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 VECTIRS WITH IT'S CLASSIFICATION:

1. Insider Threats

Attack Vector	Explanation
Malicious Insider	Employee or contractor intentionally harming the organization.
Negligent Insider	Careless actions like clicking phishing links or losing devices.
Insider Credential Abuse	Using legitimate access for unauthorized actions.

2. Social Engineering Attacks

Attack Vector	Explanation
Phishing	Fake emails or messages to steal credentials/data.
Spear Phishing	Targeted phishing at individuals or roles.
Whaling	Phishing targeting high-profile execs.
Pretexting	Impersonating authority to get info.
Baiting	Luring with false promises (e.g., free USBs).
Quid Pro Quo	Offering something in exchange for access or info.
Tailgating	Following authorized personnel into restricted areas.
Impersonation	Pretending to be someone trustworthy.

3. Software-Based Attacks

Attack Vector	Explanation

Malware	Malicious software like viruses, worms, Trojans.
Ransomware	Encrypts files; demands ransom.
SQL Injection	Injecting malicious SQL to manipulate databases.
XSS (Cross-Site Scripting)	Injecting scripts into web pages.
Remote Code Execution	Exploiting flaws to run attacker code.
Exploit Kits	Toolkits to automate vulnerability exploitation.
Zero-Day Exploits	Attacking unknown/unpatched software flaws.
Drive-by Downloads	Automatic malware downloads from compromised websites.
Credential Stuffing	Reusing stolen credentials across services.
Session Hijacking	Taking over authenticated sessions.

4. Hardware-Based Attacks

Attack Vector	Explanation
Firmware Attacks	Modifying firmware to create persistent threats.
Hardware Backdoors	Hidden, unauthorized access in hardware.
Keyloggers	Devices recording keystrokes.
Physical Implant	Malicious chips inserted into hardware.
Rowhammer Attack	Bit flipping by repeatedly accessing memory.

5. Physical Attacks

Attack Vector	Explanation
Device Theft	Stealing laptops, phones with sensitive data.
Dumpster Diving	Searching trash for sensitive info.
Tailgating / Piggybacking	Following authorized personnel into secure locations.
USB Drop Attack	Infected USB drives left for users to plug in.

Unlocked Devices	Exploiting unattended, unprotected systems.
Hardware Keyloggers	Capturing keystrokes via physical devices.

6. Network-Based Attacks

Attack Vector	Explanation
Man-in-the-Middle (MitM)	Intercepting communication between two parties.
ARP Spoofing	Mapping attacker’s MAC address to victim’s IP.
DNS Spoofing	Redirecting to fake websites.
DoS / DDoS	Flooding services to disrupt operations.
Packet Sniffing	Monitoring unencrypted network traffic.
Port Scanning	Identifying open ports and vulnerabilities.

7. Web-Based Attacks

Attack Vector	Explanation
SQL Injection	Executing malicious SQL via form inputs.
XSS (Cross-Site Scripting)	Injecting malicious scripts into trusted websites.
CSRF (Cross-Site Request Forgery)	Forcing users to perform unwanted actions.
Clickjacking	Tricking users into clicking hidden elements.
Cookie Poisoning	Modifying cookies to impersonate users.
Watering Hole Attack	Compromising sites commonly visited by targets.
Typosquatting	Using lookalike domain names to trap users.
Directory Traversal	Gaining access to restricted server files.
Command Injection	Running system commands via web inputs.
Local/Remote File Inclusion (LFI/RFI)	Loading unintended or malicious files.

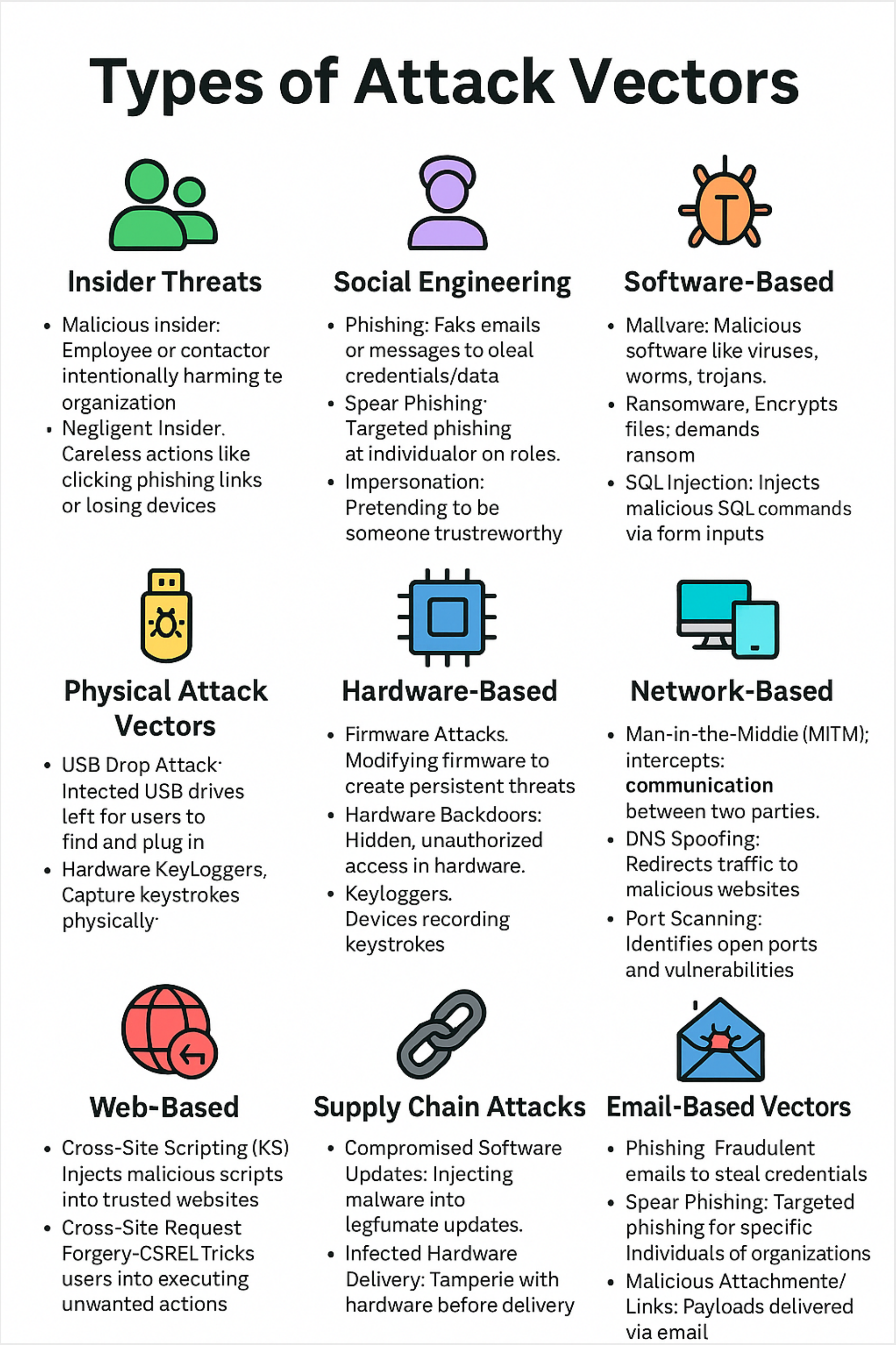
Web Cache Poisoning	Poisoning cache to serve malicious content.
Broken Authentication	Flaws in login/session handling.
Broken Access Control	Bypassing permissions to access data or actions.
API Abuse	Exploiting insecure or misconfigured APIs.
Business Logic Abuse	Misusing app logic for unintended gain.
Host Header Injection	Manipulating host headers to redirect or access data.
HTTP Response Splitting	Injecting headers to split server responses.

8. Supply Chain Attacks

Attack Vector	Explanation
Compromised Software Updates	Injecting malware into legitimate updates.
Infected Hardware Delivery	Tampering with hardware before delivery.
Vendor Access Exploitation	Abusing trust in third-party providers.

9. Email-Based Attacks

Attack Vector	Explanation
Phishing	Fraudulent emails to steal credentials.
Spear Phishing	Targeted phishing for individuals or organizations.
Malicious Attachments/Links	Delivering malware through files or URLs in email.



Types of Attack Vectors

Insider Threats

- Malicious insider: Employee or contactor intentionally harming te organization
- Negligent Insider. Careless actions like clicking phishing links or losing devices

Social Engineering

- Phishing: Faks emails or messages to oleal credentials/data
- Spear Phishing· Targeted phishing at individualor on roles.
- Impersonation: Pretending to be someone trustreworthy

Software-Based

- Mallvare: Malicious software like viruses, worms, trojans.
- Ransomware, Encrypts files; demands ransom
- SQL Injection: Injects malicious SQL commands via form inputs

Physical Attack Vectors

- USB Drop Attack· Intected USB drives left for users to find and plug in
- Hardware KeyLoggers, Capture keystrokes physically·

Hardware-Based

- Firmware Attacks. Modifying firmware to create persistent threats
- Hardware Backdoors: Hidden, unauthorized access in hardware.
- Keyloggers. Devices recording keystrokes

Network-Based

- Man-in-the-Middie (MITM); intercepts: **communication** between two parties.
- DNS Spoofing: Redirects traffic to malicious websites
- Port Scanning: Identifies open ports and vulnerabilities

Web-Based

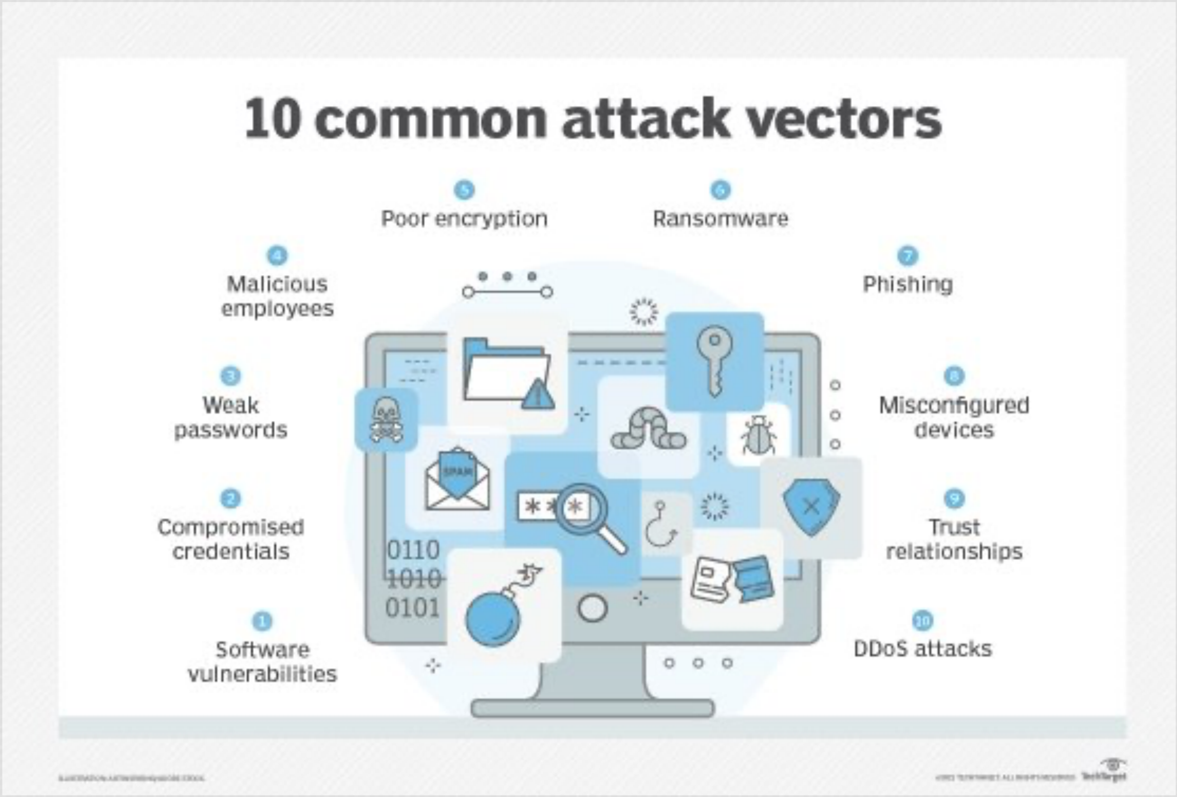
- Cross-Site Scripting (KS) Injects malicious scripts into trusted websites
- Cross-Site Request Forgery-CSREL Tricks users into executing unwanted actions

Supply Chain Attacks

- Compromised Software Updates: Injecting malware into legfumate updates.
- Infected Hardware Delivery: Tamperie with hardware before delivery

Email-Based Vectors

- Phishing Fraudulent emails to steal credentials
- Spear Phishing: Targeted phishing for specific Individuals of organizations
- Malicious Attachmente/ Links: Payloads delivered via email



<u>**Mitigation Strategies:**</u>

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