Unit 2: Advanced Persistent Threats: Applying the Cyber Kill Chain Model to a Case Study

1. Describe the Cyber Kill Chain model.

Advanced Persistent Threats (APTs) are a severe concern for conventional network defence tools due to their sophisticated methods and ample resources. Adopting an intelligence-driven computer network defence (CND) is crucial to overcome this challenge. This approach facilitates an intelligence feedback loop that empowers defenders to establish a state of information superiority and thwart adversary success. Implementing an intelligence-driven CND strategy can help guide network defence investment and resource prioritisation while providing relevant performance and effectiveness metrics (Hutchins et al. 2011).

The "kill chain" is a strategic process to target an adversary and achieve desired outcomes effectively. The United States military outlines this process in six steps, known as F2T2EA: find, fix, track, target, engage, and assess. Any disruption in this integrated process can have significant consequences. Hutchins et al. (2011) propose a fresh kill chain model for intrusions, encompassing reconnaissance, weaponisation, delivery, exploitation, installation, command and control (C2), and actions on objectives.

According to Threat Intelligence (2022), Lockheed Martin's Cyber Kill Chain outlines the seven stages attackers use to exploit network vulnerabilities. These stages include reconnaissance, weaponisation, delivery, exploitation, installation, command and control (C2), and actions on objectives.

1. Reconnaissance is the first stage in the Cyber Kill Chain, involving researching potential targets, identifying vulnerabilities and finding new entry points. It can take place both online and offline.

2. Weaponisation is the Cyber Kill Chain stage where attackers create or modify malware against a target after identifying a survey and vulnerabilities.

3. Delivery is the stage where cyberweapons infiltrate a target's network. This can be done through phishing emails or exploiting hardware or software vulnerabilities in the organisation's network.

4. Exploitation is the third stage of the Cyber Kill Chain. Attackers exploit vulnerabilities to infiltrate and move laterally across a network to reach their targets.

5. Installation is the stage where cybercriminals install malware and other cyberweapons to take control of a network's systems and steal sensitive data. They use Trojan horses, backdoors, or command-line interfaces for this purpose.

6. In the Command-and-Control stage of a cyber-attack, hackers communicate with malware to instruct it to carry out their objectives. They can use this communication to direct infected computers to overload websites with traffic or carry out other cybercrime objectives.

7. Actions on Objectives: cybercriminals accomplish their attack objectives after developing and installing cyberweapons on the target's network. The goals vary, such as a DDoS attack, stealing sensitive data, or using ransomware.

On the other hand, Exabeam (2023) states that the cyber kill chain is a robust cybersecurity model developed by Lockheed Martin's computer security incident response team (CSIRT) to help organisations identify and stop attacks at each stage. Despite the evolving threat landscape, the model has proven effective in detecting the various stages of an attack, including reconnaissance, intrusion, exploitation, privilege escalation, lateral movement, obfuscation, and data exfiltration.

Exabeam's (2023) report has identified 8 phases of a cyber-attack following the Lockheed Martin CIRT CKC model. Each stage is briefly explained below. The MITRE ATT&CK Framework provides a globally accessible knowledge base that lists real-world, observed attacks for each stage. This information is crucial for staying ahead of potential adversaries and ensuring the security of your systems.

1. During **reconnaissance**, attackers gather information about the target organisation and investigate security systems, such as firewalls, intrusion prevention systems, and authentication mechanisms. They may use automated scanners to identify vulnerabilities and weak points.

2. In the **intrusion** stage, attackers try to breach the security perimeter by injecting malware, which could be delivered through social engineering emails, a compromised system or account, an open port or unsecured endpoint, or an insider accomplice. Examples include external remote services, spear phishing attachments, and supply chain compromise.

3. At the **exploitation** stage, attackers look for vulnerabilities or weak points in the organisation's systems. Examples of attacks in this stage include PowerShell, local job scheduling, scripting, and dynamic data exchange.

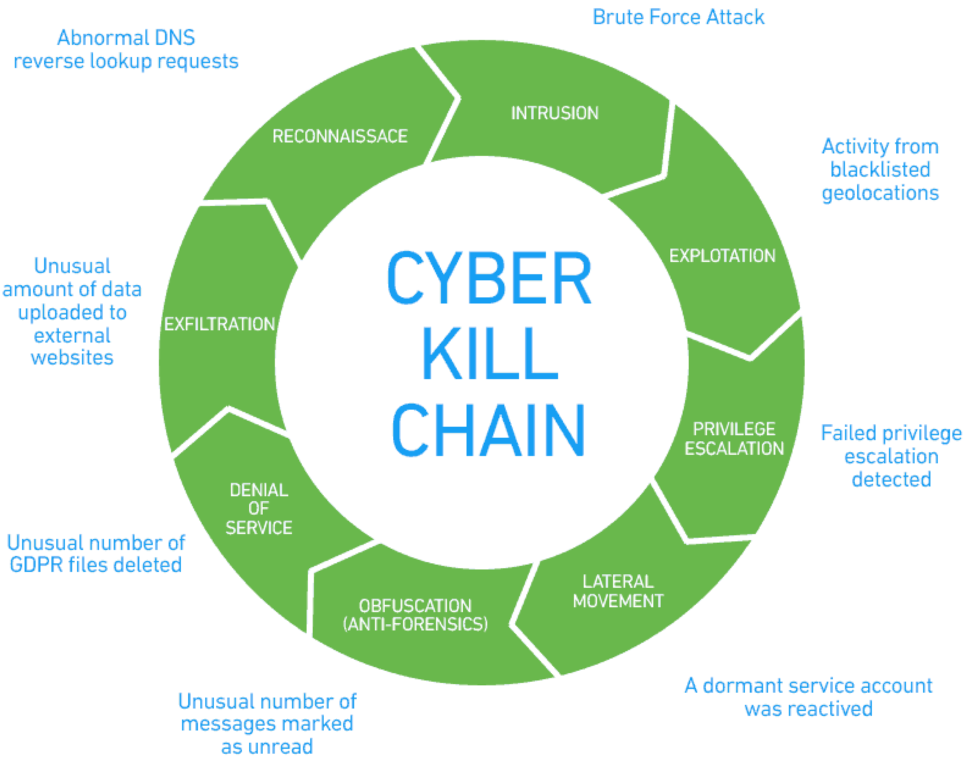
4. In the **privilege escalation** stage, attackers aim to gain higher privileges over other systems or accounts. They may use brute force attacks, search for unsecured credential repositories, monitor unencrypted network traffic, or modify permissions on compromised accounts. Examples include access token manipulation, path interception, Sodo attack, and process injection.

5. **Lateral Movement** is when attackers try to find the organisation's most valuable assets by moving from one system to another. It is a coordinated effort that may involve multiple accounts and systems. Some examples of attacks in this stage are SSH hijacking, Internal spear phishing, Shared Webroot, and Windows remote management.

6. In the **obfuscation** stage, attackers hide their tracks and make it appear that sensitive data or systems were not touched. They may modify logs, falsify timestamps, tamper with security systems, and take other actions. Examples of attacks in this stage include binary padding, code signing, file deletion, hidden users, and process hollowing.

7. **Denial of Service (DoS)** is when attackers aim to disrupt an organisation's operations. Their primary goal is data exfiltration, and they achieve it by distracting security and operational staff. DoS can target various systems, such as networks, production systems, websites, email servers, or customer-facing applications. Examples of attacks in the DoS stage include endpoint denial of service, network denial of service, resource hijacking, service stop, and system shutdown.

8. During the **exfiltration** stage, attackers obtain an organisation’s most sensitive data and find a way to copy it outside the organisation. They can use the data for additional attacks or sell it to others. Examples of attacks in the exfiltration stage include data compression, encryption, alternative protocol exfiltration, and scheduled transfer over a physical medium.


CYBER KILL CHAIN
RECONNAISSACE
INTRUSION
EXPLOTATION
PRIVILEGE ESCALATION
LATERAL MOVEMENT
OBFUSCATION (ANTI-FORENSICS)
DENIAL OF SERVICE
EXFILTRATION
Abnormal DNS reverse lookup requests
Brute Force Attack
Activity from blacklisted geolocations
Failed privilege escalation detected
A dormant service account was reactived
Unusual number of messages marked as unread
Unusual number of GDPR files deleted
Unusual amount of data uploaded to external websites

Cyber kill chain with examples (Exabeam, 2023)

2. Apply the model to analyse a well-known APT.

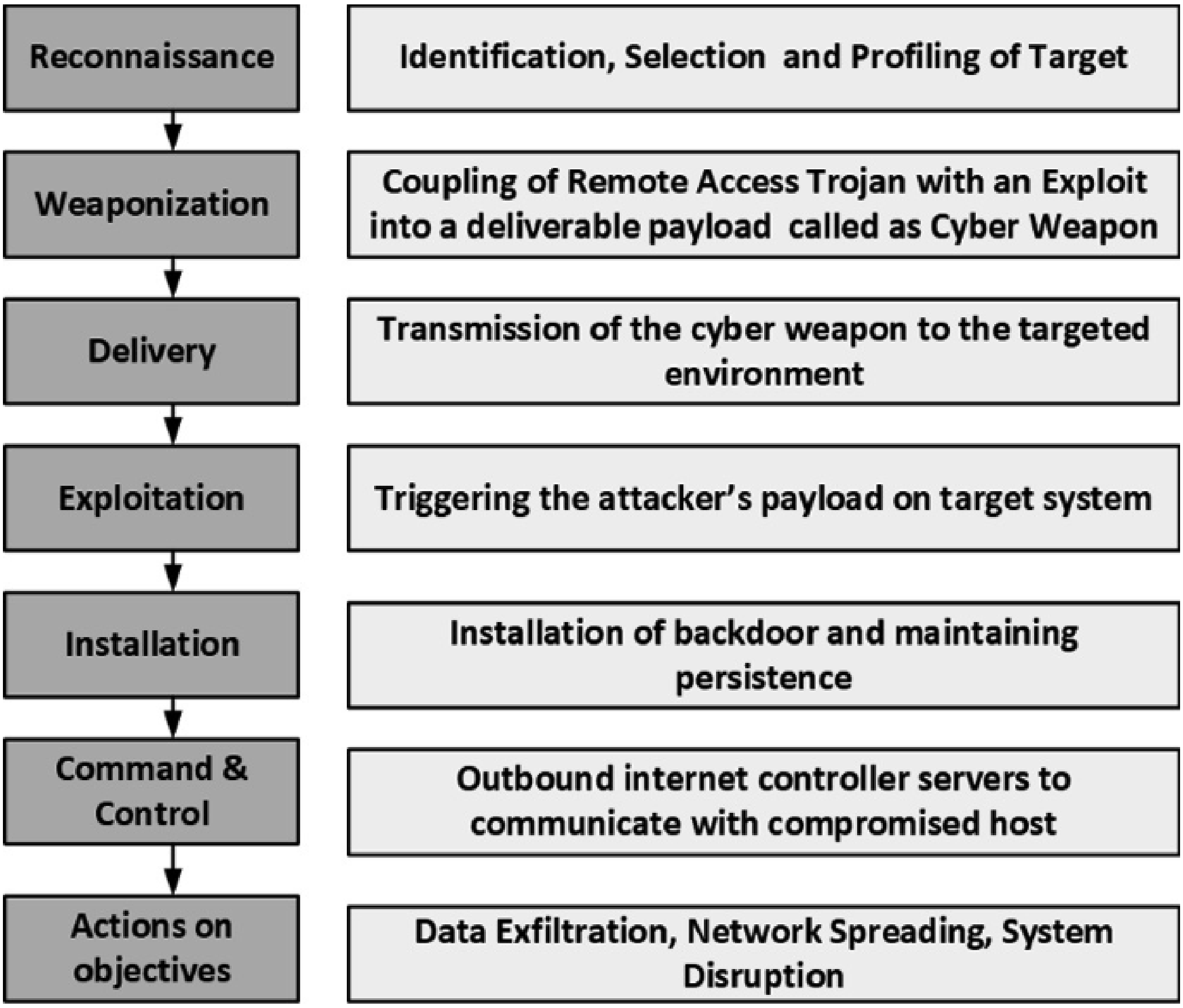
The Stuxnet worm is a well-known APT used to attack Iran's nuclear program. Stuxnet, an infamous computer worm that surfaced in 2010, is widely regarded as the most extensive and costly. It targeted Iran's uranium enrichment facilities, causing severe physical destruction to infected devices and severely crippling Iran's nuclear program. Although no country has officially admitted to creating Stuxnet, it is widely believed that the US and Israel jointly developed it. The worm exploited previously unknown Windows zero-day vulnerabilities and spread rapidly to other systems, including power plants and gas pipes. Its aggressive nature caused accidental spread beyond the limits of Iran's nuclear facilities (Ilevicius, 2022).

Fruhlinger (2022) states that Stuxnet was a mighty worm explicitly created to sabotage Iran's uranium enrichment centrifuges. It could change the programming of Siemens programmable logic controllers (PLC), causing the centrifuges to spin irregularly and become damaged or destroyed. This was done while the PLCs reported that everything was functioning correctly, making it challenging to detect any problems. Stuxnet was a highly effective and dangerous tool to achieve its specific goal.

Using the Cyber Kill Chain model, the Stuxnet worm can be analysed as follows based on the article of Fruhlinger (2022):

First, the attackers spent several years gathering information about Iran's nuclear program through reconnaissance. Next, they developed a worm designed to infect Siemens industrial control systems, known as weaponisation. Then, the worm was delivered to Iran's nuclear program via infected USB drives called delivery. Once the worm was installed on the critical systems, it spread throughout the atomic program and infected centrifuges and other vital components, known as installation. The attackers then established a command-and-control network to control the infected systems remotely, referred to as command and control. Finally, by causing centrifuges to malfunction, the attackers successfully disrupted Iran's nuclear program. The Stuxnet worm is a complex, sophisticated attack demonstrating advanced persistent threats (APT) capabilities.

Advanced persistent threats (APTs) require more than standard security mechanisms, such as firewalls and intrusion detection systems. To protect against APTs, a layered defence that includes timely detection, prevention, mitigation, and emergency planning is necessary. One way to assess the efficacy of countermeasures is by modelling and simulating attack behaviour (Kumar et al. 2021).


Reconnaissance
Identification, Selection and Profiling of Target
Weaponization
Coupling of Remote Access Trojan with an Exploit into a deliverable payload called as Cyber Weapon
Delivery
Transmission of the cyber weapon to the targeted environment
Exploitation
Triggering the attacker's payload on target system
Installation
Installation of backdoor and maintaining persistence
Command & Control
Outbound internet controller servers to communicate with compromised host
Actions on objectives
Data Exfiltration, Network Spreading, System Disruption

Cyber-kill chain model, Kumar et al. (2021).

3. Describe possible mitigations to avoid a similar exploit.

Scadahacker (2014) highlights that organisations can implement several mitigations to prevent similar exploits. These include network segmentation to limit the spread of infection, strict access controls to prevent unauthorised system access, regular vulnerability scans and prompt patching, employee training on recognising and avoiding social engineering techniques and implementing a data backup and recovery plan.

Possible mitigations to prevent a similar exploit can be implemented by applying security controls at each stage of the cyber kill chain. To stop an attack at each stage, Delzer (2019) recommends five methods that can be used:

1. **Detect** - Identify attempts to scan or penetrate the organisation.
2. **Deny** - Prevent attacks as they happen.
3. **Disrupt** - Intercept and interrupt data communications carried out by the attacker.
4. **Degrade** - Create measures that limit the effectiveness of an attack.
5. **Deceive** - Mislead attackers by providing false information or setting up decoy assets.

Here's how various security tools can be used to apply each of the security controls to each stage of the kill chain:

Reconnaissance:

- Detect: Web Analytics, Threat Intelligence, Network Intrusion Detection System
- Deny: Information Sharing Policy, Firewall Access Control Lists

Weaponisation:

- Detect: Threat Intelligence, Network Intrusion Detection System
- Deny: Network Intrusion Prevention System

Delivery:

- Detect: Endpoint Malware Protection
- Deny: Change Management, Application Allowlisting, Proxy Filter, Host-Based Intrusion Prevention System
- Disrupt: Inline Anti-Virus
- Degrade: Queuing
- Contains router Access Control Lists, App-aware Firewall, Trust Zones, Inter-zone Network Intrusion Detection System

Exploitation:

- Detect: Endpoint Malware Protection, Host-Based Intrusion Detection System
- Deny: Secure Password, Patch Management
- Disrupt: Data Execution Prevention
- Contain: App-aware Firewall, Trust Zones, Inter-zone Network Intrusion Detection System

Installation:

- Detect: Security Information and Event Management (SIEM), Host-Based Intrusion Detection System
- Deny: Privilege Separation, Strong Passwords, Two-factor Authentication
- Disrupt: Router Access Control Lists

- Contain: App-aware Firewall, Trust Zones, Inter-zone Network Intrusion Detection System

Command & Control:

- Detect: Network Intrusion Detection System, Host-Based Intrusion Detection System
- Deny: Firewall Access Control Lists, Network Segmentation
- Disrupt: Host-Based Intrusion Prevention System
- Degrade: Tarpit
- Deceive: Domain Name System Redirect
- Contain: Trust Zones, Domain Name System Sinkholes

Actions on Objectives:

- Detect: Endpoint Malware Protection
- Deny: Data-at-rest Encryption
- Disrupt: Endpoint Malware Protection
- Degrade: Quality of Service
- Deceive: Honeypot
- Contain: Incident Response

Exfiltration:

- Detect: Data Loss Prevention (DLP), SIEM
- Deny: Egress Filtering
- Disrupt: DLP
- Contain Firewall Access Control Lists

This approach is more recent, tailored to current circumstances, and aligned with the latest threats in Information Technology. It considers the latest advancements in the industry and is designed to address the most pressing cybersecurity and data privacy concerns. By staying up-to-date with the latest trends and threats, IT professionals can provide a more effective and reliable solution to the challenges organisations face in today's digital landscape.

References:

- Hutchins, E., Cloppert, M. & Amin, R. (2011). *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. [online] Available at: http://gauss.ececs.uc.edu/Project4/Documents/kill-chain.pdf.
- Threat Intelligence (2022). *The Cyber Kill Chain: The Seven Steps of a Cyberattack*. [online] Cybersecurity Exchange. Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/.
- Exabeam (2023). *Cyber Kill Chain: Understanding and Mitigating Advanced Threats*. [online] Exabeam. Available at: https://www.exabeam.com/explainers/information-security/cyber-kill-chain-understanding-and-mitigating-advanced-threats/.
- Ilevičius, P. (2022). *Stuxnet explained — the worm that went nuclear | NordVPN*. [online] nordvpn.com. Available at: https://nordvpn.com/blog/stuxnet-virus/.
- Fruhlinger, J. (2022). *Stuxnet explained: The first known cyberweapon*. [online] CSO Online. Available at: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html.
- Kumar, R., Singh, S. & Kela, R. (2021). A Quantitative Security Risk Analysis Framework for Modelling and Analyzing Advanced Persistent Threats. *Foundations and Practice of Security*, pp.29–46. doi:https://doi.org/10.1007/978-3-030-70881-8_3.
- Scadahacker (2014). *Mitigation Strategies for Stuxnet - SCADAhacker*. [online] Available at: https://scadahacker.com/resources/stuxnet-mitigation.html.
- Delzer, C. (2019). *How the Cyber Kill Chain Can Help You Protect Against Attacks | SBS CyberSecurity*. [online] Available at: https://sbscyber.com/resources/how-the-cyber-kill-chain-can-help-you-protect-against-attacks.