ISSN 2089-1083

EC-Council

Aptikom Wilayah 7
Asosiasi Perguruan Tinggi Informatika & Komputer

Forum Dosen Kota Malang

Co-host:

STMIK primakara

PROSIDING Volume 04

SNATIKA 2017

Seminar Nasional Teknologi Informasi, Komunikasi dan Aplikasinya

Malang, 23 November 2017

diorganisasi oleh:

Lembaga Penelitian dan Pengabdian pada Masyarakat

Sekolah Tinggi Informatika dan Komputer Indonesia

ISSN 2089 – 1083

SNATIKA 2017

Seminar Nasional Teknologi Informasi, Komunikasi dan Aplikasinya
Volume 04, Tahun 2017

SEKRETARIAT
Lembaga Penelitian dan Pengabdian Kepada Masyarakat
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
SNATIKA 2017
Jl. Raya Tidar 100 Malang 65146, Tel. +62-341 560823, Fax. +62-341 562525
Website: snatika.stiki.ac.id
Email: snatika2017@stiki.ac.id

KATA PENGANTAR

Bapak/Ibu/Sdr. Peserta dan Pemakalah SNATIKA 2017 yang saya hormati, pertama-tama saya ucapkan selamat datang atas kehadiran Bapak/Ibu/Sdr, dan tak lupa kami mengucapkan terimakasih atas partisipasi dan peran serta Bapak/Ibu/Sdr dalam kegiatan ini.

SNATIKA 2017 adalah Seminar Nasinal Teknologi Informasi, Komunikasi dan Aplikasinya yang diselenggarakan oleh STIKI Malang bekerjasama dengan EC-COUNCIL, APTIKOM Wilayah 7 dan Forum Dosen Kota Malang serta Perguruan Tinggi selaku Co-host: Universitas Nusantara PGRI Kediri dan STMIK Primakara Denpasar-Bali. Sesuai tujuannya SNATIKA 2017 merupakan sarana bagi peneliti, akademisi dan praktisi untuk mempublikasikan hasil-hasil penelitian, ide-ide terbaru mengenai Teknologi Informasi, Komunikasi dan Aplikasinya. Selain itu sesuai dengan tema yaitu "*Keamanan Informasi untuk Ketahanan Informasi Kota Cerdas*", topik-topik yang diambil disesuaikan dengan kompetensi dasar dari APTIKOM Wilayah 7 yang diharapkan dapat mensinergikan penelitian yang dilakukan oleh para peneliti di bidang Informatika dan Komputer. Semoga acara ini bermanfaat bagi kita semua terutama bagi perkembangan ilmu dan teknologi di bidang teknologi informasi, komunikasi dan aplikasinya.

Akhir kata, kami ucapkan selamat mengikuti seminar, dan semoga kita bisa bertemu kembali pada SNATIKA yang akan datang.

Malang, 20 November 2017
Panitia SNATIKA 2017

Daniel Rudiaman S., S.T, M.Kom

SAMBUTAN KETUA
SEKOLAH TINGGI INFORMATIKA DAN KOMPUTER INDONESIA (STIKI) MALANG

Yang saya hormati peserta Seminar Nasional SNATIKA 2017,

Puji & Syukur kita panjatkan kepada Tuhan Yang Maha Esa, atas terselenggarakannya Seminar Nasional ini sebagai rangkaian kerjasama dengan EC-COUNCIL, APTIKOM Wilayah 7 dan Forum Dosen Kota Malang serta Perguruan Tinggi selaku Co-host: Universitas Nusantara PGRI Kediri dan STMIK Primakara Denpasar-Bali. Kami ucapkan selamat datang kepada peserta Seminar Nasional serta rekan-rekan perguruan tinggi maupun mahasiswa yang telah berpartisipasi aktif sebagai pemakalah maupun peserta dalam kegiatan seminar nasional ini. Konferensi ini merupakan bagian dari 10 Flag APTIKOM untuk meningkatkan kualitas SDM ICT di Indonesia, dimana anggota APTIKOM khususnya harus haus akan ilmu untuk mampu memajukan ICT di Indonesia.

Konferensi ICT bertujuan untuk menjadi forum komunikasi antara peneliti, penggiat, birokrat pemerintah, pengembang sistem, kalangan industri dan seluruh komunitas ICT Indonesia yang ada didalam APTIKOM maupun diluar APTIKOM. Kegiatan ini diharapkan memberikan masukan kepada *stakeholder* ICT di Indonesia, yang meliputi masyarakat, pemerintah, industri dan lainnya, sehingga mampu sebagai penggerak dalam memajukan ICT Internasional.
Akhir kata, semoga forum seperti ini dapat terus dilaksanakan secara periodik sesuai dengan kegiatan tahunan APTIKOM. Dengan demikian kualitas makalah, maupun hasil penelitian dapat semakin meningkat sehingga mampu bersinergi dengan ilmuwan dan praktisi ICT internasional.

Sebagai Ketua STIKI Malang, kami mengucapkan terimakasih kepada semua pihak atas segala bantuan demi suksesnya acara ini.

“Mari Bersama Memajukan ICT Indonesia”

Malang, 20 November 2017
Ketua STIKI,

Dr. Eva Handriyantini, S.Kom, M.MT.

ISSN 2089-1083
SNATIKA 2017, Volume 04

DAFTAR ISI

Meningkatkan Keamanan Jaringan dengan Menggunakan Model Proses Forensik

Ervin Kusuma Dewi[1], Patmi Kasih[2]
[1]Sistem Informasi, Fakultas Teknik, Universitas Nusantara PGRI Kediri
[2]Teknik Informatika, Fakultas Teknik, Universitas Nusantara PGRI Kediri
[1]ervin@unpkediri.ac.id, [2]fatkasih@gmail.com

ABSTRAK

Penggunaan mobile phone yang semakin meningkat dari tahun ke tahun, yang didukung dengan kecepatan data yang terus meningkat membuat teknologi internet terus berkembang. Dampak dari perkembangan technologi internet yaitu penyerangan dan pemerasan seperti yang terjadi pada tahun 2017, yaitu serangan ransomware yang bernama "WannaCry". Serangan "WannaCry" merupakan jenis serangan phishing, yaitu serangan yang memperoleh informasi user, password atau data-data lainya dengan menggunakan website palsu yang menyerupai aslinya. Sebagai pengelola jaringan tentunya harus meningkatkan keamanan jaringan, seringkali yang terjadi ketika terjadi serangan baru melakukan perbaikan, dan tentunya dapat menambah biaya perbaikan. Oleh karena itu, perlunya sebuah metode yang mampu menganalisis ketika terjadi serangan, serta dapat menyimpan mencatat serangan, dan catatan tersebut dapat digunakan sebagai pelaporan. Salah satu metode yang support adalah Model Proses Forensik. Hasil dari penelitan adalah dengan menggunakan menggunakan Model Proses Forensik dapat menganalisis serangan pada log SNORT, data analisis tersebut bisa dijadikan salah satu pembuktian terjadinya serangan, selain itu bisa digunakan sebagai bahan untuk pelaporan kepada pihak berwajib (jika diperlukan). Dari hasil 5 serangan dapat dilakukan analisis, yaitu pukul berapa terjadi serangan, jenis serangan, serta total packet.

Kata Kunci: *Model Proses Forensik, Intrusion Detection System (IDS), SNORT.*

1. Pendahuluan

Penggunaan *mobile phone* yang semakin meningkat dari tahun ke tahun, yang didukung dengan kecepatan data yang terus meningkat membuat teknologi internet terus berkembang. Dengan semakin berkembangnya internet tentu memiliki dampak yang luar biasa, salah satunya adalah dimudahkanya dalam berkomunikasi. Namun di lain sisi juga memiliki kelemahan, seperti pada penyerangan dan pemerasan seperti yang terjadi pada tahun 2017, yaitu serangan ransomware yang bernama "WannaCry" yang menyerang 99 negara. Di Indonesia serangan "WannaCry" dilaporkan mulai menginfeksi system computer di beberapa rumah sakit. Semua data terkunci oleh wannacry dan jika mengingnkan data kembali, pihak rumah sakti harus mengirimkan uang tebusan (Kompas, 2017). Ransomware mengandalkan teknik *phishing* dimana calon korban diminta untuk klik sebuah link atau tautan untuk mengunduh ransomware, missal email atau link yang muncul di sebuah *browser*.

Serangan *phishing* merupakan serangan yang memperoleh informasi *user, password* atau data-data lainya dengan menggunakan website palsu yang menyerupai aslinya. Sebagai pengelola jaringan tentunya harus meningkatkan keamanan jaringan, seringkali yang terjadi ketika terjadi baru melakukan perbaikan, yang tentunya dapat menambah biaya perbaikan. Oleh karena itu, perlunya sebuah metode yang mampu menganalisis ketika terjadi serangan, serta dapat menyimpan mencatat serangan, dan catatan tersebut dapat digunakan sebagai pelaporan. Salah satu metode yang support dengan hal teresebut adalah metode *Network Forensic*.

Network Forensic fokus pada monitoring dan analisis pada trafik jaringan local maupun WAN/nternet untuk pengumpulan informasi, pengumpulan bukti, atau *Instruction Detection* (Mate & Kapse, 2015). Forensik memiliki dua kegunaan, pertama megidentifikasi dengan keamanan, termasuk memeriksa system dan mengenali interupsi atau *alert*. Kedua, mengidentifikasi hasil serangan yang tersimpan dalam log.

Penelitian yang memanfaatkan

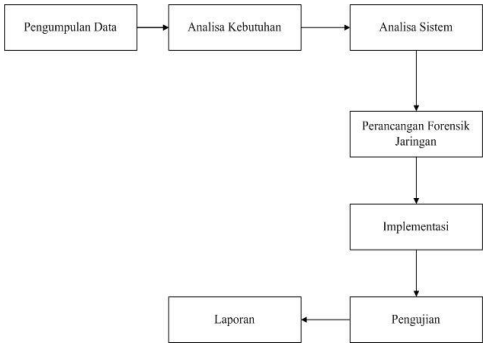
honeyopot yaitu Misra dan Dhir (2012) tentang *Network Forensic* yaitu dengan menggunakan *Honeypots* untuk memikat dan menyerang dengan menggunakan jaringan tipuan. Dengan membuat kerentanan keamanan yang kamlufase, selain itu juga menggunakan NFATs untuk pengumpulan data. Tujuan membangun sistem adalah untuk mengumpulkan data jaringan yang berbahaya dan digunakan untuk penyelidikan lebih lanjut untuk mendapatkan informasi tentang penyerang sebagai bukti *Network Forensic*. Selain itu penelitian yang menggunakan honeypot sebagai salah satu cara yang dapat digunakan sebagai jebakan dalam keamanan jaringan (Nugraha dkk, 2013). Hasil penelitan Misra dan Dhir menunjukkan bahwa teknologi *Honeypot* mudah digunakan, konfigurasi lebih *flexible*, tidak membutuhkan *resource* yang besar.

Dewi (2016) membuat rancangan keamanan jaringan dengan menggunakan pendekatan model proses jaringan, penelitian Dewi berupa konsep dan studi literature untuk membuat keamaan jaringan, sehingga penelitian ini belum di implementasikan.

Perbandingan penelitian penulis dengan penelitian sebelumnya adalah tools yang digunakan, jika penelitian sebelumnya menggunakan honeypot, pada penelitian penulis menggunakan Snort dan Base untuk menganalisis jaringan serta pada pencatatan serangan, Penelitian penulis diharapkan mampu melakukan pencatatan serangan dalam jaringan. Penelitian ini mengembangkan dari penelitian Dewi (2016).

2. Metode Penelitian

Penelitian ini menggunakan pedekatan kuantitatif. Penelitian kuantitatif menurut pendekatan-pendekatan terhadap kajian empiris untuk mengumpulkan, menganalisa, dan menampikan data dalam bentuk numerik. Riset kuantitatif mencoba melakukan pengukuran yang akurat terhadap sesuatu. Lokasi penelitian pada Biro Sistem Informasi (BSI) Kampus Universitas Nusantara PGRI Kediri. Tahapan Penelitian seperti Gambar 1.



Gambar 1. Tahapan Penelitian

Tabel 1 merupakan kebutuhan sitem yang digunakan untuk membangun system. Untuk system operasi server menggunakan Ubuntu versi 16.04, sedangkan system operasi client menggunakan windows 7. Setelah system operasi server terinstall, selanjutnya yaitu melakukan instalasi software yang dibutuhkan salah satunya yaitu SNORT IDS sebagai forensik jaringan.

Tabel 1
Kebutuhan sistem

Kebutuhan	Keterangan
Software	
System Operasi Server	Ubuntu versi 16.04
System Operasi Client	Windows 7
Intrusion Detection System	SNORT IDS Version 2.9.9.0
Tools analysis	Wiresharks
Hardware	
1 Buah PC	Sebagai server IDS SNORT
Min. 10 PC	Sebagai simualsi serangan
Kabel UTP	Sebagai kabel jaringan
1 Buat Switch	Menghubungkan antara komputer

3. Hasil dan Pembahasan

1. Instalasi SNORT

Setelah selesai melakukan instalasi Linux Ubuntu 16.04, langkah selanjutnya yaitu instalasi SNORT. Instalasi sesuai dengan petunjuk pada website SNORT https://www.snort.org/. Gambar 2 merupakan hasil instalasi SNORT. Versi yang berhasil di install yaitu version 2.9.9.0

Gambar 2. Versi SNORT

2. *Setting* dan Konfigurasi SNORT

Tahapan setelah melakukan instalasi SNORT adalah melakukan setting IP. Sebagian dari variable yang digunakan oleh SNORT rules untuk mendeterminasi fungsi system dan lokasi. Log pada SNORT dapat memberikan pilihan kondisi tentang event pada alert. Dari event tersebut kita dapat melihat IP address atau TCP port dari penyerang. Spesifik dari setting IP address pada SNORT seperti Gambar 3.

```
# Step #1: Set the network variables.  For more information, see README.variables
#####################################################

# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.173.1/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET
```

Gambar 3. Setting IP Snort

Ipvar HOME_NET merupakan IP dari PC yang akan kita lindungi. Pada kasus ini yang akan di lindungi adalah server dari universitas Nusantara PGRI Kediri. Namun pada kasus ini sebelum SNORT di fungsikan atau masih dalam uji coba, masih menggunakan Ipvar HOME_NET 192.168.173.1/24. Setelah melewati pengujian, maka untuk Ipvar HOME_NET akan di set IP Server.

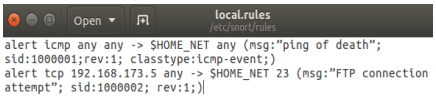
```
# Path to your rules files (this can be a relative path)
# Note for Windows users:  You are advised to make this an absolute path,
# such as:  c:\snort\rules
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

# If you are using reputation preprocessor set these
# Currently there is a bug with relative paths, they are relative to where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars work, BUG 89986
# Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules/iplists
var BLACK_LIST_PATH /etc/snort/rules/iplists
```

Gambar 4. Setting rules snort

Rules digunakan untuk mendeteksi serangan. *Rules* yang di set memberikan *knowledge* pada saat proteksi, sehingga proses inverstigasi sangat tergantung dari *knowledge rule*. Gambar 4 merupakan konfigurasi dari penyimpanan rules, ketika terdapat serangan pada server maka log dari serangan tersebut akan tersimpan pada rule.

Gambar 5 merupakan *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"*.



Gambar 5. Rules snort

3. Analisis Log SNORT

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. *Log* SNORT merupakan hasil dari *Log* yang diambil menggunakan opsi biner, TCPDump, atau *Ethereal*. Salah satu cara untuk membuka *Log* SNORT dengan menggunakan fungsi -r<filename> baik dari SNORT, TCPDump, *Ethereal* atau program lain yang membuat file format libpcap. Gambar 6 merupakan perintah untuk membaca *Log* SNORT.

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

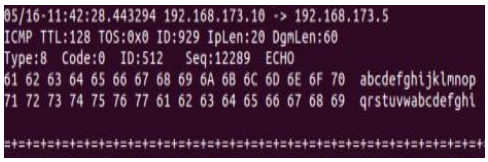
Gambar 6. Membuka Log

Arti dari perintah Gambar 6 yaitu:
d : untuk melihat isi dari paket.
v : untuk melihat header TCP/IP.
r : digunakan untuk membaca file log.

Log yang dapat dibaca adalah *Log* yang tersimpan dalam bentuk libpcap format. SNORT dapat membaca selama yang disimpan dalam *Log* ada binary format dari *sniffer* SNORT. Setelah file *Log* tersebut berhasil diparsing, maka selanjutnya adalah melakukan analisis. Dari hasil uji coba terdapat 5 serangan yang tercapture pada SNORT Log, berikut ini adalah hasil inversitasi 5 serangan tersebut:

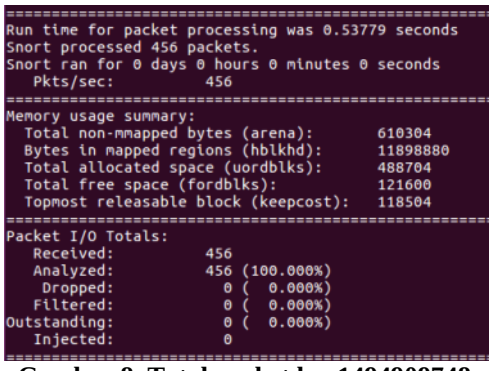
1) log.1494909748

Gambar 7 adalah hasil dari SNORT ditemukan serangan pada pukul 11:42:28 WIB, IP penyerang adalah 192.168.173.10, jenis serangan ICMP dengan Time to Live 128, ID 928, Seq 12545 dan packet 456 pkts/sec.



Gambar 7. Isi dari log. 1494909748

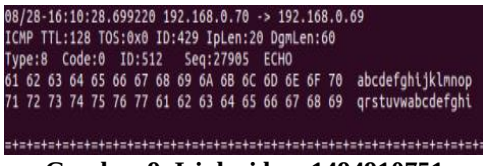
Sedangkan runtime untuk proses packet adalah 0.53779 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 8 merupakan detil dari penggunaan memory serta rincian packet yang diterima.



Gambar 8. Total packet log.1494909748

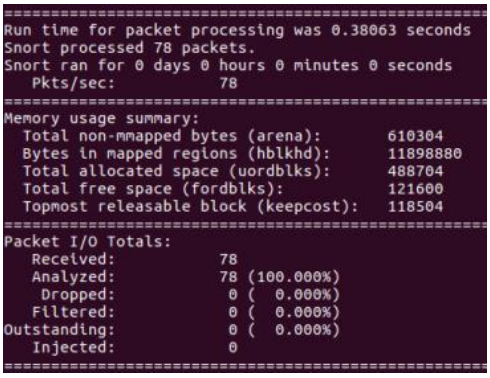
2) log.1494910751

Gambar 9 adalah hasil dari SNORT ditemukan serangan pada pukul 16:10:29 WIB, IP penyerang adalah 192.168.0.70, jenis serangan ICMP dengan Time to Live 128, ID 384, Seq 27905 dan packet 78 pkts/sec.



Gambar 9. Isi dari log. 1494910751

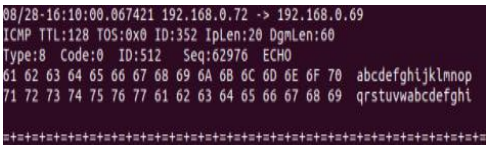
Sedangkan runtime untuk proses packet adalah 0.38063 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 10 merupakan detil dari penggunaan memory serta rincian packet yang diterima.



Gambar 10. Total packet log. 1494910751

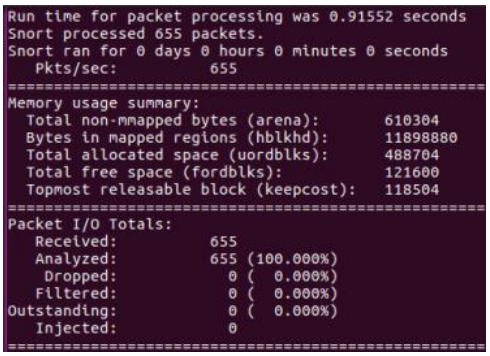
3) log.1501040067

Gambar 11 adalah hasil dari SNORT ditemukan serangan pada pukul 16:10:00 WIB, IP penyerang adalah 192.168.0.72, jenis serangan ICMP dengan Time to Live 128, ID 512, Seq 62976 dan packet 655 pkts/sec.



Gambar 11. Isi dari log.1501040067

Sedangkan runtime untuk proses packet adalah 0.91552 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 12 merupakan detil dari penggunaan memory serta rincian packet yang diterima.



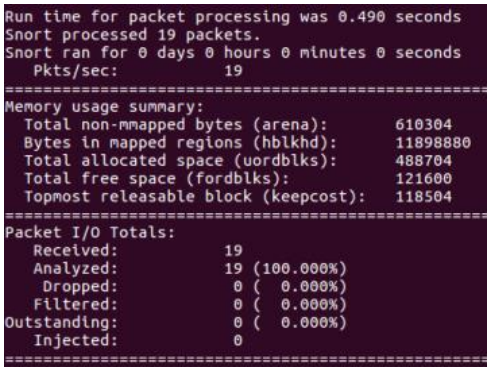
Gambar 12. Total packet log.1501040067

4) log.1503910699

Gambar 13 adalah hasil dari SNORT ditemukan serangan pada pukul 15:58:20 WIB, IP penyerang adalah 192.168.0.96, jenis serangan ICMP dengan Time to Live 128, ID 369, Seq 4096 dan packet 19 pkts/sec.

Gambar 13. Isi dari log.1503910699

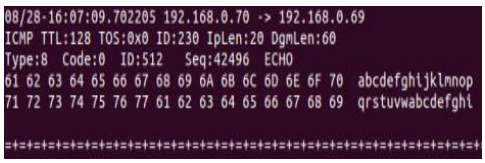
Sedangkan runtime untuk proses packet adalah 0.490 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 14 merupakan detil dari penggunaan memory serta rincian packet yang diterima.



Gambar 14. Total packet log.1503910699

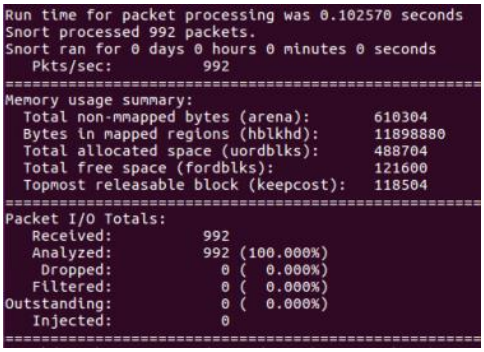
5) log.1503911199

Gambar 15 adalah hasil dari SNORT ditemukan serangan pada pukul 16:07:09 WIB, IP penyerang adalah 192.168.0.70, jenis serangan ICMP dengan Time to Live 128, ID 182, Seq 42496 dan packet 992 pkts/sec.



Gambar 15. Isi dari log.1503910699

Sedangkan runtime untuk proses packet adalah 0.102570 second dengan penggunaan memory sebesar 610.304 bytes. Gambar 16 merupakan detil dari penggunaan memory serta rincian packet yang diterima.



Gambar 16. Total packet log.1503910699

4. Kesimpulan

Berdasarkan dari metode Model Proses Forensik dan implementasi dengan menggunakan tools keamanan jaringan SNORT maka dapat disimpulkan sebagai berikut:

1) Server 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.
2) Menggunakan Model Proses Forensik dapat menganalisis serangan pada *log* SNORT, data analisis tersebut bisa dijadikan salah satu pembuktian terjadinya serangan, selain itu bisa digunakan sebagai bahan untuk pelaporan kepada pihak berwajib (jika diperlukan.)
3) Dari hasil 5 serangan dapat dilakukan analisis, yaitu pukul berapa terjadi serangan, jenis serangan, serta total packet.

5. Referensi

[1] Kompas., 2017., "Jangan Remehkan Ransomware Wannacry". http://tekno.kompas.com/read/2017/05/15/05310067/jangan.remehkan.ransomware.wannacry.

[2] Mate, H.M., Kapse R.S., 2015, “Network Forensic Tool-Concept and Architecture". Fifth International Conference on Communication System and Network Technologies.

[3] Misra, R dan Dhir, R., 2012, Cyber Crime Ivestigation and Network Forensic System Using Honeypot, International Journal of Latest Trends in Engineering and Technology (IJLTET). ISSN : 2278-621X

[4] Nugraha, S, G., Djanali, S., Pratomo, B, A., 2013, Sistem Pendeteksi dan Pencegahan Serangan SQL Injection dengan Penghapusan Nilai Atribut Query SQL dan Honeypot, Jurnal Teknik Poimits Vol. 2, No. 1, ISSN 2337-3539

[5] Dewi, E,K., 2016, Rancangan Keamanan Jaringan Dengan Menggunakan Model Proses Forensik, Jurnal Maklumatika, Vol. 2, No. 2, Januari 2016. ISSN 2407-5043.

[6] Snort. https://www.snort.org/.