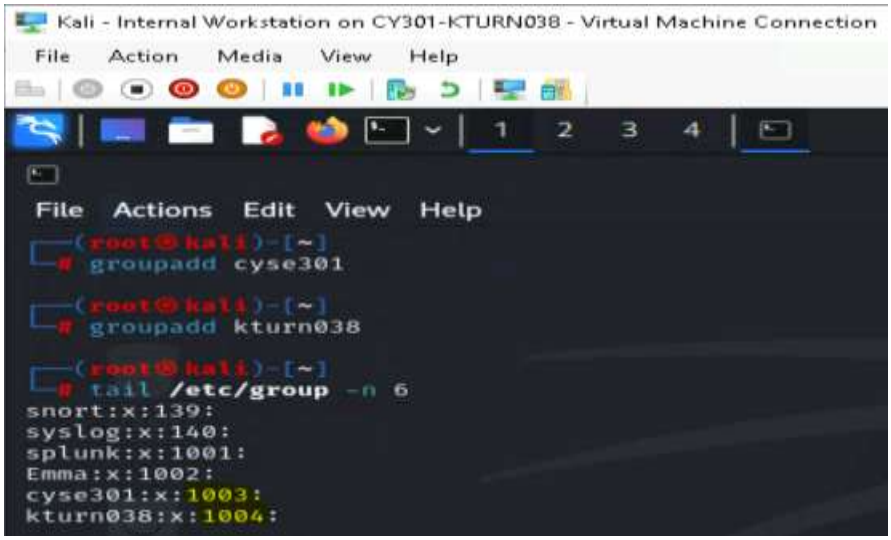
CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking (Part A)

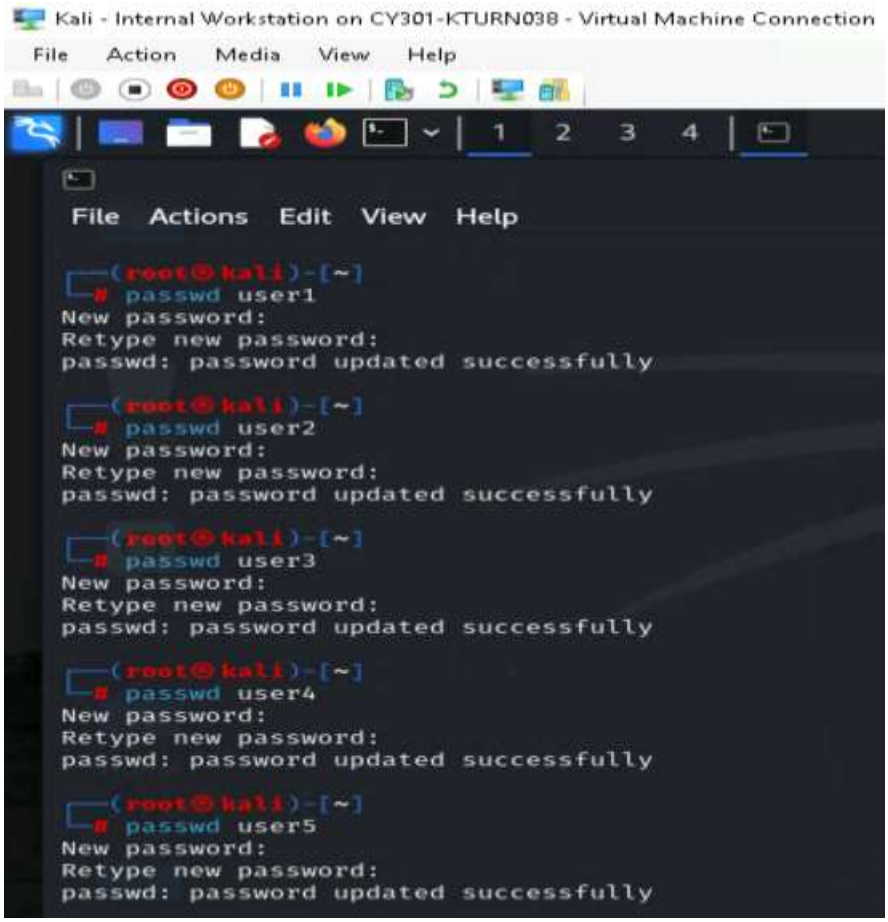
Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). 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 Three 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.



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

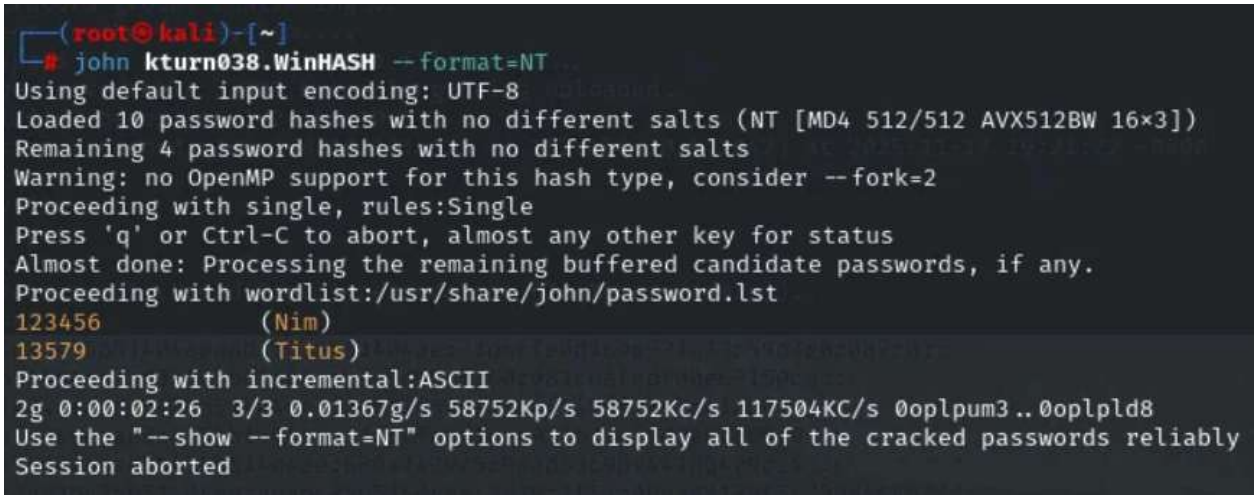
Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords (OR you may create users using net users \add command as you did in lab-4-task-c). Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

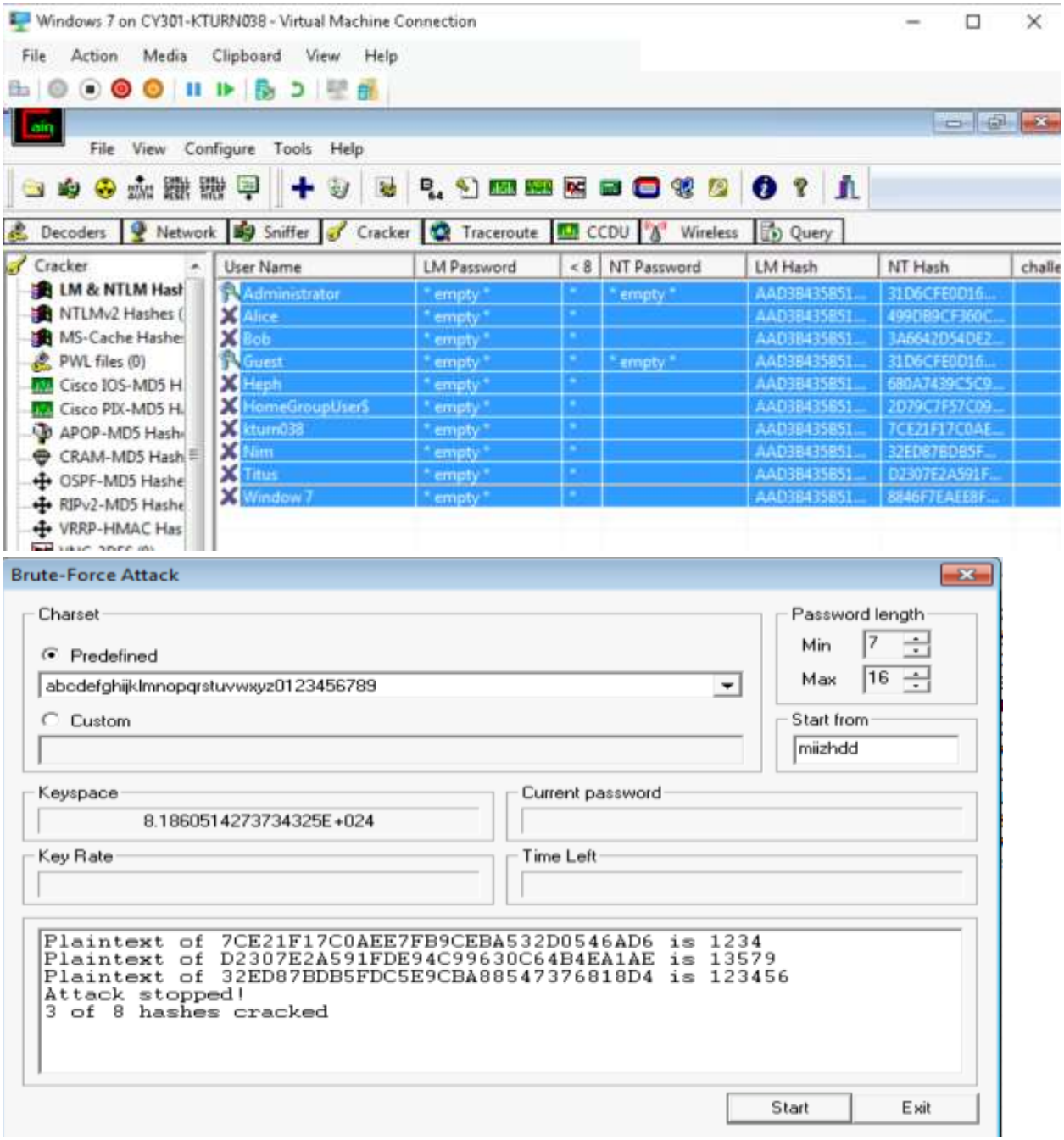
Now, complete the following tasks:

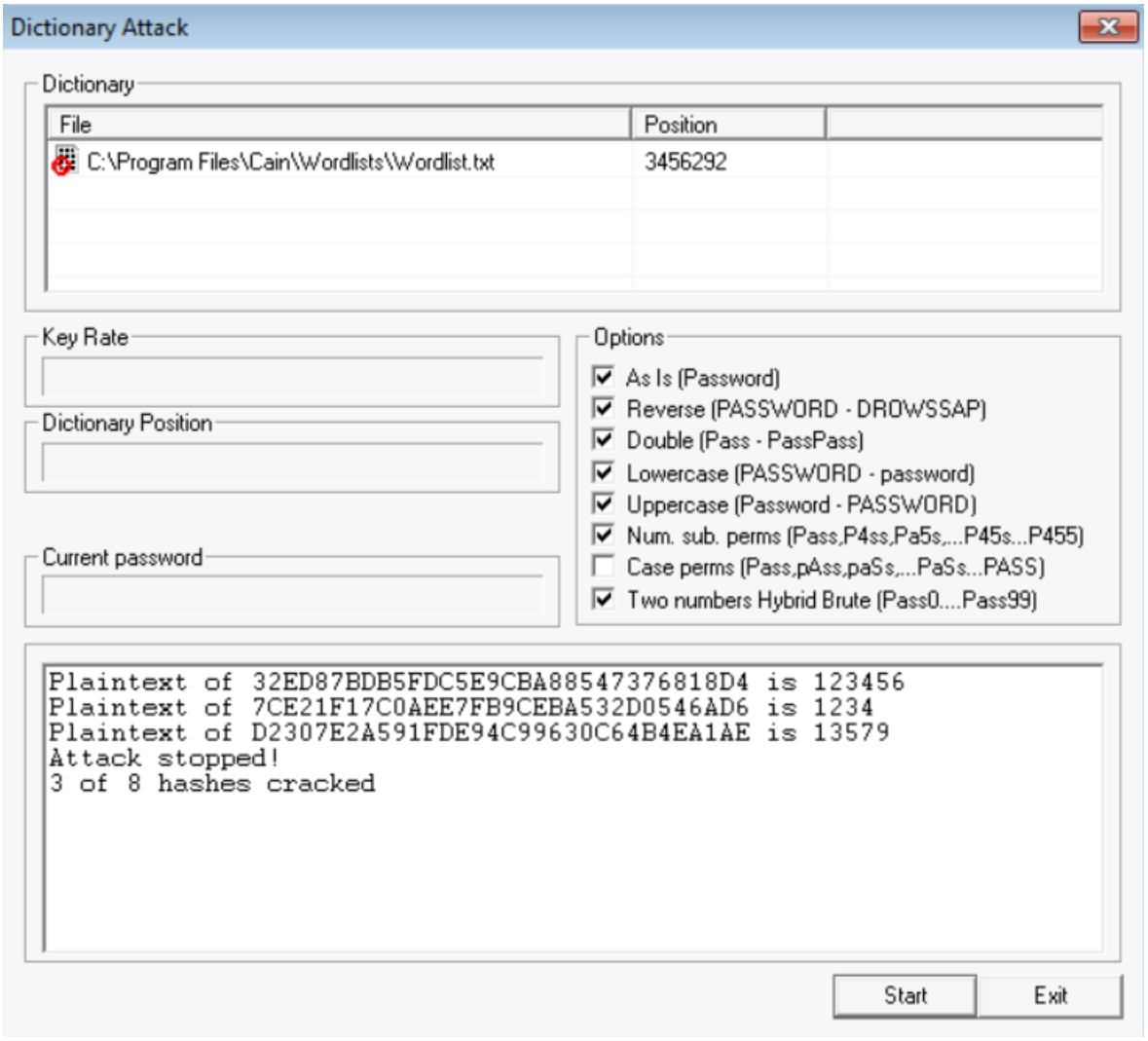
1. **5 points.** Display the password hashes by using the "hashdump" command in the meterpreter shell. Then

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 windows users' passwords (You MUST crack at least one password in order to complete this assignment.).



3. 10 points. Launch/open the password cracking tool, **Cain and Abel** in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).




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 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Plaintext of 7CE21F17C0AEE7FB9CEBA532D0546AD6 is 1234
Plaintext of D2307E2A591FDE94C99630C64B4EA1AE is 13579
Attack stopped!
3 of 8 hashes cracked
Start
Exit