BAB II

DASAR TEORI

2.1 TINJAUAN PUSTAKA

Penelitian yang dilakukan Hendri Alamsyah, Riska, Abdussalam Al Akbar mengenai Analisa Keamanan Jaringan Menggunakan *Network Intrusion Detection and Prevention System* dengan snort. Penelitian ini dilakukan untuk mendeteksi dan mencegah lalulintas data yang mencurigakan dengan menggunakan *rules* protocol telnet dan ftp. Hasil dari penelitian ini yaitu adanya alert yang masuk pada log sistem keamanan IDPS, dimana terdapat percobaan *port scanning* menggunakan Nmap [6].

Penelitian yang dilakukan Emir Risyad, Mahendra Data, Eko Sakti Pramukantoro mengenai Perbandingan Performa Intrusion Detection System (IDS) Snort Dan Snort Dalam Mendeteksi Serangan TCP SYN Flood. Untuk mengetahui performa dari *tools* snort dan snort pada metode IDS dalam menangani serangan, dilakukan dengan tiga metode dalam lingkup *core* tunggal. Adapun metode yang digunakan dalam penelitian ini yaitu melancarkan paket-paket menggunakan trafik normal, trafik serangan, dan menggabungkan kedua trafik serta melancarkannya ke lingkup penelitian. Parameter yang diuji dalam penelitian ini adalah akurasi deteksi, efektivitas deteksi, kecepatan deteksi dan penggunaan sumber daya system. Hasil dari penelitian ini yaitu IDS snort lebih unggul dibanding IDS snort dalam hal akurasi deteksi, efektivitas deteksi, kecepatan deteksi, akan tetapi IDS snort lebih hemat dalam penggunaan sumber daya system [7].

Penelitian yang dilakukan oleh Parningotan Panggabean, S.Kom., M.Kom mengenai Analisis *Network Security* Snort menggunakan Metode *Intrusion Detection System* (IDS) untuk Optimasi Keamanan Jaringan Komputer. Dimana penelitian ini didasarkan oleh adanya indikasi serangan *Denial of Service* (DoS) dengan terdapat *Log Bug* pada komputer server Dinas Lingkungan Hidup Kota Batam. Untuk menguji serangan DoS dengan snort, dilakukan dengan tiga skenario yaitu metode TCP *Flooding*, UDP *Flooding*, dan HTTP *Flooding* dengan menggunakan aplikasi *Loic*. Hasil dari penelitian ini adalah metode IDS mampu

mengoptimalkan tingkat keamanan jaringan pada komputer server Dinas Lingkungan Hidup Kota Batam dengan pendeteksian serangan menggunakan snort. Snort dapat mendeteksi serangan *Denial of Service* (DoS) dengan metode TCP *Flooding*, UDP *Flooding*, dan HTTP *Flooding* dalam menangkap ip address dari penyerang [8].

2.2 DASAR TEORI

2.2.1 JARINGAN KOMPUTER

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi, dan dapat mengakses informasi. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan. Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut server. Desain ini disebut dengan sistem *client*-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer. Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dihubungkan melalui kabel maupun nirkabel sebagai medium transmisi data, dan terdapat perangkat lunak sistem operasi jaringan akan membentuk sebuah jaringan komputer yang sederhana. Apabila ingin membuat jaringan komputer yang lebih luas lagi jangkauannya, maka diperlukan peralatan tambahan seperti *Hub, Bridge, Switch*, Router, *Gateway* sebagai peralatan interkoneksinya [9]. Konsep jaringan komputer ditunjukkan pada gambar 2.1

Gambar 2.1 Konsep Jaringan Komputer [10].

Selain itu jaringan komputer bisa diartikan sebagai kumpulan sejumlah terminal komunikasi yang berada diberbagai lokasi yang terdiri dari lebih satu komputer yang saling berhubungan. Sehingga, berdasarkan jarak dan area kerjanya jaringan komputer dibedakan menjadi tiga kelompok, yaitu :

1. *Local Area Network* (LAN)

   Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (*resouce*, misalnya printer) dan saling bertukar informasi.

2. *Metropolitan Area Network* (MAN)

   Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

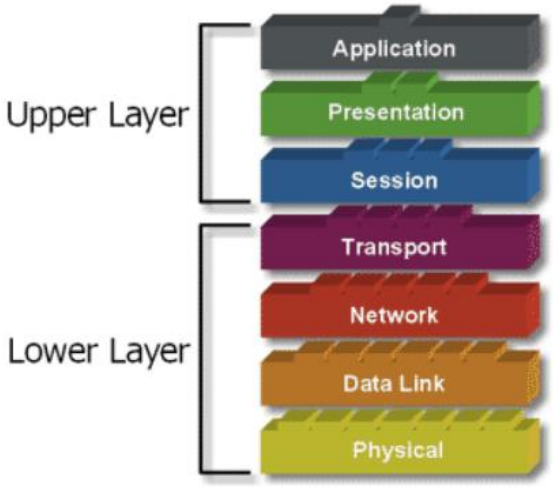
3. *Wide Area Network* (WAN)

   Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai [11].

2.2.2 OPEN SYSTEM INTERCONNECTION (OSI) LAYER

Model referensi OSI (*Open System Interconnection*) adalah model konsep bertujuan sebagai konsep komunikasi dari sistem telekomunikasi tanpa memperhatikan struktur dan teknologi internal, referensi OSI dibuat dan dikembangkan oleh *International Standards Organization* (ISO). Model referensi OSI bertujuan untuk membuat perbedaan antara tiga konsep utama arsitektur jaringan: layanan, antarmuka, dan protokol. Layanan menentukan tugas di setiap layer, antarmuka menentukan bagaimana cara mengakses layanan, dan protokol

adalah jaringan yang melakukan jenis layanan yang sebenarnya. Model ini hanya sebagai jenis fungsi dimana setiap *layer* harus penuh, bukan protokol yang tepat untuk digunakan. OSI terdiri dari tujuh *layer*, seperti yang ditunjukkan pada Gambar 2.2



Gambar 2.2 Model *Layer* OSI [12].

Ketujuh layer ini jika dilihat secara fungsional dapat dikelompokkan menjadi dua bagian saja, yaitu : *layer* 5 sampai dengan 7 dikelompokan sebagai *upper layers*. Segala sesuatu yang berkaitan dengan *user interface*, *data formatting* dan *communication session* ditangani oleh *layer* ini, diimplementasikan dalam bentuk *software*/aplikasi. Sedangkan *layer 4* sampai dengan 1 dikelompokkan sebagai *data flow layers* atau *lower layers*. Dimplementasikan dalam bentuk *hardware* atau *software* [13]. Adapun penjelasan dari 7 Model OSI *layer* tersebut adalah sebagai berikut.

1. *Application Layer*

   Layer ke-7 dari model *network* OSI, menyediakan layanan-layanan untuk prosedur-prosedur aplikasi (seperti *electronic* mail atau transfer file) yang berada diluar model OSI. Layer ini memilih dan menentukan ketersediaan dari partner komunikasi dan juga sumber daya yang diperlukan untuk membuat koneksi, mengkoordinasi aplikasi-aplikasi yang berpasangan, dan membentuk sebuah kesepakatan terhadap prosedur-prosedur untuk mengendalikan integritas data dan *error recovery.*

2. *Presentation Layer*

   Layer 6 dari model referensi OSI, mendefenisikan bagaimana data di-format, dinyatakan, di-encode, dan diubah untuk digunakan oleh software pada layer aplikasi.

3. *Session Layer*

   Layer 5 dari model referensi model OSI, bertanggung jawab untuk membuat, mengelola, dan mengakhiri session-session antara aplikasi-aplikasi dan mengawasi pertukaran data antara entitas-entitas layer presentation.

4. *Transport Layer*

   Layer 4 dari model referensi OSI, digunakan untuk komunikasi yang dapat diandalkan antara node-node akhir melalui network. Layer transport menyediakan mekanisme yang digunakan untuk membuat, memelihara, dan mengakhiri rangkaian-rangkaian virtual, mengangkut deteksi kesalahan dan recovery, dan mengendalikan aliran informasi.

5. *Data Link Layer*

   Layer 2 dari model referensi OSI, ia memastikan transmisi data yang bisa dipercaya melalui sebuah link fisikal dan terutama berkaitan dengan pengalamatan fisikal, disiplin line, topologi network, pemberitahuan error, pengiriman frame yang berurutan, dan flow control. IEEE membagi lebih lanjut layer ini menjadi sublayer MAC dan sublayer LLC. Juga dikenal sebagai *link layer.*

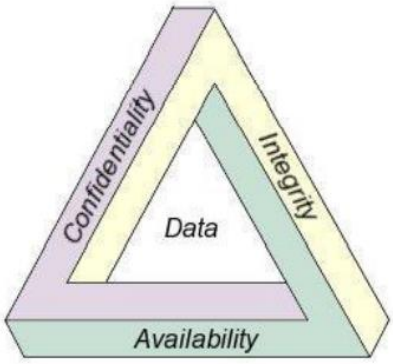
6. *Physical Layer*

   Layer terendah – layer 1 – dalam model referensi OSI, bertanggung jawab untuk mengubah frame-frame data dari layer Data Link (layer-2) menjadi sinyal-sinyal listrik. Protokol-protokol dan standar-standar layer Physical mendefenisikan, sebagai contoh, jenis kabel dan konektor yang digunakan, termasuk pemilihan pin dan skema encoding untuk pensinyalan nilai 0 dan 1 [14].

2.2.3 KEAMANAN JARINGAN

Keamanan jaringan adalah bentuk pencegahan atau deteksi pada hal yang bersifat gangguan dan akses tak seharusnya pada Sistem Jaringan Komputer. langkah-langkah pencegahanmembantu menghentikan pengguna yang tidak sah

yang disebut penyusup untuk mengaksessetiap bagian dari sistem jaringan komputer . Tujuan Keamanan jaringan komputer adalahuntuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik baik langsung ataupun tidak langsung mengganggu aktifitas yang sedang berlangsung dalam jaringancomputer. Keamanan jaringan sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan [15]. Untuk model CID (*Confidentiality*, *Integrity*, *Availability*) ditunjukkan pada Gambar 2.3



Gambar 2.3 Model CID [16].

Keamanan informasi telah dibangun atas 3 kunci dasar dari prinsip kunci keamanan informasi yaitu: *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan). Adapun penjelasan dari ketiga prinsip ini yaitu :

1 *Confidentiality*

Confidentiality (kerahasiaan) berfokus pada upaya untuk menghindari pengungkapan secara tidak sah terhadap informasi yang bersifat rahasia maupun sensitif. Pengungkapan informasi tersebut dapat terjadi secara disengaja, seperti pemecahan sandi untuk membaca informasi, atau dapat terjadi secara tidak disengaja, dikarenakan kecerobohan dari individu dalam menangani informasi.

2 *Integrity*

Dalam keamanan informasi, *integrity* (integritas atau keutuhan) berarti bahwa data tidak dapat dibuat, diganti, atau dihapus tanpa proses otorisasi.

Dengan kata lain, *integrity* merupakan prinsip yang ditujukan untuk menjaga keakuratan suatu informasi.

3 Availability

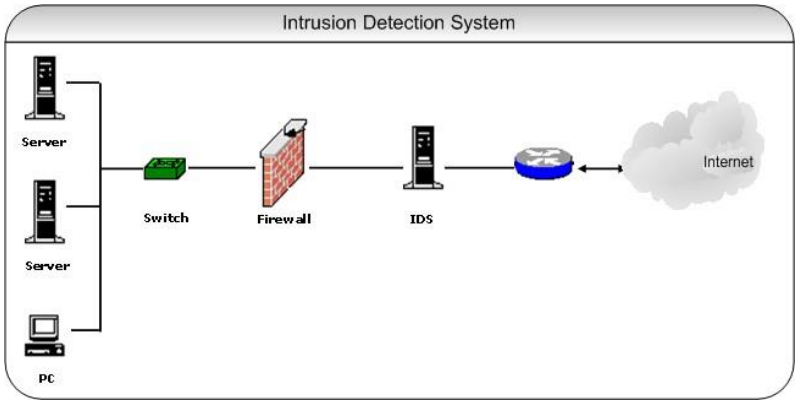
Availability menjamin bahwa pengguna sistem yang berhak memiliki akses tanpa interupsi terhadap sistem dan jaringan. Hal tersebut memastikan bahwa informasi atau sumber daya akan selalu tersedia ketika dibutuhkan [16].

2.2.4 INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS)

Intrusion Detection and Prevention Systems (IDPS) adalah sistem yang dapat me-monitor host atau jaringan untuk mencurigai aktivitas atau perilaku anomali kemudian mengambil tindakan yang tepat untuk melawan mereka. Dimana IDPS merupakan gabungan dari IDS dan IPS. Sistem IDS dapat berada di mana saja dalam jaringan. IDS hanya mendeteksi aktivitas berbahaya dan memperingatkan administrator sehingga administrator yang harus memutuskan cara mengatasi peringatan itu. Di sisi lain, sistem IPS berada sebagai sistem *inline* dan selain menghasilkan alarm, IPS bisa secara otomatis bereaksi terhadap aktivitas abnormal. IPS bisa memblokir sumber serangan atau dapat mengatur ulang koneksi [17]. Adapun penjelasan mengenai sistem IDS dan IPS yaitu :

1. *Intrusion Detection System* (IDS)

   IDS merupakan aplikasi software atau hardware yang digunakan untuk mendeteksi aktivitas yang mencurigakan dari sebuah sistem atau jaringan. IDS mampu menganalisis dan mendapatkan bukti dari percobaan penyusupan dengan melakukan pengamatan terhadap lalu lintas yang masuk dan keluar dari sebuah sistem atau jaringan. Ada dua cara kerja yang biasa digunnakan IDS untuk menganalisa sebuah paket sehingga dapat ditentukan apakah paket tersebut termasuk serangan atau bukan. Cara kerja tersebut adalah *knowledge based* dan *behavior based*. Gambar 2.4 merupakan gambaran penerapan IDS secara umum.



Gambar 2.4 Penerapan IDS [18].

Penyusupan dapat dikenali dengan cara menyadap paket data, kemudian paket data tersebut dibandingkan dengan aturan basis data yang ada pada IDS, apabila paket memiliki kesamaan maka paket tersebut dianggap sebagai serangan, cara ini disebut dengan *knowledge based*. Sedangkan penyusupan yang dikenali dengan cara mengamati kondisi aplikasi untuk menemukan kejanggalan yang membuat aplikasi berjalan tidak normal seperti penggunaan memori yang berlebihan secara terus-menerus atau bisa juga ditemukan koneksi pararel pada satu Ip, kondisi ini dapat dianggap sebagai kejanggalan yang kemudian dapat disimpulkan bahwa kejanggalan tersebut merupakan serangan, cara kerja ini dapat disebut dengan *behavior based* [18].

2. *Intrusion Prevention System* (IPS)

Intrusion Prevention System (IPS) adalah sebuah perangkat lunak atau perangkat keras yang bekerja untuk monitoring trafik jaringan, mendeteksi aktivitas yang mencurigakan dan melakukan pencegahan dini terhadap penyusupan atau kejadian yang dapat membuat jaringan menjadi berjalan tidak seperti sebagaimana mestinya. IPS merupakan pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengombinasikan teknik *firewall* dan metode *intrusion detection system* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat seragan teridentifikasi.

Jadi IPS bertindak seperti layaknya firewall yang akan mengizinkan atau menghalang paket data. Ada 2 jenis IPS, yaitu *Host Based Intrusion Prevention System* (HIPS) dan *Network Based Intrusion Prevention System* (NIPS).

a. *Host Intrusion Prevention System* (HIPS)

Host-based Intrusion Prevention System (HIPS) sama seperti halnya *Host Based Intrusion Detection System* (HIDS). Program agent HIPS diinstall secara langsung di sistem yang diproteksi untuk dimonitor aktifitas sistem internalnya. HIPS di binding dengan kernel sistem operasi dan *services* sistem operasi sehingga HIPS bisa memantau dan menghadang *system call* yang dicurigai dalam rangka mencegah terjadinya intrusi terhadap *host*. HIPS juga bisa memantau aliran data dan aktivitas pada aplikasi tertentu.

b. *Network Intrusion Prevention System* (NIPS)

Network-based Intrusion Prevention System (NIPS) tidak melakukan pantauan secara khusus di satu host saja. Tetapi melakukan pantauan dan proteksi II-16 dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan firewalldan kadang disebut sebagai *In-Line* IDS atau *Gateway Intrusion Detection System* (GIDS). Sistem kerja IPS yang populer yaitu pendeteksian berbasis *signature*, pendeteksian berbasis anomali, dan monitoring file pada sistem operasi *host* [19].

2.2.5 SNORT

Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisa paket yang melintasi jaringan secara langsung dan melakukan pencatatan ke dalam penyimpanan data serta mampu mendeteksi berbagai serangan yang berasal dari luar jaringan [20]. Snort bukanlah sebatas *protocol* analisis atau sistem pendeteksi penyusupan (*Intrusion Detection System*) IDS, melainkan sedikit gabungan diantara keduanya, dan bisa sangat berguna dalam merespons insiden-insiden peyerangan terhadap *host-host* jaringan. Fitur snort dapat menjadi penolong administrator sistem dan jaringan, dimana mampu memperingatkan kita atas penyusup yang berpeluang berbahaya. Fitur-fitur inilah yang menjadikan snort sebuah sistem pendeteksi gangguan dan serangan jaringan

yang sangat berguna bagi tim penanggulangan insiden. Snort sekarang dapat dioperasikan dengan empat (4) buah mode:

1. Paket *sniffer*

   Praktis membaca paket-paket dari jaringan dan memperlihatkan pada kita dalam bentuk aliran tak terputus pada layar.

2. *Packet logger*

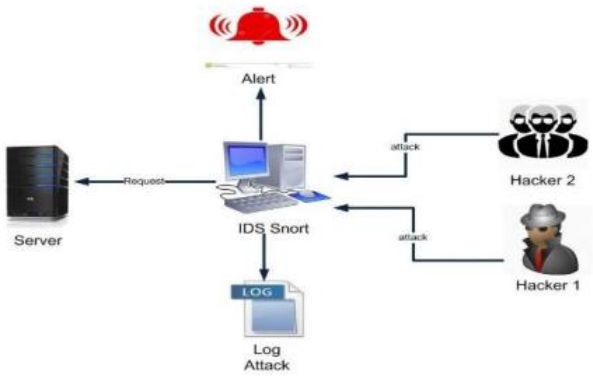
   Untuk mencatat semua paket yang lewat di dalam disk.

3. NIDS (*Network Intrusion Detection System*)

   Pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer.

4. *Inline Mode*

   Mengambil paket dari iptable dan menginstruksikan iptable untuk meneruskan paket tersebut berdasarkan jenis rule dari snort yang digunakan [21].

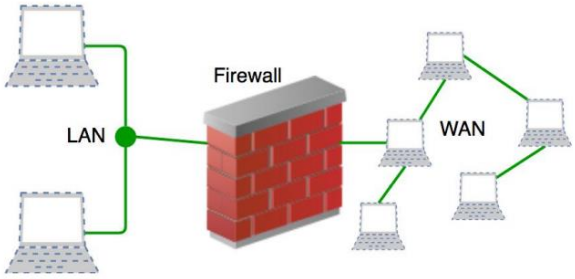


Gambar 2.5 Arsitektur Snort IDS [22].

Snort diletakkan satu *switch core* dengan Server, sehingga *user* yang mengakses server akan melewati *switch core* maka dapat dipantau oleh server IDS Snort. Snort melakukan *decode* terhadap paket layer aplikasi dan diberika rule untuk mengumpulkan *traffic* tertentu yang mengandung isi terkait dengan aplikasi yang mengeluarkan paket tersebut. Snort bekerja dengan beberapa bagian yan bertugas melakukan proses tertentu antari lain paket *capture block, decoder block*, dan preprosesor block. Rule snort di buat terlebih dahulu sehingga ketika terjadi serangan yang sama dengan rule, maka akan muncul *alert*, dan serangan tersimpan di log *database*. Log yang tersimpan di database berfungsi sebagai alat bukti pelaporan [22].

2.2.6 FIREWALL

Firewall didefinisikan sebagai suatu cara atau mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Hal ini ditunjukkan pada gambar 2.6 konfigurasi firewall.



Gambar 2.6 Konfigurasi Firewall

Firewall merupakan sebuah pembatas antara suatu jaringan *local* dengan jaringan lainnya yang sifatnya *public* (dapat diakses oleh siapapun) sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan publik. Firewall terbagi menjadi dua jenis, yakni sebagai berikut:

1. *Personal Firewall*

   Personal Firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. *Firewall* jenis ini akhirakhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditambahkannya beberapa fitur pengaman tambahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya.

2. *Network Firewall*

   Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah

perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. *Network Firewall* umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak [23].

2.2.7 SERANGAN JARINGAN

Pada dasarnya serangan terhadap suatu data dalam suatu jaringan dapat dikategorikan menjadi dua, yaitu:

1. Serangan Aktif

   Merupakan serangan yang mencoba memodifikasi data dan mendapatkan otentikasi dengan mengirimkan paket-paket data yang salah ke dalam data stream atau dengan memodifikasi paket-paket yang melewati data stream. Serangan aktif sulit untuk dicegah karena untuk melakukannya dibutuhkan perlindungan fisik untuk semua fasilitas komunikasi dan jalur-jalurnya setiap saat. Yang dapat dilakukan adalah mendeteksi dan memulihkan keadaan yang disebabkan oleh serangan ini.

2. Serangan Pasif

   Merupakan serangan pada sistem otentikasi yang tidak menyisipkan data pada aliran data, tetapi hanya memonitor pengiriman informasi ke tujuan. Informasi ini dapat digunakan oleh pihak yang tidak bertanggung jawab. Serangan pasif yang mengambil suatu unit data kemudian menggunakannya untuk memasuki sesi otentikasi dengan berpura-pura menjadi pengguna asli yang disebut sebagai *replay attack*. Serangan pasif ini sulit dideteksi karena penyerang tidak melakukan perubahan data. Oleh sebab itu untuk mengatasi serangan pasif ini lebih ditekankan pada pencegahan daripada pendeteksiannya.

Dalam serangan jaringan, terdapat banyak ancaman bagi keamanan jaringan komputer. Jenis ancaman keamanan jaringan ini lebih umum disebut sebagai *Brute Force and Dictionary*, serangan ini adalah upaya masuk ke dalam jaringan dengan menyerang *database* password atau menyerang *login prompt* yang sedang aktif untuk menemukan password dari *account user* dengan cara yang sistematis mencoba berbagai kombinasi angka, huruf, atau simbol. Ada beberapa bentuk ancaman pada jaringan komputer yang sering ditemui

diantaranya *Denial of Services* (DoS), *Spoofing*, *Spamming*, Serangan *Man-in-the-middle*, *Sniffer*, *Cracker*, dsb [24].

2.2.8 SERANGAN UDP *FLOODING* DAN SYN *FLOODING*

Serangan UDP *Flooding* dan SYN *Flooding* termasuk dalam jenis serangan *Denial of Service* (DoS), dimana secara umum serangan DOS menggunakan cara dengan mengirimkan paket dalam kuantitas yang sangat besar terhadap suatu server sehingga tidak bisa memproses semuanya yang mengakibatkan server tersebut down atau tidak berfungsi maksimal.

1. UDP *Flooding*

Merupakan salah satu jenis serangan DDoS (*Distributed Denial Of Service*) yang bersifat *connectionless*. Jenis serangan ini bekerja pada *protocol* UDP dengan cara membanjiri *port* dengan paket UDP palsu dalam jumlah besar [25]. Serangan yang dapat membanjiri paket data via port secara acak dan terus menerus dalam penyerangan target IP Address. Cara melumpuhkan target dalam UDP *Flooding* yaitu dengan mengirimkan paket data secara terus menerus dan apabila terjadi *crowded* nya permintaan data dari *user* sehingga mengakibatkan kelumpuhan pada jaringan layer data link sehingga membuat kekurangan *bandwith* dan *user* lain saat melakukan permintaan paket data pada sebuah jaringan [26].

2. SYN *Flooding*

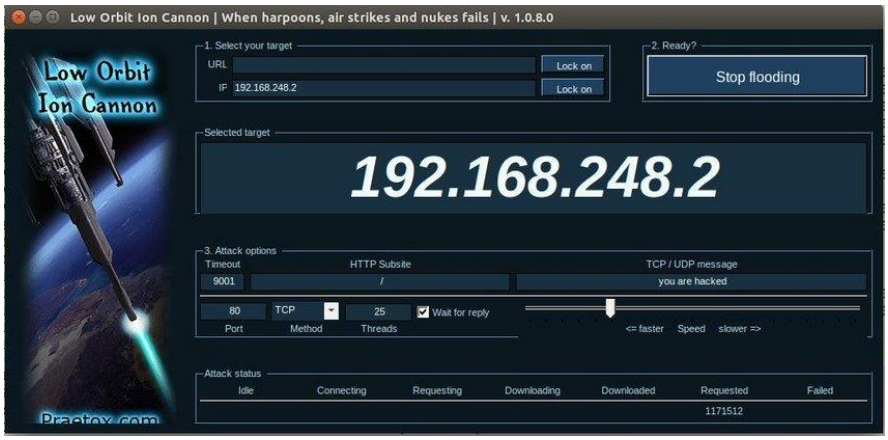
SYN *Flooding* merupakan network DDoS yang memanfaatkan *'loophole'* pada saat koneksi TCP/IP terbentuk. Pada kondisi normal, *client* akan mengirimkan paket data berupa SYN (*synchronization*) untuk men-sinkron kan pada server. Lalu server akan menerima request dari *client* dan akan memberikan jawaban ke *client* berupa ACK (*Acknowledgement*). Sebagai tanda bahwa transaksi sudah dimulai (pengiriman & penerimaan data), maka *client* akan mengirimkan kembali sebuah paket yang berupa SYN lagi. Jenis serangan ini akan membanjiri server dengan banyak paket SYN. Karena setiap pengiriman paket SYN oleh *client*, server pasti akan membalasnya dengan mengirim paket SYN ACK ke *client* [27].

2.2.9 TOOLS UDP FLOODING DAN SYN FLOODING

Dalam melakukan pengujian serangan UDP Flooding dan SYN Flooding, digunakan dua tools yaitu :

1. LOIC (*Low Orbit Ion Canon*)

Low Orbit Ion Cannon (Loic) adalah *open source network stress tools* dan *denial-of- service attack*, yang ditulis dalam C #. LOIC awalnya dikembangkan oleh *Praetox Technologies*, namun kemudian dilepaskan ke domain publik, dan sekarang di-host di beberapa platform *open source*. LOIC DDOS menggunakan tiga jenis serangan terhadap mesin target. Ini termasuk HTTP, UDP dan TCP. LOIC menerapkan mekanisme serangan yang sama yaitu membuka beberapa koneksi ke mesin target dan mengirim rangkaian pesan yang kontinyu ke mesin target. Alat LOIC terus mengirimkan lalu lintas ke server yang ditargetkan, sampai server kelebihan beban. Begitu server tidak dapat menanggapi permintaan pengguna yang sah, secara efektif akan dimatikan [28]. *Tools* LOIC ditunjukkan pada gambar 2.7 dibawah ini.



Gambar 2.7 *Tools* LOIC [29].

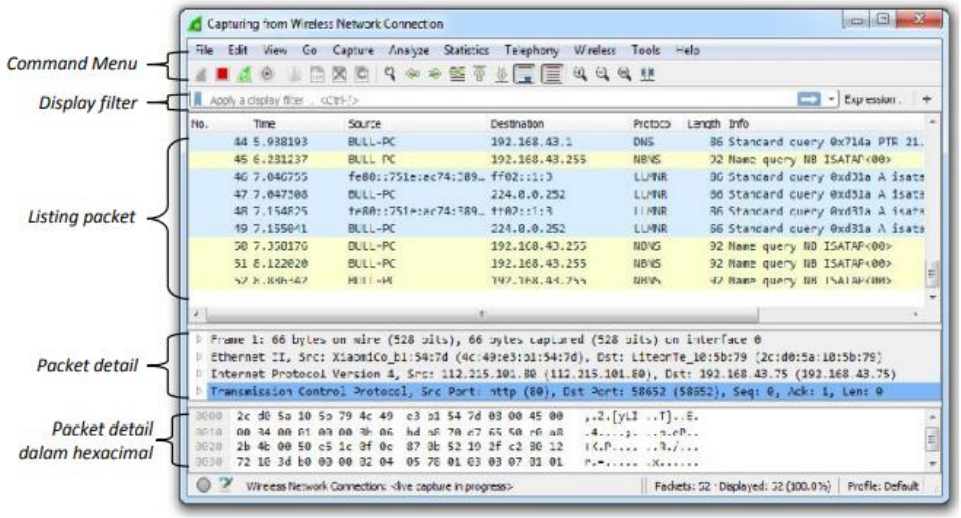
2. Hping3

Hping adalah sebuah TCP/IP assembler dan juga merupakan command-line yang berorientasi pada pemrosesan paket TCP/IP. Hping dapat digunakan untuk membuat paket IP yang berisi TCP, UDP atau ICMP *payloads*. Semua *field header* dapat dimodifikasi dan dikontrol dengan menggunakan baris perintah (*command line*). Hping3 merupakan versi terbaru dari Hping, dan Hping2 adalah aplikasi pendahulunya yang paling signifikan. Hping3 merupakan aplikasi yang berdiri sendiri (*standalone*), sedangkan Hping2 dalam beberapa kasus masih

memerlukan aplikasi dari pihak ketiga, seperti *scapy* (*tools* memanipulasi paket) dan idswakeup (sebuah aplikasi untuk sistem pendeteksian *intrutions* / penyusup). Hping3 hadir dengan mesin baru TCL scripting, sehingga lebih kuat pada perintah command line yang sederhana [30].

2.2.10 WIRESHARK

Wireshark adalah alat penganalisis paket jaringan *open source* yang menangkap paket data yang melewati jaringan dan menyajikannya dalam bentuk yang dapat dimengerti. Wireshark dapat dianggap sebagai pisau tentara Swiss karena dapat digunakan dalam situasi yang berbeda seperti masalah jaringan, operasi keamanan, dan protokol pembelajaran internal. Wireshark dapat membaca data secara langsung dari *Ethernet, Token- Ring*, FDDI, serial (PPP and SLIP), 802.11 wireless LAN , dan koneksi ATM. Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti password email atau *account* lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya [31]. Dapat dilihat pada gambar 2.8 mengenai penggunaan wireshark dibawah ini.



Gambar 2.8 Penggunaan Wireshark [31].

2.2.11 PARAMETER *QUALITY OF SERVICE*

Quality of Service (QoS) Merupakan efek kolektif dan kinerja layanan yang menentukan derajat kepuasan seorang pengguna terhadap suatu layanan. *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) mengelompokkan kualitas QoS menjadi empat kategori berdasarkan nilai parameter-parameter QoS [33].

1. Throughput

adalah bandwidth aktual yang terukur pada suatu ukuran waktu tertentu dalam mentransmisikan berkas. Berbeda dengan bandwidth walaupun satuannya sama *bits per second* (bps), tetapi *throughput* lebih menggambarkan *bandwidth* yang sebenarnya pada suatu waktu dan pada kondisi dan jaringan tertentu yang digunakan untuk mengunduh suatu file dengan ukuran tertentu. *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut. Nilai *throughput* dapat dihitung menggunakan Persamaan: [34].

$$Throughput = \frac{jumlah\ data\ yang\ dikirim\ (kb)}{waktu\ pengiriman\ data\ (s)}$$

2. Packet loss

adalah persentase paket yang hilang selama mentransmisikan data. Hal ini disebabkan oleh banyak faktor seperti penurunan sinyal dalam media jaringan, kesalahan perangkat keras jaringan atau juga radiasi dari lingkungan sekitar. Packet loss merupakan parameter yang menggambarkan suatu kondisi yang menunjukkan jumlah total paket yang hilang, dapat terjadi karena *collision* dan *congestion* pada jaringan. Untuk mencari nilai packet loss dapat dihitung dengan Persamaan: [34].

$$Packet\ loss = \frac{(paket\ data\ kirim - paket\ data\ terima)}{paket\ data\ yang\ dikirim\ (s)}\ x\ 100$$

3. Delay

Delay adalah waktu yang dibutuhkan data untuk sebuah paket yang dikirimkan dari suatu komputer ke komputer yang dituju. *Delay* dalam sebuah proses transmisi paket dalam sebuah jaringan komputer disebabkan karena adanya antrian yang panjang atau mengambil rute lain untuk menghindari kemacetan

pada routing. *Delay* dapat dipengaruhi oleh jarak, media fisik, kongesti atau juga waktu proses yang lama. Untuk mencari *delay* pada paket yang ditransmisikan dengan membagi antara panjang paket (satuannya bit) dibagi dengan link bandwidth (satuannya bit/s). Untuk menghitung rata-rata *delay* digunakan rumus seperti Persamaan: [34].

$$Delay = \frac{total\ delay}{total\ packet\ yang\ diterima}$$

4. *Jitter*

Jitter merupakan variasi *delay* (perbedaan selang waktu) antar paket yang terjadi pada jaringan, yang disebabkan oleh panjangnya antrian pada saat pengolahan data yang terjadi pada jaringan. Besarnya nilai *Jitter* dipengaruhi oleh beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan. Semakin besar beban trafik di dalam jaringan. Untuk menghitung nilai *Jitter* di gunakan persamaan: [34].

$$Jitter = \frac{total\ variasi\ delay}{total\ paket\ data\ yang\ diterima}$$