Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer

Azzahra Rahmatillah[1)], Ali Firdaus[1)], Ema Laila[1)]
[1,2,3] Jurusan Teknik Komputer, Politeknik Negeri Sriwijaya,
Jalan Srijaya Negara, Palembang, Sumatera Selatan 30139
e-mail: *azzahrarahmatillah00@gmail.com, alifirdaus1970@gmail.com, emalaila@gmail.com

Abstrak

Pada keamanan jaringan memiliki beberapa metode yang digunakan untuk mengamankan jaringan tersebut. Pada penelitian ini menggunakan metode Intrusion Prevention System yang merupakan sebuah metode keamanan yang memanfaatkan teknologi firewall pada MikroTik. Intrusion Prevention System (IPS) adalah perangkat lunak yang berkerja untuk mendeteksi aktifitas yang mencurigakan dan melakukan pencegahan terhadap intrusi pada jaringan. Pada router MikroTik yang menyediakan beberapa fasilitas untuk mendukung keamanan dan akses jaringan dapat diterapkan sebuah sistem untuk mendeteksi jika terjadi penyerangan pada jaringan komputer. Serangan atau penyusupan dapat dicegah dengan menerapkan Intrusion Prevention System dan serangan dapat terdeteksi tergantung pada pola serangan yang ada di dalam rule IPS. Administrator system dapat mengetahui serangan yang terjadi pada server internet melalui pesan notifikasi yang memuat informasi jenis serangan dan kapan terjadinya yang dikirim oleh system yang dibuat melalui Telegram.

Kata kunci*— Keamanan Jaringan, Intrusion Prevention System, MikroTik, Pencegahan Serangan, Telegram.*

Abstract

In network security, there are several methods used to secure the network. In this study, the Intrusion Prevention System method is used, which is a security method that utilizes firewall technology on MikroTik. Intrusion Prevention System (IPS) is software that works to detect suspicious activity and prevent intrusion on the network. On MikroTik routers that provide several facilities to support security and network access can be applied a system to detect in case of attacks on computer networks. Attacks or intrusions can be prevented by implementing the Intrusion Prevention System and attacks can be detected depending on the pattern of attacks contained in the IPS rules. System administrators can know the attacks that occur on internet servers through notification messages containing information on the type of attack and when it occurred sent by the system created through Telegram.

Keywords— *Network Security, Intrusion Prevention System, MicroTic, Attack Prevention, Telegram.*

1. PENDAHULUAN

Salah satu perkembangan pesat dalam bidang teknologi informasi adalah bidang jaringan. Seiring dengan pesatnya perkembangan teknologi, proses untuk mengakses jaringan *internet* menjadi sangat mudah. Jaringan *internet* bukanlah hal yang asing bagi kita karena

jaringan *internet* ini dapat kita jumpai di setiap tempat seperti sekolah, kantor, restoran, universitas, dan sebagainya.

Pada Jurusan Teknik Komputer pengaksesan jaringan *internet* bisa dilakukan secara bebas oleh mahasiswa. Contohnya seperti pada laboratorium yang memiliki komputer dimana setiap komputer saling terhubung ke jaringan *internet*, pada setiap komputer pada laboratorium menyimpan data-data yang penting dimana data tersebut merupakan data-data untuk keperluan proses pembelajaran mahasiswa. Seiring dengan semakin seringnya penggunaan jaringan *internet*, semakin besar pula potensi terkena ancaman keamanan terhadap *router* sebagai penyedia sumber *internet*.

Keamanan jaringan merupakan sebuah proses pencegahan dan identifikasi dari aktifitas penggunaan yang tidak sesuai serta dari jaringan komputer tersebut. Keamanan jaringan juga bertujuan untuk mengantisipasi ancaman dan resiko dalam bentuk logika maupun fisik yang mengganggu secara langsung dan tidak langsung [1]. Oleh karena itu diperlukan *system* yang dapat membantu administrator jaringan untuk memonitoring dan mencegah serangan.

Untuk mendeteksi dan mencegah serangan digunakan *Intrusion Prevention System* (IPS). Intrusion Prevention Sistem (IPS) adalah sebuah aplikasi yang bekerja untuk mendeteksi aktivitas mencurigakan, dan melakukan pencegahan terhadap intrusi atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti bagaimana mestinnya. Secara konsep, IPS adalah sistem yang mampu atau memiliki fungsi mendeteksi dan memberikan penanganan serangan. Dengan kata lain, IPS merupakan pengembangan dari IDS dengan menambahkan beberapa komponen seperti firewall dan beberapa komponen lain untuk bekerja sama dalam mencegah dan menghentikan terjadinya penyusupan dari client [2].

2. METODE PENELITIAN

2.1 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan adalah dengan studi pustaka dan penelitian sejenis. Dalam tahapan ini dipelajari teori – teori yang terkait dengan topik penelitian yang dapat mendukung pemecahan masalah. Pencarian referensi dilakukan dengan membaca buku maupun mencari jurnal di internet dari hasil yang sudah pernah dikerjakan sebagai bahan perbandingan terhadap penelitian yang akan dikerjakan. Pustaka – pustaka yang dijadikan acuan dapat dilihat pada halaman daftar pustaka.

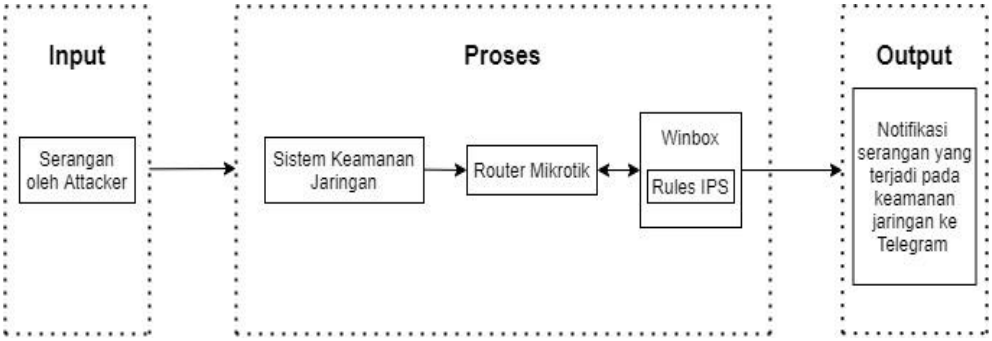
2.2 Spesifikasi Hardware dan Software

Spesifikasi *hardware* yang digunakan pada rancangan sistem ini adalah laptop ASUS dengan sistem operasi *windows* 10 *Pro* 64-bit, processor Intel(R) Core(TM) i5- 8250U CPU @ 1.60GHz 1.80 GHz- Memori 4 GB RAM dan mouse sebagai perangkat pendukung laptop dan spesifikasi *software* yang digunakan pada rancangan sistem ini adalah *winbox* sebagai aplikasi untuk mengkonfigurasi *MikroTik*.

2.3 Perancangan Sistem

Sub bab ini membahas perancangan system yang akan dilakukan pada penelitian ini :

2.3.1 Diagram Blok



Gambar 2.1 Blok Diagram

2.3.2 Flowchart

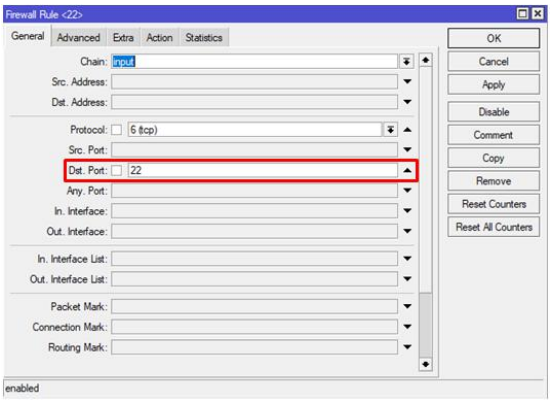
Berikut adalah diagram alir rancang bangun pada *MikroTik*.

Gambar 2.2 *Flowchart*

2.3.3 Konfigurasi IPS

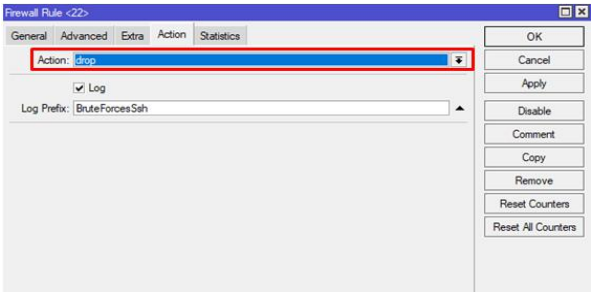
Konfigurasi IPS dilakukan pada menu *firewall* yang terdapat di *winbox*. Untuk mengkonfigurasi IPS dilakukan pada *filter rules.* Untuk menentukan rules pada setiap jenis serangan, maka ditentukan melalui port-port sesuai dengan setiap jenis serangan. Pada

penelitian digunakan 4 jenis serangan, yaitu *brute force* ssh dengan port 22, *brute force* ftp dengan port 21, dan *brute force telnet* dengan port 23. Sedikit berbeda dengan *port scanner* yang bertujuan untuk melihat port yang terbuka pada *firewall* maka untuk *port scanner* pada kolom dst *port* tidak ditentukan.



Gambar 2.3 Port Serangan

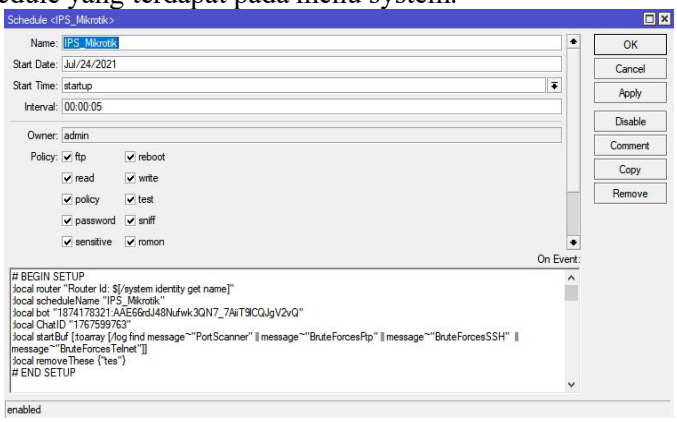
Pada konfigurasi IPS ini, selain menentukan port sesuai dengan jenis serangan, mengatur juga action atau tindakan yang akan dilakukan jika ada serangan yang masuk. IPS bertindak sebagai pencegah serangan, maka action pada *firewall* diatur menjadi *drop* yang artinya serangan yang masuk akan diblokir.



Gambar 2.4 Action Serangan

2.3.4 Koneksi MikroTik ke Telegram

Koneksi *MikroTik* ke *telegram* bertujuan untuk memberikan notifikasi serangan yang terjadi pada *MikroTik* sebagai sumber internet. Untuk menghubungkan nya maka perlu mengisikan *Log Prefix* seperti pada gambar 3.4 sesuai dengan jenis serangan. *Log prefix* ini kemudian akan dieksekusi pada script yang mengkoneksikan *MikroTik ke* telegram. Koneksi ini dilakukan pada schedule yang terdapat pada menu system.



Gambar 2.5 Koneksi Mikrotik ke Telegram

3. HASIL DAN PEMBAHASAN

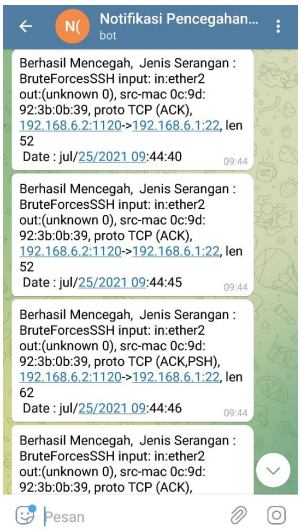
3.1 Brute Force SSH

Pengujian *Brute Force* SSH dilakukan dengan *Kali Linux* menggunakan aplikasi *Hydra.* Penyerangan dilakukan menggunakan *gateaway target*. SSH (*Secure Shell*) adalah protokol yang digunakan untuk megendalikan komputer dari jarak jauh untuk mengirim *file,* membuat tunnel yang terenkripsi, dan lainnya [3]. Pengujian SSH dilakukan dengan memasukkan *password* secara *random* berulang kali hingga mendapatkan *password* yang benar. Maka sebelum melakukan penyerangan, terlebih dahulu membuat *password list* yang akan dieksekusi.

```
root@kali:/home/laazzahra# hydra -l admin -P password.txt 192.168.100.162 ssh
```

Gambar 3.1 *Brute Force* SSH menggunakan *Kali Linux*

Jika upaya SSH sudah dilakukan, maka secara otomatis akan muncul notifikasi melalui *telegram*. Dengan adanya notifikasi melalui *telegram* berarti bahwa serangan tersebut berhasil dicegah.



Gambar 3.2 Notifikasi Serangan *Brute Force* SSH pada *Telegram*

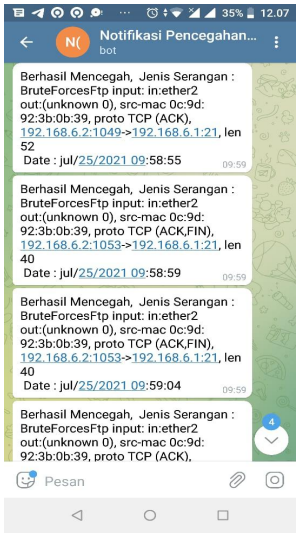
3.2 Brute Force FTP

Pengujian *Brute Force* FTP dilakukan dengan *Kali Linux* menggunakan aplikasi *Hydra.* Penyerangan dilakukan menggunakan *gateaway target*. *Port* 21 yang digunakan pada FTP diperuntukkan sebagai *transfer file*. FTP *server* menjalankan *software* yang digunakan untuk tukar – menukar *file*, yang selalu siap memberikan layanan FTP apabila mendapat *request* dari FTP *client* [4]. Pengujian FTP dilakukan dengan memasukkan *password* secara *random* berulang kali hingga mendapatkan *password* yang benar. Maka sebelum melakukan penyerangan, terlebih dahulu membuat *password list* yang akan dieksekusi.

```
root@kali:/home/laazzahra# hydra -l admin -P password.txt ftp://192.168.6.1
```

Gambar 3.3 *Brute Force* FTP menggunakan *Kali Linux*

Jika upaya FTP sudah dilakukan, maka secara otomatis akan muncul notifikasi melalui *telegram*. Dengan adanya notifikasi melalui *telegram* berarti bahwa serangan tersebut berhasil dicegah.



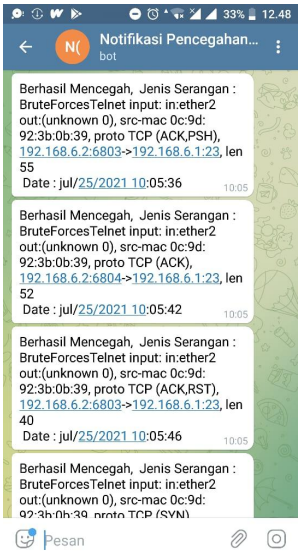
Gambar 3.4 Notifikasi Serangan *Brute Force* FTP pada *Telegram*

3.3 Brute Force Telnet

Pengujian *Brute Force* Telnet dilakukan dengan *Kali Linux* menggunakan aplikasi *Hydra.* Hampir sama seperti SSH, Telnet merupakan *protocol* yang bisa memberikan akses *remote* (jarak jauh) pada sebuah perangkat komputer. *Telnet* merupakan suatu protokol yang memungkinkan penggunanya dapat *login* dan bekerja pada sistem jarak jauh, seperti jika terdapat program maupun *file* yang tersimpan pada komputer jarak jauh tersebut berada di komputer pengguna [5]. Untuk mengeksekusi telnet juga digunakan password list.

Gambar 3.5 *Brute Force* SSH menggunakan *Kali Linux*

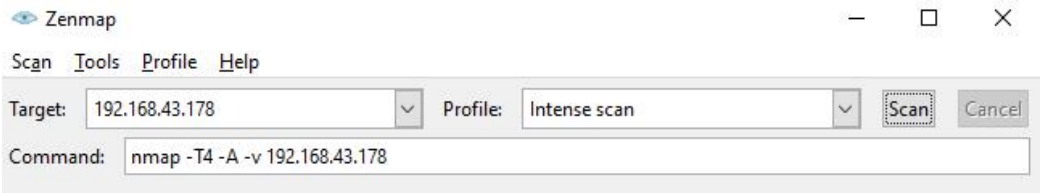
Jika upaya telnet sudah dilakukan, maka secara otomatis akan muncul notifikasi melalui *telegram*. Dengan adanya notifikasi melalui *telegram* berarti bahwa serangan tersebut berhasil dicegah.



Gambar 3.6 Notifikasi Serangan *Brute Force* Telnet pada *Telegram*

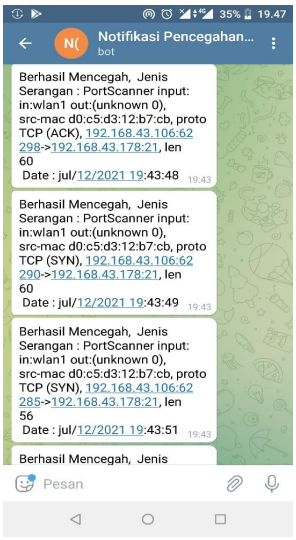
3.4 Port Scanner

Port scanning merupakan langkah awal serangan terhadap jaringan komputer. Dari keberhasilan melakukan *port scanning*, penyerang dapat melanjutkan serangan lanjutan ke jaringan komputer. Penyerangan *port scanning* dapat dilakukan dengan *Nmap* [5]. Port Scanner sedikit berbeda dari jenis serangan lain yang ditentukan melalui port. Pengujian *Port Scanner* dilakukan dengan menggunakan aplikasi *Nmap.* Penyerangan jenis *port scanner* digunakan untuk melihat *port* yang terbuka, tertutup dan *port* yang dilindungi *firewall* dengan memasukkan IP *target.*



Gambar 3.7 Port Scanner menggunakan Nmap

Saat proses port scanner sudah dijalankan melalui nmap maka secara otomatis notifikasi akan muncul melalui telegram. Dengan adanya notifikasi melalui *telegram* berarti bahwa serangan tersebut berhasil dicegah.



Gambar 3.8 Notifikasi Serangan *Port Scanner* Telnet pada *Telegram*

4. KESIMPULAN

Berdasarkan pembahasan yang telah dilakukan maka dapat ditarik kesimpulan yaitu :

1. Rules IPS yang diatur pada filter rules berfungsi untuk menentukan port dan action atau tindakan terhadap serangan yang terjadi.
2. Serangan yang terjadi akan terekam di menu log akan dikirimkan ke telegram.
3. Notifikasi telegram terjadi secara realtime sesuai dengan waktu serangan terjadi.
4. Notifikasi telegram memuat mengenai kapan serangan terjadi, jenis serangan, dan informasi IP.

5. SARAN

1. Membuat rules dengan jenis serangan yang lebih banyak.
2. Melakukan pengujian serangan dengan lebih dari satu perangkat, sehingga memiliki banyak perbandingan data.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Jurusan Teknik Komputer Politeknik Negeri Sriwijaya yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Ma'sum, Irwansyah, dan Priyanto. 2017. Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. *Jurnal Sistem dan Teknologi Informasi.* 5(1), 56.57.

[2] Monarfa, Mohammad., Najoan, Xaverius., Sinsuw, Alicia. 2016. *Analisa dan Implementasi Network Intrusion Prevention System Di Jaringan Universitas Sam Ratunglangi*. Jurnal Teknik Elektro Volume 5.

[3] Suprapto, Untung. 2018. *Komputer dan Jaringan Dasar.* Jakarta : PT. Gamedia Widiasarana Indonesia.

[4] Ryan, Nathan Gusti. 2018. *Basic Computer Networking.* Surabaya : Berkat Jaya.

[5] Huda. Miftahul. 2020. Keamanan Informasi. Nulisbuku.com.