AITI: Jurnal Teknologi Informasi, Volume 17 No. 2 Agustus 2020, 143-158
ISSN 1693-8348 E-ISSN 2615-7128

JURNAL TEKNOLOGI INFORMASI

Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT

Winrou Wesley Purba[1], Rissal Efendi[2]
[1,2]Fakultas Teknologi Informasi Universitas Kristen Satya Wacana
Jl. Dr. O. Notohamidjojo 1-10, Salatiga 50711, Indonesia
Email : [1]672016259@student.uksw.edu, [2]rissal.efendi@uksw.edu

Riwayat artikel:
Recieved: 02-08-2020 Revised: 23-02-2021 Accepted: 23-02-2021

Abstract

PT. Promanufacture Indonesia is a company that needs the Internet network to be able to process the data of members, goods, CCTV and others. All files and data of members, goods, CCTV and others will be stored in a server. The Server at PT. Promanufacture Indonesia relies only on firewall systems. By using the firewall alone network security system will not be guaranteed, but with SNORT, the computer safety system will be more maintained by the warnings that will be given by the SNORT. SNORT is a piece of software that will give you a warning when intrusion occurs into your computer system. The purpose of this research is to design and analyze computer security system in PT. Promanufacture Indonesia by using SNORT software. The results of this research can be used by the network manager of PT. Promanufacture Indonesia to maintain the security system of computer networks in the company.

Keywords: *SNORT, Network Security, System Firewall*

Abstrak

PT. Promanufacture Indonesia merupakan sebuah perusahaan yang memerlukan adanya jaringan internet agar dapat mengolah data anggota, barang, CCTV dan lain-lain. Semua file dan data anggota, barang, CCTV dan lain-lain akan disimpan di dalam sebuah *server*. *Server* di PT. Promanufacture Indonesia hanya mengandalkan sistem *firewall* saja. Dengan menggunakan *firewall* saja sistem keamanan jaringan tidak akan terjamin keamanannya. Maka diperlukan sebuah sistem untuk menjaga keamanan jaringan tersebut, yaitu *SNORT*. *SNORT* merupakan perangkat lunak yang akan memberikan peringatan ketika terjadi penyusupan kedalam sistem komputer. Tujuan dari penelitian ini adalah merancang dan menganalisa sistem keamanan komputer di PT. Promanufacture Indonesia dengan menggunakan perangkat lunak *SNORT*. Hasil dari penelitian ini dapat digunakan oleh pengelola jaringan PT. Promanufacture Indonesia untuk menjaga sistem keamanan jaringan komputer pada perusahaan tersebut.

Kata kunci: *SNORT*, Keamanan Jaringan, Sistem *Firewall*

Pendahuluan

Pada saat ini perkembangan teknologi sangatlah pesat apalagi dengan didukungnya fasilitas internet yang sangat mumpuni. Namun disamping itu semua pasti selalu ada kerugian yang didapat oleh pengguna internet tersebut. Seperti serangan dari pihak-pihak yang tidak bertanggung jawab atau sering disebut dengan *hacker.* Oleh karena itu seorang *administrator* jaringan harus memastikan bahwa sistem jaringan komputer sebuah perusahaan harus aman dari serangan *hacker*. Ada banyak jenis serangan yang mampu dilakukan oleh *hacker* agar mampu masuk ke sistem komputer yang dituju, tapi jenis serangan *Port Scanning* dan DOS (*Denial of Service*) merupakan jenis serangan yang sering digunakan oleh *hacker*. *Port* Scanning merupakan sebuah serangan yang dilakukan untuk mendeteksi *port* yang terbuka pada sistem jaringan komputer, dari hasil *port scanning* akan didapat *port-port* yang terbuka, *Port* tersebut yang akan menjadi celah untuk melakukan penyerangan lebih lanjut. Sedangkan DOS (*Denial of Service*) adalah sebuah serangan pada jaringan komputer yang beroperasi dengan cara mengirimkan *request* ke *server* secara terus-menerus agar membuat *server* tersebut menjadi sibuk dan *server* tidak bisa mengatasi *request* yang telah diterima dan membuat *server* tersebut menjadi rusak.

Penelitian ini dilakukan di perusahaan PT. Promanufacture Indonesia untuk membantu kinerja perusahaan tersebut. PT. Promanufacture Indonesia merupakan sebuah perusahaan yang aktivitasnya didukung oleh jaringan internet, mulai dari mengolah data yang ada seperti data anggota, barang, CCTV dan lain-lain. Pengelola jaringan PT. Promanufacture Indonesia selama ini membangun sistem keamanan jaringan dengan menerapkan sistem *firewall* pada tiap unit *server* di jaringannya.

Pada jaringan lokal PT. Promanufacture Indonesia menggunakan kelas subnet /16, dengan jumlah maksimal 16.777.214 host, namun saat ini baru digunakan 857 host, baik untuk komputer maupun perangkat aktif lainnya. Sistem Operasi yang digunakan pada PT. Promanufacture Indonesia adalah Microsoft Windows XP, Microsoft Windows 7, Windows 10, Linux Ubuntu, Linux Xubuntu.

Dengan adanya sistem keamanan *firewall*, sistem jaringan komputer telah banyak membantu *administrator* untuk mengamankan data perusahaan, tapi dengan seiring berjalannya waktu, semakin lama perkembangan teknologi semakin meningkat, sistem keamanan *firewall* belum mampu menjamin keamanan sistem komputer sepenuhnya. Sehingga perusahaan PT. Promanufacture Indonesia memiliki masalah pada sistem jaringan komputer karena hanya mengandalkan sistem *firewall* saja.

Sistem keamanan *firewall* dirancang untuk mengawasi paket yang keluar dan masuk dari jaringan, sehingga paket yang mencurigakan akan langsung dihentikan tanpa memisahkan apakah paket tersebut aman atau tidak, akibatnya

administrator sering sekali tertipu oleh serangan yang tidak dapat diklasifikasikan. Beberapa kasus yang terjadi pada perusahaan PT. Promanufacture Indonesia diantaranya pada bulan September 2019 sebuah PC dengan sistem operasi Windows XP terkena virus *ransomware* yang mengunci data penting yang ada di PC tersebut. Adanya virus *ransomware* diketahui melalui anti virus *Avast.* Kasus lain terjadi pada bulan Januari 2019 yaitu adanya sebuah email yang masuk ke perusahaan yang berisi virus *Worm* yang ingin mencuri data perusahaan.

Oleh karena itu, keamanan jaringan *firewall* saja tidak cukup untuk melindungi sistem jaringan komputer. Dibutuhkan keamanan yang dapat menjamin agar dapat meminimalisir ataupun bahkan menghilangkan kerugian yang disebabkan oleh serangan keamanan jaringan tersebut yaitu menggunakan *SNORT*. *SNORT* dapat meminimalisir serangan-serangan yang terjadi di dalam sistem jaringan komputer dengan cara memberikan *allert* atau peringatan kepada *administrator* jika ada kegiatan yang mencurigakan.

Kajian Pustaka

Banyak penelitian tentang keamanan jaringan yang telah dilakukan. Wijanarko[1] menggunakan SNORT untuk deteksi intrusi dari external network. Dalam rancangannya, Wijanarko menggunakan SMS gateway yang digunakan untuk mengirimkan notifikasi kepada administrator jika terjadi serangan. Sudradjat[2] menggabungkan Firewall dan SNORT untuk mendeteksi dan mencegah penyusup pada jaringan komputer.

Jaringan komputer merupakan kumpulan dari beberapa komputer yang berjumlah banyak yang terpisah-pisah namun dapat saling terkoneksi atau saling terhubung dalam melaksanakan tugasnya. Contohnya, seperti dua buah komputer dapat dikatakan saling terhubung apabila keduanya dapat saling berbagi data, bertukar informasi, program-program, dan sebagainya. Contoh lain dari jaringan komputer adalah LAN (*Local Area Network*), MAN (*Metropolitan Area Network*), WAN (*Wide Area Network*). Jaringan komputer dapat dihubungkan melalui berbagai kabel, seperti kabel tembaga, kabel *coaxial*, kabel *twisted pair*, kabel serat optik dan berbagai teknologi *wireless*[3].

IDS (*Intrution Detection System*) merupakansebuah perangkat yang dapat melakukan pengawasan secara otomatis terhadap lalu lintas jaringan yang mencurigakan[7]. Jika terjadi hal yang tidak lazim atau hal yang mencurigakan, maka IDS akan memberikan informasi kepada sistem dan *administrator* jaringan. Ada dua bentuk dasar IDS yang sering digunakan yaitu: NIDS dan HIDS.

NIDS (*Network - based Intrusion Detection System*) merupakan sebuah perangkat lunak yang bekerja secara otomatis untuk memantau suatu paket data yang masuk ke dalam sistem jaringan. Semua paket data yang berjalan pada sistem jaringan, akan dianalisis untuk melihat apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. Jika ada kecocokan dengan *rules* yang telah dibuat, maka

hasilnya akan dicatat dalam sebuah file[4]. HIDS (*Host Intrusion Detection System*) merupakan jenis IDS yang bekerja pada *host* yang individual atau perangkat tertentu pada sistem jaringan komputer secara *real-time*. HIDS akan memantau paket-paket data ketika sedang terjadi penyusupan saja.[2]

SNORT merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemindaian, maupun penyerangan. *SNORT* merupakan gabungan dari protokol analisis dan pendeteksi penyusupan yang berguna untuk merespon kejadian-kejadian yang sedang terjadi pada jaringan komputer secara *real-time*. *SNORT* akan merespon kejadian yang terjadi dalam penyerangan *host-host* jaringan [3].

SNORT memiliki fitur-fitur yang dapat menjaga kemanan sistem jaringan dengan cara memberikan peringatan atau *allert* dan juga meng-*capture* setiap sesi yang sedang berjalan. Dengan adanya fitur ini menjadikan *SNORT* merupakan sistem yang mampu mendeteksi adanya ancaman pada sistem jaringan yang sangat berguna pada *user*[3]. *SNORT* dapat dioperasikan dengan 3 mode, yaitu:

1. *Sniffer mode*, pada mode operasi ini *SNORT* dapat menangkap atau melihat semua paket yang sedang berjalan dalam jaringan dimana *SNORT* diletakkan. *SNORT* juga memiliki kemampuan menampilkan hasil *sniffing* secara *real time.*
2. *Packet logger mode*, pada mode ini *SNORT* mencatat setiap paket yang berjalan dan mengubahnya ke dalam bentuk file.
3. *Network intrusion detection mode*, pada mode ini *SNORT* berjalan dengan melakukan konfigurasi yang kompleks terlebih dahulu, yaitu menjalankan *SNORT* beserta file konfigurasi yang sudah ditentukan (secara *default* file *snort.conf*).

Keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk kedalam sistem jaringan komputer[5]. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Langkah-langkah pencegahan dapat membantu *administrator* untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer.

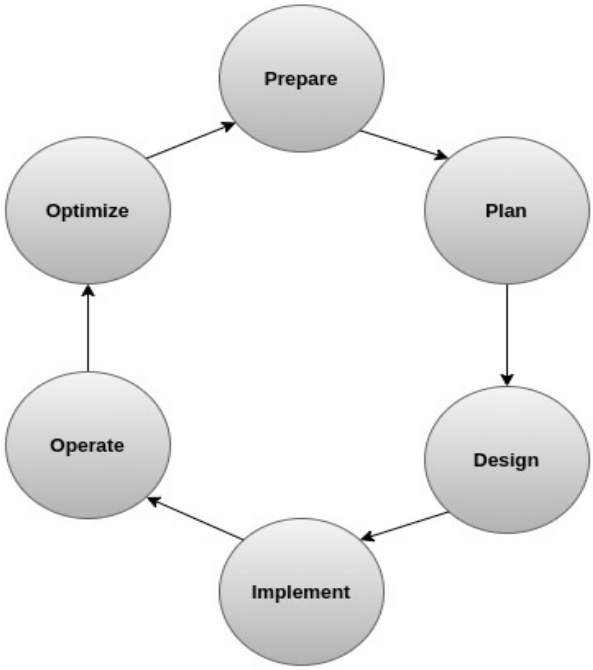
Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat menggangu aktivitas yang sedang terjadi pada sistem jaringan komputer [3]. Ada tiga hal dalam konsep keamanan jaringan, yaitu ingkat bahaya, ancaman dan kerapuhan sIstem.

John D. Howard berpendapat dalam bukunya yang berjudul “An Analysis of security incidents on the internet” bahwa: “Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab”.

Penerapan sistem keamanan jaringan dengan menggunakan aplikasi *SNORT* ini merupakan salah satu solusi yang dapat membantu sistem keamanan jaringan agar tetap terjaga dari penyusup yang mencoba masuk ke dalam sistem jaringan komputer. *SNORT* bekerja dengan cara memantau kondisi jaringan dan menganalisa paket-paket berbahaya yang terdapat dalam jaringan tersebut.

Metode Penelitian

PPDIOO adalah sebuah metode perancangan jaringan yang dirancang untuk mendukung berkembangnya jaringan. PPDIOO terdiri dari beberapa tahapan, yaitu *Prepare, Plan, Design, Implement, Operate, dan Optimize*. Dengan kebutuhan layanan jaringan yang semakin kompleks, maka diperlukan suatu metodologi yang mendukung perancangan arsitektur dan disain jaringan[9].



Gambar 1 Tahapan penelitian

1) *Prepare Phase*

Pada tahap ini, melakukan persiapan membangun sistem keamanan jaringan menggunakan *SNORT*, yaitu mulai mempersiapkan kebutuhan, konsep,dan strategi *financial*. Ada beberapa langkah yang akan dilakukan dalam tahap *Prepare Phase*, yaitu mempersiapkan:

1. Sebuah komputer atau laptop yang digunakan sebagai *intruder* (penyerang) dengan spesifikasi: Sistem Operasi Linux (Distro Linux *Mint*) dan RAM 2 *Gigabyte.*

2. Sebuah komputer atau laptop yang digunakan sebagai server SNORT dengan spesifikasi: Sistem Operasi Windows 10 dan RAM 8 Gigabyte.
3. Sebuah PC yang diserang oleh intruder (penyerang) dengan spesifikasi: Sistem Operasi Windows 10. Dan RAM 8 Gigabyte.
4. Switch
5. Kabel UTP untuk menghubungkan PC client dan server SNORT.
6. Jaringan Internet.
7. Access Point.
8. Sebuah software SNORT.

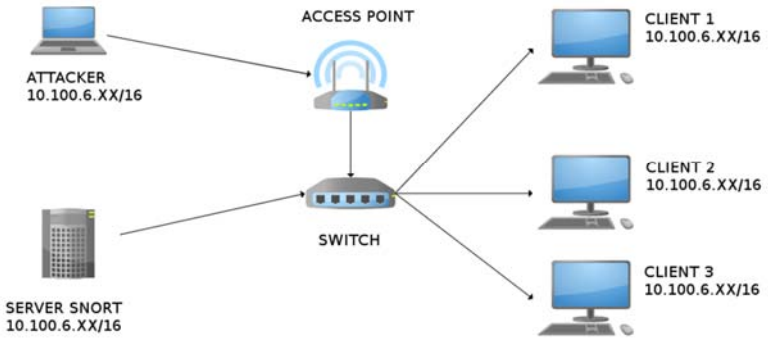
2) *Plan Phase*

Pada tahap ini dilakukan identifikasi hal-hal yang harus dipenuhi berdasarkan tujuan, fasilitas dan kebutuhan pengguna. Perencanaan yang dilakukan adalah :

1. Mengunduh *software SNORT* pada PC *server*
2. Mengunduh *tool* untuk menyerang PC *server* pada PC *attacker*
3. Memilih jenis serangan
4. Memilih skema jaringan

3) *DesignPhase*

Dalam tahap ini, dilakukan desain jaringan yang terperinci yang akan memenuhi persyaratan teknis. Topologi yang digunakan pada tahap ini ditunjukkan pada Gambar 2.



Gambar 2 Topologi jaringan

4) *Implement Phase*

Pada fase ini, dilakukan instalasi dan konfigurasi yang sesuai dengan spesifikasi desain. Dengan menginstal *software* dan konfigurasi dan pemilihan serangan yang diujicoba pada sistem jaringan komputer. Tahap-tahap yang dilakukan pada fase ini adalah sebagai berikut :

1. Menginstal *softwareSNORT* pada PC *server.*

2. Melakukan konfigurasi *SNORT* pada PC *server.*
3. Menginstal *tools* penyerangan pada PC *attacker.*
4. Melakukan konfigurasi *tool* penyerangan pada PC *attacker.*
5. Menghubungkan kabel LAN dari *switch* ke *access point.*
6. Menghubungkan kabel LAN dari PC *client* ke *switch.*
7. Menghubungkan PC *attacker* ke jaringan internet.
8. Melakukan penyerangan terhadap PC *client* dengan metode penyerangan *Ping Flood.*
9. *SNORT* membaca jika terjadi penyerangan terhadap PC *client.*

5) *Operational Phase*

Fase operasional adalah mempertahankan ketahanan kegiatan jaringan, dimana pada fase ini meliputi pengolahan komponen jaringan, melakukan pemeliharaan sistem jaringan, mengelola kinerja jaringan, dan mengoreksi jika ada kesalahan pada jaringan. Pada fase ini, aplikasi *SNORT* dijalankan sesuai dengan rencana yang telah ditentukan.

6) *Optimaze Phase*

Fase Optimalisasi, *administrator* jaringan mengidentifikasi dan menyelesaikan masalah yang sedang terjadi. Kemungkinan di fase optimalisasi akan dilakukan modifikasi desain jaringan, jika terlalu banyak masalah yang timbul. Pada fase ini *Administrator* akan menilai apakah *SNORT* mampu bekerja secara maksimal atau tidak. Jika bekerja secara maksimal, maka *SNORT* sangat berfungsi untuk meminimalisi penyerangan yang terjadi pada sistem jaringan komputer, namun jika tidak, aplikasi *SNORT* masih kurang aman untuk meminimalisir penyerangan yang terjadi pada sistem jaringan komputer.

Hasil dan Pembahasan

Penelitian ini dilakukan dengan menghubungkan beberapa komputer yaitu terdiri dari komputer *server*,*client*, dan *attacker*. Komputer *server* telah diinstal *softwareSNORT* yang berfungsi untuk menangkap paket yang menuju ke komputer *server* tersebut, Sedangkan komputer *attacker* telah diinstal *software* hping3 yang berfungsi untuk melakukan serangan *DDOS Attack* ke *server*. Pada jaringan kali ini disambungkan menggunakan *switch*. Berikut langkah-langkah yang dilakukan pada penelitian ini.

1. Instalasi Jaringan

Pada penelitian ini jaringan yang digunakan adalah jaringan lokal yang terdiri dari 1 komputer *server*, 1 komputer *attacker*, dan 1 komputer *client*. Komputer-komputer tersebut memiliki *IP address* sebagai berikut :

- *Server* : 10.100.3.147
- *client* : 10.100.4.88
- *attacker* : 10.100.6.77

2. Instalasi *SNORT*

SoftwareSNORT diinstal pada komputer *server* yang akan digunakan untuk membaca paket-paket yang menuju ke *server* tersebut. Aplikasi *SNORT* dapat di-*download* pada *website* https://www.snort.org/downloads. Pada *website* tersebut *user* harus men-*downloadsoftware* SNORT dan *rules*.

Setelah selesai menginstal SNORT, *user* terlebih dahulu harus mengkonfigurasi *SNORT* tersebut agar dapat menangkap paket-paket yang menuju ke komputer *server*. *User* harus menambahkan direktori pada *rules SNORT* agar *SNORT* dapat membedakan paket-paket yang menuju komputer *server*, apakah itu merupakan paket yang berbahaya atau bukan. Ada beberapa hal yang perlu dikonfigurasi, yaitu:

1) Konfigurasi *IP address* agar dapat membaca lalu lintas jaringan dan konfigurasi lokasi *rules* agar dapat membaca aturan yang ada pada *SNORT*.

Kode Program 1 konfigurasi *IP address* pada *SNORT*

```
1.  var HOME_NET 10.100.0.254/16
2.  var EXTERNAL_NET !$HOME_NET
3.  var RULE_PATH c:\Snort\rules
4.  var PREPROC_RULE_PATH c:\Snort\preproc_rules
5.  var WHITE_LIST_PATH c:\Snort\rules
6.  var BLACK_LIST_PATH c:\Snort\rules
```

2) Agar *server* dapat membaca intrusi, maka perlu menambahkan *rules* pada file local.rules yang terletak pada direktori C:/snort/rules/

Kode Program 2 membuat *rules* yang akan dibaca oleh *SNORT*

```
1.  alert icmp any any -> $HOME_NET any (msg:"PING to Server!!!!!"; sid:1000001;)
2.  alert tcp any any -> $HOME_NET any (msg:"Possible DoS Attack";flags:S;
    flow:stateless; detection_filter:track by_dst, count 100, seconds 10;
    sid:1000002;)
```

pada tahap ini *user* dapat menyimpan intrusi yang telah dibuat dengan menyimpan file yang telah ditambahkan

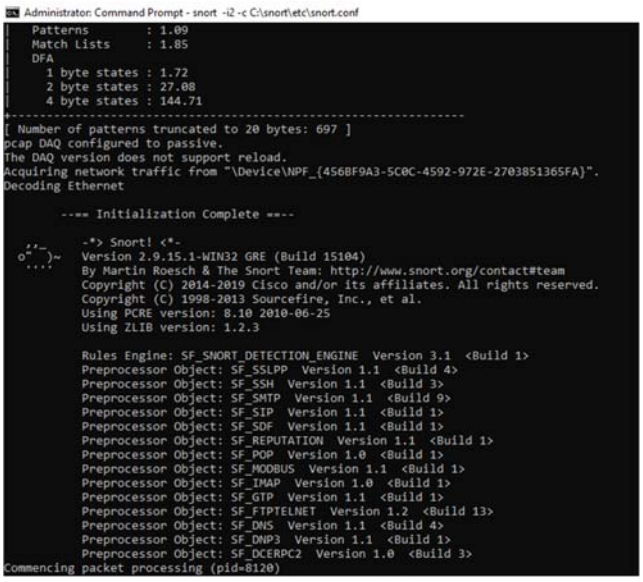
3. Mengaktifkan *server SNORT*

Setelah selesai mengkonfigurasi *SNORT* , maka *SNORT* perlu diaktifkan agar dapat agar dapat membaca paket-paket yang sedang menuju komputer

server. Untuk mengaktifkan *SNORT*, perlu memasukkan perintah pada Windows dengan menggunakan *CMD*, yaitu:

Kode Program 3 Cara mengaktifkan *SNORT*

```
1.  snort -i2 -c C:\snort\etc\snort.conf
```



Gambar 3 Hasil konfigurasi *SNORT*

Pada **Gambar 3** dapat dilihat bahwa *SNORT* telah aktif dan sudah siap digunakan untuk melakukan pendeteksian pada PC *server*.

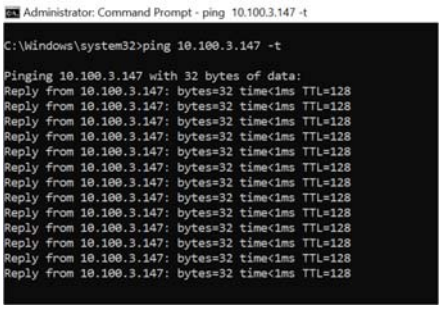
4. Melakukan *Ping*

Untuk melakukan *ping dari* PC *Client* ke PC *server* dapat kita lakukan perintah sebagai berikut :

Kode Program 4 melakukan ping ke PC *Server*

```
1.  Ping 10.100.3.147 -t
```

Ping 10.100.3.147 -t berfungsi agar PC *Client* dapat melakukan cek koneksi ke PC *server* secara terus menerus tanpa berhenti.

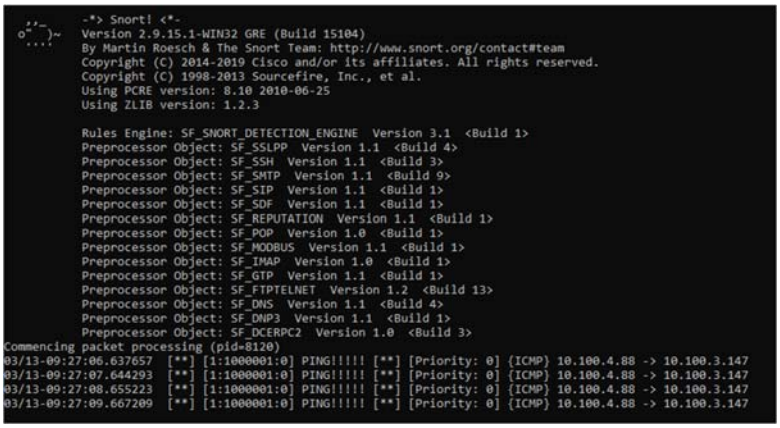


```
Administrator: Command Prompt - ping  10.100.3.147 -t

C:\Windows\system32>ping 10.100.3.147 -t

Pinging 10.100.3.147 with 32 bytes of data:
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
Reply from 10.100.3.147: bytes=32 time<1ms TTL=128
```

Gambar 4 Melakukan *Ping*

Pada **Gambar 4** dapat dilihat bahwa *IP address* 10.100.4.88 akan melakukan ping ke *server SNORT* yang memiliki *IP address* 10.100.3.147. Pada baris "*Pinging 10.100.3.147 with 32 bytes of data:"* berisi bahwa *host* yang dituju oleh PC c*lient* adalah PC *server* yang memiliki *IP address* 10.100.3.147 dan besaran paket yang dikirim secara *default*, maka besaran paket yang dikirim adalah *32 bytes.*

Pada baris *"Reply from 10.100.3.147: bytes:32 time<1ms TTL=128"* merupakan pesan balasan yang diterima oleh PC client yang dimana "*time<1ms"* merupakan total waktu yang dibutuhkan agar sebuah paket dapat terkirim ke PC *server*, yaitu sekitar 1 *millisecond(ms)* dan juga TTL*(time to live) yang* merupakan waktu maksimum PC *server* saat membalas paket yang dikirm olehPC *client,* yaitu dengan jumlah 128.



```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1-WIN32 GRE (Build 15104)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=8120)
03/13-09:27:06.637657  [**] [1:1000001:0] PING!!!!! [**] [Priority: 0] {ICMP} 10.100.4.88 -> 10.100.3.147
03/13-09:27:07.644293  [**] [1:1000001:0] PING!!!!! [**] [Priority: 0] {ICMP} 10.100.4.88 -> 10.100.3.147
03/13-09:27:08.655223  [**] [1:1000001:0] PING!!!!! [**] [Priority: 0] {ICMP} 10.100.4.88 -> 10.100.3.147
03/13-09:27:09.667209  [**] [1:1000001:0] PING!!!!! [**] [Priority: 0] {ICMP} 10.100.4.88 -> 10.100.3.147
```

Gambar 5 Hasil Ping dideteksi oleh *SNORT*

Pada **Gambar 5** dapat dilihat bahwa *server SNORT* sedang mendeteksi adanya *ping* menuju *server* komputer dan menunjukkan waktu dan tanggal serta *IP address* yang mencoba ping ke *server SNORT*

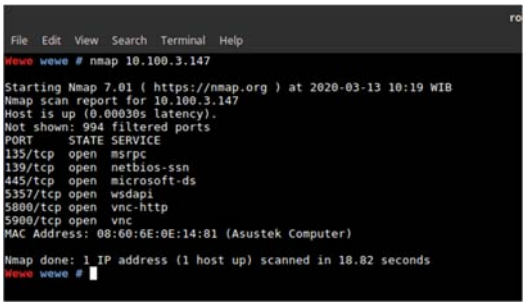
5. *DDOSAttack*

Komputer *attacker* akan mencoba melakukan *DDOS Attack* ke *server SNORT* dengan metode *Pingfloodattack*. *Pingflood* merupakan sebuah metode penyerangan dengan cara membanjiri paket data dalam waktu singkat sehingga dapat membuat komputer target menjadi error bahkan sampai rusak. Metode ini juga dapat membuat komputer itu tidak dapat berbagi file atau data ke komputer lain. Pada percobaan ini *attacker* yang memiliki *IP address* 10.100.6.77 mencoba melakukan *Pingflood* ke *server* komputer yang memiliki *IP address* 10.100.3.147.

Pada penelitian ini digunakan sistem operasi Linux untuk melakukan serangan *DDOS Attack* dengan menggunakan aplikasi "hping3". Sebelum melakukan *DDOS Attack*, terlebih dahulu *user* melakukan *port scanning* dari komputer *attacker* dengan menggunakan aplikasi "nmap". Untuk melakukan *port scanning* dapat dilakukan dengan perintah sebagai berikut :

Kode Program 5 Cara melakukan *port scanning*

```
1.  Nmap 10.100.3.147
```



Gambar 6 Melakukan *port scanning* menggunakan nmap

Setelah selesai melakukan *port scanning* dapat pada **Gambar 6** terdapat beberapa *port* yang terbuka pada PC *server* seperti *port* 135/tcp, 139/tcp, 445/tcp dan sebagainya. *Port* tersebut dapat dimanfaatkan sebagai celah untuk melakukan penyerangan.

Gambar 7 Melakukan *PingFlood*

Pada **Gambar 7** *Attacker* melakukan *Pingflood* dengan memanfaatkan *port* yang terbuka yaitu *port* 445. Untuk melakukan *Pingflood* perlu memasukkan perintah di dalam terminal sebagai berikut :

Kode Program 6 Cara melakukan *Pingflood*

```
1.  Hping3 --flood -p 445 -S 10.100.3.147
```

Pada baris perintah **Kode Program 6** terdapat beberapa hal yang perlu dipahami, yaitu :

- Hping3 merupakan pemanggilan aplikasi *Pingflood*

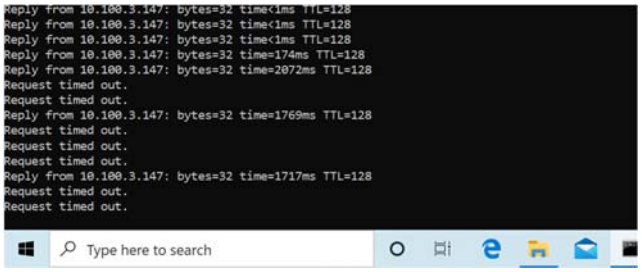
- -*flood* merupakan perintah untuk membanjiri lalu lintas data

- -p 445 adalah *port* yang dituju, yaitu *port* 445

- -S 10.100.3.147 adalah *IP address* yang akan diserang, yaitu 10.100.3.147

Gambar 8 *Server SNORT* mendeteksi adanya serangan

Dari **Gambar 8** dapat dilihat bahwa adanya serangan *DDOS Attack*. *SNORT* juga dapat membaca waktu penyerangan, *port* yang diserang dan *IP address* mana yang menyerang komputer *server*.



Gambar 9*Ping* ke *server*

Pada **Gambar 9** terlihat proses *ping* dari komputer client ke komputer *server*. Ketika *server SNORT* sedang diserang oleh *IP address* 10.100.6.77 maka, ketika *IP addressclient* me-*request* ke *server* akan terjadi *request timed out* atau pun membutuhkan waktu yang sangat tinggi.

B) Hasil Analisa

1. Penambahan Rules

Pada penelitian ini dibuat beberapa *rules*, yaitu:

```
1. alert icmp any any -> $HOME_NET any (msg:"PING to Server!!!!!"; sid:1000001;)
2. alert tcp any any -> $HOME_NET any (msg:"Possible DoS Attack";flags:S;
   flow:stateless; detection_filter:track by_dst, count 100, seconds 10;
   sid:1000002;)
```

Dari aturan *rules* diatas dibuat untuk mendeteksi jika :

1) adanya *ping* ke komputer *server*.
2) jika ada yang melakukan percobaan serangan ke komputer *server*.

Dengan Keterangan sebagai berikut:

Rule Header :
- *Alert* adalah tanda peringatan.
- icmp dan tcp adalah jenis protokol *transport.*
- *any* adalah untuk melihat *IP address*. *SNORT* akan membaca semua sumber *IP address* yang mencoba masuk atau pun me-*request* sesuatu ke *IP address* komputer *server*.
- *any* adalah untuk membaca sumber port. *SNORT* akan membaca semua sumber *port* yang mencoba menyerang *server* komputer.
- → adalah aliran *host* asal ke *host* tujuan.
- $HOME_NET adalah *host* awal yang melewati *port* manapun.
- *any* adalah untuk membaca tujuan *port*. *SNORT* akan membaca seluruh *port* yang akan dilindungi.

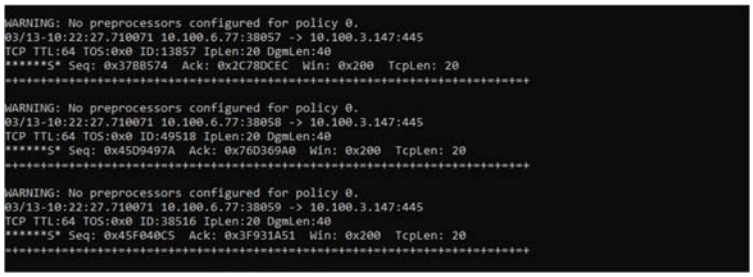
Rule Option :
- msg:"PING to Server!!!!!" dan msg:"Possible DoS Attack" merupakan pesan yang akan diberikan kepada *administrator* jika ada sesuatu hal yanng terjadi pada jaringan komputer.
- sid: 1000002 dan sid:1000001 adalah id.
- *flag*: S adalah kontrol *bit* yang berupa informasi bagaimana sebuah paket harus ditangani.
- *flow:stateless* adalah perintah untuk menentukan kemana paket data dikirim.
- *detection_filter:track by_dst* adalah *SNORT* akan melacak alamat *IP address* tujuan untuk dideteksi.
- *count* 100 adalah *SNORT* akan mencatat minimal 100 peristiwa berdasarkan *IP address* yang sama.
- *second* 10 adalah waktu yang diperlukan oleh *IP address* untuk melakukan pencatatan pada *SNORT.*

2. *LogSNORT*

SNORT juga mampu mencatat setiap paket yang telah dideteksi oleh *SNORT* dalam bentuk file dan paket itu akan disimpan ke dalam *disk* komputer. Secara otomatis file tersebut akan tersimpan di *directory* C:\snort\log. File *log* tersebut dapat dibuka menggunakan CMD dengan melakukan perintah C:\snort\log\snort.log.{angka acak}.

Kode Program 7 perintah untuk membuka *log* pada CMD

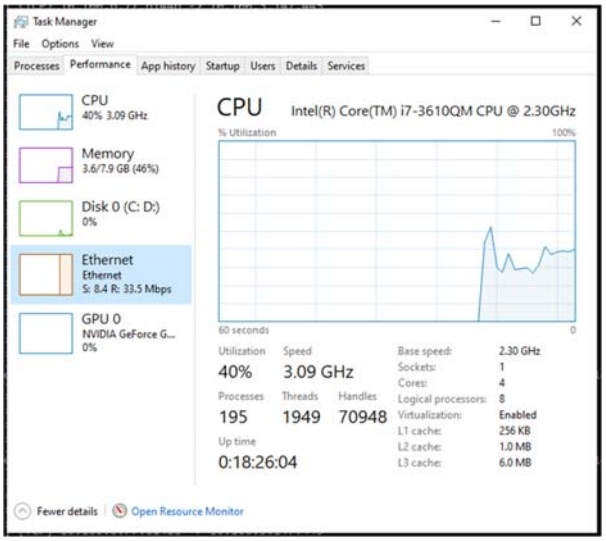
```
1.  C:\snort\log\snort.log.1584069679
```



Gambar 10 Hasil *Logger*

Pada **Gambar 10** terdapat beberapa hal yang perlu dipahami, yaitu: ,Pencatatan waktu yaitu 03/13-10.22.27, yang berarti *SNORT* mendeteksi penyerangan pada tanggal 13 maret tepat pada jam 10 lewat 22 menit 27 detik, *IP addressattacker* adalah 10.100.6.77, *port* yang digunakan oleh *attacker* untuk menyerang komputer *server* adalah *port* 445.

3. Pengaruh *Pingflood*

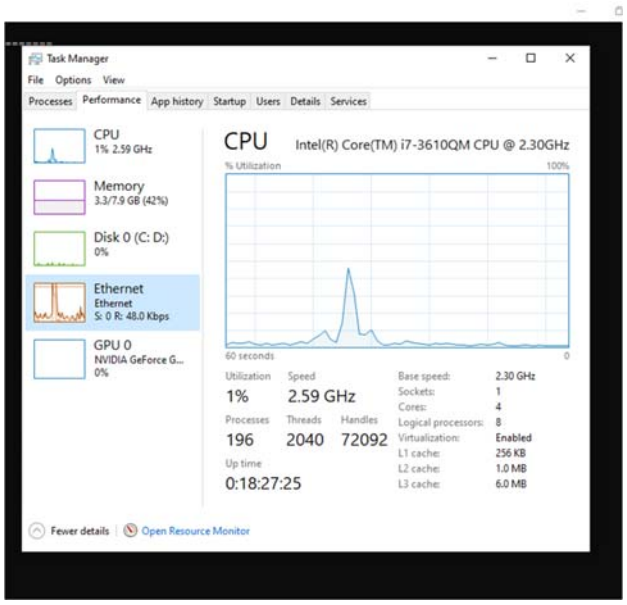


Gambar 11 Grafik *Perfomance CPU*

Dari **Gambar 11** dapat dilihat bahwa grafik pada CPU sangat tinggi, ketika *attacker* melakukan penyerangan *DDOS Attack*, maka komputer akan bekerja secara lebih maksimal karena terlalu banyaknya paket menuju komputer server. Kinerja komputer dapat dilihat pada Tabel 1.

Tabel 1 *Performance* CPU

Performance	Total
CPU	40% 3.09Ghz
Memory	3.6/7.9 GB (46%)
Utilization	40%
Speed	3.09 GHz
Processes	195
Thread	1949
Handles	70948



Gambar 12 Grafik *performance* CPU

Pada **Gambar 12**, penyerangan dari komputer *attacker* telah diberhentikan sehingga grafik performa dari komputer server lebih rendah dan komputer server dapat melakukan pemrosesan secara stabil. Kinerja komputer server dapat dilihat pada tabel berikut.

Tabel 2*Performance* CPU

Performance	Total
CPU	1% 2.59Ghz
Memory	3.3/7.9 GB (46%)
Utilization	1%

Performance	Total
Speed	2.59 GHz
Processes	196
Thread	2040
Handles	72092

Simpulan

Berdasarkan penelitian yang dilakukan dapat disimpulkan bahwa sistem keamanan jaringan komputer menggunakan aplikasi *SNORT* dapat membantu administrator PT. Promanufacture Indonesia untuk meminimalisir terjadinya serangan dari pihak-pihak yang tidak bertanggung jawab.

Daftar Pustaka

[1] D. Wijanarko, "SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SNORT," *J. Teknol. Inf. dan Terap.*, vol. 2, no. 1, pp. 171–175, 2015.

[2] B. Sudradjat, "SISTEM PENDETEKSIAN DAN PENCEGAHAN PENYUSUP PADA JARINGAN KOMPUTER DENGAN MENGUNAKAN SNORT DAN FIREWALL | Journal of Information System, Applied, Management, Accounting and Research," *JISAMAR J. Inf. Syst. Applied, Manag. Account. Res.*, vol. 1, no. 1, pp. 10–24, Dec. 2017, [Online]. Available: http://journal.stmikjayakarta.ac.id/index.php/jisamar/article/view/9.

[3] A. L. Ginting, J. Napitupulu, and J. Jamaluddin, "Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia," 2018, doi: 10.31227/osf.io/w5gt7.

[4] M. Ulfa, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) DI JARINGAN UNIVERSITAS BINA DARMA," *J. MATRIK*, vol. 15, no. 2, pp. 105–118, Aug. 2013, [Online]. Available: http://jurnal.binadarma.ac.id/index.php/jurnalmatrik/article/view/275.

[5] A. F. Mutaqin, "Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort," Nov. 2015. [Online]. Available: https://jurnal.untan.ac.id/index.php/justin/article/view/12537.