Cyber Security Fundamentals

Cyber Kill Chain

The Cyber Kill Chain is a framework developed by Lockheed Martin to describe the stages of a cyber attack:

1. **Reconnaissance**: Obtain information about the target.
2. **Weaponization**: Create malware to use against the victim.
3. **Delivery**: Infiltrate the victim's network to deliver the malware.
4. **Exploitation**: Once in the victim's network, take steps to achieve goals.
5. **Installation**: Install malware, backdoors, and other cyber weapons.
6. **Command and Control (C2)**: Communicate with the malware once installed.
7. **Actions on Objectives**: Carry out the final objective, such as stealing information or disrupting services.

MITRE ATT&CK Framework

The MITRE ATT&CK framework is a knowledge base of adversary tactics and techniques based on real-world observations:

1. **Reconnaissance**: Gather information about the victim.
2. **Resource Development**: Establish resources to use.
3. **Initial Access**: Gain access to the victim's network.
4. **Execution**: Run malicious code.
5. **Persistence**: Maintain one's foothold.
6. **Privilege Escalation**: Gain higher-level privileges.
7. **Defense Evasion**: Avoid being detected.
8. **Credential Access**: Steal account credentials.
9. **Discovery**: Learn more about the victim's network environment.
10. **Lateral Movement**: Move around in the network.
11. **Collection**: Gather data of interest to achieve one's goal.
12. **Command and Control (C2)**: Communicate from within compromised systems and control them.
13. **Exfiltration**: Steal data.
14. **Impact**: Manipulate, interrupt, or destroy systems and data.

TTP (Tactics, Techniques, Procedures)

TTPs describe how threat actors carry out their attacks:

- **Tactics**: The overall strategy or goal (e.g., gaining access).
- **Techniques**: The methods used to achieve the tactic (e.g., phishing).
- **Procedures**: The specific steps taken to execute the technique.

Common Network Threats and Attacks

What is a Threat?

A threat is something that directly impacts operational activities in a negative way. It can involve:

- **Unauthorized access** (confidentiality).
- **Modification of information** (integrity).
- **Denial of service** (availability).
- **Exploitation of vulnerabilities**.

What is a Vulnerability?

A vulnerability is a weakness in a piece of software or system that can be exploited.

Common Vulnerabilities and Exposures (CVE)

- A list of known vulnerabilities, each given a CVE number.
- Designed to make it easier to share information about vulnerabilities so cybersecurity systems can be updated to protect against them.

Types of Threats and Attacks

Spoofing

- Pretending to be something you're not.
- In the OSI model, attackers can spoof MAC and IP addresses to redirect traffic.

Phishing

- A form of social engineering to trick victims into taking action.
    - **Spear Phishing**: Targets specific high-level individuals.
    - **Vishing**: Malicious voicemail messages.

Man-in-the-Middle (On-Path Attack)

- The attacker positions themselves between the victim and another entity to intercept or alter communications.

DoS/DDoS (Denial of Service/Distributed Denial of Service)

- Overloads or confuses a system, rendering it unavailable.
- **DDoS**: Uses multiple computers to carry out the attack.

Fragment Attack

- Intercepts packets in transit and alters the fragmentation process, confusing the target system.

Over-Sized Packet Attack

- Sends packets that are too large for the system to handle.

Remote Code Execution

- Allows an attacker to remotely execute malware on a target system.

- Can exploit existing software on the target system ("living off the land").

SQL Injection

- Exploits websites that allow malicious user input to interact with a database.

Privilege Escalation

- Exploits vulnerabilities to gain higher privileges than intended.

Virus

- Malicious software that requires user interaction to activate.

Worm

- Malicious code that can replicate itself without user interaction.

Trojan

- Malicious software disguised as legitimate software, often left behind for future access.

Side-Channel Attack

- Gathers information through indirect means, such as execution time or power consumption.

References

- **CVEs**: Common Vulnerabilities and Exposures. (Take course)
- **OWASP Top 10**: A list of the most critical web application security risks. (Take course)