**Intro to Offensive Security**

**Task-1: What is Offensive Security?**

In short, offensive security is the process of breaking into computer systems, exploiting software bugs, and finding loopholes in applications to gain unauthorized access to them.

To beat a hacker, you need to behave like a hacker, finding vulnerabilities and recommending patches before a cybercriminal does, as you'll do in this room!

On the flip side, there is also defensive security, which is the process of protecting an organization's network and computer systems by analyzing and securing any potential digital threats; learn more in the digital forensics room.

In a defensive cyber role, you could be investigating infected computers or devices to understand how it was hacked, tracking down cybercriminals, or monitoring infrastructure for malicious activity.

***Answer the questions below***

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

* Offensive Security
* Defensive Security

Ans: Offensive Security

**Task-2: Hacking Your first machine**

\* FakeBank

\* Command Line Application- GoBuster (for Brute-Force FakeBank)-(find hidden directories & pages)

\* gobuster -u http://fakebank.com -w wordlist.txt dir

Hidden pages find command.

Here,

-u = scanning, -w = list of word,

\* Go following path which (Status:200)

Sender: 2276

Receiver: 8881

Amount: $2000

**Task-3: Careers in Cyber Security**

What careers are there?

The cyber careers room goes into more depth about the different careers in cyber. However, here is a short description of a few offensive security roles:

* Penetration Tester - Responsible for testing technology products for finding exploitable security vulnerabilities.
* Red Teamer - Plays the role of an adversary, attacking an organization and providing feedback from an enemy's perspective.
* Security Engineer - Design, monitor, and maintain security controls, networks, and systems to help prevent cyberattacks.

[Information Technology (IT) Certifications & Training | CompTIA](https://www.comptia.org/)

**Red Team Fundamentals**

**Task-1: Introduction:**

Room objectives

* Learn about the basics of red team engagements
* Identify the main components and stakeholders involved in a red team engagement
* Understand the main differences between red teaming and other types of cybersecurity engagements

Room prerequisites

Before beginning this room, familiarity with general hacking techniques is required. Although not strictly necessary, completing the Jr. Penetration Tester Learning Path is recommended.

**Task-2: Vulnerability Assessment and Penetration Tests Limitations:**

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

Ans: Nay

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

Ans: Nay

1. Highly organised groups of skilled attackers are nowadays referred to as ...

Ans: Advanced Persistent Threats

Important Link:

[Malwarebytes Labs - The Security Blog From Malwarebytes | Malwarebytes Labs](https://www.malwarebytes.com/blog)

[CPR - Check Point Research](https://research.checkpoint.com/)

[EternalBlue - Everything There Is To Know - Check Point Research](https://research.checkpoint.com/2017/eternalblue-everything-know/)

[Explain Like I’m 5: Remote Desktop Protocol (RDP) (cyberark.com)](https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp)

[The Hacker News | #1 Trusted Cybersecurity News Site](https://thehackernews.com/)

[FBI Takes Down BlackCat Ransomware, Releases Free Decryption Tool (thehackernews.com)](https://thehackernews.com/2023/12/fbi-takes-down-blackcat-ransomware.html?_m=3n.009a.3231.wt0ao45397.283z&m=1&fbclid=IwAR3hN4vuQK-p_fE9mpO0Qb6zsTjMgO4iULUPee_efPdoCeqV4FzpUGI17gE)

[Download Hashtab & Alternatives 2023 (implbits.com)](https://implbits.com/hashtab)

[Steganography: How to Hide Secret Data Inside an Image or Audio File in Seconds « Null Byte :: WonderHowTo](https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/)

[Steghide (sourceforge.net)](https://steghide.sourceforge.net/)

[Steganography - A list of useful tools and resources - 0xRick’s Blog](https://0xrick.github.io/lists/stego/)

[ROE Template | Red Team Development and Operations](https://redteam.guide/docs/templates/roe_template/)

[CVE - CVE-2020-14351 (mitre.org)](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14351)

[Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers (exploit-db.com)](https://www.exploit-db.com/)

[Sudo 1.8.25p - 'pwfeedback' Buffer Overflow (PoC) - Linux dos Exploit (exploit-db.com)](https://www.exploit-db.com/exploits/47995)

[CMNatic (Ben)](http://googledorking.cmnatic.co.uk/)

[PageSpeed Insights (web.dev)](https://pagespeed.web.dev/)

[Regex Cheat Sheet (rexegg.com)](https://www.rexegg.com/regex-quickstart.html)

[Linux man pages (die.net)](https://linux.die.net/man/)

[KnightCTF 2024](https://2024.knightctf.com/)

[KnightCTF 2024](https://2024.knightctf.com/?fbclid=IwAR1JzGcsfIEBVUsl6WB8Zj7M1qtHcPv8xZOiWYnX7lgUvTXN49NSMjOPh28&__cf_chl_tk=ZNzNpLQz3DGNQos_0rINMHhJk7TSen751UPHkc64H2w-1703593238-0-gaNycGzNH7s)

[Explain Like I’m 5: Remote Desktop Protocol (RDP) (cyberark.com)](https://www.cyberark.com/resources/threat-research-blog/explain-like-i-m-5-remote-desktop-protocol-rdp)

Important Note:

1. Stuxnet
2. WannaCry
3. DarkHotel
4. Keylogger
5. Fingerprints
6. Samba
7. Rammana
8. StegHide
9. CMS (Wordpress, FuelCMS, Ghost)
10. ExploitDB, NVD, CVE Mitre
11. CLI
12. Searchsploit
13. Cross-Site-Scripting (XSS)
14. WPForms
15. CONOPS
16. Tomcat
17. Crawler
18. MSN
19. Googlebot, MSNbot