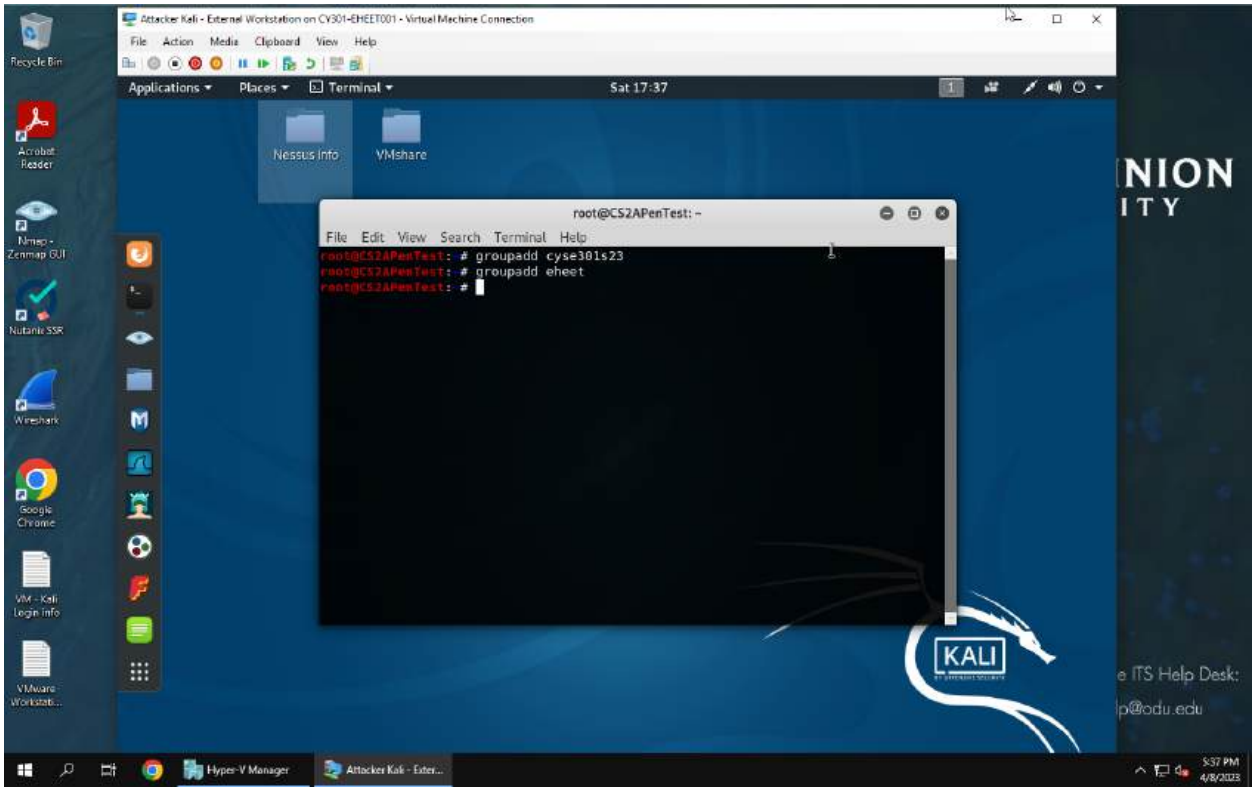
Old Dominion University
Cyse 301 Cybersecurity Techniques and Operations

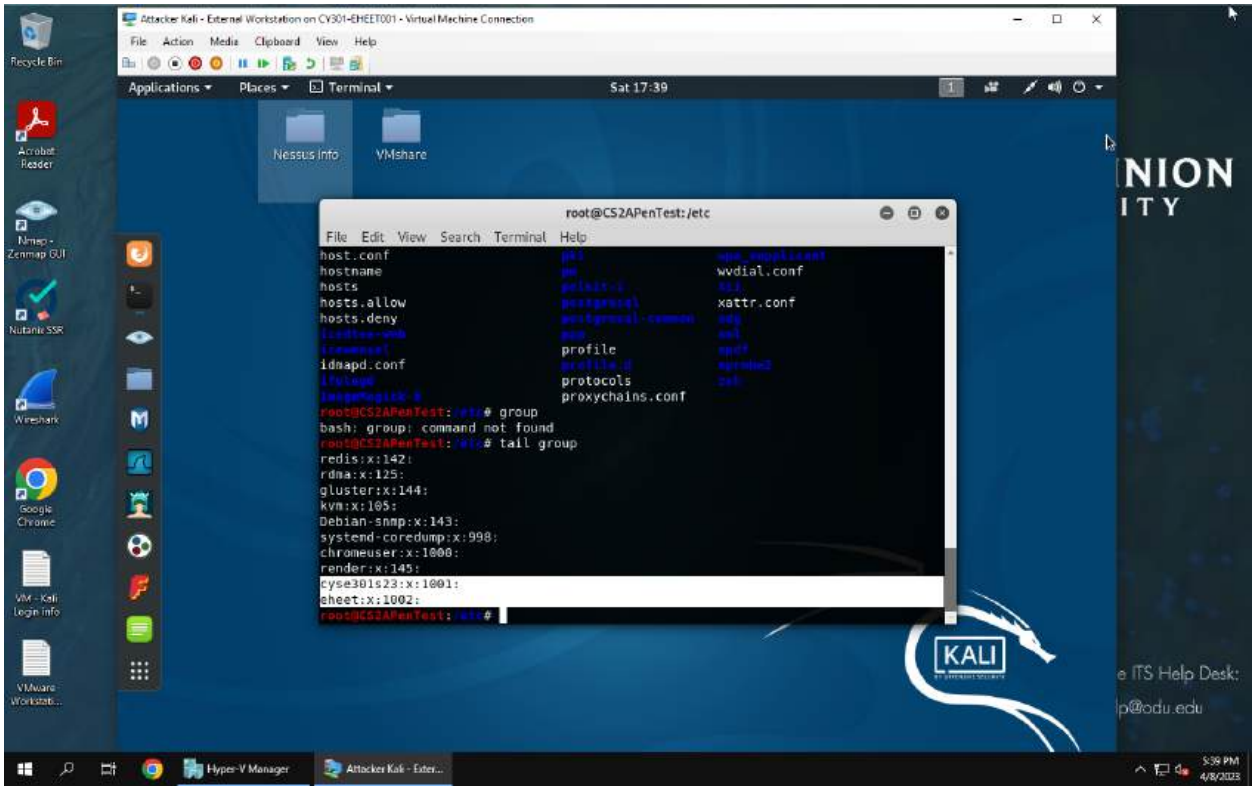
|| Password Cracking ||

Ethan Heeter
01198507

Part A

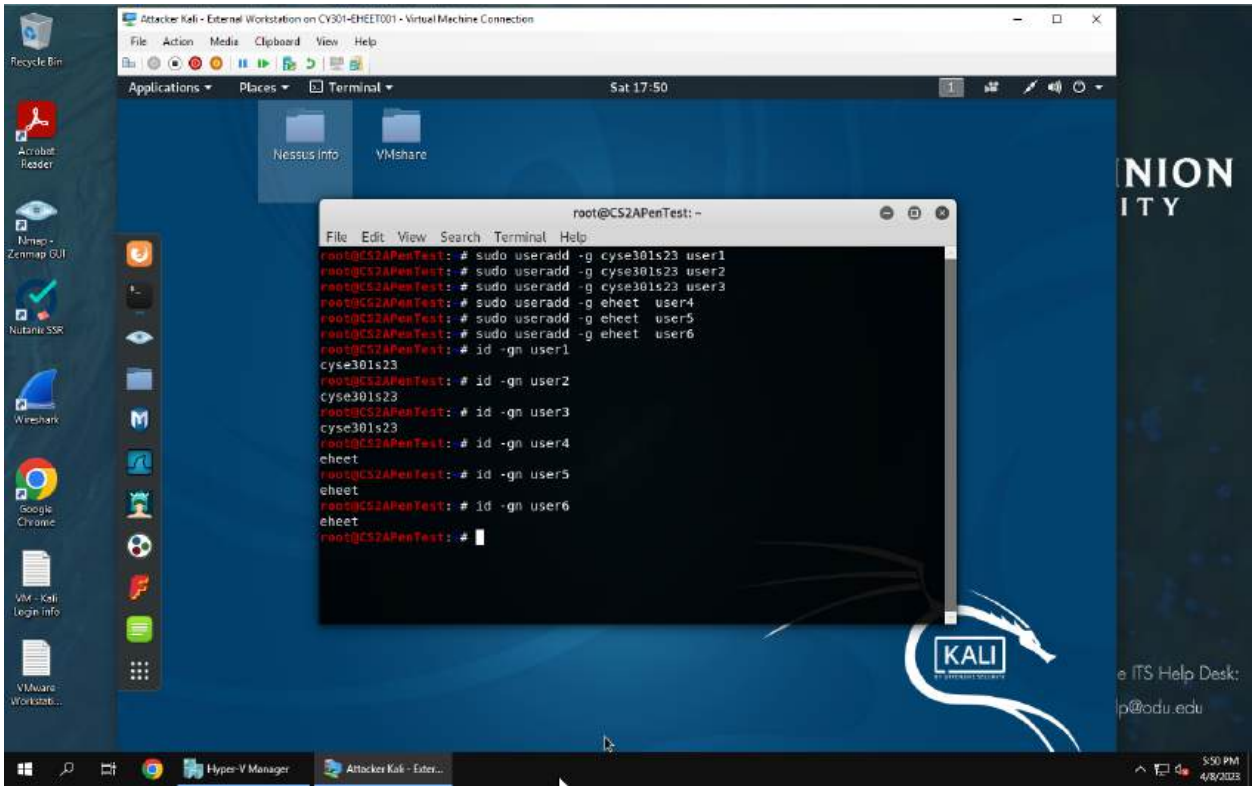
1. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.

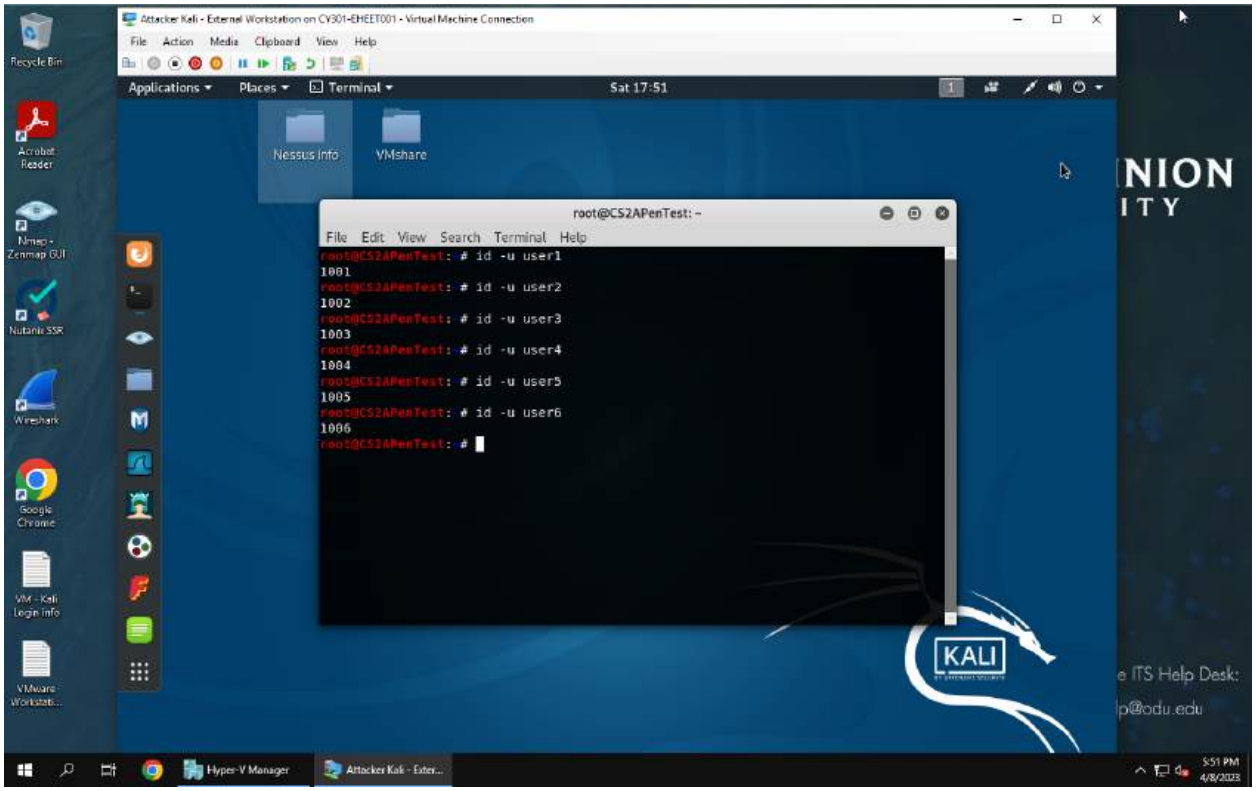




Explanation:
I used the groupadd command to add the two specified groups. I then navigated to the /etc directory and used tail group to open the file where the group ID could be found.

2. Create and assign three users to each group. Display related UID and GID information of each user.

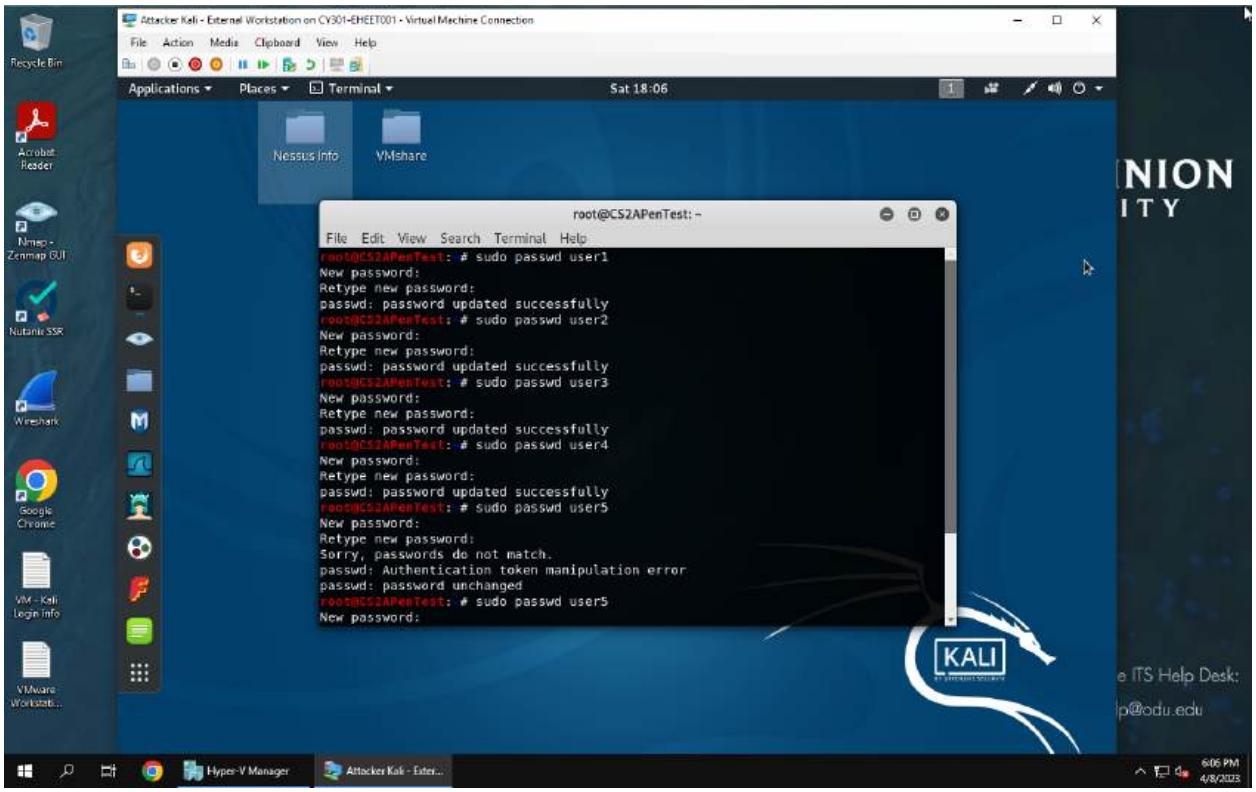


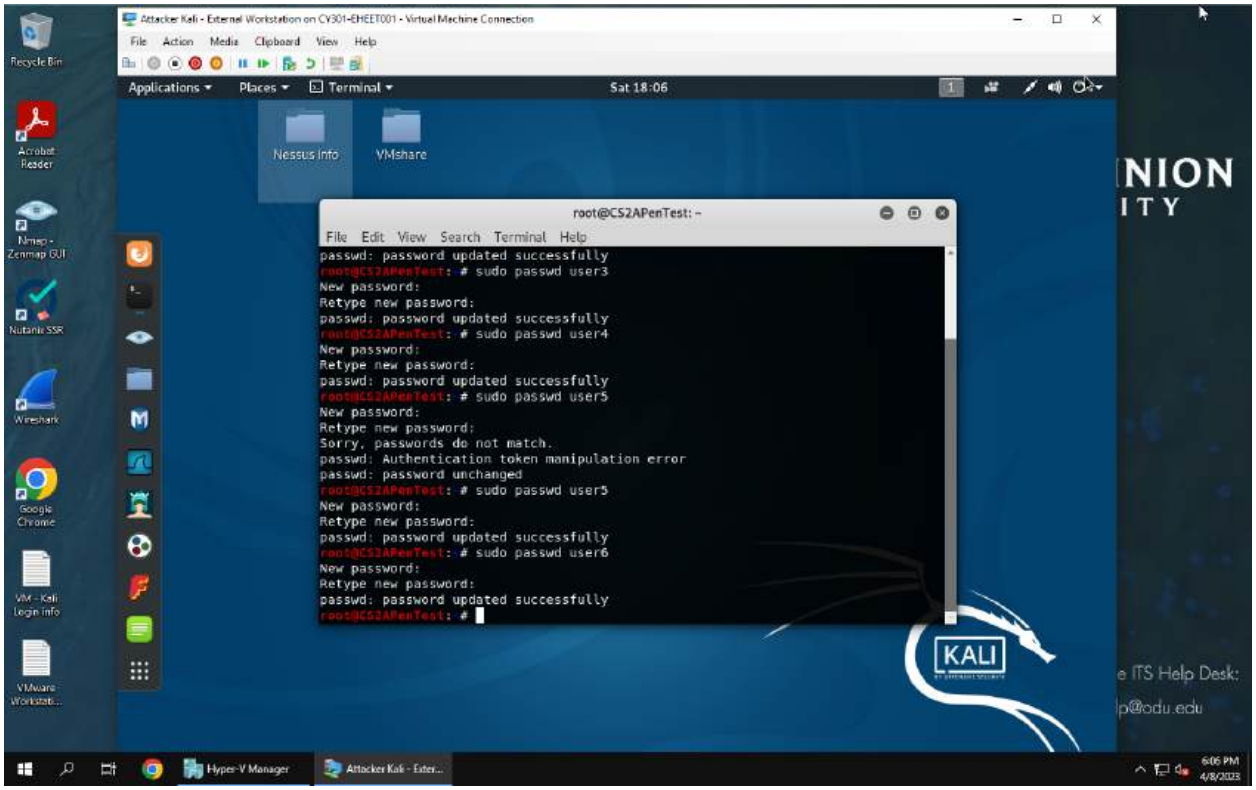


Explanation:

First I used sudo useradd -g *groupname username* to add users 1-3 to group cyse301s23 and users 4-6 to group eheet. Then I used id -gn *username* to display the users group and id -u *username* to display UID.

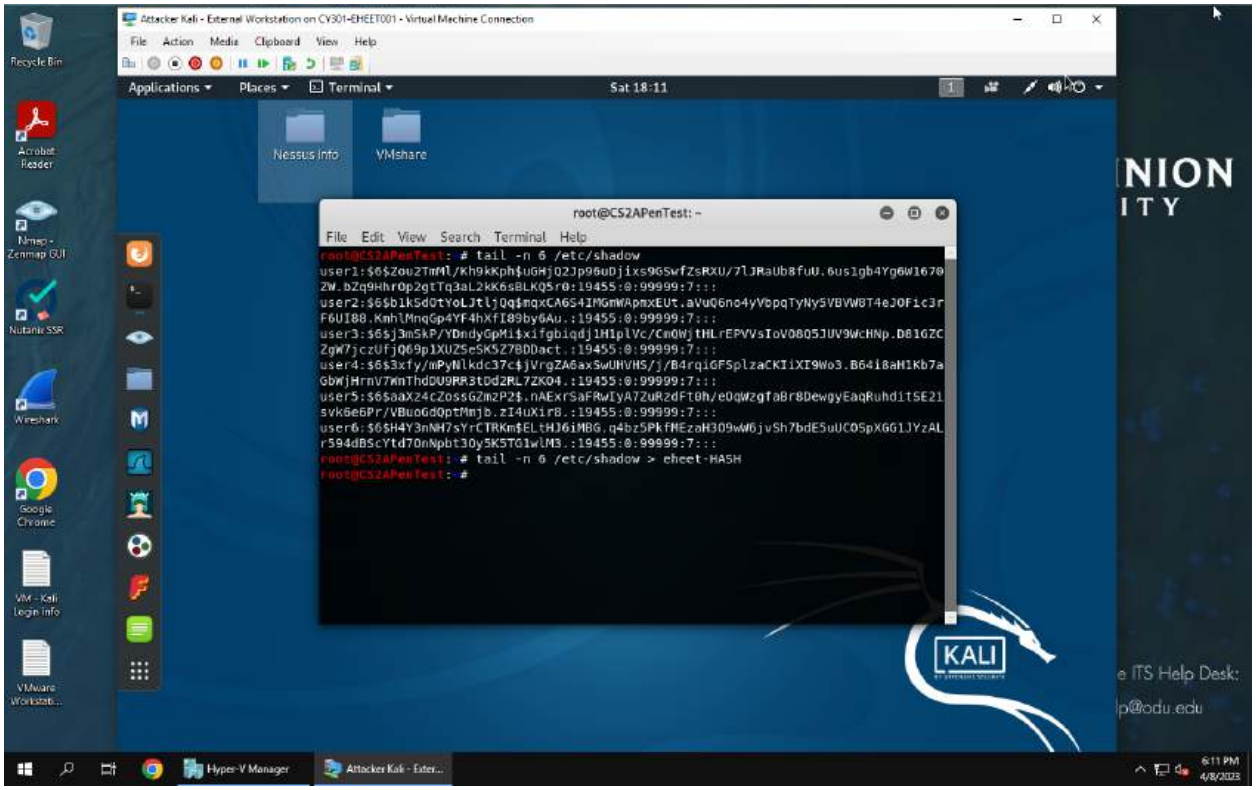
3. Choose six new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords

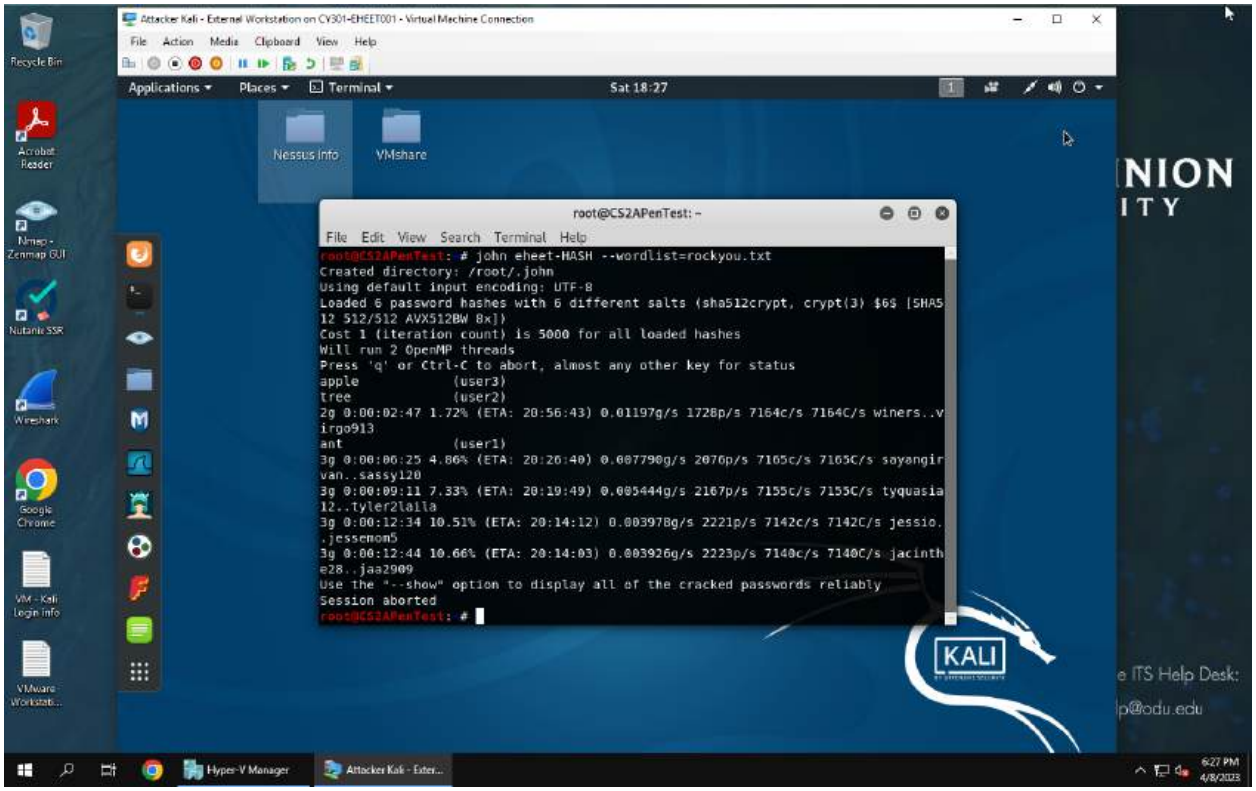




Explanation:
I used sudo passwd *username* to change the passwords of all six users. From easiest to hardest the new passwords are:
User1 - ant
User2 - tree
User3 - apple
User4 - castle1!
User5 - SecuriTy95?
User6 - UnBre@kabLe09!!

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.

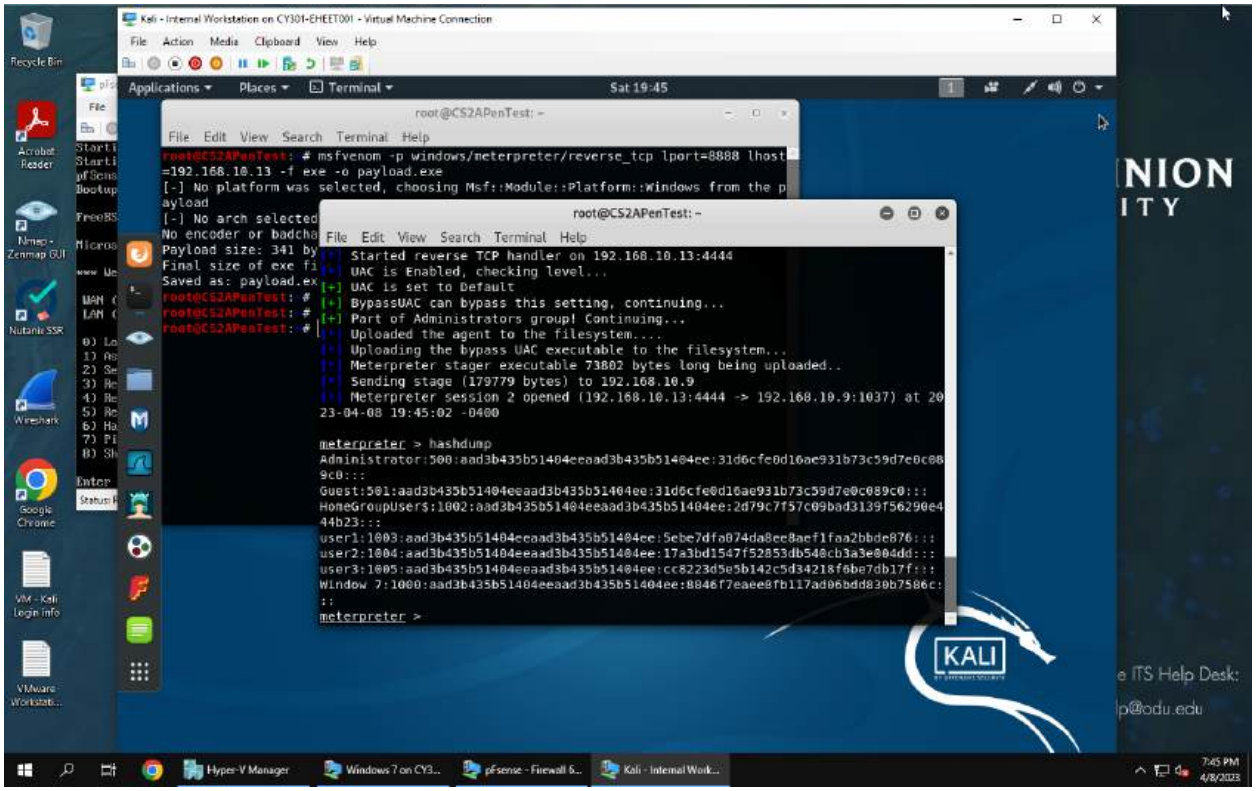




Explanation:

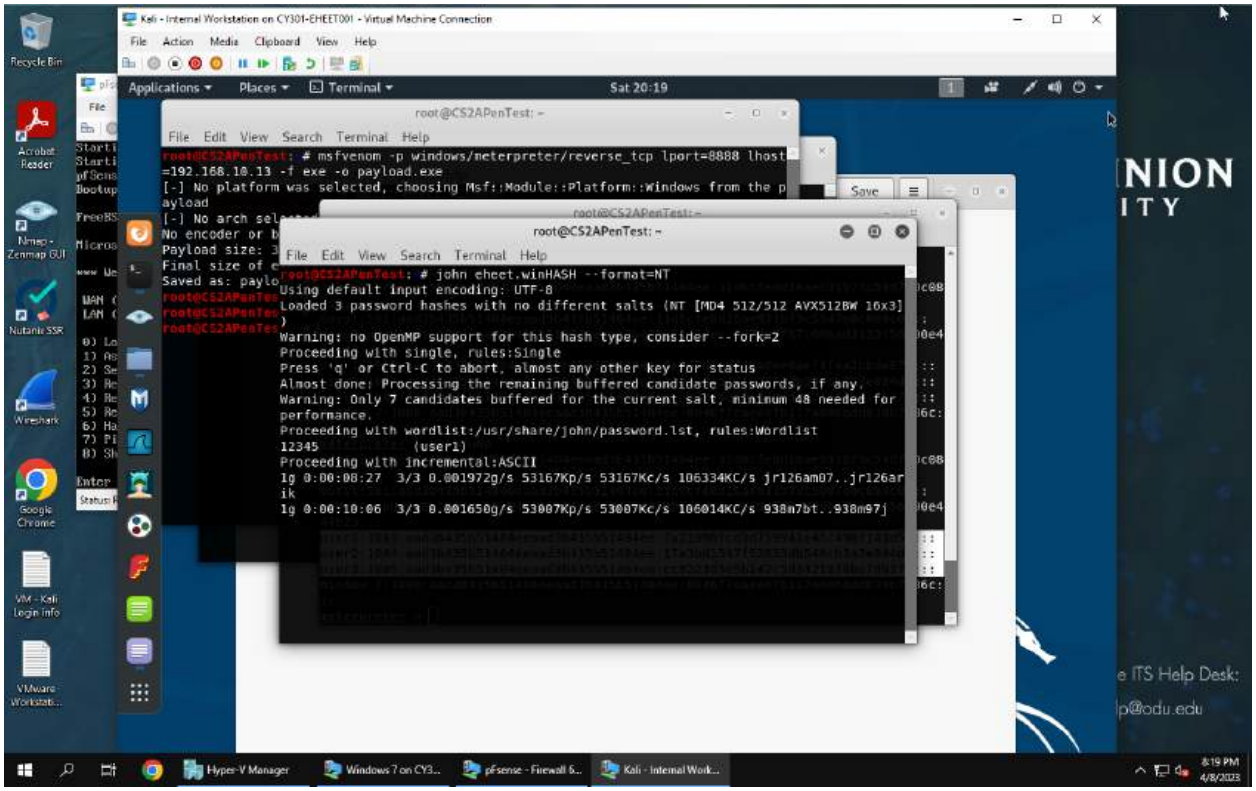
First I used tail -n 6 /etc/shadow > eheet-HASH to copy the hashes to a file which I then ran through john using rockyou.txt. After 12 minutes and 44 seconds I ended the attack which had successfully cracked the first 3 passwords, being ant tree and apple.

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



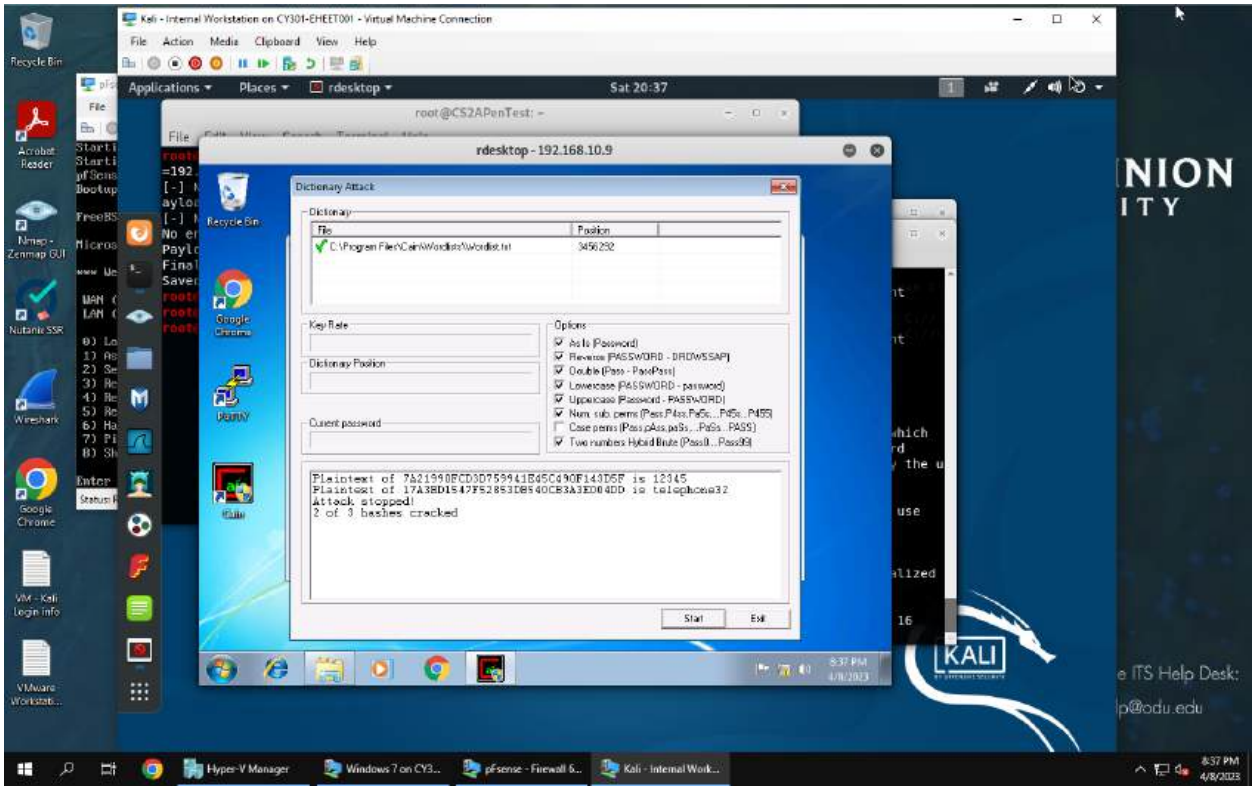
Explanation:
First I made three users with the passwords being 12345, telephone32 and Str0ngholD91!. I then gained access to the windows 7 system through linux and escalated by access to use the hashdump command.

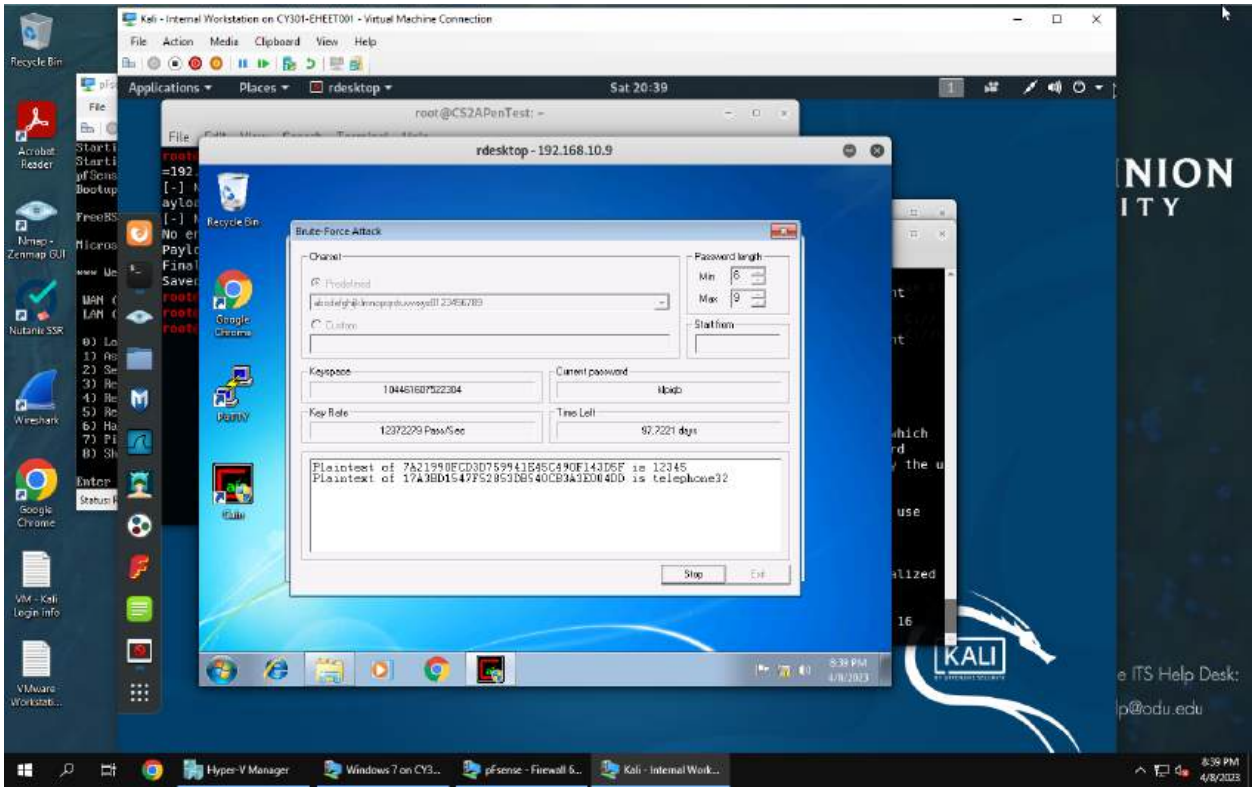
6. Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords



Explanation:
After exporting the hashes and using john the ripper on them for 10 minutes only the first password, 12345, was cracked.

7. 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.



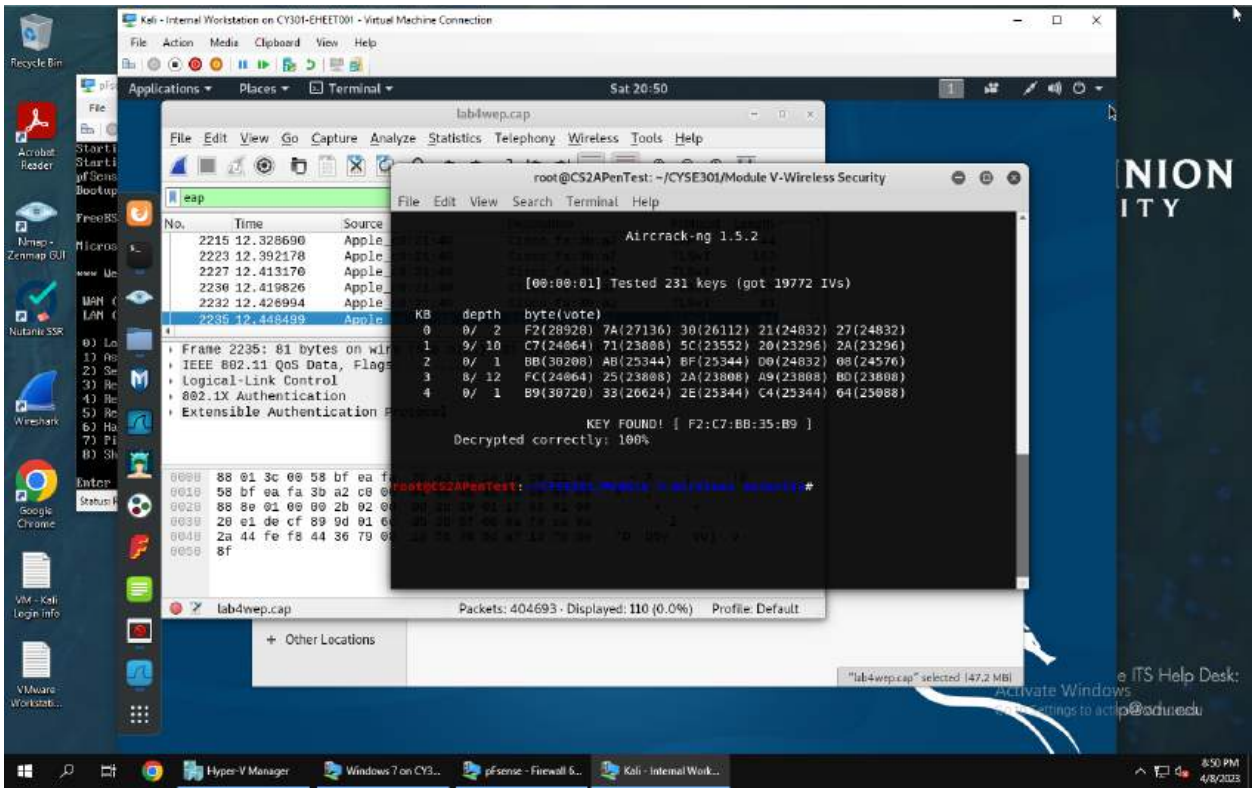


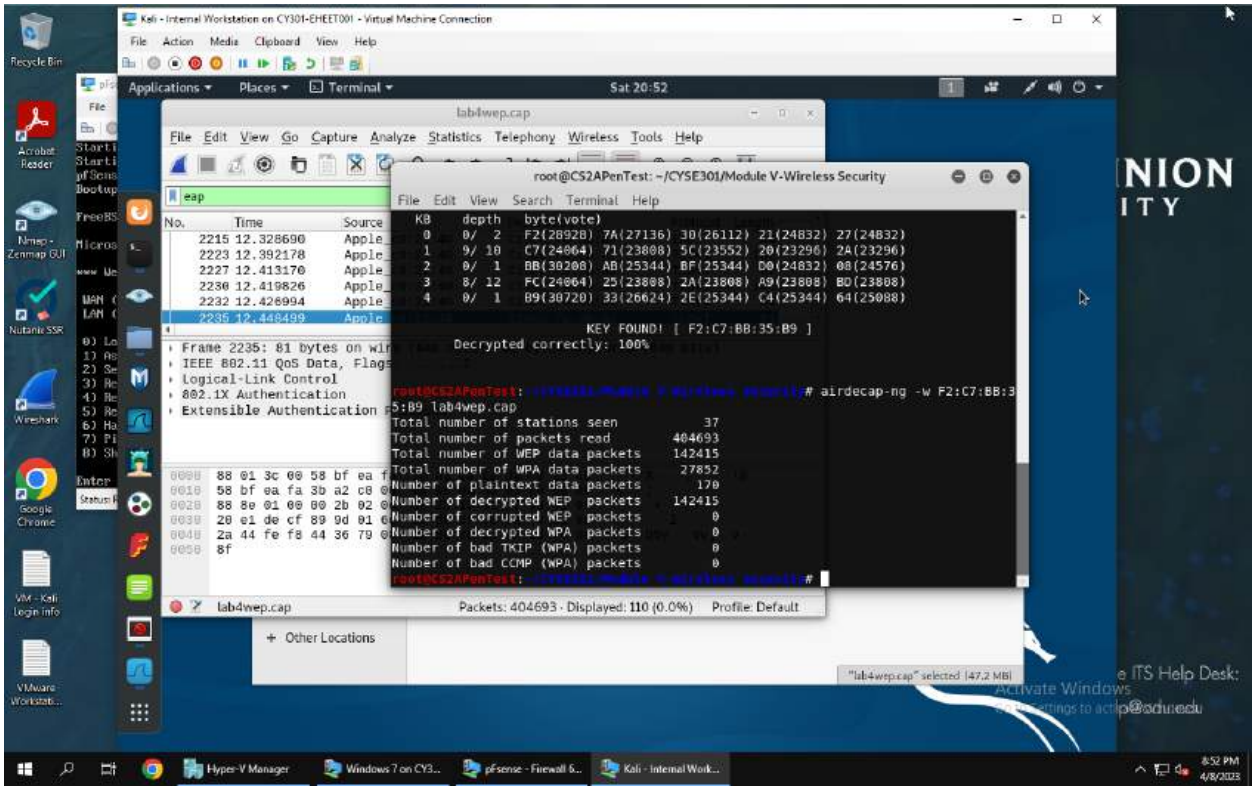
Explanation:

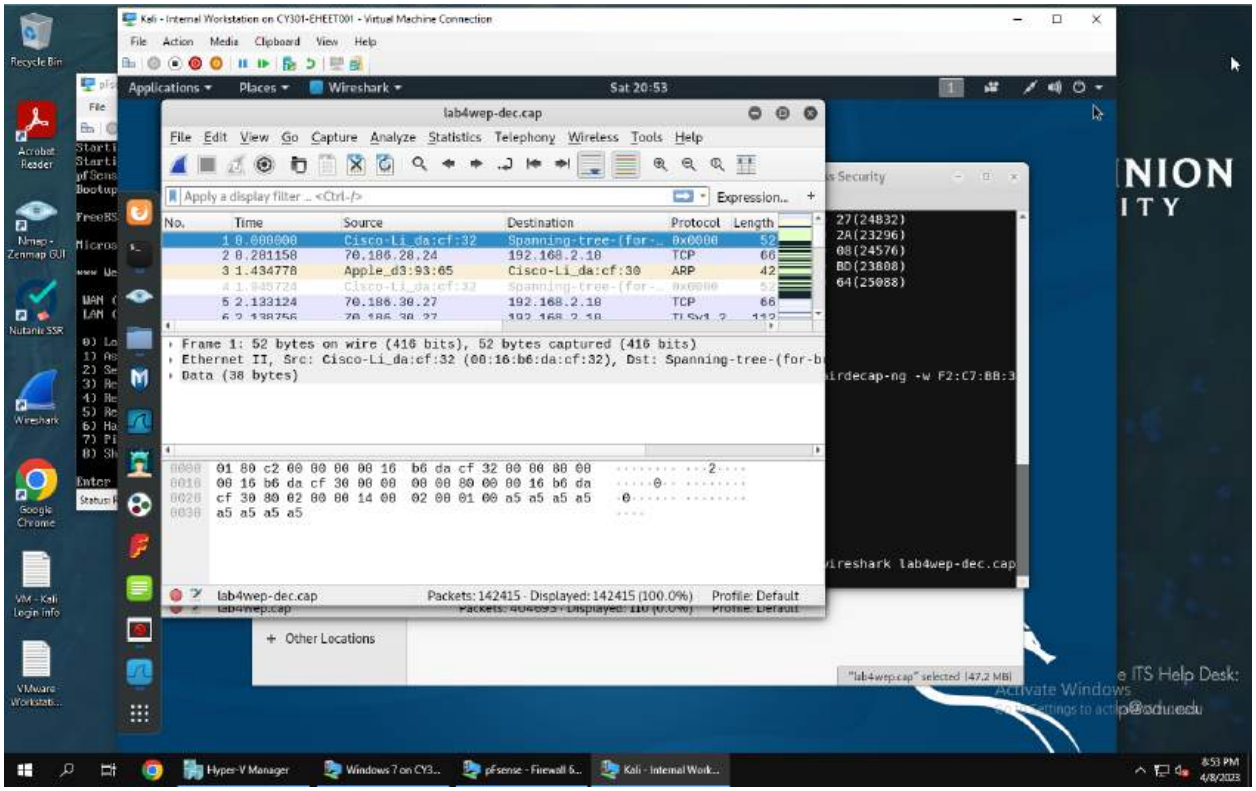
I uploaded cain to windows through the meterpreter and then accessed the hacker account made earlier to use rdestop. I then ran cain with both a dictionary attack, which found the first 2 passwords, and a brute force attack, which said it would take 90 days or so to crack all three.

Part B

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



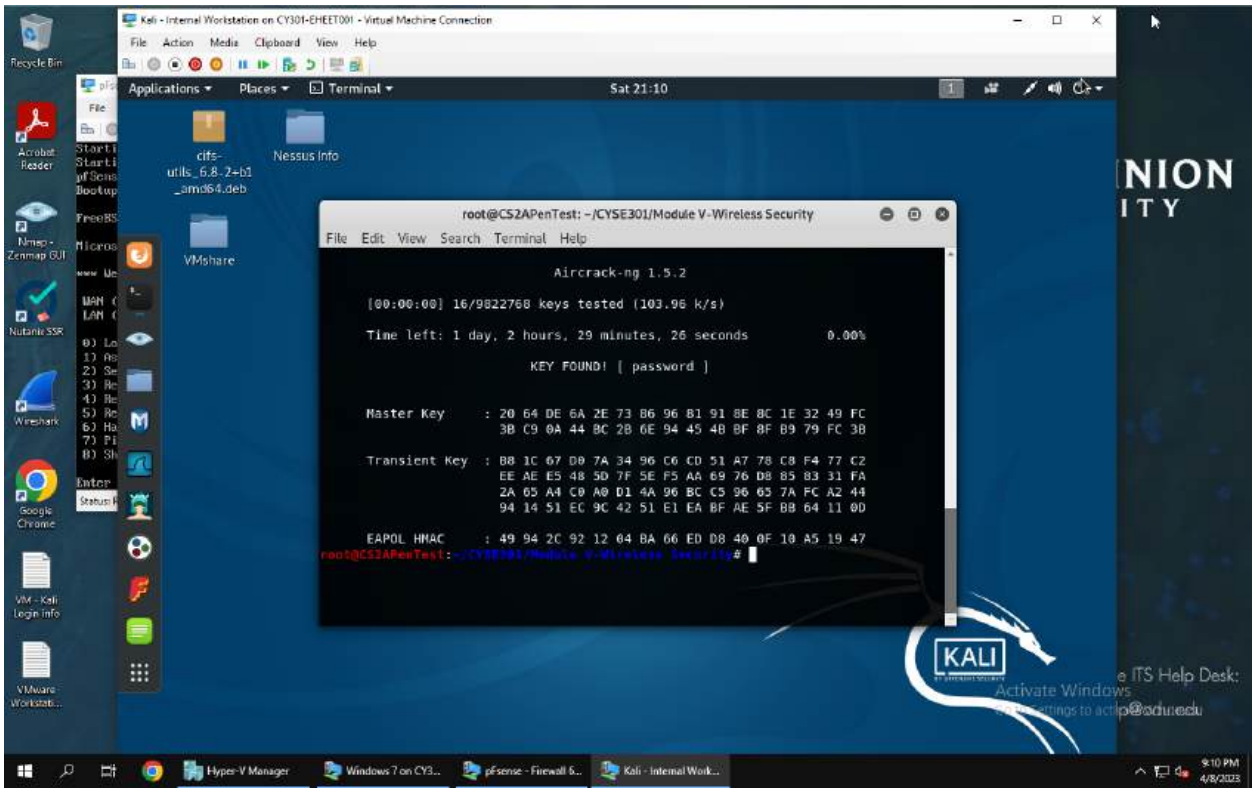


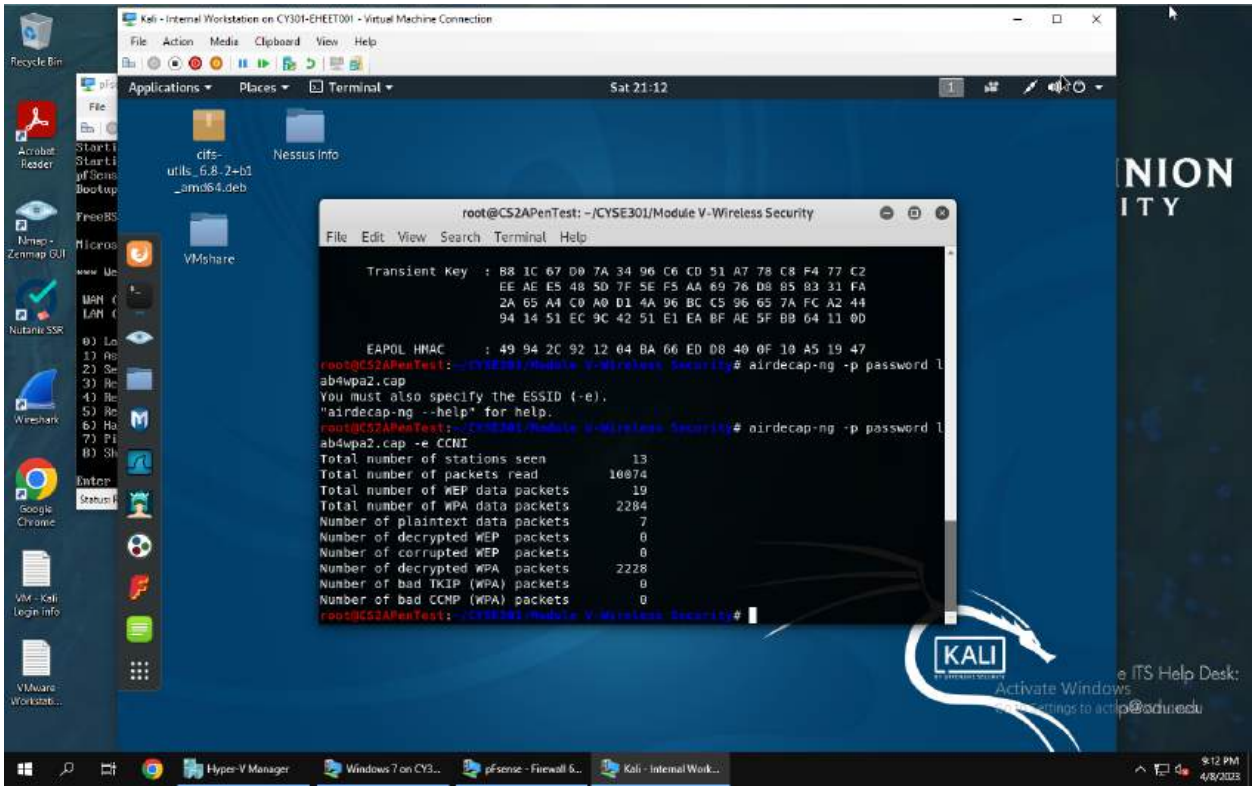


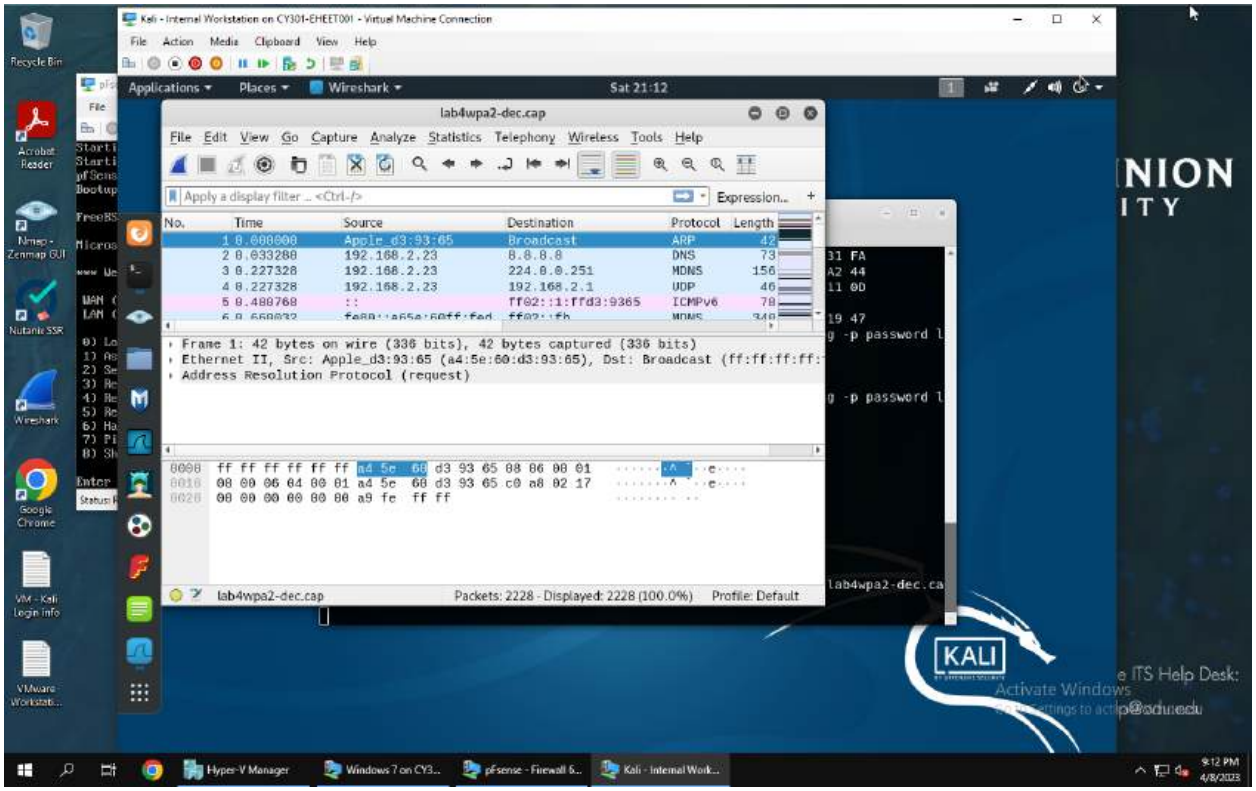
Explanation:

As seen in the screenshots above, I have decrypted the lab4wep.cap file. This has shown me all of the decrypted packets, of which a majority are tcp packets. These packets are almost all requests, with almost all being a request for who has 192.168.2.10 for 0.0.0.0 with the source being alfa. Eventually this request is answered and the connection is started.

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



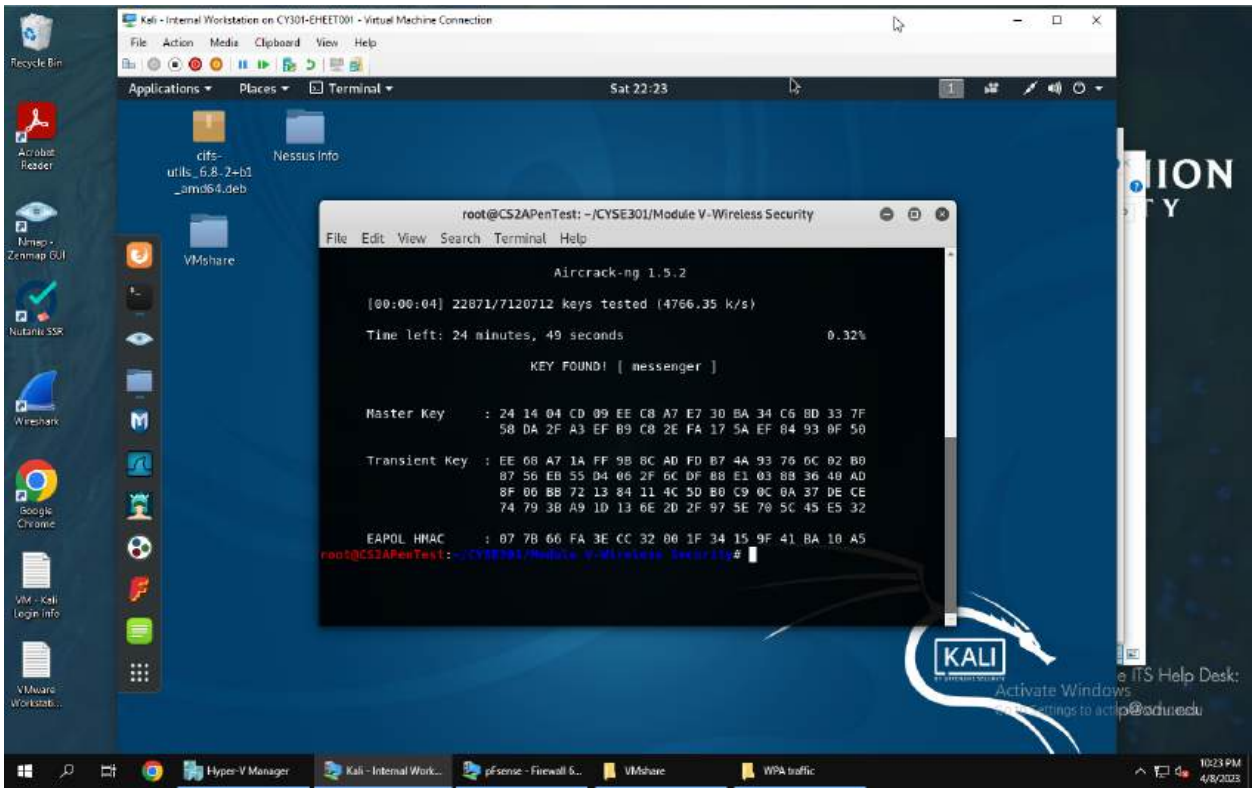


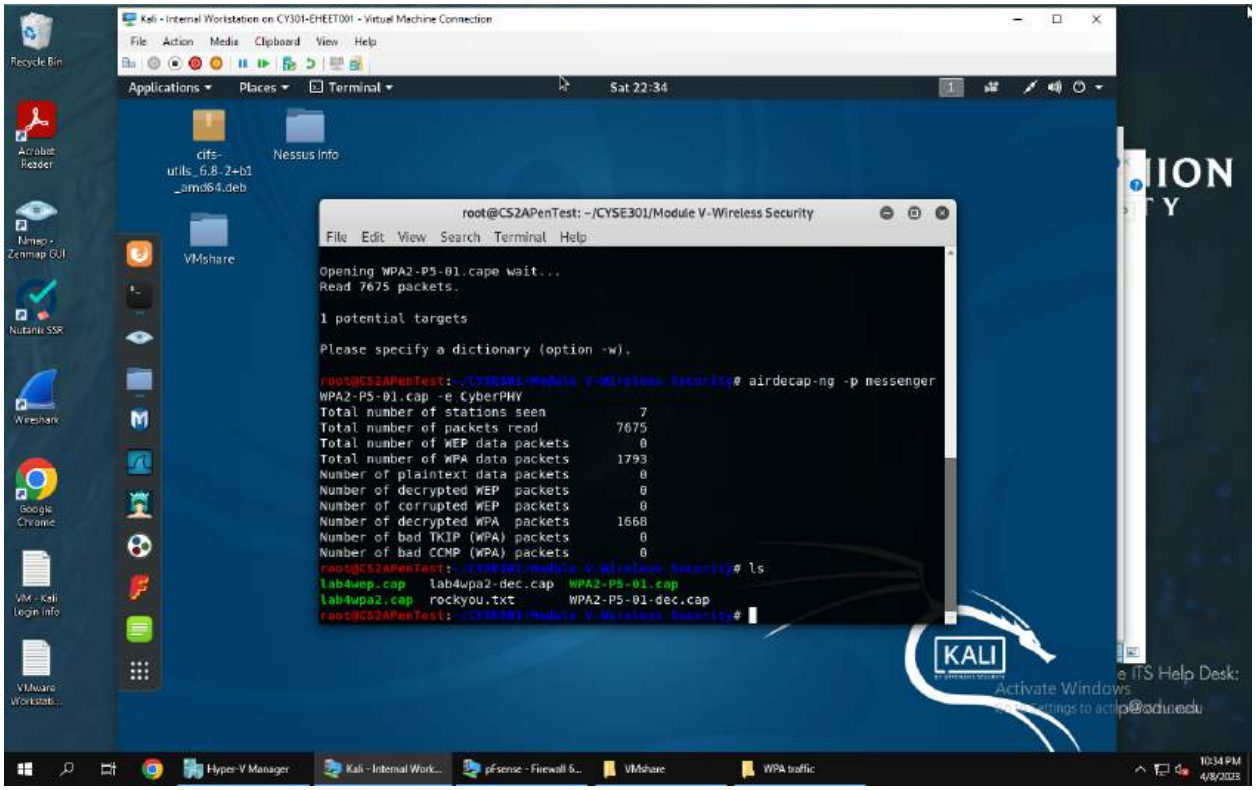


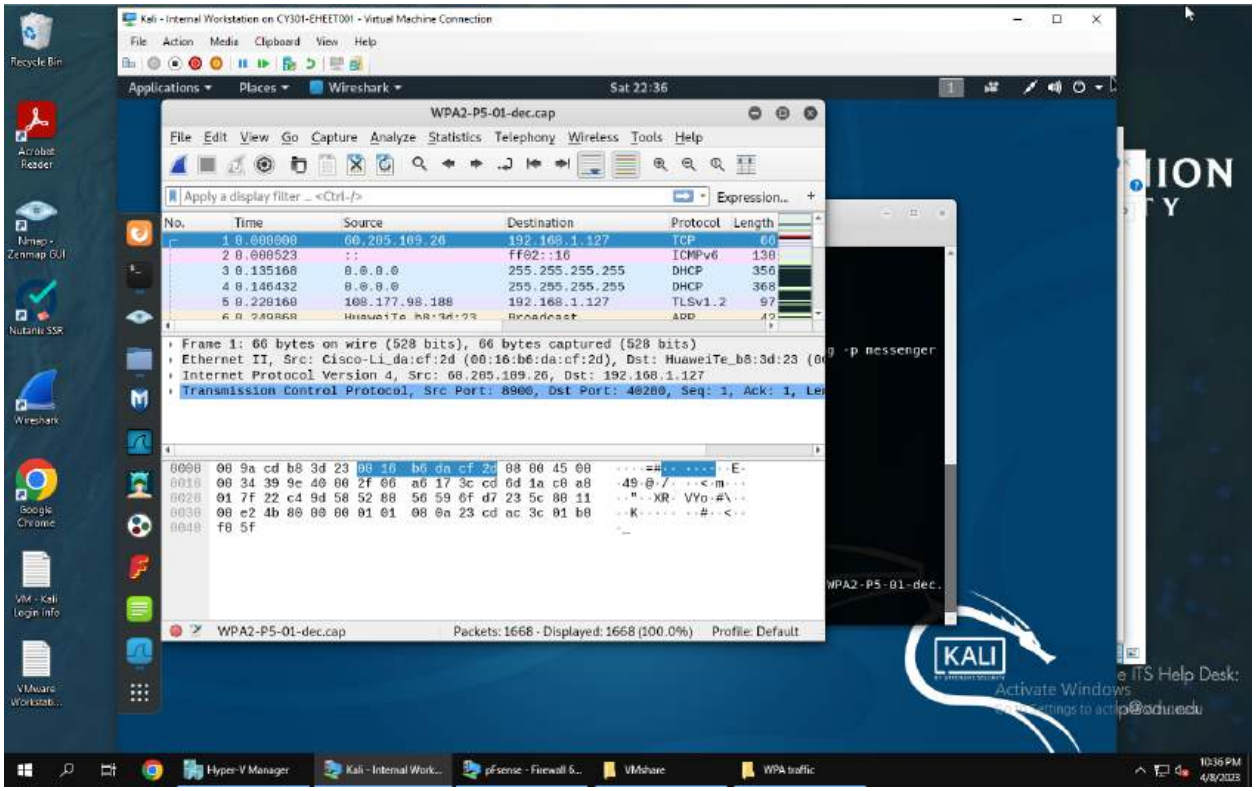
Explanation:

I broke the encryption, finding that the key is password. I then used this key to decrypt the packets, revealing their contents. One major difference with this data set when compared to the previous is that nearly all of the packets are ipv4. In the previous dataset this was not the case, containing very few if any ipv4 connections, instead containing mainly ARP. This data set however has nearly 100% ipv4, with the actual number being 99.7%.

10. Implement a dictionary attack and decrypt the traffic.
    Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file.







Explanation:
First I used aircrack with the dictionary being set to rockyou.txt to find the key, which in this case is messenger. I then used this passcode as well as the type, being CyberPHY,

to decrypt the packets so that I could view them in wireshark. This data set had quite a few differences to the previous ones. For starters, TCP was not the most common protocol used, being beaten by UDP. Many packets are GQUIC, meaning google quick UDP internet connection, between two ips, 192.168.1.127 and 70.186.28.16. Most of these communications carry encrypted payloads. This continues for a long while until 192.168.1.127 starts communicating with 172.217.4.142 using UDP. This continues for some time before 192.168.1.127 starts communicating with 103.7.29.54 through tcp packets. 192.168.1.127 then starts to communicate with 172.217.4.142 using UDP again for a long time. This pattern continued, with 172.217.4.142 communicating with different Ip addresses, with some outliers being the large number of dropped packers as well as other types of protocols being used like DNS and ICMPv6.