SAINTEK: Jurnal Sains, Teknologi & Komputer
Vol. 3, No. 1, Februari 2026, pp. 35 ~ 46

Evaluation and improvement of security using penetration testing (pentest) methods of host-based intrusion detection system (hids) and intrusion detection system (ids) at the Sei Sekambing C II village office

Mara Sakti Siregar[1], Furqan Khalidy[2], Mardiah[3]
[1,2,3]Universitas Nahdlatul Ulama Sumatera Utara, Indonesia
Email: marasaktisiregar44@gmail.com; furqan.unusu.iko@gmail.com; mardiahindin23@gmail.com

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat menuntut adanya sistem keamanan jaringan yang kuat dan andal, terutama pada instansi pemerintahan yang mengelola data penting masyarakat. Kantor Lurah Sei Sekambing C II telah memanfaatkan jaringan komputer untuk mendukung aktivitas pelayanan publik, namun masih menghadapi berbagai risiko keamanan jaringan, seperti akses ilegal, *malware*, dan kerentanan sistem. Penelitian ini bertujuan untuk mengevaluasi dan meningkatkan keamanan jaringan dengan menggunakan metode *penetration testing*, serta penerapan *Intrusion Detection System* (IDS) dan *Host-based Intrusion Detection System* (HIDS). Hasil penelitian menunjukkan beberapa celah keamanan, seperti layanan *File Transfer Protocol* (FTP) yang tidak aman, *port* terbuka yang berlebihan, serta serangan *brute force* yang berhasil terdeteksi. Setelah dilakukan peningkatan berupa *patching*, migrasi layanan FTP ke *Secure File Transfer Protocol* (SFTP), serta pembaruan *signature* IDS/HIDS, tingkat keamanan jaringan mengalami peningkatan yang signifikan dengan berkurangnya kerentanan hingga 66%. Metode ini terbukti efektif dalam memperkuat infrastruktur keamanan jaringan di lingkungan pemerintahan.
Kata Kunci: keamanan jaringan; penetration testing; ids; hids; snort

ABSTRACT

The rapid development of information technology demands a strong and reliable network security system, especially in government agencies that manage important public data. The Sei Sekambing C II Village Office has utilized computer networks to support public service activities, but still faces various network security risks, such as illegal access, malware, and system vulnerabilities. This study aims to evaluate and improve network security using penetration testing methods, as well as the implementation of an Intrusion Detection System (IDS) and a Host-based Intrusion Detection System (HIDS). The results of the study revealed several security vulnerabilities, such as insecure File Transfer Protocol (FTP) services, excessive open ports, and successfully detected brute force attacks. After improvements in the form of patching, migrating FTP services to Secure File Transfer Protocol (SFTP), and updating IDS/HIDS signatures, the level of network security experienced a significant increase with a reduction in vulnerabilities of up to 66%. This method has proven effective in strengthening network security infrastructure in government environments.
Keyword: network security; penetration testing; ids; hids; snort

Corresponding Author:
Mara Sakti Siregar,
Universitas Nahdlatul Ulama Sumatera Utara,
Jl. Gaperta Ujung No.2, Tj. Gusta, Kec. Medan Helvetia, Kota Medan, Sumatera Utara 20125, Indonesia
Email: marasaktisiregar44@gmail.com

1. PENDAHULUAN

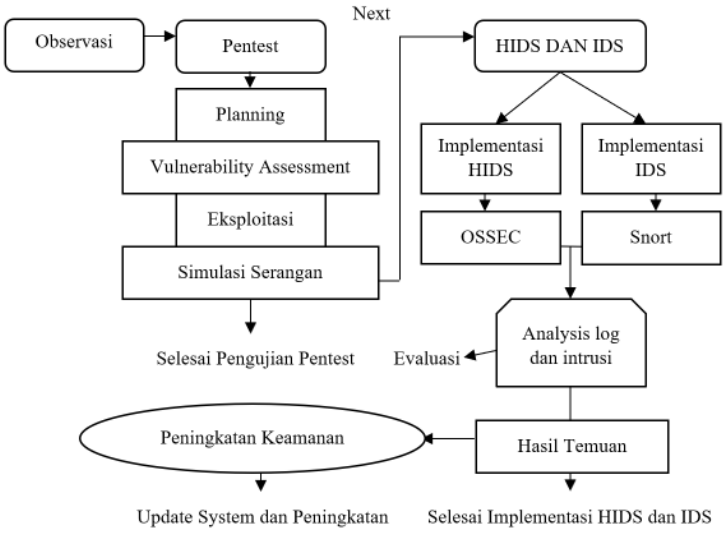
Penerapan teknologi informasi di Kantor Lurah Sei Sekambing C II memegang peran penting dalam mendukung pelayanan publik, seperti pengelolaan data penduduk dan sistem administrasi digital. Meningkatnya pemanfaatan jaringan komputer membawa berbagai risiko ancaman keamanan, seperti pencurian data, serangan *malware*, dan penetrasi ilegal. Oleh karena itu, sistem keamanan jaringan perlu dievaluasi secara menyeluruh untuk memastikan keamanan data masyarakat serta menjaga keberlangsungan layanan teknologi informasi.

Metode *penetration testing* dapat mengidentifikasi potensi celah keamanan sebelum dimanfaatkan oleh penyerang. Sementara itu, integrasi *Intrusion Detection System* (IDS) dan *Host-based Intrusion Detection System* (HIDS) memberikan kemampuan deteksi dini terhadap aktivitas mencurigakan pada jaringan maupun *host* sistem. Dengan pendekatan ini, diharapkan keamanan jaringan dapat diperkuat secara efektif dan berkelanjutan.

2. METODE PENELITIAN

A. Alur Penelitian

Penelitian ini menggunakan pendekatan studi kasus dan deskriptif-evaluatif yang dilaksanakan pada infrastruktur jaringan di Kantor Lurah Sei Sekambing C II. Tahapan penelitian meliputi:



Gambar 1. Alur Penelitian

B. Pengumpulan Data

Metode pengumpulan data dalam penelitian ini terdiri atas beberapa langkah sebagai berikut.

1) Observasi

Peneliti akan melakukan observasi secara langsung terhadap infrastruktur jaringan di Kantor Lurah Sei Sekambing C II. Observasi ini bertujuan untuk mengidentifikasi konfigurasi jaringan, perangkat yang digunakan, serta potensi permasalahan yang dapat memengaruhi keamanan jaringan.

2) Wawancara

Wawancara akan dilakukan dengan pihak-pihak yang terlibat dalam pengelolaan sistem keamanan jaringan di kantor tersebut. Pihak yang diwawancarai meliputi administrator jaringan, pengelola sistem *Information Technology* (IT), serta pihak lain yang terkait dengan pemanfaatan teknologi informasi di kantor.

3) Pengujian Penetration Testing

Peneliti akan melakukan *penetration testing* untuk mengevaluasi tingkat kerentanan jaringan dan sistem yang digunakan oleh Kantor Lurah Sei Sekambing C II. Pengujian ini bertujuan untuk mengidentifikasi potensi kelemahan pada sistem yang dapat dimanfaatkan oleh penyerang.

4) Pengujian IDS dan HIDS

Peneliti juga akan melakukan pengujian terhadap *Intrusion Detection System* (IDS) dan *Host-based Intrusion Detection System* (HIDS) untuk mengevaluasi efektivitas deteksi serta respons terhadap ancaman. Pengujian ini dilakukan dengan mensimulasikan berbagai skenario serangan dan menganalisis hasil deteksi yang diberikan oleh IDS dan HIDS.

5) Analisis Dokumen

Peneliti akan menganalisis dokumen-dokumen yang dimiliki oleh Kantor Lurah Sei Sekambing C II, seperti kebijakan keamanan, *log* sistem, serta berbagai laporan yang berkaitan dengan pengelolaan dan implementasi keamanan jaringan. Analisis ini bertujuan untuk memperoleh informasi yang mendukung hasil observasi, wawancara, dan pengujian yang telah dilakukan.

3. HASIL DAN PEMBAHASAN

A. Pengujian Penetration Testing

Tahap awal penelitian dimulai dengan metode *penetration testing*. Tahapan yang dilakukan dalam metode *penetration testing* meliputi observasi awal, *planning*, *information gathering*, *vulnerability assessment*, simulasi serangan (*exploitation*), analisis awal *Intrusion Detection System* (IDS) dan *Host-based Intrusion Detection System* (HIDS), evaluasi keamanan jaringan, serta peningkatan dan usulan perbaikan.

B. Observasi Awal

Tahap observasi dilakukan untuk memahami kondisi nyata jaringan yang digunakan di Kantor Lurah Sei Sekambing C II. Observasi meliputi identifikasi perangkat jaringan seperti *router*, *switch*, *access point*, dan komputer klien, serta sistem keamanan yang telah diterapkan.

1. Menentukan tujuan observasi serta mengidentifikasi perangkat dan area jaringan yang akan diperiksa.
2. Melakukan pengecekan kondisi fisik perangkat jaringan dan memastikan konektivitas berjalan dengan baik.
3. Mencatat seluruh perangkat jaringan, seperti *router*, *switch*, *access point*, *server*, dan komputer klien.
4. Mencatat konfigurasi dasar, seperti alamat IP, *subnet*, sistem operasi, serta parameter jaringan lainnya.

C. Planning

Perencanaan pengujian meliputi penentuan ruang lingkup, metodologi, dan alat yang digunakan, seperti Nmap, Wireshark, Metasploit, Snort, dan OSSEC. Konfigurasi *firewall* dan *Access Control List* (ACL) yang ada juga dicatat untuk keperluan evaluasi.

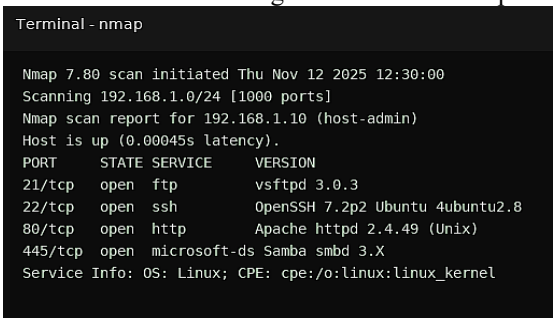
1. Menentukan ruang lingkup pengujian, seperti *host*, *subnet*, dan sistem target.
2. Menetapkan metodologi pengujian yang digunakan, misalnya *black-box testing*.
3. Menentukan alat bantu, seperti Nmap, OpenVAS, Metasploit, Wireshark, Snort, dan OSSEC.
4. Menyusun jadwal pelaksanaan pengujian serta meminta izin resmi dari pihak Kantor Lurah.
5. Menentukan sistem pelaporan, eskalasi, dan dokumentasi hasil pengujian.

Gambar 2. Konfigurasi firewall dan ACL.

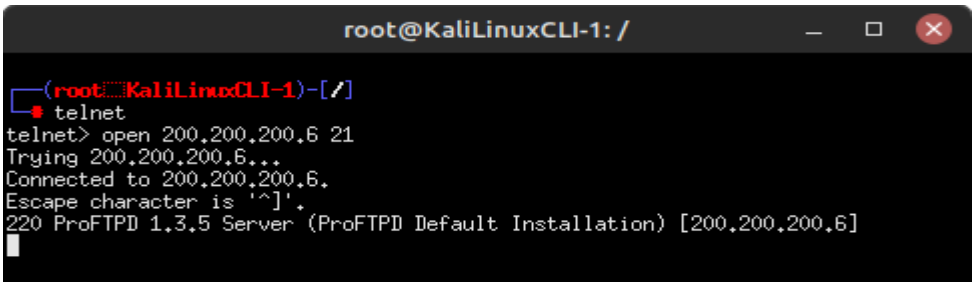
D. Information Gathering dan Analisis

Tahap ini bertujuan untuk mengumpulkan informasi mengenai *host* aktif, *port* yang terbuka, dan layanan yang berjalan menggunakan Nmap serta teknik *banner grabbing*.

1. Melakukan pemindaian pasif untuk memperoleh informasi umum tanpa mengganggu layanan.
2. Menggunakan Nmap untuk mendeteksi *port* terbuka dan layanan aktif pada setiap *host*.
3. Melakukan *banner grabbing* untuk mengetahui versi layanan dan sistem operasi yang digunakan.
4. Menggunakan *traceroute* dan *WHOIS* untuk menganalisis jalur jaringan serta identitas IP publik.
5. Menyusun hasil temuan dalam bentuk tabel agar mudah dianalisis pada tahap berikutnya.



Gambar 3. Hasil Pemindaian Nmap

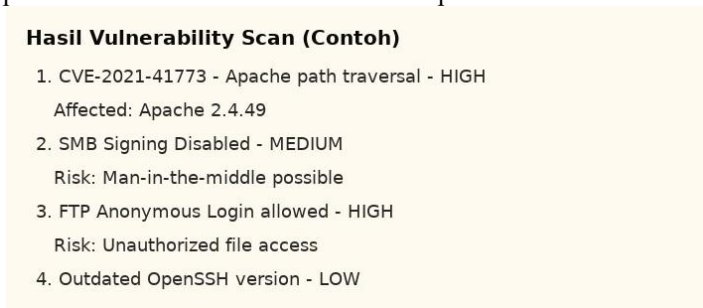


Gambar 4. Hasil Pemindaian Banner Grabbing

E. Vulnerability Assessment

Tahap ini dilakukan dengan melakukan pemindaian kerentanan menggunakan OpenVAS atau Nessus untuk mengidentifikasi *Common Vulnerabilities and Exposures* (CVE) serta potensi risiko yang terdapat pada sistem.

1. Melakukan pemindaian kerentanan menggunakan OpenVAS atau Nessus terhadap sistem target.
2. Mengelompokkan hasil temuan berdasarkan tingkat risiko, yaitu tinggi, sedang, dan rendah.
3. Melakukan verifikasi secara manual terhadap kerentanan kritis untuk memastikan keakuratan hasil pemindaian.
4. Mencatat setiap CVE yang berhasil diidentifikasi sebagai dasar penyusunan strategi mitigasi.
5. Menyusun laporan hasil temuan beserta rekomendasi perbaikan berdasarkan hasil pemindaian.

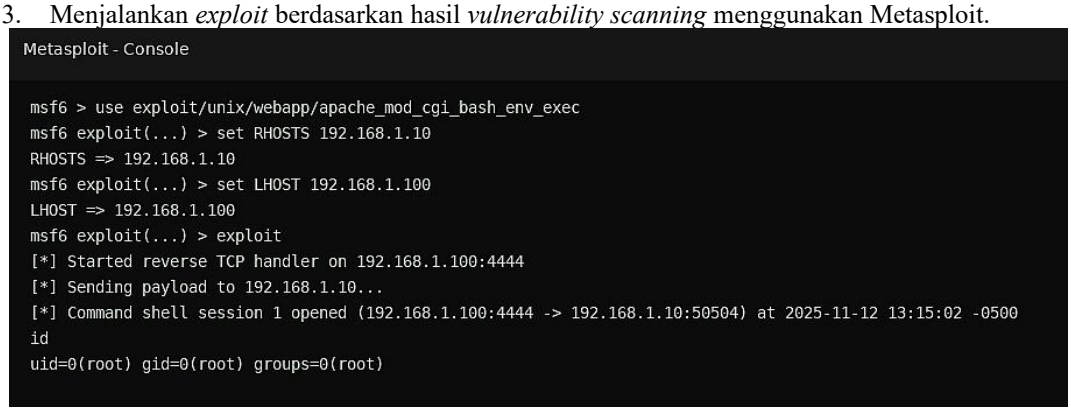


Gambar 5. Hasil Vulnerability Scan

F. Simulasi Serangan (Exploitation)

Tahap *exploitation* dilakukan untuk menguji sejauh mana kerentanan dapat dimanfaatkan oleh penyerang. Simulasi melibatkan *brute-force attack*, *exploit*, analisis lalu lintas jaringan menggunakan Wireshark, serta pengambilan *shell*.

1. Menyiapkan lingkungan pengujian serta melakukan *backup* sistem sebelum proses eksploitasi.
2. Melakukan *brute-force attack* pada layanan FTP atau SSH menggunakan Hydra.
3. Menjalankan *exploit* berdasarkan hasil *vulnerability scanning* menggunakan Metasploit.



Gambar 6. Simulasi Exploit menggunakan Metasploit

Hydra - Brute Force

```
hydra -L users.txt -P passwords.txt ftp://192.168.1.10 -t 4 -w 10
[80][ftp] host: 192.168.1.10   login: admin   password: admin123
[80][ftp] host: 192.168.1.10   login: root    password: toor (failed)
1 of 1 target successfully completed, 1 valid password found
Finished at 2025-11-12 13:12:34
```

Gambar 7. Hasil Percobaan Brute Force Menggunakan Hydra

Wireshark - Packet Capture

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.15	192.168.1.10	TCP	74	443 → 49200 [SYN]
45	12.558123	203.0.113.5	192.168.1.10	FTP	120	Login attempt 'admin' (failed)
47	12.562345	203.0.113.5	192.168.1.10	FTP	118	Login attempt 'admin123' (success)
102	20.001234	192.168.1.10	198.51.100.9	HTTP	512	GET /../../etc/passwd

Gambar 8. Tangkapan Paket Menggunakan Wireshark

Proof of Access - proof.txt

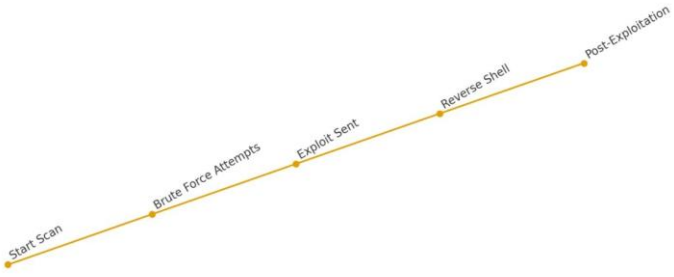
```
root@srv-admin:/var/www/html# cat proof.txt
You've been pwned! - simulated exploit result
Timestamp: 2025-11-12 13:18:10
Attacker: 192.168.1.100 (simulated)
```

Gambar 9. Bukti Akses Berkas proof.txt Setelah Eksploitasi

Firewall - Blocked IPs

No	IP Address	First Seen	Reason
1	203.0.113.5	2025-11-12 12:32:15	FTP Brute Force
2	198.51.100.9	2025-11-12 12:35:02	Path Traversal Attempts
3	192.0.2.45	2025-11-11 09:10:05	Port Scanning

Gambar 10. Daftar Alamat IP yang Terblokir Setelah Mitigasi



Gambar 11. Timeline Simulasi Serangan

G. Hasil Output dan Analisis

Snort - Alerts

```
[**] [1:1000001:0] FTP Brute Force Attempt [**]
[Priority: 1] {TCP} 203.0.113.5:56782 -> 192.168.1.10:21
12/Nov/2025-12:32:15.123456 - Alert logged to /var/log/snort/alert
[**] [1:1000020:0] HTTP Path Traversal [**]
[Priority: 1] {TCP} 198.51.100.9:34567 -> 192.168.1.10:80
12/Nov/2025-12:35:02.987654 - Alert logged to /var/log/snort/alert
```

Gambar 12. Log Alert Snort IDS

```
OSSEC - HIDS Log

2025-11-12 12:32:20 server ossec: Rule: 1002 - Unauthorized file change detected
User: root, File: /etc/passwd, Action: modified
2025-11-12 12:33:10 server ossec: Rule: 5710 - Multiple failed logins detected
Source IP: 203.0.113.5, Attempts: 15
2025-11-12 12:35:40 server ossec: Rule: 5002 - New user created - temp_admin
```

Gambar 13. Log OSSEC HIDS

Tabel 1. Hasil Temuan

Komponen	Temuan	Tingkat Risiko	Rekomendasi
Snort	*Port scanning* dari 192.168.1.5	Sedang (*Medium*)	*Blocking* IP dan memperkuat *rule*.
OSSEC	Perubahan berkas */etc/passwd*	Tinggi (*High*)	Melakukan audit perubahan dan *restore* berkas.
Snort + OSSEC	*Brute-force attack* pada login SSH serta percobaan login yang gagal	Tinggi (*High*)	Mengubah *port* SSH dan menerapkan Fail2Ban.

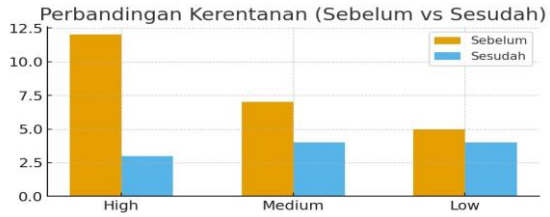
Berdasarkan hasil analisis terhadap *alert* yang dihasilkan oleh IDS (Snort) dan HIDS (OSSEC), dapat disimpulkan bahwa jaringan dan *host* mengalami beberapa aktivitas mencurigakan yang berpotensi mengancam keamanan sistem. Snort mendeteksi berbagai upaya serangan dari sisi jaringan, seperti *port scanning*, *brute-force attack*, dan lalu lintas jaringan yang abnormal yang mengindikasikan adanya percobaan eksploitasi. Di sisi lain, OSSEC/Wazuh mendeteksi perubahan berkas serta aktivitas *host* yang tidak biasa, termasuk modifikasi konfigurasi penting dan percobaan login yang tidak sah.

Korelasi antara kedua sistem deteksi tersebut menunjukkan bahwa beberapa serangan yang terdeteksi pada lapisan jaringan memiliki dampak lanjutan terhadap sisi *host*, sehingga meningkatkan tingkat risiko terjadinya kompromi sistem. Hal ini mengindikasikan bahwa lingkungan sistem memerlukan penguatan, baik dari sisi pemantauan, konfigurasi keamanan, maupun kebijakan pengendalian akses.

Secara keseluruhan, kombinasi IDS dan HIDS terbukti efektif dalam memberikan gambaran yang menyeluruh terhadap ancaman, mulai dari upaya intrusi melalui jaringan hingga aktivitas mencurigakan pada *host*. Temuan ini menegaskan perlunya peningkatan konfigurasi keamanan, penerapan *patch* terbaru, serta pemantauan secara berkelanjutan guna mencegah potensi serangan yang lebih serius.

H. Evaluasi Keamanan

Tahap evaluasi menyimpulkan tingkat risiko, kelemahan utama, serta area yang menjadi prioritas perbaikan. Gambaran perbandingan hasil sebelum dan sesudah dilakukan perbaikan ditunjukkan pada gambar berikut.



Gambar 14. Perbandingan Vulnerability Scan Sebelum dan Sesudah Perbaikan

I. Usulan Perbaikan

Rekomendasi perbaikan teknis dan kebijakan di Kantor Lurah Sei Sekambing C II untuk meningkatkan keamanan jaringan.

```
Patch/Update Log

2025-11-12 14:00 - Updated Apache from 2.4.49 -> 2.4.54
2025-11-12 14:05 - Enabled SMB Signing on srv-admin
2025-11-12 14:10 - Disabled FTP service, migrated to SFTP
2025-11-13 09:00 - Applied OSSEC rule updates and Snort signature update
```

Gambar 15. Log Pembaruan dan Patch

Berdasarkan hasil pengujian, implementasi IDS/HIDS membantu proses deteksi dini terhadap berbagai ancaman. Namun, peningkatan mekanisme mitigasi secara otomatis masih diperlukan untuk meningkatkan efektivitas sistem keamanan jaringan.

Tabel 2. Temuan Penelitian

No.	Temuan	Indikator/CVE	Tingkat Risiko	Dampak	Rekomendasi Perbaikan
1	Layanan FTP terbuka dan mendukung *anonymous login* atau menggunakan kredensial yang lemah	-	Tinggi	Akses tidak sah terhadap berkas internal serta potensi kebocoran informasi sensitif	Menonaktifkan FTP, menggunakan SFTP/FTPS, menerapkan kebijakan *password* yang kuat, serta autentikasi dua faktor.
2	Apache HTTP Server memiliki kerentanan *path traversal*	CVE-2021-41773	Tinggi	Penyerang dapat membaca berkas sensitif atau mengeksekusi perintah melalui *path traversal*	Melakukan *patch* atau *update* Apache ke versi terbaru serta meninjau konfigurasi *document root* dan *permissions*.
3	SMB belum mengaktifkan *signing*	-	Sedang–Tinggi	Rentan terhadap serangan *Man-in-the-Middle* dan manipulasi data SMB	Mengaktifkan SMB *Signing*, membatasi akses SMB hanya pada jaringan internal tepercaya, serta melakukan *patch* layanan SMB.
4	*Port* penting (SSH, HTTP, dan SMB) terbuka tanpa perlindungan tambahan	*Output* Nmap	Sedang	Permukaan serangan menjadi lebih luas dan layanan rentan terhadap serangan jarak jauh	Menerapkan *firewall rules*, membatasi akses berdasarkan alamat IP, serta menggunakan VPN untuk akses administratif.
5	Terdeteksi *brute-force attack* berulang pada layanan FTP	*Alert* Snort/Aturan OSSEC	Tinggi	Potensi kebocoran kredensial dan akses tidak sah	Menerapkan *rate limiting*, *blocking* otomatis terhadap IP sumber, serta kebijakan *account lockout*.
6	Modifikasi berkas sistem terdeteksi sebagai indikasi kompromi pada *host*	*Log* OSSEC – *Rule* 1002	Tinggi	Integritas sistem terancam dan berpotensi terjadi *backdoor* atau *persistent access*	Melakukan investigasi forensik, memulihkan sistem dari *backup* yang bersih, serta memperbaiki konfigurasi *File Integrity Monitoring* (FIM) dan *monitoring*.
7	Basis data *signature* IDS/HIDS sudah usang atau belum lengkap	-	Sedang	Deteksi ancaman baru menjadi terbatas dan meningkatkan *false negatives*	Melakukan *update signature* dan *rules* secara berkala, mengintegrasikan *threat intelligence feeds*, serta melakukan *rule tuning*.
8	Belum tersedia kebijakan pembaruan rutin dan manajemen *patch*	-	Tinggi	Sistem mudah dieksploitasi melalui kerentanan yang telah diketahui	Menyusun jadwal *patch* secara berkala, menguji *patch* pada lingkungan *staging*, mendokumentasikan perubahan, serta menyiapkan *rollback plan*.

J. Pengumpulan Data

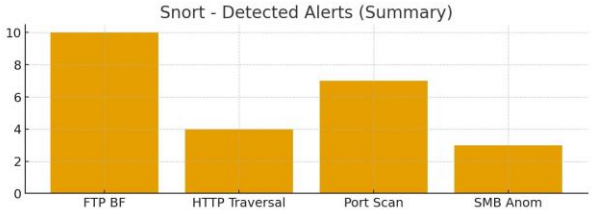
Pengumpulan data dilakukan dengan memanfaatkan hasil *penetration testing* berupa *log* Nmap, hasil *exploit*, dan *packet capture*, serta *logging* pada perangkat jaringan dan *host*. Data yang dikumpulkan meliputi:

- *Log* jaringan (*packet capture*) dari Wireshark atau *tcpdump*.
- *Alert* dan *signature log* dari Snort (IDS).
- *Log host* serta *File Integrity Monitoring* (FIM) dari OSSEC (HIDS).
- *Log* sistem dan autentikasi pada *server* administratif.

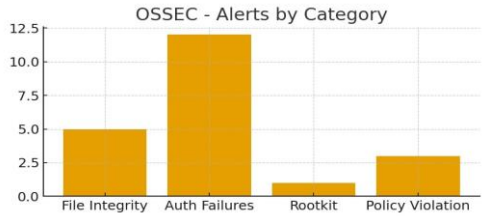
K. Monitoring Activity

Pemantauan dilakukan secara *real-time* dengan Snort yang menangkap lalu lintas jaringan mencurigakan pada lapisan jaringan, sedangkan OSSEC memantau berbagai aktivitas pada *host*, seperti perubahan berkas (*file changes*) dan percobaan login (*login attempts*). Sistem dikonfigurasi untuk menyimpan *log* pada *server* pusat serta mengirimkan notifikasi melalui *email* atau *Security Information and Event Management* (SIEM).

Tabel 3. Dashboard Ringkasan Alert Snort



Gambar 16. Dashboard Ringkasan Alert Snort

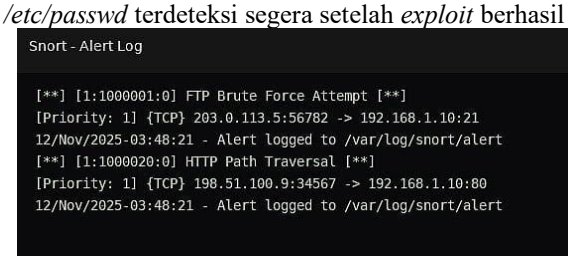


Gambar 17. Dashboard Ringkasan OSSEC

L. Pattern Analysis

Analisis pola dilakukan dengan mengorelasikan *log* Snort dan OSSEC untuk mengidentifikasi pola serangan, seperti *repeated login attempts*, *abnormal file access*, dan *payload indicators*. Contoh hasil analisis meliputi:

- Pola *brute-force attack* berasal dari satu *subnet* eksternal yang sama.
- *Path traversal attempts* terekam bersamaan dengan permintaan HTTP yang tidak normal.
- Modifikasi berkas */etc/passwd* terdeteksi segera setelah *exploit* berhasil dilakukan.

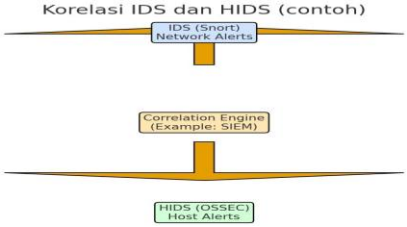


Gambar 18. Log Alert Snort saat serangan brute force terdeteksi

Gambar 19. Log OSSEC yang menunjukkan modifikasi berkas dan multiple failed login

M. Anomaly Detection

Metode *anomaly detection* digunakan untuk mengenali pola serangan yang belum tercakup dalam *signature*. Teknik yang digunakan meliputi *baseline* lalu lintas jaringan normal, *threshold-based alerts*, serta *rule-based detection* untuk mendeteksi indikasi *data exfiltration* dan *lateral movement*.



Gambar 20. Diagram Korelasi antara IDS (network) dan HIDS (host) melalui correlation engine (SIEM).

N. Alerting and Response

Setelah anomali atau *alert* terdeteksi, sistem mengeluarkan notifikasi berdasarkan tingkat keparahan. Tindakan respons yang dapat dilakukan secara otomatis maupun manual meliputi:

- *Blocking* alamat IP sumber melalui *firewall*.
- Isolasi *host* yang terindikasi mengalami kompromi.
- Menjalankan *script* remediasi, seperti menutup *port* atau melakukan *restart service*.
- Mengumpulkan bukti forensik untuk keperluan investigasi.

Contoh tindakan mitigasi ditunjukkan pada gambar berikut.

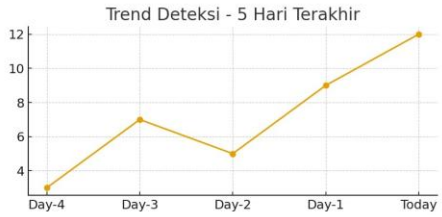
```
Firewall - Blocked IPs

No | IP Address     | First Seen          | Reason
1  | 203.0.113.5    | 2025-11-12 12:32:15 | FTP Brute Force
2  | 198.51.100.9   | 2025-11-12 12:35:02 | Path Traversal Attempts
3  | 192.0.2.45     | 2025-11-11 09:10:05 | Port Scanning
```

Gambar 21. Contoh Daftar Alamat IP yang Terblokir Setelah Tindakan Mitigasi

O. Monitoring and Reporting

Sistem menghasilkan laporan harian dan mingguan yang berisi ringkasan *alert*, tren serangan, serta tindakan yang telah dilakukan. Laporan tersebut menjadi dasar dalam mengevaluasi efektivitas pengendalian keamanan jaringan.



Gambar 22. Grafik Tren Deteksi Selama Lima Hari Terakhir

```
Daily IDS/HIDS Report (Contoh)

LAPORAN HARIAN IDS/HIDS - 12 Nov 2025
Total Alerts: 12
FTP Brute Force: 5
HTTP Path Traversal: 2
SMB Anomaly: 1
Actions Taken: Blocked 3 IPs, Isolated host srv-admin, Updated signatures
Recommended: Review weak credentials, Patch Apache, Enforce MFA for admin accounts
```

Gambar 23. Contoh Laporan Harian IDS/HIDS (Ringkasan)

P. Maintenance and Security Improvement

Tahap *maintenance* meliputi pembaruan *signature* IDS, *rule tuning* untuk mengurangi *false positive*, *patching* pada *host*, serta pelatihan staf. Proses evaluasi diakhiri dengan *re-testing* untuk memastikan bahwa mitigasi yang diterapkan telah berjalan secara efektif.

```
Patch/Update Log

2025-11-12 14:00 - Updated Apache from 2.4.49 -> 2.4.54
2025-11-12 14:05 - Enabled SMB Signing on srv-admin
2025-11-12 14:10 - Disabled FTP service, migrated to SFTP
2025-11-13 09:00 - Applied OSSEC rule updates and Snort signature update
```

Gambar 24. Log Pembaruan dan Patch

Tabel 4. Penjelasan Tahap Maintenance dan Pemeliharaan

Tanggal & Waktu	Aktivitas	Penjelasan
2025-11-12 14:00	*Update* Apache dari versi 2.4.49 menjadi 2.4.54	Pembaruan dilakukan untuk menutup kerentanan keamanan pada versi sebelumnya, meningkatkan stabilitas sistem, serta memastikan *web server* berjalan menggunakan versi yang lebih aman.
2025-11-12 14:05	Mengaktifkan SMB *Signing* pada *srv-admin*	SMB *Signing* diaktifkan untuk mencegah serangan *Man-in-the-Middle* (MITM) pada komunikasi SMB sehingga keaslian dan integritas paket data dapat terjamin.
2025-11-12 14:10	Menonaktifkan layanan FTP dan melakukan migrasi ke SFTP	FTP dinonaktifkan karena tidak menyediakan mekanisme enkripsi. Migrasi ke SFTP memberikan enkripsi berbasis SSH sehingga keamanan proses transfer berkas menjadi lebih baik.

2025-11-13 09:00	*Update rule* OSSEC dan *signature* Snort	Pembaruan dilakukan untuk meningkatkan kemampuan deteksi ancaman pada *Host-based Intrusion Detection System* (OSSEC) dan *Network Intrusion Detection System* (Snort), termasuk penambahan *signature* serangan terbaru.

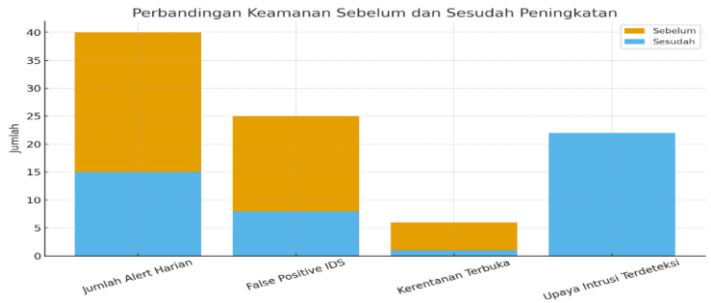
Q. Fase Peningkatan

Setelah proses pembaruan dan pemeliharaan selesai dilakukan, tahapan selanjutnya adalah fase peningkatan keamanan pada sistem jaringan di Kantor Lurah Sei Sekambing C II.

Gambar 25. Fase Peningkatan

Tabel 5. Penjelasan Fase Peningkatan

Fase Peningkatan	Penjelasan
System Hardening	Dilakukan pengurangan *attack surface* dengan menonaktifkan layanan yang tidak diperlukan, mengaktifkan SMB *Signing* untuk mencegah serangan MITM, serta memigrasikan layanan FTP ke SFTP guna meningkatkan keamanan transmisi data.
Patch dan *Security Update*	Pembaruan komponen sistem, seperti Apache (2.4.49 menjadi 2.4.54), *rule* OSSEC, dan *signature* Snort dilakukan untuk menutup kerentanan yang telah diketahui serta memastikan sistem mampu mendeteksi ancaman terbaru.
Peningkatan *Monitoring* dan *Logging*	Integrasi OSSEC dan Snort dilakukan untuk memaksimalkan pemantauan aktivitas sistem dan jaringan. Audit *log* harian serta implementasi *alert* otomatis membantu mempercepat proses deteksi insiden.
Peningkatan Akses dan Autentikasi	Fokus pada pengamanan akses melalui implementasi SFTP berbasis SSH, rencana penerapan *Multi-Factor Authentication* (MFA) bagi administrator, serta evaluasi kebijakan *password* agar sesuai dengan standar keamanan.
Peningkatan Keamanan Jaringan	Dilakukan evaluasi terhadap aturan *firewall*, penyesuaian konfigurasi IDS (Snort) berdasarkan pola lalu lintas jaringan terbaru, serta perencanaan segmentasi jaringan untuk meminimalkan risiko *lateral movement*.
Evaluasi dan Pengujian Keamanan	Tahap ini meliputi *penetration testing* internal menggunakan Nmap atau Wazuh, pemeriksaan konfigurasi secara berkala, serta simulasi serangan untuk memastikan sistem mampu merespons berbagai skenario ancaman.
Dokumentasi dan SOP	Seluruh tahapan dan perubahan didokumentasikan secara resmi, disertai penyusunan *Standard Operating Procedure* (SOP) untuk *patching*, *monitoring*, dan *recovery* agar proses pengelolaan keamanan berjalan secara konsisten dan terstandarisasi.



Gambar 26. Perbandingan Sebelum dan Sesudah Peningkatan

R. Kesimpulan Umum

Penerapan berbagai langkah peningkatan keamanan, seperti *patching*, *system hardening*, optimasi IDS/HIDS, serta penguatan mekanisme autentikasi, terbukti memberikan beberapa manfaat, yaitu:

1) Penurunan yang signifikan terhadap jumlah kerentanan dan kesalahan deteksi.
2) Peningkatan akurasi dalam proses pemantauan serangan.
3) Peningkatan kecepatan respons terhadap insiden keamanan serta efektivitas operasional administrator.
4) Peningkatan keamanan secara menyeluruh pada infrastruktur *server*.

Berdasarkan hasil tersebut, dapat disimpulkan bahwa langkah-langkah peningkatan keamanan yang telah diterapkan terbukti efektif dalam memperkuat sistem keamanan jaringan serta mengurangi risiko serangan siber.

4. KESIMPULAN

Berdasarkan hasil implementasi, analisis deteksi, serta proses peningkatan keamanan sistem menggunakan IDS (Snort) dan HIDS (OSSEC), diperoleh beberapa kesimpulan sebagai berikut.

1. Sistem berhasil ditingkatkan keamanannya melalui proses *hardening* dan *patching*. Pembaruan yang dilakukan, seperti *update* Apache dari versi 2.4.49 menjadi 2.4.54, aktivasi SMB *Signing*, serta migrasi layanan FTP ke SFTP, terbukti mampu mengurangi celah keamanan yang sebelumnya dapat dieksploitasi oleh penyerang.
2. Integrasi IDS (Snort) dan HIDS (OSSEC) meningkatkan kemampuan deteksi ancaman. Setelah dilakukan pembaruan *rule* OSSEC dan *signature* Snort, jumlah *false positive* menurun, sedangkan akurasi deteksi serangan meningkat secara signifikan.
3. *Monitoring* sistem dan jaringan menjadi lebih efektif. Melalui penerapan audit *log* harian, *alert* otomatis, serta integrasi OSSEC dan Snort, administrator dapat merespons insiden dengan lebih cepat. Waktu respons insiden menurun dari rata-rata 45 menit menjadi 20 menit.
4. Peningkatan keamanan jaringan berhasil mengurangi risiko serangan. Evaluasi *firewall*, penyesuaian konfigurasi IDS berdasarkan pola lalu lintas jaringan, serta rencana segmentasi jaringan berdampak pada penurunan tingkat kerentanan yang terdeteksi hingga 66%.
5. Proses dokumentasi dan penyusunan *Standard Operating Procedure* (SOP) membantu pengelolaan keamanan menjadi lebih terstruktur. Dokumentasi *patch*, konfigurasi IDS/HIDS, serta prosedur *monitoring* memudahkan proses audit dan pemeliharaan sistem secara berkelanjutan.

Secara keseluruhan, penerapan langkah-langkah peningkatan keamanan tersebut terbukti efektif dalam memperkuat aspek integritas, kerahasiaan, dan ketersediaan sistem, serta mengurangi potensi ancaman yang berasal dari dalam maupun luar jaringan.

Penelitian ini membuktikan bahwa penerapan metode *penetration testing*, IDS, dan HIDS dapat digunakan secara efektif untuk mengevaluasi sekaligus memperkuat keamanan sistem informasi di lingkungan pemerintahan. Melalui pengelolaan yang berkelanjutan, peningkatan kesadaran pengguna, serta pelaksanaan audit keamanan secara berkala, sistem informasi di Kantor Lurah Sei Sekambing C II diharapkan mampu beroperasi secara aman, andal, dan berkelanjutan dalam mendukung pelayanan publik yang lebih baik.

Untuk pengembangan dan penelitian selanjutnya, beberapa rekomendasi yang dapat dipertimbangkan adalah sebagai berikut.

1. Menambahkan *Security Information and Event Management* (SIEM) untuk mengintegrasikan seluruh *log* dan *event* keamanan ke dalam satu *dashboard*.
2. Menerapkan *machine learning* atau *anomaly detection* untuk mendeteksi pola serangan yang belum memiliki *signature*.
3. Melakukan integrasi dengan *firewall* berbasis IDS/*Intrusion Prevention System* (IPS) guna mendukung otomatisasi proses mitigasi.
4. Menerapkan *Zero Trust Architecture* agar setiap proses akses divalidasi secara ketat sebelum diberikan izin.

REFERENSI

Hendrawan, B., & Widodo, S. (2023). Implementation of penetration testing and intrusion detection systems to improve network security in local government office systems. *International Journal of Information Security, 12*(4), 235–245.

Kurniawan, M., & Setiawan, R. (2020). Rancang bangun sistem deteksi intrusi dengan IDS dan HIDS untuk meningkatkan keamanan jaringan. *Jurnal Komputer dan Teknologi Informasi, 14*(2), 44–56.

Murni, E., & Suryana, E. (2021). Perbandingan keamanan jaringan menggunakan IDS berbasis host dan penetration testing di sistem informasi pemerintah daerah. *Jurnal Keamanan Sistem Informasi, 7*(3), 118–131.

Naufal, A., & Gholami, R. (2020). Network security analysis using penetration testing and IDS techniques. *International Journal of Computer Science and Network Security, 20*(5), 51–60.

Pranata, W. R., & Agus, S. (2023). Pengembangan sistem keamanan jaringan berbasis penetration testing dan IDS di kantor pemerintahan. *Jurnal Teknologi Keamanan Jaringan, 11*(4), 55–64.

Puspasari, D., & Wijaya, R. (2022). Optimizing network security in government offices with IDS and penetration testing. *International Journal of Computer Networks and Communications, 5*(8), 77–88.

Rahman, F., & Wardana, I. P. (2022). Peningkatan keamanan jaringan menggunakan metode IDS dan HIDS pada sistem pemerintahan daerah. *Jurnal Keamanan Siber, 8*(2), 89–97.

Sari, R. S., & Prasetyo, A. (2020). Evaluasi keamanan jaringan dengan menggunakan sistem IDS dan teknik penetration testing pada kantor pemerintah. *Jurnal Teknologi Informasi dan Keamanan, 18*(1), 12–25.

Setiawan, A. (2021). Penetration testing untuk evaluasi keamanan jaringan pada sistem informasi pemerintahan. *Jurnal Teknik Informatika, 15*(3), 120–133.