# TryHackMe Traffic Analysis Essentials Room

Haircutfish · Follow
7 min read · Dec 15, 2022



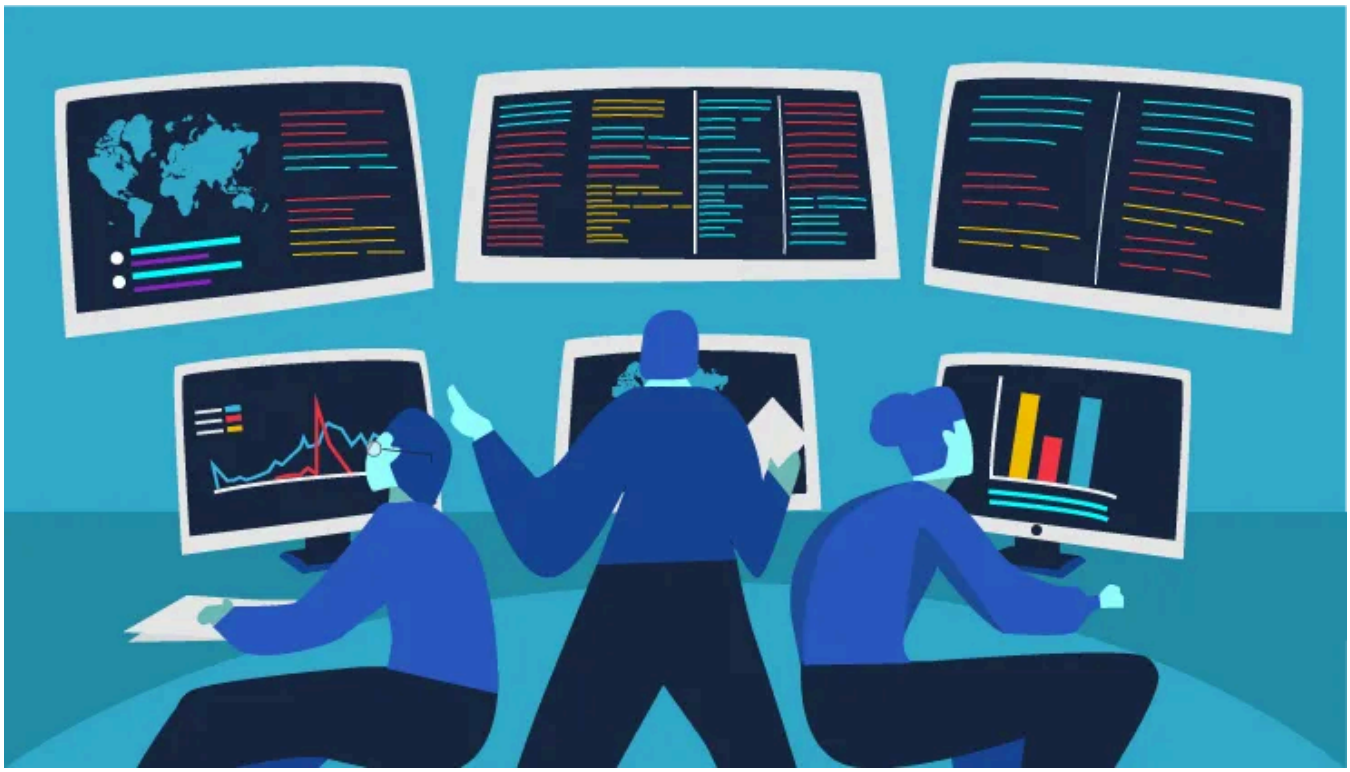
Learn Network Security and Traffic Analysis foundations and take a step into probing network anomalies.

## Task 1 Introduction

Network Security is a set of operations for protecting data, applications, devices and systems connected to the network. It is accepted as one of the significant subdomains of cyber security. It focuses on the system design, operation and management of the architecture/infrastructure to provide network accessibility, integrity, continuity and reliability. Traffic analysis (often called Network Traffic Analysis) is a subdomain of the Network Security domain, and its primary focus is investigating the network data to identify problems and anomalies.

This room will cover the foundations of Network Security and Traffic analysis and introduce the essential concepts of these disciplines to help you step into Traffic/Packet Analysis. We suggest completing the "Network Fundamentals" module before starting working in this room.

## Task 2 Network Security and Network Data



### Network Security

The essential concern of Network Security focuses on two core concepts: authentication and authorization. There are a variety of tools, technologies, and approaches to ensure and measure implementations of these two key concepts and go beyond to provide continuity and reliability. Network security operations contain three base control levels to ensure the maximum available security management.

### Base Network Security Control Levels:

| | |
|---|---|
| **Physical** | Physical security controls prevent unauthorised physical access to networking devices, cable boards, locks, and all linked components. |
| **Technical** | Data security controls prevent unauthorised access to network data, like installing tunnels and implementing security layers. |
| **Administrative** | Administrative security controls provide consistency in security operations like creating policies, access levels and authentication processes. |

There are two main approaches and multiple elements under these control levels. The most common elements used in network security operations are explained below.

### The main approaches:

| Access Control | Threat Control |
| --- | --- |
| The starting point of Network Security. It is a set of controls to ensure authentication and authorisation. | Detecting and preventing anomalous/malicious activities on the network. It contains both internal (trusted) and external traffic data probes. |

## The key elements of Access Control:

| | |
| --- | --- |
| **Firewall Protection** | Controls incoming and outgoing network traffic with predetermined security rules. Designed to block suspicious/malicious traffic and application-layer threats while allowing legitimate and expected traffic. |
| **Network Access Control (NAC)** | Controls the devices' suitability before access to the network. Designed to verify device specifications and conditions are compliant with the predetermined profile before connecting to the network. |
| **Identity and Access Management (IAM)** | Controls and manages the asset identities and user access to data systems and resources over the network. |
| **Load Balancing** | Controls the resource usage to distribute (based on metrics) tasks over a set of resources and improve overall data processing flow. |
| **Network Segmentation** | Creates and controls network ranges and segmentation to isolate the users' access levels, group assets with common functionalities, and improve the protection of sensitive/internal devices/data in a safer network. |
| **Virtual Private Networks (VPN)** | Creates and controls encrypted communication between devices (typically for secure remote access) over the network (including communications over the internet). |
| **Zero Trust Model** | Suggests configuring and implementing the access and permissions at a minimum level (providing access required to fulfil the assigned role). The mindset is focused on: "Never trust, always verify". |

## The key elements of Threat Control:

| | |
| --- | --- |
| **Intrusion Detection and Prevention (IDS/IPS)** | Inspects the traffic and creates alerts (IDS) or resets the connection (IPS) when detecting an anomaly/threat. |
| **Data Loss Prevention (DLP)** | Inspects the traffic (performs content inspection and contextual analysis of the data on the wire) and blocks the extraction of sensitive data. |
| **Endpoint Protection** | Protecting all kinds of endpoints and appliances that connect to the network by using a multi-layered approach like encryption, antivirus, antimalware, DLP, and IDS/IPS. |
| **Cloud Security** | Protecting cloud/online-based systems resources from threats and data leakage by applying suitable countermeasures like VPN and data encryption. |
| **Security Information and Event Management (SIEM)** | Technology that helps threat detection, compliance, and security incident management, through available data (logs and traffic statistics) by using event and context analysis to identify anomalies, threats, and vulnerabilities. |
| **Security Orchestration Automation and Response (SOAR)** | Technology that helps coordinate and automates tasks between various people, tools, and data within a single platform to identify anomalies, threats, and vulnerabilities. It also supports vulnerability management, incident response, and security operations. |
| **Network Traffic Analysis & Network Detection and Response** | Inspecting network traffic or traffic capture to identify anomalies and threats. |

## Typical Network Security Management Operation is explained in the given table:

| Deployment | Configuration | Management | Monitoring | Maintenance |
|---|---|---|---|---|
| • Device and software installation<br>• Initial configuration<br>• Automation | • Feature configuration<br>• Initial network access configuration | • Security policy implementation<br>• NAT and VPN implementation<br>• Threat mitigation | • System monitoring<br>• User activity monitoring<br>• Threat monitoring<br>• Log and traffic sample capturing | • Upgrades<br>• Security updates<br>• Rule adjustments<br>• Licence management<br>• Configuration updates |

### Managed Security Services

Not every organisation has enough resources to create dedicated groups for specific security domains. There are plenty of reasons for this: budget, employee skillset, and organisation size could determine how security operations are handled. At this point, Managed Security Services (MSS) come up to fulfil the required effort to ensure/enhance security needs. MSS are services that have been outsourced to service providers. These service providers are called Managed Security Service Providers (MSSPs). Today, most MSS are time and cost effective, can be conducted in-house or outsourced, are easy to engage, and ease the management process. There are various elements of MSS, and the most common ones are explained below.

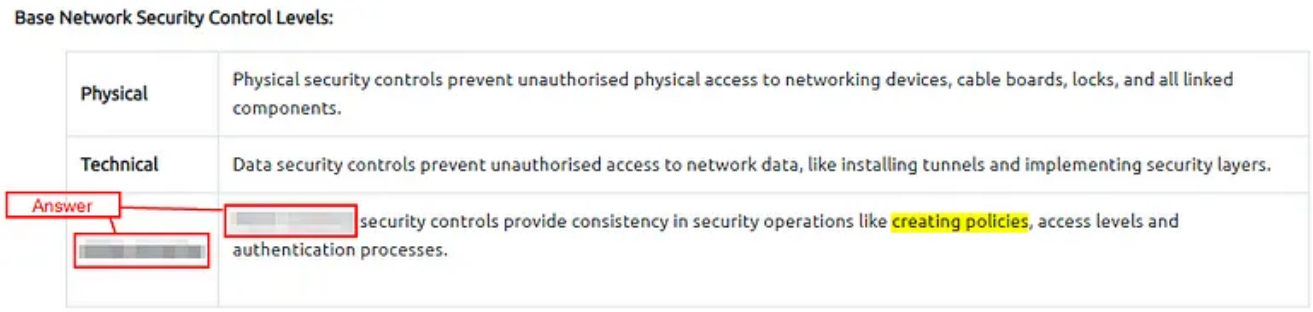
| | |
|---|---|
| Network Penetration Testing | Assessing network security by simulating external/internal attacker techniques to breach the network. |
| Vulnerability Assessment | Assessing network security by discovering and analysing vulnerabilities in the environment. |
| Incident Response | An organised approach to addressing and managing a security breach. It contains a set of actions to identify, contain, and eliminate incidents. |
| Behavioural Analysis | An organised approach to addressing system and user behaviours, creating baselines and traffic profiles for specific patterns to detect anomalies, threats, vulnerabilities, and attacks. |

### Answer the questions below

Since the answer can be found above, I won't be posting the answers below. Follow along to help find the answer.

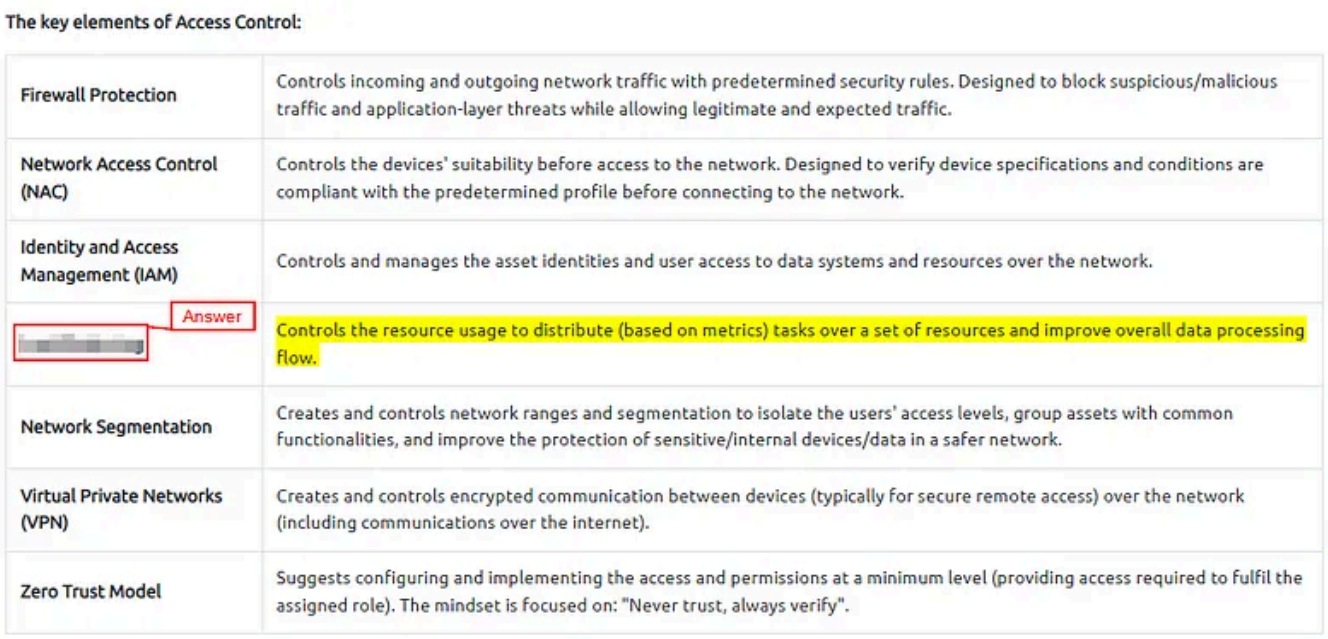
### Which Security Control Level covers contain creating security policies?

Go up to the Base Network Security Control Levels table, in this table you will find the answer, just read through. Once you find it, Highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer into the TryHackMe answer Field, then click submit.




**Which Access Control element works with data metrics to manage data flow?**

Scroll up to The Key Elements of Access Control table, in this table you will find the answer, manage data flow is the key. Once you find it, Highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer into the TryHackMe answer Field, then click submit.



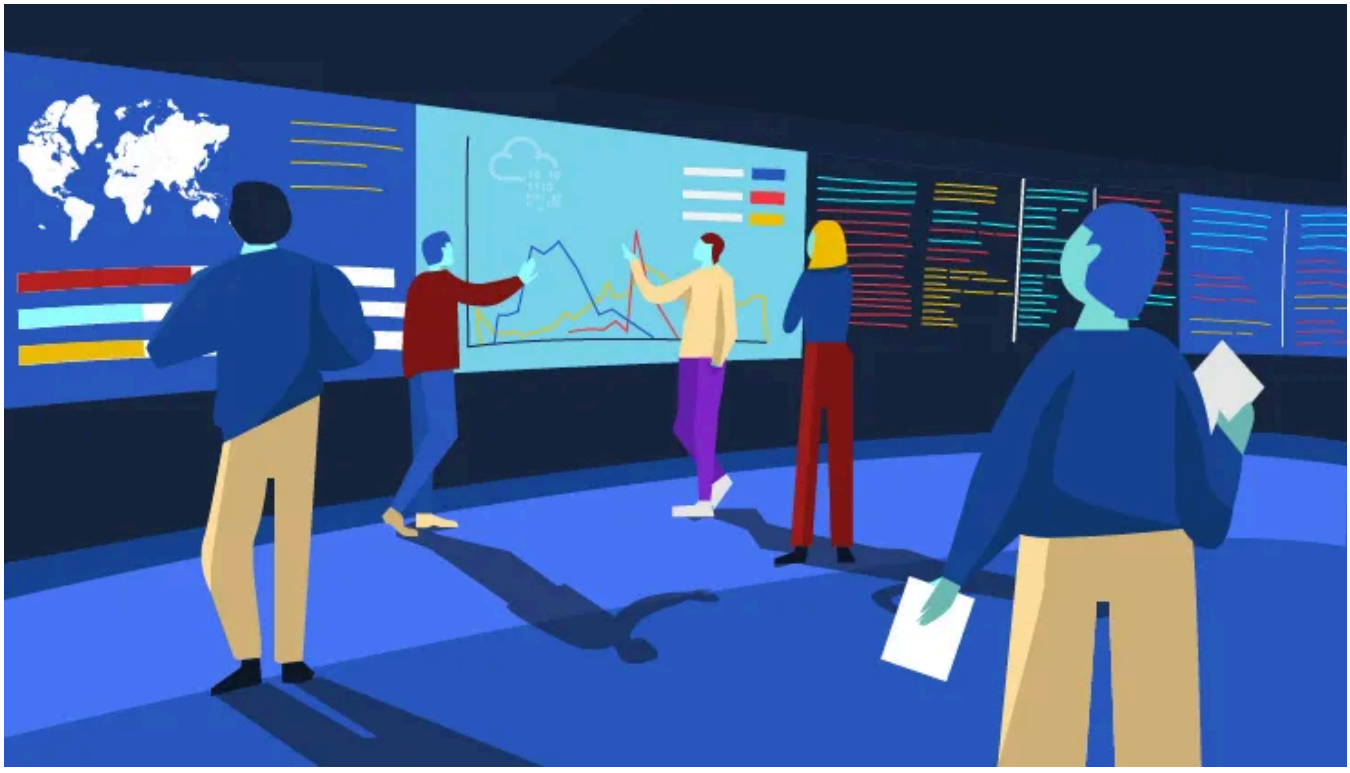

**Which technology helps correlate different tool outputs and data sources?**

Scroll up to The Key Elements of Threat Control table, the answer can be found towards the bottom of this table. TryHackMe is looking for the acronym for the answer. Once you find it, Highlight copy (ctrl + c) and paste (ctrl + v) or type, the answer into the TryHackMe answer Field, then click submit.

The key elements of Threat Control:

| | |
|---|---|
| Intrusion Detection and Prevention (IDS/IPS) | Inspects the traffic and creates alerts (IDS) or resets the connection (IPS) when detecting an anomaly/threat. |
| Data Loss Prevention (DLP) | Inspects the traffic (performs content inspection and contextual analysis of the data on the wire) and blocks the extraction of sensitive data. |
| Endpoint Protection | Protecting all kinds of endpoints and appliances that connect to the network by using a multi-layered approach like encryption, antivirus, antimalware, DLP, and IDS/IPS. |
| Cloud Security | Protecting cloud/online-based systems resources from threats and data leakage by applying suitable countermeasures like VPN and data encryption. |
| Security Information and Event Management (SIEM) | Technology that helps threat detection, compliance, and security incident management, through available data (logs and traffic statistics) by using event and context analysis to identify anomalies, threats, and vulnerabilities. |
| Security Orchestration Automation and Response [redacted] Answer | Technology that helps coordinate and automates tasks between various people, tools, and data within a single platform to identify anomalies, threats, and vulnerabilities. It also supports vulnerability management, incident response, and security operations. |
| Network Traffic Analysis & Network Detection and Response | Inspecting network traffic or traffic capture to identify anomalies and threats. |

## Task 3 Traffic Analysis



### Traffic Analysis / Network Traffic Analysis

Traffic Analysis is a method of intercepting, recording/monitoring, and analysing network data and communication patterns to detect and respond to system health issues, network anomalies, and threats. The network is a rich data source, so traffic analysis is useful for security and operational matters. The operational issues cover system availability checks and measuring performance, and the security issues cover anomaly and suspicious activity detection on the network.

Traffic analysis is one of the essential approaches used in network security, and it is part of multiple disciplines of network security operations listed below:

- Network Sniffing and Packet Analysis (Covered in **Wireshark room**)
- Network Monitoring (Covered in **Zeek room**)
- Intrusion Detection and Prevention (Covered in **Snort room**)
- Network Forensics (Covered in **NetworkMiner room**)
- Threat Hunting (Covered in **Brim room**)

There are two main techniques used in Traffic Analysis:

| Flow Analysis | Packet Analysis |
| --- | --- |
| Collecting data/evidence from the networking devices. This type of analysis aims to provide statistical results through the data summary without applying in-depth packet-level investigation.<br>• **Advantage:** Easy to collect and analyse.<br>• **Challenge:** Doesn't provide full packet details to get the root cause of a case. | Collecting all available network data. Applying in-depth packet-level investigation (often called Deep Packet Inspection (DPI) ) to detect and block anomalous and malicious packets.<br>• **Advantage:** Provides full packet details to get the root cause of a case.<br>• **Challenge:** Requires time and skillset to analyse. |

Benefits of the Traffic Analysis:

- Provides full network visibility.
- Helps comprehensive baselining for asset tracking.
- Helps to detect/respond to anomalies and threats.

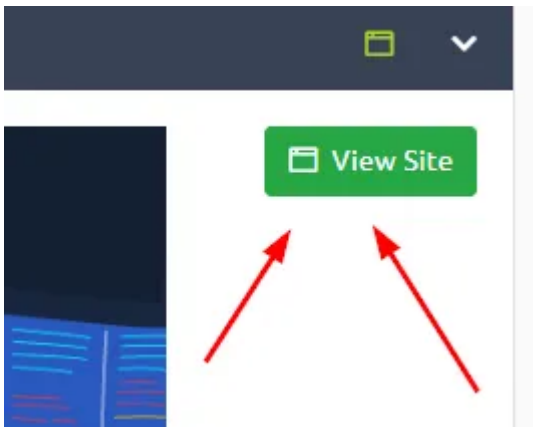
**Does the Traffic Analysis Still Matter?**

The widespread usage of security tools/services and an increasing shift to cloud computing force attackers to modify their tactics and techniques to avoid detection. Network data is a pure and rich data source. Even if it is encoded/encrypted, it still provides a value by pointing to an odd, weird or unexpected pattern/situation. Therefore traffic analysis is still a must-to-have skill for any security analyst who wants to detect and respond to advanced threats.

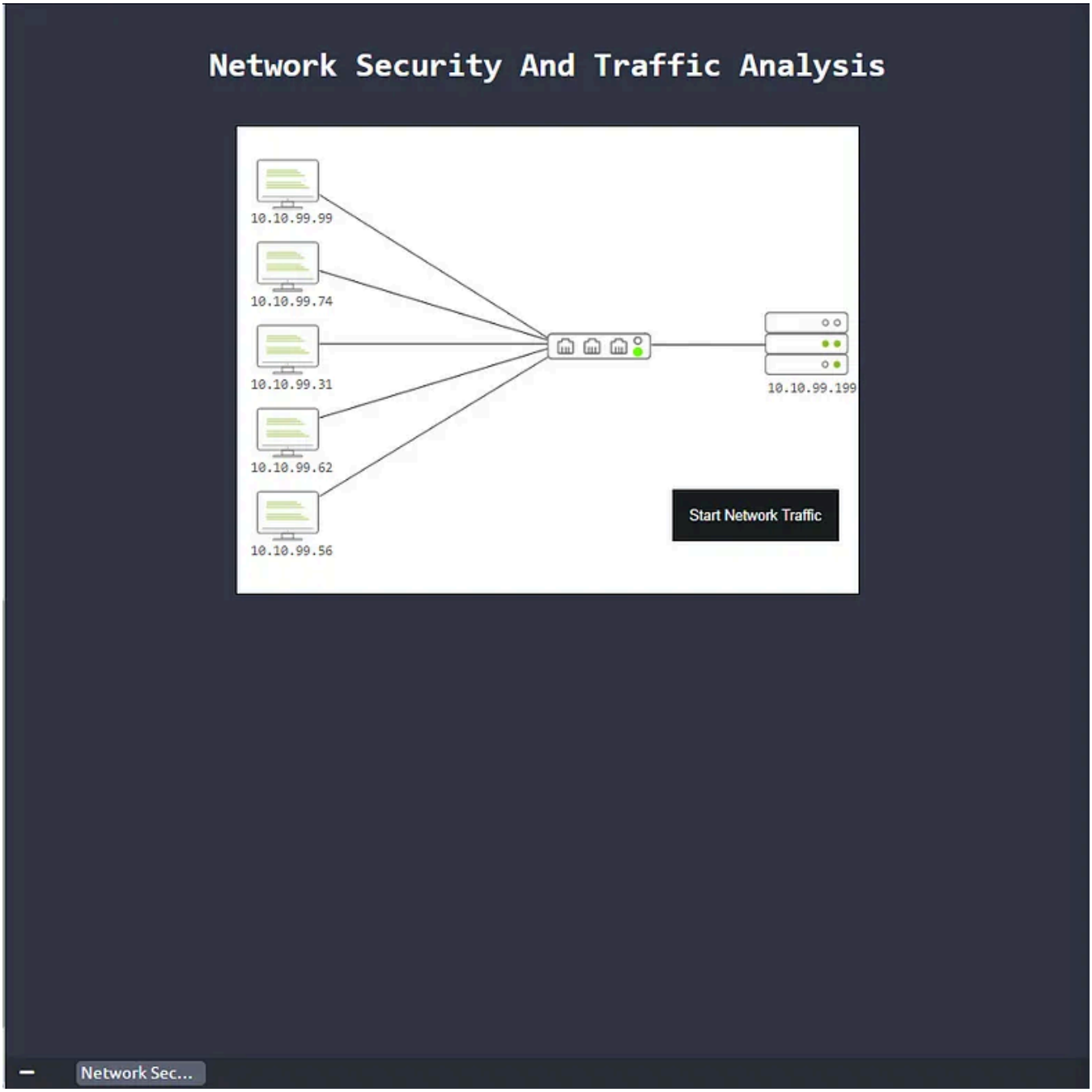
Now you know what Traffic Analysis is and how it operates. Now use the static site to simulate a traffic analysis operation and find the flags.

## Answer the questions below

At the top of the task, click the green View Site button.

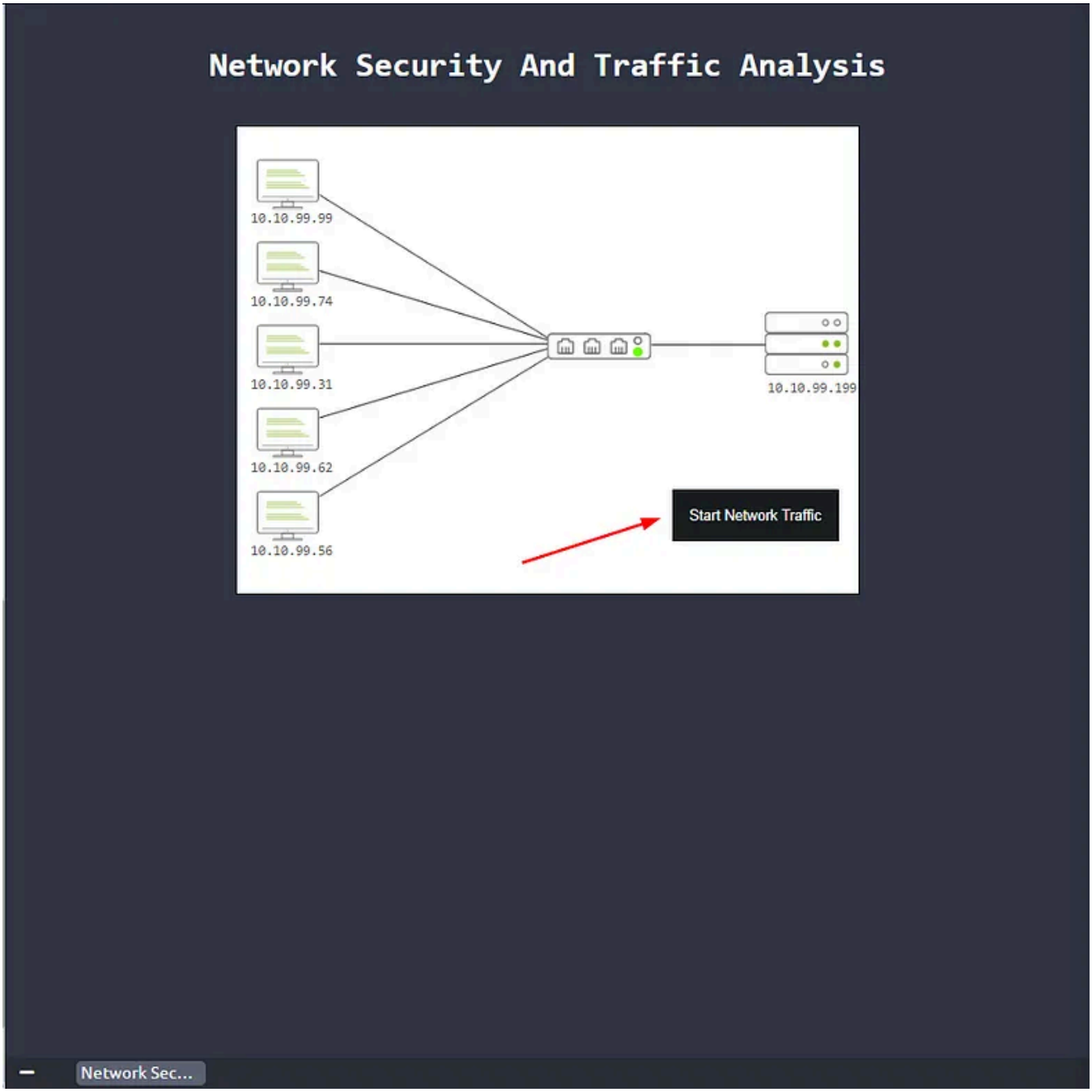



The screen will split, and you will be ready to start.

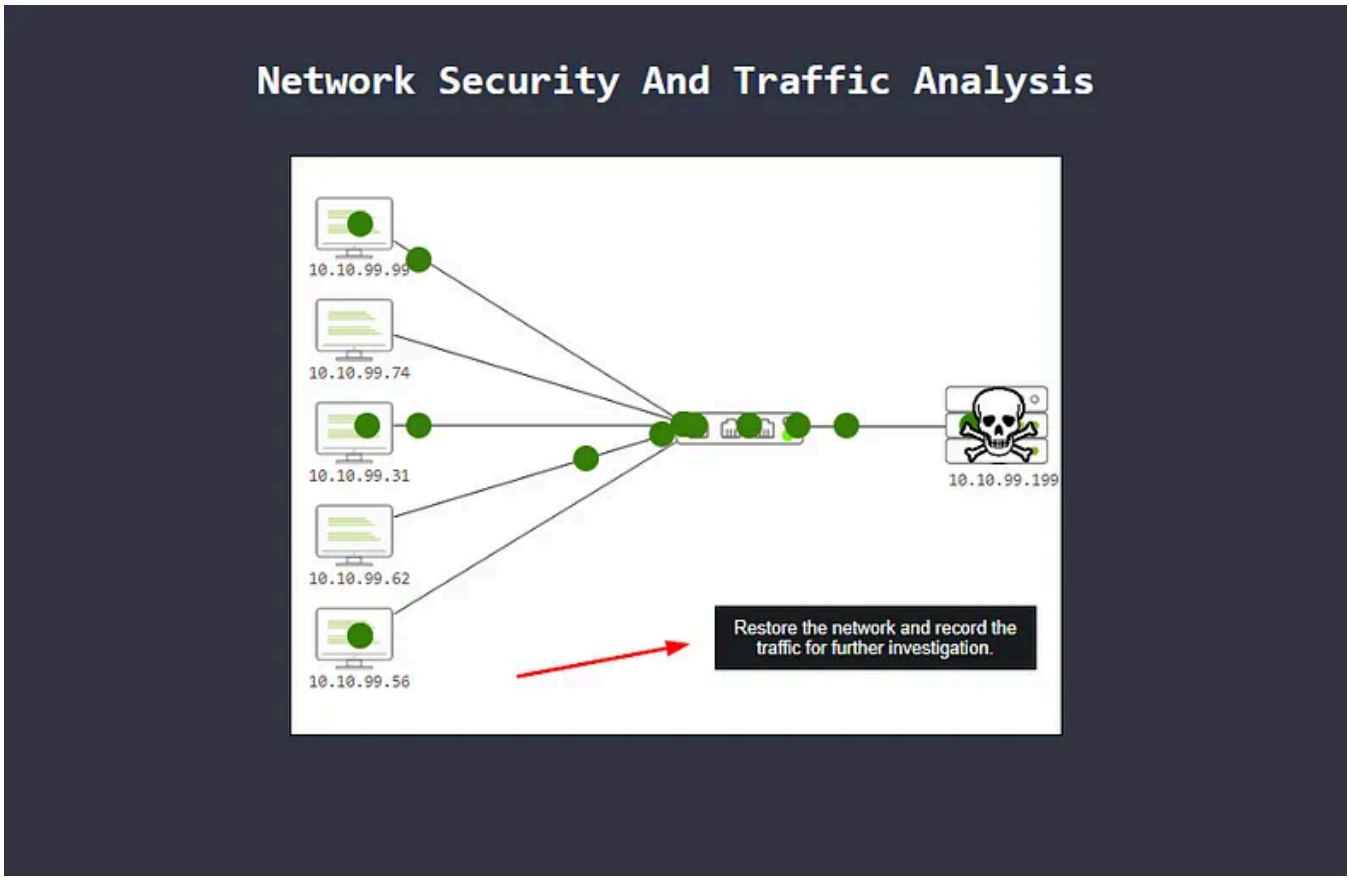


**Level-1 is simulating the identification and filtering of malicious IP addresses.**

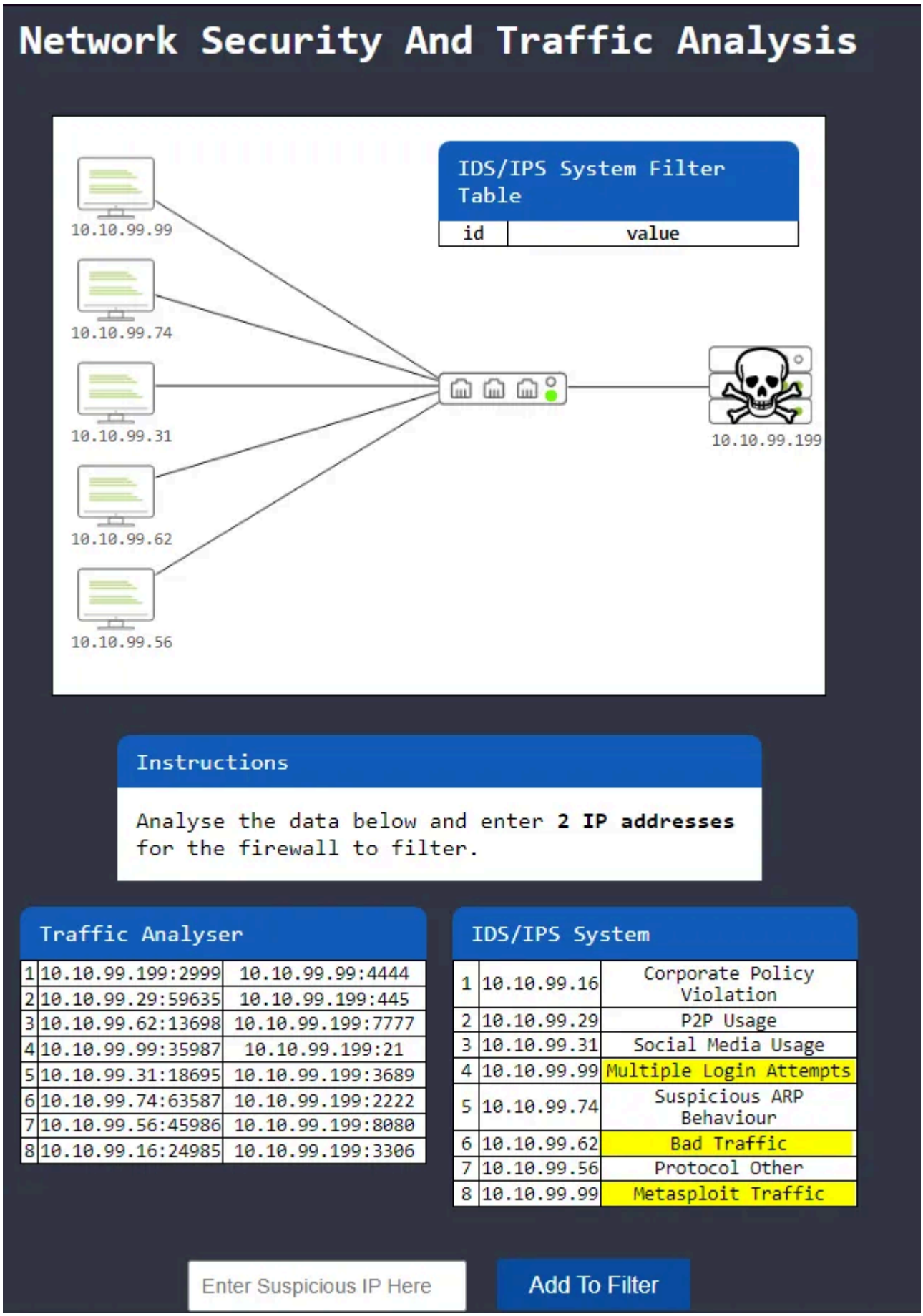
Click the black Start Network Traffic button.



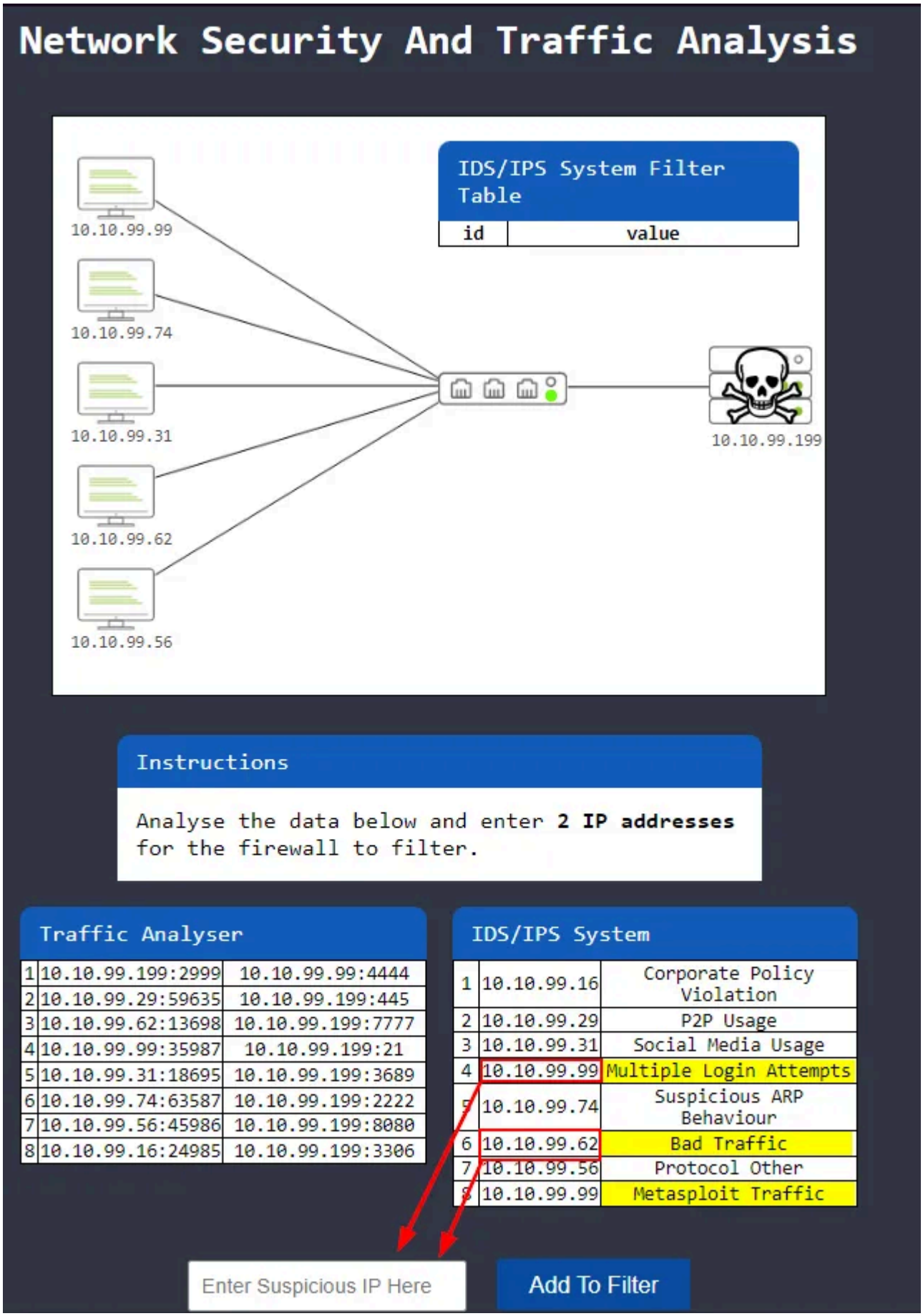

You will see traffic running across the network, but uh-no we got malware!!! So a black button labeled Restore the Network and record the traffic for further investigation, click this button.



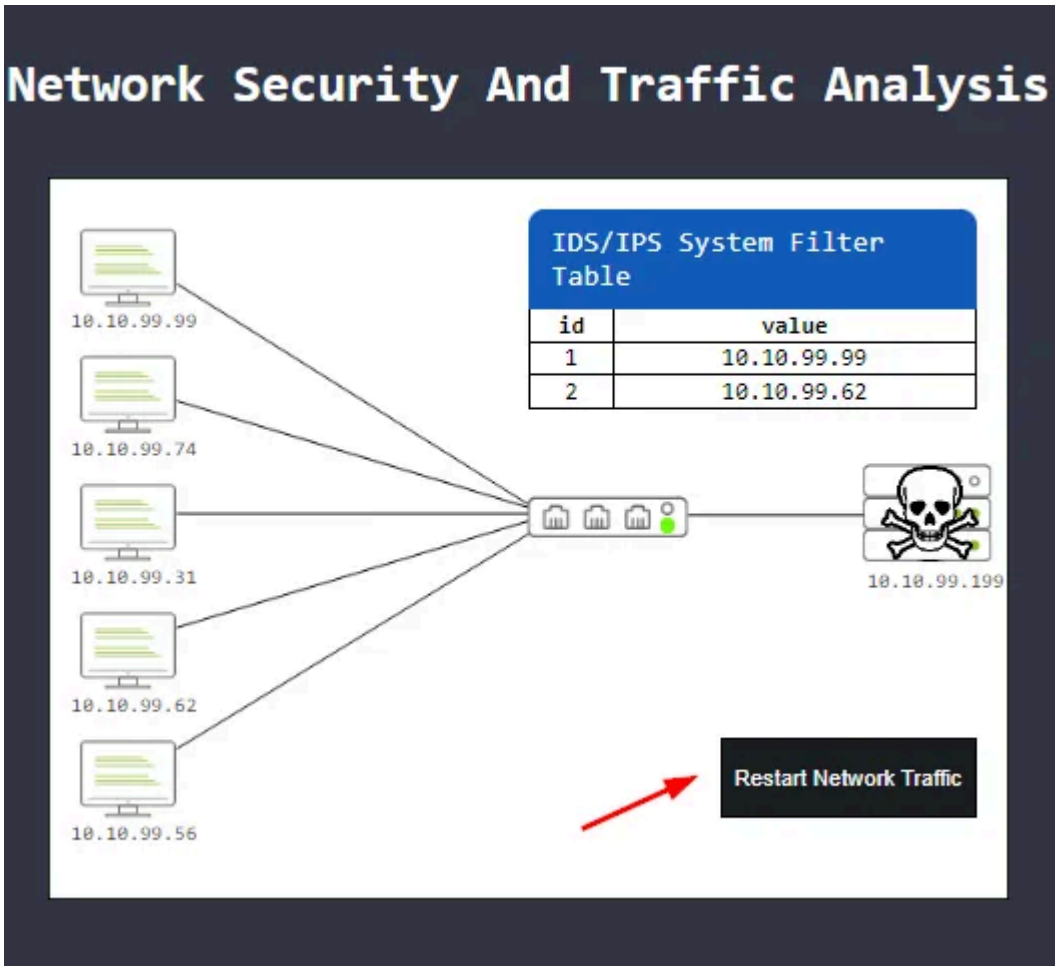

So we will have traffic run over the network again, this time we are getting logs of what is running over it. Once we have enough logs, you will be instructed to analyze the data to find two IP addresses to filter through the firewall. Looking through the IDS/IPS system, we can see a couple of suspicious IP addesses.




Highlight copy (ctrl + c) and paste (ctrl + v) or type the IP addresses into the Filter box, then click the blue Add to Filter.




Once you have added both of them, you will have a black Restart Network Traffic Button. Click it.




After restarting the Network Traffic, you will have successfully block the malware. You will get a pop-up window, this window will contain the first flag. Type the answer into the TryHackMe answer field, then click submit.

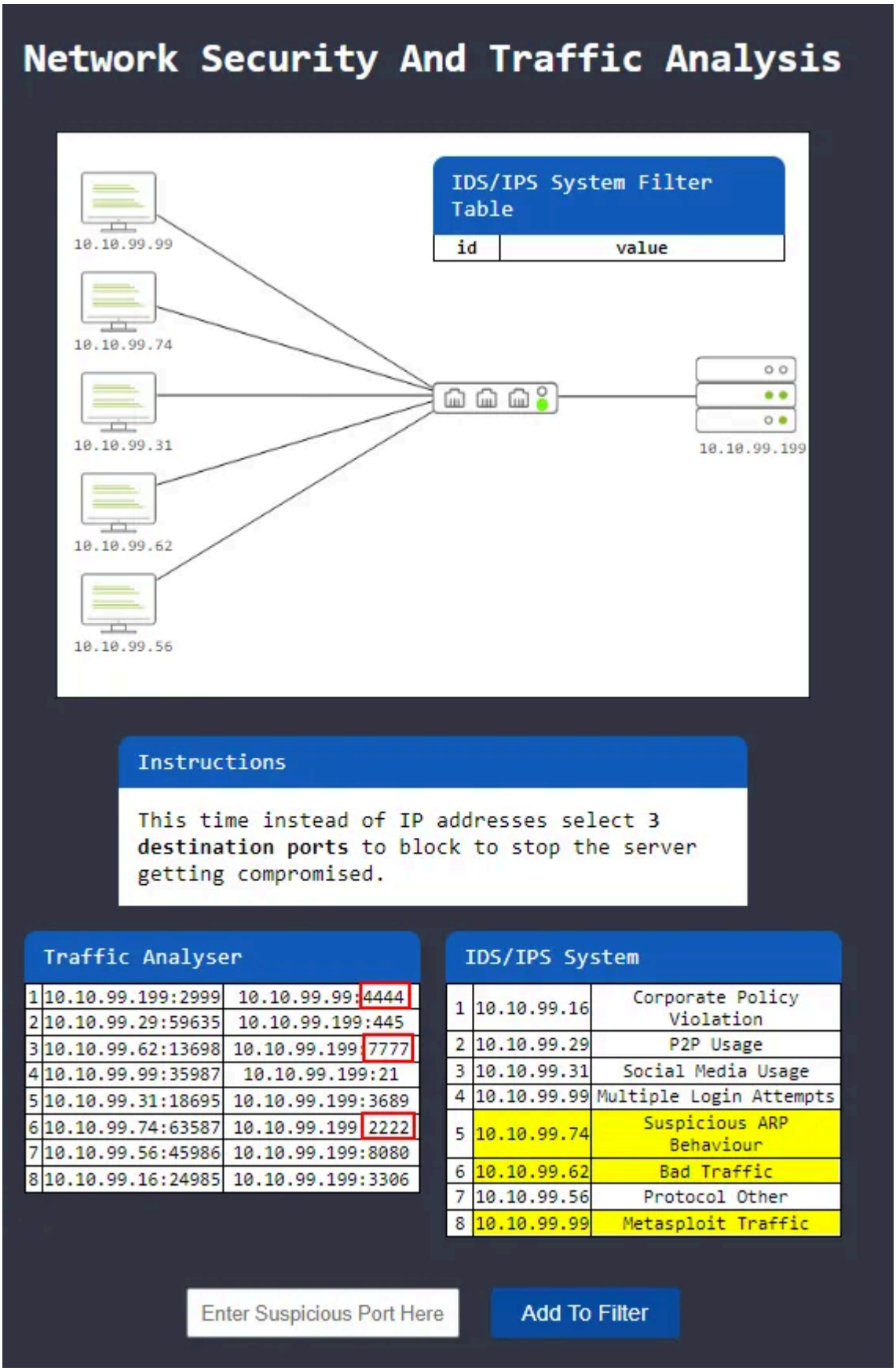

**What is the flag?**

**Answer: THM{PACKET_MASTER}**

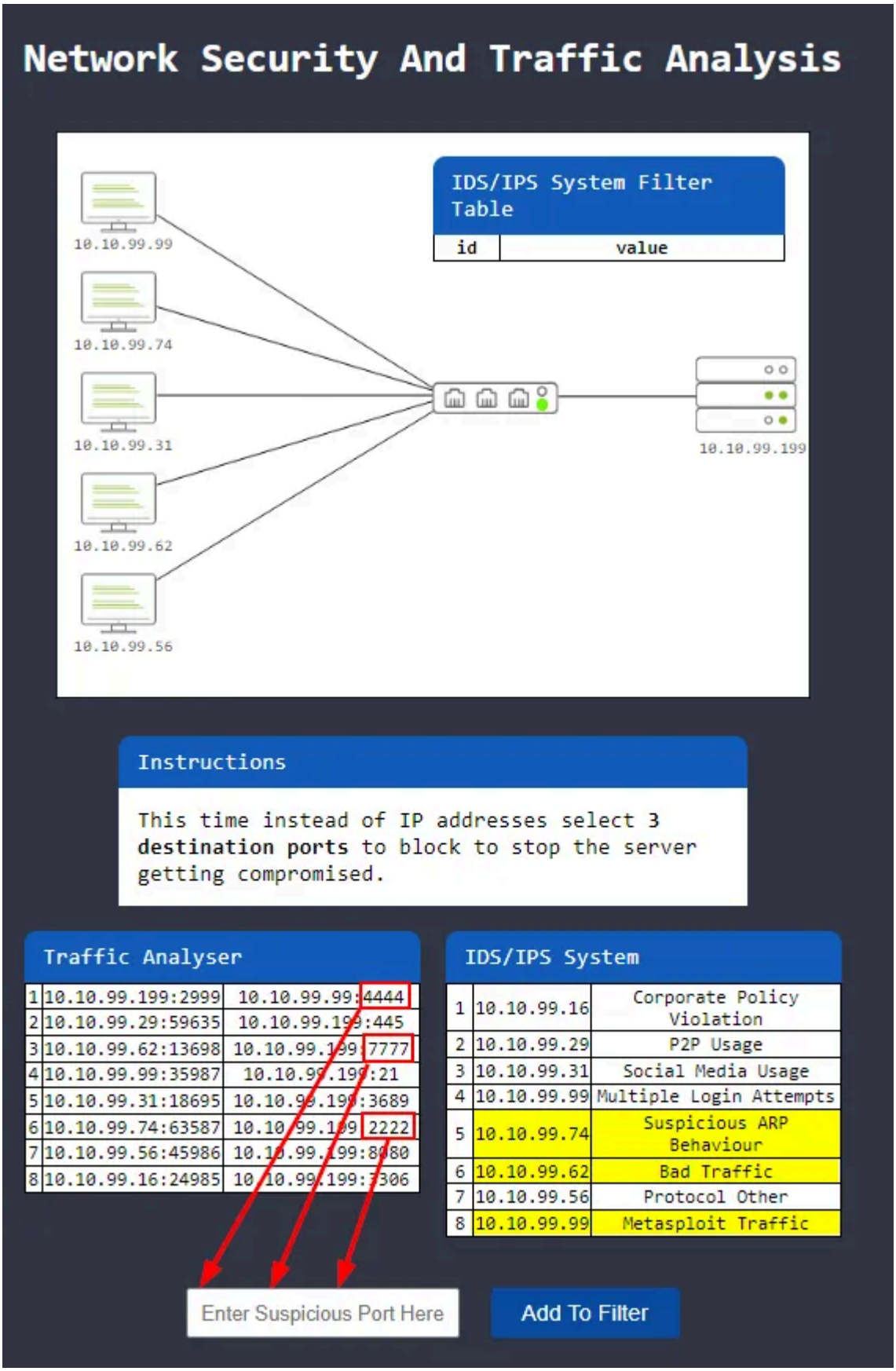
**Level-2 is simulating the identification and filtering of malicious IP and Port addresses.**

Now we are tasked with blocking destination ports, we need to get these from the Traffic Analyzer table. If we look at the sus IP addresses from the previous question,

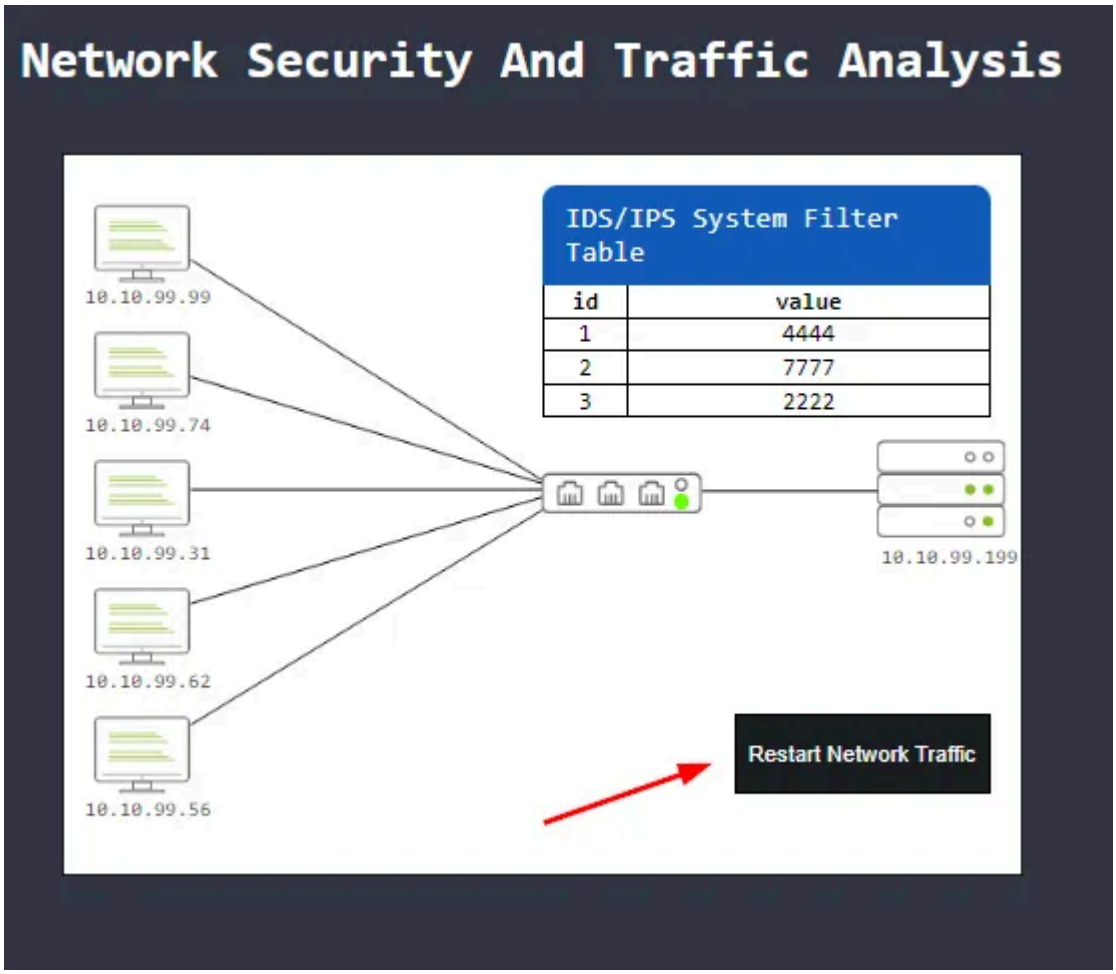
along with number five, since it is labeled as Suspicious ARP Behavior. We can see the destination ports they correlate to in the Traffic Analyzer table on the right.




Since we only need the port numbers, Highlight copy (ctrl + c) and paste (ctrl + v) or type, the port number into the Filter box, then click the blue Add to Filter.




Once you have added all the ports, a black Restart Network Traffic button will apper. Click it.




After restarting the Network Traffic, you will have successfully block the malware. You will get a pop-up window, this window will contain the first flag. Type the answer into the TryHackMe answer field, then click submit.


**What is the flag?**

**Answer: THM{DETECTION_MASTER}**

## Task 4 Conclusion

**Congratulations!** You just finished the “Traffic Analysis Essentials” room.

In this room, we covered the foundations of the network security and traffic analysis concepts:

- Network Security Operations
- Network Traffic Analysis

Now, you are ready to complete the “**Network Security and Traffic Analysis**” module.

🎉 🎉 🎉 CONGRAT!!!! You completed the Traffic Analysis Essentials Room 🎉 🎉 🎉

Tryhackme | Tryhackme Walkthrough | Tryhackme Writeup | Traffic Analysis Essent | Soc Level One

Follow

## Written by Haircutfish

5.9K Followers · 20 Following

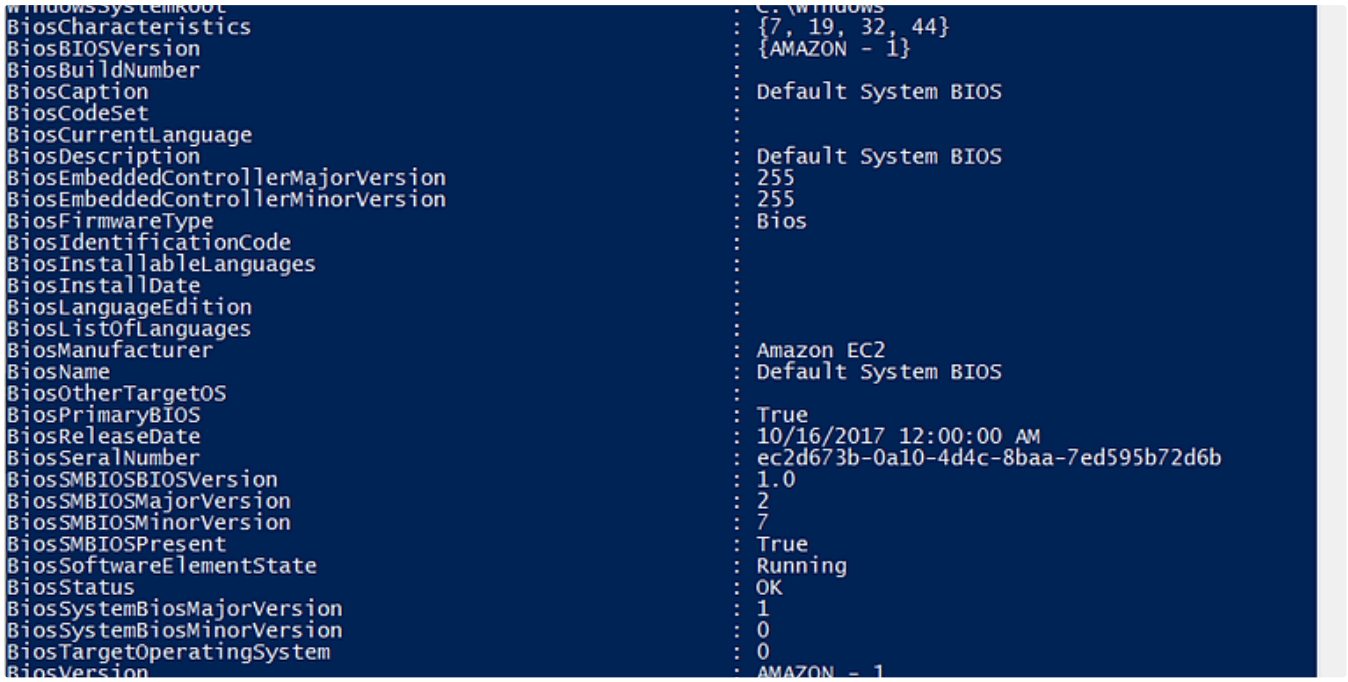
SOC Analyst | LPI Linux Essentials Certification | Top 1% on TryHackMe

## No responses yet

What are your thoughts?

Respond

## More from Haircutfish

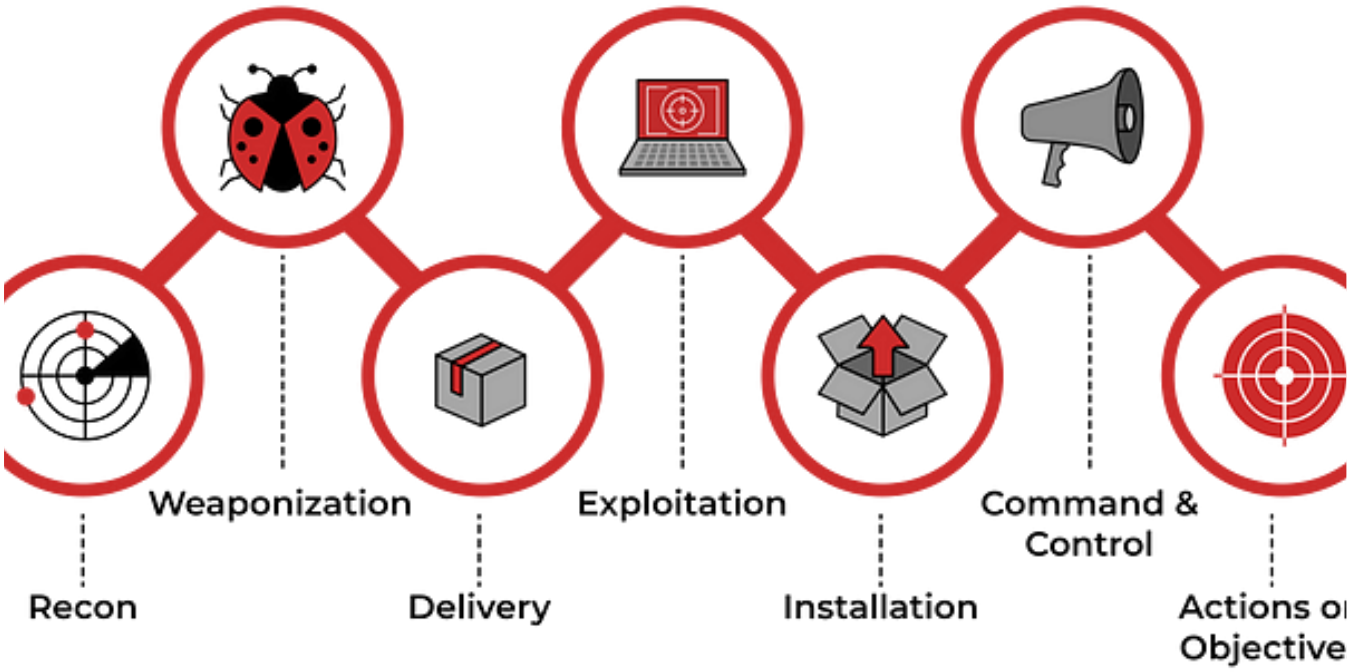



Haircutfish

### TryHackMe Investigating Windows — Task 1 Investigating Windows

A windows machine has been hacked, its your job to go investigate this windows machine and find clues to what the hacker might have done.

Nov 2, 2022 156 3

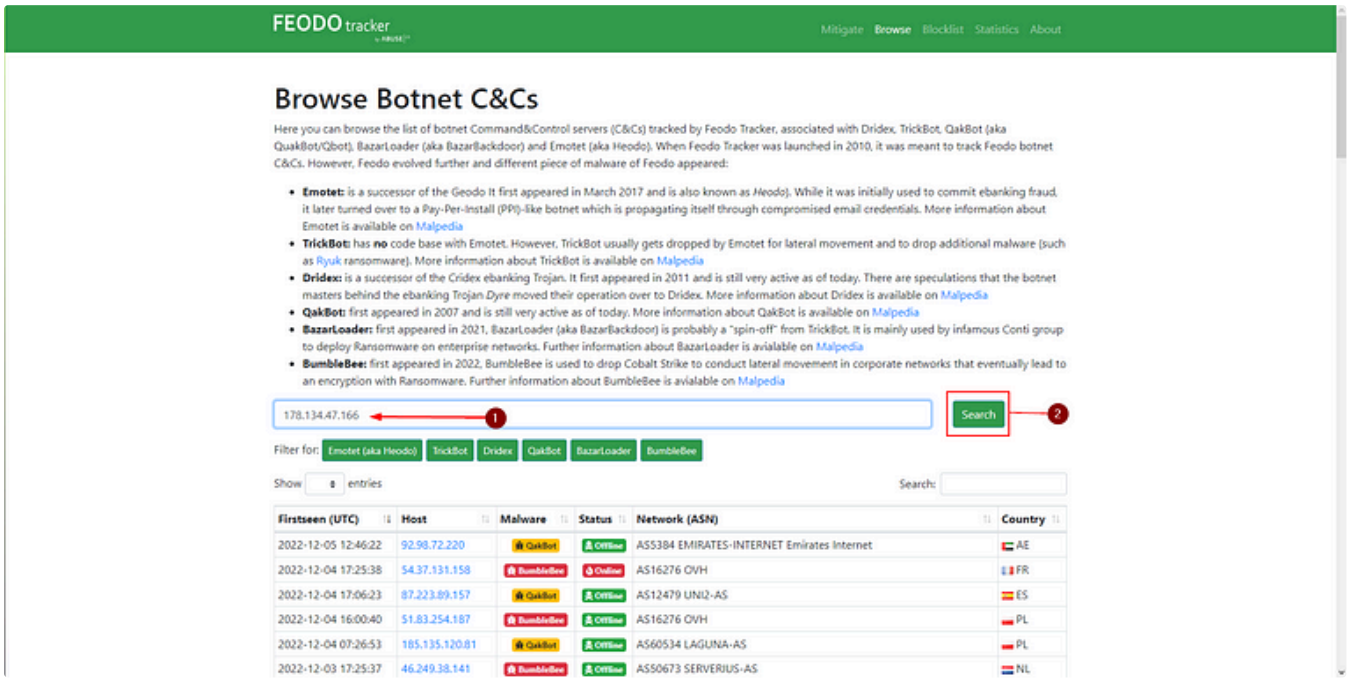


Haircutfish

## TryHackMe Cyber Kill Chain Room

The Cyber Kill Chain framework is designed for identification and prevention of the network intrusions. You will learn what the adversaries...

Nov 18, 2022 27 1




Haircutfish

## TryHackMe Threat Intelligence Tools — Task 4 Abuse.ch,

If you haven't done task 1, 2, & 3 yet, here is the link to my write-up it: Tools Task 1 Room Outline, Task 2 Threat Intelligence, and Task...

Dec 6, 2022 22

| | | |
|---|---|---|
| 2 | **Weaponization** | *Preparatory activities aimed at setting up the infrastructure required for the attack.* |
| 3 | **Delivery** | *Techniques resulting in the transmission of a weaponized object to the targeted environment.* |
| 4 | **Social Engineering** | *Techniques aimed at the manipulation of people to perform unsafe actions.* |
| 5 | **Exploitation** | *Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.* |
| 6 | **Persistence** | *Any access, action or change to a system that gives an attacker persistent presence on the system.* |
| 7 | **Defense Evasion** | *Techniques an attacker may specifically use for evading detection or avoiding other defenses.* |
| 8 | **Command & Control** | *Techniques that allow attackers to communicate with controlled systems within a target network.* |
| 9 | **Pivoting** | *Tunneling traffic through a controlled system to other systems that are not directly accessible.* |
| 10 | **Discovery** | *Techniques that allow an attacker to gain knowledge about a system and its network environment.* |
| 11 | **Privilege Escalation** | *The result of techniques that provide an attacker with higher permissions on a system or network.* |
| 12 | **Execution** | *Techniques that result in execution of attacker-controlled code on a local or remote system.* |
| 13 | **Credential Access** | *Techniques resulting in the access of, or control over, system, service or domain credentials.* |
| 14 | **Lateral Movement** | *Techniques that enable an adversary to horizontally access and control other remote systems.* |
| 15 | **Collection** | *Techniques used to identify and gather data from a target network prior to exfiltration.* |
| 16 | **Exfiltration** | *Techniques that result or aid in an attacker removing data from a target network.* |

Haircutfish

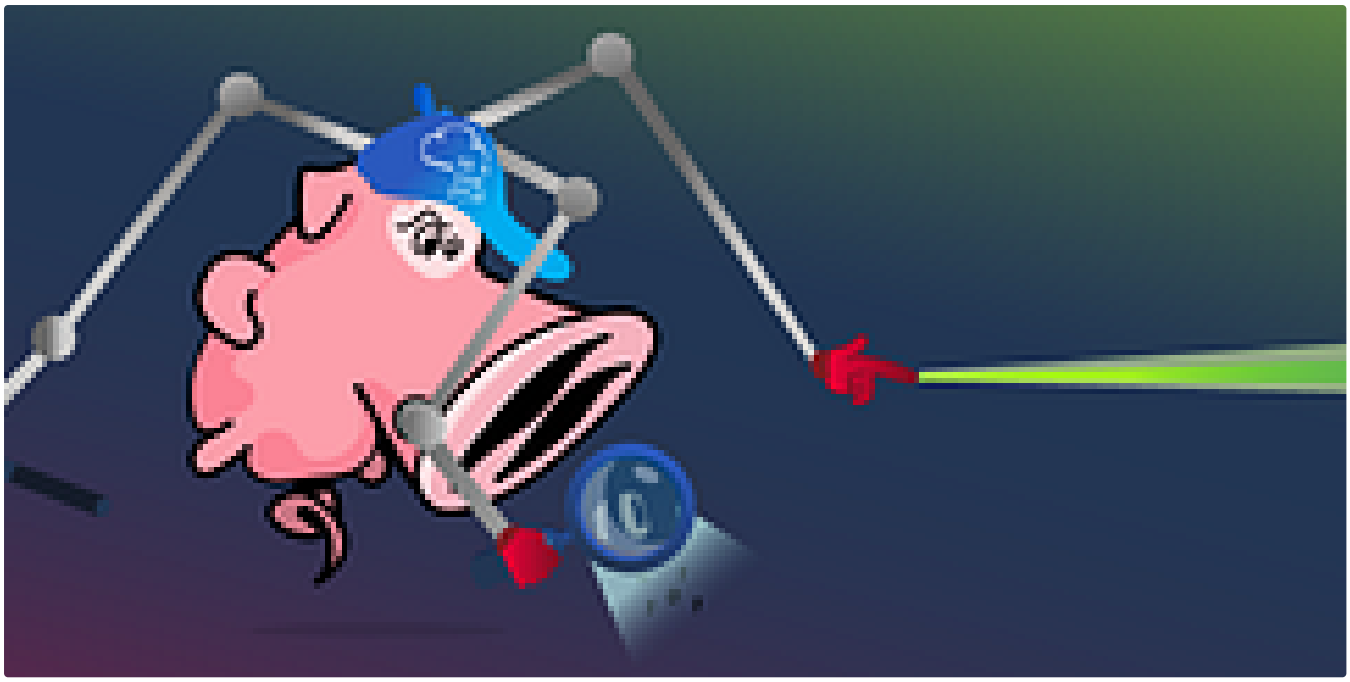
## TryHackMe Unified Kill Chain Room

The Unified Kill Chain is a framework which establishes the phases of an attack, and a means of identifying and mitigating risk to IT...

Nov 21, 2022 5

See all from Haircutfish

## Recommended from Medium



In T3CH by Axoloth

# TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

Trnty

# TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10

## Lists

### Staff picks

796 stories · 1558 saves

### Stories to Help You Level-Up at Work

19 stories · 912 saves

### Self-Improvement 101

20 stories · 3191 saves

### Productivity 101

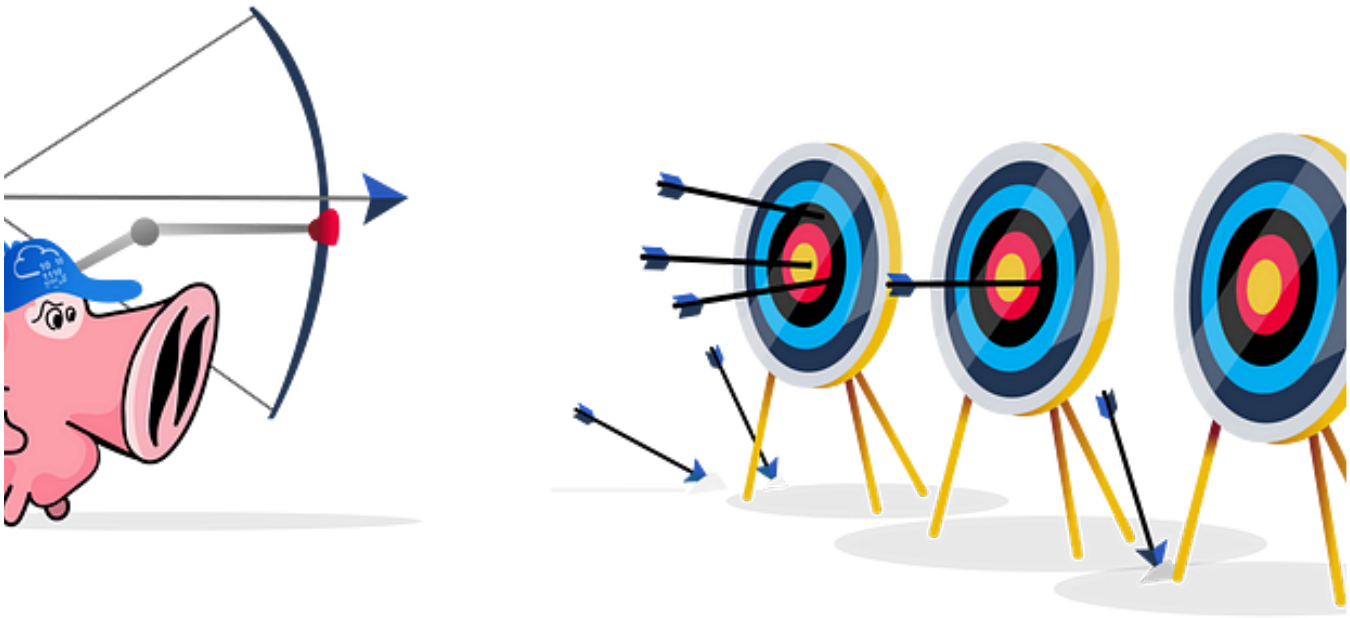
20 stories · 2705 saves

In T3CH by Axoloth

## TryHackMe | FlareVM: Arsenal of Tools| WriteUp

Learn the arsenal of investigative tools in FlareVM

Nov 28, 2024 50

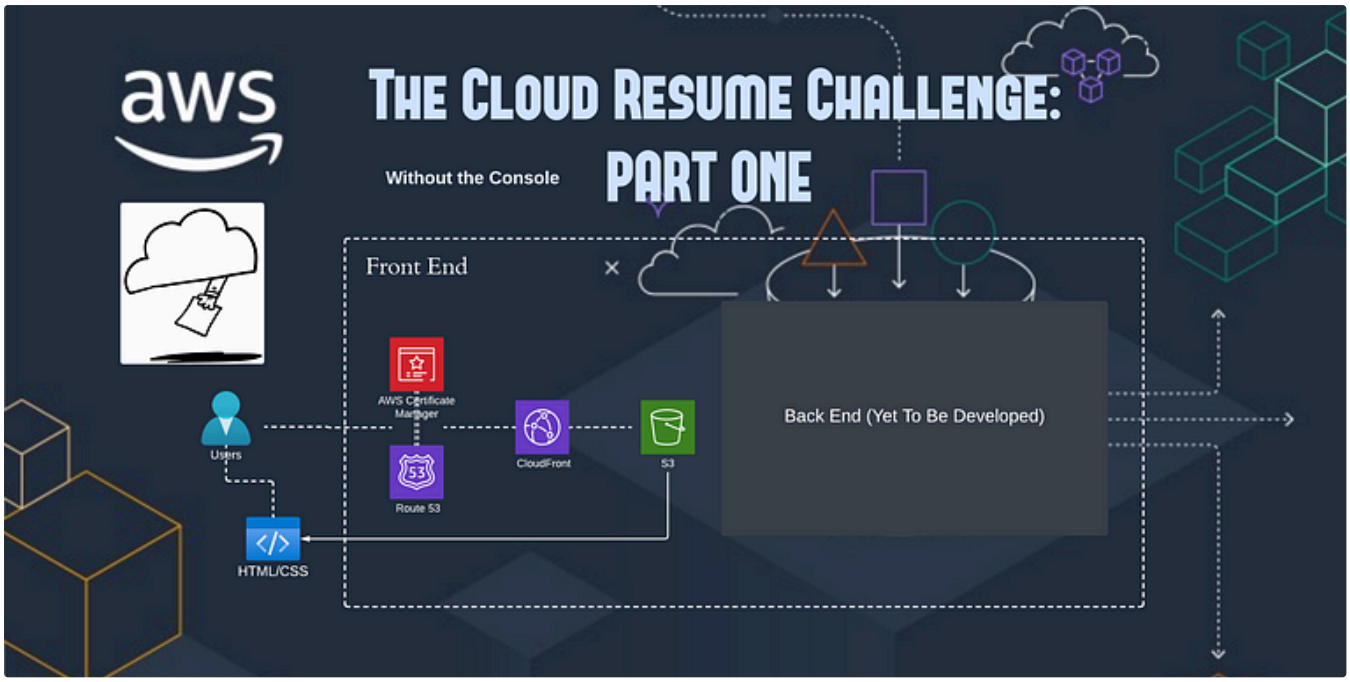


Manivel

## Snort Challenge—The Basics : TryHackMe—Medium

Snort Challenge—The Basics by TryHackMe. Writeup and Answers the question below

Dec 30, 2024 3

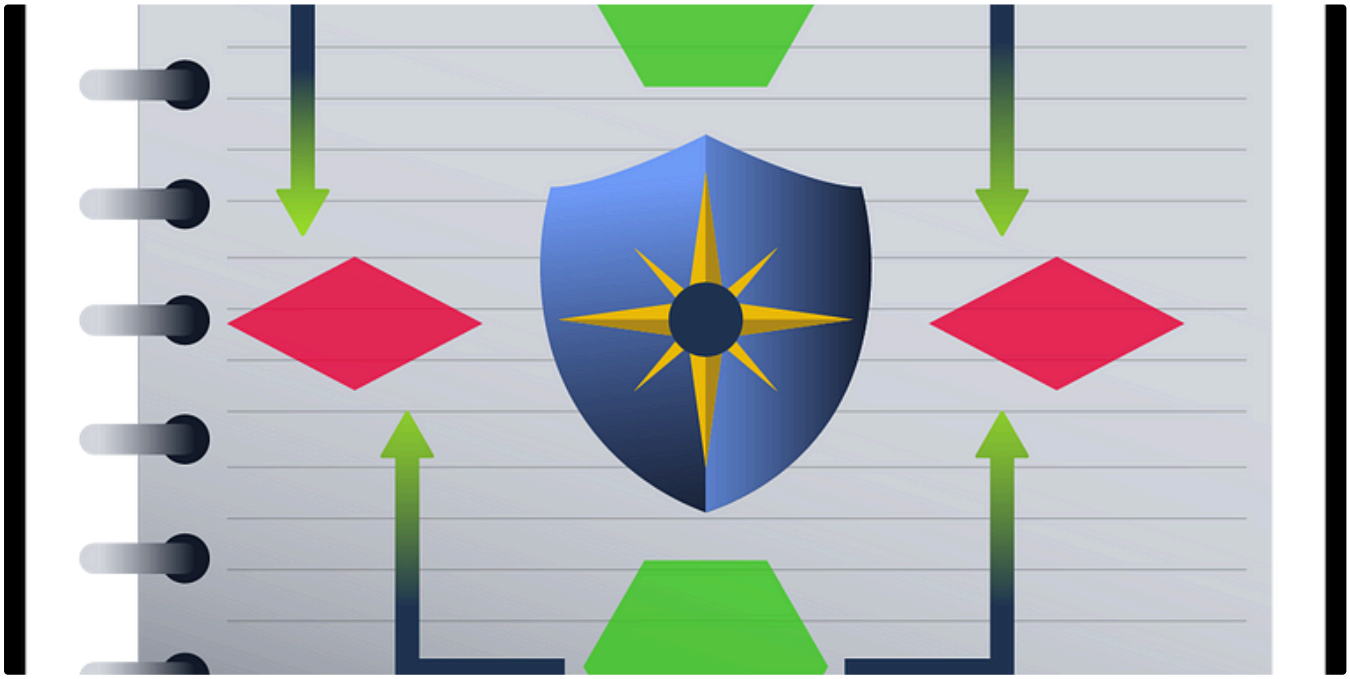



Gabriel Binion

## 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



Sunny Singh Verma [ SuNnY ]

## IR Playbooks TryHackMe Walkthrough Writeup THM |—SuNnY

Kudos to The Creators of this Room :

Sep 13, 2024 100 1


See more recommendations