



TRYHACKME - Introduction to Cybersecurity Walkthrough

By h4kim

Offensive Security Intro

A screenshot of the TRYHACKME platform interface. At the top, there's a navigation bar with icons for cloud, user count (10), and the text "Try Hack Me". The main menu includes "Dashboard", "Learn", "Compete", and "Other". A green notification box in the top right corner says "Done! Room progress has been reset". Below the menu, the breadcrumb navigation shows "Introduction to Cyber Security > Introduction to Cyber Security > Offensive Security Intro". The main content area features a title "Offensive Security Intro" with a red and black stylized logo to its left. The description below the title reads "Hack your first website (legally in a safe environment) and experience an ethical hacker's job." It indicates the difficulty level as "Easy" and the estimated time as "15 min". There are buttons for "Help", "Save Room", "57946" (likely a score or rating), and "Options". On the right side of the screen, there's a dark-themed illustration of a computer setup with multiple monitors and server racks. At the bottom, a progress bar shows "Room progress (0%)".

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.

"To outsmart a hacker, you need to think like one."

This is the core of "Offensive Security." It involves breaking into computer systems, exploiting software bugs, and finding loopholes in systems to understand hacker tactics and enhance our system defences.

Beginning Your Learning Journey

In this TryHackMe room, you will be guided through hacking your first website in a legal and safe environment. The goal is to show you how an ethical hacker operates.

But before we do that, let's review by answering the questions below. Type your answer in the text box after the question and click the "Submit" button. When you're done, proceed to Task 2.

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

Offensive Security ✓ Correct Answer ✗ Hint

Task 2 Hacking your first machine

Task 3 Careers in cyber security

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.

Your mission is to transfer \$2000 from bank account 2276 to your account (account number 8881). If your transfer was successful, you should now be able to see your new balance reflected on your account page.

Go there now and confirm you got the money! (You may need to hit Refresh for the changes to appear)

Answer the questions below

Above your account balance, you should now see a message indicating the answer to this question. Can you find the answer you need?

BANK-HACKED ✓ Correct Answer ✗ Hint

If you were a penetration tester or security consultant, this is an exercise you'd perform for companies to test for vulnerabilities in their web applications and find hidden pages to investigate for vulnerabilities.

No answer needed ✗ Complete

Terminate the machine by clicking the red "Terminate" button at the top of the page.

No answer needed ✗ Complete

FakeBank | Accounts

Mrs G. Benjamin
Bank Account Number: 8881

Accounts

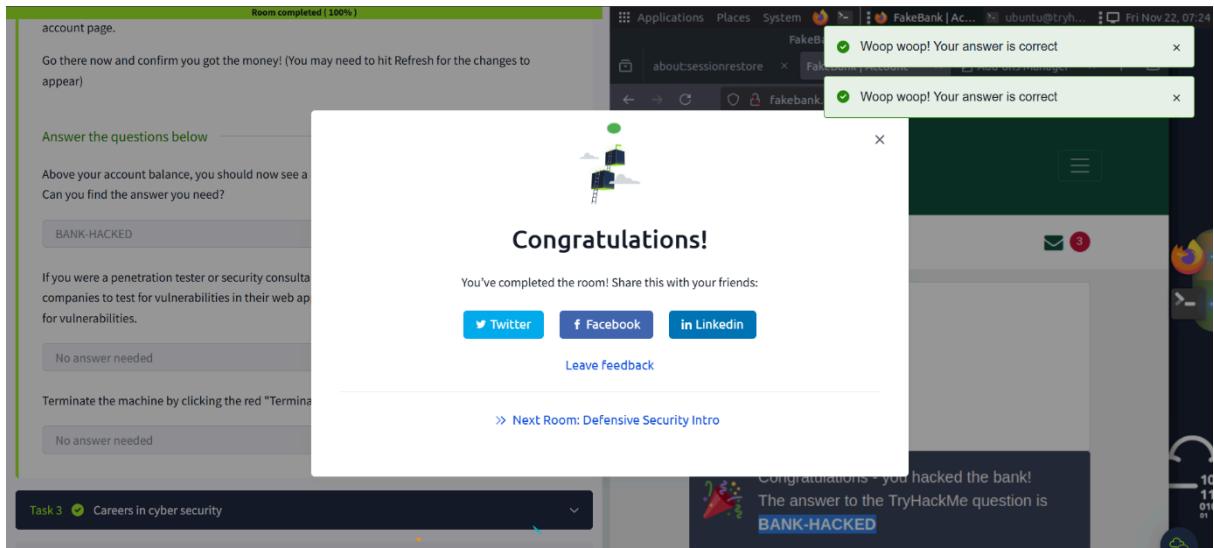
	Classic Account	\$3,767.68
	Credit Card	\$0.00

Congratulations - you hacked the bank!
The answer to the TryHackMe question is **BANK-HACKED**

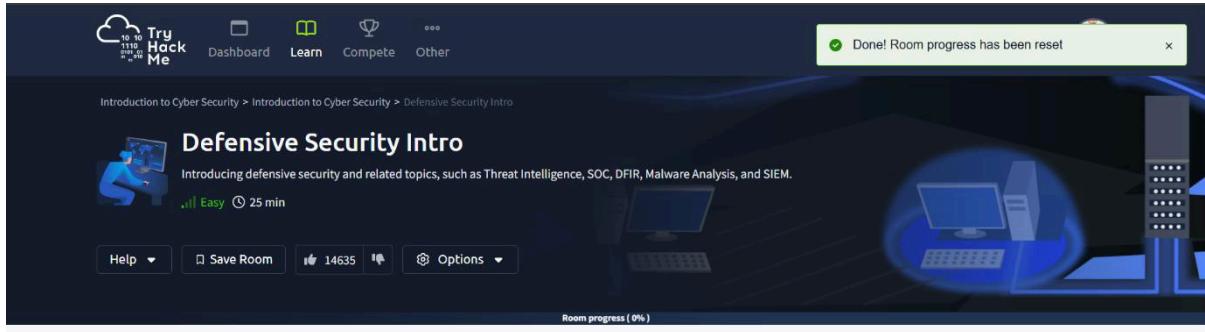
Task 3: Careers in Cybersecurity

- **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.

Room progress (20%)

- User cyber security awareness: Training users about cyber security helps protect against attacks targeting their systems.
- Documenting and managing assets: We need to know the systems and devices we must manage and protect adequately.
- Updating and patching systems: Ensuring that computers, servers, and network devices are correctly updated and patched against any known vulnerability (weakness).
- Setting up preventative security devices: firewall and intrusion prevention systems (IPS) are critical components of preventative security. Firewalls control what network traffic can go inside and what can leave the system or network. IPS blocks any network traffic that matches present rules and attack signatures.
- Setting up logging and monitoring devices: Proper network logging and monitoring are essential for detecting malicious activities and intrusions. If a new unauthorized device appears on our network, we should be able to detect it.

There is much more to defensive security. Aside from the above, we will also cover the following related topics:

- Security Operations Center (SOC)
- Threat Intelligence
- Digital Forensics and Incident Response (DFIR)
- Malware Analysis

Answer the questions below

Which team focuses on defensive security?

Blue Team ✓ Correct Answer

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.

Malware analysis aims to learn about such malicious programs using various means:

1. Static analysis works by inspecting the malicious program without running it. This usually requires solid knowledge of assembly (computer's fundamental instructions).
2. Dynamic analysis works by running the malware in a controlled environment and monitoring its activities. It lets you observe how the malware behaves when running.

Answer the questions below

What would you call a team of cyber security professionals that monitors a network and its systems for malicious events?

Security Operations Center ✓ Correct Answer

What does DFIR stand for?

Digital Forensics and Incident Response ✓ Correct Answer

Which kind of malware requires the user to pay money to regain access to their files?

Ransomware ✓ Correct Answer

Task 3 Practical Example of Defensive Security

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.

In this room, we've discussed the different subfields (SOC, Threat Intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in the series: [A Day In the Life of a Junior SIEM Analyst](#).

If you want to skip ahead and learn more about the other rooms in the series, here are some recommended:

- [Introduction to SIEM - An Introduction to Security Information and Event Management](#)
- [Security Operations - Learn about the Security Operations Center \(SOC\), threat intelligence services, and data sources](#)
- [DFIR : An Introduction - Introductory room for Digital Forensics and Incident Response](#)
- [Intro to Malware Analysis - What to do when you find a malicious file](#)

Answer the questions below

What is the flag that you obtained by following along?

THM[THREAT-BLOCKED]

Challenge Complete

Woop woop! Your answer is correct

A Day In the Life of a Junior SIEM Analyst

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook LinkedIn

Leave feedback

Next Room: Careers in Cyber

Created by tryhackme, strategos, arebel

Room Type Users in Room Created

Defensive Security

Careers in Cyber

Introduction to Cyber Security > Introduction to Cyber Security > Careers in Cyber

Careers in Cyber

Learn about the different careers in cyber security.

Info 30 min

Options

Help Save Room 8998 Options

Room progress (0%)

Done! Room progress has been reset

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.

Room progress (11%)

Cyber security careers are becoming more in demand and offer [high salaries](#). There are many different jobs within the security industry, from offensive pentesting (hacking machines and reporting on vulnerabilities) to defensive security (defending against and investigating cyberattacks).

Why get a career in cyber:

- High Pay - jobs in security have high starting salaries
- Exciting - work can include legally hacking systems or defending against cyber attacks
- Be in demand - there are over 3.5 million unfilled cyber positions

This room helps you break into cyber security by providing information about various cyber security roles; it also links to different learning paths that you can use to start building your cyber skills.

Answer the questions below

Let's start exploring the different roles in cyber security!

No answer needed ✓ Correct Answer

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.

Room progress (22%)

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a security analyst.

• [Introduction to Cyber Security](#)
• [Pre Security](#)
• [SOC Level 1](#)

Relevant Career Guides

• [Becoming a Cyber Security Analyst](#)
• [How to Become a Level 1 SOC Analyst](#)
• [A Day in the Life of a SOC Analyst](#)
• [The Ultimate SOC L1 Analyst Interview Guide](#)
• [From Student to SOC Analyst: Hayden's Success Story](#)

Answer the questions below

Read about what a security analyst does.

No answer needed ✓ Correct Answer

Task 3 Security Engineer

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.

Room progress (33%)

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Security Engineer.

- SOC Level 1
- JR Penetration Tester
- Offensive Pentesting

Relevant Career Guides

- Becoming a Security Engineer
- How to Become a Security Engineer
- A Day in the Life of a Security Engineer
- Preparing for a Security Engineering Interview
- Becoming a Security Engineer: Richard's Success Story

Answer the questions below

Read about what a security engineer does.

No answer needed ✓ Correct Answer

Task 4 Incident Responder

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.

Room progress (44%)

Identifies and mitigates attacks whilst an attacker's operations are still unfolding ✓ Woop woop! Your answer is correct

Incident responders respond productively and efficiently to security breaches. Responsibilities include creating plans, policies, and protocols for organisations to enact during and following incidents. This is often a highly pressurised position with assessments and responses required in real-time, as attacks are unfolding. Incident response metrics include MTTD, MTTR, and MTTR - the meantime to detect, acknowledge, and recover (from attacks.) The aim is to achieve a swift and effective response, retain financial standing and avoid negative breach implications. Ultimately, incident responders protect the company's data, reputation, and financial standing from cyber attacks.

Responsibilities

- Developing and adopting a thorough, actionable incident response plan
- Maintaining strong security best practices and supporting incident response measures
- Post-incident reporting and preparation for future attacks, considering learnings and adaptations to take from incidents

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Incident Responder.

- SOC Level 1

Answer the questions below

Read about what an incident responder does.

No answer needed ✓ Correct Answer

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.

Room progress (55%)



Woop woop! Your answer is correct

Responsible for using digital forensics to investigate incidents and crimes

If you like to play detective, this might be the perfect job. If you are working as part of a law-enforcement department, you would be focused on collecting and analysing evidence to help solve crimes: charging the guilty and exonerating the innocent. On the other hand, if your work falls under defending a company's network, you will be using your forensic skills to analyse incidents, such as policy violations.

Responsibilities

- Collect digital evidence while observing legal procedures
- Analyse digital evidence to find answers related to the case
- Document your findings and report on the case

Answer the questions below

Read about what a digital forensics examiner does.

No answer needed ✓ Correct Answer

Task 6 Malware Analyst

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.

Room progress (60%)



Woop woop! Your answer is correct

Analyses all types of malware to learn more about how they work and what they do

A malware analyst's work involves analysing suspicious programs, discovering what they do and writing reports about their findings. A malware analyst is sometimes called a reverse-engineer as their core task revolves around converting compiled programs from machine language to readable code, usually in a low-level language. This work requires the malware analyst to have a strong programming background, especially in low-level languages such as assembly language and C language. The ultimate goal is to learn about all the activities that a malicious program carries out, find out how to detect it and report it.

Responsibilities

- Carry out static analysis of malicious programs, which entails reverse-engineering
- Conduct dynamic analysis of malware samples by observing their activities in a controlled environment
- Document and report all the findings

Answer the questions below

Read about what a malware analyst does.

No answer needed ✓ Correct Answer

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.

Room progress (77%)

- Perform security assessments, audits, and analyse policies
- Evaluate and report on insights, recommending actions for attack prevention

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Penetration Tester.

- JR Penetration Tester
- Offensive Pentesting

Relevant Career Guides

- Becoming a Penetration Tester
- How to Become a Penetration Tester
- Preparing for a Junior Penetration Tester Interview
- From IT Support to Pentester: Tom's Success Story

Answer the questions below

Read about what a penetration tester does.

No answer needed ✓ Correct Answer

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.

Room progress (77%)

- Perform security assessments, audits, and analyse policies
- Evaluate and report on insights, recommending actions for attack prevention

Learning Paths

TryHackMe's learning paths will give you both the fundamental technical knowledge and hands-on experience, which is crucial to becoming a successful Penetration Tester.

- JR Penetration Tester
- Offensive Pentesting

Relevant Career Guides

- Becoming a Penetration Tester
- How to Become a Penetration Tester
- Preparing for a Junior Penetration Tester Interview
- From IT Support to Pentester: Tom's Success Story

Answer the questions below

Read about what a penetration tester does.

No answer needed ✓ Correct Answer

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.

This room has provided you with a general overview of the different careers in cyber security. Don't forget that you can leverage online training to land your dream job in cyber security. To find out which cyber security role suits you best, try our fun quiz, which you can access by clicking the "View Site" button on the right.

Answer the questions below

Complete the careers quiz and share your chosen job!

No answer needed ✓ Correct Answer

Created by tryhackme strategos

Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed)! **Users in Room** 486,636 **Created** 926 days ago

Copyright TryHackMe 2018-2024

Learn about the different [cyber security career roles](#)

JR PENETRATION TESTER

OFFENSIVE PENTESTING

Share

Do Cyber Careers Quiz

Web Application Security

Introduction to Cyber Security > Introduction to Offensive Security > Web Application Security

Web Application Security

Learn about web applications and explore some of their common security issues.

Easy 90 min

Share your achievement Help Save Room Options

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.

Room completed (100%)

Many companies offer bug bounty programs. A bug bounty program allows the company to offer a reward for anyone who discovers a security vulnerability (weakness) in the company's systems. The main condition is that the found vulnerability is within the bug bounty scope and rules. Among many others, Google, Microsoft, and Facebook have bug bounty programs. Discovering a bug can earn you from a few hundred USD to tens of thousands of USD, depending on the severity of the vulnerability, i.e., the weakness you discovered.

Answer the questions below

What do you need to access a web application?

Browser ✓ Correct Answer

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.

Room progress (75%)

Woop woop! Your answer is correct

Don't worry if these techniques look challenging or sophisticated at first. TryHackMe has dedicated in-depth rooms to help you understand and experiment with the various attacks against web applications.

Answer the questions below

You discovered that the login page allows an unlimited number of login attempts without trying to slow down the user or lock the account. What is the category of this security risk?

Identification and Authentication Failure ✓ Correct Answer

You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk?

Cryptographic Failures ✓ Correct Answer

Task 3 Practical Example of Web Application Security

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.

Room completed (100%)

guess that there are also `IMG_1002.JPG` and `IMG_1004.JPG`; however, the web application should not provide us with that image even if we figured out its name. In general, an IDOR vulnerability can occur if too much trust has been placed on that input data. In other words, the web application does not validate whether the user has permission to access the requested object.

Just providing the correct URL for a user or a product does not necessarily mean the user should be able to access that URL. For instance, consider the product page `https://store.tryhackme.thm/products/product?id=52`. We can expect this URL to provide details about product number `52`. In the database, items would be assigned numbers sequentially. The attacker would try other numbers such as `51` or `53` instead of `52`; this might reveal other retired or unreleased products if the web application is vulnerable.

Let's consider a more critical example; the URL `https://store.tryhackme.thm/customers/user?id=16` would return the user with `id=16`. Again, we expect the users to have sequential ID numbers. The attacker would try other numbers and possibly access other user accounts. This vulnerability might work with sequential files; for instance, if the attacker sees `007.txt`, the attacker might try other numbers such as `001.txt`, `006.txt`, and `008.txt`. Similarly, if you were ID number 16 and ID number 17 was another user, by changing the ID to 17, you could see sensitive data that belongs to another user. Likewise, they can change the ID to 16 and see sensitive data that belongs to you. (Of course, we assume here that the system is vulnerable to IDOR.)

Click on "View Site," and let's see this in action. You will see a page showing an Inventory Management System. If you click on the "Planned Shipments" tab, you will discover that an attacker has managed to mix things up as part of sabotage plans. Notice how they send the wrong tires to each assembly line; for instance, they assign scooter tires and motorcycle tires to bike assembly! If left unfixed, all tires will go to the wrong assembly.

We will hack the system back and undo the attacker's steps. On "Your Activity," you can see the activity of one of the users. We have reason to believe that this website has an IDOR vulnerability.

Answer the questions below

Check the other users to discover which user account was used to make the malicious changes and revert them. After reverting the changes, what is the flag that you have received?

THM[IDOR_EXPLORED]

✓ Correct Answer ? Hint

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.

Room progress (20%)



In the next task, we will discuss common attacks against these security pillars.

Answer the questions below

Which of the following is **not** an operating system?

- AIX
- Android
- Chrome OS
- Solaris
- Thunderbird

Thunderbird

✓ Correct Answer

Task 2 Common Examples of OS Security

Woop woop! Your answer is correct

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.

Room progress (40%)



Some types of malicious programs, such as Trojan horses, give the attacker access to your system. Consequently, the attacker would be able to read your files or even modify them.

Some types of malicious programs attack availability. One such example is ransomware. Ransomware is a malicious program that encrypts the user's files. Encryption makes the file(s) unreadable without knowing the encryption password; in other words, the files become gibberish without decryption (reversing the encryption). The attacker offers the user the ability to restore availability, i.e., regain access to their original files: they would give them the encryption password if the user is willing to pay the "ransom."

Answer the questions below

Which of the following is a strong password, in your opinion?

- iloveyou
- 1q2w3e4r5t
- LearnM00r
- qwertyuiop

LearnM00r

✓ Correct Answer

💡 Hint

Woop woop! Your answer is correct

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.

Room progress (60%)

We know that both of these users have little regard for cybersecurity best practices. We can use several ways to guess the passwords for these two users. Here we list two approaches:

- If you are **not** logged in as **sammie** or any other user, you can use `ssh johnny@10.10.159.254` and manually try one password after the next to see which password works for **johnny**.
- If you are logged in as **sammie** or any other user, you can use `su - johnny` and manually try one password after the next to see which password works for **johnny**.

Answer the questions below

Based on the top 7 passwords, let's try to find Johnny's password. What is the password for the user **johnny**?

✓ Correct Answer ✗ Hint

Once you are logged in as Johnny, use the command `history` to check the commands that Johnny has typed. We expect Johnny to have mistakenly typed the `root` password instead of a command. What is the root password?

✗ Submit ✗ Hint

While logged in as Johnny, use the command `su - root` to switch to the `root` account. Display the contents of the file `flag.txt` in the `root` directory. What is the content of the file?

✗ Submit ✗ Hint

Fri 22 Nov, 10:25 **AttackBox IP:10.10.151.228**

Woop woop! Your answer is correct

johnny@beginner-os-security:~

File Edit View Search Terminal Help

System information as of Fri 22 Nov 10:25:27 UTC 2024

```
System load: 0.14 Processes: 118
Usage of /: 54.3% of 6.53GB Users logged in: 1
Memory usage: 23% IPv4 address for eth0: 10.10.159.254
Swap usage: 0%
```

* Super-optimized for small spaces - read how we shrank the memory footprint of MicroK8s to make it the smallest full K8s around.
<https://ubuntu.com/blog/microk8s-memory-optimisation>

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Mar 2 08:30:34 2022 from 10.20.30.1
johnny@beginner-os-security:~

THM AttackBox 1h 55min 22s

Room completed (100%)

If you are logged in as **sammie** or any other user, you can use `su - johnny` and manually try one password after the next to see which password works for **johnny**.

Answer the questions below

Based on the top 7 passwords, let's try to find Johnny's password. What is the password for the user **johnny**?

✓ Correct Answer ✗ Hint

Once you are logged in as Johnny, use the command `history` to check the commands that Johnny has typed. We expect Johnny to have mistakenly typed the `root` password instead of a command. What is the root password?

✓ Correct Answer ✗ Hint

While logged in as Johnny, use the command `su - root` to switch to the `root` account. Display the contents of the file `flag.txt` in the `root` directory. What is the content of the file?

✓ Correct Answer ✗ Hint

Fri 22 Nov, 10:28 **AttackBox IP:10.10.151.228**

Woop woop! Try swithc to root!

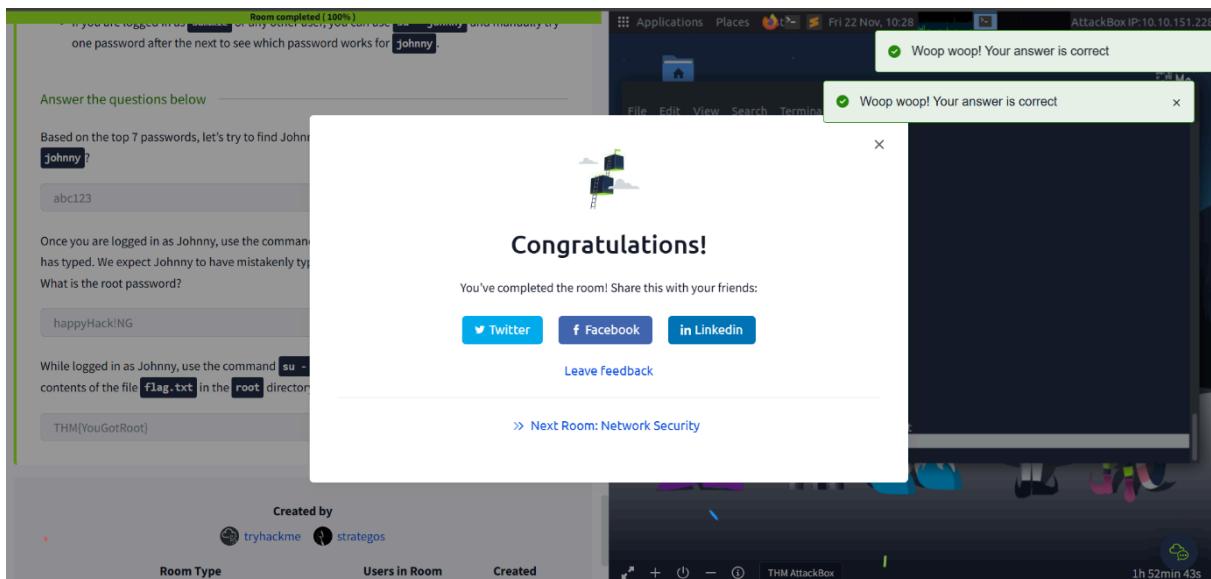
root@beginner-os-security:~

File Edit View Search Terminal Help

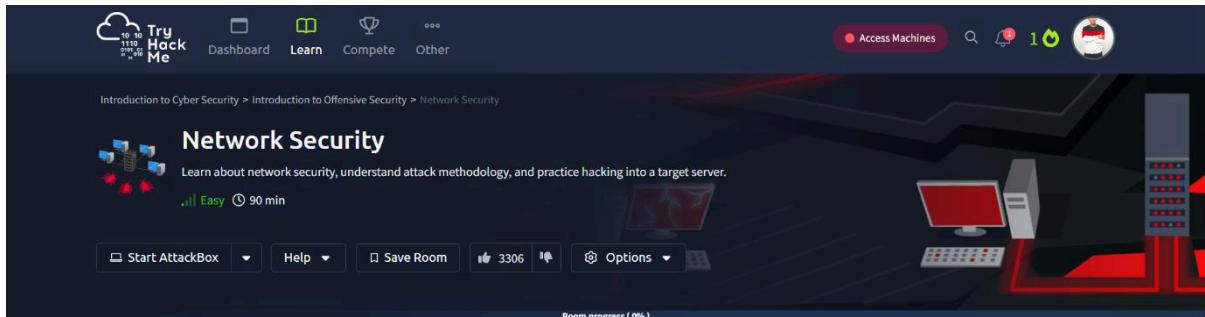
```
11 ls
12 cat coffee.txt
13 whoami
14 pwd
15 date
16 exit
17 history
johnny@beginner-os-security:~$ su -root
su: Invalid option -- 'r'
Try 'su --help' for more information.
johnny@beginner-os-security:~$ sudo -i
[sudo] password for johnny:
Sorry, try again.
[sudo] password for johnny:
Sorry, try again.
[sudo] password for johnny:
sudo: 3 incorrect password attempts
johnny@beginner-os-security:~$ su - root
Password:
root@beginner-os-security:~# ls
flag.txt snap
root@beginner-os-security:~# cat flag.txt
THM[YouGotRoot]
root@beginner-os-security:~#
```

THM AttackBox 1h 52min 30s

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.

In this room, we've discussed the different subfields (SOC, Threat intelligence, Malware Analysis, and DFIR) and experienced firsthand how to deal with alerts in a simulated SIEM environment. While we've covered a lot, the depth and complexity of this field mean there's more to learn and explore. The lessons learned here will serve as your foundation as cyber threats evolve, demanding continuous learning, vigilance, and adaptation.

Continue learning by checking out the next room in this series, "Search Skills." This room will teach you valuable techniques for searching for information online to aid your investigations and learning.

If you want to skip ahead and learn more about the topics discussed in this room, the following rooms are recommended:

- [Introduction to SIEM](#) - An Introduction to Security Information and Event Management
- [Security Operations](#) - Learn about the Security Operations Center (SOC): its responsibilities, services, and data sources
- [DFIR : An Introduction](#) - Introductory room for the DFIR module
- [Intro to Malware Analysis](#) - What to do when you run into a suspected malware

Answer the questions below

What is the flag that you obtained by following along?

✓ Correct Answer

Created by tryhackme strategos arebel

Room Type Users in Room Created

— | Defensive Security

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.

According to the [Cost of a Data Breach Report 2021](#) by IBM Security, a data breach in 2021 cost a company \$4.24 million per incident. The average cost changes with the sector and the country. For example, the average total cost for a data breach was \$9.23 million for the healthcare sector, while \$3.79 million for the education sector.

Answer the questions below

What type of firewall is Windows Defender Firewall?

✓ Correct Answer

Task 2 Methodology

Task 3 Practical Example of Network 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.

Room progress (40%)

Woop woop! Your answer is correct

Another analogy would be a thief interested in a target house. The thief will spend some time learning about the target house, who lives there, when they leave, and when they return home. The thief will determine whether they have security cameras and alarm systems. Once enough information has been gathered, the thief will plan the best entrance strategy. Physical theft planning and execution resemble, in a way, the malicious attack that aims to break into a network and steal data.

In the next task, we will carry out a practical example of the Cyber Kill Chain.

Answer the questions below

During which step of the Cyber Kill Chain does the attacker gather information about the target?

Recon

✓ Correct Answer

Task 3 Practical Example of Network Security

Room completed (100%)

Let's summarize what we have done in this task to get `root` access on the target system of IP address `10.10.211.82`:

1. We used `nmap` to learn about the running services.
2. We connected to the FTP server to learn more about the system.
3. We discovered a file containing the root password.
4. We used the password we found, allowing us to gain root access.
5. We gained access to all the users' files.

Answer the questions below

What is the password in the `secret.txt` file?

ABC789xyz123

What is the content of the `flag.txt` in the `/root` directory?

THM{FTP_SERVER OWNED}

What is the content of the `flag.txt` in the `/home/` directory?

THM{LIBRARIAN_ACCOUNT_COMPROMISED}

Woop woop! Your answer is correct

Congratulations!

You've completed the room! Share this with your friends:

Twitter Facebook LinkedIn

Leave feedback

>> Next Room: Intro to Digital Forensics

https://www.facebook.com/share.php?u=www.tryhackme.com%2Fr%2Froom%2Fintronetc... 1h 54min 7s

Intro to Digital Forensics

Try Hack Me

Dashboard Learn Compete Other

Introduction to Cyber Security > Introduction to Defensive Security > Intro to Digital Forensics

Intro to Digital Forensics

Learn about digital forensics and related processes and experiment with a practical example.

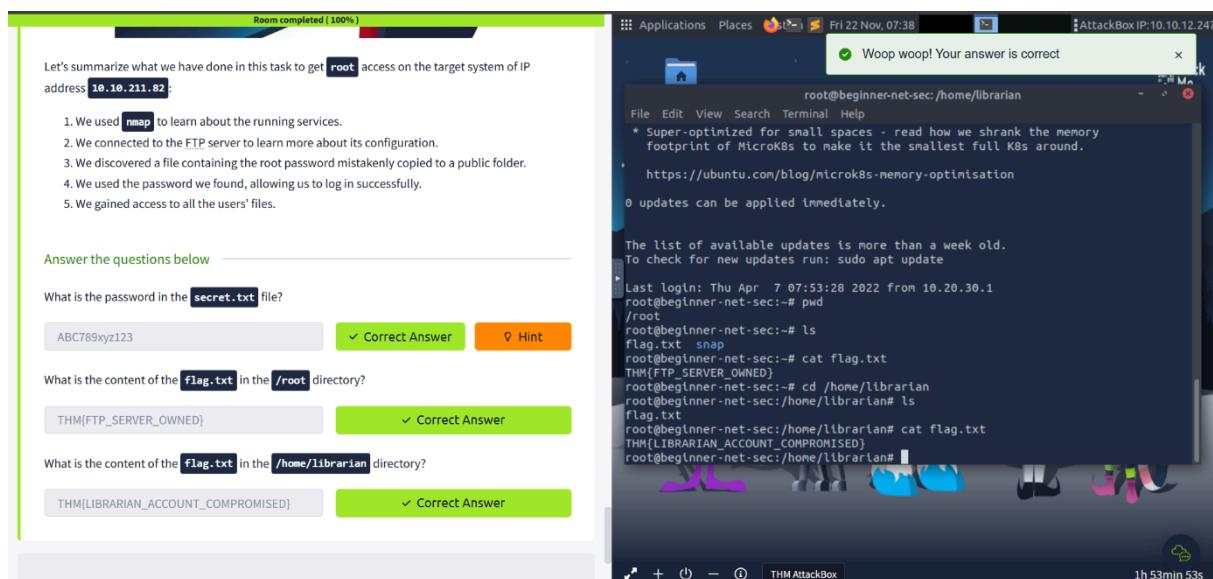
100% Complete | Easy | 90 min

Help Save Room Like 4571

Room progress (0%)

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.

Room progress (20%)

Woop woop! Your answer is correct

Answer the questions below

Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics?

laptop

✓ Correct Answer

💡 Hint

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.

Room progress (40%)

Woop woop! Your answer is correct

1. Retrieve the digital evidence from the secure container.
2. Create a forensic copy of the evidence: The forensic copy requires advanced software to avoid modifying the original data.
3. Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you can always create a new one.
4. Start processing the copy on your forensics workstation.

The above steps have been adapted from [Guide to Computer Forensics and Investigations, 6th Edition](#).

More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:

- Proper search authority: Investigators cannot commence without the proper legal authority.
- Chain of custody: This is necessary to keep track of who was holding the evidence at any time.
- Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.
- Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.
- Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.
- Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.

Answer the questions below

It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?

Chain of Custody

✓ Correct Answer

💡 Hint

Task 3 Practical Example of Digital Forensics

The screenshot shows two windows. The left window displays PDF metadata from a file named 'ransom-letter.pdf' with the following details:

```

Pages: 20
Encrypted: no
Page size: 595.32 x 841.92 pts (A4)
Page rot: 0
File size: 560362 bytes
Optimized: no
PDF version: 1.7

```

The right window shows terminal output for EXIF data extraction from an image file. The output includes various camera settings and GPS coordinates:

```

Megapixels : 0.960
Scale Factor To 35 mm Equivalent : 0.7
Shutter Speed : 1/200
Create Date : 2022:02:25 13:37:33.42+03:00
Date/Time Original : 2022:02:25 13:37:33.42+03:00
Modify Date : 2022:02:15 17:23:40+01:00
Thumbnail Image : (binary data 4941 bytes, use -b option to extract)
GPS Latitude : 51 deg 30' 51.90" N
GPS Longitude : 0 deg 5' 38.73" W
Date/Time Created : 2022:02:15 17:23:40-17:23
Digital Creation Date/Time : 2021:11:05 14:06:13+03:00
Circle Of Confusion : 0.043 mm
Depth Of Field : 0.06 mm (0.76 - 0.82 m)
Field Of View : 54.9 deg
Focal Length : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance : 20.58 m
Light Value : 7.9
Lens ID : Canon EF 50mm f/1.8 STM

```

Completion:

The screenshot shows a completed room interface. On the left, a terminal window shows the command 'exiftool IMAGE.jpg' and its output, which includes GPS coordinates. A central modal window displays a 'Congratulations!' message with the text: 'You've completed the room! Share this with your friends:' followed by social sharing buttons for Twitter, Facebook, and LinkedIn. Below the modal, there are links to 'Leave feedback' and '» Next Room: Security Operations'. The right side of the screen shows a terminal window with the same EXIF data as the previous screenshot.

Security Operations

The screenshot shows a digital learning platform interface. At the top, there are navigation icons for a tablet, three dots, a search bar, a user icon with a '1' and a green flame-like icon, and a profile picture of a person in a white shirt and red vest. Below the header, the breadcrumb navigation reads: 'Introduction to Cyber Security > Introduction to Defensive Security > Security Operations'. The main title 'Security Operations' is displayed in large, bold, white font. A descriptive subtitle below it says, 'Learn about Security Operations Center (SOC): its responsibilities, services, and data sources.' To the left of the title is a small illustration of two people in a control room. Below the title, there are two status indicators: 'Easy' with a green signal icon and '60 min' with a clock icon. At the bottom of the screen, there are several interactive buttons: 'Help ▾', 'Save Room', '2403' with a thumbs-up icon, 'Options ▾', and a progress bar labeled 'Room progress (0%)'.

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.

Room progress (50%)

protect a company against security threats and ensure compliance. What is considered a violation would vary from one company to another; examples include downloading pirated media files and sending confidential company files insecurely.

- **Detect intrusions:** *Intrusions* refer to system and network intrusions. One example scenario would be an attacker successfully exploiting our web application. Another example scenario would be a user visiting a malicious site and getting their computer infected.
- **Support with the incident response:** An *incident* can be an observation, a policy violation, an intrusion attempt, or something more damaging such as a major breach. Responding correctly to a severe incident is not an easy task. The *SOC* can support the incident response team handle the situation.

This room focuses on the *SOC* services and everyday work. We recommend that you finish the Introduction to Defensive Security room before going through this one.

Answer the questions below

What does SOC stand for?

Security Operations Center

✓ Correct Answer

How many hours a day does the SOC monitor the network?

24

✓ Correct Answer

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.

Room progress (40%)

1. Retrieve the digital evidence from the secure container.
2. Create a forensic copy of the evidence: The forensic copy requires advanced software to avoid modifying the original data.
3. Return the digital evidence to the secure container: You will be working on the copy. If you damage the copy, you can always create a new one.
4. Start processing the copy on your forensics workstation.

The above steps have been adapted from [Guide to Computer Forensics and Investigations, 6th Edition](#).

More generally, according to the former director of the Defense Computer Forensics Laboratory, Ken Zatyko, digital forensics includes:

- Proper search authority: Investigators cannot commence without the proper legal authority.
- Chain of custody: This is necessary to keep track of who was holding the evidence at any time.
- Validation with mathematics: Using a special kind of mathematical function, called a hash function, we can confirm that a file has not been modified.
- Use of validated tools: The tools used in digital forensics should be validated to ensure that they work correctly. For example, if you are creating an image of a disk, you want to ensure that the forensic image is identical to the data on the disk.
- Repeatability: The findings of digital forensics can be reproduced as long as the proper skills and tools are available.
- Reporting: The digital forensics investigation is concluded with a report that shows the evidence related to the case that was discovered.

Answer the questions below

It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?

Chain of Custody ✓ Correct Answer

Task 3 Practical Example of Digital Forensics

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.

Room progress (40%)

```
Pages: 28
Encrypted: no
Page size: 595.32 x 841.92 pts (A4)
Page rot: 0
File size: 560362 bytes
Optimized: no
PDF version: 1.7
```

The PDF metadata clearly shows that it was created using MS Word for Office 365 on October 10, 2018.

Answer the questions below

Using [pdfinfo](#), find out the author of the attached PDF file, [ransom-letter.pdf](#).

Ann Gee Shepherd ✓ Correct Answer

Photo EXIF Data

EXIF stands for Exchangeable Image File Format; it is a standard for saving metadata to image files. Whenever you take a photo with your smartphone or with your digital camera, plenty of information gets embedded in the image. The following are examples of metadata that can be found in the original digital images:

- Camera model / Smartphone model
- Date and time of image capture
- Photo settings such as focal length, aperture, shutter speed, and ISO settings

Basura@smashbox:~\$ exiftool -s *.JPG

File Edit View Search Terminal Help

```
Megapixels : 0.960
Scale Factor To 35 mm Equivalent: 0.7
Shutter Speed : 1/200
Create Date : 2022:02:15 13:37:33.42+03:00
Date/Time Original : 2022:02:15 13:37:33.42+03:00
Modify Date : 2022:02:15 17:23:40+01:00
Thumbnail Image : (Binary data 4941 bytes, use -b option to extract)
GPS Latitude : 51 deg 30' 51.90" N
GPS Longitude : 0 deg 5' 38.73" W
Date/Time Created : 2022:02:15 17:23:40-17:23
Digital Creation Date/Time : 2021:11:05 14:06:13+03:00
Circle Of Confusion : 0.043 mm
Depth Of Field : 0.06 m (0.76 - 0.82 m)
Field Of View : 54.9 deg
Focal Length : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance : 20.58 m
Light Value : 7.9
Lens ID : Canon EF 50mm f/1.8 STM
root@ip-10-10-162-224:~/Rooms/introdigitalforensics#
root@ip-10-10-162-224:~/Rooms/introdigitalforensics#
root@ip-10-10-162-224:~/Rooms/introdigitalforensics# ^C
root@ip-10-10-162-224:~/Rooms/introdigitalforensics#
```

1h 54min 37s

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 **172.16.4.1** to the destination port number **80** to the destination IP address **10.10.10.41** to the destination port number **80** will be passed.
- All IP packets from the source IP address **172.16.8.1** to the destination port number **80** to the destination IP address **10.10.10.81** to the destination port number **80** will be dropped.

Click on "View Site" to begin the simulation. As a member of the security team, you notice one malicious IP address attempting to connect to the server. It seems that they are targeting many different ports. It would be best if we block them at the firewall level.

Answer the questions below

Congratulations!

You've completed the room! Share this with your friends:

[Twitter](#) [Facebook](#) [LinkedIn](#)

Firewall Rules

the server!
K_BLOCKED

Source IP Address	Destination IP Address	Port	Action
0.110.1		22	DROP
0.110.1		80	DROP
0.110.1		3306	DROP