WIRESHARK CAPTURE THE FLAG

AKHILESH ANAND UNDRALLA
UNIVERSITY AT BUFFALO

12/09/2021

TABLE OF CONTENTS

Flag 1- Haveibeenpwned?

Flag: `hugerhinolover@hotmail.com`

Email address for the user agent is hugerhinolover@hotmail.com since there is evidence of User-Agent and pre-installed cookies installed on the user's device.

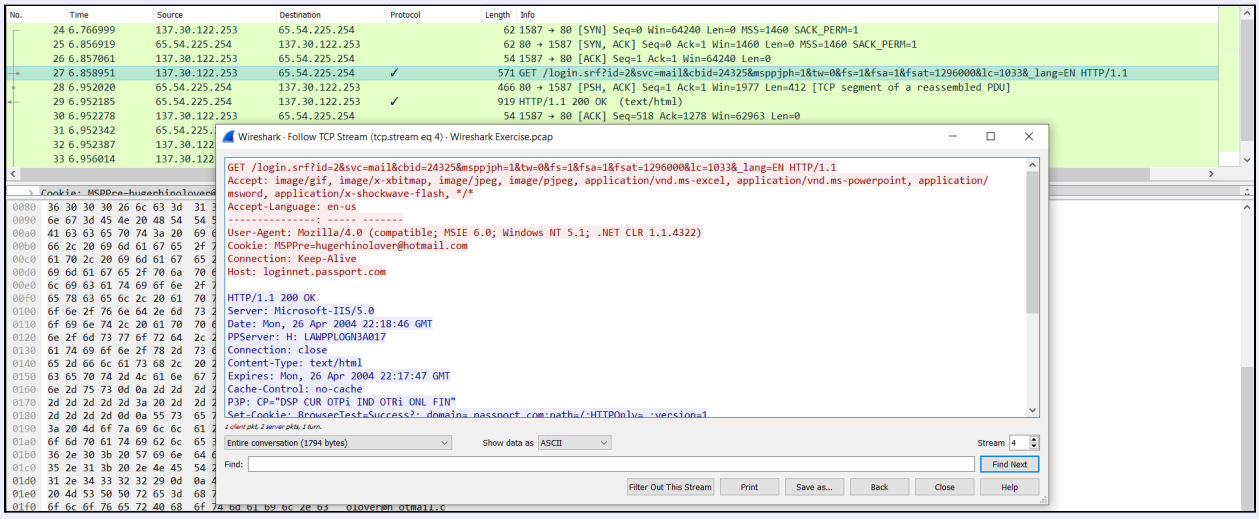


Figure 1.1: Packet details showing email address of the user involved in this network activity

Flag 2: What's the password?

Flag: `gnome123`

This flag was found by searching for packet search of keyword "password" and following a prospective TCP stream and checking the packet data in ASCII format.

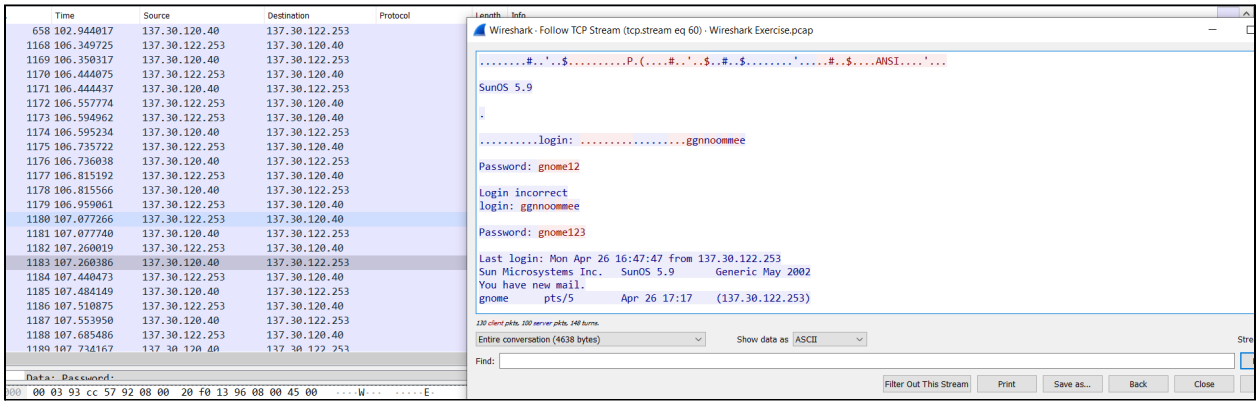


Figure 1.2: Packet details acquired by following a TCP stream with password keyword

Flag 3 - I need a new password

Flag: `Old and new passwords must differ by at least 3 positions.`

This flag was found by following a TCP stream of a potential packet and checking the packet data in ASCII format. This indicate a possible control to restrict having weak passwords.

```
passwd: Changing password for gnome
Enter existing login password: gnome123

New Password: gnome1234

passwd: Old and new passwords must differ by at least 3 positions.

Please try again
New Password: gnome12345

Re-enter new Password: gnome12345

Permission denied
cook:[gnome]$ llooggoouutt

ksh: logout:  not found
```

Figure 1.3: Packet details acquired by following a TCP stream with password control information

Flag 4 - Hidden in plain sight

Flag: `contraband.zip`

The file “contraband.zip” user accessed looks suspicious since it is password protected and has rhino2.jpg inside that zip file. Other two files user accessed are rhino1.jpg and thino3.jpg.

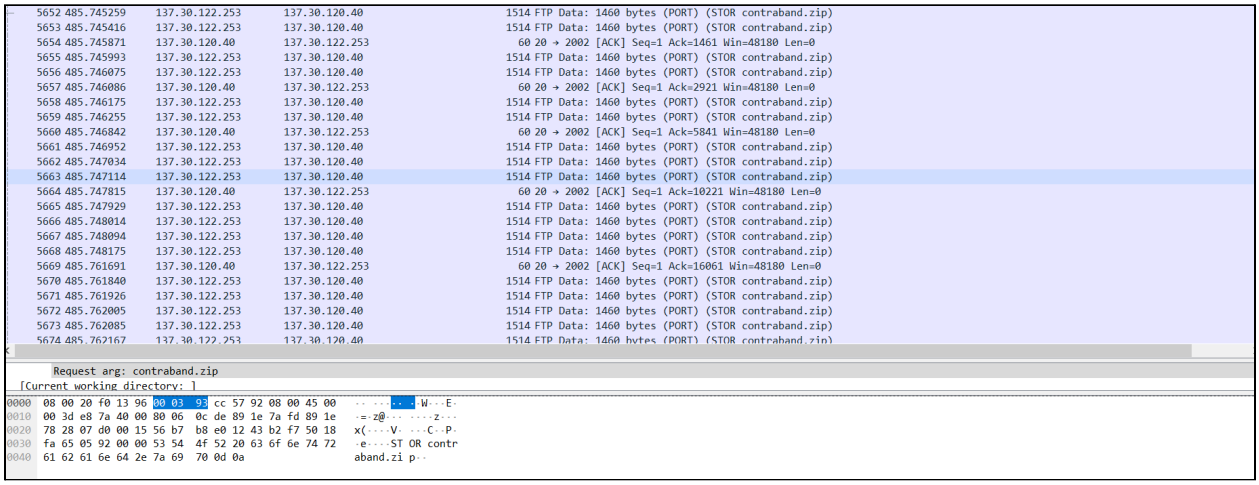
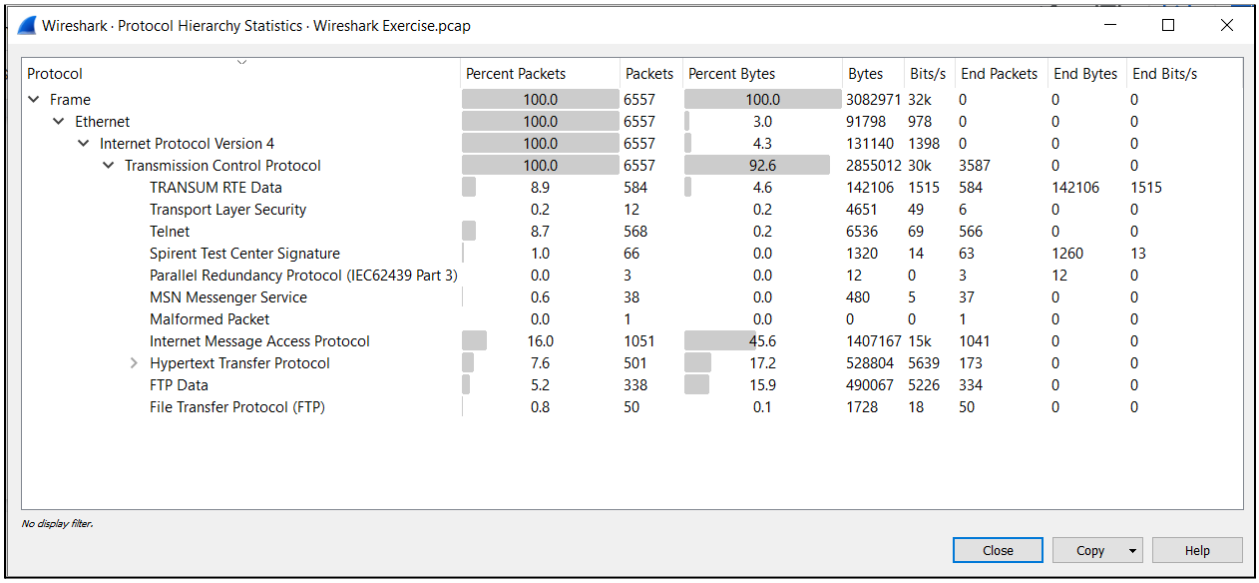


Figure 1.4: network packet for contraband.zip

Flag 5 -Higher-level thinking

Flag:

```
Transmission Control Protocol
Transport Layer Security
Telnet
Parallel Redundancy Protocol (IEC62439 Part 3)
Internet Message Access Protocol
Hypertext Transfer Protocol
File Transfer Protocol (FTP)
```



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	6557	100.0	3082971	32k	0	0	0
Ethernet	100.0	6557	3.0	91798	978	0	0	0
Internet Protocol Version 4	100.0	6557	4.3	131140	1398	0	0	0
Transmission Control Protocol	100.0	6557	92.6	2855012	30k	3587	0	0
TRANSUM RTE Data	8.9	584	4.6	142106	1515	584	142106	1515
Transport Layer Security	0.2	12	0.2	4651	49	6	0	0
Telnet	8.7	568	0.2	6536	69	566	0	0
Spirent Test Center Signature	1.0	66	0.0	1320	14	63	1260	13
Parallel Redundancy Protocol (IEC62439 Part 3)	0.0	3	0.0	12	0	3	12	0
MSN Messenger Service	0.6	38	0.0	480	5	37	0	0
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Internet Message Access Protocol	16.0	1051	45.6	1407167	15k	1041	0	0
Hypertext Transfer Protocol	7.6	501	17.2	528804	5639	173	0	0
FTP Data	5.2	338	15.9	490067	5226	334	0	0
File Transfer Protocol (FTP)	0.8	50	0.1	1728	18	50	0	0

Figure 1.5: Protocols used by the user

FTP Protocol

File Transfer Protocol (FTP) is a client-server protocol that is used to transfer files directly between computers i.e., FTP client and user's web server over the internet. FTP is older than HTTP and preceded TCP/IP protocol. The web client creates a connection to the FTP server port 21 inorder to transfer a file.

FTP doesn't encrypt network traffic and all the transmissions are done in clear text. Incase of a packet capture on the network, it is possible to read packet data, usernames, passwords and commands in clear text. This is a major security weakness in using FTP.

FTP is used to send files between computers in a corporate network whereas websites use FTP to transfer files i.e uploading and downloading of files from respective web servers. FTP

has the ability to transfer very large multiple files (Eg. file in gigabytes) at once with lossless transmission which can improve workflows.

SFTP- Secure Shell (SSH) File Transfer Protocol or Secure File Transfer Protocol transfers files between FTP client and web server via SSH. SFTP allows inbound communication on port 22. Unlike FTP, SFTP requires the user to be authenticated via a user ID and password, SSH keys, or a combination of the two inorder to establish a connection between the sender and receiver and uses a tunneling method to transfer data.