Day 2: Cyber Kill Chain, Reconnaissance, and Ethical Hacking Phases

1. Cyber Kill Chain Methodology

- Reconnaissance: Attacker gathers information about the target.
- Weaponization: Creation of malicious payload using collected data.
- Delivery: Sending the payload (email, USB, website).
- Exploitation: Triggering the payload using a system vulnerability.
- Installation: Installing malware/backdoor on the system.
- Command & Control (C2): Remote communication/control by attacker.
- Actions on Objectives: Final goals like data theft or system takeover.

2. Introduction to Reconnaissance

Reconnaissance is the first step in both the Cyber Kill Chain and Ethical Hacking. It involves gathering intel about the target system.

Two types:

- Passive Reconnaissance: No direct interaction (e.g., WHOIS, Google Dorks).
- Active Reconnaissance: Direct probing/scanning (e.g., Nmap, traceroute).

3. Passive vs Active Reconnaissance

Feature	Passive Reconnaissance	Active Reconnaissance
Definition	No direct interaction	Direct interaction with target
Detection Risk	Low	High
Tools	Google Dorking, Whois, Shodan	Nmap, Netcat, Traceroute
Data Gathered	Public Info (DNS, Email, etc.)	Ports, OS, Services

4. 5 Phases of Ethical Hacking

- Reconnaissance: Gathering info (Google Dorking, WHOIS, Social Engineering)
- Scanning: Network mapping, Port scanning, Vulnerability scanning
- Gaining Access: Exploiting vulnerabilities (SQLi, Phishing)
- Maintaining Access: Rootkits, Hidden users, Tunneling
- Clearing Tracks: Log modification, Evidence deletion