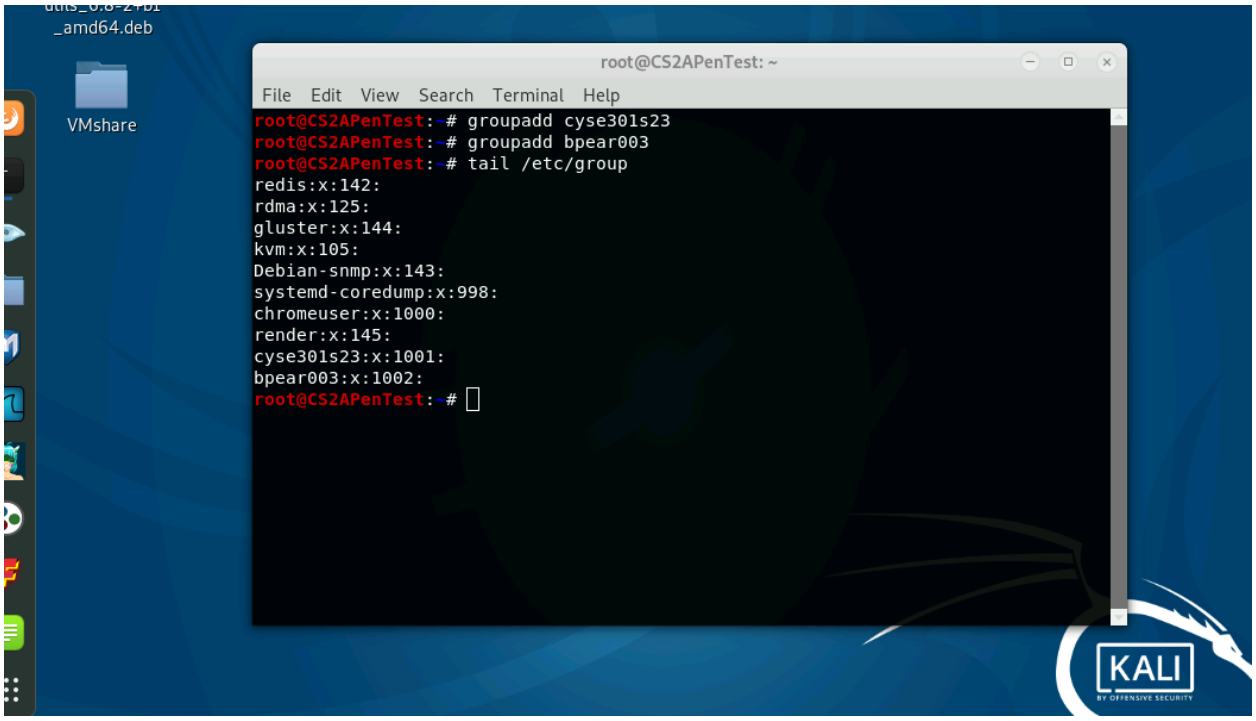
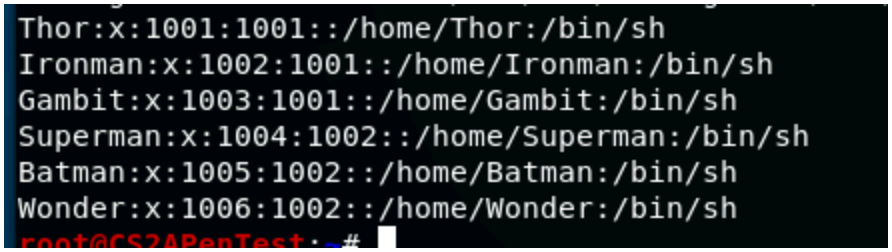
At the end of this module, each student needs to submit a report that includes the solutions to the
following tasks. Make sure you take a screenshot for every single step as proof.
You need to use
Task A: Linux Password Cracking (25 points)
1. 5 points. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example,
pjiang). Then display the corresponding group IDs.



2. 5 points. Create and assign three users to each group. Display related UID and GID information of
each user.

```
root@CS2APenTest:~# useradd Thor -g cyse301s23
root@CS2APenTest:~# useradd Ironman -g cyse301s23
root@CS2APenTest:~# useradd Gambit -g cyse301s23
root@CS2APenTest:~# useradd Superman -g bpear003
root@CS2APenTest:~# useradd Batman -g bpear003
root@CS2APenTest:~# useradd Wonder - bpear003
```

Useradd wonder -g bpear003 *

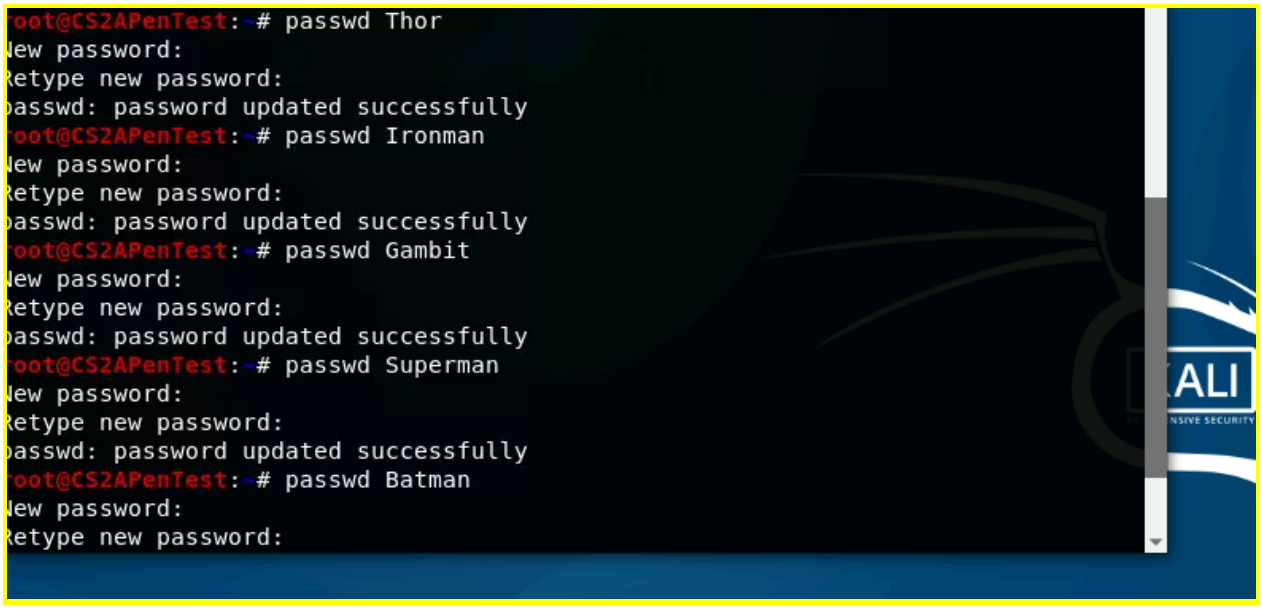


Cat /etc/passwd

group 1001 and group 1002 are the two group id numbers

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.

Thor - Password
Ironman - P@ssw0rd
Gambi - Apple
Superman - Teacher
Batman- Candy!
Wonder- RnD4#

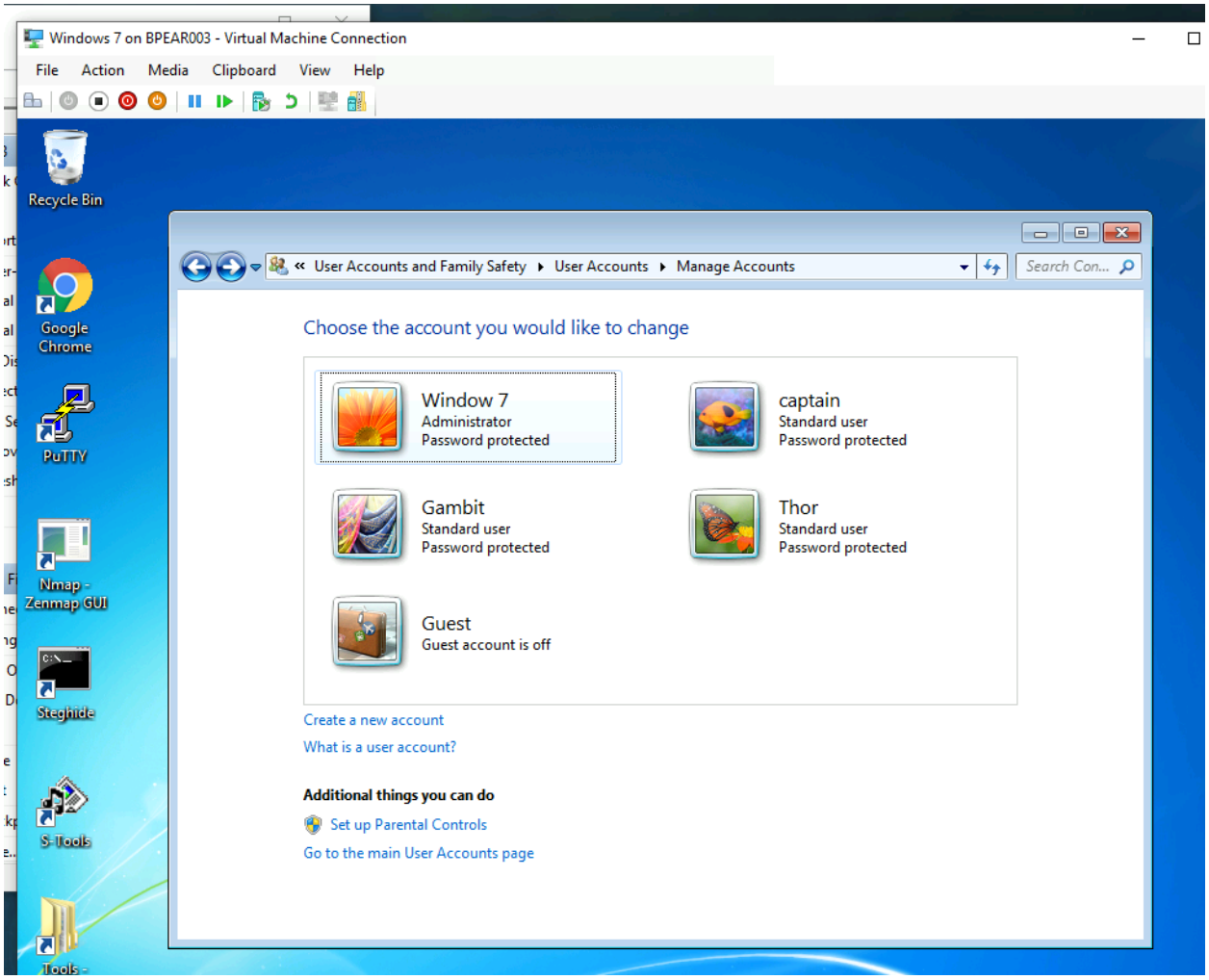


4. 5 points. Export all six users' password hashes into a file named "YourMIDAS-HASH" (for example, pjiang-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.

```
root@CS2APenTest:~# tail -n6 /etc/shadow > bpear003_hashfile
root@CS2APenTest:~# ls
bpear003_hashfile  CYSE301  Documents  Music     Public     Videos
core               Desktop  Downloads  Pictures  Templates  VMshare
root@CS2APenTest:~#
```

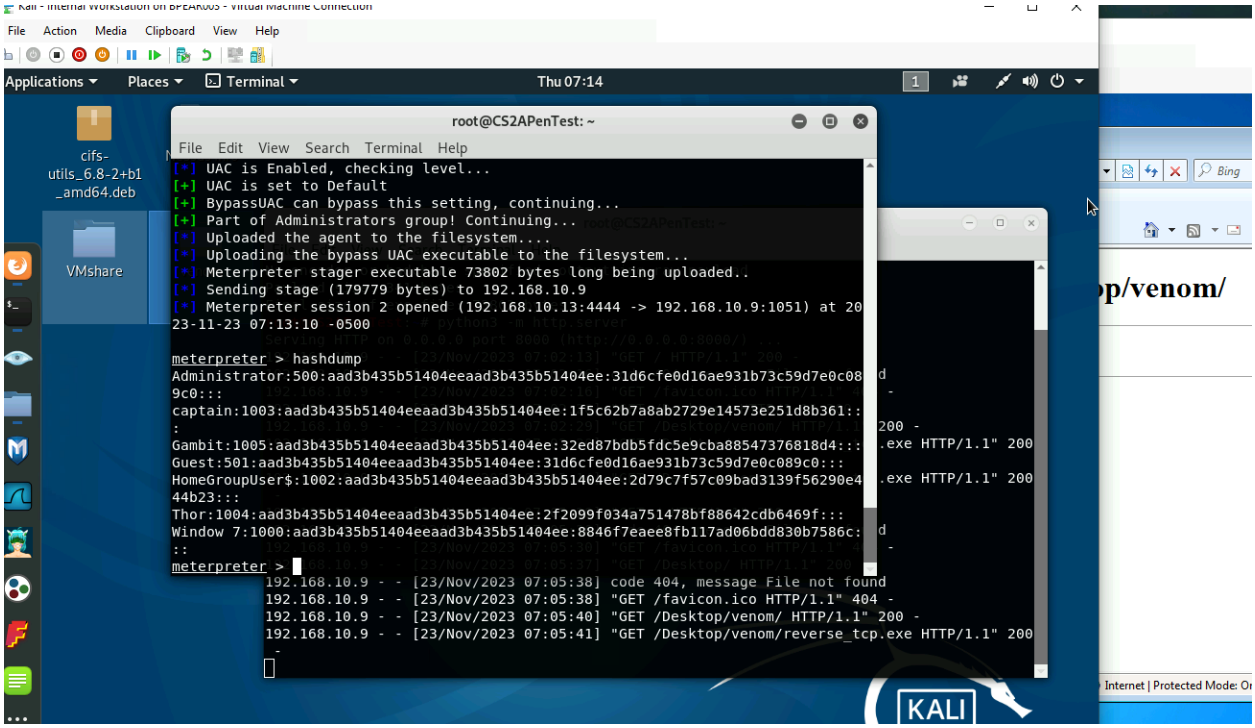
```
File  Edit  View  Search  Terminal  Help
root@CS2APenTest:~# john bpear003_hashfile
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Password         (Thor)
Apple            (Gambit)
Teacher          (Superman)
```

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.

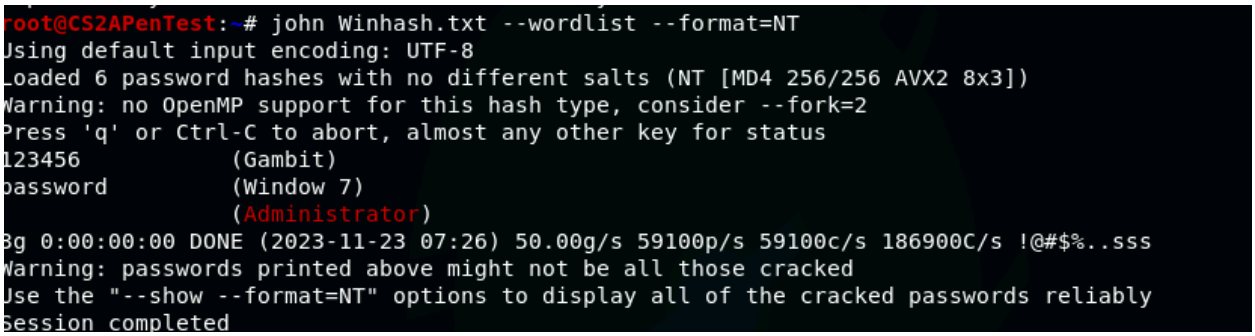


123456 gambit
Longtime captain
Easytoo thor

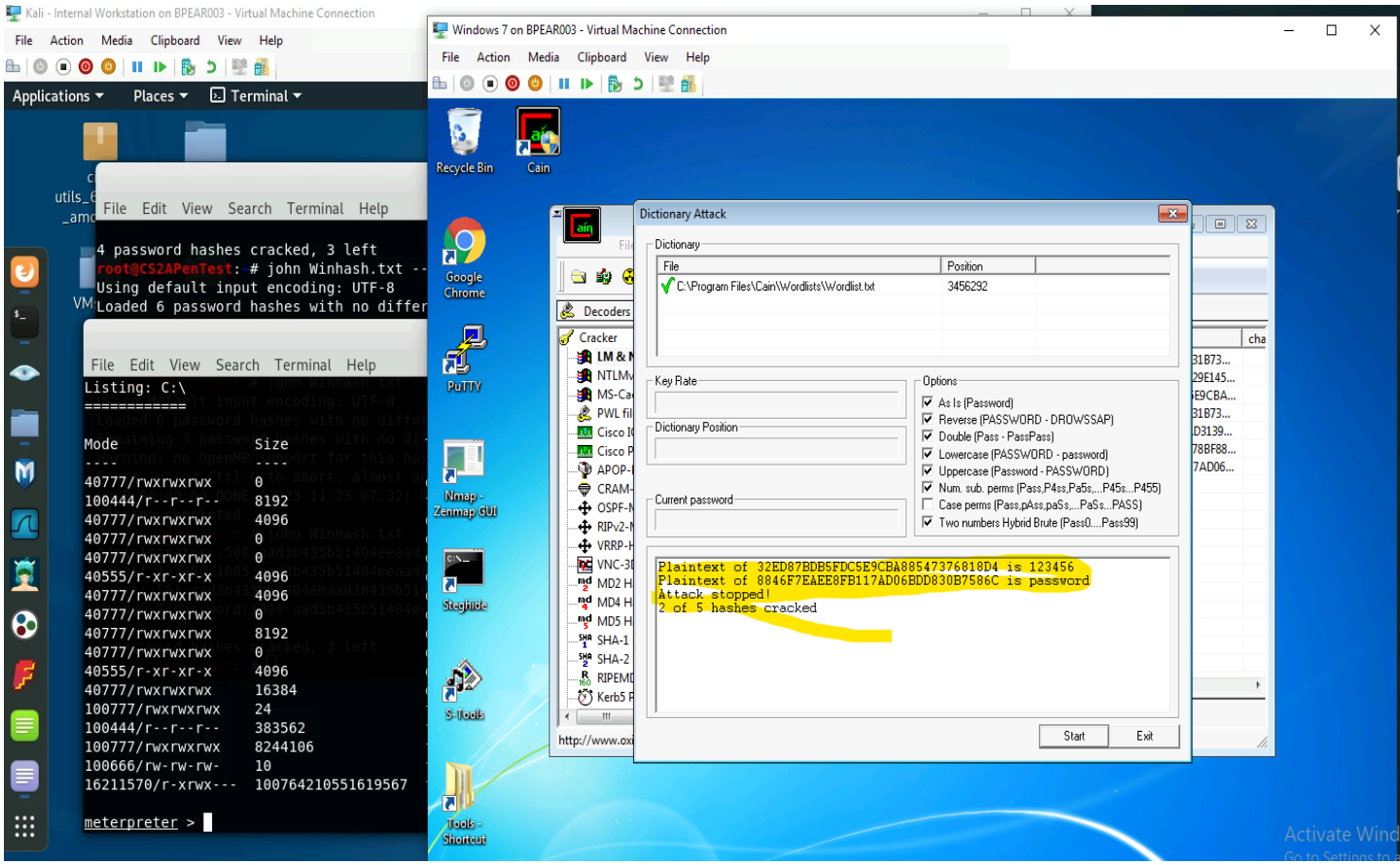
Tried the eternal blue method then realized since no port is open- when nmap -sv Upon this, I created a backdoor .exe file on kali; that windows 7 computer would search online in order to download the backdoor. This gave me access to the windows 7 computer then once I gained privilege; I could get the hash dump to work.

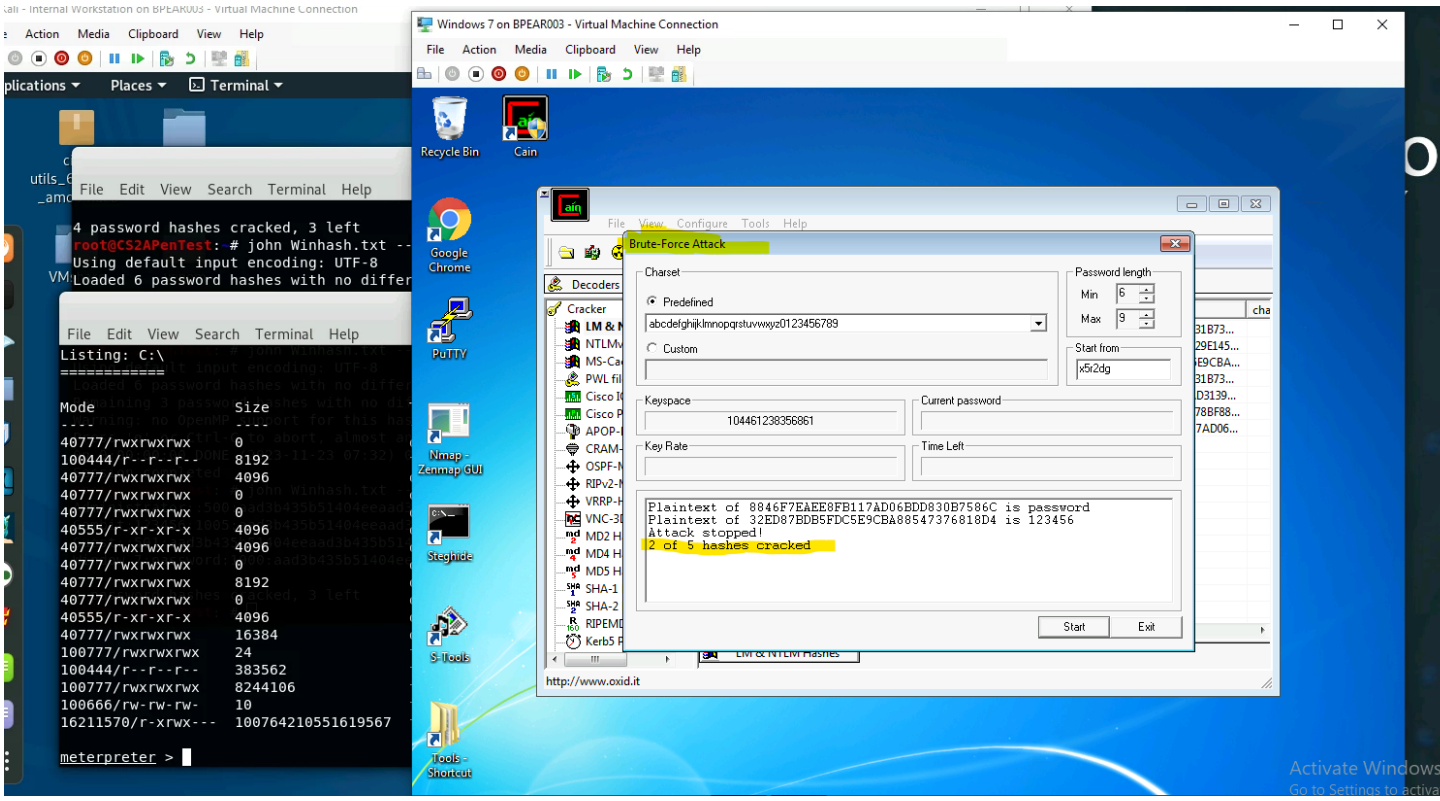


2. 10 points. Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).



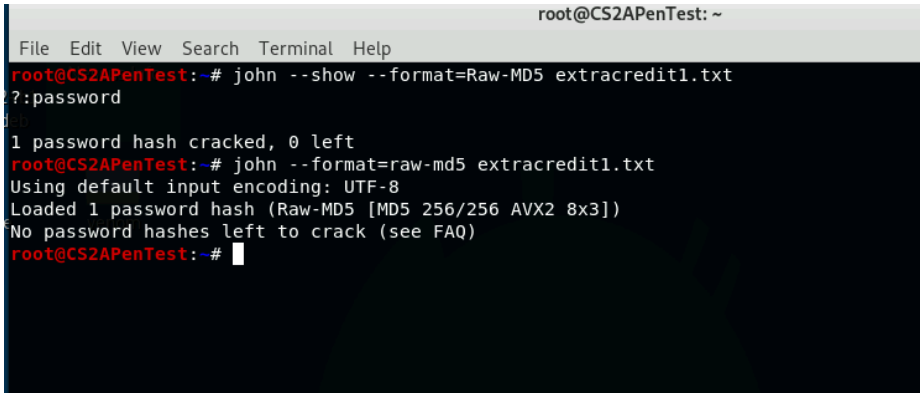
3. 10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).

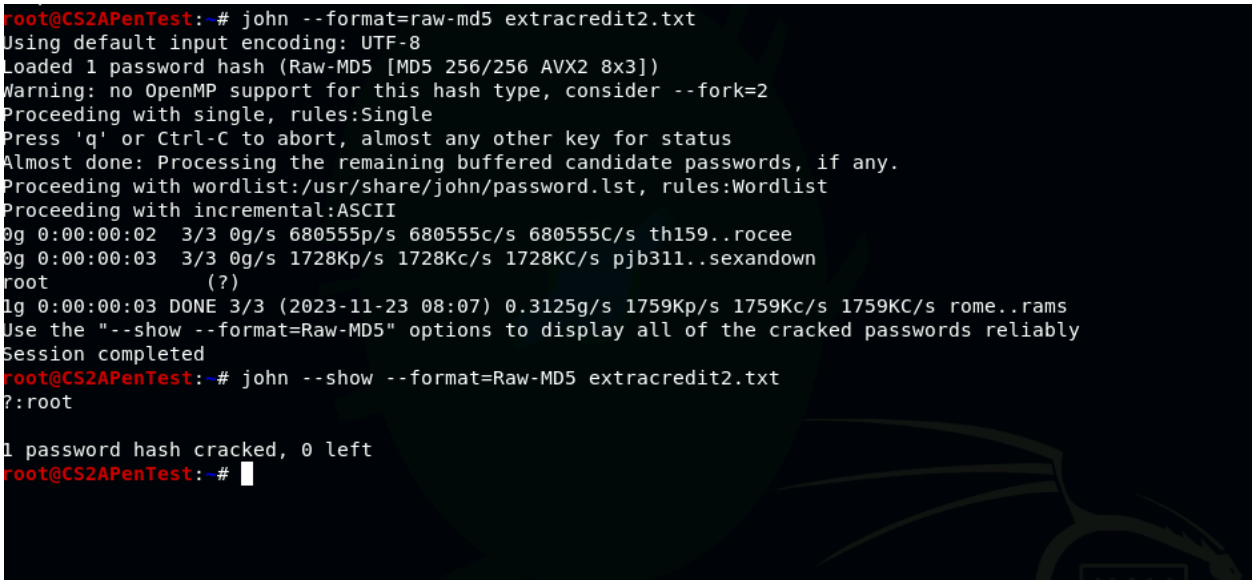




Task C: Extra credit: (10 points)
Search the proper format in John the Ripper to crack the following MD5 hashes (use the --list=formats
option to list all supported formats) . Show your steps and results.
1. 5f4dcc3b5aa765d61d8327deb882cf99 password
2. 63a9f0ea7bb98050796b649e85481845 root

I typed the first hash into a notepad. Saved it to home dir. Then John --format=raw-md5 filename.txt for it to crack the password.
The hash after cracked was " password
For the second hash repeat the steps.




root@CS2APenTest:~# john --format=raw-md5 extracredit2.txt
Using default input encoding: UTF-8
Loaded 1 password hash (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
Proceeding with incremental:ASCII
0g 0:00:00:02 3/3 0g/s 680555p/s 680555c/s 680555C/s th159..rocee
0g 0:00:00:03 3/3 0g/s 1728Kp/s 1728Kc/s 1728KC/s pjb311..sexandown
root   (?)
1g 0:00:00:03 DONE 3/3 (2023-11-23 08:07) 0.3125g/s 1759Kp/s 1759Kc/s 1759KC/s rome..rams
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@CS2APenTest:~# john --show --format=Raw-MD5 extracredit2.txt
?:root
1 password hash cracked, 0 left
root@CS2APenTest:~#