BAB II
TINJAUAN PUSTAKA

Pada bab ini akan dibahas teori penunjang yang menjadi dasar dari penerapan DMZ dan IPS pada sistem keamanan jaringan. Pembahasan berisi tentang dasar dasar jaringan komputer, potokol, keamanan jaringan, komponen komponen pembentuk DMZ dan IPS.

2.1 Jaringan Komputer

Jaringan Komputer adalah himpunan dari dua atau lebih komputer otonom yang saling terhubung. Komputer yang terhubung ke jaringan dapat berertukar informasi atau disebut juga interkoneksi, bisa berupa text, gambar, suara atau bahkan video. Media penghubung jaringan komputer bisa berupa kabel tembaga, fiber optic, gelombang radio, atau sinyal satelit.

Jaringan komputer dapat dibagi berdasarkan beberapa kategori, diantaranya:

1. Cakupan Area
2. Media Transmisi
3. Fungsi
4. Tipe Koneksi

2.1.1 Berdasarkan Cakupan Area

Berdasarkan cakupan areanya, jaringan komputer secara umum dibagi menjadi tiga jenis, yaitu:

1. Local Area Network (LAN)

   Local area network merupakan jaringan milik pribadi didalam 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 untuk memakai bersama sumberdaya dan saling bertukar informasi.

2. Metropolitan Area Network (MAN)

   Merupakan jaringan komputer yang memiliki cakupan cukup besar hingga 80km, misalkan jaringan yang menghubungkan LAN kantor-kantor perusahaan yang berdekatan. Teknologi yang di terapkan pada MAN tidak

jauh berbeda dengan LAN. Pada dasarnya MAN adalah LAN yang memiliki cakupan lebih luas.

3. Wide Area Network (WAN)

   Merupakan jaringan yang cakupannya sangat luas, seringkali mencakup antar negara bahkan benua, misalkan kantor cabang sebuah perusahaan yang tersebar di seluruh dunia yang saling terhubung melewati Internet.

   Pada sebagian besar WAN, jaringan terdiri dari sejumlah banyak kabel atau saluran telepon yang menghubungkan sepasang router. Bila dua router yang tidak menggunakan kabel yang sama akan melakukan komunikasi, keduanya harus berkomunikasi secara tidak langsung melalui router lainnya. Ketika sebuah paket dikirimkan dari sebuah router ke router lainnya melalui sebuah router perantara atau lebih, maka paket akan diterima router perantara dalam keadaan lengkap, disimpan sampai saluran output menjadi bebas, dan kemudian baru diteruskan[1].

2.1.2 Berdasarkan Media Transmisi

Media transmisi adalah zat atau benda penghubung antar perangkat yang merambatkan sinyal sinyal informasi dari data yang saling di pertukarkan pada jaringan. Berdasarkan media transmisinya jaringan dibagi menjadi dua jenis, yaitu:

1. *Wired Network*

   Wired network disebut juga *guided media* adalah jaringan yang menggunakan kabel sebagai media transmisinya. Pada umumnya kabel yang digunakan pada LAN adalah kabel UTP, yaitu kabel yang memiliki tembaga sebagai intinya, mengalirkan data menggunakan sinyal listrik . ada juga kabel dengan fiber optik sebagai intinya, mengalirkan data dengan merambatkan sinyal berupa gelombang cahaya.

2. *Wireless Network*

   Wireless network atau *unguided media*,menggunakan sinyal satelit, gelombang radio, microwave atau infrared sebagai media transmisinya

2.1.3 Berdasarkan Fungsi

Berdasarkan fungsinya jaringan komputer dibagi menjadi dua jenis, yaitu:

1. *Client-Server*

Merupakan jaringan komputer yang didalamnya terdapat komputer yang berperan sebagai *client* dan sebagai *server*. *Client* adalah komputer yang berperan penerima layanan dalam sebuah jaringan. *Server* adalah sebuah komputer yang cenderung lebih kuat dari *client* dan berperan penyedia layanan dalam sebuah jaringan yang mampu menangani banyak permintaan layanan secara serentak.

2. *Peer to Peer*

   Peer to peer adalah jaringan komputer yang mana didalamnya setiap komputer memiliki kedudukan dan hak akses untuk bertukar data yang sama.

2.1.4 Berdasarkan Tipe Koneksi

Berdasarkan tipe koneksinya jaringan komputer dibagi menjadi dua bagian, yaitu:

1. Point-to-Point

   Tipe koneksi point to point menyediakan sebuah link diantara dua perangkat jaringan. Yang mana kapasitas link tersebut hanya diperuntukan bagi kedua perangkat tersebut.[2]

2. Multipoint

   Pada tipe koneksi multipoint sebuah link bisa digunakan lebih dari dua perangkat jaringan. Pada lingkungan mutlipoint, kapasitas kanal dari link tersebut dibagi, apakah secara spasial atau temporal.[2]

2.2 Topologi Jaringan

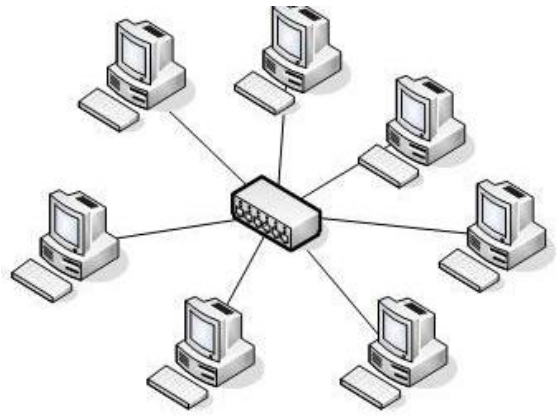
Topologi jaringan adalah konfigurasi pola atau cara bagaimana komponen-komponen dalam sebuah jaringan komputer saling terhubung. Topologi jaringan dibagi menjadi dua jenis, yaitu topologi fisik dan topologi logika.

2.2.1 Topologi Fisik

Topologi fisik atau *physical topology* merupakan bentuk nyata dari konfigurasi pola hubungan antara device yang terhubung pada jaringan (*node*) . Topologi jaringan yang sering digunakan diantaranya adalah:

1. Topologi Star

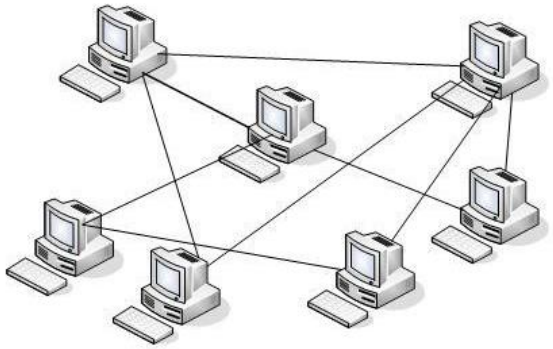
   Dalam topologi ini salah satu dari konsentrator berupa hub atau switch dibuat menjadi pusat sehingga setiap data yang keluar atau masuk dari setiap node akan melewati konsentrator terlebih dahulu. Bentuk topologi star diperlihatkan pada Gambar 2.1.



Gambar 2.1 Topologi Star

2. Topologi Mesh

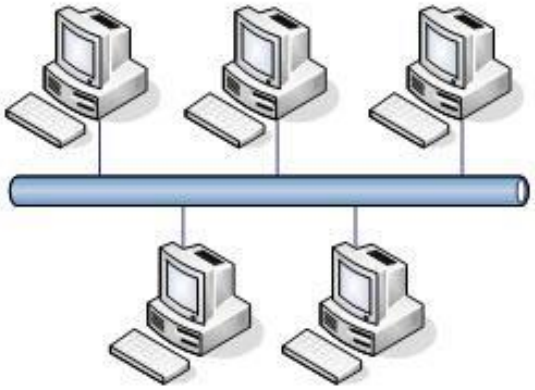
   Pada topologi ini konsentrator tidak diperlikan, karena tiap node berhubungan satu sama lain secara langsung. Topologi ini cenderung membutuhkan media transmisi lebih banyak. Bentuk dari topologi mesh diperlihatkan pada Gambar 2.2.



Gambar 2.2 Topologi Mesh

3. Topologi Bus

Topologi ini sering juga disebut topologi *backbone*.dimana sebuah kabel coaxial dibentangkan dan diberi terminator di setiap ujungnya, kemudian beberapa node dihubungkan kekabel tersebut menggunakan konektor T. Bentuk topologi bus diperlihatkan pada Gambar 2.3.

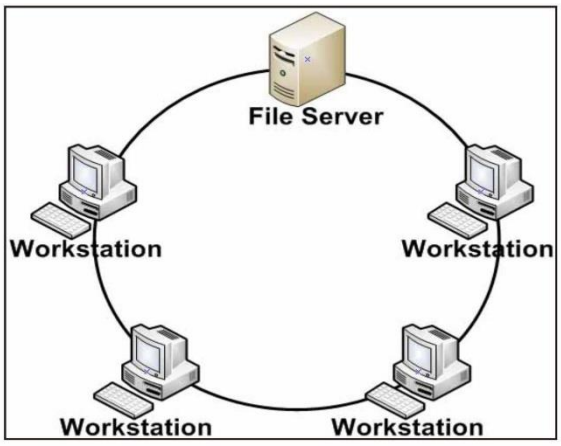


Gambar 2.3 Topologi Bus

4. Topologi Ring

Pada topologi ini setiap node dihubungkan media transmisi secara serial sehingga membentuk lingkaran aliran data hanya bisa mengalir ke satu arah.oleh karena itu, ketika salah satu node mati, maka seluruh aktifitas pertukaran data akan lumpuh.

Bentuk topologi ring diperlihatkan pada Gambar 2.4



Gambar 2.4 Topologi Ring

2.2.2 Topologi Logikal

Topologi logikal menjelaskan tentang bagaimana bentuk aliran data serta aturan saat ditransmisikan. Berikut ini beberapa topologi logikal yang dibedakan berdasarkan metode aksesnya.

1. *Shared Media Topology*

   Pada topologi ini seluruh *node* bisa dengan bebas kapanpun mengirim ataupun menerima data melalui media transmisi yang tersedia. Hal ini berpengaruh positif pada fleksibilitas waktu pengiriman atau penerimaan data. Namun di sisi lain jika beberapa *node* melakukan pengiriman secara serentak, ada kemungkinan terjadi *collision.* Topologi ini digunakan pada semua teknologi ethernet card

2. *Token Based Topology*

   Pada topoligi ini sebuah frame yang bertugas untung mengatur akses seluruh *node* ke media transmisi. Frame ini bernama *token.* Pergerakan *token* selalu satu arah, berkeliling mengunjungi tiap tiap node pada jaringan. Jadi karenatoken hanya mengunjungi satu *node* dalam satu waktu, tiap *node* harus menunggu giliran untuk mengakses media. Delay pengiriman data memang pasti terjadi, namun dengan topologi ini, kemungkinan tabrakan hampir tidak mungkin terjadi.

2.3 Protokol Jaringan

Protokol adalah sebuah set aturan yang mengatur komunikasi data. Protokol jaringan mendefinisikan apa yang dikomunikasikan, bagaimana caranya, dan kapan waktunya.[2]. Protokol pada jaringan komputer bisa dimisalkan sebagai bahasa, sehingga komputer akan bisa saling berkomunikasi apabila pengirim dan penerima tahu dan setuju untuk menggunakan bahasa yang sama.

2.4 OSI Model (*Open System Interconnection*)

OSI model merupakan acuan protokol jaringan yang di kembangkan oleh *International Organization of Standarization* (ISO) yang dimaksudkan sebagai standar protokol yang bisa diigunakan oleh semua vendor, komponen jaringan komputer agar komunikasi antar vendor menjadi mungkin. OSI model terdiri dari tujuh lapisan. Yangmana setiap lapisan harus bisa berkpmunikasi dengan lapisan

yangada di atasnya atau pun yang dibawahnya. Berikut gambaran dari OSI model ditampilkan pada Gambar 2.5.



Gambar 2.5 Layer pada OSI model

Berikut penjelasan dari fungsi setiap layer yang dimiliki OSI model :

1. *Physical Layer*

   Layer ini berfungsi untuk mengatur NIC yang terhubung pada media transmisi, juga bertanggungjawab untuk metode pengsinyalan saat transmisi data dilakukan.

2. *Data Link Layer*

   Layer ini membagi aliran bit yang di terima dari laposan network menjadi *frame*. Tugas utama dari layer ini adalah *error checking*, *flow control*, dan *media access control* untuk mengatur frame yang akan dikirim.

3. *Network Layer*

   Layer ini berfungsi untuk menentukan-alamat IP, dan mencari jalur terbaik agar kemudian kemudian melakukan routing melalui internetworking dengan menggunakan router dan switch agar *packet* sampai ditujuan dengan benar.

4. *Transport Layer*

Berfungsi untuk membagi data menjadi segmen, dan memberi nomor urut agar bisa disusun kembali saat sampai ke tujuan. Dan juga menjamin reliabilitas koneksi *end to end*

5. *Session Layer*

   Layer ini menyiapkan saluran komunikasi dan terminal dalam hubungan antar terminal, menkoordinasikan proses pengiriman dan penerimaan serta mengatur pertukaran data. Lapisan ini membangun, mempertahankan dan menyelaraskan interaksi antara sistem komunikasi.

6. *Presentation layer*

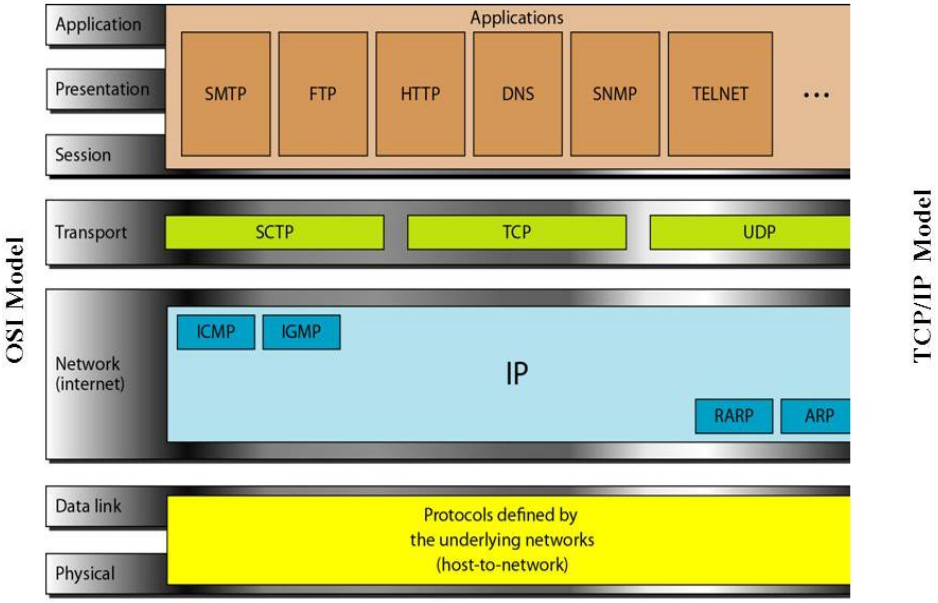
   Layer ini bertanggung jawab untuk mengkonversi, enkripsi juga kompresi data yang akan dikirim.

7. *Aplication Layer*

   Berfungsi sebagai antar muka dengan aplikasi dengan fungsionalitas jaringan. Mengatur bagaimana aplikasi dapat mengakses jaringan.

2.5 TCP/IP Protocol Suite

TCP/IP Protocol Suite adalah serangkaian protokol yang sudah dikembangan sebelum OSI Model ada. Berikut gambaran layer layer yang bekerja pada prtokol TCP/IP ditampilkan pada Gambar 2.6.



Gambar 2.6 OSI Model dan TCI/IP

Berikut penjelasan dari fungsi setiap layer yang dimiliki Protokol TCP/IP :

1. *Network Interface Layer*

   Layer ini berfungsi untuk mengatur NIC yang langsung terhubung pada media transmisi, juga bertanggungjawab untuk menangani *data flow control*. Pengalamatan pada layer ini menggunakan MAC address.

2. *Internet Protocol Layer*

   Layer ini bertugas untuk memulai, mempertahankan dan mengahiri hubungan *end to end*. pada proses transmisi data. Pengalamatan pada layer ini menggunakan IP address

3. *Transport Layer*

   Pada layer ini terdapat protokol TCP dan UDP yang bekerja sesuai dengan kebutuhan dari *application layer*. TCP menangani data data yang memerlukan tipe koneksi *connection oriented* dengan integritas pesan yang sangat reliabel. Sedangkan UDP menangani paket data yang memerluka tipe koneksi yang *connectionless* dengan kata lain, tidak reliabel namun

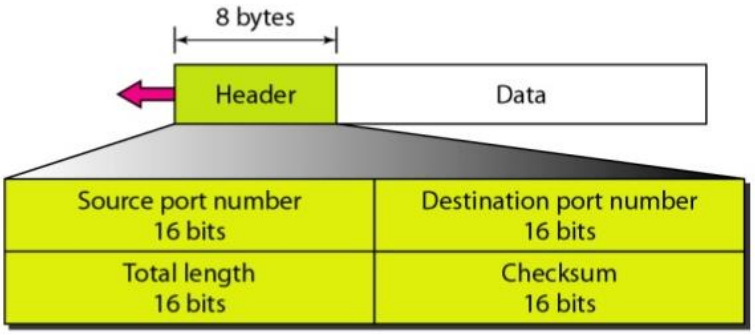
cenderung lebih cepat. Pengalamatan pada layer ini menggunakan port number.

4. *Application Layer*

   Layer ini memiliki fungsi setara dengan gabungan *application layer*,*presentation layer* dan *session layer* yang dimiliki OSI model.

2.6 Protokol UDP

User Datagram Protocol (UDP) adalah sebuah protokol yang berjalan di transport layer. Protokol ini memiliki service bertipe *connectionless* dan *unreliable.* Protokol ini tidak memerlukan jabat tangan untuk memulai pengiriman paket ke tujuan. Protokol ini memiliki header yang sangat simple, yang mana sehingga ketika sebuah proses ingin mengirim sebuah pesan kecil dan tidak mementingkan reiliabilitas, protokol ini bisa digunakan[2]. Berikut ini merupakan format paket UDP, atau disebut juga *user datagram*, diperlihatkan pada gambar 2.7



Gambar 2.7 Format User Datagram

Berikut adalah penjelasan dari Gambar 2.7:

1. *Source port number*, ini merupakan nomor port yang digunakan proses yang berjalan pada source host. Panjangnya 16 bit yang berarti nomor port bisa memiliki rentang dari 0 sampai 65535.
2. *Destination port number*, ini merupakan nomor port yang digunakan proses yang berjalan pada destination host. Panjangnya sama 16 bit yang berarti nomor port bisa memiliki rentang dari 0 sampai 65535. Apabila destinasi yang dituju adalah server biasanya nomor port yang digunakan adalah *well-known port.*
3. *Length*, memiliki panjang 16 bit, ini mendefinisikan panjang dari user datagram, header ditambah data, yakni 0 - 65535 byte.

4. *Checksum*, Bagian ini digunakan untuk mendeteksi error pada seluruh user datagram.

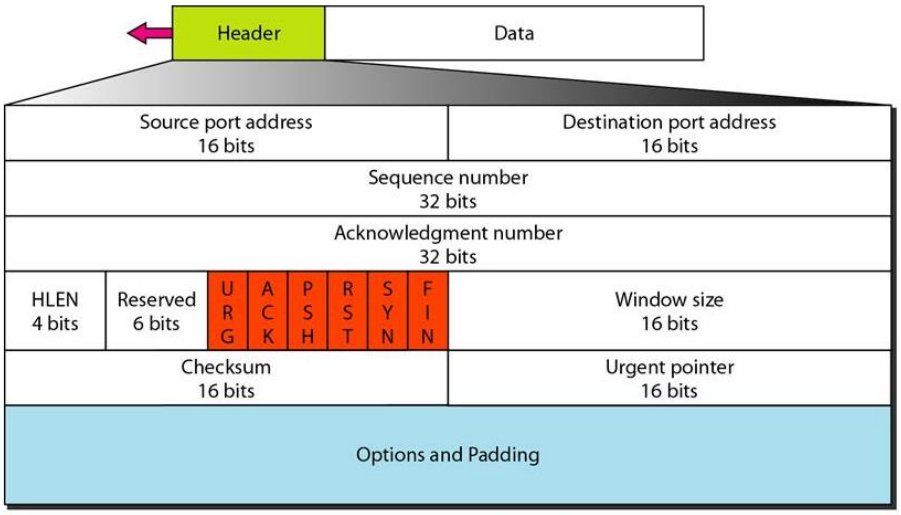
Berikut ini merupakan beberapa *well-known port* pada protokol UDP, diperlihatkan pada tabel 2.1

Tabel 2.1 Well-known Port yang Digunakan UDP

Port	Protokol	Deskripsi
7	Echo	Mengirim datagram yang diterima kembali kepengirim
9	Discard	Membuang datagram yang diterima
11	Users	*Active user*
13	Daytime	Membalas permintaan tanggal dan waktu
17	Quote	Membalas permintaan *quote of the day*
19	Chargen	Membalas permintaan string
53	Nameserver	Domain Name Service
67	BOOTPs	Port server untuk mengunduh informasi *bootstrap*
68	BOOTPs	Port client untuk mengunduh informasi *bootstrap*
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

2.7 Protokol TCP

Transmission Control Protocol (TCP) adalah sebuah protokol yang berjalan di transport layer. Protokol ini memiliki service bertipe *connection oriented* dan *reliable*. Tidak seperti UDP, TCP adalah *conncection-oriented protocol*; protokol ini membuat koneksi virtual diantara pengirim dan penerima untuk mengirim data[2]. TCP menggunakan mekanisme *flow control*,dan *error control* pada layer transport. Berikut adalah format paket TCP, atau disebut juga *segment*, diperlihatkan pada Gambar 2.8.

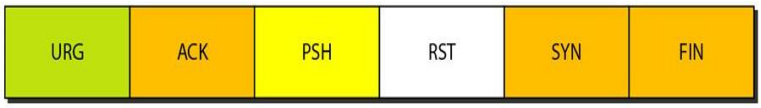


Gambar 2.8 Format Segment

Berikut adalah penjelasan dari Gambar 2.8:

1. *Source port number*, ini merupakan nomor port yang digunakan proses yang berjalan pada source host. Panjangnya 16 bit yang berarti nomor port bisa memiliki rentang dari 0 sampai 65535.
2. *Destination port number*, ini merupakan nomor port yang digunakan proses yang berjalan pada destination host. Panjangnya sama 16 bit yang berarti nomor port bisa memiliki rentang dari 0 sampai 65535.
3. *Sequence number*, panjangnya 32bit memiliki fungsi untuk menomori setiap segment yang akan dikirim.
4. *Acknowledgment number*, panjangnya 32bit memiliki fungsi untuk mendefinisikan nomor segment yang diharapkan oleh penerima dari pengirim di sesi pengiriman segment berikutnya.
5. *Header length*, panjangnya 4bit, mengindikasikan nomor dari 4 byte word pada header TCP. Panjang header memiliki rentang diantara 20 byte dan 60 byte. Sedangkan value dari header length bisa diantara 5 dan 15.
6. *Reserved*, merupakan 6 bit yang di sisakan untuk penggunaan dimasa yang akan datang.

7. *Control*, ini mendefinisikan 6 bit *control flag* seperti yang diperlihatkan pada Gambar 2.9.



Gambar 2.9 Control Flag

Berikut penjelasan 6 bit *control flag* dari Gambar 2.9 diperlihatkan pada Tabel 2.2.

Tabel 2.2 Deskripsi dari Control Flag

Flag	Deskripsi
URG	Nilai dari *urgent pointer* valid
ACK	Nilai dari *Acknowledgment* valid
PSH	Push data
RST	Reset koneksi
SYN	Singkronisasi *sequence number* saat koneksi
FIN	Akhiri koneksi

8. *Window Size*, mendefinisikan seberapa besar window yang digunakan keduabelah pihak dalam proses pengiriman data, dalam hal ini penerima mengikuti pengirim.
9. *Checksum*, bagian ini digunakan untuk mendeteksi error pada seluruh segment. Pada UDP *checksum* opsional, namun pada TCP *checksum* harus dilakukan.
10. *Urgent pointer*, panjangnya 16 bit, hanya akan dianggap valid jika flag URG di set.
11. *Options*, merupakan tempat untuk menambahkan informasi opsional pada TCP header. Panjangnya bisa mencapai 40 byte.

Berikut ini merupakan beberapa *well-known port* pada protokol TCP, diperlihatkan pada tabel 2.3

Tabel 2.3 Well-known Port yang digunakan TCP

Port	Protokol	Deskripsi
7	Echo	Mengirim datagram yang diterima kembali kepengirim
9	Discard	Membuang datagram yang diterima
11	Users	*Active user*
13	Daytime	Membalas permintaan tanggal dan waktu
17	Quote	Membalas permintaan *quote of the day*
19	Chargen	Membalas permintaan string
20	FTP,Data	File Transfer Protocol (data connection)
21	FTP,Control	File Transfer Protocol (control connection)
22	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol;
111	RPC	Remote Procedur Call

2.8 IPv4

IP address adalah nomor yang berfungsi sebagai tanda pengenal logis masing masing device pada jaringan komputer yang diperlukan untuk saling berkomunikasi. IPv4 dikembangkan pada tahun 1980. Pengalamatan IP versi 4 memiliki pengalamatan terstruktur, terdiri dari 32 bit yang dibagi dalam 4 segmen. Tiap segmen terdiri atas 8 bit yang berarti memiliki nilai decimal dari 0 sampai 255. Jadi jaringan TCP/IP dengan alamat 32 bit ini mampu membuat sebanyak 2^{32} atau lebih dari 4 milyar *host*.

2.8.1 Classful Addressing

Pengalamatan IPv4 yang menerapkan konsep kelas pada pembagianya disebut *classful addressing.* Pada pengalamatan ini IP address dibagi menjadi lima kelas, yaitu kelas A, B, C, D, dan E. Pada pengalamatan ini, alamat IP dibagi menjadi dua bagian, yaitu netid dan hostid. Netid berfungsi untuk identifikasi satu network dengan network lainnya, sedangkan hostid berfungsi untuk identifikasi antar host dalam suatu jaringan. Pada tabel 2.4 ditunjukan bagaimana alamat IP didistribusikan kepada setiap kelas.

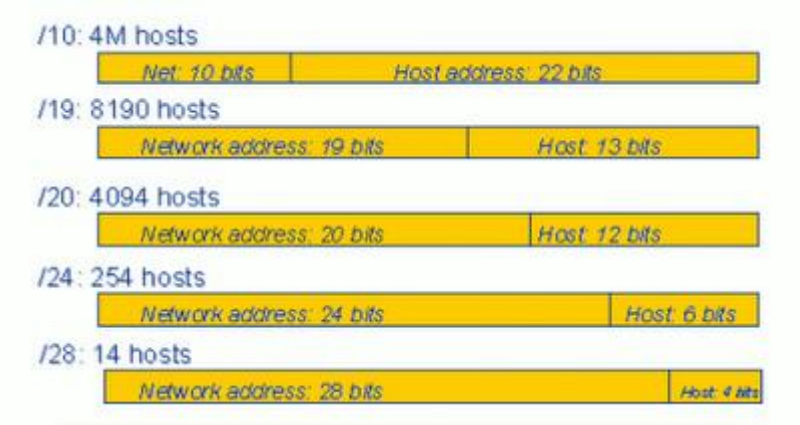
Tabel 2.4 Classful Addressing

Kelas	Oktet Pertama	Bit Oktet Pertama	Bagian NetID (N), HostID (H)	Subnetmask	CIDR
A	1 -127	00000000 – 01111111	N.H.H.H	255.0.0.0	/8
B	128-191	10000000 – 10111111	N.N.H.H	255.255.0.0	/16
C	192-223	11000000 – 11011111	N.N.N.H	255.255.255.0	/24
D	224-239	11100000 - 11101111	- (multicast)	-	
E	240-255	11110000 – 11111111	- (experimental)	-	

2.8.2 Classless Addressing

Pada konsep *classless* apabila sebuah jaringan baik besar ataupun kecil, hendak terhubung dengan jaringan lain, maka pengalamatan IP bisa dilakukan sesuai dengan kebutuhan host pada jaringan tersebut tanpa menggunakan kelas.

Subnetting adalah sebuah proses pemecahan sebuah jaringan menjadi beberapa jaringan lebih kecil disebut subnet. Subnetting dilakukan dengan cara mengatur jumlah bit satu pada netmask, semakin banyak bit satu pada netmask, semakin kecil jumlah host pada jaringan tersebut. Sebaliknya, semakin sedikit bit satu pada netmask semakin banyak host yang bisa ditampung jaringan tersebut. Berikut adalah gambar yang menunjukan hubungan antara banyak host dengan jumlah bit “1’ pada netmask, diperlihatkan pada gambar 2.10



Gambar 2.10 Jumlah Host pada Classless Addressing

2.9 Sistem Keamanan Jaringan

Sistem keamanan jaringan adalah sebuah sistem yang dibangun untuk menjamin beberapa faktor utama keamanan jaringan, yakni:

1. Kerahasiaan *(Confidentiality)*

   Faktor terjaminnya kerahasiaan pertukaran data yang dilakukan. pengirim mengenkripsi dan penerima .mendekripsi. dan yang paling penting keduabelah pihak dapat mengerti isi data tersebut.

2. Autentikasi *(Authentication)*

   Faktor terjaminnya identitas pengirim dan penerima yang melakukan pertukaran data.hal ini menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul

   orang yang dimaksud, atau server yang dihubungi adalah betul-betul server yang asli.

3. Integritas *(Integrity)*

   Faktor terjaminnya data yang dikirim bisa sampai kepada penerima dengan utuh. Dan data tidak bisa diubah oleh pihak yang tidak berhak.

4. Ketersediaan *(Availability)*

   Faktor terjaminnya layanan yang tersedia pada jaringan dapat selalu diakses.

5. Bebas Sangkalan *(Non-Repudiation)*

   Faktor terjaminnya setelah pengirim mengirimkan perintah untuk melakukan sesuatu, maka dikemudian waktu pengirim tidak bisa menyangkal telah mengirimkan pesan tersebut.

Sistem keamanan ini diharapkan akan bisa menjaga faktor faktor ini agar selalu terjamin. Tapi tidak menutup kemungkinan keamanan jaringan akan terganggu oleh beberapa hal diantaranya: ancaman, kelemahan, dan serangan.

2.9.1 Ancaman (*Threat*)

Pada jaringan komputer Ancaman adalah segalahal yang berpotensi mengganggu operasi, fungsi, kerahasiaan, integritas, dan ketesediaan dari jaringan tersebut.

Microsoft membuat model klasifikasi dari ancaman *(threat)* pada keamanan komputer yang disebut STRIDE, didalamnya terdapat enam kategori yaitu:

1. *Spoofing*

   Hal yang memungkinkan seseorang atau suatu program menyamar menjadi seperti orang atau program lain dengan memalsukan data sehuingga memperoleh keuntungan yang tidak sah terhadap suatu sistem.
2. *Tampering*

   Hal yang memungkinkan seseorang untuk mengubah data atau kode dari suatu sistem tanpa hak akses yang sah.
3. *Repudiation*

   Hal yang memungkinkan seseorang untuk tidak mengakui atau menyangkal suatu aksi yang telah dilakukannya.
4. *Information Disclosure*

   Hal yang memungkinkan seseorang yang tidak memiliki hak untuk melihat data yang sepatutnya dirahasiakan.
5. *Denial of Service*

   Hal yang membuat terjadi penolakan atau penurunan performa dari sebuah layanan pada suatu sistem.
6. *Elevation of Privilege*

   Hal yang memungkinkan peningkatan kewenangan tidak sah terhadap hak akses pada suatu sistem

2.9.2 Kelemahan (*Vulnerability*)

Pada jaringan komputer kelemahan yang muncul, tidak lain merupakan efek dari kelemahan protokol pada jaringan itu sendiri. Misal pada protokol TCP/IP.di layer *Datalink* ada sebuah protokol yang bernama *Address Resolution Protocol*

(ARP) fungsinya untuk mentranslasi alamat logic (IP address) menjadi alamat fisik (MAC adress) atau sebaliknya berdasarkan ARP tables pada perangkat tersebut.. Adanya kemungkinan isi ARP table dirubah(*ARP Poisoning*) atau dikelabui (*ARP Spoofing)* menjadi kelemahan pada protokol ini, yang tentu berdampak juga pada jaringan.

Selain itu ada juga kelemahan yang disebabkan oleh kesalahan desain, konfigurasi, implementasi atau manajemen jaringan atau sistem yang membuat sistem rentan terhadap ancaman. Pada dasarnya setiap sistem dan jaringan pasti memiliki kelemahan.

2.9.3 Serangan (*Attack*)

Serangan adalah upaya untuk mengeksploitasi kelemahan sistem. Serangan terjadi berimbas pada kerahasiaan, integritas dan ketersediaan sistem tersebut. Ada dua tipe serangan yaitu serangan aktif dan pasif.

Serangan pasif merupakan serangan diam diam dan sulit dideteksi salah satu contohnya adalah packet sniffing (sadap). Sedangkan serangan aktif merupakan serangan yang mengakibatkan efek yang terlihat nyata, cenderung mudah di deteksi, contoh DoS hingga sebuah layanan pada server down.

Berikuet merupakan langkah langkah penyerangan pada jaringan.

1. *Reconaissance (footprinting)*

   Langkah pertama yang bertujuan untuk mengumpulkan informasi awal target, seperti alamat IP, DNS server, domain, table routing, sistem operasi dan lain sebagainya

2. *Vurnerability Scanning*

   Langkah selanjutnya adalah pencarian kelemahan sistem yang mungkin bisa dijadikan jalur penyusupan. Jalur penyusupan tersebut dapat berupa port yang umum digunakan oleh sistem, misal: port 80 untuk HTTP, port 21 untuk FTP, port 22 untuk Telnet, port 443 untuk SSH.

3. *Enumeration*

   Langkah ini dilakukan untuk mencari informasi yang lebih mendetail dari target seperti *user list*, *sharing folder*, dan layanan yang sedang berjalan pada target.

4. *Penetration*

   Pada langkah ini penyerang masuk kedalam sistem target menggunakan informasi yang telah terkumpul sebelumnya.

5. *Elevation*

   Setelah mendapatkan hak akses terhadap sistem pada langkah sebelumnya, kemudian penyerang meningkatkan hak aksesnya menjadi user yang memiliki akses penuh terhadap sistem seperti administrator. Setelahnya penyerang bebas melakukan eksploitasi apapun terhadap sistem tersebut

6. *Post-Exploitation*

   Setelah tujuannya tercapai penyerang biasanya memasang *rootkit* atau *backdoor* untuk memudahkan akses penyusupan kedepannya. Setelah itu penyerang membersihkan jejak penyusupannya.

2.10Mikrotik Router OS

Mikrotik RouterOS adalah sistem operasi yang berbasis CLI (command line interface) dikhususkan untuk membuat PC-router. Mikrotik dapat berjalan pada komputer yang berspesifikasi minimal processor kompatibel x86, RAM 32MB, media penyimpanan 64MB. Dengan fitur-fitur yang ada didalamnya administrator dapat membangun system keamanan jaringan menggunalan PC dengan spesifikasi

sangat minim, jika tersedia administrator dapat menghemat biaya dengan menggunakan PC yang tidak terpakai.

2.11Firewall

Firewall adalah sistem keamanan jaringan computer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari untrusted network. Firewall merupakan suatu alat (biasanya ada di router) yang didalamnya memiliki set aturan yang berfungsi untuk memutuskan apakah suatu packet akan dibiarkan lewat (*forward*) atau dibuang (*discard*) [2]

2.12Packet Sniffer

Packet Sniffer adalah sebuah alat untuk memantau paket-paket data yang melitas di jaringan. Informasi yang dikumpulkan oleh *packet sniffer* dapat digunakan administrator untuk mengidentifikasi masalah yang terjadi pada jaringan.

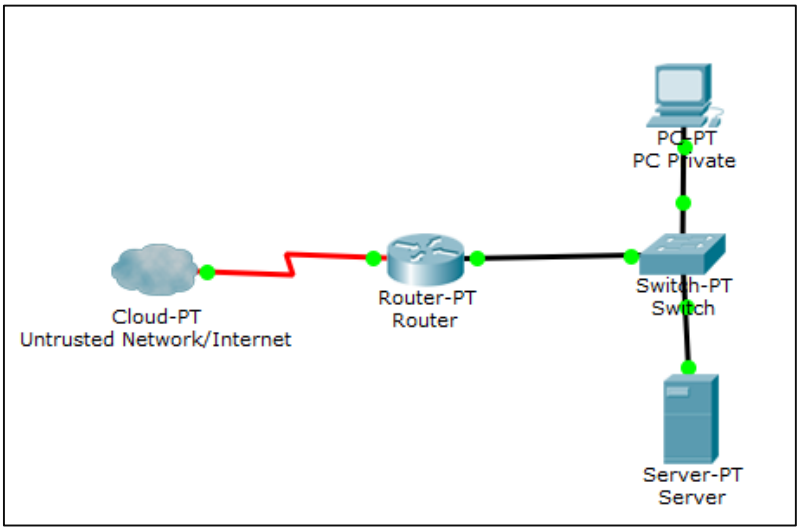
Packet sniffing dibagi menjadi dua jenis, yaitu *passive sniffing* dan *active sniffing*. *Passive sniffing* adalah suati kegiatan penyadapan tanpa merubah data atau paket apapun dalam jaringan, biasanya ditempatkan pada hub. Contoh aplikasinya adalah wireshark, cain&abel, dan ada juga packet sniffer bawaan mikrotik.Sedangkan *Active sniffing* adalah kegiatan penyadapan dengan melakukan perubahan data atau paket pada jaringan, misalnya melakukan *ARP posioning, Man in the Middle.*

2.13 Demilitarized Zone

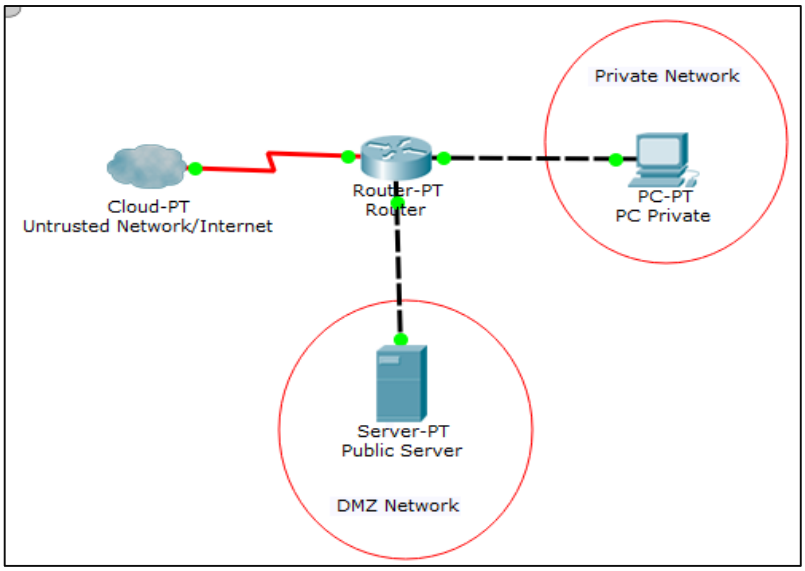
Demilitarized Zone adalah sebuah istilah kemiliteran untuk menyebut suatu kawasan di wilayah perbatasan dua atau lebih kekuatan militer yang mana didalam kawasan tersebut tidak diperkenankan adanya aktifitas militer apapun Biasanya wilayah ini berfungsi untuk melindungi wilayah yang memiliki keanekaragaman flora dan fauna, atau tergantung dari isi perjanjian damai, gencatan senjata, atau perjanjian bilateral atau multilateral lainnya.

Dalam istilah komputerisasi *Demilitarized Zone* (DMZ) adalah adalah metode untuk membagi jaringan dan layanan yang perlu diberikan kepada pengguna, pengunjung, atau patner melalui penggunaan firewall dan beberapa lapisan penyaringan dan kontrol untuk melindungi sistem internal [3]. DMZ sering

disebut juga jaringan perimeter adalah sebuah metode dimana dibuatnya jaringan tambahan yang berada diantara *private network* dan *untrusted network* (Internet). Sehingga akses dari *untrusted network* ke *private network* dapat diperketat. Selain itu, layanan server yang sudah dipindahkan ke DMZ dapat dengan mudah diakses oleh publik. Gambaran dari topologi jaringan sebelum DMZ diterapkan diperlihatkan pada gambar2.11 ,sedangkan gambar 2.12 memperlihatakan topologi jaringan setelah DMZ diterapkan.



Gambar 2.11 Topology Jaringan Sebelum DMZ Diterapkan



Gambar 2.12 Topology Jaringan Setelah DMZ Diterapkan

2.14 Intrusion Detection System

Intrusion Detection system (IDS) adalah suatu sistem yang digunakan untuk mencatat log seluruh lalulintas data pada jaringan untuk kemudian diperiksa jika ada pola-pola yang dicurigai sebagai usaha penyusupan pada jaringan. IDS secara otomatis akan memberi peringatan biasanya berupa email kepada administrator jika sebuah usaha penyusupan terdeteksi.

IDS memiliki metode untuk mendeteksi penyusupan, diantaranya *Signature-based* mendeteksi dengan cara mencocokan paket data yang masuk dengan database IDS yang berisi pola-pola serangan yang sering digunakan oleh penyusup.Selain itu ada metode yang benama *Anomaly-based* mendeteksi dengan cara membandingkan lalu lintas data yang sedang dipantau dengan lalu lintas data keadaan normal (normal state)

2.15 Intrusion Prevention System

Intrusion Preventiong System (IPS) adalah suatu device atau program yang digunakan untuk mendeteksi tanda penyusupan pada sebuah sistem atau jaringan kemudian memberikan aksi. Aksi dalam hal ini bisa berupa membuat peringatan atau/dan memblokir penyusupan secara aktif. IPS adalah versi lebih maju dari *Intrusion Detection System (IDS).* Pada penelitian ini IPS menyediakan perlindungan dengan cara menambahkan IP address pengirim paket mencurigakan ke blacklist pada IP Address list di firewall, sehingga segala lalulintas data yang berasal dari IP tersebut akan ditolak. Secara umum, ada dua jenis IPS, yaitu *Host-based Intrusion Prevention System (HIPS)* dan *Network-based Intrusion Prevention System (NIPS).*

2.15.1 *Host-based Intrusion Prevention System (HIPS)*

Host-based Intrusion Prevention System (HIPS) dipasang secara langsung di sistem yang diproteksi untuk memonitor hanya keadaan hostnya. HIPS adalah versi lebih maju dari HIDS. HIPS ini melibatkan perangkat lunak atau komponen agen yang dijalankan pada server, router, switch atau alat jaringan. Namun, versi agen harus melaporkan ke konsol atau dapat dijalankan bersama-sama pada host yang sama. Pada dasarnya, HIPS jauh lebih baik dalam mendeteksi dan merespon serangan jangka panjang seperti pencurian data[4]. HIDS juga mampu melakukan pemeriksaan sistem tambahan yang hanya bisa dilakukan bila aplikasi IDS dipasang

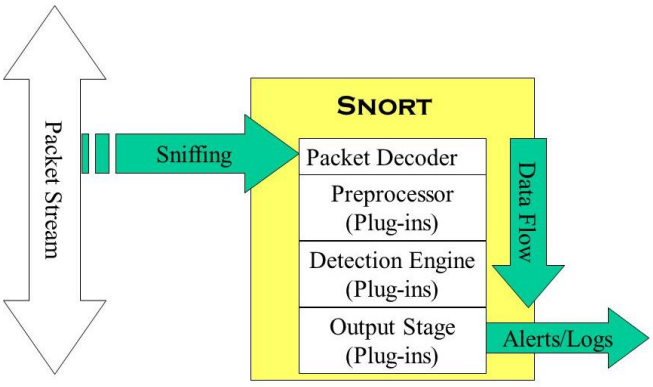
pada *host*, seperti *file integrity checking, registry monitoring.* Karena menginstall dan binding HIPS pada sistem operasi mengakibatkan penggunaan *resource* komputer host menjadi semakin besar.

2.15.2 Network-based Intrusion Prevention System (NIPS)

Network-based Intrusion Prevention System (NIPS) atau disebut juga I*n-line proactive protection* dapat memantau seluruh trafik pada jaringan yang dilindungi dan mendeteksi .tanda penyusupan yang mungkin terjadi. NIPS tidak harus melakukan pantauan secara khusus di satu host saja. Akan tetapi melakukan pantauan dan proteksi dalam satu jaringan secara global. Pada penelitian ini NIPS menggabungkan fitur NIDS sebagai pendeteksi, dan firewall sebagai pemblokir.

2.16 Snort

Snort adalah sebuah perangkatlunak *open-source,* multiplatform yang berfungsi sebagai sistem *network intrusion detection system* (NIDS). Snort mendeteksi penyusupan menggunakan metode Signature-based. Snort mampu melakukan analisis lalulintas data dan *packet-loging* secara *real-time* pada jaringan. Aplikasi ini bisa mendeteksi banyak tipe seragan diantaranya: *buffer overflows, stealth port scan, CGI Attack, SMB probes, dan OS fingger printing.* Berikut merupakan gambar dari aliran data pada snort diperlihatkan pada gambar 2.13



Gambar 2.13 Data Flow pada Snort

Berikut merupakan penjelasan dari gambar 2.13 :

1. *Sniffing*, pada tahap ini paket data yang melewati NIC akan disadap. Paket data yang di ambil merupakan paket data layer *datalink* atau layer ke dua dari ISO model seperti Ethernet Frames. Pada linux proses ini dilakukan menggunakan libpcap

2. *Packet Decoder,* pada tahap ini packet decoder men-*decode* seluruh data layer datalink yang disadap. Pertama adalah datalink frame seperti (ethernet, token ring, 802.11), kemudian protokol IP, kemudian paket TCP dan UDP. Sehingga snort mengetahui semua protokol yang digunakan paket tersebut.[5]
3. *Preprocessor,* pada tahap ini snort akan memproses paket data yang telah di-*decode* pada tahap sebelumnya. Preprocessor melakukan beberapa transformasi dan klasifikasi pada data agar mudah dicerna oleh snort ditahap berikutnya [5].
4. *Detection Engine* merupakan pusat dari IDS snort pada tahap ini snort akan menggunakan informasi yang terkumpul dari *packet decoder* dan *preprocessor*. Kemudian dibandingkan dengan informasi pada rule yang tersedia sebagai plugin pada snort[5].
5. *Output Stage,* ketika rule pada snort terpicu, sebuah alert akan dibuat dan dicatat. Ada beberapa jenis plugin output snort, salah satunya menggunakan *Syslog.*

2.16.1 Snort Rules

Snort memberikan banyak pilihan rule yang disediakan sebagai bagian dari instalasi bawaan. Lebih banyak lagi rule yang bisa digunakan dengan berlangganan ke www.snort.org [. Selain itu snort juga memberikan kebebasan untuk membuat rule agar bisa disesuaikan dengan kebutuhan jaringan yang dikelola. Berikut adalah rule snort untuk membuat alert jika mendeteksi ping request ke server.

```
Alert icmp any any -> 172.16.1.2 any \
(msg:”Ping request ke server terdeteksi”; \
Classtype:test-ping; priority:3; sid:1000001;)
```

Berikut ini merupakan penjelasan dari rule deteksi ping ke server, diperlihatkan pada Tabel 2.5

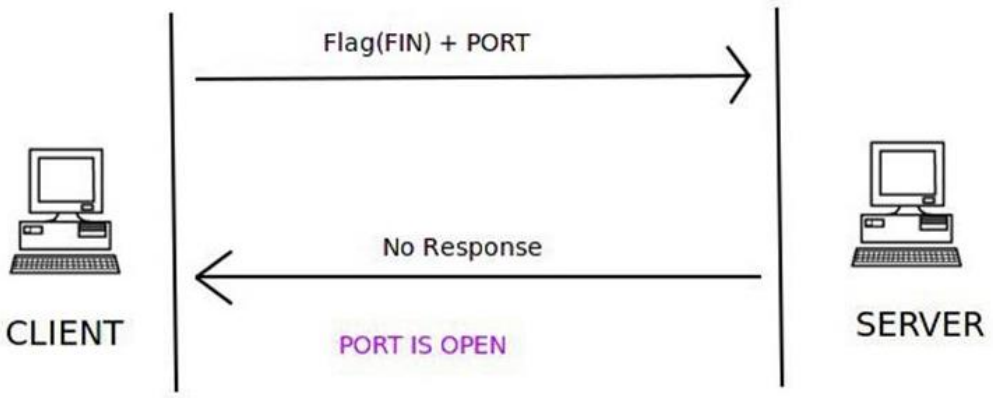
Tabel 2.5 Rincian Rule Deteksi Ping

No.	Field	Value	Deskripsi
1	Action	Alert	Keluarkan alert jika rule terpicu
2	Protocol	icmp	Protokol yang akan di filter
3	Src. Address	any	IP pengirim paket data
4	Src. Port	any	Port pengirim paket data
5	Data flow	->	Arah aliran data
6	Dst. Address	172.16.1.2	IP tujuan paket data
7	Dst. Port	any	Port tujuan paket data
8	(option1;	Msg:”Test Ping!”;	Pesan yang akan muncul pada output snort
9	Option2;	Classtype: test-ping;	Klasifikasi event
10	Option3;	Priority: 3;	Tingkat prioritas, 3 (rendah) 2(sedang) 1(tinggi)
11	Option4;)	Sid:1000001;)	Nomor unik identifikasi snort rule

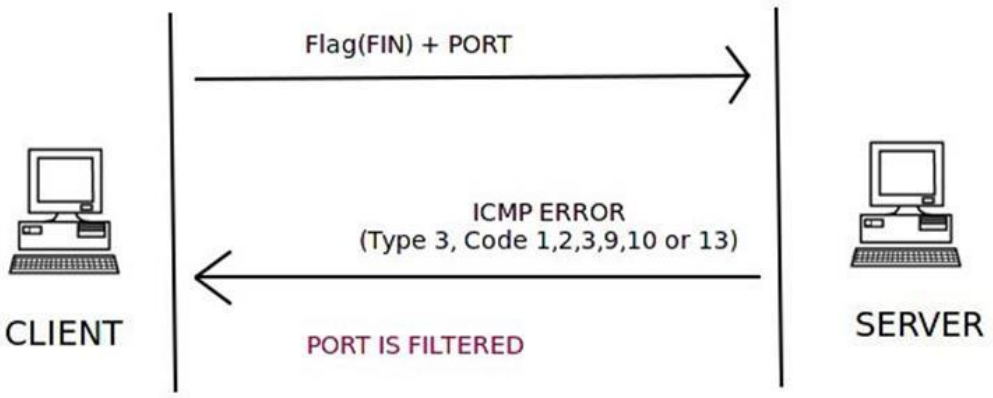
2.17 Scan FIN

Scan FIN adalah sebuah tehnik scanning yang manfaatkan kelemahan dari protokol TCP yaitu control flag FIN. Teknik ini dilakukan dengan cara mengirimkan sebuah paket tcp yang berisi hanya flag FIN yang di set kepada port milik sebuah host. Proses ini membuat port pada server yang dituju akan mengeluarkan respon tertentu.

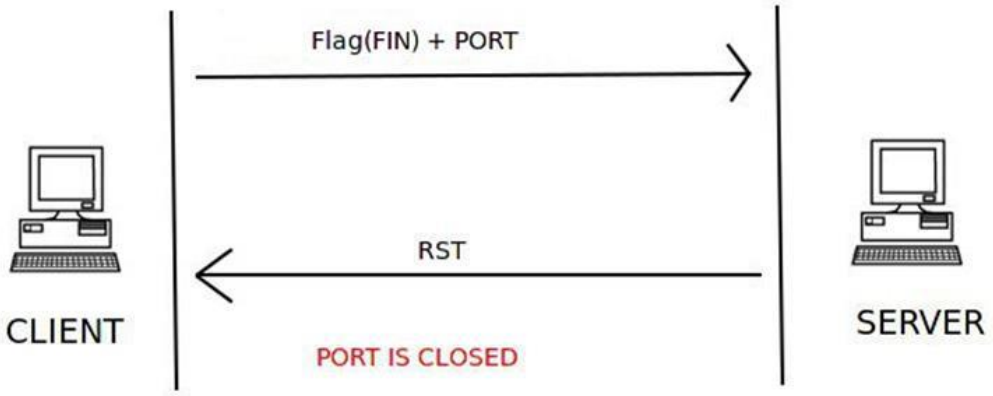
Berikut adalah respon yang diberikan jika scan FIN dilakukan pada sebuah port, diperlihatkan pada gambar 2.14, 2.15, dan 2.16.



Gambar 2.14 Respon Scan FIN jika Port Terbuka



Gambar 2.15 Respon Scan FIN jika Port Filtered



Gambar 2.16 Respon Scan FIN jika Port Tertutup

2.18 Ping of Death Attack

PoD Adalah salah satu jenis serangan *Denial of Sercive* (DoS) yang memanfaatkan bug Protokol ICMP yang berada pada layer IP. Dimana data icmp yang dikirim yang biasanya hanya sebesar 56 byte, dirubah menjadi lebih dari batasas maksimum paket IP yaitu 65.507 byte. Seperti paket besar lainnya, sebelum dikirim paket PoD akan dipecah menjadi beberapa bagian. Kemudian setelah ditransmisikan paket tersebut disusun kembali di pc target. Disinilah paket PoD menyebabkan *buffer over flow* yang mungkin menyebabkan sistem *crash.* Berikut adalah bentuk dari paket PoD, diperlihatkan pada gambar 2.17



Gambar 2.17 Paket Ping of Death

2.19 Apache Range Header Attack

Disebut juga *Apache Killer*, merupakan salah satu serangan *Denial of Sercive* (DoS) yang memanfaatkan *HTTP range request header data* pada webserver Apache 2. Header ini biasanya digunakan ketika client melakukan request file yang terlalu besar untuk dikirimkan dalam satu sesi, sehingga client meminta file tersebut dibagi menjadi beberapa segmen. Serangan dilakukan dengan cara mengirimkan sebuah *http request* yang memiliki banyak field yang dibuat saling timpang tindih didalam *range header*-nya. Berikut adalah contoh http request yang digunakan *Apache Killer.*

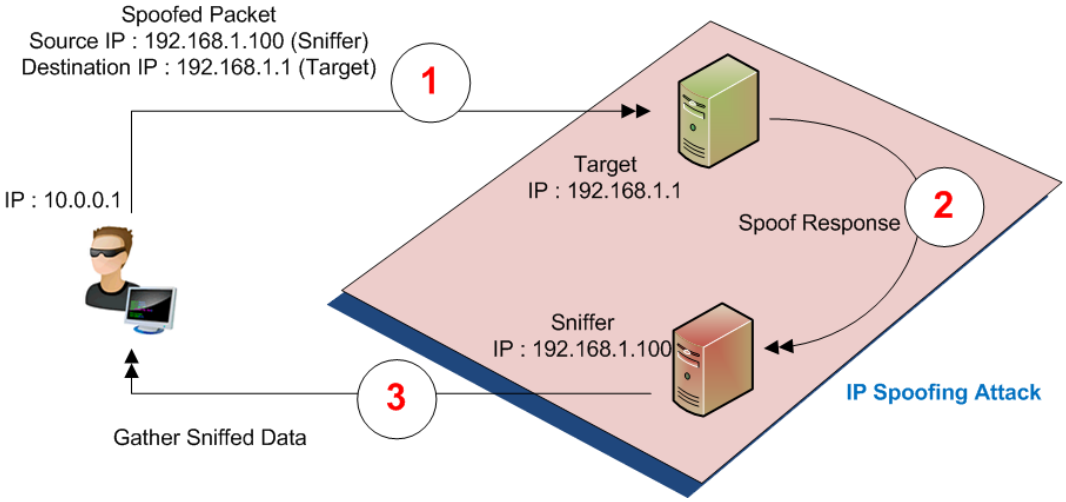
```
HEAD / HTTP/1.1Host: 127.0.0.1Range: bytes=0-,5-0,5-
1,5-2,5-3,5-4,5-5,5-6,5-7,5-8,5-9,5-10, . . .
```

Dengan mengirimkan request ini, penyerang memaksa webserver Apache untuk membuat salinan terpisah dari setiap byte pada field *range header*, yang mana akan menguras sumber daya dari server tersebut.

2.20 IP Spoofing

IP Spoofing adalah sebuah teknik dimana dibuatnya sebuap paket IP dengan *source address* yang dipalsukan. Hal ini memungkinkan sebuah node pada jaringan untuk memanipulasi aliran data atau bahkan bertindak sebagai node lain.

Berikut gambaran umum dari teknik *IP spoofing* diperlihatkan pada gambar 2.18



Gambar 2.188 Teknik IP spoofing