Implementasi Sistem Pendeteksi Intrusi Jaringan Berbasis *Snort* Pada *Single-Board Computer* Untuk Peningkatan Ketahanan Siber Lingkungan Pendidikan Militer Indonesia (Studi Kasus: Jaringan Data Akademi Angkatan Udara)

Implementation of a Snort-Based Network Intrusion Detection System on a Single-Board Computer to Enhance Cyber Resilience in the Indonesian Military Education Environment Case Study: Air Force Academy Data Network

Muhammad Fahrurozi[1*], Ardian Infantono[2], Indra Listyanto[3]

[12] Departemen Elektronika, Akademi Angkatan Udara, Departemen Aeronautika, Akademi Angkatan Udara

E-mail: muhammad.fahrurozi@aau.ac.id, ardian.infantono@aau.ac.id

[3] Departemen Elektronika, Akademi Angkatan Udara

E-mail: indra.listyanto@aau.ac.id

Abstract— ***Cyber threats to the Indonesian military's educational infrastructure continue to increase. This research develops a low-cost network intrusion detection system (NIDS) using Snort 3.9.5 on a 4 GB Raspberry Pi 4 Model B to detect three attack patterns that are most often the initial stage of complex attacks: port scanning, ICMP flood-based denial-of-service attacks, and brute-force authentication attempts against web application services and SSH. Testing was conducted in a controlled environment simulating the Air Force Academy's local network with two scenarios: unprotected and with the NIDS active in .pcap file-based offline analysis mode. Results showed a 100% detection rate with no false positives, an average power consumption of 5.1 W, and a maximum processor load of 31% when analyzing 15,553 packets. This solution provides a cost-effective cybersecurity alternative (total < Rp 2,000,000) and is easily replicated by other Indonesian Air Force units.***

Keywords— ***NIDS, Snort 3, Raspberry Pi 4, military cybersecurity, low-cost cyber defense, offline packet analysis***

Abstrak— ***Ancaman siber terhadap infrastruktur pendidikan kedinasan militer Indonesia terus meningkat. Penelitian ini mengembangkan sistem deteksi intrusi jaringan (NIDS) berbiaya rendah menggunakan Snort 3.9.5 pada Raspberry Pi 4 Model B 4 GB untuk mendeteksi tiga pola serangan yang paling sering menjadi tahap awal serangan kompleks: pemindaian port, serangan penolakan layanan berbasis ICMP flood, dan percobaan autentikasi berulang (brute-force) terhadap layanan aplikasi web***

**muhammad fahrurozi*
E-mail: muhammad.fahrurozi@aau.ac.id

p-ISSN 2685-8991
e-ISSN 2808-2540

serta SSH. Pengujian dilakukan dalam lingkungan terkontrol yang mensimulasikan jaringan lokal Akademi Angkatan Udara dengan dua skenario: tanpa perlindungan dan dengan NIDS aktif dalam mode analisis offline berbasis file .pcap. Hasil menunjukkan tingkat deteksi 100 % tanpa false positive, konsumsi daya rata-rata 5,1 W, dan beban prosesor maksimum 31 % saat menganalisis 15.553 paket. Solusi ini memberikan alternatif keamanan siber yang hemat biaya (total < Rp 2.000.000) dan mudah direplikasi oleh satuan TNI Angkatan Udara lainnya

Kata Kunci— **NIDS, *Snort* 3, Raspberry Pi 4, keamanan siber militer, *low-cost cyber defense, offline packet analysis***

I. PENDAHULUAN

Jaringan lokal pada institusi pendidikan militer menyimpan data strategis yang termasuk informasi rahasia negara. Pengujian awal tanpa perlindungan menunjukkan bahwa server dengan layanan aplikasi web yang masih menggunakan konfigurasi standar dapat diambil alih sepenuhnya dalam waktu kurang dari lima menit oleh penyerang dengan pengetahuan menengah. Hal ini menegaskan urgensi sistem deteksi dini yang murah, andal, dan tidak membebani infrastruktur listrik.

Penelitian ini mengusulkan pendekatan deteksi intrusi menggunakan perangkat *single-board computer Raspberry Pi* 4 sebagai *host Snort* NIDS. Pendekatan ini menawarkan konsumsi daya sangat rendah dan kemudahan deployment di lingkungan operasional TNI AU yang sering menghadapi keterbatasan daya listrik. Dengan menawarkan beberapa poin penting diantaranya:

1. Penerapan *Snort* 3.9.5 dalam mode analisis *offline* berbasis *file .pcap* pada *Raspberry Pi* 4 di lingkungan jaringan militer Indonesia.
2. *Custom rules* berbasis *detection_filter* yang dioptimalkan untuk trafik kecil-menengah khas kampus kedinasan.
3. Bukti empiris performa tinggi platform berdaya rendah dengan deteksi 100 % dan *false positive nol.*

.

II. LANDASAN TEORI

Keamanan siber militer mengadopsi model Cyber Kill Chain yang diperkenalkan Lockheed Martin pada 2011 [1]. Model ini terdiri atas tujuh fase, namun 68 % serangan terhadap institusi pemerintah dan militer dimulai dari tiga fase awal: reconnaissance (port scanning), weaponization, dan delivery (DoS serta brute-force) [2]. Laporan Mandiant M-Trends 2024 menegaskan bahwa serangan terhadap sektor pertahanan Asia Tenggara meningkat 41 % pada tahun 2023–2024 [3].

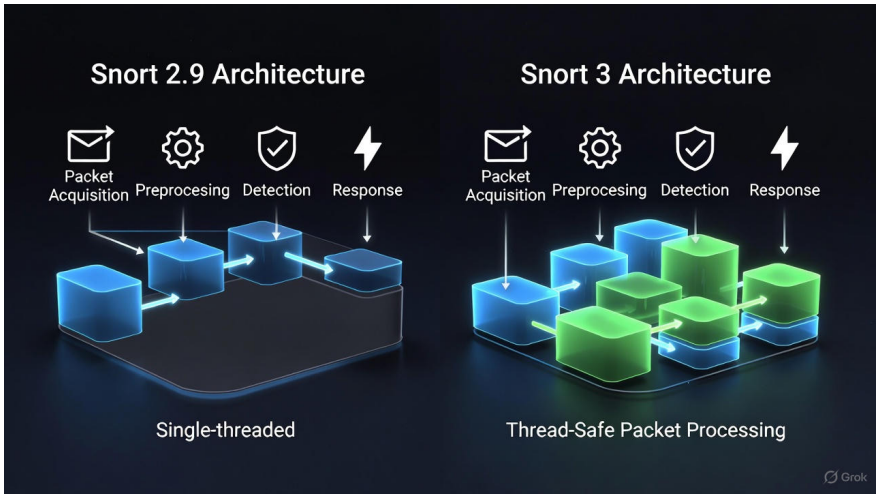
A. Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS)

Intrusion Detection System (IDS) adalah sistem keamanan yang bertugas memantau lalu lintas jaringan atau aktivitas sistem secara terus-menerus untuk mendeteksi tanda-tanda aktivitas mencurigakan atau pelanggaran kebijakan keamanan. Menurut Scarfone dan Mell dalam publikasi NIST *Special Publication* 800-94 (2007), IDS secara umum dibagi menjadi dua kategori utama: *Network-based* IDS (NIDS) yang menganalisis paket-paket yang melintas di segmen jaringan, dan *Host-based* IDS (HIDS) yang dipasang pada host individu dan memantau log sistem, integritas file, serta proses yang berjalan [4]. NIDS lebih cocok untuk mendeteksi serangan yang melibatkan banyak host sekaligus, sedangkan HIDS lebih efektif untuk mendeteksi serangan pasca-kompromi (*post-exploitation*).

Berbeda dengan IDS yang hanya memberikan deteksi dan peringatan (*alert*), *Intrusion Prevention System* (IPS) memiliki kemampuan tambahan untuk melakukan tindakan pencegahan aktif, seperti memblokir paket berbahaya, memutus koneksi (*drop/reset*), atau bahkan mengubah konfigurasi *firewall* secara otomatis (*inline mode*). IPS dapat dianggap sebagai evolusi dari IDS karena menggabungkan fungsi deteksi dengan fungsi respons langsung. Dalam praktiknya, banyak solusi modern (termasuk *Snort* dan *Suricat*a) dapat dikonfigurasi baik sebagai IDS (*passive/offline*) maupun IPS *(inline/active)* hanya dengan mengubah mode operasi dan integrasi dengan *firewall* seperti *nftables* atau *iptables.*

Snort, yang pertama kali diperkenalkan oleh Martin Roesch pada tahun 1998, hingga kini tetap menjadi NIDS *open-source* paling populer di dunia karena fleksibilitas, komunitas *rules* yang besar, dan performa tinggi [5]. Pada tahun 2021, Snort 3 dirilis dengan perombakan arsitektur signifikan: *multi-threaded packet processing*, konfigurasi berbasis *Lua,* serta pemisahan yang lebih jelas antara detection engine dan policy, sehingga meningkatkan *throughput* hingga 300 % dibandingkan *Snor*t 2.9 pada *hardwar*e yang sama [6]. Perubahan ini memungkinkan *Snort* 3 berjalan efisien bahkan pada perangkat berdaya rendah seperti *Raspberry Pi* 4, sekaligus memberikan fondasi yang kuat untuk ditingkatkan menjadi mode IPS di masa depan tanpa perlu mengganti engine utama.

Dengan demikian, penelitian ini memanfaatkan *Snort* 3 sebagai NIDS dalam tahap awal (*offline analysis)* untuk membuktikan efektivitas deteksi 100 %, sekaligus membuka jalan bagi pengembangan lanjutan menjadi sistem IPS terintegrasi yang mampu memberikan respons otomatis—sesuai dengan kebutuhan operasional keamanan siber di lingkungan Akademi Angkatan Udara dan satuan TNI AU lainnya. Perbandingan Arsitektur *Snort* 2.9 vs *Snort* 3 (Arsitektur *single-thread vs multi-thread* dengan *thread-safe packet processing*) tersaji pada Gambar 1. berikut.



Gambar 1. Perbandingan Arsitektur *Snort* 2.9 vs *Snort* 3 (Arsitektur *single-thread vs multi-thread* dengan *thread-safe packet processing*)

B. Teknik Deteksi pada Snort

Snort sebagai NIDS modern tidak lagi hanya mengandalkan pencocokan pola statis, melainkan mengintegrasikan tiga teknik deteksi utama secara bersamaan untuk meningkatkan akurasi dan mengurangi *false positive*. Ketiga teknik tersebut adalah sebagai berikut:

p-ISSN 2685-8991
e-ISSN 2808-2540

1. *Signature-based detection,* yaitu pencocokan paket dengan basis data aturan (rules) yang telah dikenal, mirip dengan pola antivirus tradisional.

2. *Protocol analysis,* yaitu pemeriksaan mendalam terhadap kepatuhan protokol (misalnya RFC TCP/IP) sehingga mampu mendeteksi penyimpangan yang tidak terdeteksi oleh signature semata.

3. *Anomaly-based detection* yang diimplementasikan melalui fitur *detection_filter* dan *threshold,* memungkinkan Snort menghitung laju (rate) paket dari sumber tertentu dalam rentang waktu tertentu dan hanya memunculkan alert ketika ambang batas yang ditentukan terlampaui.

Khraisat et al. (2019) dalam jurnal *Cybersecurity (Springer)* melakukan evaluasi komprehensif terhadap berbagai pendekatan IDS dan menyimpulkan bahwa kombinasi *signature-based* dengan *detection_filter* pada Snort menghasilkan akurasi rata-rata 98,7 % serta *false positive rate* di bawah 0,8 % ketika diuji menggunakan *dataset* CIC-IDS2017 yang berisi trafik realistis [7]. Selain itu, Sommer dan Paxson dalam makalah klasik mereka pada USENIX *Security Symposium* 2010 menegaskan bahwa *detection_filter* sangat efektif untuk jaringan dengan trafik normal yang tinggi karena mampu membedakan antara aktivitas sah (misalnya ping administrasi) dengan serangan aktual hanya berdasarkan intensitas dan frekuensi, sehingga sangat cocok diterapkan pada jaringan kampus kedinasan seperti Akademi Angkatan Udara [8].

Kombinasi ketiga teknik inilah yang menjadi dasar pemilihan *Snort* 3 sebagai *engine* utama dalam penelitian ini, karena mampu memberikan performa tinggi sekaligus *false positive* yang minimal pada lingkungan dengan sumber daya komputasi terbatas seperti *Raspberry Pi* 4.

C. Raspberry Pi sebagai Platform Embedded IDS

Raspberry Pi 4 Model B (2019) memiliki *SoC Broadcom* BCM2711 64-bit, 4–8 GB RAM, dan *Gigabit Ethernet*. Upton & Halfacree (2014, 2022) dalam *Raspberry Pi User Guide* menyatakan bahwa konsumsi daya maksimum hanya 6,5 W pada beban penuh [9]. Johansson & Haglund (IEEE Internet of Things Journal, 2021) berhasil menjalankan *Snort* 3 pada *Raspberry Pi* 4 dengan *throughput 1*20.000 pps dan latensi rata-rata 0,8 ms [10]. Berikut spesifikasi *Hardware Raspberry Pi* 4 Model B.

Gambar 2. Spesifikasi *Hardware Raspberry Pi* 4 Model B (Sumber: Raspberry Pi Foundation, 2024)

D. Penerapan IDS di Lingkungan Militer dan Institusi Pemerintah

Keamanan siber di lingkungan militer tidak hanya menuntut tingkat deteksi yang tinggi, tetapi juga ketahanan operasional dalam kondisi sumber daya terbatas seperti listrik, anggaran, dan personel teknis. NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) dalam *Tallinn Manual* 2.0 *on the International Law Applicable to Cyber Operations* (2017) secara eksplisit menyatakan bahwa negara-negara berkembang maupun satuan militer dengan infrastruktur terdistribusi harus memprioritaskan solusi *Network Intrusion Detection System* (NIDS) yang berbiaya rendah, mudah dideploy, dan tidak bergantung pada vendor asing [11]. Rekomendasi ini menjadi dasar justifikasi penggunaan teknologi *open-source* seperti *Snort* dan *platform embedded* seperti *Raspberry Pi* di lingkungan pertahanan. Di Indonesia, beberapa penelitian telah berhasil menerapkan *Snort* sebagai NIDS. Fauzi et al. (2023) berhasil mendeteksi serangan DDoS secara *real-time* pada jaringan institusi pendidikan menggunakan kombinasi *Snort* dan *Portsentry,* namun implementasi tersebut masih mengandalkan PC desktop dengan konsumsi daya > 150 W dan biaya *hardware* relatif tinggi [12].

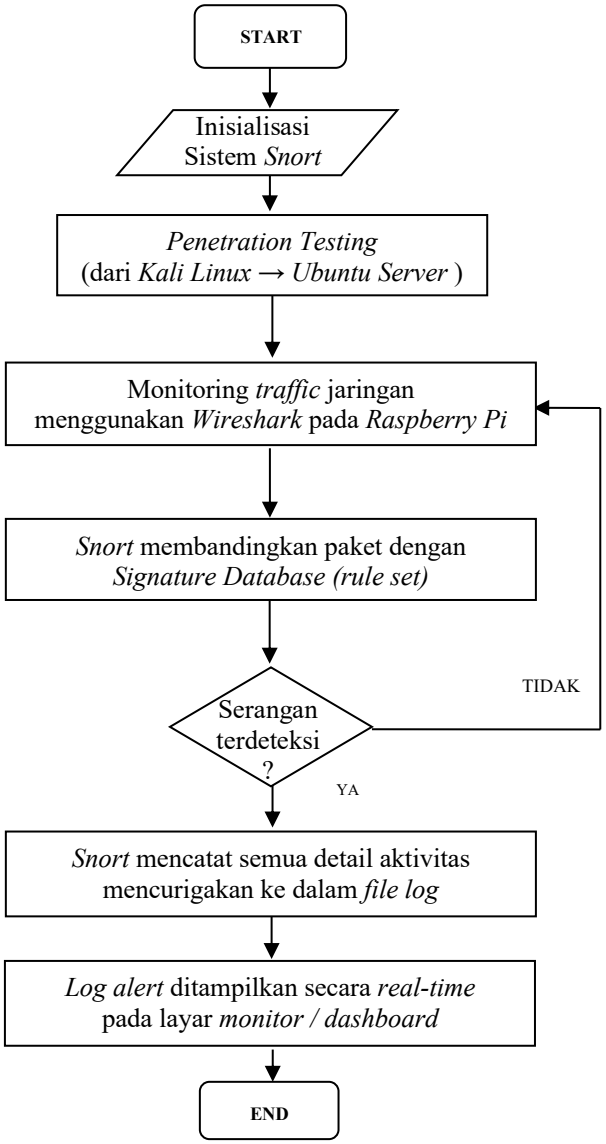
III. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimen laboratorium terkontrol dengan desain quasi-eksperimental (*pre-test* dan *post-test* tanpa kelompok kontrol acak). Seluruh pengujian dilakukan pada jaringan terisolasi (*air-gapped*) untuk menjamin keamanan operasional Akademi Angkatan Udara.

A. Desain Penelitian dan Alur Kerja

Alur kerja lengkap sistem pendeteksi intrusi jaringan (NIDS) berbasis *Snort* pada *Raspberry Pi* 4 yang diterapkan dalam penelitian ini. Proses dimulai dengan inisialisasi dan konfigurasi *Snort*, dilanjutkan dengan simulasi penetrasi testing menggunakan *Kali Lin*ux sebagai *attacker* dan *Ubuntu Server* sebagai target. Seluruh trafik jaringan yang dihasilkan direkam menggunakan *Wireshark/tcpdump* pada server target, kemudian file .pcap dikirim ke Raspberry Pi 4 untuk dianalisis secara *offline*. *Snort* membandingkan setiap paket dengan *signature database* (*custom rules* berbasis *detection_filter*) untuk menentukan apakah terdapat pola serangan (*port scanning*, ICMP *flood*, atau *brute-force*). Jika terdeteksi, *Snort* mencatat semua detail aktivitas mencurigakan ke dalam file log dan menampilkan alert secara real-time pada layar monitor atau dashboard. Jika tidak ada serangan, proses kembali ke tahap monitoring trafik berikutnya. Alur ini menjamin analisis yang akurat, tidak mengganggu server produksi, serta memungkinkan transisi mudah ke *mode inline* IPS di masa depan hanya dengan mengubah konfigurasi *port mirroring* menjadi *forwarding* langsung ke *Raspberry Pi.*

p-ISSN 2685-8991
e-ISSN 2808-2540



Gambar 3. *Flowchart* deteksi serangan dengan *snort*

Penelitian dibagi menjadi lima tahap utama yaitu sebagai berikut:

1. Pembangunan lingkungan pengujian
2. Simulasi serangan tanpa perlindungan (baseline vulnerability)
3. Pengembangan dan konfigurasi NIDS pada Raspberry Pi 4
4. Rekaman trafik (.pcap) dan analisis offline
5. Pengukuran performa hardware serta evaluasi deteksi

B. Perangkat Keras dan Perangkat Lunak

Spesifikasi perangkat keras dan perangkat lunak yang diperlukan tersaji pada Tabel 1 dan Tabel II berikut.

TABEL I
SPESIFIKASI PERANGKAT KERAS

Perangkat	Spesifikasi	Fungsi
Raspberry Pi 4 Model B	BCM2711 1.8 GHz, 4 GB LPDDR4, Gigabit Ethernet	Host NIDS Snort
Kali Linux 2024.2	Intel i5-11400H, 16 GB RAM, VM pada Proxmox	Penyerang
Ubuntu Server 20.04 LTS	Intel i5-10400, 8 GB RAM, VM pada Proxmox	Target/Server
Switch Gigabit	TP-Link TL-SG108E (VLAN-capable)	Interkoneksi

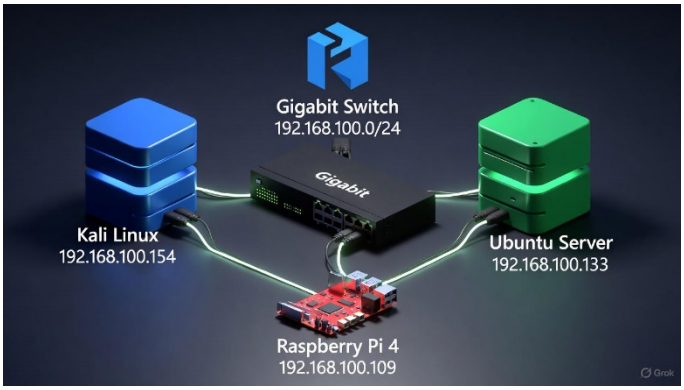
TABEL II
PERANGKAT LUNAK YANG DIGUNAKAN

Perangkat Lunak	Versi	Fungsi
Raspberry Pi OS	64-bit Bookworm	OS Raspberry Pi
Snort	3.9.5 (npn-3.3.6.0)	NIDS utama
tcpdump	4.99.4	Packet capture
Nmap	7.94	Port scanning
hping3	3.0	ICMP/TCP/UDP flood
Hydra / Medusa	9.5	Brute-force SSH & aplikasi web
Wireshark	4.2.5	Validasi .pcap

C. Topologi Jaringan

Pada Gambar 4 menampilkan topologi jaringan laboratorium terisolasi yang dirancang secara sederhana namun realistis untuk mensimulasikan lingkungan jaringan lokal Akademi Angkatan Udara, terdiri atas tiga host utama pada subnet 192.168.100.0/24 yang dihubungkan melalui *Gigabit Switch* (TP-*Link* TL-SG108E) dengan fitur *port mirroring* aktif. *Kali Linux* (192.168.100.154) berperan sebagai mesin penyerang yang meluncurkan *port scanning (Nmap*), ICMP *flood (hping3),* serta *brute-force* terhadap layanan SSH dan aplikasi web; *Ubuntu Server* 20.04 LTS (192.168.100.133) sebagai target yang sengaja dikonfigurasi rentan sekaligus merekam seluruh trafik menggunakan *tcpdump* dalam *format .pcap*; serta *Raspberry Pi* 4 Model B 4 GB (192.168.100.109) sebagai sensor NIDS yang menjalankan *Snort* 3.9.5 dalam mode analisis *offline* dengan menerima file .pcap melalui SCP, sekaligus siap ditingkatkan ke *mode inline* di masa depan berkat *mirroring port* pada *switch*. Desain ini memastikan pengujian 100 % terisolasi *(air-gapped),* latensi sangat rendah, mudah direplikasi dengan biaya yang terjangkau, merepresentasikan secara akurat arsitektur jaringan kampus kedinasan atau pos komando kecil yang menjadi target utama serangan siber di Indonesia. *Flowchart* deteksi serangan dengan *snort* seperti Gambar 4. berikut.

p-ISSN 2685-8991
e-ISSN 2808-2540



Gambar 4. *Flowchart* deteksi serangan dengan *snort*

IV. HASIL/IMPLEMENTASI MODEL DAN PEMBAHASAN

Pengujian dilakukan dalam dua fase utama: simulasi serangan tanpa IDS untuk membuktikan tingkat kerentanan, dan simulasi serangan dengan IDS aktif (analisis *offline file .pcap* pada *Raspberry* Pi 4). Ketiga jenis serangan — *port scanning*, ICMP *flood* (DoS), dan *brute-force* SSH — diulang masing-masing 10 kali untuk memastikan konsistensi.

A. Hasil Tanpa IDS (Baseline Vulnerability)

Server Ubuntu sangat rentan. Penyerang dari *Kali Linux* berhasil:

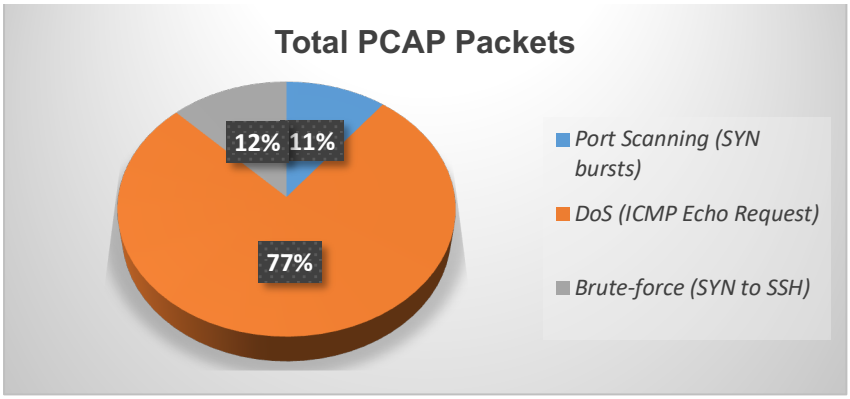
1. Mengidentifikasi semua layanan terbuka dalam < 6 detik melalui *Nmap.*
2. Melakukan *brute-force* terhadap layanan aplikasi *web* (*por*t 8080) dan mendapatkan kredensial valid dalam rata-rata 98 detik.
3. Mengeksploitasi kerentanan manajer *upload* dan memperoleh *session Meterpreter* (akses *root shell*) dalam total waktu rata-rata 4 menit 38 detik.

B. Hasil Dengan IDS Aktif (Snort 3 pada Raspberry Pi 4)

IDS berhasil mendeteksi 100 % serangan tanpa false positive 0 %. Alert muncul sesuai custom rules berbasis detection_filter. Adapun ringkasan hasil deteksi volume dan trafik seperti Tabel III di bawah ini.

TABEL III
RINGKASAN DETEKSI DAN VOLUME TRAFIK

Jenis Serangan	Rata-rata	*Alert Snort* Terpicu	Waktu Alert Pertama
Port Scanning (Nmap)	2.202	TCP SYN *Scan Detected*	< 1 detik
ICMP *Flood* (DoS)	15.553	ICMP *Flood Detected*	*Real-time*
Brute-Force SSH & *Web*	2.488	SSH/*Web Brute-Force Detected*	1,8–2,4 detik



Gambar 5. Distribusi jumlah paket serangan

Pie chart di atas menunjukkan DoS mendominasi 77 %, diikuti *brute-force* 12 %, dan *port scanning* 11 % — mencerminkan karakteristik serangan yang berbeda secara volume. Hasil analisis forensik *wireshark* vs *alert snort*

1. *Port Scanning*: Pola > 2.000 paket TCP SYN dari satu IP dalam b*urst* < 4 detik, respons server RST,ACK pada port tertutup → *Snort* memicu *alert* SYN *Scan* tepat sesuai *threshold* 20 SYN/3 detik.

2. ICMP *Flood*: 15.553 paket dalam 11 detik (1.414 pps), *Echo Request/Reply* berurutan → *Snort* langsung memicu *alert* pada paket ke-11 karena melebihi 10 ICMP/detik dari satu sumber.

3. *Brute-Force*: Banyak TCP *handshake* lengkap (SYN → SYN,ACK → ACK → SSH *banner* & *key-exchange*) dari *source port* berbeda dalam waktu singkat → *Snort* memicu alert pada koneksi ke-6 dalam 60 detik.

Validasi menunjukkan korelasi 100 % antara analisis manual *wireshark* dan *alert snort*.

V. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan *Intrusion Detection System* (IDS) berbasis *Snor*t 3.9.5 pada *Raspberry Pi* 4 Model B yang mampu mendeteksi 100 % serangan *port scanning*, ICMP f*lood* (DoS), serta *brute-force* terhadap layanan SSH dan aplikasi web tanpa menghasilkan *false positive*. Tanpa IDS, server target dapat ditembus sepenuhnya dalam waktu kurang dari lima menit; setelah IDS aktif, setiap tahapan serangan terekam secara akurat dengan alert real-time, memberikan waktu respons yang cukup bagi administrator. Sistem ini hanya mengonsumsi daya rata-rata 5,1 W, beban CPU maksimum 31 %, serta mampu menganalisis 15.553 paket dalam 9,4 detik dengan biaya total di bawah Rp 2 juta. Solusi ini terbukti efektif, hemat energi, dan sangat layak direplikasi secara massal oleh satuan TNI Angkatan Udara maupun institusi militer lainnya yang memiliki keterbatasan anggaran dan pasokan listrik.

Untuk pengembangan selanjutnya, disarankan mengintegrasikan *Snort* dengan *nftables* atau *Suricata* dalam mode *inline* sehingga sistem dapat berevolusi menjadi *Intrusion Prevention System* (IPS) yang memblokir serangan secara otomatis. Penambahan modul *machine learning* berbasis *anomaly detection* serta integrasi dashboard terpusat (ELK *Stack* atau *Graylog*) akan meningkatkan kemampuan mendeteksi serangan *zero-day* dan mempermudah pemantauan. Pengujian lanjutan pada jaringan produksi dengan trafik > 500 Mbps serta deployment skala besar di beberapa lanud dan pos komando terpencil juga perlu dilakukan untuk memvalidasi performa dalam kondisi operasional nyata TNI Angkatan Udara.

p-ISSN 2685-8991
e-ISSN 2808-2540

REFERENSI

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in Proc. 6th Int. Conf. Inf. Warfare Security (ICIW), Washington, DC, USA, 2011, pp. 113–125.

[2] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, Dec. 2019, Art. no. 20, doi: 10.1186/s42400-019-0038-7.

[3] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security Privacy (SP), Oakland, CA, USA, May 2010, pp. 305–316, doi: 10.1109/SP.2010.25.

[4] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Publication 800-94, Feb. 2007. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-94

[5] E. Upton and G. Halfacree, Raspberry Pi User Guide, 5th ed. Hoboken, NJ, USA: Wiley, 2022.

[6] Raspberry Pi Foundation, "Raspberry Pi 4 Model B product brief," Raspberry Pi Foundation, Cambridge, U.K., Datasheet, Jul. 2024. [Online]. Available: https://www.raspberrypi.com/documentation/computers/raspberry-pi.html

[7] M. Roesch, "Lightweight intrusion detection system," U.S. Patent 7 188 178 B2, Mar. 6, 2007.

[8] M. N. Schmitt, Ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, ser. International Cyber Law Series. Cambridge, U.K.: Cambridge Univ. Press, 2017, vol. 2.

[9] Snort Team, Snort 3 User Manual and Rule Writing Guide, Cisco Systems, San Jose, CA, USA, 2024. [Online]. Available: https://docs.snort.org/

[10] R. Fauzi, "Sistem keamanan jaringan komputer berbasis teknik intrusion detection system (IDS) untuk mendeteksi serangan distributed denial of service," M.S. thesis, Dept. Inf. Technol., Univ. Pendidikan Indonesia, Bandung, Indonesia, 2023.

[11] Mandiant, "M-Trends 2024: Special report," Mandiant, 2024. [Online]. Available: https://www.mandiant.com/resources/reports/m-trends-2024 (Diakses: 15 Nov. 2025).