

## 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 HackTheBox 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.

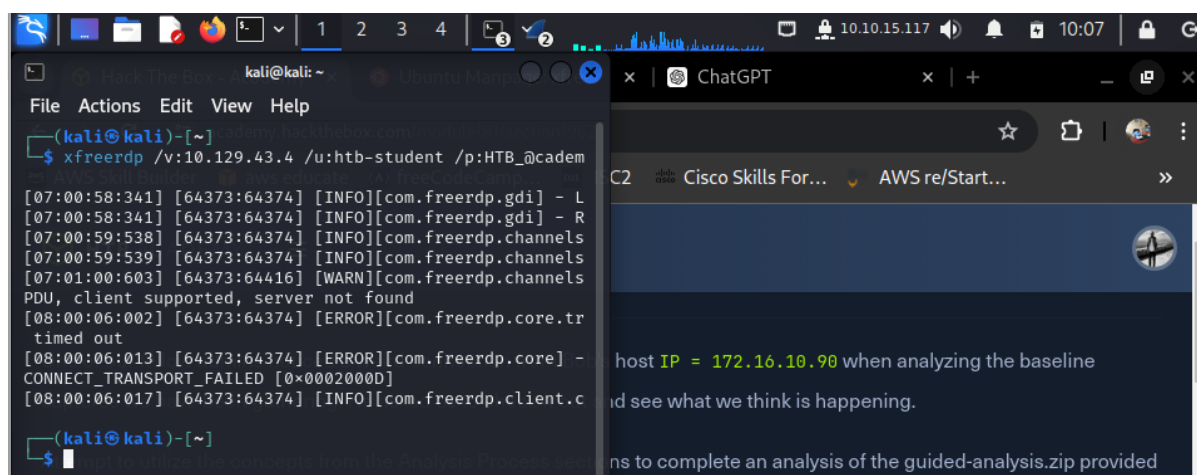
Through this exercise, I gained practical insights into the everyday use cases of Network Traffic Analysis and its importance in enhancing our network security.

### 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.



The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal window displays the command `xfreerdp /v:10.129.43.4 /u:htb-student /p:HTB_academ` and its output, which includes log messages from the `com.freerdp.gdi` and `com.freerdp.channels` modules. The output shows a successful connection to the host `10.129.43.4` at `10:00:06:002`. The web browser window shows a page with a dark background and white text, which appears to be a remote desktop session. The text on the page includes the phrase "host IP = 172.16.10.90 when analyzing the baseline" and "d see what we think is happening."

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**.

The image shows a Wireshark packet capture of a TCP stream (eq 0) between 10.129.43.29 and 10.129.43.4. The selected packet (No. 29) is a successful response from the server. The packet details show an Ethernet II frame, an Internet Protocol Version 4 header, and a Transmission Control Protocol header. The data field contains a directory listing and a command prompt output.

No.	Time	Source	Destination
23	22.646451	10.129.43.29	10.129.43.4
24	22.646488	10.129.43.29	10.129.43.4
25	22.646503	10.129.43.4	10.129.43.29
26	22.646648	10.129.43.29	10.129.43.4
27	22.646653	10.129.43.4	10.129.43.29
28	41.703799	10.129.43.4	10.129.43.29
29	41.720894	10.129.43.29	10.129.43.4
30	41.720929	10.129.43.4	10.129.43.29
31	41.783461	10.129.43.29	10.129.43.4
32	41.783497	10.129.43.4	10.129.43.29
38	51.245569	10.129.43.4	10.129.43.29
39	51.247032	10.129.43.29	10.129.43.4
40	51.247672	10.129.43.4	10.129.43.29

Frame 29: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0  
Ethernet II, Src: VMware\_b9:93:48 (00:50:56:00:10:00), Dst: 08:00:2b:04:c5:b4  
Internet Protocol Version 4, Src: 10.129.43.29, Dst: 10.129.43.4  
Transmission Control Protocol, Src Port: 5000, Dst Port: 4444, Seq: 300000000, Win: 65535, Len: 0  
Data (32 bytes)

```
dir
Volume in drive C has no label.
Volume Serial Number is E8C0-6EAE

Directory of c:\

07/16/2016  04:47 AM    <DIR>          PerfLogs
05/10/2021  01:08 PM    <DIR>          Program Files
05/10/2021  01:08 PM    <DIR>          Program Files (x86)
05/10/2021  07:34 PM    <DIR>          Users
05/10/2021  12:46 PM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  21,421,400,064 bytes free

c:\>net user hacker Passw0rd1 /add
net user hacker Passw0rd1 /add
The command completed successfully.

c:\>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.

c:\>
```

The image shows the HTB Academy interface. The page title is "Hack The Box - Academy". The URL is "academy.hackthebox.com/module/81/section/962". The page content includes a toggle for "Enable step-by-step solutions for all questions", a "Questions" section, and a "Cheat Sheet" button. The question is: "What was the name of the new user created on mrb3n's host?". The answer is "hacker".

HTB ACADEMY

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Target: 10.129.43.4

Life Left: 38 minute(s) + Terminate

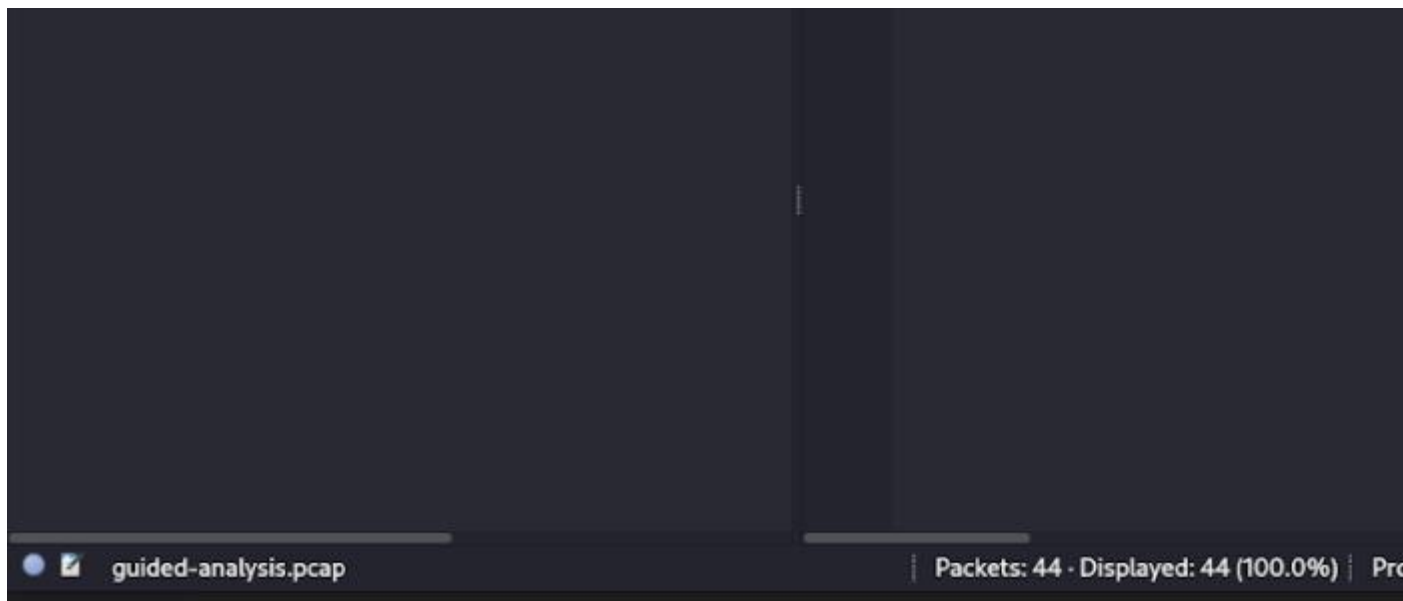
RDP to 10.129.43.4 with user "htb-student" and password "HTB\_@cademy\_stdnt!"

+ 1 What was the name of the new user created on mrb3n's host?

hacker

Submit Hint

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



+ 2

How many total packets were there in the Guided-analysis PCAP?

44

Submit

Hint

+ 1

What was the suspicious port that was being used?

4444

Submit

Hint

**Decrypting RDP connections.**

**Task (a)**

Open the rdp.pcapng file in Wireshark.

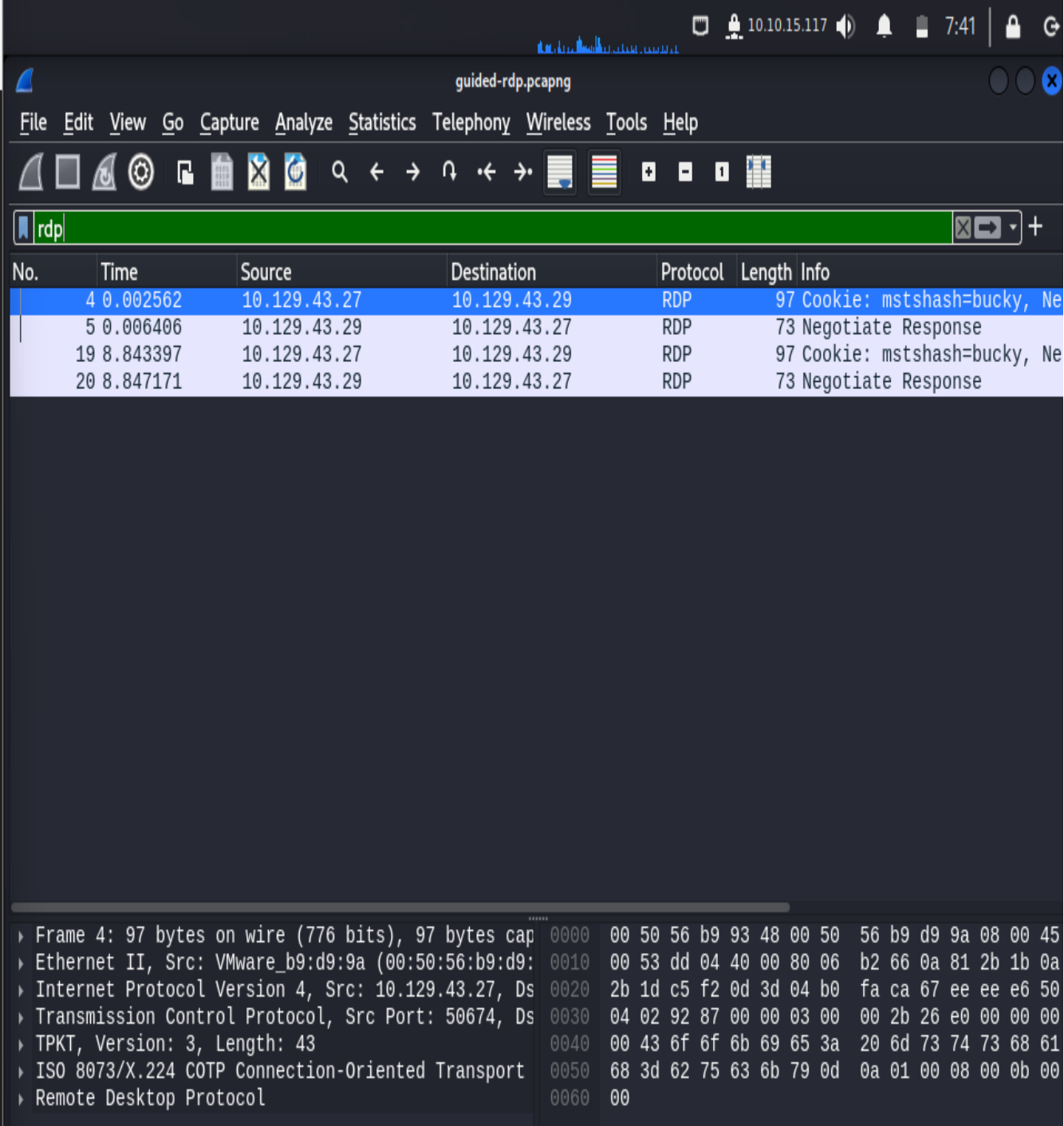
The screenshot shows the Wireshark interface with a packet capture of a network connection between 10.129.43.27 and 10.129.43.29. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, navigation, and analysis. A filter bar at the top displays "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] Seq=...
2	0.000231	10.129.43.29	10.129.43.27	TCP	66	3389 → 50674 [SYN, ACK] Seq=...
3	0.000521	10.129.43.27	10.129.43.29	TCP	60	50674 → 3389 [ACK] Seq=...
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] Seq=...
7	6.256391	10.129.43.27	10.129.43.29	TLSv1.2	185	Client Hello (SNI=10.129.43.27)
8	6.257006	10.129.43.29	10.129.43.27	TLSv1.2	896	Server Hello, Certificate...
9	6.258365	10.129.43.27	10.129.43.29	TLSv1.2	372	Client Key Exchange, Encrypted...
10	6.260974	10.129.43.29	10.129.43.27	TLSv1.2	105	Change Cipher Spec, Finished
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, ACK] Seq=...
16	8.842069	10.129.43.27	10.129.43.29	TCP	66	50675 → 3389 [SYN] Seq=...
17	8.842195	10.129.43.29	10.129.43.27	TCP	66	3389 → 50675 [SYN, ACK] Seq=...
18	8.842471	10.129.43.27	10.129.43.29	TCP	60	50675 → 3389 [ACK] Seq=...
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=10.129.43.27)
22	8.850662	10.129.43.29	10.129.43.27	TLSv1.2	896	Server Hello, Certificate...
23	8.851306	10.129.43.27	10.129.43.29	TLSv1.2	372	Client Key Exchange, Encrypted...

The bottom pane shows the details of the selected packet (No. 15). It identifies it as an Internet Protocol Version 4 packet from 10.129.43.27 to 10.129.43.29. The Transmission Control Protocol section indicates it's a Reset (RST) packet with sequence number 50674 and acknowledgment number 3389. The raw packet bytes are displayed in hexadecimal and ASCII format below.

### Task (b)

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



The screenshot shows the Wireshark network protocol analyzer interface. The top status bar indicates the current file is 'guided-rdp.pcapng' and the system time is 7:41. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows four packets, all of which are RDP. The selected packet (No. 4) is expanded, showing its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Remote Desktop Protocol. The RDP section shows a 'Cookie: msthash=ucky, Ne'.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.002562	10.129.43.27	10.129.43.29	RDP	97	Cookie: msthash=ucky, Ne
5	0.006406	10.129.43.29	10.129.43.27	RDP	73	Negotiate Response
19	8.843397	10.129.43.27	10.129.43.29	RDP	97	Cookie: msthash=ucky, Ne
20	8.847171	10.129.43.29	10.129.43.27	RDP	73	Negotiate Response

Frame 4: 97 bytes on wire (776 bits), 97 bytes captured on interface 0, 97 bytes from 10.129.43.27 to 10.129.43.29 on interface 0

Ethernet II, Src: VMware\_b9:d9:9a (00:50:56:b9:d9:9a), Dst: 10.129.43.29 (08:00:27:1d:c5:f2)

Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29

Transmission Control Protocol, Src Port: 50674, Dst Port: 3389, Seq: 123456789, Len: 97

TPKT, Version: 3, Length: 43

ISO 8073/X.224 COTP Connection-Oriented Transport

Remote Desktop Protocol

### 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

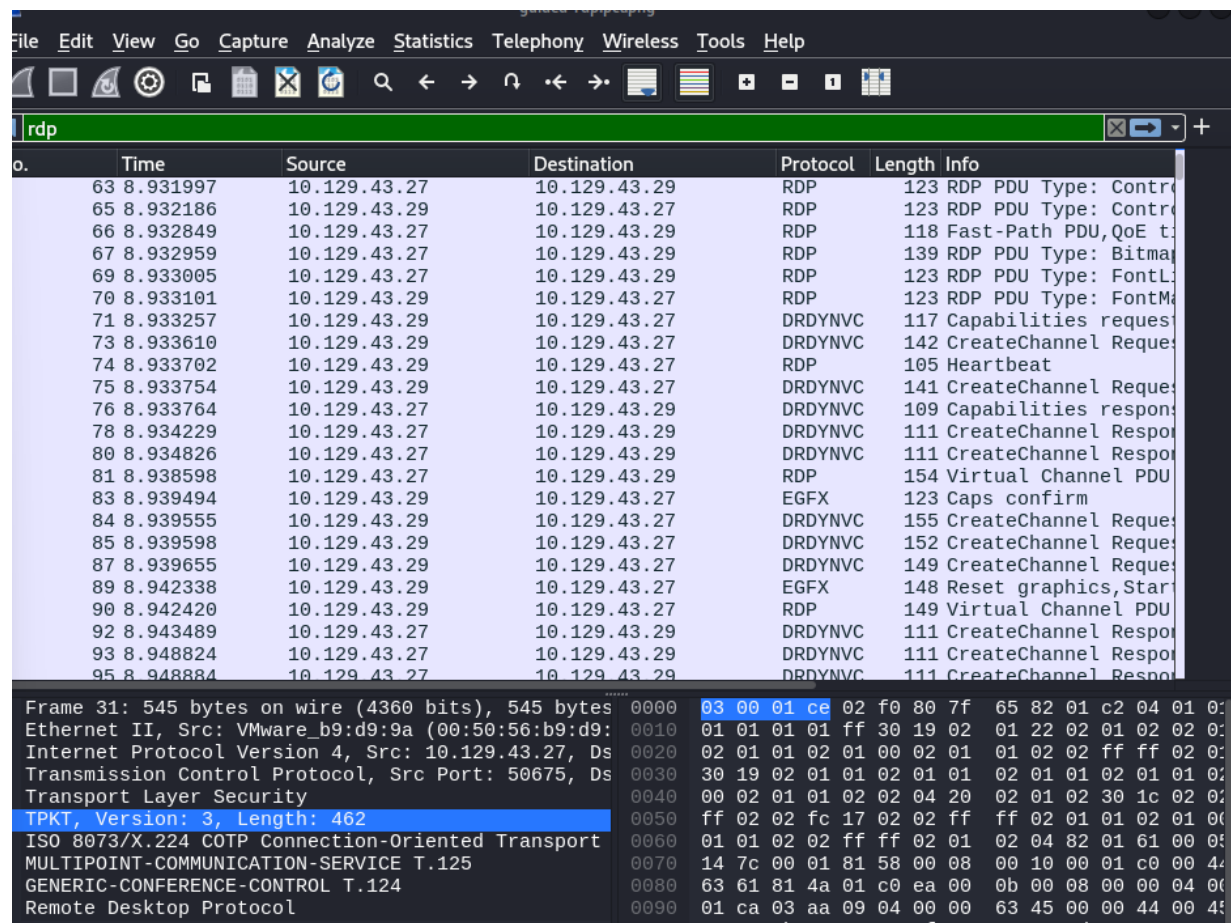
Click the + to add a new key

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

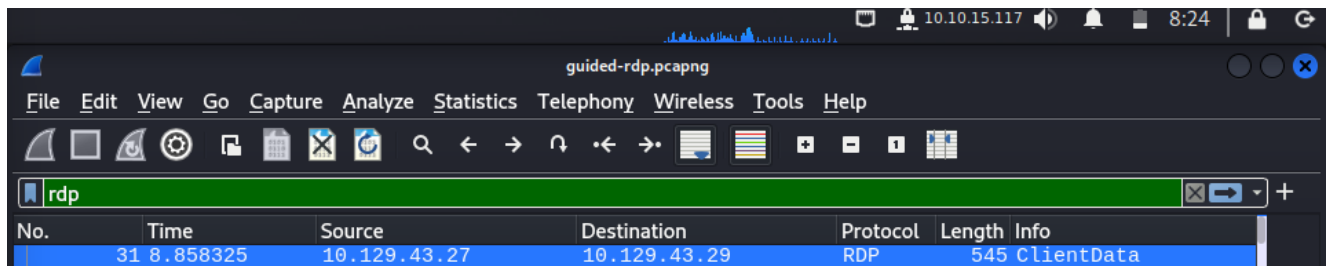
Now that we have broken RDP out of the TLS tunnel, what can we find?

Questions:



1. What host initiated the RDP session with our server?

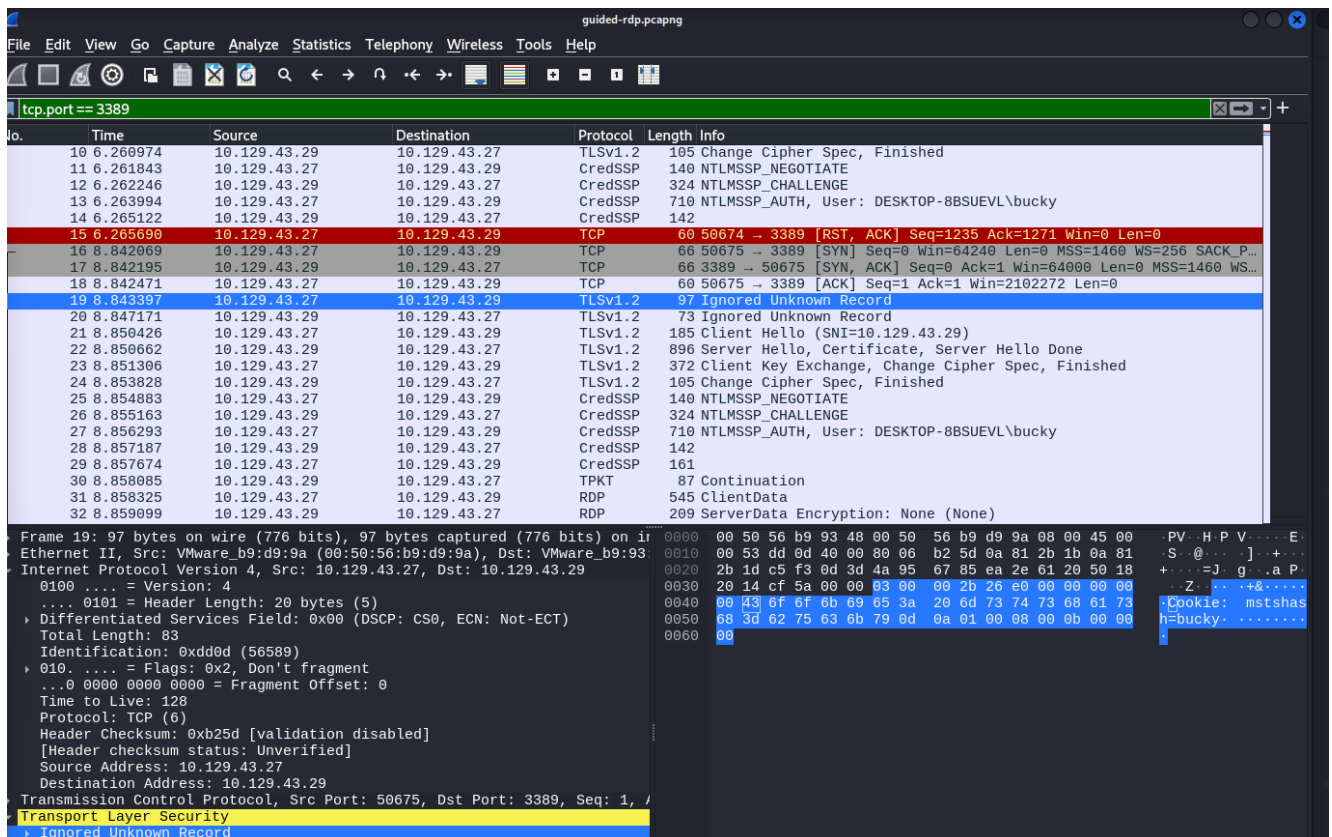
If we pay attention to the first packet, packet # 8 of the three-way handshake, we can see the host who initiated the connection is **10.129.43.27**



No.	Time	Source	Destination	Protocol	Length	Info
31	8.858325	10.129.43.27	10.129.43.29	RDP	545	ClientData

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

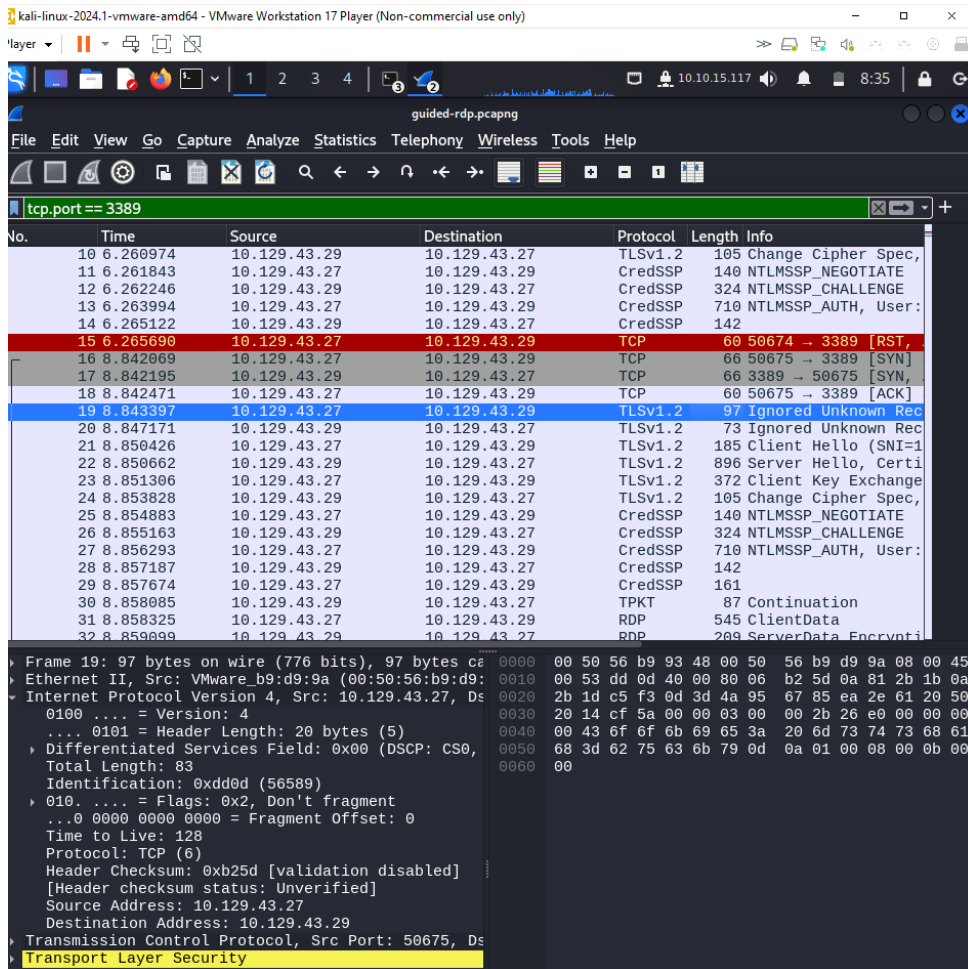
When filter on `tcp.port == 3389`, we can see a record labelled Ignored Unknown Record. If we examine the ASCII, it will show us a username.



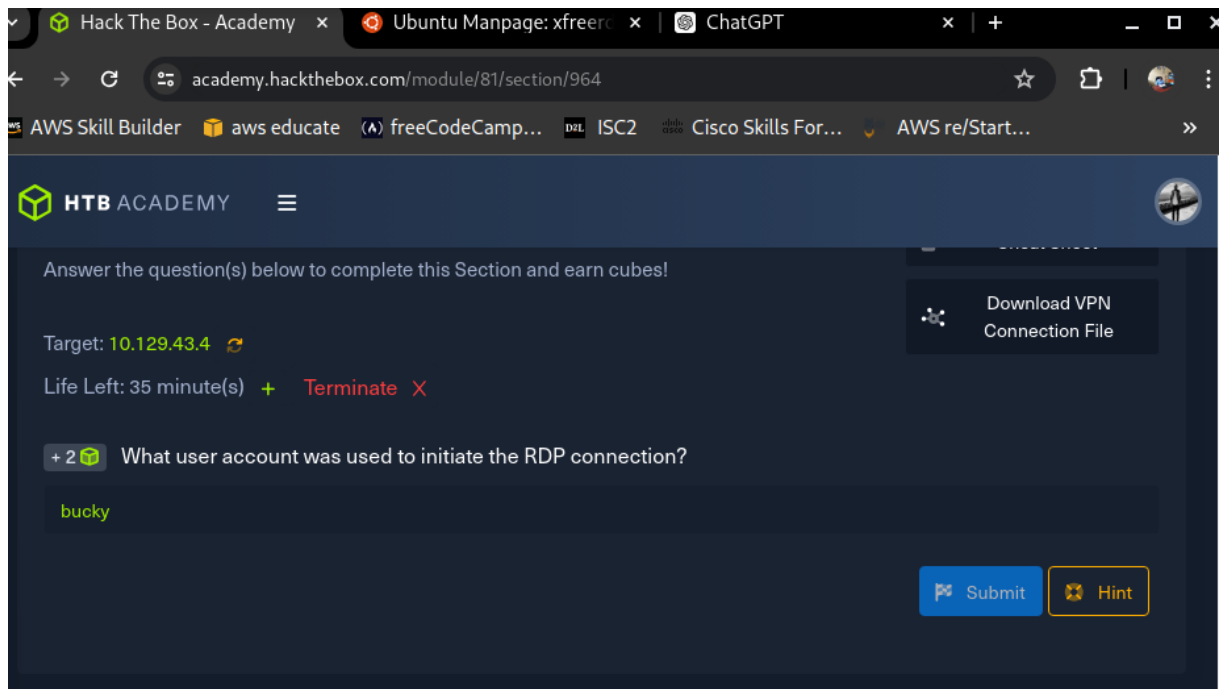
No.	Time	Source	Destination	Protocol	Length	Info
10	6.260974	10.129.43.29	10.129.43.27	TLSv1.2	105	Change Cipher Spec, Finished
11	6.261843	10.129.43.27	10.129.43.29	CredSSP	140	NTLMSSP_NEGOTIATE
12	6.262246	10.129.43.29	10.129.43.27	CredSSP	324	NTLMSSP_CHALLENGE
13	6.263994	10.129.43.27	10.129.43.29	CredSSP	710	NTLMSSP_AUTH, User: DESKTOP-8BSUEVL\bucky
14	6.265122	10.129.43.29	10.129.43.27	CredSSP	142	
15	6.265690	10.129.43.27	10.129.43.29	TCP	60	50674 → 3389 [RST, ACK] Seq=1235 Ack=1271 Win=0 Len=0
16	8.842069	10.129.43.27	10.129.43.29	TCP	66	50675 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
17	8.842195	10.129.43.29	10.129.43.27	TCP	66	3389 → 50675 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS...
18	8.842471	10.129.43.27	10.129.43.29	TCP	60	50675 → 3389 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
19	8.843397	10.129.43.27	10.129.43.29	TLSv1.2	97	Ignored Unknown Record
20	8.847171	10.129.43.29	10.129.43.27	TLSv1.2	73	Ignored Unknown Record
21	8.850426	10.129.43.27	10.129.43.29	TLSv1.2	185	Client Hello (SNI=10.129.43.29)
22	8.850662	10.129.43.29	10.129.43.27	TLSv1.2	896	Server Hello, Certificate, Server Hello Done
23	8.851306	10.129.43.27	10.129.43.29	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Finished
24	8.853828	10.129.43.29	10.129.43.27	TLSv1.2	105	Change Cipher Spec, Finished
25	8.854883	10.129.43.27	10.129.43.29	CredSSP	140	NTLMSSP_NEGOTIATE
26	8.855163	10.129.43.29	10.129.43.27	CredSSP	324	NTLMSSP_CHALLENGE
27	8.856293	10.129.43.27	10.129.43.29	CredSSP	710	NTLMSSP_AUTH, User: DESKTOP-8BSUEVL\bucky
28	8.857187	10.129.43.29	10.129.43.27	CredSSP	142	
29	8.857674	10.129.43.27	10.129.43.29	CredSSP	161	
30	8.858085	10.129.43.29	10.129.43.27	TPKT	87	Continuation
31	8.858325	10.129.43.27	10.129.43.29	RDP	545	ClientData
32	8.859099	10.129.43.29	10.129.43.27	RDP	209	ServerData Encryption: None (None)

Frame 19: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface 0  
Ethernet II, Src: VMware\_b9:d9:9a (00:50:56:b9:d9:9a), Dst: VMware\_b9:93:ca:46:3d:14 (00:0c:29:93:ca:46:3d:14)  
Internet Protocol Version 4, Src: 10.129.43.27, Dst: 10.129.43.29  
... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 83  
Identification: 0xdd0d (56589)  
... 010 = Flags: 0x2, Don't fragment  
... 0000 0000 0000 = Fragment Offset: 0  
Time to Live: 128  
Protocol: TCP (6)  
Header Checksum: 0xb25d [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 10.129.43.27  
Destination Address: 10.129.43.29  
Transmission Control Protocol, Src Port: 50675, Dst Port: 3389, Seq: 1, Len: 97  
Transport Layer Security  
Ignored Unknown Record

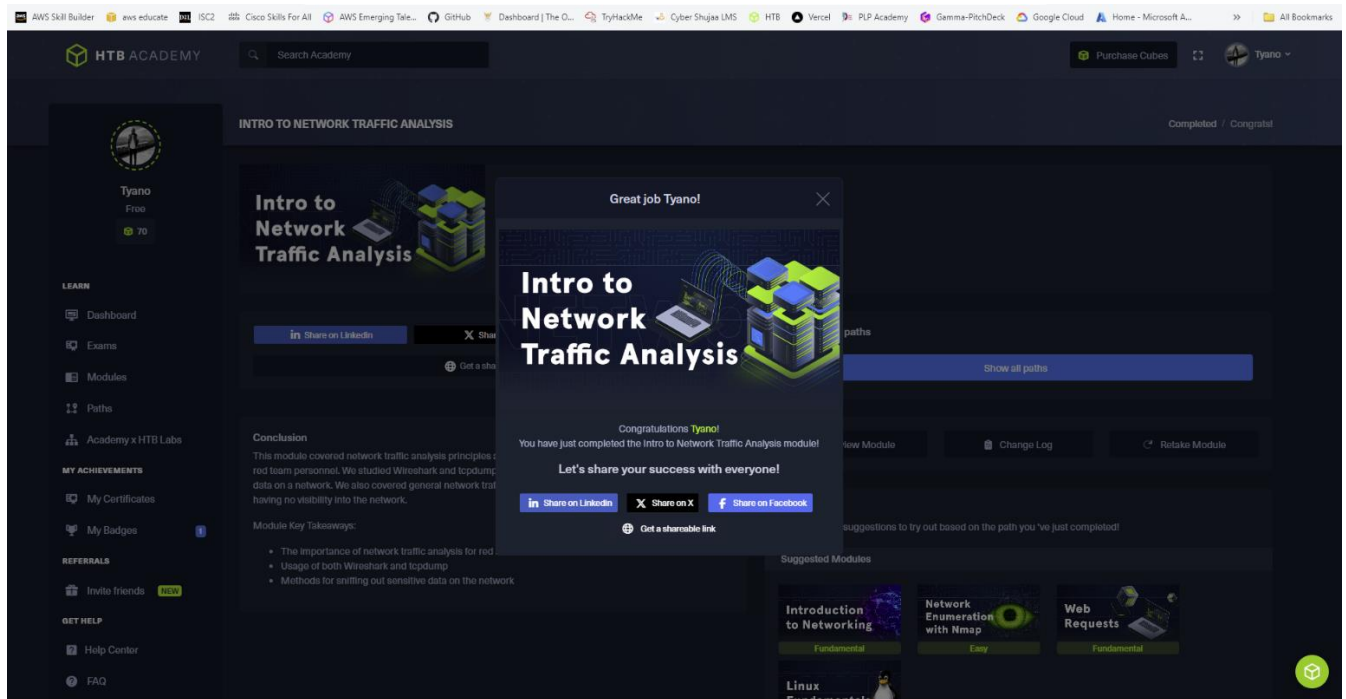
The user account we get when we examine the ASCII is **bucky** as shown in the screenshot above.



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.