**Cybersecurity Threats & Attacks Cheatsheet**

**1. Network-Based Attacks**

**A. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS)**

* **Description**: Overloads a target system with traffic, making it unavailable.
* **Common Methods**: SYN Flood, UDP Flood, HTTP Flood, Ping of Death.
* **Detection/Prevention**: Rate limiting, traffic analysis, firewalls, anomaly detection.

**B. Man-in-the-Middle (MitM) Attack**

* **Description**: Attacker intercepts communication between two parties.
* **Common Methods**: ARP Spoofing, DNS Spoofing, Wi-Fi Eavesdropping.
* **Detection/Prevention**: Encryption (TLS/SSL), VPN, secure authentication mechanisms.

**C. DNS Spoofing**

* **Description**: Redirects users to malicious websites by altering DNS responses.
* **Detection/Prevention**: DNSSEC, monitoring DNS traffic, avoiding untrusted DNS servers.

**2. Endpoint Attacks**

**A. Malware (Viruses, Worms, Trojans, Ransomware, Spyware, Rootkits)**

* **Description**: Malicious software that disrupts or steals data.
* **Common Methods**: Drive-by downloads, phishing, infected USBs.
* **Detection/Prevention**: Antivirus, endpoint protection, behavioral analysis.

**B. Ransomware**

* **Description**: Encrypts files and demands ransom for decryption.
* **Common Methods**: Email attachments, exploit kits, remote desktop protocol (RDP) attacks.
* **Detection/Prevention**: Backups, security patches, endpoint security tools.

**C. Keylogging & Credential Theft**

* **Description**: Captures keystrokes to steal login credentials.
* **Common Methods**: Keylogger malware, hardware keyloggers, screen capture tools.
* **Detection/Prevention**: MFA, password managers, endpoint monitoring.

**3. Web & Application Attacks**

**A. SQL Injection (SQLi)**

* **Description**: Injects malicious SQL queries to manipulate databases.
* **Common Methods**: Bypassing authentication, extracting sensitive data.
* **Detection/Prevention**: Input validation, parameterized queries, web application firewalls (WAF).

**B. Cross-Site Scripting (XSS)**

* **Description**: Injects malicious scripts into web pages, executed by users.
* **Common Methods**: Stored XSS, Reflected XSS, DOM-based XSS.
* **Detection/Prevention**: Input sanitization, Content Security Policy (CSP).

**C. Cross-Site Request Forgery (CSRF)**

* **Description**: Forces a user to perform unintended actions on a web application.
* **Common Methods**: Hidden forms, malicious links.
* **Detection/Prevention**: CSRF tokens, SameSite cookies.

**4. Social Engineering Attacks**

**A. Phishing**

* **Description**: Tricking users into revealing sensitive data.
* **Common Methods**: Email phishing, spear phishing, smishing (SMS phishing).
* **Detection/Prevention**: User education, email filtering, MFA.

**B. Pretexting**

* **Description**: Manipulating victims into sharing information by creating a false scenario.
* **Common Methods**: Fake customer support calls, impersonation.
* **Detection/Prevention**: User awareness, verification procedures.

**C. Baiting & Quid Pro Quo**

* **Description**: Offering something enticing (e.g., free software) to trick users into installing malware.
* **Detection/Prevention**: Security awareness training, endpoint protection.

**5. Insider Threats**

**A. Malicious Insider**

* **Description**: Employees or contractors abusing their access.
* **Common Methods**: Data theft, privilege escalation, sabotage.
* **Detection/Prevention**: User activity monitoring, least privilege principle.

**B. Accidental Insider**

* **Description**: Employees unintentionally causing security breaches.
* **Common Methods**: Misconfigurations, accidental data sharing.
* **Detection/Prevention**: Security training, enforcing policies.

**6. Emerging Threats**

**A. AI-Powered Cyber Attacks**

* **Description**: Use of AI to generate phishing emails, deepfake frauds, or automate attacks.
* **Detection/Prevention**: AI-based threat detection, behavioral analysis.

**B. Supply Chain Attacks**

* **Description**: Attacks targeting third-party vendors to compromise businesses.
* **Common Methods**: Software backdoors, hardware tampering.
* **Detection/Prevention**: Vendor security assessments, software integrity checks.

**C. Zero-Day Exploits**

* **Description**: Exploiting undiscovered vulnerabilities before patches are available.
* **Detection/Prevention**: Threat intelligence, virtual patching, behavior-based detection.

**7. Attack Mitigation & Prevention**

| **Threat Type** | **Best Mitigation Strategies** |
| --- | --- |
| Network Attacks | Firewalls, IDS/IPS, TLS encryption |
| Endpoint Attacks | EDR, antivirus, patch management |
| Web Attacks | WAF, secure coding practices |
| Social Engineering | Security awareness training |
| Insider Threats | Least privilege, activity monitoring |
| Emerging Threats | Threat intelligence, AI-driven security |