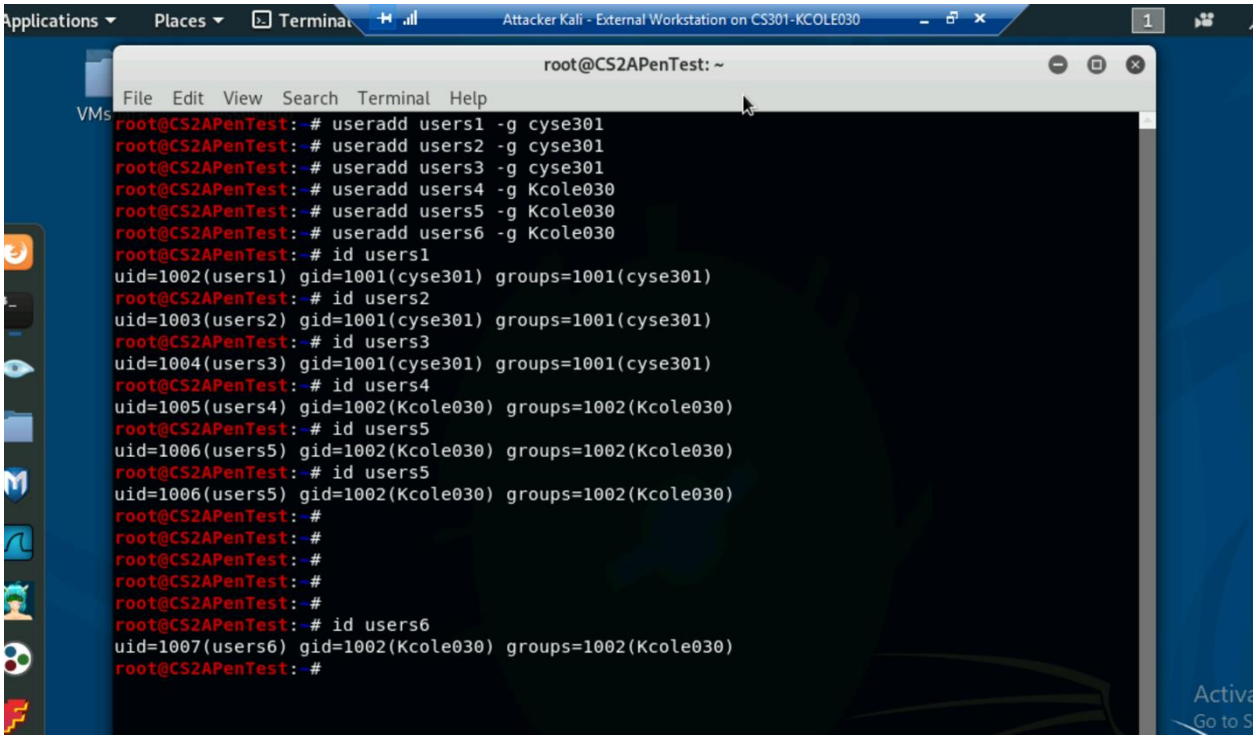
CYSE 301: Cybersecurity Technique and Operations

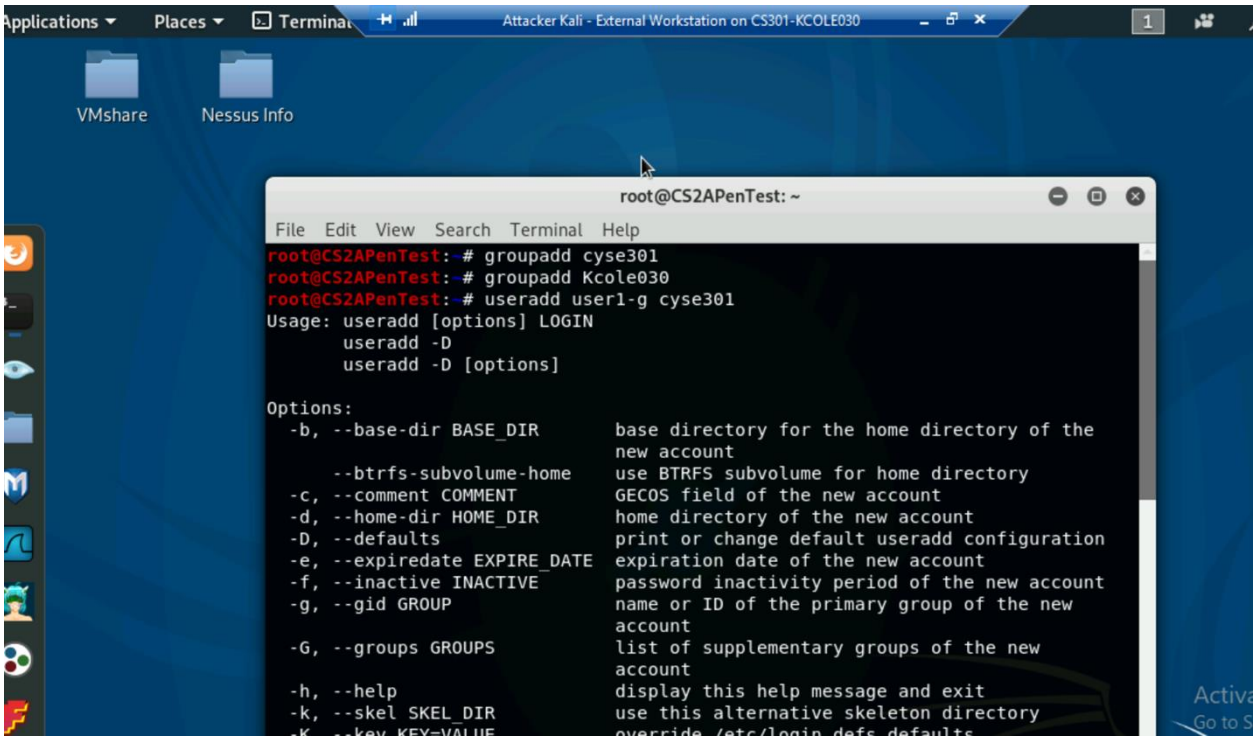
Assignment 4: Password Cracking (Part A)

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

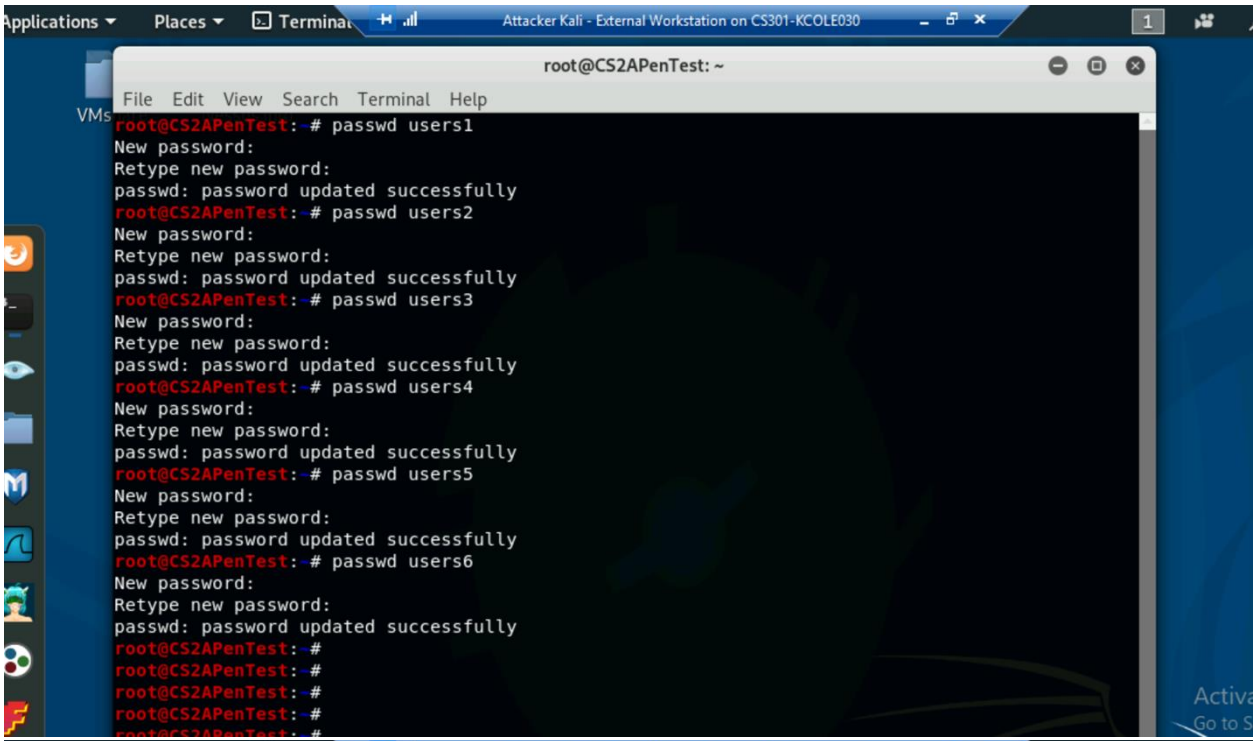
Task A: Linux Password Cracking (25 points)

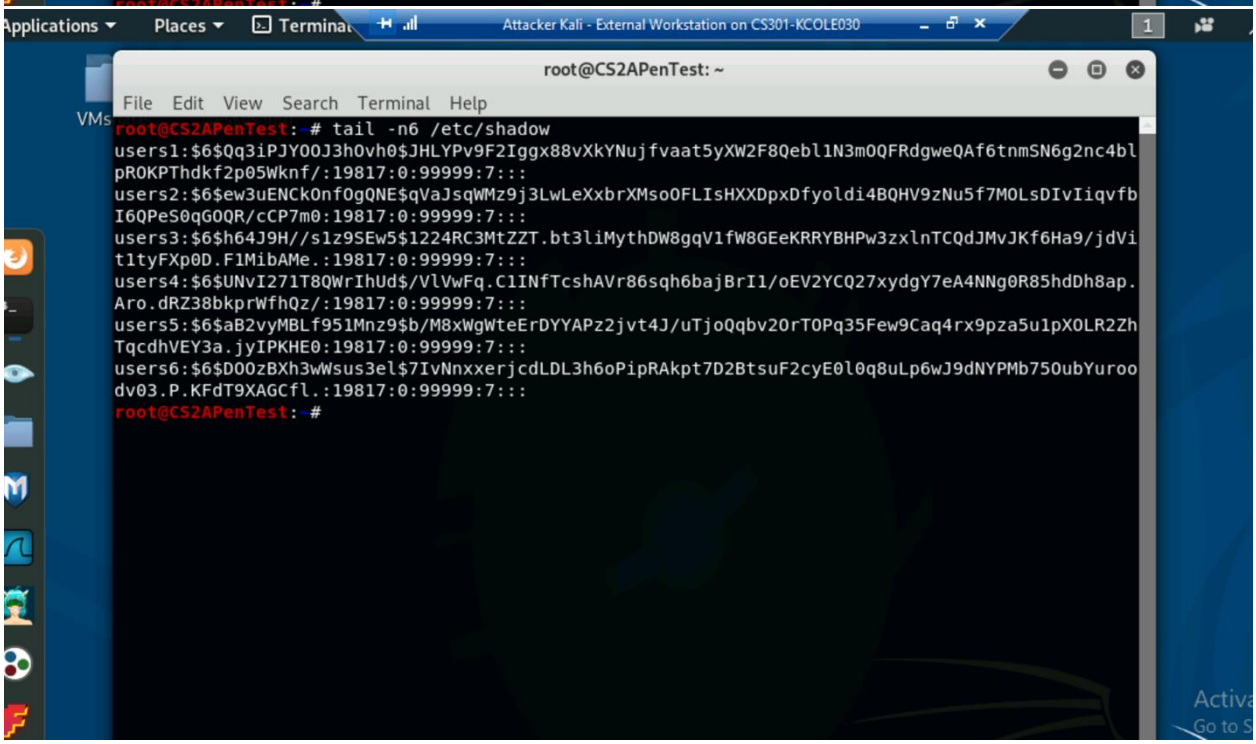
1. **5 points.** Create two groups, one is **cyse301s23**, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.



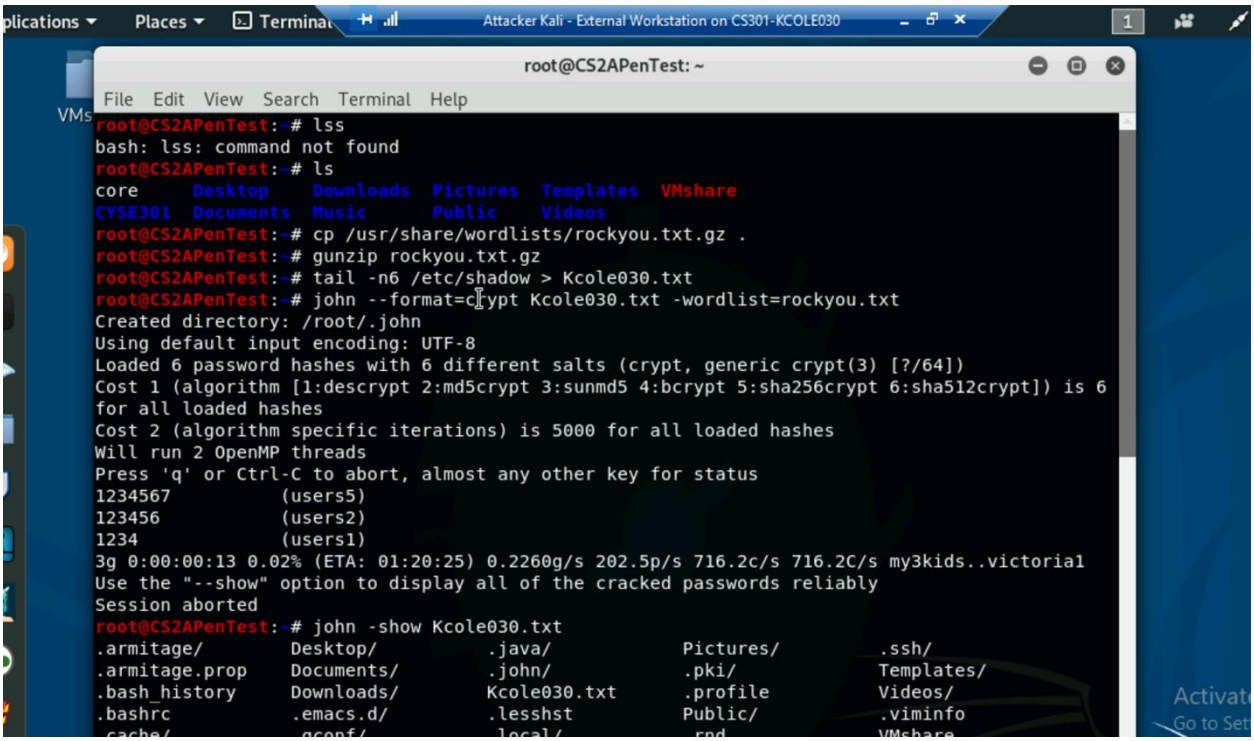


2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.

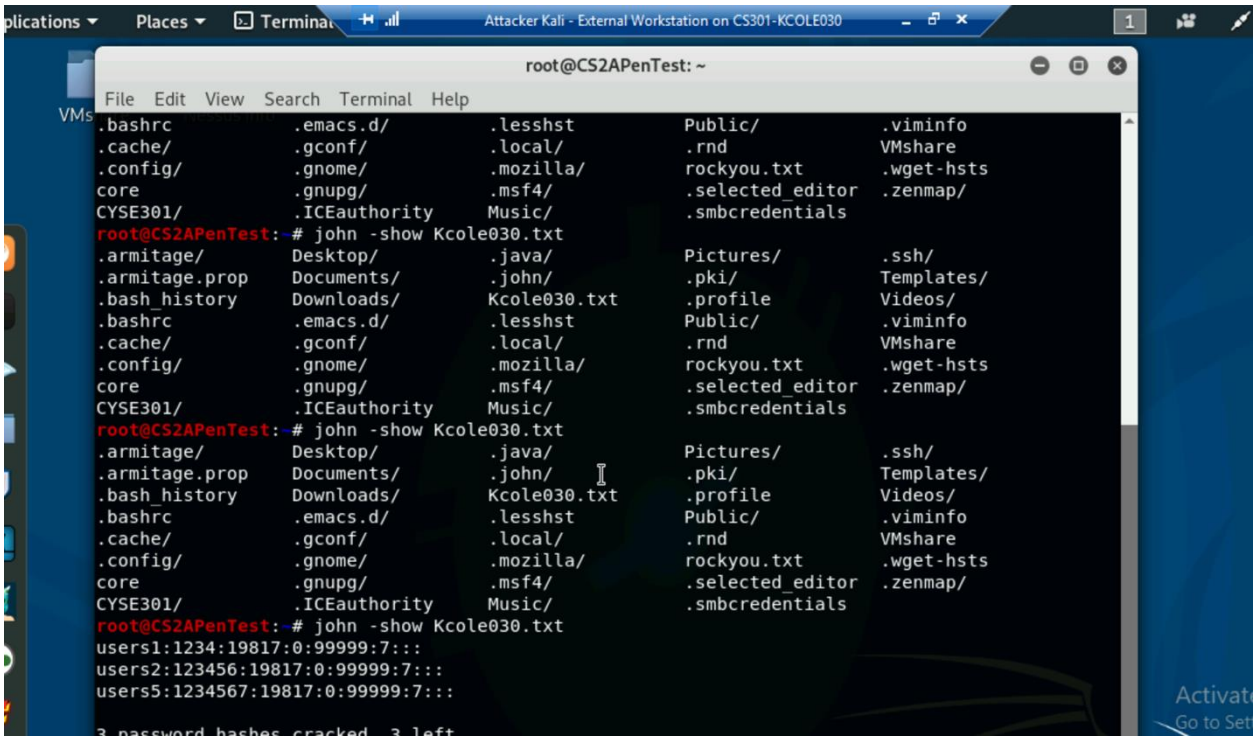




3. **5 points.** Choose six new passwords, **from easy to hard**, and assign them to the users you created. You need to show me the password you selected in your report, and **DO NOT** use your real-world passwor



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.



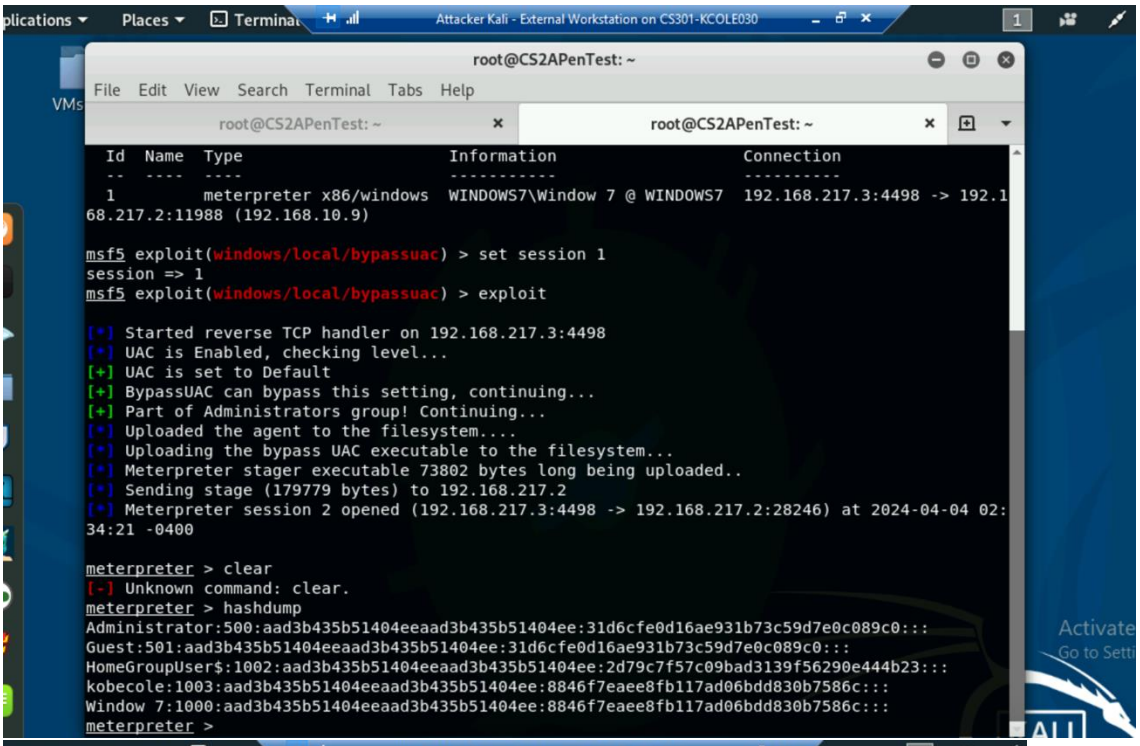
Task B: Windows Password Cracking (25 points)

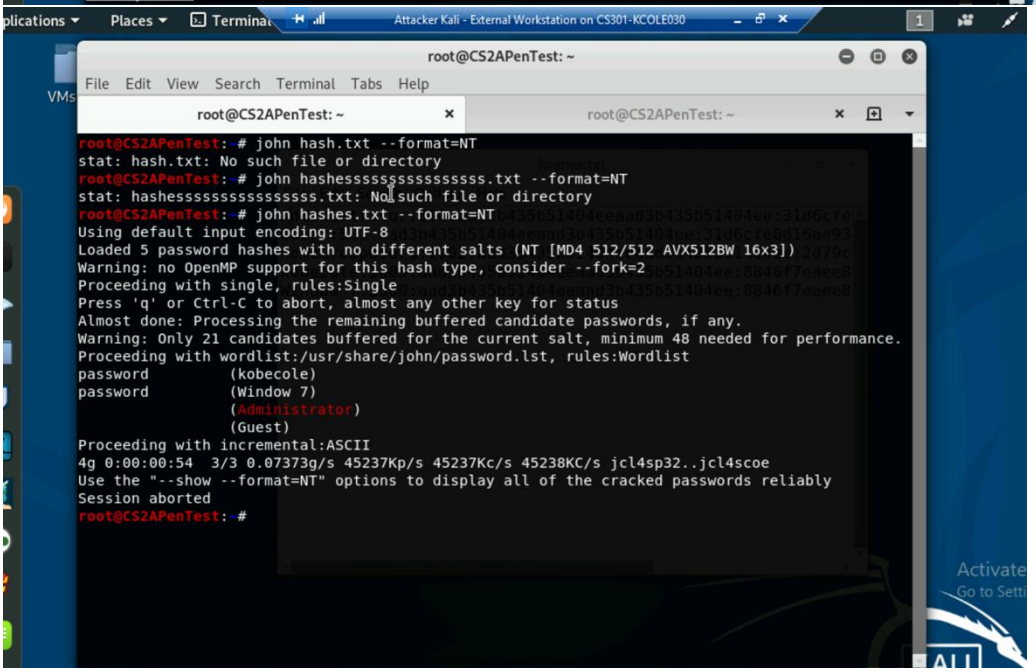
Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to establish

a reverse shell connection with the admin privilege to the target Windows 7 VM.

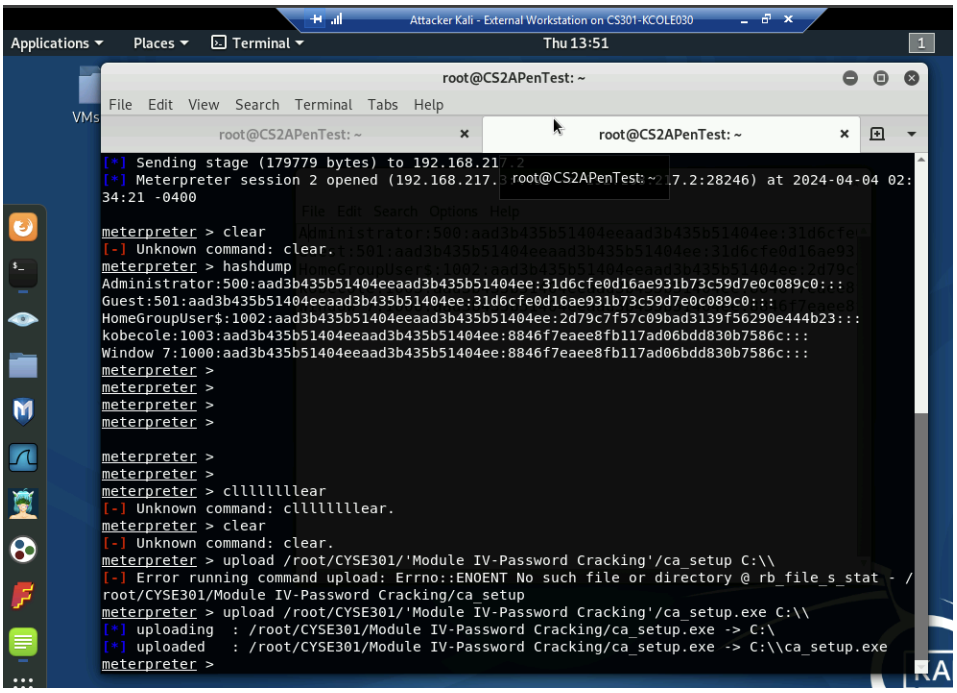
Now, complete the following tasks:

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

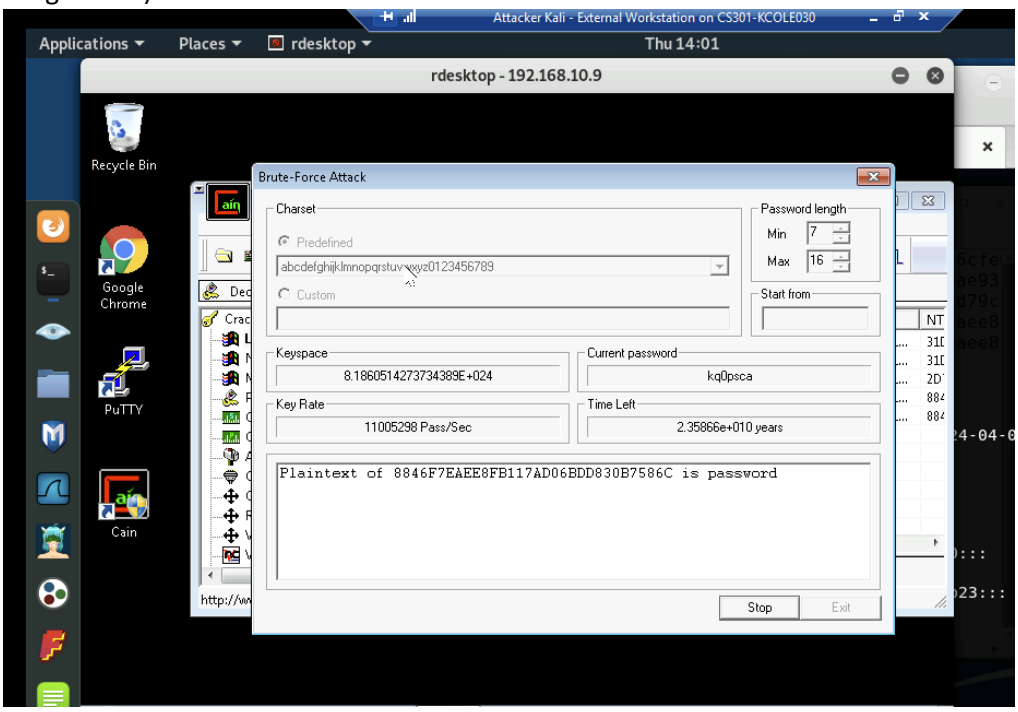


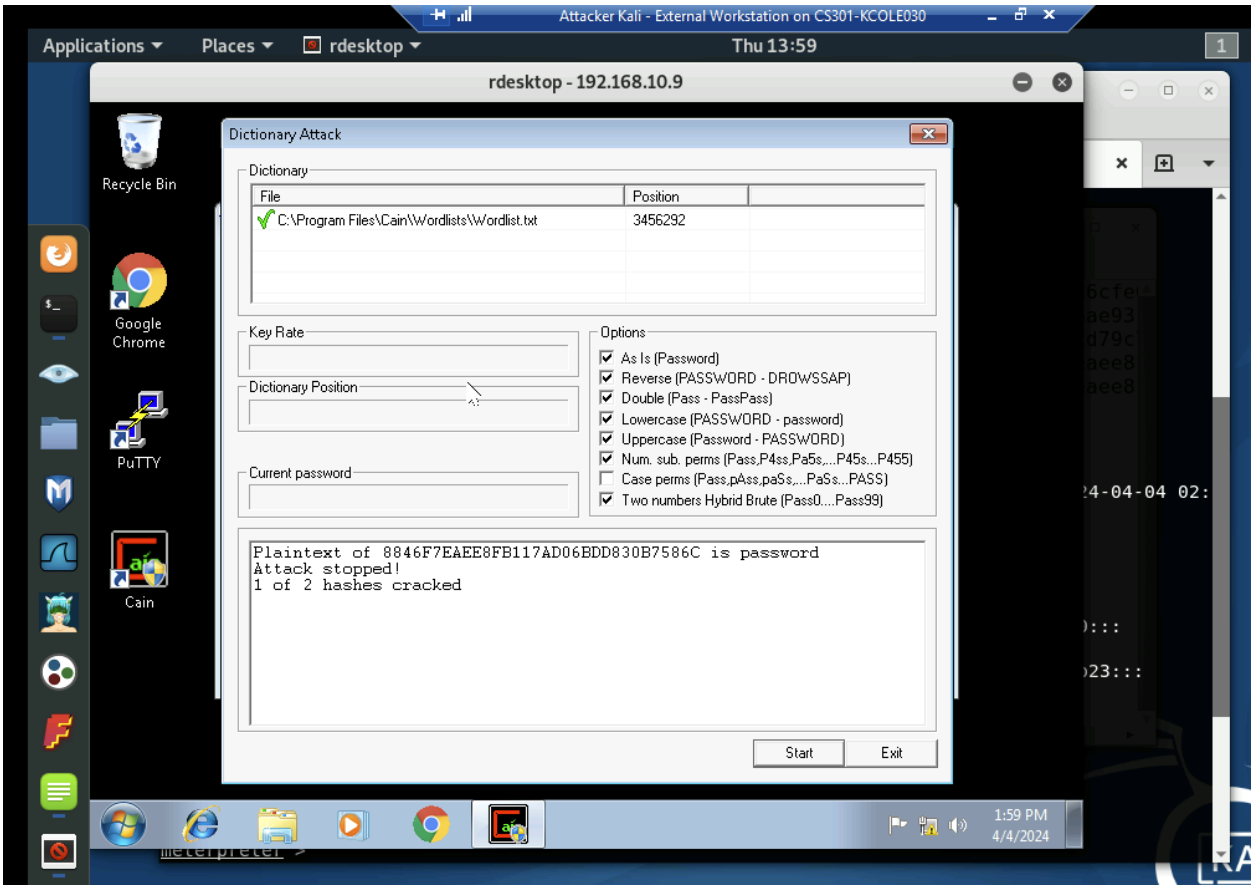


2. **10 points.** Save the password hashes into a file named "**your_midas.WinHASH**" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run John the ripper for **10 minutes** to crack the passwords (You MUST crack at least one password in order to complete this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



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
2. 63a9f0ea7bb98050796b649e85481845