OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

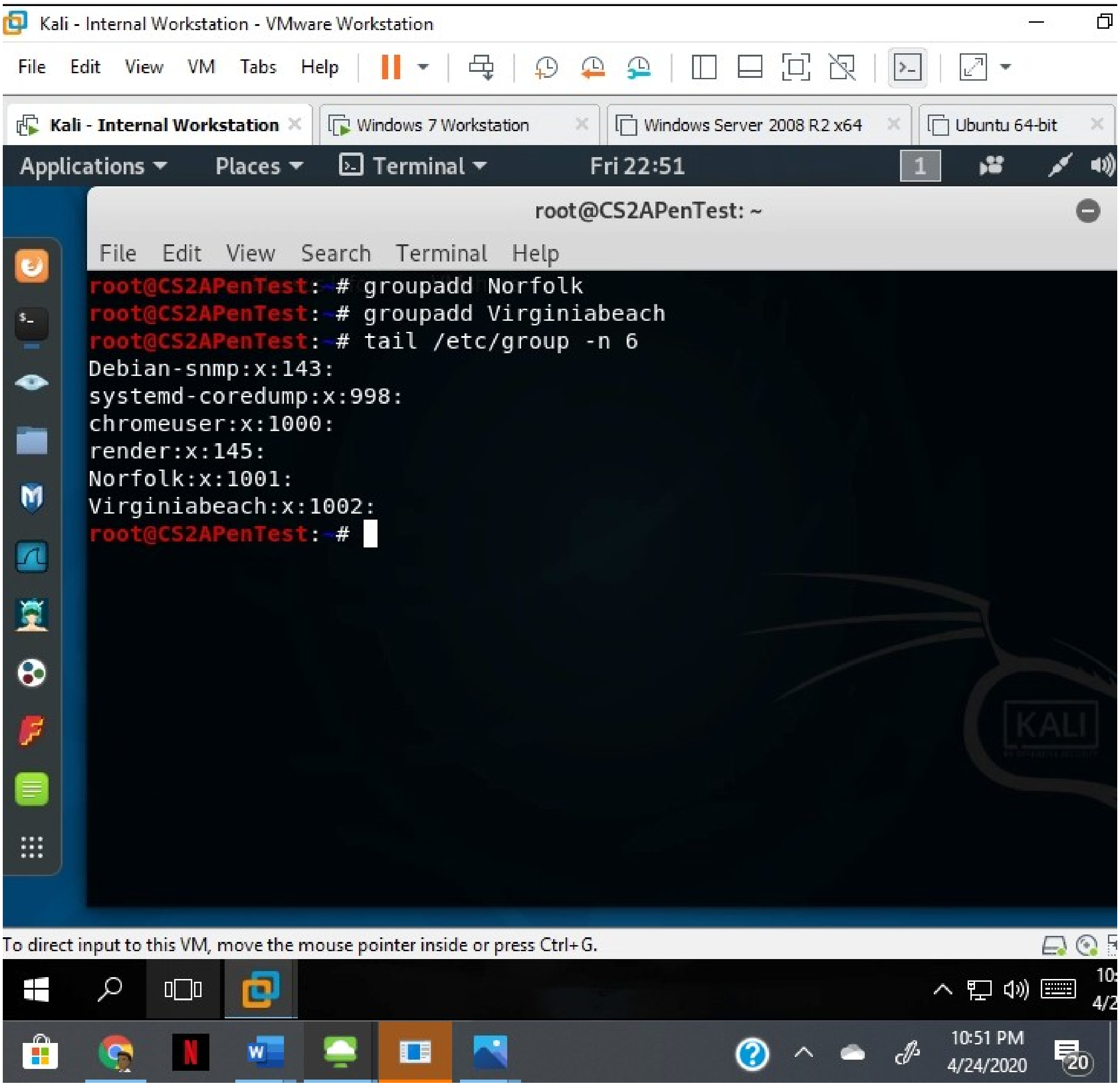
Assignment #4

Malcolm Marcus and 01109293

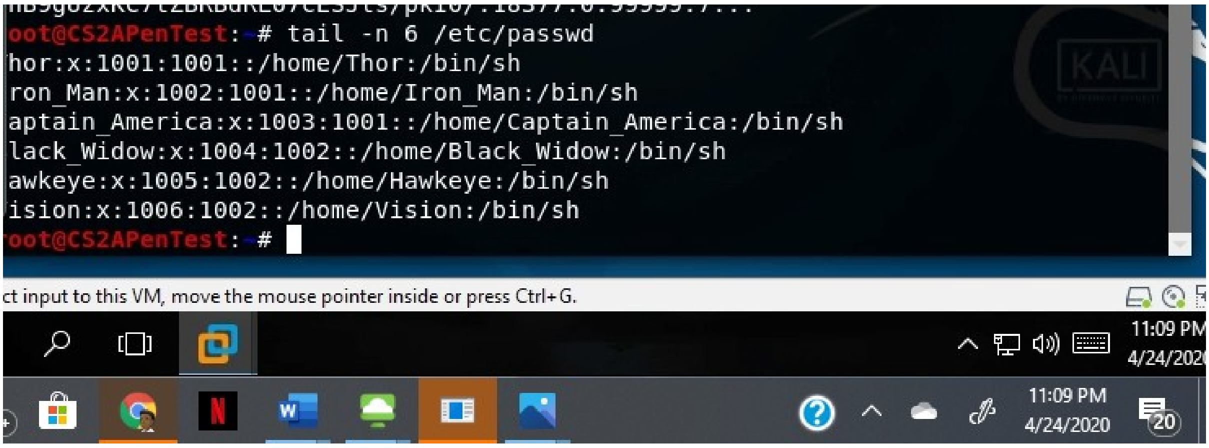
Spring 2020

TASK A: John The Ripper

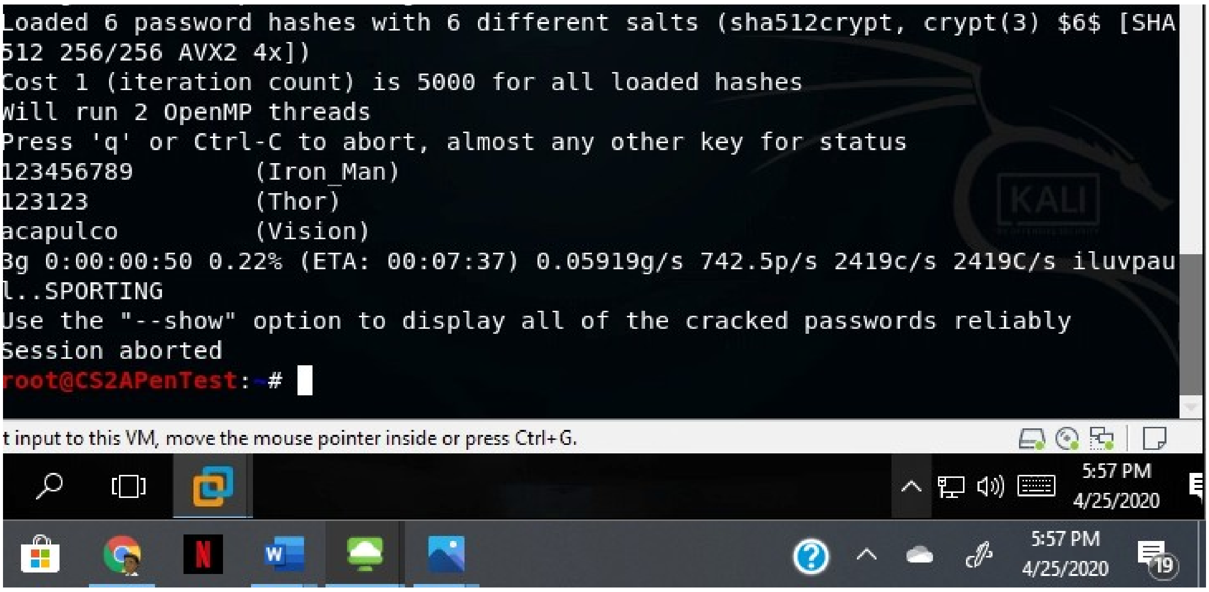
1. Create six different users with different passwords (separate into two groups) and add them to Kali VM. Then use John the Ripper to implement a dictionary attack to crack the passwords(no need to crack all of the passwords).


Kali - Internal Workstation - VMware Workstation
File Edit View VM Tabs Help
Kali - Internal Workstation
Windows 7 Workstation
Windows Server 2008 R2 x64
Ubuntu 64-bit
Applications
Places
Terminal
Fri 22:51
root@CS2APenTest: ~
File Edit View Search Terminal Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
10:51 PM
4/24/2020

```
root@CS2APenTest:~# groupadd Norfolk
root@CS2APenTest:~# groupadd Virginiabeach
root@CS2APenTest:~# tail /etc/group -n 6
Debian-snmp:x:143:
systemd-coredump:x:998:
chromeuser:x:1000:
render:x:145:
Norfolk:x:1001:
Virginiabeach:x:1002:
root@CS2APenTest:~# 
```


ct input to this VM, move the mouse pointer inside or press Ctrl+G.
11:09 PM
4/24/2020

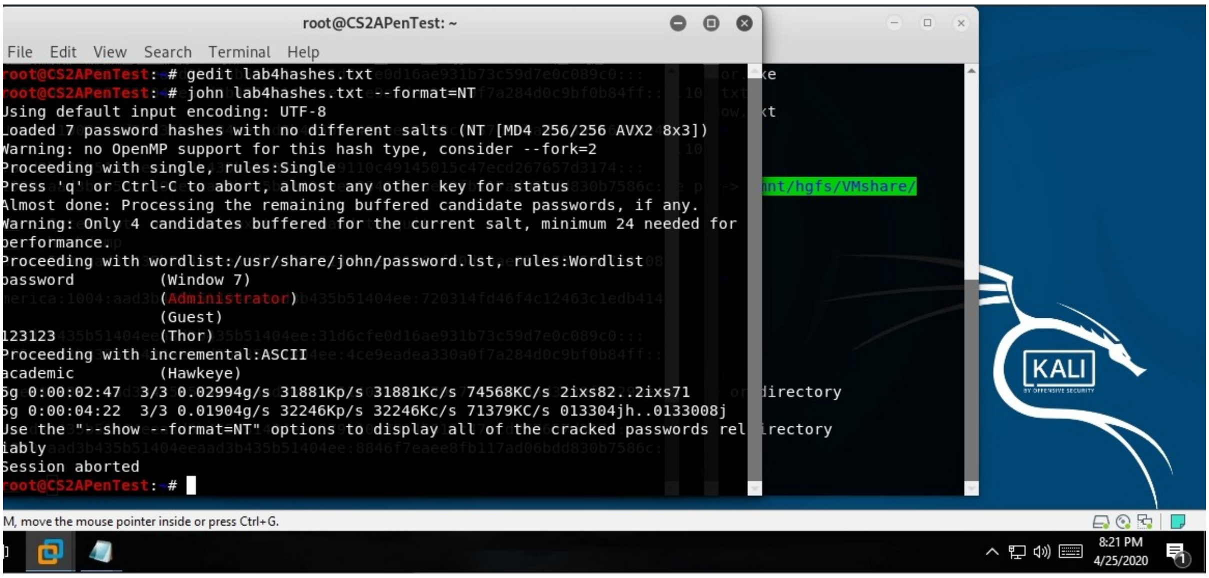
```
mB5gGzxRC/tZBRBuRL0/cLSJts/pK10/:18377:0:99999:7:::
oot@CS2APenTest:~# tail -n 6 /etc/passwd
hor:x:1001:1001::/home/Thor:/bin/sh
ron_Man:x:1002:1001::/home/Iron_Man:/bin/sh
aptain_America:x:1003:1001::/home/Captain_America:/bin/sh
lack_Widow:x:1004:1002::/home/Black_Widow:/bin/sh
awkeye:x:1005:1002::/home/Hawkeye:/bin/sh
ision:x:1006:1002::/home/Vision:/bin/sh
oot@CS2APenTest:~# 
```



```
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA
512 256/256 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
123456789        (Iron_Man)
123123           (Thor)
acapulco         (Vision)
3g 0:00:00:50 0.22% (ETA: 00:07:37) 0.05919g/s 742.5p/s 2419c/s 2419C/s iluvpau
l..SPORTING
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest:~#
```

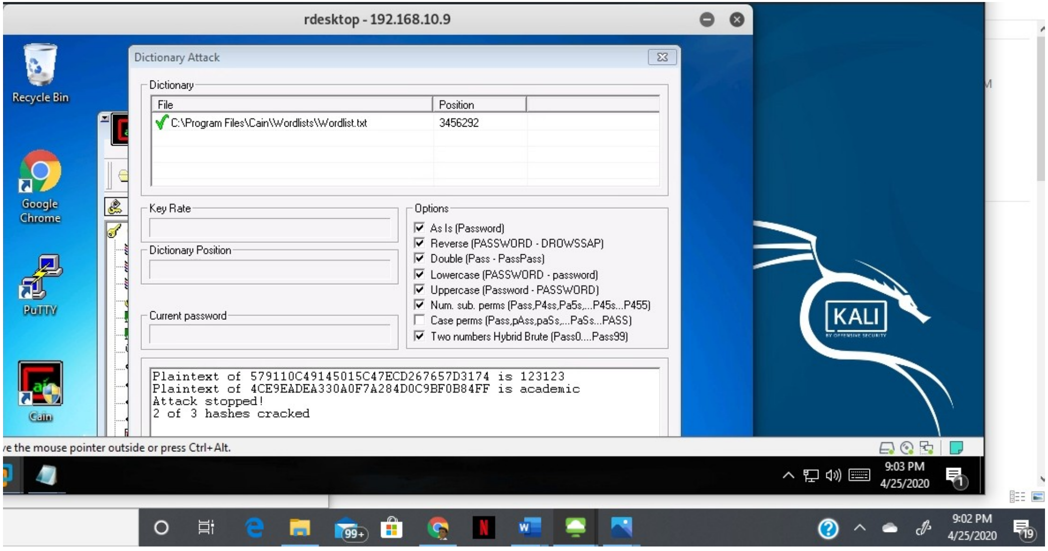
t input to this VM, move the mouse pointer inside or press Ctrl+G.
5:57 PM
4/25/2020
5:57 PM
4/25/2020
19

2. Create a list of three users with the simple password in Windows 7 VM and use John the Ripper to crack the passwords(no need to crack all the passwords).



```
root@CS2APenTest:~# gedit lab4hashes.txt
root@CS2APenTest:~# john lab4hashes.txt --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 4 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)
123123           (Thor)
Proceeding with incremental:ASCII
academic         (Hawkeye)
5g 0:00:02:47  3/3 0.02994g/s 31881Kp/s 31881Kc/s 74568KC/s 2ixs82..2ixs71
5g 0:00:04:22  3/3 0.01904g/s 32246Kp/s 32246Kc/s 71379KC/s 013304jh..0133008j
Use the "--show --format=NT" options to display all of the cracked passwords rel
iably
Session aborted
root@CS2APenTest:~#
```

3. Use the same set of accounts you created in the previous step, use Cain and Abel to implement either a brute force attack or a dictionary attack to crack the passwords (no need to crack all the passwords)



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 579110C49145015C47ECD267657D3174 is 123123
Plaintext of 4CE9EADEA330A0F7A284D0C9BF0B84FF is academic
Attack stopped!
2 of 3 hashes cracked
```