Exam Cram Notes: Security Techniques for Computing Resources

1. Overview

Security techniques for computing resources focus on **protecting hardware, software, networks, and data** from unauthorized access, threats, and attacks. This includes **endpoint protection, access controls, encryption, and monitoring strategies** to maintain system integrity, confidentiality, and availability.

---

2. Endpoint Security

A. Antivirus & Anti-Malware Solutions

✅ **Signature-Based Detection** – Identifies known threats using a database.
✅ **Heuristic Analysis –** Detects new threats by analyzing behavior.
✅ **Behavioral-Based Detection** – Identifies anomalies in real time.
✅ **Cloud-Based Security –** Updates signatures dynamically to detect emerging threats.

B. Host-Based Firewalls

✅ Blocks **unauthorized inbound & outbound traffic** at the device level.
✅ Can be configured using **whitelisting or blacklisting**.

C. Host-Based Intrusion Detection Systems (HIDS)

✅ Monitors logs & system activities for **suspicious behavior**.
✅ Can provide alerts or **automatically respond** to threats.

D. Endpoint Detection & Response (EDR)

✅ Advanced **real-time monitoring** and response to **sophisticated attacks**.
✅ Uses **AI & machine learning** to analyze threats.

---

3. Access Control Mechanisms

A. Authentication Techniques

✅ **MFA (Multi-Factor Authentication)** – Requires at least two factors:

- Something You Know (Password, PIN)
- Something You Have (Smart Card, Token)
- Something You Are (Biometrics: Fingerprint, Face ID)

✅ **Password Policies –** Strong passwords, rotation, and complexity enforcement.
✅ **SSO (Single Sign-On)** – One authentication for multiple services.

✅ **Federated Identity Management (FIM)** – Cross-organizational identity verification (e.g., SAML, OAuth).

B. Authorization & Role-Based Access Control (RBAC)

✅ **Least Privilege Principle** – Users only get permissions they need.
✅ **RBAC (Role-Based Access Control)** – Permissions assigned by job roles.
✅ **ABAC (Attribute-Based Access Control)** – Uses attributes like location, device, or time for access control.
✅ **Zero Trust Architecture (ZTA)** – No implicit trust; continuous verification.

C. Privileged Access Management (PAM)

✅ **Monitors & restricts privileged accounts** (e.g., administrators).
✅ Uses **just-in-time (JIT) access** to limit exposure.
✅ Logs & audits **privileged user activities**.

---

4. Network Security Techniques

A. Network Segmentation

✅ **DMZ (Demilitarized Zone)** – Isolates public-facing systems from the internal network.
✅ **Micro-Segmentation** – Divides the network into isolated sections for enhanced security.
✅ **Virtual LANs (VLANs)** – Separate network traffic logically.

B. Firewalls & Network Access Controls

✅ **Next-Generation Firewalls (NGFWs)** – Use **deep packet inspection** & application-layer filtering.
✅ **Network Access Control (NAC)** – Restricts devices based on security posture before granting access.

C. Intrusion Detection & Prevention Systems (IDS/IPS)

✅ **IDS** – Detects suspicious activities but does not block them.
✅ **IPS** – Actively blocks attacks before they reach critical systems.

---

5. Data Security Techniques

A. Encryption Techniques

✅ **Data at Rest** – Encrypt stored data (BitLocker, AES-256).
✅ **Data in Transit** – Use TLS/SSL for secure communication.
✅ **Data in Use** – Protect sensitive data while being processed.

B. Data Loss Prevention (DLP)

✅ **Prevents sensitive data leaks** via email, USB, or cloud services.
✅ **Monitors & blocks unauthorized data transfers**.

C. Secure Boot & Trusted Platform Module (TPM)

✅ **Secure Boot** – Ensures only trusted OS and firmware load during startup.
✅ **TPM (Trusted Platform Module)** – Hardware-based encryption for securing cryptographic keys.

---

6. Cloud Security & Virtualization Protections

A. Secure Virtualization

✅ **Hypervisor Security** – Protects virtual machines from attacks.
✅ **Virtual Private Cloud (VPC)** – Isolated cloud environments for enhanced security.

B. Cloud Security Controls

✅ **CASB (Cloud Access Security Broker)** – Monitors cloud applications for compliance.
✅ **Cloud Encryption** – Encrypts data before storing it in the cloud.
✅ **Container Security** – Uses tools like Kubernetes security policies & runtime protection.

---

7. Logging & Monitoring for Threat Detection

A. Security Information & Event Management (SIEM)

✅ **Aggregates & analyzes logs** from multiple sources.
✅ Uses **real-time correlation** to detect security incidents.
✅ Supports **automated threat response**.

B. Endpoint Logging

✅ Tracks **user activities, file access, and software execution**.
✅ Helps in **forensic analysis** after an attack.

C. Threat Intelligence Feeds

✅ Helps **identify new and emerging threats**.
✅ Uses external threat data to **proactively defend against attacks**.

---

8. Key Exam Takeaways

✅ **Use Endpoint Security** (Antivirus, EDR, Firewalls, IDS/IPS).
✅ **Enforce Access Controls** (MFA, RBAC, Zero Trust).

✅ **Secure Networks** (Firewalls, NAC, Segmentation).

✅ **Encrypt Data** (TLS, BitLocker, AES-256).

✅ **Use Cloud Security Measures** (CASB, Secure Virtualization).

✅ **Monitor & Log Security Events** (SIEM, Threat Intelligence).