Cyber Security Fundamentals

Cyber Kill Chain

A framework by Lockheed Martin that describes the stages of a cyber attack:

1. **Reconnaissance**: Gather information about the target.
2. **Weaponization**: Create malware for the attack.
3. **Delivery**: Get the malware into the victim's network.
4. **Exploitation**: Use the malware to take control.
5. **Installation**: Install backdoors and other malicious tools.
6. **Command and Control (C2)**: Communicate with the malware.
7. **Actions on Objectives**: Complete the goal (steal data, disrupt systems, etc.).

MITRE ATT&CK Framework

A knowledge base of real-world hacking tactics and techniques:

1. **Reconnaissance**: Gather victim info.
2. **Resource Development**: Build attack tools.
3. **Initial Access**: Gain entry into the victim's network.
4. **Execution**: Run malicious programs.
5. **Persistence**: Maintain control over the system.
6. **Privilege Escalation**: Gain higher system privileges.
7. **Defense Evasion**: Hide from security tools.
8. **Credential Access**: Steal passwords.
9. **Discovery**: Learn about the victim's network.
10. **Lateral Movement**: Move through the network.
11. **Collection**: Gather valuable data.
12. **Command and Control (C2)**: Maintain control of compromised systems.
13. **Exfiltration**: Steal data.
14. **Impact**: Disrupt, destroy, or manipulate systems.

TTP (Tactics, Techniques, Procedures)

Describes how attackers operate:

- **Tactics**: Their overall strategy.
- **Techniques**: The methods they use.
- **Procedures**: The specific steps taken.

Common Network Threats & Attacks

Threats & Vulnerabilities

- **Threat**: A potential attack or security risk.

- **Vulnerability**: A weakness that can be exploited.
- **CVE (Common Vulnerabilities and Exposures)**: A list of known security flaws.

Types of Attacks

- **Spoofing**: Pretending to be someone else (IP, MAC address, etc.).
- **Phishing**: Tricking users into providing sensitive information.
  - **Spear Phishing**: Targeted phishing attacks.
  - **Vishing**: Voice-based phishing.
- **Man-in-the-Middle (On-Path Attack)**: Intercepting communication between two parties.
- **DoS/DDoS**: Overloading a system to make it unavailable.
- **Fragment Attack**: Manipulating network packets to confuse systems.
- **Over-Sized Packet Attack**: Sending large packets to crash a system.
- **Remote Code Execution**: Running malicious code remotely.
- **SQL Injection**: Exploiting weak database input validation.
- **Privilege Escalation**: Gaining unauthorized higher-level access.
- **Malware Types**:
  - **Virus**: Requires user action to spread.
  - **Worm**: Spreads automatically.
  - **Trojan**: Disguised as legitimate software.
- **Side-Channel Attack**: Gaining info indirectly, like monitoring power use.

References

- **CVEs**: A list of known vulnerabilities.
- **OWASP Top 10**: A list of the most critical web application security risks.