Similar to the Cyber Kill Chain this is a framework used to help understand how cyber attacks occur

**What is a Kill Chain**
A term used to explain various stages of an attack. The methodology attackers use to approach and exploit a target

**What is Threat Modelling**
This is a series of steps to improve the security of a system

- Identify - What systems/applications need to be secured
- Assess - Looking at the vulnerabilities and weaknesses
- Plan - A plan to secure the systems and applications
- Policies - Putting policies in place to prevent these vulnerabilities

**Introducing the Unified Kill Chain**
There are 18 phases to an attack. Everything from reconnaissance to data exfiltration and understanding an attacker's motive

- Recon
- Weaponisation
- Delivery
- Social Engineering
- Exploitation
- Persistence
- Defense Evasion
- Command and Control
- Pivoting
- Discovery
- Privilege Escalation

- Execution
- Credential Access
- Lateral Movement
- Collection
- Exfiltration
- Impact
- Objectives

**In what year was the Unified Kill Chain framework released?**
2017

**According to the Unified Kill Chain, how many phases are there to an attack?**
18

**What is the name of the attack phase where an attacker employs techniques to evade detection?**
Defense Evasion

**What is the name of the attack phase where an attacker employs techniques to remove data from a network?**
Exfiltration

**What is the name of the attack phase where an attacker achieves their objectives?**
Objectives

**Phase: In (Initial Foothold)**

Recon:
This is to gain information on the target, which the following will include:

- Discover what systems and services are running
- Contact lists

- Credentials
- Network Topology

Weaponisation:
Creating a tool to exploit the target

Social Engineering:
A way for an attacker to manipulate the employee to perform certain actions in their favor. Which some may include:

- Opening a file that is malicious
- Creating a fake webpage and then a user entering their credentials
- Impersonation of a user

Exploitation:
This is where the attacker will exploit the vulnerability to gain access to the system. Here are some ways the attacker may gain access to the system:

- Reverse shell on a web application
- Interfering with an automated script on the system to execute code
- Abusing a web application vulnerability to execute code

Persistence:
The attacker will want to make sure they stay on the targets machine. They will do this by doing:

- Creating a service to allow for the attacker to regain access
- Adding to a command and control server to execute certain commands
- Backdoors, which is a type of exploit that allows for the attacker to gain unauthorized access easily

Defense Evasion:
This is how the attacker will be able to evade detection services, the following they may evade is:

- Web application firewalls (WAFs)
- Network Firewalls
- Antivirus
- Intrusion Detection System (IDS)

Command and Control:
Command and Control is to establish the connections with the attacker and target machine. With command and control the attacker will:

- Execute commands
- Steal sensitive data
- Pivot to other systems on the network

Pivoting:
Pivoting is where an attacker will have access to the server and then be able to hop onto a new one located on the network that might not be accessible

**What is an example of a tactic to gain a foothold using emails?**
Phishing

**Impersonating an employee to request a password reset is a form of what?**
Social Engineering

**An adversary setting up the Command & Control server infrastructure is what phase of the Unified Kill Chain?**
Weaponisation

**Exploiting a vulnerability present on a system is what phase of the Unified Kill Chain?**
Exploitation

**Moving from one system to another is an example of?**
Pivoting

**Leaving behind a malicious service that allows the adversary to log back into the target is what?**
Persistence

**Phase: Through (Network Propagation)**
Once an attacker is in the system they will try to gain additional access by trying to escalate their privileges

Discovery:
This is where the attacker will try to gain more information on the network, such as accounts, permissions granted, applications and much more

Privilege Escalation:
This is where the attacker will try to find ways to become an admin/root on the network

Execution:
This stage is where the adversary will execute commands and installations with installing malware, backdoors and other payloads

Credential Access:
The attacker on this phase will steal the credentials of the accounts they have located. They could obtain this information with keylogging or credential dumping

Lateral Movement:
Lateral movement is the phase of moving around the network and

jumping onto different target server to achieve their objective

**As a SOC analyst, you pick up numerous alerts pointing to failed login attempts from an administrator account. What stage of the kill chain would an attacker be seeking to achieve?**
Privilege Escalation

**Mimikatz, a known attack tool, was detected running on the IT Manager's computer. What is the mission of the tool?**
Credential Dumping

**Phase: Out (Action on Objectives)**
This phase is where the attacker has achieved all their objective and will cover their tracks to make it seem no one had accessed the system

Collection:
The attacker will have collected all the information they had found on the system

Exfiltration:
Exfiltration is the phase where the attacker will extract the data they have found by using encryption measures to avoid detection

Impact:
The impact that the adversary would have achieved is disrupting the business. They could do the following to harm the business:

- Remove accounts
- Wipe data
- Infect with ransomware
- Deface the website
- DoS

Objectives:
This is the last phase of the unified kill chain where the adversary has achieved everything and gathered all the information

**While monitoring the network as a SOC analyst, you realise that there is a spike in the network activity, and all the traffic is outbound to an unknown IP address. What stage could describe this activity?**
Exfiltration

**Personally identifiable information (PII) has been released to the public by an adversary, and your organization is facing scrutiny for the breach. What part of the CIA triad would be affected by this action?**
Confidentiality

**Practical**

**The Attacker uses tools to gather information about a system**
Reconnaissance

**The Attacker installs a malicious script to allow them remote access at a later date**
Persistence

**The hacked machine is being controlled from an Attacker's own server**
Command and Control

**The Attacker uses the hacked machine to access other servers on the same network**
Pivoting

**The Attacker steals a database and sells this to a 3rd party**
Actions and Objectives

**Match the scenario prompt to the correct phase of the Unified Kill Chain to reveal the flag at the end. What is the flag?**

THM{UKC_SCENARIO}