkan pemindaian deteksi kerentanan. Hal ini menunjukkan bahwa alur kerja yang terkombinasi penuh dapat mengoptimalkan proses pemindaian deteksi dibandingkan dengan hanya menjalankan Nmap dan OpenVAS secara terpisah tanpa tujuan eksploitasi.

2. Perbandingan ABC vs BC

Metode BC sedikit lebih cepat dibandingkan metode ABC. Pertama, metode ABC memiliki tahap awal tambahan yaitu pemindaian Nmap yang tidak ada pada BC. Kedua, saat OpenVAS pada metode ABC mendapatkan informasi dari Nmap, hasil pemindaiannya menjadi lebih luas atau mendalam pada port-port yang teridentifikasi, sehingga menambah durasi pemindaian dibandingkan metode BC yang mungkin melakukan pemindaian dengan konfigurasi default.

3. Perbandingan ABC vs AC

Terdapat perbedaan kecepatan antara metode AC dan ABC. Metode AC menunjukkan kecepatan tertinggi untuk tahap port scanning. Kecepatan ini dicapai karena metode AC menghilangkan tahap vulnerability scanning menggunakan OpenVAS, yang membutuhkan waktu lama. Metode ini langsung beralih dari identifikasi port ke upaya eksploitasi. Meskipun lebih cepat dari metode ABC, kelemahannya adalah metode AC tidak menyediakan analisis kerentanan yang mendalam.

3.4.3. Perbandingan Validitas Eksploitasi Kerentanan

Analisis validitas eksploitasi merupakan indikator untuk menilai dari setiap pendekatan metodologi. Studi perbandingan tingkat keberhasilan eksploitasi menunjukkan bahwa metode kombinasi penuh memiliki keunggulan dalam menghasilkan hasil yang dapat ditindaklanjuti *(actionable results)*. Dapat dilihat pada Tabel 4, hasil eksperimen ini memperlihatkan adanya variasi signifikan antara metode kombinasi penuh (ABC) dan metode parsial (AB, BC, AC). Hal ini mengindikasikan perbedaan fundamental dalam kualitas hasil deteksi dan validitas eksploitasi yang dihasilkan oleh setiap metode.

Tabel 4. Hasil Perbandingan Validitas Eksploitasi Kerentanan

Perbandingan	Validitas ABC	Validitas Parsial	Selisih	Persentase Validitas
ABC vs AB	100%	0% (Tidak diuji)	100%	Tidak terukur (karena AB tidak validasi)
ABC vs BC	100%	100%	0%	100% (Sama)
ABC vs AC	100%	100%	0%	100% (Sama)

1. Perbandingan ABC vs AB

Metode ABC menunjukkan keunggulan mutlak dalam validitas eksploitasi. Berbeda dengan metode AB yang hanya mengidentifikasi kerentanan tanpa validasi, ABC berhasil memvalidasi kerentanan kritis pada layanan SSH (CVE dengan skor 9.8) dan FTP (skor 6.4) melalui eksploitasi yang berhasil. Tingkat keberhasilan eksploitasi ABC mencapai 100% untuk kerentanan berisiko tinggi yang diuji.

Perbandingan antara kedua metode ini menyoroti perbedaan fundamental antara deteksi dan validasi. Metode AB berhasil mengidentifikasi 11 potensi kerentanan CVE, dengan tingkat keparahan High dan Medium. Namun, tanpa tahap eksploitasi, seluruh temuan ini berstatus potensial dan belum terbukti, yang dapat menimbulkan alert fatigue. Sebaliknya, metode ABC secara empiris mengkonfirmasi bahwa 2 dari 11 potensi kerentanan tersebut dapat dieksploitasi. Dari segi validitas,

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

metode ABC jelas lebih unggul karena menghasilkan laporan yang dapat ditindaklanjuti (actionable intelligence).

2. Perbandingan ABC vs BC

Kedua metode ABC dan BC, menunjukkan kapabilitas validasi eksploitasi yang identik, keduanya berhasil membuktikan dua kerentanan yang sama dengan tingkat keberhasilan eksploitasi 100% untuk target yang diuji. Rasio validitas keduanya pun setara. Ini berarti keunggulan metode ABC tidak terletak pada hasil akhir eksploitasi.

Namun, metode ABC memberikan konteks yang lebih lengkap karena pendekatannya dengan menggunakan ketiga metode. Metode ini memulai dengan tahap awal port scanning yang menggunakan Nmap untuk pemetaan permukaan serangan (attack surface mapping). Proses ini menyediakan pemetaan awal dan konteks situasional yang lengkap sebelum vulnerability scanning dilakukan. Sebaliknya, metode BC langsung memulai dengan vulnerability scanning, yang berpotensi menghilangkan konteks awal. Pendekatan ABC ini memungkinkan analisis risiko yang lebih akurat dan prioritas eksploitasi yang lebih tepat

3. Perbandingan ABC vs AC

Perbandingan ini antara efisiensi waktu dan validitas komprehensif. Metode AC, meskipun sangat cepat, hanya mampu memvalidasi dua kerentanan yang sama dengan metode ABC. Namun, validitas hasilnya terbatas dan tidak kontekstual. Keberhasilan metode AC disebabkan oleh penargetan kerentanan umum seperti login anonim dan kredensial lemah. Meskipun AC menunjukkan efisiensi waktu tertinggi dengan keberhasilan eksploitasi yang baik, metode ini memiliki keterbatasan dalam cakupan analisis.

Sebaliknya, ABC menghasilkan data eksploitasi yang lebih terfokus. Dengan demikian, meskipun jumlah kerentanan tervalidasi sama, kualitas dan cakupan validitas pada metode ABC lebih unggul. Ini karena validitasnya didasarkan pada analisis komprehensif awal, bukan semata-mata pada pengujian eksploitasi.

Sebagai rangkuman dari seluruh tahapan penelitian eksperimen yang telah dijelaskan sebelumnya, berikut disajikan pada Tabel 5 yang merangkum metric indicator hasil eksperimen dari masing-masing kombinasi metode (ABC, AB, BC, dan AC), berdasarkan tiga indikator utama: jumlah kerentanan yang terdeteksi, waktu deteksi, dan validitas eksploitasi.

Tabel 5. Ringkasan Hasil Perbandingan Kombinasi Metode

Metode Kombinasi	Jumlah Kerentanan	Waktu Deteksi (Menit)	Validitas Eksploitasi	False Positive	False Negative
AB	62 (11 CVE)	133	0% (tidak diuji)	Potensial ada	Potensial ada
BC	59 (10 CVE)	80	100% (2/2 eksploitasi)	Tidak ada	Sedikit
AC	7 (0 CVE)	0.61	100% (2/2 eksploitasi)	Tidak ada	Tinggi
ABC	62 (11 CVE)	91	100% (2/2 eksploitasi)	Tidak ada	Tidak ada

Potensi false positive teridentifikasi pada metode AB, karena hasil pemindaian OpenVAS menghasilkan deteksi sejumlah CVE tanpa adanya proses validasi eksploitasi, sehingga memungkinkan beberapa kerentanan yang terdeteksi tidak benar-benar dapat dimanfaatkan. Sementara itu, false negative paling tinggi terjadi pada metode AC, karena tidak dilakukan vulnerability scanning, sehingga

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

banyak potensi kerentanan tidak terdeteksi. Pada metode BC, risiko false negative relatif rendah, namun tetap ada karena tidak adanya proses pemetaan awal menggunakan port scanning dari Nmap, yang dapat menyebabkan sebagian layanan luput dari analisis OpenVAS.

4. DISKUSI

Penelitian ini secara kuantitatif membuktikan bahwa metode kombinasi penuh (ABC) yang mengkombinasikan Nmap, OpenVAS, dan Metasploit secara kombinasi merupakan pendekatan paling unggul untuk deteksi kerentanan jaringan. Hasil ini dikuatkan dengan analisis terhadap tiga indikator utama jumlah kerentanan, waktu deteksi, dan validitas eksploitasi, serta kemudian dibandingkan dengan penelitian-penelitian sebelumnya.

1. Jumlah Cakupan Deteksi Kerentanan

Metode ABC terbukti paling komprehensif, dengan 62 kerentanan terdeteksi, termasuk 11 CVE dengan tingkat keparahan High dan Medium. Ini menunjukkan kesamaan dalam jumlah kerentanan dengan metode AB, namun berbeda dari metode AC yang hanya mendeteksi 7 kerentanan tanpa satupun CVE. Hasil seperti ini dengan penelitian sebelumnya oleh Ahsan dan Rochmah[28], yang menegaskan bahwa penggunaan OpenVAS secara mendalam memungkinkan deteksi CVE dengan akurasi tinggi, namun tanpa kombinasi port scanning, cakupan bisa menjadi kurang optimal. Selain itu, keunggulan ABC dibanding BC yang mendeteksi 59 kerentanan juga mencerminkan dengan penelitian sebelumnya oleh Guruprasad [2], di mana deteksi kerentanan akan lebih maksimal ketika ada hal pemetaan layanan yang diberikan oleh port scanner seperti Nmap sebelum pemindaian kerentanan dilakukan. Secara keseluruhan, kelemahan pada metode AC yang tidak mendeteksi CVE disebabkan oleh tidak adanya tahap vulnerability scanning OpenVas, sesuai hasil analisis penelitian oleh Raza dan Jaison [1], yang menyebutkan bahwa pengujian penetrasi tanpa assessment awal rentan terhadap hasil yang tidak menyeluruh.

2. Waktu Deteksi

Dari segi waktu deteksi, metode ABC memberikan keseimbangan antara kecepatan dan kedalaman analisis kerentanan. Dengan total waktu 91 menit, metode ABC terbukti 31,58% lebih cepat dibandingkan metode AB (133 menit). Efisiensi waktu ini sejalan dengan studi penelitian oleh Pittman [9], yang meneliti perbedaan penggunaan sumber daya CPU, RAM, dan waktu di antara tools scanning, di mana kombinasi alat dapat mengurangi waktu proses. Meskipun metode AC menjadi yang tercepat (0,61 menit), tetapi analisis yang dihasilkan menjadi kurang menyeluruh. Hal ini membuat metodenya kurang bisa diandalkan untuk deteksi kerentanan yang mendalam. Penelitian sebelumnya oleh Roslan [14], juga menyoroti bahwa teknik pemindaian cepat seperti TCP SYN memiliki keterbatasan dalam melakukan pemindaian yang komprehensif.

3. Validitas Eksploitasi

Validitas eksploitasi adalah indikator di mana metode ABC menunjukkan hasil eksploitasi. Dengan tingkat keberhasilan 100% dalam memvalidasi kerentanan kritis (FTP dan SSH) menggunakan Metasploit, metode ABC mengubah hasil temuan kerentanan potensial menjadi bukti nyata dan actionable. Temuan ini konsisten dengan hasil penelitian oleh Raza dan Jaison [1], yang menyatakan pentingnya tahap penetration testing untuk memverifikasi hasil scanning guna menghindari false positives dan meningkatkan actionable intelligence. Walau metode BC dan AC juga menunjukkan validasi 100%, validitas eksploitasi pada metode ABC lebih unggul secara metodologis karena berdasarkan hasil pemindaian menyeluruh dan sistematis. Ini berbeda dari metode AC yang hanya mengeksploitasi pada layanan umum dengan kredensial lemah, seperti hasil penelitian sebelumnya oleh Lachkov et al. [29], bahwa eksistensi login anonim dan kredensial default sering kali menjadi target eksploitasi cepat namun tidak mencerminkan kedalaman analisis keamanan sistem.

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

Meskipun ABC menawarkan deteksi yang paling komprehensif, pendekatan ini juga memiliki kekurangan, yaitu memerlukan waktu deteksi paling lama di antara kombinasi lain, yang dapat memengaruhi penerapannya dalam sistem jaringan berskala besar yang memerlukan pemindaian cepat dan berkelanjutan. Dibandingkan metode konvensional berbasis satu metode, seperti hanya menggunakan OpenVAS, metode ABC memberikan keunggulan signifikan berupa validasi eksploitasi kerentanan yang membuat hasil deteksi lebih akurat dan actionable bagi administrator jaringan. Namun, kompleksitas konfigurasi, kebutuhan sumber daya lebih besar, serta tantangan skalabilitas menjadi faktor yang harus diperhatikan dalam implementasi nyata. Oleh karena itu, meskipun metode ABC sangat sesuai untuk audit keamanan menyeluruh atau pengujian periodik, penyesuaian perlu dilakukan agar dapat diintegrasikan secara efisien ke sistem deteksi kerentanan waktu nyata.

5. KESIMPULAN

Penelitian ini mengembangkan dan mengevaluasi metodologi deteksi kerentanan jaringan dengan membandingkan pendekatan kombinasi penuh (ABC) dan kombinasi parsial (AB, BC, AC) dalam lingkungan TestBed GNS3 yang terkontrol. Hasil menunjukkan bahwa metode ABC menjadi pendekatan yang paling unggul karena mampu menggabungkan kecepatan, kedalaman deteksi, serta validitas eksploitasi yang lebih dapat diandalkan dibandingkan metode parsial. Secara konseptual, metode ABC mengkombinasikan tiga tahapan penting port scanning, vulnerability scanning berbasis CVE, dan validasi eksploitasi nyata sehingga menghasilkan deteksi yang tidak hanya prediktif, tetapi juga konfirmatif. Meskipun metode ABC memerlukan waktu deteksi lebih lama dibandingkan metode paling cepat (AC), keunggulannya terletak pada cakupan deteksi yang lebih komprehensif dan hasil yang lebih actionable bagi administrator jaringan. Temuan ini juga menegaskan bahwa pendekatan terintegrasi seperti ABC lebih unggul dibandingkan metode konvensional berbasis satu teknik atau satu metode, seperti hanya menggunakan OpenVAS, yang hanya memberikan daftar potensi kerentanan tanpa konfirmasi eksploitasi. Dengan demikian, penelitian ini berkontribusi pada praktik keamanan siber dengan mengusulkan metodologi gabungan yang menyeimbangkan kecepatan dan kedalaman deteksi kerentanan, serta dapat mendukung perumusan kebijakan atau kerangka kerja audit keamanan nasional. Selain itu, studi ini menetapkan tolok ukur untuk metodologi deteksi kerentanan terintegrasi dalam penelitian keamanan siber, yang dapat dijadikan acuan oleh peneliti maupun praktisi. Adapun saran untuk penelitian selanjutnya adalah melakukan pengujian metode kombinasi penuh (ABC) pada lingkungan jaringan nyata berskala lebih besar, serta memperluas cakupan ke infrastruktur modern seperti cloud dan Internet of Things (IoT) agar hasilnya semakin relevan untuk implementasi di dunia nyata.

DAFTAR PUSTAKA

[1] S. Raza and F. Jaison, “A Comparative Study between Vulnerability Assessment and Penetration Testing,” *International Journal of Trend in Scientific Research and Development (IJTSRD)*, vol. 5, no. 3, pp. 1208–1211, Apr. 2021, doi: 10.46293/4N6/2021.03.02.08.

[2] H. S. Guruprasad, “Evaluation and Analysis of Vulnerability Scanners: Nessus and OpenVAS,” *International Research Journal of Engineering and Technology*, vol. 7, no. 5, pp. 2068–2073, Apr. 2020.

[3] “Vulnerability and Threat Trends Report 2024,” 2024. Accessed: Jun. 15, 2025. [Online]. Available: https://www.skyboxsecurity.com/resources/report/vulnerability-threat-trends-report-2024/

[4] Fortra, “2024 Penetration Testing Report,” 2024. Accessed: Jun. 18, 2025. [Online]. Available: https://static.fortra.com/core-security/pdfs/guides/fta-cs-2024-pen-testing-report-gd.pdf

[5] D. K. Adamsyach Prana Walidin, Fahra Pebiana Putri, “KALI LINUX SEBAGAI ALAT ANALISIS KEAMANAN JARINGAN MELALUI PENGGUNAAN NMAP, WIRESHARK,

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

DAN METASPLOIT," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, pp. 1188–1196, 2025, doi: https://doi.org/10.36040/jati.v9i1.12661.

[6] Hanafi, *Dasar Cyber Security dan Forensic*, 1st ed. Yogyakarta: Deepublish Publisher, 2022. Accessed: Jun. 04, 2025. [Online]. Available: https://eprints.amikom.ac.id/id/eprint/10688/

[7] D. Septian Firdaus and A. Hendri Hendrawan, "Analisis Keamanan Vulnerability pada Server Cloud Open Media Vault di Fakultas Teknik Universitas Ibn Khaldun Bogor," *Prosiding Semnastek*, vol. 16, Oct. 2019, Accessed: Jun. 12, 2025. [Online]. Available: jurnal.umj.ac.id/index.php/semnastek

[8] D. Bayu Rendro and W. Nugroho Aji, "ANALISIS MONITORING SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP (STUDI KASUS DI SMK NEGERI 1 KOTA SERANG)," *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer,* vol. 7, no. 2, pp. 108–115, Sep. 2020, doi: https://doi.org/10.30656/prosisko.v7i2.2522.

[9] J. M. Pittman, "A Comparative Analysis of Port Scanning Tool Efficacy," *arXiv preprint*, Mar. 2023, doi: https://doi.org/10.48550/arXiv.2303.11282.

[10] A. Riad, Imam, Kurniawan, *Forensik Jaringan dan Cloud*, 2nd ed. Yogyakarta: Diandra Kreatif, 2020. Accessed: Jun. 20, 2025. [Online]. Available: www.diandracreative.com

[11] F. Holik, J. Horalek, O. Marik, S. Neradova, and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," in *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, 2014, pp. 237–242. doi: 10.1109/CINTI.2014.7028682.

[12] R. Azani Akbar and H. Bayu Seta, "Pengujian Celah Keamanan Untuk Mengetahui Kerentanan Keamanan Jaringan Wireless Dengan Metode Penetration Testing Execution Standard (PTES) Pada PT. QWE," in *Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)*, Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA), Aug. 2022, pp. 991–1000.

[13] M. Anis, A. Hilmi, and E. Khujaemah, "Network Security Monitoring With Intrusion Detection System," *Jurnal Teknik Informatika (JUTIF)*, vol. 3, no. 2, pp. 249–253, 2022, doi: https://doi.org/10.20884/1.jutif.2022.3.2.117.

[14] F. H. Roslan, "A Comparative Performance of Port Scanning Techniques," *Journal of Soft Computing and Data Mining*, vol. 4, no. 2, pp. 43–51, Oct. 2023, doi: 10.30880/jscdm.2023.04.02.004.

[15] D. Sudirman and A. N. Yaqin, "Network Penetration dan Security Audit Menggunakan Nmap," *SATIN - Sains dan Teknologi Informasi*, vol. 7, no. 1, pp. 32–44, Jun. 2021, doi: 10.33372/stn.v7i1.702.

[16] M. Alhamed and M. M. H. Rahman, "A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions," *Applied Sciences (Switzerland)*, vol. 13, no. 12, Jun. 2023, doi: 10.3390/app13126986.

[17] S. Sunny and A. G. Christy, "COMPARISON OF TCP SCANNING TECHNIQUES USING NMAP," *J Pharm Negat Results*, vol. 13, no. 10, pp. 919–925, 2022, doi: 10.47750/pnr.2022.13.S10.104.

[18] W. A. binti W. M. T. Rukhiyah binti Adnan, "Implementing Penetration Testing in Simulation Environment," vol. 4, no. 2, pp. 1–8, 2023, doi: https://doi.org/10.61688/jev.v4i2.137.

[19] A. Agustinus and I. Sembiring, "WEBSITE VULNERABILITY TESTING USING THE PENETRATION TESTING METHOD REFERRING TO NIST SP 800 –155 (CASE STUDY (Astonprinter.com Domain))," *Jurnal Teknik Informatika (JUTIF)*, vol. 5, no. 6, pp. 1651–1662, 2024, doi: https://doi.org/10.52436/1.jutif.2024.5.6.3859.

[20] K. Božić, N. Penevski, and S. Adamović, "Penetration Testing and Vulnerability Assessment: Introduction, Phases, Tools and Methods," in *International Scientific Conference on Information Technology and Data Related Research-SINTEZA 2019*, Belgrade, Serbia: SINTEZA 2019, 2019, pp. 229–234. doi: 10.15308/sinteza-2019-229-234.

[21] A. Kejiou and G. Bekaroo, "A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs," *International Conference on Next Generation Computing Applications (NextComp)*, p. 1, Oct. 2022, doi: 10.1109/NextComp55567.2022.9932245.

Vol. 6, No. 5, October 2025, Page. 3526-3542
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.5.4917

[22] R. Abu Bakar and B. Kijsirikul, "Enhancing Network Visibility and Security with Advanced Port Scanning Techniques," *Sensors*, vol. 23, no. 17, pp. 1–27, Aug. 2023, doi: https://doi.org/10.3390/s23177541.

[23] K. N. Isnaini, ; Muhammad, H. Asyari, ; Sigit, F. Amrillah, and ; Didit Suhartono, "Vulnerability Assessment and Penetration Testing on Student Service Center System," *ILKOM Jurnal Ilmiah*, vol. 16, no. 2, pp. 161–171, Aug. 2024, doi: https://doi.org/10.33096/ilkom.v16i2.1969.161-171.

[24] M. Ayyas, A. Fauzi, and S. Widodo, "Studi Komparatif Teknik Analisis Keamanan Sistem Informasi e-Government: Penetration Testing VS Vulnerability Assessment," *SATIN - Sains dan Teknologi Informasi*, vol. 10, no. 1, pp. 25–34, Jun. 2024, doi: 10.33372/stn.v9i2.1000.

[25] I. G. P. K. Juliharta, I. K. Suwidiana, and I. P. C. Taruna, "VULNERABILITY ASSESSMENT SISTEM MANAJEMEN KEAMANAN INFORMASI STUDI KASUS SISTEM SIDARLING DAN JAGABAYA KOTA DENPASAR," *Jurnal Teknologi Informasi dan Komputer*, vol. 8, no. 4, pp. 354–358, 2022, doi: https://doi.org/10.36002/jutik.v8i4.2089.

[26] R. R and Y. Muin, "MikroTik Router Vulnerability Testing for Network Vulnerability Evaluation using Penetration Testing Method," *Int J Comput Appl*, vol. 183, no. 47, pp. 33–37, Jan. 2022, doi: 10.5120/ijca2022921878.

[27] S. Abdulaziz Alkhathlan, L. Hasan Alzahrani, S. Hamad Alfulayj, and S. Kamel Hussein, "A Comparative Study on Network Exploration and Performance Evaluation Techniques for Vulnerability Assessment Tools in Security Systems," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 26, no. 3, pp. 5–20, May 2024, doi: 10.9790/0661-2603020520.

[28] M. Ahsan and D. A. Rochmah, "Analisa Kerentanan Sistem Dengan Menerapkan Open Vulnerability Assessment System Menggunakan Greenbone Vulnerability Management (GVM)," *INFORMATIKA DAN TEKNOLOGI (INTECH)*, vol. 3, no. 2, pp. 23–29, Nov. 2022, doi: 10.54895/intech.v3i2.1509.

[29] P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *Journal of Web Engineering*, vol. 21, no. 7, pp. 2187–2208, Dec. 2022, doi: 10.13052/jwe1540-9589.2178