PEMANFAATAN NOTIFIKASI TELEGRAM UNTUK MONITORING JARINGAN

Febriyanti Panjaitan
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Bina Darma
Email: febriyanti_panjaitan@binadarma.ac.id

Rusmin Syafari
Fakultas Ilmu Komputer, Program Studi Sistem Informasi
Universitas Bian Darma
Email: rusmin.syafari@binadarma.ac.id

ABSTRAK

Pemantauan server jaringan komputer sangat penting dilakukan untuk mempermudah seorang administrator dalam mengamati dan mengontrol sistem jaringan yang terpasang. Server harus mendapatkan perhatian yang lebih karena memiliki celah kelemahan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pada salah satu perguruan tinggi yang ada di sumatera selatan pada Tahun 2017 pernah mendapatkan sebuah serangan yaitu pada situs *web* sehingga mengakibatkan terjadinya perubahan tampilan (*deface*). Berdasarkan data yang didapat bahwa sistem pada *server* terdapat *port* yang cukup banyak terbuka seperti pada *port 80 hypertext transfer protocol (http), port 22 secure shell (SSH) dan port 21 ftp server.* Untuk mengatasi permasalahan tersebut maka perlu membuat model sistem *monitoring* serangan pada jaringan menggunakan *snort* dengan notifikasi Telegram untuk mendeteksi ada atau tidaknya serangan yang masuk kedalam sistem. Untuk melakukan deteksi serangan tersebut, maka digunakan IDS (*Intrusion Detection System*) sebagai perangkat dalam monitoring sistem, salah satu aplikasi yang digunakan IDS adalah Snort yang memanfaaatkan Aplikasi Telegram sebagai pemberitahuan adanya ancamanan serangan. Pengujian Serangan dilakukan dengan beberapa teknik yaiu *FTP Bruteforce Attack, Ddos Attack,* dan *SSH Bruteforce Attack* sehingga didapat sumber serangan berasal dari IP Address Luar dengan target IP Address server pada *port* 21, *port 80, port 22* serta mendapatkan *username "root"* dan *password* "*rockyou.txt*" menggunakan aplikasi Hping3 dan Hydra. Hasil penelitian menunjukkan sistem berhasil mendeteksi serangan yang dilakukan *attacker* yaitu adanya notifikasi yang dikirimkan secara otomatis melalui aplikasi telegram saat terjadi serangan sehingga administrator dapat mengetahui tentang kondisi server pada saat itu juga, rata-rata waktu dibutuhkan untuk mendeteksi serangan yang terkirim ke aplikasi telegram sekitar 0 *(nol)* detik.

Kata kunci: *monitoring; intrusion detection system; snort; telegram messenger.*

ABSTRACT

Monitoring a computer network server is very important to make it easier for an administrator to observe and control the installed network system. The server must get more attention because it has a vulnerability gap that can be exploited by irresponsible parties. In one of the universities in Sumatera Selatan in 2017, there was an attack on the website which resulted in a deface. Based on the data obtained that the system on the server there are quite a lot of open ports such as port 80 Hypertext Transfer Protocol (HTTP), port 22 Secure Shell (SSH) and port 21 FTP Server. To overcome these problems, it is necessary to make a model of monitoring the network attack system using snort with Telegram notification to detect the presence or absence of attacks that enter the system. In order to detect these attacks, IDS (Intrusion Detection System) is used as a device in monitoring the system, one of the applications used by IDS is Snort which utilizes the Telegram Application as a notification of the threat of attack. The attack test was carried out with several techniques, namely FTP Bruteforce Attack, Ddos Attack, and SSH Bruteforce Attack so that the source of the attack was obtained from the External IP Address with the target IP Address server on port 21, port 80, port 22 and get the username "root" and password " rockyou.txt "using the Hping3 and Hydra applications. The results showed the system succeeded in detecting attacks carried out by the attacker namely the notification that was sent automatically through the telegram application when an attack occurred so that the administrator could find out about the condition of the server at that time, the average time needed to detect attacks sent to the telegram application was around zero seconds.

Keywords: *monitoring; intrusion detection system; snort; telegram messenger.*

1. PENDAHULUAN

Kegiatan pendidikan dengan aktivitas yang cukup banyak membuat hampir sebagian besar operasional dilakukan secara *online*, sehingga dari hal tersebut dapat disimpulkan bahwa teknologi *internet* menjadi pilar utama dalam operasional institusi. Seiring dengan semakin berkembangnya teknologi *internet*, kejahatan yang memanfaatkan teknologi ini juga semakin meningkat, karena maraknya kegiatan *cyber crime* akhir-akhir ini yang bisa mencuri data dan penyadapan transmisi pada jaringan. Pemantauan server jaringan komputer sangat penting dilakukan untuk mempermudah seorang administrator dalam mengamati dan mengontrol sistem jaringan yang terpasang. Server harus mendapatkan perhatian yang lebih karena memiliki celah kelemahan yang bisa dimanfaatkan oleh pihak yang tidak bertanggung jawab.

Salah satu perguruan tinggi yang ada di sumatera selatan pada Tahun 2017 pernah mendapatkan sebuah serangan pada situs web yang mengakibatkan terjadinya perubahan tampilan *(deface).* Berdasarkan data penelitian terlihat bahwa sistem pada server terdapat port yang cukup banyak terbuka, sehingga dapat berpotensi kembali oleh para attacker untuk mengambil alih sistem tersebut. Hasil dari scanning terdapat banyak port yang terbuka seperti port 80 *hypertext transfer protocol* (http), port 22 *secure shell* (ssh) port 21 ftp server. Port 21 dan port 22 adalah port yang paling banyak digunakan oleh para attacker untuk menyerang suatu sistem demi mendapatkan akses ke sistem server dan file-file data yang akhirnya seorang attacker bisa membuat akses root yang mempunyai hak penuh terhadap system yang diserang.

Perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (monitoring) insiden yang terjadi dalam sistem jaringan serta menganalisa adanya masalah terhadap keamanan adalah *Intrusion Detection System* (IDS) [1]. Salah satu aplikasi yang digunakan sebagai IDS adalah Snort. Snort merupakan salah satu contoh dari *tools IDS opensource* yang dapat digunakan untuk mendeteksi ada atau tidaknya serangan yang masuk ke dalam sistem. *Snort* akan mendeteksi dan merekam serta menyimpannya ke database apabila ada seseorang yang mencoba masuk ke dalam sistem. Selain IDS, model monitoring akan memanfaaatkan Aplikasi Telegram sebagai pemberitahuan adanya ancamanan serangan. Aplikasi *instant messaging* Telegram saat ini popular digunakan oleh berbagai kalangan, karena mempunyai fitur-fitur yang sangat canggih dalam hal keamanan. Salah satu fitur dari telegram yaitu *Secret Chat, Secret Chat* dienkripsi dengan prosedur *end-to-end* sehingga isi pesan tersebut tidak bisa diakses oleh siapapun di perangkat lain hanya pengirim dan penerima sajalah yang dapat mengaksesnya.

Dari dua literatur review yang dilakukan yang berkaitan dengan penelitian yang ada, yaitu pada [2] melakukan pengujian serangan dengan menggunakan IDS dengan notifikasi serangan menggunakan Bot Telegram dan memberikan hasil notifikasi sebanyak 606 dari 8053 serangan dalam 24 jam. Sedangkan pada [3] menyatakan bahwa aplikasi snort dengan IDS dapat memberikan notifikasi pada administrator dan melakukan kontrol server melalui instant messaging Telegram dengan beberapa serangan seperti port scanning, FTP *Attack*, SSH *Attack* dan Ddos. Oleh karena itu IDS diterapkan karena mampu mendeteksi paket data pada lalu lintas jaringan, yang bertujuan untuk menemukan bukti berdasarkan sumber serangan, waktu kejadian, serta dampak dari serangan dan memberikan peringatan kepada administrator tentang kondisi jaringan saat itu untuk meminimalisir terjadinya pengambilan hak akses pada system.

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode tindakan atau *action research.* "*Action research* adalah penelitian untuk mengembangkan keterampilan-keterampilan baru atau cara pendekatan baru atau cara pendekatan baru untuk memecahkan masalah di dunia kerja atau dunia terapan lain. Tahapan penelitian dari *action research* ini adalah *Diagnosing, Action Planning, Action Taking, Evaluating, Learning.* [4] [5]

2.1 Diagnosing

Data yang didapat dalam melakukan penelitian ini adalah data sebuah serangan pada situs *web* salah satu perguruan tinggi yang ada di Sumatra Selatan beberapa tahun lalu yang mengakibatkan terjadinya perubahan tampilan *(deface)*. Dengan adanya data tersebut, maka dilakukan pengujian pada situs *web* dan peneliti bisa berhasil masuk sebagai Administrator ke salah satu *website* yang ada.

Gambar 1. ***Login Admin***

Dari hasil scanning sistem pada server terdapat *port* yang cukup banyak terbuka, sehingga dapat berpotensi kembali oleh para *attacker* untuk mengambil alih sistem tersebut. Tahap ini juga melakukan identifikasi *service* yang ada pada *webservice* tersebut, sehingga informasi mengenai sistem dapat diketahui secara detail. Berdasarkan hasil dari scanning sebelumnya terdapat banyak port yang terbuka seperti, *port 80 hypertext transfer protocol (http), port 22 secure shell (ssh)* dan *port 21 ftp server*. Biasanya serangan banyak dilakukan pada port yang rawan sepeti pada *port* 21 dan *port* 22 yang paling banyak digunakan oleh para attacker untuk menyerang suatu sistem demi mendapatkan akses ke *sistem server* dan *file-file* data yang akhirnya seorang *attacker* bisa membuat akases root yang mempunyai hak penuh terhadap sistem yang diserang.

```
Host is up (0.017s latency).
Not shown: 977 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
25/tcp   open|filtered smtp
80/tcp   open|filtered http
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
139/tcp  open|filtered netbios-ssn
143/tcp  open|filtered imap
443/tcp  open|filtered https
```

Gambar 2. ***scanning server***

2.2 Action Planning

Membuat rencana tindakan *(Action Planning),* Pada tahapan ini penelitian dilakukan dengan memahami pokok masalah yang ada dan menyusun rencana tindakan yang tepat dalam menyelesaikan masalah dan melakukan rencana tindakan yang akan dilakukan pada jaringan Universitas PGRI Palembang dengan membuat perancangan dan penerapan *Intrusion Detection System* dengan notifikasi Telegram. Rencana tindakan yang dilakukan sebagai berikut:

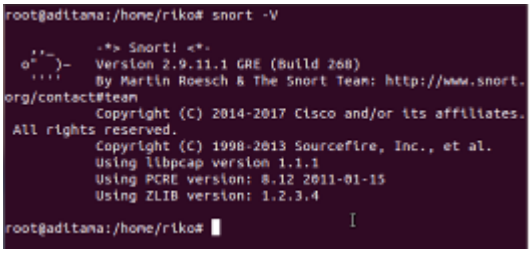
a. Melakukan instalasi dan konfigurasi *snort* serta aplikasi pendukung lainnya.
b. Melakukan konfigurasi pada IDS sehingga dapat terhubung dengan Aplikasi Telegram Messenger.
c. Melakukan pengujian serangan terhadap server untuk mengetahui system IDS sudah berjalan sesuai dengan keinginan. *Attacker* akan mencoba melakukan serangan dengan cara mencari kelemahan sistem keamanan jaringan pada Server. IDS yang terpasang pada server akan melakukan pengawasan terhadap kegiatan-kegiatan yang mencurigakan terjadi pada server, ketika *attacker* melakukan usaha penyusupan atau penerobosan ke server maka snort akan secara otomatis mendeteksi adanya *intruder*. Setelah *snort* mendeteksi usaha penyusupan, snort akan membuat *log file* hasi *capture* paket penyusupan tersebut.

3. HASIL DAN PEMBAHASAN

3.1 Action Taking

Bagian ini menjelaskan tentang proses instalasi serta konfigurasi yang harus dilakukan terlebih dahulu untuk membentuk sistem monitoring sebelum dilakukan pengujian.

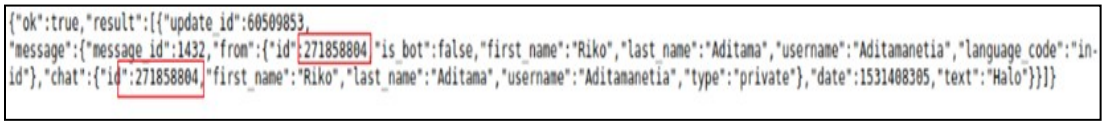
a. Instalasi Snort
Sistem operasi yang digunakan Ubuntu Desktop 12.04, dengan tahapan instalasi yaitu (1) install aplikasi pendukung snort, (2) instalasi *library* DAQ, (3) Instalsi Snort.



Gambar 3. Instaslasi Snort IDS berhasil

b. Konfirgurasi Snort
IDS snort akan melakukan proteksi terhadap ip, pada pengaturan ip IDS snort tidak hanya memberikan perlindungan pada 1 host saja (server web), tetapi juga memberikan perlindungan terhadap seluruh host serperti server database dan server *e-mail.*

c. Telegram Bot
Bot merupakan kependekan dari robot. Salah satu fungsi utama telegram bot adalah dimanfaatkan sebagai mesin robot otomatis yang mampu menjembatani antara pengguna dengan system **[1]**. Untuk membuat Bot penggunakan harus memlili akun yang sudah terdaftar pada Aplikasi Telegram, kemudian pengguna melakukan permintaan kepada @BotFather untuk mendapatkan *username, token* dan *id chat user.*

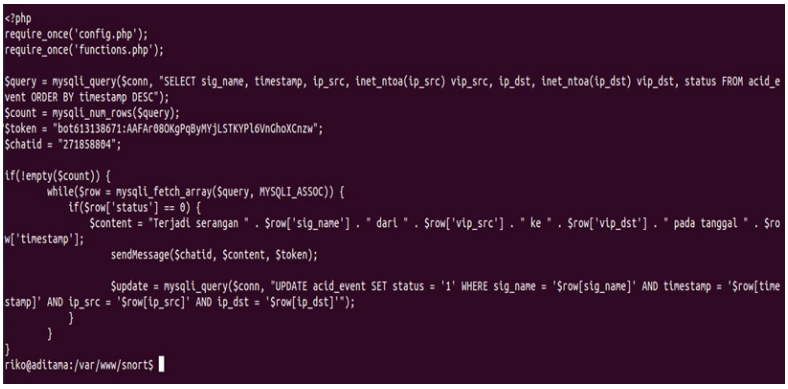


Gambar 4. ID Chart Pengguna

Tabel 1. Telegram bot informasi

Nama bot	***snortalarmBot***
Username	*snortalarmbot*
Token	*bot613138671:AAFAr08OKgPqByMYjLSTKYPl6VnGhoXCnzw*
ID Chat	*271858804*

d. Impelementasi Trigger
Trigger merupakan pemicu yang akan mengeksekusi sebuah perintah secara otomatis untuk menanggapi perubahan tertentu [3]. Implementasi ini perlu adanya kode program *(script)* untuk menghubungkan Telegram Bot dengan IDS agar mendapatkan notifikasi dari aplikasi Telegram. Potongan kode program digunakan sebagai *trigger* untuk mengirimkan notifikasi ke aplikasi Telegram. Saat terjadi serangan yang dilaukan oleh *attacker* pada server, *trigger* akan secara otomatis memberikan respon dengan mengirimkan notifikasi ke aplikasi telegram dengan cara mengambil data yang ada didalam *database snort*.

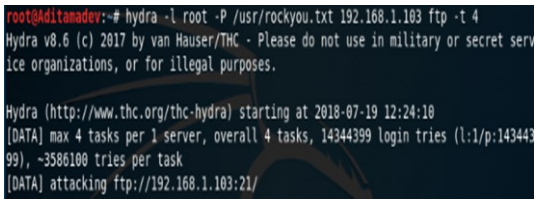


Gambar 5. Notifikasi Telegram

e. Pengujian Serangan dilakukan untuk mengetahui kinerja system keamanan komputer yang telah dibuat dengan teknik:

1) FTP *Bruteforce Attack*

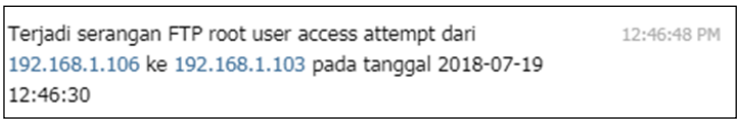
Pengujian menggunakan FTP *Bruteforce Attack* untuk mendapatkan *username* dan *password* dengan target IP 192.168.1.103. Sistem IDS akan mendeteksi serangan pada server.



Gambar 6. FTP *Bruteforce Attack*

Gambar 7. Deteksi FTP Bruteforce Attack

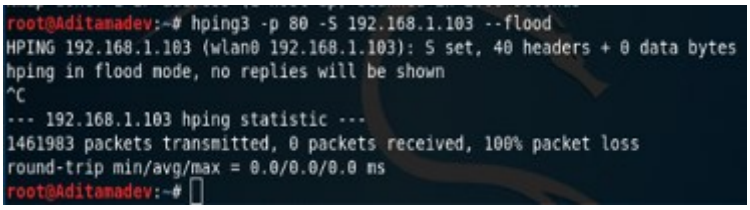
Serangan yang terdeteksi pada tanggal 19 Juli 2018 jam 12.46.30 memiliki SID 10000006 sumber serangan berasal dari IP 192.168.1.106 dengan target IPT 192.168.1.103 dengan port 21. Kemudian terjadi *trigger* yang mengirimkan notifikasi kepada administrator melalui aplikasi Telegram.



Gambar 8. Notifikasi FTP *Bruteforce Attack*

2) Ddos *Attack*

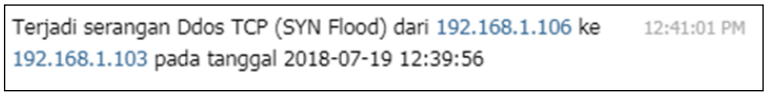
Pengujian Ddso dilakukan untuk melumpuhkan sumber daya menggunakan aplikasi Hping3 dengan target ip 192.168.1.103 denga port 80.



Gambar 9. Ddos *Attack* menggunakan Hping3

Gambar 10. Deteksi *Ddos Attack*

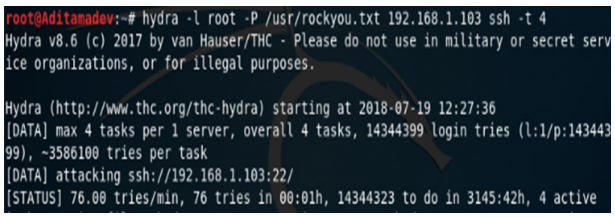
Serangan memiliki SID 10000003 pada tanggal 19 Juli 2018 jam 12.39.56. Sumber serangan dari ip 192.168.1.106 dengan target ip 192.168.1.103 dengan *port* 80. Adminstrator akan mendapatkan notifikasi tentang adanya serangan, pada gambar 10 menujukkan notifikasi yang dikirim ke aplikasi telegram saat *terjadi serangan syn attack* pada server.



Gambar 11. Notifikasi *Ddos Attack*

3) SSH *Bruteforce Attack*

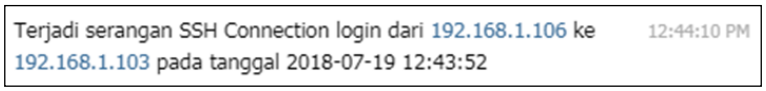
Pengujian dengan SSH akan dilakukan dengan teknik *Bruteforce* untuk mendapatkan *username* dan *password* yang digunakan untuk login pada SSH. *Attacker* akan mencoba menggunakan username "*root*" dan password *rockyou.txt*. yang telah disedikan pada kali linux.



Gambar 12. SSH *Bruteforce Attack* menggunakan Hydra

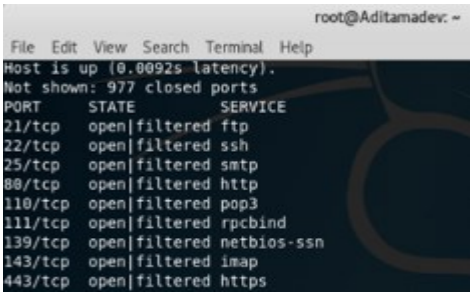
Gambar 13. Deteksi SSH *Bruteforce Attack*

Serangan terjadi pada ip 192.168.1.103 dengan port 22, serangan terhadap SSH memiliki SID 10000004 dan berasal dari ip 192.168.1.106 pada tanggal 19 Juli 2018 jam 12.43.52. Administrator mendapatkan notifikasi Telegram tentang adanya serangan SSH *Bruteforce Attack*



Gambar 14. Notifikasi SSH Bruteforce Attack

4) *Port Scanning*
Tujuan dari *port scanning* adalah untuk mendapatkan informasi mengenai port yang terbuka pada server. Pengujian menggunakan nmap.



Gambar 15. *Port Scanning* Menggunakan Nmap

Pengujian port scanning menggunakan FIN scan untuk mengetahui port yang terbuka, dan setelah terdeteksi adanya serangan administrator akan mendapatkan notifikasi melalui aplikasi Telegram pada tanggal 19 Juli 2018 jam 12.39.16.

Gambar 16. *Notifikasi Port Scanning*

Data hasil perhitungan dari tabel 2, terlihat ketiga pengujian yang dilakukan, miliki rata-rata waktu yang dibutuhkan untuk proses deteksi serangan sekitar 0 *(nol)* detik.

Tabel 2. Hasil akurasi waktu

No.	*Pengujian Sistem*	*Tipe Serangan*	*Port*	*Waktu*		
				Awal serangan	*Terdeteksi*	*Terkirim*
1	*FTP*	*Bruteforce Attack*	*21*	*12:46:30*	*12:46:30*	*12:46:30*
2	*Ddos*	*Ddos TCP 80*	*80*	*12:39:56*	*12:39:56*	*12:39:56*
3	*SSH*	*Bruteforce Attack*	*22*	*12:43:52*	*12:43:52*	*12:43:52*
4	*Port Scanning*	*Scan FIN Nmap*	*80*	*12.39.16*	*12.39.16*	*12.39.16*

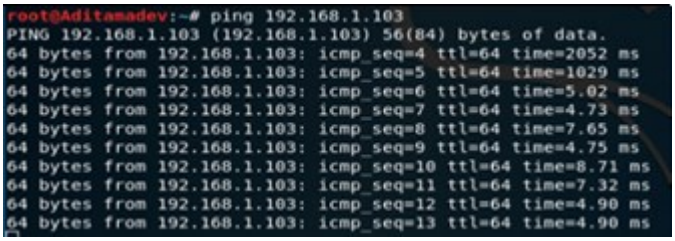
Dari hasil pengujian sistem diambil kesimpulan yang tertera pada tabel 3, sehingga menunjukkan Sistem dapat mendeteksi adanya serangan yang dilakukan oleh *attacker* kemudian mengirimkan notifikasi melalui aplikasi Telegram. Pendeteksian serangan telah sesuai dengan aturan yang dibuat mulai dari *FTP Bruteforce Attack, Ddos Attack, SSH Brureforce Attack dan Port Scanning* telah sesuai dengan hasil yang diharapkan.

Tabel 3. Hasil pengujian sistem

No	*Pengujian Sistem*	*Tipe Serangan*	*Hasil Pengujian*	*Kesimpulan*
1	*FTP*	*Bruteforce Attack*	*Terdeteksi*	*Berhasil*
2	*Ddos*	*Ddos TCP 80*	*Terdeteksi*	*Berhasil*
3	*SSH*	*Bruteforce Attack*	*Terdeteksi*	*Berhasil*
4	*PORT Scanning*	*Scan FIN Nmap*	*Terdeteksi*	*Berhasil*

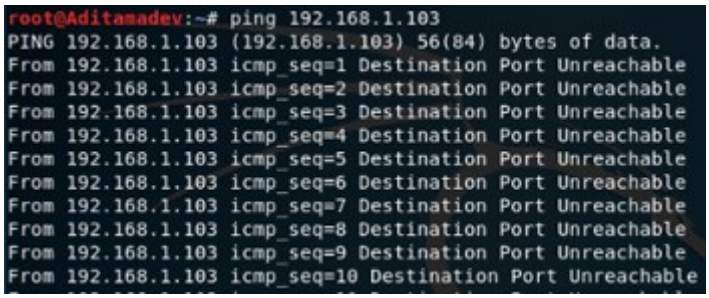
3.2 Evaluating

Setelah dilakukan tahapan *action tacking*, maka untuk meningkatkan keamanan untuk keberhasilan system yang telah dibuat. Selanjutnya mencoba dengan cara *Intrusion Prevention System (IPS)* yang terdapat pada snort. IPS merupakan system yang digunakan untuk mencegah serangan yang akan masuk pada jaringan dengan memeriksa dan mencatat semua paket data [6]. IPS bertindak seperti layaknya *firewall* yang melakukan *allow* dan *block* jika telah terindetifikasi sebagai serangan. IPS akan menolak aksec (*block)* dan mencatat semua paket data *(log)* yang telah terindentifikasi.



Gambar 17. *Ping ICMP Tanpa Perlindungan IPS*

Setelah system keaman IPS diterapkan terhadap ICMP dengan perintah drop, maka system akses PING yang ditujukkan ke server kan diblokir, terlihat pada gambar 18.



Gambar 18. *Akses Ping ICMP Diblokir*

3.3 Learning

Hasil yang didapat menunjukkan system berhasi mendeteksi serangan yang dilakukan oleh *attacker*, namun hal tersebut belum dapat dijadikan acuan bahwa system IDS bekerja secara optimal, sebab semakin berkembangnya teknologi, maka metode penyerangan akan semakin beragam. Adminstrator dituntut untuk selalu mengupdate *rules* untuk keamanan server. Dengan demikian, akan mudah memonitoring server ketika ada serangan baru. Selain mendeteksi serangan, perlu adanya sistem yang mampu melakukan tindakan pencegahan yang sering dinamakan sebagai IPS. Pada kasus tertentu sebuah serangan dapat membahayakan sistem dan fungsi IPS untuk mencegah serangan agar tidak menggangu server.

Dengan adanya notifikasi yang dikirimkan secara otomatis melalui aplikasi telegram saat terjadi serangan menjadi suatu hal yang sangat penting. Administrator dapat mengetahui tentang kondisi server pada saat itu juga. Disisi lain penerapan Sistem monitoring serangan dengan notifikasi telegram ini, dapat di jadikan sebagai acuan bagi seseorang administrator jaringan untuk melakukan tindakan selanjutnya. Contoh yang dapat dilakukan oleh Administrator adalah dengan menambahkan *Firewall* atau menutup

port-port yang digunakan untuk pertukaran data demi meningkatkan keamanan pada server sehingga server tersebut mampu menjalankan tugasnya secara optimal.

4. KESIMPULAN

Dengan adanya IDS, administrator jaringan dapat mengetahui jika terjadi serangan pada server dan semua informasi akan mengirimkan notifikasi ke administrator melalui aplikasi telegram secara *real time*. Rata-rata waktu yang dibutuhkan dalam pengiriman notifikasi serangan pada aplikasi telegram sekitar 0 *(nol)* detik. Hasil pengujian dari *FTP Bruteforce Attack, Ddos Attack, SSH Bruteforce Attack* mendapatkan *username* "root" dan *password* "rockyou.txt" dengan target IP 192.168.1.103, menggunakan aplikasi Hping3 dan Hydra.

UCAPAN TERIMA KASIH

Saya ingin menyampaikan ucapan terimakasih yang sangat besar kepada Universitas Bina Darma dan Direktorat Riset dan Pengabdian Masyarakat Bina Darma (DRPM) atas dukungannya selama pengembangan karya penelitian ini.

DAFTAR PUSTAKA

[1] D. Utomo, M. Sholeh, And A. Avorizano, "Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata Dan Bot Telegram Channel," Vol. 2, No. 2502, P. 7, 2017.
[2] B. Alfiansyah And D. Risqiwati, "Notifikasi Alert Intrusion Detection System Snort Pada Bot Telegram," P. 7, 2018.
[3] D. T. Atmaja, E. B. Prasetya, And P. E. Kresnha, "Notifikasi Adanya Serangan Pada Jaringan Komputer Dengan Mengirim Pesan Melalui Aplikasi Telegram Dan Kontrol Server," P. 8.
[4] E. R. S. Moningkey And P. Kapele, "Analisa Quality Of Service (Qos) Jaringan Komputer Di Smk Kristen I Tomohon," Vol. 5, No. 1, P. 7, 2017.
[5] M. K. Umam, L. B. Handoko, And M. Kom, "Analisis Kinerja Jaringan Wlan Menggunakan Metode Action Research Pada Dinas Perhubungan Komunikasi Dan Informasi Kabupaten Pemalang," P. 10.
[6] M. S. Pratama, "Pengamanan Jaringan Komputer Menggunakan Metode Ips (Intrusion Prevention System) Terhadap Serangan Backdoor Dan Synflood Berbasis Snort Inline," P. 16.