SVKM’S NMIMS (Deemed-to-be University)
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT AND ENGINEERING
MUMBAI CAMPUS

LAB Manual
PART A
(PART A: TO BE REFFERED BY STUDENTS)

Experiment No.01

A.1 Aim:
To Study of Cyber Kill Chain Framework for any Critical Infrastructure Cyber Attack

A.2 Prerequisite:
Fundamentals of cyber-attack, types of attack, Cyber Kill Chain Framework, Critical Infrastructure.

A.3 Outcome:
After successful completion of this experiment students will be able to

1. Study the different types of attack focused on Critical Infrastructure
2. Study and able to investigate the attack tactics.

A.4 Theory:
The **Cyber Kill Chain** offers a comprehensive framework as a part of the **Intelligence Driven Defense model**.

What is the Cyber Kill Chain?

The term “**kill chain**” was first used as a military concept that defines the structure of an attack that covers:

- The identification of the target
- The force dispatch towards the target
- The decision and order to attack the target
- The destruction of the target

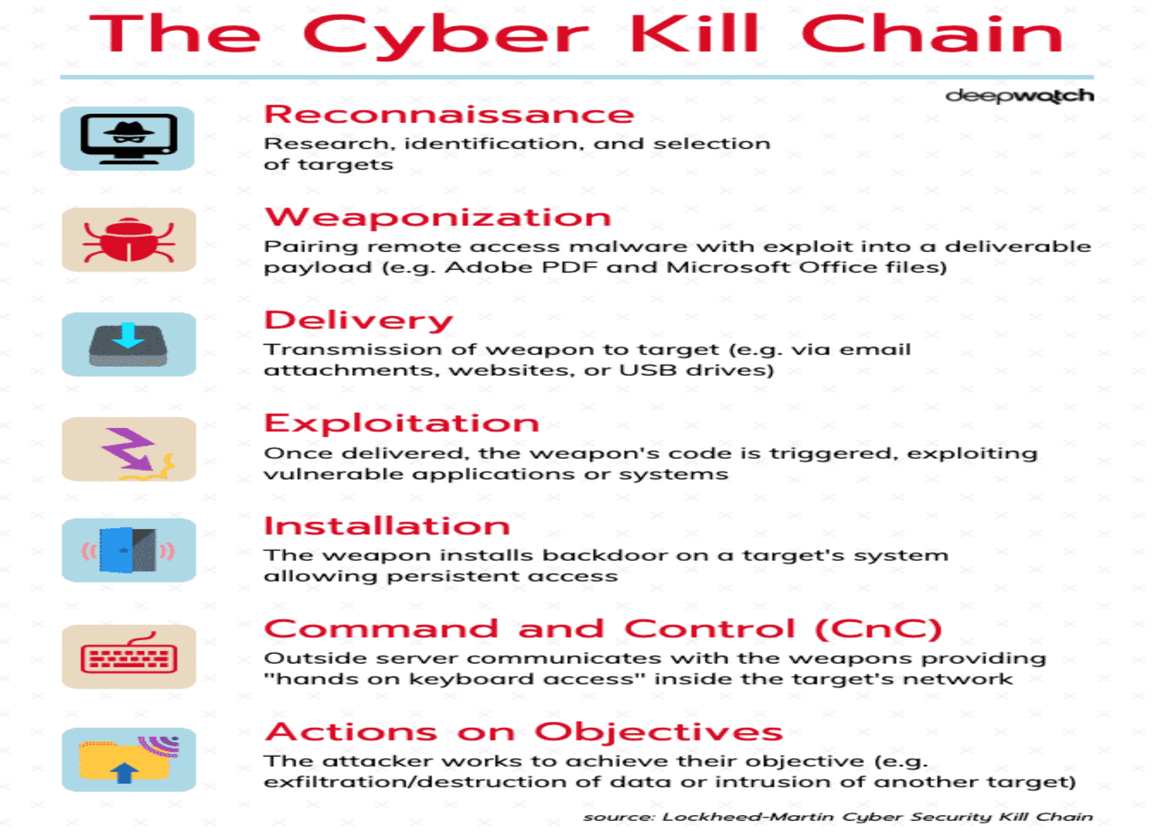
The idea of interrupting the opponent’s kill chain activity is often employed as a defence. Inspired by the whole kill chain concept, Lockheed Martin (an aerospace, security, arms, defence and advanced technologies company based in the United States of America) created the Cyber Kill Chain. It is a **cybersecurity framework** that offers a method to deal with the intrusions on a computer network.

Since it first emerged, the Cyber Kill Chain has evolved significantly in order to anticipate and recognize **insider threats** much better, detect various other attack techniques like advanced ransomware and **social engineering.**

The Cyber Kill Chain consists of seven steps that aim to offer a better attack visibility while supporting the cyberattack / cybersecurity analyst to get a better understanding of the adversary's tactics, procedures and techniques. The **seven steps of the Cyber Kill Chain** illustrates the different phases of a **cyberattack** starting from reconnaissance, reaching to the exfiltration.

What are the 7 steps of the Cyber Kill Chain?

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.



The Cyber Kill Chain

deepwatch

Reconnaissance
Research, identification, and selection of targets

Weaponization
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

Installation
The weapon installs backdoor on a target's system allowing persistent access

Command and Control (CnC)
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network

Actions on Objectives
The attacker works to achieve their objective (e.g. exfiltration/destruction of data or intrusion of another target)

source: Lockheed-Martin Cyber Security Kill Chain

Figure 1. Cyber Kill Chain Framework

1. Reconnaissance: In this step, the attacker / intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exp+-9loited.

2. Weaponization: In this step, the intruder creates a **malware weapon** like a virus, worm, or such in order to exploit the vulnerabilities of the target. Depending on the target and the purpose of the attacker, this malware can exploit new, **undetected vulnerabilities** (also known as the **zero-day exploits**) or it can focus on a combination of different vulnerabilities.

3. Delivery: This step involves transmitting the weapon to the target. The intruder / attacker can employ different methods like USB drives, e-mail attachments and websites for this purpose.

4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.

5. Installation: In this step, the malware installs an access point for the intruder / attacker. This access point is also known as the backdoor.

6. Command and Control: The malware gives the intruder / attacker access in the network/system.

7. Actions on Objective: Once the attacker / intruder gains persistent access, they finally take action to fulfill their purpose, such as **encryption** for ransom, **data exfiltration** or even **data destruction**.

PART B

(PART B: TO BE COMPLETED BY STUDENTS)

(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

Roll. No. A016	Name: Varun Mahendra Khadayate
Class Btech CsBs Third Year	Batch: 1
Date of Experiment:10-12-2021	Date of Submission: 24-12-2021
Grade:	

Team members

1. Varun Khadayate A016
2. Simran Kumari A018
3. Kartik Padave A022

B.1Aim

To Study of Cyber Kill Chain Framework for any 2011: The Paris G20 Summit Cyber Attack

B.2 History of an Attack

Cyber-attacks in France generally include attacks on websites by DDoS attacks as well as malware. Attacks have so far been to the civil and private sectors instead of the military. Like the UK, Germany, and many other European nations, France has been proactive in cyber defense and cyber security in recent years. The White Paper on Defense and National Security proclaimed cyberattacks as "one of the main threats to the national territory" and "made prevention and reaction to cyberattacks a major priority in the organization of national security". This led to the creation of the French Agency for National Security of Information Systems (ANSSI) in 2009.

The cyberattack during the Paris G20 Summit refers to an event that took place shortly before the beginning of the G20 Summit held in Paris, France in February 2011. This summit was a Group of 20 conferences held at the level of governance of the finance ministers and central bank governors (as opposed to the 6th G20 summit later that year, held in Cannes and involving the heads of government). Unlike other well-known cyberattacks, such as the 2009 attacks affecting the South Korean/American government, news media, and financial websites, or the 2007 cyberattacks on Estonia, the attack that took place during the Paris G20 Summit was not a DDoS style attack. Instead, these attacks involved the proliferation of an email with a malware attachment, which permitted access to the infected computer.

B.3 Affected Areas/Impact

The Areas Affected were the Finance Ministry Computers on approximately 150 of 170000 computers. And took the control from there.

B.4 Observations and learning: Comparing with Cyber Kill Chain Framework

(Students are expected to comment on the output obtained with clear observations and learning for each task/ sub part assigned)

1. Reconnaissance:

The attack that took place during the Paris G20 Summit was not a DDoS-style attack. Instead, these attacks involved the proliferation of an email with a malware attachment, which permitted access to the infected computer.

2. Weaponization:

The email's attachment was a 'Trojan Horse' type consisting of a pdf document with embedded malware. Once accessed, the virus infected the computers of some of the government's senior officials as well as forwarded the offensive email to others.

3. Delivery:

- The internet viruses were introduced via emails to ministry employees. "Trojan Horse" software, or a seemingly benign program that steals information or harms a system, was used to gain access to computers remotely.
- The targeted employees knew the attackers and the virus was introduced in attachments that personally interested those employees.

4. Exploitation:

The attack infected approximately 150 of the finance ministry's 170,000 computers. While access to the computers at the highest levels of office of infiltrated departments was successfully blocked, most of the owners of infiltrated computers worked on the G20.

5. Installation:

No Need to install it as an attachment via which the attack took place

6. Command and Control:

Once inside the finance ministry's system, the cyber attackers took control of 150 workstations, out of the 170,000 used in the ministry.

7. Actions on Objective:

The intrusion only targeted the exfiltration of G20 documents. Tax and financial information and other sensitive information for individuals, which is also located in the Ministry of Finance's servers, was left alone as it circulates only on an intranet accessible only within the ministry.

B.5 Conclusion

(Students must write the conclusion as per the attainment of individual outcome listed above and learning/observation noted in section B.4)

Hence, we were able to conclude the 2011: The Paris G20 Summit Cyber Attack based on **Cyberkill Chain Framework**. We also came to know the various vulnerabilities they have passed to reach to their destined position to make their Agenda fulfilled.

B.6 Reference

1. **https://en.wikipedia.org/wiki/Cyberattack_during_the_Paris_G20_Summit**
2. **https://www.bbc.com/news/business-12662596**
3. **https://www.france24.com/en/20110307-cyber-attack-french-finance-ministry-g20-presidency-target-baroin**
4. **https://www.reuters.com/article/us-g20-france-espionage-idUSTRE72619F20110307**

B.7 Questions:

1. Give presentation of your study experiment. Time limit is 10 minutes