NAMA : YULI DWI KARTIKASARI
NIM : 1310651115
KELAS : A

Jawaban nomor 1

Domain 2: Telecommunications and Network Security

Telecommunications and Network Security is fundamental to our modern life. The Internet, the World Wide Web, online banking, instant messaging e-mail, and many other technologies rely on Network Security: our modern world cannot exist without it. Telecommunications and Network Security (often called "telecommunications," for short) focuses on the confidentiality, integrity, and availability of data in motion

NETWORK ARCHITECTURE AND DESIGN

we need to understand the fundamental concepts behind them. Terms like broadband are often used informally: the exam requires a precise understanding of information security terminology.

- **Simplex, half-duplex, and full-duplex communication**

  communication is one-way, like a car radio tuned to a music station

- **LANs, WANs, MANs, and PANs**
  - ✓ A LAN
    is a Local Area Network. A LAN is a comparatively small network, typically confined to a building or an area within one.
  - ✓ MAN
    is a Metropolitan Area Network,which is typically confined to a city, a zip code, a campus, or an office park.
  - ✓ A WAN
    is a Wide Area Network, typically covering cities, states, or countries. At the other end of the spectrum, the smallest of these networks are PANs: Personal Area Networks, with a range of 100 m or much less. Low-power wireless technologies such as Bluetooth are used to create PANs.
- **Internet, Intranet, and Extrane**

  a global collection of peered networks running TCP/IP, providing best-effort service. An

- **Intranet**

  is a privately owned network running TCP/IP, such as a company network. An

- **Extranet**

  is a connection between private Intranets, such as connections to business partner Intranets.

The OSI model

is a Layered network model. The model is abstract: we do not directly run the OSI model in our systems (most now use the TCP/IP model); it is used as a reference point, so "Layer 1" (physical) is universally understood, whether you are running Ethernet or ATM, for example. "Layer X" in this book refers to the OSI model.

- **Layer 1: Physical**
  The Physical Layer is Layer 1 of the OSI model. Layer 1 describes units of data such.
- **Layer 2: Data Link**
  The Data Link Layer handles access to the Physical Layer as well as Local Area Network communication. An Ethernet card and its MAC(Media Access Control) address are at Layer 2, as are switches and bridges.
- **Layer 3: Network**
  The Network Layer describes routing: moving data from a system on one LAN to a system on another.
- **Layer 4: Transport**
  Taking advantage of these features is a protocol implementation decision. As we will see later, TCP takes advantage of these features, at the expense of speed
- **Layer 5: Session**
  the Session Layer's function is "connections between applications." The Session Layer uses simplex, half-duplex, and full-duplex communication.

- **Layer 6: Presentation**
  The Presentation Layer presents data to the application (and user) in a comprehensible way. Presentation Layer concepts include data conversion, characters sets such as ASCII, and image formats such as GIF (Graphics Interchange Format), JPEG (Joint Photographic Experts Group), and TIFF (Tagged Image File Format).
- **Layer 7: Application**
  The Application Layer is where you interface with your computer application. Your Web browser, word processor, and instant messaging client exist at Layer 7. The protocols Telnet and FTP are Application-Layer protocols.

The TCP/IP model

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a popular network model created by the U.S. Defense Advanced Research Projects Agency in the 1970s. TCP/IP is an informal name (named after the first two protocols created); the formal name is the Internet Protocol Suite. The TCP/IP model is simpler than the OSI model, as shown in.

- **Network Access Layer**
  The Network Access Layer of the TCP/IP model combines Layers 1 (Physical) and 2 (Data Link) of the OSI model. It describes Layer 1 issues such as energy, bits, and the medium used to carry them (copper, fiber, wireless, etc.). It also describes Layer 2 issues such as converting bits into protocol units such as Ethernet frames, MAC (Media Access Control) addresses, and Network Interface Cards (NICs).

- **Internet Layer**
  The Internet Layer of the TCP/IP model aligns with the Layer 3 (Network) Layer ofthe OSI model. This is where IP addresses and routing live. When data is transmitted from a node on one LAN to a node on a different LAN, the Internet Layer is used.
- **Host-to-Host Transport Layer**
  Host-to-Host Transport Layer (sometimes called either "Host-to-Host" or, more commonly, "Transport" alone; this book will use "Transport") connects the Internet Layer to the Application Layer. It is where applications are addressed on a network,via ports.
- **Application Layer**
  The TCP/IP Application Layer combines Layers 5 through 7 (Session, Presentation, and Application) of the OSI model. Most of these protocols use a client-server architecture, where a client (such as ssh) connects to a listening server (called a daemon on UNIX systems) such as sshd.

MAC addresses

A Media Access Control (MAC) address is the unique hardware address of an Ethernet network interface card (NIC), typically "burned in" at the factory. MAC addresses may be changed in software

IPv4

IPv4 is Internet Protocol version 4, commonly called "IP." It is the fundamental protocol of the Internet, designed in the 1970s to support packet-switched networking for the U.S. Defense Advanced Research Projects Agency (DARPA). IPv4 was used for the ARPAnet, which later became the Internet.

IPv6

IPv6 is the successor to IPv4, featuring far larger address space (128-bit addresses compared to IPv4's 32 bits), simpler routing, and simpler address assignment. A lack of IPv4 addresses was the primary factor that led to the creation of IPv6.

TCP

TCP is the Transmission Control Protocol, a reliable Layer 4 protocol. TCP ports TCP connects from a source port to a destination port. The TCP port field is 16 bits, allowing port numbers from 0 to 65535. There are two types of ports:Reserved and ephemeral.

UDP

UDP is the User Datagram Protocol, a simpler and faster cousin to TCP. UDP is commonly used for applications that are "lossy" (can handle some packet loss), such as streaming audio and video.

ICMP

ICMP is the Internet Control Message Protocol, a helper protocol that helps Layer 3.ICMP is used to troubleshoot and report error conditions: Without ICMP to help, IP would fail when faced with routing loops, ports, hosts, or networks that are down, etc.

Application-Layer TCP/IP protocols and concepts

A multitude of protocols exist at TCP/IP's Application Layer, which combines the Presentation, Session, and Application Layers of the OSI model.

Telnet

Telnet was the standard way to access an interactive command shell over a network for over 20 years.

FTP

FTP is the File Transfer Protocol, used to transfer files to and from servers. Like Telnet, traditional FTP has no confidentiality or integrity and should not be used to transfer sensitive data over insecure channels.

SSH

SSH was designed as a secure replacement for Telnet, FTP, and the UNIX "R" commands (rlogin, rshell, etc). It provides confidentiality, integrity, and secure authentication, among other feature SMTP, POP, and IMAP

SMTP

is the Simple Mail Transfer Protocol, used to transfer e-mail between servers.
SMTP servers listen on TCP port 25

DNS

is the Domain Name System, a distributed global hierarchical database that translates names to IP addresses and vice versa.

HTTP and HTTPS

HTTP is the Hypertext Transfer Protocol, which is used to transfer unencrypted Web-based data. HTTP uses TCP port 80, and HTTPS uses TCP port 443. HTML (Hypertext Markup Language) is used to display Web content.

LAN technologies and protocols

Local Area Network concepts focus on Layer 1-3 technologies such as network cabling types, physical and logical network topologies, Ethernet, FDDI, and others.

Ethernet

operates at Layer 2 and is a dominant Local Area Networking technology that transmits network data via frames.

Frame Relay

is a packet-switched Layer 2 WAN protocol that provides no error recovery and focuses on speed. rame Relay multiplexes multiple logical connections over a single physical connection to create Virtual Circuits;

MPLS

Multiprotocol Label Switching (MPLS) provides a way to forward WAN data via labels, via a shared MPLS cloud network.

NETWORK DEVICES AND PROTOCOLS

- Repeaters and hubs are Layer 1 devices.
- Bridges and switches are Layer 2 devices.
- Switches
  A switch is a bridge with more than two ports.
- Routers
  Routers are Layer 3 devices that route traffic from one LAN to another.
- Firewalls filter traffic between networks.
- Packet filter
  A packet filteris a simple and fast firewall
- Stateful firewalls
  have a state table that allows the firewall to compare current packets to previous ones.
- Proxies are firewalls that act as intermediary servers.

Modem

A modem is a modulator/demodulator

Jawaban nomor 2

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan sistem saat ini. Perkembangan teknologi komputer, selain menimbulkan banyak manfaat juga memiliki banyak sisi buruk. Salah satunya adalah serangan terhadap sistem komputer yang terhubung ke Internet. Sebagai akibat dari serangan itu, banyak sistem komputer atau jaringan yang terganggu bahkan menjadi rusak. Untuk menanggulangi hal tersebut, diperlukan sistem keamanan yang dapat menanggulangi dan mencegah kegiatan-kegiatan yang mungkin menyerang sistem jaringan kita.
Dalam perkembangan teknologi dewasa ini, sebuah informasi menjadi sangat penting bagi sebuah organisasi. Informasi tersebut biasanya dapat diakses oleh para penggunanya. Akan tetapi, ada masalah baru yang berakibat dari keterbukaan akses tersebut. Masalah-masalah tersebut antara lain adalah sebagai berikut:

- Pemeliharaan validitas dan integritas data atau informasi tersebut
- Jaminan ketersediaan informasi bagi pengguna yang berhak.
- Pencegahan akses sistem dari yang tidak berhak.
- Pencegahan akses informasi dari yang tidak berhak

Hal yang Membahayakan Jaringan
Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah hal-hal sebagai berikut:

- Probe

  Probe atau yang biasa disebut probing adalah suatu usaha untuk mengakses sistem atau mendapatkan informasi tentang sistem. Contoh sederhana dari probing adalah percobaan log in ke suatu account yang tidak digunakan. Probing dapat dianalogikan dengan menguji kenop-kenop pintu untuk mencari pintu yang tidak dikunci sehingga dapat masuk dengan mudah. Probing tidak begitu berbahaya bagi sistem jaringan kita namun biasanya diikuti oleh tindakan lain yang lebih membahayakan keamanan.
- Scan

  Scan adalah probing dalam jumlah besar menggunakan suatu tool. Scan biasanya merupakan awal dari serangan langsung terhadap sistem yang oleh pelakunya ditemukan mudah diserang.
- Account Compromise
- Root Compromise
- Packet Sniffer
- Packet sniffer adalah sebuah program yang menangkap (capture) data dari paket yang lewat di jaringan. Data tersebut bisa termasuk user name, password, dan informasi-informasi penting lainnya yang lewat di jaringan dalam bentuk text. Paket yang dapat ditangkap tidak hanya satu paket tapi bisa berjumlah ratusan bahkan ribuan, yang berarti pelaku mendapatkan ribuan user name dan password. Dengan password itu pelaku dapat mengirimkan serangan besar-besaran ke sistem.
- Denial of Service

  Denial of service (DoS) bertujuan untuk mencegah pengguna mendapatkan layanan dari sistem. Serangan DoS dapat terjadi dalam banyak bentuk. Penyerang dapat membanjiri (flood) jaringandengan data yang sangat besar atau dengan sengaja menghabiskan sumber daya yang memang terbatas, seperti process control block (PCB) atau pending network connection. Penyerang juga mungkin saja mengacaukan komponen fisik dari jaringan atau memanipulasi data yang sedang dikirim termasuk data yang terenkripsi.

- Exploitation of Trust
- Malicious Code
- Internet Infrastructure Attacks

Perencanaan Keamanan

Untuk menjamin keamanan dalam jaringan, perlu dilakukan perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam keamanan jaringan. Perencanaan tersebut akan membantu dalam hal-hal berikut ini:

- Menentukan data atau informasi apa saja yang harus dilindungi
- Menentukan berapa besar biaya yang harus ditanamkan dalam melindunginya
- Menentukan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagian tersebut

Metode Keamanan Jaringan

Dalam merencanakan suatu keamanan jaringan, ada beberapa metode yang dapat diterapkan. Metode-metode tersebut adalah sebagai berikut:

❖ Pembatasan akses pada suatu jaringan

Ada 3 beberapa konsep yang ada dalam pembatasan akses jaringan, yakni sebagai berikut:

- Internal Password Authentication
  Password yang baik menjadi penting dan sederhana dalam keamanan suatu jaringan. Kebanyakan masalah dalam keamanan jaringan disebabkan karena password yang buruk. Cara yang tepat antara lain dengan menggunakan shadow password dan menonaktifkan TFTP.
- Server-based password authentication
- Firewall dan Routing Control
  Untuk firewall akan dijelaskan pada bagian selanjutnya.

❖ Menggunakan metode enkripsi tertentu

Dasar enkripsi cukup sederhana. Pengirim menjalankan fungsi enkripsi pada pesan plaintext, ciphertext yang dihasilkan kemudian dikirimkan lewat jaringan, dan penerima menjalankan fungsi dekripsi (decryption) untuk mendapatkan plaintext semula. Proses enkripsi/dekripsi tergantung pada kunci (key) rahasia yang hanya diketahui oleh pengirim dan penerima. Ketika kunci dan enkripsi ini digunakan, sulit bagi penyadap untuk mematahkan ciphertext, sehingga komunikasi data antara pengirim dan penerima aman. Lebih lanjut mengenai enkripsi akan dijelaskan pada bagian selanjutnya.

❖ Pemonitoran terjadwal terhadap jaringan

Proses memonitor dan melakukan administrasi terhadap keamanan jaringan akan dibahas pada bagian lain.

Password

Akun administrator pada suatu server sebaiknya diubah namanya dan sebaiknya hanya satu akun saja yang dapat mengakses. Pada sistem operasi Windows, cara membuat password adalah sebagai berikut:

- Tekan tombol pada start menu
- Klik Control Panel
- Klik User Account
- Klik Create a password
- Masukkan password
- Tekan tombol create password

Pemberian password yang tepat dengan kebijakan keamanan dalam akun admin, password itu harus memiliki suatu karakter yang unik dan sukar ditebak. Ada beberapa karakter yang dapat digunakan agar password sukar untuk ditebak, antara lain adalah sebagai berikut:

- Karakter #
- Karakter %
- Karakter $
- Dll

Untuk meminimalisir penyerangan terhadap keamanan jaringan, hal yang dapat dilakukan administrator dalam memonitoring jaringan sebaiknya adalah dengan membatasi user yang dapat melakukan full-access ke dalam suatu server. Cara paling sederhana adalah dengan memberlakukan wewenang read only untuk semua user. Cara lain adalah dengan melakukan pembatasan berdasarkan hal berikut ini:

- MAC Address
  Contohnya, user yang dapat melakukan akses secara penuh adalah user yang memiliki alamat abcd:1020:fa02:1:2:3.
- IP Address
  Contohnya, user yang dapat melakukan akses secara penuh adalah user yang memiliki alamat 192.168.2.1.

Pemonitoran juga dapat dilakukan dengan melakukan pengauditan sistem Log pada server tertentu oleh administrator jaringan. Tujuannya adalah mengidentifikasi gangguan dan ancaman keamanan yang akan terjadi pada jaringan. Administrator dapat juga menggunakan software seperti NSauditor yang bertujuan untuk mengevaluasi keamanan jaringan dan dapat melakukan audit untuk penanggulangan kesalahan. Slain NSauditor, ada pula tools yang lain yang dapat digunakan untuk mendiagnosis seperti:

- GFI Network Server Monitoring
- MRTG

Selain perangkat lunak, perangkat keras pun perlu dilakukan monitoring. Hal apakah yang perlu diperhatikan dalam monitoring perangkat keras antara lain adalah sebagai berikut:

- Waktu respon perangkat keras
- Kompatibilitas dengan perangkat lunak

Pada sistem operasi tertentu perlu dirancang sistem monitoring yang bersifat user friendly, seperti merancang sistem monitoring berbasis web (misalnya menggunakan PHP dan Apache, dengan browser dan Linux kernel 2.4.xx). Untuk dapat menerapkan sistem monitoring berbasis web ada dua hal yang perlu diperhatikan, sebagai berikut:

- Koneksi ke internet atau intranet
- Kompatibilitas dengan browser

Metode pemonitoran melalui web ini dapat dilakukan melalui protokol HTTP. Akan tetapi protokol ini tidak dijamin keamanannya, karena itu perlu dilakukan pengenkripsian informasi yang dikirim melalui browser dengan menggunakan sebuah enkripsi yang dinamakan dengan SSH.

❖ Intrusion Detection System

Intrusion Detection System (IDS) adalah sebuah sistem untuk mendeteksi penyalahgunaan jaringan dan sumber daya komputer. IDS memiliki sejumlah sensor yang digunakan untuk mendeteksi penyusupan. Contoh sensor meliputi:

- Sebuah sensor untuk memonitor TCP request
- Log file monitor
- File integrity checker

IDS memiliki diagram blok yang terdiri dari 3 buah modul, sebagai berikut:

- Modul sensor (sensor modul)
- Modul analisis (analyzer modul)
- Modul basis data (database modul)

Sistem IDS bertanggung jawab untuk mengumpulkan dara-data dari sensor dan

kemudian menganalisisnya untuk diberikan kepada administrator keamanan jaringan. Tujuannya adalah untuk memberikan peringatan terhadap gangguan pada jaringan.

Teknologi IDS secara umum terbagi menjadi

- NIDS (Network Intrusion Detection System) dan
- HIDS (Host Intrusion Detection System). Snort adalah salah satu open source yang baik untuk NIDS.

Sistem deteksi Snort terdiri dari sensor dan analyzer. AIRIDS (Automatic Interactiv e Reactive Intrusion Detection System) adalah suatu metode kemanan jaringan yang bertujuan untuk membentuk suatu arsitektur sistem keamanan yang terintegrasi. Untuk mewujudkan AIRIDS perlu dirancang komponen-komponen sistem jaringan sebagai berikut:

- IDS
- Sistem firewall
- Sistem basis data