p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

NOTIFIKASI ADANYA SERANGAN PADA JARINGAN KOMPUTER DENGAN MENGIRIM PESAN MELALUI APLIKASI TELEGRAM DAN KONTROL SERVER

Danang Tri Atmaja, Eka Budhy Prasetya, Priadhana Edi Kresnha
Teknik Informatika Fakultas Teknik Unviersitas Muhammadiyah, Jakarta
Jl Cempaka Putih Tengah No. 27 Jakarta Pusat 10510
danang.contact@gmail.com

Abstrak

Server menjadi hal yang perlu mendapat perhatian lebih mengenai tingkat keamananya. Server yang memiliki celah keretanan keamanan pada server dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab. Administrator harus memastikan bahwa sistem benar-benar aman, salah satu cara menjaga keamanan server adalah dengan pendeteksian intrusi yang dianggap berbahaya menggunakan Intrusion Detection System (IDS). Sistem pendeteksian intrusi dibangun berdasarkan aturan yang telah disimpan dalam sebuah database (signature-based). Snort merupakan salah satu perangkat lunak yang berfungsi untuk mengetahui adanya intrusi. Paket-paket data yang melalui lalu lintas jaringan akan dianalisis terlebih dahulu. Paket-paket data yang terdeteksi sebagai intrusi akan memincu alert yang kemudian disimpan dalam file log. Dengan begitu, administrator dapat mengetahui intrusi yang terjadi pada server, serta adanya aplikasi instant messaging dapat membantu administrator untuk memperoleh pemberitahuan secara realtime dan melakukan kontrol pada server secara realtime, salah satunya menggunakan aplikasi Telegram selain administrator mendapatkan informasi singkat dan laporan notifikasi adanya percobaan intrusi pada server, administrator juga dapat melakukan kontrol terhadap server secara realtime.

Kata kunci : IDS (*Intrusion Detection System*), Snort, Telegram, Bot Telegram, Percobaan Intrusi

Abstract

Servers become things that need to get more attention about their security level. Servers that have security vulnerabilities on the server can be used by irresponsible parties. Administrators must ensure that the system is completely safe, one way to maintain server security is by detecting intrusions that are considered dangerous using the Intrusion Detection System (IDS). The intrusion detection system is built based on rules that have been stored in a (signature-based) database. Snort is one software that functions to find out the intrusion. Data packages through network traffic will be analyzed first. Data packets detected as intrusions will call for alerts which are then stored in log files. That way, administrators can find out the intrusions that occur on the server, and the presence of instant messaging applications can help administrators to obtain real-time notifications and control the server in realtime, one of which uses the Telegram application in addition to administrators get brief information and notification reports of intrusion attempts on server, the administrator can also control the server in realtime.

Keywords: IDS (Intrusion Detection System), Snort, Telegram, Telegram Bot, Intrusion Experiment

PENDAHULUAN

Perkembangan dalam bidang teknologi dan informasi saat ini khususnya dunia internet semakin berkembang pesat disertai kebutuhan manusia akan kebutuhan teknologi internet semakin meningkat karena dengan internet

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

setiap orang dapat saling terhubung. Seiring dengan perkembangan internet yang sedemikian pesat menjadikan keamanan suatu data dan informasi menjadi sangat penting terkhusus pada sebuah *server* yang terhubung dengan jaringan komputer yang saling terhubung tentu menjadi sangatlah penting.

Keamanan merupakan salah satu masalah terbesar bagi pengguna internet terutama penyedia sebuah *server* maupun sistem jaringan komputer. Masalah tersebut menimbulkan kecenderungan besar untuk memiliki *Intrusion Detection System* (IDS) pada setiap jaringan komputer. IDS *(Intrusion Detection System)* merupakan sebuah perangkat lunak yang secara otomatis melakukan proses pemantauan (*monitoring*) terhadap insiden yang terjadi dalam sistem komputer atau jaringan komputer serta menganalisis tanda-tanda adanya masalah terhadap keamanan sistem. IDS (*Intrusion Detection System*) melakukan penyaringan *(filtering)* terhadap lalu lintas data didalam jaringan komputer dan melakukan analisis terhadap informasi yang didapatkan guna mendapatkan bukti adanya percobaan penyusupan atau percobaan intrusi terhadap sistem jaringan komputer salah satunya percobaan intrusi terhadap *server*.

Sistem jaringan komputer yang tidak aman tentu akan berdampak negatif bagi penyedia maupun pengguna sistem. Oleh karena itu, perlu adanya *monitoring* keamanan jaringan dengan tujuan meminimalisir jika terjadinya percobaan penyusupan atau percobaan intrusi. Salah satu aplikasi yang digunakan IDS (*Intrusion Detection System)* adalah Snort. Aplikasi *open source* tersebut memiliki kemampuan mendeteksi adanya penyusupan terhadap sistem keamanan jaringan yang sesuai dengan aturan (*rule*) yang telah ditetapkan didalam IDS (*Intrusion Detection System)*. Peringatan deteksi adanya penyusupan atau percobaan intrusi tersebut dapat memanfaatkan aplikasi *instant messaging* sebagai media untuk memberitahu kepada seorang *Administrator* didalam jaringan komputer jika terdapat indikasi penyusupan yang terjadi pada *server* di dalam jaringan komputer serta dapat dilakukan antisipasi penanganan awal dengan kontrol langsung terhadap *server* secara *real time.* Aplikasi *instant messaging* saat ini populer digunakan oleh berbagai kalangan. Salah satu aplikasi tersebut yang memiliki berbagai fitur adalah Telegram. Aplikasi tersebut selain untuk *chatting*, terdapat fitur pertukaran dokumen. Fitur tersebut dapat dimanfaatkan untuk memberikan laporan keamanan sistem jaringan komputer.

Instant Messaging Telegram

Instant Messaging Telegram adalah sebuah perangkat lunak atau aplikasi saat ini yang sangat populer di kalangan masyarakat. Tujuan utama aplikasi tersebut yaitu menyajikan fitur obrolan yang berjalan secara *real time* sehingga pesan langsung dapat terkirim dan diterima. Aplikasi *instant messaging* berjalan secara *online* atau dengan kata lain membutuhkan koneksi *Internet*. Saat ini terdapat banyak aplikasi *instant messaging* yang digunakan oleh masyarakat untuk mengobrol dengan individu maupun komunitas. Fitur yang disajikan aplikasi tersebut tidak hanya melalui *text based* saja, tetapi bisa juga untuk melakukan obrolan melalui suara, bertukar foto, audio, video hingga dokumen digital. Salah satu aplikasi yang memiliki fitur tersebut yaitu Telegram. Telegram secara definisi menurut telegram.org (Vico, 2014) merupakan alternatif layanan aplikasi perpesanan untuk ponsel (*mobile*) maupun desktop yang berbasis *cloud* dengan keamanan tingkat tinggi serta kecepatan aksesnya. Aplikasi instant messaging tersebut tersedia untuk berbagai device seperti ponsel yang berjalan pada system operasi Android, iOS, Windows Phone. Tidak hanya berjalan pada perangakt *mobile*, tetapi juga dapat berjalan system desktop seperti Windows dan Linux. Meskipun terlihat sederhana aplikasi instant messaging Telegram memiliki fitur yang lebih unggul dibandingkan aplikasi instant messaging lainnya. Telegram diklaim sebagai aplikasi yang aman dimana menyediakan pilihan pesan end-to-end yang akan di enskripsi.

Telegram Bot API

Telegram Bot API *(Application Progamming Interface)* adalah sebuah perangkat lunak atau aplikasi yang digunakan untuk berinteraksi antara Bot dengan penggunannya maka dari itu dibutuhkanlah sebuah API. (*Mutaqin*, 2016).

Bot tersebut dapat melakukan beberapa pekerjaan yaitu:

1.Mengintegrasikan dengan layanan lainnya, Bot dapat mengirimkan komentar jarak jauh atau mengendalikan *smart home*. Selain itu, *bot* juga mampu mengirimkan

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

pemberitahuan melalui Telegram ketika terjadi sesuatu di suatu tempat

2.Menciptakan alat khusus, Bot mampu memberikan pemberitahuan maupun memberikan sebuah peringatan, ramalan cuaca, terjemahan, atau layanan lain.

3.Membangun *single player* ataupun *multiplayer game,* Keunggulan lainnya yaitu *bot* mampu memainkan permainan seperti catur.

4.Membangun layanan social, Sebuah *bot* dapat menghubungkan orang-orang untuk mencari mitra percakapan berdasarkan kepentingan bersama

SNORT

Snort merupakan aplikasi atau perangkat lunak berbasis *opensource* yang memiliki keunggulan untuk mengetahui adanya indikasi penyusupan pada jaringan berbasis TCP/IP secara *real time* (*Mutaqin*, 2016). Jika terindikasi adanya penyusupan, Snort akan melakukan pencatatan atau *logging* terhadap paket-paket yang telah terdeteksi sebagai intrusi berdasarkan aturan yang telah ditetapkan. (*Mutaqin*, 2016).

METODE

Tahapan yang dilakukan didalam penelitian ini adalah sebagai berikut :

1. Pengumpulan Data

Pada tahap ini penulis melakukan pengumpulan data dengan studi literatur yaitu dengan mempelajari dan mencari bahan-bahan atau data-data maupun informasi yang berhubungan dengan IDS (Intrusion Detection System) serta mencari cara untuk menghasilkan notifikasi laporan berupan serangan yang bersumber dari Snort yang dikirim ke aplikasi *instant messaging* Telegram lalu dapat dilakukan kontrol server melalui instant messaging Telegram secara *realtime*

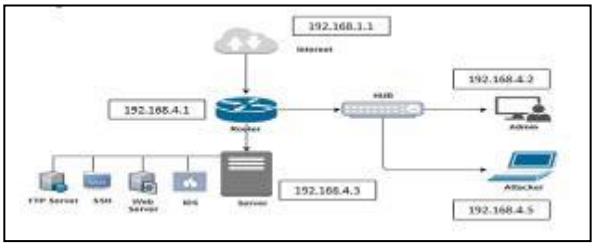
2. Perancangan

Menyusun arsitektur jaringan yang akan digunakan untuk pengujian sistem serta cara untuk menentukan alur kerja sistem

3. Implementasi dan Uji Coba

Melakukan implementasi dan uji coba dengan percobaan penyerangan terhadap *server* yang telah ditentukan sesuai dengan aturan (*rule*) serta mengetahui pengujian terhadap notifikasi kedalam aplikasi instant messaging Telegram dan kontrol server secara realtime, guna mengetahui kelebihan dan kekurangan dalam penelitian ini.

HASIL DAN PEMBAHASAN



Tabel 1. Keterangan perangkat keras topologi jaringan

No	Parameter	Value
1	Modem	Smartfriend Andromax M2s
2	Mikrotik	RB941-2^{nD-TC}
3	Switch	Tp-link
4	Kabel	UTP

Serta pada topologi jaringan tersebut memiliki konfigurasi IP Address, berikut konfigurasinya pada tabel 2.

Tabel 2. Konfigurasi IP *Address* Komputer *Server*

Network Adapter	Enp3s0
IP Address	192.168.4.3
Network	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.4.1
Broadcast	192.168.4.255

Tabel 3. Konfigurasi IP *Address Attacker*

Network Adapter	Eth0
IP Address	192.168.4.5
Network	192.168.4.0
Netmask	255.255.255.0
Gateway	192.168.4.1
Broadcast	192.168.4.255

Tabel 4. Konfigurasi IP Address Attacker

Network Adapter	Eth0
IP Address	192.168.4.5
Network	192.168.4.0
Netmask	255.255.255.0

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Gateway	192.168.4.1
Broadcast	192.168.4.255

Desain Pengiriman Alur Informasi Serangan

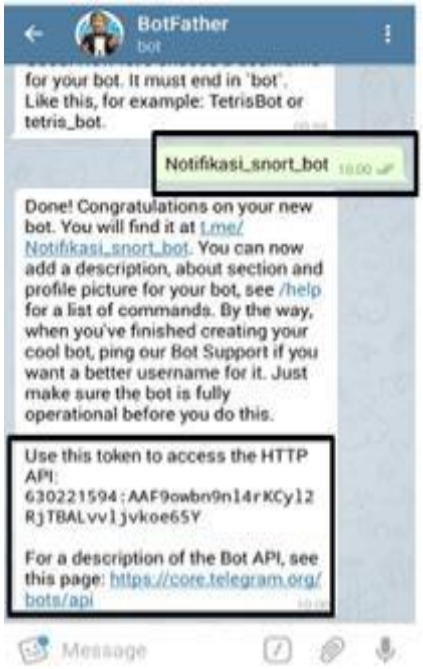
Desain alur pengiriman informasi serangan pada perancangan Intrusion Detection System (IDS) menggunakan Snort yang kemudian notifikasi peringatan deteksi tersebut terhubung pada sebuah website dan Telegram, untuk menghubungkan antara sistem dengan snort dibutuhkan sebuah trigger yaitu dengan memanfaatkan sebuah API (Application Programming Interface). Apps tersebut dibangun menggunakan bahasa program PHP yang bertujuan agar Apps dan Telegram dapat terhubung dan memeriksa informasi terbaru terkait data-data serangan yang digunakan sebagai notifikasi di Telegram. Desain pengiriman alur informasi serangan. Seperti pada Gambar 2. Desain pengiriman alur informasi serangan

Gambar 2. Desain pengiriman alur informasi serangan

Apps interface yang dirancang khusus untuk mendapatkan informasi terbaru dari database melalui waktu yang telah di tetapkan dengan me-refresh 10 detik sekali untuk mendapatkan data terbaru secara realtime. Informasi yang dikirimkan telegram berdasarkan jenis serangan, port tujuan, IP address penyerang, IP Address server serta waktu terjadinya insiden percobaan intrusi yang terjadi.

Bot Telegram

Dalam penelitian ini, peneliti memanfaatkan "Bot Father" yang tersedia pada aplikasi Telegram untuk mendaftarkan Bot Telegram untuk menciptakan Bot Telegram sendiri, setelah berhasil mendaftarkan Bot Telegram akan mendapatkan kode khusus mengenai data-data (Application Programming Interface) API kemudian kode khusus tersebut akan dihubungkan dengan IDS (Intrusion Detection System) melalui Apps yang dibuat menggunakan bahasa program PHP sehingga menghasilkan sebuah notifikasi informasi terkait serangan percobaan intrusi yang terjadi.



Gambar 3. API Bot Telegram

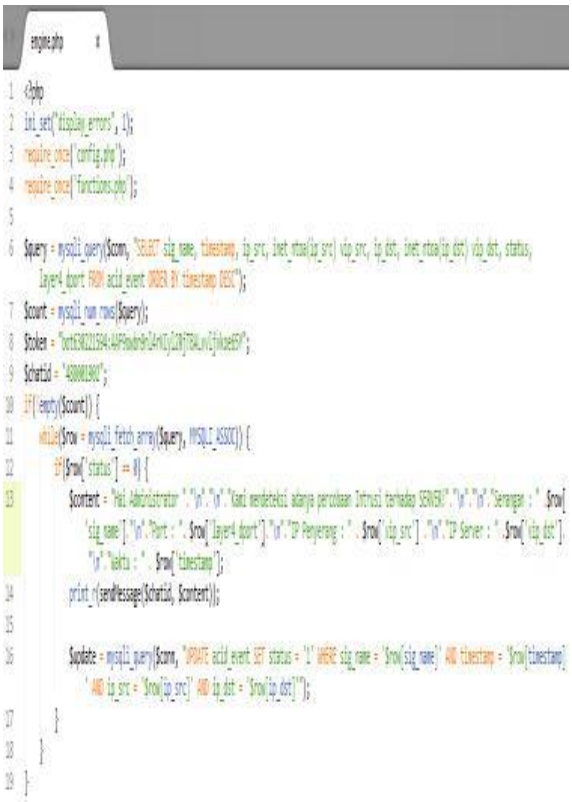
Adapun informasi lengkap mengenai Bot Telegram dapat dilihat pada tabel 5.

Tabel 5. Informasi Bot Telegram

Parameter	*Value*
Nama	Notifikasi_snort
Username	Notifikasi_snort_*bot*
Token	630221594:AAF9owbn9nl4 rKCyl2RjTBALvvljvkoe65Y
IID *Chat User*	488001902

Jika Bot telah siap dipasang dan data informasi Bot Telegram telah didapatkan, selanjutnya penulis memanfaatkan token API tersebut untuk menghubungkan Telegram dengan *Apps Interface* untuk mendapatkan dan menerima informasi apabila terjadi intrusi secara *realtime*. Token akan dihubungkan menggunakan pemrograman bahasa PHP. Seperti pada gambar 4 adalah sebagai berikut :

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek



Gambar 4. Function Penghubung API Telegram

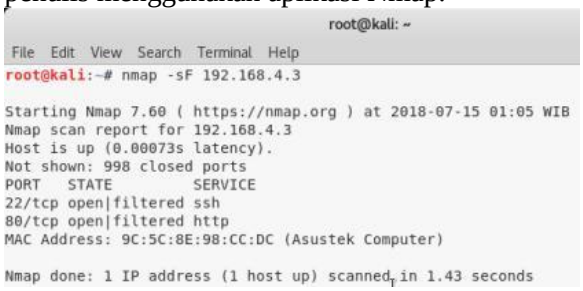
Gambar 5. Function Penghubung API Telegram

Simulasi Pengujian

Simulasi pengujian dilakukan berdasarkan skenario pengujian diantaranya *ddos attack, port scanning, ssh brute force*. Pengujian dengan menggunakan skenario tersebut bertujuan untuk mengetahui alert IDS yang diimplementasikan pada jaringan komputer tersebut, serta mengetahui notifikasi yang terkirim ke aplikasi Telegram.

Pengujian Port Scanning

Pengujian *Port* Scanning bertujuan untuk mendapatkan informasi-informasi mengenai *port-port* yang terbuka pada *server* target penulis menggunakan aplikasi Nmap.



Gambar 6. Pengujian Port Scanning

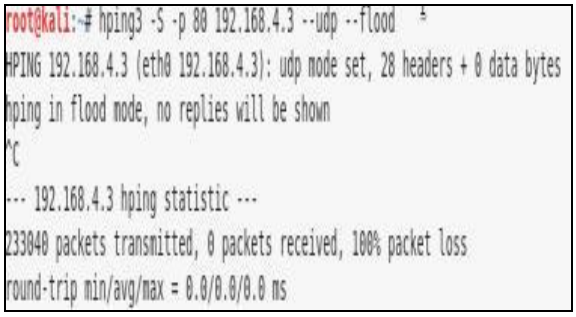
Pada sisi lain IDS (Intrusion Detection System) telah aktif dan berhasil mendeteksi adanya percobaan intrusi pada tanggal 2018-07-15 jam 15:37 dan SID '10000002' berhasil mendeteksi percobaan intrusi yang dilakukan IP *Address* 192.168.4.5 menuju IP *Address* 192.168.4.3 *port* 22 dan 80.

```
07/16-01:05:45.812818  [**] [114:10000002:7] NMAP Scan detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.5:55902 -> 192.168.4.3:80

07/16-01:05:45.812832  [**] [114:10000002:7] NMAP Scan detected [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.4.5:55902 -> 192.168.4.3:22
```

Pengujian Ddos Attack

Pengujian Ddos menggunakan aplikasi hping3 pada komputer *attacker*. Target pengujian yaitu IP Addres 192.168.4.3 dengan *port* 80.



Gambar 7. Pengujian Ddos Attack

Intrusi berhasil terdeteksi oleh IDS pada tanggal 07/15 pada pukul 17:30:52 dengan SID '10000005' berasal dari IP *Address* 192.168.4.5 dengan target 192.168.4.3 yang memiliki *port* 80. Hasil deteksi IDS (*Intrusion Detection System*)

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

```
07/16-01:07:02.003765 [**] [117:10000005:8] Snort Alert [117:10000005:8] [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 192.168.4.5:12770 -> 192.168.4.3:80
```

Pengujian SSH Brute Force

Pengujian SSH Brute Force dilakukan menggunakan aplikasi hydra. Aplikasi tersebut akan mem-*brute force* terhadap layanan SSH. *Attacker* dengan cara kerjanya adalah mencoba dengan *username* "root" dan beberapa kombinasi *password* yang tersimpan didalam *file* pass.txt. Target serangan adalah IP *Address* yaitu 192.168.4.3.

Gambar 8. Pengujian SSH Brute Force

Intrusi yang terdeteksi oleh IDS pada tanggal 07/15 pada pukul 17:30:52 dengan SID '10000005' berasal dari IP *Address* 192.168.4.5 dengn target 192.168.4.3 yang memiliki *port* 80.

```
07/15-19:20:44.671495 [**] [115:10000004:8] Snort Alert [115:10000004:8] [**] [Classification: SSH login attempt] [Priority: 3] {TCP} 192.168.4.5:40854 -> 192.168.4.3:22
```

Pengujian Kontrol Server

Pengujian kontrol *server* menggunakan aplikasi *instant messaging Bot* Telegram jika terdapat sebuah percobaan intrusi terhadap *server* dapat dicegah menggunakan perintah-perintah di linux dengan mem-*block* IP *Address attacker*. Kontrol server ini terintegrasi dengan aplikasi shell-bot yang telah terinstall didalam server.

```
cd /{path}/shell-bot/          //path : alamat direktori shell-bot
# ./server.js
# Bot Ready.
```

Jika aplikasi shell-bot telah siap digunakan maka ketikan perintah-perintah pada aplikasi Telegram adalah sebagai berikut :

Gambar 9. Pengujian Block IP Addres Server

Jika ingin membuka *block* IP Address *attacker* tersebut dapat menggunakan perintah-perintah sebagai berikut :

Gambar 10. Pengujian Membuka IP Address Server

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Hasil Port Scanning

Gambar 11. Hasil Port Scanning

Hasil Ddos Attack

Gambar 12. Ddos Attack

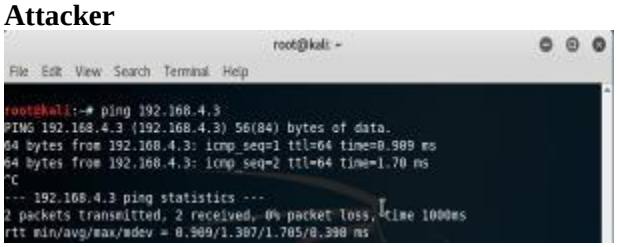
Hasil SSH Brute Force

Gambar 13. SSH Brute Force

Hasil Kontrol Server Block IP Address Attacker

Gambar 14. Block IP Address Attacker

Hasil Kontrol Server Membuka IP Address Attacker



Gambar 15. Membuka IP Address Attacker

Hasil Akurasi Deteksi Pengujian

Hasil dari aktifitas pengujian terhadap *server*, didapatkan hasil waktu terhadap masing-masing aktifitas mulai dari penyerangan, pendeteksian dan terkirimnya notifikasi ke aplikasi *instant messaging* telegram. Hasil catatan tersebut diukur untuk mengukur tingkat ke akurasi deteksi hingga terkirimnya notifikasi.

Tabel 6. Hasil Akurasi Deteksi Pengujian

No	Tipe Serangan	Tingkat Akurasi Deteksi Pengujian (Waktu)		
		Awal Serangan	Terdeteksi	Terkirim Notifikasi
1	*Port* Scanning	01:05:45 WIB	01:05:45	01:05:45
2	SSH Brute Force	19:20:44 WIB	19:20:44	19:20:44
3	Ddos Attack	01:07:02 WIB	01:07:02	01:07:02

Tabel 7. Hasil Selisih Waktu Serangan (Detik)

No	Tipe Serangan	Tingkat Selisih Waktu Deteksi Serangan (Detik)	
		Awal serangan dan Terdeteksi	Terdeteksi dan Terkirim Notifikasi
1	*Port* Scanning	0 detik	0 detik
2	SSH Brute Force	0 detik	0 detik
3	Ddos Attack	0 detik	0 detik
Total		0 detik	0 detik
Rata – Rata		0 detik	0 detik

Tabel 8. Hasil Pengujian Serangan

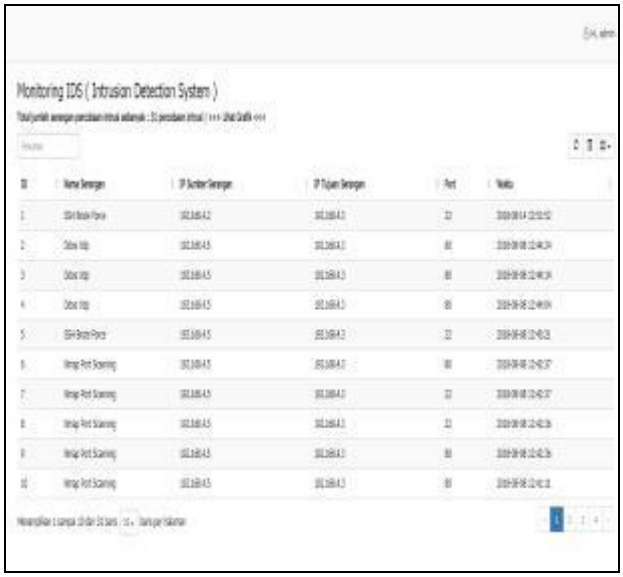
No	Tipe Serangan	Uji Coba	Hasil yang di harapkan	Kesimpulan
1	*Port* Scanning	NMAP FIN scan	Terdeteksi	Berhasil
2	SSH	SSH Brute force	Terdeteksi	Berhasil
3	Ddos	Ddos UDP 80	Terdeteksi	Berhasil

Tabel 9. Hasil Pengujian Kontrol Server

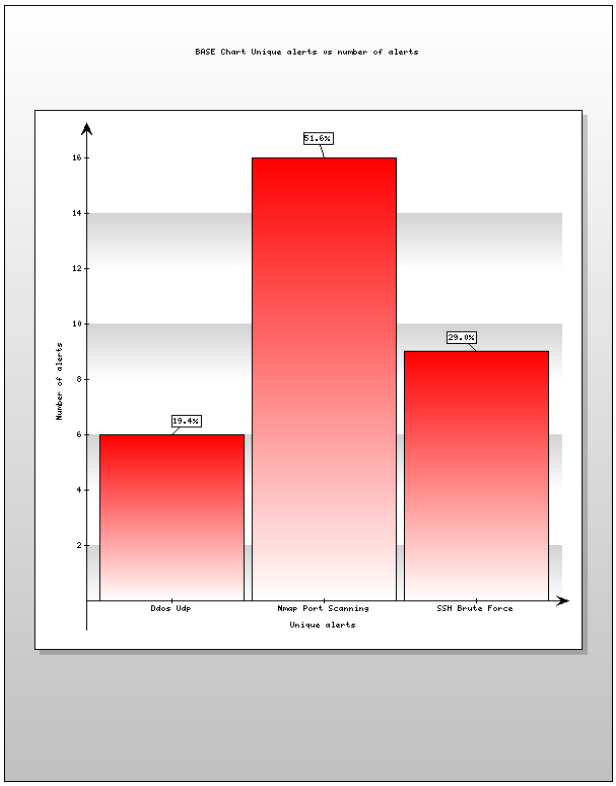
No	Uji Coba	Hasil yang diharapkan	Kesimpulan
1	Blokir IP *Address* Attacker	Terdeteksi	Berhasil
2	Membuka IP *Address* Attacker	Terdeteksi	Berhasil

p- ISSN : 2407 – 1846
e-ISSN : 2460 – 8416
Website : jurnal.umj.ac.id/index.php/semnastek

Hasil Laporan Serangan Melalui Apps Interface



Gambar 16. Hasil Laporan Serangan Melalui Apps Interface



Gambar 17. Laporan Berbentuk Grafik Bar

Berdasarkan hasil laporan serangan melalui Apps Interface, dapat dilihat informasi yang disajikan yaitu : Nama serangan, IP sumber serangan, IP tujuan serangan, port yang diserang, grafik berbentuk bar serta waktu terjadinya insiden percobaan intrusi.

SIMPULAN DAN SARAN

Berdasarkan hasil analisis dan pembahasan maka didapatkan kesimpulan sebagai berikut :

1. Dengan penerapan IDS *(Intrusion Detection System)* pada sebuah jaringan komputer, seorang yang berlaku sebagai *administrator* jaringan pada mengetahui jika terdapat sebuah serangan atau percobaan intrusi yang ditujukan pada salah satu *server* yang dimiliki, sesuai dengan *rule* yang telah dibuat
2. IDS *(Intrusion Detection System)* yang dibangun dapat memberikan notifikasi ke *administrator* jaringan melalui aplikasi *instant messaging* Telegram secara *real time* dan dapat melakukan kontrol *server* melalui *instant messaging* Telegram
3. IDS *(Intrusion Detection System)* yang telah dirancang dan dibangun dapat mendeteksi beberapa serangan seperti Ddos *attack*, SSH *brute force*, *Port Scanning.*

UCAPAN TERIMAKASIH

Ucapan terima kasih kepada Bapak Eka Budhy Prasetya dan Bapak Priadhana Edi Kreshna yang telah membimbing, mendukung dalam melakukan penelitian ini.

DAFTAR PUSTAKA

Aji S.Kom & Rianto S.Kom. *"Jaringan Komputer konsep dasar pengembangan jaringan dan keamanan jaringan"*. Yogyakarta : Andi, 2008.

Rendra Towidjojo. "*Mikrotik KungFu Kitab 1"*. Jakarta : Jasakom,2013.

"*Linux & Mikrotik"*. Yogyakarta : penerbit Andi, 2008.

Sofana, Iwan "*Membangun jaringan komputer"*. Bandung : Informatika, 2008

Dony Ariyus,M.(2013). *Intrusion Detection System*.Jakarta:Penerbit Andi.