## Unit IV: Security Technologies and Tools

### 1. Firewall

A firewall is a network security device (or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and an untrusted external network (like the Internet).

**How it Works:** It establishes a choke point where all traffic is inspected. Rules are defined to allow or block specific types of traffic (based on IP address, port number, protocol, etc.).

**Types:**

- **Packet-Filtering Firewall:** Examines each packet in isolation and accepts or rejects it based on rules. (e.g., "Block all traffic from IP 192.168.1.100").
- **Stateful Inspection Firewall:** Tracks the state of active connections and makes decisions based on the context of the traffic. More intelligent than packet filtering.
- **Application-Level Gateway (Proxy Firewall):** Acts as an intermediary between two hosts. The internal client connects to the proxy, which then establishes a connection to the external server. It can inspect application-layer data (e.g., HTTP).
- **Next-Generation Firewall (NGFW):** Integrates traditional firewall capabilities with advanced features like Intrusion Prevention Systems (IPS), deep packet inspection (DPI), and application awareness.

**Example:**

- A company sets a firewall rule: **"Allow outbound traffic on port 80 (HTTP) and 443 (HTTPS) but block all inbound traffic on those ports except for the company's web server (IP: 203.0.113.10)."**

**Advantages:**

- Prevents unauthorized access to a network.
- Can block malicious software (malware).
- Logs network traffic for auditing and analysis.
- Simple to implement for basic protection.

**Disadvantages:**

- Cannot protect against attacks that bypass it (e.g., a user downloading a malicious file via allowed HTTPS).
- Cannot stop internal threats.
- Configuration can be complex and prone to errors.
- Can be a single point of failure and a performance bottleneck.

**2. Intrusion Detection and Prevention System (IDPS)**

An IDPS monitors network or system activities for malicious activities or policy violations.

- **Intrusion Detection System (IDS):** A passive system that detects and alerts administrators about potential incidents. It does not take action to stop them.
  - **Network-based (NIDS):** Monitors network traffic.
  - **Host-based (HIDS):** Monitors activity on a single host (e.g., file changes, log analysis).
- **Intrusion Prevention System (IPS):** An active system placed in-line with the traffic. It can automatically block or drop malicious packets in real-time.

**Detection Methods:**

- **Signature-based:** Matches activity against a database of known attack signatures (like an antivirus). Effective against known threats.
- **Anomaly-based:** Establishes a baseline of "normal" behavior and flags significant deviations. Effective against zero-day attacks.

**Example:**

- **IDS:** An IDS sensor sees a surge of TCP SYN packets from a single IP (a potential SYN flood attack) and sends an alert to the security team.
- **IPS:** An IPS detects a packet with the signature of a known SQL injection attack and immediately drops the packet before it reaches the web server.

**Advantages:**

- Provides real-time (IPS) or near-real-time (IDS) monitoring.
- Can detect both known and unknown (anomaly-based) threats.
- Helps in meeting regulatory compliance.

**Disadvantages:**

- Can generate false positives (blocking legitimate traffic) and false negatives (missing real attacks).
- Requires significant tuning and maintenance.
- IPS can impact network performance if not properly configured.

**3. Honeypots**

A honeypot is a decoy system designed to attract, detect, and study cyber-attacks. It has no authorized production value; any interaction with it is considered suspicious.

**Types:**

- **Low-Interaction Honeypot:** Emulates only limited services and operating systems (e.g., Kippo for SSH). Low risk, easy to deploy.
- **High-Interaction Honeypot:** Involves a real operating system and applications. Provides extensive information but is complex and risky to manage.

**Example:**

- A security researcher sets up a server that appears to be a vulnerable database server with default credentials. When an attacker connects and tries to exploit it, the researcher can study the attacker's methods, tools, and motives.

**Advantages:**

- Diverts attackers from real production systems.
- Provides valuable intelligence on new attack vectors and tools.
- Low false positive rate (any activity is likely malicious).

**Disadvantages:**

- Only monitors attacks against itself.
- High-interaction honeypots can be compromised and used as a launchpad for further attacks if not isolated properly.
- Requires expertise to set up and maintain.

---

### 4. Scanning and Analysis Tools

These tools are used to discover weaknesses and analyze network traffic.

- **Port Scanner:** Scans a network host for open ports, which can indicate running services.
  - **Tool:** `Nmap`
  - **Example:** `nmap -sS 192.168.1.1` performs a TCP SYN scan on the target IP to find open ports.
- **Vulnerability Scanner:** Automatically scans systems for known vulnerabilities (missing patches, misconfigurations).
  - **Tool:** Nessus, OpenVAS
  - **Example:** A scan reveals that a server is missing a critical security patch for Apache, making it vulnerable to a specific exploit.
- **Packet Sniffer (Protocol Analyzer):** Captures and logs network traffic for analysis. Used for troubleshooting and security analysis.
  - **Tool:** Wireshark, tcpdump
  - **Example:** Using Wireshark to capture traffic and filter for `http` to see unencrypted usernames and passwords being transmitted.

**Advantages:**

- Proactive identification of security weaknesses.
- Essential for network inventory and management.
- Helps in compliance auditing.

**Disadvantages:**

- Can be used maliciously by attackers for reconnaissance.
- May cause system instability if scans are too aggressive.
- Can generate a large volume of data that requires expert analysis.

### 5. Penetration Testing

Penetration Testing (or Pen Testing) is an authorized, simulated cyber-attack on a computer system, performed to evaluate the security of the system. It goes beyond vulnerability scanning by actively exploiting found vulnerabilities.

**Phases:**

1. **Planning & Reconnaissance:** Defining scope, gathering intelligence.
2. **Scanning:** Using tools to understand how the target responds.
3. **Gaining Access:** Exploiting vulnerabilities to break in (e.g., SQL injection, buffer overflow).
4. **Maintaining Access:** Seeing if a persistent presence can be established (like a backdoor).
5. **Analysis & Reporting:** Documenting the findings, risks, and remediation advice.

**Example:**

- A pen tester is hired to test a company's web application. They discover an input field vulnerable to SQL injection, use it to extract the user database, and then use a cracked password to gain admin access. All steps are documented in a report for the company.

**Advantages:**

- Provides a real-world assessment of security posture.
- Helps prioritize remediation efforts based on actual risk.
- Validates the effectiveness of security controls.

**Disadvantages:**

- Can be expensive and time-consuming.
- Carries a risk of disrupting systems if not done carefully.
- Scope limitations might prevent a full assessment.

**6. Secure Communication**

Technologies that ensure the confidentiality, integrity, and authenticity of data transmitted over a network.

- **VPN (Virtual Private Network):** Extends a private network across a public network, allowing users to send and receive data as if their devices were directly connected to the private network.

- **Example:** An employee working from home uses a VPN client to securely connect to the corporate network.
- **SSL/TLS (Secure Sockets Layer / Transport Layer Security):** Cryptographic protocols designed to provide communications security over a computer network (e.g., HTTPS).
  - **Example:** The padlock icon in your browser when you visit your bank's website indicates a TLS-encrypted connection.
- **IPsec (Internet Protocol Security):** A suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a data stream.
  - **Example:** Used to create site-to-site VPNs between corporate offices.
- **WEP, WPA, WPA2, WPA3:** Security protocols for wireless networks.
  - **WEP:** Insecure and easily broken. **Avoid.**
  - **WPA/WPA2:** Significant improvement over WEP. WPA2 is the long-standing standard.
  - **WPA3:** The latest standard, providing stronger encryption and protection against offline attacks.
- **SET (Secure Electronic Transaction):** An old, complex standard for securing credit card transactions over the Internet. It was largely superseded by SSL/TLS and is now obsolete.

**Advantages:**

- Ensures privacy and data integrity over untrusted networks.
- Enables secure remote access.
- Protects against eavesdropping and man-in-the-middle attacks.

**Disadvantages:**

- Can add latency and overhead to communication.
- Misconfiguration can lead to security gaps.
- Older protocols (WEP, SSL) have known, exploitable vulnerabilities.

### 7. Concept of Access Control, Authentication, and Authorization

These are three core security concepts that work together.

- **Identification:** Claiming an identity (e.g., providing a username).
- **Authentication:** Proving the identity (e.g., providing a password).
- **Authorization:** Determining what resources and actions the authenticated identity is permitted to access (e.g., "User X can read file A but cannot delete it").
- **Access Control:** The process of implementing authorization.

**Example:**

- **Identification:** You enter your email `user@company.com`.
- **Authentication:** You provide your password and a code from your phone (2FA).
- **Authorization:** The system checks that you are a "Manager" and grants you access to the project budget files.
- **Access Control:** The system enforces that you cannot access the "HR Salaries" folder.

**8. Identification and Authentication Techniques**

**Identification Techniques:**

- Username, Email, Employee ID, Smart Card.

**Authentication Techniques (Factors):**

- **Something You Know:** Passwords, PINs.
- **Something You Have:** Smart cards, Security tokens (RSA SecurID), Mobile phones (for SMS codes).
- **Something You Are:** Biometrics (Fingerprint, Iris scan, Facial recognition).

**Multi-Factor Authentication (MFA):** Using two or more of the above factors. (e.g., Password + SMS code).

**Advantages of MFA:**

- Significantly increases security by adding layers of defense.
- Mitigates the risk of stolen passwords.

**Disadvantages of MFA:**

- Can be inconvenient for users.

- "Something you have" factors can be lost or stolen.
- Biometrics can raise privacy concerns.

**9. Access Control Techniques**

Models that define how access rights are granted to subjects (users, processes) over objects (files, resources).

- **Discretionary Access Control (DAC):** The owner of the resource decides who has access.
  - **Example:** In a Windows file system, you right-click a folder, go to "Properties" > "Security," and grant "Read" permission to a specific user.
- **Mandatory Access Control (MAC):** Access is controlled by a central authority based on mandated regulations. Users cannot change permissions.
  - **Example:** Used in military and government systems. Data is labeled "Top Secret," "Secret," etc., and users have corresponding clearances.
- **Role-Based Access Control (RBAC):** Access is granted based on the user's role within the organization.
  - **Example:** All "Doctors" in a hospital system can access patient records, but "Receptionists" can only access appointment schedules.
- **Attribute-Based Access Control (ABAC):** A more dynamic model where access is granted based on attributes of the user, resource, and environment.
  - **Example:** "A user from the `Finance` department (`user attribute`) can `edit` (`action`) the `Budget` file (`resource attribute`) only during `business hours 9 AM - 5 PM` (`environment attribute`)."

**Advantages:**

- **DAC:** Flexible and easy to manage for small groups.
- **MAC & RBAC:** Provide strong, consistent security and are easier to manage at scale.
- **ABAC:** Highly granular and flexible, suitable for complex environments.

**Disadvantages:**

- **DAC:** Prone to error; users may grant excessive permissions (the "confused deputy" problem).

- **MAC & RBAC:** Can be inflexible and require significant upfront planning.
- **ABAC:** Can be complex to implement and manage.

nmap