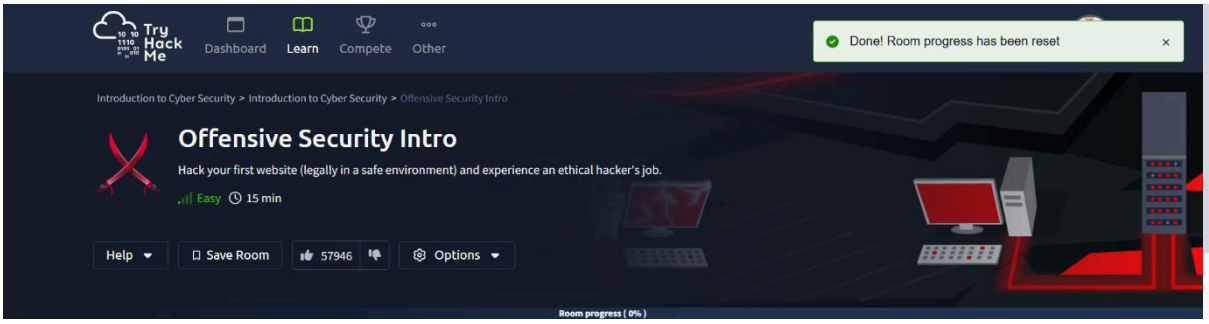
TRYHACKME - Introduction to Cybersecurity Walkthrough

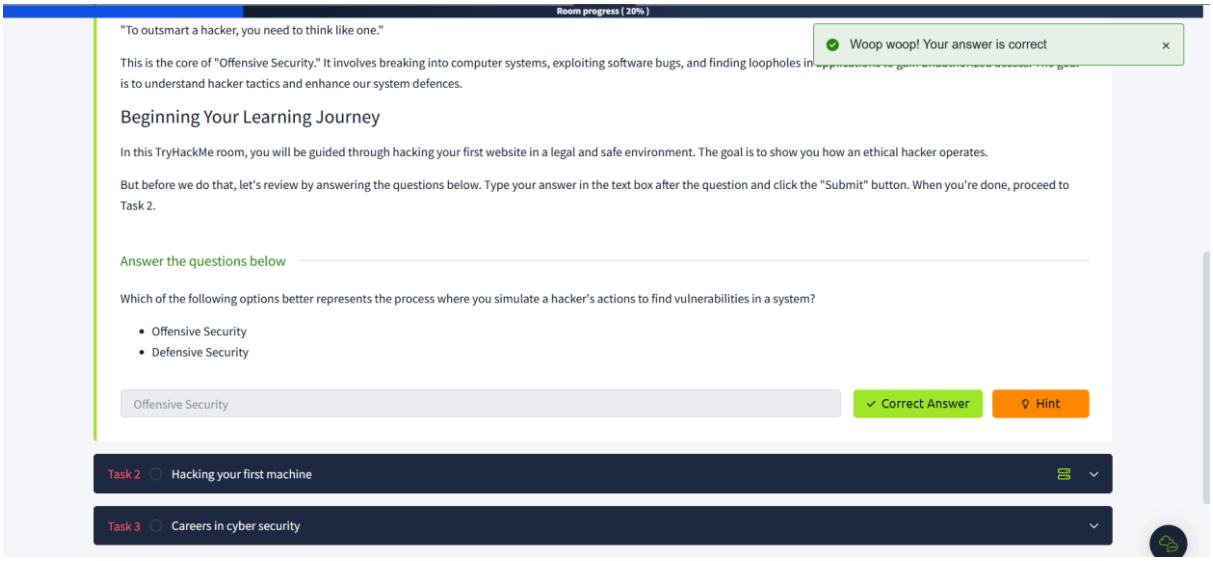
By h4kim

Offensive Security Intro



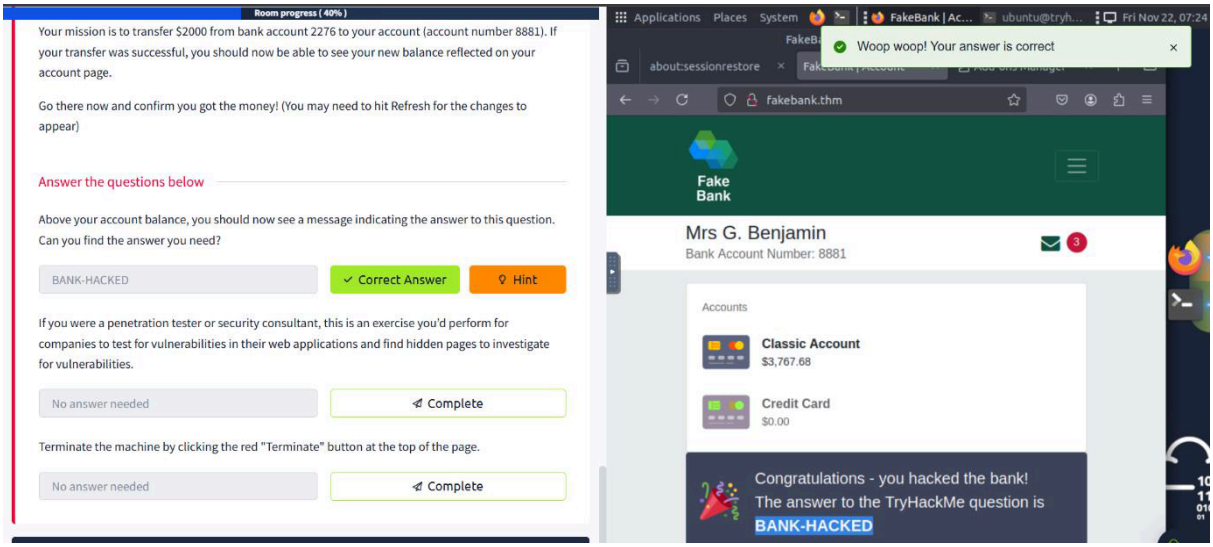
Task 1: What is Offensive Security?

- **Explanation**: Offensive security involves actively testing and exploiting systems to uncover vulnerabilities before malicious hackers can exploit them. It focuses on proactively identifying weaknesses and mitigating them to prevent future attacks.



Task 2: Hacking your first machine

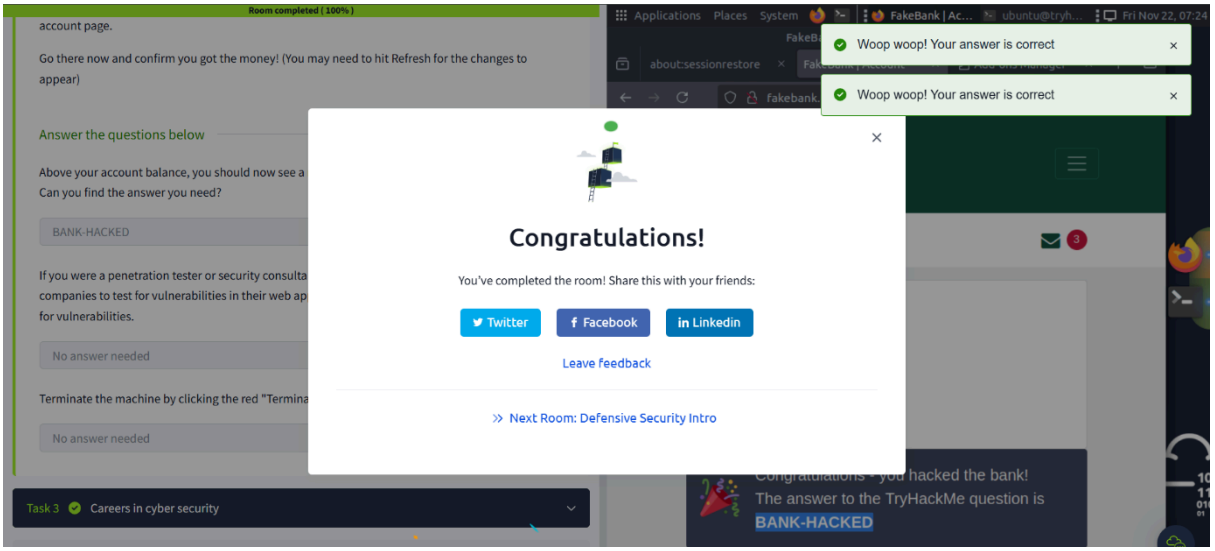
• **Explanation**: This task introduces you to the practical aspect of hacking by legally exploiting vulnerabilities in a virtual machine. The objective is to understand how attackers work and learn the ethical hacking skills required to secure systems.



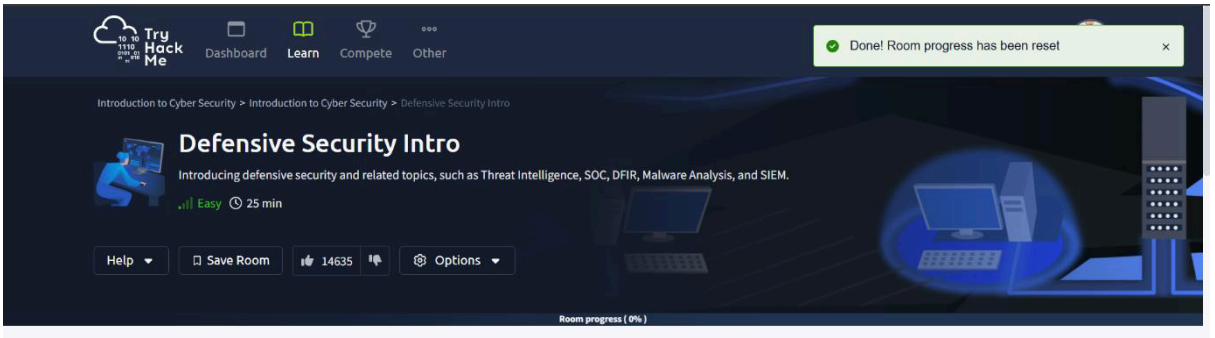
Task 3: Careers in Cybersecurity

- **Explanation**: This task outlines various career opportunities within the cybersecurity field, including roles like penetration tester, ethical hacker, security analyst, and more.

It highlights the importance of these roles in protecting systems and networks from cyber threats.

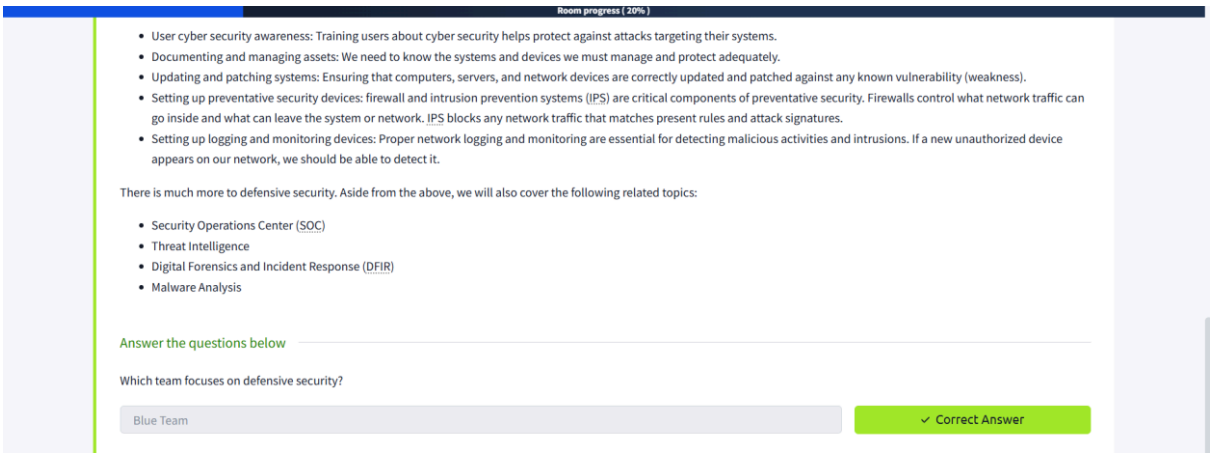


Defensive Security Intro



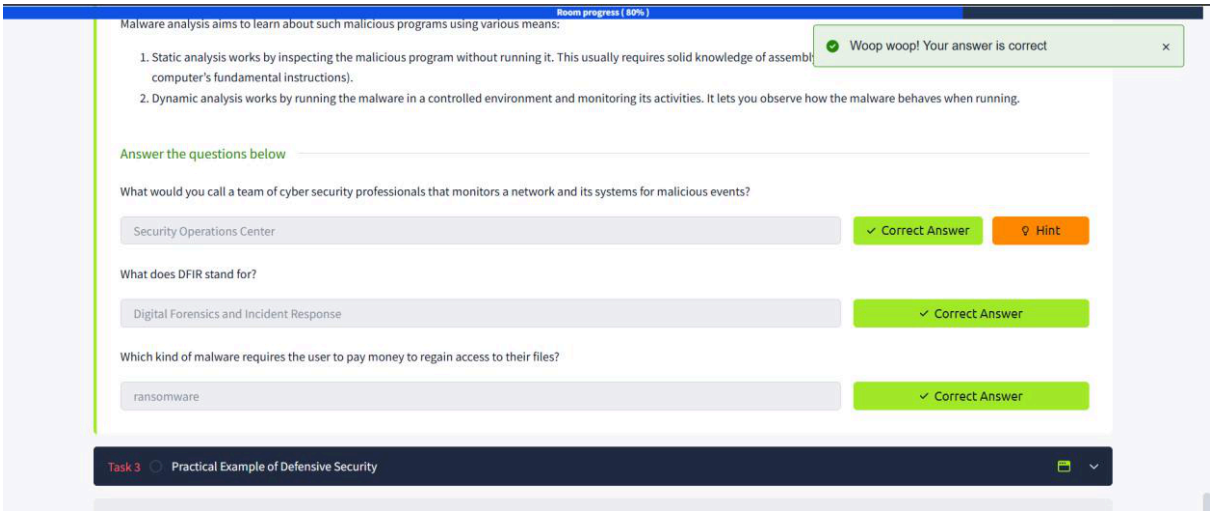
Task 1: Introduction to Defensive Security

- **Explanation**: Defensive security involves measures and practices to protect systems, networks, and data from cyber threats. It focuses on safeguarding against attacks through proactive monitoring, response strategies, and hardening systems to prevent unauthorized access.



Task 2: Areas of Defensive Security

- **Explanation**: This task discusses key areas of defensive security, such as Threat Intelligence, Security Operations Centers (SOC), Digital Forensics and Incident Response (DFIR), Malware Analysis, and Security Information and Event Management (SIEM). These areas work together to detect, prevent, and respond to cyberattacks effectively.

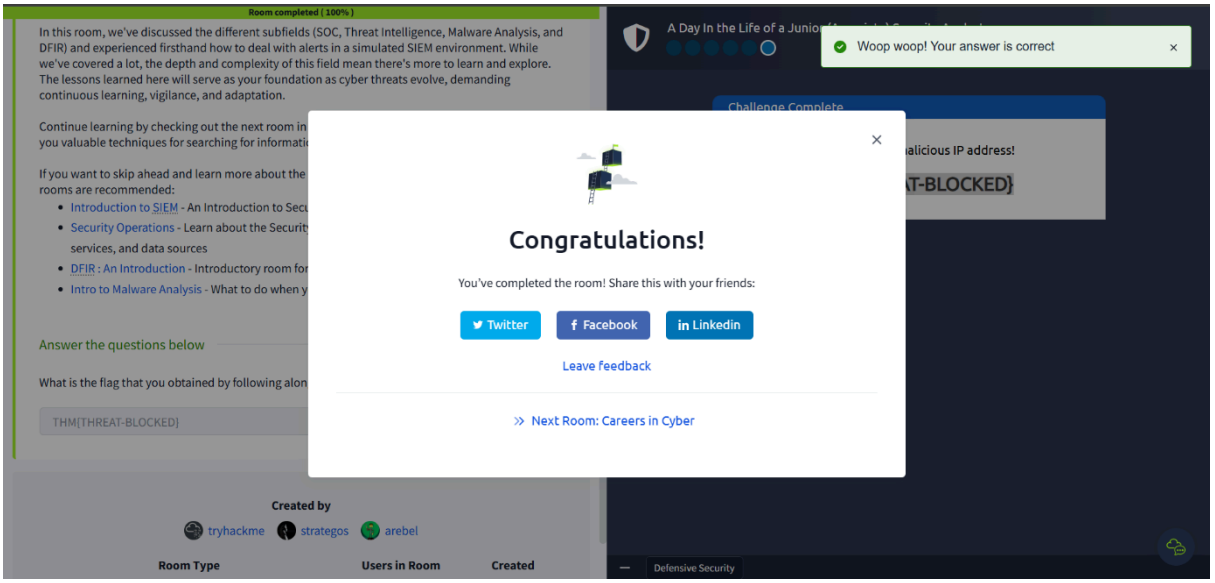


Task 3: Practical Example of Defensive Security

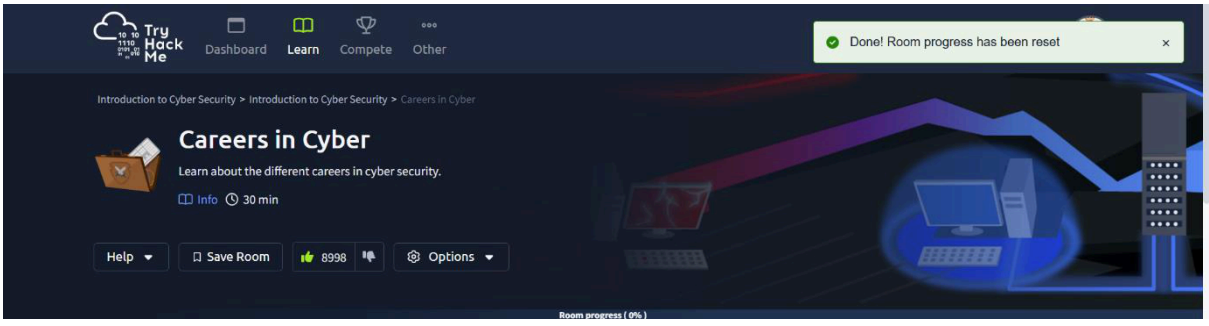
- **Explanation**: This task provides a practical example of defensive security in action,

where you will explore how various defensive techniques, such as monitoring and

incident response, are applied to secure systems and protect against real-world threats.

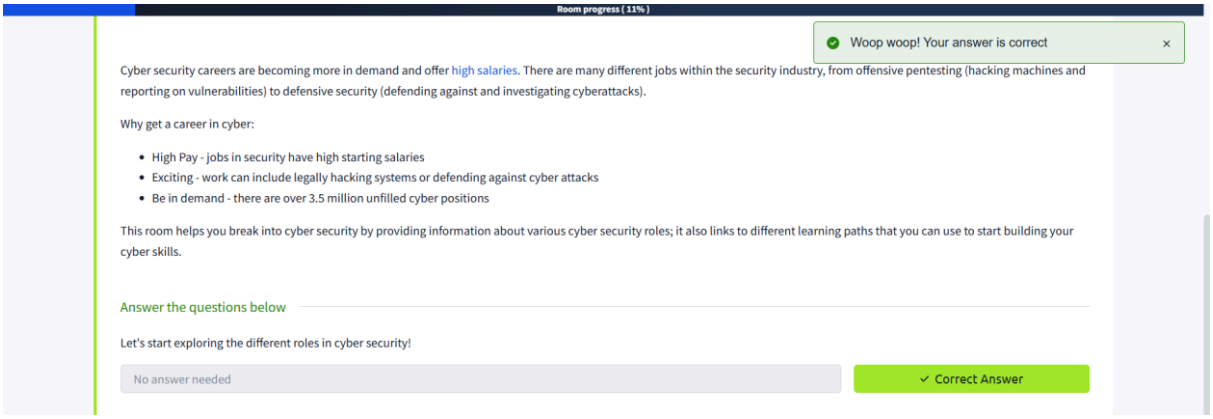


Careers in Cyber



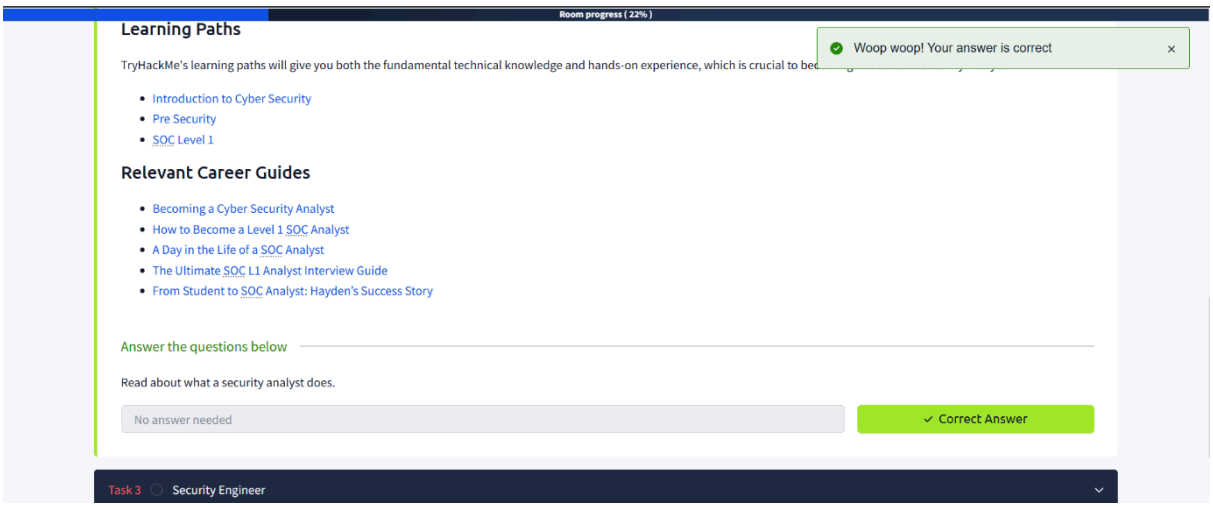
Task 1: Introduction

• **Explanation**: This task introduces the various career paths in the cybersecurity industry, providing an overview of the different roles available to professionals. It emphasizes the importance of cybersecurity in today's digital world and the need for skilled professionals to protect sensitive information.



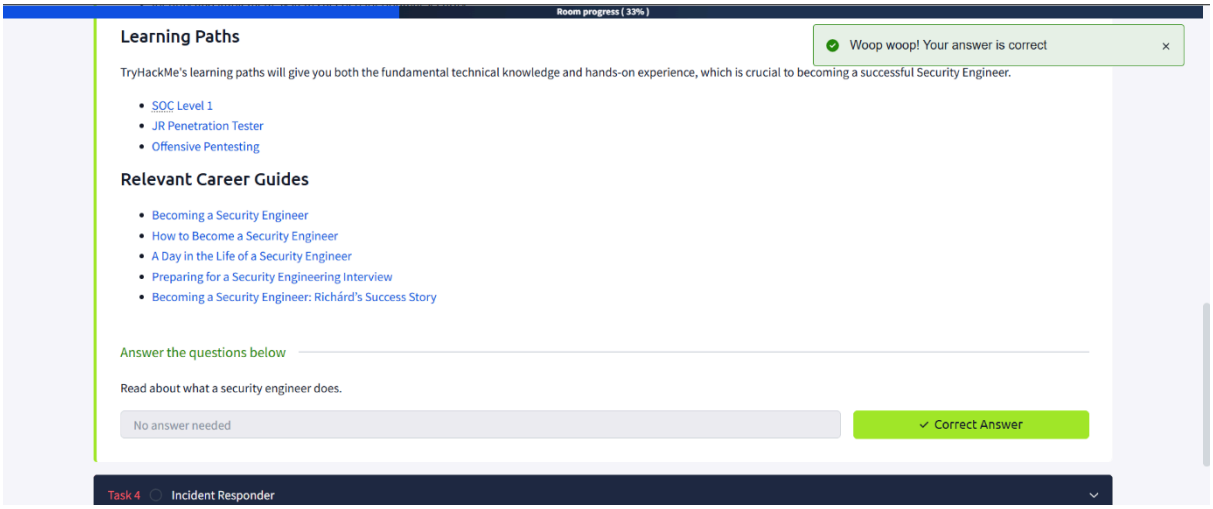
Task 2: Security Analyst

• **Explanation**: Security analysts are responsible for monitoring and defending an organization's networks and systems. They analyze vulnerabilities, detect threats, and respond to incidents, often working closely with other cybersecurity teams to ensure protection against potential attacks.



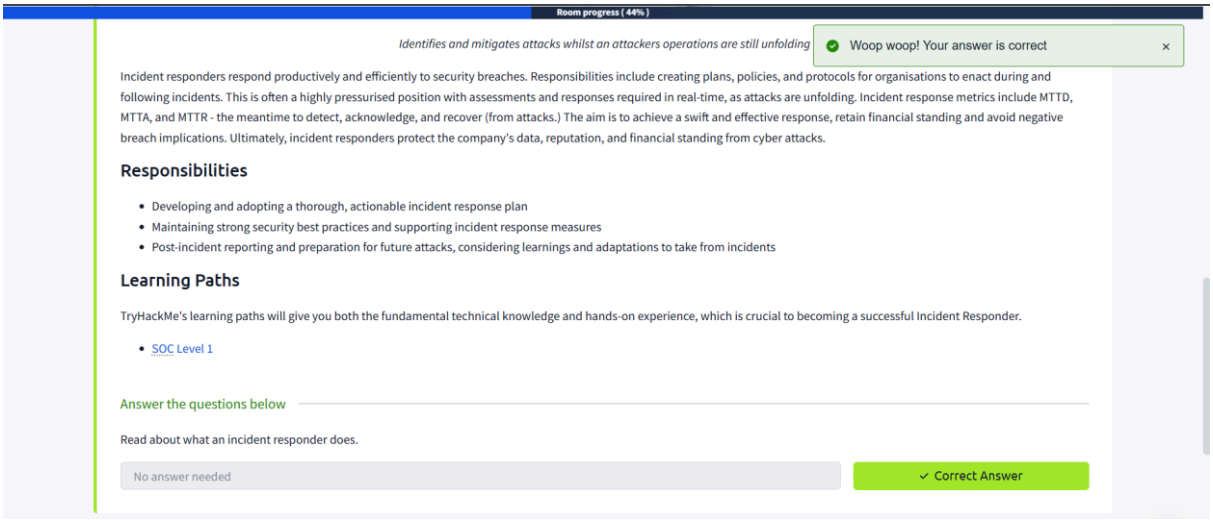
Task 3: Security Engineer

- **Explanation**: Security engineers focus on building and implementing security infrastructure to protect systems and data. They design secure networks, firewalls, and encryption protocols, as well as troubleshoot and maintain security systems to ensure an organization's IT environment is secure.



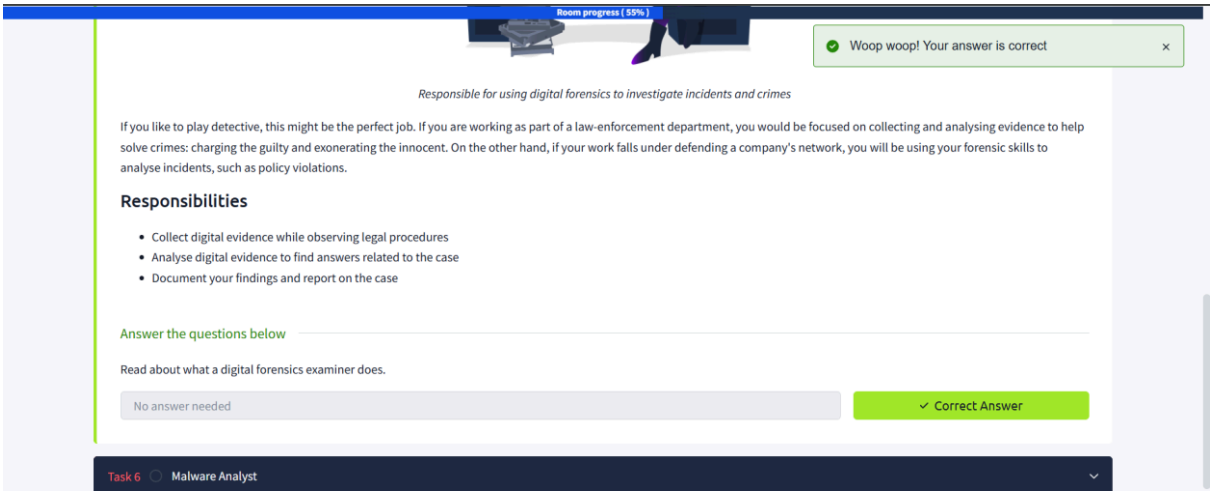
Task 4: Incident Responder

- **Explanation**: Incident responders manage and respond to security breaches or cyberattacks. Their role is to identify, contain, and mitigate the impact of security incidents while performing post-incident analysis to prevent future attacks.



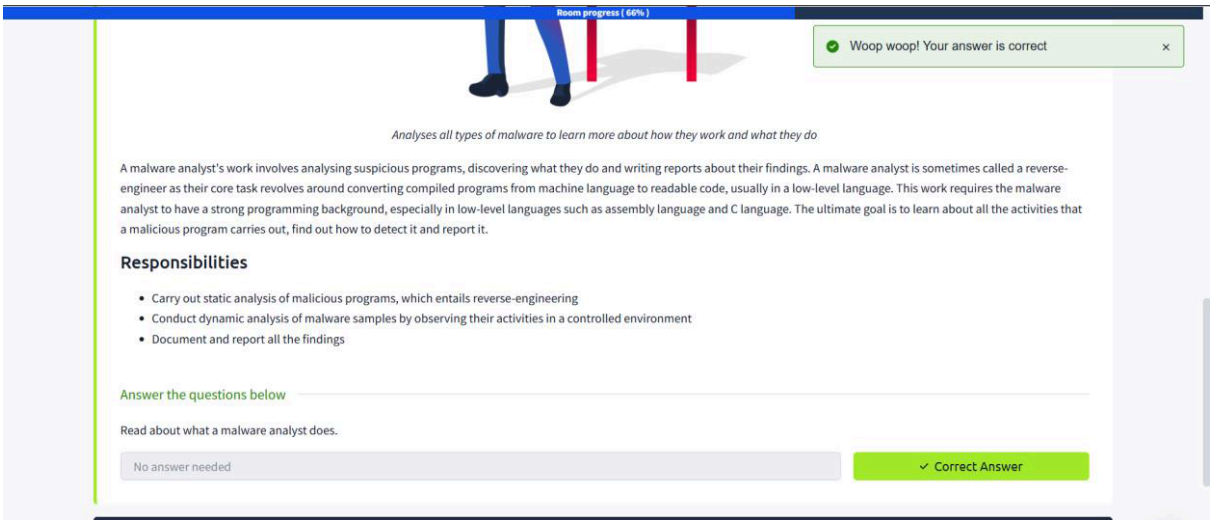
Task 5: Digital Forensics Examiner

- **Explanation**: Digital forensics examiners analyze and recover data from computers and other digital devices after security incidents. They use various tools and techniques to trace cybercrimes, ensuring the evidence is collected and preserved for legal purposes.



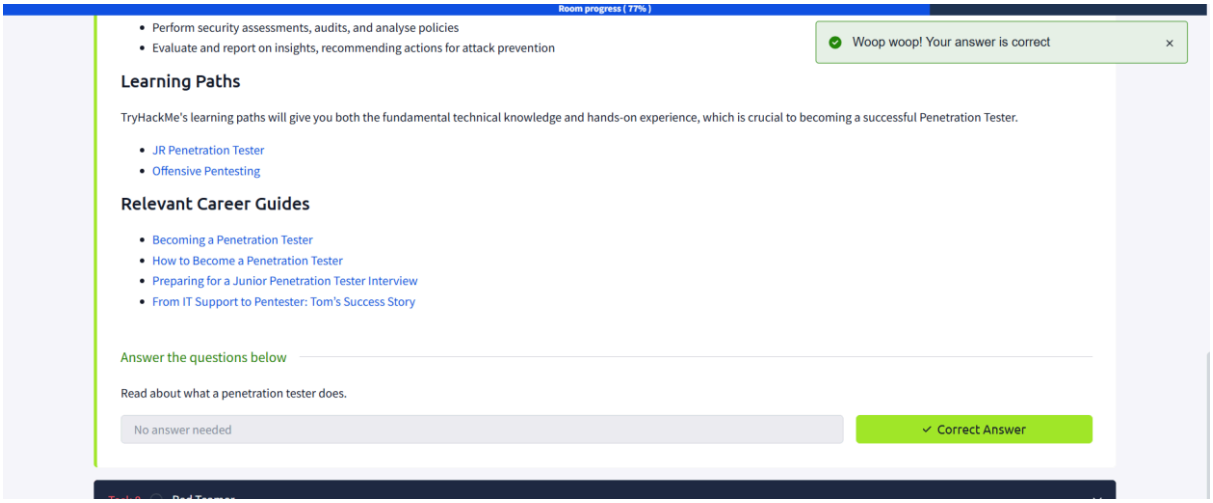
Task 6: Malware Analyst

- **Explanation**: Malware analysts study malicious software to understand how it works, its behavior, and how it can be neutralized. They create defenses against malware and help organizations detect, remove, and prevent future infections.



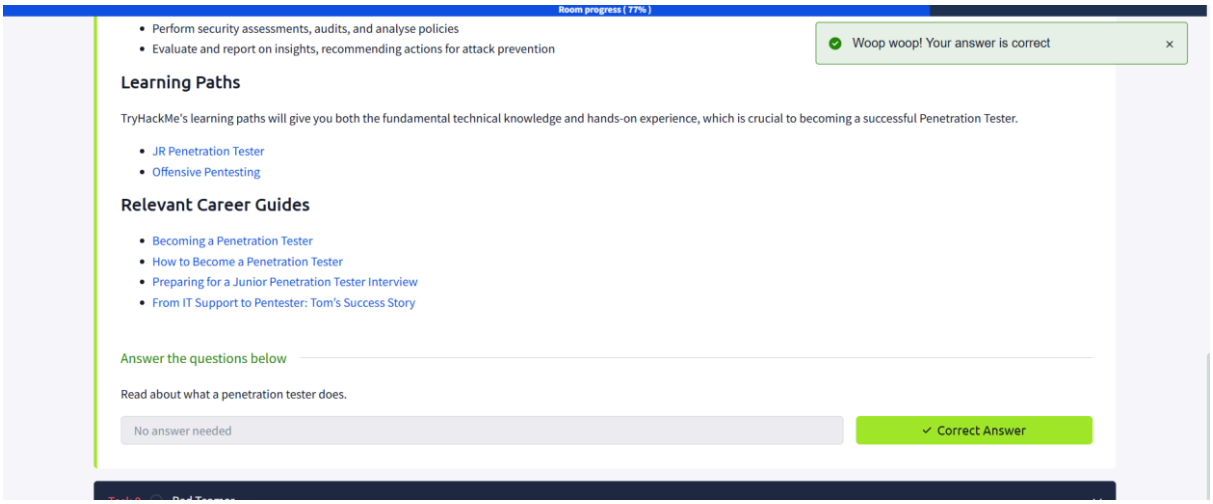
Task 7: Penetration Tester

• **Explanation**: Penetration testers, also known as ethical hackers, simulate cyber attacks on systems to identify vulnerabilities. Their goal is to exploit weaknesses in order to help organizations strengthen their security posture by patching identified flaws.



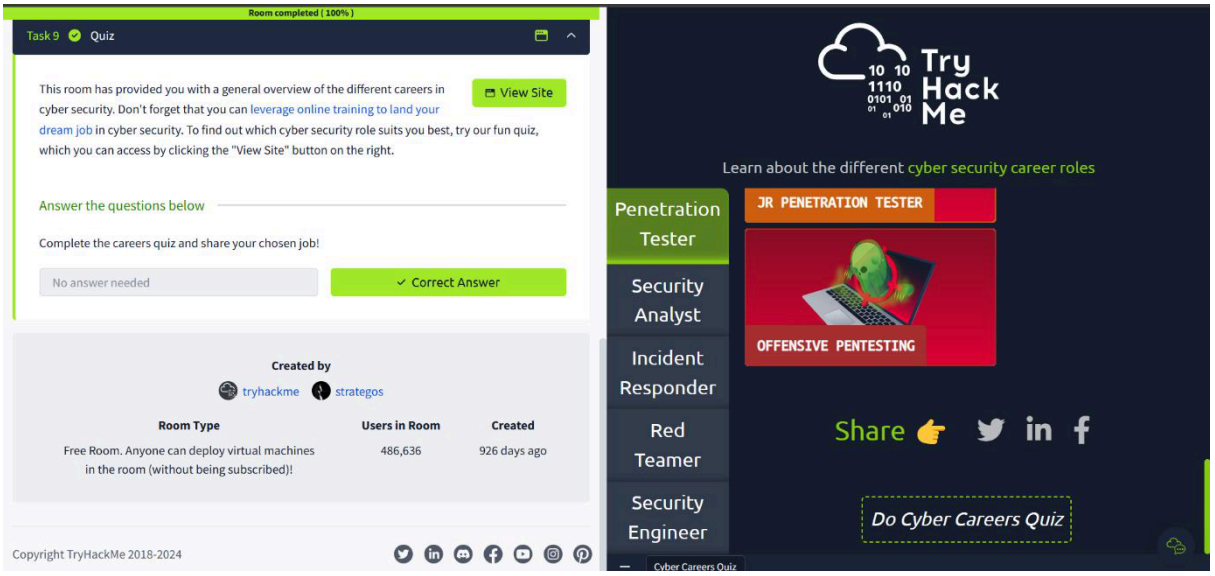
Task 8: Red Teamer

• **Explanation**: Red teamers simulate sophisticated attacks by using real-world tactics to assess an organization's security defenses. Unlike penetration testers, they conduct full-scale attack simulations, including physical security testing and social engineering techniques, to evaluate how well an organization can withstand attacks.

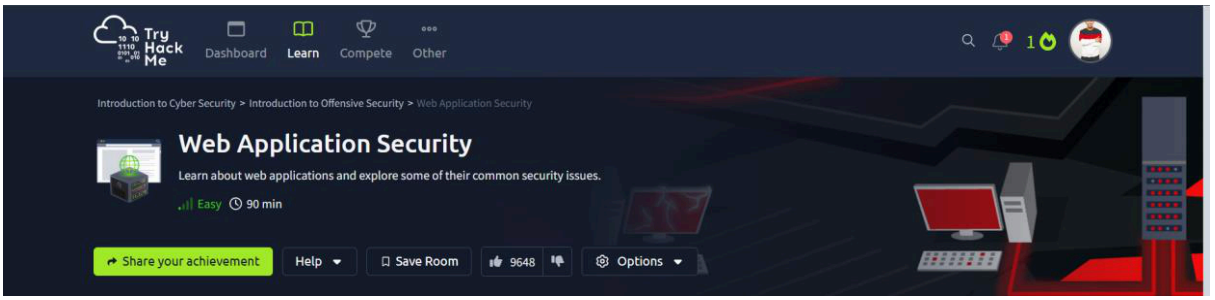


Task 9: Quiz

- **Explanation**: The quiz assesses your understanding of the various careers in cybersecurity discussed throughout the room. It helps reinforce the knowledge gained and ensures you are familiar with the roles, responsibilities, and skills required in different cybersecurity careers.

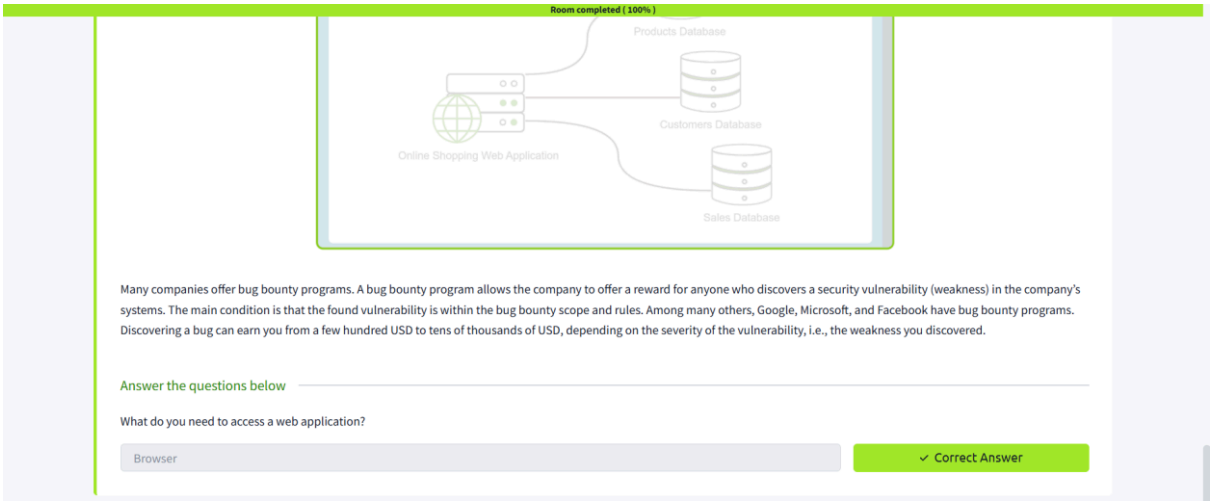


Web Application Security



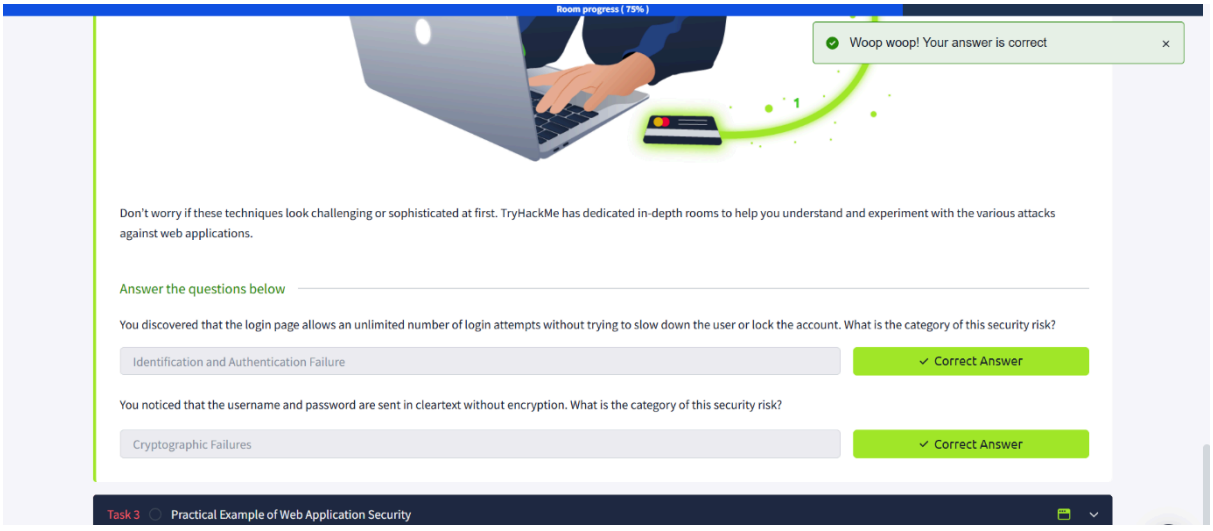
Task 1: Introduction

• **Explanation**: This task introduces the basics of web applications and their common vulnerabilities. It covers how web applications function and why security is essential to protect both users and the underlying infrastructure from cyber threats.



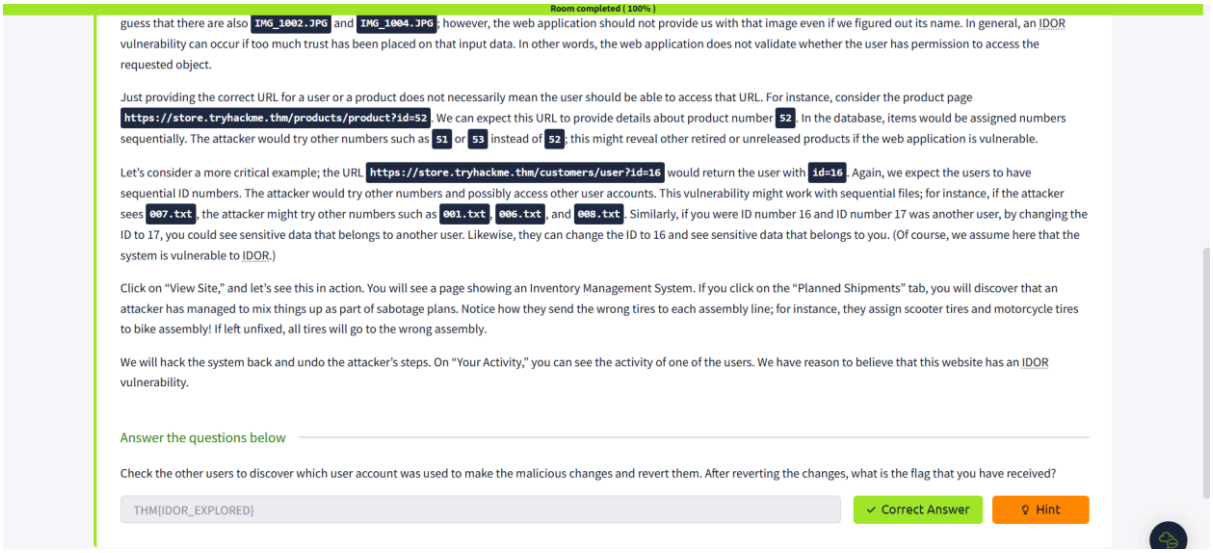
Task 2: Web Application Security Risks

• **Explanation**: This task focuses on common security risks in web applications, such as SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF). It explains how these vulnerabilities can be exploited and the importance of securing web applications against them.

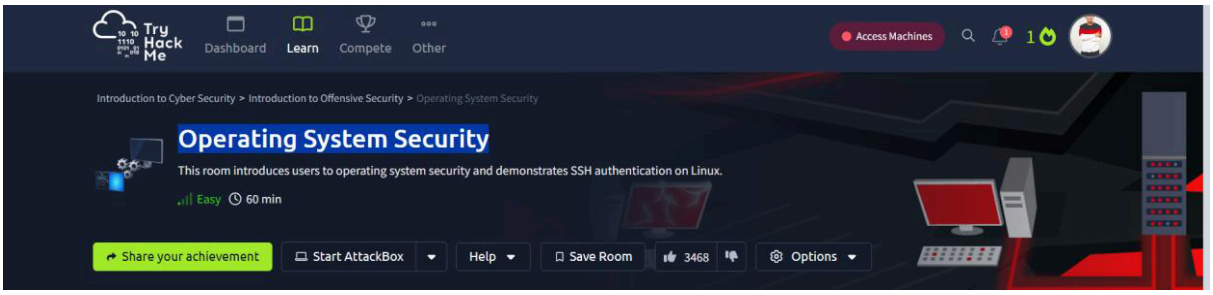


Task 3: Practical Example of Web Application Security

- **Explanation**: This task provides a hands-on example of web application security. It allows you to explore how web application vulnerabilities are identified and mitigated, giving you practical experience in securing web applications against common threats.

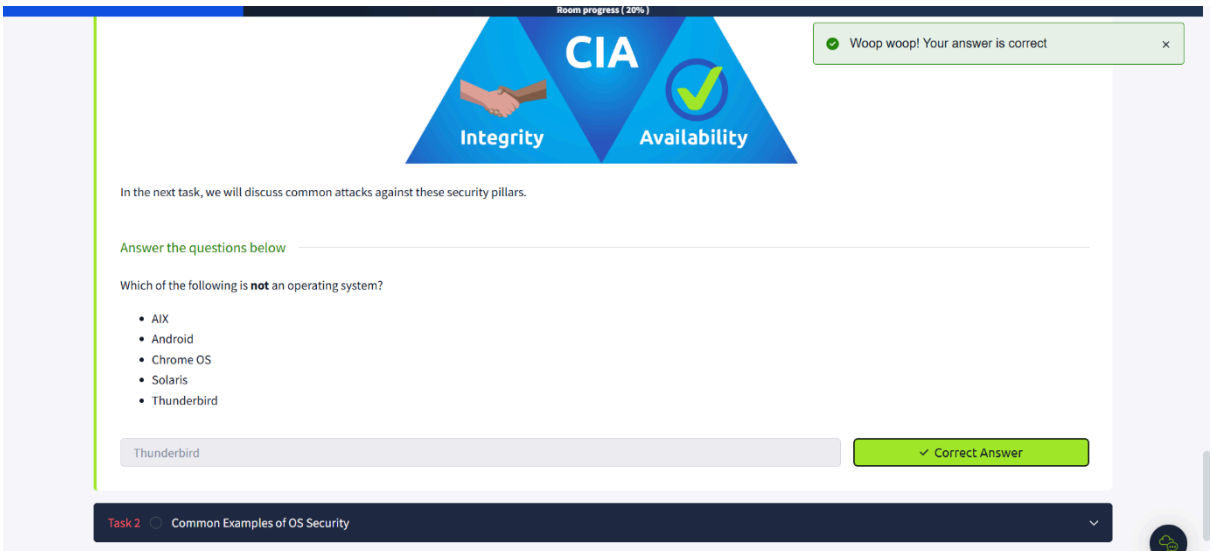


Operating System Security



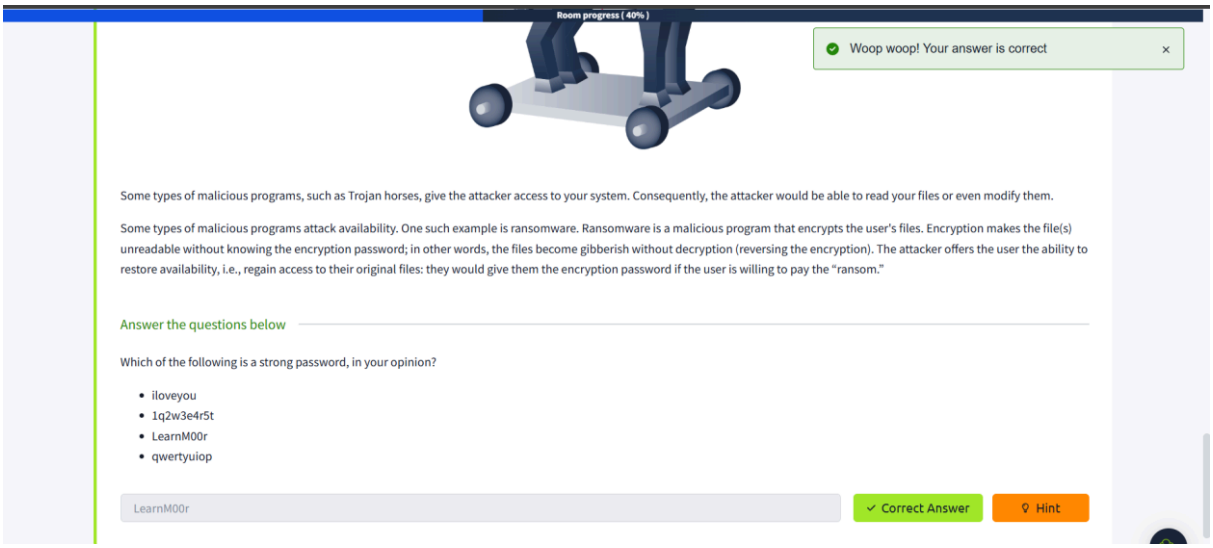
Task 1: Introduction to Operating System Security

• **Explanation**: This task introduces the concept of operating system security, covering how OS-level vulnerabilities can be exploited and the importance of securing operating systems to prevent unauthorized access and data breaches. It also explains the role of security measures such as firewalls, updates, and user permissions.



Task 2: Common Examples of OS Security

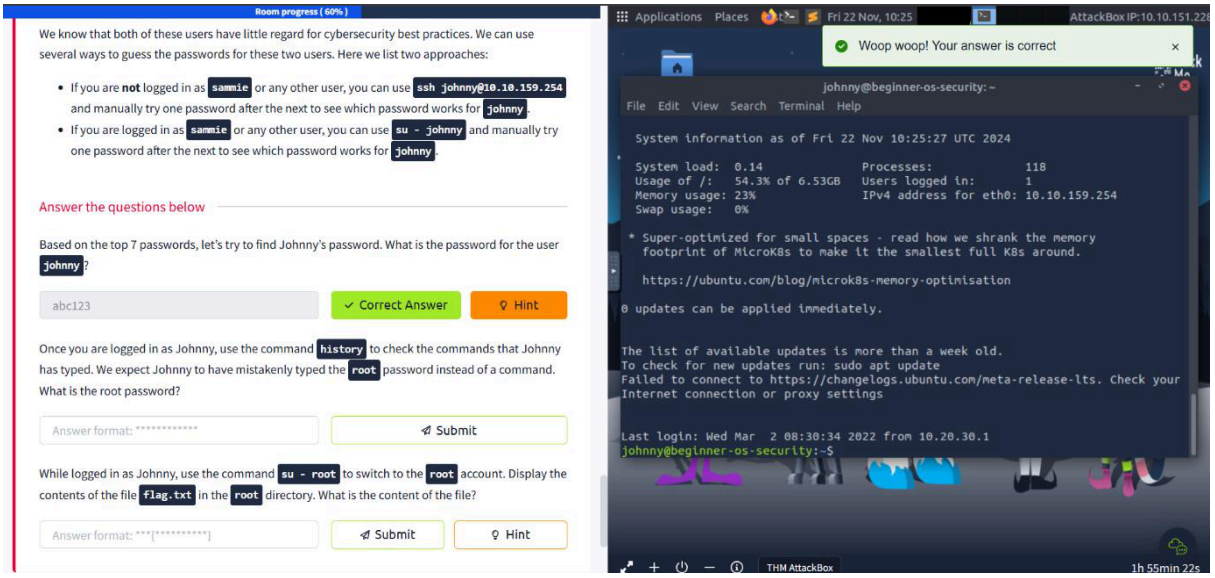
- **Explanation**: This task highlights common security threats and risks related to operating systems, such as privilege escalation, unauthorized access, and insecure configurations. It discusses how these vulnerabilities can affect system integrity and confidentiality, and outlines measures to mitigate them.

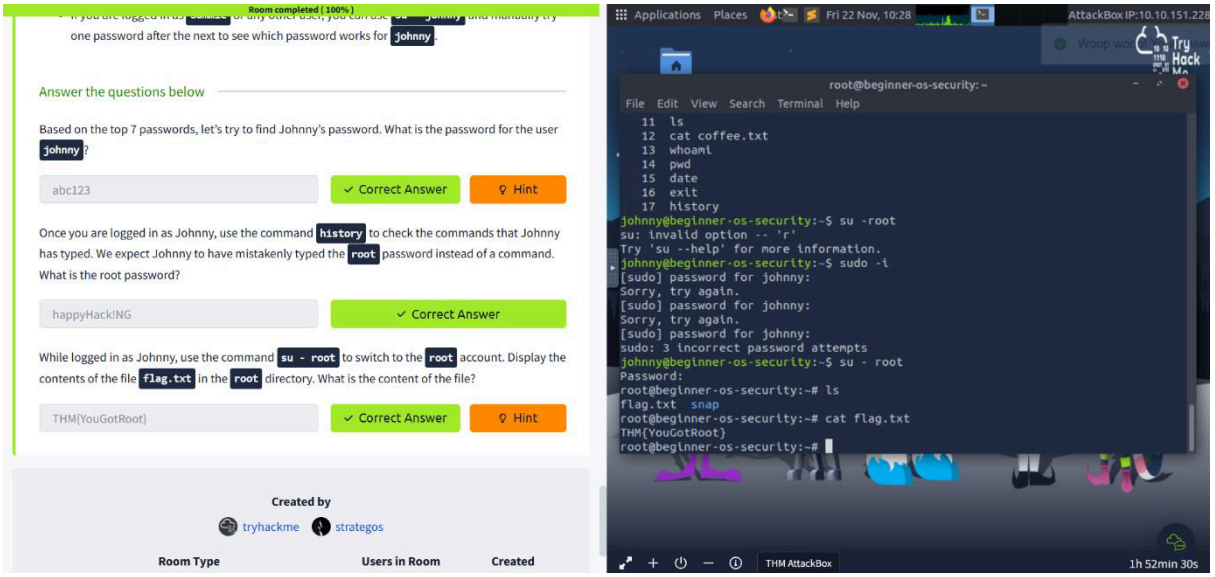


Task 3: Practical Example of OS Security

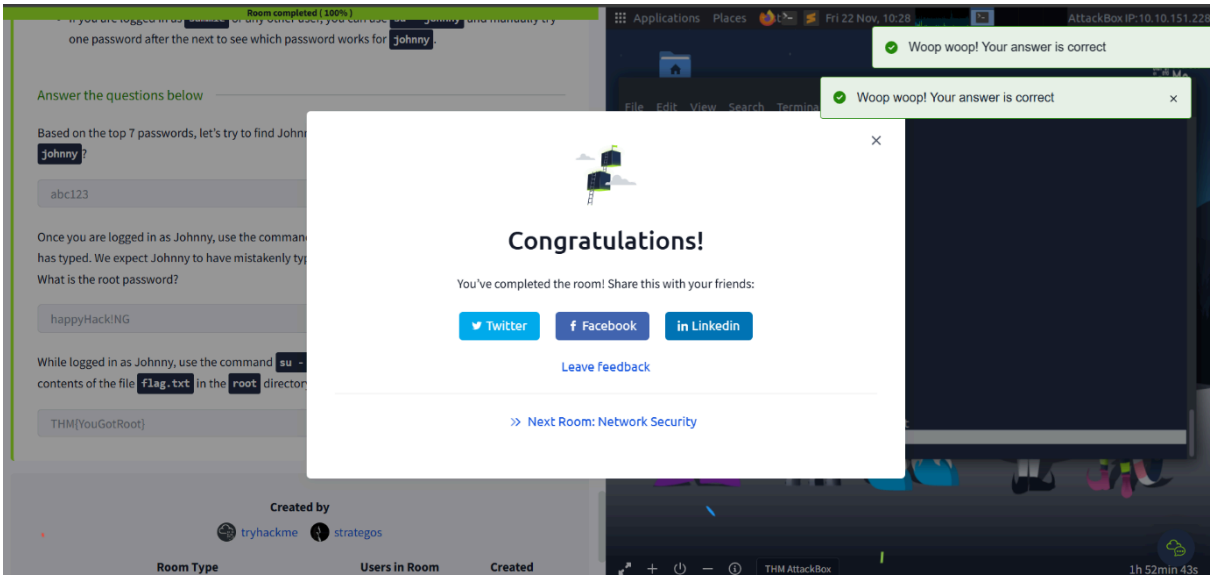
- **Explanation**: This task provides a hands-on demonstration of operating system security, focusing on SSH authentication in Linux. It walks through

securing access to a Linux machine using SSH keys, highlighting best practices for system administration and remote access security.

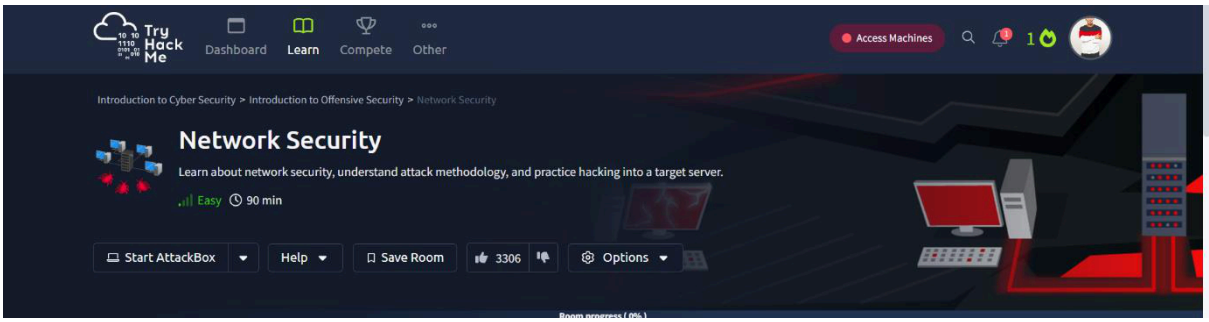




Completion :

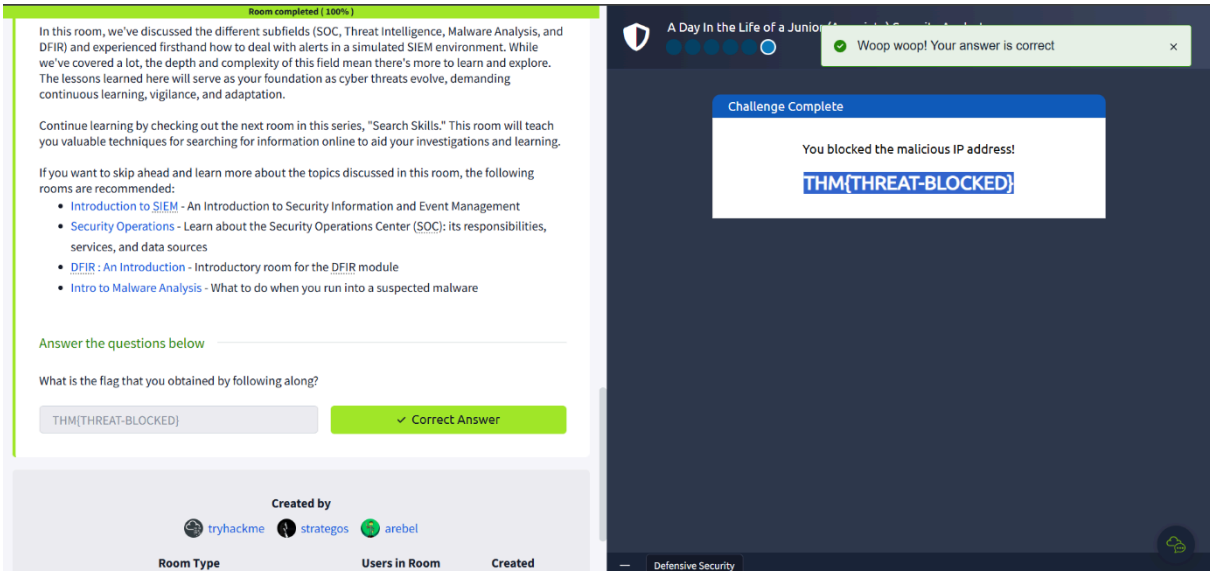


Network Security



Task 1: Introduction

• **Explanation**: This task introduces the basics of network security, including its importance in safeguarding data and systems within a network. It explains the role of security measures such as firewalls, encryption, and intrusion detection systems to protect against unauthorized access and attacks.

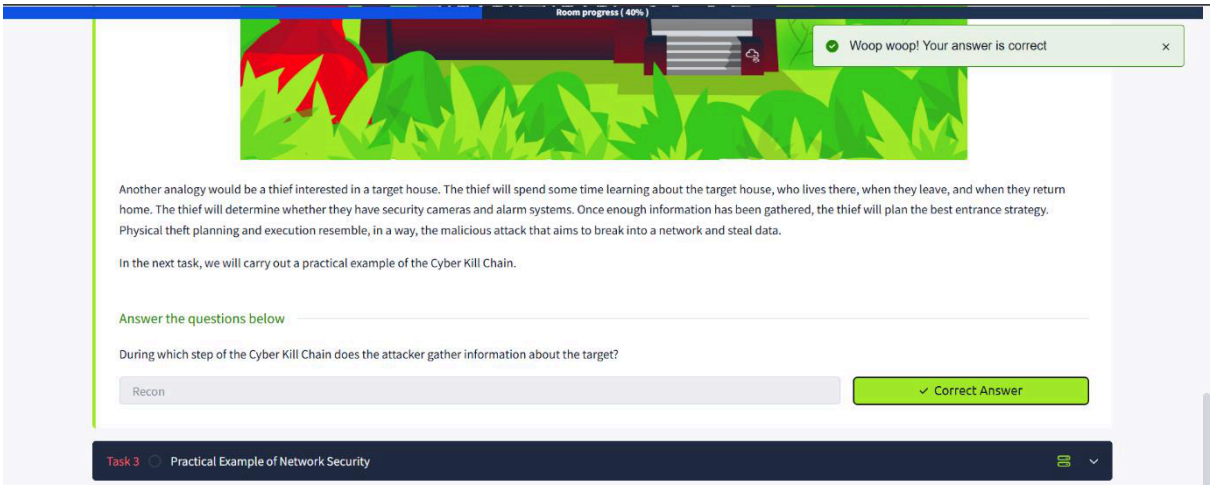


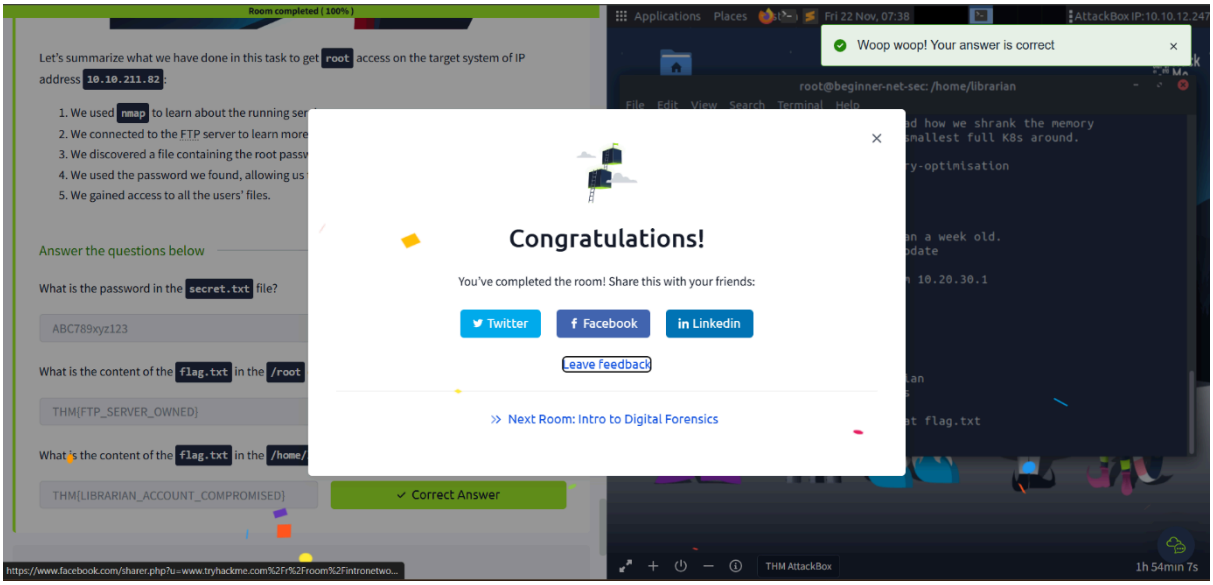
Task 2: Methodology

• **Explanation**: This task outlines the standard methodology used in network security assessments. It covers steps like information gathering, vulnerability scanning, exploitation, and post-exploitation. The methodology helps identify weaknesses in a network and provides a structured approach to improving security.

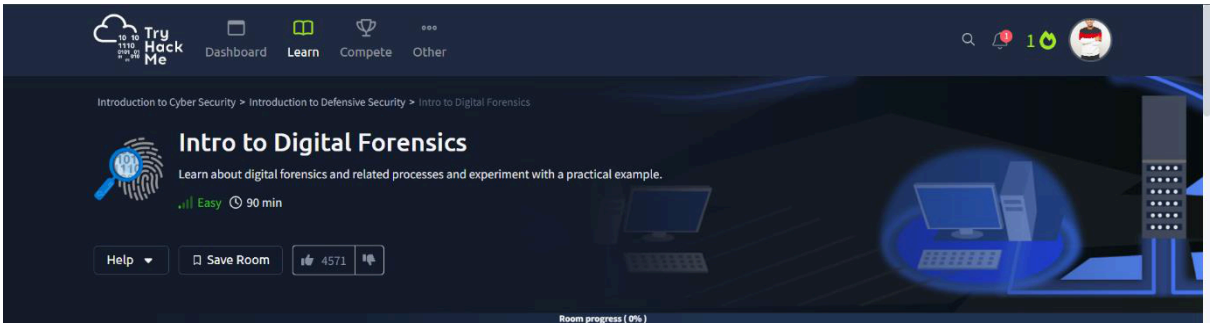
Task 3: Practical Example of Network Security

• **Explanation**: This task provides a practical example where you will practice hacking into a target server. It walks through real-world network security vulnerabilities and demonstrates how attackers exploit these weaknesses to gain unauthorized access. You will also learn techniques to defend against such attacks.



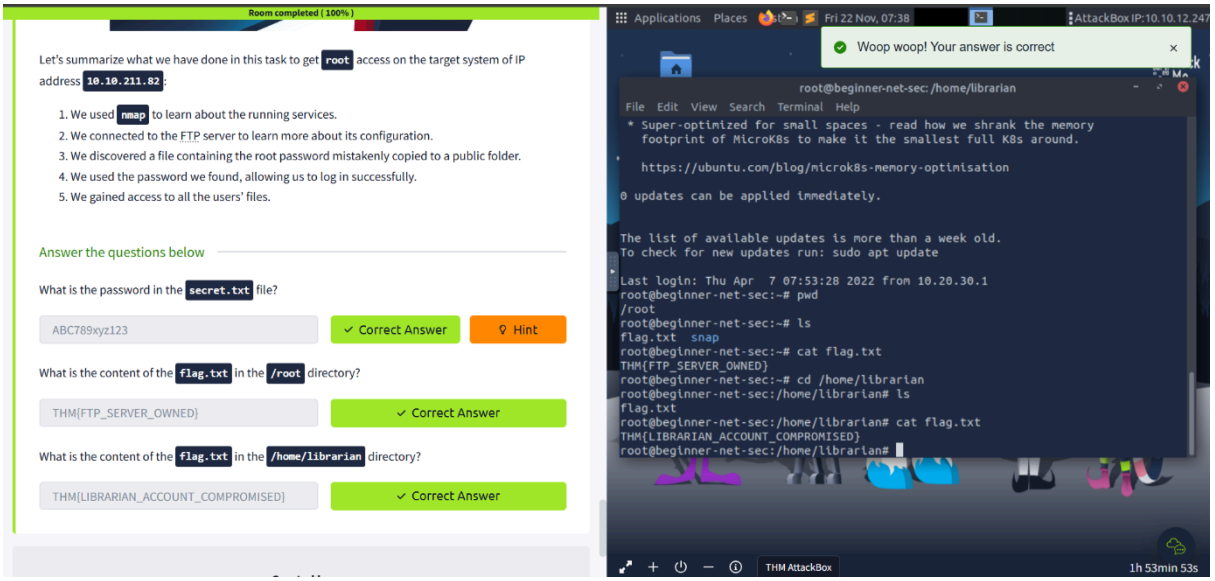


Intro to Digital Forensics



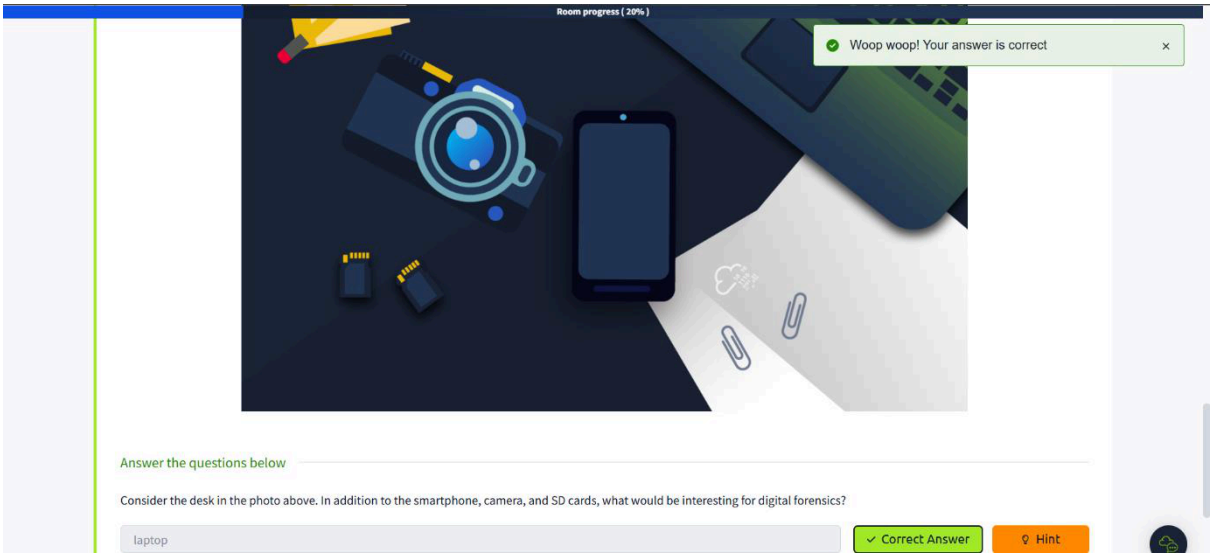
Task 1: Introduction to Digital Forensics

• **Explanation**: This task introduces the concept of digital forensics, which involves the recovery, investigation, and analysis of digital data to be used as evidence in criminal investigations. It covers the importance of digital forensics in the context of cybercrimes and how it helps in gathering actionable evidence.



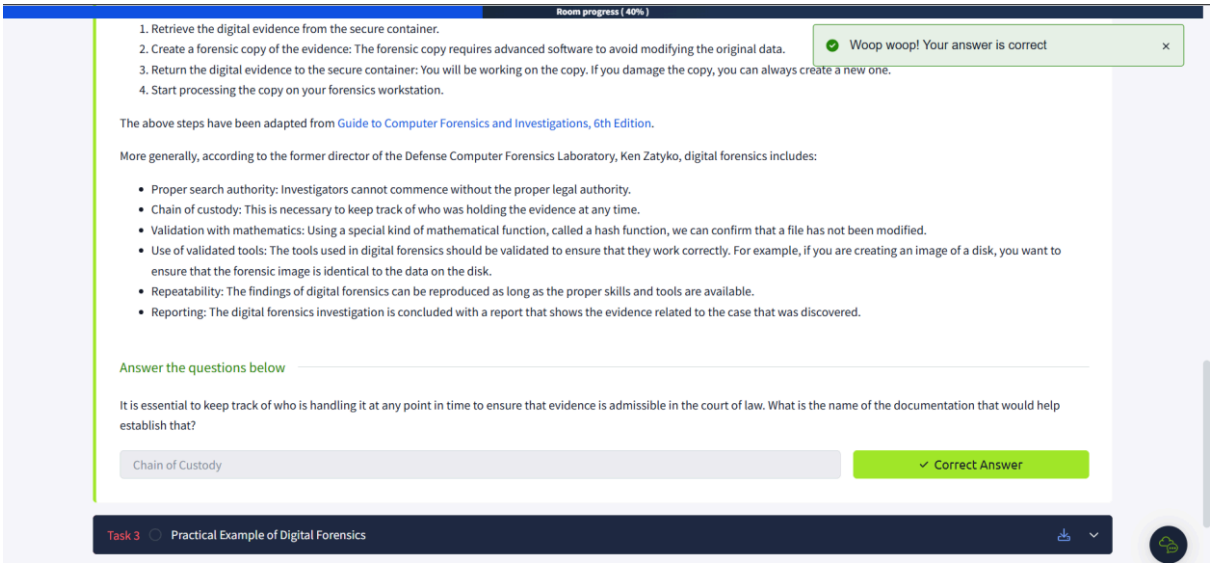
Task 2: Digital Forensics Process

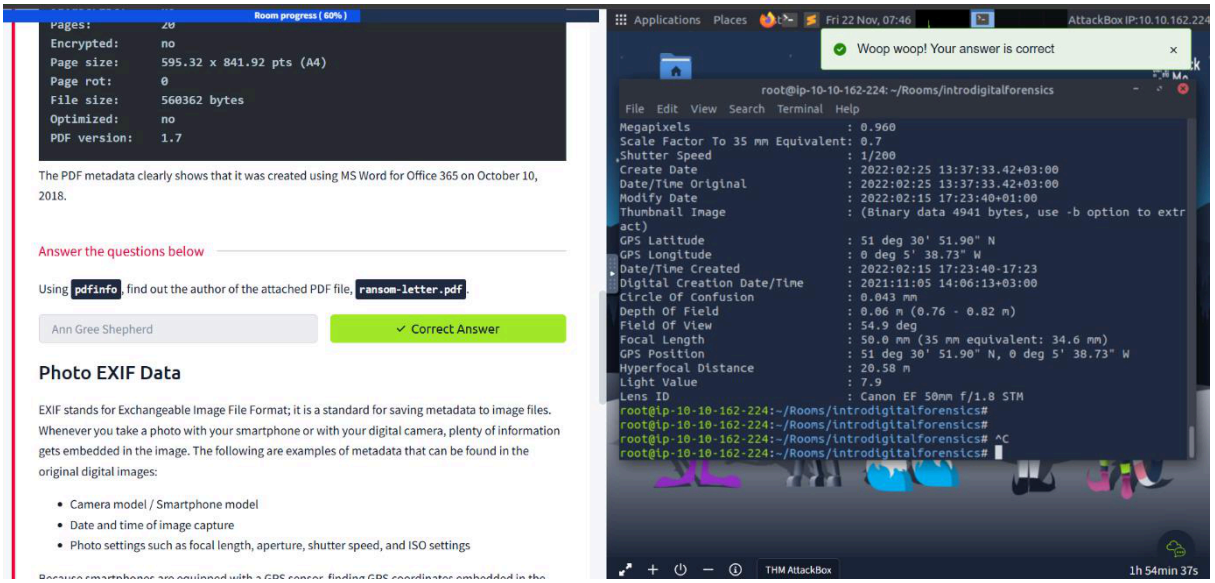
- **Explanation**: This task explains the steps involved in the digital forensics process, including identification, collection, preservation, analysis, and reporting of digital evidence. It also covers how to maintain the integrity of evidence to ensure it is admissible in legal proceedings.



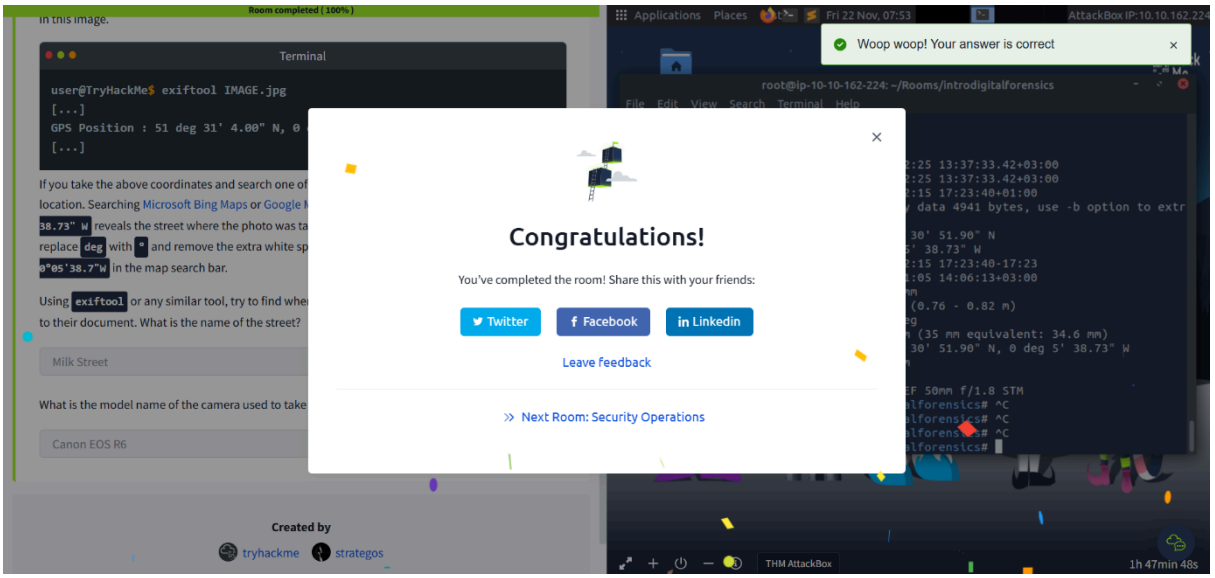
Task 3: Practical Example of Digital Forensics

- **Explanation**: This task provides a hands-on example of digital forensics, where you will analyze data from a digital device. You will learn how to identify relevant evidence, preserve it properly, and analyze it to uncover important information that can be used for legal or investigative purposes.





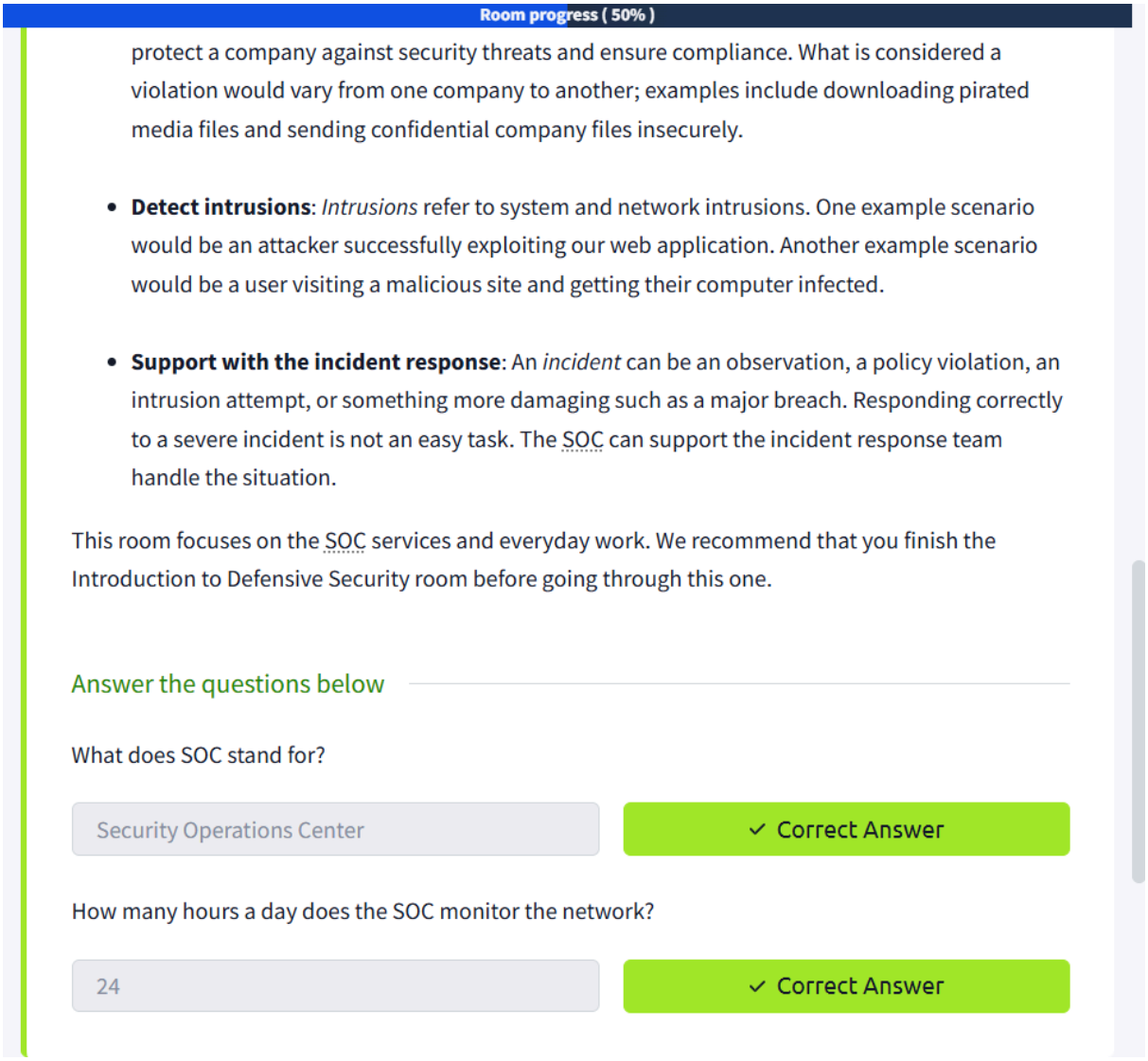
Completion:



Security Operations

Task 1: Introduction to Security Operations

• **Explanation**: This task introduces the concept of Security Operations, focusing on the role of a Security Operations Center (SOC). It covers its importance in monitoring, detecting, and responding to security incidents within an organization to maintain a secure environment.



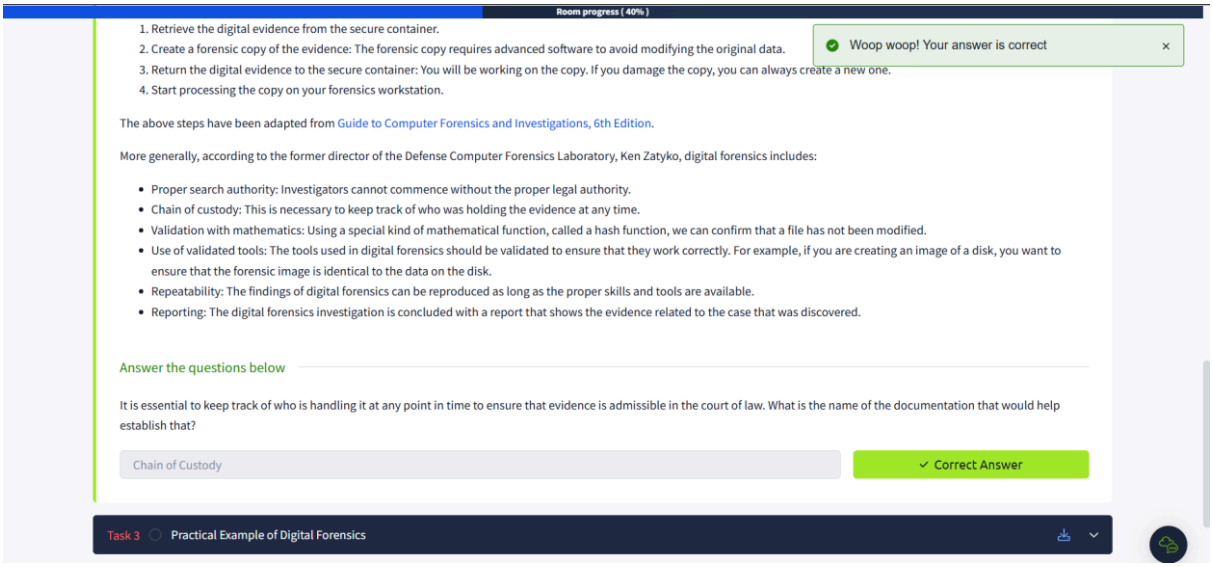
Task 2: Elements of Security Operations

- **Explanation**: This task explores the key components of a Security Operations Center

(SOC), such as monitoring systems, incident response, threat intelligence, and data

collection. It discusses how these elements come together to provide comprehensive

security monitoring and defense.

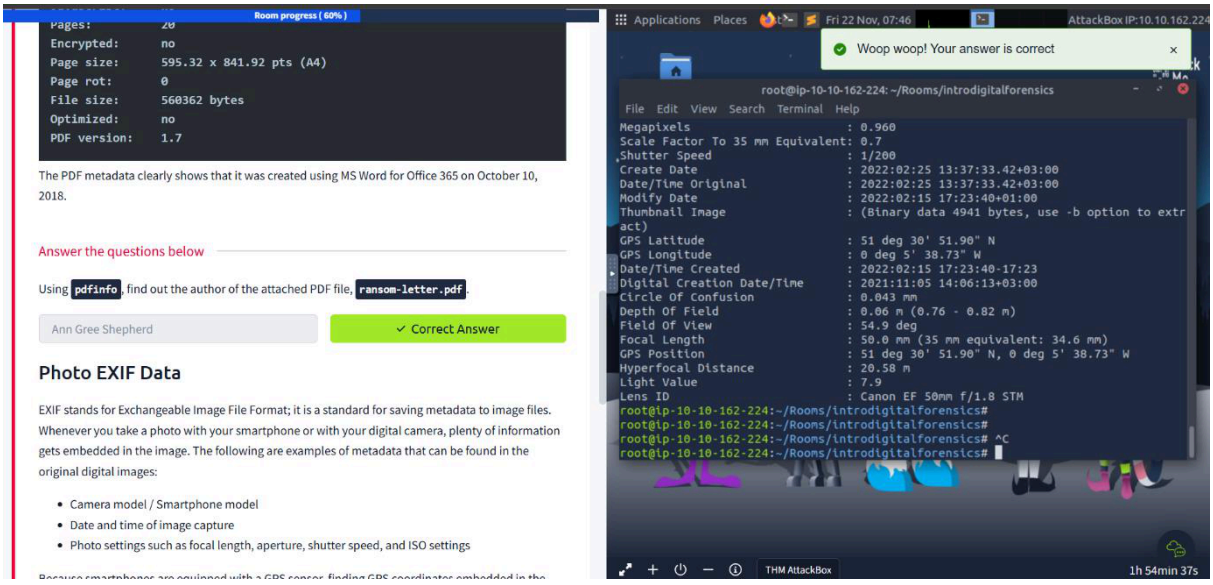


Task 3: Practical Example of SOC

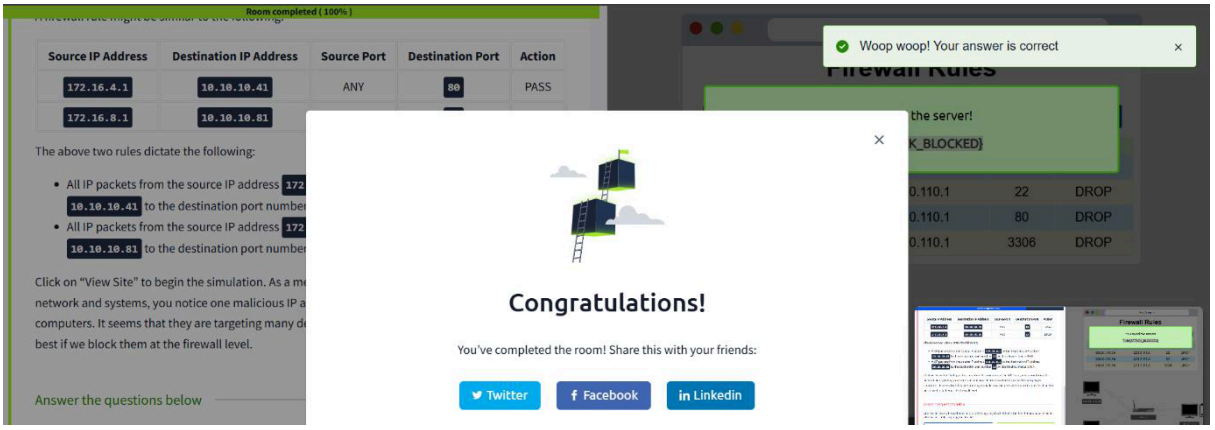
- **Explanation**: This task provides a practical example of how a Security Operations

Center functions. You will see how SOC teams respond to security incidents, analyze

alerts, and manage incidents to mitigate potential risks to the organization.



Completion:


Room completed (100%)
Source IP Address
Destination IP Address
Source Port
Destination Port
Action
172.16.4.1
10.10.10.41
ANY
80
PASS
172.16.8.1
10.10.10.81
The above two rules dictate the following:
All IP packets from the source IP address
10.10.10.41
to the destination port
All IP packets from the source IP address
10.10.10.81
to the destination port
Click on "View Site" to begin the simulation. As a
network and systems, you notice one malicious IP
computers. It seems that they are targeting many
best if we block them at the firewall level.
Answer the questions below
Woop woop! Your answer is correct
Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
0.110.1
22
DROP
0.110.1
80
DROP
0.110.1
3306
DROP