Navigating the Network Security Landscape

A Comprehensive Exploration from OSI Layers to Security Protocols and Beyond

CISSP Study Guide - VII

Introduction to Network Security

- Focus on the OSI Model's Layers

- Highlighting Importance for Hardware/Software Interoperability

OSI Model Overview

1   **Function:** Breakdown of communication process into layers

2   Allows for flexibility in altering a single layer

3   Fosters interoperability among diverse systems

OSI Model Detailed Layers - Part 1

Layer 7: Application

- **Services:** File Transfer, Email, Web Browsing
- **Protocols:** HTTP, DNS, FTP, SMTP

Layer 6: Presentation

- **Role:** Data Format Standardization
- **Protocols:** MIME, XDR

Layer 5: Session

- Manages Communication Sessions
- Uses Port Numbers to Identify Services

OSI Model Detailed Layers - Part 2

Layer 4: Transport

- **Types:** Connection-Oriented (TCP) or Connectionless (UDP)

- **PDU:** Segment

- Ensures Reliable Data Delivery

Layer 3: Network

- Assigns Logical Addresses for Routing

- **PDU:** Packet

- **Protocols:** IP, ICMP, IGMP, ARP

TCP/IP Model Mapping to OSI

1 **TCP/IP Model Layers**

- Application

- Transport

- Internet

- Network Access

2 **OSI Model Correspondence**

- Application to Application & Presentation & Session

- Transport to Transport

- Internet to Network

- Network Access to Data-Link & Physical

IP Addressing and Encapsulation

IP Address Types

- External Classes: A, B, C

- Internal Private Ranges

MAC Addressing

- Unique per NIC

- 48-bit hex format, e.g., 01:23:34:67:89:ab

Encapsulation Process

- Layer-by-layer addition of Protocol Headers

- Critical for Data Flow across Network Layers

Network Transmission Methods

Asynchronous vs. Synchronous

- Timing and Coordination in Data Transmission

Broadband vs. Baseband

- **Broadband:** Multiple Frequency Bands
- **Baseband:** Single Frequency Band

Unicast, Multicast, Broadcast

- Targeting Data Transmission Methods

Wireless and Wired Technologies

1 **Wired Technologies Variants**

- Twisted Pair (Category 3 up to 10GBaseT)
- Fiber Optics (Core and Cladding)

2 **Network Topologies**

- Ring, Bus, Star, Hybrid

3 **Wireless Technologies**

- **Standards:** 802.11 (WiFi), 802.16 (WiMax)

WAN and Remote Connection Technologies

WAN Connectivity

- T1, E1, E3 Lines, and SONET

Remote Connections Options

- Dial-Up, ISDN, Cable, DSL

- VPN with PPTP, L2TP, IPsec Components

Cellular Wireless Techniques

- FDMA, TDMA, CDMA, OFDMA, GSM

Security in Networking

Security Protocols and Components

- RADIUS, TACACS for Centralized Authentication

- SSL/TLS for Secure Web Transactions

- IPsec for Secure Network Layer Transmissions

Wireless Security Models

- WEP, WPA, WPA2 with Various Authentication and Encryption Techniques

Common Network Attacks

- ICMP, DNS, Email, and Wireless Attacks

- Precautions and Methods to Mitigate Risks

Information Security Buzz

Discover more at our InfoSec Knowledge Hub