Nama : iis nurjanah

Nim :1310651078

Uas : keamanan informasi

Kelas : E

|  |  |
| --- | --- |
| No. | Jawaban |
| 1. | Konsep jaringan dasar  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.  Internet, Intranet, dan Extranet Internet adalah kumpulan global jaringan mengintip menjalankan TCP / IP, menyediakan layanan terbaik-usaha. Intranet adalah jaringan milik pribadi menjalankan TCP / IP, seperti sebagai jaringan perusahaan. Sebuah Extranet adalah hubungan antara intranet pribadi.  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, misalnya. "Layer X" dalam buku ini mengacu pada model OSI. Model OSI memiliki tujuh lapisan.  Layer 1: Physical Layer fisik adalah Layer 1 dari model OSI. Lapisan 1 menggambarkan unit data tersebut sebagai bit diwakili oleh energi (seperti cahaya, listrik, atau gelombang radio) dan media yang digunakan untuk membawa mereka (seperti kabel tembaga atau fiber optik)  Layer 2: Data Link Data Link Layer menangani akses ke layer Physical serta Local Area Network komunikasi. Kartu Ethernet dan MAC (Media Access Control) address berada di Layer 2, seperti switch dan jembatan.  Layer 3: Jaringan The Network Layer menggambarkan routing yang: memindahkan data dari sistem pada satu LAN ke sistem yang lain. Alamat IP dan router ada pada Layer 3. Layer 3 protokol termasuk IPv4 dan IPv6, antara lain.  Layer 4: Transport Transport Layer menangani paket sequencing, kontrol aliran, dan deteksi kesalahan. TCP dan UDP adalah Layer 4 protokol. Layer 4 membuat sejumlah fitur yang tersedia, seperti pengiriman ulang atau resequencing paket.  Layer 5: Session Session Layer mengelola sesi, yang menyediakan perawatan pada koneksi. Mount berbagi file melalui jaringan memerlukan sejumlah sesi perawatan, seperti sebagai Remote Procedure Calls (RPC): ini ada di Session Layer. Cara yang baik untuk ingat fungsi Session Layer adalah "hubungan antara aplikasi."  Layer 6: Presentation The Presentation Layer menyajikan data ke aplikasi (dan pengguna) dalam dipahami cara. Konsep Presentation Layer meliputi konversi data, karakter set seperti sebagai ASCII, dan gambar format seperti GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group), dan TIFF (Tagged Image File Format). Layer 7: Application Application Layer adalah di mana Anda berinteraksi dengan aplikasi komputer. Browser Anda Web, pengolah kata, dan instant messaging client yang ada di Layer 7. Protokol Telnet dan FTP adalah protokol Aplikasi-Layer. TCP / IP model Model TCP / IP (Transmission Control Protocol / Internet Protocol) adalah populer model jaringan yang dibuat oleh AS Defense Advanced Research Projects Agency pada 1970-an. TCP / IP adalah nama informal (dinamai dua protokol pertama dibuat); nama resmi adalah Internet Protocol Suite. Model TCP / IP lebih sederhana dari model OSI, Sementara TCP dan IP menerima tagihan atas, TCP / IP sebenarnya merupakan suite protokol termasuk UDP (User Datagram Protocol) dan ICMP (Internet Control Message Protocol), di antara banyak lainnya. Jaringan Access Layer Jaringan Access Layer dari model TCP / IP menggabungkan Layer 1 (Physical) dan 2 (Data Link) dari model OSI. Ini menggambarkan Lapisan 1 masalah seperti energi, bit, dan media yang digunakan untuk membawa mereka (tembaga, serat, nirkabel, dll). Internet layer Layer Internet dari model TCP / IP sejalan dengan Layer 3 (Network) Lapisan model OSI. Di sinilah alamat IP dan routing hidup. Ketika data ditransmisikan dari node pada satu LAN ke node pada LAN yang berbeda, Layer Internet yang digunakan.  Host-to-Host Transport Layer Host-to-Host Transport Layer (kadang-kadang disebut baik "Host-to-Host" atau, lebih umum, "Transportasi" sendiri; buku ini akan menggunakan "Transportasi") menghubungkan Internet Lapisan ke Application Layer. Ini adalah di mana aplikasi yang ditujukan pada jaringan, melalui port. TCP dan UDP adalah dua protokol Transport Layer dari TCP / IP. Application Layer TCP / IP Application Layer menggabungkan Layer 5 sampai 7 (Session, Presentation, dan Aplikasi) dari model OSI. Sebagian besar protokol ini menggunakan arsitektur client-server, di mana klien (seperti ssh) terhubung ke server mendengarkan (disebut daemon pada Sistem UNIX) seperti sshd. Klien dan server menggunakan baik TCP atau UDP (dan kadang-kadang keduanya) sebagai protokol Transport Layer. TCP / IP protokol Aplikasi-Layer termasuk SSH, Telnet, dan FTP, di antara banyak lainnya. Alamat MAC Sebuah Media Access Control (MAC) alamat adalah alamat hardware yang unik dari Ethernet kartu jaringan antarmuka (NIC), biasanya "terbakar di" di pabrik. MAC alamat dapat diubah dalam perangkat lunak.  IPv4 IPv4 adalah Internet Protocol versi 4, yang biasa disebut "IP." Ini adalah protokol yang mendasar Internet, yang dirancang pada tahun 1970 untuk mendukung packet-switched jaringan bagi AS Defense Advanced Research Projects Agency (DARPA). IPv4 digunakan untuk ARPAnet, yang kemudian menjadi Internet. IP adalah protokol sederhana, dirancang untuk membawa data melalui jaringan. Hal ini sangat sederhana yang membutuhkan "protokol pembantu" disebut ICMP (lihat di bawah). Jika koneksi atau keandalan diperlukan, harus disediakan oleh protokol tingkat tinggi yang dilakukan oleh IP, seperti TCP.  IPv6 IPv6 adalah penerus IPv4, menampilkan ruang alamat yang jauh lebih besar (alamat 128-bit dibandingkan dengan IPv4 yang 32 bit), sederhana routing, dan alamat sederhana tugas. kurangnya A alamat IPv4 adalah faktor utama yang menyebabkan penciptaan IPv6.  IPv6 IPv6 adalah penerus IPv4, menampilkan alamat yang jauh lebih besar spaceTCP 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 rusak dan memancarkan kembali segmen yang hilang. Port TCP TCP menghubungkan dari port sumber ke port tujuan. Bidang TCP port adalah 16 bit, memungkinkan nomor port 0-65535. 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 superuser hak untuk membuka port-undang. Setiap pengguna dapat membuka (tidak terpakai) port fana. UDP UDP adalah User Datagram Protocol, sepupu 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, protokol pembantu 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.  Telnet Telnet menyediakan emulasi terminal melalui jaringan. Server Telnet mendengarkan pada port TCP Telnet adalah cara standar untuk mengakses perintah shell interaktif melalui jaringan selama lebih dari 20 tahun. Telnet lemah karena tidak memberikan kerahasiaan: semua data yang dikirimkan selama Sesi Telnet adalah plaintext, termasuk username dan password yang digunakan untuk mengotentikasi ke sistem. FTP FTP adalah File Transfer Protocol, digunakan untuk mentransfer file ke dan dari server. Seperti Telnet, FTP tradisional tidak memiliki kerahasiaan atau integritas dan tidak boleh digunakan untuk mentransfer data sensitif melalui saluran tidak aman. SSH SSH dirancang sebagai pengganti yang aman untuk Telnet, FTP, dan UNIX "R" perintah (Rlogin, rshell, dll). Ini menyediakan kerahasiaan, integritas, dan otentikasi aman, antara fitur-fitur lainnya. SSH juga dapat digunakan untuk aman terowongan lainnya protokol, seperti HTTP. Server SSH mendengarkan pada TCP port 22 secara default. SMTP, POP, dan IMAP SMTP adalah Simple Mail Transfer Protocol, digunakan untuk mentransfer e-mail antara server. Server SMTP mendengarkan pada port TCP 25. POPv3 (Post Office Protocol) dan IMAP (Internet Message Access Protocol) digunakan untuk akses client-server e-mail, yang digunakan Port TCP 110 dan 143, masing-masing. DNS DNS adalah Domain Name System, database hirarki global yang terdistribusi yang menerjemahkan nama ke alamat IP dan sebaliknya. DNS menggunakan TCP dan UDP: kecil jawaban menggunakan UDP port 53; jawaban besar (seperti transfer zona) menggunakan port TCP 53. HTTP dan HTTPS 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. HTTP menggunakan port TCP 80, dan HTTPS menggunakan port TCP 443. HTML (Hypertext Markup Language) digunakan untuk menampilkan konten 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 di Area yang mentransmisikan data jaringan melalui frame. Ethernet adalah baseband (satu saluran), alamat sehingga itmust isu-isu seperti tabrakan, di mana dua node mencoba untuk mengirimkan data secara bersamaan. |
| 2. | switch Switch adalah sebuah jembatan dengan lebih dari dua port. Juga, itu adalah praktek terbaik untuk hanya menghubungkan satu perangkat per port switch. Jika tidak, segala sesuatu yang benar tentang jembatan juga benar tentang switch. Gambar 2.1 menunjukkan switch jaringan. Switch menyediakan isolasi lalu lintas dengan menghubungkan alamat MAC dari setiap komputer dan server dengan port-nya. Switch menyusut tabrakan domain ke port tunggal. Anda biasanya akan memiliki tabrakan dengan asumsi satu perangkat yang terhubung per port (yang praktek terbaik). Batang digunakan untuk menghubungkan beberapa switch.    firewall stateful Firewall Stateful memiliki tabel negara yang memungkinkan firewall untuk membandingkan saat paket ke yang sebelumnya. Firewall Stateful lebih lambat dari paket filter, tetapi jauh lebih aman. Komputer 1 mengirimkan ICMP Echo Request ke bank.example.com. Firewall dikonfigurasi untuk memungkinkan ping ke situs internet, sehingga firewall stateful memungkinkan lalu lintas dan menambahkan entri untuk itu state table.    firewall Proxy Proxy firewall yang bertindak sebagai server perantara. Kedua filter paket dan stateful firewall lulus lalu lintas melalui atau menyangkalnya: mereka hop lain di sepanjang rute. proxy mengakhiri koneksi. Aplikasi-Layer firewall Proxy Firewall aplikasi-Layer Proxy beroperasi sampai ke Layer 7. Tidak seperti filter paket dan firewall stateful yang membuat keputusan berdasarkan Layers 3 dan 4 saja, Aplikasi- Proxy lapisan dapat membuat keputusan filtering berdasarkan data Aplikasi-Layer, seperti sebagai lalu lintas HTTP, selain Layers 3 dan 4. modem Modem adalah modulator / demodulator. Dibutuhkan data biner dan memodulasi itu menjadi suara analog yang dapat dilakukan pada jaringan telepon dirancang untuk membawa suara manusia. Modem penerima kemudian demodulates suara analog kembali ke Data biner.  Intrusion Detection Systems dan Intrusion Prevention System. Sebuah Intrusion Detection System (IDS) adalah perangkat detektif yang dirancang untuk mendeteksi berbahaya (Termasuk melanggar kebijakan-) tindakan. Sebuah Intrusion Prevention System (IPS) adalah perangkat preventif dirancang untuk mencegah tindakan jahat. Ada dua tipe dasar IDS dan IPSS: jaringan berbasis dan berbasis host. Endpoint keamanan Karena titik akhir adalah target serangan, kemampuan pencegahan dan detektif endpoint sendiri memberikan lapisan pertahanan luar keamanan jaringan-sentris perangkat. Banyak produk titik dapat dianggap sebagai bagian dari keseluruhan Suite keamanan endpoint. Yang paling penting adalah antivirus, aplikasi membolehkan akses, kontrol media removable, enkripsi disk, Host Intrusion Prevention System, dan firewall desktop yang. Anti Virus Yang paling umum digunakan produk keamanan endpoint adalah perangkat lunak antivirus. Anti Virus adalah satu lapisan (banyak) pertahanan keamanan endpoint secara mendalam. Meskipun antivirus vendor sering menggunakan metode heuristik atau statistik untuk deteksi malware, dominan berarti mendeteksi malware masih signature berbasis. Pendekatan berbasis signature mengharuskan spesimen malware tersedia untuk Vendor antivirus untuk menciptakan tanda tangan. Ini adalah contoh dari daftar hitam. Aplikasi membolehkan akses Aplikasi membolehkan akses adalah tambahan yang lebih baru untuk endpoint security suite. Itu Fokus utama dari aplikasi membolehkan akses adalah untuk menentukan di muka yang binari dianggap aman untuk mengeksekusi pada sistem tertentu. Setelah dasar ini telah didirikan, setiap biner mencoba untuk menjalankan yang tidak pada daftar binari dikenal-baik dicegah dari mengeksekusi. Kelemahan dari pendekatan ini adalah ketika sebuah "dikenal baik" biner dimanfaatkan oleh penyerang dan digunakan jahat. Kontrol media removable Produk keamanan endpoint lain baru-baru ini membantu dengan kontrol removable media. Malware pengiriman dan data exfiltration telah memaksa organisasi untuk mengerahkan ketat kontrol atas apa jenis removable media dapat dihubungkan. Removable media produk kontrol adalah kontrol teknis yang cocok kontrol administrasi seperti sebagai mandat kebijakan penggunaan yang tidak sah dari removable media. Enkripsi disk Produk lain keamanan endpoint ditemukan dengan meningkatnya keteraturan adalah enkripsi disk software. Penuh Disk Encryption (FDE), juga disebut enkripsi seluruh disk, mengenkripsi seluruh disk. Ini adalah solusi yang dienkripsi unggul sebagian, seperti volume terenkripsi, direktori, folder, atau file. Masalah dengan yang terakhir Pendekatan adalah risiko meninggalkan data sensitif pada daerah yang tidak terenkripsi dari disk. |