Pemanfaatan *Iptables* Sebagai *Intrusion Detection System* (IDS) pada Linux Server

Ery Setiyawan Jullev A[#1],Bekti Maryuni Susanto[2]

Prodi Teknik Informatika[1] dan Prodi Teknik Komputer[2]

[1]ery@polije.ac.id

[2]bekti@polije.ac.id

[#] *Jurusan Teknologi Informasi Politeknik Negeri Jember*
Jl. Mastrip PO BOX 164 Jember, 68121

Abstract

Network security becomes an important thing for all industries and companies to protect the important data and information inside it. Security protection in a network is generally based on the security of data transmission created and applied to help secure a particular network. To further optimize the decision making then required a machine that is able to collaborate with the IDS database and IPS, so that a very wide range of attacks can be mapped with more optimal. One of the databases that have an existing rule is IPTABLES, this is because in IPTABLES there is a firewall function that can handle multiple types of attacks and masife. Server that will be used is server with linux operating system. While the IDS attack database used is a KDD 99 database that has been recognized as one of the database attacks are very complex. With the utilization of IPTABLES is expected server security will be monitored with more optimal. IPTABLES is usually used as one of the firewalls used on the server.

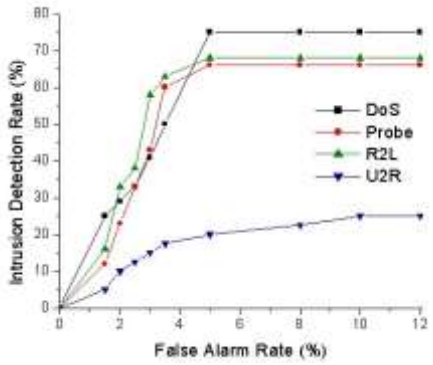
Keywords— ***Monitoring Network Security*, IDS, IP TABLES, KDD99..**

I. PENDAHULUAN

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. 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. Iptables 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 (Sondakh et al., 2014).

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) (Hammersland, 2007).



Gambar 1 Kurva ROC

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 masife.

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 system operasi linux sebagai salah satu system 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. TINJAUAN PUSTAKA

a. Cyber Crime

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

Sedangkan menurut Peter (Stephenson, 2002), 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 (Anif et al., 2015), 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 kegiatankegiatan 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 (Cyril Jose and Malekian, 2015).

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 (Chadli et al., 2014). 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 computer.

c. *Intrusion Prevention* 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 pengembangann 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 memblock 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.

1. 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.

2. 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 (Intrusion Detection System) dan IPS (Intrusion Prevention System) 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 (Intrusion Detection System) dan IPS (Intrusion Prevention System) menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS (Intrusion Detection System) dan IPS(Intrusion Prevention System) akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS).

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

a.

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 dating dari IP Publik dan bukan dari IP local.

Tabel NAT adalah tabel yang bertanggung jawab untuk melakukan Network Address Translation (NAT)..

III. TUJUAN DAN MANFAAT PENELITIAN

Tujuan dalam penelitian ini adalah Untuk Mengetahui cara kerja dari kombinasi antara IPTABLES dengan KDD 99 sebagai Intrussion Detection System, serta Mengetahui bagaimana IPTABLES mampu melakukan upaya preventif pada serangan pada jaringan komputer.

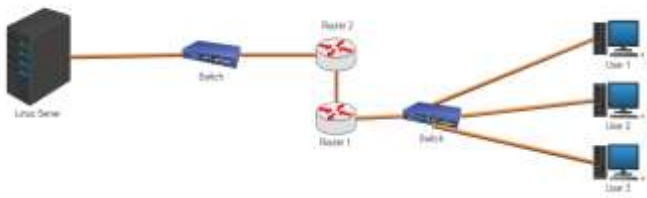
Sedangkan Manfaat Penelitian adalah Memberikan kontribusi keilmuan pada bidang Teknologi Informasi. Memberikan informasi tentang penggunaan IPTABLES dan KDD 99 sebagai salah satu metode preventif pada serangan di jaringan computer, serta sebagai panduan kajian teoritis keilmuan tentang metode keamanan jaringan komputer dengan pemanfaatan database yang telah dikembangkan.

IV. METODOLOGI PENELITIAN

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 Permainan

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 system operasi linux. Server dengan system operasi jenis ini sering digunakan baik di industry maupun di dunia edukasi. Karena sebuah perangkat yang dapat diakses secara langsung pada jaringan public 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 dimonitoring dengan lebih optimal. IPTABLES biasanya digunakan sebagai salah satu firewall yang digunakan pada server. IPtables pada system 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 Bagan 2.



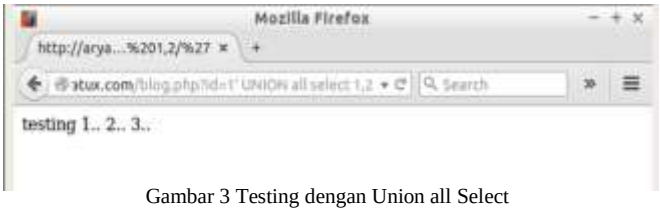
Gambar 2. Perancangan Sistem

V. HASIL DAN LUARAN YANG DICAPAI

a. Pembahasan

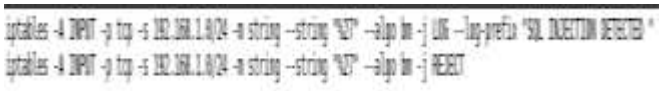
Pengujian pada penelitian ini meliputi Denial Of Service (DOS), SQL Injection, dan Port Scanning. Untuk server menggunakan Sistem Operasi Linux Ubuntu Server 14.04, sedangkan attacker menggunakan Sistem Operasi Linux Ubuntu Desktop 14.04 dan Windows 7. Pada attacker yang menggunakan Sistem Operasi Linux 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

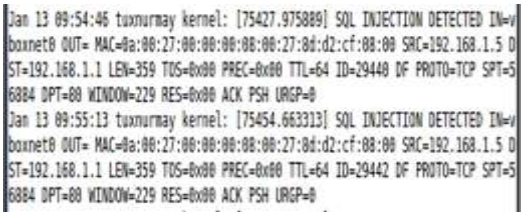
Untuk mendeteksi dan mengatasi serangan SQL Injection dengan mencegah attacker menggunakan eksploitasi pada bug SQL. Pada terminal server menggunakan perintah rule iptable seperti pada Bagan 4.



Gambar 4 Rules untuk mendeteksi dan mencegah SQL Injection

Pada baris pertama dari rules iptables gambar 4.22 digunakan untuk mendeteksi adanya serangan SQL Injection dan baris kedua digunakan untuk mengatasi serangan SQL Injection. Pada gambar 4.22 rules iptables menggunakan string %27 dikarenakan tanda kutip (quote) pada browser diencoding, 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.



Gambar 5 Mendeteksi serangan SQL Injection

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

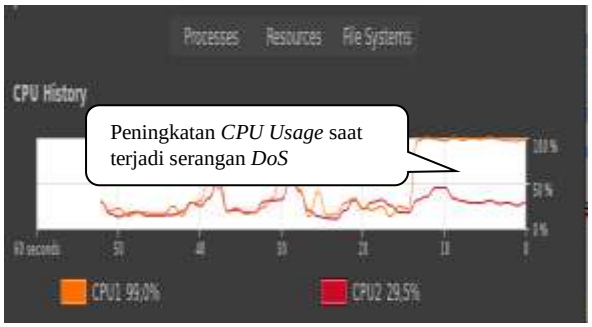
Gambar 6 Tampilan program DoS pada attacker Windows 7

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 bagan 8.

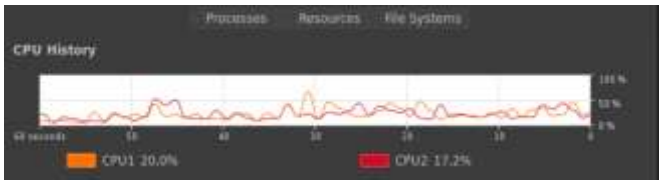


Gambar 8 Grafik CPU Usage sebelum menggunakan IPTables ketika terjadi serangan DoS

Setelah menggunakan iptables, serangan Denial of Service (DoS) akan terdeteksi pada sistem server dan serangan DoS tidak semassive 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=59200 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 (sanning) port pada komputer. Pada proyek tugas akhir ini menggunakan nmap sebagai tool untuk memindai (scanning) port. Untuk mendeteksi adanya serangan Port Scanning maka menggunakan rules pada gambar 4.28 sedangkan untuk mengatasi serangan Port Scanning dengan menggunakan rules iptables pada Bagan 11.

```
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 bagan 11 berfungsi untuk mendeteksi serangan Port Scanning. Pada rules iptables bagan 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 bloking 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=48474 PROTO=TCP SPT=62523 DPT
=1034 WINDOW=1024 RES=0x00 SYN URGP=0
```

Gambar 13 Mendeteksi serangan Port Scanning

VI. KESIMPULAN DAN SARAN

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.

DAFTAR PUSTAKA

[1] Anif, M., Hws, S. and Huri, M.D., 2015, Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang. JURNAL TELE, Volume 13 Nomor 1, 13(1), pp.25–30.

[2] [2] Chadli, S., Saber, M. and Emharraf, M., 2014, A new model of IDS architecture based on multi - agent systems for MANET. , (ii).

[3] Chitnis, S., Deshpande, N. and Shaligram, A., 2016, An investigative study for smart home security: Issues, challenges and countermeasures. Wireless Sensor Network, 8(4), pp.61–68. Available at: http://dx.doi.org/10.4236/wsn.2016.84006.

[4] [3] COMMONWEALTH OF VIRGINIA, R.O.T.J.C.O.T.A.S., 2016, States Confront the Cyber Challenge. , pp.1–4.

[5] Cyril Jose, A. and Malekian, R., 2015, Smart Home Automation Security: A Literature Review. The Smart Computing Review, 5(4), pp.269–285. Available at: http://smartcr.org/view/download.php?filename=smartcr_vol5no4p004.pdf.

[6] [5] Hammersland, R., 2007, ROC in assessing IDS quality. Norwegian Information Security, Gjovik, pp.1–7. Available at: http://rune.hammersland.net/tekst/roc.pdf.

[7] [6] Kumar, B.S. et al., 2013, Intrusion Detection System- Types and Prevention. International Journal of Computer Science and Information Technologies, 4(1), pp.77–82.

[8] Kurniawan, A., Putri, Sayyidah, N. and Hermanto, D.;, 2012, Implementasi Intrusion Prevention System (Ips) Menggunakan Snort, Ip Tables, dan Honeypot pada Router Mikrotik. Stmik Gi Mdp, (x), pp.1–12.

[9] [7] Sondakh, G., I Najoan, M.E. and Lumenta, A.S., 2014, Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat. , pp.2301–8402.

[10] Stephenson, P., 2002, I NVESTIGATING C OMPUTER -R ELATED C RIME A H ANDBOOK FOR C ORPORATE I NVESTIGATORS,