

ANALISIS LOG SNORT MENGGUNAKAN *NETWORK FORENSIC*

Ervin Kusuma Dewi¹⁾, Patmi Kasih²⁾

¹⁾Sistem Informasi Universitas Nusantara PGRI Kediri

²⁾Teknik Informatika Universitas Nusantara PGRI Kediri

^{1,2)} Jl. KH. Ahmad Dahlan No.76, Mojoroto, Kota Kediri, Jawa Timur 64112

e-mail: ervin@unpkediri.ac.id¹⁾, Fatkasih@gmail.com²⁾

ABSTRAK

Keamanan yang terjamin dapat meminimalisir kerugian yang disebabkan oleh serangan keamanan jaringan. Sistem keamanan jaringan merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data. Keamanan tersebut dapat dibangun dengan menggunakan Pendekatan Forensik Jaringan. Forensik Jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan. Sistem pengamatan serangan dapat menggunakan tools Intrusion Detection System (IDS) Snort. Snort adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Tujuan dari penelitian ini yaitu menganalisis Log snort sebagai hasil Forensik Jaringan. Pada eksperimen menggunakan topology star. Terdapat 1 PC sebagai snort, 3 PC client yang melakukan serangan, 7 PC sebagai client biasa. Dari hasil uji coba, dilakukan set rules sebagai kecerdasan. Hasil eksperimen menunjukkan bahwa snort yang dibangun mampu memantau lalu lintas jaringan, sehingga ketika terjadi packet mencurigakan yang mengandung serangan maka snort akan mengirimkan alert, selain itu juga menyimpan data serangan pada Log snort. Log tersebut dapat di investigasi dengan menggunakan Model Proses Forensik. Hasil investigasi menunjukkan bahwa terdapat 3 IP menyerang serta menunjukkan data serangan yaitu tanggal melakukan serangan, IP penyerang, waktu serangan, dan jenis serangan..

Kata Kunci: *Network Forensik, Snort, Model Proses Forensik.*

ABSTRACT

Security is assured to minimize losses caused by network security attack. Network security system is an important factor to ensure the ability, integrity and validity of data. Such security can be built using the Network Forensic Approach. Network forensic focuses on data obtained based on observation on the network. Observing attacks can use Snort Intrusion Detection System (IDS) tool. Snort is an open source-based NIDS software, widely used to secure a network from malicious activity. The working of snort similar to tcpdump, but focus as a security packet sniffing. The aim of this study is to analyze the log snort as a result of network forensic. In the experiment using topology star. There is 1 PC as a snort, 3 PC client that perform attacks, 7 PC as a client too. In the test conducted set as rules as intelligence. The experimental results show that snort is able to monitor network traffic, so that when the suspicious packet containing the attack will send alerts snort, but it also stores the data in the log. The logs can be investigated using the forensic process model. The results of the investigation indicate there are 3 IP attack, as well as showing the attack data are the date of the attack, attacker IP, attack time, and type of attack.

Keywords: *Network Forensic, Snort, Forensic Process Model.*

I. LATAR BELAKANG

Keamanan yang terjamin dapat meminimalisir kerugian yang disebabkan oleh serangan keamanan jaringan. Berdasarkan data dari direktur lembaga riset Telematika Sharing Vision yang melakukan penelitian pada Tahun 2013, indonesia mendapatkan 42.000 serangan di dunia maya per hari [1]. Begitu juga dengan Akamai yang melaporkan indonesia menjadi Negara nomor 1 sumber serangan internet (*malicious traffic*) [2].

Banyaknya pengguna internet dapat menimbulkan masalah, mulai dari kasus perbuatan yang tidak menyenangkan hingga terjadi kejahatan (*fraud*). Berdasarkan statistic yang dikeluarkan oleh ID-CERT menunjukkan masalah keamanan (*security*) berupa serangan melalui jaringan (*network attack*) termasuk perusakan situs web (*deface*) dan penerobosan hak akses, virus atau malware, *phising*, dan *fraud* [3].

Sistem keamanan jaringan merupakan faktor penting untuk menjamin stabilitas, integritas dan validitas data.

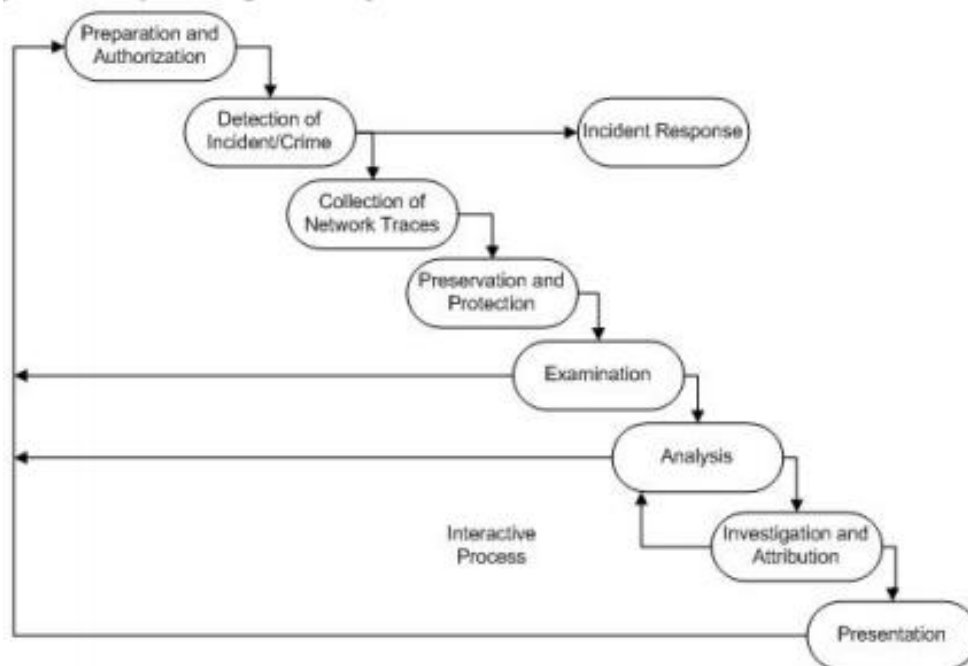
Keamanan tersebut dapat dibangun dengan menggunakan Pendekatan *Network Forensic*. Forensik Jaringan memfokuskan pada data yang diperoleh berdasarkan pengamatan pada jaringan [4]. Kelebihan dari Network Forensic yaitu mampu menganalisis trafik pada jaringan dan mengobservasi jaringan yang merupakan bagian dari investigasi.

Pengumpulan data Network Forensic menggunakan sebuah tool yang bisa menyimpan semua kejadian data-data lalu lintas jaringan. Salah satu tool yang mampu memenuhi kebutuhan Network Forensic yaitu Snort. Snort merupakan tool cross platform yang mampu diinstall pada Windows, Mac OS, dan Linux. Snort merupakan tool yang open source dan update dari Snort dapat diakses oleh semua pengguna. Snort merupakan tool yang berbasis Intrusion Detection System (IDS) yang dapat memonitor jaringan yang berdampak serangan, selain itu juga menyimpan serangan tersebut pada Log.

Tujuan dari penelitian ini yaitu mengimplementasikan snort serta menganalisis Log snort dengan menggunakan Network Forensik, yaitu melakukan investigasi dari data serangan yang tersimpan pada Log snort. Pada implementasi akan dibangun sebuah topology star.

II. NETWORK FORENSIK

Forensik sebagian besar menangani kejahatan yang dilakukan sebelumnya, fokusnya untuk mencegah kejahatan di masa depan [5]. Forensik jaringan merupakan salah satu ilmu forensik digital yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital. Menurut Lazzez [6] tahapan Model Proses Forensik (*The Forensic Process Model*) pada ditunjukkan pada diagram alir Gambar 1.



Gambar 1. Diagram Alir Penelitian [6]

1. *Preparation And Authorization* (Persiapan dan Otorisasi)

Network Forensik bisa diterapkan jika dimana *network security tools* seperti system deteksi instruksi, *packet analyzer*, dan firewall ditempatkan di beberapa titik jaringan. Otorisasi sangat diperlukan untuk memantau lalu lintas jaringan, selain itu aturan keamanan diterapkan dengan baik sehingga tidak menyalahi privasi individu dan organisasi.

2. *Detection and Incident/Crime* (Deteksi insiden / kejahatan)

Alert yang disinyalkan oleh *security tools* menunjukkan serangan dan tahap selanjutnya akan di analisis. Sifat serangan ditentukan dari berbagai parameter. Validasi dilakukan untuk menilai dan mengkonfirmasi dugaan penyerangan. Hal ini dilakukan untuk menentukan apakah penyelidikan dilanjutkan atau mengabaikan alert sebagai *false alarm*.

3. *Incident Response* (Penanganan Insiden)

Respon terhadap serangan keamanan terdeteksi berdasarkan informasi yang dikumpulkan untuk memvalidasi dan mengevaluasi kejadian. Respon dimulai tergantung pada jenis serangan dan diarahkan oleh organisasi atau kebijakan hukum yaitu rencana untuk mencegah serangan dan *recover* kerusakan, pada saat

yang bersamaan keputusan apakah penyelidikan dilanjutkan atau tidak. Fase ini berlaku untuk kasus-kasus dimana investigasi dimulai pada saat serangan berlangsung dan tidak dapat dilakukan setelah notifikasi serangan.

4. *Collection of Network Traces* (Koleksi Jejak Jaringan)

Network trace dikumpulkan oleh *security tools*. Pada tahap ini melakukan pencarian bukti dan pengumpulan bukti, pengenalan terhadap bukti-bukti penyerangan dan pengumpulan bukti.

5. *Preservation and Protection* (Presentasi dan Ulasan)

Data asli yang diperoleh dan *log* disimpan pada perangkat *backup*. Memastikan akurasi data, salinan dari data yang akan di analisis. Hal ini dilakukan agar penyelidikan dilakukan dapat dibuktikan lagi sehingga memenuhi persyaratan hukum.

6. *Examination* (Pemeriksaan)

Data yang diperoleh membentuk dataset dan dapat dianalisis serta dipetakan. Pemeriksaan dilakukan agar informasi penting tidak hilang atau tercampur dengan data lain. Data akan diklasifikasikan, informasi dan data yang tidak penting dihapus.

7. *Analysis* (Analisis)

Bukti-bukti dikumpulkan dan dianalisis pola serangan yang digunakan penyerang. Beberapa parameter penting yang berhubungan dengan pembentukan koneksi, protokol, sistem operasi, fragmentasi paket semua dianalisis untuk mengetahui cara penyerang. Hasil dari tahap ini adalah validasi dari aktivitas yang mencurigakan.

8. *Investigation and Attribution* (Investigasi dan Atribusi)

Bukti informasi yang diperoleh dari hasil analisis digunakan untuk mengidentifikasi :

- 1) Serangan apa yang terjadi?
- 2) IP siapa yang melakukan serangan?
- 3) Kapan serangan terjadi?
- 4) Dimana serangan itu terjadi?
- 5) Bagaimana serangan tersebut bisa terjadi?
- 6) Mengapa itu terjadi?

9. *Presentation* (Presentasi dan Review)

Semua hasil di sajikan dengan bahasa yang dimengerti serta menjelaskan berbagai prosedur yang digunakan sampai pada kesimpulan dari proses penyidikan. Dokumentasi penyidikan juga disertakan agar bisa digunakan untuk mencegah kejadian serangan yang sama di masa yang akan datang.

III. IMPLEMENTASI

Snort [7] adalah perangkat lunak IDS dan NIDS berbasis opensource dan banyak digunakan untuk untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya. Cara kerja Snort mirip dengan TcpDump, tetapi fokus sebagai security packet sniffing. Fitur utama Snort yang membedakan dengan TcpDump adalah payload inspection, dimana Snort melakukan analisis payload rule set yang disediakan [8].

Snort mempunyai tiga komponen :

- 1)Sesor yang dapat mengenali adanya *security events*.
- 2)Console yang dapat memonitor event dan alerts dan mengontrol sensor
- 3) Central Engine yang berguna untuk menyimpan *event logged* yang dilakukan oleh sensor kedalam database dan menggunakan aturanaturan keamanan yang berguna untuk menangani *event* yang terjadi.

Snort di install pada Linux Ubuntu versi 16.04, versi Snort yang di install adalah versi 2.9.9.0 yang dapat di download pada <https://www.snort.org/> [9]. Gambar 2 merupakan Snort yang sudah berhasil di install.

```

Running in packet dump mode

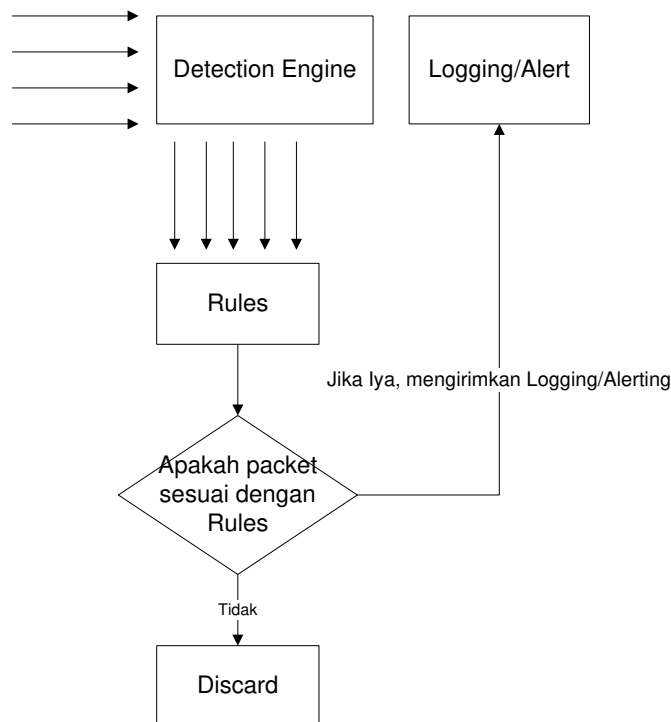
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to read-file.
Acquiring network traffic from "snort.log.1494909748".

--== Initialization Complete ==--

-*> Snort! <*-
Version 2.9.9.0 GRE (Build 56)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2016 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.7.4
Using PCRE version: 8.38 2015-11-23
Using ZLIB version: 1.2.8
    
```

Gambar 2. SNORT

Pada Gambar 3 merupakan cara kerja Snort *detection engine* dengan *IDS mode*. Ketika terdapat *packet* datang melalui *switch* maka akan terdeteksi oleh *detection engine* yang sudah terinstall Snort sebagai IDS di cocokkan dengan *rules* yang sudah di *set*. *Packet* tersebut dicek apakah *packet* sesuai dengan *rules*. Ketika *packet* tersebut mengandung konten serangan maka akan tersimpan di *Log Snort* dan akan memunculkan *alarm*. Namun ketika *packet* tersebut tidak mengandung konten serangan maka *packet* tersebut di *discard* (diabaikan) dan langsung dikirimkan.



Gambar 3. Snort *detection engine* [10]

Pada Snort terdapat *rule* sebagai kecerdasan Snort. Pengambilan dan penandaan *packet* dilakukan dengan cara sniffing pada lalu lintas *packet* pada *transport* protokol TCP baik *packet* yang dikirim maupun yang diterima. *Rules* yang di *set* memberikan kecerdasan pada saat proteksi, sehingga proses investigasi sangat tergantung dari kecerdasan rule. Gambar 4 merupakan konfigurasi dari penyimpanan rules, ketika terdapat serangan pada *server* maka log dari serangan tersebut akan tersimpan pada *rule*. *Rules* yang diterapkan yaitu : 1) *Ping of death*. Snort melakukan pencatatan untuk semua paket ICMP yang masuk ke jaringan. Ketika ada paket yang di curigai maka akan muncul pesan “*ping of death*”, 2) Ketika terjadi serangan pada FTP maka akan muncul notifikasi “*FTP connection attempt*”

Rule 1					
alert	icmp	any	any	->	\$HOME_NET any (msg:"ping of death"; sid:1000001; rev:1; classtype:icmp-event;)
Rule 2					
alert	tcp	192.168.0.69	any	->	\$HOME_NET 23 (msg:"FTP connection attempt"; sid:1000002; rev:1;)

Gambar 4. Rules

Implementasi dilakukan pada *server* SNORT, log yang tersimpan akan di analisis mengikuti alur Model Proses Forensik. Log akan di parsing untuk melihat isi dari SNORT log, apakah serangan itu bentuk berbahaya atau tidak.

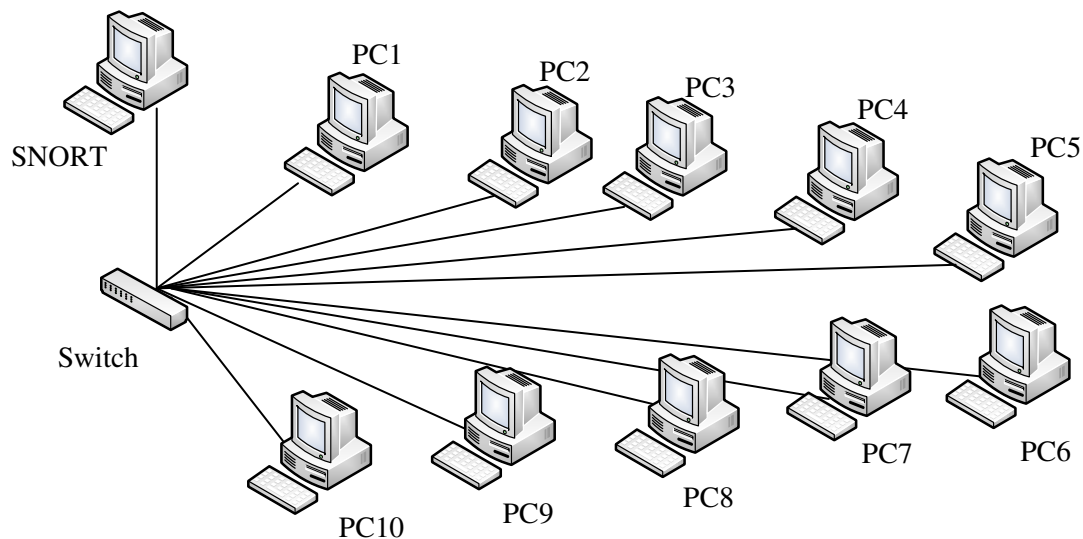
```
Snort -dvr snort.log 1494909748
```

Gambar 5. Membuka Log SNORT

Salah satu cara untuk membuka *Log Snort* dengan menggunakan fungsi `-r<filename>` baik dari Snort, TCPDump, *Etherreal* atau program lain yang membuat file format libpcap. Gambar 5 merupakan perintah untuk membaca *Log Snort*.

IV. EKSPERIMENT DAN ANALISIS

Topologi yang digunakan untuk eksperimen adalah topologi *star*. Terdapat 1 PC sebagai Snort, 10 PC sebagai client dan semuanya terhubung dengan *Switch*. Gambar 6 merupakan desain topologi yang digunakan untuk eksperimen.



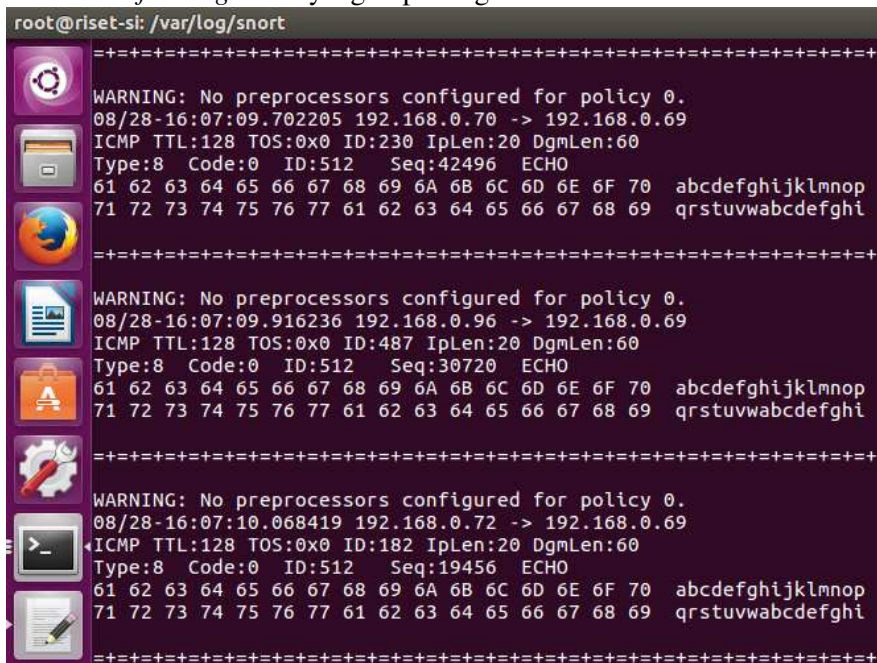
Gambar 6. Topologi

Pada eksperimen ini 3 PC akan melakukan serangan kepada *server Snort*, selain itu 3 PC lainnya hanya sebagai *client* biasa yang mengirimkan *packet data* ke PC Snort dan ke PC lainnya. Lalu lintas tersebut akan di analisis. Konfigurasi dari eksperimen ini seperti Tabel 1.

Tabel 1. Konfigurasi ekperimen

Nama PC dan IP Address	Sistem Operasi	Toosl pendukung	Konfigurasi Aplication
PC 0 IP : 192.168.0.69	Ubuntu versi 16.04 LTS	SNORT versi 2.9.9.9	NIDS with alert SNORT Rules, TCP.
PC 1 IP : 192.168.0.70	Microsoft Windows 7	Command Prompt	Ping flood & ftp attack
PC 2 IP : 192.168.0.71	Microsoft Windows 7	Command Prompt	-
PC 3 IP : 192.168.0.72	Microsoft Windows 7	Command Prompt	Ping flood & ftp attack
PC 4 IP : 192.168.0.73	Microsoft Windows 7	Command Prompt	-
PC 5 IP : 192.168.0.75	Microsoft Windows 7	Command Prompt	-
PC 6 IP : 192.168.0.76	Microsoft Windows 7	Command Prompt	-
PC 7 IP : 192.168.0.77	Microsoft Windows 7	Command Prompt	-
PC 8 IP : 192.168.0.78	Microsoft Windows 7	Command Prompt	-
PC 9 IP : 192.168.0.96	Microsoft Windows 7	Command Prompt	Ping flood & ftp attack
PC 10 IP : 192.168.0.80	Microsoft Windows 7	Command Prompt	-

Pengujian dilakukan dengan melakukan serangan dengan menggunakan *ping flood* dan *FTP attack*. IP yang akan melakukan serangan adalah IP : 192.168.0.70, IP : 192.168.0.72 dan IP : 192.168.0.96. Dari hasil pengujian ketika dilakukan serangan, Snort mampu mendeteksi serangan tersebut berdasarkan kecerdasarn rules yang diberikan. Snort akan memberikan alert, selain itu menyimpan file data serangan pada *Log Snort /var/log/snort*. Gambar 7 adalah salah satu contoh *file Log Snort* yang di parsing.



```

root@riset-si: /var/log/snort
=====
WARNING: No preprocessors configured for policy 0.
08/28-16:07:09.702205 192.168.0.70 -> 192.168.0.69
ICMP TTL:128 TOS:0x0 ID:230 IpLen:20 DgmLen:60
Type:8 Code:0 ID:512 Seq:42496 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
=====
WARNING: No preprocessors configured for policy 0.
08/28-16:07:09.916236 192.168.0.96 -> 192.168.0.69
ICMP TTL:128 TOS:0x0 ID:487 IpLen:20 DgmLen:60
Type:8 Code:0 ID:512 Seq:30720 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
=====
WARNING: No preprocessors configured for policy 0.
08/28-16:07:10.068419 192.168.0.72 -> 192.168.0.69
ICMP TTL:128 TOS:0x0 ID:182 IpLen:20 DgmLen:60
Type:8 Code:0 ID:512 Seq:19456 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi
=====

```

Gambar 7. Parsing Log Snort 1

Dari Gambar 7 dapat diketahui serangan terjadi pada bulan Agustus dan tanggal 28 , waktu serangan 16:07:09,

IP penyerang yaitu 192.168.0.70, dan jenis serangan ICMP (*Internet Control Message Protocol*) dengan TTL (*Time to Live*) 128, ID 512.

```

root@riset-si: /var/log/snort
=====
Run time for packet processing was 0.102570 seconds
Snort processed 992 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
Pkts/sec:          992
=====
Memory usage summary:
Total non-mmapped bytes (arena):      610304
Bytes in mapped regions (hblkhd):    11898880
Total allocated space (uordblks):    488704
Total free space (fordblks):        121600
Topmost releasable block (keepcost): 118504
=====
Packet I/O Totals:
Received:          992
Analyzed:         992 (100.000%)
Dropped:          0 ( 0.000%)
Filtered:         0 ( 0.000%)
Outstanding:      0 ( 0.000%)
Injected:         0
=====
Breakdown by protocol (includes rebuilt packets):
Eth:              992 (100.000%)
VLAN:             0 ( 0.000%)
IP4:             992 (100.000%)
Frag:            0 ( 0.000%)
ICMP:           992 (100.000%)
UDP:             0 ( 0.000%)
TCP:             0 ( 0.000%)
IP6:             0 ( 0.000%)
IP6 Ext:         0 ( 0.000%)
IP6 Opts:        0 ( 0.000%)
Frag6:           0 ( 0.000%)
ICMP6:           0 ( 0.000%)
UDP6:           0 ( 0.000%)
TCP6:           0 ( 0.000%)
Teredo:          0 ( 0.000%)
ICMP-IP:         0 ( 0.000%)
IP4/IP4:         0 ( 0.000%)
IP4/IP6:         0 ( 0.000%)
IP6/IP4:         0 ( 0.000%)

```

Gambar 8. Parsing SNORT Log 2

Selain itu pada Gambar 8 juga merupakan hasil dari *parsing Log Snort* yang diketahui bahwa runtime untuk proses *packet* adalah 0.102570 *second* dengan total packet 992 *packet*. *Memory* sebesar 610.304 *bytes*. Informasi dari *packet log* merupakan bahan investigasi forensik jaringan. Dari informasi tersebut *administrator* jaringan mengetahui apa saja yang terjadi pada jaringan sehingga dapat menelusuri data serangan. Pada *file log* memungkinkan semua trafik jaringan di *capture* dan dilakukan analisis. *File log* yang berasal dari Snort IDS digunakan sebagai bukti kejadian yang terjadi pada jaringan dan digunakan sebagai bukti. Untuk memudahkan dalam membaca hasil serangan, maka disajikan dalam bentuk tabel. Tabel 2 merupakan hasil investigasi.

Tabel 2. Hasil investigasi

No	Log	IP penyerang	Time (WIB)	ID	Seq	Total Packet (pkt/sec)	Packet Processing (seconds)
1	1494910751	192.168.0.70	16:10:29	384	27905	78	0.38063
2	1503910699	192.168.0.96	15:58:20	369	4096	19	0.490
3	1501040067	192.168.0.72	16:10:00	512	62976	655	0.91552
4	1503911199	192.168.0.70	16:07:09	512	42496	992	0.102570

V. KESIMPULAN

Berdasarkan implementasi dengan menggunakan tools keamanan jaringan Snort maka dapat disimpulkan Snort

yang dibangun dapat memantau lalu lintas packet di dalam jaringan serta mampu mendeteksi serangan berdasarkan rule yang diset, sehingga serangan jaringan komputer tersebut dapat segera ditangani segera mungkin oleh administrator karena terdapat alert. Dari hasil uji coba serangan, total serangan sebanyak 4 (empat) kali. Serangan 2 (dua) kali dilakukan oleh IP yang sama yaitu 192.168.0.70 namun waktu serangan yang berbeda. Dengan menggunakan *Network Forensic* dapat di kumpulkan bukti-bukti serangan dan dilakukan investigasi untuk mendapatkan Bukti. Bukti serangan yang didapat meliputi tanggal dan bulan pada saat menyerang, IP penyerang, jenis serangan, waktu serangan dan jumlah *packet* yang dikirimkan.

DAFTAR PUSTAKA

- [1] R. Wahyudi. (Oktober, 2014). Kejahatan Dunia Maya di Indonesia Mengkhawatirkan. Kompas Tekno. [Online]. Tersedia : <http://teknokompas.com/read/2014/10/18/0808000/Kejahatan.Dunia.Maya.di.Indonesia>
- [2] Akamai. (Oktober, 2013). Akamai Releases Second Quarter 2013 'State Of The Internet' Report. [Online] : <http://www.akamai.com/>
- [3] ID-CERT.(Agustus 2013). Incident Handling Report. [Online] . Tersedia : http://www.cert.or.id/incident_handling/penelitian/3/
- [4] B. Raharjo. (Agustus, 2013). Sekilas Mengenai Forensik Digital. Jurnal Sositoteknologi. [Online]. vol. 12 No. 29, p. 384. Tersedia : <http://journals.itb.ac.id/index.php/sostek/article/view/1116/722>.
- [5] K. Franke. (September, 2010). Digital and Computation Forensics, Forensic Lab Testimoni : NISLab. [Online]. Tersedia : <https://sites.google.com/site/testimonlab/>
- [6] A. Lazzez.(January, 2013) . A Survey about Network Forensic Tools. Int. J. Comput. Inf. Technol. [Online]. vol. 2, no. 1, p. 74. Tersedia : <https://www.ijcit.com/archives/volume2/issue1/Paper020110.pdf>
- [7] N. Dietrich. (Desember, 2017). Snort 2.9.8.x on Ubuntu 12, 14, 15. Document Snort. [Online]. Tersedia : <https://www.snort.org/documents>.
- [8] E. K. Dewi. (Januari, 2016). Model, ancaman Keamanan Jaringan Dengan Menggunakan Proses Forensik. Jurnal Maklumatika. [Online] vol. 2, p. 34. Tersedia : <http://maklumatika.uniat.ac.id/post-152-volume-3-no-2-januari-2017.html>
- [9] Snort. (Juni, 2017). Snort. [Online]. Tersedia : <https://www.snort.org/>.
- [10] R. R. Singh and D. S. Tomar. (Februari, 2015). Network Forensics : Detection and Analysis of Stealth Port Scanning Attack. Interantional J. Comput. Netw. Commun. Secur. [Online]. vol. 3, p. 33. Tersedia : http://www.ijcnscs.org/published/volume3/issue2/p2_3-2.pdf