PERANGKAT PENDUKUNG FORENSIK LALU LINTAS JARINGAN

Aprianti Putri Sujana
Teknik Komputer Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung (STEI ITB)
putrisujana@students.itb.ac.id

ABSTRAK

Internet merupakan media yang kini sangat luas penggunanya. Dari berbagai sektor kehidupan, sebagian menggunakan media internet. Hal ini juga menjadikan lingkungan perang cyber di berbagai jenis media dalam jaringan internet. Media yang berkaitan dengan media sosial, penjualan online, portal berita, atau yang berkaitan dengan edukasi digital. Internet harus dilindungi dari berbagai macam serangan dan respons yang tepat harus dihasilkan untuk menangani kejahatan untuk mengurangi dampaknya.

Forensik jaringan adalah ilmu yang berhubungan dengan menangkap, merekam, dan analisi jaringan lalu lintas untuk tujuan investigasi dan respon dari sebuah insiden. Terdapat banyak cara yang dilakukan untuk merusak jaringan dari berbagai protokol yang dilewatkan. Paper ini akan menyajikan beberapa perangkat yang digunakan dalam menangkap, merekam, dan menganalisa jaringan yang dianggap bermasalah.

Langkah-langkah yang akan ditempuh untuk mempersiapkan forensik jaringan ini adalah pemahaman tentang lalu lintas jaringan melalui protokol. Selanjutnya cara yang digunakan untuk menyerang jaringan. Paper ini juga akan memaparkan bukti yang akan dihasilkan dari protokol standar OSI Layer.

Kata kunci: Forensik, Forensik Jaringan, Protokol OSI Layer

1. PENDAHULUAN

Awalnya internet diciptakan untuk melayani kebutuhan dari pertahanan. Seiring dengan berkembangnya teknologi kini internet dapat digunakan komersil yang menghubungakan juataan manusia dari berbagai sektor, baik militer maupun sipil. Internet kini mengakomodasi seluruh layanan bervariasi dengan bebagai kepentingan. Meluas penggunaan internet ini juga mengakibatkan munculnya kejahatan. Sehingga diperlukan pengamanan yang cukup baik untuk melindungi jaringan untuk mengakses internet dan jika sudah terjadi kejahatan makan penanganan yang cukup handal sangat diperlukan untuk mengatasi kejahatan dalam jaringan internet.

Ada banyak alasan yang memotivasi para penyerang untuk menjadi berani melakukan serangan mereka. Kecepatan yang serangan dapat dilakukan, anonimitas yang disediakan oleh media, sifat media dimana informasi digital dicuri tanpa benar-benar menghapus itu, peningkatan ketersediaan calon korban dan dampak global dari serangan beberapa aspek.

Konsep forensik jaringan berhubungan dengan data yang yang ditemukan pada lalu lintas jaringan internet. Forensik jaringan menganalisis lalu lintas data login melalui firewall atau sistem deteksi intrusi atau perangkat seperti router. Tujuannya adalah untuk penelusuran balik ke sumber serangan. Forensik jaringan didefinisikan sebagai teknik ilmiah yang telah terbukti untuk mengumpulkan, mengidentifikasi, mengkaji, berkolerasi, menganalisis dan mendokumentasikan bukti digital dari beberapa pengolahan dan transmisi sumber digital untuk tujuan mengungkapkan fakta-fakta yang berkaitan dengan maksud yang direncanakan atau diukur untuk mengganggu atau merusak.

Ranum, forensik jaringan didefinisikan sebagai "capture, merekam, dan analisis peristiwa jaringan untuk menemukan sumber serangan keamanan.

"Jaringan forensic melibatkan pemantauan lalu lintas jaringan dan menentukan apakah ada anomali dalam lalu lintas dan memastikan apakah itu menunjukkan penyerangan.

2. PROTOKOL JARINGAN KOMPUTER

Jaringan komputer dapat didefinisikan sebagai sekumpulan komputer yang saling berhubungan. Jaringan komputer dapat terdiri dari dua stasion, atau lebih. Kumpulan komputer tersebut dihubungkan menggunakan perangkat jaringan lainnya.

1. Skema Pengalamatan Jaringan

Terdapat dua metode dari pengalamatan jaringan yaitu ; pengalamatan LAN dan *Internetwork addressing.*

Pengalamatan LAN

LAN adalah kumpulan host yang jangkauannya relative lebih dekat yang memungkinkan untuk kecepatan transfer data yang tinggi di host pada jaringan IP yang sama. Dalam LAN setiap nodenya memiliki kode unik pada setiap perangkat disebut MAC Address. Sebuah MAC Address adalah 48-bit nomor seri unik yang diberikan disetiap kartu antar muka jaringan menyediakan alamat fisik ke mesin host dan nilainya tidak akan pernah berubah walaupun pada jaringan yang berbeda.

Internetwork Addressing

Internetwork addressing yang digunakan dalam jaringan dimana LAN yang saling terhubung dengan router. Setiap jaringan pada internetwork addressing ini memiliki alamat yang unik.

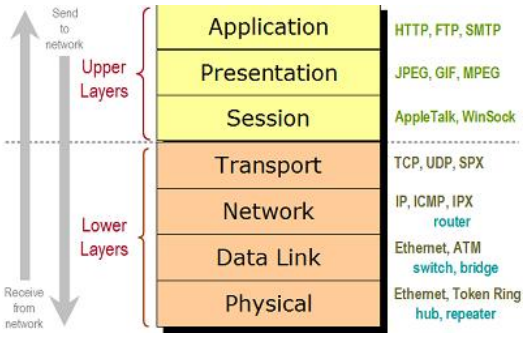
Ketika paket data ditransmisikan dari satu host ke yang lain dalam *internetwork*, router tidak mengetahui alamat host, tetapi router mengetahui alamat jaringan, setelah paket ditransmisikan ke jaringan yang benar, paket akan pergi ke host tujuan.

2. Protokol Jaringan OSI Layer

Model OSI menerapkan konsep yang dikenal dengan enkapsulasi. Enkapsulasi adalah metode membungkus data dari satu lapisan model OSI dalam struktur data baru sehingga setiap lapisan model OSI hanya akan melihat dan berurusan dengan formasi yang dibutuhkan untuk dengan benanr menangani dan memberikan data pada jaringan komputer.

Model referensi OSi didasarkan pada prinsip-prinsip sebagai berikut :

a. Setiap lapisan memiliki fungsi yang dapat didefinisikan,
b. Batas-batas laisan telah dirancang untuk mengurangi arus informasi dalam antarmuka,
c. Ketika tingkat tambahan abstraksi diperlukan, makan lapisan selanjutnya akan dibuat, dan
d. Setiap lapisan memiliki fungsi protokol standar internasional.



Gambar 2.2 Protokol OSI Layer

- **Physical Layer**
  Tidak mempunyai protokol yan spesifik di layer ini, karena pada layer ini hanya mengirimkan bit data.

  Data Link Layer
- PPP (*Point to Point Protocol*)
  Protokol yang digunakan untuk point to point pada suatu jaringan.
- SLIP (*Serial Line Internet Protocol*)
  Protokol yang digunakan untuk menyambung serial.

  Network Layer
- IP (Internetworking Protocol)
  Mekanisme transmisi yang digunakan untuk menstransportasikan data dalam-dalam paket yang disebut datagram.
- ARP (*Address Resulotion Protocol*)
  Protokol yang digunakan untuk mengetahui alamat IP berdasarkan alamat fisik dari sebuah komputer.
- RARP (*Reverse Address Resulotion Protocol*)
  Protokol yang digunakan untuk mengetahui alamat fisik melalui IP komputer.
- ICMP (*Internet Control Message Protocol*)
  Mekanisme yang digunakan oleh sejumlah host untuk mengirim notifikasi datagram yang mengalami masalah pada hostnya.
- IGMP (*Internet Group Message Protocol*)
  Protokol yang digunakan untuk memberi fasilitas message yang simultan kepada group penerima.

  Transport Layer
- TCP (*Trasmission Control Protocol*)
  Protokol yang menyediakan layanan penuh lapisan transport untuk aplikasi.
- UDP (*User Datagram Protocol*)

Protokol connectionless dan proses-to-procces yang hanya menambahkan alamat port, cheksum error control dan panjang informasi data pada layer di atasnya.

Session Layer

- NETBIOS
  Berfungsi sebagai penyiaran pesan maksud nya memungkinkan user mengirim pesan tunggal secara serempak ke komputer lain yang terkoneksi.
  NETBEUI (*NETBIOS Extended User Interface*)
  Berfungsi sama dengat NETBIOS hanya sedikit di kembangkan lagi dengan menambahkan fungsi yang memungkinkan bekerja dengan beragam perangkat keras dan perangkat lunak.
- ADSP (*AppleTalk Data Stream Protocol*)
  Berfungsi protokol ini memantau aliran datadiantara dua komputer dan untuk memeriksa aliran data tersebut tidak terputus.
- PAP (*Printer Access Protocol*)
  Berfungsi printer Postscript untuk akses pada jaringan AppleTalk dan untuk mengendalikan bagaimana pola komunikasi antar node.
- SPDU (*Session Protokol Data Unit*)
  Berfungsi mendukung hubungan antara dua session service user.

Presentasi Layer

- TELNET
  Protokol yang digunakan untuk akses remote masuk ke suatu host, data berjalan secara lain teks.
- SMTP (*Simple Mail Transfer Protocol*)
  Salah satu protokol yang biasa digunakan dalam pengiriman e-mail di internet atau untuk mengirimkan data dari komputer pengirim e-mail ke server e-mail penerima.
- SNMP (*Simple Network Management Protocol*)
  Protokol yang digunakan dalam suatu manajemen jaringan.

Application Layer

- HTTP (*Hyper Text Transfer Protocol*)
  Protokol yang dipergunakan untuk mentransfer dokumen dan web dalam sebuah web browser, melalui www. HTTP juga merupakan protokol yang meminta dan menjawab antar klien dan server.
- FTP (*File Transfer Protokol*)
  Protokol internet yang berjalam dalam layer aplikasi yang merupakan standar untuk mentransfer file komputer antar mesin-mesin dalam sebuat jaringan internet.
- NFS (*Network File System*)
  Jaringan protokol yang memungkinkan pengguna di klien komputer untuk menngakses file melalui jaringan dengan cara yang sama dengan bagaiman penyimpanan lokal yang diaksesnya.
- DNS (*Domain Name System*)
  Protokol yang digunakkan untuk memberikan suatu nama domain pada sebuah alamat IP agar lebih mudah diingat.
- POP3 (*Post Office Protocol*)
  Protokol yang digunakan untuk mengambil mail dari suatu mail transfer agent yang akhirnya mail tersebut akan di dowbload kedalam jaringan local.
- MIME (*Multipurpose Internet Mail Exension*)
  Protokol yang digunakan untuk mengirim file binary dalam bentuk teks.
- SMB (*Server Messange Block*)
  Protokol yang digunakan untuk mentransfer server-server file ke DOS dan Windows.
- NNTP (*Network News Transfer Protocol*)
  Protokol yang digunakan untuk menerima dan mengirim newsgroup.
- DHCP (*Dynamic Configuration Protocol*)
  Layanan yang memberikan no IP kepada komputer yang meminta nya secara otomatis.

3. Jenis Serangan Jaringan

Terdapat beberapa kategori serangan pada lalu lintas jaringan, yaitu :

a) *IP Spoofing* ; salah satu kejahatan yang banyak digunakan pada lalu lintas jaringan dengan cara memalsukan IP address.
b) Penyerangan router

c) *Sniffing* ; aplikasi yang dapat menangkap paket dalam sebuah jaringan.
d) *Data Modification* ; data yang dimodifikasi
e) *Denial of service* ; serangan yang bertujuan untuk melumpuhkan target sehingga sumber atau tujuan tidak dapat memberikan layanan.

3. PERANGKAT ANALISIS FORENSIK

Analisis lalu lintas jaringan dilakukan dengan beberapa alasan diantaranya :

- Terdapat lalu lintas jaringan yang mencurigakan
- Jaringan akan menghasilkan lalu lintas yang begitu kompleks
- Mengidentifikasi masalah jaringan
- Mengurangi kejahatan dengan memanfaatkan lalu lintas jaringan pada internet.

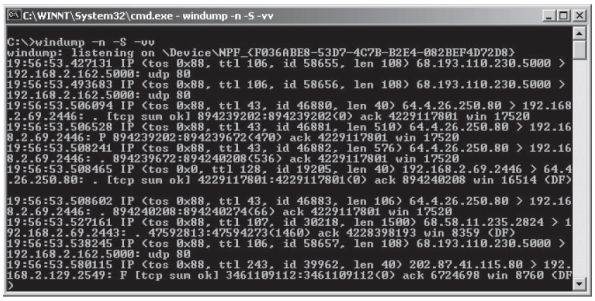
3.1. Tcpdump

Tcpdump adalah alat yang ampuh yang ekstrak paket jaringan dan melakukan analisis statistik pada mereka pembuangan. Ini beroperasi dengan menempatkan kartu jaringan ke mode *promiscuous*. Hal ini digunakan untuk mengukur waktu respon dan persentase packet loss, dan untuk melihat TCP / UDP pembentukan koneksi dan pemutusan. Salah satu kelemahan utama Tcpdump adalah bahwa ukuran file datar yang berisi output teks besar. Laporan Tcpdump terdiri dari:

1. Tampilan jumlah paket : Ini adalah jumlah paket yang Tcpdump telah diterima dan diproses.
2. Jumlah paket yang diterima : Arti dari ini tergantung pada OS yang penyidik sedang berjalan sampah TCP-. Hal ini juga tergantung pada cara OS dikonfigurasi. Jika filter ditentukan pada baris perintah, pada beberapa OS itu penting paket, terlepas dari apakah mereka cocok dengan ekspresi filter dan, bahkan jika mereka cocok dengan ekspresi filter, terlepas dari apakah Tcpdump telah membaca dan pro-olahan mereka belum.
3. Hitungan paket yang disimpan oleh kernel: ini adalah jumlah paket yang disimpan, karena kurangnya buffer, dengan mekanisme menangkap paket di OS yang Tcpdump berjalan, jika OS tidak melaporkan informasi ini, Tcpdump akan melaporkannya sebagai nol.

3.2. WinDump

WinDump adalah port dari Tcpdump pada platform Windows. WinDump kompatibel dengan Tcpdump yang digunakan untuk melihat dan mendiagnosa lalu lintas jaringan yang kompleks. WinDump mudah digunakan dan bekerja dengan *command line*.

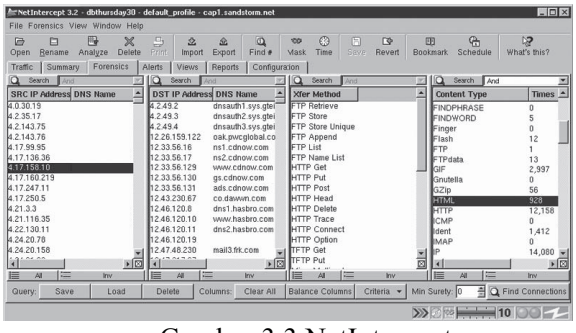


Gambar 3.2 WinDump

3.3. NetIntercept

NetIntercept merupakan perangkat lunak dari Sandstrom Enterprises yang digunakan untuk analisis jaringan yang memungkinkan suatu organisasi untuk meningkatkan keamanan jaringan. NetIntercept menangkap lalu lintas dalam LAN menggunakan Ethernet standar yang ditempatkan dalam mode promiscuous dan kernel UNIX yang telah dimodifikasi.

NetIntercept melakukan rekontruksi aliran on demand, ketika pengguna memilih bagian yang akan ditangkap untuk proses analisis, NetInrecept merakit paket tersebut ke dalam koneksi jaringan data stream.



Gambar 3.3 NetIntercept

NetIntercept menggunakan GUI menawarkan kriteria pencarian canggih.

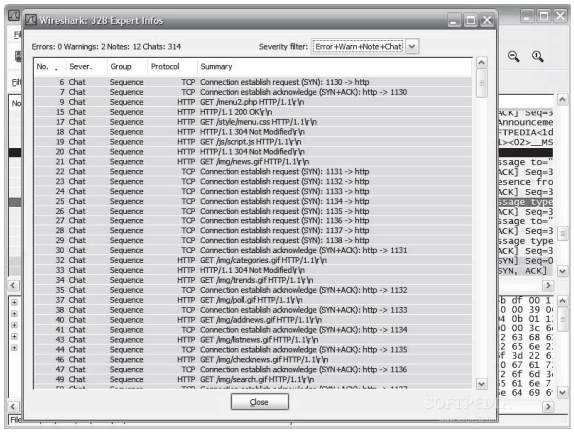
Seorang pengguna dapat menemukan satu atau banyak koneksi jaringan menurut berikut:

1. Dalam satuan waktu hari

2. Sumber alamat atau tujuan hardware atau Internet
3. Sumber atau tujuan TCP atau nama port UDP atau nomor
4. Nama yang terkait dengan koneksi
5. E-mail pengirim, penerima, atau kepala subjek
6. File name atau URL World Wide Web yang terkait dengan transfer
7. Protokol khusus atau jenis konten yang diakui dalam isi koneksi

3.4. Wireshark

Wireshark sebelumnya dikenal sebagai Ethereal adalah perangkat lunak berbasis GUI dalam protokol untuk jaringan lalu lintas. Wireshark memungkinkan pengguna interaktif menelusuri paket dari jaringan komputer yang sibuk atau *file capture* yang sebelumnya.

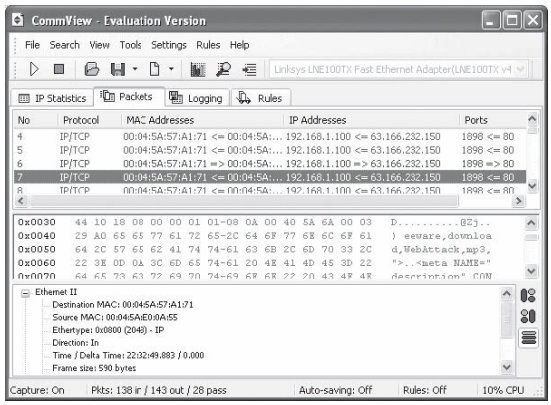


Gambar 3.4 Wireshark

Wireshark dapat menentukan jenis file capture dengan sendirinya, tanpa ada campur tangan pengguna, jika dilakukan kompresi makan file yang akan dihasilkan menggunakan gzip.

3.5. CommView

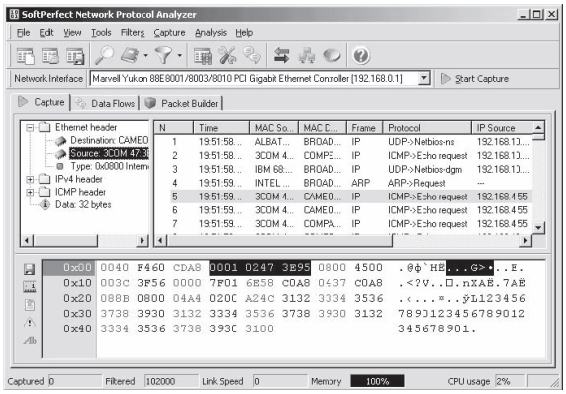
CommView adalah monitor jaringan dan alat analisis yang meberikan gambaran lengkap dari lalu lintas yang mengalir melalui PC atau bagian dari LAN. Aplikasi ini menangkap setiap paket dan menampilkan informasi dan statistic yang penting tentang paket yang diambil. Untuk pemantauan jarak jauh, CommView termasuk add-on yang disebut remote agent. Hal ini memungkinkan untuk dapat diakses dimanapun.



Gambar 3.5 CommView

3.6. SoftPerfect Network Protocol Analyzer

Perangkat lunak ini digunakan untuk debug, memelihara, menganalisa, dan memonitor jaringan dan koneksi internet local. Ia menangkap dan melewati koneksi jaringan data, menganalisa data ini, dan kemudian membuatnya menjadi lebih mudah dibaca. Hal ini memungkinkan pengguna untuk defragment dan mengumpulkan kempali paket yang terpisah. Aplikasi ini menganalisis lalu lintas jaringan berdasarkan sejulah protocol yang berbeda, diantaranya : AH, APR, FTP, HTTP, ICMP, IP, IPV6, IPX, TCP, UDP, Telnet



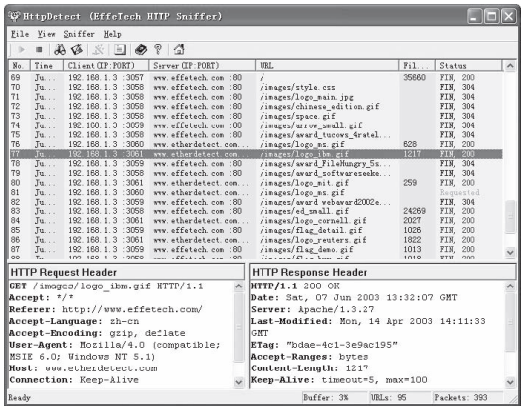
Gambar 3.6 SoftPerfect Network Protocol

3.7. HTTP Sniffer

HTTP Sniffer adalah protokol analyzer dan alat reassembly dengan platform hanya untuk windows. Sniffer ini menangkap paket IP yang berisi pesan HTTP, membangun kembali sesi HTTP, dan reassembles file dikirim melalui protokol HTTP. HTTP sniffer menyediakan analisis real-time dari konten saat menangkap paket, meanalisis, parsing dan pesan decoding HTTP.

Berikut ini adalah beberapa fitur dari HTTP Sniffer:

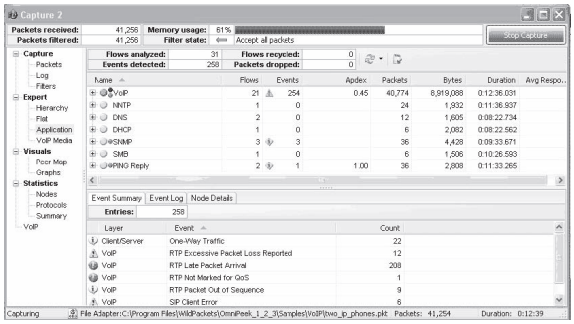
- Powerfull berkas HTTP rebuilder: HTTP Sniffer mengakui aliran direkonstruksi setiap sesi TCP. Melalui analisis dari paket HTTP dalam koneksi TCP yang sama, menyusun kembali file asli ditransfer oleh HTTP. Pengguna dapat melihat dan menyimpan file dibangun kembali.
- Beberapa jenis berkas dukungan: Aplikasi ini mendukung HTML, XML, GIF, JPG, dan jenis file lainnya.
- Powerfull packet untuk menangkap filter: Fitur ini menyediakan mekanisme fleksibel untuk memantau target khusus host dan jenis file.
- Logging disesuaikan : HTTP Sniffer ekspor log file dalam format HTML atau format CSV disesuaikan.



Gambar 3.7 HTTP **Sniffer**

3.8. OmniPeek

OmniPeek adalah alat analisis jaringan yang administrator dapat digunakan untuk dengan cepat menganalisa dan memecahkan masalah jaringan ditingkat perusahaan.



Gambar 3.8 OmniPeek Tools

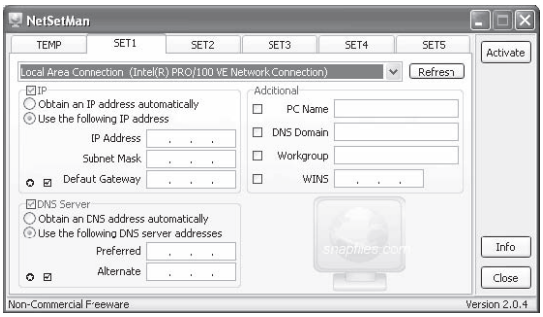
Beberapa fitur dari OmniPeek :

- Kemampuan untuk menganalisis lalu lintas dari setiap segmen jaringan local, termasuk gigabit dan segmen WAN
- Kemampuan untuk menelusuri untuk melihat mana node jaringan yang berkomunikasi dan karakteristik lalu lintas jaringan yang mempengaruhi kinerja jaringan.
- Kemampuan untuk mengubah filter dengan cepat tanpa harus berhenti dan restart menangkap paket.
- Kemampuan untuk melihat analisis berbabisis aliran paket oleh pasangan percakapan.
- Kemampuan untuk secara bersamaan memantau beberapa bagian dari jaringan.

3.9. NetSetMan

NetSetMan adalah manajer pengaturan jaringan yang memungkinkan pengguna untuk dengan mudah beralih di antara enam pengaturan jaringan yang berbeda profil. Profil ini meliputi pengaturan berikut:

- Alamat IP
- Subnet mask
- Default gateway
- Preferred dan server DNS alternatif
- Nama komputer
- Workgroup
- Domain DNS
- WINS Server
- Printer default
- Skrip Jalankan
- Domain Jaringan
- Pengaturan proxy Lengkap (Internet Explorer dan Firefox)
- Home page (Internet Explorer dan Firefox)



Gambar 3.9 NetSetMan Tools

4. KESIMPULAN

Dari paparan diatas dapat ditarik kesimpulan :

1. Skema pengalamatan jaringan diperlukan sebagai ujung dari sebuah permasalahan.

2. Dengan menggunakan perangkat *Sniffing* dapat mencegah dan memperhatikan, memonitor lalu lintas jaringan.

5. DAFTAR PUSTAKA

[1] Perry, S. *Network forensic and The Inside Job Network Security*. 2006

[2] Ec-Council Press. *Computer Forensic Invesrigating Intrusions & Cyber Crime*

[3] Pilli S. Emamanuel, Joshi R.C., Niyogi R., *A Generic Framework for Network Forensic,* International Journal of Computer Applications(0975 - 8887). Volume 1 No. 11