Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server

Ery Setiyawan Jullev Atmadji
Program Studi Teknik Informatika
Politeknik Negeri Jember
ery@polije.ac.id

Bekti Maryuni Susanto
Program Studi Teknik Komputer
Politeknik Negeri Jember
bekti @polije.ac.id

Rahardian Wiratama
Program Studi Teknik Komputer
Politeknik Negeri Jember
aryatuxpub@gmail.com

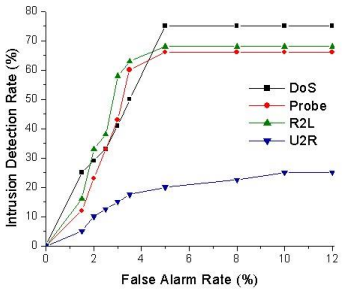
Abstrak - Keamanan jaringan menjadi hal yang penting untuk semua industri dan perusahaan untuk melindungi data dan informasi penting yang berada didalamnnya. Perlindungan keamanan dalam suatu jaringan umumnya berbasis pada keamanan transmisi data yang dibuat dan diaplikasikan untuk membantu mengamankan suatu jaringan tertentu. Untuk lebih mengoptimalkan pengambilan keputusan maka diperlukan sebuah mesin yang mampu berkolaborasi dengan database IDS maupun IPS, sehingga tipikal serangan yang sangat beragam dapat dipetakan dengan lebih optimal. Salah satu *database* yang mempunyai *rule* yang sudah ada adalah IPTABLES, hal ini dikarenakan pada IPTABLES terdapat fungsi *firewall* yang mampu menangani jenis serangan yang berlipat serta masif. *Server* yang akan digunakan adalah *server* dengan sistem operasi Linux. Sedangkan *database* serangan IDS yang digunakan adalah *database* KDD 99 yang sudah diakui sebagai salah satu *database* serangan yang sangat kompleks. Dengan pemanfaatan IPTABLES ini maka diharapkan keamanan *server* akan bisa dimonitor dengan lebih optimal. IPTABLES biasanya digunakan sebagai salah satu *firewall* yang digunakan pada *server*.
Kata Kunci : *Monitoring* Keamanan Jaringan, IDS, IPS, IP TABLES, KDD99.

I. PENDAHULUAN

Keamanan jaringan menjadi hal yang penting untuk semua industri dan perusahaan untuk melindungi data dan informasi penting yang berada di dalamnnya. Perlindungan keamanan dalam suatu jaringan umumnya berbasis pada keamanan transmisi data yang dibuat dan diaplikasikan untuk membantu mengamankan suatu jaringan tertentu. Teori keamanan data biasanya menggunakan teori kriptografi, integritas dan ketersediaan data serta strategi keamanan lainnya.

Metode-metode keamanan jaringan yang sudah muncul seperti menggunakan IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*), *Firewall*, *Network Security Based of Knowledge* untuk menghambat terjadinya penyerangan atau penyusupan. Cara-cara yang digunakan bervariasi tergantung kebutuhan pengguna. IP tables adalah salah satu sistem yang dirancang sebagai sistem keamanan jaringan komputer yang penting perananya dalam menjaga integritas dan validitas, serta memastikan ketersediaan layanan bagi seluruh pengguna [1].

Tugas utama dari setiap sistem pendeteksi serangan adalah mengenali apakah suatu kondisi serangan tercapai atau tidak. Pendeteksi penyerangan tersebut biasanya disebut dengan IDS (*Intrusion Detection System*), pada IDS kondisi dimana terdapat serangan atau tidak disebut model intrusi untuk menentukan apakah ada gangguan atau tidak, dimana setiap gangguan dapat mempunyai banyak bentuk yang berbeda. Apapun modelnya, kinerja detektor dapat digambarkan dengan kurva karakteristik operasi penerima atau yang biasa disebut dengan *Receiver Operating Characteristic* (ROC) [2].



Gambar 1. Contoh ROC [2]

Kurva ROC adalah nilai dari probabilitas deteksi (H) *versus* tingkat alarm palsu (F). Analisis ROC awalnya Diperkenalkan di bidang teori deteksi sinyal pada awal tahun 50an.

Selama ini penelitain masih berkutat pada bagaimana lebih mengefisienkan kinerja dari IDS itu sendiri. Salah satu caranya adalah dengan memanfaatkan IPTABLES sebagai salah satu mekanisme pengambilan keputusan tentang jenis serangan dan respon yang akan di ambil oleh IDS tersebut.

Sehingga untuk lebih mengoptimalkan pengambilan keputusan maka diperlukan sebuah mesin yang mampu berkolaborasi dengan *database* IDS, sehingga tipikal

serangan yang sangat beragam dapat dipetakan dengan lebih optimal. Salah satu *database* yang mempunyai *rule* yang sudah ada adalah IPTABLES, hal ini dikarenakan pada IPTABLES terdapat fungsi *firewall* yang mampu menangani jenis serangan yang berlipat serta masif.

Penelitian ini menerapkan IPTABLES yang selama ini berfungsi hanya sebagai *firewall* pada *server*, akan lebih dioptimalkan sebagai salah satu mekanisme IDS dan IPS. Sistem ini diterapkan pada *server* yang menggunakan sistem operasi Linux sebagai salah satu sistem operasi *server* yang sangat sering digunakan. Sedangkan *database* IDS yang digunakan adalah *database* KDD 99 yang sudah diakui sebagai salah satu *database* serangan yang sangat kompleks, sehingga diharapkan akan lebih memaksimalkan kinerja dari IPTABLES itu sendiri

II. METODOLOGI PENELITIAN

A. *Cyber Crime*

Menurut Kepolisian Ingris, *cyber crime* adalah segala macam penggunaan jaringan komputer untuk tujuan kriminal dan/atau kriminal berteknologi tinggi dengan menyalahgunakan kemudahan teknologi digital.

Sedangkan menurut Peter [3], *cyber crime* adalah "*The easy definition of cyber crime is crimes directed at a computer or a computer system. The nature of cyber crime, however, is far more complex. As we will see later, cyber crime can take the form of simple snooping into a computer system for which we have no authorization. It can be the feeing of a computer virus into the wild. It may be malicious vandalism by a disgruntled employee. Or it may be theft of data, money, or sensitive information using a computer system.*"

Dalam dua dokumen Kongres PBB yang dikutip oleh Barda Nawawi Arief [4], mengenai *The Prevention of Crime and the Treatment of Offenders* di Havana Cuba pada tahun 1990 dan di Wina Austria pada tahun 2000, menjelaskan adanya dua istilah yang terkait dengan pengertian *Cyber crime*, yaitu *cyber crime* dan *computer related crime*. Dalam *back ground paper* untuk lokakarya Kongres PBB X/2000 di Wina Austria, istilah *cyber crime* dibagi dalam dua kategori. Pertama, *cyber crime* dalam arti sempit (*in a narrow sense*) disebut *computer crime*. Kedua, *cyber crime* dalam arti luas (*in a broader sense*) disebut *computer related crime*.

B. *Intrusion Detection System*

IDS (*Intrution Detection System*) adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau *administrator* jaringan. Dalam banyak kasus IDS juga merespon terhadap *traffic* yang tidak normal/ anomali melalui aksi pemblokiran seorang *user* atau alamat IP (*Internet Protocol*) sumber dari usaha pengaksesan jaringan [5].

IDS sendiri muncul dengan beberapa jenis dan pendekatan yang berbeda yang intinya berfungsi untuk mendeteksi *traffic* yang mencurigakan didalam sebuah jaringan. Beberapa jenis IDS adalah : yang berbasis jaringan (NIDS) dan berbasis host (HIDS). Ada IDS yang bekerja dengan cara mendeteksi berdasarkan pada pencarian ciri-ciri khusus dari percobaan yang sering dilakukan. Cara ini hampir sama dengan cara kerja perangkat lunak antivirus dalam mendeteksi dan melindungi sistem terhadap ancaman. Kemudian ada juga IDS yang bekerja dengan cara mendeteksi berdasarkan pada pembandingan pola *traffic* normal yang ada dan kemudian mencari ketidaknormalan *traffic* yang ada [6]. Ada IDS yang fungsinya hanya sebagai pengawas dan pemberi peringatan ketika terjadi serangan dan ada juga IDS yang bekerja tidak hanya sebagai pengawas dan pemberi peringatan melainkan juga dapat melakukan sebuah kegiatan yang merespon adanya percobaan serangan terhadap sistem jaringan dan komputer.

C. *Intrusion Detection System*

IPS (*Intrusion Prevention System*) merupakan jenis metode pengamanan jaringan baik *software* atau *hardware* yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. IPS (*Intrusion Prevention System*) merupakan pengembangan dari dari IDS (*Intrusion Detection System*). Sebagai pengembangan dari teknologi *firewall*, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *ports* atau IP *address* seperti *firewall* umumnya. *Intrusion Detection System* selain dapat memantau dan *monitoring*, IPS (*Intrusion Prevention System*) dapat juga mengambil kebijakan dengan memblok paket yang lewat dengan cara 'melapor' ke *firewall*.

Ada beberapa metode IPS (*Intrusion Prevention System*) melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut:

i. *Signature-based Intrusion Detection System*

Pada metode ini, telah tersedia daftar *signature* yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data *signature* yang ada harus tetap ter-*update*.

ii. *Anomaly-based Intrusion Detection System*

Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*), sehingga IDS dan IPS dapat mengatahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS dan IPS menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan

(IDS) atau akan menolak paket tersebut untuk diteruskan (IPS).

IPS mengkombinasikan kemampuan *network based* IDS dengan kemampuan *firewall*, sehingga selain mendeteksi adanya penyusup juga bisa menindaklanjuti dengan melakukan pengeblokan terhadap IP yang melakukan serangan.

D. *IP TABLES*

IPTables adalah program aplikasi (berbasis Linux) yang memungkinkan *administrator* sistem untuk mengkonfigurasi tabel yang disediakan oleh *firewall kernel* Linux (diimplementasikan sebagai modul Netfilter yang berbeda) dan rantai dan aturan di tempat itu. Modul kernel yang berbeda dan program yang saat ini digunakan untuk protokol yang berbeda, *iptables* berlaku untuk IPV4, *ip6tables* ke IPV6, *arptables* ARP, dan *tables* ke *frame* Ethernet. IPTables membutuhkan hak akses yang tinggi untuk beroperasi atau melakukan konfigurasi yang dijalankan oleh "*root*" pengguna, selain itu gagal.

IPTables memiliki beberapa buah tabel yaitu NAT, MANGEL, dan FILTER. Penjelasannya sebagai berikut :

Table Mangle adalah tabel yang bertanggung jawab untuk melakukan penghalusan (*mangle*) paket seperti merubah *Quality of Service* (QOS), TTL, dan MARK di header TCP. Biasanya tabel ini jarang digunakan di lingkungan SOHO (*Small Office Home Ofiice*).

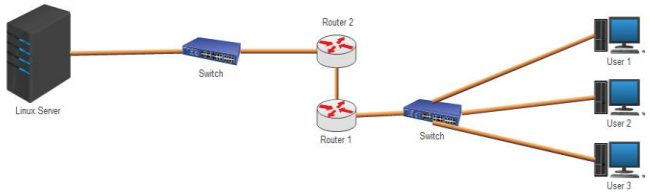
Table Filter adalah tabel yang bertanggung jawab untuk pemfilteran paket. Tabel ini mempunyai 3 rantai (*chain*) yaitu : - Rantai *Forward* yaitu rantai yang memfilter paket-paket yang akan ke server yang dilindungi oleh firewall. Rantai ini digunakan ketika paket-paket datang dari IP publik dan bukan dari IP lokal. Tabel NAT adalah tabel yang bertanggung jawab untuk melakukan *Network Address Translation* (NAT).

III. HASIL DAN PEMBAHASAN

Sebelum dilakukan implementasi program, perlu dilakukan analisa dan desain sistem untuk mempermudah implementasi program karena sebagai acuan untuk menghasilkan program yang baik.

A. Desain Arsitektural

Sistem keamanan pada server yang terkoneksi pada jaringan selama ini masih menggunakan *firewall* dengan konfigurasi *iptracking*, sehingga apabila ada serangan yang menggunakan *spoofing* maupun yang lain dibutuhkan sebuah mekanisme tambahan pula. Hal ini membuat kinerja dari *server* akan semakin berat. *monitoring* keamanan jaringan akan ditambahkan dengan mekanisme IDS dan IPS. *Server* yang akan digunakan adalah *server* dengan sistem operasi Linux. *Server* dengan sistem operasi jenis ini sering digunakan baik di industri maupun di dunia edukasi. Karena sebuah perangkat yang dapat diakses secara langsung pada jaringan publik membutuhkan mekanisme pengamanan agar terhindar dari kejadian pelanggaran keamanan. Untuk itu pada penelitian ini mengusulkan sebuah mekanisme pengamanan saluran komunikasi antara *user* dengan pemanfaatan IPTABLES sebagai IDS dan IPS. Dengan pemanfaatan IPTABLES ini maka keamanan server akan bias di *monitoring* dengan lebih optimal. IPTABLES biasanya digunakan sebagai salah satu *firewall* yang digunakan pada *server*. IPtables pada sistem ini berfungsi sebagai pendeteksi serangan serta pencegahan terhadap serangan serupa diwaktu yang lain. Gambaran sistem keamanan *server* dengan memanfaatkan IPTABLES sebagai IDS dan IPS dapat ditunjukkan pada Gambar 2.



Gambar 2. Perancangan Sistem.

B. Pembahasan

Pengujian pada penelitian ini meliputi *Denial Of Service* (DOS), SQL *Injection*, dan *Port Scanning*. Untuk *server* menggunakan Sistem Operasi Linux Ubuntu *Server* 14.04, sedangkan *attacker* menggunakan Sistem Operasi Linux Ubuntu *Desktop* 14.04 dan Windows 7. Pada *attacker* yang menggunakan Sistem Operasi Linux Ubuntu *Desktop* 14.04 akan melakukan penyerangan SQL *Injection* dan *Port Scanning*, sedangkan *attacker* Windows7 akan melakukan penyerangan DOS, *IPTables* akan mengatasi serangan-serangan tersebut.

Pengujian pertama adalah dengan menggunakan serangan berupa *SQLInjection*, hal yang dilakukan pertama adalah melakukan pengujian dengan memberikan karakter '(*quote*) pada akhir *address* sehingga didapatkan error yang kemudian dilakukan ekploitasi untuk mendapatkan *username* dan *password* admin. Untuk mendapatkan *username* dan *password* admin, terlebih dahulu mengetahui berapa kolom yang dimiliki. Dengan menggunakan perintah *union all select* untuk mengetahui banyaknya kolom dan *schema* dari *database* seperti ditunjukkan pada bagan 3

Gambar 3. *Testing* Dengan *Union All Select*

Untuk mendeteksi dan mengatasi serangan SQL *Injection* dengan mencegah *attacker* menggunakan eksploitasi pada *bug* SQL. Pada terminal *server* menggunakan perintah *rule iptable* seperti pada gambar 4.

```
iptables -A INPUT -p tcp -s 192.168.1.0/24 -m string --string "%27" --algo bm -j LOG --log-prefix "SQL INJECTION DETECTED "
iptables -A INPUT -p tcp -s 192.168.1.0/24 -m string --string "%27" --algo bm -j REJECT
```

Gambar 4. Rules Untuk Mendeteksi dan Mencegah SQL *Injection.*

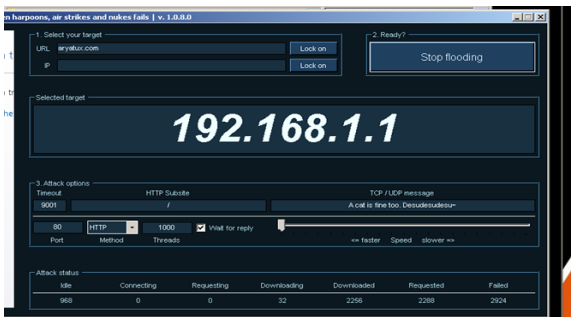
Pada baris pertama dari *rules* iptables gambar 4 digunakan untuk mendeteksi adanya serangan SQL *Injection* dan baris kedua digunakan untuk mengatasi serangan SQL *Injection*. Pada gambar 4 *rules iptables* menggunakan *string* %27 dikarenakan tanda kutip (*quote*) pada *browser* di-*encoding*, kemudian pada *rules iptables* tersebut menggunakan tipe algoritma BM (Boyer-Moore). Dalam *iptables* untuk tipe algoritma terdapat dua tipe yaitu BM (Boyer-Moore) dan KMP (Knuth-Morris-Pratt) dimana perbedaan dari dua tipe algoritma ini terletak pada cara kerjanya. KMP melakukan pencarian *string* dari kiri ke kanan sedangkan BM melakukan pencarian *string* dari karakter terakhir.

Pada saat serangan SQL *Injection* sebelum menggunakan iptables, *attacker* dapat mengakses *bug* SQL *Injection* dan mengeksploitasinya sehingga mendapatkan *username* dan *password* admin web. Namun setelah menggunakan *iptables*, serangan SQL *Injection* akan terdeteksi pada sistem *server* dan *attacker* tidak dapat mengakses *bug* SQL *Injection* sehingga *attacker* tidak dapat melakukan eksploitasi.

```
Jan 13 09:54:46 tuxnurmay kernel: [75427.975889] SQL INJECTION DETECTED IN=v
boxnet0 OUT= MAC=0a:00:27:00:00:00:08:00:27:8d:d2:cf:08:00 SRC=192.168.1.5 D
ST=192.168.1.1 LEN=359 TOS=0x00 PREC=0x00 TTL=64 ID=29440 DF PROTO=TCP SPT=5
6884 DPT=80 WINDOW=229 RES=0x00 ACK PSH URGP=0
Jan 13 09:55:13 tuxnurmay kernel: [75454.663313] SQL INJECTION DETECTED IN=v
boxnet0 OUT= MAC=0a:00:27:00:00:00:08:00:27:8d:d2:cf:08:00 SRC=192.168.1.5 D
ST=192.168.1.1 LEN=359 TOS=0x00 PREC=0x00 TTL=64 ID=29442 DF PROTO=TCP SPT=5
6884 DPT=80 WINDOW=229 RES=0x00 ACK PSH URGP=0
```

Gambar 5. Mendeteksi Serangan SQL *Injection.*

Serangan selanjutnya adalah *Denial of Service* (DoS) yang merupakan serangan yang dilakukan secara individual menggunakan satu mesin komputer. Pada percobaan kali ini attacker Windows 7 untuk menggunakan LOIC yaitu dengan memasukkan alamat target dan jenis metode serangannya yaitu HTTP.



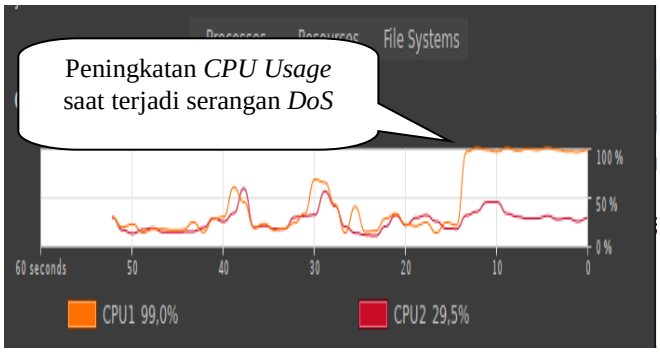
Gambar 6. Tampilan Program DoS Pada *Attacker* Windows 7.

Untuk mengatasi serangan DoS maka menggunakan *rules iptables* seperti pada bagan 7.

```
iptables -A INPUT -p tcp -m state --state NEW -m limit --limit 2/second --limit-burst 2 -j ACCEPT
iptables -A INPUT -p tcp -m state --state NEW -j LOG --log-prefix "DoS Detected "
iptables -A INPUT -p tcp -m state --state NEW -j DROP
```

Gambar 7 Rules IPTables Mendeteksi dan Mengatasi Serangan DoS.

Pada baris pertama pada *rules iptables* bagan 7 berfungsi untuk membatasi (limit) paket data yang baru masuk selama 2 detik, yang kemudian paket tersebut di *drop*. Pada baris kedua *rules iptables* berfungsi untuk mendeteksi serangan DoS. Pada saat terjadi serangan *Denial of Service* (DoS) sebelum menggunakan *iptables*, terjadi peningkatan pada CPU *Usage* yang mengakibatkan kinerja *server* berat seperti ditunjukkan pada gambar 8.

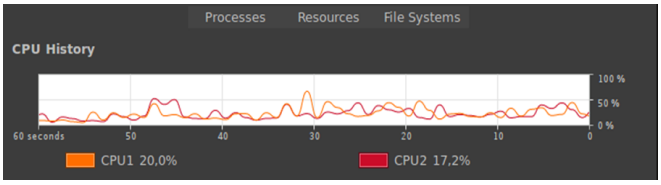


Gambar 8. Grafik CPU *Usage* Sebelum Menggunakan IPTables Ketika Terjadi Serangan DoS.

Setelah menggunakan iptables, serangan *Denial of Service* (DoS) akan terdeteksi pada sistem *server* dan serangan DoS tidak semasif sebelum menggunakan *iptables* sehingga tidak terjadi peningkatan yang drastis pada CPU *Usage.*

```
 WINDOW=29200 RES=0x00 SYN URGP=0
Jan 13 10:28:36 tuxnurmay kernel: [77457.372605] DoS Detected IN=vboxnet0 OU
T= MAC=0a:00:27:00:00:00:08:00:27:8d:d2:cf:08:00 SRC=192.168.1.5 DST=192.168
.1.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=6237 DF PROTO=TCP SPT=59208 DPT=80
WINDOW=29200 RES=0x00 SYN URGP=0
```

Gambar 9. Mendeteksi Serangan *Denial of Service* (DoS).



Gambar 10. Grafik CPU *Usage* Setelah Menggunakan *IPTables* Ketika Terjadi Serangan DoS.

Pengujian terakhir adalah dengan melakukan pengujian *port scanning*. *Port Scaning* adalah tindakan sistematis untuk memindai (*scanning*) *port* pada komputer. Pada proyek ini menggunakan nmap sebagai *tool* untuk memindai (*scanning*) *port*. Untuk mendeteksi adanya serangan *Port Scanning* maka menggunakan *rules* pada gambar 11 sedangkan untuk mengatasi serangan Port Scanning dengan menggunakan *rules iptables* pada gambar 12.

```
iptables -A INPUT -p tcp -i eth0 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j LOG --log-prefix "Port Scan Detected "
iptables -A FORWARD -p tcp -i eth0 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j LOG --log-prefix "Port Scan Detected "
```

Gambar 11. *Rules IPTables* untuk mendeteksi serangan *Port Scanning*.

```
iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
iptables -A INPUT -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
iptables -A INPUT -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
iptables -A INPUT -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -A INPUT -p tcp --tcp-flags ACK,FIN FIN -j DROP
iptables -A INPUT -p tcp --tcp-flags ACK,PSH PSH -j DROP
iptables -A INPUT -p tcp --tcp-flags ACK,URG URG -j DROP

iptables -A INPUT -p tcp -i eth0 -m state --state NEW -m recent --set
iptables -A INPUT -p tcp -i eth0 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j DROP
iptables -A FORWARD -p tcp -i eth0 -m state --state NEW -m recent --set
iptables -A FORWARD -p tcp -i eth0 -m state --state NEW -m recent --update --seconds 30 --hitcount 10 -j DROP
```

Gambar 12. Rules *IPTables* untuk mengatasi serangan *Port Scanning*.

Pada *rules iptables* gambar 11 berfungsi untuk mendeteksi serangan *Port Scanning*. Pada *rules iptables* gambar 12 untuk mengatasi serangan *Port Scanning*, pada baris pertama hingga baris sembilan berfungsi untuk memblok atau *drop* semua proses *stealth scanning port*, dimana prosesnya terdapat enam *packet flags* yang digunakan yaitu SYN (*Synchronize*), ACK (*Acknowledgement*), RST (*Reset*), URG (*Urgent*), PSH (*Push*), dan FIN (*Finished*). Kemudian pada *rules iptables* baris sepuluh hingga baris tiga belas berfungsi agar proses pengiriman paket data ke *web service* tidak terganggu oleh proses blok dari serangan *port scanning* tersebut.

Pada serangan *Port Scanning* sebelum menggunakan *iptables*, *attacker* dapat melakukan *scanning* terhadap *server* sehingga *attacker* mengetahui *port server* yang terbuka. Namun setelah menggunakan *iptables*, serangan *Port Scanning* akan terdeteksi pada sistem *server* dan *tool* nmap yang digunakan *attacker* akan mengalami *freeze* sehingga tidak berhasil melakukan proses *scanning port* pada *server*.

```
Jan 13 10:41:51 tuxnurmay kernel: [78253.005682] Port Scan Detected IN=vboxn
et0 OUT= MAC=0a:00:27:00:00:00:08:00:27:8d:d2:cf:08:00 SRC=192.168.1.5 DST=1
92.168.1.1 LEN=44 TOS=0x00 PREC=0x00 TTL=50 ID=40474 PROTO=TCP SPT=62523 DPT
=1034 WINDOW=1024 RES=0x00 SYN URGP=0
```

Gambar 13. Mendeteksi serangan *Port Scanning*.

IV. KESIMPULAN

Berdasarkan permasalahan dan pembahasan yang dikemukakan pada penelitian yang berjudul Pemanfaatan *IPTables* sebagai *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) pada Linux *Server*, maka dapat diambil kesimpulan yaitu *rule* yang ada pada *IPTables* dapat digunakan sebagai mekanisme pencegahan dan mengatasi serangan SQL *Injection*, *Denial of Service* (DoS) serta *Port Scanning* pada Linux *server*.

REFERENSI

[1] Sondakh, G, Najoan, M.E.I dan Lumenta, A. S. (2014). *Perancangan Filtering Firewall Menggunakan Iptables di Jaringan Pusat Teknologi Informasi Unsrat.* pp. 2301–8402.

[2] Hammersland. R. (2007). ROC in assessing IDS quality. *Nor. Inf. Secur. Gjovik*, pp. 1–7.

[3] Stephenson, P., (2002). *Investigating Computer-Related Crime Handbook For Corporate Investigators*.

[4] Anif, M., Hws, S., dan Huri, M.D. (2015). Penerapan Intrusion Detection System (IDS) dengan Metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang, *J. TELE*, Vol. 13 Nomor 1, pp. 25–30.

[5] Jose, A.C. dan Malekian, R.. (2015). Smart Home Automation Security: A Literature Review. *Smart Comput. Rev.*, Vol. 5, No. 4, pp. 269–285

[6] Chadli, S., Saber, M., dan Emharraf, M. (2014). *A New Model of IDS Architecture Based on Multi-Agent Systems for MANET No. ii*.