e-ISSN. 2685-4066

Jurnal BITe
Vol.1 No.2 (Desember) 2019, Hal 102-109

Analisa Penerapan Intrusion Prevention System (IPS) Berbasis Snort Sebagai Pengaman Server Internet Yang Terintegrasi Dengan Telegram

Abdul Muhaimi[1], I Putu Hariyadi[2], Akbar Juliansyah[3]

[1]Universitas Bumigora, abdulmuhaimi27@gmail.com
[2]Universitas Bumigora, putu.hariyadi@stmikbumigora.ac.id
[3]Universitas Bumigora, akbar.juliansyah@stmikbumigora.ac.id

ABSTRAK

Keamanan merupakan salah satu bagian yang sangat penting dalam Teknologi Informasi (TI) yang telah dimanfaatkan di berbagai bidang. Pemanfaatan TI dapat memperlancar operasional sehingga meningkatkan kualitas layanan. Namun di sisi lain apabila tidak dijaga keamanannya maka akan berdampak pada ketersediaan layanan. Setiap institusi atau lembaga harus memiliki pencegahan terhadap keterbukaan akses dari pihak yang tidak berhak. Peran pertahanan sistem pada umumnya terletak pada *administrator* sebagai pengelola jaringan yang memiliki akses penuh terhadap infrastruktur jaringan yang dibangunnya. Terdapat berbagai metode yang dihasilkan oleh beberapa peneliti yang telah menerapkan pengamanan terkait layanan pada server Internet salah satunya adalah *Intrusion Prevention System (IPS)*. Sistem IPS yang diterapkan oleh peneliti terdahulu belum terintegrasi dengan telegram sehingga administrator system yang sedang berada di luar instansi atau perusahaan tidak dapat mengetahui ketika server mengalami serangan. Selain itu pemblokiran terhadap serangan masih dilakukan secara manual menggunakan IPTables sehingga memerlukan campur tangan administrator system. Berdasarkan permasalahan tersebut maka mendorong peneliti mengembangkan system IPS yang diintegrasikan dengan Telegram dan IPTables sehingga administrator system dapat memperoleh notifikasi ketika terjadi serangan kapan pun dan dimana pun. Selain itu system dapat secara otomatis melakukan pemblokiran serangan. Pada tahap *analysis* dilakukan pengumpulan data dan analisa data. Pada tahap *desain* dilakukan rancangan jaringan ujicoba, pengalamatan IP, perancangan alur kerja system dan kebutuhan perangkat keras dan lunak. Pada tahap simulation prototyping memuat tentang instalasi konfigurasi pada masing-masing perangkat, ujicoba dan analisa hasil ujicoba. Terdapat 5 skenario uji coba yang dilakukan meliputi *Ftp Attack, Telnet Attack, Bruteforce Form Login menggunakan Hydra Attack, Remote File Incusion (RFI) Attack* serta *Http Bruteforce menggunakan Hydra Attack*. Adapun kesimpulan dari penelitian ini adalah penerapan IPS berbasis Snort yang diintegrasikan dengan telegram serta IPTables maka server dapat mendeteksi serangan yang masuk.

Kata Kunci: Jaringan, *IPS, Telegram, Server, Administrator, Internet, NDLC.*

ABSTRACT

Security is one very important part in Information Technology (IT) which has been utilized in various fields. Utilization of IT can facilitate operations so as to improve service quality. But on the other hand if it is not maintained its security will have an impact on the availability of services. Every institution or institution must have a prevention against open access from unauthorized parties. The role of the defense system in general lies with the administrator as a network manager who has full access to the network infrastructure that he built. There are various methods produced by several researchers who have implemented security-related services on an Internet server, one of which is the Intrusion Prevention System (IPS). The IPS system implemented by previous researchers has not been integrated with telegrams so that system administrators who are outside the agency or company cannot find out when the server has an attack. Besides blocking attacks is still done manually using IPTables so that it requires the intervention of a system administrator. Based on these problems, it encourages researchers to develop IPS systems that are integrated with Telegram and IPTables so that system administrators can get notifications when an attack occurs anytime and anywhere. In addition the system can automatically block attacks. In the analysis phase, data collection and data analysis are carried out. At the design stage, a trial network design, IP addressing, system workflow design and hardware and software requirements are carried out. At the simulation stage prototyping includes the configuration installation on each device, testing and analyzing the results of trials. There are 5 test scenarios conducted including Ftp Attack, Telnet Attack, Bruteforce Form Login using Hydra Attack, Remote File Incusion (RFI) Attack and Http Bruteforce using Hydra Attack. The conclusion of this study is the application of Snort-based IPS integrated with telegram and IPTables, the server can detect incoming attacks.

Keyword: *Network, IPS, Telegram, Server, Administrator, Internet, NDLC.*

I. PENDAHULUAN

Keamanan merupakan salah satu bagian yang sangat penting dalam Teknologi Informasi (TI) yang telah dimanfaatkan di berbagai bidang baik institusi pendidikan, industri maupun kesehatan. Pemanfaatan TI dapat memperlancar operasional sehingga meningkatkan kualitas layanan. Namun di sisi lain apabila tidak dijaga keamanannya maka akan berdampak pada ketersediaan layanan. Setiap institusi atau lembaga harus memiliki pencegahan terhadap keterbukaan akses dari pihak yang tidak berhak. Peran pertahanan sistem pada umumnya terletak pada *administrator* sebagai pengelola jaringan yang memiliki akses penuh terhadap infrastruktur jaringan yang dibangunnya. Salah satu metode pencegahan jika sebuah serangan masuk ke system server adalah *Intrusion Prevention System(IPS)*.

Menurut Monoarfa [1] 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.

Seorang *administrator* bertanggung jawab terhadap segala jenis serangan yang tiba-tiba datang mengancam sebuah system server, Sebuah jaringan komputer harus mampu memberikan rasa aman terhadap segala jenis akses yang dilakukan oleh seorang *user*, dengan memberikan jaminan informasi atau data pribadi aman dari pengaksesan dari seorang *intruder* (penyerang). Penelitian yang dilakukan oleh Gundohanindijo [2] mengkolaborasikan *Intrusion Detection System (IDS)* dan IPS untuk membuat sebuah sistem yang dapat mengamankan informasi yang terdapat pada jaringan komputer dari pihak lain. Dalam penelitian yang di lakukan Oleh Eky [3] menghasilkan system pengamanan server internet menggunakan IDS yang mampu mengirimkan notifikasi ke telegram saat terjadi serangan sehingga administrator akan mengetahui jika nanti adanya sebuah seragan dari attacker, setelah itu administrator akan menindaklanjuti serangan tersebut melalui *Telegram*. Selain itu penelitian yang dilakukan oleh Kusnadi [4] Membahas tentang bagaimana mengamankan daringan computer menggunakan Firewall yang di tambahkan VPN sebagai Autentifiksai, IDS sebagai mendeteksi adanya serangan dari penyusup dan IPS untuk mendeteksi sekaligus mencegah dengan memfilter serangan. Dalam penelitian Yoga Widya Pradipta, Asmunin [5] juga membahas tentang penanggulangan serangan dari attacker dengan bantuan snort dan IP Tables, kemudian memblock IP attacker agar tidak bisa melakukan komunikasi dengan server. Sedangkan penelitian yang dilakukan oleh Khadafi [6] yang tentang sistem keamanan open cloud computing menggunakan IDS dan IPS untuk layanan *Infrastructure as a Service (IaaS)* yang diimplementasikan pada aplikasi open cloud computing. Tujuannya digunakan untuk memantau dan memproteksi serangan penyusup dari luar yang hendak masuk ke system, dan selanjutnya memberikan laporan ke administrator jaringan jika terdapat serangan yang terjadi di dalam lingkungan cloud.

Berdasarkan penelitian sebelumnya maka mendorong peneliti untuk mengkolaborasikan IPS berbasis *Snort* dengan Telegram sebagai pengamanan server internet sehingga administrator dapat memperoleh notifikasi di mana dan kapan pun ketika terjadi serangan. Selain itu system dapat melakukan pemblokiran secara otomatis menggunakan *IPTables* yang dikemas dalam bentuk *shell script* dan dipicu eksekusinya oleh aplikasi *IM Auto Reply* ketika serangan tersebut terjadi sehingga meminimalkan campur tangan secara manual dari administrator. Administrator juga memperoleh pesan terkait status eksekusi shell script dan status dari *IPTables*.

Manfaat dari penelitian ini adalah *administrator* tidak perlu lagi memantau keamanan server internet selama 24 jam karna setiap akan terjadi serangan maka aka ada notifikasi secara langsung lewat telegram untuk mengetahui kondisi sistem yang dikelola dan jika terjadi serangan otomatis dapat diketahui jenis serangan yang dilakukan oleh *attacker*. *Administrator* juga tidak perlu melakukan tindakan lebih karena secara otomatis serangan akan dicegah menggunakan metode IPS.

II. METODOLOGI PENELITIAN

Metode penelitian yang digunakan adalah *Network Development Life Cycle (NDLC*). Dari 6 (enam) tahapan yang ada pada *NDLC* penulis hanya menggunakan 3 tahapan yaitu *Analysis, Design, Simulation Prototyping.*

A. Tahap Analis (*Analysis*)

Tahapan ini dibagi menjadi dua bagian yaitu tahap pengumpulan data dan tahap analisa data.

1) Pengumpulan Data

Pada tahap pengumpulan data ini penulis menggunakan metode studi literatur yaitu

dengan mempelajari beberapa artikel ilmiah yang membahas tentang analisa keamanan *server internet* dengan menggunakan *Intrusion Prevention System (IPS)*.

TABEL I
ARTIKEL TENTANG PEMBAHASAN *IPS*

No	Penulis	Tahun	Jurnal	Pembahasan
1	Eky Galih Gunanda	2018	Analisa Penerapan Intrution Detection System (IDS) Berbasis Snort Dengan Telegram Untuk Pengamanan Server Internet	Membahas tentang system pendeteksi terhadap serangan terhadap server internet menggunakan metode Intrution Detection System yang langsung terintegrasi dengan telegram.
2	Jutono Gondoha nindijo	2012	*IPS (Intrusion Prevention System)* Untuk Mencegah Tindak Penyusupan / Intrusi	Membahas tentang cara kerja Intrusion Prevention System dalam menyeleksi paket-paket yang masuk ke server dan akan menjalankan suatu tindakan jika terjadisebuah kejadian yang sudah di konfigurasi oleh administrator.
3	Irwan Tanu Kusnadi	2018	Pengamanan Jaringan Komputer Dengan VPN, Firewall, IDS dan IPS	Membahas tentang bagaimana mengamankan daringan computer menggunakan *Firewall* yang di tambahkan VPN sebagai otentikasi, IDS sebagai mendeteksi adanya serangan dari penyusup dan IPS untuk mendeteksi sekaligus mencegah dengan memfilter serangan.
4	Yoga Widya Pradipta, Asmunin	2017	Implementasi Intrusion *Prevention System (IPS)* Menggunakan *Snort* Dan *IP Tables* Berbasis *Linux*	Membahas tentang penanggulangan serangan dari *attacker* dengan bantuan *snort* dan *IP Tables*, kemudian memblock *IP attacker* agar tidak bisa melakukan komunikasi dengan server.

2) Analisa Data

Berdasarkan hasil penelusuran artikel jurnal ilmiah yang terkait, bahwa Keamanan server internet yang terfokus untuk melakukan pencegahan terhadap serangan yang masuk ke server internet dengan menerapkan system IDS dan IPS yang menggunakan *snort*.

B. Tahap Desain (*Design*)

Tahap ini membuat rancangan yang meliputi rancangan jaringan ujicoba, rancangan pengalamat *IP*, rancangan alur kerja sistem, kebutuhan perangkat keras dan perangkat lunak.

C. Tahap Simulation *Prototyping*

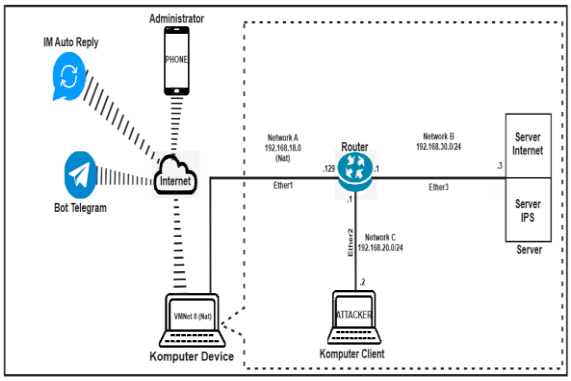
Pada tahap ini memuat tentang tahap instalasi konfigurasi, uji coba dan analisa hasil uji coba yang dilakukan pada masing-masing perangkat yang digunakan berdasarkan rancangan ujicoba.

III. HASIL DAN PEMBAHASAN

A. Perancangan Jaringan Ujicoba

Pengujian disimulasikan menggunakan virtualisasi berbasis *VMWare Workstation* terdiri dari 3 Dimana 1 (satu) laptop tersebut akan digunakan untuk 3 OS virtual machine. 1 (satu) *server* untuk dialokasikan sebagai *snort dan server internet*, 1 (satu)

perangkan *router* dan 1 (satu) *client* yang akan menjadi *attacker*.



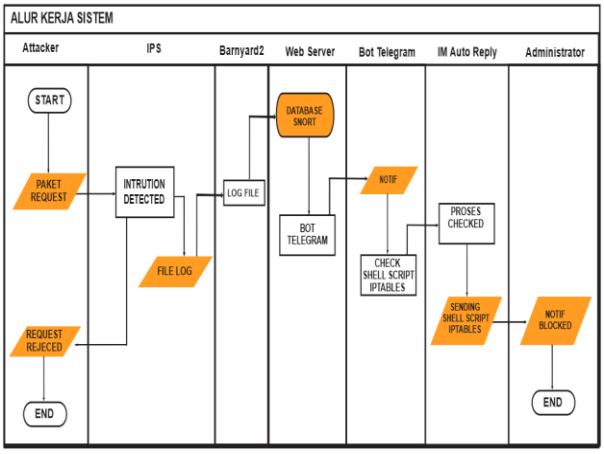
Gbr. 1 Topologi jaringan ujicoba

Untuk keterangan pengalamatan IP yang digunakan pada jaringan ujicoba ini dapat dilihat pada tabel berikut:

TABEL II
PENGALAMATAN *IP ADDRESS*

No	Perngkat	*IP Address*	*Netmask*
1.	*server internet*	192.168.30.3	255.255.255.0
2.	*Snort*	192.168.30.3	255.255.255.0
3.	*Attacker*	192.168.20.2	255.255.255.0
4.	*Router Ether1*	192.168.20.1	255.255.255.0
5.	*Router Ether2*	192.168.30.1	255.255.255.0

Setiap ada *request* yang masuk ke *server internet* akan di kroscek oleh *snort* terlebih dahulu, selanjutnya paket yang masuk akan dilakukan pengecekan terhadap *rule* yang sudah di buat, apabila *request* yang masuk memiliki kecocokan dengan aturan pada *rule* yang sudah dibuat maka snort akan merekam aktifitas tersebut lalu menyimpan hasil rekaman ke dalam direktori log. Setelah itu *barnyard2* akan menyimpan file *log* tersebut ke dalam *database* dalam bentuk *record*. *Kemudia server Internet* akan mengirimkan *notification* kepada *administrator* melalui aplikasi *telegram*. Setelah pesan terkirim ketelegram, telegram akan mengirim paket ke aplikasi *IM Auto Reply* berupa kalimat yang sudah dipilih dan juga sudah terdaftar pada aplikasi *IM Auto Reply* yang kemudian nanti akan mengirimkan balasan berupa *shell script telegram* yang berisikan aturan *IPTables* untuk memblokir *intrusi* yang masuk. Desain alur kerja sistem dapat dilihat pada gambar berikut:



Gbr. 2 Rancangan alur kerja sistem

B. Skenario Ujicoba

Pada tahap skenario hasil ujicoba ini, ada 5 (lima) jenis skenario ujicoba yang diterapkan yaitu *Ftp Attack, Telnet Attack, Bruteforce Form Login WEB menggunakan Hydra Attack, Remote File Incusion (RFI) Attack dan HTTP Bruteforce menggunakan Hydra Attack.* Pengujian ini dilakukan untuk

mengetahui apakah server internet dapat mendeteksi serangan sebelum penerapan IDS dilakukan dan Pengujian ini dilakukan untuk mengetahui apakah IDS yang diterapkan ke dalam server internet dapat merekam intrusi yang masuk serta dapat mengirimkan notifikasi ke administrtator, sehingga administrator dapat melakukan tindakan pencegahan untuk mengamankan server internet.

Adapun tahapan pengujian serangan yang akan dilakukan adalah sebagai berikut:

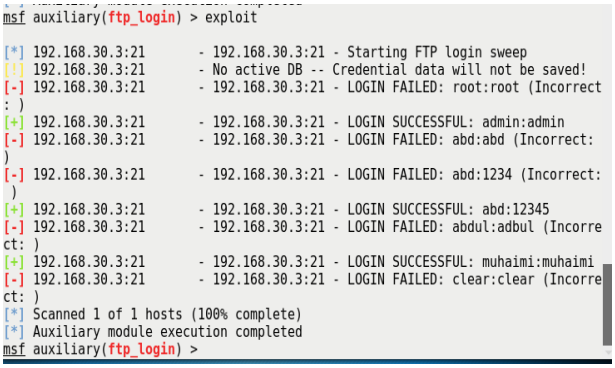
1) Pengujian dengan *FTP Attack*, yaitu dengan mencoba mendapatkan akses
2) Pengujian dengan Telnet Attack, yaitu dengan mencoba mendapatkan *username* dan *password* untuk mengakses *server internet* dengan *SSH*.
3) Pengujian dengan *Bruteforce Form Login WEB* Menggunakan *Hydra Attack*, yaitu dengan mencoba mendapatkan *username* dan *password* untuk mengakses *Form Login* pada sebuah *server*.
4) Pengujian dengan *Remote File Incusion (RFI) Attack*, yaitu dengan mencoba mengakses server dengan membuat *backdoor* sebagai jalan untuk mengakses *server*.
5) Pengujian dengan *HTTP Bruteforce Menggunakan Hydra Attack*, yaitu sebuah metode untuk menebak suatu kunci dari sebuah enkripsi atau sebuah otentikasi dengan cara mencobanya berkali-kali dengan berbagai macam kombinasi huruf, angka dan simbol.

C. Hasil Analisa Ujicoba Sebelum dan Setelah Penerapan IDS

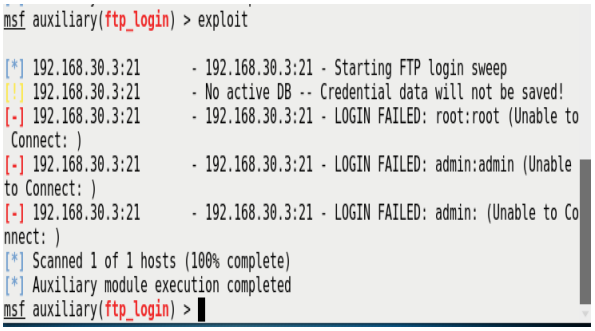
Pengujian ini dilakukan untuk mengetahui apakah *server internet* dapat mendeteksi serangan sebelum penerapan *IPS* dilakukan dan Pengujian ini dilakukan untuk mengetahui apakah *IPS* yang diterapkan ke dalam *server internet* dapat merekam intrusi yang masuk serta dapat mengirimkan notifikasi ke *telegram dan nantinya pengaktifan IPTable* dilakukan secara otomatis oleh *IM Auto Reply*, sehingga *administrator* tidak perlu melakukan tindakan pencegahan secara manual.

1) Brute force FTP Attack

Pada penelitian ini metode *brute force* digunakan untuk mengekplorasi *username* dan *password ftp* dengan bantuan *wordlist* yang sudah disediakan.



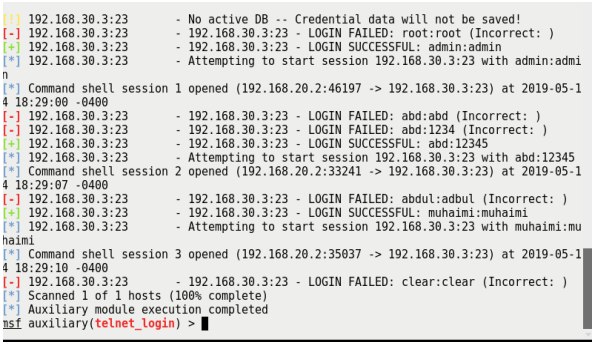
Gbr. 3 Hasil intrusi *ftp attack* sebelum penerapan *IPS*



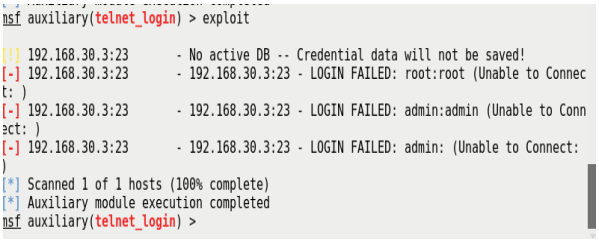
Gbr. 4 Hasil intrusi *ftp attack* setelah penerapan *IPS*

2) Brute force Telnet Attack

Pada penelitian ini metode *brute force* digunakan untuk mengekplorasi *username* dan *password telnet* dengan bantuan *wordlist* yang sudah disediakan.



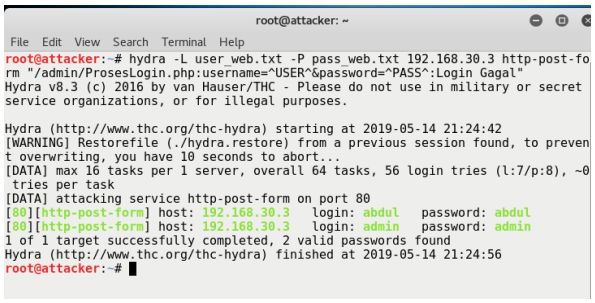
Gbr. 5 Hasil intrusi *Telnet attack* sebelum penerapan *IPS*



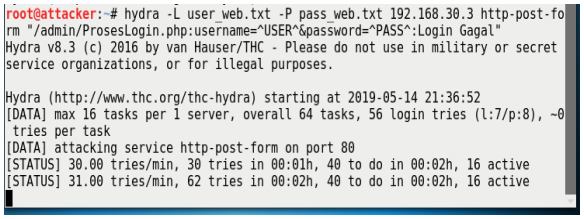
Gbr. 6 Hasil intrusi *Telnet attack* setelah penerapan *IPS*

3) Brute force Form Login WEB Menggunakan Hydra Attack

Pada penelitian ini metode *brute force* digunakan untuk mendapatkan username dan password untuk mengakses Form Login pada sebuah server.

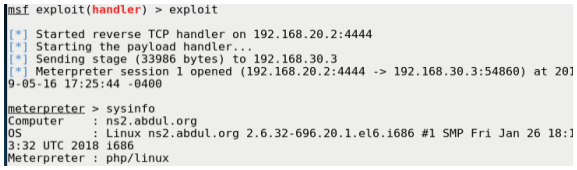


Gbr. 7 Hasil intrusi *Form Login WEB Menggunakan Hydra Attack* sebelum penerapan *IPS*



Gbr. 8 Hasil intrusi *Form Login WEB Menggunakan Hydra Attack* setelah penerapan *IPS*

4) Remote File Incusion (RFI) Attack
yaitu dengan mencoba mengakses server dengan membuat *backdoor* sebagai jalan untuk mengakses *server*..

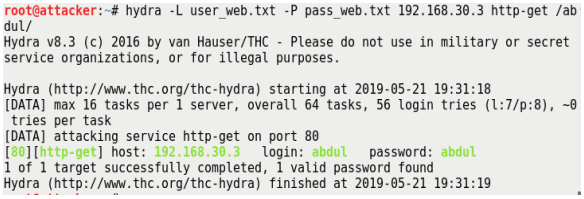


Gbr. 9 Hasil intrusi *Remote File Incusion Attack* sebelum penerapan *IPS*

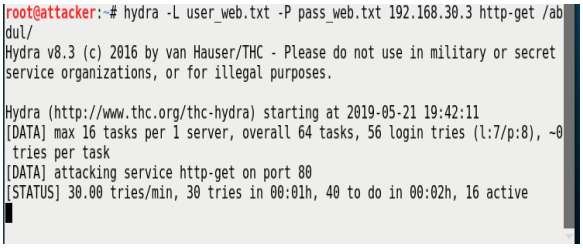
Gbr. 10 Hasil intrusi *Remote File Incusion Attack* setelah penerapan *IPS*

5) Brute force HTTP Menggunakan Hydra Attack

yaitu sebuah metode untuk menebak suatu kunci dari sebuah enkripsi atau sebuah otentikasi dengan cara mencobanya berkali-kali dengan berbagai macam kombinasi huruf, angka dan simbol.



Gbr. 11 Hasil intrusi *Bruteforce HTTP Menggunakan Hydra Attack* sebelum penerapan *IPS*



Gbr. 12 Hasil intrusi *Bruteforce HTTP Menggunakan Hydra Attack* setelah penerapan *IPS*

Berdasarkan hasil uji coba yang telah dilakukan maka dapat diperoleh hasil analisa sebagai berikut:

1. Serangan yang dilakukan oleh attacker terhadap server Internet tidak dapat terdeteksi sebelum dilakukan penerapan IPS. Sebaliknya setelah IPS diterapkan maka aktifitas serangan yang masuk ke server internet akan terdeteksi oleh snort sebagai dampak dari pencocokan trafik terhadap rule snort yang sudah dibuat. Table memperlihatkan perbandingan kemunculan pesan notifikasi sebelum dan sesudah penerapan IPS.

TABEL III
TABEL PERBANDINGAN PENERAPAN *IPS* SEBELUM DAN SESUDAH

No	Jenis Serangan	Sebelum Penerapan IPS	Sesudah Penerapan IPS
1	*FTP Attack*	Intrusi yang masuk ke server internet tidak dapat di identifikasi sebagai sebuah intrusi	Terdeteksi pesan 05/14-02:11:39.106142 [**] [1:10000002:2] Snort Alert [1:10000002:2] [**] [classification ID: 0] [Priority ID: 0] {TCP} 192.168.20.2:34163 -> 192.168.30.3:21
2	Telnet Attack		Terdeteksi Pesan 05/14-03:03:44.798463 [**] [1:10000022:23] Snort Alert [1:10000023:23] [**] [classification ID: 0] [Priority ID: 0] {TCP} 192.168.20.2:34099 -> 192.168.30.3:23
3	Bruteforce Form Login WEB Menggunakan hydra Attack		Terdeteksi Pesan 05/14-05:39:20.973449 [**] [1:10000012:12] Snort Alert [1:10000012:12] [**] [classification ID: 0] [Priority ID: 0] {TCP} 192.168.20.2:41530 -> 192.168.30.3:80
4	Remote File Incusion (RFI) Attack		Terdeteksi Pesan 05/16-01:43:59.970366 [**] [1:10000020:20] Snort Alert [1:10000020:20] [**] [classification ID: 0] [Priority ID: 0] {TCP} 192.168.20.2:51002 -> 192.168.30.3:80
5	Http Bruteforce Menggunakan Hydra Attack		Terdeteksi Pesan 05/21-01:50:31.787361 [**] [1:10000021:21] Snort Alert [1:10000021:21] [**] [classification ID: 0] [Priority ID: 0] {TCP} 192.168.20.2:51176 -> 192.168.30.3:80

2. Serangan yang terdeteksi akan memicu alert dan disimpan sebagai file log di dalam directory /var/log/snort serta disimpan ke database snort yang nantinya akan memicu sistem untuk mengirimkan notifikasi melalui telegram bahwa telah terjadi intrusi ke dalam server internet.
3. Server akan mengirimkan notifikasi ke telegram ketika serangan terdeteksi oleh IPS Snort.

TABEL IV
NOTIFIKASI SERANGAN MELALUI *TELEGRAM*

No	Jenis Serangan	Isi Pesan
1	*FTP Attack*	WARNING FTP!! Ada percobaan akses ke FTP pada 2019-05-14 02:11:39 dan berhasil ditindak lanjuti

2	Telnet Attack	WARNING TELNET!! Ada percobaan akses ke TELNET pada 2019-05-14 03:26:06 dan berhasil ditindak lanjuti
3	Bruteforce Form Login WEB Menggunakan hydra Attack	WARNING FORM BRUTEFORCE!! Ada serangan Brute Force pada form login website pada 2019-05-14 05:39:20 dan berhasil ditindak lanjuti
4	Remote File Incusion (RFI) Attack	WARNING RFI!! Ada serangan RFI masuk ke web server pada 2019-05-16 01:43:56 dan berhasil ditindak lanjuti
5	Http Bruteforce Menggunakan Hydra Attack	WARNING AUTH BRUTEFORCE!! Brute Force http auth basic terdeteksi ke web server pada 2019-05-21 01:50:22 dan berhasil ditindak lanjuti

4. Pesan peringatan terkait terjadinya serangan yang diterima melalui telegram akan secara otomatis di respon oleh aplikasi IM AUTO REPLY. Aplikasi tersebut akan memcocokkan kalimat-kalimat yang di kirimkan oleh system ke Telegram seperti WARNING FTP!!, WARNING TELNET!!, WARNING FORM BRUTEFORCE!!, WARNING RFI!!, WARNING AUTH BRUTEFORCE!!. yang nantinya akan menyesuaikan dengan shell script telegram yang berisikan aturan IPTables sehingga dapat memblokir intrusi yang masuk. Pencocokan pesan yang masuk pada telegram oleh IM Auto Reply

TABEL V
PENCOCOKAN *SHELL SCRIPT TELEGRAM* UNTUK MENGAKTIFKAN *IPTABLES*

No	Pesan Masuk	shell script telegram
1	*WARNING FTP!!*	/run sh /root/blok_ftp.sh
2	WARNING TELNET!!	/run sh /root/blok_telnet.sh
3	WARNING FORM BRUTEFORCE!!	/run sh /root/blok_web.sh
4	WARNING RFI!!	/run sh /root/blok_web.sh
5	WARNING AUTH BRUTEFORCE!!	/run sh /root/blok_web.sh

5. Administrator dari server Internet akan memperoleh pesan notifikasi pada telegram terkait Shell script IPTables yang telah dieksekusi secara otomatis, serta status dari IPTables melalui pencocokan pesan yang masuk pada telegram. Tables dibawah memperlihatkan pencocokan pesan yang masuk pada telegram agar IM Auto Reply memicu eksekusi perintah " /run iptables –L".

TABEL VI
TABEL PENCOCOKAN SHELL SCRIPT TELEGRAM UNTUK PENGECEKAN IPTABLES

No	Pesan Masuk	shell script telegram
1	*$ sh /root/blok_ftp.sh*	/run iptables -L
2	$ sh /root/blok_telnet.sh	/run iptables -L
3	$ sh /root/blok_web.sh	/run iptables -L
4	$ sh /root/blok_web.sh	/run iptables -L
5	$ sh /root/blok_web.sh	/run iptables -L

6. Sebelum aturan IPTables diterapkan maka sistem tidak dapat menangani serangan yang masuk. Sebaliknya serangan dapat diblokir setelah aturan IPTables diterapkan,

TABEL VII
TABEL BUKTI SEBELUM DAN SESUDAH PENERAPAN IPTABEL

No	Jenis Serangan	Sebelum Penerapan IPTabel	Sesudah Penerapan IPTabel
1	*FTP Attack*	Intrusi yang dilakukan oleh attacker berhasil masuk ke Server	DROP tcp – 192.168.20.2 abdul.org tcp dpt:ftp
2	Telnet Attack		DROP tcp – 192.168.20.2 abdul.org tcp dpt:telnet
3	Bruteforce Form Login WEB Menggunakan hydra Attack		DROP tcp – 192.168.20.2 abdul.org tcp dpt:http
4	Remote File Incusion (RFI) Attack		DROP tcp – 192.168.20.2 abdul.org tcp dpt:http
5	Http Bruteforce Menggunakan Hydra Attack		DROP tcp – 192.168.20.2 abdul.org tcp dpt:http

IV. KESIMPULAN

Berdasarkan hasil pembahasan dan hasil uji coba dengan menggunakan metode *Port Scanning, Http Attack, FTP Attack, SSH, Attack, Telnet Attack* dapat disimpulkan sebagai berikut:

1. *IPS* berbasis *Snort* dapat *diintegrasikan* dengan *Telegram* dan *IPTables* sehingga dapat mendeteksi dan memblokir lima serangan yang terjadi secara otomatis meliputi *Ftp Attack, Telnet Attack, Bruteforce Form Login* menggunakan *Hydra Attack, Remote File Incusion (RFI) Attack serta Http Bruteforce* menggunakan *Hydra Attack.*
2. Administrator sistem dapat mengetahui serangan yang terjadi pada server internet melalui pesan notifikasi yang memuat informasi jenis serangan dan kapan terjadinya yang dikirim oleh sistem yang dibuat melalui Telegram.
3. Sistem yang dibuat meminimalkan campur tangan dari administrator untuk mengatasi serangan yang terjadi pada server Internet. Hal ini berbanding terbalik dengan sebelum diterapkannya sistem IPS yang terintegrasikan dengan telegram pada server internet, dimana pemblokiran dilakukan dengan cara mengaktifkan IPTables dilakukan secara manual oleh adminitrator baik dengan cara mengetikkan perintah pengaktifan IPTables melalui terminal server atau melalui bot telegram.
4. Sistem yang dibuat dapat mengatasi serangan yang masuk ke server internet dengan menggunakan aturan IPTables yang dieksekusi secara otomatis menggunakan aplikasi IM Auto Reply yang diawali dengan pencocokan terhadap pesan notifikasi serangan yang terjadi pada telegram.
5. Administrator memperoleh 3 (tiga) jenis pesan melalui telegram meliputi pesan notifikasi terkait serangan, pesan hasil eksekusi shell script IPTables, dan pesan status dari IPTables.

V. SARAN

Adapun saran-saran untuk pengembangan skripsi ini lebih lanjut adalah sebagai berikut:

1. Mengembangkan aplikasi agar mendukung notifikasi serangan yang terdeteksi oleh *snort* melalui *telegram* secara *real-time*.
2. Mengembangkan system agar dapat mengirimkan pesan notifikasi ke telegram agar langsung mengaktifkan IPTables tanpa menggunakan aplikasi pihak ketiga.
3. Mengembangkan sistem IPS yang ditempatkan secara terpisah atau mandiri sehingga dapat digunakan untuk mengamankan sistem lainnya yang terhubung di jaringan.
4. Mengembangkan aplikasi agar notifikasi yang masuk ke aplikasi telegram dapat terkirim secara real-time begitu serangan terdeteksi oleh snort.
5. Menguji coba serangan lain pada system IPS.
6. Mengembangkan sistem agar dapat membuat rule atapun memperbaharui rule snort secara otomatis.

REFERENSI

[1] Mohamad Nurul Huda Monoarfa, Xaverius B.N Najoan, A. A. . S. (2016). Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi. *E-Journal Teknik Elektro Dan Komputer*, *5*(Keamanan Jaringan), 34–45.

[2] Gondohanindijo, J. (2012). IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan/Intrusi. *Majalah Ilmiah INFORMATIKA*. Retrieved from http://www.unaki.ac.id/ejournal/index.php/majalah-ilmiah-informatika/article/view/78

[3] Eky Galih Gunanda (2017). Analisa Penerapan *Intrution Detection System* (IDS) Berbasis *Snort* Dengan *Telegram* Untuk Pengamanan *Server Internet*. Skripsi. Mataram: STMIK Bumigora Mataram.

[4] Kusnadi, I. T. (2018). Pengamanan Jaringan Komputer Dengan VPN , Firewall , IDS dan IPS Pengamanan Jaringan Komputer Dengan VPN , Firewall , IDS dan IPS. *Jurnal Informatika*, (April 2016), 0–7.

[5] Pradipta, Y. W., & Asmunin. (2017). *IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES*. surabaya: Universitas Negeri Surabaya.

[6] Khadafi, S., Meilani, B. D., & Arifin, S. (2017). Sistem Keamanan Open Cloud Computing Menggunakan Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System). *Jurnal IPTEK*, *21*(2), 67–76. Retrieved fromhttp://ejurnal.itats.ac.id/index.php/iptek/article/view/207