OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

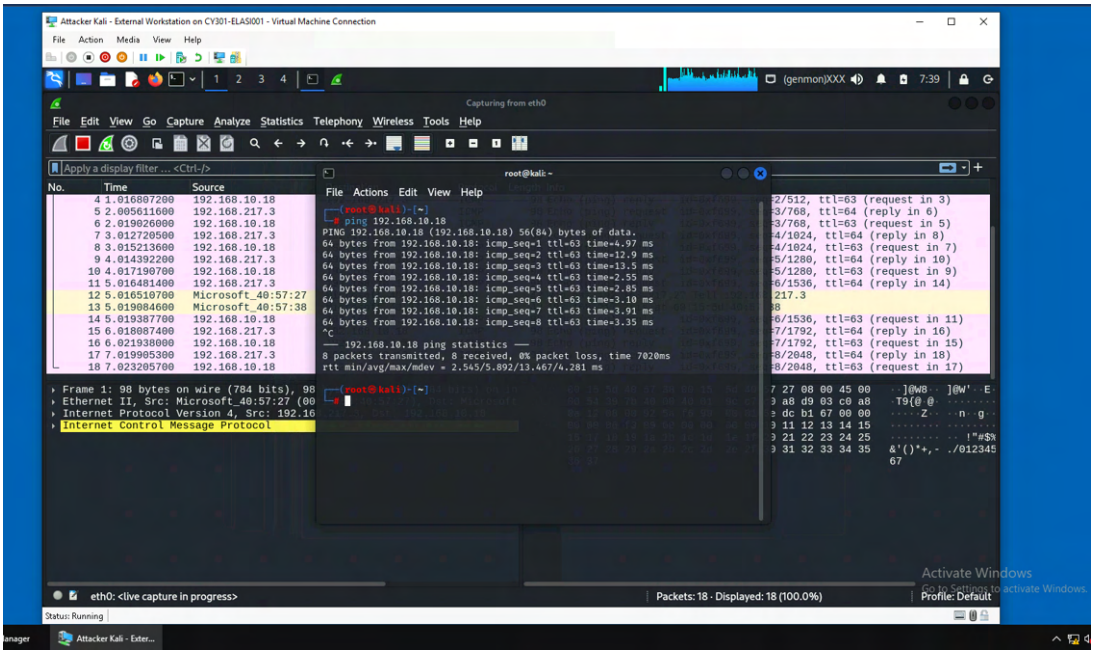
Ethan Lasich

01280954

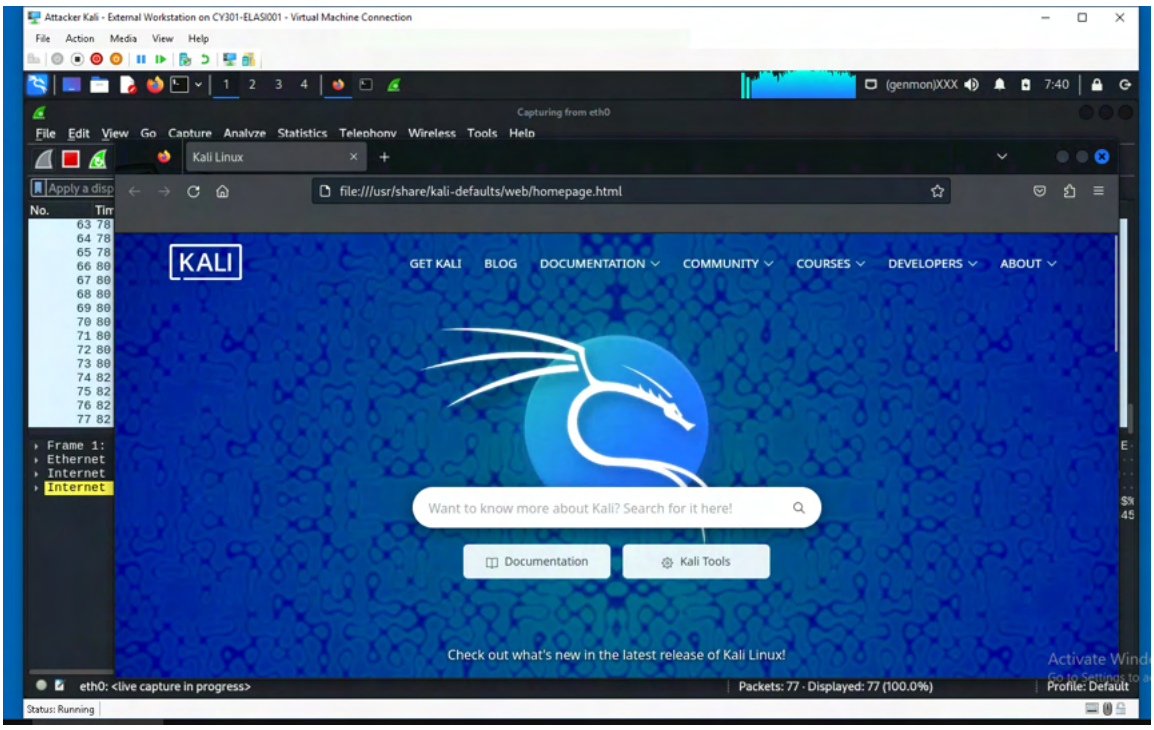
Below is the snippet of a sample lab report.

TASK A

Steps 1-2:



Steps 3-4:



Q1. How many packets are captured in total? How many packets are displayed?

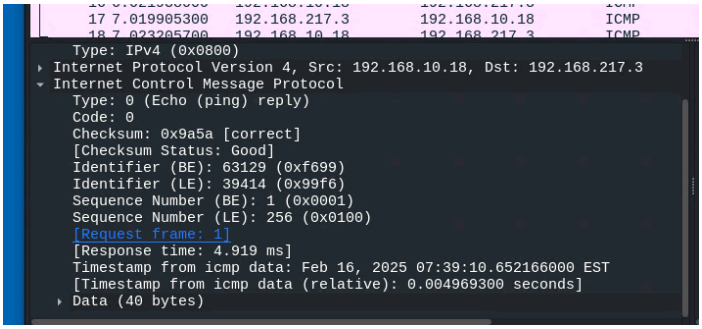
I captured 211 packets, all of which are displayed.

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1).

With the filter, there’s only 18 packets displayed.

Q3. Select an Echo (replay) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time?

The source of the IP was 192.168.10.18, and the destination was 192.168.217.3. The sequence number was 1/256, the size of the data is 40 bytes, and the response time was 4.919ms.

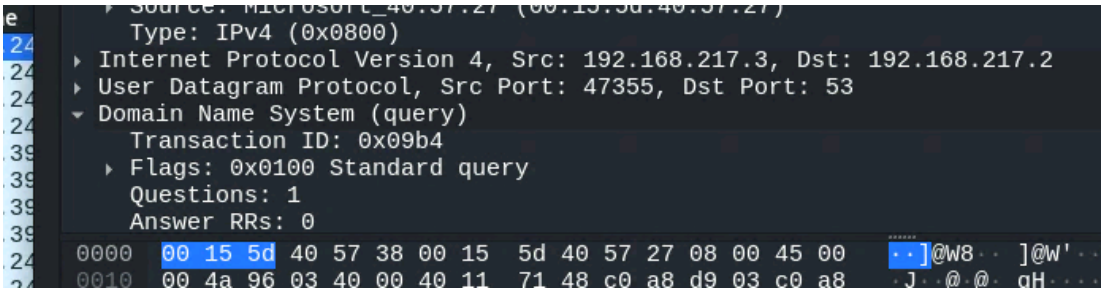


Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed?

With the DNS filter there are 190 packets displayed.

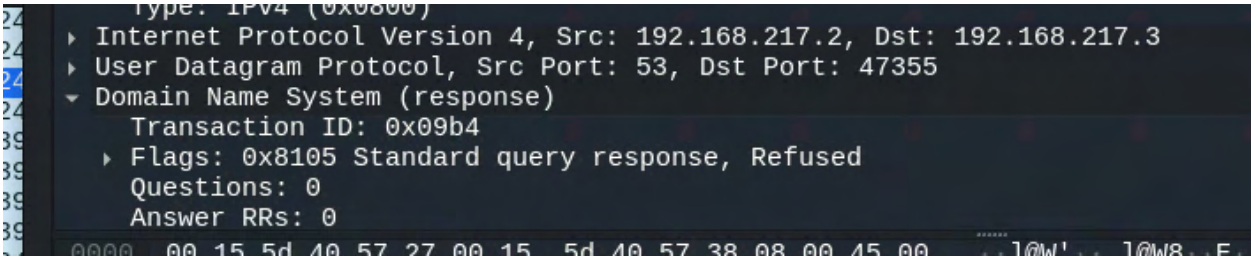
Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

The source is 192.168.217.3:47355 and the destination is 192.168.217.2:53.



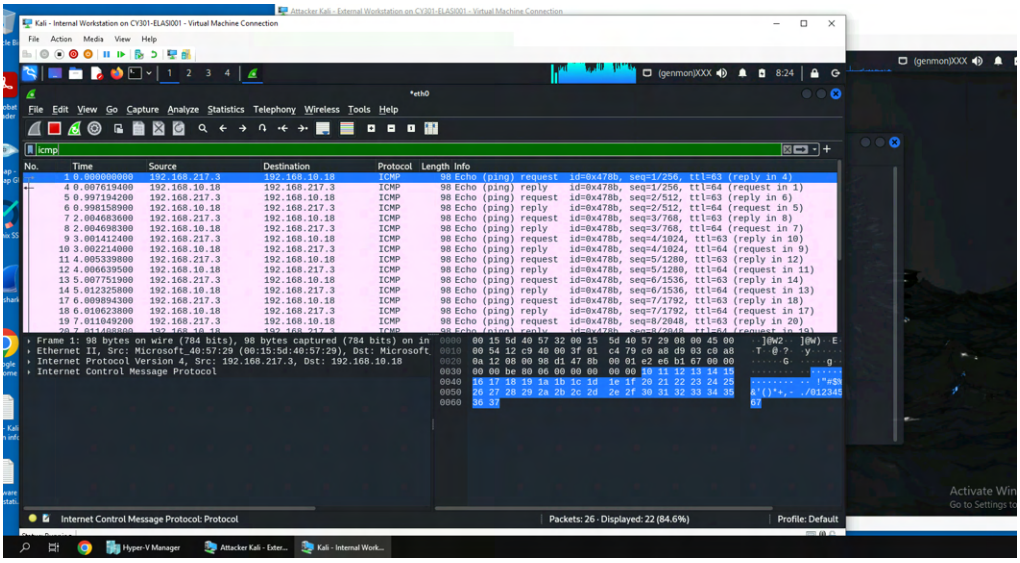
Q6. Find the corresponding DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server?

The source for the response is from 192.168.217.2:53 with a destination of 192.168.217:47355. The reply message just says “Refused.”

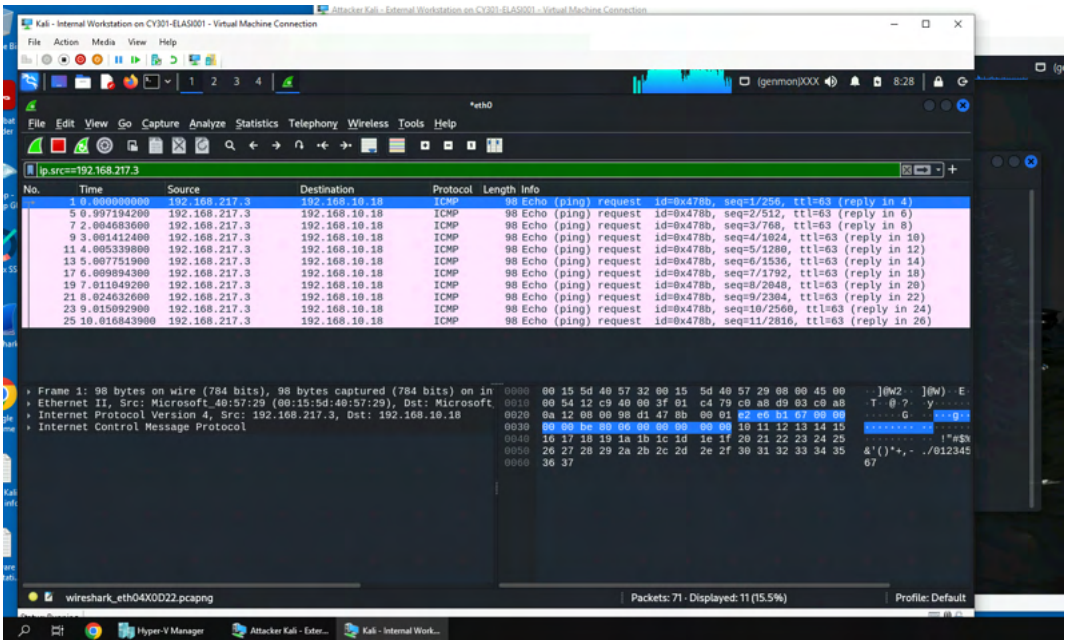


Task B:

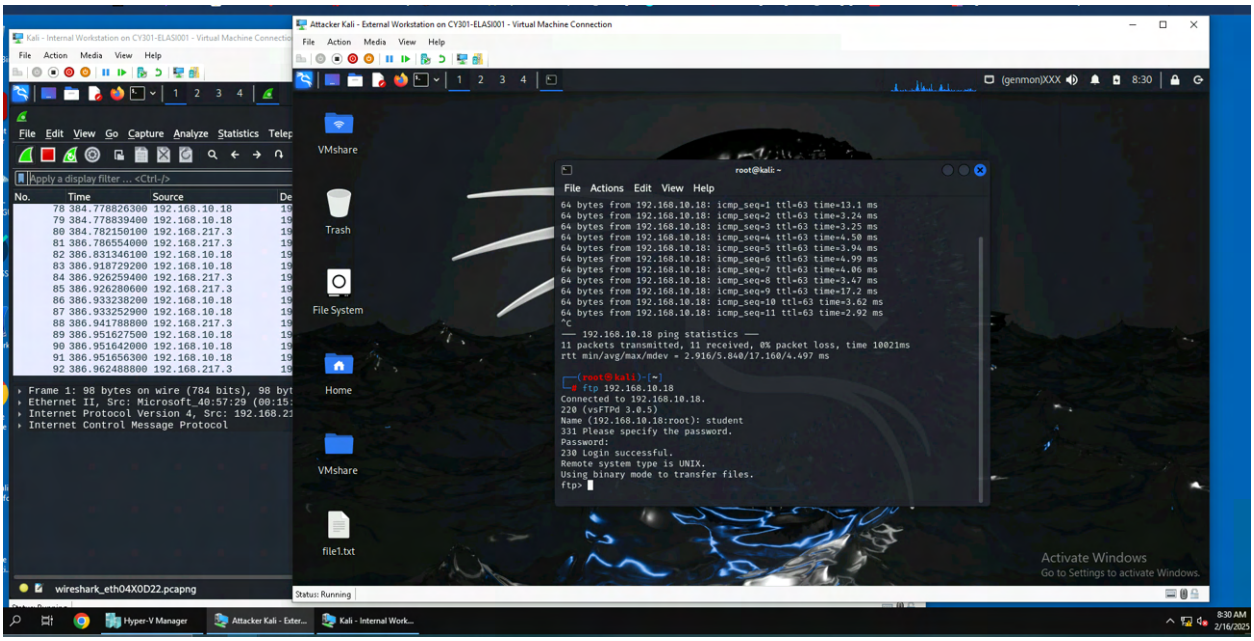
Part 1 Step a:



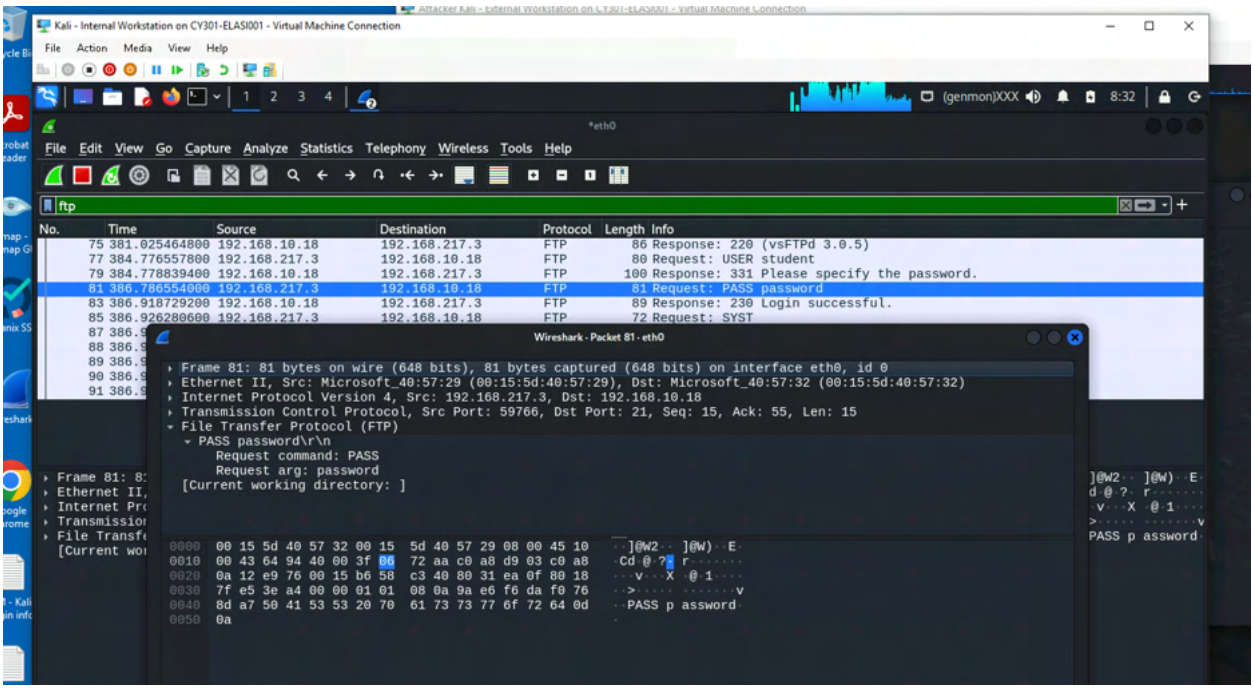
Part 1 Step b:



Part 2 step a:

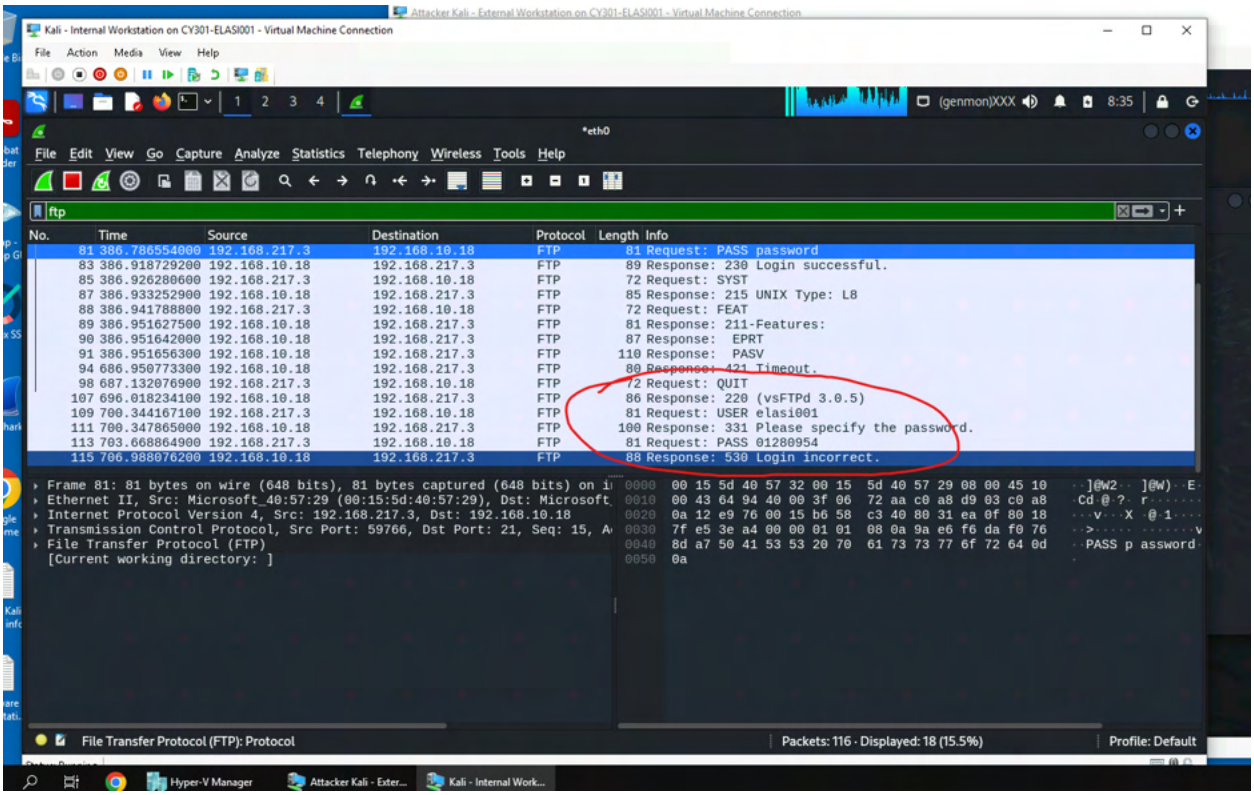


Step b:



By filtering the traffic to “ftp” and reading through the info tab on the right, I was able to read the messages between the two machines in plaintext. The server sent “Please specify the password” and by looking at the next packet, I saw the request argument was “password.”

Step c:


Kali - Internal Workstation on CY301-ELASI001 - Virtual Machine Connection
File Action Media View Help
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
No. Time Source Destination Protocol Length Info
81 386.786554000 192.168.217.3 192.168.10.18 FTP 81 Request: PASS password
83 386.918729200 192.168.10.18 192.168.217.3 FTP 89 Response: 230 Login successful.
85 386.926280600 192.168.217.3 192.168.10.18 FTP 72 Request: SYST
87 386.933252900 192.168.10.18 192.168.217.3 FTP 85 Response: 215 UNIX Type: L8
88 386.941788800 192.168.217.3 192.168.10.18 FTP 72 Request: FEAT
89 386.951627500 192.168.10.18 192.168.217.3 FTP 81 Response: 211-Features:
90 386.951642000 192.168.10.18 192.168.217.3 FTP 87 Response: EPRT
91 386.951656300 192.168.10.18 192.168.217.3 FTP 110 Response: PASV
94 686.950773300 192.168.10.18 192.168.217.3 FTP 80 Response: 421 Timeout.
98 687.132076900 192.168.217.3 192.168.10.18 FTP 72 Request: QUIT
107 696.018234100 192.168.10.18 192.168.217.3 FTP 86 Response: 220 (vsFTPd 3.0.5)
109 700.344167100 192.168.217.3 192.168.10.18 FTP 81 Request: USER elasi001
111 700.347865000 192.168.10.18 192.168.217.3 FTP 100 Response: 331 Please specify the password.
113 703.668864900 192.168.217.3 192.168.10.18 FTP 81 Request: PASS 01280954
115 706.988076200 192.168.10.18 192.168.217.3 FTP 88 Response: 530 Login incorrect.
Frame 81: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on i
Ethernet II, Src: Microsoft_40:57:29 (00:15:5d:40:57:29), Dst: Microsoft
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.18
Transmission Control Protocol, Src Port: 59766, Dst Port: 21, Seq: 15, A
File Transfer Protocol (FTP)
[Current working directory:]
0000 00 15 5d 40 57 32 00 15 5d 40 57 29 08 00 45 10
0010 00 43 64 94 40 00 3f 06 72 aa c0 a8 d9 03 c0 a8
0020 0a 12 e9 76 00 15 b6 58 c3 40 80 31 ea 0f 80 18
0030 7f e5 3e a4 00 00 01 01 08 0a 9a e6 f6 da f0 76
0040 8d a7 50 41 53 53 20 70 61 73 73 77 6f 72 64 0d
0050 0a
PASS p assword
File Transfer Protocol (FTP): Protocol
Packets: 116 · Displayed: 18 (15.5%)
Profile: Default
Hyper-V Manager
Attacker Kali - Exter...
Kali - Internal Work...