Assignment 3 HTB Academy: Introduction to Network Traffic Analysis

Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction

Network Traffic Analysis (NTA) is a crucial tool in securing our network infrastructure. By examining network traffic, we can identify common ports and protocols, establish a baseline for normal activity, and monitor for potential threats. This proactive approach allows us to detect anomalies and respond to security threats effectively.

In this report, I will detail my experience with Network Traffic Analysis during an exercise on HackThe Box Academy. This exercise helped me understand how to use NTA to identify deviations from normal network behaviour and pinpoint potential security threats early. It also illustrated how NTA can aid in meeting security guidelines and detecting malicious activities, even when attackers use legitimate credentials and widely-accepted tools.

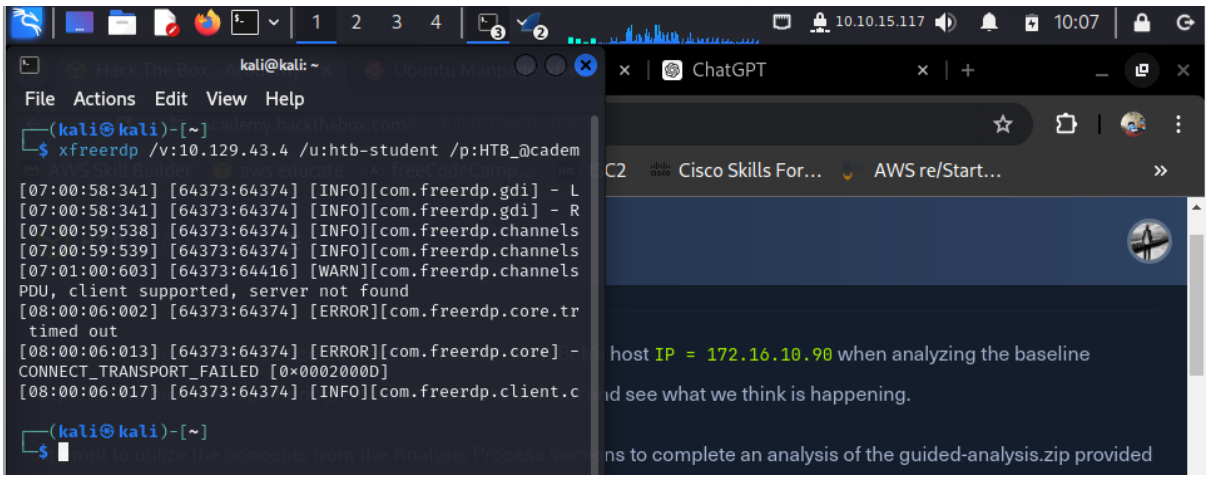
Through this exercise, I gained practical insights into the everyday use cases of Network Traffic Analysis and its importance in enhancing our network security.

Traffic Analysis Workflow

Task (a)

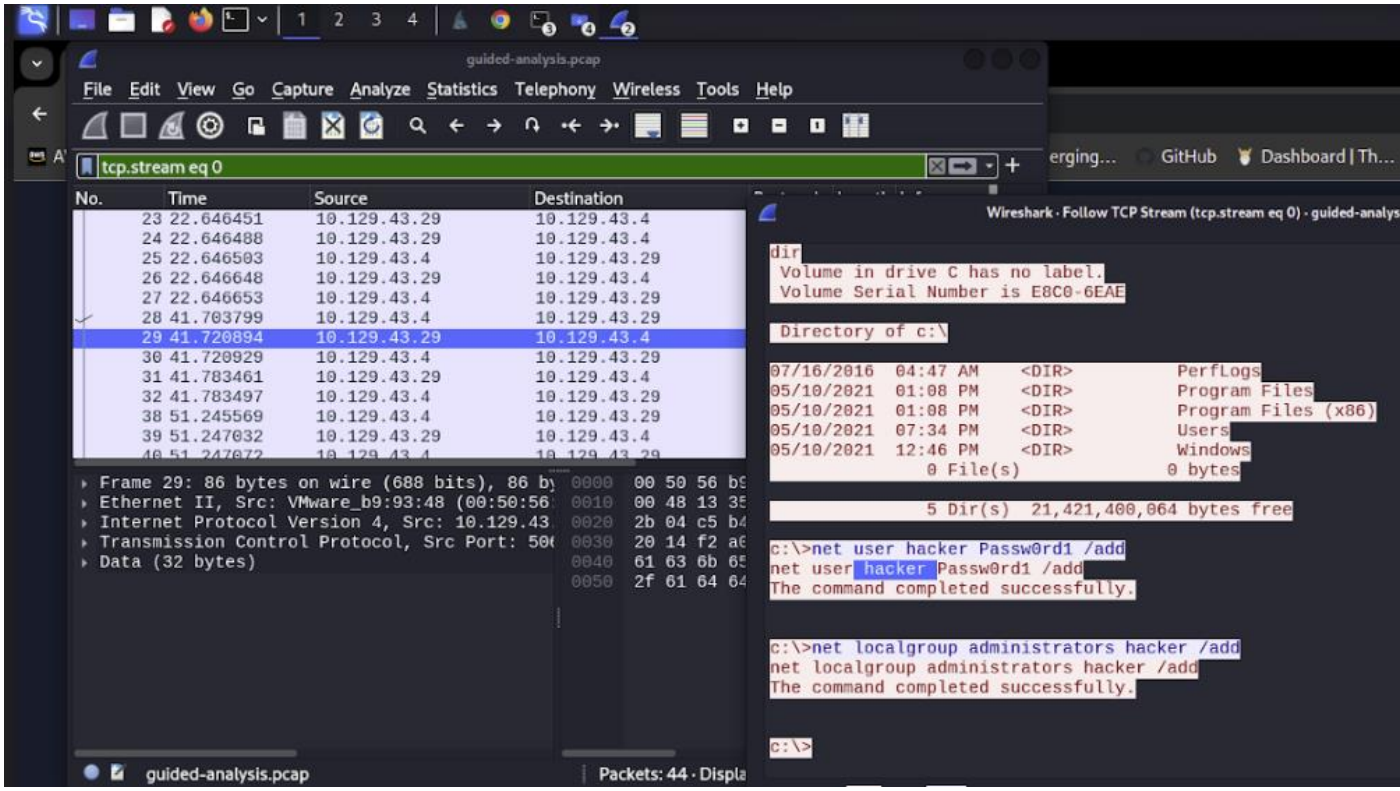
Connect to the live host for capture.

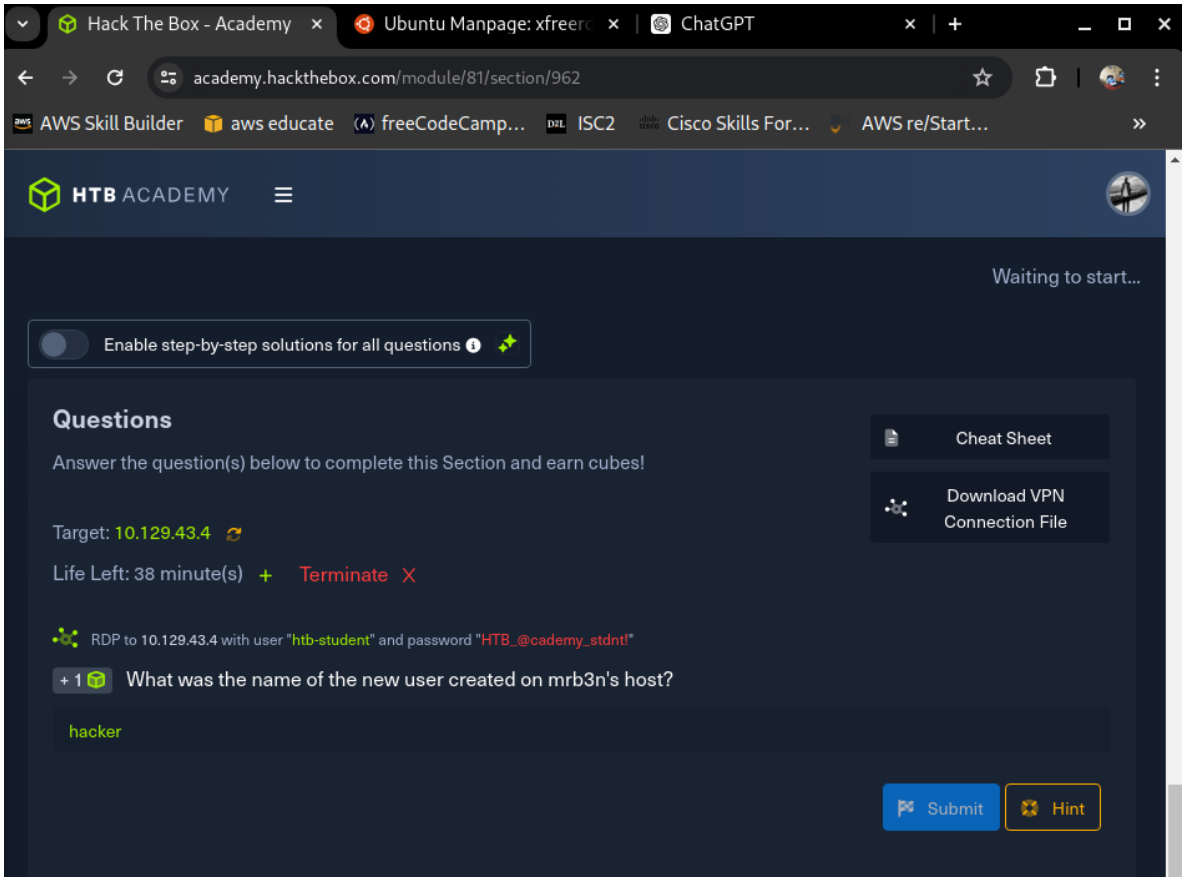
Here I used the provided credentials in the lab to connect to a remote desktop from my terminal as shown below.



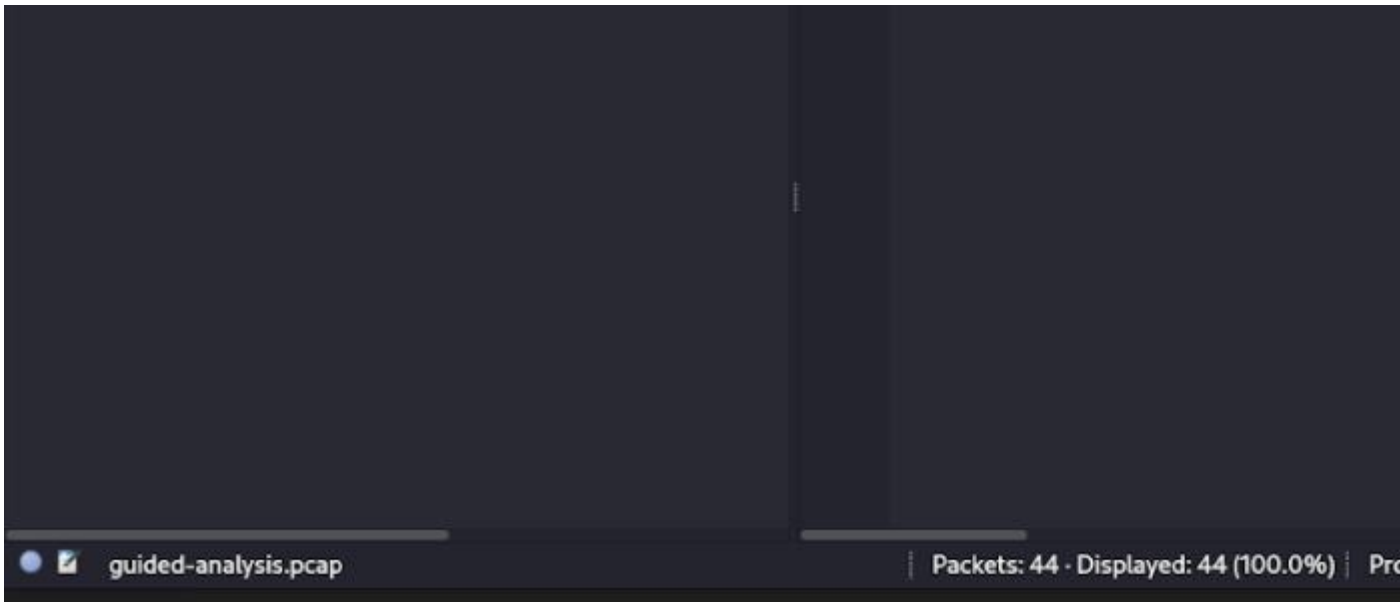
After the connection was established, I verified if indeed it was established by pinging the **target IP address 10.129.43.4**

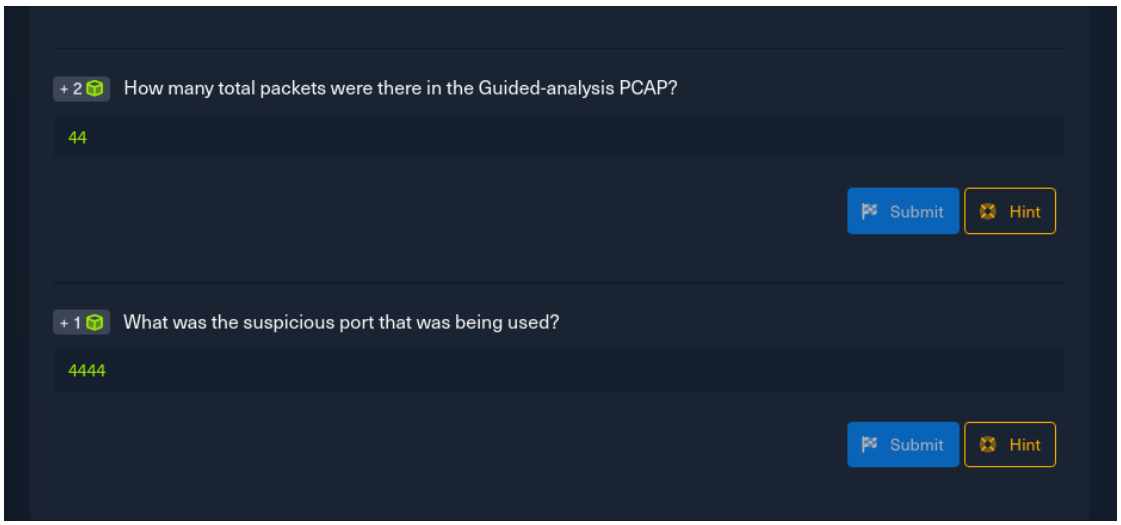
For the first question, the name of the new user created was **hacker.**





For the second question, the total number of packets were **44.**





Decrypting RDP connections.

Task (a)

Open the rdp.pcapng file in Wireshark**.**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter … <Ctrl-/>

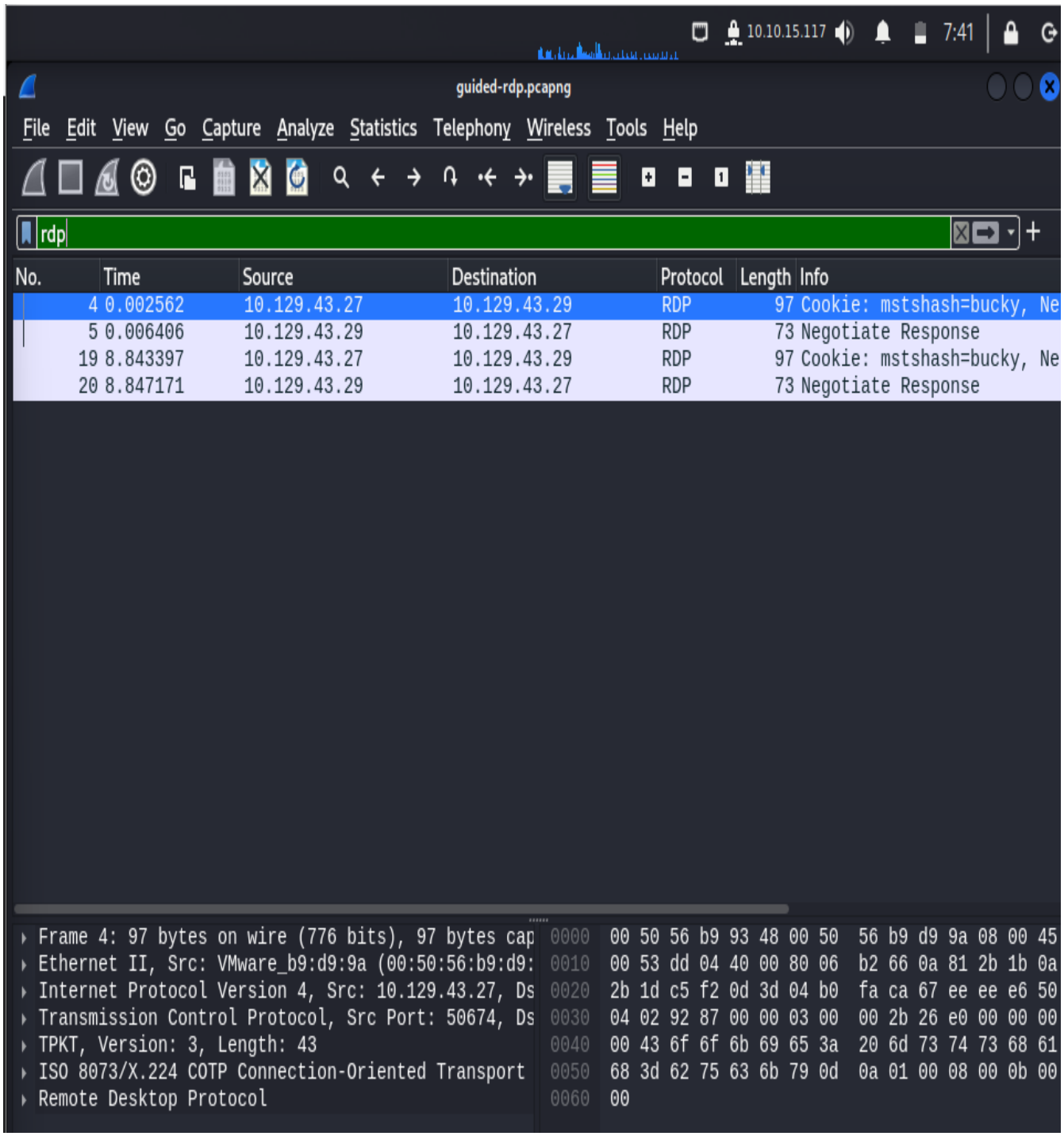
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.129.43.27	10.129.43.29	TCP	66	50674 → 3389 [SYN] Se
2	0.000231	10.129.43.29	10.129.43.27	TCP	66	3389 → 50674 [SYN, AC
3	0.000521	10.129.43.27	10.129.43.29	TCP	60	50674 → 3389 [ACK] Se
4	0.002562	10.129.43.27	10.129.43.29	RDP	97	Cookie: mstshash=buck
5	0.006406	10.129.43.29	10.129.43.27	RDP	73	Negotiate Response
6	0.050370	10.129.43.27	10.129.43.29	TCP	60	50674 → 3389 [ACK] Se
7	6.256391	10.129.43.27	10.129.43.29	TLSv1.2	185	Client Hello (SNI=10.
8	6.257006	10.129.43.29	10.129.43.27	TLSv1.2	896	Server Hello, Certifi
9	6.258365	10.129.43.27	10.129.43.29	TLSv1.2	372	Client Key Exchange,
10	6.260974	10.129.43.29	10.129.43.27	TLSv1.2	105	Change Cipher Spec, E
11	6.261843	10.129.43.27	10.129.43.29	TLSv1.2	140	Application Data
12	6.262246	10.129.43.29	10.129.43.27	TLSv1.2	324	Application Data
13	6.263994	10.129.43.27	10.129.43.29	TLSv1.2	710	Application Data
14	6.265122	10.129.43.29	10.129.43.27	TLSv1.2	142	Application Data
15	6.265690	10.129.43.27	10.129.43.29	TCP	60	50674 → 3389 [RST, AC
16	8.842069	10.129.43.27	10.129.43.29	TCP	66	50675 → 3389 [SYN] Se
17	8.842195	10.129.43.29	10.129.43.27	TCP	66	3389 → 50675 [SYN, AC
18	8.842471	10.129.43.27	10.129.43.29	TCP	60	50675 → 3389 [ACK] Se
19	8.843397	10.129.43.27	10.129.43.29	RDP	97	Cookie: mstshash=buck
20	8.847171	10.129.43.29	10.129.43.27	RDP	73	Negotiate Response
21	8.850426	10.129.43.27	10.129.43.29	TLSv1.2	185	Client Hello (SNI=10.
22	8.850662	10.129.43.29	10.129.43.27	TLSv1.2	896	Server Hello, Certifi
23	8.851306	10.129.43.27	10.129.43.29	TLSv1.2	372	Client Key Exchange

```
▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes cap
▸ Ethernet II, Src: VMware_b9:d9:9a (00:50:56:b9:d9:
▸ Internet Protocol Version 4, Src: 10.129.43.27, Ds
▸ Transmission Control Protocol, Src Port: 50674, Ds

0000  00 50 56 b9 93 48 00 50  56 b9 d9 9a 08 00
0010  00 34 dd 02 40 00 80 06  b2 87 0a 81 2b 1b
0020  2b 1d c5 f2 0d 3d 04 b0  fa c9 00 00 00 00
0030  fa f0 36 3c 00 00 02 04  05 b4 01 03 03 08
0040  04 02
```

Task (b)

This is the analysis of the traffic included and application of the rdp filter.



Task (c)

Here, I used an RDP-Key provided in the lab in wireshark to decrypt the files.

Now, let's take this a step further and use the key we found to try and decrypt the traffic.

To apply the key in Wireshark:

go to Edit → Preferences → Protocols → TLS

On the TLS page, select Edit by RSA keys list → a new window will open.

To Import An RDP Key to wireshark, below are the steps

Steps

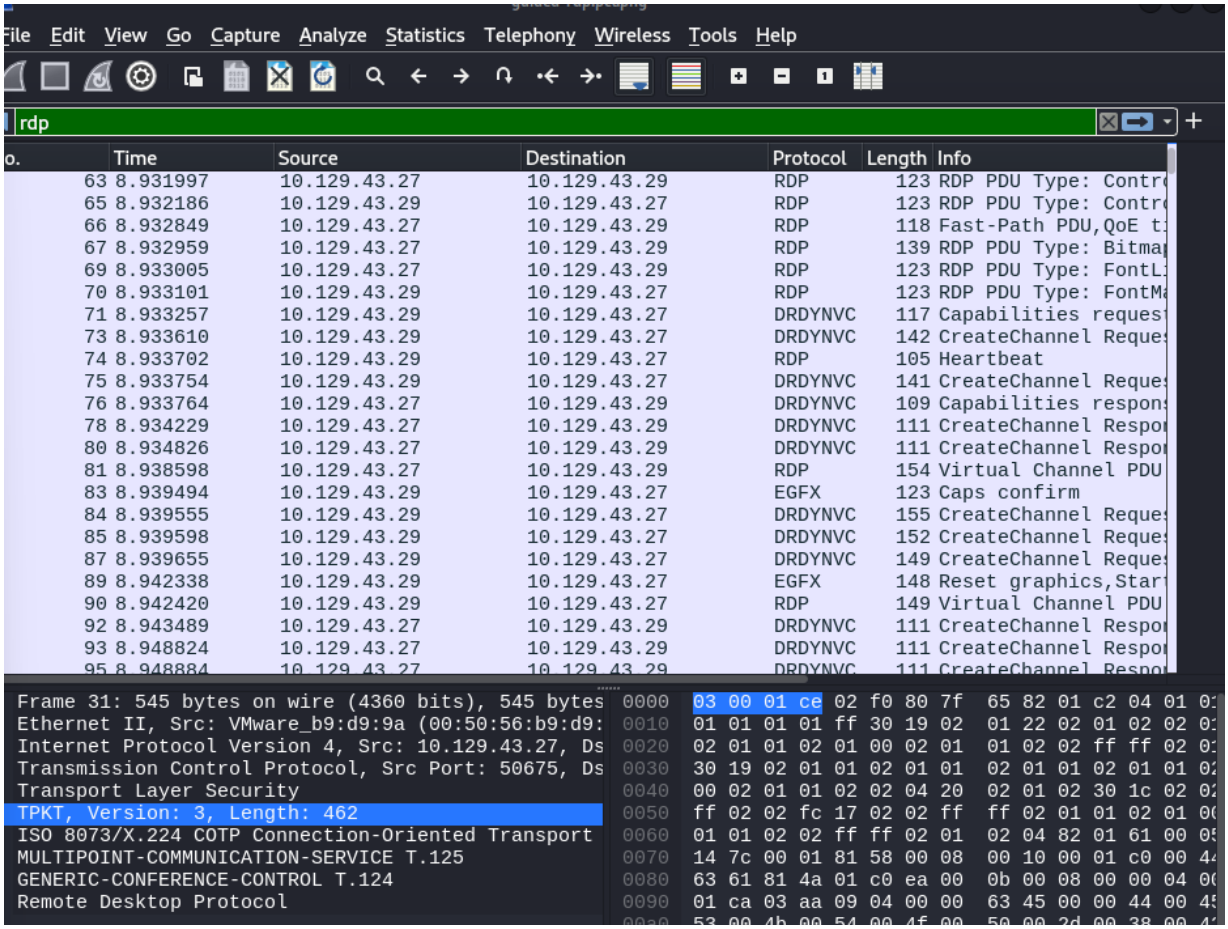
Click the + to add a new key

Type in the IP address of the RDP server 10.129.43.29

Type in the port used 3389

Protocol filed equals tpkt or blank.

Browse to the server.key file and add it in the key file section.

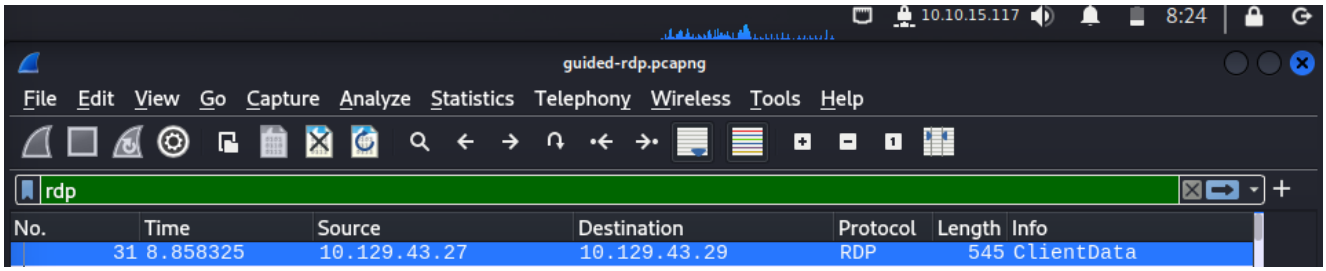


Performing Analysis of the Unencrypted Traffic

Now that we have broken RDP out of the TLS tunnel, what can we find?

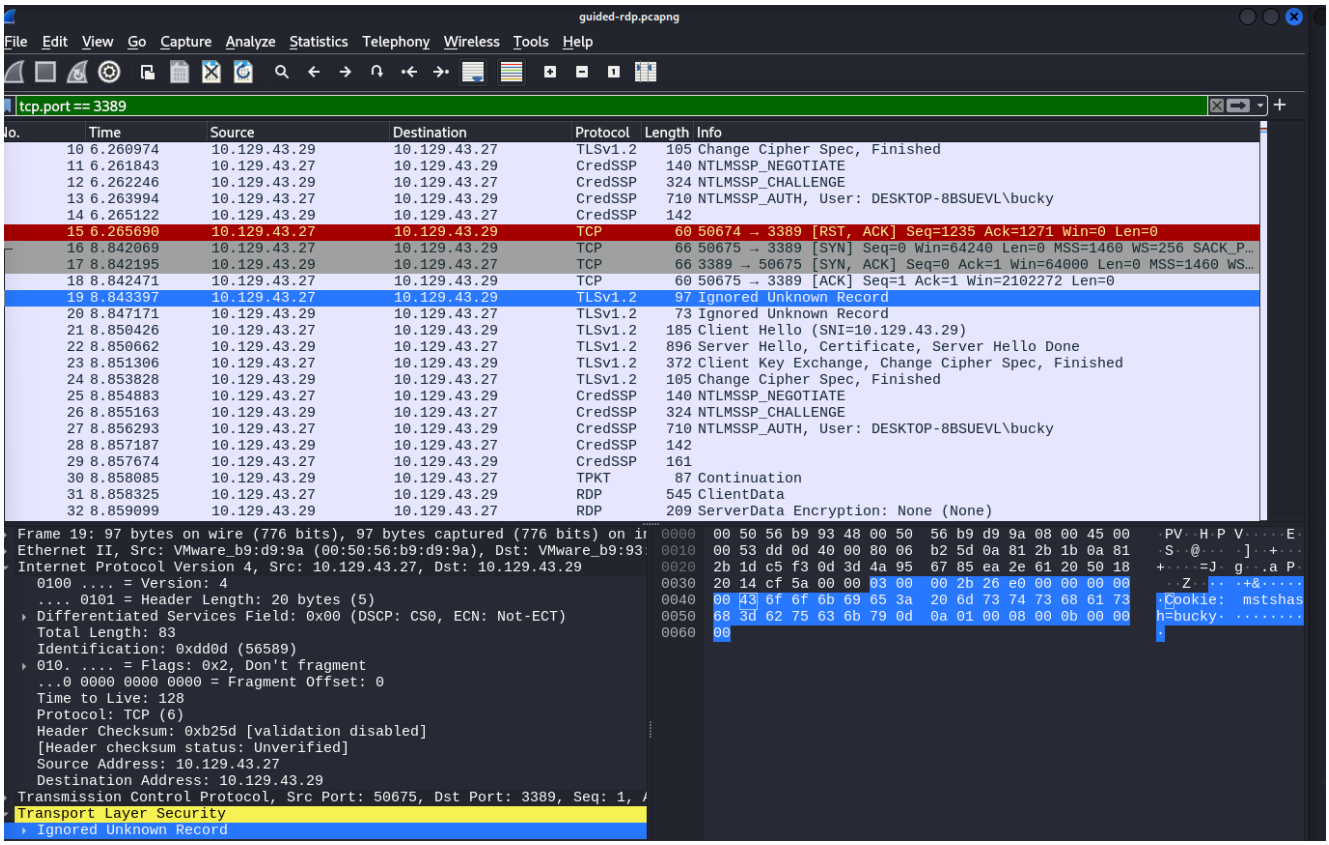
Questions:

1. What host initiated the RDP session with our server?
   If we pay attention to the first packet, packet # 8 of the three-way handshake, we can see the host who initiated the connection is **10.129.43.27**

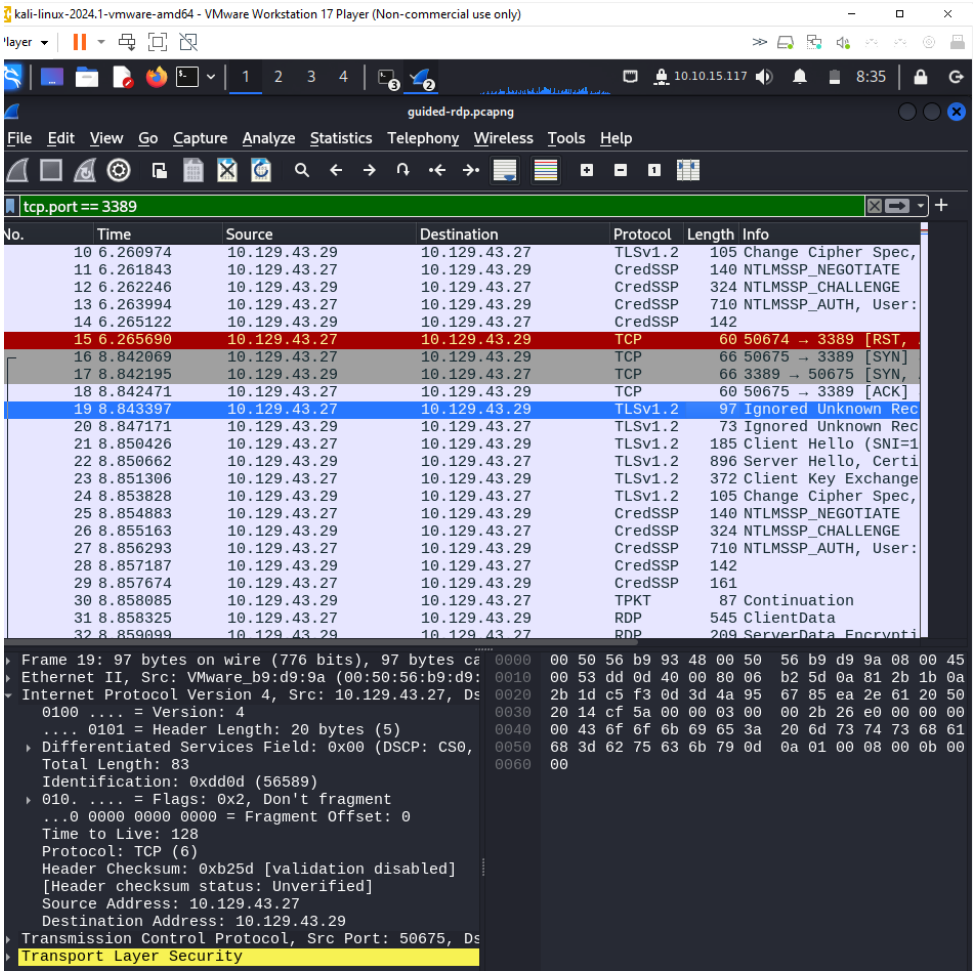


2. Which user account was used to initiate the RDP connection?

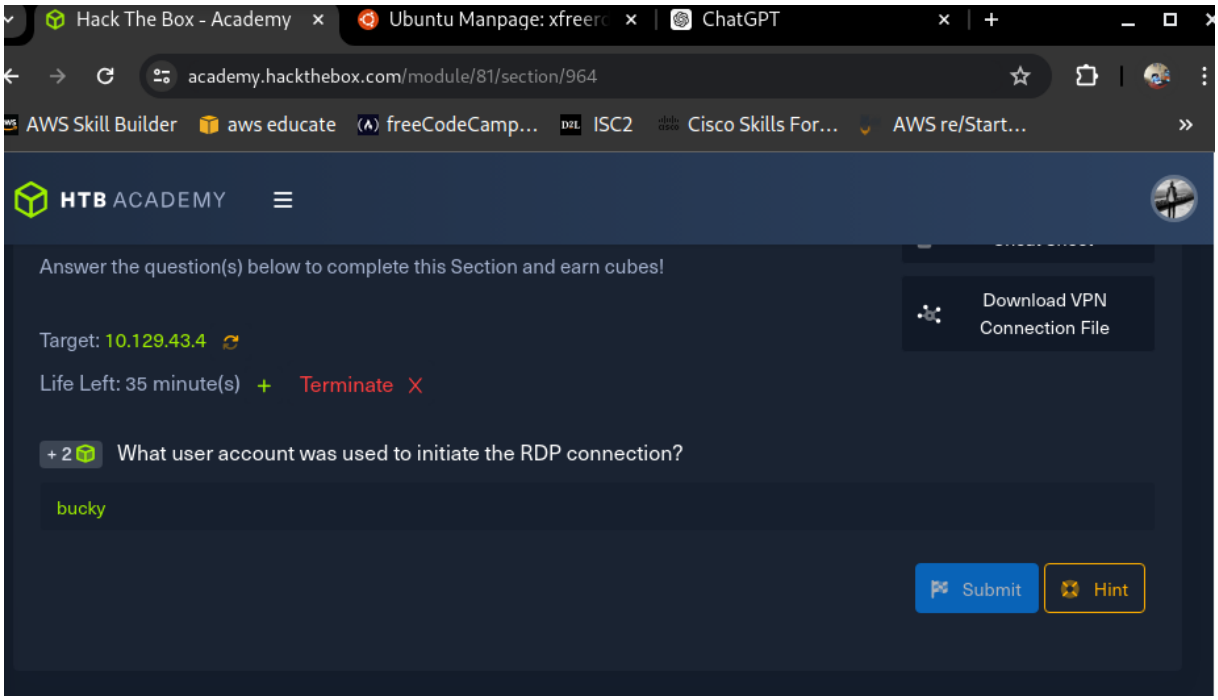
When filter on tcp.port == 3389, we can see a record labelled Ignored Unknown Record. If we examine the ASCII, it will show us a username.

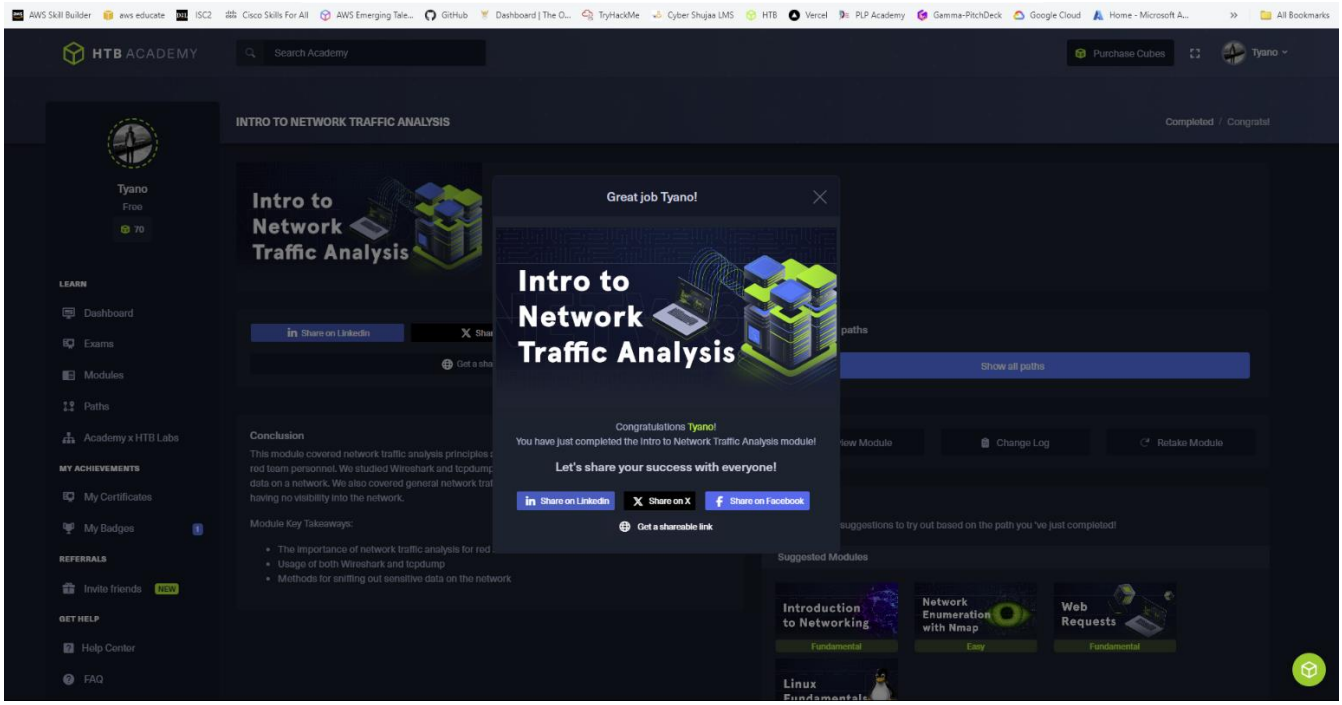


The user account we get when we examine the ASCII is **bucky** as shown in the screenshot above.



The below screenshot answers the question of which account was used to initiate the RDP connection which we have since established as **bucky.**





Here is a link as further proof of my completion of this module
https://academy.hackthebox.com/achievement/942061/81

Conclusion

In conclusion, my experience with the Network Traffic Analysis (NTA) exercise on Hack The Box Academy has provided me with practical insights into enhancing network security. Through the meticulous examination of network traffic, I have learned to identify anomalies, detect potential threats early, and maintain a proactive security posture.

This exercise has emphasized the importance of NTA in meeting security guidelines and detecting malicious activities, highlighting its crucial role in safeguarding our network infrastructure. By leveraging NTA techniques, I can effectively mitigate risks and safeguard our digital assets against evolving cyber threats.

As I reflect on this exercise, it becomes evident that NTA is not merely a reactive measure but a proactive strategy in enhancing network security. The knowledge and skills acquired through this exercise will serve as invaluable assets in my ongoing endeavours to strengthen network defences and ensure the integrity of our network infrastructure.