📌 Cyber Kill Chain Overview

- **Origin**: Lockheed Martin, 2011 (military-inspired)
- **Purpose**: Understand and break down cyber attacks in 7 stages
- **Goal**: Detect & interrupt attacks early

1. Reconnaissance

Objective: Gather info on target's vulnerabilities

🔹 **Types**:

- **Passive**: OSINT, WHOIS, DNS queries, Google Dorking, social media
- **Active**: Port scanning, vulnerability scans, physical visits

🔹 **Examples**:

- WHOIS = domain info
- DNS = server IPs
- Social Engineering, Shodan, Nmap

🔹 **Countermeasures**:

- Limit public data exposure
- Use WHOIS privacy services
- Monitor network traffic/logs
- Detect scan patterns

2. Weaponisation

Objective: Create tailored payload to exploit discovered vulnerabilities

🔹 **Tactics**:

- Modify exploits or use kits (e.g. Exploit kits)
- Embed in Word docs (macros), PDFs, USBs
- Encrypt/obfuscate payloads

🔹 **Examples**:

- MS Office macros
- PDF exploits
- Exploit kits like Metasploit

- **Countermeasures**:
  - User awareness & training
  - Disable macros by default
  - Remove unnecessary software/plugins
  - Apply group policy restrictions

3. Delivery

Objective: Transmit payload to target

- **Methods**:
  - Phishing/spear phishing emails
  - Malicious links or file sharing
  - USB/DVD drops
  - Smishing (SMS phishing)
  - Malvertising, social engineering
- **Examples**:
  - “Invoice.pdf.exe”
  - Fake Dropbox links
  - Spoofed manager email
- **Countermeasures**:
  - Cyber awareness training
  - Email/web filters
  - WAFs (Web App Firewalls)
  - Monitor patch status

4. Exploitation

Objective: Trigger vulnerability to gain access

- **Methods**:
  - Software vulnerabilities (e.g., buffer overflow, SQLi)
  - Weak/default passwords
  - Zero-day exploits

🔹 **Examples**:

- Phishing login credentials
- Remote code execution
- Exploiting outdated services

🔹 **Countermeasures**:

- Enforce strong passwords + MFA
- Patch management
- Vulnerability scanning
- Use IPS/WAF for filtering malicious input

5. Installation

Objective: Ensure persistent access

🔹 **Techniques**:

- Malware/backdoor/rootkit install
- Scheduled tasks/cron jobs
- Web shells
- Living-off-the-land binaries (LOLBins)

🔹 **Examples**:

- Remote Access Trojans (RATs)
- Add services (Windows/Linux)
- Hidden payloads in HTTPS

🔹 **Countermeasures**:

- Endpoint Detection & Response (EDR)
- Monitor startup items/new processes
- Application allowlisting
- Regular system auditing

6. Command & Control (C2)

Objective: Establish covert channel to control infected system

🔹 **Tactics**:

- Use HTTP/S, DNS, SMTP for C2
- Domain Generation Algorithms (DGAs)
- Fast Flux IP rotation
- Social media or cloud service-based C2

🔹 **Examples**:

- DNS tunneling
- Encrypted HTTPS C2 traffic
- Dropbox for data staging

🔹 **Countermeasures**:

- Monitor DNS & network traffic
- Inspect HTTPS traffic
- Use firewalls, IDS/IPS
- Deploy honeypots

7. Actions on Objectives

Objective: Execute attacker's goal (data theft, sabotage, etc.)

🔹 **Types**:

- Data exfiltration (e.g., espionage)
- Ransomware
- System disruption/deletion
- Lateral movement (network spread)
- ICS/SCADA manipulation

🔹 **Examples**:

- Financial fraud via wire transfer
- Encrypt data + demand ransom
- Stealthy system control

🔹 **Countermeasures**:

- Data Loss Prevention (DLP)
- Backups + recovery planning
- Network segmentation
- Least privilege access
- Monitor user and endpoint behavior