

**Course: Cloud and Network Security-C1-2026**  
**Cyber Shujaa Program**

**Week 2: Assignment 2 HTB Academy:  
Introduction to Network Traffic Analysis**

**Student Name:** Salim Katana Karuku

**Student ID:** CS-CNS11-26048

## Table of Contents

Course: Cloud and Network Security-C1-2026 .....	1
Cyber Shujaa Program.....	1
Week 2:Assignment 2 HTB Academy: Introduction to Network Traffic Analysis .....	1
Introduction .....	3
Objectives .....	4
1. The name of the new user created on mrb3n's host .....	5
2. Total packets that were there in the Guided analysis PCAP .....	5
3. The suspicious port that was being used .....	6
Conclusion .....	7

## Introduction

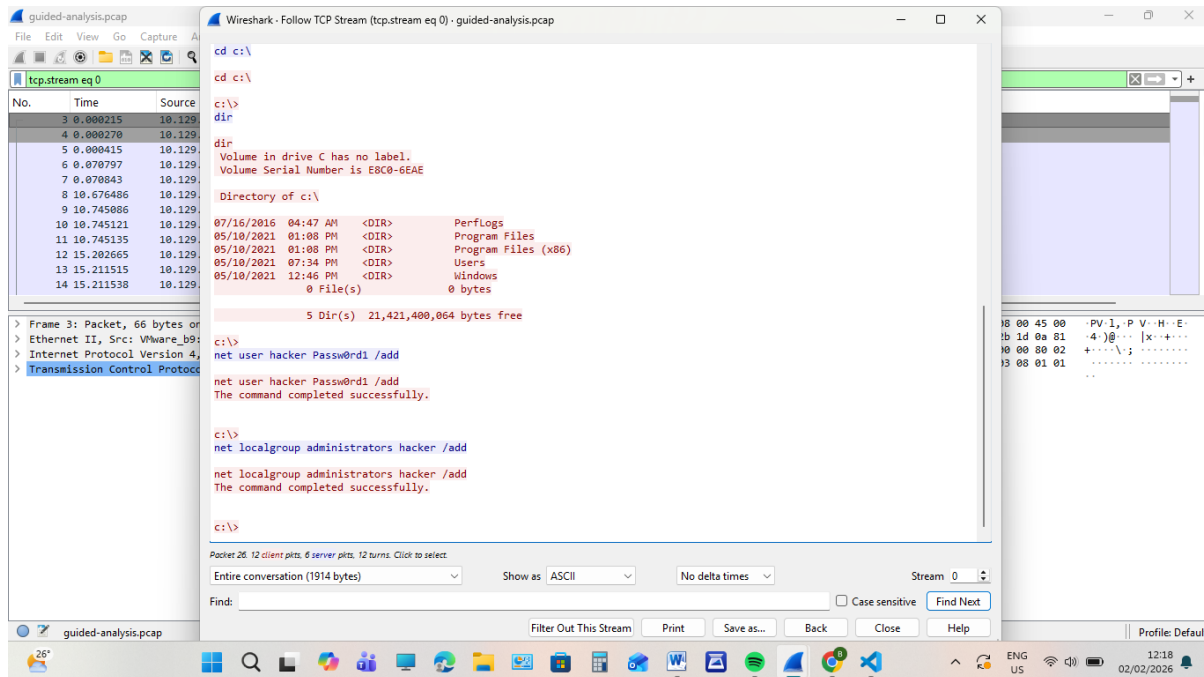
This assignment was carried out to help me develop a foundational understanding of network traffic, common network protocols and packet analysis techniques. The module introduces practical tools used to capture and analyse network traffic, enabling learners to observe real network behaviour.

## Objectives

The objectives of the assignment were:

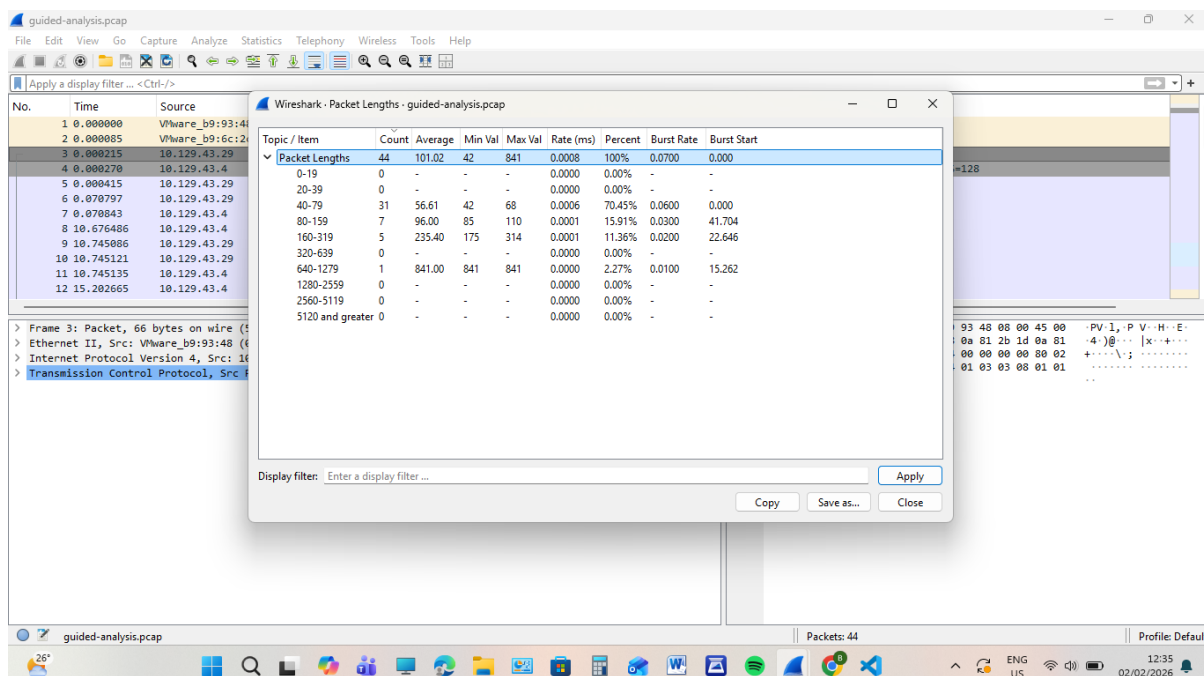
1. To understand the concept of network traffic analysis
2. To identify and understand common network protocols
3. To learn how to capture and analyse network traffic
4. To interpret packet data
5. To apply theoretical knowledge through practical exercises
6. To develop foundational skills in traffic monitoring and incident analysis

## 1. The name of the new user created on mrb3n's host



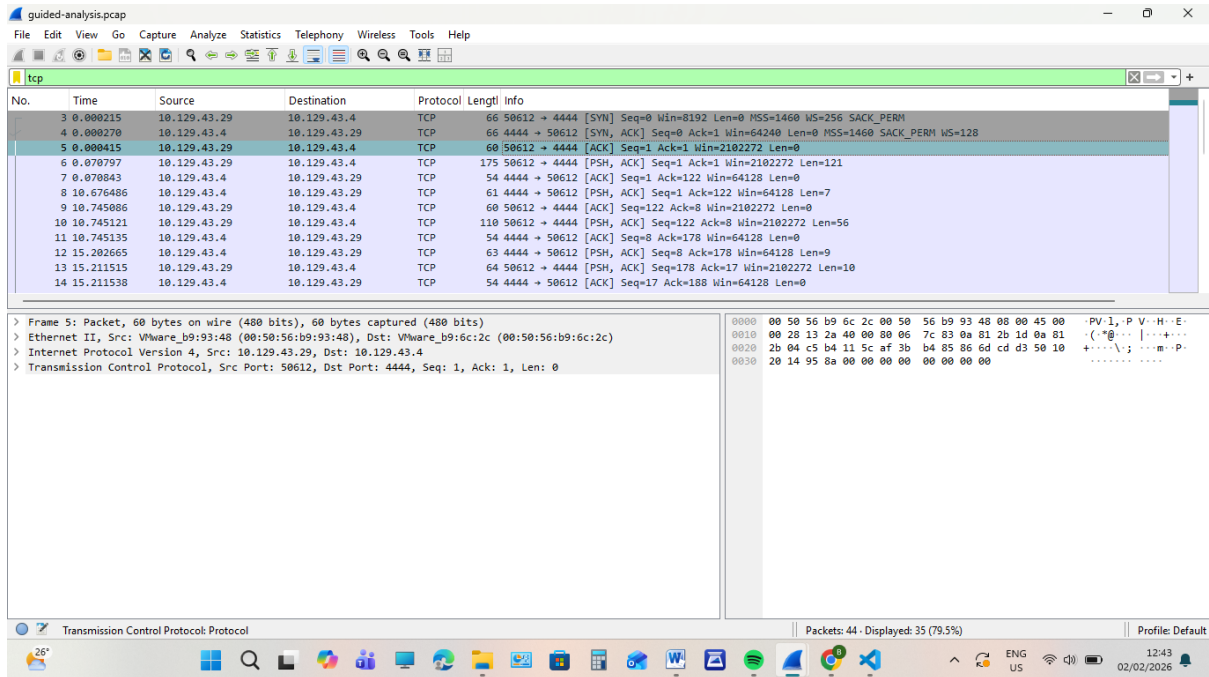
Then name of the user created in the user mrb3n's host is hacker

## 2. Total packets that were there in the Guided analysis PCAP



After click and know the number of packets I found out that were 44

### 3. The suspicious port that was being used



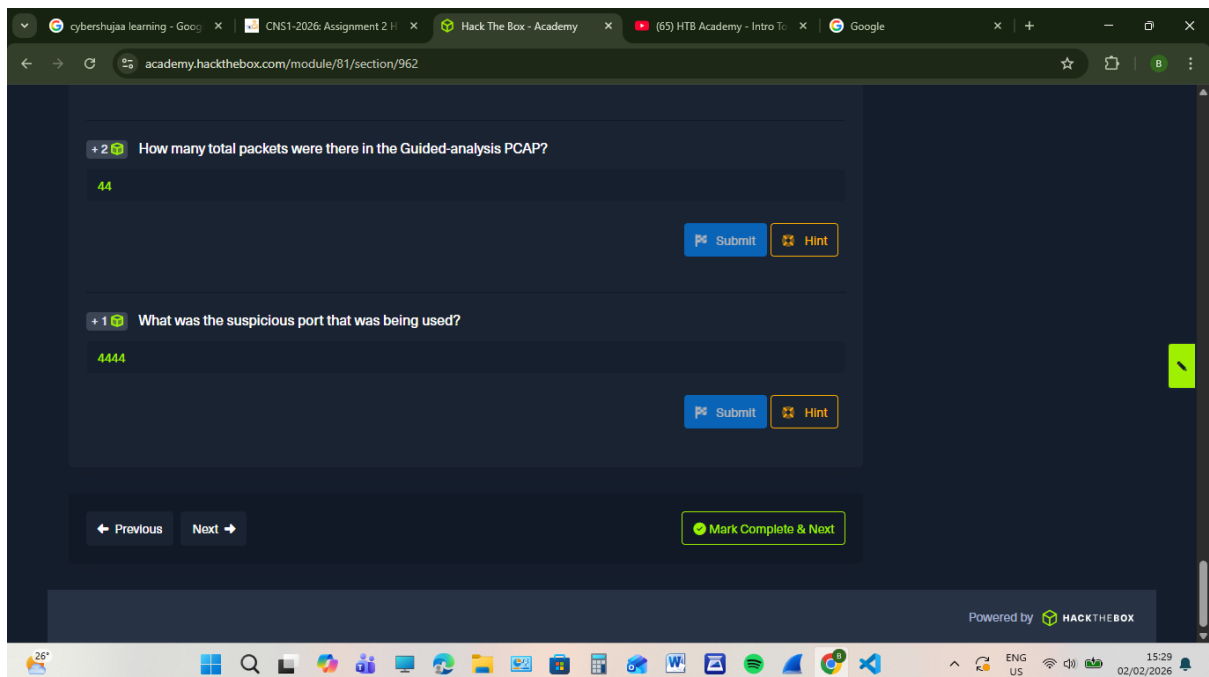
The screenshot shows a Wireshark packet capture of a file named 'guided-analysis.pcap'. The 'tcp' filter is applied, and the packet list shows several TCP connections. The packet details pane for packet 5 (Frame 5) is expanded, showing the following information:

- Frame 5: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
- Ethernet II, Src: VMware\_b9:93:48 (00:50:56:b9:93:48), Dst: VMware\_b9:6c:2c (00:50:56:b9:6c:2c)
- Internet Protocol Version 4, Src: 10.129.43.29, Dst: 10.129.43.4
- Transmission Control Protocol, Src Port: 50612, Dst Port: 4444, Seq: 1, Ack: 1, Len: 0

The packet bytes pane shows the raw data of the packet, which is a SYN packet (0000 00 50 56 b9 6c 2c 00 50 56 b9 93 48 00 00 45 00 PV: 1, P V: H: E: 0010 00 28 13 2a 40 00 00 06 7c 83 0a 81 2b 1d 0a 81 (\*@...|...+... 0020 2b 04 c5 b4 11 5c af 3b b4 85 86 6d cd d3 50 10 +...~\; ...m~P- 0030 20 14 95 8a 00 00 00 00 00 00 00 00).

The suspicious port that was being used was 4444

- It uses the source port of 50612 but its star machine is connected to the server 10.129.43.4, so the server is listening on 4444 so that it can connect



The screenshot shows the HackTheBox Academy module completion page for the 'CNS1-2026: Assignment 2' module. The page displays two questions that have been answered:

- Question 1: How many total packets were there in the Guided-analysis PCAP? Answer: 44
- Question 2: What was the suspicious port that was being used? Answer: 4444

The page includes 'Submit' and 'Hint' buttons for each question, and a 'Mark Complete & Next' button at the bottom. The page is powered by HackTheBox.

I have completed the module as shown above

Here is the link for assignment

<https://academy.hackthebox.com/module/81/section/962>

## Conclusion

This assignment provided a foundation understanding of network traffic analysis and its importance in cybersecurity. Through the HTB Academy Introduction to Network Traffic Analysis module, key concepts and practical skills for capturing and analysing network traffic were developed. The knowledge gained is essential for identifying abnormal network behaviour and supporting effective network security practices.