ATTACK VECTORS

Definition:

An attack vector is a path or method used by a hacker to gain unauthorized access to a computer system or network to deliver a malicious payload or outcome. Attack vectors exploit vulnerabilities in systems, applications, or user behavior.

Types of Attack Vectors:

1. **Network-Based Vectors**
   - **Man-in-the-Middle (MITM):** Intercepts communication between two parties.
   - **DNS Spoofing:** Redirects traffic to malicious websites.
   - **Port Scanning:** Identifies open ports and vulnerabilities.
2. **Web-Based Vectors**
   - **Cross-Site Scripting (XSS):** Injects malicious scripts into trusted websites.
   - **SQL Injection:** Executes malicious SQL commands via form inputs.
   - **Cross-Site Request Forgery (CSRF):** Tricks users into executing unwanted actions.
3. **Email-Based Vectors**
   - **Phishing:** Fraudulent emails to steal credentials.
   - **Spear Phishing:** Targeted phishing for specific individuals or organizations.
   - **Malicious Attachments/Links:** Payloads delivered via email.
4. **Software-Based Vectors**
   - **Malware:** Includes viruses, worms, trojans, ransomware, etc.
   - **Zero-Day Exploits:** Exploits unknown vulnerabilities.
   - **Drive-by Downloads:** Automatic download of malware from compromised websites.
5. **Physical Attack Vectors**
   - **USB Drop Attack:** Infected USB drives left for users to find and plug in.
   - **Tailgating:** Unauthorized person following someone into a secure area.
   - **Hardware Keyloggers:** Capture keystrokes physically.
6. **Insider Threats**
   - **Disgruntled Employees:** Malicious actions from current or former staff.
   - **Unintentional Errors:** Accidental exposure due to poor security awareness.
7. **Social Engineering**

- **Impersonation:** Pretending to be someone trustworthy.
- **Pretexting:** Using a fabricated scenario to extract information.
- **Baiting:** Enticing a victim to take action (e.g., click a fake link).

Mitigation Strategies:

1. Network-Based Attack Vectors

Attack	Mitigation Techniques
MITM (Man-in-the-Middle)	- Use **TLS/SSL** for encryption (force HTTPS)- Implement **certificate pinning** in applications- Deploy **VPNs** for remote access- Use **DNSSEC** to secure DNS queries
DNS Spoofing	- Use **DNSSEC** to validate DNS records- Configure **firewalls** to block unauthorized DNS responses- Monitor DNS logs for anomalies
Port Scanning	- Implement **firewalls** with default-deny policies- Use **port knocking** to hide open ports- Deploy **intrusion detection systems (IDS)** like Snort/Suricata- Disable unnecessary services and ports

2. Web-Based Attack Vectors

Attack	Mitigation Techniques
XSS (Cross-Site Scripting)	- Use **input validation** and **output encoding** (e.g., htmlspecialchars())- Implement **Content Security Policy (CSP)** headers- Use frameworks with built-in XSS protection (e.g., Django, React)

SQL Injection	- Use **parameterized queries** or **ORMs**- Validate and sanitize all user inputs- Limit database permissions for web apps- Use **Web Application Firewalls (WAFs)**
CSRF	- Use **anti-CSRF tokens** for all state-changing requests- Set **SameSite** cookie attribute to Strict or Lax- Require **re-authentication** for critical actions

3. Email-Based Attack Vectors

Attack	Mitigation Techniques
Phishing/Spear Phishing	- Use **email filtering solutions** (e.g., Proofpoint, Mimecast)- Train users with **security awareness programs**- Implement **DMARC, SPF, and DKIM** for email authentication
Malicious Attachments/Links	- Use **sandboxing** to analyze attachments- Disable **macros** in Office documents- Scan links and attachments with **antivirus/ antimalware** solutions

4. Software/Application-Based Attack Vectors

Attack	Mitigation Techniques
Malware	- Use **Endpoint Detection & Response (EDR)** tools- Keep systems **patched and updated** regularly- Apply **least privilege principle** for users and services
Zero-Day Exploits	- Use **behavioral analysis tools** (e.g., CrowdStrike, SentinelOne)- Monitor for **indicators of compromise (IoC)**- Regularly update and rotate **security configurations**

Drive-by Downloads	- Block unknown/malicious domains using **web proxies**- Disable automatic downloads and JavaScript in browsers- Use **browser isolation** technology

5. Insider Threats

Threat Type	Mitigation Techniques
Malicious Insiders	- Enforce **role-based access control (RBAC)**- Log and **monitor privileged user activity** (SIEM solutions)- Perform **background checks** and enforce **exit policies**
Negligent Users	- Regular **security training** on phishing, data handling- Use **Data Loss Prevention (DLP)** solutions- Disable **USB storage access** if not needed

6. Social Engineering

Technique	Mitigation Techniques
Impersonation/Pretexting	- Conduct **security drills and simulations**- Train employees to **verify identities** via trusted channels- Use **two-person rule** for sensitive operations
Baiting	- Restrict external media (e.g., **block USBs**) and enforce endpoint policies- Use **host-based security tools** to detect unknown devices- Educate users not to plug in unknown devices

7. General Best Practices

Category	Techniques

Access Control	- Use **Multi-Factor Authentication (MFA)**- Enforce **least privilege principle**- Use **identity and access management (IAM)** tools
Monitoring & Logging	- Deploy a **Security Information and Event Management (SIEM)** system- Enable **audit logging** for sensitive operations- Set up **alerts for abnormal behavior**
Patch Management	- Automate updates with tools like **WSUS**, **Ansible**, or **Patch Manager Plus**- Maintain an **asset inventory** and track versioning- Subscribe to **CVE feeds** for threat intelligence
Incident Response	- Have an updated **incident response plan (IRP)**- Perform **regular tabletop exercises**- Define **playbooks** for common attacks using **SOAR** tools
Backups	- Schedule **regular encrypted backups**- Store backups **offline or in immutable storage**- Test **restoration processes** regularly