OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Password Cracking

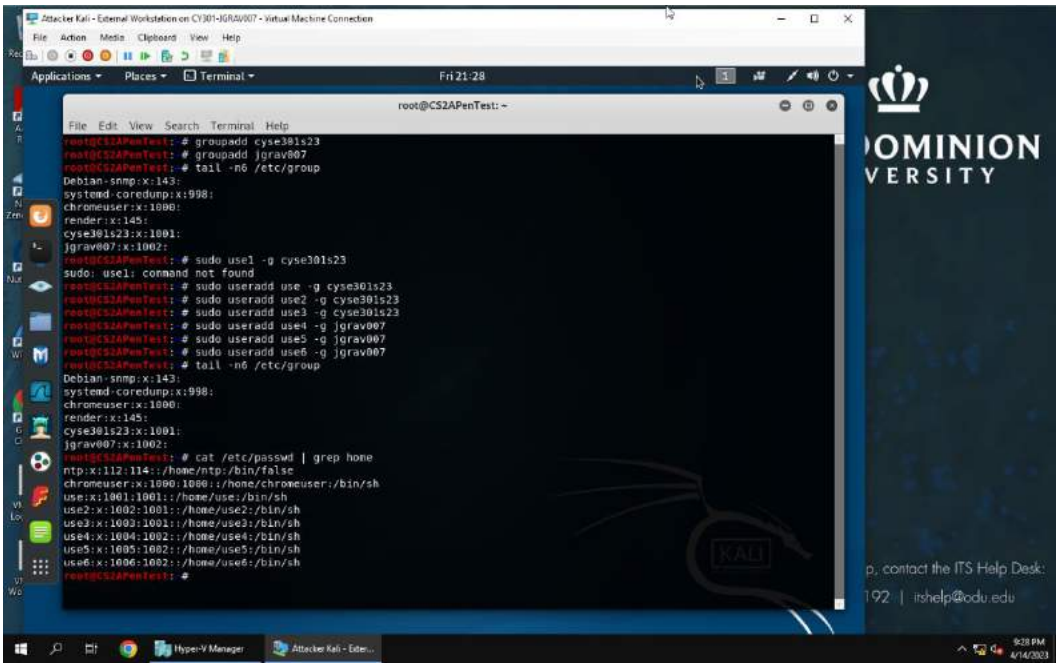
Simon Graves

01195419

Below is the snippet of a sample lab report.

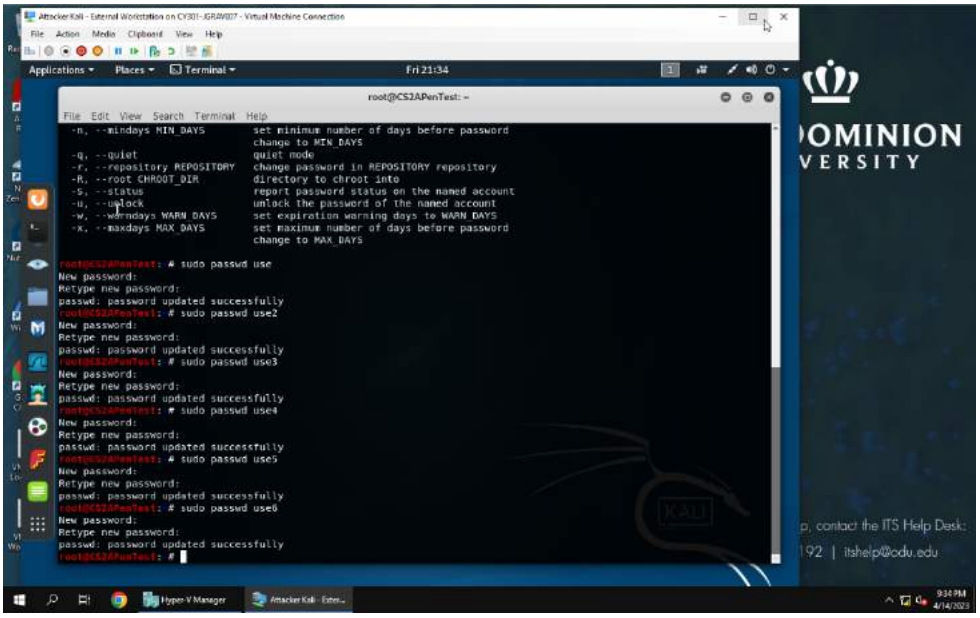
TASK A

1. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.
2. Create and assign three users to each group. Display related UID and GID information of each user.



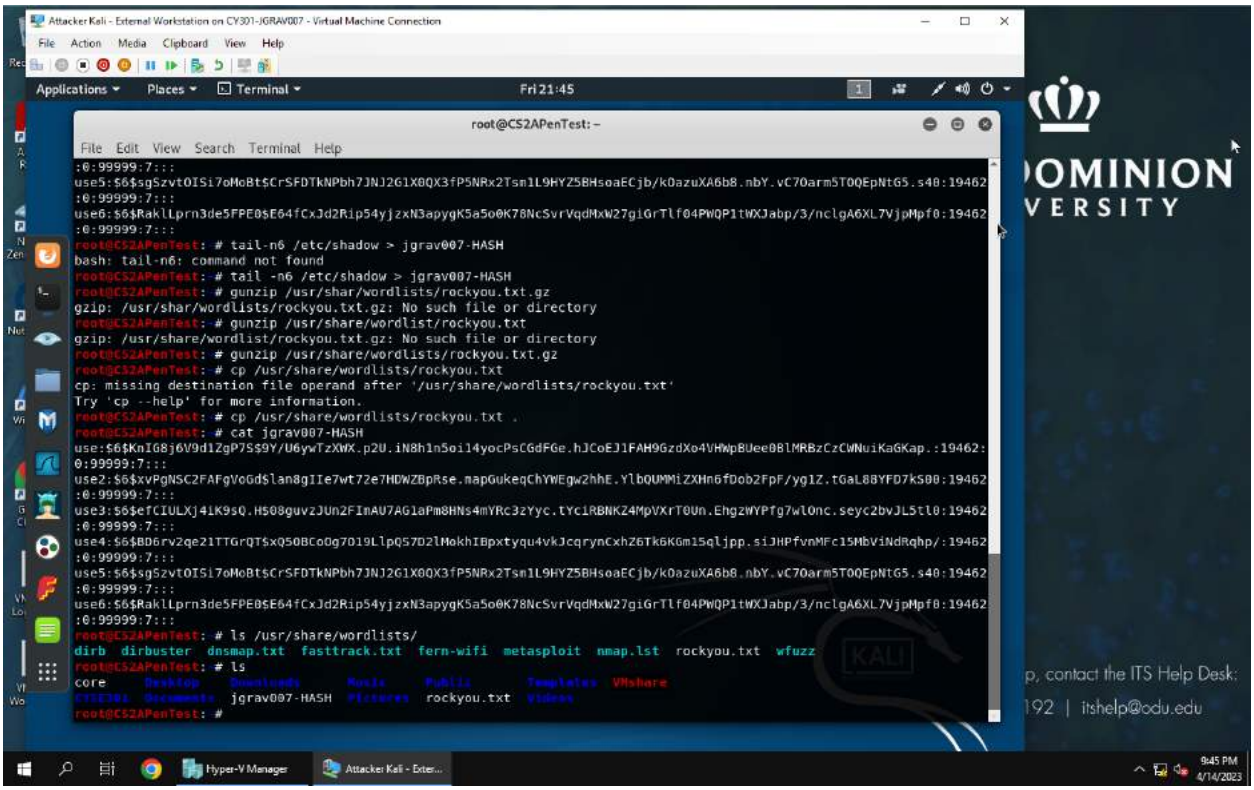
In figure 1 I created 2 groups cyse301s23 and jgrav007. Then I used the command “tail /etc/group -n6” to show the corresponding group IDs. Then I used “sudo useradd” to add users to the groups I had pervious made. I made six groups.

3. Choose six new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords.

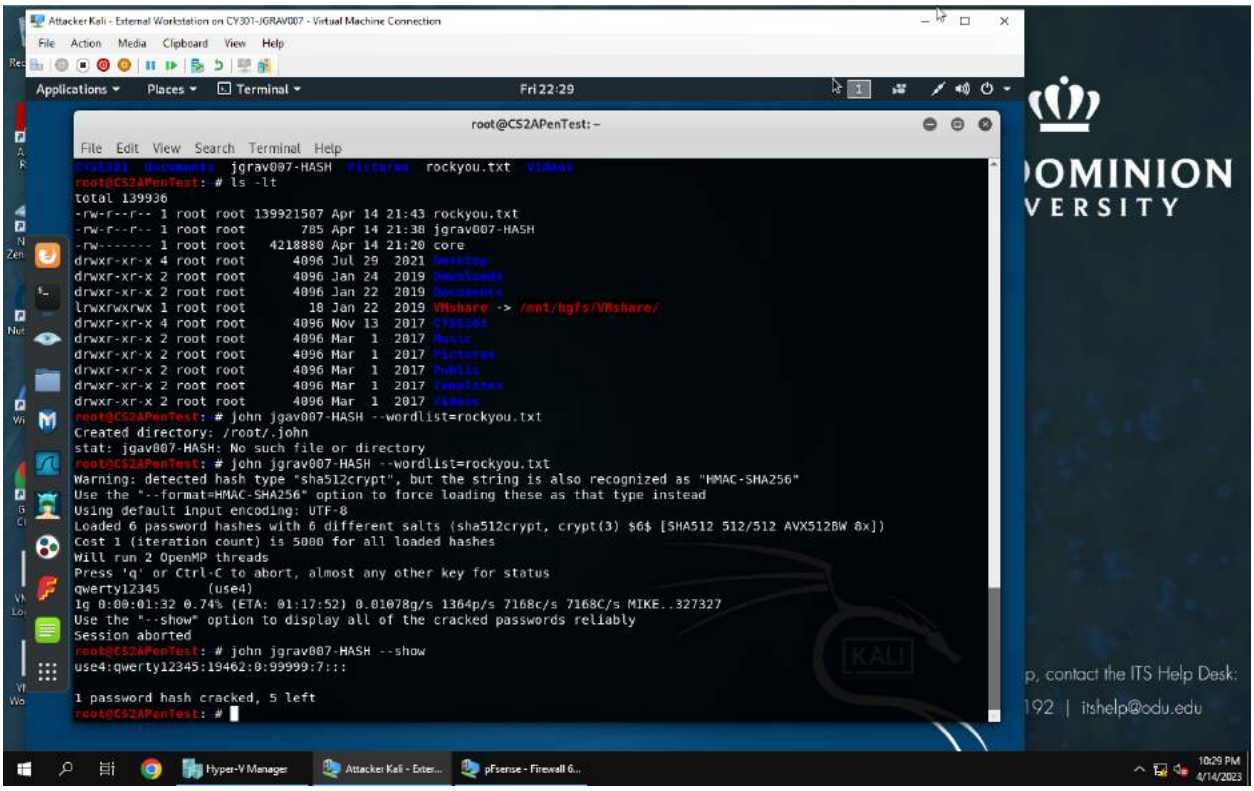


I used command “sudo passwd” to add passwords to the different users. Username1 - Password1!; USername2- SuperPassword123; Username3- ilovepizza77; Username4- qwerty12345; USername5- aardvark#1; Username6- @sdf#$^gfK^&*76

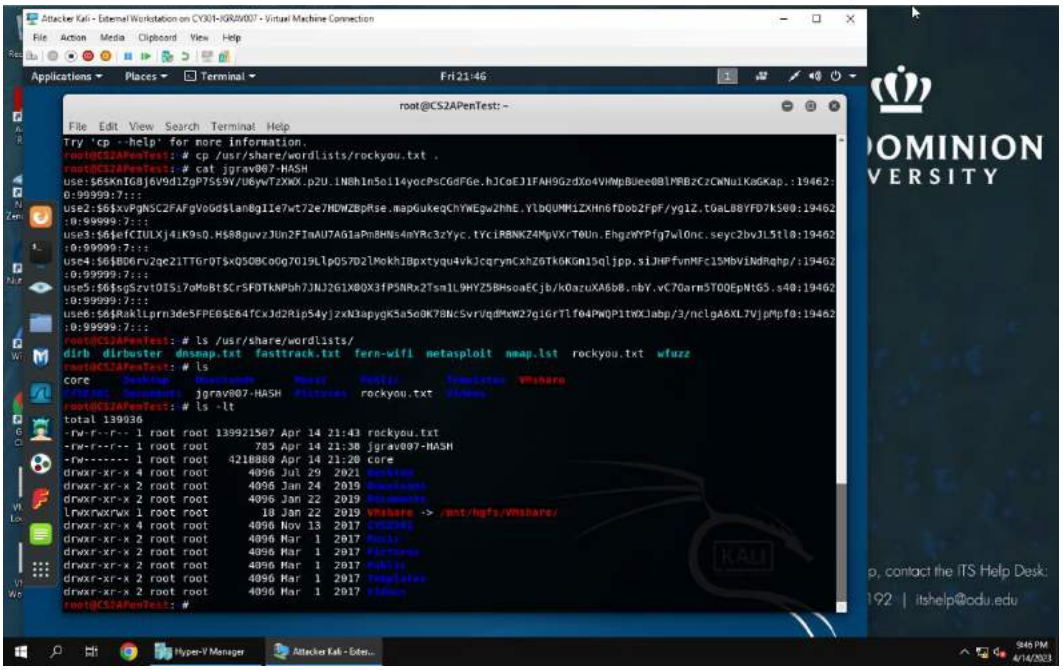
4. Export all six users' password hashes into a file named "YourMIDAS-HASH" (for example, pjiang-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



Above I used the command tail -n6 /etc/shadow which display the password hash. It's then copied it to jgrav007 hash using tail -n6 /etc/shadow/ > jgrav007-HASH. The commanded I used next was unzip /usr/share/wordlists/rockyou.txt.gz" to use the dictionary attack and finally "cp /usr/share/wordlists/rockyou.txt" to copy the file.



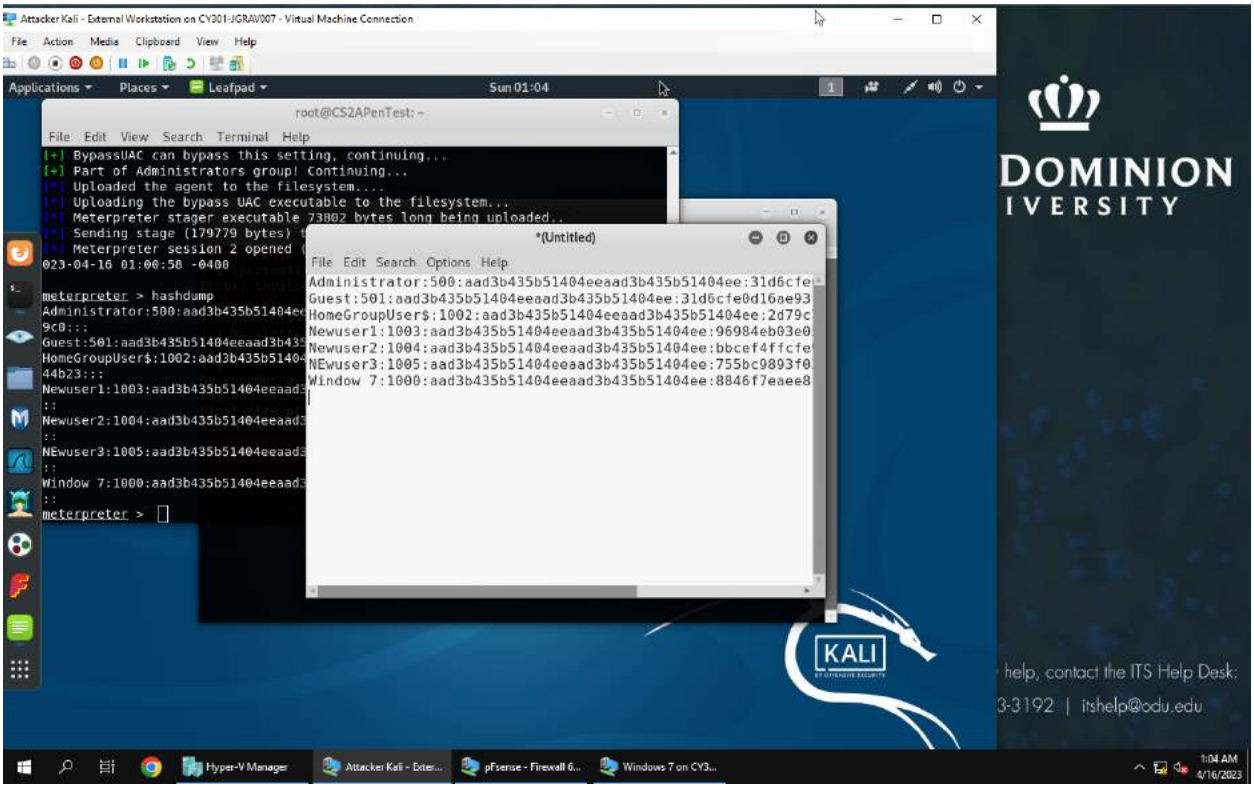
Above in figure 4 I used the command "john jgrav007-HASH –wordlist-rockyou.txt" to find the password of the HASH. To attack and finally crack 1 password. Which the easiest password was qwerty12345.



Above is cat jgrav007-HASH which is used to concatenate and display the file.

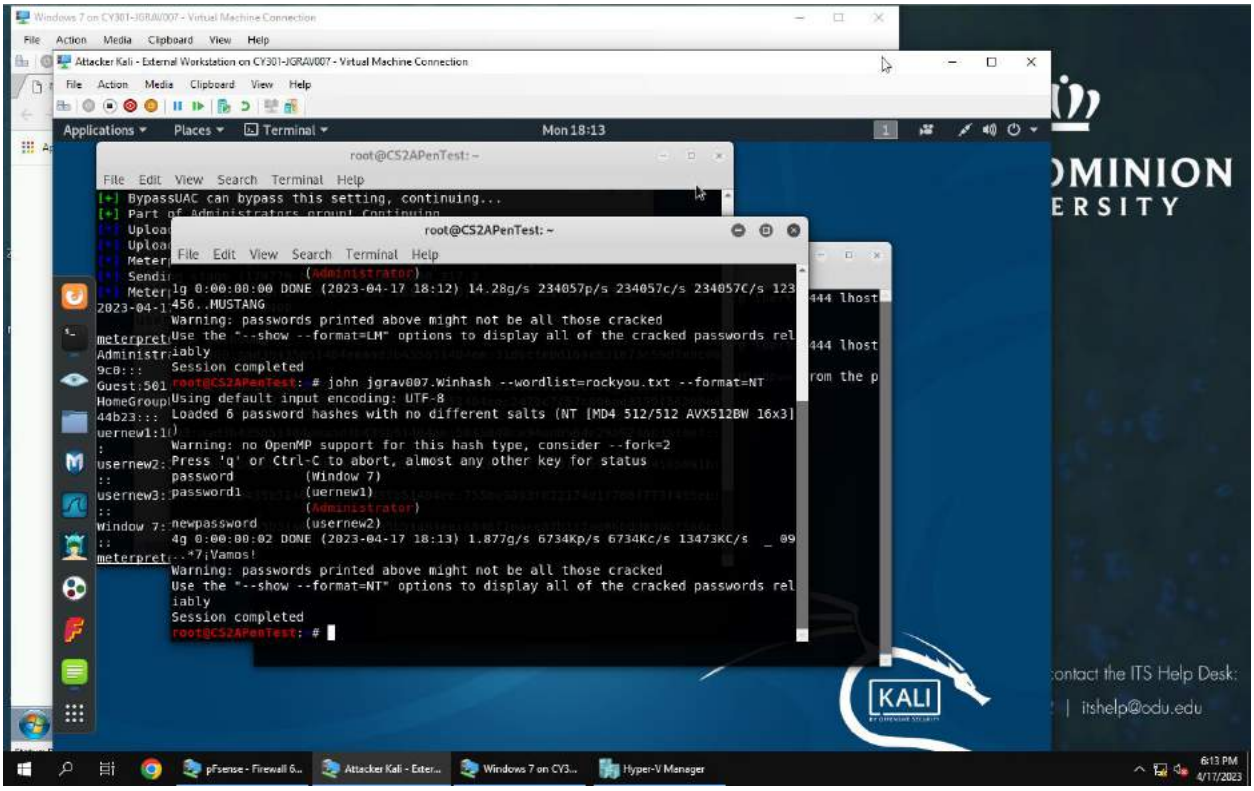
TASK B

1. Display the password hashes by using the “hashdump” command in the meterpreter shell.



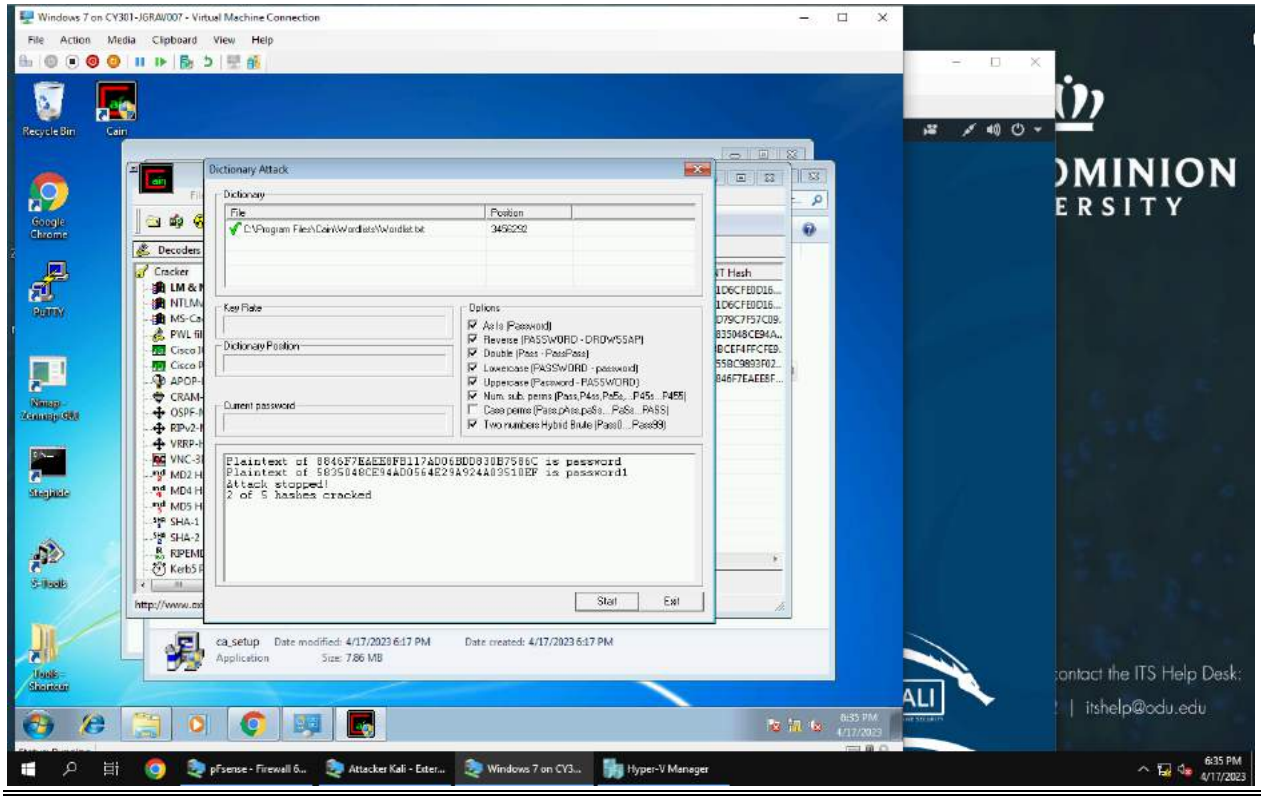
Used command hashdump in meterpreter to show all the hash in the account and put into a notpad.

2.Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.

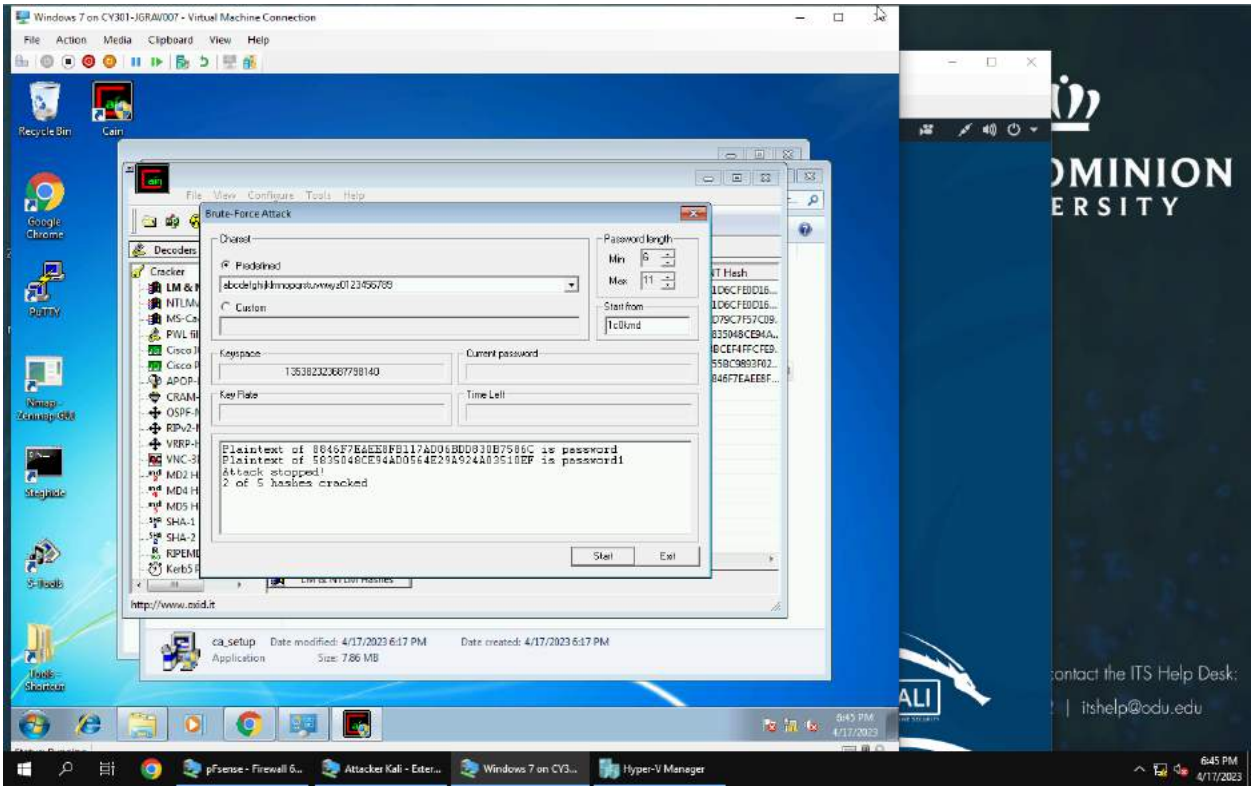


Then I used the john command to crack the password to the accounts I made in windows 7.

3.Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).



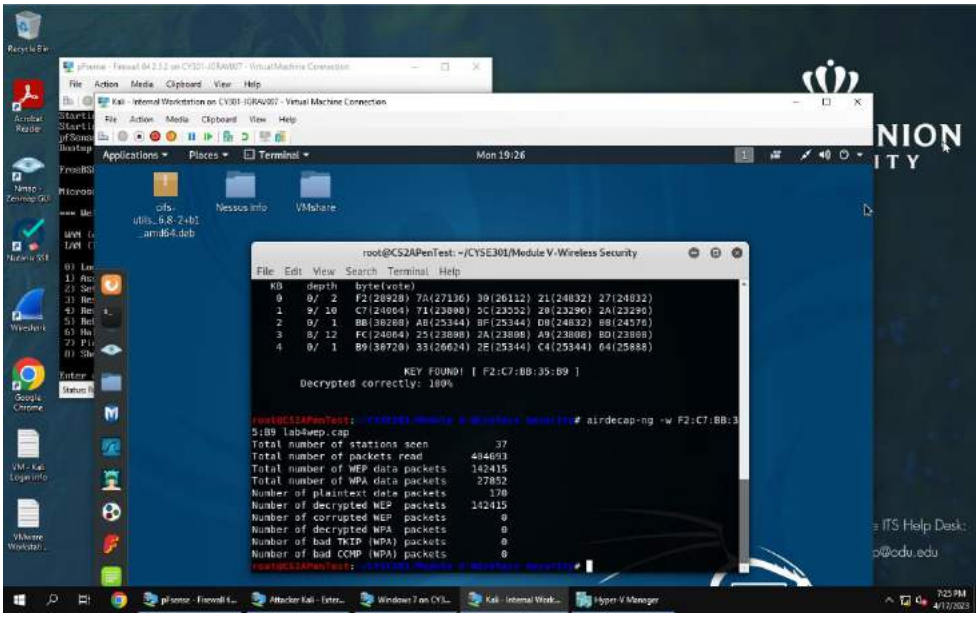
This is me doing a dictionary attack in windows 7 cracking the password. These passwords were creak within seconds.



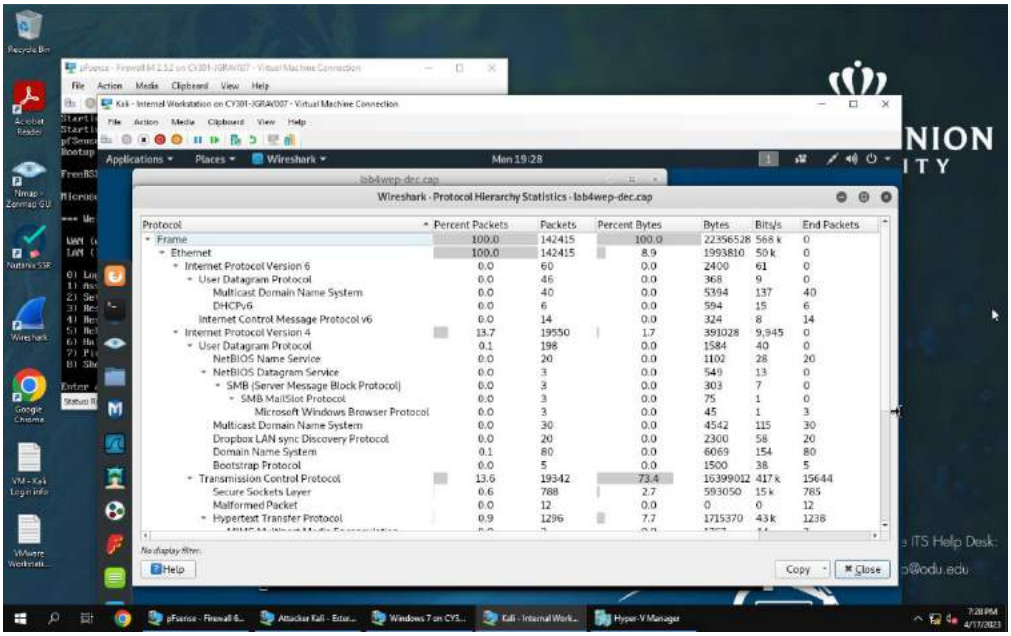
I used brute-force attack to creak some passwords and the same two were creaked within seconds and the setting was min. 6 max. 11.

TASK C

1.Decrypt the lab4wep. cap file and perform a detailed traffic analysis.

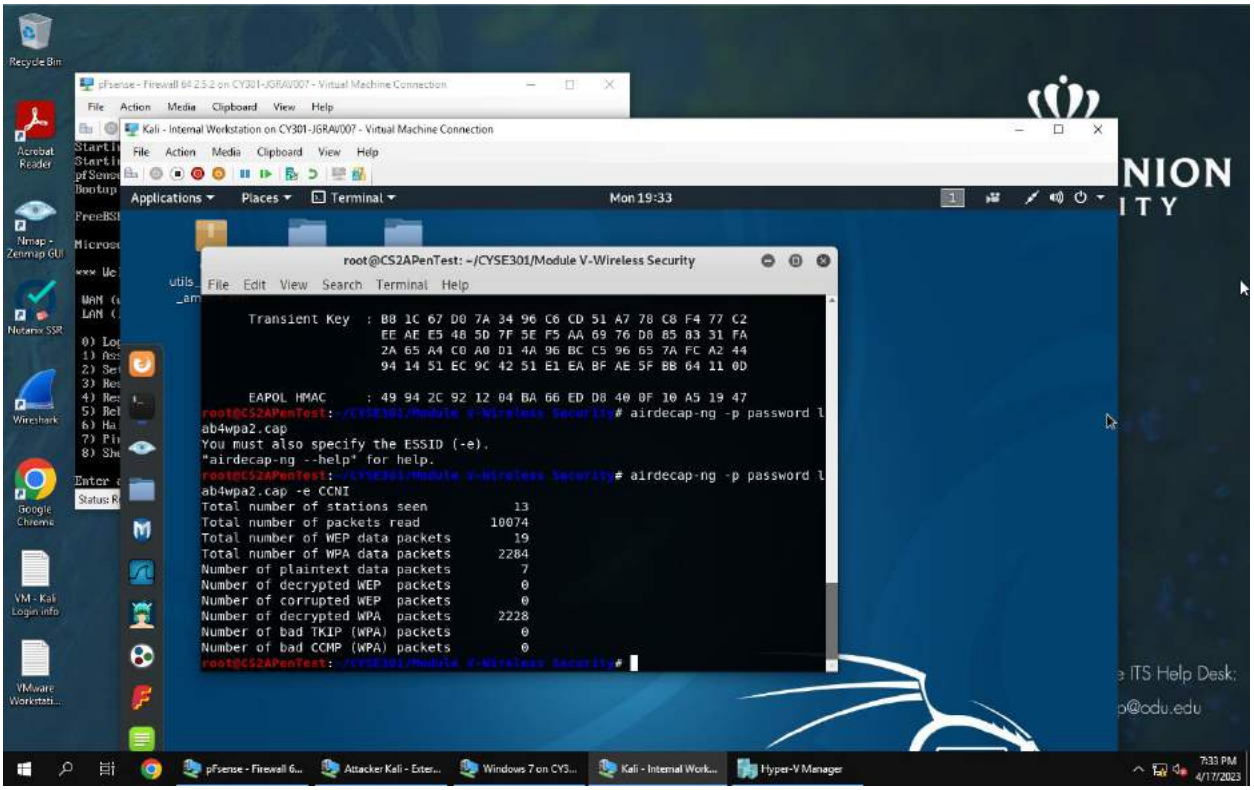


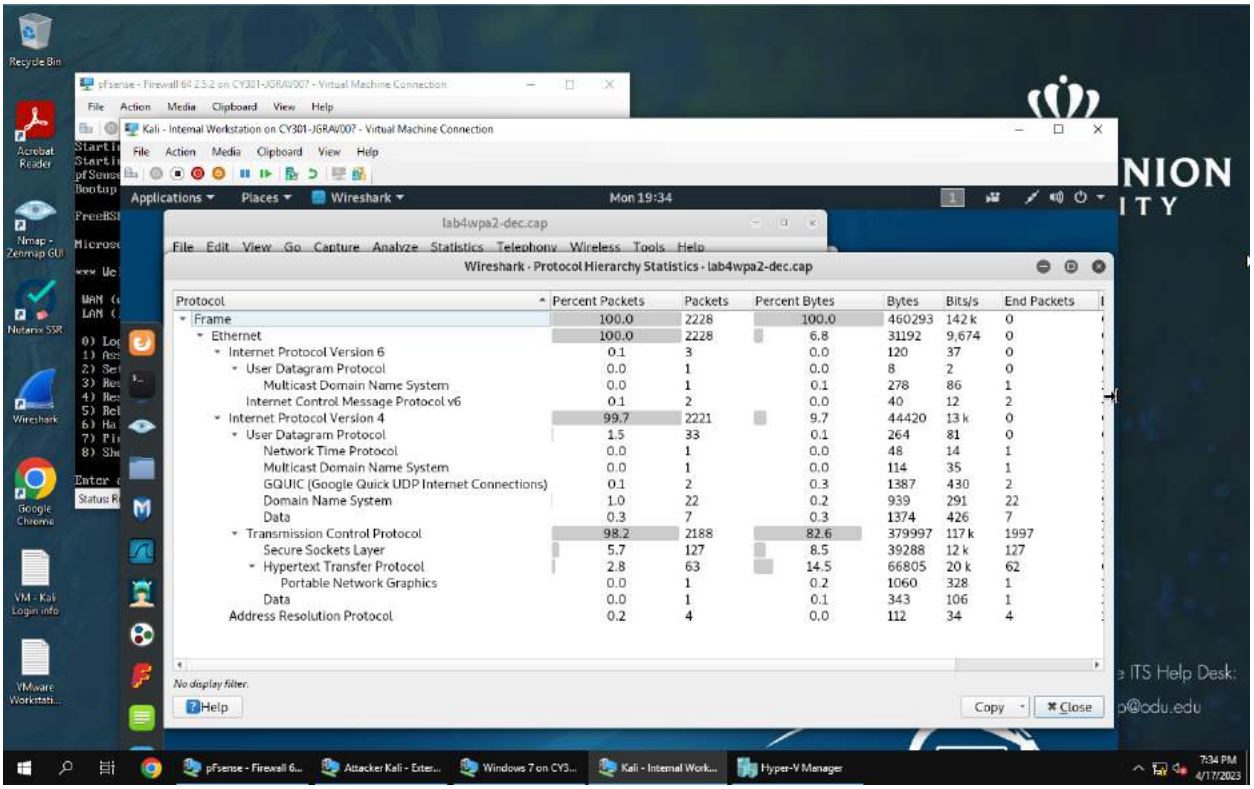
This is command “cd ~/CYSE301/Module\ V-Wireless\ Security/”



Finding the frame in Wireshark.

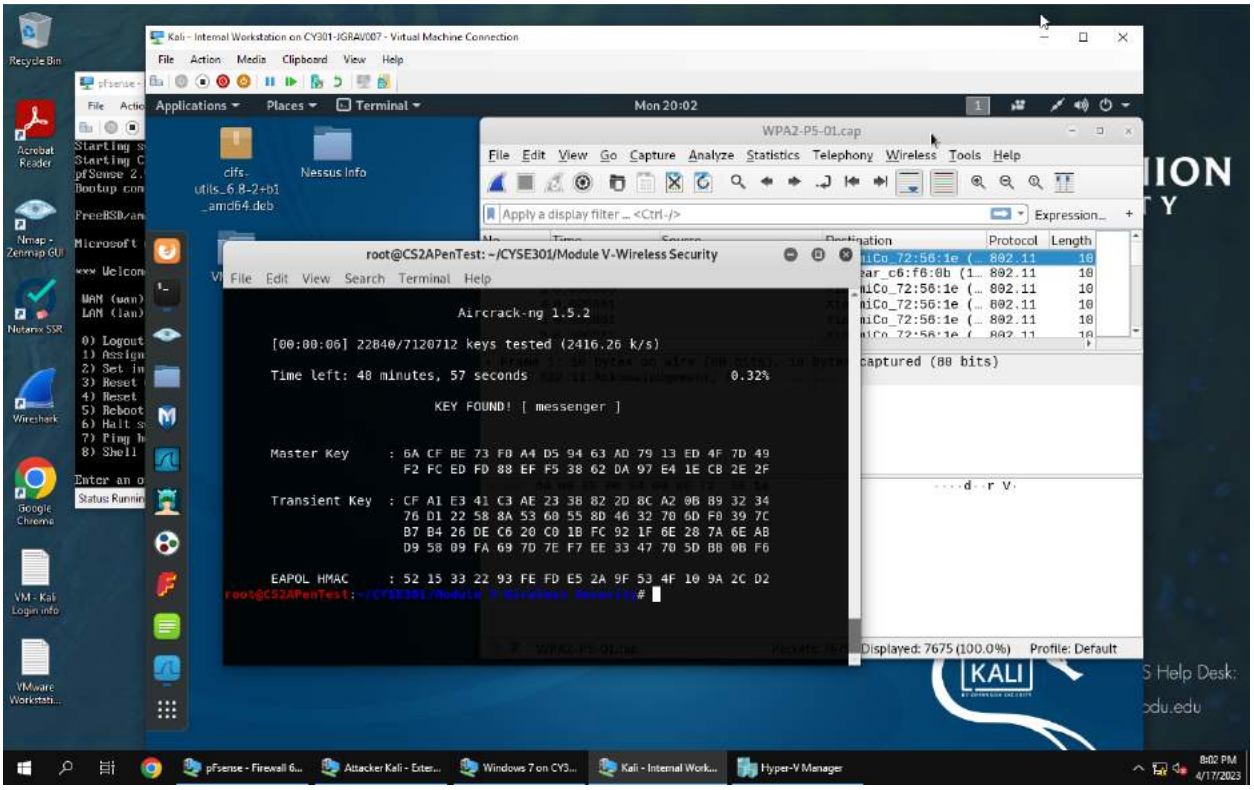
2. Decrypt the lab4wpa2. cap file and perform a detailed traffic analysis.


root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Transient Key : B8 1C 67 D0 7A 34 96 C6 CD 51 A7 78 C8 F4 77 C2
EE AE E5 4B 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA
2A 65 A4 C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44
94 14 51 EC 9C 42 51 E1 EA BF AE 5F BB 64 11 0D
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
root@CS2APenTest: /CYSE301/Module V-Wireless Security# airdecap-ng -p password l
ab4wpa2.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
root@CS2APenTest: /CYSE301/Module V-Wireless Security# airdecap-ng -p password l
ab4wpa2.cap -e CCNI
Total number of stations seen 13
Total number of packets read 10074
Total number of WEP data packets 19
Total number of WPA data packets 2284
Number of plaintext data packets 7
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 2228
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
root@CS2APenTest: /CYSE301/Module V-Wireless Security#

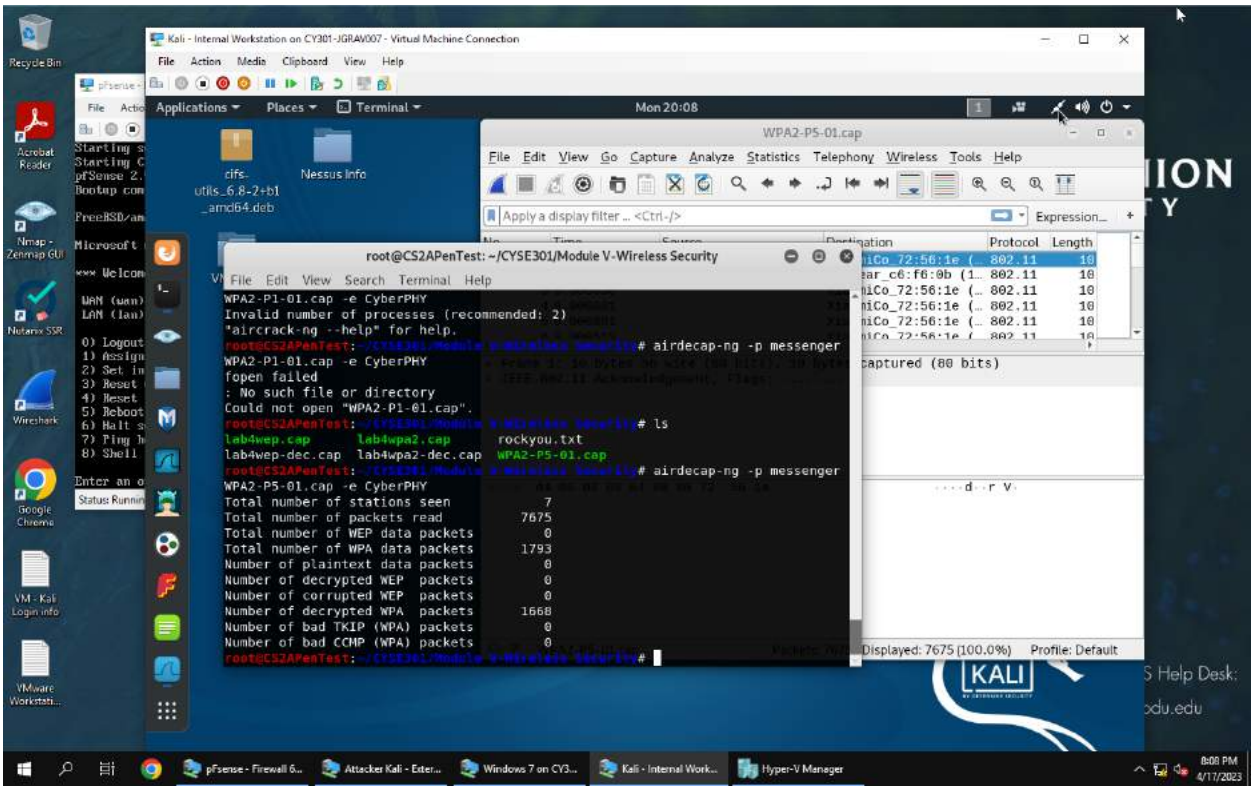

Wireshark · Protocol Hierarchy Statistics · lab4wpa2-dec.cap
Protocol | Percent Packets | Packets | Percent Bytes | Bytes | Bits/s | End Packets
Frame 100.0 2228 100.0 460293 142 k 0
Ethernet 100.0 2228 6.8 31192 9,674 0
Internet Protocol Version 6 0.1 3 0.0 120 37 0
User Datagram Protocol 0.0 1 0.0 8 2 0
Multicast Domain Name System 0.0 1 0.1 278 86 1
Internet Control Message Protocol v6 0.1 2 0.0 40 12 2
Internet Protocol Version 4 99.7 2221 9.7 44420 13 k 0
User Datagram Protocol 1.5 33 0.1 264 81 0
Network Time Protocol 0.0 1 0.0 48 14 1
Multicast Domain Name System 0.0 1 0.0 114 35 1
GQUIC (Google Quick UDP Internet Connections) 0.1 2 0.3 1387 430 2
Domain Name System 1.0 22 0.2 939 291 22
Data 0.3 7 0.3 1374 426 7
Transmission Control Protocol 98.2 2188 82.6 379997 117 k 1997
Secure Sockets Layer 5.7 127 8.5 39288 12 k 127
Hypertext Transfer Protocol 2.8 63 14.5 66805 20 k 62
Portable Network Graphics 0.0 1 0.2 1060 328 1
Data 0.0 1 0.1 343 106 1
Address Resolution Protocol 0.2 4 0.0 112 34 4
No display filter.
Help
Copy
Close

TASK D

1.Implement a dictionary attack and decrypt the traffic.



2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file.


Kali - Internal Workstation on CY301-JGRAV007 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 20:08
WPA2-P5-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Protocol Length
802.11 10
captured (80 bits)
Displayed: 7675 (100.0%) Profile: Default
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
WPA2-P1-01.cap -e CyberPHY
Invalid number of processes (recommended: 2)
"aircrack-ng --help" for help.
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p messenger
WPA2-P1-01.cap -e CyberPHY
fopen failed
: No such file or directory
Could not open "WPA2-P1-01.cap".
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# ls
lab4wep.cap lab4wpa2.cap rockyou.txt
lab4wep-dec.cap lab4wpa2-dec.cap WPA2-P5-01.cap
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p messenger
WPA2-P5-01.cap -e CyberPHY
Total number of stations seen 7
Total number of packets read 7675
Total number of WEP data packets 0
Total number of WPA data packets 1793
Number of plaintext data packets 0
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 1668
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
root@CS2APenTest:~/CYSE301/Module V-Wireless Security#
KALI
pfSense - Firewall 6...
Attacker Kali - Exter...
Windows 7 on CY3...
Kali - Internal Work...
Hyper-V Manager
8:08 PM
4/17/2023