e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

IMPLEMENTASI KEAMANAN IDS/IPS DENGAN SNORT DAN IPTABLES PADA SERVER

Giovanni Tambunan [1], IGN Mantra [2]
Teknik Informatika / Fakultas Teknologi Informasi
Perbanas Institute
Jl. Perbanas, RT.16/RW.7 Kuningan, Karet Kuningan, Kecamatan Setiabudi, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12940
giovannitambunan@gmail.com1 ignmantra@gmail.com2

Abstrak. Pemanfaatan teknologi *server* pada kegiatan di kampus sangat memudahkan menyimpan data-data penting mahasiswa. Keamanan informasinya pun sangat harus diperhatikan dikarenakan data data di kampus bisa jadi penting dan di salah gunakan oleh para *hacker* di luar sana. Keamanan informasi di era modern ini sangat penting, informasi atau data data kita yang tersimpan bisa jadi sasaran para *hacker* yang ingin mencuri data kampus atau fakultas terkait. Keamanan *IDS* dan *IPS* adalah cara untuk mengamankan/memperkuat sebuah *server*. Pengamanan ditentukan memakai beberapa elemen fitur yang tersedia seperti melakukan *Snort, IPTables, SSH, Firewall* dan lainnya. Dan setelahnya dilakukan pengujian pada *server* yang ingin diberikan penguatan lebih, yang biasa disebut dengan *Penetration Testing*. Tujuan dari penelitian ini salah satunya adalah untuk merancang sebuah metode untuk menutupi celah keamanan dan memberikan keamanan untuk *server* FTI di kampus Institut Perbanas.

Kata Kunci: *Server, Penetration Testing, Snort, Ubuntu Linux, IPTables,* Teknik Informatika, Perbanas Institute Jakarta.

1 Pendahuluan

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak berhak. Komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada *host* yang tidak terhubung kemana-mana. Dengan mengendalikan *network security*, resiko tersebut dapat dikurangi. Suatu jaringan didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan didesain untuk mengontrol akses. Penyediaan *network security* adalah sebagai aksi penyeimbang antara *open access* dengan *security*. Keamanan komputer adalah tindakan pencegahan dari serangan atau pengakses jaringan yang tidak bertanggung jawab. Keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak terhubung ke mana – mana[1].

Server sebagai sarana vital untuk menyimpan *database*, aplikasi dan layanan penting sangat diperlukan sisi keamanannya. Baik dari segi infrastruktur sendiri maupun aplikasi pendukungnya. Diharapkan *server* terhindar dari hal-hal yang menggangu kinerjanya sehingga pelayanan terhadap *client* berfungsi secara maksimal. Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya[2]. Suatu serangan ke dalam *server* jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam *server* itu sendiri yang mampu mendeteksi

2 Landasan Teori

Keamanan informasi menurut G. J. Simons adalah bagaimana kita dapat mencegah penipuan *(cheating)* atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Permasalahan pokok sebenarnya dalam hal keamanan sistem informasi terletak pada

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

kelemahan dan ancaman atas sistem informasi yang pada gilirannya masalah tersebut akan berdampak kepada resiko dan pada gilirannya.

Server adalah komputer yang mendukung aplikasi dan telekomunikasi dalam jaringan, serta pembagian peralatan software, dan database di antara berbagai terminal kerja dalam jaringan[3].

Ubuntu Server merupakan sistem yang berbasis *open source* yang diterbitkan oleh *Linux* yang berbasiskan *Debian* dan didistribusikan sebagai perangkat lunak bebas. Nama *Ubuntu* berasal dari filosofi dari Afrika Selatan yang berarti "kemanusiaan kepada sesama". *Ubuntu* dirancang untuk kepentingan penggunaan pribadi, namun versi *server Ubuntu* juga tersedia, dan telah dipakai secara luas. Proyek *Ubuntu* resmi disponsori oleh *Canonical Ltd*. yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan Mark Shuttleworth. Tujuan dari distribusi *Linux Ubuntu* adalah membawa semangat yang terkandung di dalam filosofi *Ubuntu* ke dalam dunia perangkat lunak. *Ubuntu* adalah sistem operasi lengkap berbasis *Linux*, tersedia secara bebas, dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional

Keamanan komputer adalah berhubungan dengan pencegahan dini dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer[4].

Firewall adalah alat yang digunakan untuk mencegah orang luar memperoleh akses ke suatu jaringan[5]. *Firewall* merupakan bagian perangkat keamanan. *Firewall* dapat berupa program ataupun *hardware* yang dirancang khusus untuk memfilter informasi diantara jaringan publik dan jaringan privat[6]. *Firewall* memberikan keamanan pada sebuah jaringan komputer, ibarat sebuah tembok, semua aktifitas yang masuk ke dalam komputer atau sebaliknya harus melewati *firewall* sehingga keamanan komputer lebih terjamin. Berikut ini merupakan sebuah ilustrasi perlindungan *firewall* pada suatu jaringan komputer dalam melindungi *host* yang berada dibelakangnya.

Denial of Service (DOS) merupakan serangan dengan ditandai oleh suatu usaha yang eksplisit dari penyerang untuk mencegah para pemakai yang sah menggunakan jasa pelayanan jaringan. Serangan Denial of Service utamanya bertujuan melumpuhkan komputer atau jaringan[7]. Ada beberapa motif penyerang dalam melakukan Denial of Service yaitu: status sub-kultural, untuk mendapatkan akses, balas dendam, alasan politik, dan alasan ekonomi[8].

2.1 *Snort*

Snort memiliki keunggulan untuk mengetahui adanya indikasi penyusupan pada jaringan berbasis *TCP/IP* secara *real time*[9]. Jika terindikasi adanya penyusupan, *Snort* akan melakukan pencatatan atau *logging* terhadap paket-paket yang telah terdeteksi sebagai intrusi berdasarkan aturan yang telah ditetapkan. Pada implementasinya, *Snort* memiliki aturan yang telah dikonfigurasi untuk mendeteksi intrusi dalam sebuah jaringan. Terdapat sebuah *database* yang mencakup aturan-aturan yang memiliki fungsi tertentu sehingga dapat digunakan sesuai dengan kebutuhan. Setiap paket yang lalu lintas jaringan akan dianalisa dengan cara melakukan pencocokkan terhadap aturan yang telah ditetapkan. Hasilnya, *Snort* akan melakukan *logging* ke dalam *database* seperti *MySQL* maupun *file log* terhadap paket yang terindikasi sebagai sebuah intrusi.

2.1.1 Mode *Snort*

Dalam pemahaman lain, *Snort* dapat didefinisikan sebagai *single-threaded* yang artinya hanya dapat mengeksekusi satu tugas dalam satu waktu yang mana dapat berjalan pada empat mode[10]. Keempat mode operasional tersebut yaitu:

1. *Packet Sniffer Mode*, pada modus operasi ini bertugas untuk menangkap paket-paket pada lalu lintas jaringan serta menampilkan dalam bentuk aliran yang bersifat *continuous* pada sebuah layar..
2. *Packet Logger Mode,* umumnya modus operasi ini mencatat *log* dari paket-paket pada lalu lintas jaringan dan menyimpannya ke dalam disk.
3. *Detection Mode*, pada modus ini *Snort* akan menangkap paket-paket lalu lintas jaringan dan menganalisanya untuk dibandingkan dengan aturan yang sudah ditetapkan oleh Administrator.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

4. *Inline Mode*, pada *inline mode*, *Snort* memperoleh paket dari *IP table* bukan *library libpcap* dan kemudian menggunakan jenis aturan yang baru untuk membantu *IP table* mengijinkan atau menghentikan paket berdasarkan aturan *Snort*.

2.2 IPTables

IPTables merupakan sebuah tambahan dari sisi IPS yang dapat bekesinambungan dengan *snort* disetiap perangkat komputer yang diinstal dengan sistem operasi *Linux* dan resmi diluncurkan pada kernell 2.4. Fitur ini harus diaktifkan terlebih dahulu saat melakukan kompilasi kernel untuk dapat menggunakannya. IPTables merupakan fasilitas tambahan yang memiliki tugas untuk menjaga keamanan perangkat komputer anda dalam jaringan. Atau dengan kata lain, IPTables merupakan sebuah *firewall* atau program *IP filter build-in* yang disediakan oleh kernell *Linux* untuk tetap menjaga agar perangkat tetap dalam keadaan aman[11]. Fitur yang dimiliki IPTables:

1. *Connection Tracking Capability* yaitu kemampuan untuk menginspeksi dan menyaring paket data pada *TCP* dan *MAC address* serta bekerja dengan *ICMP* dan *UDP*.
2. Menyederhanakan perilaku paket-paket dalam melakukan negosiasi *built in chain (input,output, dan forward)*.
3. *Rate-Limited connection* dan *logging capability* yang bertujuan membatasi *traffic* sebagai tindakan pencegahan serangan *Syn flooding, Denial Of Services (DOS).*

2.3 *Intrusion Detection System*

Intrusion Detection System (IDS) merupakan perangkat lunak atau perangkat keras sistem yang secara otomatis melakukan proses pemantauan (*monitoring*) insiden yang terjadi dalam sistem komputer atau jaringan serta menganalisis tanda-tanda adanya masalah terhadap keamanan sistem[12]. Jika terindikasi adanya aktifitas yang mencurigakan terhadap aliran (*traffic*) paket-paket yang keluar dan masuk pada sistem, maka *IDS* akan merekam aktifitas tersebut.

2.3.1 Klasifikasi IDS

Penerapan *IDS* dapat dilakukan diberbagai tempat pada suatu jaringan di sebuah instansi atau perusahaan dengan tujuan tercapainya keamanan sistem. *IDS* sendiri dapat diklasifikasikan menjadi dua jenis yaitu *Host-based Intrusion Detection System (HIDS)* dan *Network-based Intrusion Detection System (NIDS)*[13]. Kedua jenis *IDS* adalah sebagai berikut :

1. *Host-based Instrusion Detection System* (HIDS)
   IDS tipe ini diterapkan dan beroperasi pada sebuah komputer *server* yang dianggap kritis atau rawan. Dalam pengertian lainnya, *HIDS* sesuai untuk arsitektur yang berupa *single server* yang memberikan layanan seperti *web server*, *mail server*, maupun layanan lainnya. Tujuan *HIDS* untuk memantau serta mendeteksi aliran paket-paket yang masuk dan keluar yang terindikasi berbahaya pada *host* sehingga tipe ini disebut juga *host-based IDS*.
2. *Network-based Instrusion Detection* System (NIDS)
   Pada *IDS* jenis ini diterapkan dan beroperasi dengan melihat semua lalu lintas aliran yang melewati jaringan sehingga disebut *network-based IDS*. Pada klasifikasi ini semua paket yang keluar maupun masuk pada sebuah jaringan komputer akan terlebih dahulu dianalisa dengan tujuan untuk menemukan adanya percobaan penyusupan ke dalam sistem jaringan. Hal ini efektif untuk menganalisa traffic diantara host maupun segmen jaringan lokal. Berbeda dengan *HIDS*, pada jenis ini *NIDS* akan ditempatkan pada pintu masuk jaringan (*gateway*).

2.3.2 Metode Deteksi

HIDS dan *NIDS* memiliki tujuan yang sama yaitu sebagai deteksi intrusi terhadap keamanan sistem. Meskipun memiliki perbedaan pada penerapannya, kedua *IDS* tersebut memiliki beberapa metode dalam mendeteksi adanya intrusi yaitu *Signature-based IDS* dan *Anomaly-based IDS*[10].

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

1. *Signature-based IDS*
   Pada teknik berbasis *signature*, *IDS* memeriksa lalu lintas yang sedang berlangsung yang kemudian dibandingkan dengan pola tertentu agar dapat diketahui apakah terjadi serangan. Cara kerja metode ini sama halnya seperti antivirus dimana akan dilakukan perbandingan pada lalu lintas jaringan dengan *database*. Oleh karena itu, metode ini membutuhkan pembaharuan terhadap database *IDS*.
2. *Anomaly-based IDS*
   Teknik ini memeriksa pola lalu lintas yang sedang berlangsung pada jaringan atau sistem yang dapat menunjukkan serangan. Secara umum, metode ini membandingkan lalu lintas yang sedang dipantau dengan lalu lintas normal yang biasanya terjadi. Dalam membandingkan keduanya, metode ini menggunakan teknik statistik.

2.4 *Intrusion Prevention System*

Intrusion Prevention System (*IPS*) adalah sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. *IPS* merupakan pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, *IPS* mengombinasikan teknik *firewall* dan metode *intrusion detection system* (*IDS*) dengan sangat baik. Tekno*log*i ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi. Jadi *IPS* bertindak seperti layaknya *firewall* yang akan mengizinkan atau menghalang paket data[11].Secara khusus, *IPS* memiliki empat komponen utama, yaitu:

1. *Normalisasi Traffic* : menginterpretasikan *traffic* jaringan dan melakukan analisa terhadap paket yang disusun kembali, seperti halnya fungsi block sederhana.
2. *Detection Engine* : mendeteksi *traffic* jaringan dan melakukan pattern matching terhadap tabel acuan dan respon yang sesuai.
3. *Service Scanner* : membangun suatu tabel acuan untuk mengelompokkan informasi.
4. *Traffic Shaper* : membentuk dan mengatur *traffic* jaringan.

Terdapat 2 jenis *IPS*, yaitu *Host Based Intrusion Prevention System* (*HIPS*) dan *Network Based Intrusion Prevention System* (*NIPS*).

1. *Host Intrusion Prevention System (HIPS*)
   Host-based Intrusion Prevention System (HIPS) sama seperti halnya *Host Based Intrusion Detection System (HIDS)*. Program agent *HIPS* diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. *HIPS* di *binding* dengan kernel sistem operasi dan *services* sistem operasi sehingga *HIPS* bisa memantau dan menghadang *system call* yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap *host. HIPS* juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu. Sebagai contoh *HIPS* untuk mencegah intrusion pada *webserver* misalnya. Dari sisi *security* mungkin solusi *HIPS* bisa mencegah datangnya ancaman terhadap *host.* Tetapi dari sisi *performance*, harus diperhatikan apakah *HIPS* memberikan dampak negatif terhadap *performance host*. Karena menginstall dan dinding *HIPS* pada sistem operasi mengakibatkan penggunaan *resource* komputer *host* menjadi semakin besar.
2. *Network Intrusion Prevention System (NIPS)*
   Network-based Intrusion Prevention System (NIPS) tidak melakukan pantauan secara khusus di satu *hos*t saja. Tetapi melakukan pantauan dan proteksi dalam satu jaringan secara global. *NIPS* menggabungkan fitur *IPS* dengan *firewall* dan kadang disebut sebagai *In-Line IDS* atau *Gateway Intrusion Detection System (GIDS)*. Sistem kerja *IPS* yang populer yaitu pendeteksian berbasis *signature*, pendeteksian berbasis anomali, dan *monitoring file* pada sistem operasi *host.*

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

3 Metodologi Penelitian

Metodologi penelitian berasal dari kata "*Metode*" yang artinya cara yang tepat untuk melakukan sesuatu dan "*Logos*" yang artinya ilmu atau pengetahuan. Sehingga metodologi dapat diartikan sebagai cara melakukan sesuatu dengan menggunakan pikiran secara seksama untuk mencapai suatu tujuan. Sedangkan "Penelitian" adalah suatu kegiatan untuk mencari, mencatat, merumuskan dan menganalisis hingga menyusun laporan[14]. Penelitian ini memenuhi kriteria untuk dikategorikan sebagai penelitian dengan pendekatan *Action Research*. *Action Research* Menurut Gunawan (2007), *Action Research* adalah kegiatan dan atau tindakan perbaikan sesuatu perencanaan, pelaksanaan. *Action Research* juga merupakan proses yang mencakup siklus aksi, yang mendasarkan pada refleksi, umpan balik (*feedback*), bukti (*evidence*), dan evaluasi atas aksi sebelumnya dan situasi sekarang. Penelitian tindakan ditujukan untuk memberikan andil pada pemecahan masalah praktis dalam situasi problematik yang mendesak dan pada pencapaian tujuan melalui kolaborasi patungan dalam rangka kerja etis yang saling berterima[15].

4 Hasil dan Pembahasan

Tahapan pertama dalam *Action Research* adalah melakukan analisa *server*nya. Kondisi *server* saat ini belum mendapatkan keamanan yang lanjut seperti yang diketahui *server* digunakan sebagai alat penyimpanan data - data namun belum ada perlindungan keamanan yang di terapkan, maka dilakukan konfigurasi *snort*. *Snort* berfungsi untuk proteksi mendeteksi *server* dari serangan penyerang. Kondisi ini didasari dari seringnya para *hacker*/ penyerang melakukan sebuah serangan yang menyerang *server* dengan cara mengetest dengan memanggil menggunakan *ping* maupun *nmap.*

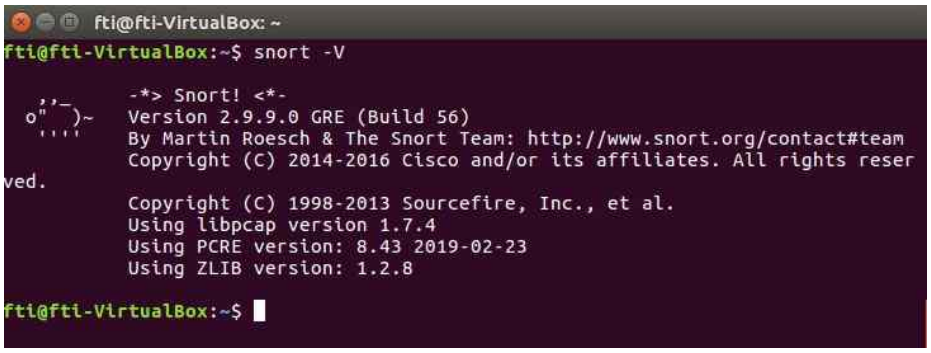
Selanjutnya dilakukan konfigurasi IPTables. *IPTable*s berfungsi untuk melakukan penyaringan atau *filter* terhadap lalulintas dalam sebuah *server*, Secara sederhana digambarkan sebagai pengatur lalulintas data. Inti dari *IPTable*s adalah semacam suatu *firewall* yang membatasi sebuah lalu lintas dari keluar dan masuk. *Firewall* sendiri adalah suatu dinding pembatas yang bertujuan melindungi suatu sistem jaringan. Kondisi ini didasari dari adanya serangan para penyerang/*hacker* yang bisa terdeteksi sebagai ancaman berbagai informasi didalamnya dan memanfaatkan celah keamanan tersebut.

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar. Salah satunya dengan mengaktifkan *IPTable*s akan memblokir *IP*. Kondisi ini didasari sebagai langkah pertahanan dan masih berkesinambungan dengan *Snort* sebagai penyempurnaan dari pertahanan di *server*nya yang dapat menahan serangan yang bisa ditembus oleh *hacker*.

Pada tahapan berikutnya dilakukan rencana tindakan (*action planning)*, pada tahapan ini penulis melakukan analisis terhadap tindakan yang akan dilakukan selanjutnya.

Lalu melakukan tindakan (*action taking*). Langkah pertama dalam melakukan tindakan adalah instalasi dan *settings virtual box* dan instalasi sistem operasi ubuntu. Setelah melakukan instalasi, berikutnya adalah konfigurasi SSH yang berfungsi untuk *remote server*, memonitoring *log file* dan memulai atau menghentikan *service*. juga dapat melakukan pengamanan enskripsi data, sehingga kemungkinan virus seperti halnya malicious tidak dapat mengakses informasi *user* dan *password*, dan juga *DNS spoofing.* Selanjutnya melakukan konfigurasi *snort* yang berfungsi untuk mendeteksi dari serangan penyerang. Penerapan ini merupakan *package* keamanan yang digunakan untuk mendeteksi dan memberitahu bahwa informasi ada yang mencoba berkomunikasi dengan *server* dan dari serangan *Ping Flood* pada *Linux*. *Snort* bekerja dengan memonitor *IP Address*, tanggal dan waktu untuk selanjutnya di rekam dan di tampilkan sebagai informasi.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

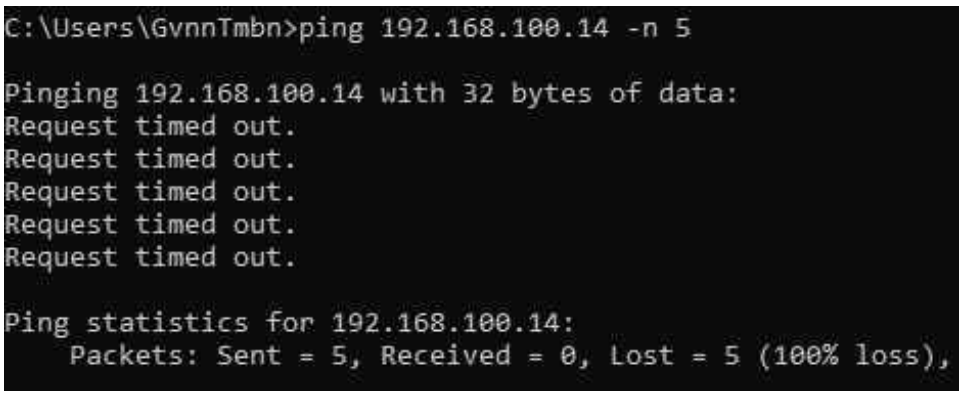


Gambar 1. Status *Snort*

Sebagai upaya tindak pencegahan, penulis menggunakan *IPTable*s untuk melakukan *filtering* terhadap *IP Source (attacker)*. Penulis mengambil salah satu *IP source* pada *list* dalam *BASE* dan mencoba melakukan *filtering* pada *IP Address* 192.168.100.5 dengan cara menginputkan *IP* yang akan di *filter* pada *IPTables.*

Gambar 2. *Rules* IPTables

Setelah melakukan *test ping flood* kembali melalui jaringan dengan mengulangnya kembali ke dalam pada target dan akses ditolak.



Gambar 3. *Test Ping Flood* Akses Ditolak

5 Kesimpulan

Setelah melakukan penanaman metode dan pengujian terhadap server yang menjadi bahan penulisan dari tugas akhir maka penulis mendapat kesimpulan sebagai berikut:

1. Dari penanaman metode tersebut terdapat kelemahan seperti server yang belum aman (secure), belum adanya penerapan pengamanan atas server tersebut maka dari itu penulis melakukan pengamanan server
2. Peningkatan Pengamanan yang di terapkan snort dapat mendeteksi jika ada serangan dan terintegrasi dengan Telegram sehingga admin tersebut mendapat notifikasi dan melakukan tindakan dengan IPS IPTables.
3. Memudahkan Admin Server untuk mengawasi aktifitas server.
4. Menghasilkan sebuah rancangan keamanan server.

e-ISBN 978-623-93343-0-7
Seminar Nasional Mahasiswa Ilmu Komputer dan Aplikasinya (SENAMIKA)
Jakarta-Indonesia, 28 Januari 2020

Referensi

[1] J. D. Howard, "An Analysis Of Security Incidents Of The Internet," 1997.
[2] R. U. Rehman, "Introduction to Intrusion Detection and Snort. In Intrusion detection systems with Snort: advanced IDS techniques using Snort, Apache, MySQL, PHP, and ACID," 2003.
[3] O'brien, "The impact of affect and social exchange on outcomes of psychological contract breach," 2011.
[4] Gollmann, "Computer Security," 1999.
[5] Ariyus and Doni, "Sistem Penyusupan pada Jaringan Komputer," *Yogyakarta Andi*, 2007. [6]
R. Rafiudin, "IP routing dan firewall dalam linux," *Yogyakarta Andi*, 2006.
[7] B. Sadono, "Tinjauan Tentang Buffer Overflow dan denial of Service Attack," *ITB Bandung*, pp. 15–16, 2003. [8]
H. Sammir, "Serangan Denial of service," *infokomputer.com*, pp. 1–2, 2003.
[9] A. Mutaqin, "Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort," *Citeseer. Int. J. Res. Comput. Sci.*, 2016.
[10] S. Rani and V. Singh, "SNORT: an open source network security tool for intrusion detection in campus network environment.," *IJCTEE*, 2012.
[11] A. Raven, "Snort 2.1 intrusion detection," 2004.
[12] A. Anitha, "Network Security using Linux Intrusion Detection System," *Citeseer. Int. J. Res. Comput. Sci.*, 2011.
[13] J. Thomas, "D-SCIDS: Distributed soft computing intrusion detection system," *Sci. Direct*, 2005.
[14] M. Priyono, "Metode penelitian kuantitatif," *Sidoarjo Zifatma Publ.*, 2016.
[15] R. N. Rapoport, "Three Dilemmas in Action Research: With Special Reference to the Tavistock Experience," 1970.