INTRUSION DETECTION SYSTEM (IDS) MENGGUNAKAN *RASPBERRY PI* 4 DENGAN *SNORT* STUDI KASUS : LABORATORIUM JARINGAN KOMPUTER POLITEKNIK NEGERI BENGKALIS

Wahyat wahyat[1)], Ryci Rahmatil Fiska[2)], Dedi Hermawan[3)]

[1,2]Teknik Informatika, Politeknik Negeri Bengkalis, Jl. Bathin Alam, Bengkalis, 28711
[3]Pranata Laboratorium Pendidikan, Politeknik Negeri Bengkalis, Jl. Bathin Alam, Bengkalis, 28711
Email : wahyat@polbeng.ac.id, rycirahmatilfiska@polbeng.ac.id, dedihermawan@polbeng.ac.id

Abstract

Server security on a computer network is very important, maintaining computer network security for the sake of maintaining information, data and maintaining infrastructure so that it can work and function properly and provide access rights to registered users, this research, aims to build an Intrusion Detection System (IDS) on networks and servers using Raspberry Pi 4 with SNORT which is useful for monitoring server activities when an attack attempt occurs by sending notifications to the Telegram BOT via the administrator's cellphone in realtime, this IDS system is carried out with three attack testing scenarios, namely, scenario 1 PING Attack, scenario 2 Port Scanning, scenario 3 DOS / DDoS Attack. From the results of testing attacks or attacks using Linux times, SNORT can detect and provide alerts that are stored in the Snort Log and forwarded to the Telegram BOT notification in real time.

Keywords: *Raspberry pi 4, Server, IDS, Snort, Bot Telegram*

Abstrak

Keamanan server pada jaringan komputer menjadi hal yang sangat penting, menjaga keamanan jaringan komputer demi terjaganya informasi, data-data serta menjaga infrastruktur agar dapat bekerja dan berfungsi dengan baik dan memberikan hak akses kepada pengguna yang terdaftar, penelitian ini, bertujuan membangun *Intrusion Detection System (IDS)* pada jaringan dan Server menggunakan *Raspberry Pi 4* dengan *SNORT* yang berguna untuk memonitoring aktivitas Server ketika terjadi percobaan serangan dengan mengirimkan notifikasi ke *BOT Telegram* melalui handphone administrator secara *realtime*, sistem IDS ini di lakukan dengan tiga skenario pengujian serangan yaitu, skenario 1 *PING Attack*, skenario 2 *Port Scanning*, skenario 3 *DOS/DDoS Attack*. Dari hasil pengujian *attack* atau serangan menggunakan kali linux, *SNORT* dapat mendeteksi dan memberikan *alert* yang disimpan pada *Log Snort* dan diteruskan ke notifikasi *BOT Telegram* secara *realtime*.

Kata Kunci: *Raspberry pi 4, Server, IDS, Snort, Bot Telegram*

PENDAHULUAN

Keamanan jaringan komputer dan server menjadi poin utama yang harus di rawat dan dijaga, bagi seorang administrator jaringan sangat penting untuk bisa melakukan pencegahan dan identifikasi pengguna yang tidak berhak untuk mengakses jaringan komputer (Anis et al., 2022)

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

Keamanan jaringan komputer bertujuan untuk menjaga stabilitas, integritas, dan validitas data, pentingnya dalam menjaga keamanan jaringan membantu dalam menjaga informasi-informasi, data-data, serta menjaga infrastruktur agar berfungsi dengan baik dan benar (Zuma et al., 2021). Menjaga keamanan jaringan komputer bisa menghindari resiko terjadinya penyusupan atau ancaman yang bisa mengakibatkan kerusakan fungsi pada jaringan tersebut. Akibat dari tidak menjaga keamanan jaringan komputer dapat berupa *interruption, interception, modification,* dan *fabrication* pada jaringan komputer (Satwika et al., 2020).

Pada Laboratorium jaringan komputer jurusan teknik informatika Politeknik Negeri Bengkalis belum tersedianya layanan *Intrusion Detection System (IDS),* Bagaimana membangun *Intrusion Detection System* berbasis *Raspberry Pi* 4 dengan *Snort*, penelitian ini bertujuan untuk meningkatkan keamanan jaringan dengan menerapkan (*IDS*) berbasis *Raspberry pi 4* dengan *Snort* dan notifikasi *BOT Telegram*. *Snort* adalah aplikasi berbasis *open source* yang dapat berfungsi untuk mendeteksi atau memberikan *alert* adanya percobaan serangan pada jaringan komputer (Parag Vadher, 2020), *BOT Telegram* menjadi media untuk menerima *alert* atau notifikasi ketika terjadi upaya *attack* atau penyerangan sehingga informasi serangan bisa di terima secara *realtime.*(Yuwono, 2022)

METODE PENELITIAN

Pelaksananaan penelitian agar terarah dan terstruktur maka tahapan penelitian dimulai dari pengumpulan data, analisa kebutuhan dan perancangan *Intrusion Detection System* (IDS), Pembuatan *Intrusion Detection System*, integrasi dan implementasi *Intrusion Detection System*, pengujian dan analisa hasil pengujian, dokumentasi dan pelaporan hasil penelitian. Tahapan penelitian dapat dilihat pada gambar

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

Gambar 1. Tahapan Penelitian

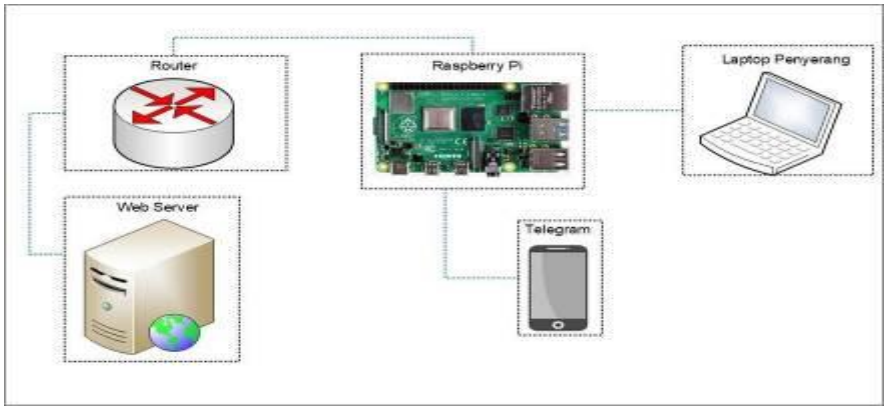
Analisa kebutuhan dilakukan untuk mendapatkan kebutuhan pengguna, untuk membangun *Intrusion Detection System* memerlukan perangkat keras dan perangkat lunak sebagai berikut :

Tabel 1. Kebutuhan *Hardware* dan *Software*

Hardware/Software	**Penggunaan**
Router Board	Manajemen IP Addres dan Jaringan Komputer
***Raspberry Pi* 4 (*Sd Card* dan *case*)**	*Intrusion Detection System (IDS)*
Switch	Terminal Jaringan Komputer
Kabel *UTP*	Kabel LAN
Laptop/PC	*Attacker / Kali Linux*
Komputer *PC*	*Web Server*
Ubuntu Server	Sistem Operasi *IDS*
Snort	*Rule Intrusion Detection System (IDS)*

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

Topologi *Intrusion Detection System (IDS)* menerapkan konsep Jaringan *Client – Server*, Laptop Penyerang terhubung ke *Raspberry Pi 4*, *Smartphone* terhubung ke *Raspberry Pi* 4, *Router Board/Mikrotik* Terhubung ke *Raspberry Pi (IDS),* dan *Router* terhubung ke *Web Server.*



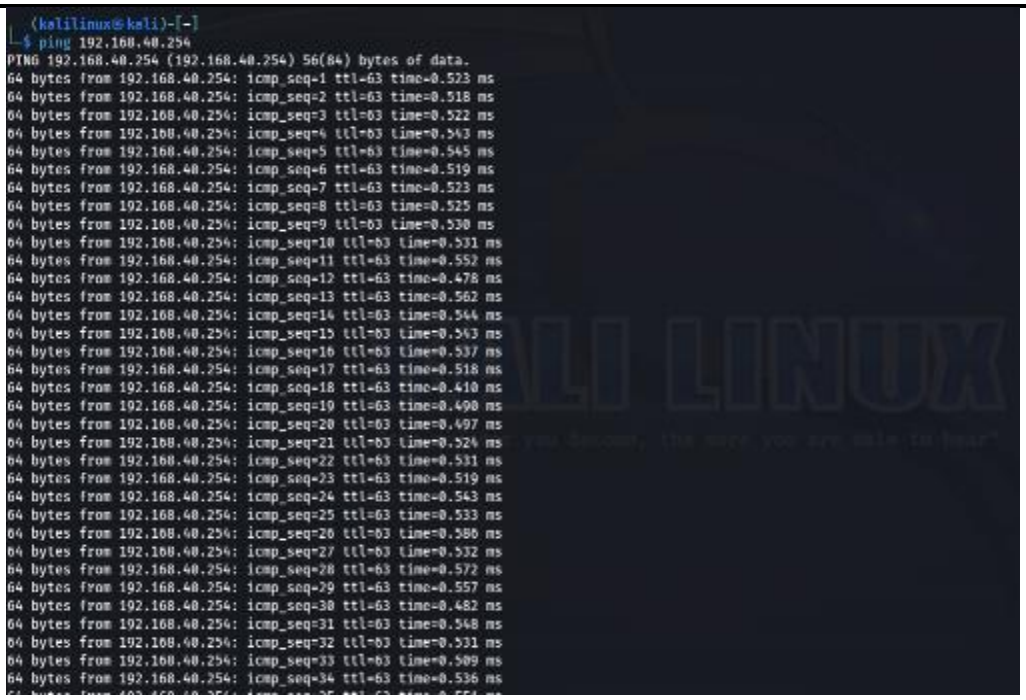
Gambar 2. Topologi *Intrusion Detection System (IDS)*

HASIL DAN PEMBAHASAN

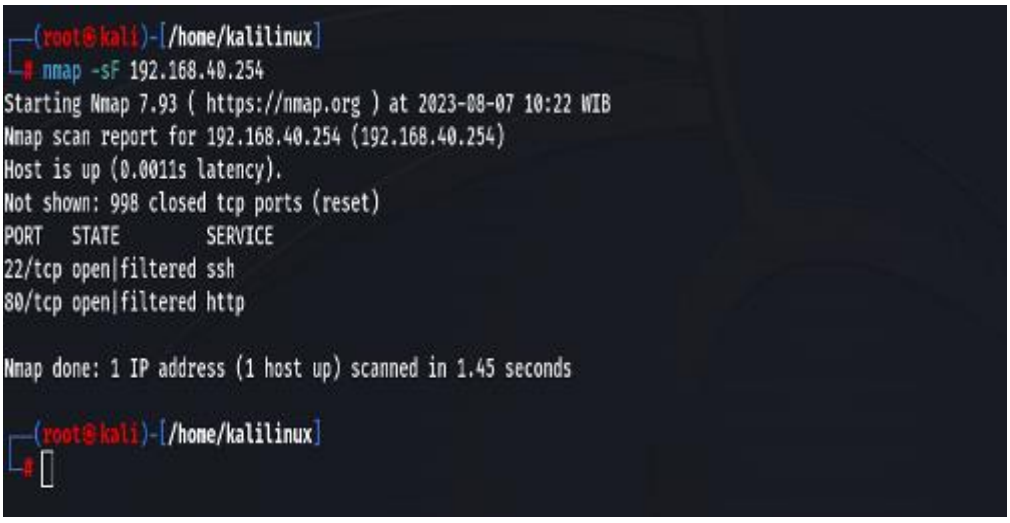
Hasil penelitian yang dilakukan berupa *prototype Intrusion Detection System (IDS)* di Laboratorium Jaringan Komputer Politeknik Negeri Bengkalis. Skenario pengujian *Intrusion Detection System (IDS)* ada 3 yaitu *PING Attack, Port Scanning*, dan *DOS/DDoS Attack* menggunakan sistem operasi *Kali Linux.*

Skenario pengujian ke 1 adalah *ping Attack* menggunakan *Kali Linux* dengan Alamat perintah "`ping 192.168.40.254`", skenario pengujian ke 2 adalah *Port* Scanning menggunakan *Kali Linux* dengan perintah "`nmap -sF 192.168.40.254`", skenario pengujian ke 3 *DOS/DDoS Attack* menggunakan *Kali Linux* dengan perintah "`hping3 -S -p 80 192.168.40.254`", hasil perintah pengujian skenario 1 *ping attack* dapat di tunjukkan pada gambar 3, hasil perintah pengujian skenario 2 *port scanning* dapat di tunjukkan pada gambar 4 dan hasil perintah pengujian skenario 3 *DOS/DDOS Attack* pada gambar 5.

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

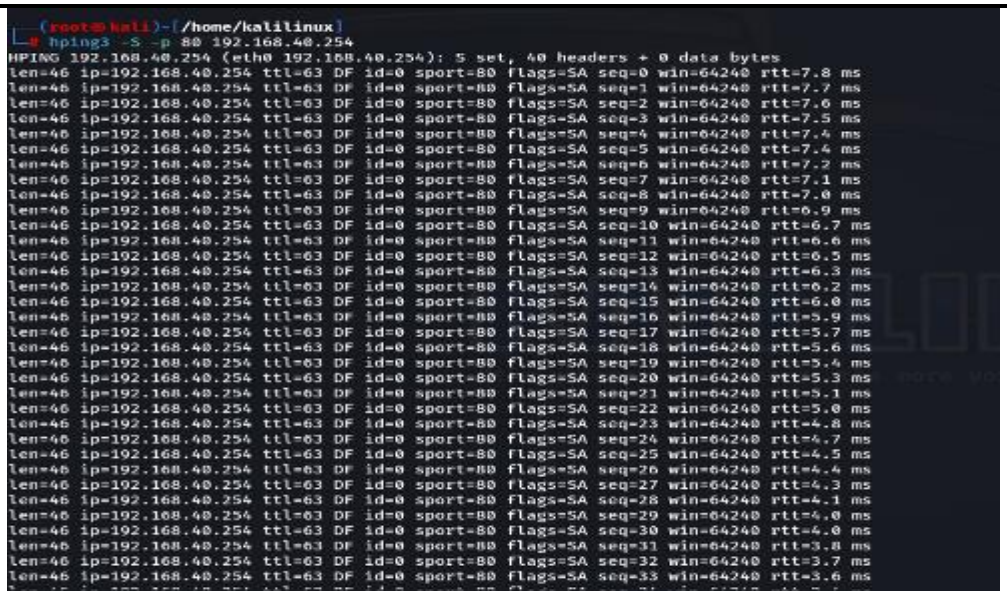


Gambar 3. Skenario 1 *Ping Attack*



Gambar 4. Skenario 2 *Port Scanning*

ISSN: 2303 – 2790
Bengkalis, 27 September 2023



Gambar 5. Skenario 3 *DDOS Attack*

Berikut hasil 3 skenario pengujian yaitu *PING Attack, Port Scanning,* dan *DOS/DDoS Attack, alert* atau notifikasi *attack* masuk pada *BOT Telegram.* Hasil pengujian skenario 1 dapat ditunjukan pada gambar 6, hasil pengujian skenario 2 dapat di tunjukkan pada gambar 7 dan hasil pengujian skenario 3 dapat ditunjukkan pada gambar 8.

Gambar 6. Notifikasi Skenario 1 *Ping Attack*

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

Gambar 7. Notifikasi Skenario 2 *Port Scanning*

Gambar 8. Notifikasi Skenario 3 *DDOS Attack*

ISSN: 2303 – 2790
Bengkalis, 27 September 2023

SIMPULAN

Sistem yang di usulkan adalah Intrusion Detection System (IDS) yang digunakan untuk mendeteksi attack atau serangan pada jaringan komputer, prototype IDS dibuat menggunakan Raspberry Pi 4 dengan SNORT, IDS diintegrasikan dengan BOT Telegram sebagai penerima alert atau notifikasi Ketika terjadi attack atau serangan secara realtime, dari hasil pengujian menggunakan 3 skenario *PING Attack, Port Scanning*, dan *DOS/DDoS Attack IDS* dapat mendeteksi adanya *attack* atau serangan dengan memberikan *alert* atau notifikasi ke *BOT Telegram* secara *realtime*.

DAFTAR PUSTAKA

Anis, M., Hilmi, A., & Khujaemah, E. (2022). Network Security Monitoring With Intrusion Detection System. *Jurnal Teknik Informatika (JUTIF)*, *3*(2), 249–253. https://doi.org/10.20884/1.jutif.2022.3.2.117

Parag Vadher. (2020). Snort IDPS using Raspberry Pi 4. *International Journal of Engineering Research And*, *V9*(07), 151–154. https://doi.org/10.17577/ijertv9is070099

Satwika, I. K. S., Sudiarsa, I. W., & Swari, M. H. P. (2020). Intrusion Detection System (Ids) Menggunakan Raspberry Pi 3 Berbasis Snort Studi Kasus: Stmik Stikom Indonesia. *SCAN - Jurnal Teknologi Informasi Dan Komunikasi*, *15*(3), 2–7. https://doi.org/10.33005/scan.v15i3.2279

Yuwono, D. T. (2022). Analysis Performance Intrusion Detection System in Detecting Cyber-Attack on Apache Web Server. *IT Journal Research and Development*, *6*(2), 169–178. https://doi.org/10.25299/itjrd.2022.7853

Zuma, M., Owolawi, P. A., Malele, V., Odeyemi, K., Aiyetoro, G., & Ojo, J. S. (2021). *Intrusion Detection System using Raspberry Pi and Telegram Integration*. 1–7. https://doi.org/10.1145/3487923.3487928

ISSN: 2303 – 2790
Bengkalis, 27 September 2023