

Intro to Defensive Security | TryHackMe



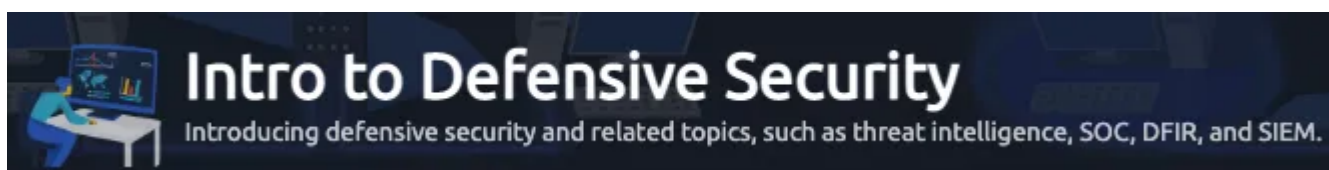
Aircon · Follow

8 min read · Jun 12, 2022

Listen

Share

More



Lab Access: <https://tryhackme.com/room/defensivesecurity>

Task 1 ○ Introduction to Defensive Security

Before we get into the “Defensive” side, let’s take a look at the “Offensive” side, which is all about **“breaking into systems.”**

- It could be accomplished, among other things, by exploiting defects, leveraging unsafe installations, and exploiting unenforced access control policies.
- Offensive security is handled by red teams and penetration testers.

Defensive Security — Basically the contrary of “offensive.”

1. **Preventing** intrusions from happening
2. **Detecting** and **responding** to intrusions when they occur



The following are some of the tasks associated with defensive security:

1. **User cyber security awareness** — Educating users about cyber security can help them secure their systems from a variety of attacks.
2. **Documenting and managing assets** — We must understand the many systems and gadgets that we must effectively manage and secure.
3. **Updating and patching systems** — Ensure that all computers, servers, and network devices are up to date and patched against any known vulnerabilities (weakness).
4. **Setting up preventative security devices** — Intrusion Prevention Systems (IPS) and firewalls are essential components of preventative security. Firewalls limit the amount of network traffic that can enter and depart a system or network. Any network traffic that matches the current rules and attack signatures is blocked by the IPS.
5. **Setting up logging and monitoring devices** — It will be impossible to discover malicious actions and attacks without effective network logging and monitoring. We should be able to detect any new illegal devices that come on our network.

In fact, the five pointers listed above are just a few of the nuggets; there are many more, including **Security Operations Center (SOC)**, **Threat Intelligence**, **Digital Forensics and Incident Response (DFIR)**, and **Malware Analysis**.

[Question 1.1] Which team focuses on defensive security?

Answer: Blue Team

Task 2 ○ Areas of Defensive Security

Security Operations Center (SOC) — It is carried out by a group of cyber security experts who **monitor the network and its systems** in order to **discover malicious cyber security events**.

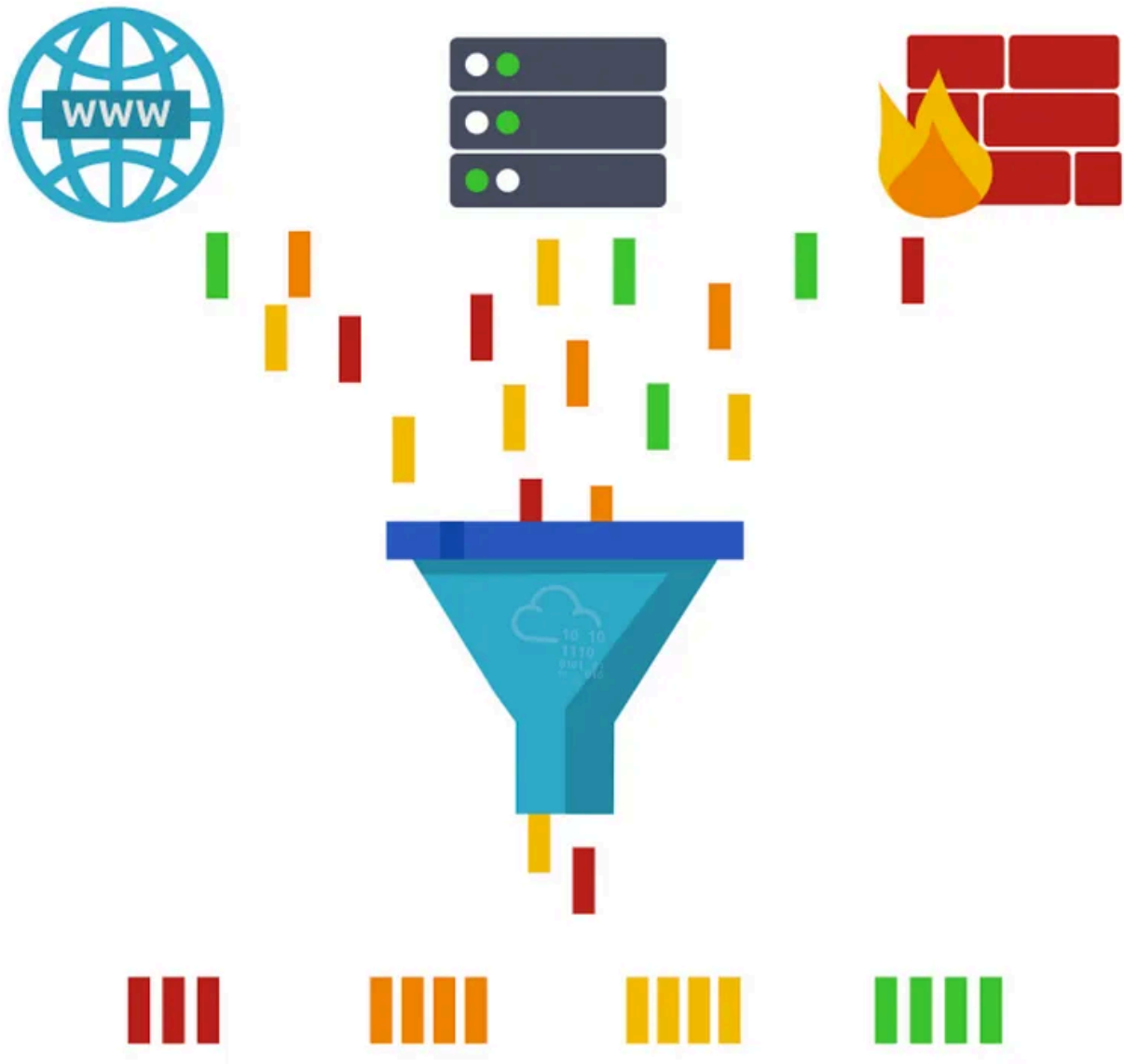
The following are some of the primary areas of interest for a SOC:

- **Vulnerabilities** — When a **system vulnerability (weakness)** is detected, it is critical to address it by applying a **patch or update**. When a remedy isn't available, take the appropriate precautions to prevent an attacker from exploiting the flaw. Although vulnerability remediation is important to a SOC, it is not always assigned to them.
- **Policy Violations** — A security policy is a set of rules that must be followed in order to protect the network and systems. Users **downloading confidential company data** to an internet storage site, for example, could be a policy violation.
- **Unauthorized Activity** — Consider the situation in which a **user's login name and password are stolen and used** by an attacker to gain access to the network. A SOC must recognize and block such an occurrence as quickly as possible to prevent further damage.
- **Network Intrusion** — There is always the possibility of an intrusion, no matter how solid your protection is. When a **user clicks on a malicious link or an**

attacker abuses a public server, an intrusion occurs. In either case, we must notice an infiltration as soon as possible to avoid further damage.



Threat Intelligence — It is accomplished through “Threat-Informed Defense,” which seeks to **acquire actual or possible intelligence to enable the organization to better prepare against future enemies**. Even though each attacker has a different objective, it is critical to obtain as much information as possible to avoid accidents from happening.



Data is required for intelligence.

- It is necessary to collect, process, and analyze data.
- Data is gathered from both local and public sources, such as network logs and forums.
- The goal of data processing is to organize data into a format that can be analyzed.
- The goal of the analysis phase is to learn more about the attackers and their motivations, as well as to compile a list of recommendations and practical activities.

You can **learn about your opponents' tactics, techniques, and procedures** by learning about them. Threat intelligence allows us to **identify the threat actor**

(adversary), **predict their behaviour**, and, as a result, **minimize their attacks and plan a response strategy**.

Digital Forensics and Incident Response (DFIR)

There are 3 components to this:

1. Digital Forensics
2. Incident Response
3. Malware Analysis

Digital Forensics — Science is used in forensics to investigate crimes and establish facts. With the widespread usage and adoption of digital devices such as computers and smartphones, a new field of forensics called computer forensics, which eventually evolved into digital forensics, was established to investigate associated crimes.

- Digital forensics now focuses on assessing evidence of an attack and its perpetrators, as well as additional issues including intellectual property theft, cyber espionage, and the possession of unlawful content.

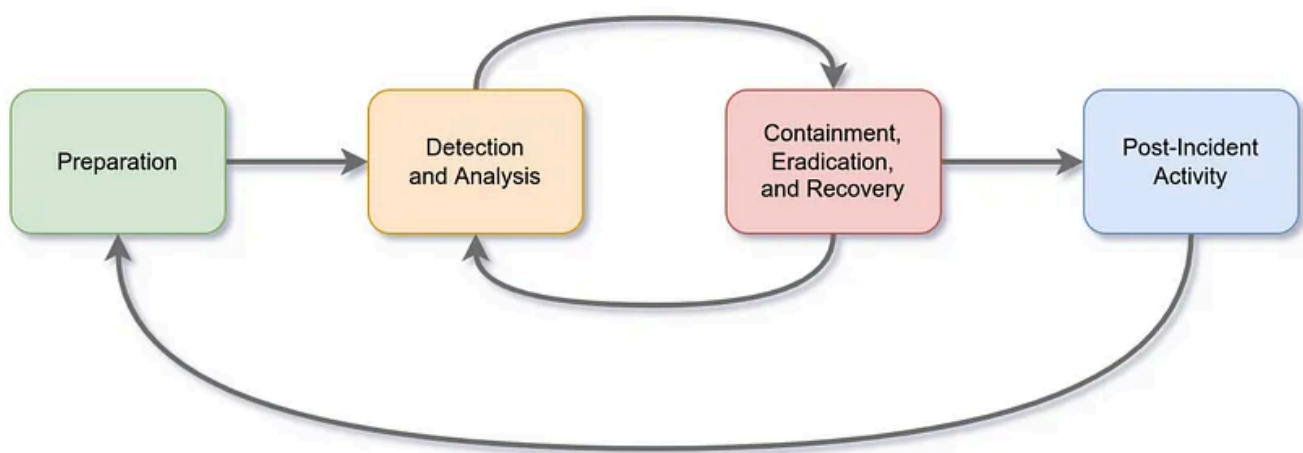
As a result, digital forensics will concentrate on a variety of topics, including:

1. **File System** — Analyzing a digital forensics image (low-level duplicate) of a system's storage exposes a wealth of information, including **installed programs, produced files, partially overwritten data, and deleted files**.
2. **System Memory** — If the attacker is running their malicious program in memory rather than writing it to disk, the **best way to evaluate its contents and learn about the attack is to create a forensic image (low-level copy) of the system memory**.
3. **System Logs** — Different log files about what is happening are kept on each client and server machine. Log files include a **wealth of information about what occurred on a computer system**. Even if the attacker tries to erase their traces, **some will remain**.
4. **Network Logs** — Logs of **network packets passing a network** would help in **answering more questions about whether or not an attack is taking place and**

what it comprises.

Incident Response — A data breach or cyber attack is typically referred to as an incident; however, it can also refer to something less serious, such as a misconfiguration, an infiltration attempt, or a policy violation.

- An attacker rendering our network or systems inaccessible, defacing (altering) the public website, and data leak are all examples of cyber attacks (stealing company data).
- What would you do if you were targeted by a cyber-attack? The mechanism for dealing with such a situation is defined by incident response.
- The goal is to minimize harm and recover as quickly as possible. In an ideal world, you'd prepare an incident response strategy ahead of time.



The incident response procedure is divided into four primary phases:

1. **Preparation** — This needs a team that has been trained and is ready to respond to incidents. In an ideal world, different procedures would be implemented to prevent accidents from occurring in the first place.
2. **Detection and Analysis** — The team has the resources to detect any issue; therefore, it is critical to investigate each discovered incident further to determine its seriousness.
3. **Containment, Eradication, and Recovery** — Once an incident has been identified, it is critical to stop it from spreading to other systems, eradicate it, and restore the systems that have been impacted. For example, if we discover that a system has been infected with a computer virus, we want to prevent the

virus from spreading to other systems, clean (eradicate) the virus, and ensure that the system is properly recovered.

4. **Post-Incident Activity** — After a successful recovery, a report is created, and the lesson learned is communicated in order to prevent similar situations in the future.

Malware Analysis — Malware is a term that refers to malicious software. Programs, documents, and data that you can save on a disk or send over the network are referred to as software.

The following are just a few examples of malware:

1. **Virus** — A piece of code (part of a program) that connects to another program. It is designed to spread from one machine to another; also, once infected, it modifies, overwrites, and deletes files. The computer may become slow or unusable as a result.
2. **Trojan Horse** — A program that displays one useful feature while concealing a dangerous feature underneath. A victim might, for example, download a video player from a dodgy website, giving the attacker complete access to their system.
3. **Ransomware** — This is a malicious application that encrypts the files of the user. Without knowing the encryption password, the data are rendered inaccessible. If the user is willing to pay a “ransom,” the attacker will give them the encryption password.



Malware analysis seeks to learn about malicious programs through a variety of methods, including:

1. **Static Analysis** — simply looking through the malicious program without running it. This usually necessitates a thorough understanding of assembly language (the processor's instruction set, or the computer's fundamental commands).
2. **Dynamic Analysis** — by monitoring the malware's actions and operating it in a controlled environment. It allows you to watch how the malware operates when it is active.

[Question 2.1] What would you call a team of cyber security professionals that monitors a network and its systems for malicious events?

Answer: Security Operations Center

[Question 2.2] What does DFIR stand for?

Answer: Digital Forensics Incident Response

[Question 2.3] Which kind of malware requires the user to pay money to regain access to their files?

Answer: Ransomware

Task 3 ○ Practical Example of Defensive Security

1st — Access to the SIEM Dashboard

 A Day In the Life of a Junior (Associate) Security Analyst

● ● ● ● ● ●

Instructions

Inspect the alerts in your SIEM dashboard. Find the malicious IP address from the alerts, make a note of it, and then click on the alert to proceed.

https://siem.internal



The screenshot shows a SIEM dashboard with a pie chart, a bar chart, and an alert log. The pie chart shows 40% (blue), 30% (orange), and 30% (red). The bar chart shows counts for UK, US, Brazil, China, Russia, and N. Korea. The alert log contains five entries with dates, times, and messages.

● Operations: Information ◀ 1/3 ▶

Alert Log	
Date	Message
July 16th 2021, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
July 16th 2021, 05:25:28:235	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
July 16th 2021, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
July 16th 2021, 02:43:20:658	Multiple failed login attempts from John Doe
July 16th 2021, 02:30:20:215	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

2nd — Only one “Alert Log” appears to be highlighted in “Red Color” out of the five.

Alert Log	
Date	Message
July 16th 2021, 05:27:00:347	Successful SSH authentication attempt to port 22 from IP address 143.110.250.149
July 16th 2021, 05:25:28:235	Unauthorized connection attempt detected from IP address 143.110.250.149 to port 22
July 16th 2021, 02:43:22:456	The user John Doe logged in successfully (Event ID 4624)
July 16th 2021, 02:43:20:658	Multiple failed login attempts from John Doe
July 16th 2021, 02:30:20:215	Logon Failure: Specified Account's Password Has Expired (Event ID 535)

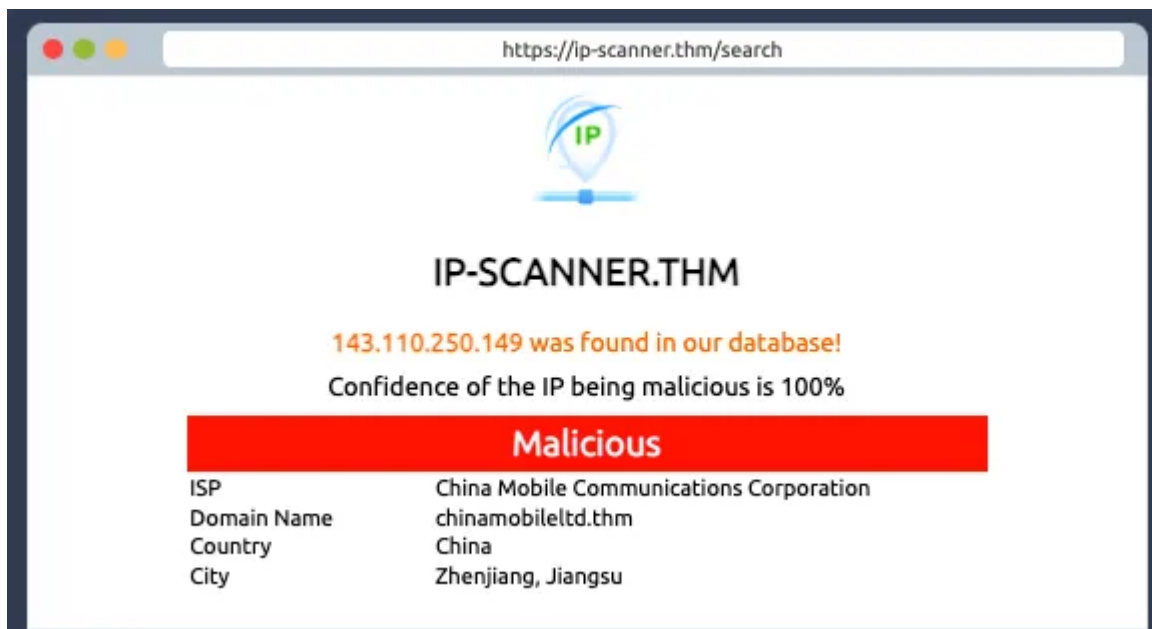
3rd — Copy the IP Address

- 143.110.250.149

4th — Paste the IP Address

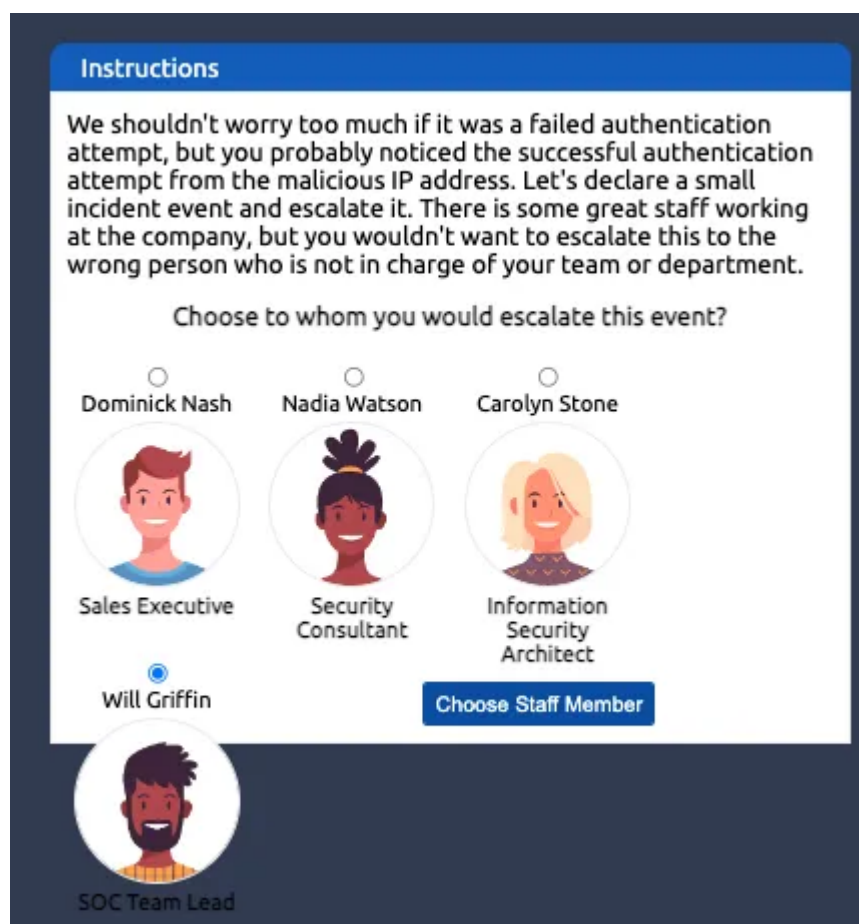


5th — Result Found!

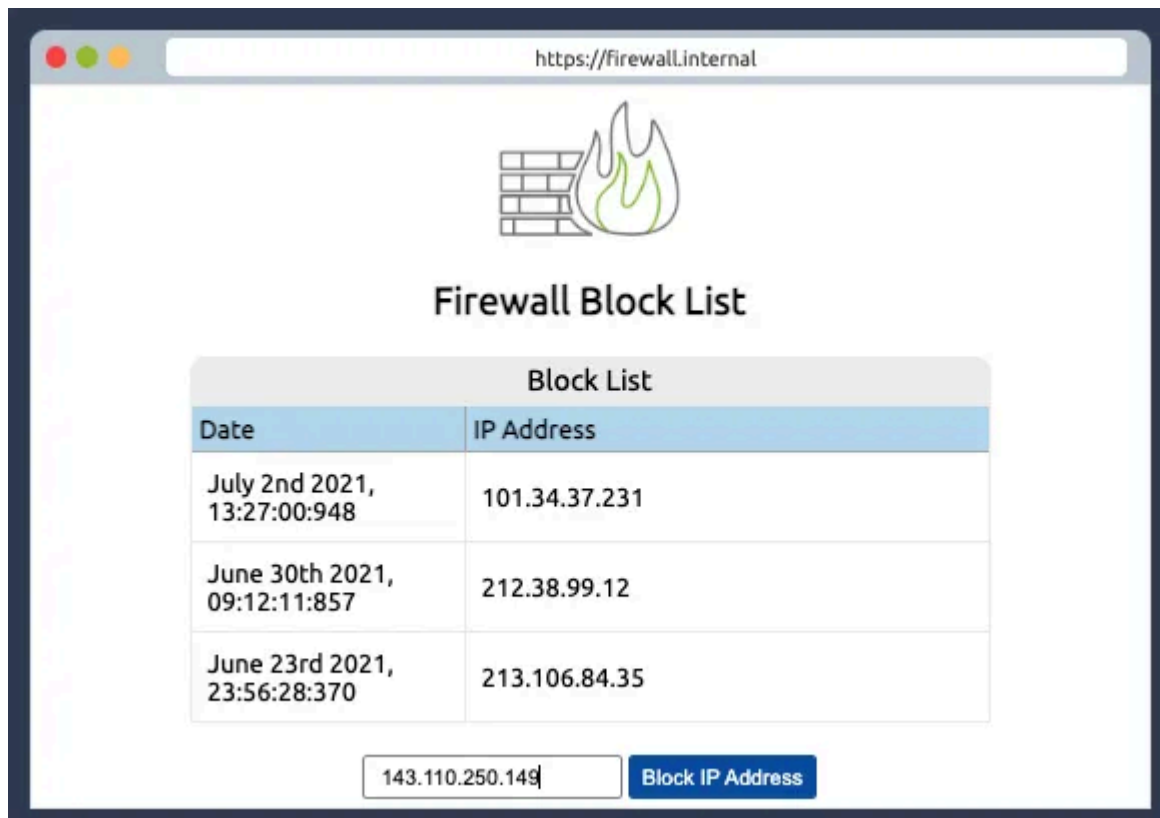


There are various open-source databases, such as AbuseIPDB and Cisco Talos Intelligence, where you may examine the IP address's reputation and location. These tools are used by the majority of security analysts to assist them with alert investigations. You can also help to make the Internet safer by reporting malicious IP addresses to sites like AbuseIPDB.

6th —Select a person to whom the incident should be escalated.



7th — Add the Malicious IP Address to Firewall Block List



8th — Flag appeared!



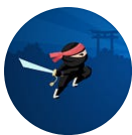
Answer: `THM{THREAT-BLOCKED}`

Cheers! ☺

Tryhackme

Defensive Security

Cybersecurity

[Follow](#)

Written by Aircon

523 Followers · 0 Following

Responses (2)



What are your thoughts?

[Respond](#)

Dominus_Falchion

almost 2 years ago



What is the answer after this already solved all of this, I'm here for the answer.

What is the flag that you obtained by following along?



5

[Reply](#)

Mohdsm

11 months ago



Thanks for the post

[Reply](#)

More from Aircon

192.168.0.202



IP (tos 0x0, ttl 1, id 61007,...)
192.168.0.202.33615 > 10.1.2.254.33435:...

192.168.0.1

192.168.0.202



Aircon

Active Reconnaissance | TryHackMe (THM)

Lab Access: <https://tryhackme.com/room/activercon>

May 21, 2022 🖱️ 25 💬 3



```

ester@TryHackMe$ sudo nmap -sV 10.10.76.34

Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-10 05:03 BST
Nmap scan report for 10.10.76.34
Host is up (0.0040s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0)
25/tcp    open  smtp      Postfix smtpd
80/tcp    open  http      nginx 1.6.2
110/tcp   open  pop3      Dovecot pop3d
4242/tcp  open  rpcbind  2-4 (RPC #100000)
Address: 02:A0:E7:B5:B6:C5 (Unknown)
Device Info: Host: deبرا2.thm.local; OS: Linux; CPE: cpe:/o:linux:linux_kernel
  
```



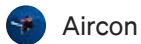
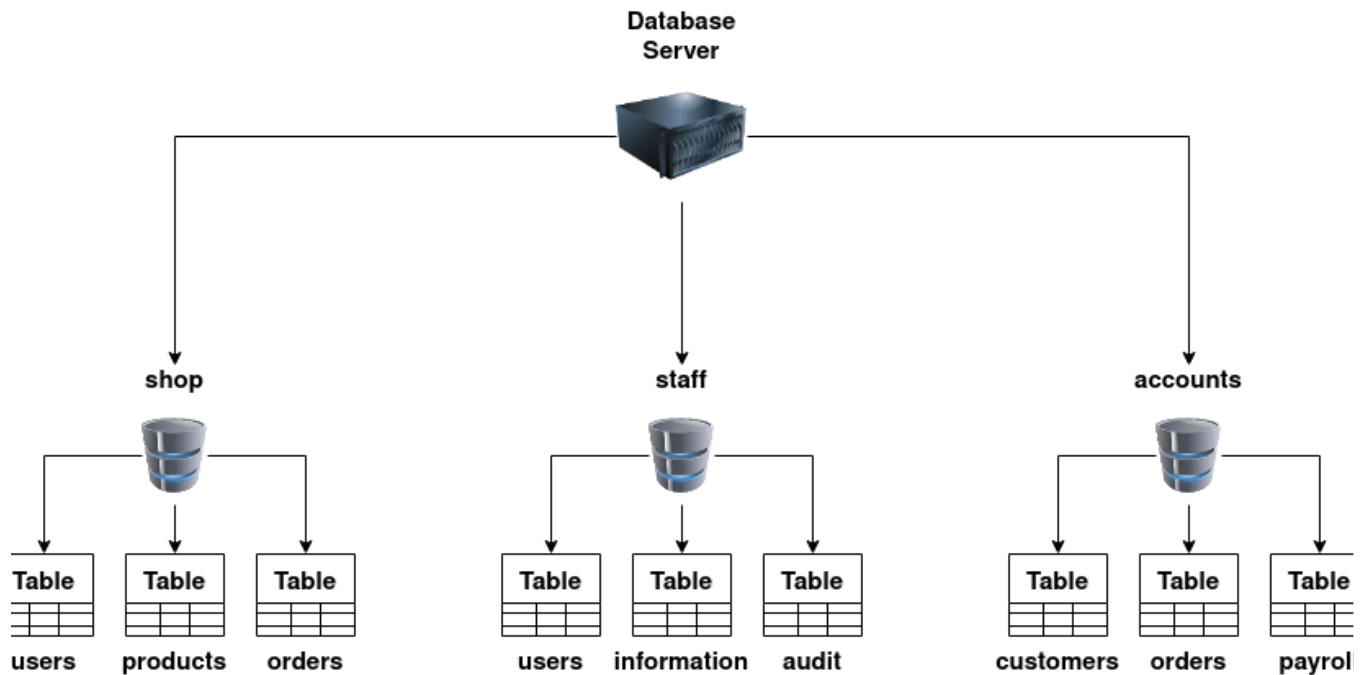
Aircon

Nmap Post Port Scans | TryHackMe (THM)

Lab Access: <https://tryhackme.com/room/nmap04>

Jun 1, 2022 🖱️ 25 💬 4



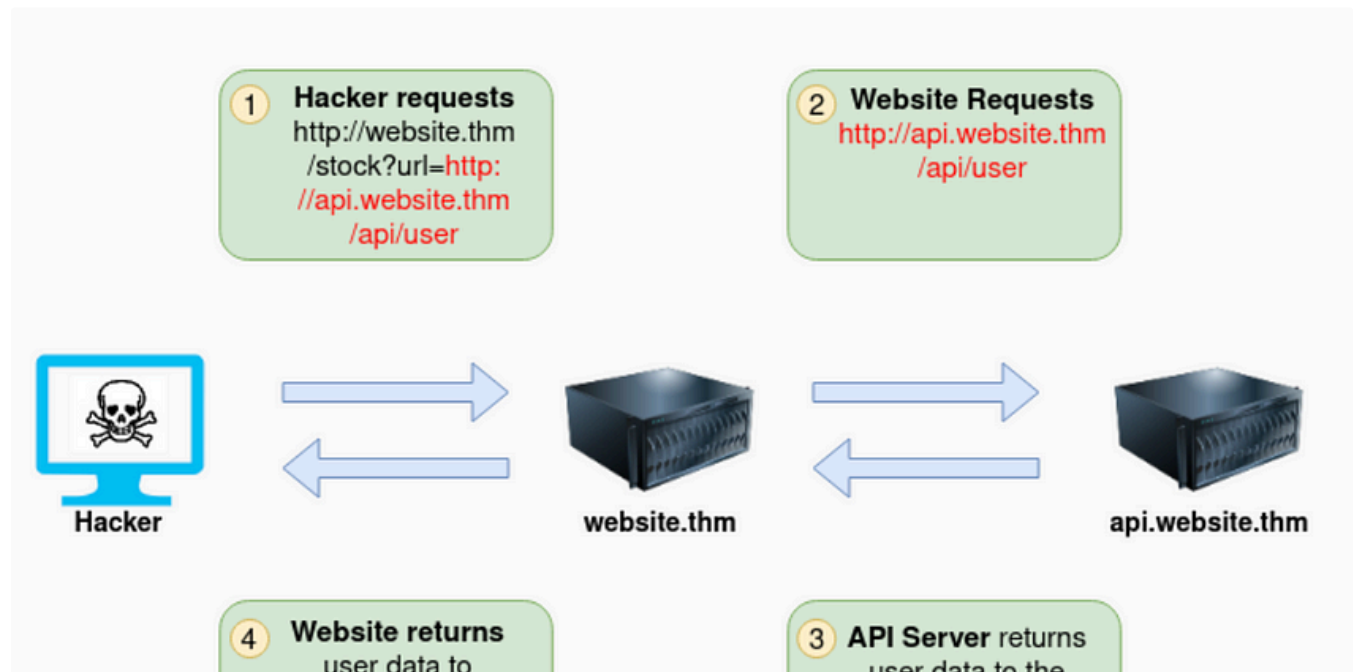


Aircon

SQL Injection | TryHackMe (THM)

Lab Access: <https://tryhackme.com/room/sqlinjectionlm>

May 19, 2022 🖱️ 100 💬 1



Aircon

SSRF | TryHackMe (THM)

Lab Access: <https://tryhackme.com/room/ssrfqi>

May 8, 2022 🖱 123



See all from Aircon

Recommended from Medium



Open in app ↗

Medium



Search



In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

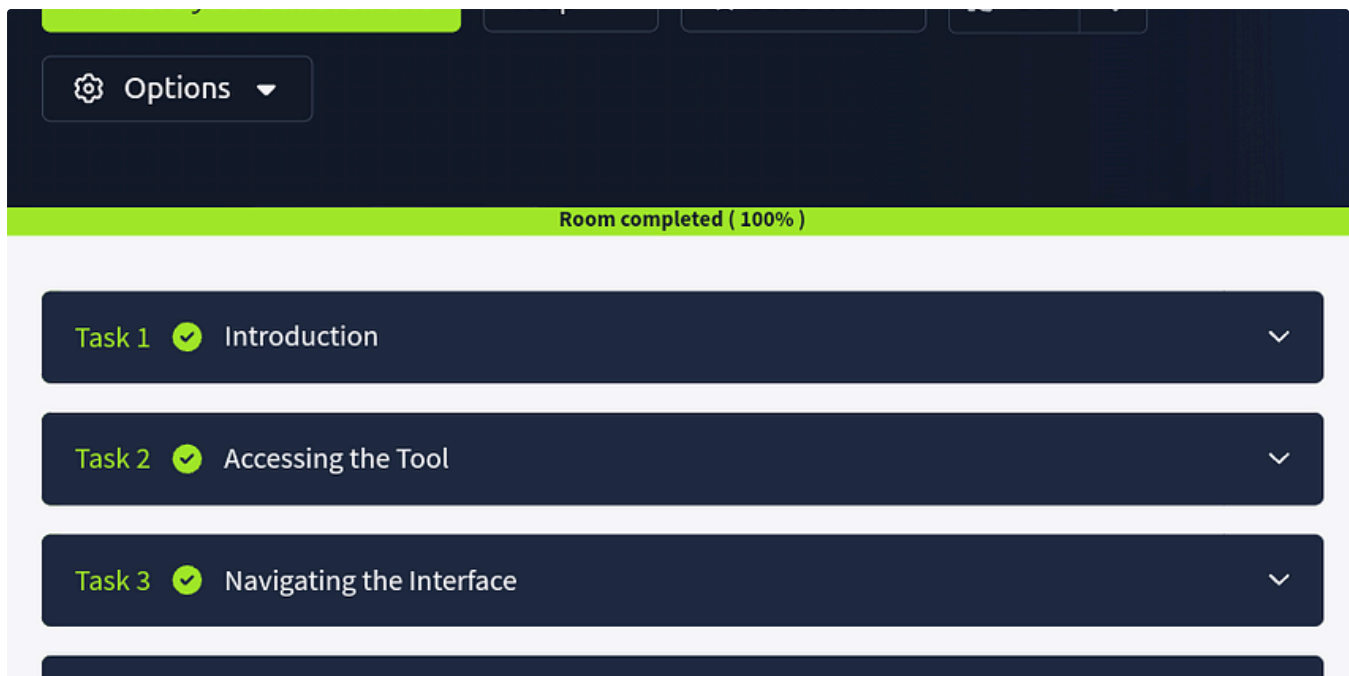


Nov 5, 2024



60





 Jawstar

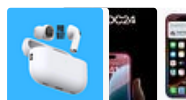
CyberChef: The Basics Tryhackme Write up

Tryhackme

★ Nov 7, 2024 🖱 8

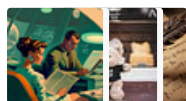


Lists



Tech & Tools

22 stories · 377 saves



Medium's Huge List of Publications Accepting Submissions

377 stories · 4298 saves



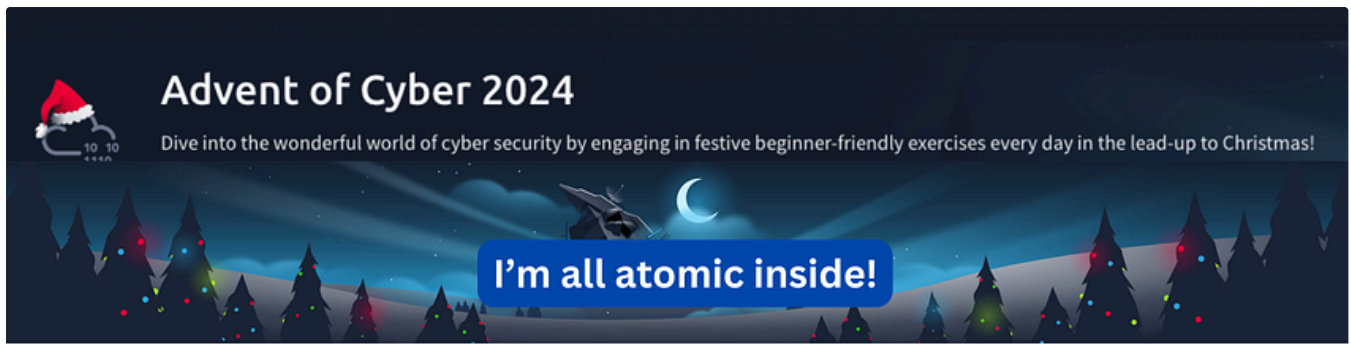
Staff picks

791 stories · 1541 saves




Natural Language Processing

1881 stories · 1517 saves



Day 4
Answers

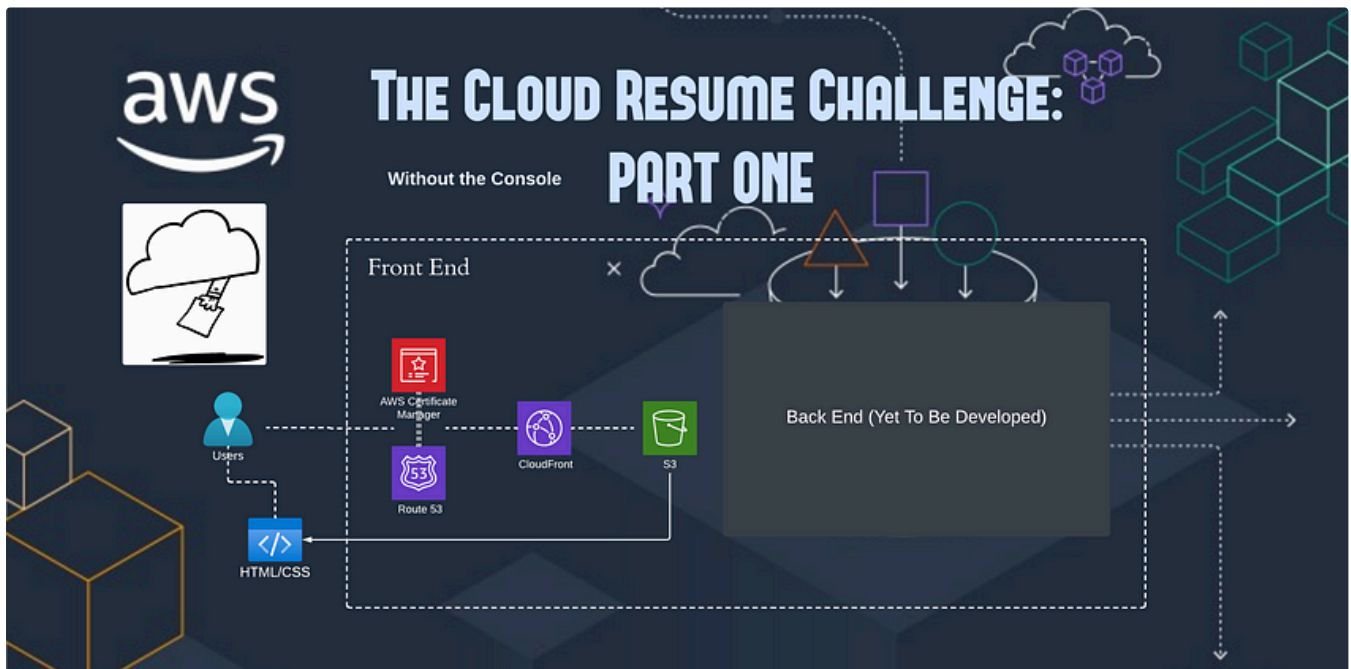
cyberw1ng.medium.com

 In InfoSec Write-ups by Karthikeyan Nagaraj

Advent of Cyber 2024 [Day 4] Writeup with Answers | TryHackMe Walkthrough

I'm all atomic inside!

★ Dec 4, 2024 🖱 882 💬 1



 Gabriel Binion

The Cloud Resume Challenge (AWS): Part One

Hello everyone, this is part one of my documentation of 'The Cloud Resume Challenge' my first cloud project where I showcase my knowledge...

Nov 18, 2024



In T3CH by Axoloth

TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM



Nov 28, 2024



50



IritT

Phishing Analysis Fundamentals

Learn all the components that make up an email.

Nov 26, 2024  1



See more recommendations