# 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

## Introduction

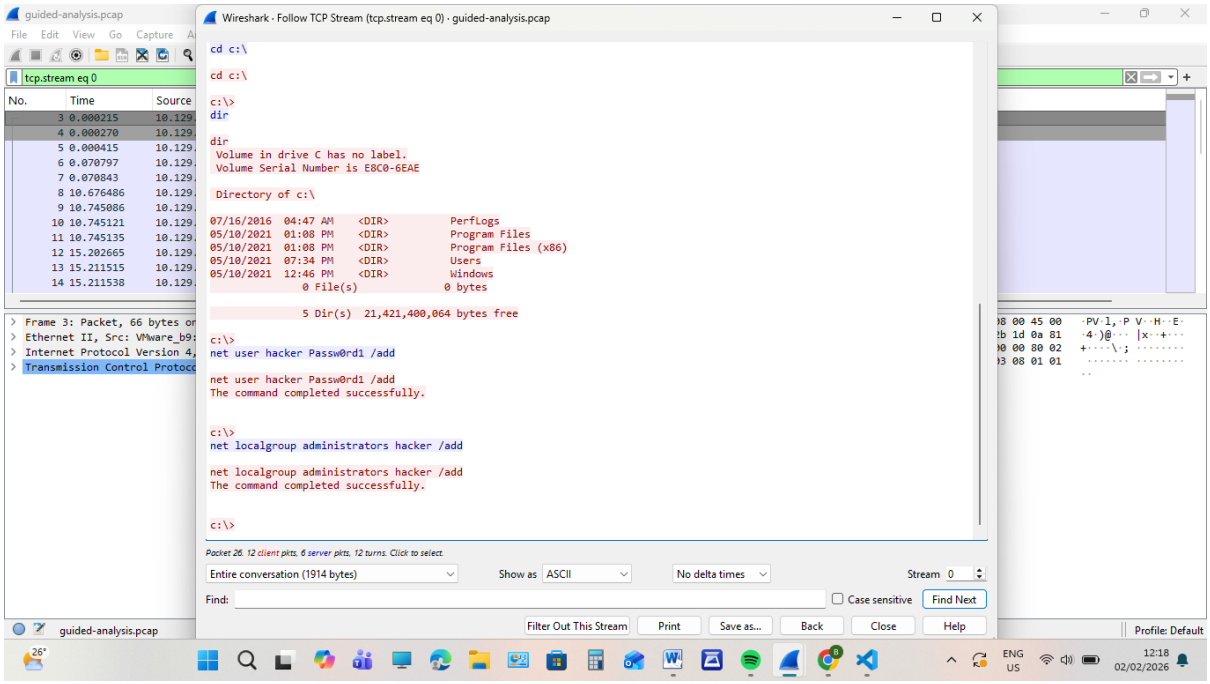
This assignment was carried out to help me develop a foundational understanding of network traffic, common network protocols and packet analysis techniques. The module introduces practical tools used to capture and analyse network traffic, enabling learners to observe real network behaviour.

## Objectives

The objectives of the assignment were:

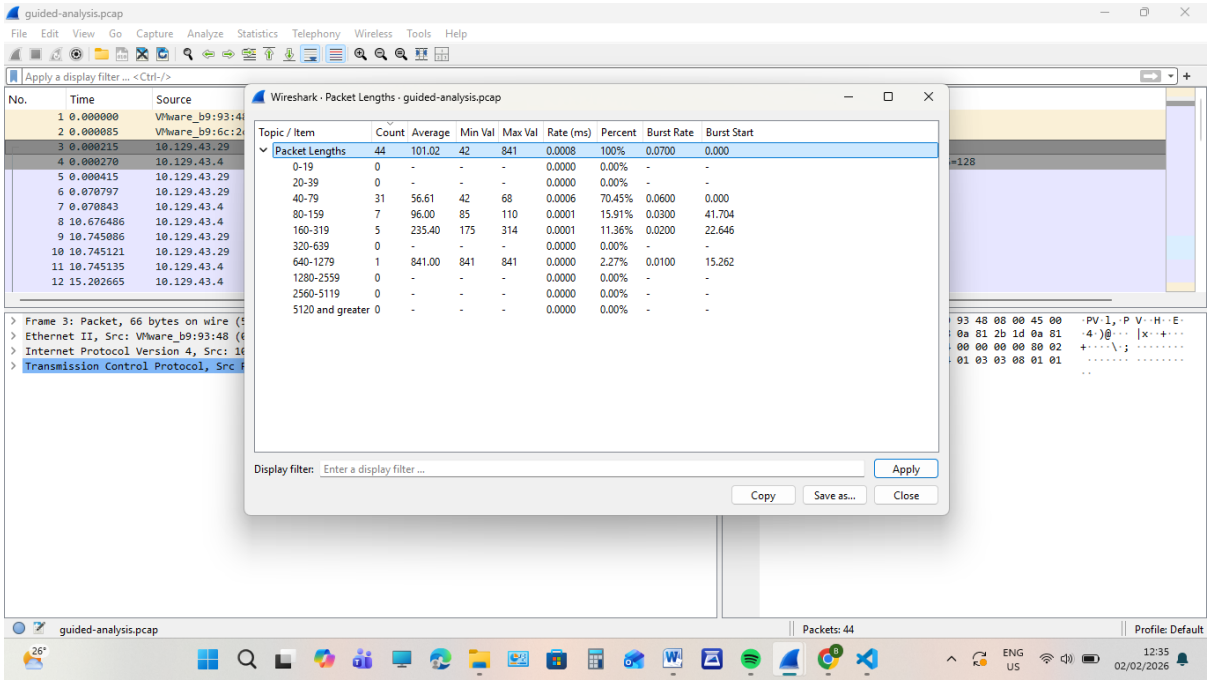
1. To understand the concept of network traffic analysis
2. To identify and understand common network protocols
3. To learn how to capture and analyse network traffic
4. To interpret packet data
5. To apply theoretical knowledge through practical exercises
6. To develop foundational skills in traffic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

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



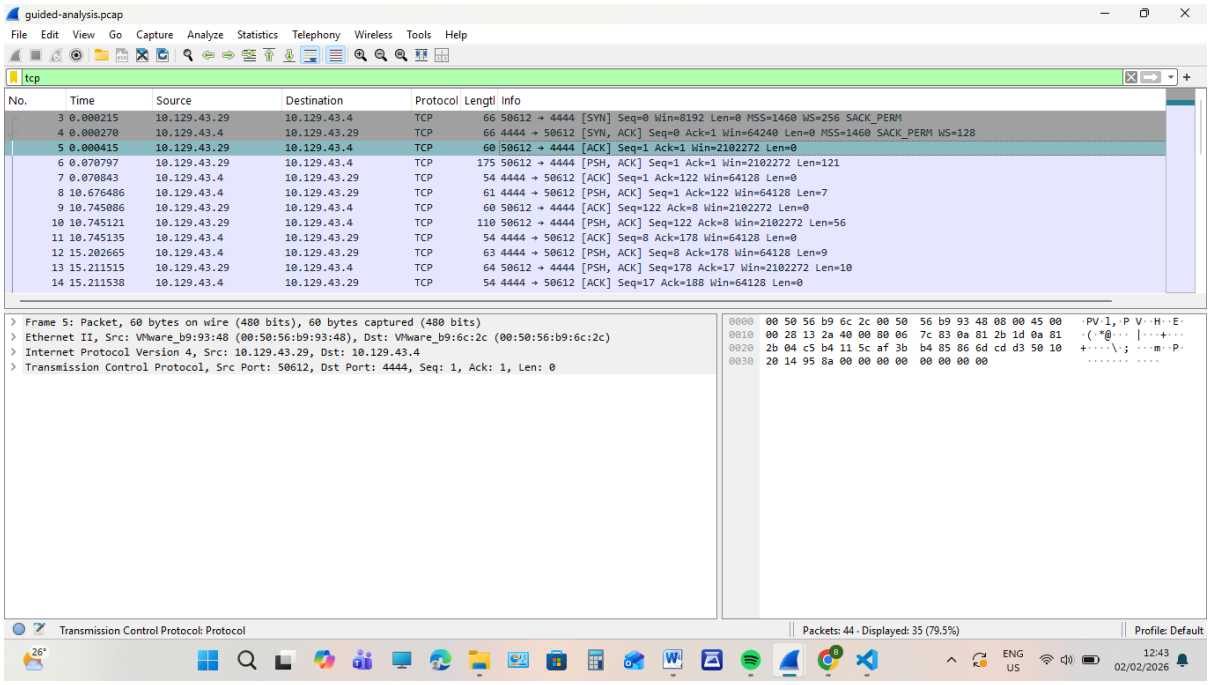

Then name of the user created in the user mrb3n's host is hacker

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



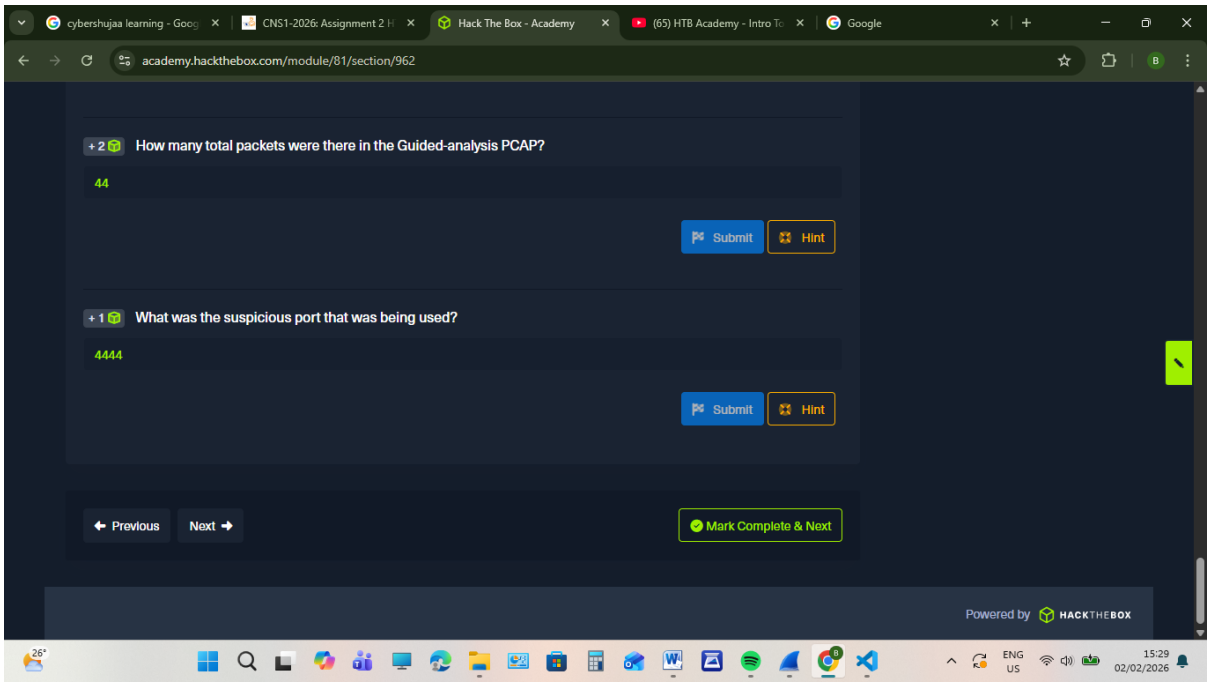

After click and know the number of packets I found out that were 44

## 3. The suspicious port that was being used




The 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




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.