RANCANGAN KEAMANAN JARINGAN DENGAN MENGGUNAKAN MODEL PROSES FORENSIK

Ervin Kusuma Dewi
Program Studi Sistem Informasi, Universitas Nusantara PGRI Kediri
Jl. KH Ahmad Dahlan No. 76 Kediri, Jawa Timur
Email: ervin.kusumadewi3@gmail.com

Abstrak

Banyaknya penggunaan *internet* dapat menimbulkan masalah, mulai dari kasus perbuatan tidak menyenangkan hingga kejahatan (*fraud*). Berdasarkan statistik yang dikeluarkan oleh ID-CERT (2012) menunjukkan masalah keamanan (*security*) berupa serangan melalui jaringan (*network attack*) termasuk perusakan situs web (*deface*), penerobosan hak akses, virus atau malware, *phising*, dan *fraud*. Serangan melalui jaringan dapat di analisis dengan menggunakan Model Proses Forensik karena Model Proses Forensik adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan. Pada paper ini dibahas mengenai rancangan keamanan jaringan Universitas Nusantara PGRI Kediri, rancangan pengambilan data akan dilakukan dengan menggunakan *Tools Instruction Detection System* (IDS) *Snort*. Rancangan *server* IDS *Snort* akan diletakkan di *Switch Core Server*, sehingga dapat melakukan analisa aktifitas jaringan. Rancangan pelaporan awal dengan cara menggunakan notifikasi melalu jejaring sosial (whatsapp), sehingga ketika terjadi serangan, maka *server* akan mengirimkan *alert* melalui *mobile phone*. Penelitian ini masih berupa rancangan yang nantinya akan dijadikan sebagai acuan penelitian selanjutnya.

Kata kunci : *Network Forensic, Instrution Detection System(IDS), Snort, Rancangan Keamanan.*

I. PENDAHULUAN

1.1. Latar Belakang

Perkembangan *internet* begitu cepat serta memudahkan pengguna sehingga mengubah pelayanan traditional menjadi menjadi layanan yang berbasis internet (*internet based*) seperti, *banking*, transportasi, *medicine*, pendidikan dan lainya. Dengan internet semua menjadi dimudahkan sehingga membuat ketergantungan internet. Berdasarkan statistik dari Asosiasi Penyelenggara Jasa Internet (APJII, 2012), jumlah pengguna internet Indonesia saat ini mencapai 63 juta orang.

Banyaknya pengguna *internet* dapat menimbulkan masalah, mulai dari kasus perbuatan yang tidak menyenangkan hingga terjadi kejahatan (*fraud*). Berdasarkan statistik yang dikeluarkan oleh ID-CERT menunjukkan masalah keamanan (*security*) berupa serangan melalui jaringan (*network attack*) termasuk perusakan situs web (*deface*), penerobosan hak akses, virus atau malware, *phising*, dan *fraud* (ID-CERT, 2012).

Kejahatan-kejahatan tersebut dapat dicegah dengan menggunakan metode Model Proses Forensik karena Model Proses Forensik adalah kegiatan menangkap, mencatat dan menganalisis kejadian pada jaringan untuk menemukan sumber serangan keamanan atau malasah kejadian lainya (Singh, 2009). Kekuatan forensik ada pada pengumpulan dan menganalisis data dari berbagai sumber daya komputer seperti *log* antivirus, *log database* atau *log* dari aplikasi yang digunakan (Sulianta, 2008). Sistem pendeteksi serangan dapat menggunakan tools *Instrusion Detection System* (IDS) Snort. *Snort* merupakan IDS yang berbasis *open source*. Pada Model Proses Forensik, Snort digunakan untuk menganalisis semua lalu lintas jaringan untuk menyadap dan mencari jenis penyusupan dalam sebuah jaringan.

Universitas Nusantara (UN) PGRI Kediri memiliki jaringan yang luas, sehingga rentan terhadap serangan jaringan. Penelitian dilakukan pada Biro Sistem Informasi (BSI) yang merupakan pusat jaringan di UN PGRI. Sejauh ini belum terdapat sistem keamanan yang dapat melakukan analisis,

sehingga serangan yang terjadi dapat bedampak fatal pada server. Tujuan dari penelitian ini adalah membuat rancangan keamanan jaringan yang dapat menganalisis kejadian serangan pada jaringan dengan menggunakan Model Proses Forensik serta sistem yang mampu mengirimkan notifikasi melalui *mobile phone* administrator ketika terjadi serangan sehingga serangan tersebut dapat segera diatasi.

1.2. Rumusan Masalah

Berdasarkan latar belakangan yang sudah di paparkan, maka rumusan masalah dalam penelitian kali ini sebagai berikut :

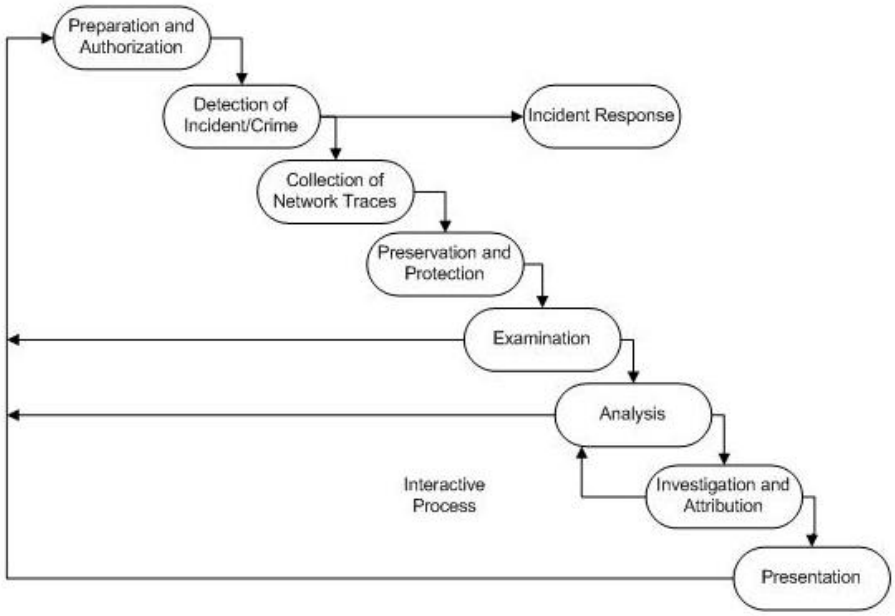
1. Bagaimana membuat rancangan dan analisa server dengan menggunakan Model Proses Forensik jaringan sebagai bukti bahwa telah terjadi serangan pada *server* UN PGRI Kediri ?
2. Bagaimana membuat racangan pelaporan serangan ?
3. Bagaimana membuat notifikasi ketika terjadi serangan *server* melalui *mobile phone* ?

2. METODE PENELITIAN

Metodologi yang dugunakan adalah Model Proses Forensik (*The Forensic Process Model*) yang ditunjukkan pada diagram alir Gambar 1. Tahapan penelitian pada Gambar 1 yaitu (Lazzez, 2013) :

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

   Network Forensik bisa diterapkan jika dimana *network security tools* seperi sistem deteksi instrusi, *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.



Gambar 1. Diagram Alir Penelitian (Lazzez, 2013).

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 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 :
   a. Serangan apa yang terjadi?
   b. IP siapa yang melakukan serangan?
   c. Kapan serangan terjadi?
   d. Dimana serangan itu terjadi?
   e. Bagaimana serangan tersebut bisa terjadi?
   f. 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.

3. HASIL DAN PEMBAHASAN

Beberapa penelitian terkait forensik jaringan antara lain, Kausik dan Joshi (2010) melakukan forensik jaringan untuk serangan *Internet Control Message Protocol* (ICMP). Selain itu Kausik dan Joshi (2010) mengusulkan Model Sistem Forensik untuk ICMP untuk mengumpulkan data jaringan, mengidentifikasi paket yang mencurigakan, memeriksa protokol dan validasi serangan. Untuk mengatasi jumlah data yang besar akan diperiksa maka hanya digunakan informasi header paket ICMP

saja dengan format paket *capture*: libcap dan ekstensi file pcap. Eksperimen dilakukan menggunakan nmap, sing dan tracerote.

Pomeroy dan Tan (2011) membahas mengenai perekaman jaringan yang memberikan solusi untuk mendeteksi serangan dan mengungkap serangan web. Pomeroy dan Tan juga menjelaskan cara meningkatkan rekostruksi serangan web adalah memahami dan memperbaiki kelamahan aplikasi web. Penelitianya juga mengulas bahwa firewall tidak efektif untuk memblokir lalu lintas sedangkan IDS(*Instruction Detection System*) mampu melakukan perekaman aplikasi jaringan yang dapat meningkatkan efektifitas dalam rekonstruksi serangan *SQL Injection.*

Putri dan Istiyanto (2012) meneliti serangan *SQL Injection* dengan menggunakan model proses forensik (*The Forensic Process Model*). Pengambilan data dengan menggunakan IDS (*Instruction Detection System*) Snort. Dari hasil analisis data log serangan *SQL Injection* yang menuju ke server Universitas Gadjah Mada (www.ugm.ac.id), serangan dilakukan kebanyakan menggunakan *tools* seperti Havij dan SQL Map. Selain itu, ada yang menggunakan skrip Python yang berasal dari benua eropa, tepatnya diromalia. *Tools* yang dibuat adalah parsing pcap yang dapat mencegah *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 *tools* untuk mengubah *file log* pcap ke bentuk database sehingga data *log* bisa dianalisis secara lebih mandalam

Mahrouqi dkk (2014) membuat simulasi serangan *SQL Injection* dengan menggunakan GNS3(*Graphic Network Simulator).* Tujuan utama penelitianya adalah merancang serangan virtual network untuk mebuat sandbox yang memungkinkan untuk melakukan eksperimen yang tidak mengeluarkan biaya besar. Hasil dari penelitiannya digunakan sebagai rekomendasi dalam infrastruktur TI yang menguji website dengan menggunakan serangan *SQL Injection*. Untuk mensimulasikan skenario serangan dengan menggunakan *tools open source* GNS3, Oracle VM Virtual Box, VMWare Workstation. Selain itu juga menggunakan *tools* Whireshark untuk menganalisis aktifitas jaringan.

Perbandingan penelitian penulis dengan penelitian sebelumnya adalah pada pencatatan serangan, jika penelitian sebelumnya hanya serangan *SQL Injection* saja yang di catatat, sedangkan penelitian penulis mampu melakukan pencatatan serangan selain *SQL Injection*. Selain itu pada racangan penulis juga menambahkan notifikasi serangan, sehingga ketika terjadi serangan maka administrator BSI akan mendapatkan notifikasi melalui *mobile phone*, manfaat dari sistem notifikasi adalah dengan adanya notifikasi agar segera melakukan tindakan untuk menghentikan serangan.

3.1. Analisis Kebutuhan

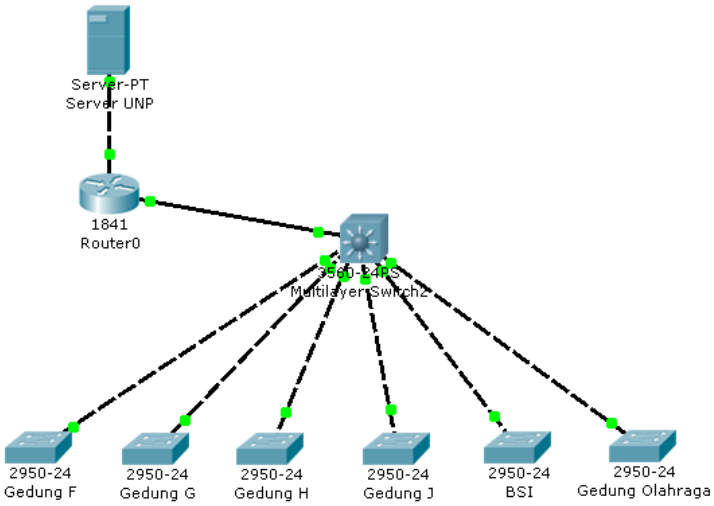
Alat dan bahan yang dibutuhkan untuk melakukan keamanan dengan menggunakan Model Proses Forensik :

1. Satu buah komputer sebagai IDS Snort Server
2. *Tools* IDS Snort
3. *Tools* Wireshark
4. OS Linux(Ubuntu) atau OS Windows 7
5. Tempat penelitian di Bina Sarana Informatika(BSI) Universitas Nusantara PGRI Kediri
6. PHP sebagai bahasa pemrograman dan MySQL sebagai database yang digunakan untuk menyimpan data serangan.
7. API Jejaring Sosial sebagai media notifikasi

3.2. Analisis Sistem

Jaringan intranet Universitas Nusantara PGRI adalah jaringan yang menghubungkan komputer-komputer yang tersebar dilingkungan kampus Universitas Nusantara PGRI baik yang terhubung secara *Local Area Network* (LAN). Pusat jaringan intranet terletak pada Biro Sarana Informasi (BSI). Topologi jaringan Universitas Nusantara PGRI Kediri adalah pengembangan dari topologi *star*, dimana beban kinerja dari *server* sebagai penyedia layanan terbesar sehingga data dapat diakses. Akses jaringan Dosen, karyawan, dan mahasiswa menggunakan *user* dan *password* yang diberikan

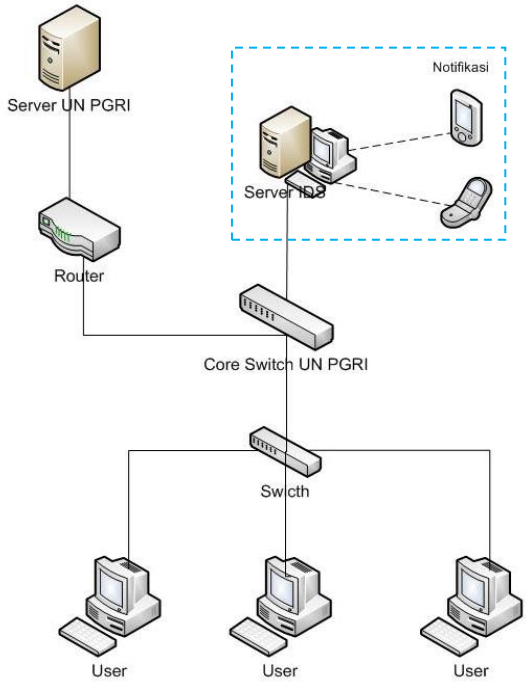
oleh admin. Kondisi jaringan pada kondisi waktu tertentu *traffic* dari penggunaan jaringan meningkat. Peningkatan tersebut seiring dengan bertambahnya pengguna (*user*) seperti mahasiswa, dosen, dan karyawan yang aktif dan mengakses data secara bersamaan. Gambar 2 merupakan topologi jaringan komputer UN PGRI Kediri.



Gambar 2. Topologi jaringan UN PGRI Kampus 1.

3.3. Rancangan Forensik Jaringan

Berdasarkan Gambar 2, belum terdapat sebuah *server* yang digunakan untuk keamanan jaringan. Sejauh ini, analisis serangan belum terdapat pada jaringan UN PGRI, jika terjadi perusakan oleh penyerang, mencoba untuk melakukan perbaikan, belum terdapat sistem *server* yang bisa mengidentifikasi penyerangan sehingga dirancangan keamanan jaringan seperti Gambar 3.

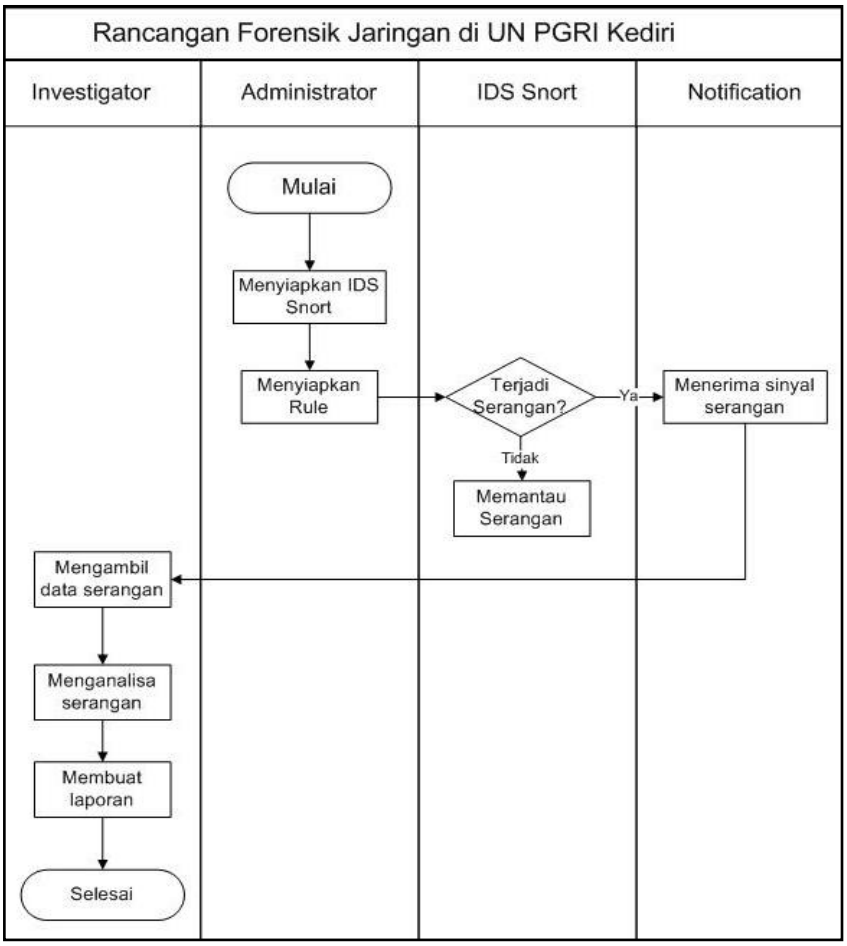


Gambar 3. Rancangan IDS Server

Pada rancangan akan ditambahkan sebuah *server* IDS Snort. *Server* IDS diletakan sejajar dengan *core switch* sehingga *user* yang akan mengakses *server* akan melewati *core Switch* sehingga dapat

dipantau oleh *server* IDS Snort. Ketika terjadi serangan, terdapat notifikasi ke administrator melalui jejaring sosial yang terhubung melalui *mobile phone* administrator BSI UN PGRI. Pada rancangan akan ditambahkan sebuah server IDS Snort. *Server* IDS diletakan sejajar dengan *core switch* sehingga *user* yang akan mengakses *server* akan melewati *core Switch* sehingga dapat dipantau oleh *server* IDS Snort. Ketika terjadi serangan, terdapat notifikasi ke administrator melalui jejaring *social* yang terhubung melalui *mobile phone* administrator BSI UN PGRI.

Gambar 4 merupakan alur yang akan dikerjakan untuk rancangan forensik jaringan pada UN PGRI Kediri, diawali dengan menyiapkan *server* yang diinstall *Snort*, *server* ini diletakkan diantara *server* UN PGRI seperti Gambar 3. Setelah selesai melakukan *install Snort* dan melakukan *troubleshooting*, maka melakukan konfigurasi untuk akses ke *mobile phone* melalui jejaring *social* (whatsapp) melalui API. Konfigurasi ini dilakukan dengan membuat *script* PHP dan terhubung dengan database sebagai media penyimpanan serangan. *Script* PHP juga terhubung dengan API untuk menjalankan notifikasi ke jejaring sosial, konfigurasi ini dilakukan agar terintergrasi dengan *server* IDS *Snort*, dan jika terjadi serangan maka secara otomatis akan memberikan notifikasi.

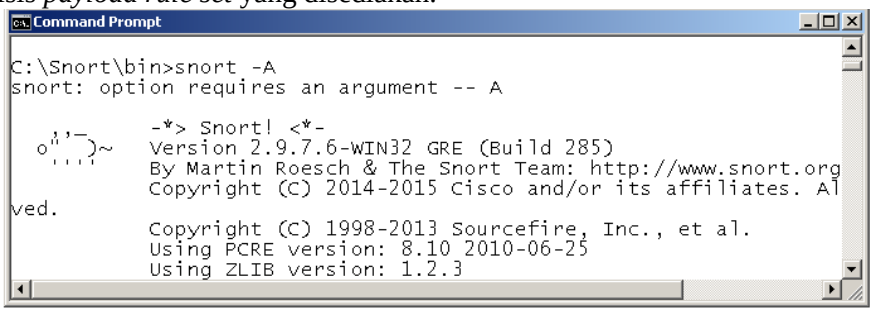


Gambar 4. Rancangan Forensik jaringan

3.4. Tools IDS

Pada peracangan pendeteksi serangan pada server menggunakan *tools Intrution Detection System* (IDS). IDS adalah sistem perangkat lunak (*software*) dan perangkat keras (*hadrware*) yang mengotomatisasi proses deteksi serangan**.** Deteksi serangan bisa menggunakan tools IDS *Snort*. *Snort* (Roesch, 1999) adalah perangkat lunak IDS dan NIDS berbasis *open source* dan banyak digunakan untuk mengamankan sebuah jaringan dari aktifitas yang berbahaya.

Cara kerja *Snort* mirip dengan *TcpDump*, tetapi lebih fokus sebagai *security* packet *sniffing*. Fitur Utama *Snort* yang membedakan dengan *TcpDump* adalah *payload inspection*, dimana *Snort* melakukan analisis *payload rule set* yang disediakan.



Gambar 5. Snort pada windows

Selain itu cara kerja *Snort* menganalisa paket data yang ada di dalam jaringan dengan melakukan *capture* dan membuat *log* berdasarkan ciri yang ada di dalam *database engine* pendeteksi. *Snort* data diinstall di sistem operasi berbasis *Linux* maupun sistem operasi *windows* seperti pada Gambar 5.

Snort memiliki *rule* yang digunakan untuk *knowledge base* dalam deteksi :

1. *Pass* : Rule ini akan melakukan drop terhadap paket yang cocok dengan pola deteksi.
2. *Log* : menulis paket secara rutin pada pencatatan log yang telah didefinisikan oleh *user* di awal *run time*.
3. *Alert* : Menghasilkan sebuah even notifikasi menggunakan metode yang telah ditentukan oleh pengguna *command line* dan kemudian mencatat *log* dari paket secara keseluruhan dengan menggunakan mekanisme *log* untuk proses analisa lebih lanjut.

Sintak penulisan rule pada snort yaitu :

```
[tipe rule] [protokol] [alamat ip | any (semua)][nomor
port | any (semua)] [-> (satu arah) | <> (dua arah)] [pola
deteksi, penandaan, pencatatan log, dll]
```

Gambar 6. Sintak Rule Snort

4. KESIMPULAN

Pada paper ini merupakan racangan penelitian keamanan *server* dengan menggunakan model forensik jaringan. *Server* yang akan diteliti adalah server UN PGRI Kediri. Model Forensik merupakan kegiatan menangkap, mencatat dan menganalisis kajadian serangan pada jaringan, sehingga model ini sangat cocok digunakan untuk rancangan keamanan jaringan di lingkungan UN PGRI. *Tools* yang digunakan adalah *Instrution Detection System*(IDS) Snort. Karena Snort mampu melakukan analisis semua lalu lintas jaringan. Pada racangan juga akan dibangun notifikasi, sehingga ketika terjadi serangan *server* UN PGRI, maka notifikasi akan dikirimkan ke *mobile phone* administrator, sehingga serangan yang tarjadi dapat sergera diatasi. Penelitian ini merupakan rancangan penelitian yang nantinya akan dijadikan acuan untuk penelitian selanjutnya yaitu implementasi *Network Forensik*.

DAFTAR PUSTAKA

APJII, 2012. *Profil Internet Indonesia*, http://www.apjii.or.id/v2/index.php/read/content/laporan-publik/177/profilinternet-indonesia-2012.html, 2012.

ID-CERT, 2012. *Incident Handling Report*.

online, http://www.cert.or.id/incident_handling/penelitian/3/, 2012.

Kausik A.K dan Joshi R.C. 2010. *Network Forensic System for ICMP Attacks*. International Journal of Computer Applications(0975 - 8887) Volume 2-No.3.

Lazzez A. 2013. *A Survey about Network Forensic Tools*. International Journal of Computer and Information Technology, Vol. 2-Issue 1.

Mahrouqi A.P, Tobin P, Abdalla S dan Kechadi T. 2014. *Simulating SQL-Injection Cyber-attacks using GNS3*. IACSIT.

Putri R.U dan Istiyanto J.E. 2012. *Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada*. IJCCS , Vol.6, No.2,July 2012, pp. 101-112.

Pomeroy A dan Tan Q. 2011. *Effective SQL Injection Attack Reconstruction Using Network Recording*. IEEE International Conference on Computer and Information Technology. Canada.

Roesch M. 1999. *Snort-Lightweight Intrusion Detection for Networks*. Proceedings of LISA '99: 13th System Administration Conference

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

Sulianta F. 2008. *Komputer Forensik*. Jakarta : PT. Elex Media Komputindo.