PEMBAHASAN UAS JARINGAN KOMPUTER 2018/2019

-Diperingatkan bahwa jawaban belum tentu sepenuhnya betul-

Selamat belajar!

1. Berdoa dulu ya ☺
2. Diketahui IP 182.255.0.0/16.

   Dibagi menjadi:

   - Fakultas A = ½
   - Fakultas C = 1/8
   - Fakultas B = sisanya

   Penyelesaian:

   Address: 182.255.0.0 10110110.11111111 .00000000.00000000 (Class B)

   Netmask: 255.255.0.0 11111111.11111111 .00000000.00000000

   Jumlah subnet = 2^x = 2^0 = 1 subnet

   Blok subnet = 256 – 0 = 256

   Jumlah host/ subnet = 2^y – 2 = 2^{16} – 2 = 65536 – 2 = 65534 host

   Sehingga,

   Network: 182.255.0.0/16 10110110.11111111 .00000000.00000000

   Broadcast: 182.255.255.255 10110110.11111111 .11111111.11111111

   HostMin: 182.255.0.1 10110110.11111111 .00000000.00000001

   HostMax: 182.255.255.254 10110110.11111111 .11111111.11111110

   - Jumlah host fakultas A = ½ x 65534 = 32767 host

     Range IP : 182.255.0.1 sampai 182.255.127.255 (dengan /16)
   - Jumlah host fakultas C = 1/8 x 65534 = 8191,75 → dibulatkan mjd 8192 host

     Range IP : 182.255.128.0 sampai 182.255.159.255 (dengan /16)
   - Jumlah host fakultas B = 65534 – 32767 – 8192 =24575 host

     Range IP : 182.255.160.0 sampai 182.255.255.254 (dengan /16)

3. Perbedaan prinsip kerja UDP dan TCP:

   UDP (*User Datagram Protocol*)

   - UDP (*User Datagram Protocol*) adalah *transport layer* yang tidak handal, *unreliable*/ *connectionless* dan merupakan kebalikan dari transport layer TCP. Dengan menggunakan UDP, setiap aplikasi *socket* dapat mengirimkan paket-

paket yang berupa datagram. Istilah datagram diperuntukkan terhadap paket dengan koneksi yang tidak handal (*unreliable service*). Koneksi yang handal selalu memberikan keterangan apabila pengiriman data gagal, sedangkan koneksi yang tidak handal tidak akan mengirimkan keterangan (*acknowledgment*) meski pengiriman data gagal.

- Data dalam protokol UDP akan dikirimkan sebagai datagram tanpa adanya nomor *identifier*. Sehingga sangat besar sekali kemungkinan data sampai tidak berurutan dan sangat mungkin hilang/rusak dalam perjalananan dari *host* asal ke *host* tujuan.

TCP (*Transfer Control Protocol*)

- Datagram dibagi-bagi ke dalam bagian-bagian kecil yang sesuai dengan ukuran bandwith (lebar frekuensi) dimana data tersebut akan dikirimkan.
- Pada lapisan TCP, data tersebut lalu "dibungkus" dengan informasi header yang dibutuhkan. Misalnya seperti cara mengarahkan data tersebut ke tujuannya, cara merangkai kembali kebagian-bagian data tersebut jika sudah sampai pada tujuannya, dan sebagainya.
- Setelah datagram dibungkus dengan header TCP, datagram tersebut dikirim kepada lapisan IP.
- IP menerima datagram dari TCP dan menambahkan headernya sendiri pada datagram tersebut.
- IP lalu mengarahkan datagram tersebut ke tujuannya. Komputer penerima melakukan proses-proses perhitungan, ia memeriksa perhitungan checksum yang sama dengan data yang diterima. Jika kedua perhitungan tersebut tidak cocok berarti ada error sewaktu pengiriman dan datagram akan dikirimkan kembali.

4. Prinsip kerja pengiriman *email*:
   - Ketika akan mengirim *email*, pengirim menggunakan *User Agent* untuk meng-*compose* pesan ke *email* yang akan dituju.
   - *User Agent* milik pengirim akan mengirim pesan ke *mail server* menggunakan POP3, dan menempatkan pesan ke message queue.
   - Sisi klien akan menggunakan protokol SMTP untuk membuka koneksi TCP dengan *mail server* penerima.

- Klien dari protokol SMTP akan mengirim pesan penerima melalui koneksi TCP. Jika domain email pengirim dan penerima sama, maka server SMTP akan ditransfer ke *server mail* lokal, yaitu dengan protokol POP3 atau IMAP.
- *Mail server* penerima akan menempatkan pesan yang diterima ke *mailbox*.
- *User Agent* penerima kemudian akan mentransfer pesan dari *mail server* ke *host*-nya melalui POP3

5. Contoh ancaman keamanan jaringan:
   1) **Spoofing** adalah Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah host yang dapat dipercaya. Hal ini biasanya dilakukan oleh seorang hacker/ cracker.

      Pencegahan: penggunaan SSL, pasang filter di *router*, enkripsi dan autentifikasi
   2) **Serangan DOS** (Denial-Of-Service attacks) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang.

      Pencegahan: penggunaan software keamanan jaringan, kombinasi firewall
   3) **Trojan horse** atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicious software/malware) yang dapat merusak sebuah sistem atau jaringan.

      Pencegahan: pemasangan anti virus
   4) **DNS Poisoning** merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi IP Address yang salah mengenai sebuah host, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya.

      Pencegahan: ganti port winbox 8291, blokir akses DNS mikrotik dari publik, hindari upgrade routerOS otomatis.