PENGAMAN JARINGAN MENGGUNAKAN SISTEM BERBASIS MIKROKONTROLER BERDASARKAN ANALISIS FORENSIK JARINGAN

Abdul Fadlil, Imam Riadi, Sukma Aji
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
Email: fadlil@mti.uad.ac.id

Abstrak *— **Forensik jaringan merupakan ilmu keamanan komputer berkaitan dengan investigasi untuk menemukan sumber serangan pada jaringan berdasarkan bukti log, mengidentifikasi, menganalisis serta merekonstruksi ulang kejadian tersebut. Penelitian forensik jaringan pada penelitian ini dilakukan di Laboratorium Telekomunikasi dan Frekuensi Tinggi Universitas Ahmad Dahlan Yogyakarta. Metode yang digunakan adalah model proses forensik (The Forensic Process Model), yaitu sebuah model proses investigasi forensik digital, yang terdiri dari tahap pengkoleksian, pemeriksaan, analisis pelaporan, dan eksekusi. Penelitian dilakukan dengan mengambil data dari Intrusion Detection System (IDS) Snort. Beberapa file log digabungkan menjadi satu file log, lalu data dibersihkan agar sesuai untuk penelitian. Hasil file log tersebut menjadi acuan sistem berbasis mikrokontroler sebagai pengaman untuk mengeksekusi konektivitas jaringan dengan internet yang berupa pemutusan atau pengalihan IP address server supaya terhindar dari serangan-serangan. Interfacing Mikrokontroler dengan server dilakukan menggunakan kabel USB.***

Kata kunci*— **forensik jaringan, model proses forensik, mikrokontroler***

I. PENDAHULUAN

Metode paling mudah untuk mengatasi serangan jaringan adalah dengan cara memutuskan jaringan untuk sementara waktu atau dengan cara menggunakan 2 atau lebih IP address untuk digunakan bergantian ketika jaringan yang kita akses mendapat serangan. Dengan cara tersebut maka secara otomatis IP address penyerang dengan IP address target terputus sehingga serangan jaringan dapat digagalkan. Namun sebelum menjalankan metode diatas masih perlu dilakukan *Network forensics* (forensik jaringan) pada jaringan IP address Target atau komputer yang akan kita proteksi sehingga aman dari berbagai serangan jaringan.

Network forensics (forensik jaringan) adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan atau masalah kejadian lainnya [1]. Kekuatan dari forensik adalah memungkinkan analisis dan mendapatkan kembali fakta dan kejadian dari lingkungan, karena fakta mungkin saja tersembunyi. Berbeda dari forensik pada umumnya, forensik komputer adalah kegiatan mengumpulkan dan menganalisis data dari berbagai sumber daya komputer [2]. Log yang berasal dari komputer (forensik komputer) adalah log antivirus, log database atau log dari aplikasi yang digunakan.

Forensik jaringan merupakan bagian dari forensik digital, dimana bukti ditangkap dari jaringan dan di interpretasikan berdasarkan pengetahuan dari serangan jaringan. Hal ini bertujuan untuk menemukan penyerang dan merekonstruksi tindakan serangan penyerang melalui analisis bukti penyusupan [3]. Kasus *SQL Injection* terjadi ketika seorang penyerang dapat memasukkan serangkaian pernyataan SQL ke query dengan memanipulasi data input ke aplikasi [4]. Sedangkan pada [5], SQL Injection adalah sebuah metodologi serangan yang menargetkan data yang berada dalam database melalui firewall yang melindungi data tersebut. Forensik jaringan berakar dari keamanan jaringan dan deteksi penyusupan. Forensik jaringan berkaitan dengan perubahan data dari milidetik ke milidetik. Investigasi serangan *cyber* atau penyusupan adalah investigasi forensik jaringan. Tantangan utama yang dihadapi dari forensik jaringan adalah bagaimana caranya mempertahankan bukti kemudian digunakan di pengadilan [6].

Memerangi kejahatan internet telah menjadi porsi utama bagi agen-agen penegak hukum dan intelijen, baik nasional maupun internasional, tak terkecuali para praktisi bisnis, para pelanggan, sampai kepada *end-user*. Umumnya, kejahatan internet dimulai dengan mengekploitasi host-host dan jaringan komputer sehingga para penipu dan penyusup datang melintasi jaringan, terutama jaringan yang berbasiskan protokol *TCP/IP* [7].

Terlepas dari tindakan penegakan hukum, tindakan serangan jaringan dapat diantisipasi untuk mengurangi kerugian-kerugian akibat serangan jaringan tersebut. Baik berupa penyusupan, menghilangkan data, ataupun tindakan ilegal lain yang merugikan banyak pihak.

Tujuan dari penelitian forensik jaringan adalah untuk membuat sistem forensik jaringan yang dapat menganalisis kejadian serangan pada jaringan, menganalisis file log sebagai bukti tindakan illegal terhadap jaringan dan membuat tools pada server forensik jaringan yang akan menganalisis dan mengetahui port yang terbuka, kemudian setelah itu membuat perlindungan terhadap serangan jaringan secara online. Sedangkan manfaat dari penelitian forensik jaringan adalah dapat mengeksekusi hasil forensik jaringan yang telah diketahui dari port yang terbuka, banyaknya IP address yang melakukan

ISBN: 978-602-19568-1-6

penyerangan, port yang digunakan penyerang untuk masuk ke server dan tools yang digunakan oleh penyerang.

Dalam penelitian Ruchandani [3] telah melakukan eksperimen dasar forensik jaringan dengan menangkap lalu lintas paket pada jaringan, menganalisis karakteristiknya, dan mencoba untuk mengetahui aktivitas yang berbahaya dalam membantu mengidentifikasi sumber aktivitas sebagai kerusakan yang dilakukan pada jaringan menggunakan tools *tcp-dump, ethereal*, dan *nmap*. Disimpulkan bahwa *tcp-dump, ethereal*, dan *n-map* sangat ampuh untuk membantu menangkap dan menganalisis paket jaringan diantaranya paket sniffing dan port scanning.

Selanjutnya penelitian [8] membahas tentang *ForNet*, untuk memantau, mengumpulkan dan mempertahankan data untuk mendukung forensik jaringan di internet. *ForNet,* berbeda dari *logger*, menghasilkan ringkasan kompak data mentah jaringan yang dikenal sebagai sinopsis. Sinopsis menangkap informasi yang cukup untuk melakukan otopsi yang efektif. *ForNet* juga menerapkan strategi koleksi terdistribusi.

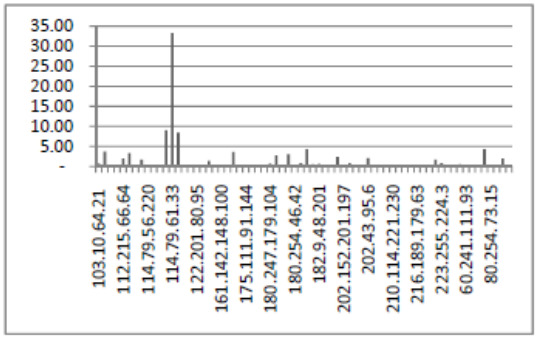
Penelitian [9] membahas tentang sistem logging forensik yaitu *Network Processor* (NP) yang dapat mengumpulkan bukti, melacak perilaku yang mencurigakan dan mengevaluasi tingkat kerusakan mesin yang diserang. Forensik sebagai ilmu keamanan baru yang berkaitan dengan penangkapan, analisis dan rekonstruksi yang bertujuan untuk membuat bukti akurat. Tugas utama dari forensik adalah analisis dan rekonstruksi. Tujuan sistem logging forensik adalah sistem yang memonitor aktivitas server pada kernel dari server sistem operasi, informasi detail pengguna dikumpulkan dari server ke *Network Processor* (NP) dan dikirim ke server forensik (mesin log) dimana terdapat sistem operasi untuk memastikan kontrol akses, dan tersedianya basis data untuk merespon query dari file log disimpan ke server forensik.

Sedangkan penelitian Meghanathan [10] membahas berbagai alat dan teknik yang tersedia untuk melakukan forensik jaringan. Diantara alat yang dibahas adalah *eMailTrackerPro* untuk mengidentifikasi lokasi fisik dari pengirim email, *Web Historian* untuk mengetahui durasi kunjungan masing-masing *upload file* dan *download* dari website yang dikunjungi, *packet sniffers* seperti *ethereal* untuk menangkap dan menganalisis pertukaran data antara komputer yang berbeda di dalam jaringan.

Penelitian [10] juga melakukan review teknik penelusuran IP yang berbeda untuk menandai paket dalam membantu seorang penyelidik forensik mengidentifikasi sumber-sumber serangan dan juga tentang penggunaan *Honeypots* dan *Honeynets*. Dapat disimpulkan untuk mendeteksi semua jenis serangan dan melakukan analisis forensik yang komprehensif, seseorang harus menyebarkan dan menganalisis efektivitas alat komersial dan mengekplorasi alat dan teknik untuk forensik jaringan.

II. FORENSIK JARINGAN

Hasil dari penelitian oleh Resi Utami [11] forensik jaringan dituangkan dalam Gambar 1. Merupakan persentase IP address yang paling banyak melakukan tindakan illegal ke server. Terlihat pada Gambar tersebut persentase tertinggi dimiliki oleh IP 114.79.61.33.



Gambar 1. Persentase penyerang [11]

A. Parsing File Log Pcap

Implementasi dilakukan pada server forensik jaringan yang akan membaca file log yang telah setelah itu, dilakukan analisis terhadap file log tersebut. Guna melihat aliran header paket yang melewati jaringan, lihat Gambar 2.

```
resiutami@resi-laptop:~$ perl parsingpcap.pl |less
Time: 09-11 20:49:11.142797
        IP Address Source: 175.111.91.144
                Mac Address Source: 00144f403975
                Port Numbers: 17379
        IP Address Destination: 10.13.254.43
                Mac Address Destination: 000912053bfc
                Port Numbers: 80
Time: 09-12 23:27:27.381076
        IP Address Source: 180.151.1.68
                Mac Address Source: 00144f403975
                Port Numbers: 45308
        IP Address Destination: 10.13.254.43
                Mac Address Destination: 000912053bfc
                Port Numbers: 80
```

Gambar 2. hasil parsing terhadap file log [11]

B. Port Scanning

Program port scanning merupakan sebuah alat untuk mengetahui port mana saja yang terbuka maupun tertutup pada sebuah server atau host. Cara menjalankannya adalah dengan cara mengetikkan perl portscan.pl lalu ip address sebuah server atau host yang ingin diketahui setelah itu nomot port yang diinginkan (Gambar 2 dan 3).

```
root@resi-laptop:/home/resiutami# perl portscan.pl 175.111.91.159 21-
25
Hasilnya adalah...

Target 175.111.91.159 : Port 21 is closed
Target 175.111.91.159 : Port 22 is open
Target 175.111.91.159 : Port 23 is closed
Target 175.111.91.159 : Port 24 is closed
Target 175.111.91.159 : Port 25 is open
```

Gambar 3. Implementasi port scanning port 21-25 [11]

C. Analisis File Log

Skrip terakhir adalah parsing log dan port scan digunakan untuk menganalisis file log yang telah diambil dari IDS, sehingga bisa menjawab beberapa pertanyaan seputar forensik seperti berapa ip address yang menyerang suatu server, penyerang menggunakan port apa saja untuk memasuki suatu sistem, dan beberapa hal lain yang ingin diketahui. Skrip ketiga ini menggunakan SQLite untuk melakukan analisis terhadap file log. Proses file log menjadi sebuah basis data adalah dengan memanggil skrip

ISBN: 978-602-19568-1-6

pkts2db.pl diikuti dengan membuka file (-read) logfileall.pcap yaitu file log yang akan dieksekusi lalu –d (untuk membuat basis data) dan nama file log basis data yang baru. Gambar 4 menunjukkan perintah sql sebagai scan untuk menemukan host yang menuju ke server target.

```
resiutami@resi-laptop:~$ perl logkedb.pl -r datalog.pcap -d datalog.db
sqlite> select saddr, daddr, count(*) as count
   ...> from ip
   ...> group by saddr, daddr
   ...> order by count desc;
saddr           daddr         count
--------------  ------------  ----------
114.79.61.33    10.13.254.43  778
114.79.60.21    10.13.254.43  212
118.137.85.6    10.13.254.43  197
80.254.66.15    10.13.254.43  101
182.2.136.59    10.13.254.43  99
103.10.64.25    10.13.254.43  86
167.205.134.    10.13.254.43  83
114.79.12.11    10.13.254.43  77
180.254.2.17    10.13.254.43  71
180.247.250.    10.13.254.43  65
202.152.201.    10.13.254.43  54
202.43.95.6     10.13.254.43  47
112.215.66.6    10.13.254.43  46
86.127.220.3    10.13.254.43  45
114.79.54.40    10.13.254.43  39
```

Gambar 4. Host yang mengunjungi situs target [11]

D. Analisis Tool Penyerang

Analisis tool yang digunakan oleh penyerang hanya akan dianalisis beberapa IP address saja. Pada Gambar 5. penyerang dengan IP 182.9.48.201 diketahui berada di Indonesia dengan nama net telkomsel setelah di cek pada arin.net. Setelah di cek menggunakan tshark, tool yang digunakan penyerang adalah Havij. Havij memang cukup sering digunakan untuk *sql injection* (Gambar 6.).

```
sqlite> select  strftime('%Y-%d-%d %H:%M', time) as time, saddr, daddr
   ...> from tcp,ip
   ...> where tcp.id=ip.id and saddr='182.9.48.201';
time              saddr         daddr
----------------  ------------  ------------
2011-23-23 16:11  182.9.48.201  10.13.254.43
2011-23-23 16:11  182.9.48.201  10.13.254.43
2011-23-23 16:11  182.9.48.201  10.13.254.43
```

Gambar 5. IP penyerang pertama [11]

```
182.9.48.201    10.13.254.43    Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij
```

Gambar 6. Penyerang menggunakan Havij [11]

Gambar 7 melukiskan penyerang yang memiliki IP address 114.79.56.220 yang diketahui berada di Indonesia dengan nama net smartaitelekom. Penyerang tersebut menggunakan sqlmap (gambar 8) untuk melakukan penyerangan ke server.

```
sqlite> select  strftime('%Y-%d-%d %H:%M', time) as time, saddr, daddr
   ...> from tcp,ip
   ...> where tcp.id=ip.id and saddr='182.9.48.201';
time              saddr         daddr
----------------  ------------  ------------
2011-23-23 16:11  182.9.48.201  10.13.254.43
2011-23-23 16:11  182.9.48.201  10.13.254.43
2011-23-23 16:11  182.9.48.201  10.13.254.43
```

Gambar 7. IP penyerang kedua [11]

```
182.9.48.201    10.13.254.43    Mozilla/4.0 (compatible; MSIE 7.0;
Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij
```

Gambar 8. Penyerang menggunakan sqlmap [11]

Untuk penyerang terakhir dengan IP address 86.127.220.36, yang setelah ditelusuri berada di benua Eropa, tepatnya di Romania dari *Universitatea Petre Andrei.* Ternyata memang sering melakukan tindakan illegal hacking, pelanggaran, spam dan sebagainya (Gambar 9).

```
sqlite> select  strftime('%Y-%d-%d %H:%M', time) as time, saddr, daddr
   ...> from tcp,ip
   ...> where tcp.id=ip.id and saddr='86.127.220.36';
time              saddr         daddr
----------------  ------------  ------------
2012-20-20 18:57  86.127.220.36  10.13.254.43
2012-20-20 18:57  86.127.220.36  10.13.254.43
2012-20-20 18:57  86.127.220.36  10.13.254.43
```

Gambar 9. Penyerang dari Eropa [11]

```
86.127.220.36   10.13.254.43    Python-urllib/2.7
86.127.220.36   10.13.254.43    Python-urllib/2.7
```

Gambar 10. Penyerang menggunakan Python [11]

Setelah dicek ternyata penyerang tersebut menggunakan skrip Python untuk mencari isi konten pada sebuah artikel di website target (Gambar 10).

E. Laporan Hasil Investigasi Forensik Jaringan

Investigasi forensik jaringan dilakukan untuk mengetahui apa saja yang terjadi pada jaringan sehingga dapat ditelusuri jejak-jejak dari penyerang. Pencarian jejak dari tindakan illegal pada jaringan di dapat dari file log. Pada penelitian forensik jaringan di server target dilakukan dengan mengambil data pada IDS Snort yang merupakan sistem pendeteksi penyusup pada jaringan. Pada IDS Snort terdapat beberapa aturan (rule) yang digunakan dalam mendeteksi penyusup pada jaringan, aturan tersebut dipakai oleh server dalam mendeteksi serangan yang terjadi.

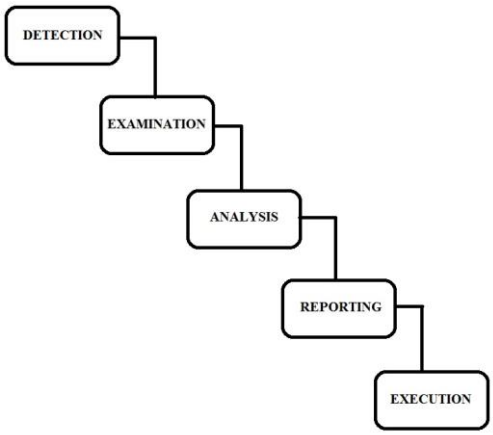
Investigator forensik jaringan melakukan dengan membangun suatu server forensik jaringan yang terhubung ke core switch server tetapi tidak terhubung ke server IDS. Sehingga pengambilan data dilakukan secara online dan analisis dilakukan secara offline. Pada server forensik jaringan digunakan script perl untuk menganalisis kejadian, script parsing pcap untuk memecah file log berdasarkan waktu, ip, mac address dan port, script port scanning untuk mengetahui port yang terbuka pada suatu server dan script untuk analisis file log dengan SQLite. Kegunaan script port scan, biasanya apabila penyerang telah berhasil masuk ke suatu sistem dengan cara SQL Injection atau mengekploitasi kelemahan web dengan basis data, penyerang akan melakukan port scan untuk mengetahui port mana saja yang terbuka. Sedangkan script SQLite sebagai alat untuk menganalisis file log sesuai dengan perintah sql yang kita masukkan. Ketiga script tersebut diletakkan pada server forensik jaringan beserta dengan modul yang digunakan.

Penelitian di server dilakukan investigator forensik jaringan selama lima bulan dan telah menghasilkan file log sebesar 13MB yang telah digabung (*merged*) dan dibersihkan (*cleaning*). Dengan adanya penelitian forensik jaringan di server dapat diharapkan agar dapat menjadi kesadaran bahwa cukup sulit untuk melindungi sebuah jaringan dari tindakan serangan karena yang bisa dilakukan adalah mencegahnya agar kejadian tersebut tidak terulang kembali atau diminimalisir kerusakan akibat dari serangan tersebut.

ISBN: 978-602-19568-1-6

II. METODE PENELITIAN

Metodologi yang digunakan dalam penelitian ini adalah model proses forensik (*The Forensic Process Model*) yang dilukiskan oleh Gambar 11.



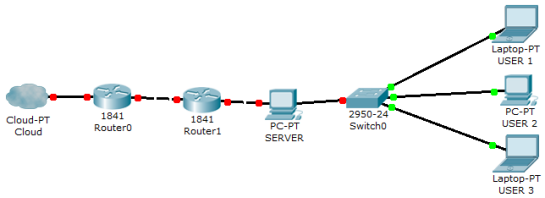
Gambar 11. Model proses Forensik [12]

Tahapan penelitian pada gambar yaitu:

1. Tahap Pengkoleksian (*Collection*): Pada tahap ini yang dilakukan meneliti dan mencari bukti-bukti, pengenalan terhadap bukti-bukti penyusupan, dan pengumpulan bukti. Sistem IDS Snort digunakan untuk mendeteksi serangan. Pada Snort terdapat aturan yang mengekstrak ciri dari paket yang melewati jaringan, sehingga jika ada paket yang mencurigakan dan sesuai dengan aturan lalu mengirimkan pesan alert dan menyimpannya sebagai log.
2. Tahap Pemeriksaan (*Examination*): Pada tahap ini, pencarian informasi yang tersembunyi dan mengungkapkan dokumentasi yang relevan. Pemeriksaan dilakukan pada file log yang telah diambil menggunakan IDS Snort. Setelah log tersimpan sebagai alert, maka log diteliti dan diperiksa. Misalnya memeriksa urutan paket.
3. Tahap analisis (*Analysis*): Telihat pada hasil pemeriksaan untuk nilai pembuktian pada kasus yang ada. Tahap ini digunakan untuk menjawab pertanyaan forensik yaitu serangan **apa** yang terjadi, IP **siapa** yang melakukan serangan, **kapan** serangan itu terjadi, **dimana** serangan itu terjadi, **bagaimana** serangan tersebut bisa terjadi, dan **mengapa** itu terjadi.
4. Tahap pelaporan (*Reporting*): Penulisan laporan mengenai proses pemeriksaan dan data yang diperoleh dari semua penyelidikan. Untuk membuat laporan tentang serangan yang terjadi pada jaringan dari hasil analisis bukti log dan setelah itu dilakukan rekontruksi aliran data dari kejadian tersebut. Tentunya tidak merusak log yang sudah ada.
5. Tahap Tindakan (Execution): Pada tahap ini, hasil alert yang dikirimkan oleh Sistem IDS Snort digunakan untuk memutus jaringan sementara selama kurun waktu tertentu yang dilakukan oeh mikrokontroler sebagai langkah perlindungan secara langsung.

A. Analisis Sistem

Topologi Jaringan Komputer Laboratorium Telekomunikasi dan Frekuensi Tinggi Universitas Ahmad Dahlan (JKLTFT UAD) Yogyakarta adalah distributed (tersebar), pengembangan dari topologi star. Jaringan Komputer Laboratorium Telekomunikasi dan Frekuensi Tinggi Universitas Ahmad Dahlan Yogyakarta menjadi pusat jaringan sekaligus pembagi *bandwitdh* dari tiap-tiap client.

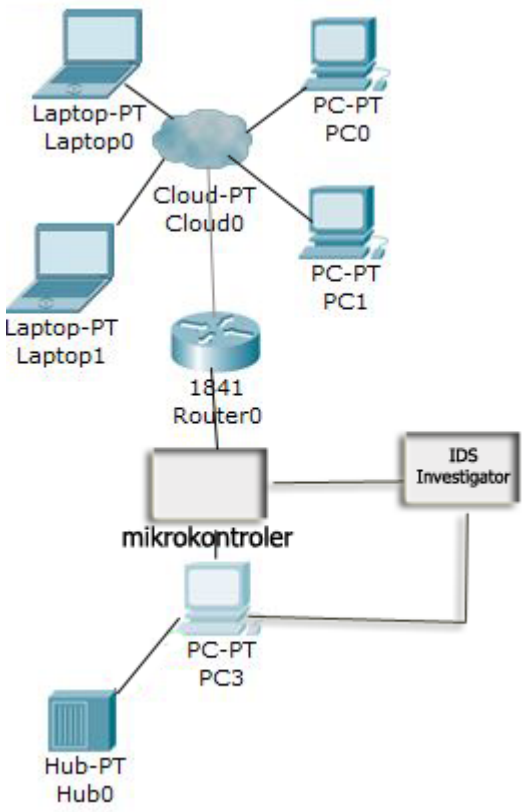


Gambar 12. Topologi Jaringan Komputer Laboratorium Telekomunikasi dan Frekuensi Tinggi Universitas Ahmad Dahlan Yogyakarta

B. Rancangan Server Forensik Jaringan

Rancangan sistem pada penelitian forensik jaringan adalah arsitektur forensik jaringan seperti ditunjukkan gambar yang merupakan arsitektur forensik jaringan yang dibangun di JKLTFT UAD Yogyakarta. User yang ingin mengakses server yang ada di JKLTFT UAD melewati switch terlebih dahulu lalu masuk ke server. Server IDS diletakkan sejajar dengan core switch dengan *port mirroring* lalu dilihat melalui PC administrator lalu data tersebut diambil dengan harddisk.

ISBN: 978-602-19568-1-6



Gambar 13. Arsitektur forensik jaringan

B. *Rancangan Penelitian*

Pada rancangan penelitian (Gambar 13) yang bertindak sebagai admin adalah server JKLTFT UAD Yogyakarta sedangkan investigator forensik jaringan adalah peneliti forensik jaringan di JKLTFT UAD Yogyakarta. Penelitian forensik jaringan dimulai dengan mempersiapkan tool yang akan digunakan untuk penelitian, IDS Snort untuk mendeteksi penyusup pada jaringan dan script Perl untuk menganalisis paket yang ditangkap oleh Snort. Pada Snort telah dimasukan aturan sebagai pendeteksi pola pada jaringan, aturan yang digunakan pada *Snort* adalah aturan yang digunakan pada tempat penelitian di JKLTFT UAD Yogyakarta telah disesuaikan yang sering terjadi. Ketika terjadi serangan jaringan, IDS Snort akan memerintahkan Mikrokontroler untuk mengeksekusi serangan berupa pemutusan jaringan dan mengalihkan IP address awal ke IP addres Opsional.

C. *Implementasi*

Penelitian forensik jaringan ini menggunakan server *virtual machine* yang disediakan oleh administrator JKLTFT UAD Yogyakarta kepada investigator forensik jaringan. Server ini menggunakan ip statik 172.10.201.2 yang diakses melalui jaringan Universitas Ahmad Dahlan. Remote server dapat dihubungi dengan menggunakan protokol ssh pada port 22 sehingga proses komunikasi menjadi lebih aman karena terenkripsi, dibanding protokol telnet atau protokol lainnya yang sejenis.

Algoritma Parsing Pcap

Adapun algoritma untuk memparsing hasil log file adalah sebagai berikut.

1. Membaca file log dalam bentuk pcap.
2. Menggunakan modul untuk membaca file pcap
3. Modul yang digunakan adalah tcpdumplog.pm, Ethernet.pm, ip.pm, tcp.pm, stricts, warnings dan diagnostics.
4. Pendefinisian variabel verbose, pcap_in, file_out, dir, dump_range, lookup, dan help sebagai pilihan input.
5. Lakukan pengulangan dalam membaca masing-masing variabel
6. Tampilkan parsing

Algoritma Port Scanning

Adapun langkah-langkah algoritma yang digunakan adalah:

1. Menggunakan modul socket untuk mendeteksi keberadaan port.
2. Pendefinisian variabel yang akan menampilkan host, server dan port.
3. Menampilkan hasil pencarian port yang terbuka maupun yang tertutup.

Algoritma untuk Analisis File Log

Algoritma yang digunakan adalah sebagai berikut.

1. Menggunakan modul CPAN.
2. Mendeklarasikan variabel yang digunakan.
3. Opsi untuk membaca file log pcap ke file database.
4. Membuka file untuk menyimpan header field.
5. Membaca dan memprose file pcap.
6. Sub routine untuk memproses masing-masing paket.
7. Membuat tabel IP, TCP, UDP dan ICMP.

III. HASIL DAN PEMBAHASAN

Hasil penelitian tersebut, dioptimalkan dengan membuat eksekusi dari hasil forensik jaringan menggunakan sistem berbasis mikrokontroler untuk mengantisipasi berbagai macam bentuk serangan yang sudah ada pada file log menggunakan Delphi sebagai pemberi informasi kepada mikrokontroler. Kemudian perintah tersebut dieksekusi oleh mikrokontroler untuk memutus dan mengalihkan jaringan ke IP address lain yang sudah ditentukan, sehingga tidak terjadi dampak yang merugikan pengguna ketika sedang mengakses jaringan.

IV. KESIMPULAN

Setelah dilakukan penelitian, maka dapat disimpulkan sebagai berikut:

1. Sistem forensik jaringan yang dirancang merupakan sebuah alat untuk menganalisis bukti dari file log. Sistem forensik jaringan diletakkan pada server forensik jaringan yang terhubung dengan *core switch* dan memiliki IP statik 10.13.253.36. Sistem tersebut terdiri dari skrip *parsing pcap*, skrip *port scanning* dan skrip untuk merubah *file log* ke *database*.
2. Dari hasil analisis data log serangan *SQL Injection* yang menuju ke server, serangan dilakukan kebanyakan menggunakan tools eperti *Havij* dan *SQLMap*. Selain

ISBN: 978-602-19568-1-6

itu, ada yang menggunakan skrip Python yaitu berasal dari benua Eropa, tepatnya di Romania.

3. Tools yang dibuat adalah parsing pcap yang dapat memecah file log dalam bentuk pcap berdasarkan tanggal, IP address, mac address dan nomor port, sedangkan tools kedua yaitu port scanning yang dapat mengetahui port yang terbuka maupun yang tertutup pada suatu host atau server, dan yang terakhir adalah tools untuk mengubah file log pcap ke bentuk database sehingga data log bisa dianalisis secara lebih mendalam.
4. Sistem Berbasis Mikroprosesor mungkin untuk diaplikasikan sebagai tool pengaman jaringan.

DAFTAR PUSTAKA

[1] Singh, O., 2009. *Network Forensics*. Indian Computer Response Team (CERT-In) Department of Information Technology, New Delhi, India.

[2] Sulianta, F., 2008, *Komputer Forensik*. Jakarta : PT. Elex Media Komputindo.

[3] Ruchandani, B., Kumar, M., Kumar, A., Kumari, K., Sinha., A.,K., 2006, Ekperimentation
In Network Forensics Analysis. *Proceedings of the Term Paper Series under CDACCNIE Bangalore*, India, December 2006.

[4] Anley, C., 2002, Advanced SQL Injection in SQL Server Applications. *An NGSSoftware Insight Security Research (NISR) Publications*: Next Generation Security Software Ltd.

[5] Anonymous, 2011, Ethical Hacking. EC-Council.

[6] Volonino, L. and Reynaldo A., 2008, *Computer Forensics For Dummies*. Indianapolis, Indiana : Wiley Publishing, Inc.

[7] Rafiudin, R., 2009, *Investigasi Sumber-sumber Kejahatan Internet: Internet Forensik*.Yogyakarta : Penerbit Andi.

[8] Shanmugasundaram, K., 2005, *ForNet: A Distributed Forensic Network*. Polytechnic University.

[9] Park, T.K., Ra, I., 2008. Design and Evaluation of A Network Forensic Logging system. *International Conference on Convergence and Hybrid Information Technology*. Third 2008 IEEE.

[10] Meghanathan, N., Allam, S., R., Moore, L., A., 2009. Tools and Techniques For NetworkForensics. *International Journal of Network Security & ItsApplications (IJNSA)*, Volume .1, No.1,April 2009 14.

[11] Resi Utami Putri, Jazi Eko Istiyanto (2012). Analisis Forensik Jaringan Studi Kasus Serangan *SQL Injection* pada Server Universitas Gadjah Mada. *Jurnal UGM*, Vol.6, No.2, Juli 2012, 101~112

[12] Baryamureeba,V., Tushabe, F., 2004, The Enhanced Digital Investigation Process Model. *Proceedings of the Fourth Digital Forensic Research Workshop*, May 27.

ISBN: 978-602-19568-1-6