

Nama : Edo septian Pratama Putra  
Nim : 1310651186  
Kelas : E

# Telecommunications and Network Security

## ➤ Telekomunikasi dan keamanan jaringan

Telekomunikasi dan jaringan keamanan adalah dasar kehidupan modern kita. Internet, world wide web, online banking, instant messaging e-mail, dan banyak teknologi lainnya mengandalkan keamanan jaringan.

Telekomunikasi dan keamanan jaringan adalah dasar kehidupan modern kita. Internet, world wide web, online banking, instant messaging e-mail, dan banyak teknologi lainnya mengandalkan keamanan jaringan

Telekomunikasi adalah salah satu domain terbesar di tubuh umum pengetahuan dan berisi lebih konsep dari domain lainnya. Domain ini juga salah satu domain yang paling teknis yang mendalam, yang membutuhkan pengetahuan teknis ke paket, segmen, frame, dan header mereka. Memahami domain ini sangat penting untuk memastikan keberhasilan pada ujian.

Arsitektur jaringan dan desain

Arsitektur jaringan dan desain membahas bagaimana jaringan harus dirancang dan kontrol

Konsep dasar jaringan

memahami konsep dasar jaringan. memerlukan pemahaman yang tepat dari informasi terminologi keamanan

## ➤ Simplex, half-duplex, dan komunikasi full-duplex

komunikasi simpleks adalah satu arah, seperti radio mobil disetel ke stasiun musik.

Halfduplex

komunikasi mengirim atau menerima pada satu waktu saja (tidak bersamaan), seperti walkie-talkie. Komunikasi full-duplex mengirim dan menerima secara bersamaan, seperti dua orang memiliki percakapan tatap muka.\

## ➤ Lan, wan, man, dan pans

sebuah lan adalah local area network. Sebuah lan adalah jaringan yang relatif kecil, biasanya terbatas pada bangunan atau area dalam satu. Sebuah man adalah metropolitan area network, yang biasanya terbatas pada sebuah kota, kode pos, kampus, atau office park. Sebuah wan

adalah wide area network, biasanya meliputi kota, negara, atau negara. Di ujung lain dari spektrum, yang terkecil dari jaringan ini adalah pans: personal area networks, dengan kisaran 100 m atau kurang. Teknologi nirkabel daya rendah seperti bluetooth digunakan untuk membuat pans.

### ➤ **Model osi.**

osi (open sistem interkoneksi) model referensi adalah jaringan layered model. Model ini abstrak: kita tidak langsung menjalankan model osi dalam sistem kami (paling sekarang menggunakan model tcp / ip); digunakan sebagai titik acuan, sehingga "layer 1" (fisik) secara universal dipahami, apakah anda menjalankan ethernet atau atm, model osi memiliki tujuh lapisan . Physical, data link, jaringan, transport, sesi, presentasi, dan aplikasi

#### ✓ **Tcp / ip model**

- **Network access layer**
- **Internet layer**
- **Host-to-host transport layer**
- **Application layer**
- **Mac addresses**

model tcp / ip (transmission control protocol / internet protocol) ,tcp / ip adalah nama informal (dinamai dua protokol pertama dibuat); nama resmi adalah internet protocol suite. Model tcp / ip lebih sederhana dari model osi, tcp / ip sebenarnya merupakan suite protokol termasuk udp (user datagram protocol) dan icmp (internet control message protocol), di antara banyak lainnya.

#### **Tcp**

tcp adalah transmission control protocol, layer 4 protokol yang handal. Tcp menggunakan jabat tangan tiga arah untuk membuat koneksi yang dapat diandalkan di seluruh jaringan. Tcp dapat menyusun ulang segmen yang tiba-tiba rusak dan memancarkan kembali segmen yang hilang.

##### **port tcp**

tcp menghubungkan dari port sumber ke port tujuan. Bidang tcp port adalah 16 bit, yang memungkinkan nomor port dari 0 sampai 65535. Ada dua jenis port: dilindungi dan singkat. Sebuah port dicadangkan adalah 1023 atau lebih rendah; port fana adalah 1024-65535. Sebagian besar sistem operasi membutuhkan hak akses superuser untuk membuka port-undang. Setiap pengguna dapat membuka (tidak terpakai) port fana.

#### **Udp**

udp adalah user datagram protocol, penghubung sederhana dan lebih cepat untuk tcp. Udp

umumnya digunakan untuk aplikasi yang "lossy" (dapat menangani beberapa packet loss), seperti streaming audio dan video. Hal ini juga digunakan untuk aplikasi permintaan-respon, seperti query dns.

icmp

icmp adalah internet control message protocol, yang membantu layer 3.

Icmp digunakan untuk memecahkan masalah dan melaporkan kondisi kesalahan: tanpa icmp untuk membantu, ip akan gagal ketika menghadapi routing yang loop, port, host, atau jaringan yang turun, dll

icmp tidak memiliki konsep port, tcp dan udp lakukan, melainkan menggunakan jenis dan kode.

### **Konsep dan protokol aplikasi-layer tcp / ip**

banyak protokol ada pada tcp / ip application layer, yang menggabungkan presentasi, sesi, dan aplikasi lapisan model osi.

Telnet

telnet menyediakan emulasi terminal melalui jaringan. Server telnet mendengarkan pada port tcp

23. Telnet adalah cara standar untuk mengakses perintah shell interaktif melalui jaringan telnet memiliki kelemahan karena tidak memberikan kerahasiaan: semua plaintext.

Ftp

ftp adalah file transfer protocol, digunakan untuk mentransfer file ke server dan dari server. Seperti telnet,

ftp tradisional tidak memiliki kerahasiaan atau integritas dan tidak boleh digunakan untuk mentransfer.

Ssh

ssh menggunakan port 22, ssh dirancang sebagai pengganti yang aman untuk telnet, ftp, dan unix, ssh menyediakan kerahasiaan, integritas, dan otentikasi aman.

Smtp, pop, dan imap

smtp adalah simple mail transfer protocol, digunakan untuk mentransfer e-mail antara server.

Dns

Dns adalah domain name system, dns menggunakan tcp dan udp

http dan https

Http menggunakan port 80, http adalah hypertext transfer protocol, yang digunakan untuk mentransfer terenkripsi data berbasis web. Https (hypertext transfer protocol secure) transfer dienkripsi data berbasis web melalui ssl / tls yang memiliki keunggulan lebih aman "secure" untuk menampilkan web

### **➤ Teknologi lan dan protokol**

Local area network konsep fokus pada layer 1-3 teknologi seperti jaringan jenis kabel, topologi jaringan fisik dan logis, ethernet, fddi, dan lain-lain.

## Ethernet

ethernet beroperasi pada layer 2 dan merupakan dominan lokal teknologi jaringan melalui frame. Ethernet adalah baseband (satu saluran).

## Teknologi wan dan protokol

isp dan penyedia jaringan "jarak jauh" lainnya yang sering menggunakan teknologi wide area network. Banyak dari kita memiliki pengalaman mengkonfigurasi teknologi lan seperti menghubungkan jaringan kabel cat5; kurang umum untuk memiliki pengalaman tangan membangun wans.

T1s, t3s, e1s, dan e3s adalah sejumlah standar sirkuit internasional.

Serta teknologi lain frame relay yang juga protokol dari wan yang memberikan recovery dan berfokus pada kecepatan,

## Mpls

multiprotocol label switching (mpls) menyediakan cara untuk meneruskan data wan melalui label, melalui jaringan cloud mpls bersama. Dan dapat di gunakan untuk menyederhanakan routing dari wan

### ➤ Perangkat dan protokol jaringan

#### Protokol routing

1. Repeater dan hub sebuah repeater menerima bit pada satu port dan "mengulangi" mereka port lainnya. Memiliki fungsi untuk memperpanjang jaringan
2. Bridges adlah sebuah penghubung jaringan bersama yang selalu memiliki node dan jembatan penghubung
3. Switches adalah sebuah penghubung lebih dari dua, witch menyediakan isolasi lalu lintas dengan menghubungkan alamat mac dari setiap komputer dan server dengan port-nya.
4. Router adalah pembuat keputusan routing berbasis pada sumber dan tujuan alamat ip.
5. Firewall menyaring dan memilah lalu lintas antara jaringan, untuk membuat keputusan dan memberikan keputusan pada sebuah jalur penghubung jaringan. Yang di dalamnya memiliki banyak komponen lain yaitu: Packet filter, Stateful firewalls, Proxy firewalls, dalam proxy firewalls memiliki Application-Layer Proxy firewalls
6. Modem adalah modulator / demodulator. Dibutuhkan data biner dan memodulasi itu menjadi suara analog yang dapat dilakukan pada jaringan telepon.
7. Intrusion Detection Systems dan Intrusion Prevention System adalah sebuah perangkat yang memiliki fungsi untuk menjaga dan mendeteksi bahaya yang mungkin adalah pelanggaran kebijakan dan Intrusion Prevention System memiliki fungsi untuk mencegah tindakan kejahatan

8. Endpoint security adalah kemampuan lain untuk mencegah dan mendeteksi, untuk memberikan lapisan pertahanan luar, seperti fungsi antivirus, Application whitelisting, Removable media controls, Disk encryption

### ➤ **SECURE COMMUNICATIONS”keamanan komunikasi”**

Protokol otentikasi mengotentikasi klaim identitas melalui jaringan

- Authentication protocols and frameworks keamanan mengasumsikan bahwa jaringan eavesdropper bisa mengendus semua paket yang dikirim antara client server dan otentikasi: protokol harus tetap aman. Seperti yang akan kita lihat segera, PAP gagal tes ini, tapi CHAP dan EAP lulus.
- PAP dan CHAP adalah protokol otentikasi sangat lemah, PAP tidak aman dan tidak boleh digunakan.  
CHAP (Tantangan-Handshake Authentication Protocol) adalah otentikasi yang lebih aman  
protokol yang tidak mengekspos password teks-jelas dan tidak rentan terhadap serangan replay.
- VPN memberikan privasi melibatkan otentikasi aman, kriptografi hash seperti SHA-1 untuk memberikan integritas, dan cipher seperti AES untuk memberikan kerahasiaan. Yang di dalamnya terdapat PPP yang menambahkan kerahasiaan, integritas, dan otentikasi melalui point-to-point, IPv4 telah ada built-in kerahasiaan; -lapisan yang lebih.

### ➤ **Remote meeting technology**

Teknologi pertemuan jarak jauh adalah teknologi baru yang memungkinkan pengguna untuk melakukan secara online pertemuan melalui internet, termasuk fungsi desktop sharing. teknologi ini biasanya termasuk menampilkan slide PowerPoint pada semua PC yang terhubung ke sebuah pertemuan, berbagi dokumen seperti spreadsheet, dan juga berbagi audio atau video. Banyak dari solusi ini dirancang untuk terowongan keluar SSL atau TLS lalu lintas, yang sering bisa lewat melalui firewall dan setiap proxy Web. Penggunaan teknologi pertemuan jarak jauh harus dipahami, dikendalikan, dan sesuai dengan semua kebijakan yang berlaku.