

Soal 1

Resume Telecommunications and Network Security

Menurut referensi dari ebook CISSP

Pengertian simplex duplex, half duplex dan full duplex

A. *Simplex*

Adalah mode komunikasi satu arah. Di sini pihak penerima tidak dapat memberikan informasi balikan. Atau sering juga disebut komunikasi broadcast (media penyiaran). Contoh yang sering ditemukan menggunakan mode ini adalah siaran televisi dan siaran radio. Disebut mode simplex karena saat anda menonton sinetron anda tidak diperkenankan untuk berkomunikasi dengan para pemain di sinetron tersebut.

B. *duplex*

Duplex adalah media komunikasi dua arah. Dimana pihak pengirim dan penerima bisa berkomunikasi dua arah secara bersama-sama. Contoh media yang menggunakan mode ini adalah telepon baik selular maupun fixed telepon rumah. Kedua belah pihak bisa berbincang secara bersama-sama.

C. *Half Duplex*

Adalah media komunikasi dua arah. Namun berbeda dengan *duplex*, *half duplex* berkomunikasi dua arah secara saling bergantian. Jadi saat terjadi komunikasi antara A dan B. Saat A mengirim informasi (berbicara) maka B akan menerima informasi (mendengarkan). Demikian terjadi proses yang sebaliknya (*vice versa*). Contoh media yang menggunakan media ini adalah radio walkie talkie.

D. *full duplex*

Dalam komunikasi *full-duplex*, dua pihak yang saling berkomunikasi akan mengirimkan informasi dan menerima informasi dalam waktu yang sama, dan umumnya membutuhkan dua jalur komunikasi.

Komunikasi full-duplex juga dapat diraih dengan menggunakan teknik multiplexing, di mana sinyal yang berjalan dengan arah yang berbeda akan diletakkan pada slot waktu (time slot) yang berbeda. Kelemahan teknik ini adalah bahwa teknik ini memotong kecepatan transmisi yang mungkin menjadi setengahnya.

Macam-macam Jaringan

1. LAN (Local Area Network)

Local Area Network atau LAN, merupakan suatu Jenis Jaringan Komputer dengan mencakup wilayah lokal.

Keuntungan dari penggunaan Jenis Jaringan Komputer LAN seperti lebih irit dalam pengeluaran biaya operasional, lebih irit dalam penggunaan kabel, transfer data antar node dan komputer lebih cepat karena mencakup wilayah yang sempit atau lokal, dan tidak memerlukan operator telekomunikasi untuk membuat sebuah jaringan LAN.

Kerugian dari penggunaan Jenis Jaringan LAN adalah cakupan wilayah jaringan lebih sempit sehingga untuk berkomunikasi ke luar jaringan menjadi lebih sulit dan area cakupan transfer data tidak begitu luas.

2. MAN (Metropolitan Area Network)

MAN (Metropolitan Area Network) adalah suatu jaringan dalam suatu kota dengan transfer data berkecepatan tinggi, yang menghubungkan berbagai lokasi, seperti; Kampus, perkantoran, pemerintah, dll.

Jaringan MAN adalah gabungan dari beberapa LAN. Jangkauan dari MAN ini antar 10 hingga 50 km, MAN ini merupakan jaringan yang tepat untuk membangun jaringan antar kantor-kantor dalam satu kota antara pabrik/instansi dan kantor pusat yang berada dalam jangkauannya.

3. WAN (Wide Area Network)

WAN (Wide Area Network) merupakan jaringan komputer yang mencakup area yang besar sebagai contoh yaitu jaringan komputer antar wilayah, kota atau bahkan negara, atau dapat didefinisikan juga sebagai jaringan komputer yang membutuhkan *router* dan saluran komunikasi publik.

WAN digunakan untuk menghubungkan jaringan area lokal yang satu dengan jaringan lokal yang lain, sehingga pengguna atau komputer di lokasi yang satu dapat berkomunikasi dengan pengguna dan komputer di lokasi yang lain

4. INTRANET

Intranet adalah sebuah jaringan komputer berbasis protokol TCP/IP seperti internet hanya saja digunakan dalam internal perusahaan, kantor, bahkan warung internet (WARNET) pun dapat di kategorikan Intranet.

5. INTERNET

Internet dapat diartikan sebagai jaringan komputer luas dan besar yang mendunia, yaitu menghubungkan pemakai komputer dari suatu negara ke negara lain di seluruh dunia, dimana di dalamnya terdapat berbagai sumber daya informasi dari mulai yang statis hingga yang dinamis dan interaktif.

OSI LAYER

Berikut ini Fungsi Masing-Masing Layer beserta Protokol dan Perangkatnya

1. **Physical Layer** : Berfungsi untuk mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan, topologi jaringan dan pengabelan. Adapun perangkat-perangkat yang dapat dihubungkan dengan Physical layer adalah NIC (Network Interface Card) berikut dengan Kabel - kabelnya
2. **DataLink Layer** : Berfungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Pada Layer ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras seperti halnya MAC Address, dan menentukan bagaimana perangkat-perangkat jaringan seperti HUB, Bridge, Repeater, dan Switch layer 2 (Switch un-manage) beroperasi. Spesifikasi IEEE 802, membagi Layer ini menjadi dua Layer anak, yaitu lapisan Logical Link Control (LLC) dan lapisan Media Access Control (MAC).
3. **Network Layer** : Berfungsi untuk mendefinisikan alamat-alamat IP, membuat header untuk paket-paket, dan kemudian melakukan routing melalui internetworking dengan menggunakan Router dan Switch layer-3 (Switch Manage).
4. **Transport Layer** : Berfungsi untuk memecah data ke dalam paket-paket data serta memberikan nomor urut ke paket-paket tersebut sehingga dapat disusun kembali pada sisi tujuan setelah diterima. Selain itu, pada layer ini juga membuat sebuah tanda bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang di tengah jalan.
5. **Session Layer** : Berfungsi untuk mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Selain itu, di layer ini juga dilakukan resolusi nama.
6. **Presentation Layer** : Berfungsi untuk mentranslasikan data yang hendak ditransmisikan oleh aplikasi ke dalam format yang dapat ditransmisikan melalui jaringan. Protokol yang berada dalam Layer ini adalah perangkat lunak redirektor

(redirector software), seperti layanan Workstation (dalam Windows NT) dan juga Network shell (semacam Virtual Network Computing (VNC) atau Remote Desktop Protocol (RDP)).

7. **Application Layer** : Berfungsi sebagai antarmuka dengan aplikasi dengan fungsionalitas jaringan, mengatur bagaimana aplikasi dapat mengakses jaringan, dan kemudian membuat pesan-pesan kesalahan. Protokol yang berada dalam layer ini adalah HTTP, FTP, SMTP, dan NFS.

Dari ke Tujuh layer tersebut mempunyai 2 (dua) Tingkatan Layer, yaitu:

1. Lower Layer yang meliputi : Physical Layer, DataLink Layer, dan Network Layer.
2. Upper Layer yang meliputi : Transport Layer, Session Layer, Presentation Layer, dan Application Layer

PENGERTIAN DAN JENIS-JENIS PROTOKOL JARINGAN

Protokol adalah sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.

TCP/IP (singkatan dari Transmission Control Protocol/Internet Protocol)

Adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet.

UDP (User Datagram Protokol)

UDP, singkatan dari User Datagram Protocol, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (unreliable), tanpa koneksi (connectionless) antara host-host dalam jaringan yang menggunakan TCP/IP. Protokol ini didefinisikan dalam RFC 768.

Domain Name System (DNS)

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang menggunakan TCP/IP (Transmission Control Protocol/Internet Protocol).

Point-to-Point Protocol

Point-to-Point Protocol (sering disingkat menjadi PPP) adalah sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network (WAN).

Serial Line Internet Protocol

Serial Line Internet Protocol dianggap berkaitan erat dengan pengertian berikut
Disingkat dengan SLIP.

Internet Control Message Protocol (ICMP)

adalah salah satu protokol inti dari keluarga. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau.

POP3 (Post Office Protocol)

POP3 adalah kepanjangan dari Post Office Protocol version 3, yakni protokol yang digunakan untuk mengambil email dari email server.

IMAP (Internet Message Access Protocol)

IMAP (Internet Message Access Protocol) adalah protokol standar untuk mengakses/mengambil e-mail dari server.

SMTP (Simple Mail Transfer Protocol)

adalah suatu protokol yang umum digunakan untuk pengiriman surat elektronik atau email di Internet. Protokol ini digunakan untuk mengirimkan data dari komputer pengirim surat elektronik ke server surat elektronik penerima.

HTTP (Hypertext Transfer Protocol)

HTTP (Hypertext Transfer Protocol) suatu protokol yang digunakan oleh WWW (World Wide Web). HTTP mendefinisikan bagaimana suatu pesan bisa diformat dan dikirimkan dari server ke client.

HTTPS

HTTPS adalah versi aman dari HTTP, protokol komunikasi dari World Wide Web. Ditemukan oleh Netscape Communications Corporation untuk menyediakan autentikasi dan komunikasi tersandi dan penggunaan dalam komersial elektronik.

SSH (Secure Shell)

SSH adalah protokol jaringan yang memungkinkan pertukaran data secara aman antara dua komputer. SSH dapat digunakan untuk mengendalikan komputer dari jarak jauh mengirim file, membuat Tunnel yang terenkripsi dan lain-lain.

Telnet (Telecommunication network)

Adalah sebuah protokol jaringan yang digunakan di koneksi Internet atau Local Area Network. TELNET dikembangkan pada 1969 dan distandarisasi sebagai IETF STD 8, salah satu standar Internet pertama.

FTP (File Transfer Protocol)

FTP (File Transfer Protocol) adalah sebuah protocol internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pentransferan berkas (file) computer antar mesin-mesin dalam sebuah internetwork

LDAP

LDAP (Lightweight Directory Access Protocol) adalah protokol perangkat lunak untuk memungkinkan semua orang mencari resource organisasi, perorangan dan lainnya, seperti file atau printer di dalam jaringan baik di internet atau intranet.

SSL (Secure Socket Layer)

Secure Sockets Layer (SSL) merupakan sistem yang digunakan untuk mengenkripsi pengiriman informasi pada internet, sehingga data dapat dikirim dengan aman. Protokol SSL mengatur keamanan dan integritas menggunakan enkripsi, autentikasi, dan kode autentikasi pesan.

Perangkat Jaringan (Network Device)

NIC (*Network Interface Card*) atau Kartu Jaringan

NIC adalah sebuah kartu yang berfungsi sebagai jembatan dari komputer ke sebuah jaringan komputer. Tugas NIC adalah untuk mengubah aliran data paralel dalam bus komputer menjadi bentuk data serial sehingga dapat ditransmisikan di atas media jaringan.

HUB

Hub adalah Alat penghubung antar komputer, semua jenis komunikasi hanya dilewatkan oleh hub. hub digunakan untuk sebuah bentuk jaringan yang sederhana (misal hanya untuk menyambungkan beberapa komputer di satu group IP lokal) ketika ada satu paket yang masuk ke satu port di hub, maka akan tersalin ke port lainnya di hub yg sama dan semua komputer yg tersambung di hub yang sama dapat membaca paket tersebut

SWITCH

Switch adalah Sebuah alat yang menyaring/filter dan melewatkan(mengijinkan lewat) paket yang ada di sebuah LAN. switcher bekerja pada layer data link (layer 2) dan terkadang di Network Layer (layer 3) berdasarkan referensi OSI Layer Model. sehingga dapat bekerja untuk paket protokol apapun.

BRIDGE

bridge membaca alamat MAC (media access control) dari setiap paket data yang diterima yang kemudian akan mempelajari bridging table untuk memutuskan apa yang akan dikerjakan bridge selanjutnya pada paket data tersebut, apakah diteruskan atau diabaikan.

ROUTER

Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Switch merupakan penghubung beberapa alat untuk membentuk suatu Local Area Network (LAN).

Soal 2

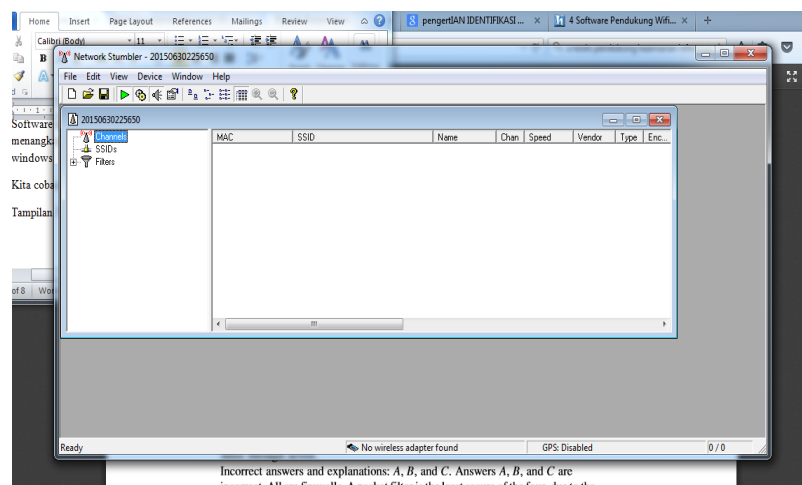
Software atau tools pendukung keamanan informasi

Saya Akan mengambil contoh software Network Stumbler

Software ini digunakan untuk memonitoring jaringan wireless. Aplikasi ini juga dapat menangkap sinyal wifi yang lebih jauh dari yg bisa di tangkap oleh software bawaan windows. Umumnya Aplikasi ini digunakan untuk keperluan Hacking.

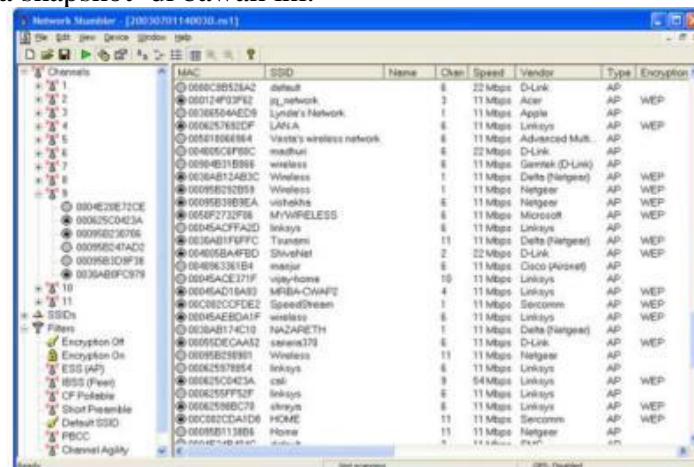
Kita coba install software NetStumbler

Tampilan Utama setelah di install seperti berikut ini



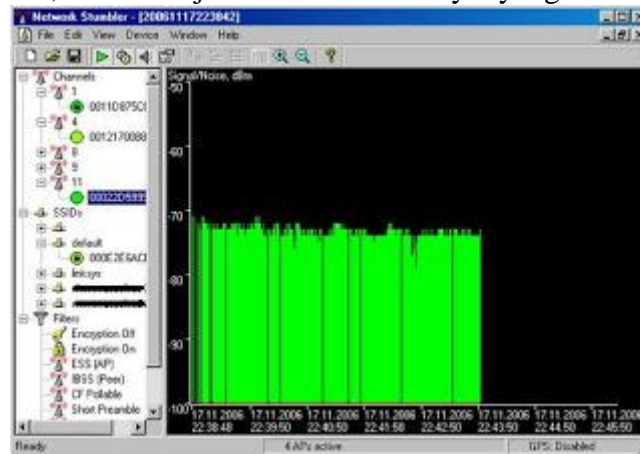
Cara menggunakan Netstumbler untuk Scanning Jaringan Nirkabel

1. Jalankan Netstumbler ini. Maka secara otomatis akan mulai memindai Jaringan nirkabel di sekitar yang aktif.
2. Setelah selesai, akan melihat daftar lengkap jaringan nirkabel di sekitar kita seperti yang ditunjukkan pada snapshot di bawah ini:



Di sini dapat melihat kolom yang berbeda seperti MAC, SSID, SPEED, VENDOR, JENIS, Dll

3. Coba kita pilih salah satu alamat MAC address yang ingin kita cari informasinya, lalu akan melihat grafik yang menunjukkan jaringan nirkabel kekuatan 's sinyal. Semakin hijau dan ruang kurang di sana, itu menunjukkan kekuatan sinyal yang lebih baik adalah.



5. Seperti yang Anda lihat Netstumbler menyediakan banyak lebih dari sekedar nama (SSID) dari jaringan nirkabel. Ini menyediakan alamat MAC, saluran nomor, enkripsi jenis, dan banyak lagi. Semua ini datang di gunakan ketika kita memutuskan bahwa kita ingin mendapatkan dalam jaringan diamankan oleh enkripsi retak.

Cara Melindungi jaringan kita dari hacker yaitu dengan cara

1. Tidak broadcast SSID Anda.
2. Selalu mencoba untuk menggunakan password yang kuat seperti atleast satu digit, satu karakter khusus, Atau Kalimat yg susah di pahami.
3. Tapi intinya kedua tidak peduli banyak sehingga mencoba untuk menggunakan enkripsi metode yang lebih baik yaitu untuk melindungi sandi WAP Jaringan nirkabel Anda.