EncryptEdge Labs

Cybersecurity Analyst Internship

Task Report

atalmamun@gmail.com

Task No: 04

Credit: Offensive Security

EncryptEdge Labs

Table of Contents

1.0 EncryptEdge Labs Internship Task Report

1.1 Introduction

This report provides an overview of fundamental cybersecurity concepts, including key terminology, common cyber threats, and the essential responsibilities of a cybersecurity analyst. Additionally, the report presents insights gained from hands-on practical exercises conducted through TryHackMe labs, reinforcing theoretical knowledge with practical application. By understanding these foundational principles, cybersecurity professionals can enhance their ability to detect, prevent, and respond to security incidents effectively.

1.2 Objective

The primary objective of this report is to develop a foundational understanding of cybersecurity principles and their practical applications. This includes:

- Gaining familiarity with essential cybersecurity terminology to enhance technical comprehension.
- Analyzing different types of cyber threats, such as malware, phishing, ransomware, and Distributed Denial of Service (DDoS) attacks, to understand their impact and mitigation strategies.
- Exploring the critical role of cybersecurity analysts in identifying, analyzing, and responding to security threats.
- Demonstrating knowledge gained through hands-on practical exercises in TryHackMe labs, reinforcing theoretical concepts with real-world applications.

By achieving these objectives, this report aims to strengthen cybersecurity awareness and improve the ability to implement effective security measures within an organizational context.

1.3 Requirements

To successfully complete this task, several requirements were met to ensure a comprehensive understanding of cybersecurity fundamentals. These requirements include:

- **Research and Documentation:** Conducting in-depth research on essential cybersecurity concepts, including encryption, firewalls, penetration testing, incident response, and Security Operations Centers (SOC).
- **Cyber Threat Analysis:** Examining common cyber threats such as malware, phishing, ransomware, Distributed Denial of Service (DDoS) attacks, and insider threats to understand their mechanisms, impact, and mitigation strategies.
- **Understanding the Role of a Cybersecurity Analyst:** Exploring the responsibilities of a cybersecurity analyst, including monitoring network activity, incident response, vulnerability management, and threat hunting.
- **Hands-on Practical Labs:** Completing three TryHackMe labs—'Learning Cybersecurity,' 'Intro to Defensive Security,' and 'Security Principles'—to reinforce theoretical knowledge with practical application.
- **Report Compilation:** Organizing findings into a structured report following the given template, incorporating theoretical insights, practical experiences, and relevant screenshots from completed labs.

These requirements collectively ensure a well-rounded understanding of cybersecurity fundamentals and their real-world applications.

2.0 Cybersecurity Terminology Glossary

This section provides definitions for essential cybersecurity terms, forming a foundational understanding of key concepts relevant to the field.

Encryption

Encryption is the process of converting plaintext data into an unreadable format (ciphertext) using cryptographic algorithms. It ensures data confidentiality by allowing only authorized parties with the correct decryption key to access the original information. Common encryption methods include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).

Firewall

A firewall is a network security device or software that monitors and controls incoming and outgoing traffic based on predefined security rules. It acts as a barrier between trusted internal networks and untrusted external networks, preventing unauthorized access and potential cyber threats. Firewalls can be categorized as network firewalls, host-based firewalls, and next-generation firewalls (NGFW).

Penetration Testing

Penetration testing, commonly referred to as ethical hacking, is a simulated cyberattack conducted on a system, network, or application to identify vulnerabilities before malicious attackers can exploit them. This process helps organizations strengthen their security posture by proactively addressing weaknesses. Penetration testing follows methodologies such as OWASP Testing Guide and NIST 800-115.

Incident Response

Incident response is a structured approach to identifying, containing, eradicating, and recovering from cybersecurity incidents. It involves predefined protocols and procedures to minimize damage, restore normal operations, and prevent future attacks. Organizations often use incident response frameworks like NIST Cybersecurity Framework and SANS Incident Handling Process.

SOC (Security Operations Center)

A Security Operations Center (SOC) is a centralized team or facility responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats in real-time. SOC analysts use tools like Security Information and Event Management (SIEM) systems to identify and mitigate potential security incidents. The SOC plays a critical role in ensuring an organization's cybersecurity resilience.

Additional Key Terms:

- **Zero Trust Security:** A security model that requires continuous verification of every user and device attempting to access a network, assuming no entity is inherently trustworthy.
- **Multi-Factor Authentication (MFA):** A security mechanism requiring users to authenticate their identity using multiple factors, such as passwords, biometrics, or authentication apps.
- **Threat Intelligence:** The process of collecting, analyzing, and applying information about potential cybersecurity threats to enhance an organization's defensive strategies.
- **Social Engineering:** A manipulation technique used by cybercriminals to deceive individuals into disclosing sensitive information or performing actions that compromise security.

This glossary establishes a foundational understanding of critical cybersecurity terms, aiding in better comprehension of threats, defenses, and security protocols.

3.0 Cyber Threats Summary

Cyber threats are malicious activities aimed at compromising the confidentiality, integrity, or availability of digital assets. Understanding these threats, their mechanisms, and mitigation strategies is crucial for securing organizational systems. This section outlines some of the most common cyber threats.

3.1 Malware

Mechanism: Malware (malicious software) is designed to infiltrate, damage, or disrupt computer systems. It includes various types such as viruses, worms, trojans, spyware, and rootkits. Malware spreads through infected email attachments, malicious websites, or software downloads.

Impact: Malware can cause data breaches, financial losses, system failures, and unauthorized access to sensitive information. Ransomware, a type of malware, can encrypt critical files and demand payment for decryption.

Mitigation:

- Use up-to-date antivirus and anti-malware software.
- Avoid downloading files or clicking on suspicious links from untrusted sources.
- Regularly update software and operating systems to patch vulnerabilities.

3.2 Phishing

Mechanism: Phishing attacks use deceptive emails, messages, or websites to trick individuals into providing sensitive information such as login credentials, financial details, or personal data. Attackers often impersonate trusted entities to gain the victim's confidence.

Impact: Phishing can lead to identity theft, financial fraud, and unauthorized access to corporate systems, often resulting in significant data breaches.

Mitigation:

- Implement email filtering and anti-phishing software.
- Train employees to recognize phishing attempts and verify suspicious messages.
- Enable multi-factor authentication (MFA) to add an extra layer of security.

3.3 Distributed Denial of Service (DDoS) Attacks

Mechanism: A DDoS attack floods a target server, network, or website with excessive traffic, overwhelming resources and making services unavailable to legitimate users. Attackers use botnets—networks of compromised devices—to generate large-scale traffic surges.

Impact: DDoS attacks disrupt business operations, cause website downtime, and lead to financial losses, especially for e-commerce and online services.

Mitigation:

- Use DDoS mitigation tools such as content delivery networks (CDNs) and web application firewalls (WAFs).
- Monitor network traffic for unusual activity and configure rate-limiting mechanisms.
- Implement cloud-based DDoS protection services for scalability and resilience.

3.4 Ransomware

Mechanism: Ransomware is a type of malware that encrypts files and demands a ransom payment for their decryption. Attackers typically distribute ransomware through phishing emails, malicious downloads, or exploiting unpatched software vulnerabilities.

Impact: Victims may lose access to critical data, face business interruptions, and suffer financial losses from ransom demands and recovery efforts. Even if a ransom is paid, there is no guarantee that the data will be restored.

Mitigation:

- Regularly back up important data and store it offline or in a secure cloud service.
- Implement endpoint protection solutions and security awareness training.
- Restrict user permissions and apply software patches promptly.

3.5 Insider Threats

Mechanism: Insider threats arise from employees, contractors, or business partners who misuse their authorized access to harm an organization. This can be intentional (e.g., data theft, sabotage) or unintentional (e.g., negligent handling of sensitive information).

Impact: Insider threats can lead to data breaches, intellectual property theft, and reputational damage. Malicious insiders may leak confidential data or disrupt critical systems.

Mitigation:

- Implement access controls and follow the principle of least privilege (PoLP).
- Conduct regular security audits and monitor user activity for suspicious behavior.
- Foster a security-conscious culture and enforce strict policies for handling sensitive data.

Cyber threats continue to evolve, posing significant risks to individuals and organizations. By understanding their mechanisms, impacts, and mitigation strategies,

cybersecurity professionals can implement effective defense measures to protect digital assets and maintain a secure environment.

4.0 Cybersecurity Analyst Role

A **Cybersecurity Analyst** plays a crucial role in protecting an organization's digital assets by identifying, analyzing, and mitigating security threats. They are responsible for implementing security measures, monitoring network activity, responding to incidents, and proactively hunting for potential cyber threats. This section outlines the key responsibilities of a cybersecurity analyst.

4.1 Threat Detection

Role: A cybersecurity analyst continuously monitors an organization's network for potential threats using specialized security tools. This involves analyzing logs, detecting anomalies, and identifying indicators of compromise (IoCs).

Key Tasks:

- Utilize **Security Information and Event Management (SIEM)** systems to collect and analyze security logs.
- Detect and investigate unauthorized access attempts, malware infections, or suspicious user activities.
- Implement **Intrusion Detection Systems (IDS)** and **Intrusion Prevention Systems (IPS)** to identify and prevent cyber threats in real time.

4.2 Incident Response

Role: When a security breach occurs, a cybersecurity analyst follows a structured **Incident Response Plan (IRP)** to contain, mitigate, and recover from the attack.

Key Tasks:

- Identify and assess the scope of the security incident.
- Contain the attack by isolating affected systems to prevent further damage.
- Eradicate the root cause of the incident, such as removing malware or closing exploited vulnerabilities.
- Document findings and recommend preventive measures to avoid recurrence.

4.3 Vulnerability Management

Role: Cybersecurity analysts regularly assess an organization's IT infrastructure for security weaknesses and ensure vulnerabilities are patched before attackers can exploit them.

Key Tasks:

- Conduct **vulnerability assessments** using tools such as **Nessus, OpenVAS, and Qualys** to identify security gaps.
- Work with IT teams to apply security patches and updates to software and systems.
- Implement **penetration testing** strategies to simulate real-world attacks and uncover security flaws.
- Ensure compliance with industry security standards such as **ISO 27001, NIST, and CIS Controls**.

4.4 Threat Hunting

Role: Threat hunting is a proactive approach where cybersecurity analysts search for hidden threats within an organization's network before they cause harm. Unlike traditional threat detection, which relies on alerts, threat hunting involves manual investigations and hypothesis-driven analysis.

Key Tasks:

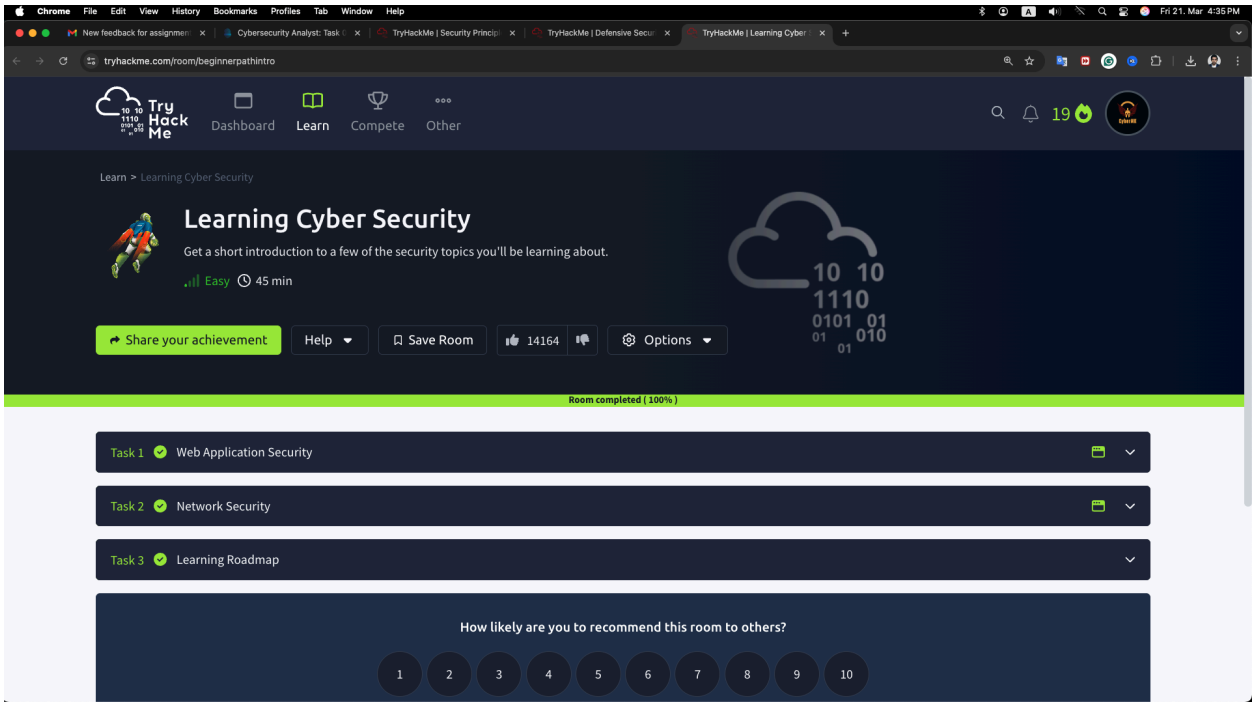
- Analyze **endpoint activity, network traffic, and user behavior** to detect signs of advanced persistent threats (APTs).

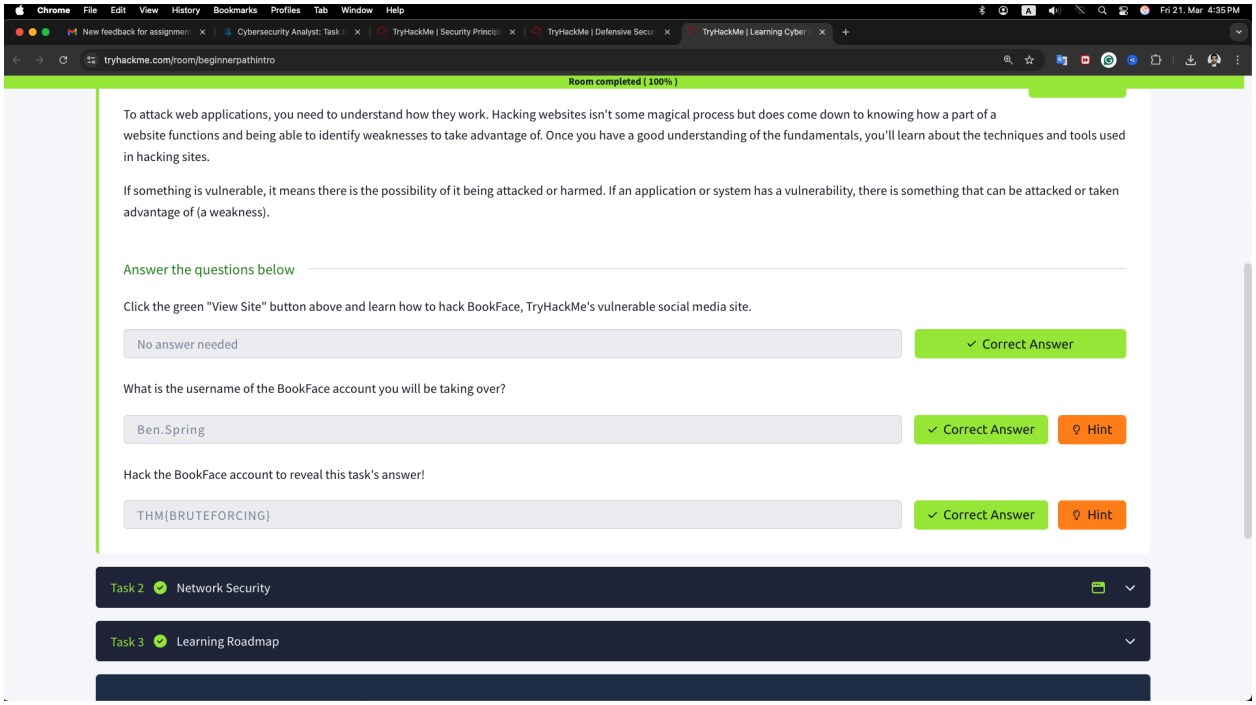
- Use **Threat Intelligence Feeds** to stay informed about emerging threats and attack techniques.
- Apply **behavioral analysis and machine learning tools** to uncover sophisticated cyber threats.
- Develop and refine security detection rules to enhance an organization's defensive capabilities.

The role of a cybersecurity analyst is critical in defending organizations against evolving cyber threats. By focusing on threat detection, incident response, vulnerability management, and threat hunting, analysts help maintain the integrity, confidentiality, and availability of digital assets. Continuous learning, hands-on experience, and proactive security measures are essential for effectively mitigating cyber risks.

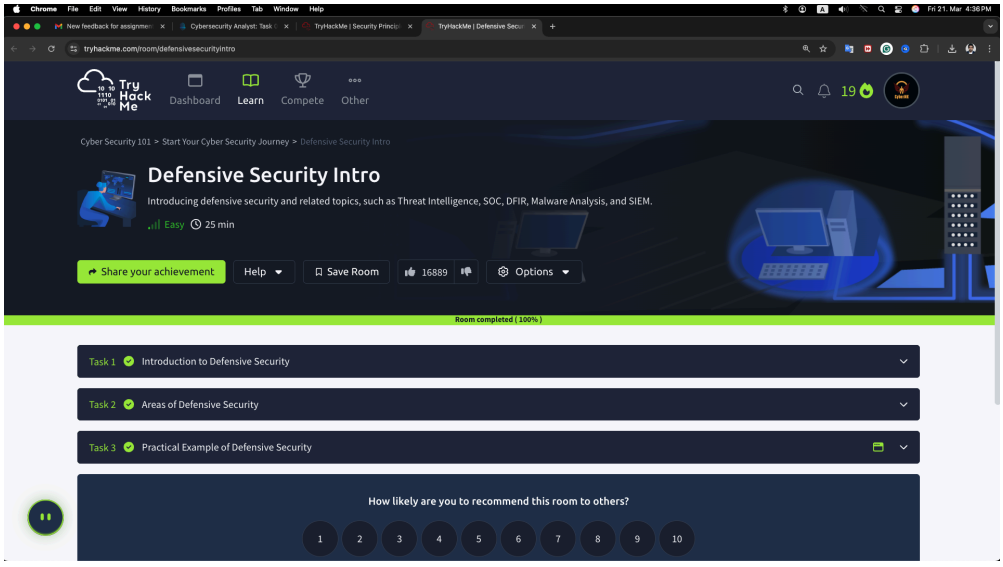
5.0 Lab Completion Screenshots

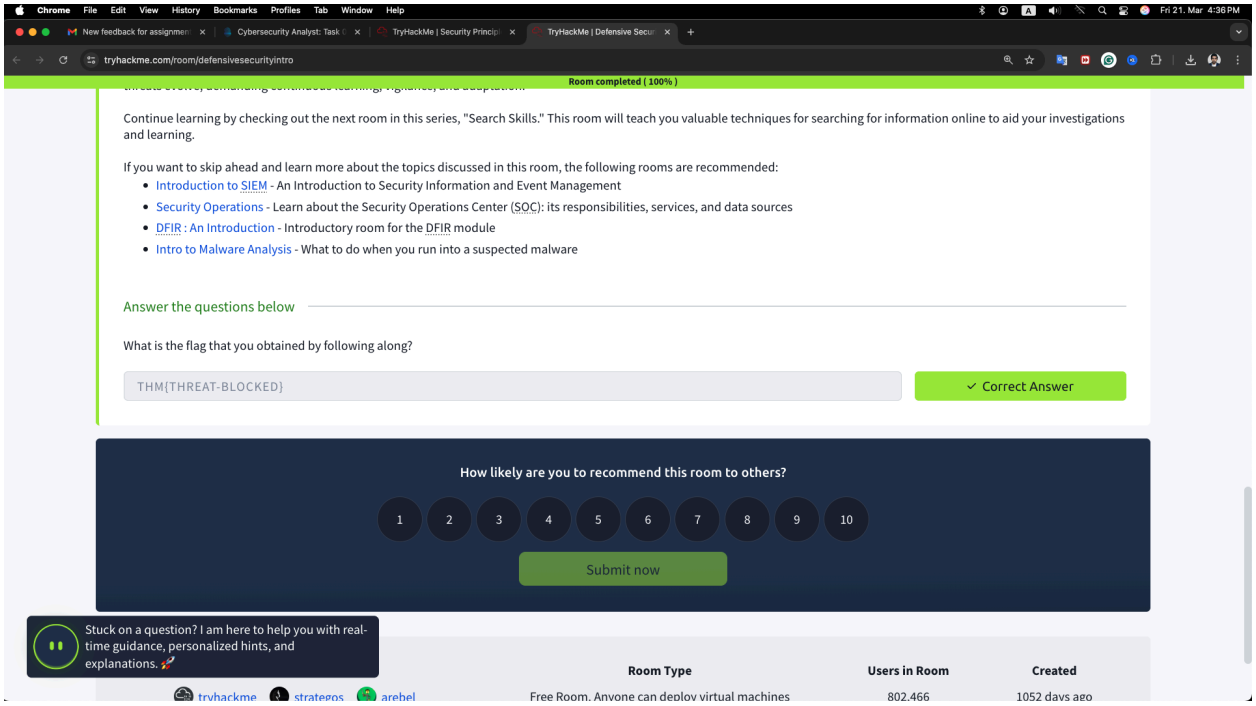
5.1 Learning Cybersecurity Lab



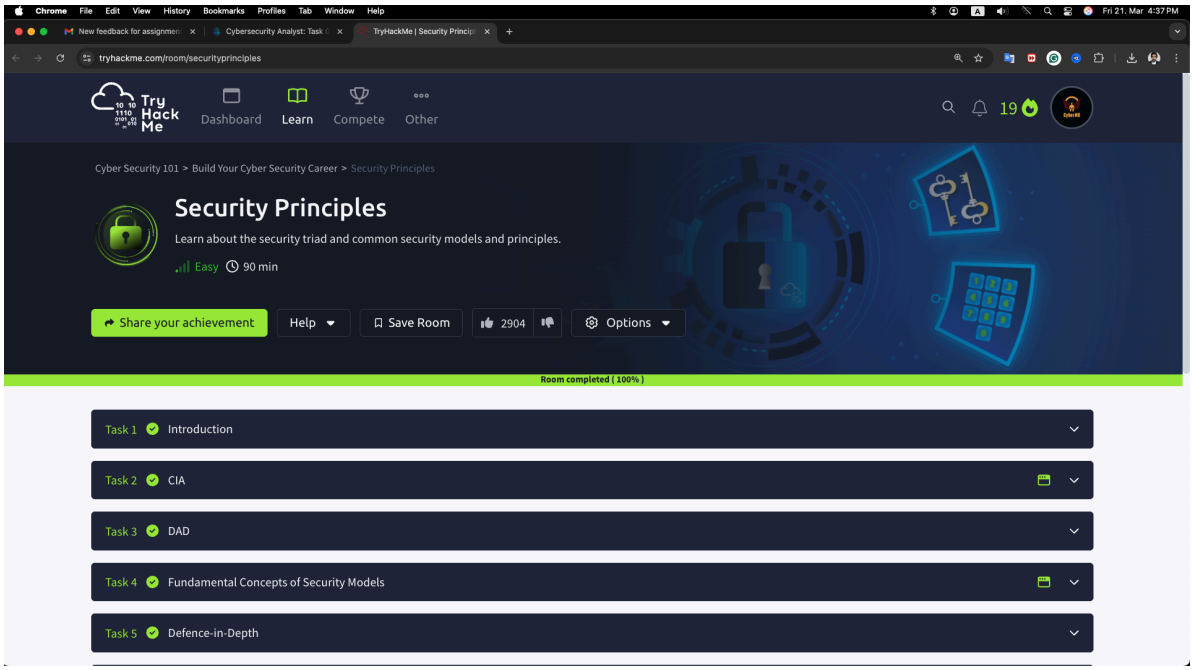


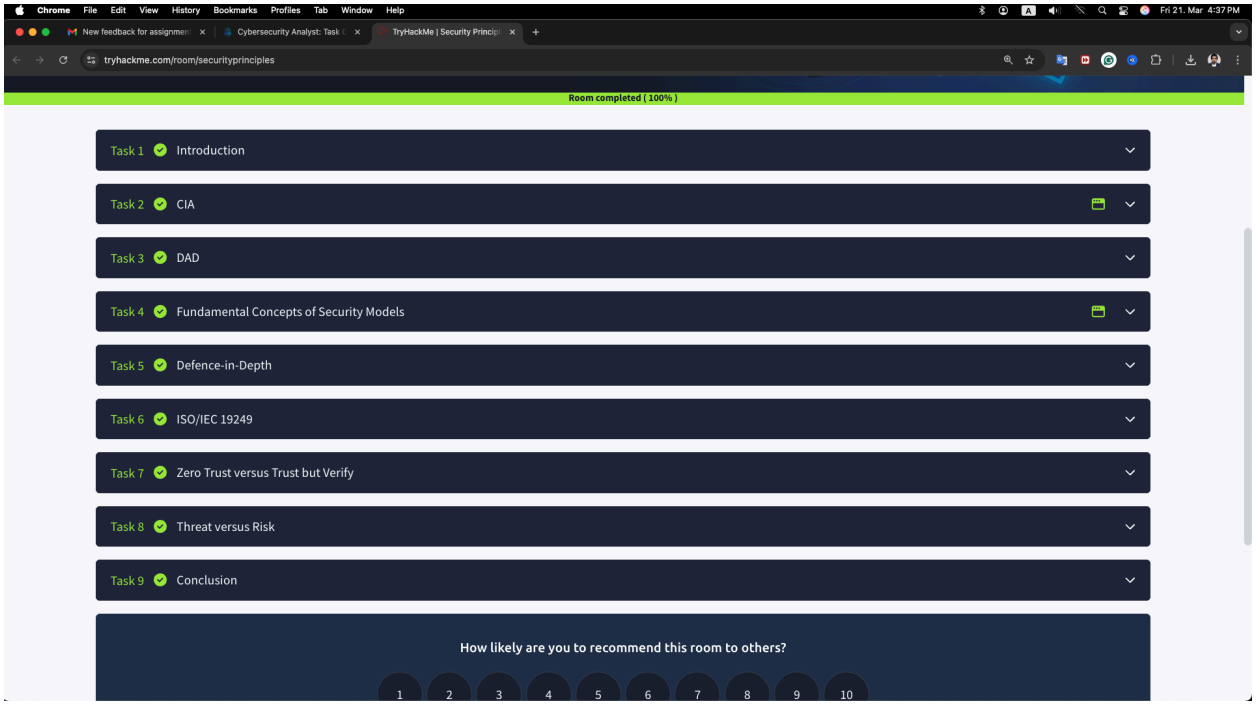
5.2 Intro to Defensive Security Lab

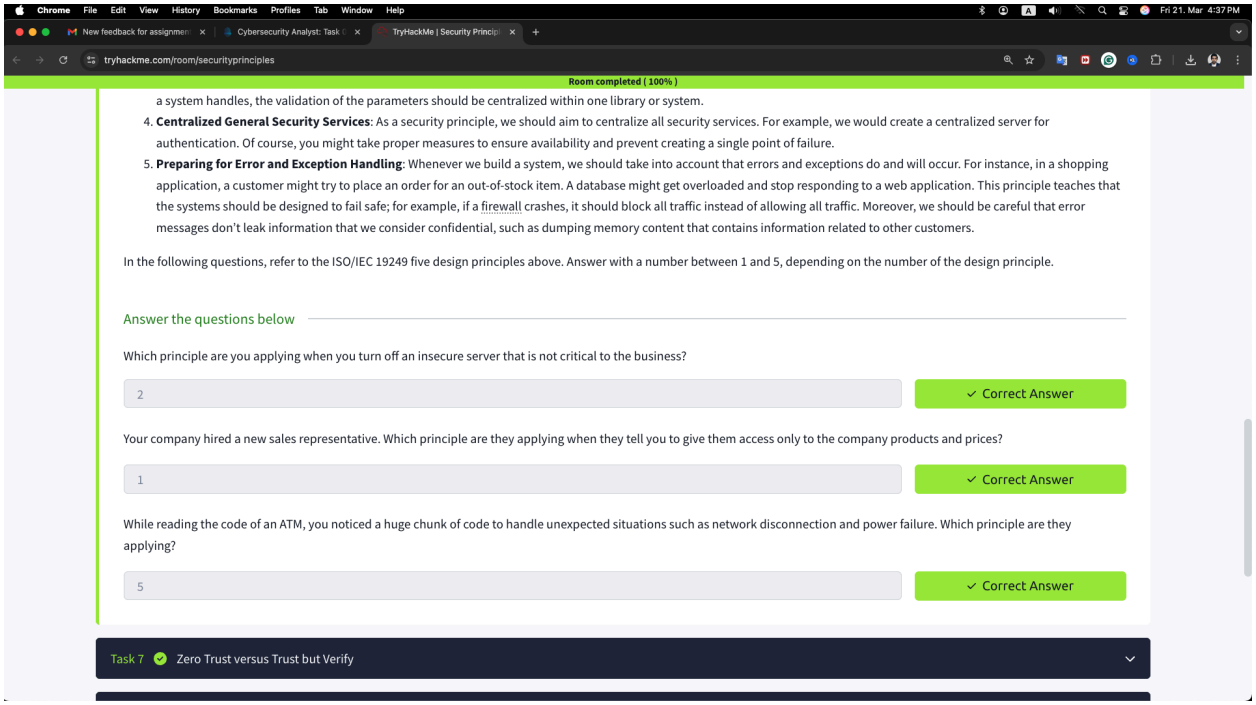




5.3 Security Principles Lab




Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri 21. Mar 4:37 PM
tryhackme.com/room/securityprinciples
Room completed (100%)
Task 1 Introduction
Task 2 CIA
Task 3 DAD
Task 4 Fundamental Concepts of Security Models
Task 5 Defence-in-Depth
Task 6 ISO/IEC 19249
Task 7 Zero Trust versus Trust but Verify
Task 8 Threat versus Risk
Task 9 Conclusion
How likely are you to recommend this room to others?
1 2 3 4 5 6 7 8 9 10


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Fri 21. Mar 4:37 PM
tryhackme.com/room/securityprinciples
Room completed (100%)
a system handles, the validation of the parameters should be centralized within one library or system.
4. **Centralized General Security Services**: As a security principle, we should aim to centralize all security services. For example, we would create a centralized server for authentication. Of course, you might take proper measures to ensure availability and prevent creating a single point of failure.
5. **Preparing for Error and Exception Handling**: Whenever we build a system, we should take into account that errors and exceptions do and will occur. For instance, in a shopping application, a customer might try to place an order for an out-of-stock item. A database might get overloaded and stop responding to a web application. This principle teaches that the systems should be designed to fail safe; for example, if a firewall crashes, it should block all traffic instead of allowing all traffic. Moreover, we should be careful that error messages don't leak information that we consider confidential, such as dumping memory content that contains information related to other customers.
In the following questions, refer to the ISO/IEC 19249 five design principles above. Answer with a number between 1 and 5, depending on the number of the design principle.
Answer the questions below
Which principle are you applying when you turn off an insecure server that is not critical to the business?
2
✓ Correct Answer
Your company hired a new sales representative. Which principle are they applying when they tell you to give them access only to the company products and prices?
1
✓ Correct Answer
While reading the code of an ATM, you noticed a huge chunk of code to handle unexpected situations such as network disconnection and power failure. Which principle are they applying?
5
✓ Correct Answer
Task 7 Zero Trust versus Trust but Verify

6.0 Reflection

During this task, I gained valuable insights into fundamental cybersecurity concepts, including key terminologies, various cyber threats, and the critical responsibilities of a cybersecurity analyst. The hands-on labs provided a practical understanding of real-world security scenarios, reinforcing theoretical knowledge with interactive challenges.

Understanding cyber threats such as malware, phishing, ransomware, and insider threats highlighted the importance of proactive security measures. Learning about mitigation strategies emphasized that cybersecurity is not just about defense but also about early detection and response. Additionally, exploring the role of a cybersecurity analyst shed light on the importance of continuous monitoring, threat hunting, and incident response in protecting an organization's digital assets.

This knowledge is highly relevant in today's cybersecurity landscape, where organizations face an increasing number of sophisticated cyber threats. The principles of confidentiality, integrity, and availability (CIA triad) are crucial for ensuring robust security. By applying these concepts, cybersecurity analysts play a vital role in safeguarding data, mitigating risks, and ensuring business continuity.

Overall, this task provided a strong foundation in cybersecurity and reinforced the importance of adopting a proactive and strategic approach to securing digital environments.

EncryptEdge Labs

This Internship Task report was developed on [March, 21, 2025]

By:

atalmamun@gmail.com