OLD DOMINION UNIVERSITY

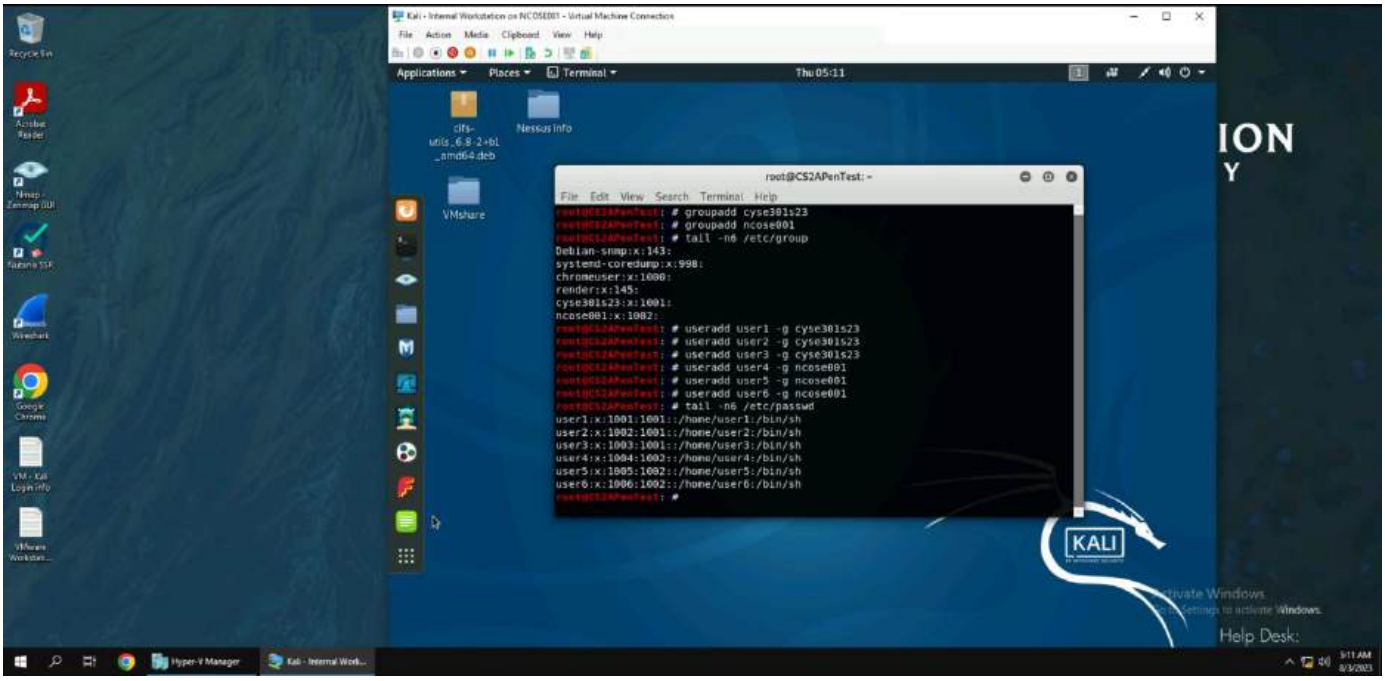
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Ethical Hacking

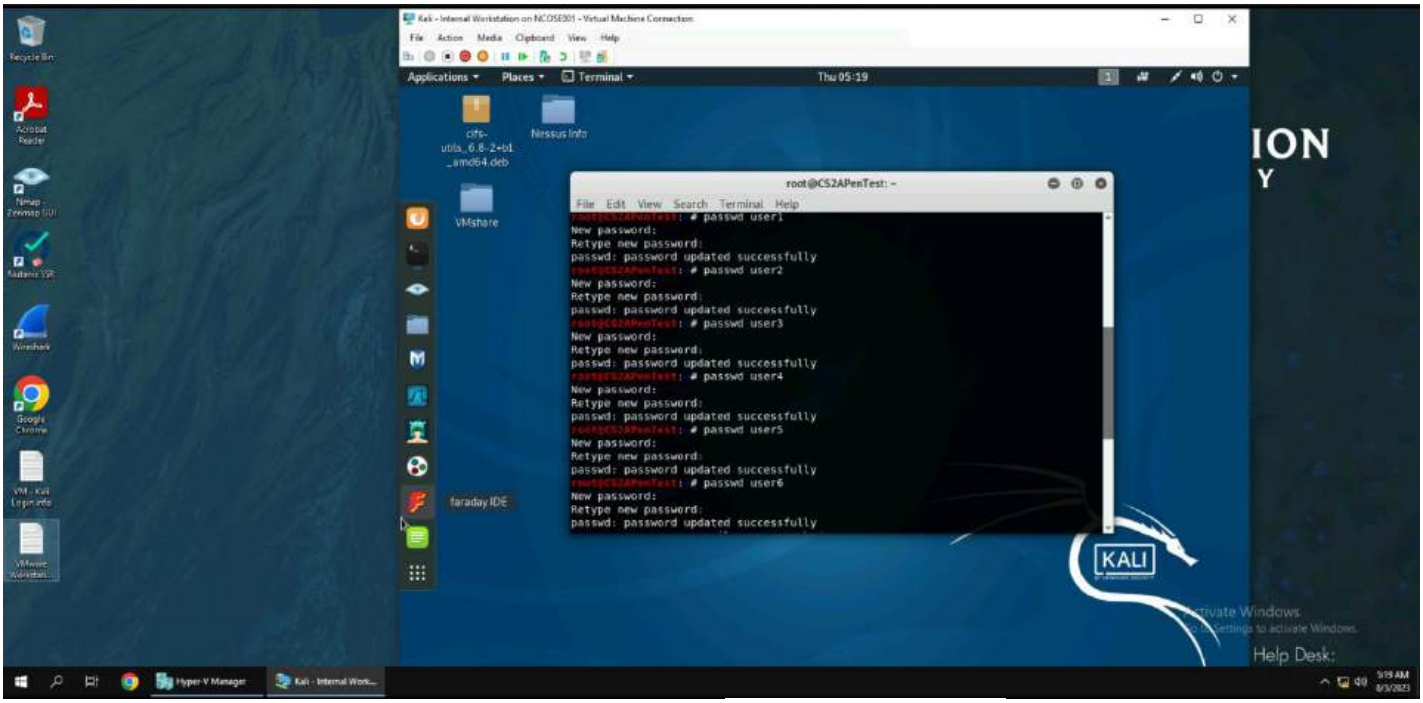
Nathan Cosendine

01243314

TASK A

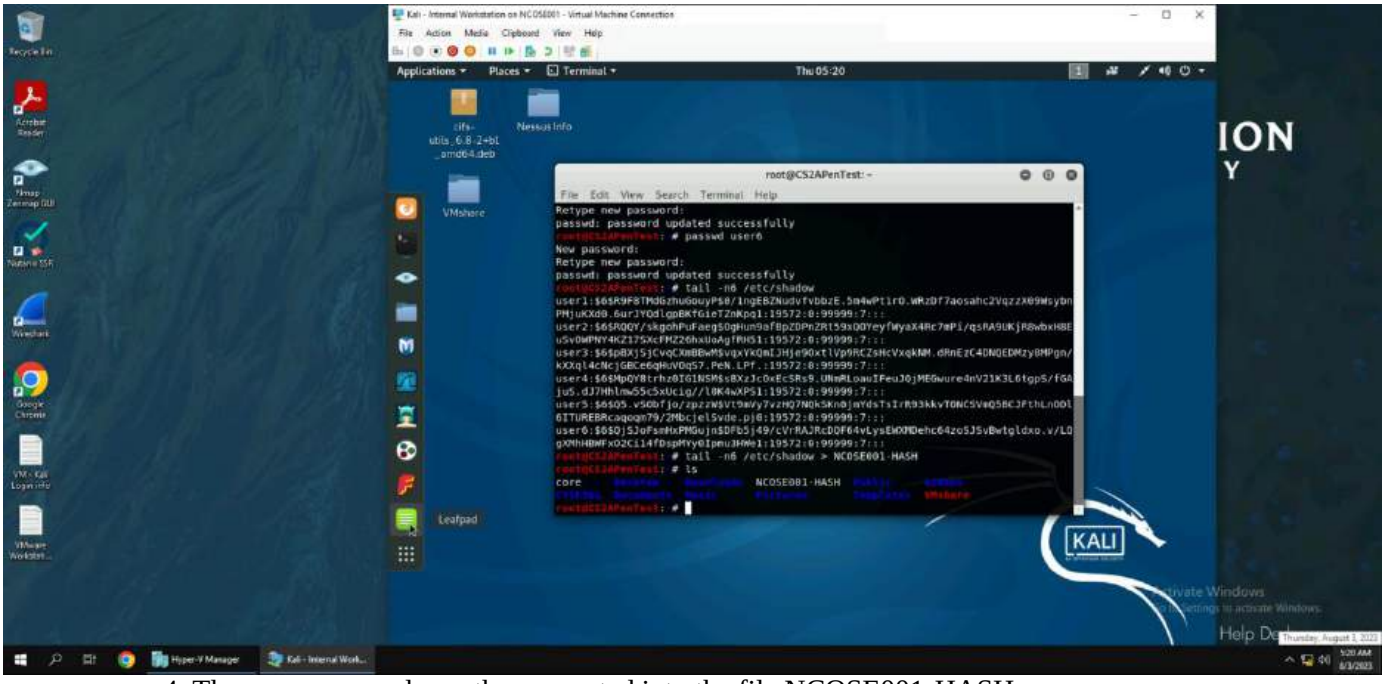


1-2. Above I create 2 groups, cyse301s23 and ncose001. I also create 6 users (user1-6), 3 being added to the cyse301s23 group and the other 3 being added to the ncose001 group.

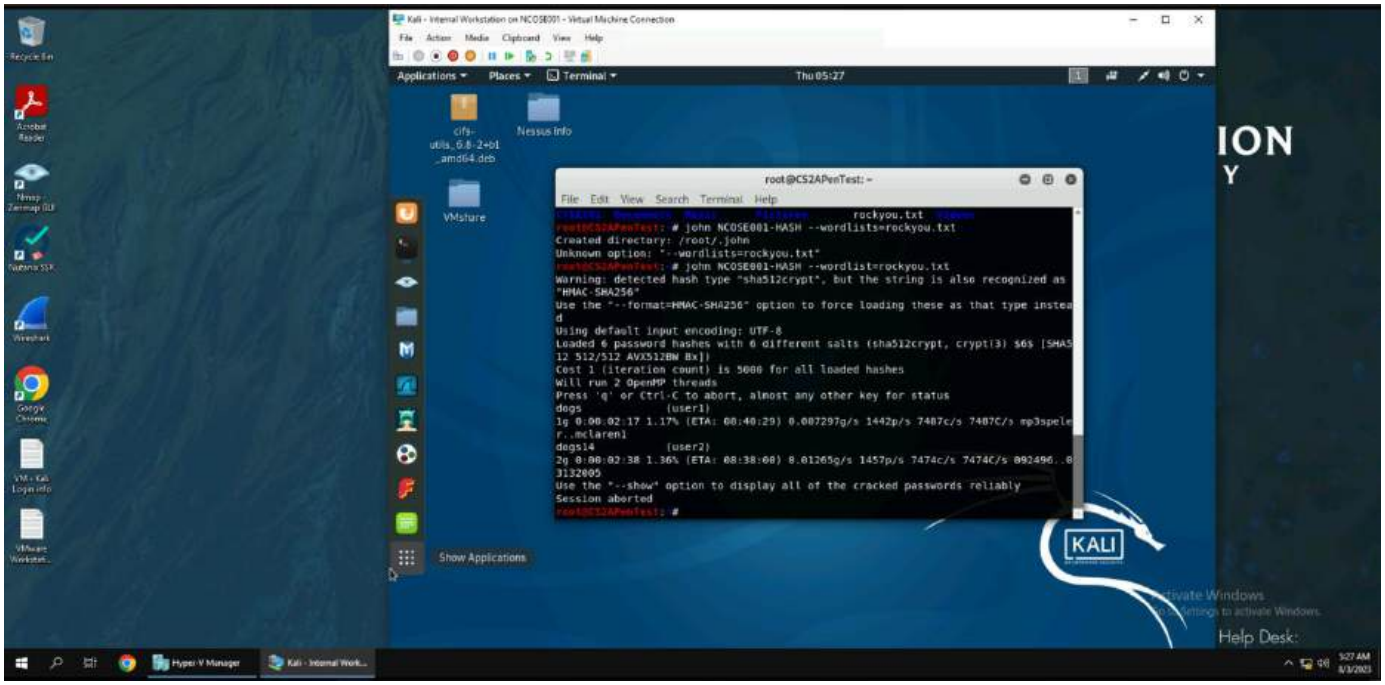


3. Passwords are then created for each user.

user1: dogs
user2: dogs14
user3: dogs50!
user4: Dogs50!
user5: D0g5!4
user6: !rldyk06%

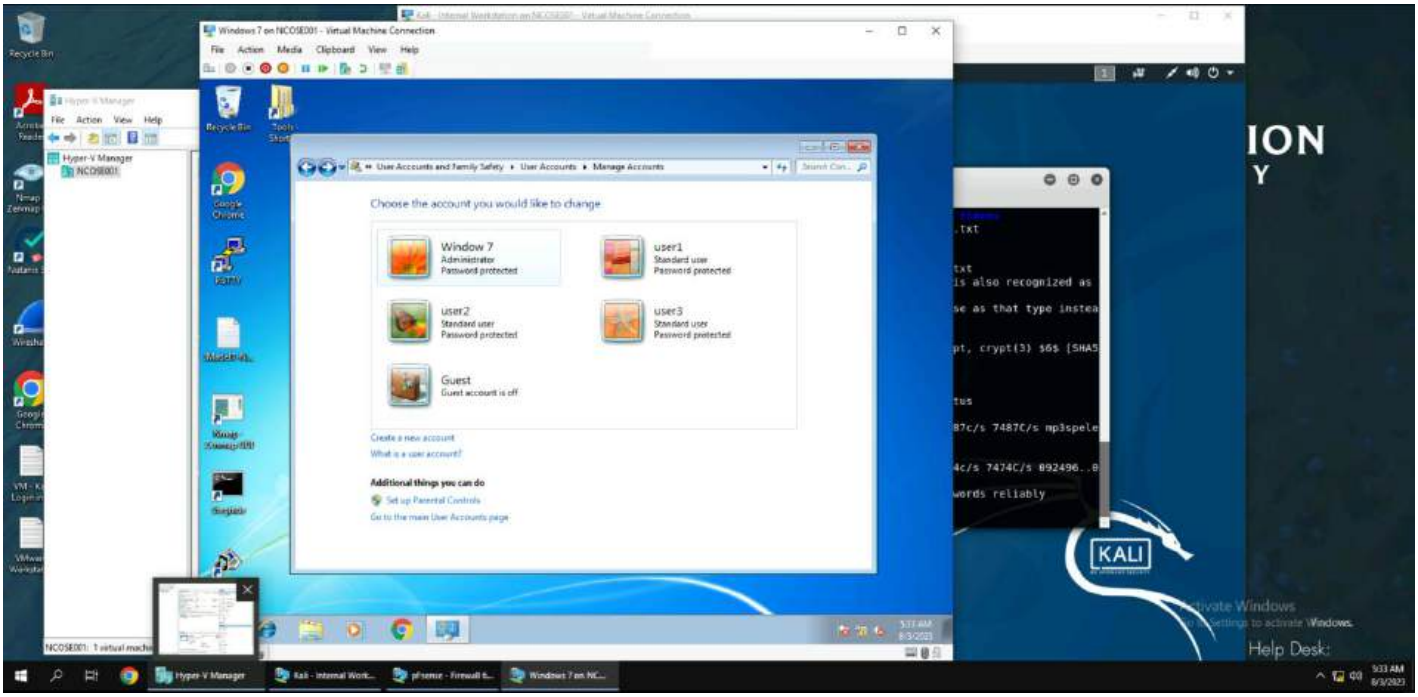


4. The user passwords are then exported into the file NCOSE001-HASH.

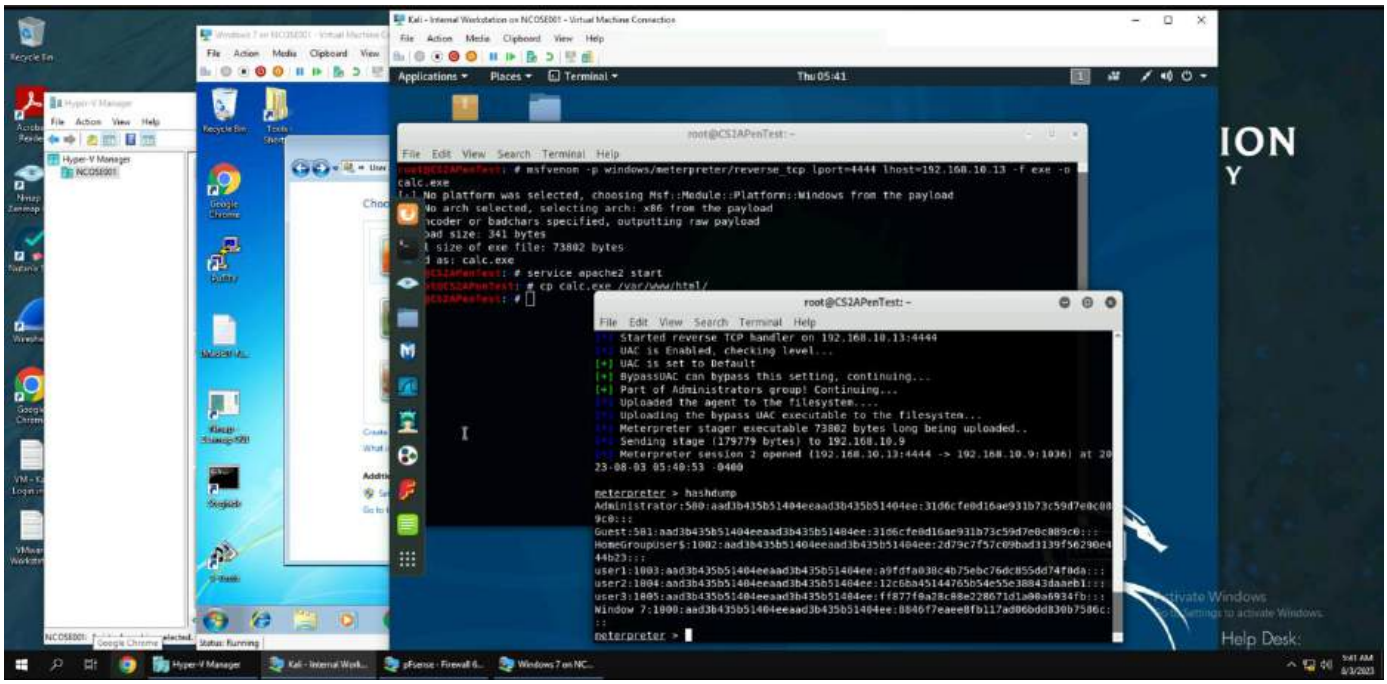


4b. The hashes are cracked with John the ripper using the rockyou.txt wordlist. The passwords dogs and dogs14 and shown.

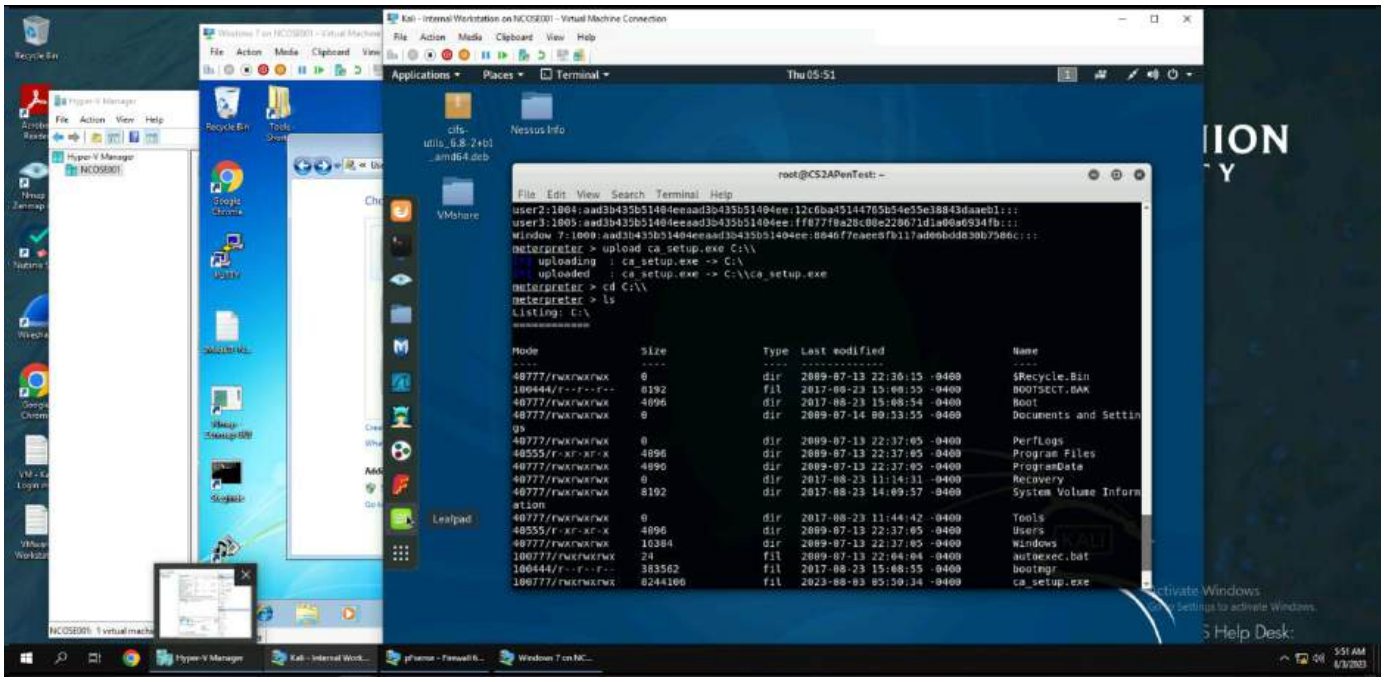
TASK B



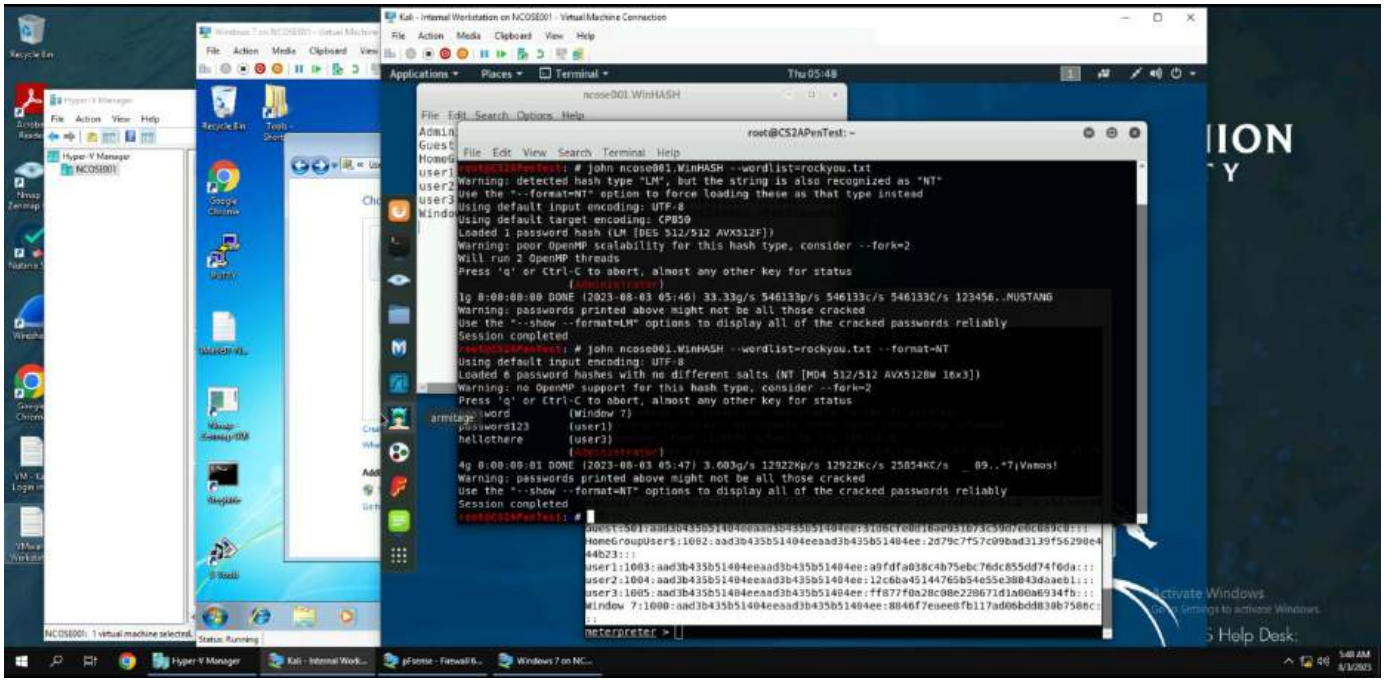
0. Three users are created on the Windows 7 system and given passwords.



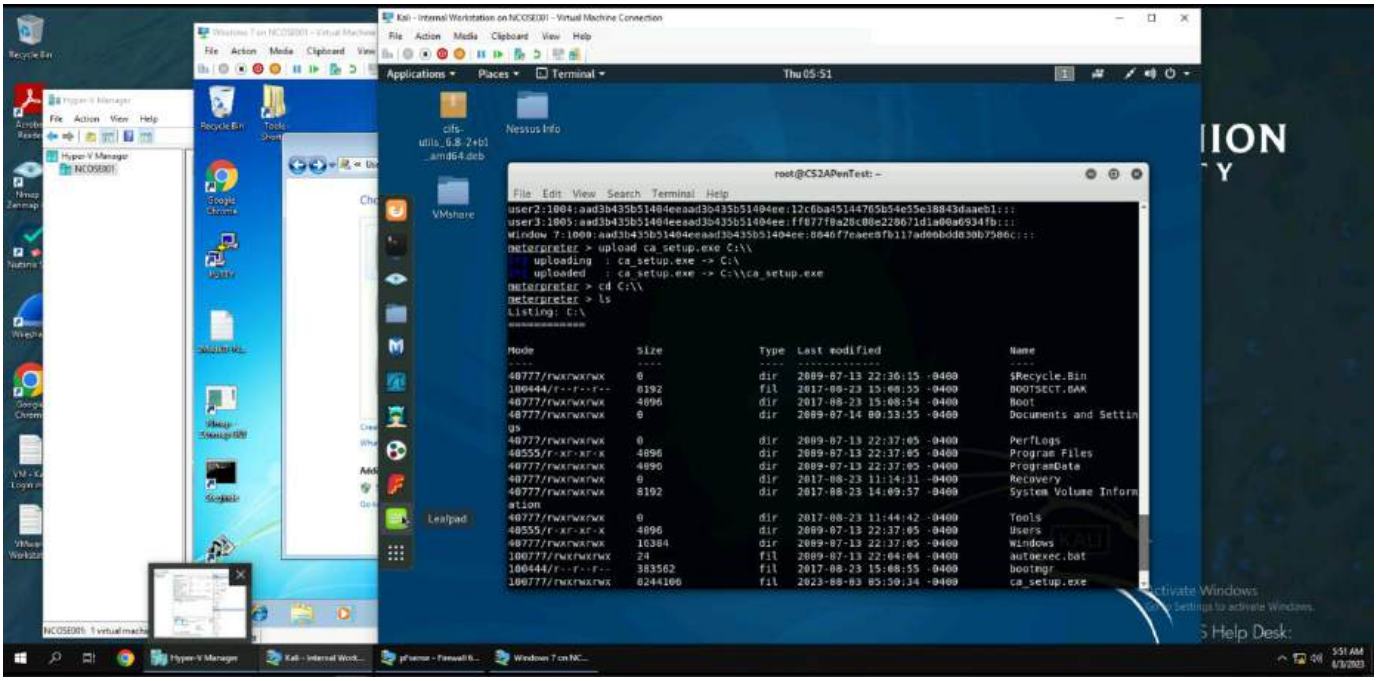
1. The password hashes are displayed using the hashdump command in meterpreter shell.



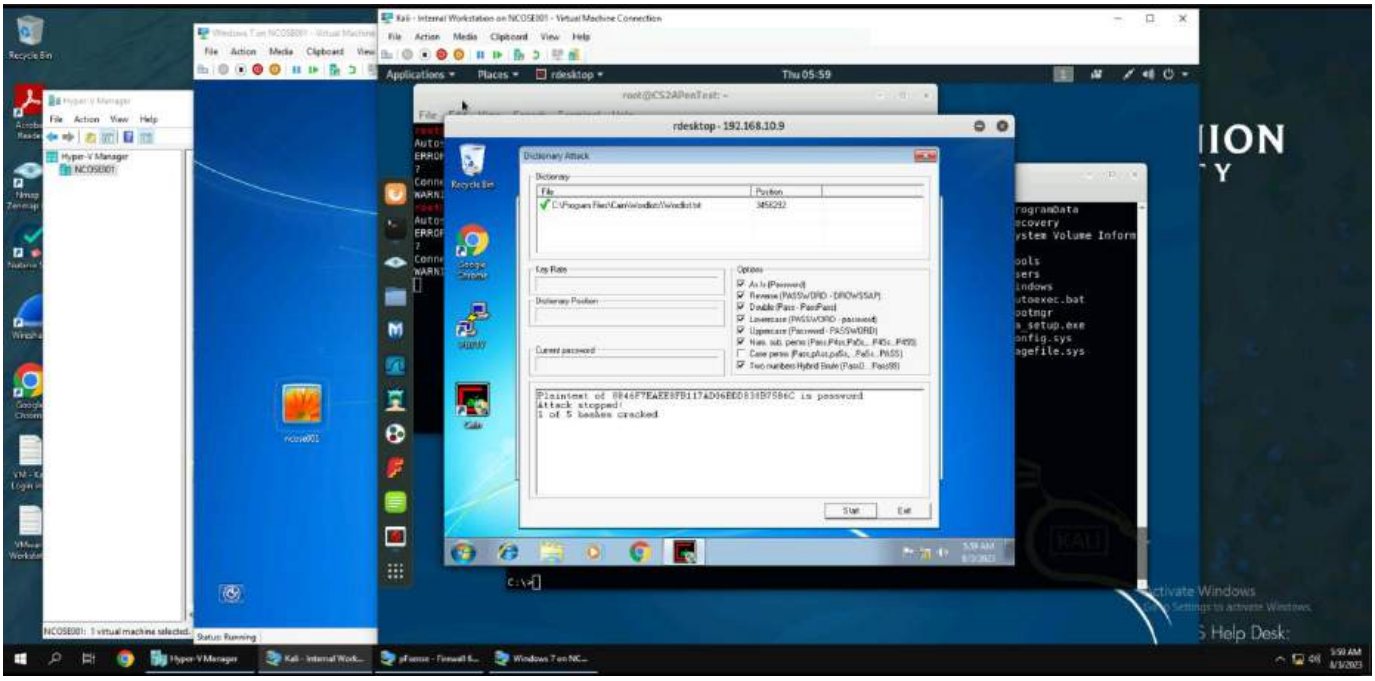
2. The password hashes are saved into the file ncose001.WinHASH.



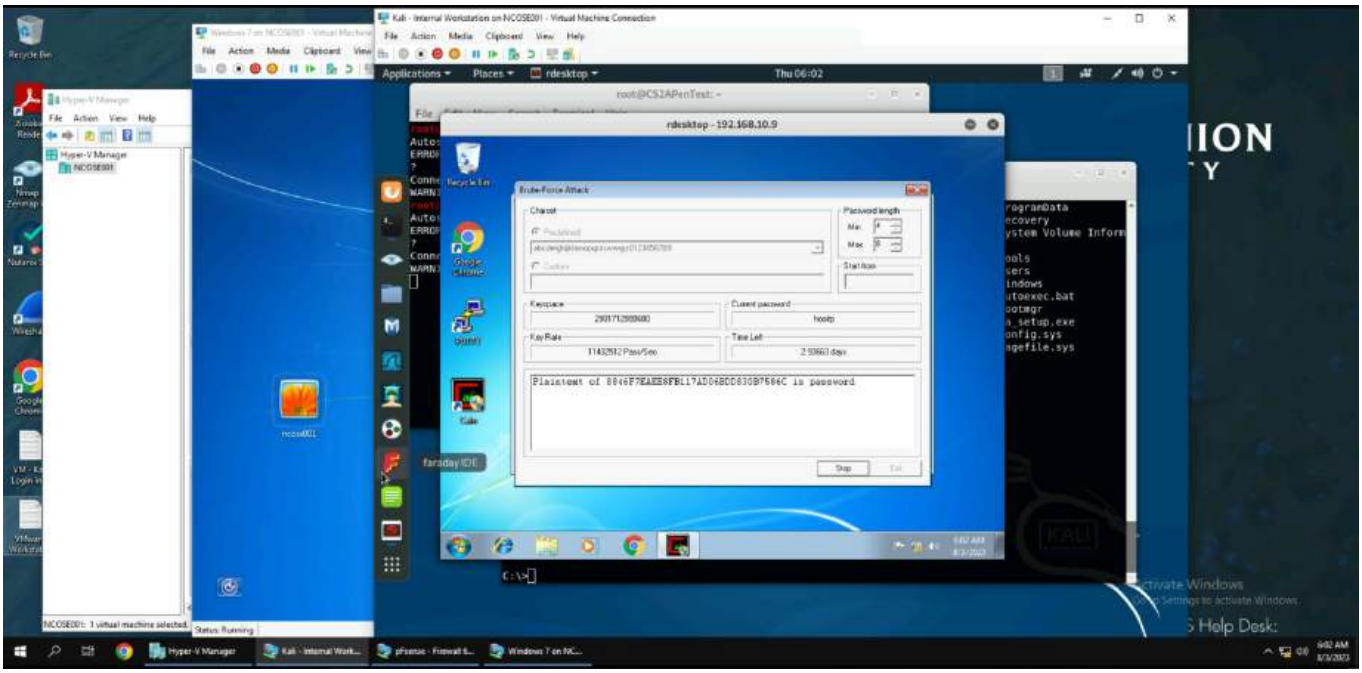
2b. The passwords are then cracked using john the ripper and the rockyou.txt wordlist. This shows the user passwords “password”, “password123”, and “hellothere”.



3. The password cracking tool Cain and Abel are uploaded to the remote Windows 7 VM.

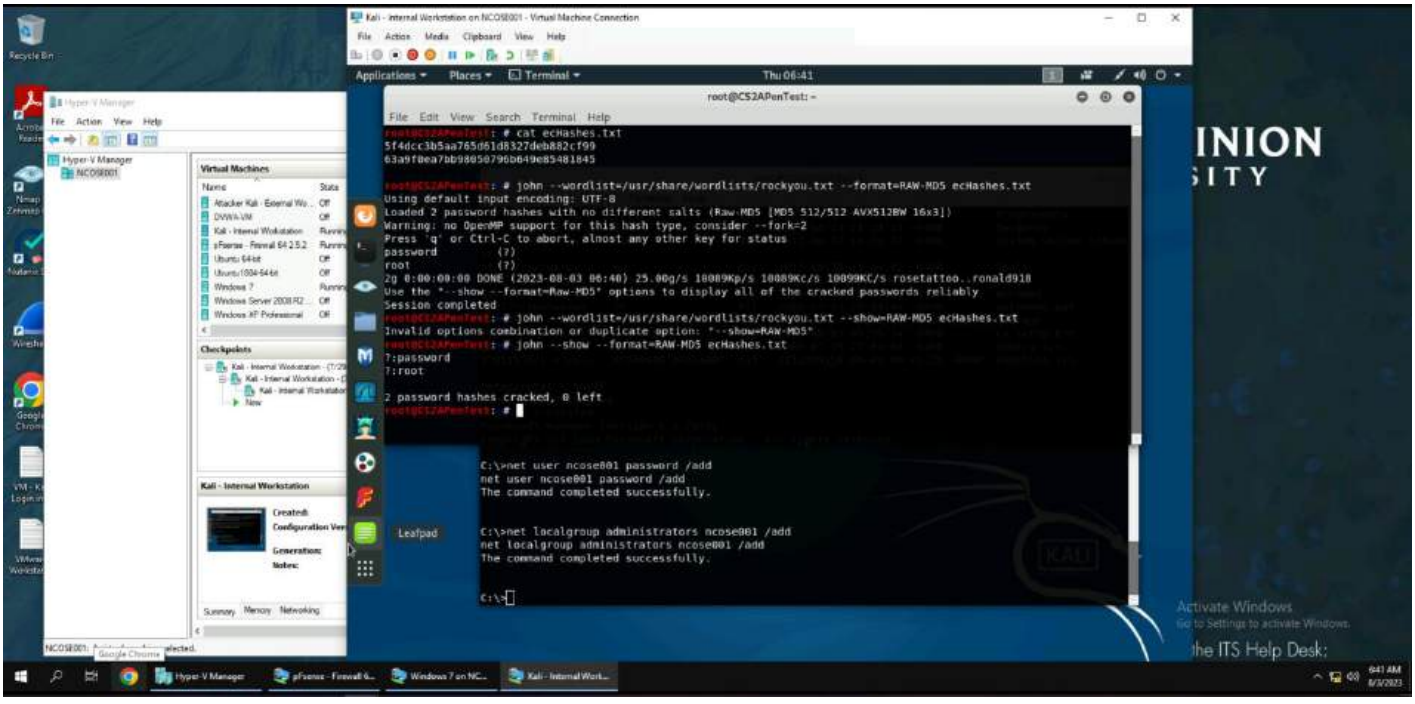


3b. A dictionary attack is ran and shows the plaintext “password”.



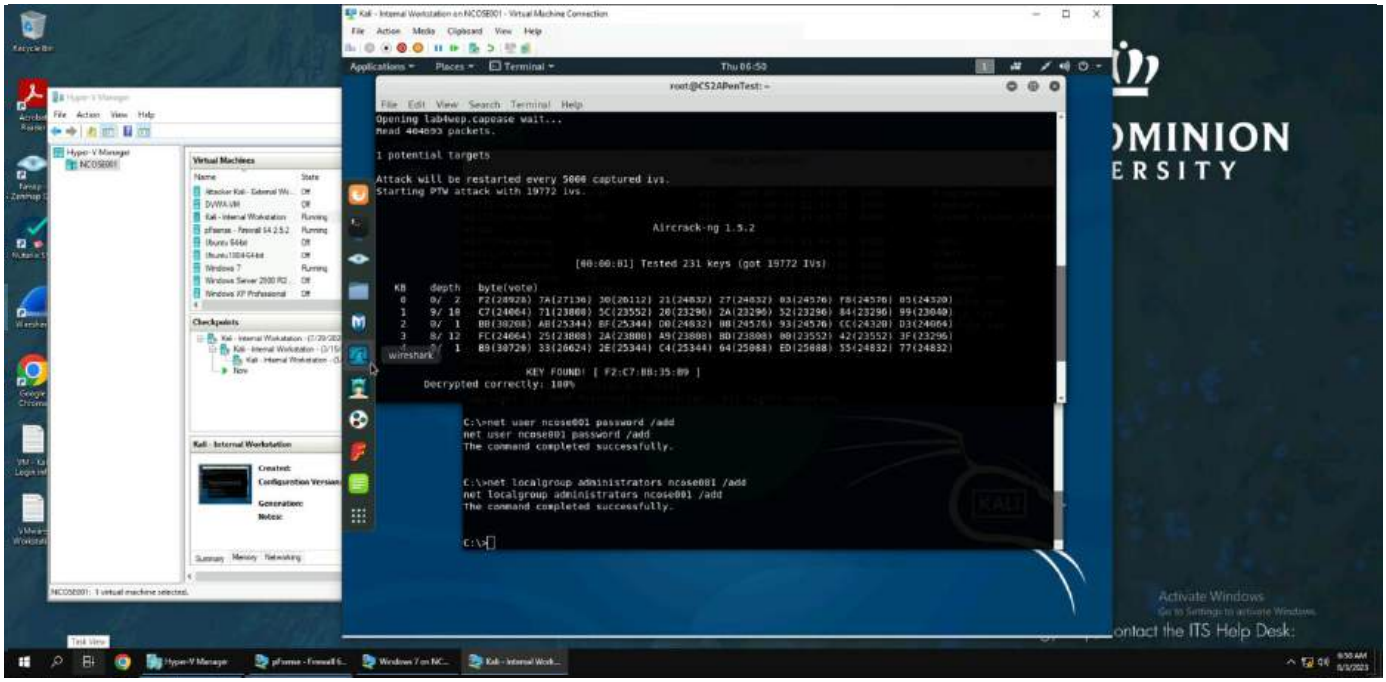
3c. A bruteforce attack is ran and shows the plaintext “password”.

TASK C EXTRA CREDIT

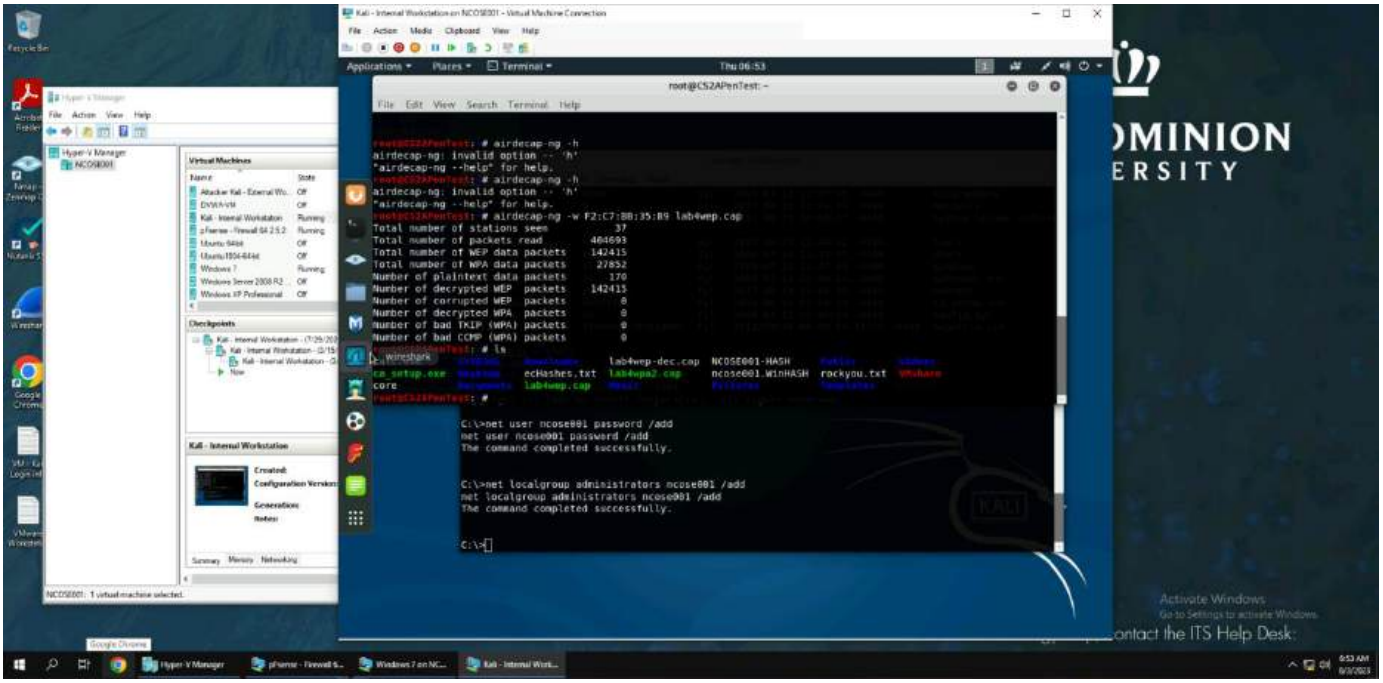


To crack the two hashes I first put them into a txt file named ecHashes.txt. John the ripper was then used on this txt file with the RawMD5 Format, showing the two hashes in plain text as password and root.

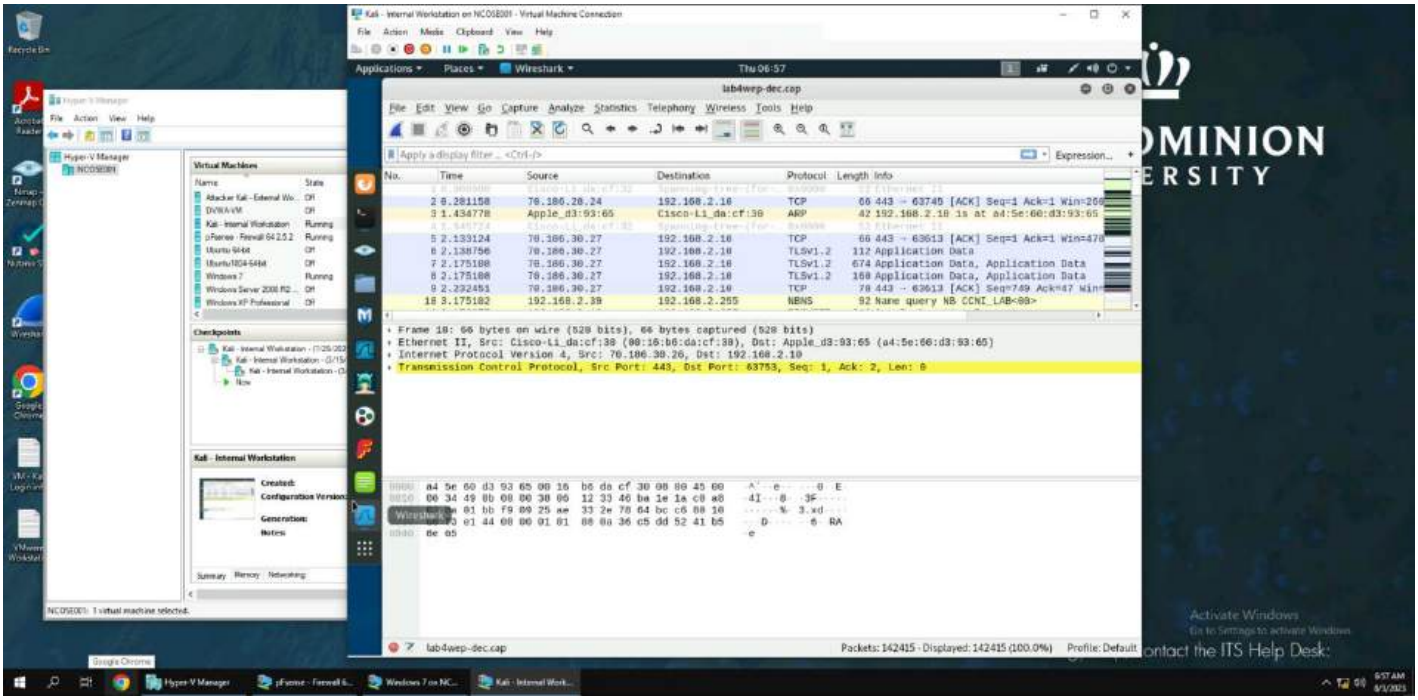
TASK C



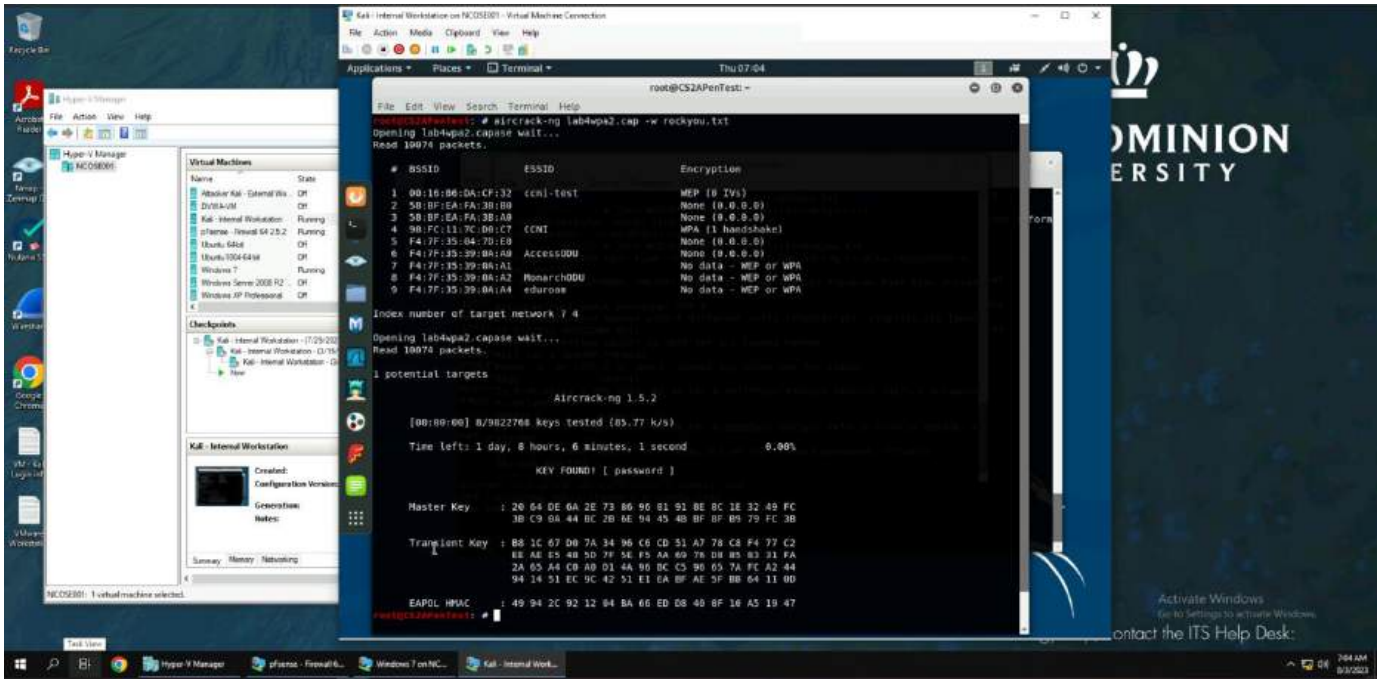
1. Using aircrack-ng, the key is found for lab4.wep



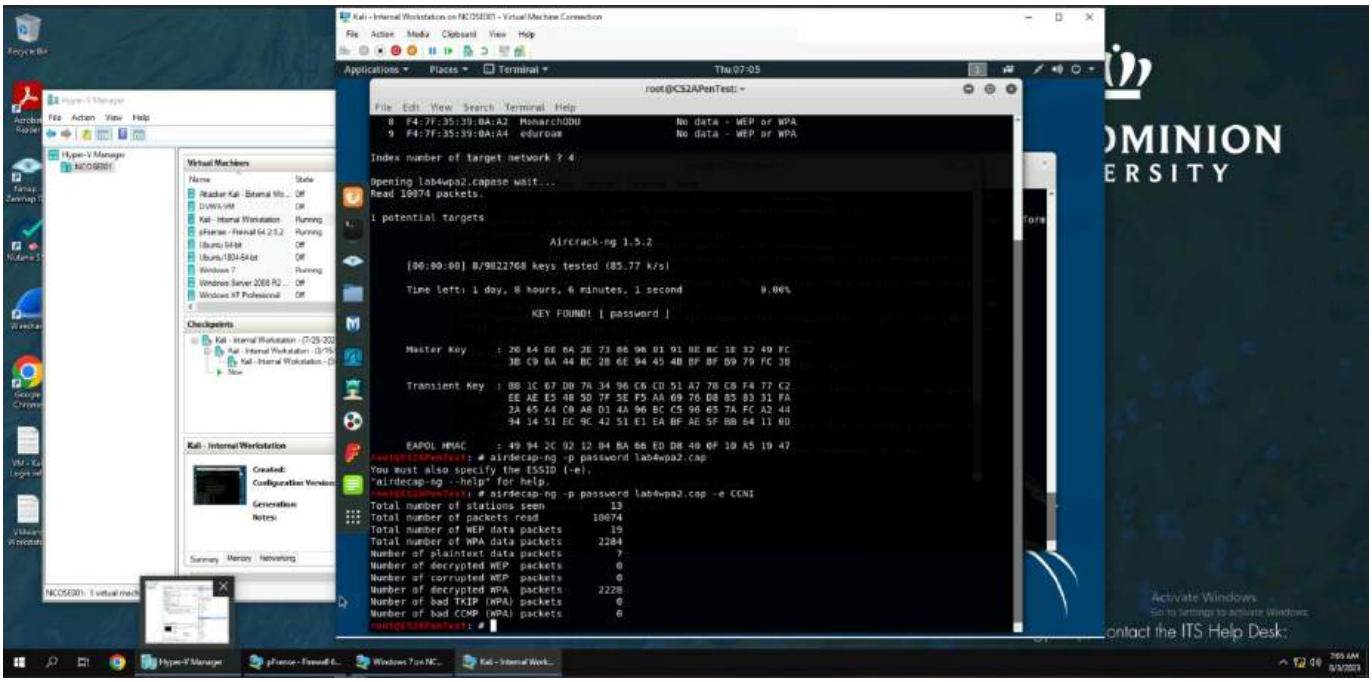
1b. The key is then used to decrypt the WEP packets.



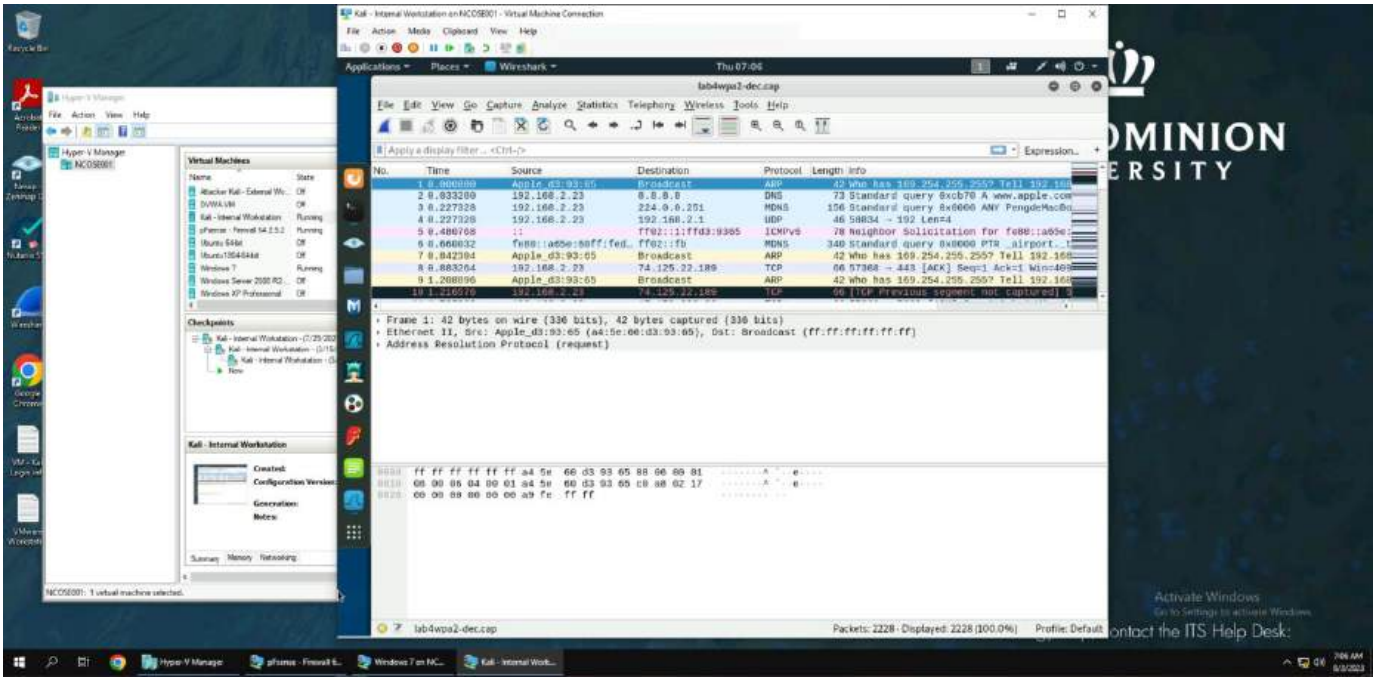
1c. lab4wep wireshark



2. Using aircrack-ng, the key “password” is found for lab4wpa2.

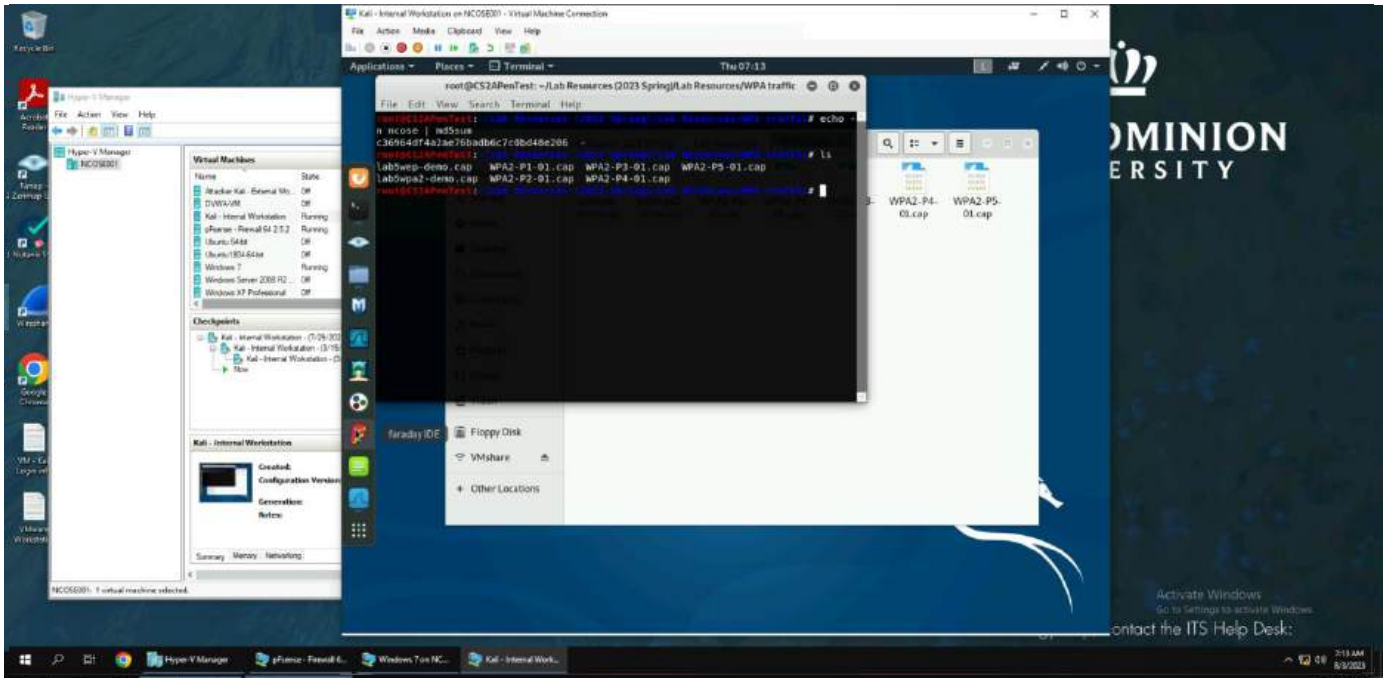


2b. The key is then used to decrypt the WPA packets.

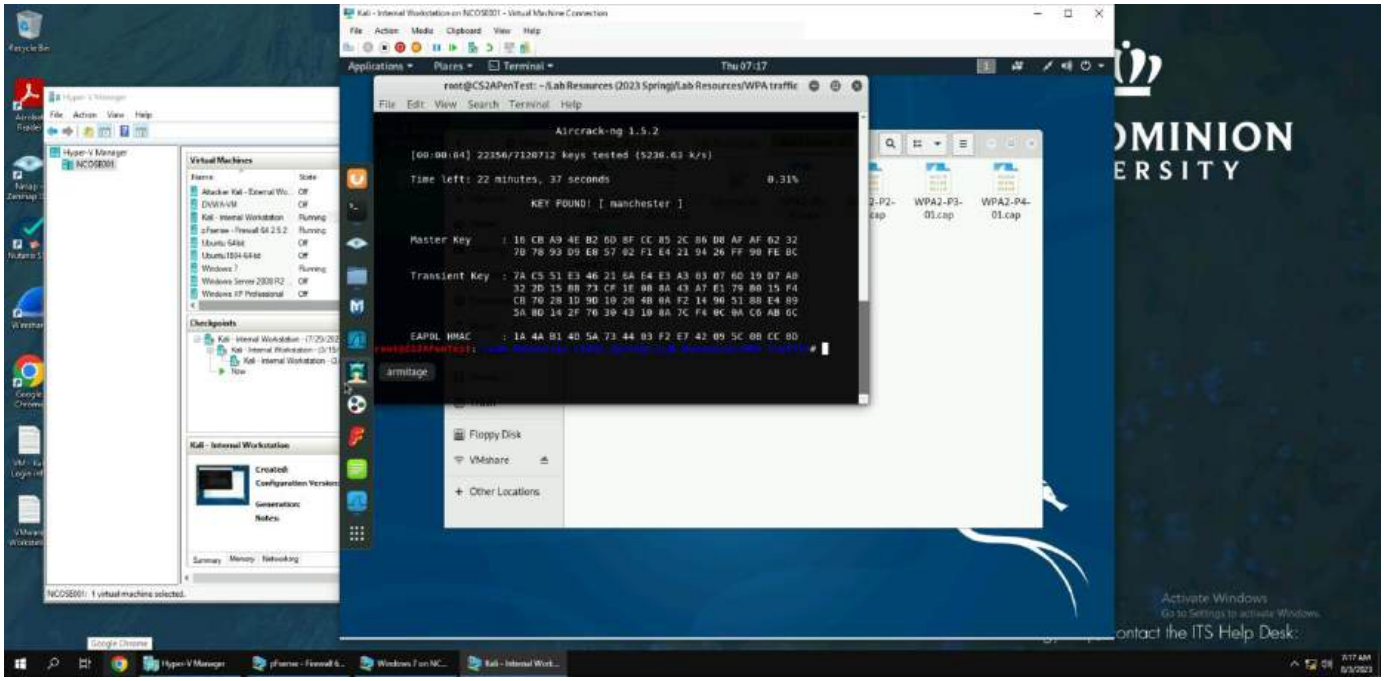


2c. lab4wpa2 wireshark

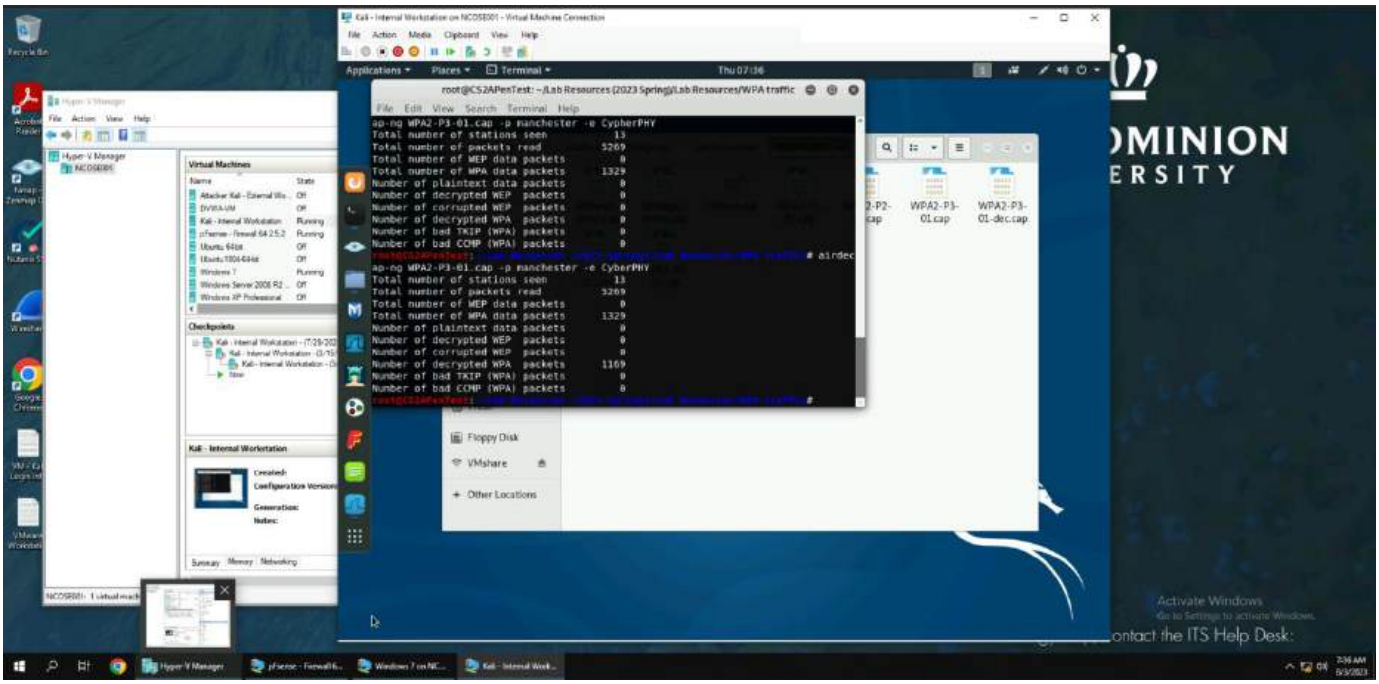
TASK D



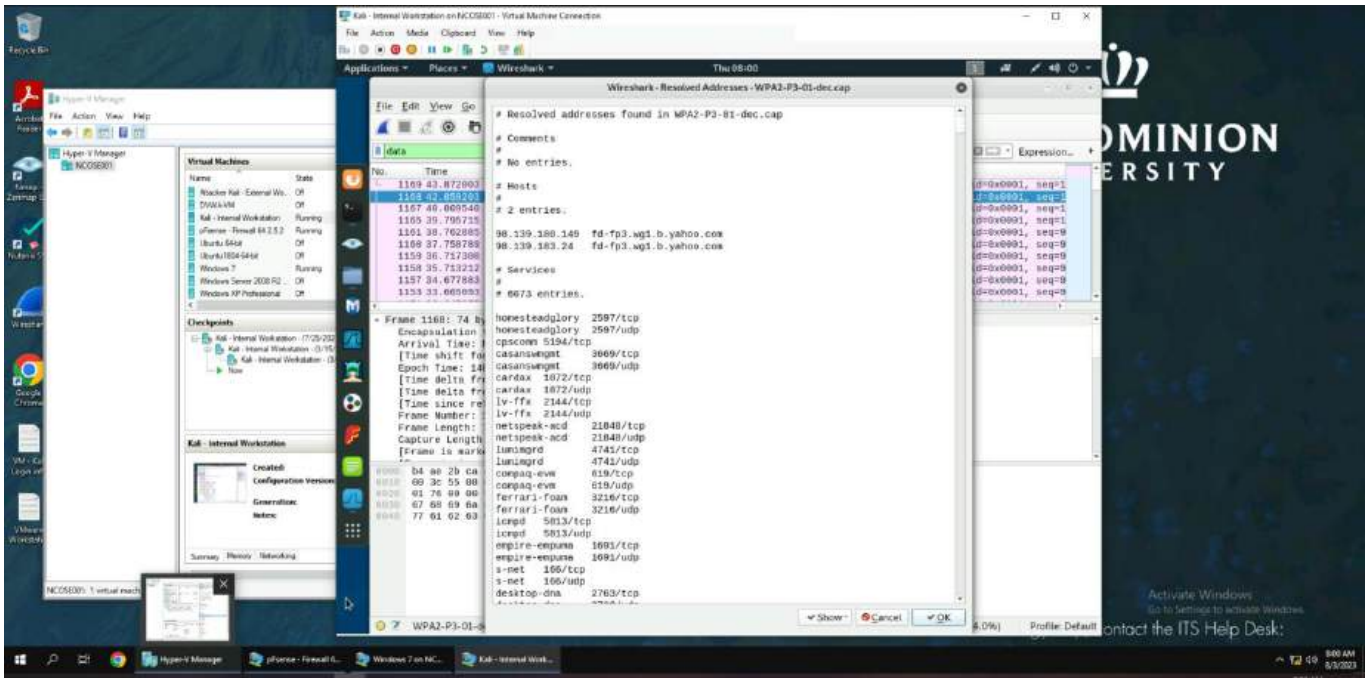
1. By using echo –n ncose001 | md5sum, I find that I am supposed to be using the file WPA2-P3-01.cap.

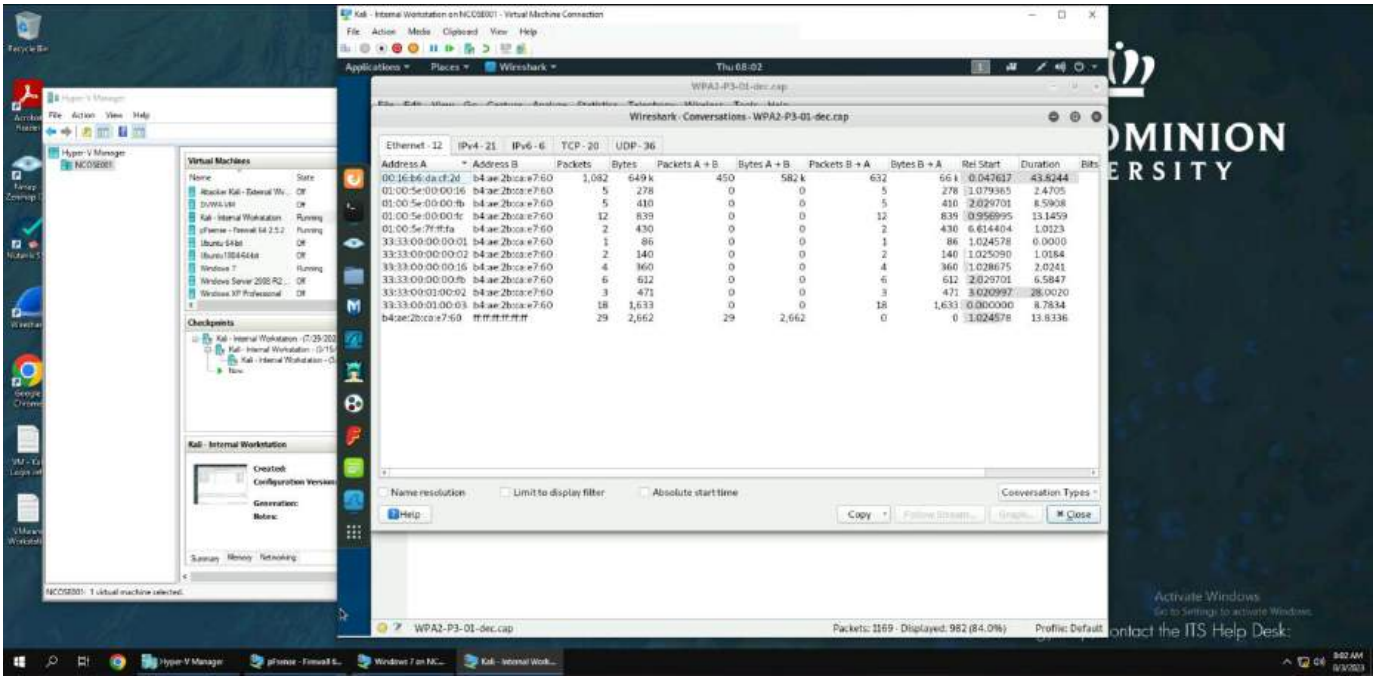


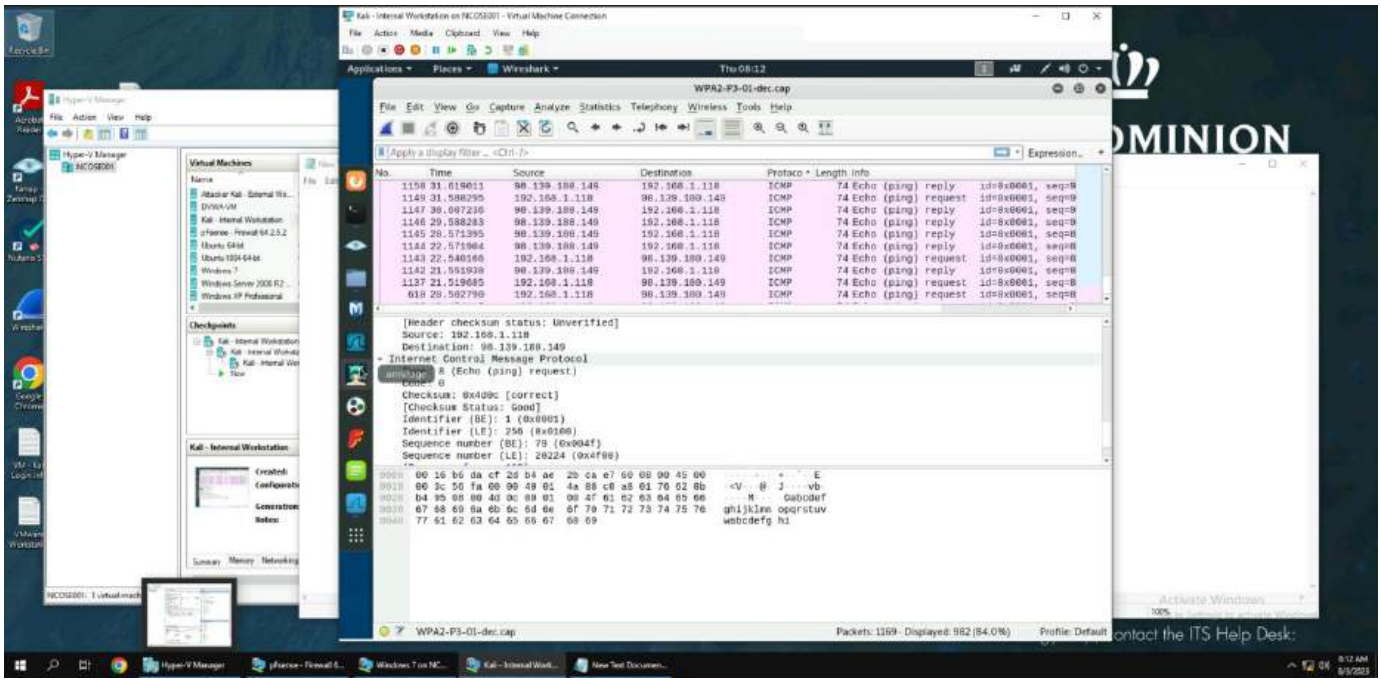
1b. Aircrack is used to find the key (manchester) for file.

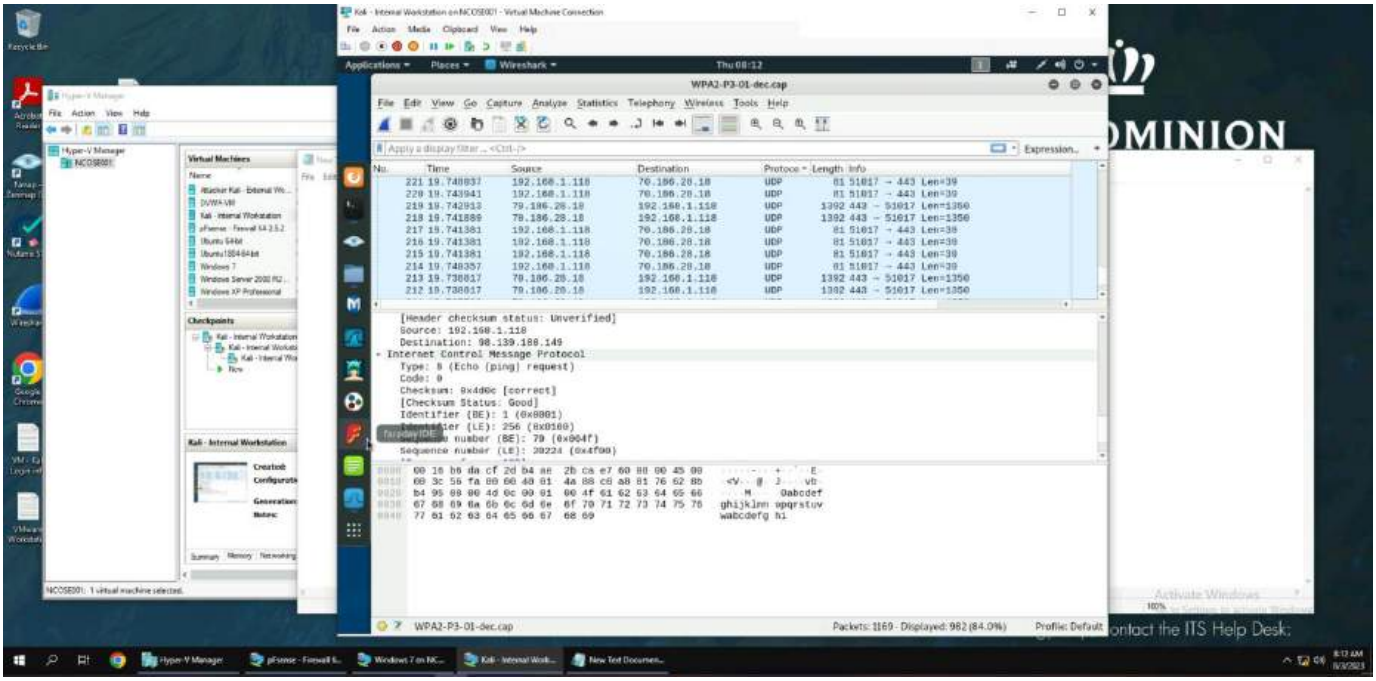


1c. Using airdecap, the key (Manchester) and ESSID (CyberPHY) are used to decrypt the WPA packets.




Wireshark · Conversations · WPA2-P3-01-dec.cap
Ethernet · 12
IPv4 · 21
IPv6 · 6
TCP · 20
UDP · 36
Address A
Address B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
00:16:b6:da:cf:2d b4:ae:2b:ca:e7:60 1,082 649 k 450 582 k 632 66 k 0.047617 43.8244
01:00:5e:00:00:16 b4:ae:2b:ca:e7:60 5 278 0 0 5 278 1.079365 2.4705
01:00:5e:00:00:fb b4:ae:2b:ca:e7:60 5 410 0 0 5 410 2.029701 8.5908
01:00:5e:00:00:fc b4:ae:2b:ca:e7:60 12 839 0 0 12 839 0.956995 13.1459
01:00:5e:7f:ff:fa b4:ae:2b:ca:e7:60 2 430 0 0 2 430 6.614404 1.0123
33:33:00:00:00:01 b4:ae:2b:ca:e7:60 1 86 0 0 1 86 1.024578 0.0000
33:33:00:00:00:02 b4:ae:2b:ca:e7:60 2 140 0 0 2 140 1.025090 1.0184
33:33:00:00:00:16 b4:ae:2b:ca:e7:60 4 360 0 0 4 360 1.028675 2.0241
33:33:00:00:00:fb b4:ae:2b:ca:e7:60 6 612 0 0 6 612 2.029701 6.5847
33:33:00:01:00:02 b4:ae:2b:ca:e7:60 3 471 0 0 3 471 3.020997 28.0020
33:33:00:01:00:03 b4:ae:2b:ca:e7:60 18 1,633 0 0 18 1,633 0.000000 8.7834
b4:ae:2b:ca:e7:60 ff:ff:ff:ff:ff:ff 29 2,662 29 2,662 0 0 1.024578 13.8336
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Help
Copy
Close
WPA2-P3-01-dec.cap
Packets: 1169 · Displayed: 982 (84.0%)
Profile: Default


WPA2-P3-01-dec.cap
No. Time Source Destination Protoco Length Info
1158 31.618011 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=9
1149 31.588295 192.168.1.118 98.139.188.149 ICMP 74 Echo (ping) request id=0x0001, seq=9
1147 30.087236 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=9
1146 29.588283 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=9
1145 29.571395 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=8
1144 22.571004 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=8
1143 22.540166 192.168.1.118 98.139.188.149 ICMP 74 Echo (ping) request id=0x0001, seq=8
1142 21.551938 98.139.188.149 192.168.1.118 ICMP 74 Echo (ping) reply id=0x0001, seq=8
1137 21.519685 192.168.1.118 98.139.188.149 ICMP 74 Echo (ping) request id=0x0001, seq=8
618 29.582790 192.168.1.118 98.139.188.149 ICMP 74 Echo (ping) request id=0x0001, seq=8
[Header checksum status: Unverified]
Source: 192.168.1.118
Destination: 98.139.188.149
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d0c [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence number (BE): 79 (0x004f)
Sequence number (LE): 20224 (0x4f00)
0000 00 16 b6 da cf 2d b4 ae 2b ca e7 60 08 00 45 00
0010 00 3c 50 fa 00 00 40 01 4a 88 c0 a8 01 76 62 8b
0020 b4 95 08 00 4d 0c 00 01 00 4f 61 62 63 64 65 66
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040 77 61 62 63 64 65 66 67 68 69
WPA2-P3-01-dec.cap
Packets: 1169 · Displayed: 982 (84.0%)
Profile: Default



Here are my findings from using Wireshark to see the decrypted WPA packets. Resolved Addresses shows 2 hosts, 98.139.180.149 and 98.139.183.24, as well as 6073 service entries. There were a lot of UDP protocol packets with the source being 192.168.1.118 with source port 51017, and the destination being 70.186.28.18 with destination port 443. About half of the UDP packets were with these IPs but flipped, so the source was 70.186.28.18 with source port 443, and destination being 192.168.1.118 with destination port 51017. Wireshark also showed some reply and request packets between 98.139.180.149 and 192.168.1.118.