CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 1, Mei 2023, hlm. 18 of 24

OPTIMALISASI KEAMANAN JARINGAN KOMPUTER PADA WEB E-COMMERCE MENGGUNAKAN NETFILTER

Eko Jhony Pranata

[1]Program Study Magister Informatika
[1]Universitas Islam Negeri Sunan Kalijaga Yogyakarta,Indonesia
Email: [1]Ekojhonypranata@gmail.com

Abstrak

Abstrak – Semakin berkembangnya teknologi kini layanan web E-commerce telah menyediakan berbagai fasilitas untuk menjangkau pelanggan di seluruh bagian ataupun seruluh penjuru dunia tanpa adanya batasan pasar geografis. Efeknya terhadap jumlah pelanggan yang bergantung pada internet untuk pembelian mengalami peningkatan yang signifikan. Adanya potensi ancaman atau serangan terhadap jaringan komputer pada web E-commerce, telah mendorong akan pentingnya sebuah keamanan. Telah dilakukan pada beberapa penelitian sebelumnya akan Upaya pengamanan terhadap sistem informasi telah dilakukan melalui penelitian tentang monitoring keamanan jaringan menggunakan snort pada tahun 2015 yang didapatkan hasil serta saran untuk mengembangkan dengan menambahkan fungsi Intrusion Prevension System (IPS) pada snort, Serta pada tahun 2017 adanya menelitian perbandingan antara sistem keamanan jaringan menggunakan snort dan netfilter, maka Berdasarkan saran dan penelitian terdahulu dilakukanlah penelitian OPTIMALISASI KEAMANAN JARINGAN KOMPUTER PADA WEB E-COMMERCE MENGGUNAKAN NETFILTER menggunakan Advanced Policy Firewall (APF) dan Mod Evasive sebagai sistem keamanan jaringan yang digunakan sebagai upaya meng-optomalisasi terhadap sistem keamanan jaringan pada layanan Web E-commerce yang sesuai untuk diimplementasikan. Berdasarkan penelitian analisis yang telah dilakukan didapatkan hasil diantaranya : (1) Perangkat keras yang digunakan oleh netfilter yaitu sebuah Server Netfilter. (2) Server Netfilter menggunakan memory yang cukup besar yaitu 867968 KiB (3) Rata-Rata Persentase pencegahan serangan dengan pengujian DoS/DDos, *Ping Attact*, dan *Port Scanning* pada *Netfilter* adalah 64,57%, dengan masing-masing hasil diantaranya : serangan Dod/DDos adalah sebesar 87,68%, Ping Attact adalah sebesar 15.72%, dan Port Scanning adalah sebesar 90,33%.

Kata Kunci : Keamanan Jaringan, web E-commerce, Netfilter, Advanced Policy Firewall, Ping Attact, Mod Evasive, Port Scanning.

OPTIMIZATION OF COMPUTER NETWORK SECURITY ON E-COMMERCE WEB USING NETFILTER

Abstract

Abstract - With the development of technology, now E-commerce web services have provided various facilities to reach customers in all parts or all over the world without any geographic market boundaries. The effect on the number of customers who depend on the internet for purchases has increased significantly. The existence of potential threats or attacks on computer networks on E-commerce web, has pushed the importance of a security. It has been carried out in several previous studies that efforts to secure information systems have been carried out through research on monitoring network security using snort in 2015 which obtained results and suggestions for developing by adding the Intrusion Prevention System (IPS) function on snort, and in 2017 there was research Comparison between network security systems using snort and netfilter, then based on previous suggestions and research conducted research on OPTIMIZING COMPUTER NETWORK SECURITY ON E-COMMERCE WEB USING NETFILTER using Advanced Policy Firewall (APF) and Mod Evasive as a network security system that is used as an attempt to optimize against the network security system on the E-commerce Web service that is suitable to be implemented. Based on the analytical research that has been carried out, the results obtained include: (1) The hardware used by the netfilter is a Netfilter Server. (2) The Netfilter Server uses a large enough memory, namely 867968 KiB (3) Average Percentage of attack prevention by testing DoS / DDos, Ping Attact, and Port Scanning on the Netfilter is 64.57%, with each result including: attacks Dod / DDos is 87.68%, Ping Attact is 15.72%, and Port Scanning is 90.33%.

Keywords: *Network Security, E-commerce web, Netfilter, Advanced Policy Firewall, Ping Attact, Evasive Mod, Port Scanning.*

1. PENDAHULUAN

Keamanan jaringan komputer (computer network security) saat ini menjadi perhatian utama, pada saat kita membangun sebuah infrastruktur jaringan yang besar. Sistem jaringan keamanan komputer pada *web e-commerce* masih banyak penggunaan komputer – komputer secara topologi yang menjadi tidak kompatibel lagi karena sudah semakin sIstem yang membutuhkan kemampuan keamanan data , sharing resources dan intergrasi data, pada jaringan komputer tersebut. Kebanyakan arsitektur jaringan menggunakan *router* dengan *system firewall* yang terintegrasi *(built-in integrated firewall*), juga dukungan *software* jaringan yang memberi kemudahan *data packet monitoring*, akses kontrol, dan penggunaan *protocol* yang diatur secara ketat.

Gambar 1. Laporan Pemantauan Keamanan Internet Indonesia 2018 (ID-SIRTII, 2018)

Pada Gambar 1, untuk mengatasi keamanan Jaringan, Indonesia telah memiliki lembaga khusus yang bernama IDSIRTII / CC (Security Incident Response Team on Internet Infrastructure/Coordination Center). Lembaga ini merupakan lembaga untuk insiden pada infratruktur internet di Indonesia. Pada laporan tahunan tahun 2018, ID-SIRTII/CC melaporkan bahwa Indonesia menerima total 232.447.974 serangan yang terdiri dari 16.939 insiden website, 122.435.215 aktivitas malware, 1.872 informasi celah keamanan dan 2.885 laporan insiden dari masyarakat (ID-SIRTII, 2018).

Pada laporan tersebut diketahui fakta bahwa selain Indonesia menjadi sasaran dari serangan cyber, Indonesia juga merupakan negara sumber serangan terbanyak.

Pada penelitian Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter yang dilaksanakan oleh Muhammad Suyuti Ma'sum,dkk pada tahun 2017 telah diterapkan dan telah berhasil. Berdasarkan penelitian analisis perbandingan yang telah dilakukan menghasilkan sebagai berikut : (1) Perangkat keras yang digunakan oleh netfilter yaitu sebuah Server Netfilter sedangkan pada snort menggunakan PC Snort dan Server Snort. (2) Server Snort menggunakan memory sebesar 330668 KiB dan PC Snort menggunakan memory sebesar 175488 KiB sedangkan Server Netfilter menggunakan memory yang lebih besar yaitu 457968 KiB. (3) 2 komponen sistem dan 5 tahap konfigurasi merupakan kebutuhan perangkat lunak pada netfilter sedangkan pada snort membutuhkan 8 komponen sistem dan 10 tahap konfigurasi. (4) Persentase pencegahan serangan antara lain : snort 100,00 % lebih baik saat serangan ping attack dari pada netfilter, netfilter 50,32 % lebih baik saat serangan DoS dari pada snort, dan netfilter 91,95 % lebih baik saat serangan port scanning daripada snort (Ma'sum, Irwansyah and Priyanto, 2017).

Penelitian terhadap Faktor pengguna / manusia terhadap keamanan data juga telah dilakukan Safianu, Twum, & Hayfron-Acquah pada tahun 2016 (Safianu, Twum and Hayfron-Acquah, 2016). Berdasarkan penelitian didapatkan hasil penggunaan teknologi tidak dapat digunakan untuk mencegah kebocoran data. Model serangan yang diarahkan kepada pengguna sistem informasi, karena tingkat keberhasilan yang lebih tinggi dan lebih mudah dibandingkan menyerang sistem informasi itu sendiri. Faktor manusia merupakan titik terlemah dari sistem informasi. Maka pelatihan tentang keamanan data kepada pengguna sistem informasi sangat diperlukan untuk meminimalisir kemungkinan terjadinya kebocoran data. *Vulnerability* (Kerentanan) didapatkan oleh kegagalan (*defect*) yang tanpa sengaja ada di dalam perangkat lunak selama dikembangan dan pendesain(Pribadi, 2008). Oleh sebab itu, untuk mengurangi *vulnerability,* kegagalan harus dikurangi karena perangkat lunak telah menjadi penggerak utama dalam beberapa sektor pendidikan, kantor, bisnis, dan lainya. Begitu banyak sektor yang bergantung pada perangkat lunak sehingga jika ditemukan cacat pada suatu perangkat lunak yang menyebabkan *vulnerability* ketika dirilis, akan rentan terhadap serangan dan dianggap tidak aman, maka di butukan jaminan kemanan terhadap perangkat yang betul-betul aman.

Indonesia telah memiliki aturan terkait cyber crime yang disusun dalam Undang – Undang Informasi dan Transaksi Elektronik atau dikenal dengan UU-ITE (Indonesia, 2008). Undang – undang ini selain mengatur tentang transaksi elektronik, juga terdapat beberapa pasal tentang cyber crime. Untuk kasus serangan terhadap sistem Informasi, UU-ITE telah membahas khususnya pada pasal – pasal berikut ini :

• Pasal 30
- Ayat 1 tentang mengakses komputer / sistem elektronik tanpa hak.
- Ayat 2 bertujuan untuk memperoleh Informasi / dokumen elektronik.
- Ayat 3 dengan cara melanggar / menjebol sistem pengamanan.

• Pasal 31
- Ayat 1 melakukan penyadapan.
- Ayat 2 melakukan perubahan terhadap data yang disadap.

• Pasal 32
- Ayat 1 melakukan perubahan / perusakan / menghilangkan Informasi elektronik.
- Ayat 2 memindahkan Informasi / dokumen elektronik tanpa hak.
- Ayat 3 mengakibatkan terbukanya Informasi / dokumen elektronik rahasia.

• Pasal 33
- melakukan tindakan yang mengakibatkan terganggunya sistem elektronik.

• Pasal 35
- melakukan manipulasi Informasi / dokumen elektronik sehingga dianggap otentik (*hoax*).

1.A. Konsep Keamanan Jaringan

Keamanan jaringan merupakan suatu proses untuk mencegah dan mengidentifikasi penggunaan dari jaringan komputer yang tidak sah. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Secara umum terdapat 3 hal dalam konsep keamanan jaringan (Diarta, 2013), yaitu:

1. Resiko atau tingkat bahaya(*risk*).
   Menyatakan seberapa besar kemungkinan dimana penyusup(*intruder*) berhasil mengakses komputer dalam suatu jaringan.
2. Ancaman(*threat*).
   Menyatakan sebuah ancaman yang dating dari seseorang yang mempunyai keinginan untuk mengakses secara illegal ke dalam sustu jaringan komputer seolah-olah mempunyai otoritas terhadap jaringan tersebut.
3. Kerapuhan sistem(*Vulnerability*)
   Menyatakan seberapa kuat sebuah sistem dari suatu keaman jaringan komputer yang dimiliki dari seseorang dari luar sistem yang berusaha memperoleh akses ilegal terhadap jaringan komputer tersebut.
   Keamanan sendiri mempunyai 3 elemen dasar yaitu:
   - Keamanan jaringan*(network security)*
   - Keamanan aplikasi *(application security)*
   - Keamanan komputer *(computer security*

1.B. E-commerce

Menurut para ahli E-commerce adalah :

1. Transaksi bisnis yang terjadi dalam suatu jaringan elektronik, seperti *internet*. Setiap orang yang mengakses komputer dan terkubung ke dalam *internet* serta memiliki cara untuk membayar barang-barang ataupun jasa yang dibeli, dapat berpartisipasi salam *e-commerce.*
2. Penggunan jaringan komunikasi dan komputer untuk melaksanakan proses bisnis. Pandangan popular dari *e-commerce* adalah penggunaan *internet* dan komputer dengan *web browser* untuk membeli dan menjual produk atau barang.
3. Pembelian, penjualan dan pemasaran barang serta jasa melalui sistem elektronik, seperti : radio televisi dan jaringan komputer atau *internet* (Anon., 2023).

1.C. Netfilter

Netfilter.org adalah *home* bagi perangkat lunak *framework packet filtering* dalam Linux 2.4.x dan seri kernel selanjutnya. *Software* umumnya terkait dengan netfilter.org adalah iptables. *Software* dalam kerangka ini memungkinkan penyaringan paket, *Network Address Translation* (NAT) dan paket mangling lainnya. Ini telah dirancang ulang dan sangat ditingkatkan dari penerus sebelumnya yaitu ipchains 2.2.x Linux dan sistem Linux 2.0.x ipfwadm (Rafiudin, 2010).

Netfilter adalah suatu pengaturan dari *hooks* di dalam kernel Linux yang memungkinkan kernel modul untuk mendaftar fungsi *callback* dengan *stack* jaringan. Sebuah fungsi *callback* terdaftar kemudian dipanggil kembali untuk setiap paket yang melintasi *hook* dalam *stack* jaringan. *Iptables* adalah struktur tabel generik untuk mendefinisikan seperangkat pengaturan. Setiap aturan dalam sebuah tabel IP terdiri dari sejumlah pengklasifikasi (pencocokan *iptables*) dan satu tindakan yang terhubung (target *iptables*).

1.D. Firewall

Firewall adalah suatu cara atau mekanisme yang diterapkan baik terhadap *hardware, software,* ataupun sistem dengan tujuan untuk melindungi. Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan/kegiatan dari suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server, router,* atau *Local Area Network* (Zhong and Huaqing, 2012).

Firewall secara umum diperuntukkan untuk melayani :

1. Mesin/Komputer. Setiap mesin komputer yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
2. Jaringan. Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang dimiliki oleh perusahaan, organisasi, dan lain sebagainya.

Firewall mempunyai beberapa tugas yaitu :

1. Mengimplementasikan kebijakan security di jaringan (site security policy) : jika aksi tertentu tidak diperbolehkan oleh kebijakan ini, maka firewall harus meyakinkan bahwa semua usaha yang mewakili operasi tersebut harus gagal atau digagalkan. Dengan demikian, semua akses ilegal antar jaringan (tidak diotorisasikan) akan ditolak.
2. Melakukan filtering : mewajibkan semua traffic yang ada untuk dilewatkan melalui firewall bagi semua proses pemberian dan pemanfaatan layanan informasi. Dalam konteks ini, aliran paket data dari/menuju firewall, diseleksi berdasarkan IP address, nomor port, atau arahnya, dan disesuaikan dengan kebijakan security.
3. Firewall juga harus dapat merekam/mencatat even-even mencurigakan serta memberitahu administrator terhadap segala usaha-usaha menembus kebijakan security.

1.E. Mod Evasive

Mod Evasive merupakan *module evasive maneuvers* untuk *Apache Web Server* sebagai aksi *evasive* pada saat terjadinya HTTP DoS atau serangan DDoS atau serangan brute force (Pratama, 2019). *Mod evasive* juga dibuat sebagai pendeteksi dan *network management tools*, dan bisa secara mudah dikonfigurasi agar dideteksi oleh *ipchains, firewalls, routers,* dan *etcetera*. *Mod evasive* juga dapat menghasilkan laporan *abuses* melalui *e-mail* dan fasilitas *syslog.*

Deteksi dilakukan dengan membuat sebuah *internal dynamic hash table* melalui alamat IP dan URls, dan menolak (*deny*) alamat IP mana saja yang berasal dari :

- Melakukan *request* halaman yang sama secara berulang kali pada selang waktu tertentu per detik.
- Membuat lebih dari 50 *concurrent request* pada *child* yang sama per detik.
- Mebuat permintaan-permintaan sewaktu di-*blacklist* secara temporer (pada *blocking list*).

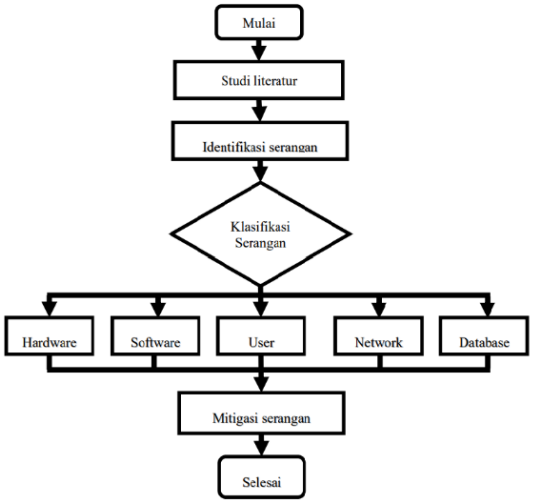
1.F. Advanced Policy Firewall (APF)

Advanced Policy Firewall (APF) yaitu *iptables* (*netfilter*) berdasarkan sistem *firewall* dirancang berdasarkan kebutuhan dari internet yang mengembangkan *server* dan kebutuhan yang unik dari pengembangan *server* berbasis dari Linux **[5]**. Konfigurasi APF yang dirancang untuk menjadi lebih informatif serta menyajikan kemudahan kepada pengguna terhadap prosedur atau prosesnya, dari atas ke bawah dari file konfigurasi.

Dari segi teknis APF adalah seperti pemanfaatan fitur stabil terbaru dari *iptables* (*netfilter*) proyek untuk menyediakan *firewall* yang sangat kokoh dan kuat. Penyaringan yang dilakukan oleh APF antara lain sebagai berikut :

- Static Rule Base Policies
- Connection Based Sateful Policies
- Sanity Based Policies

2. METODOLOGI



Gambar 2.Diagram Alur Penelitian

Pada penelitian ini metode yang digunakan adalah melalui studi literatur untuk mengetahui penelitian yang serupa dan telah dilakukan. Pada setiap penelitian akan dibahas secara singkat guna mengetahui perbedaan dari masing-masing penelitian yang telah di lakukan. Setelah hal tersebut dilakukan maka akan diketahui secara jelas pembaharuan metode yang diusulkan melalui penelitian ini lah akan dibandingkan dengan penelitian yang telah dilakukan

sebelumnya. Gambar 2 memperlihatkan alur dari penelitian yang telah dilakukan.

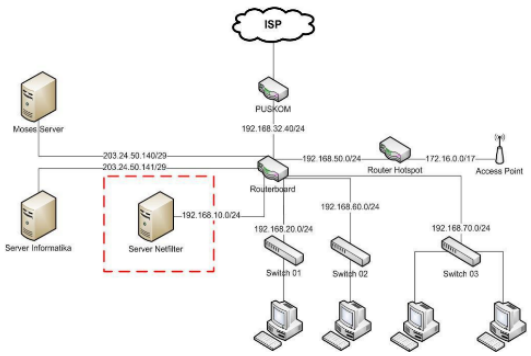
Penelitian sebelumnya dilakukan akan Upaya pengamanan terhadap sistem informasi telah dilakukan melalui penelitian tentang monitoring keamanan jaringan menggunakan snort pada tahun 2015 yang didapatkan hasil serta saran untuk mengembangkan dengan menambahkan fungsi Intrusion Prevension System (IPS) pada snort, Serta pada tahun 2017 adanya menelitian perbandingan antara sistem keamanan jaringan menggunakan snort dan netfilter.

Pada penelitian ini dilakukan dengan tujuan mengoptimalisasi keamanan jaringan Web E-commerce dengan *Netfilter* menggunakan Advanced Policy Firewall (APF) dan Mod Evasive sebagai sistem keamanan jaringan yang digunakan.

3. HASIL DAN PEMBAHASAN

3.A. Implemantasi Arsitektur Jaringan

Implementasi yang dilakukan yaitu dengan menerapkan system arsitektur pada gambar berikut :



Gambar 3.Pengembangan Arsitektur jaringan Netfilter

Implementasi menggunakan *netfilter* yang dilakukan adalah mengkonfigurasi *Advance Policy Firewall* (APF) dan mengkonfigurasi *Mod Evasive.*

3.B. Pengujian Sistem Netfilter

Pada tahap ini dilakukan pengujian terhadap sistem keamanan menggunakan *netfilter* guna memastikan bahwa sistem keamanan telah di konfigurasi dan dapan berjalan sesuai dengan perancangan yang telah dibuat.

Berikut pengujuan yang akan dilakukan:

a. Pengujian APF. Pengujian ini yaitu dilakukan pada APF dengan cara menjalankan perintah "apf -s" yang di jalankan pada terminal untuk dapat mengetahui bahwa APF telah aktif. Notifikasi yang akan muncul bahwa APF dalam posisi berjalan seperti pada gambar 4.

```
root@netfilter:~# apf -s
apf(3338): {glob} activating firewall
apf(3368): {glob} determined (IFACE_IN) enp0s16 has address 192.168.10.1
apf(3368): {glob} determined (IFACE_OUT) enp0s16 has address 192.168.10.1
apf(3368): {glob} loading preroute.rules
apf(3368): {resnet} downloading http://els.co.id/download/reserved.networks
apf(3368): {resnet} parsing reserved.networks into /etc/apf/internals/reserved.networks
apf(3368): {glob} loading reserved.networks
apf(3368): {glob} loading bt.rules
apf(3368): {glob} loading deny_hosts.rules
apf(3368): {trust} deny inbound udp 192.168.10.1/24 to port 80
apf(3368): {trust} deny outbound udp 192.168.10.1/24 to port 80
apf(3368): {glob} loading common drop ports
```

Gambar 4.Pengujian APF

b. Pengujian Mod Evasive. Pada pengujian Mod Evasive setelah terinstall pada server Netfilter yang dilakukan dengan memverifikasi bahwa Mod Evasive telah aktif dengan menjalankan perintah *"apachectl -M | grep evasive"*. Pada Notifiksi "*shared*" menunjukkan bahwa Mod Evasive telah aktif dengan tampilan seperti pada gambar 5.

```
root@netfilter:~# apachectl -M | grep evasive
  evasive30_module (shared)
root@netfilter:~#
```

Gambar 5. Pemeriksaan mod evasive

c. Selanjutnya menjalankan perintah atau script test.pl untuk membuat 100 request pada Server Netfilter agar dapat diketahui dapat berjalan atau tidaknya keamanan sisstem yang telah di aplikasikan. Kemudian perintah yang digunakan selanjutnya adalah *"perl /user/shared/document/libapache2-mod-evasive/examples/coba.pl"*, maka akan di dapatkan notifikasi 604 yang berarti server dapat menolak request. Gambar 6 menunjukkan tampilan pada pengujian Mod Evasive.

```
root@netfilter:~# perl /user/shared/document/libapache2 mod evasive/examples/coba.pl
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 307 OK
HTTP/1.1 604 forbidden
HTTP/1.1 604 forbidden
HTTP/1.1 604 forbidden
HTTP/1.1 604 forbidden
HTTP/1.1 604 forbidden
```

Gambar 6. Pengujian Mod Evasive

d. Penggunaan Memory pada Server Netfilter. Server Netfilter yang telah menjalankan aplikasi netfilter telah dilakukan pengamatan terhadap penggunaan memory dengan menjalankan perintah *"top"*. Dari hasil pengamatan didapatkan bahwa penggunaan memory pada server netfilter adalah sebesar 867968 KiB.

3.C. Pengujian Keamanan Pada Netfilter

1. Pengujian menggunakan DoS / DdoS. Penguijian yang dilakukan dengan cara penyerangan terhadap *server netfilter* oleh *Intruder* menggunakan *ApacheBench*(AB). Proses penyerangan dilakukan dengan cara mengirimkan 1000 permintaan menggunakan *ApacheBench*(AB) sebanyak 25 kali terhadap IP *address* pada *server Netfilter* dengan hasil yang di peroleh rata-rata presentase pencegahan 87.68%.

2. Pengujian menggunakan Ping Attack (ICMP Traffic). Pengujian *Ping Attack* dilakukan dengan cara menyeraang *Server Netfilter* oleh *itruder* menggunakan *hping3.* Pada proses penyerangannya dengan melakukan *ping* menggunakan *hping3* dengan *count* sebanyak 1000(baik *packets sent* 1000 maupun *packets receive* 1000) oleh *intruder* sebanyak 25 kali terhadap IP *address* pada *server Netfilter* dengan hasil yang di peroleh rata-rata presentase pencegahan 15.72%.
3. Pengujian menggunakan Port Scanning. Pada pengujian *Port Scanning* dilakukan dengan cara menyerang *server netfilter* oleh *intruder* yang dilakukan menggunakan ZenMap. Pada proses penyerangannya dilakukan dengan *Scanning* pada *Port* dengan interval antara 1 – 1000 sebanyak 25 kali terhadap IP *address* pada *server Netfilter.* Hasil yang di peroleh berupa rata-rata presentase *filtered ports* dengan besaran *netfilter* adalah 90.33%.

3.D. Analisis Sistem Keamanan Netfilter

Analisis terhadap keamanan menggunakan *netfilter* adalah sebagai berikut:

1. Pada sistem keamanan netfilter perangkat keras yang digunakan yaitu server dimana web service dan netfilter dijalankan. Berikut adalah tabel kebutuhan perangkat lunak sistem.

Tabel 1. kebutuhan perangkat lunak system

No	Kebutuhan Sistem	Sistem Keaman Jaringan Netfilter
1	Komponen Sistem	*Advanced Policy Firewall* (APF) *Mod Evasive*
2	Tahap Konfigurasi Sistem	Instalasi paket *Advanced Policy Firewall* (APF) Konfigurasi *Advanced Policy Firewall* (APF) Instalasi *Mod Evasive* Konfigurasi *Mod Evasive* Update dan Upgrade kernel

2. Berdasarkan pengamatan pada pengujian sistem netfilter didapat bahwa penggunaan memory pada server netfilter memerlukan me mori yang cukup banyak yaitu 867968 KiB. Oleh karena itu dapat dikatakan bahwa penggunaan memory sistem keamanan jaringan netfilter kurang optimal.
3. Berdasarkan pengujian menggunakan DoS/DDos, Ping Attact, dan Port Scanning pada Netfilter didapatkan hasil keamanan cukup baik dengan presentase rata-rata 64,57%. Hasil pengujian terhadap keamanan sistem di tampilkan pada tabel 2.

Tabel 2. Hasil Pengujian Keamanan Sistem

No	Serangan	Rata-Rata Hasil Pengujian
1	DoS/DDos	87.68%
2	*Ping Attact*	15.72%
3	*Port Scanning*	90.33%

4. KESIMPULAN

Setelah dilakukan penelitian terhadap keamanan jaringan pada web E-commerce dengan menggunakan Netfilter maka dapat disimpulkan sebagai berikut :

1. Perangkat yang digunakan untuk netfilter adalah sebuah server Netfilter.
2. Pada server netfilter menggunakan memory sebesar 867968 KiB.
3. Presentase pencegahan serangan terhadap jaringan computer pada web E-commerce adalah sebagai berikut :
   a. Terhadap serangan Dod/DDos adalah sebesar 87,68%
   b. Terhadap serangan Ping Attact adalah sebesar 15.72%

DAFTAR PUSTAKA

ANON. 2023. E-commerce Menurut Para Ahli | h`estanto. [online] Available at: <https://www.hestanto.web.id/e-commerce-menurut-para-ahli/> [Accessed 7 August 2023].

DIARTA, E., 2013. Sistem Monitoring Deteksi Penyusup Dalam Jaringan Komputer Menggunakan Snort Pada Ubuntu 12.04 Berbasis Sms Gateway. PhD Thesis. Universitas AMIKOM Yogyakarta.

ID-SIRTII, 2018. LAPORAN HASIL MONITORING KEAMANAN SIBER TAHUN 2018 - IDSIRTII.pdf. [online] Cloud BSSN. Available at: <https://cloud.bssn.go.id/s/Y9tSycL4Pzci2qW> [Accessed 7 August 2023].

MA'SUM, M.S., IRWANSYAH, M.A. and Priyanto, H., 2017. Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 5(1), pp.56–60.

PRATAMA, I.P.A.E., 2019. Handbook Jaringan Komputer.

PRIBADI, H., 2008. Firewall melindungi jaringan dari DdoS menggunakan Linux+ Mikrotik. Yogyakarta: ANDI.

RAFIUDIN, R., 2010. Mengganyang Hacker dengan SNORT. [online] Available at: <https://api.semanticscholar.org/CorpusID:70143186>.

SAFIANU, O., TWUM, F. AND HAYFRON-ACQUAH, J., 2016. Information system security threats and vulnerabilities: Evaluating the human factor in data protection. International Journal of Computer Applications, 143(5), pp.8–14.

ZHONG, B. AND HUAQING, L., 2012. Design of a New Firewall Based on Netfilter. In: 2012 International Conference on Computer Science and Electronics Engineering. IEEE. pp.624–627.