Wireshark Basics

Objective

Wireshark is a great packet analysis tool. Ranging from HTTP, FTP to VOIP it supports more than 1000 different protocols to analyse, filter and dissect.

Network admins use it to solve critical network problems. Network security Admins use it for static or passive analysis to prevent network Intrusion, and hackers use it to capture and analyse traffic to extract useful information, actively or passively.

Background:
Your employer has sent your colleague to a penetration testing site.
Due to lack of time he couldn't perform a penetration test, but managed to get IP level access to the rootsh3ll labs wired LAN.
He has sent you a packet capture file which you'll find on your Desktop under `pcap-analysis` folder. Your task is to recover as much information from the *pcap* file and report it to your admin via the Verify Flag section.

This lab will help you learn:

1. How to identify source and destination address of sender/receiver.
2. How to filter various packets based on the protocol used for transmission
3. How to recover credentials from packet trace.
4. How to extract a complete file from a packet trace

The `rootsh3ll-labs-dump.pcap` file is stored under `/root/Desktop/pcap-analysis/`. Open the file in Wireshark for analysis and save the recovered file in the same folder with the appropriate name, as used during the transmission, for information integrity.

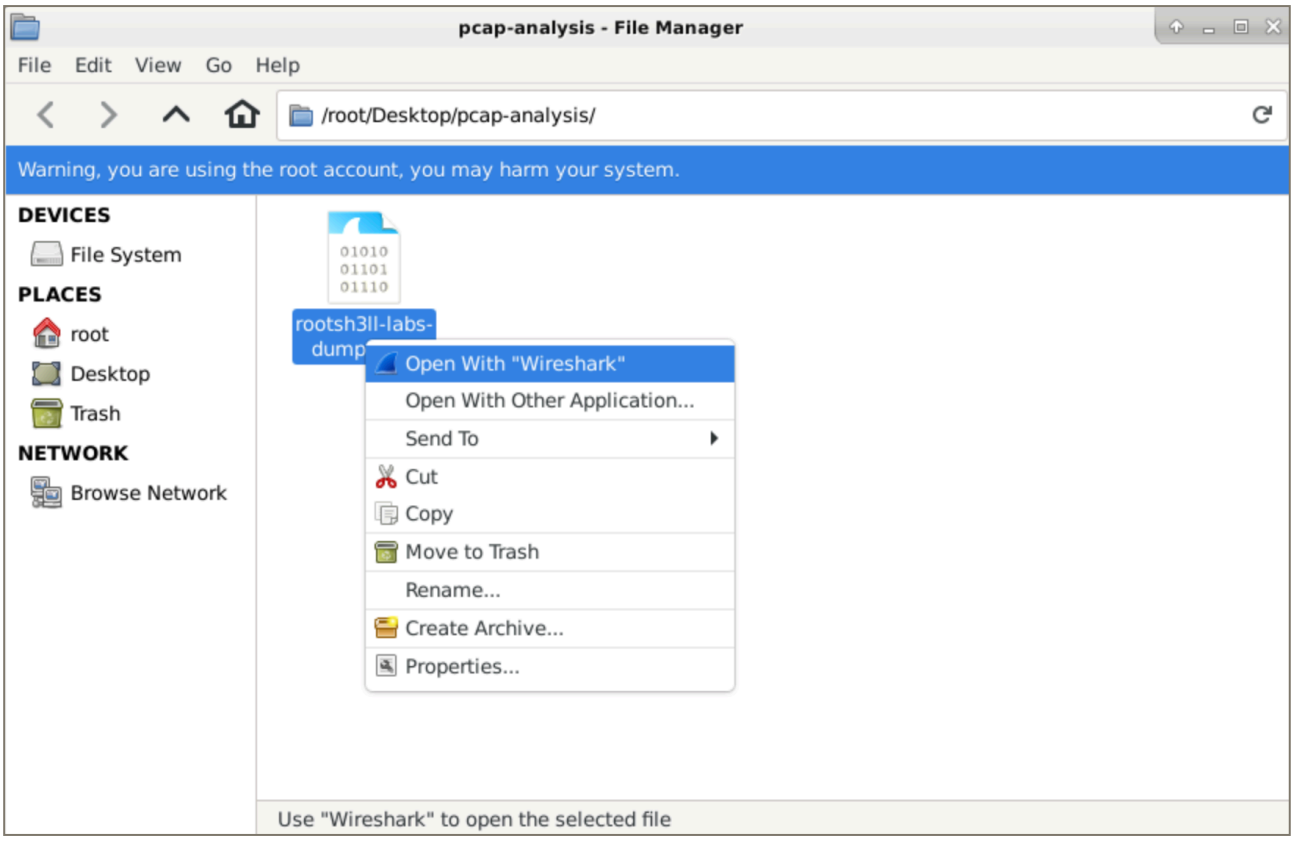
TABLE OF CONTENTS

Skip to Step 1 - Reconnaissance >>

1. What IP was found sending ICMP Ping requests over the network?

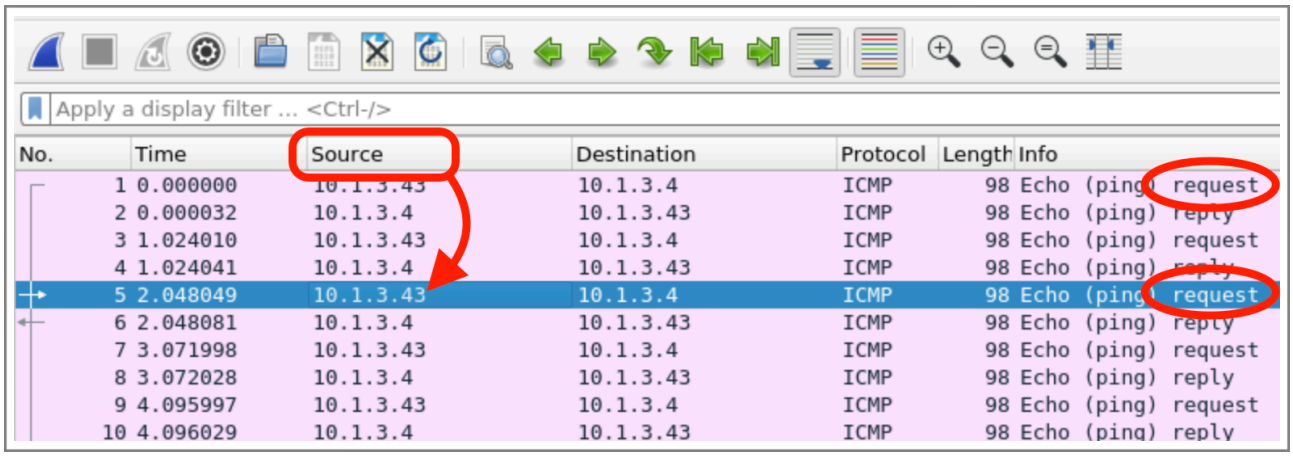
Open pcap-analysis/ folder located on Desktop

Right click on rootsh3ll-labs-dump.pcap > Open with "Wireshark"



Look at the first few packets. Note, the `Source` which is sending ICMP type requests to Destination `10.1.3.4`

You can also filter ICMP packets by typing `icmp` in search filter box.

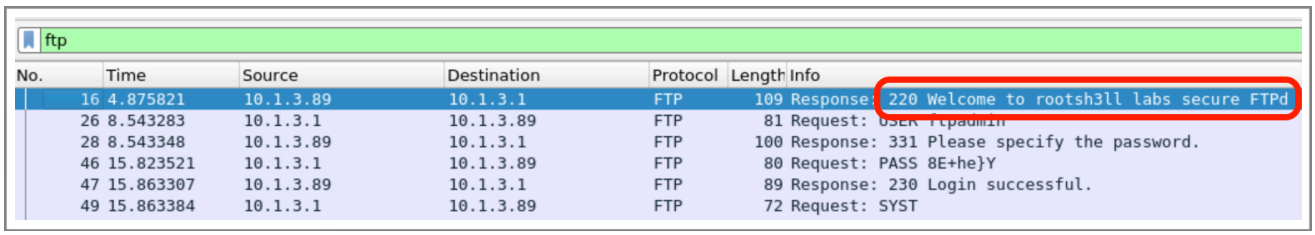


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.3.43	10.1.3.4	ICMP	98	Echo (ping) request
2	0.000032	10.1.3.4	10.1.3.43	ICMP	98	Echo (ping) reply
3	1.024010	10.1.3.43	10.1.3.4	ICMP	98	Echo (ping) request
4	1.024041	10.1.3.4	10.1.3.43	ICMP	98	Echo (ping) reply
5	2.048049	10.1.3.43	10.1.3.4	ICMP	98	Echo (ping) request
6	2.048081	10.1.3.4	10.1.3.43	ICMP	98	Echo (ping) reply
7	3.071998	10.1.3.43	10.1.3.4	ICMP	98	Echo (ping) request
8	3.072028	10.1.3.4	10.1.3.43	ICMP	98	Echo (ping) reply
9	4.095997	10.1.3.43	10.1.3.4	ICMP	98	Echo (ping) request
10	4.096029	10.1.3.4	10.1.3.43	ICMP	98	Echo (ping) reply

2. What does the FTP server's Welcome banner says?

We can use Wireshark filters in the green text input box. Since we want the FTP banner, we'd tell Wireshark to show data only transferred under FTP protocol

Click the search box > type `ftp`

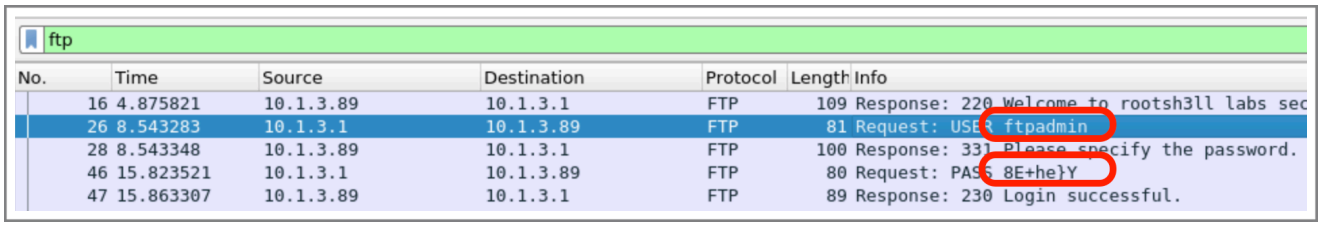


No.	Time	Source	Destination	Protocol	Length	Info
16	4.875821	10.1.3.89	10.1.3.1	FTP	109	Response: 220 Welcome to rootsh3ll labs secure FTPd
26	8.543283	10.1.3.1	10.1.3.89	FTP	81	Request: USER ftpadmin
28	8.543348	10.1.3.89	10.1.3.1	FTP	100	Response: 331 Please specify the password.
46	15.823521	10.1.3.1	10.1.3.89	FTP	80	Request: PASS 8E+he}Y
47	15.863307	10.1.3.89	10.1.3.1	FTP	89	Response: 230 Login successful.
49	15.863384	10.1.3.1	10.1.3.89	FTP	72	Request: SYST

3. Enter recovered FTP credentials from the packet capture file

Hint: Format - Username:Password

Packet number 26, and 46 clearly shows us the FTP credentials in plain-text format as the victim used plain



No.	Time	Source	Destination	Protocol	Length	Info
16	4.875821	10.1.3.89	10.1.3.1	FTP	109	Response: 220 Welcome to rootsh3ll labs sec
26	8.543283	10.1.3.1	10.1.3.89	FTP	81	Request: USER ftpadmin
28	8.543348	10.1.3.89	10.1.3.1	FTP	100	Response: 331 Please specify the password.
46	15.823521	10.1.3.1	10.1.3.89	FTP	80	Request: PASS 8E+he}Y
47	15.863307	10.1.3.89	10.1.3.1	FTP	89	Response: 230 Login successful.

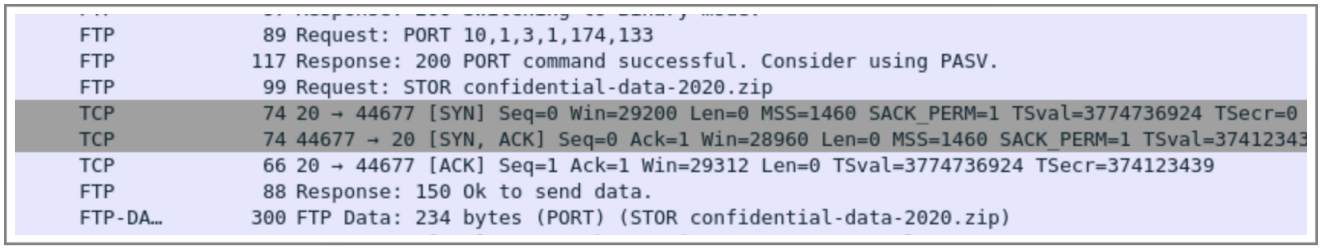
FTP protocol which is susceptible to such credential theft sniffing attacks.

4. FTP user was found uploading a file. What was the filename?

If you traverse the FTP packet trace, you'd notice the packet number 127 suggests that a zip file has been transferred from `10.1.3.89` (target host) to remote `FTP` server (`10.1.3.1`)

Discover the filename and enter into the appropriate field under **Verify Flags** section.

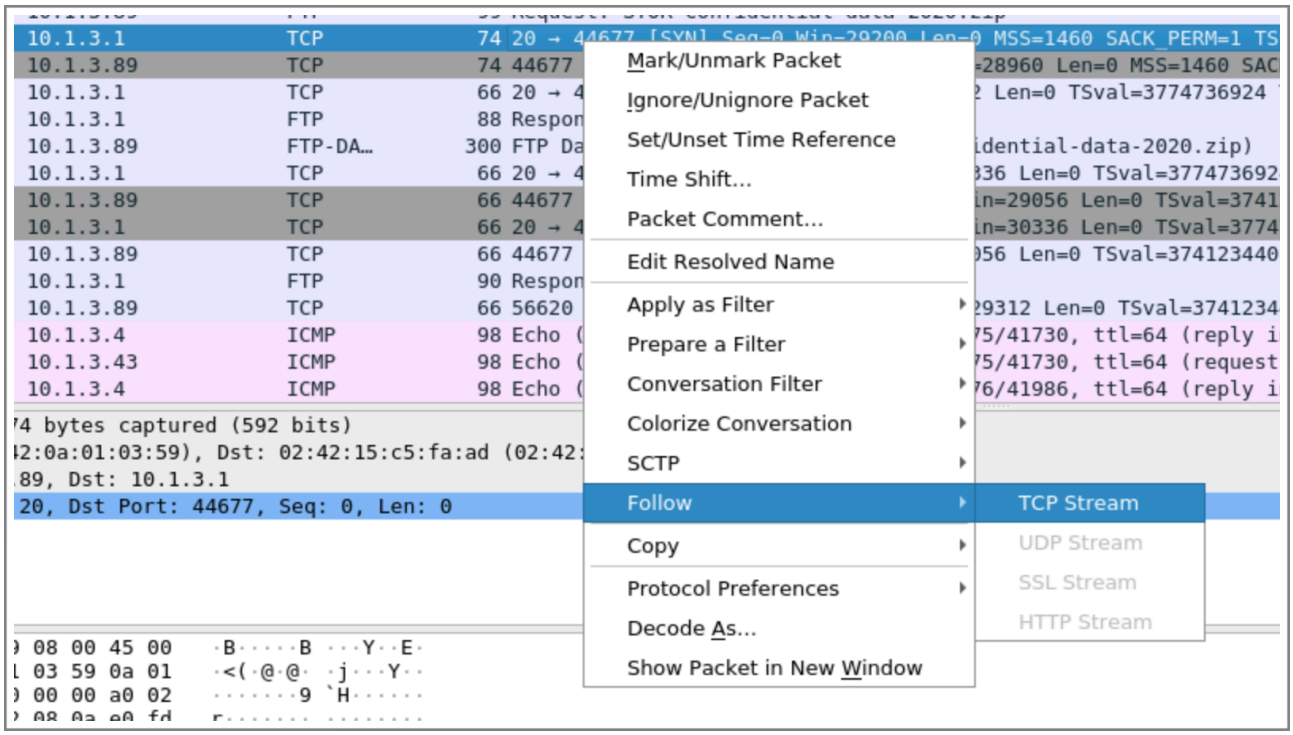
5. Recover the transferred file from packet trace using Wireshark. Enter md5sum of the recovered file



FTP	89	Request: PORT 10,1,3,1,174,133
FTP	117	Response: 200 PORT command successful. Consider using PASV.
FTP	99	Request: STOR confidential-data-2020.zip
TCP	74	20 → 44677 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3774736924 TSecr=0
TCP	74	44677 → 20 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=37412343
TCP	66	20 → 44677 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3774736924 TSecr=374123439
FTP	88	Response: 150 Ok to send data.
FTP-DA…	300	FTP Data: 234 bytes (PORT) (STOR confidential-data-2020.zip)

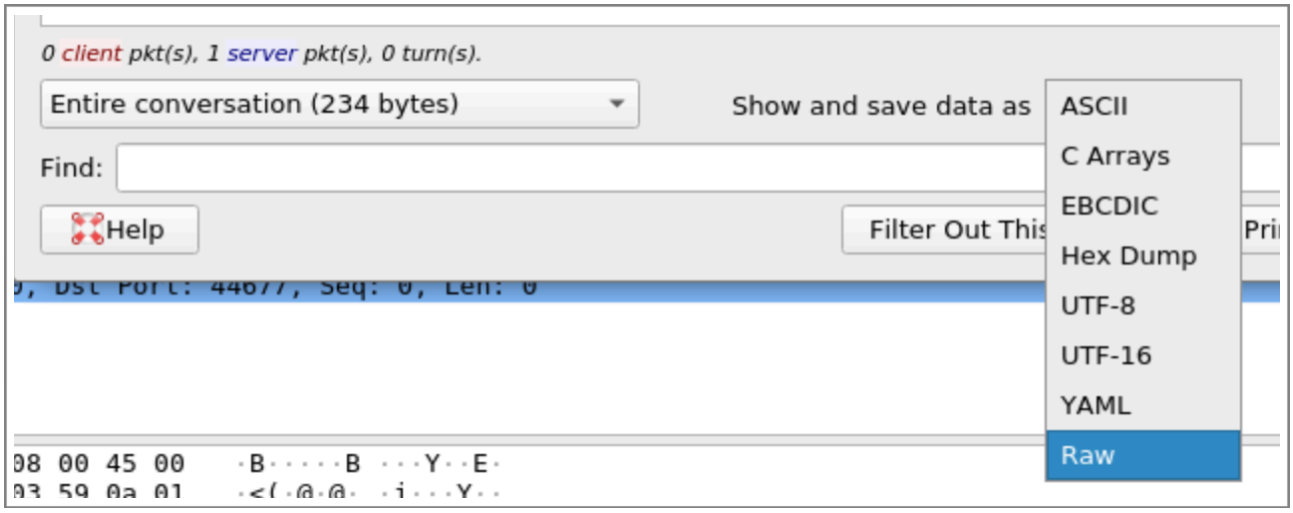
If you notice, the grey blocks of packets show the data transfer under TCP protocol. Following the TCP data stream of these packets will show you the actual bytes transferred through the network.

Right click TCP packet > Follow > TCP Stream



The data you see here are the actual bytes transferred from the victim to the FTP server.

Saving the ASCII data will result in corrupted .zip file. So we need to save the raw data to a file with the filename we recovered in the 4th step.



Click on Save as... > Give the .zip filename recovered in the 4th step.

Open Terminal and go to pcap-analysis/ directory

```
cd /root/Desktop/pcap-analysis/
```

Calculate md5 Hash of the downloaded file

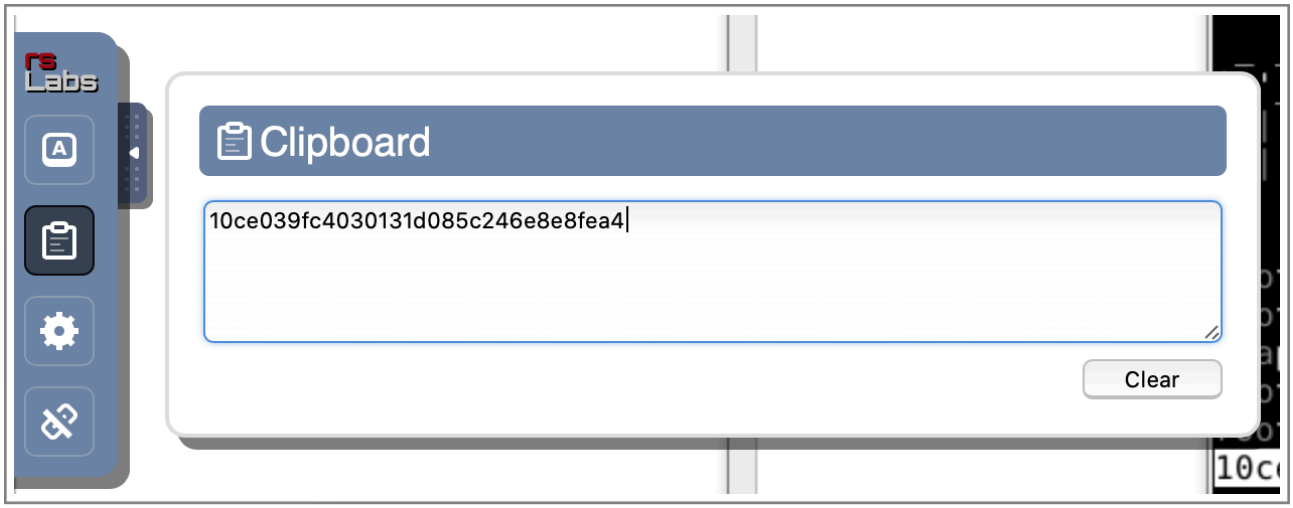
```
md5sum [Recovered-Filename.zip]
```

This will return the final flag to you as a 32-bit random alpha-numeric text. Enter the value in the final flag under Verify Flag section.

6. How to Copy text in and out of rootsh3ll Labs GUI

Copy the 32 bit random string returned by the md5sum program.

Click on the little blue floating tip on the centre-left of your screen. And select the clipboard icon.



Using this text box you can copy the data in and out of the GUI. Use the copied string from this text box and paste into your final flag.