**PROSIDING**
**Seminar Nasional Inovasi Teknologi Penerbangan (SNITP) Tahun 2023**
**ISSN : 2548 – 8112 eISSN: 2622-8890**

# MONITORING SISTEM KEAMANAN JARINGAN BERBASIS TELEGRAM PADA *LOCAL AREA NETWORK* DI POLITEKNIK PENERBANGAN SURABAYA

**Rifqi Fathin Al Hamid[1], Nyaris Pambudiyatno[2], Totok Warsito[3]**
[1,2,3)] Politeknik Penerbangan Surabaya, Surabaya, Indonesia, 60236
Email: rifqi5fathin@gmail.com

## Abstrak

Ancaman serangan siber menjadi masalah serius bagi keamanan jaringan,. Konsekuensi dari serangan siber dapat berdampak besar, bahkan mengganggu kinerja jaringan atau bahkan mengambil alih kontrolnya, contohnya pada jaringan kampus Politeknik Penerbangan Surabaya yang melayani layanan public . Monitoring sistem keamanan jaringan berbasis Telegram pada Local Area Network di Politeknik Penerbangan Surabaya adalah salah satu langkah awal dalam mencegah serangan yang berpotensi merusak jaringan. dengan merancang sistem untuk mendeteksi dan memberikan peringatan dini terhadap kemungkinan serangan. Hal ini memungkinkan administrator untuk segera mengambil tindakan pencegahan dan penanggulangan terhadap serangan tersebut. Metode yang digunakan dalam penelitian ini menggunakan metode pengembangan ADDIE.

**Kata Kunci:** Bot Telegram, Snort, IDS, IPS, Keamanan Jaringan, Honeypot

## Abstract

*The threat of cyber attacks is a serious problem for network security,. The consequences of a cyber attack can have a big impact, even disrupting network performance or even taking over its control, for example on the Surabaya Aviation Polytechnic campus network that serves public services. Telegram-based network security system monitoring on the Local Area Network at the Aviation Polytechnic of Surabaya is one of the first steps in preventing attacks that have the potential to damage the network. by designing a system to detect and provide early warning of possible attacks. This allows the administrator to immediately take preventive and countermeasures against the attack. The method used in this research uses the ADDIE development method.*

***Keywords:*** *Telegram Bot, Snort, IDS, IPS, Network Security, Honeypot*

## PENDAHULUAN

Aktivitas Pendidikan saat ini hampir sebagian besar operasional dilakukan secara online, hal ini dapat diartikan bahwa teknologi internet menjadi pilar utama dalam operasional institusi. Maraknya kegiatan cyber crime baru-baru ini dapat mencuri data melakukan penyadapan transmisi pada jaringan. Ancaman pada keamanan jaringan internet menjadi hantu yang menakutkan, khususnya bagi perusahaan maupun instansi dalam bidang teknologi yang memanfaatkan teknologi cloud computing. Selain itu dalam sepuluh tahun terakhir masyarakat kita sudah bergantung pada teknologi. Orang bergantung pada jaringan komputer untuk mendapatkan berita, berkomunikasi, belanja, hingga untuk keperluan penyimpanan file yang bersifat pribadi.

**ISSN : 2548 – 8112 eISSN: 2622-8890**

Karena mayoritas sistem cloud computing memberikan layanan kepada banyak individu, sistem ini rentan terhadap penyusupan oleh kejahatan siber. Biasanya, setiap sistem memiliki log yang mencatat peristiwa pada setiap perangkatnya. Data log memiliki peran krusial dalam mengidentifikasi aktivitas kriminal di dunia siber. Informasi mengenai sumber serangan, waktu kejadian, jenis serangan, dan dampak yang timbul yang tercatat dalam basis data intrusi, berguna untuk analisis forensik jaringan.

Diperlukan suatu sistem yang mampu memberikan informasi kepada administrator saat terjadi serangan, dan solusi yang diusulkan adalah merancang sistem notifikasi melalui aplikasi pesan instan Telegram. Langkah ini tidak hanya berfungsi sebagai tindakan pencegahan, tetapi juga memiliki manfaat dalam proses pengumpulan data forensik. Telegram, yang saat ini populer sebagai layanan pesan instan dengan model open-source, menawarkan berbagai fitur termasuk kemampuan bot yang dapat dimanfaatkan melalui berbagai API yang disediakan oleh platform ini. Bot Telegram mampu secara otomatis mengirimkan pesan dan perintah sesuai dengan perannya masing-masing.

Pilihan Telegram sebagai sarana notifikasi dalam penelitian ini didasarkan pada kemampuannya untuk mengirimkan banyak notifikasi dari sistem keamanan. Dengan Telegram, semua file dan pesan yang diterima akan disimpan di cloud, mengurangi penggunaan memori pada perangkat administrator dan memungkinkan proses pengiriman yang lebih cepat.

## METODE

Penelitian ini menggunakan Teknik Intrusion Detection and Prevention System (IDPS) yang merupakan gabungan teknologi IDS dan IPS yang berfungsi sebagai sistem pencegahan intrusi dan peringatan dini. IDS adalah fungsi pemantauan dan kemudian menganalisis kejadian sistem pada jaringan komputer untuk menemukan kemungkinan gangguan eksternal pada sistem yang melanggar atau mengancam kebijakan keamanan komputer atau praktik keamanan informasi standar.[1]

IDS adalah aktivitas memantau aktivitas pada sistem jaringan komputer dan kemudian menganalisisnya untuk kemungkinan gangguan asing yang memasuki sistem yang melanggar atau mengancam kebijakan keamanan informasi atau praktik keamanan standar. Pada penelitian yang dilakukan menggunakan jenis IDPS berdasarkan setupnya yaitu Network Intrusion Detection and Prevention System (NIDPS). Jenis penerapan ini memposisikan sistem IDPS sebagai pintu gerbang ke jaringan yang dilindungi. Semua akses ke jaringan server melewati sistem IDPS untuk diperiksa dan dicocokkan dengan aturan aplikasi IDPS (dalam hal ini Snort) untuk paket yang masuk.[2]

Pada tahap pengumpulan data, dilakukan analisis mendalam terhadap kebutuhan system monitoring keamanan jaringan dalam LAN, analisis jenis intrusi yang akan diuji coba dan analisis proses kerja Snort. Aplikasi Telegram yang terintegrasi dengan Snort dibutuhkan sebagai monitoring sistem keamanan jaringan. Beberapa jenis intrusi yang akan diuji adalah DoS (Denial of Service), Port Scanning, Worm/Botnet, dan Brute Force.

Terdapat 2 tahapan yaitu Needs Assessment dan Front-end Analysis. Needs Assessment (Analisis Kebutuhan) berupa analisis keadaan lapangan dan peserta serta

**ISSN : 2548 – 8112 eISSN: 2622-8890**

pengumpulan referensi materi yang akan dijadikan pokok bahasan dalam pengembangan. Kegiatan analisis lapangan dilakukan dengan pengumpulan informasi tentang monitoring keamanan jaringan LAN kampus Politeknik Penerbaangan Surabaya. Hasil informasi yang didapat mengenai monitoring keamanan jaringan LAN di kampus Politeknik Penerbangan Surabaya yaitu:

1. Monitoring dilakukan saat jam kerja dan juga kondisional dengan sistem keamanan yang disediakan oleh server.
2. Maintenance yang dilakukan saat setalah mengetahui adanya kerusakan atau hal aneh telah masuk pada server.
3. Memerlukan Hazard agar potensi atau kemungkinan terjadinya bahaya maupun risiko yang dapat menyebabkan kerusakan, kecacatan, atau bahkan unfunction terhadap jaringan juga server dapat ditaukenali dan lebih dahulu untuk antisipasi.
4. Memerlukan monitoring system keamanan jaringan berbasis telegram agar hazard dapat berjalan dengan baik.

Kegiatan selanjutnya ialah Front-end Analysis dengan cara mengumpulkan referensi berupa jurnal, website, serta video dalam kanal yang berkaitan dengan proyek dan lain-lain yang dibutuhkan dalam pengembangan.

Proses kerja Snort dimulai dengan mendownload serta instalasi snort. Setelah instalasi, tahap selanjutnya adalah konfigurasi snort, menentukan antarmuka jaringan yang akan dipantau sehingga dapat memantau jaringan secara real-time. Selanjutnya memasukkan rules yang akan disiapkan sebagai deteksi penyerangan dalam format bahasa dan aturan khusus yang dimiliki oleh Snort. Snort siap dijalankan, pemantauan akan dilakukan oleh Snort sesuai dengan lalu lintas jaringan antar muka yang telah ditetapkan diawal. Snort menganalisis paket jaringan yang melewati antarmuka tersebut dan membandingkannya dengan rules deteksi yang telah ditentukan.[3]

Snort akan memeriksa setiap paket yang diterima berdasarkan aturan deteksi yang telah dikonfigurasi. Jika ada paket yang cocok dengan pola atau perilaku mencurigakan yang dijelaskan dalam aturan, Snort akan memicu alarm atau menghasilkan pesan peringatan. Snort mencatat semua kejadian yang terjadi, termasuk serangan yang terdeteksi dan informasi paket terkait. Log ini dapat digunakan untuk analisis lebih lanjut dan pelaporan keamanan. Selanjutnya Snort didesain agar dapat mengirimkan isi log secara real-time melalui pesan API bot Telegram.[4]

Tahap desain merupakan tahapan perancangan monitoring sistem keamanan jaringan berbasis Telegram pada Local Area Network di kampus Politeknik Penerbangan Surabaya yang meliputi rumusan tujuan pembuatan, pembuatan flowchart untuk alur monitoring sistem keamanan jaringan berbasis Telegram, pengumpulan objek rancangan, dan penyusunan instrument untuk menguji kelayakan monitoring sistem keamanan jaringan berbasis Telegram ini.

Pada tahap ini, monitoring sistem keamanan jaringan berbasis Telegram akan dikembangkan sesuai dengan rencana yang telah dirancang sebelumnya. Ini melibatkan pengkodean dan konfigurasi perangkat lunak yang diperlukan, serta integrasi dengan infrastruktur jaringan yang ada.

a) Instalasi VirtualBox

VirtualBox adalah perangkat lunak

**ISSN : 2548 – 8112 eISSN: 2622-8890**

virtualisasi yang digunakan untuk mengeksekusi sistem operasi "tambahan" di dalam sistem operasi "utama".

b) Instalasi Linux Ubuntu pada VirtualBox

Linux adalah sebuah sistem operasi berbasis kernel (inti sistem operasi) yang bersifat open source (sumber terbuka). Penulis men-install Linux Ubuntu pada VirtualBox.

c) Instalasi dan konfigurasi aplikasi Snort pada Linux Ubuntu

d) Pembuatan Bot API Telegram

e) Setting Snort agar terhubung dengan Telegram

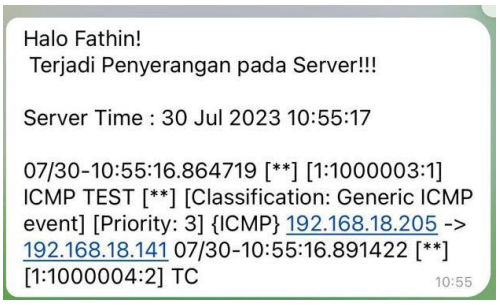
Setelah sistem monitoring dapat dijalankan, langkah selanjutnya adalah mengimplementasikannya di dalam jaringan lokal area. Penulis akan menampilkan data serangan yang terdeteksi oleh Snort dan data monitoring yang tampil pada telegram selama pengujian.

## HASIL DAN PEMBAHASAN

Pada penelitian ini dilakukan percobaan ping IP dan serangan Nmap kepada replica server menggunakan Laptop.

1. Pengujian ping IP

Percobaan ping IP dilakukan menggunakan bantuan device lain untuk ping IP server.




*Gambar 1 Notifikasi Percobaan Ping IP*

Notifikasi muncul pada pukul 10:55:57 sebab dari ping IP yang telah dilakukan pada percobaan dari IP 192.168.18.205 kepada 192.168.18.141.

2. Pengujian serangan Nmap


*Gambar 2 Notifikasi Serangan Nmap*

Notifikasi muncul pada Admin saat pengujian serangan Nmap pukul 11:07:42 dengan keterangan "TCP Port Scanning" dari IP 192.168.18.205 menyerang IP 192.168.18.141.

## PENUTUP

### Simpulan

Pemanfaatan sebuah Intrusion Detection System (IDS) efektif dalam pemantauan lalu lintas jaringan. Berdasarkan hasil penelitian pada artikel ini, sistem IDS berhasil mendeteksi serangan yang pertama kali dilakukan pada proses konfigurasi dan penambahan aturan sehingga snort dapat mendeteksi serangan berdasarkan pencocokan signature yang terdapat pada aturan tersebut. Fokus proyek ini lebih pada membangun sistem pemantauan keamanan jaringan, menghasilkan output melalui notifikasi pesan instan Telegram.

### Saran

Berdasarkan proyek yang telah dilakukan, saran dari penulis terhadap proyek ini adalah :

1. Tingkat keamanan yang perlu ditingkatkan, perihal fasilitas tambahan yang telah direncanakan yaitu aplikasi

**ISSN : 2548 – 8112 eISSN: 2622-8890**

Honeypot. Hal ini dapat menjadi pengembangan dalam penelitian selanjutnya.

2. Diharapkan peneliti selanjutnya untuk dapat meningkatkan keamanan dan menambahkan rules pada snort agar dapat mendeteksi serangan yang lebih bervariasi.

## DAFTAR PUSTAKA

[1] Nasution M I P 2012 Implementasi Pemrograman Java Untuk Alert Intrusion Detection System Unpublished

[2] Riadi I, Mualfah D and Riadi I 2017 Network Forensics for Detecting Flooding Attack on Web Server Int. J. Comput. Sci. Inf. Secur. 15 326–31

[3] Dasmen R N, Ariyanto C, Surya M H and Ramadhan H 2022 Penerapan Snort Sebagai Sistem Pendeteksi Serangan Keamanan Jaringan Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform. 7 8

[4] M.R. A and P. V 2022 Review of Cyber Attack Detection: Honeypot System Webology 19 5497–514