

Course: Cloud and Network Security - C3 – 2025

Student Name: Johnmark Gichuki

Student No: CS-CNS10-25101

Sunday, September 28, 2025

Week 2 Assignment 2:

Class Exercise: Assignment 2 HTB Academy Introduction to Network Traffic Analysis

Table of Contents

Introduction.....	3
Step 1: Accessing the Module.....	4
Part 1: Network Traffic Analysis	4
Part 2: Networking Primer - Layers 1-4	5
Questions.....	5
Part 3: Networking Primer - Layers 5-7	6
Questions.....	6
Part 4: The Analysis Process	8
Part 5: Tcpdump Fundamentals.....	9
Questions.....	9
Part 6: Fundamentals Lab	11
Questions.....	11
Part 7: Tcpdump Packet Filtering.....	13
Questions.....	13
Part 8: Interrogating Network Traffic with Capture and Display Filters	13
Questions.....	13
Part 9: Analysis with Wireshark.....	14
Questions.....	14
Part 10: Wireshark Advanced Usage.....	16
Questions.....	16
Part 11: Packet Inception, Dissecting Network Traffic with Wireshark	17
Questions.....	17
Part 12: Guided Lab: Traffic Analysis Workflow	18
Questions.....	18
Part 13: Decrypting RDP connections	18
Questions.....	18
Module completion and Completion link	19
Conclusion	20

Introduction

The "Intro to Network Traffic Analysis (Tier 0)" module introduced me to the fundamental concepts of network traffic analysis, which is essential for both offensive and defensive cybersecurity practices. Network traffic analysis involves the collection and examination of real-time and historical data to understand network activities. For defenders, this skill helps in detecting suspicious activities, identifying vulnerabilities, and improving incident response. For offensive security practitioners, traffic analysis is useful for identifying weak points in protocols and configurations.

This module covered network traffic analysis principles, tcpdump fundamentals, working with Wireshark, and Wireshark filtering techniques. It also included hands-on exercises and labs to reinforce learning.

The primary tools explored were Wireshark, a graphical packet analysis tool, and tcpdump, a command-line tool for capturing and inspecting network traffic. These tools are commonly used to diagnose network issues, monitor suspicious activity, and perform penetration testing.

To successfully complete this module, a solid foundation in Linux fundamentals, basic networking, and web requests was necessary. By the end of this module, I developed practical skills in capturing, filtering, and analyzing network packets, which are critical for real-world cybersecurity roles such as SOC analysts, penetration testers, and network engineers.

Step 1: Accessing the Module

The screenshot shows the HTB Academy website in a web browser. The URL is `academy.hackthebox.com/module/details/81`. The page features a dark theme with a sidebar on the left containing a user profile for 'Jmark2002' (Free, 30 cubes) and a 'LEARN' menu with links to Dashboard, Exams, Modules, and Paths. The main content area is titled 'INTRO TO NETWORK TRAFFIC ANALYSIS' and includes an 'Unlock' button. Below this is a card for the module, 'Intro to Network Traffic Analysis', which is Tier 0, Medium difficulty, General category, and 8 hours long. The card includes a description: 'Network traffic analysis is used by security teams to monitor network activity and look for anomalies that could indicate security and operational issues. Offensive security practitioners can use network traffic analysis to search for sensitive data such as credentials, hidden applications, reachable network segments, or other potentially sensitive information "on the wire." Network traffic analysis has many uses for attackers and defenders alike.' It also shows a 5-star rating and is created by 'TreyCraf7_1'. The Windows taskbar at the bottom shows the time as 14:26 on 26/09/2025.

Part 1: Network Traffic Analysis

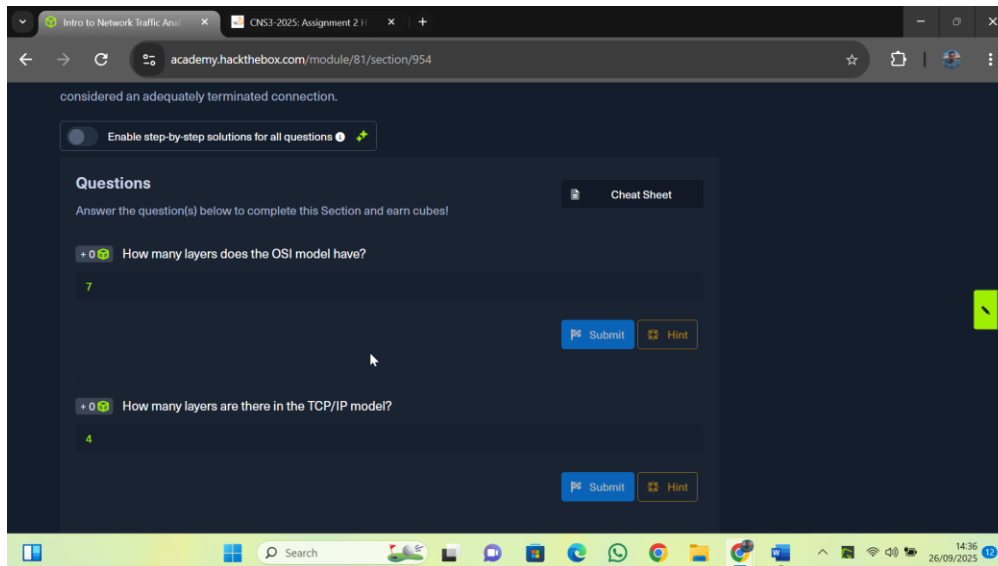
The screenshot shows the HTB Academy website in a web browser, displaying the content of the 'Intro to Network Traffic Analysis' module. The URL is `academy.hackthebox.com/module/81/section/773`. The page features a dark theme with a sidebar on the left containing a user profile for 'Jmark2002' and a 'LEARN' menu. The main content area is titled 'INTRO TO NETWORK TRAFFIC ANALYSIS' and includes a 'Page 1 / Network Traffic Analysis' indicator. The main heading is 'Network Traffic Analysis'. Below this is a paragraph describing Network Traffic Analysis (NTA): 'Network Traffic Analysis (NTA) can be described as the act of examining network traffic to characterize common ports and protocols utilized, establish a baseline for our environment, monitor and respond to threats, and ensure the greatest possible insight into our organization's network.' This is followed by another paragraph: 'This process helps security specialists determine anomalies, including security threats in the network, early and effectively pinpoint threats. Network Traffic Analysis can also facilitate the process of meeting security guidelines. Attackers update their tactics frequently to avoid detection and leverage legitimate credentials with tools that most companies allow in their networks, making detection and, subsequently, response challenging for defenders. In such cases, Network Traffic Analysis can again prove helpful. Everyday use cases of NTA include:'. On the right side, there is a sidebar with a 'Cheat Sheet' button, a 'Resources' button, and a 'Table of Contents' section. The 'Table of Contents' includes links to 'Introduction', 'Network Traffic Analysis' (which is highlighted), 'Networking Primer - Layers 1-4', and 'Networking Primer - Layers 5-7'. The Windows taskbar at the bottom shows the time as 14:29 on 26/09/2025.

Part 2: Networking Primer - Layers 1-4

This section provided a refresher on fundamental networking concepts, focusing on the first four layers of the OSI (Open Systems Interconnection) model. Understanding these layers is essential for accurately capturing and analyzing network traffic, as each layer plays a unique role in data communication.

Questions

1. How many layers does the OSI model have? [7 Layers](#)
2. How many layers are there in the TCP/IP model? [4 layers](#)



3. True or False: Routers operate at layer 2 of the OSI model? [False](#)
4. What addressing mechanism is used at the Link Layer of the TCP/IP model?
[MAC-Address](#)
5. At what layer of the OSI model is a PDU encapsulated into a packet? (the number)
[3](#)
6. What addressing mechanism utilizes a 32-bit address? [IPv4](#)
7. What Transport layer protocol is connection oriented? [TCP](#)
8. What Transport Layer protocol is considered unreliable? [UDP](#)
9. TCP's three-way handshake consists of 3 packets: 1.Syn, 2.Syn & ACK, 3. _? What is the final packet of the handshake?
[ACK](#)

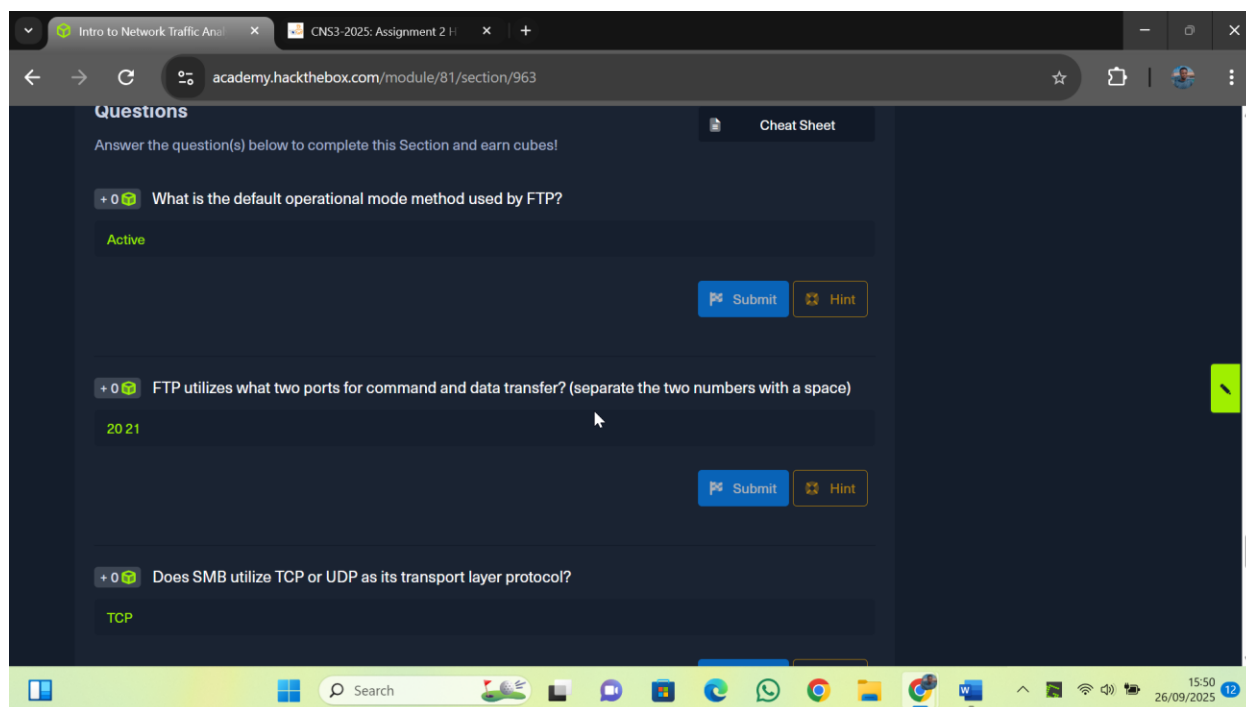


Part 3: Networking Primer - Layers 5-7

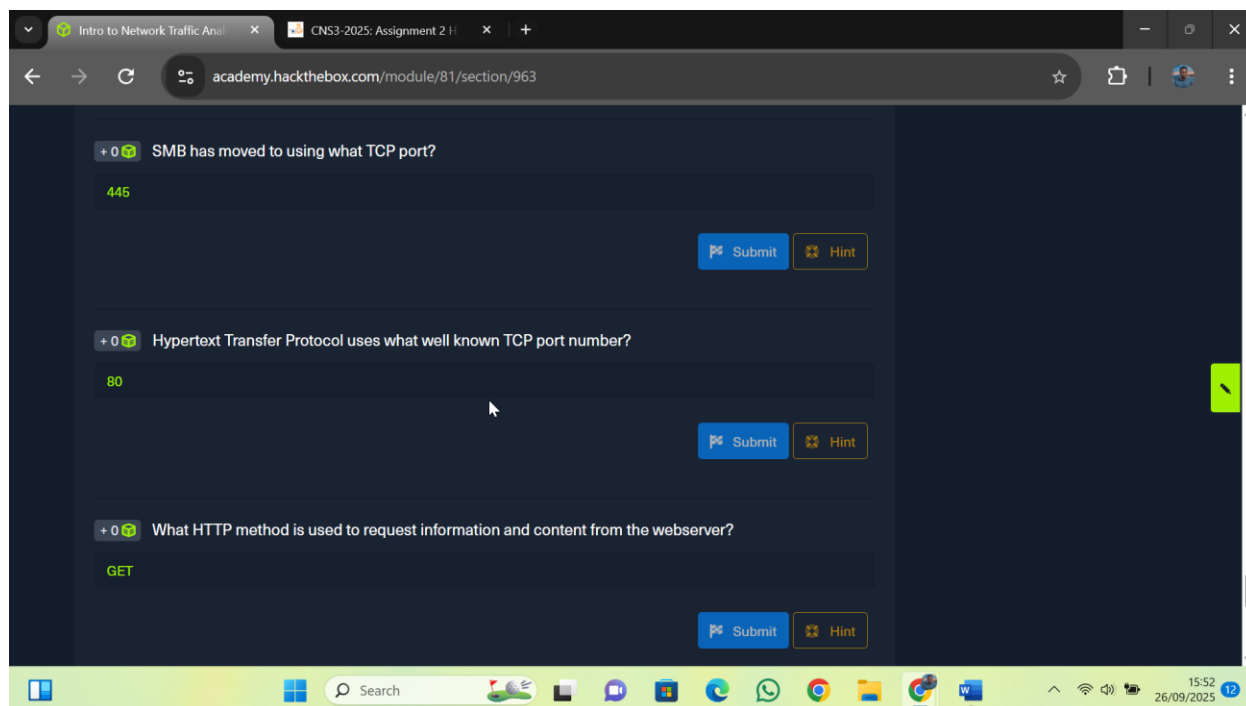
In this section, we move beyond the lower layers of the OSI model, which focus on how data is physically transmitted, routed, and delivered, to explore the upper layers (Layers 5–7). These layers are responsible for how applications interact across a network, ensuring that communication between devices is smooth, secure, and meaningful for end users. While there are many protocols and services at these layers, this section focused on a few key protocols that are critical for maintaining and managing network connections.

Questions

1. What is the default operational mode method used by FTP? [Active](#)
2. FTP utilizes what two ports for command and data transfer? (separate the two numbers with a space) [20 21](#)
3. Does SMB utilize TCP or UDP as its transport layer protocol? [TCP](#)

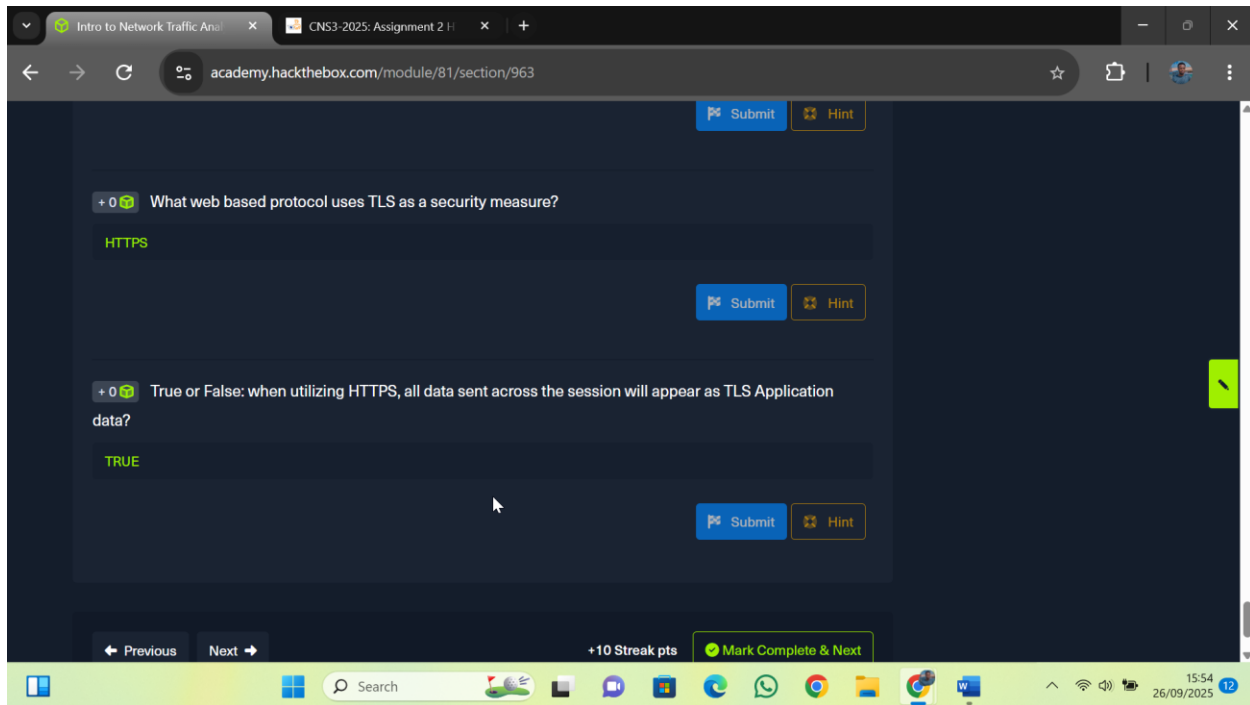


4. SMB has moved to using what TCP port? [445](#)
5. Hypertext Transfer Protocol uses what well known TCP port number? [80](#)
6. What HTTP method is used to request information and content from the webserver? [GET](#)



7. What web-based protocol uses TLS as a security measure? [HTTPS](#)

8. True or False: when utilizing HTTPS, all data sent across the session will appear as TLS Application data? **TRUE**



Part 4: The Analysis Process

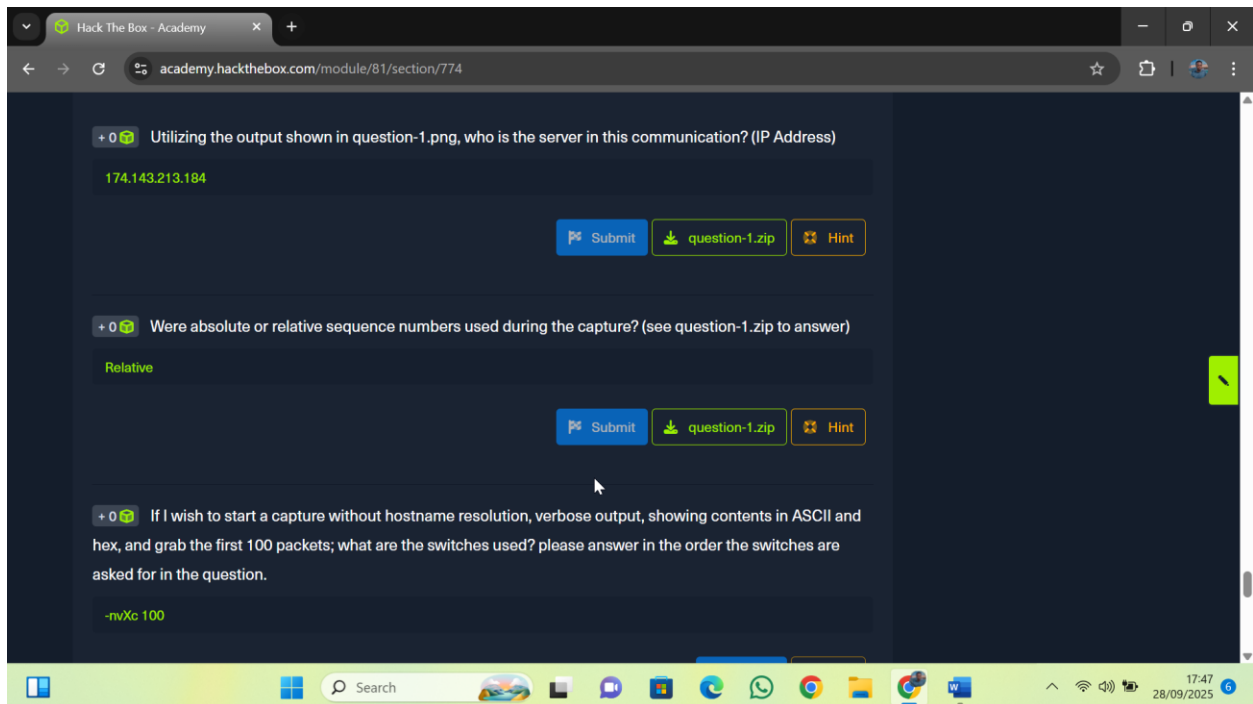
Network Traffic Analysis (NTA) is an essential process in cybersecurity that involves monitoring, capturing, and analyzing network data to identify irregularities, troubleshoot problems, and prevent potential attacks. It provides visibility into network operations, allowing administrators to establish a baseline of normal activity and quickly detect suspicious behavior. This visibility is vital for both defensive security and daily operations, helping organizations identify malicious traffic, such as unauthorized remote access attempts, and fix issues like connectivity problems. By combining NTA with advanced tools like firewalls, intrusion detection systems (IDS/IPS), and platforms like Splunk or ELK Stack, analysts can quickly detect and respond to threats, making network monitoring a proactive defense measure.

There are two main approaches to traffic analysis: **passive** and **active**. Passive capture involves copying traffic without interfering with it, often through mirrored ports, while active capture, also known as in-line capturing, requires inserting devices like network taps directly into the traffic flow. Each method has unique dependencies, such as permissions, specialized hardware, storage space, and processing power. Establishing a network baseline is crucial to filter out normal traffic and quickly identify anomalies. For example, noticing two user computers communicating over unusual ports could indicate a breach. Overall, NTA is a dynamic skill that requires both automated tools and human expertise to effectively secure networks and ensure smooth daily operations.

Part 5: Tcpdump Fundamentals

Questions

1. Utilizing the output shown in question-1.png, who is the server in this communication? (IP Address) [174.143.213.184](#)
2. Were absolute or relative sequence numbers used during the capture? (see question-1.zip to answer) [Relative](#)
3. If I wish to start a capture without hostname resolution, verbose output, showing contents in ASCII and hex, and grab the first 100 packets; what are the switches used? please answer in the order the switches are asked for in the question. [-nvXc 100](#)



4. Given the capture file at /tmp/capture.pcap, what tcpdump command will enable you to read from the capture and show the output contents in Hex and ASCII? (Please use best practices when using switches) [sudo tcpdump -Xr /tmp/capture.pcap](#)
5. What TCPDump switch will increase the verbosity of our output? (Include the - with the proper switch) [-v](#)
6. What built in terminal help reference can tell us more about TCPDump? [Man](#)

The screenshot shows a web browser window with the URL `academy.hackthebox.com/module/81/section/774`. The page contains three questions, each with a "Submit" and "Hint" button. The first question asks for a tcpdump command to read a capture file and show output in Hex and ASCII, with the answer `sudo tcpdump -Xr /tmp/capture.pcap`. The second question asks for a TCPDump switch to increase verbosity, with the answer `-v`. The third question asks for a built-in terminal help reference, with the answer `man`. The Windows taskbar at the bottom shows the time as 17:47 on 28/09/2025.

Given the capture file at `/tmp/capture.pcap`, what tcpdump command will enable you to read from the capture and show the output contents in Hex and ASCII? (Please use best practices when using switches)

```
sudo tcpdump -Xr /tmp/capture.pcap
```

Submit Hint

What TCPDump switch will increase the verbosity of our output? (Include the - with the proper switch)

```
-v
```

Submit Hint

What built in terminal help reference can tell us more about TCPDump?

```
man
```

Submit Hint

7. What TCPDump switch will let me write my output to a file? `-w`

This screenshot shows the same Hack The Box Academy interface, but the third question is now visible: "What TCPDump switch will let me write my output to a file?" with the answer `-w`. Below the question are "Submit" and "Hint" buttons. At the bottom of the question area, there are navigation buttons: "Previous", "Next", and a green button labeled "+10 Streak pts Mark Complete & Next". The Windows taskbar at the bottom shows the time as 17:48 on 28/09/2025.

What built in terminal help reference can tell us more about TCPDump?

```
man
```

Submit Hint

What TCPDump switch will let me write my output to a file?

```
-w
```

Submit Hint

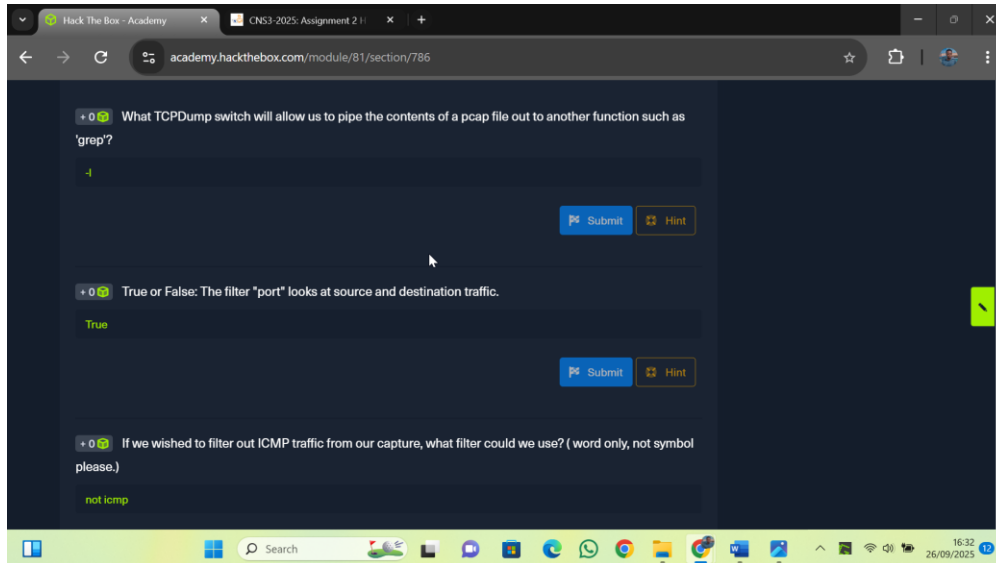
← Previous Next → +10 Streak pts Mark Complete & Next

Powered by HACKTHEBOX

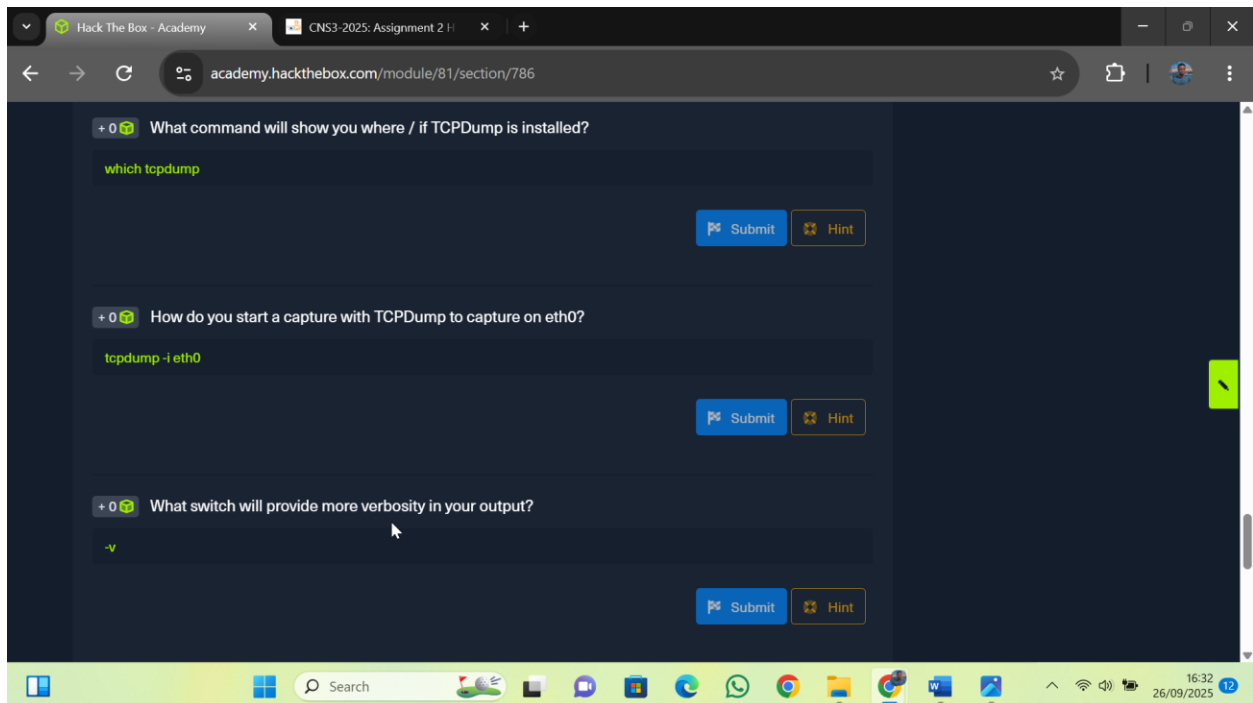
Part 6: Fundamentals Lab

Questions

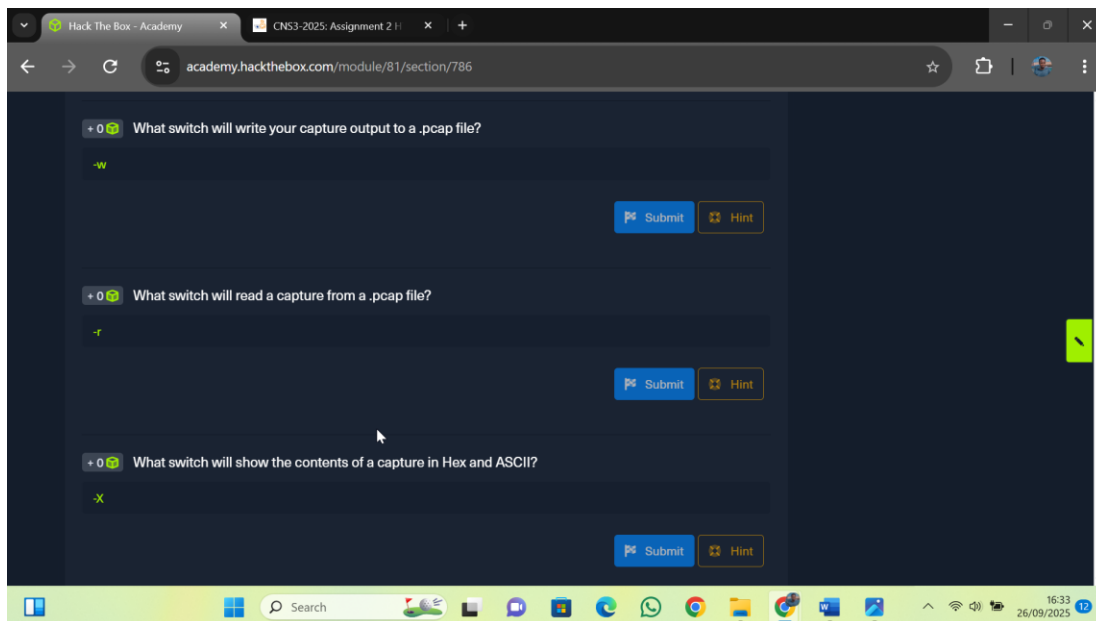
1. What TCPDump switch will allow us to pipe the contents of a pcap file out to another function such as 'grep'? `-l`
2. True or False: The filter "port" looks at source and destination traffic. `True`
3. If we wished to filter out ICMP traffic from our capture, what filter could we use? (word only, not symbol please.) `not icmp`



4. What command will show you where / if TCPDump is installed? `which tcpdump`
5. How do you start a capture with TCPDump to capture on eth0? `tcpdump -i eth0`
6. What switch will provide more verbosity in your output? `-v`



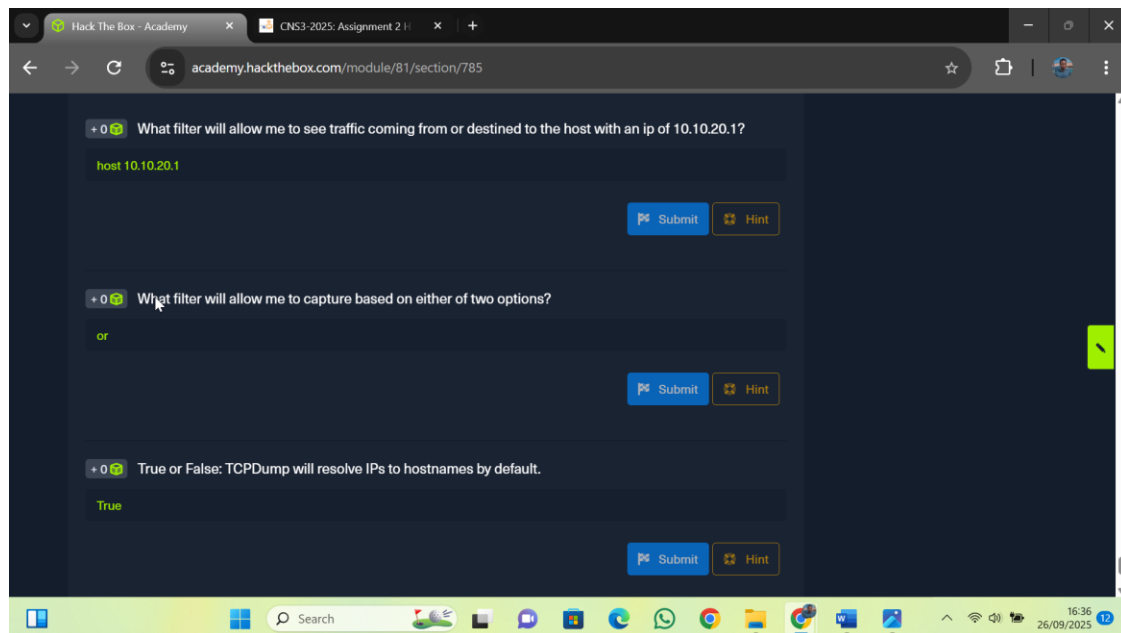
7. What switch will write your capture output to a .pcap file? `-w`
8. What switch will read a capture from a .pcap file? `-r`
9. What switch will show the contents of a capture in Hex and ASCII? `-X`



Part 7: Tcpdump Packet Filtering

Questions

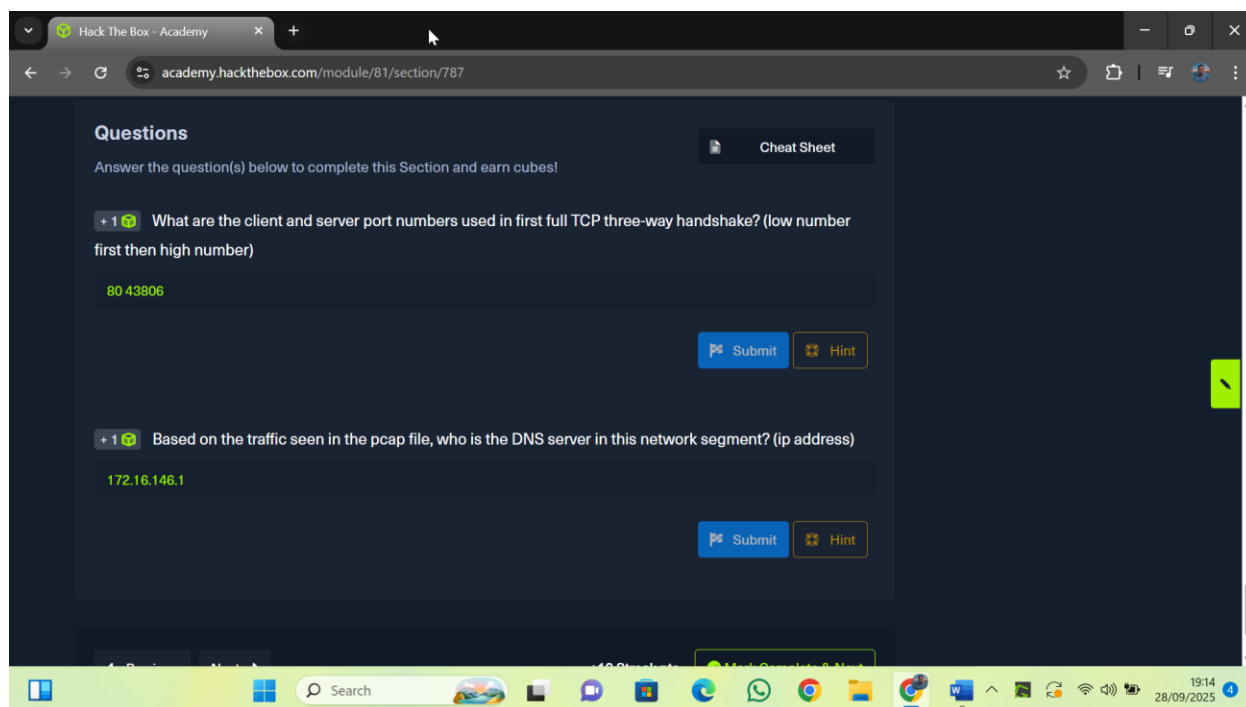
1. What filter will allow me to see traffic coming from or destined to the host with an ip of 10.10.20.1? [host 10.10.20.1](#)
2. What filter will allow me to capture based on either of two options? [Or](#)
3. True or False: TCPDump will resolve IPs to hostnames by default. [True](#)



Part 8: Interrogating Network Traffic with Capture and Display Filters

Questions

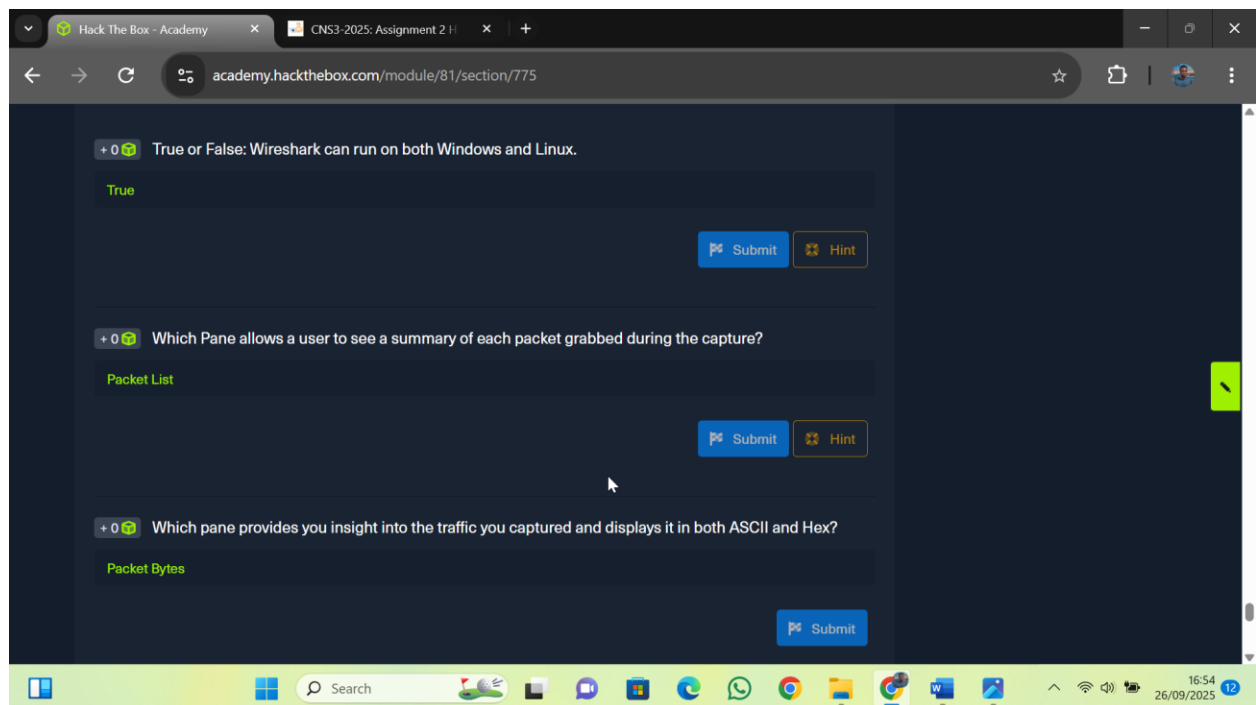
1. What are the client and server port numbers used in first full TCP three-way handshake? (low number first then high number) [80 43806](#)
2. Based on the traffic seen in the pcap file, who is the DNS server in this network segment? (ip address) [172.16.146.1](#)



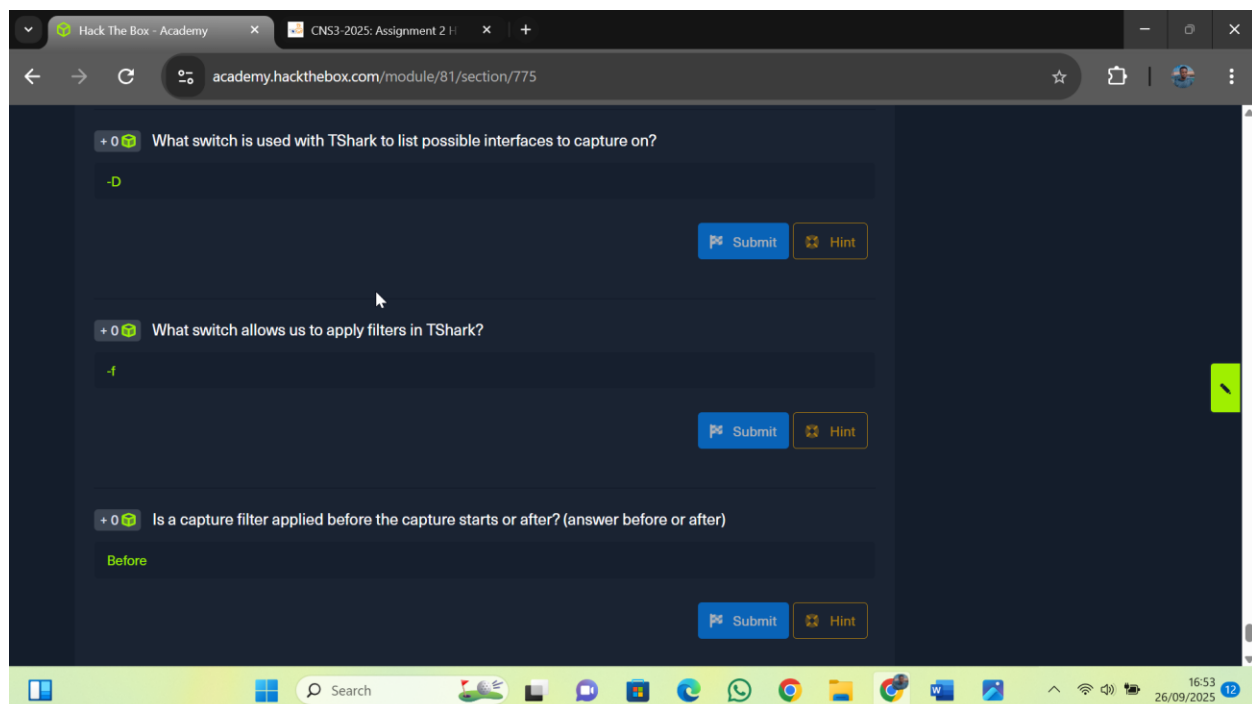
Part 9: Analysis with Wireshark

Questions

1. True or False: Wireshark can run on both Windows and Linux. [True](#)
2. Which Pane allows a user to see a summary of each packet grabbed during the capture?
[Packet List](#)
3. Which pane provides you insight into the traffic you captured and displays it in both ASCII and Hex? [Packet Bytes](#)



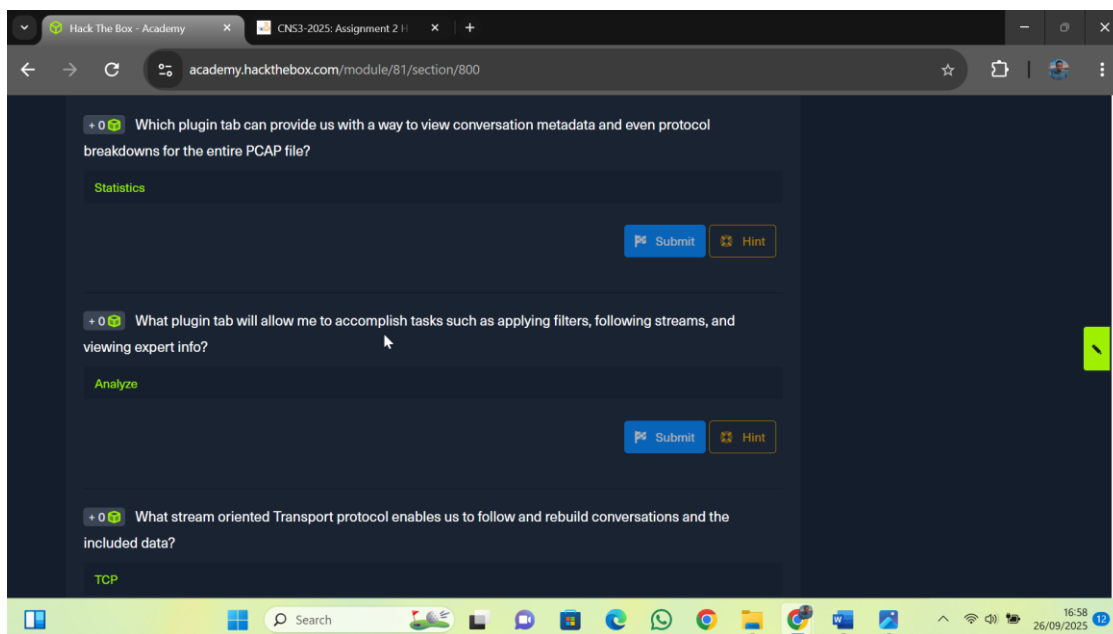
4. What switch is used with TShark to list possible interfaces to capture on? -D
5. What switch allows us to apply filters in TShark? -f
6. Is a capture filter applied before the capture starts or after? (answer before or after)
Before



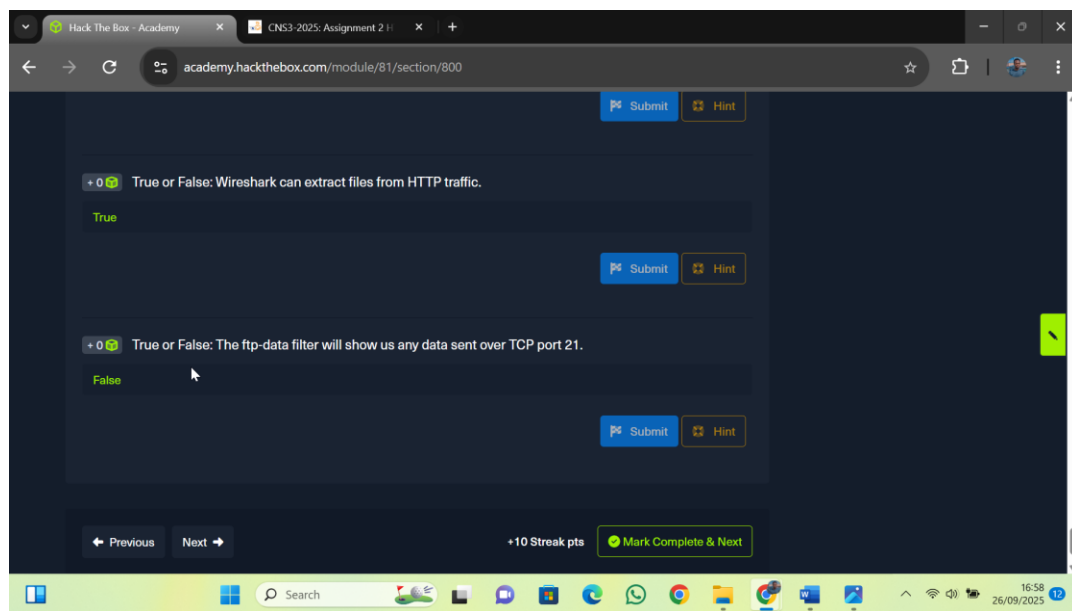
Part 10: Wireshark Advanced Usage

Questions

1. Which plugin tab can provide us with a way to view conversation metadata and even protocol breakdowns for the entire PCAP file? [Statistics](#)
2. What plugin tab will allow me to accomplish tasks such as applying filters, following streams, and viewing expert info? [Analyze](#)
3. What stream oriented Transport protocol enables us to follow and rebuild conversations and the included data? [TCP](#)



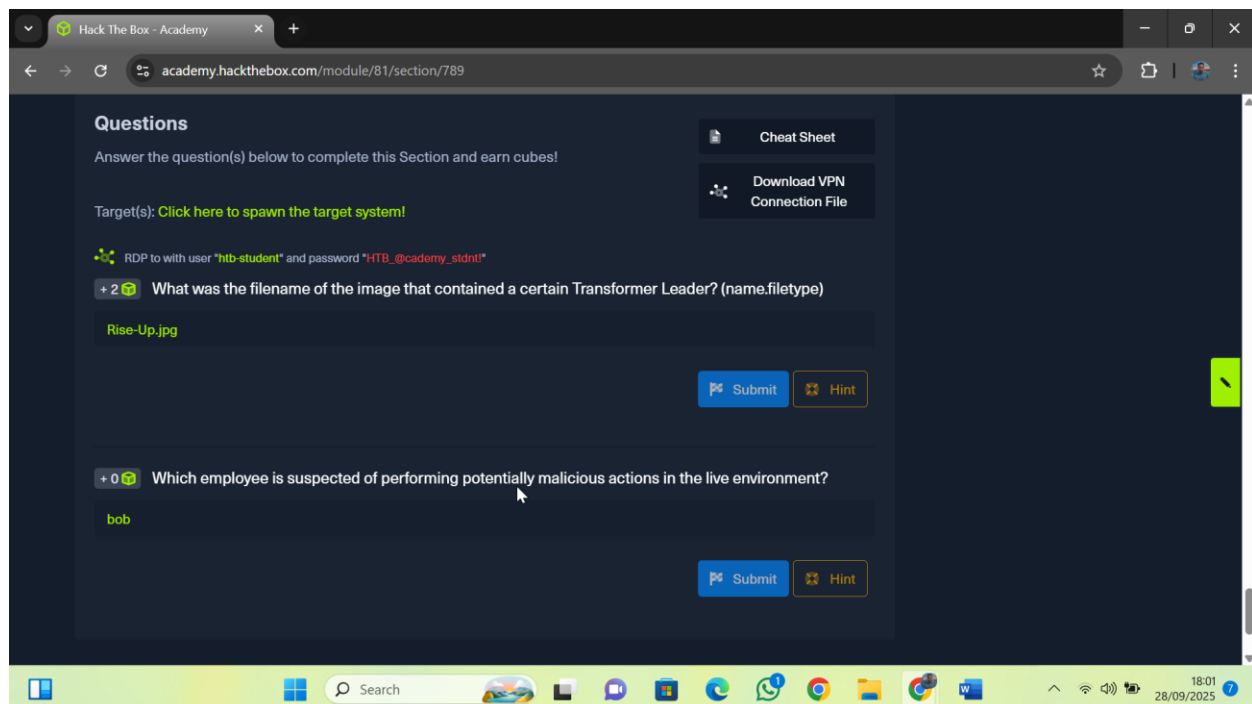
4. True or False: Wireshark can extract files from HTTP traffic. [True](#)
5. True or False: The ftp-data filter will show us any data sent over TCP port 21. [False](#)



Part 11: Packet Inception, Dissecting Network Traffic with Wireshark

Questions

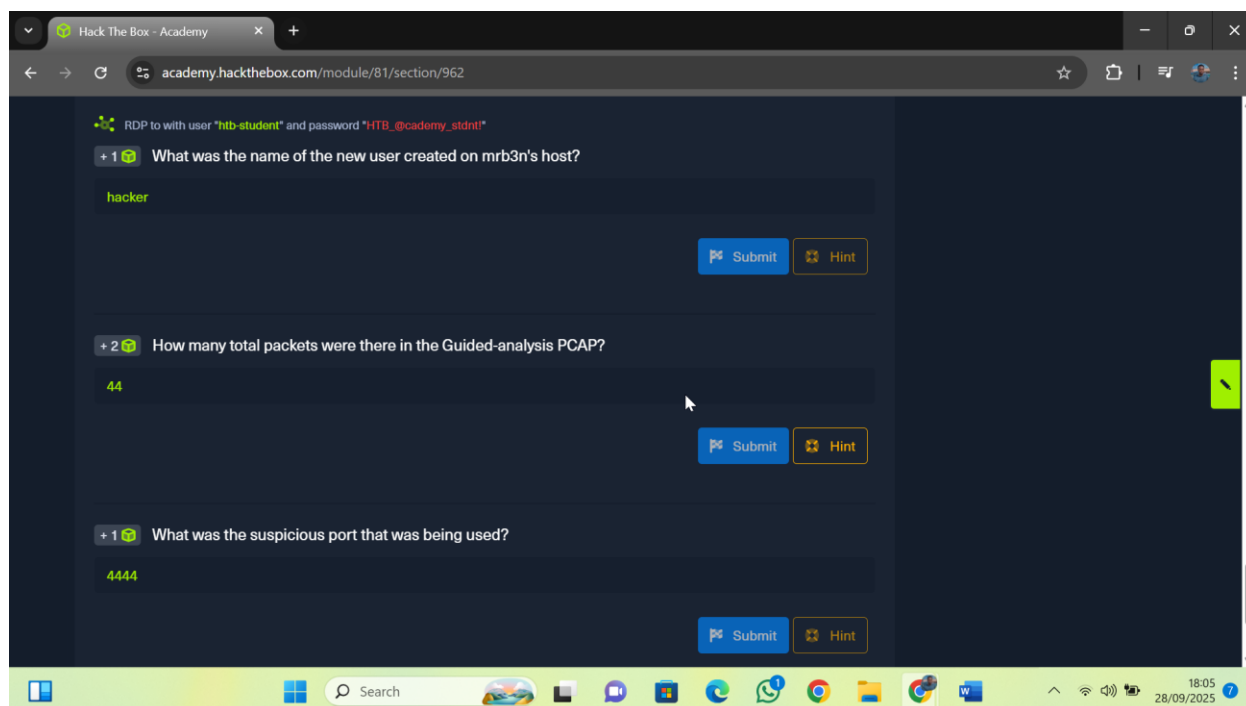
1. What was the filename of the image that contained a certain Transformer Leader?
(name.filetype) **Rise-Up.jpg**
2. Which employee is suspected of performing potentially malicious actions in the live environment? **Bob**



Part 12: Guided Lab: Traffic Analysis Workflow

Questions

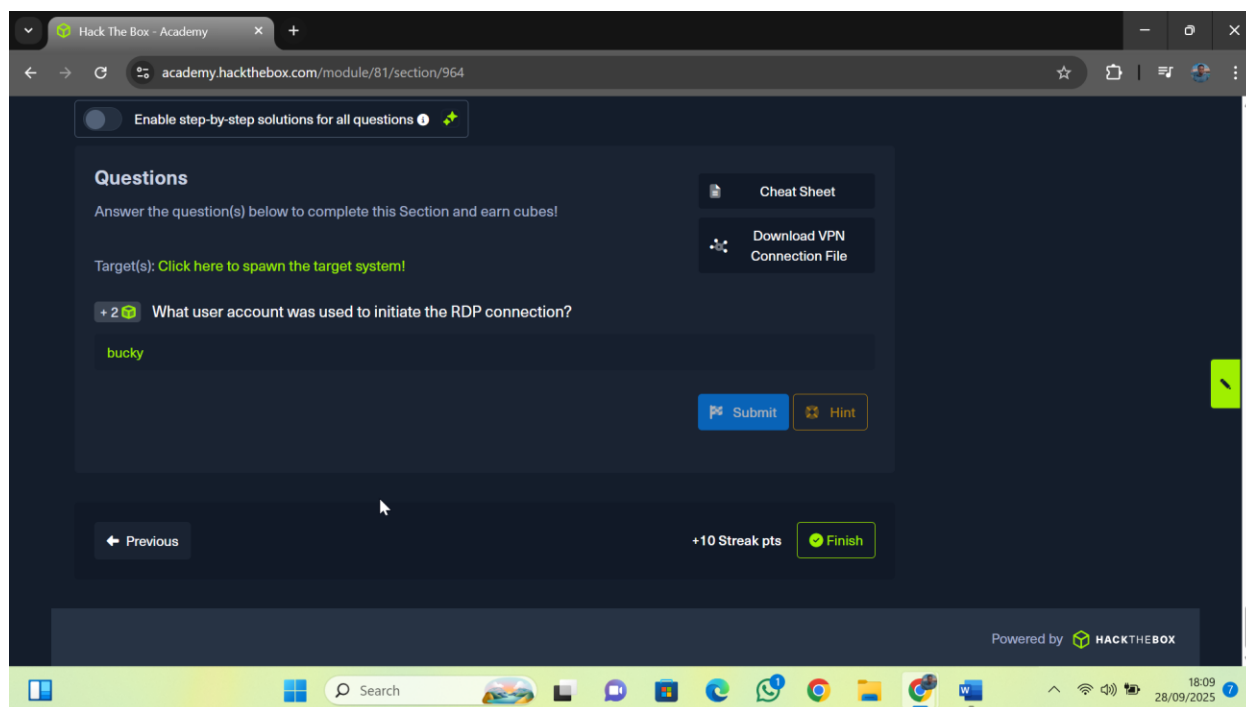
1. What was the name of the new user created on mrb3n's host? [hacker](#)
2. How many total packets were there in the Guided-analysis PCAP? [44](#)
3. What was the suspicious port that was being used? [4444](#)



Part 13: Decrypting RDP connections

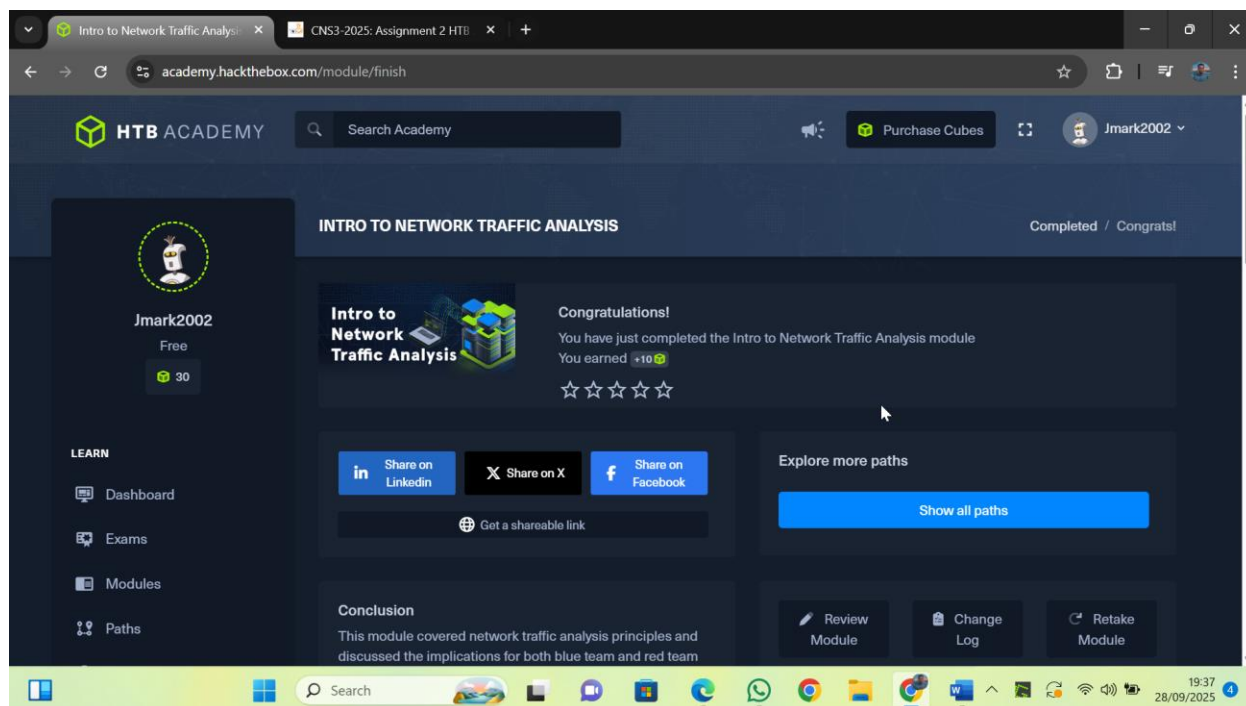
Questions

1. What user account was used to initiate the RDP connection? [bucky](#)



Module completion and Completion link:

<https://academy.hackthebox.com/achievement/2178420/81>



Conclusion

Through this assignment, I gained a deeper understanding of network traffic analysis and the important role it plays in both offensive and defensive cybersecurity. I learned how to identify, capture, and analyze network traffic using tools like Wireshark and tcpdump, as well as how to apply different filters to pinpoint suspicious or malicious activities. The module gave me a clear view of how network communication works, including how protocols such as TCP, HTTP, FTP, and SMB function within the OSI and TCP/IP models. This knowledge helped me better interpret packet data and understand the flow of information across a network.