Lecture 2 - notes

Core Security Concepts

- CIA Triad
- Confidentiality: Prevent unauthorized access to data.
- Integrity: Ensure data is accurate and unaltered.
- Availability: Ensure reliable access to data and systems.

TCP/IP Network Stack

- Layers
- Application: Encodes/decodes messages.
- Transport: Breaks messages into packets; ensures correct order.
- Network: Adds sender/receiver IP addresses.
- Link: Transfers packets between nodes/networks.

IP Addressing

- CIDR Notation: e.g., 192.168.192.0/19 defines a range of IPs.
- Special IPs:
- Private: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- Loopback: 127.0.0.1

DHCP & DNS Workflow

- DHCP: Assigns IP, router, and DNS info to clients.
- ARP: Resolves MAC addresses before sending DNS queries.
- DNS: Resolves domain names to IP addresses.

HTTP Communication

- TCP Handshake: SYN → SYN-ACK → ACK
- HTTP Request/Reply: Sent over established TCP connection.

Cryptography Basics

- Public-Key (Asymmetric): Used for authentication & integrity.
- Symmetric-Key: Used for confidentiality.

PGP (Pretty Good Privacy)

- Hybrid System: Combines symmetric & asymmetric encryption.
- Services:
- Authentication
- Confidentiality
- Compression (ZIP)
- Email compatibility (Base64)
- Segmentation

Key Management

- Key Rings: Store private/public keys.
- Web of Trust: Decentralized trust model.

IPSec Overview

- Purpose: Secure IP communications across networks.
- Functions:
- Authentication (AH)
- Confidentiality (ESP)
- Key Management (IKE)
- Modes
- Transport Mode: Encrypts payload only.
- Tunnel Mode: Encrypts entire IP packet.

IPSec Components

- AH: Authenticates source & integrity.
- ESP: Encrypts payload; optional authentication.
- SA (Security Association): Defines security parameters.
- SAD/SPD: Databases for managing SAs and policies.

SSL/TLS

- Purpose: Secure transport layer communication.
- Authentication: Server-only or mutual.
- Protocols:
- Handshake
- Record
- Cipher Change
- Alert
- Record Protocol Steps
- Fragmentation
- Compression (optional)
- MAC addition
- Encryption
- Header addition

SSL Handshake Phases

- Establish capabilities
- Server authentication & key exchange
- Client key exchange & authentication
- Finalize secure connection

13. Heartbeat Extension & Heartbleed Bug

- Heartbeat: Keeps session alive.
- Heartbleed: Exploited unchecked payload length to leak memory.