**Red Team Fundamentals**

Task 1: Introduction:

No Answer Required.

Task 2: Vulnerability Assessment and Penetration Tests Limitations

***Answer the questions below***

*1# Would vulnerability assessments prepare us to****detect****a real attacker on our networks? (Yay/Nay)*

*Correct Answer: Nay*

*2# During a penetration test, are you concerned about being detected by the client? (Yay/Nay)*

*Correct Answer: Nay*

*3# Highly organized groups of skilled attackers are nowadays referred to as ...*

*Correct Answer: Advanced persistent threats*

Task 3: Red Team Engagements

***Answer the questions below***

*1# The goals of a red team engagement will often be referred to as flags or...*

*Correct Answer: crown jewels*

*2# During a red team engagement, common methods used by attackers are emulated against the target. Such methods are usually called TTPs. What does TTP stand for?*

*Correct Answer: Tactics, Techniques and Procedures*

*3#The main objective of a red team engagement is to detect as many vulnerabilities in as many hosts as possible (Yay/Nay)*

*Correct Answer: Nay*

Task 4: Teams and Functions of an Engagement

***Answer the questions below***

*1#What cell is responsible for the offensive operations of an engagement?*

*Correct Answer: Red Cell*

*2#What cell is the trusted agent considered part of?*

*Correct Answer: White cell*

Task 5: Engagement Structure

Components of the kill chain are broken down in the table below.

| **Technique** | **Purpose** | **Examples** |
| --- | --- | --- |
| Reconnaissance | Obtain information on the target | Harvesting emails, OSINT |
| Weaponization | Combine the objective with an exploit. Commonly results in a deliverable payload. | Exploit with backdoor, malicious office document |
| Delivery | How will the weaponized function be delivered to the target | Email, web, USB |
| Exploitation | Exploit the target's system to execute code | MS17-010, Zero-Logon, etc. |
| Installation | Install malware or other tooling | Mimikatz, Rubeus, etc. |
| Command & Control | Control the compromised asset from a remote central controller | Empire, Cobalt Strike, etc. |
| Actions on Objectives | Any end objectives: ransomware, data exfiltration, etc. | Conti, LockBit2.0, etc. |

***Answer the questions below***

*1#If an adversary deployed Mimikatz on a target machine, where would they be placed in the Lockheed Martin cyber kill chain?*

*Correct Answer: Installation*

*2#What technique's purpose is to exploit the target's system to execute code?*

*Correct Answer: Exploitation*

Task 6: Overview of a Red Team Engagement

***Answer the questions below***

*1#Click the "View Site" button and follow the example engagement to get the flag*

*Correct Answer: THM{RED\_TEAM\_ROCKS}*

Task 7: Conclusion

***Answer the questions below***

*1#Read the above and continue learning!*

*Answer: No Answer Needed*