Computer Security

Short Notes based on ***Exit Exam***

Zemzem labs

1. Fundamentals of Computer Security

✦ Key Goals

1. **Confidentiality** – Prevent unauthorized access to data
2. **Integrity** – Prevent unauthorized modification
3. **Availability** – Ensure data/services are accessible

Additional Principles:

- **Authentication** – Verify identity
- **Authorization** – Grant permissions
- **Non-repudiation** – Ensure sender cannot deny actions
- **Accountability** – Track actions (logging, auditing)

2. Security Threats & Attacks

Types of Attacks

- **Passive attacks** – Eavesdropping, traffic analysis
- **Active attacks** – Modification, impersonation, DoS, MITM

Malware

- Virus
- Worm
- Trojan horse
- Ransomware
- Spyware
- Rootkits
- Botnets

Attack Techniques

- Phishing / Spear phishing
- SQL Injection
- Cross-Site Scripting (XSS)
- Brute-force attack
- Dictionary attack
- Buffer overflow attack
- Session hijacking
- Denial of Service (DoS/DDoS)

3. Cryptography

Two Types

1. **Symmetric-key cryptography**

   - Same key for encryption/decryption
   - Examples: **AES, DES, 3DES, RC4**
   - Fast; used for bulk data
2. **Asymmetric-key cryptography**
   - Public key ↔ Private key
   - Examples: **RSA, ECC, Diffie–Hellman**
   - Used for key exchange, digital signatures

Hash Functions

- One-way, collision-resistant
- Examples: **SHA-256, SHA-3, MD5 (broken)**

Digital Signature

- Provides:
   - **Authentication**
   - **Integrity**
   - **Non-repudiation**
- Uses **private key** to sign; **public key** to verify

4. Network Security

Firewalls

- Packet-filtering firewall
- Stateful firewall
- Application-level firewall
- NG-Firewall (next-gen)

IDS/IPS

- IDS (Intrusion Detection System) – detects attacks
- IPS (Intrusion Prevention System) – detects + blocks attacks

VPN

- Provides secure tunneling
- Uses encryption protocols like IPsec, SSL/TLS

Secure Protocols

- HTTPS
- SSH
- TLS/SSL
- IPsec
- S/MIME (for email)

5. Access Control Models

DAC – Discretionary Access Control

- Owner controls access
- Flexible but less secure

MAC – Mandatory Access Control

- Access based on labels (Top Secret → Secret → Public)
- Used in military/government

RBAC – Role-Based Access Control

- Access based on roles (Admin, Student, Manager)
- Most common in organizations

ABAC – Attribute-Based Access Control

- Access based on multiple attributes (user, environment, resource)

6. Authentication Methods

- Passwords
- Two-Factor Authentication (2FA)
- Biometrics (fingerprint, iris scan)
- Tokens (smartcards)
- OTP (One-Time Passwords)

Password Attacks

- Brute-force
- Dictionary
- Rainbow table
- Credential stuffing

7. Software & Application Security

Vulnerabilities

- Buffer overflow
- Input validation weaknesses
- SQL Injection
- XSS
- CSRF (Cross Site Request Forgery)

Secure Coding Practices

- Validate input
- Sanitize data
- Avoid unsafe functions

- Principle of least privilege

8. Operating System Security

Protection Mechanisms

- User accounts & permissions
- Access control lists (ACLs)
- Sandboxing
- SELinux / AppArmor
- Patch management
- System logs & auditing

9. Security Policies & Management

Key Concepts

- Strong password policy
- Backup & recovery plan
- Patch/update policy
- Incident response plan
- Disaster recovery

Risk Management

- Identify → Analyze → Evaluate → Mitigate risks

Security Standards

- ISO 27001
- NIST
- PCI-DSS
- GDPR compliance

10. Modern Security Topics

Cloud Security

- Shared responsibility model
- Data encryption
- IAM (Identity & Access Management)

Web Security

- Same-Origin Policy
- Secure cookies
- HSTS
- CSP (Content Security Policy)

Zero Trust Security

- "Never trust, always verify"
- Continuous authentication & monitoring