OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4

Kilah Summer 2020

Module 4: Password Cracking

Task A:

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).**

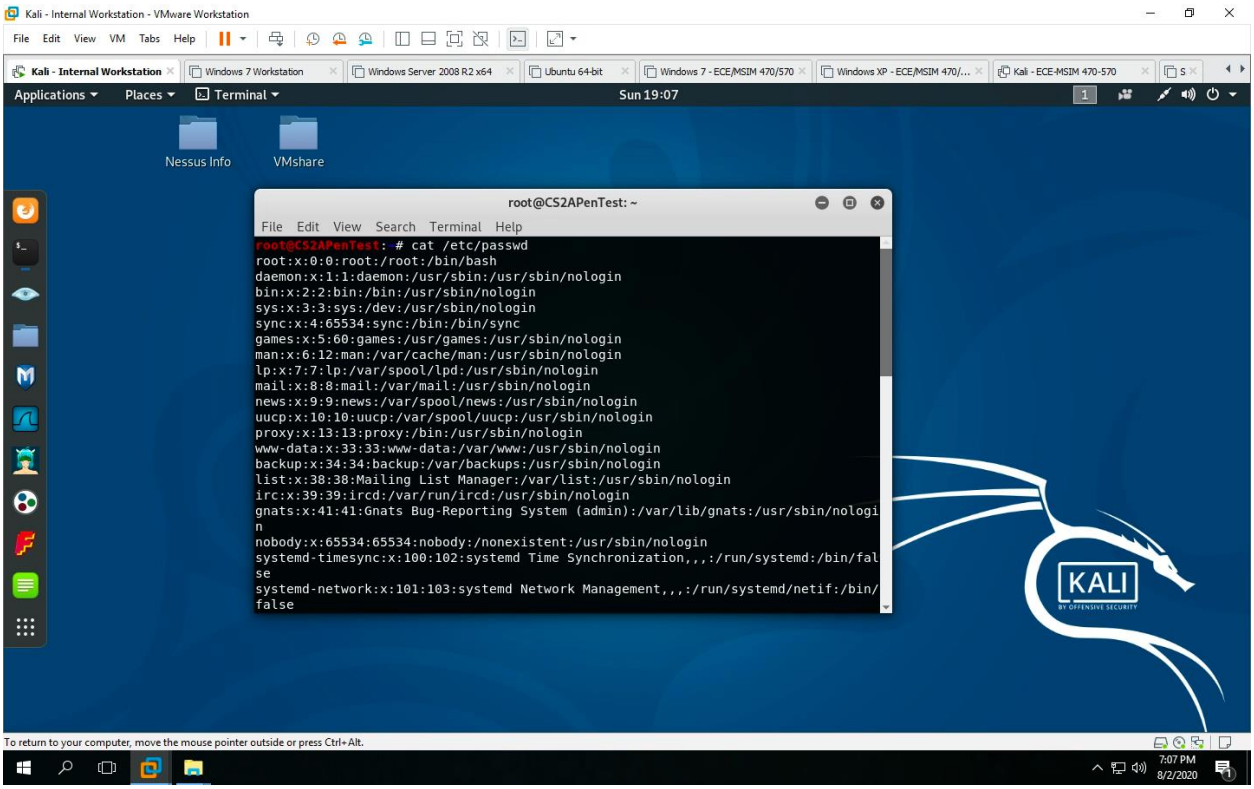


figure 4.1 Using the command #***cat /etc/passwd***

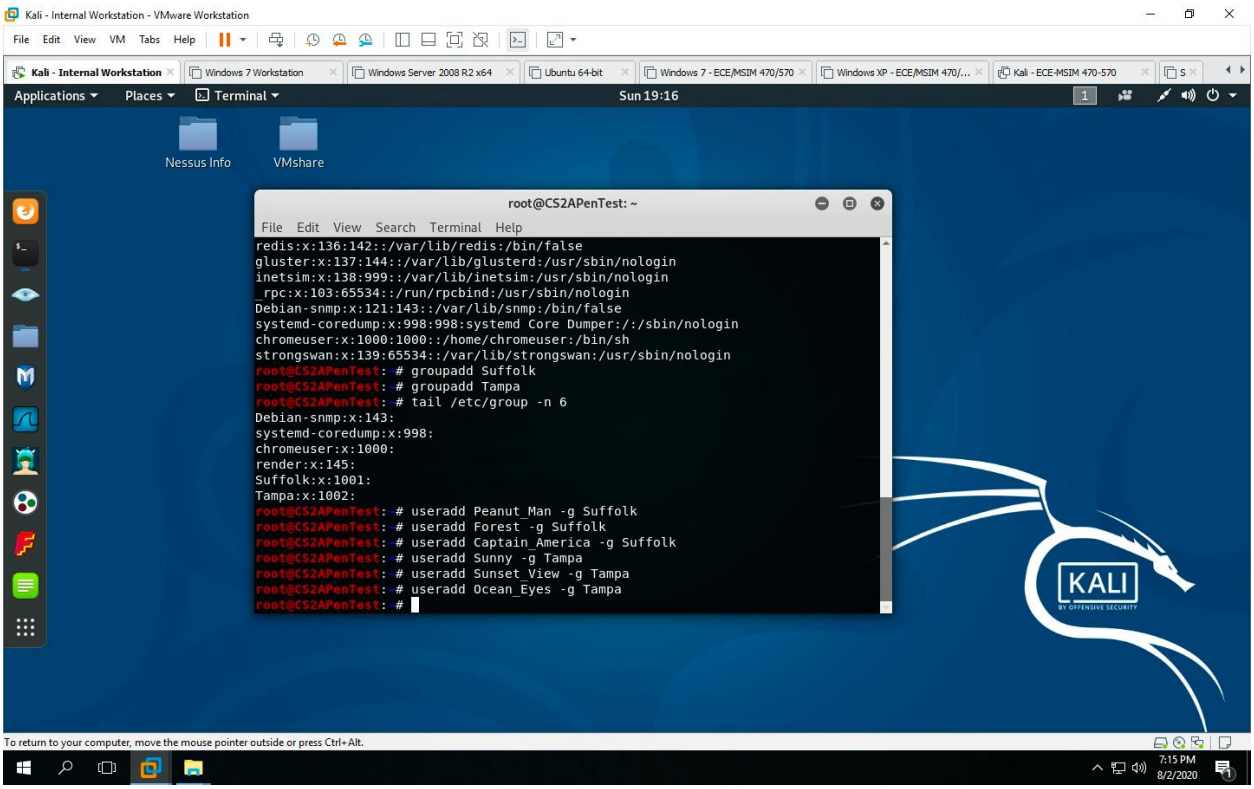


Figure 4.2 Adding three users to two groups each

- I used the **command *useradd Peanut_Man -ig Suffolk*** to add a user to the Suffolk group

Suffolk Tampa

Username	**Password**		**Username**	**Password**
Peanut_Man	123123		Sunny	2welcome
Forest	123456789		Sunset_View	academic
Captain_America	1sarjose		Ocean_Eyes	acapulco

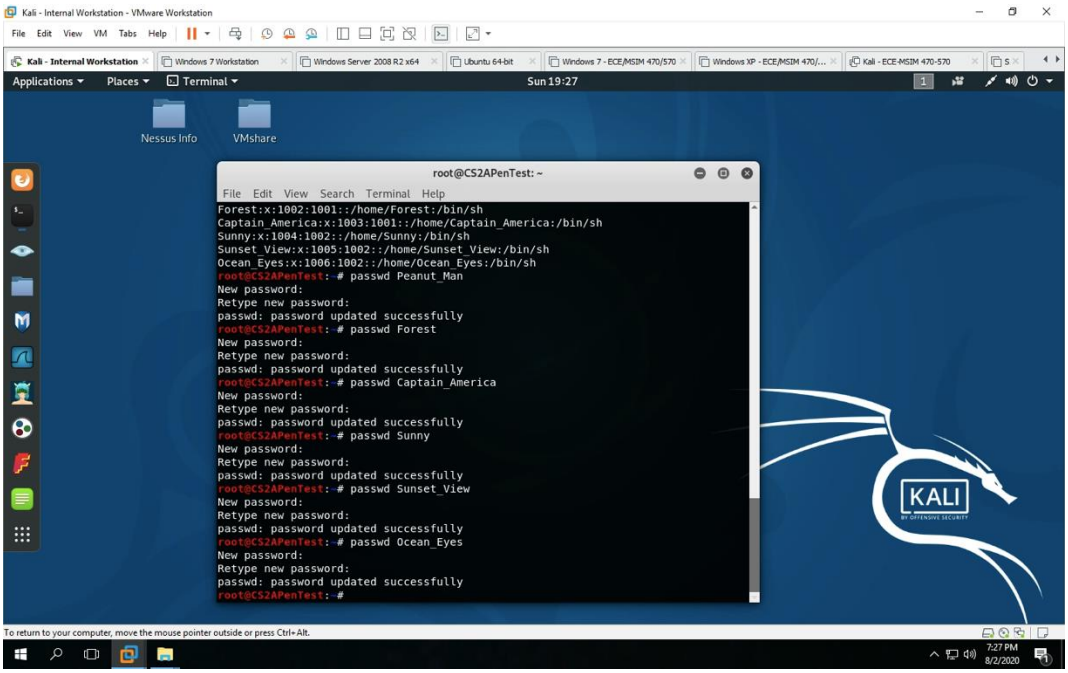


Figure 4.3 Password added to each user using command ***passwd***

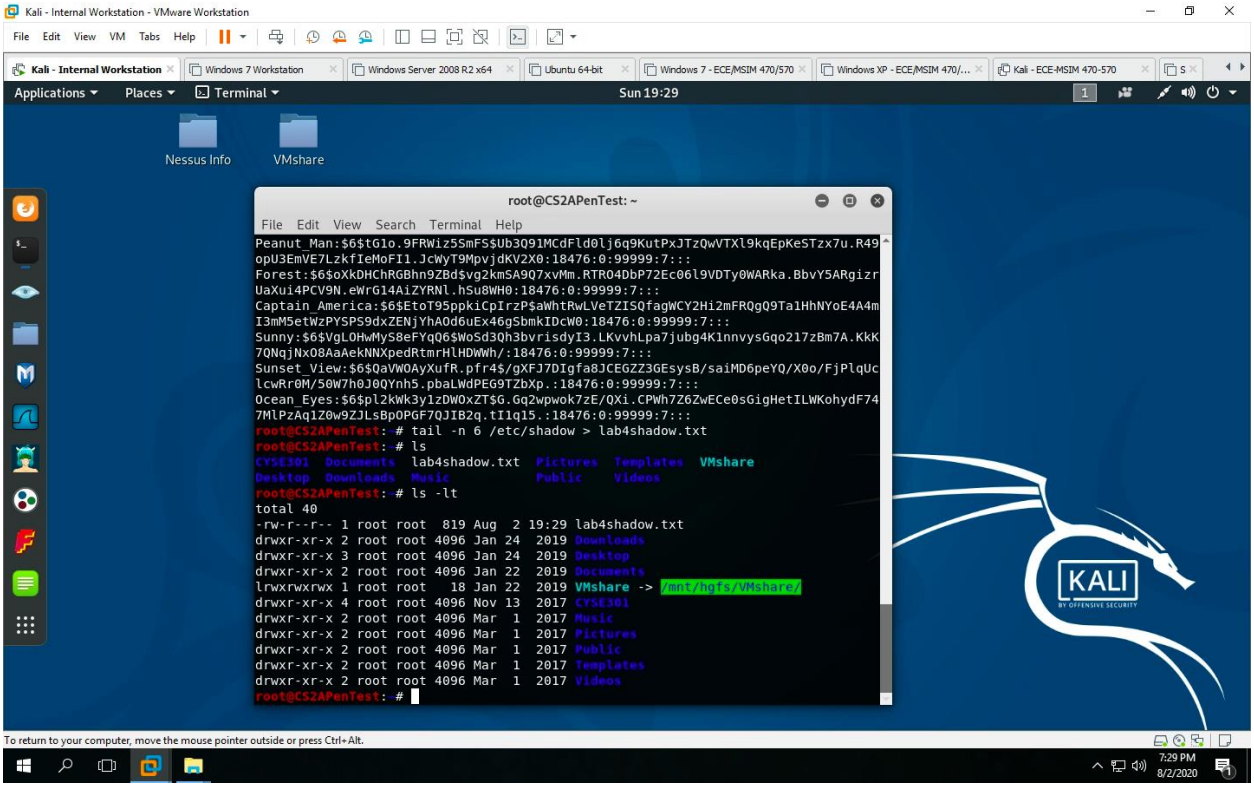


Figure 4.4 Saved and exported shadow file

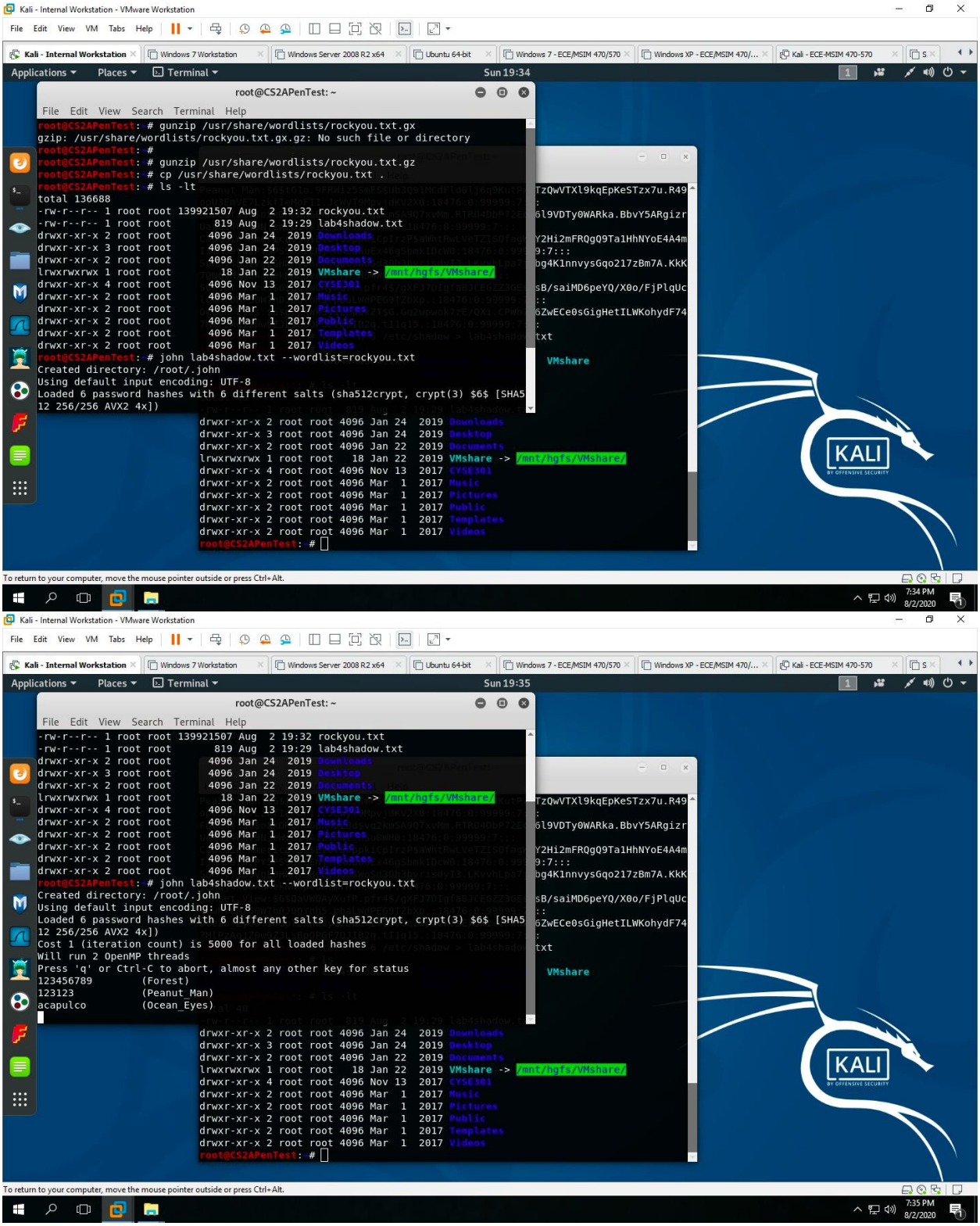


Figure 4.5 Starting John Attack

- used command #***john lab4shadow.txt --wordlist=rockyou.txt*** to retrieve passwords.

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).**

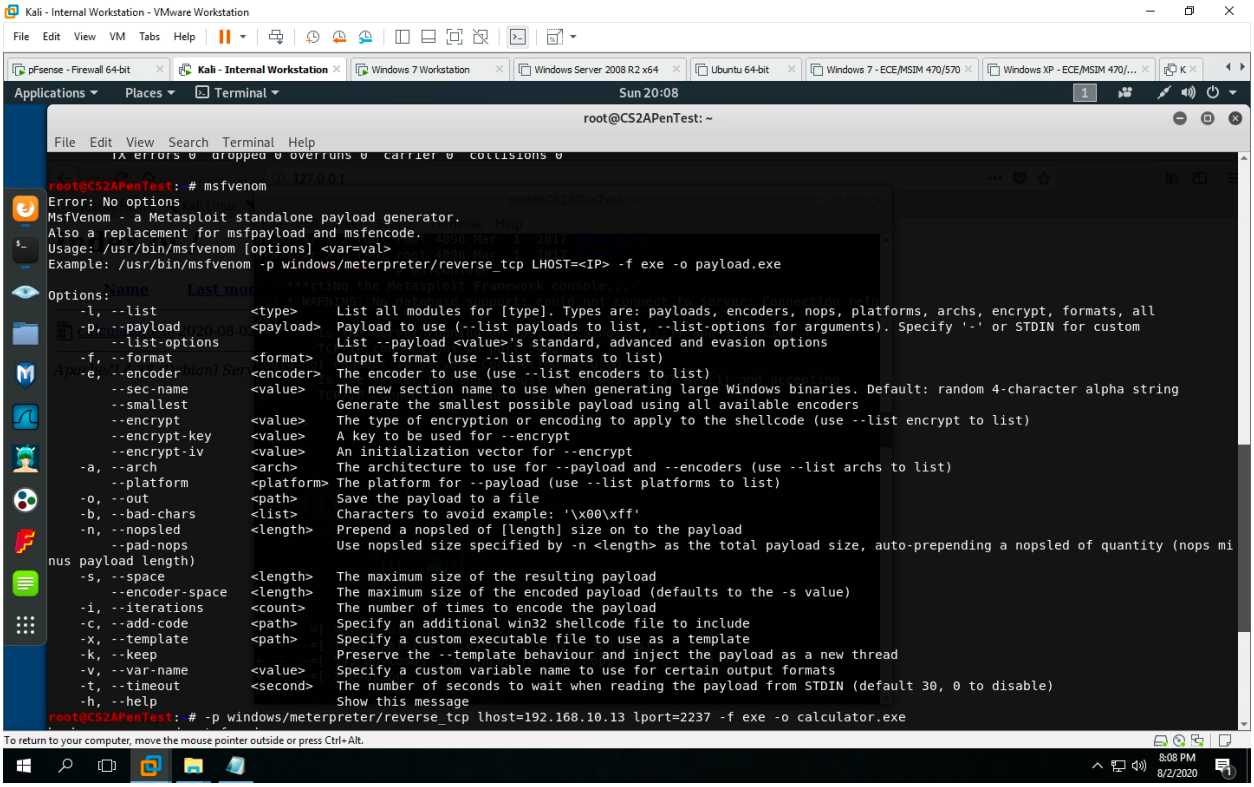


Figure 4.6 Used ***msfvenom*** to establish a reverse shell connection with Windows 7

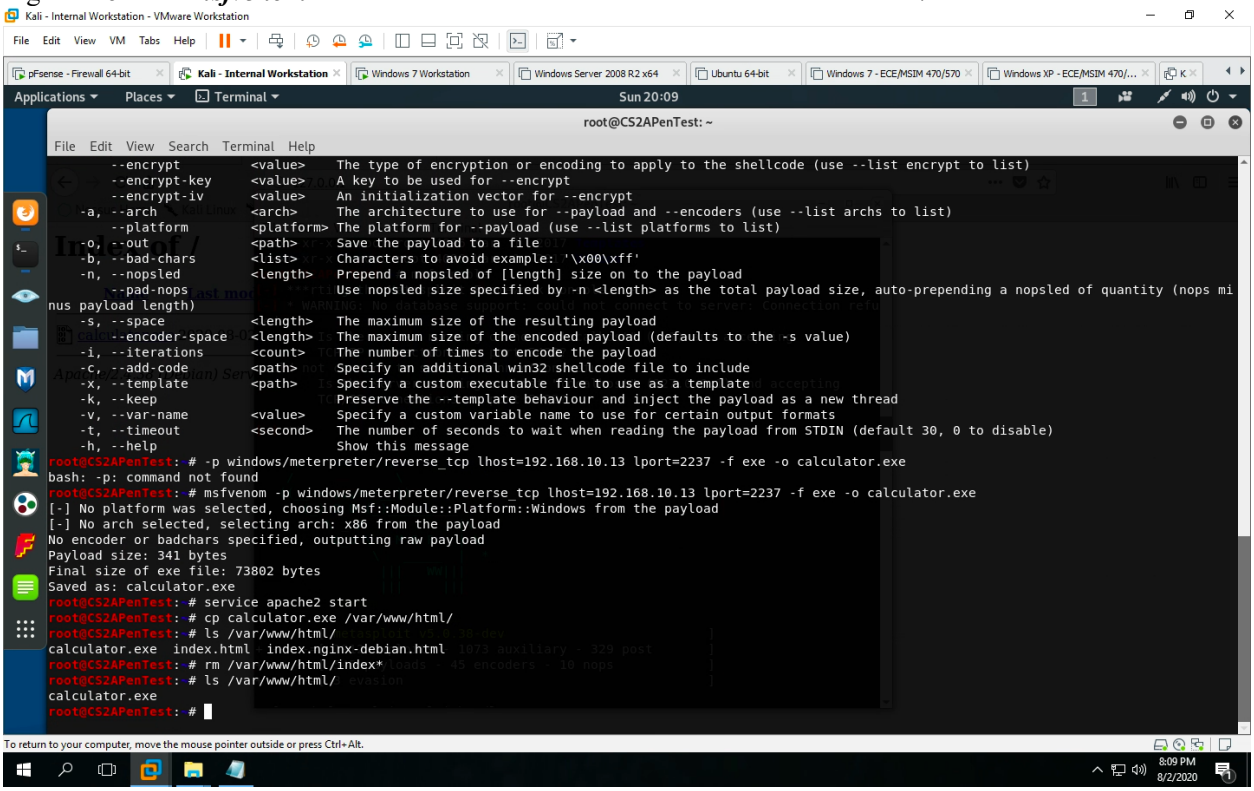


Figure 4.7 Created malicious file for target machine to download (Windows 7)

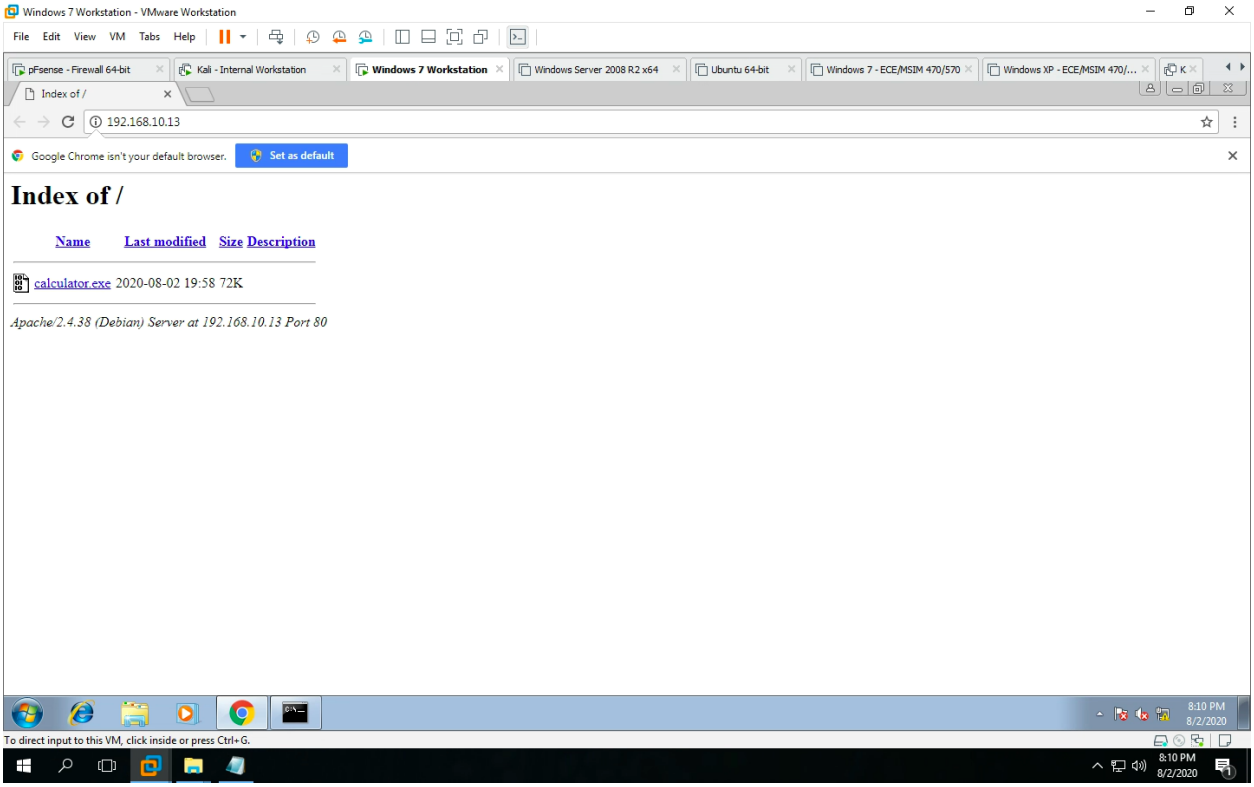


Figure 4.8 Downloaded and ran malicious file on Windows 7 to begin exploit from Internal Kali

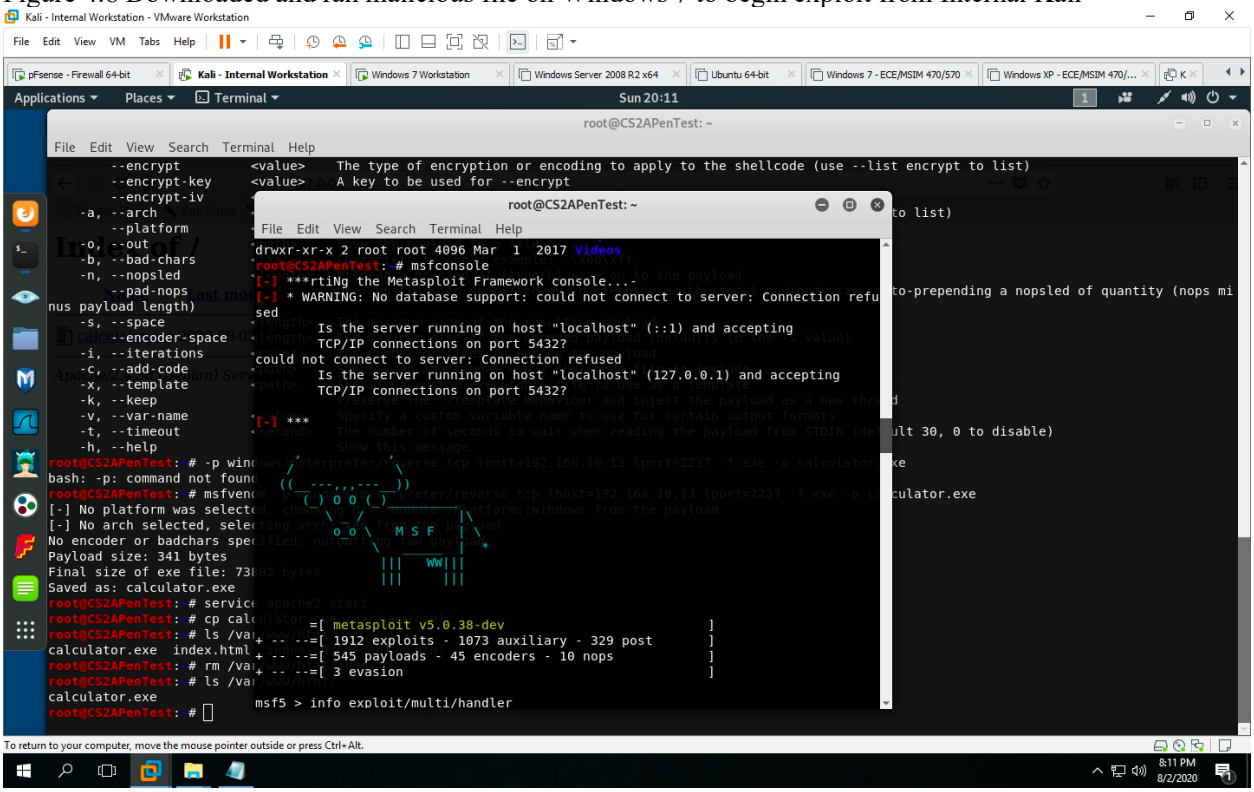


Figure 4.9 continued to use command ***msfconsole*** to exploit Windows 7

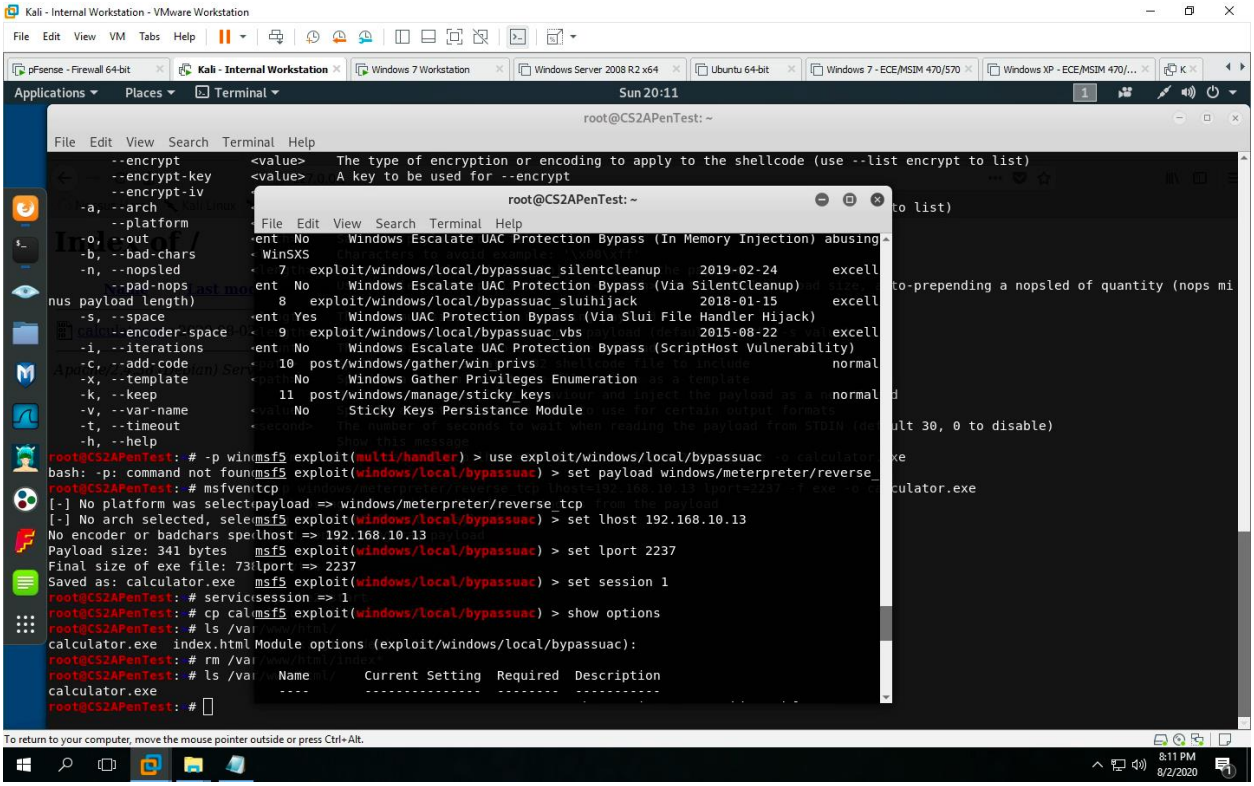


Figure 4.10 bypassed uac to gain administrative access to Windows 7

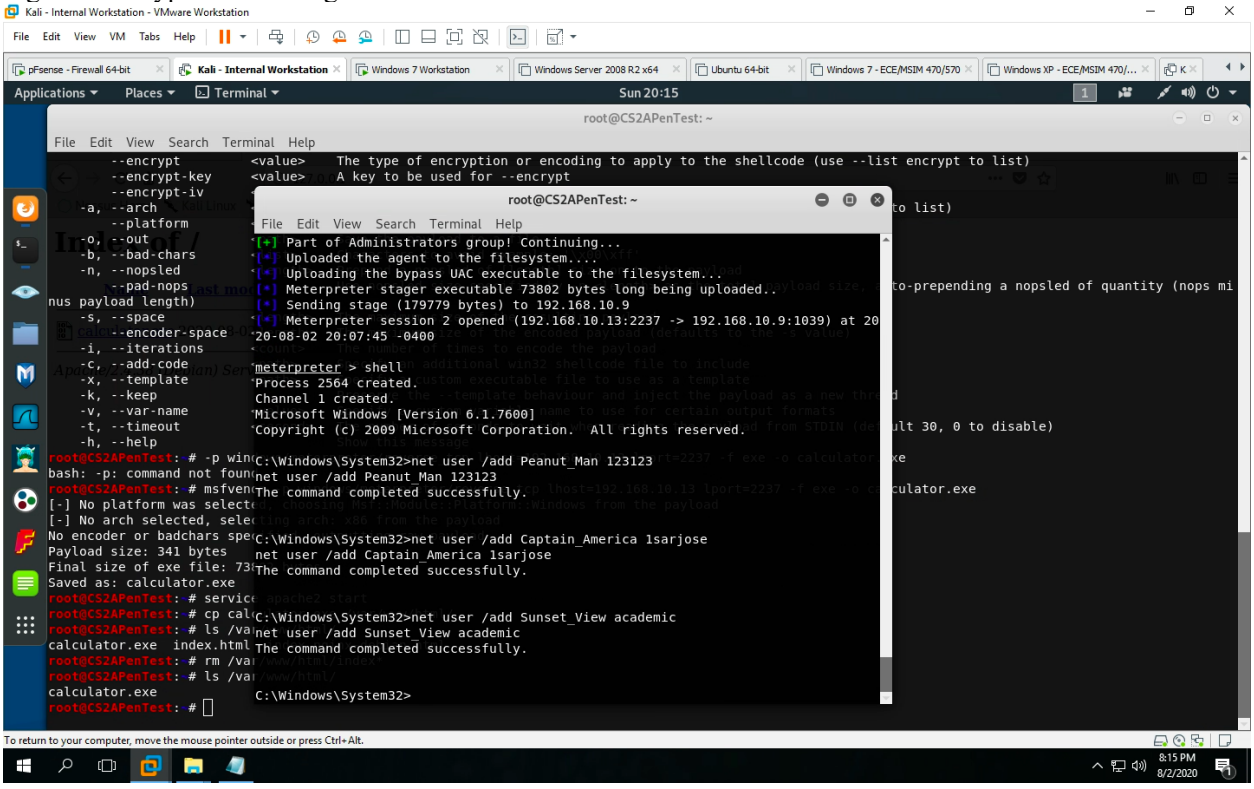


Figure 4.11 Administrative access gained and three users created using command ***net user /add***

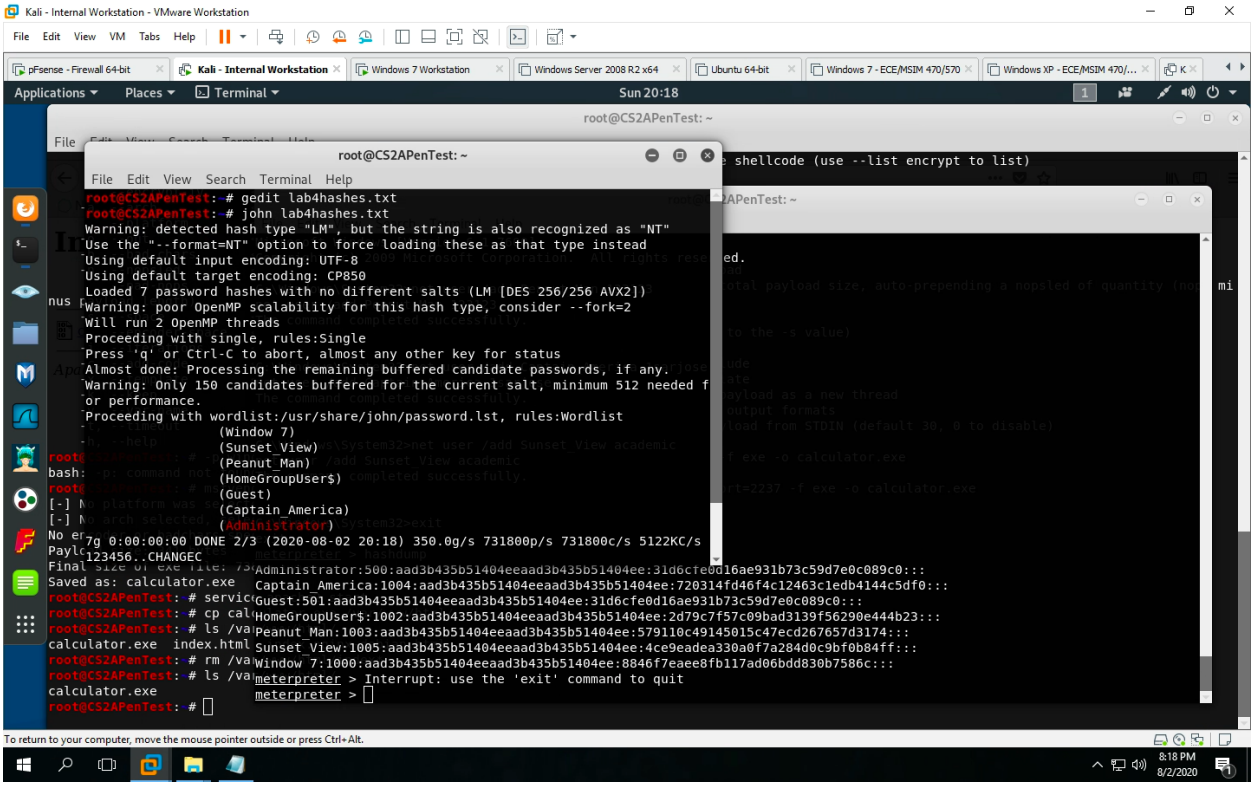


Figure 4.12 Used command ***gedit lab4hashes.txt*** to create a file for the hashes

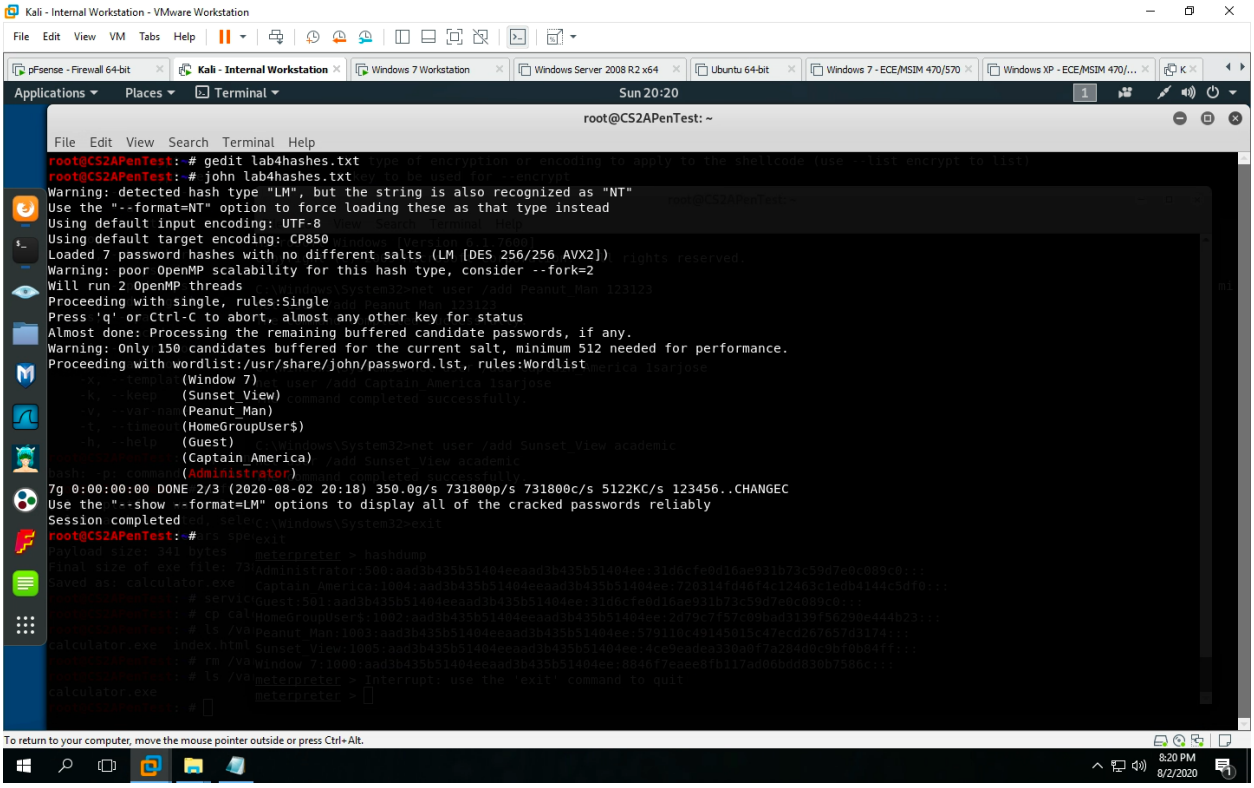


Figure 4.13 Used command ***john lab4hashes.txt*** to John the Ripper crack the passwords

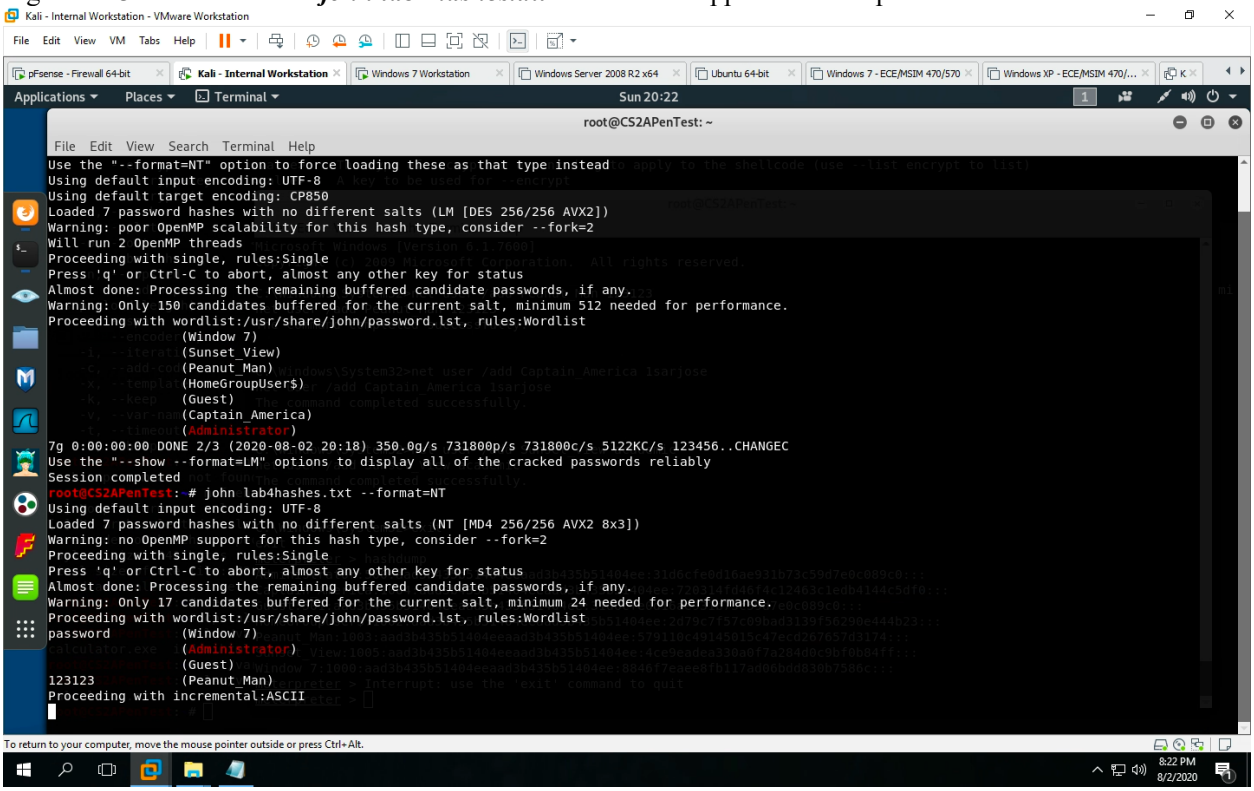


Figure 4.14 Password successfully cracked using John the Ripper for Peanut Man

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).**

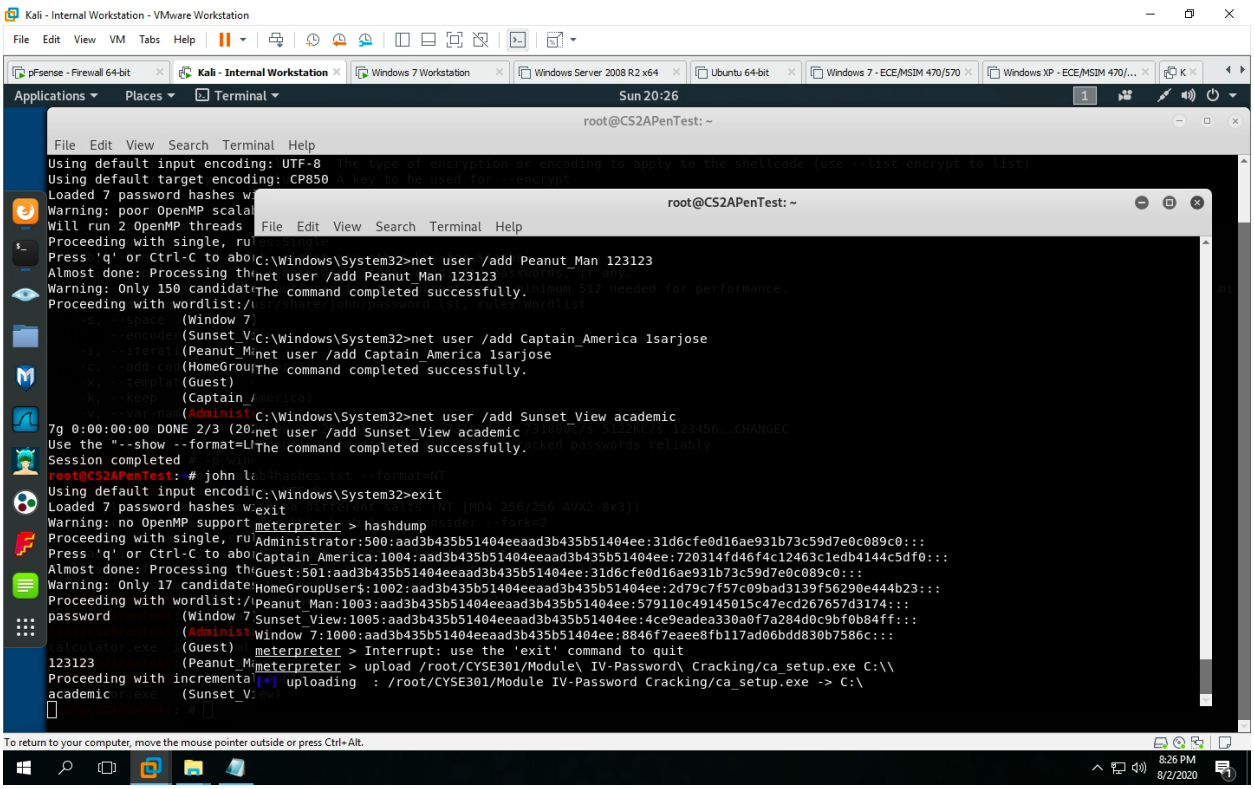


Figure 4.15 Install Cain

- I used command ***meterpreter > upload /root/CYSE301/Module\ IV-Password\ Cracking/ca_setup.exe C:*** to install Cain

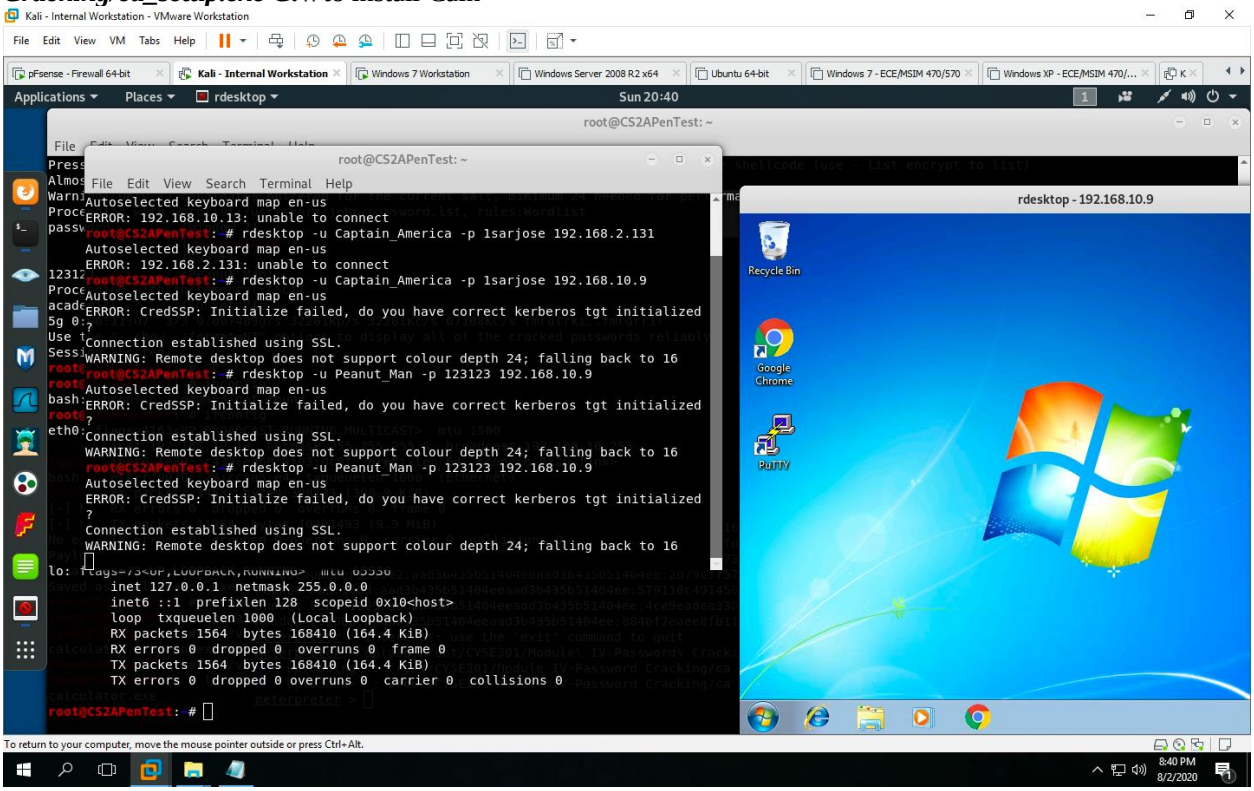


Figure 4.16 Remote Desktop established (after multiple attempts)

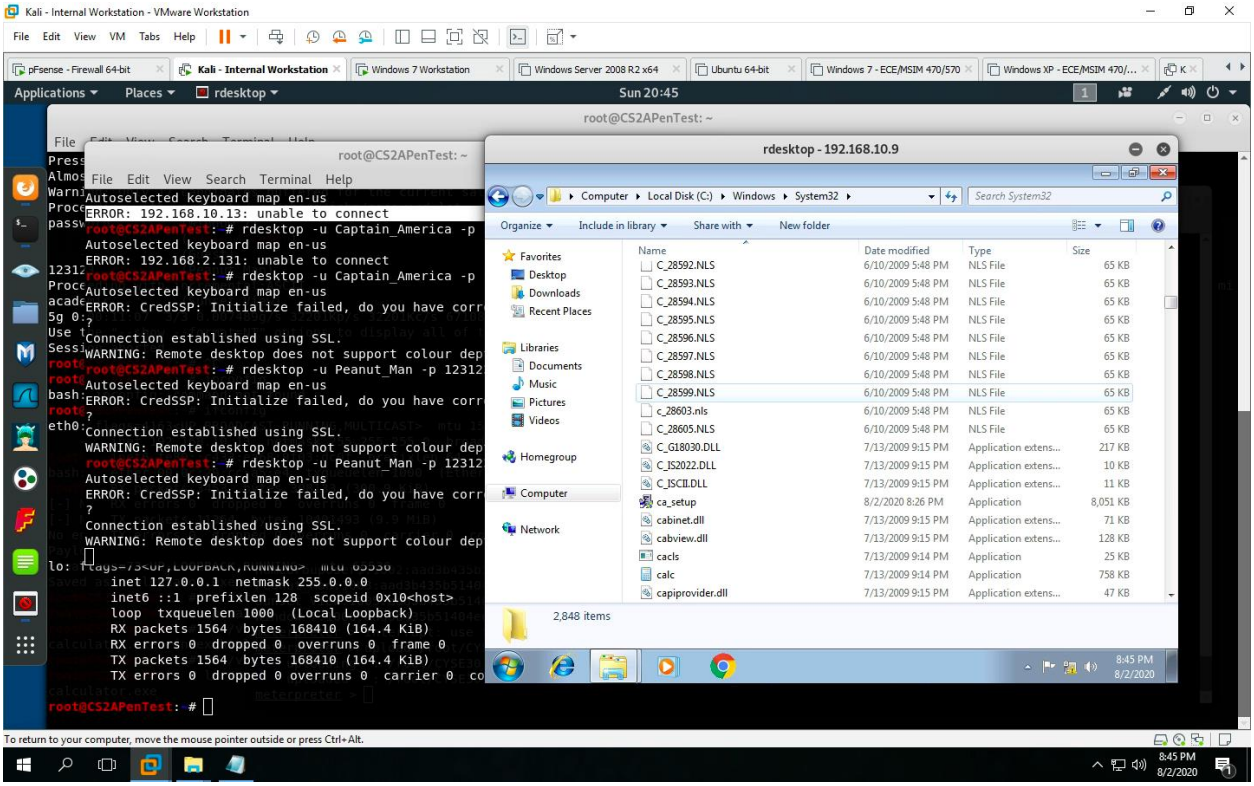


Figure 4.17 Installing CA_Setup

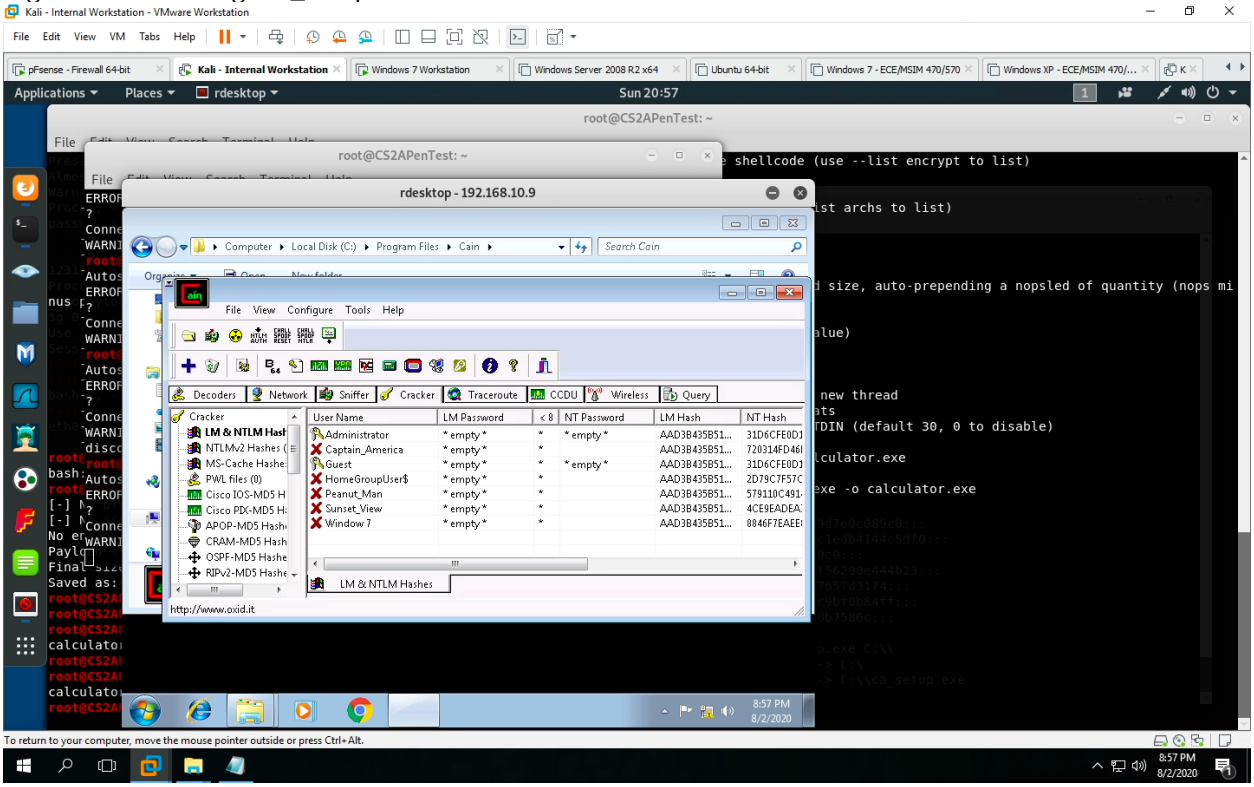


Figure 4.18 Cain displaying usernames

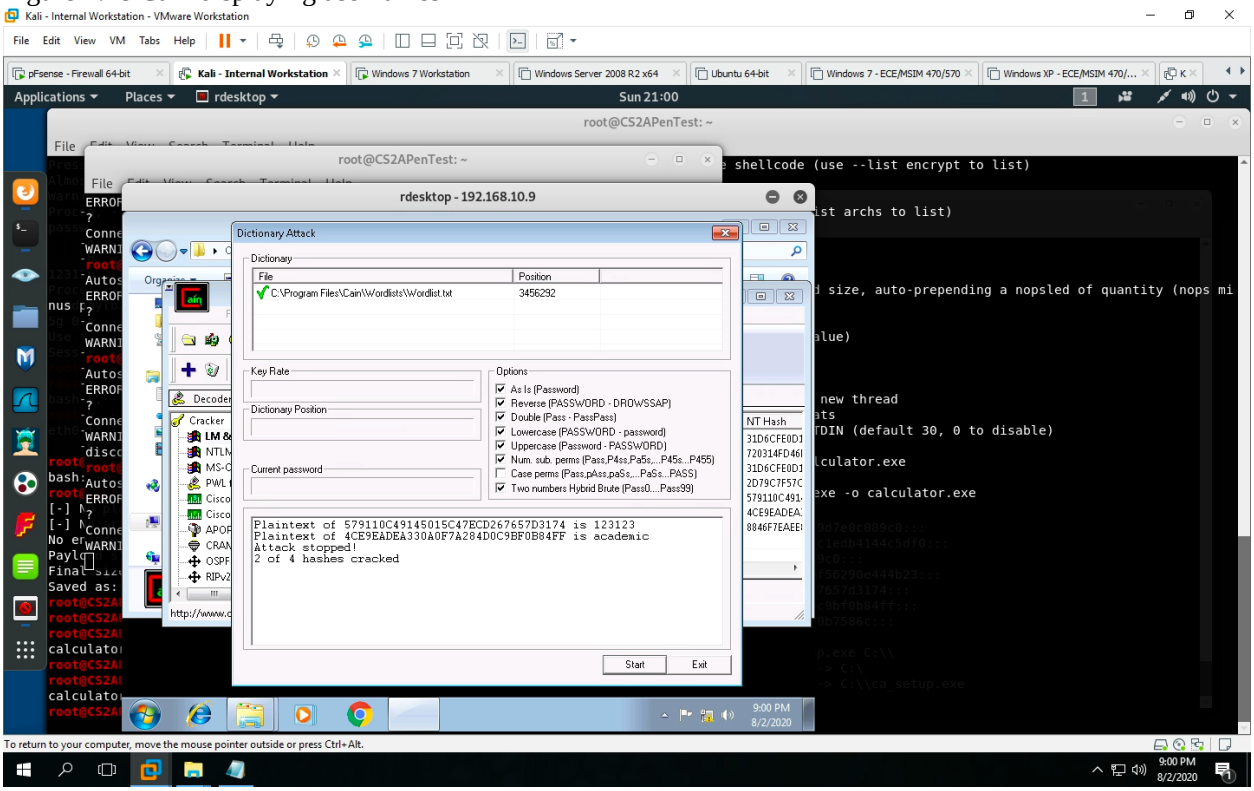


Figure 4.19 Used Dictionary attack to crack passwords

Task B: 10 points + 10 points (Bonus)

In this assignment, you will need to decrypt an MD5 cipher (10 points) **and an encrypted ZIP file** (10 extra points) **in order to get full credits.**

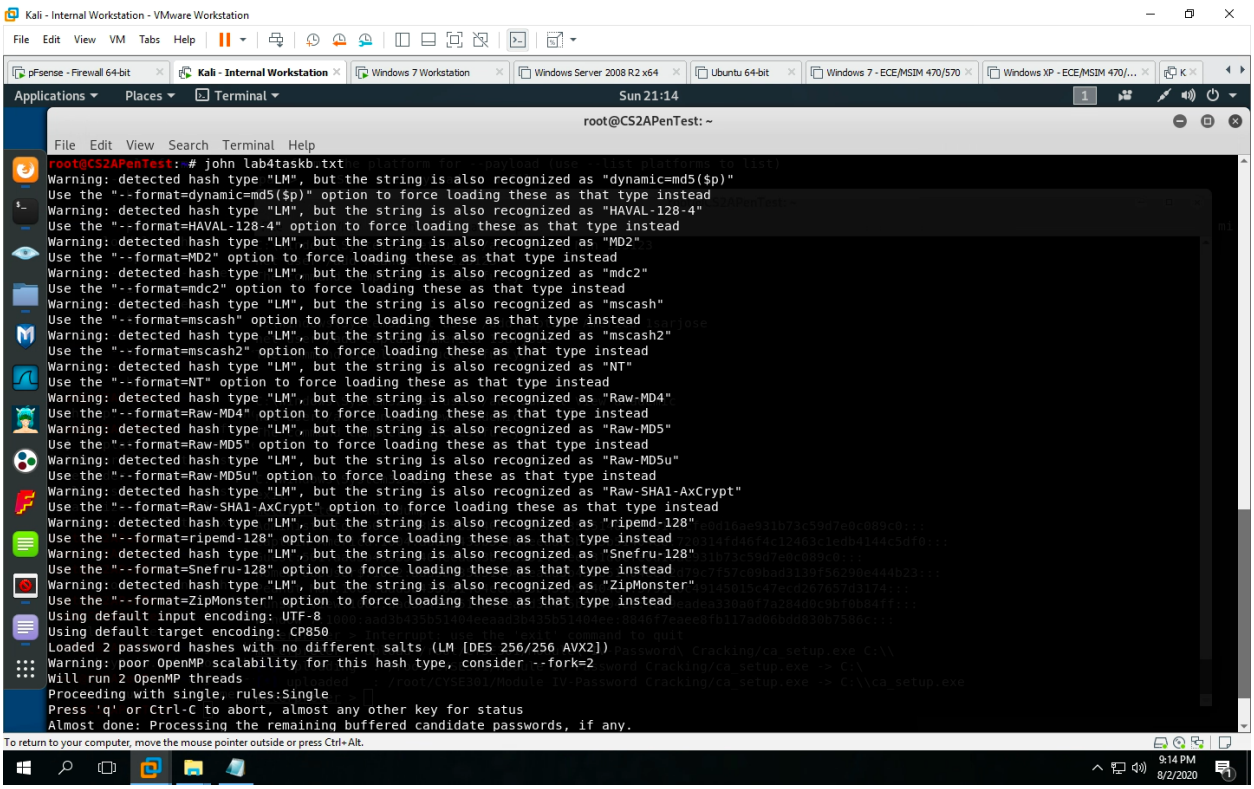


Figure 4.20 John the Ripper without Format

I used the command ***gedit*** to create a file for the key2zip.txt and copied/pasted into new file *lab4taskb.txt*

- I then used John the Ripper to attempt to decrypt the passwords

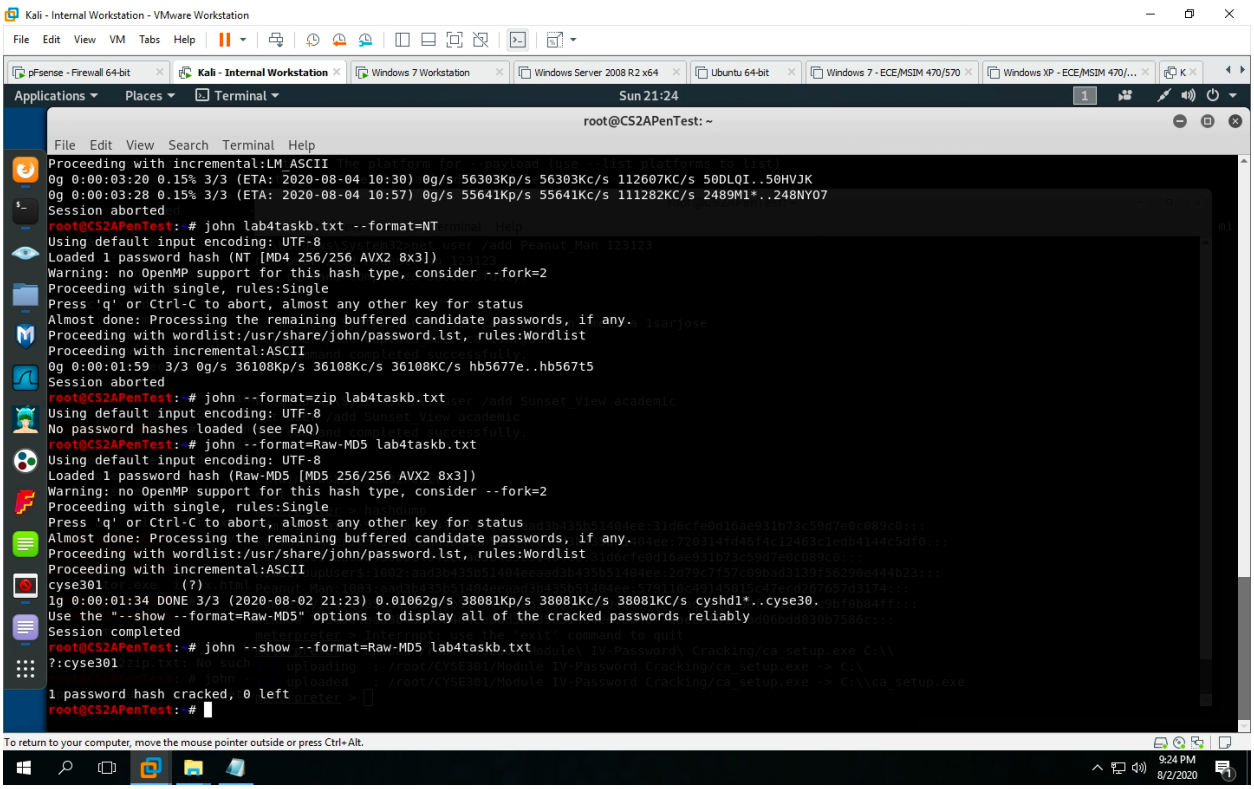
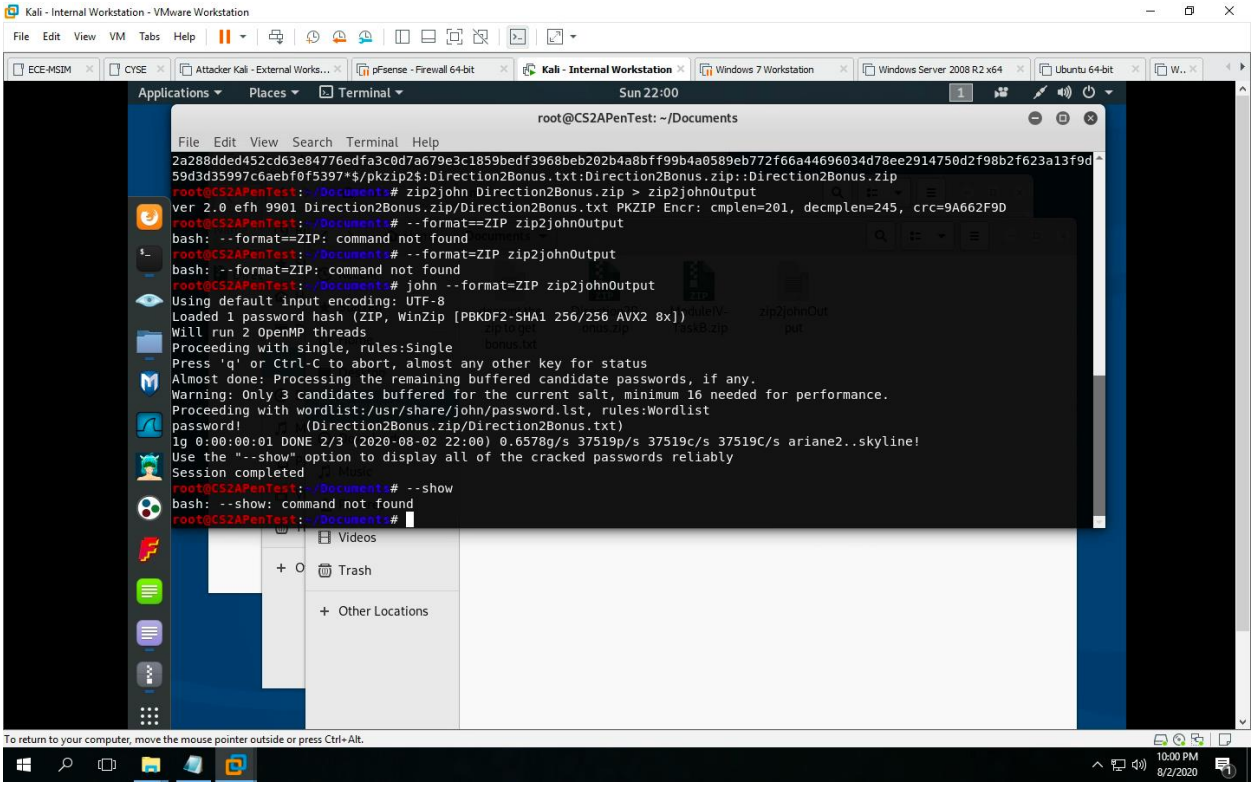


Figure 4.21 Password Cracked?

- (If my attempts were correct) I used the command ***john --format=Raw-MD5*** *lab4taskb.txt* to attempt to crack the password. The session was successful, therefore I then used the command

- ***john --show --format=Raw-MD5 lab4taskb.txt*** to show any successful password cracks
    - Password **cyse301**



EXTRA CREDIT Figure 4.22
attempting to crack password for ***direction2bonus.zip***

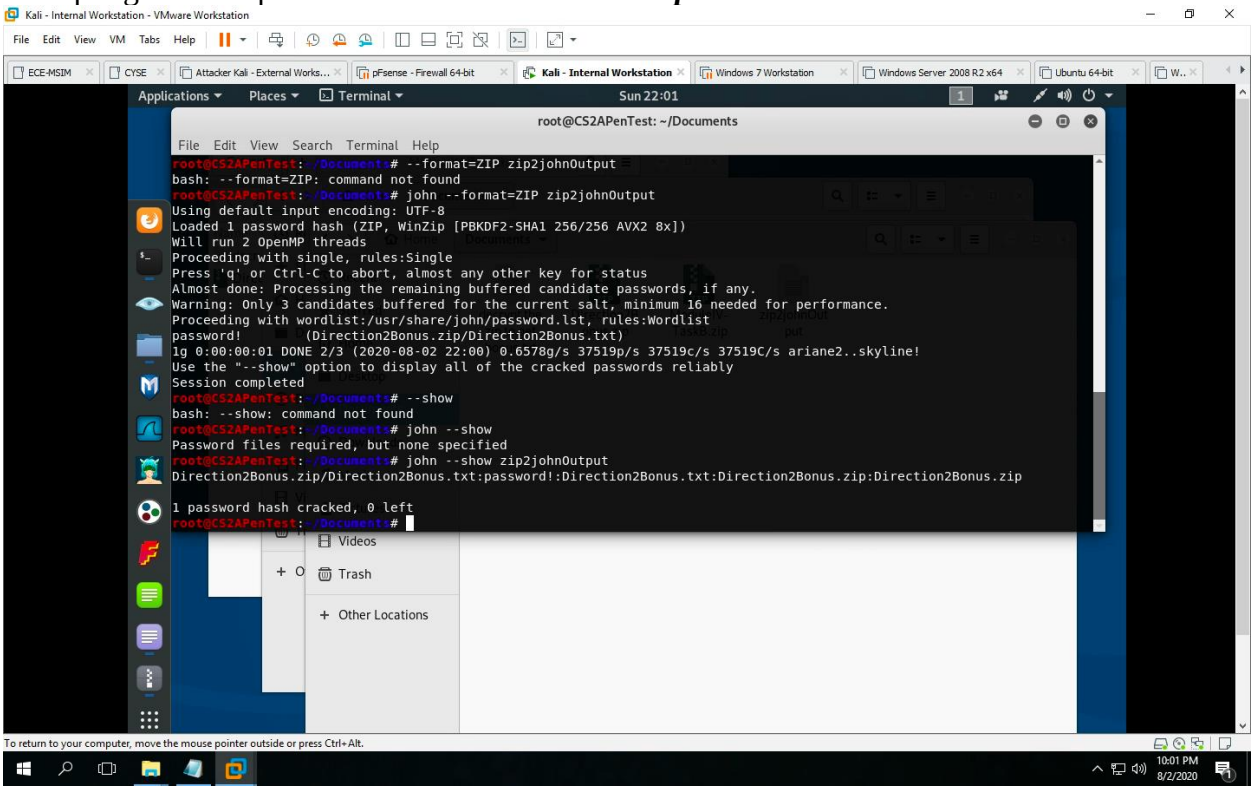


Figure 4.23 Using John the Ripper

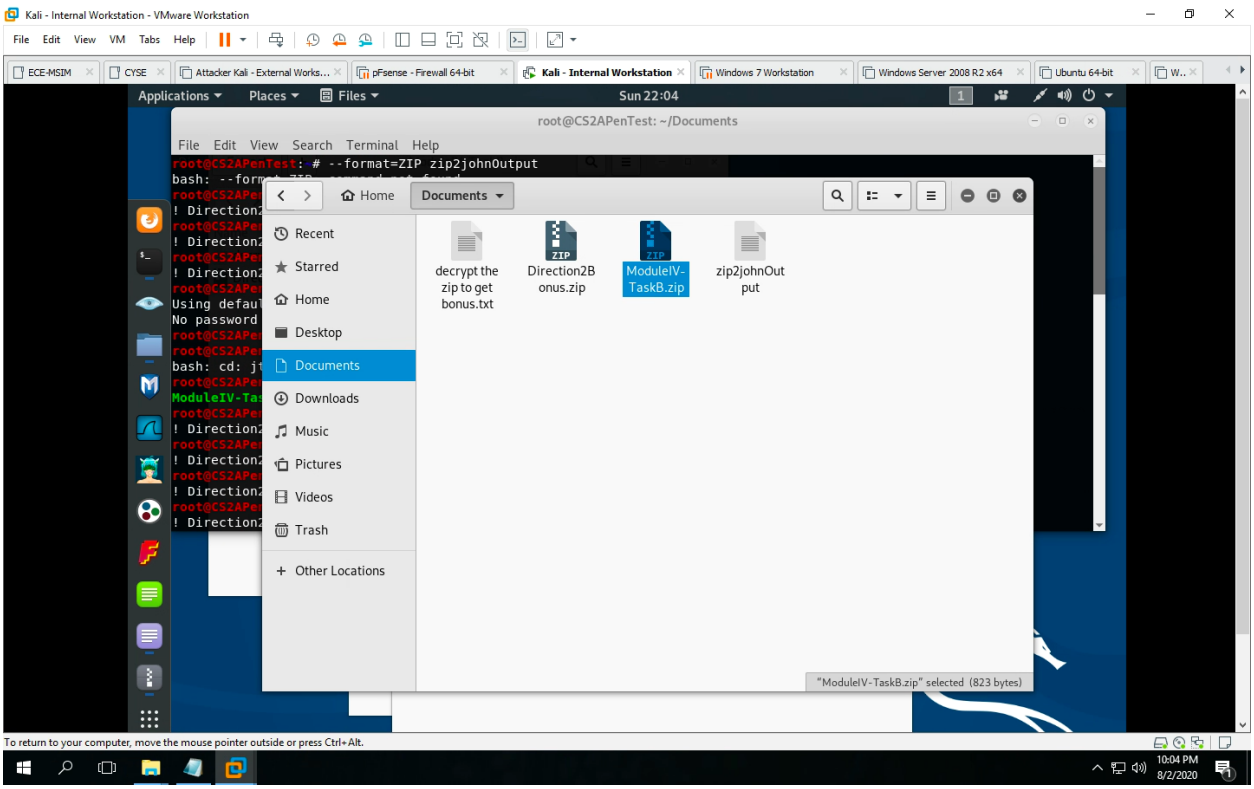


Figure 4.24 Files extracted into Documents

-I used the password **cyse301** to open the folder and once inside, I extracted the files to the documents.

-used the command ***cd Documents***

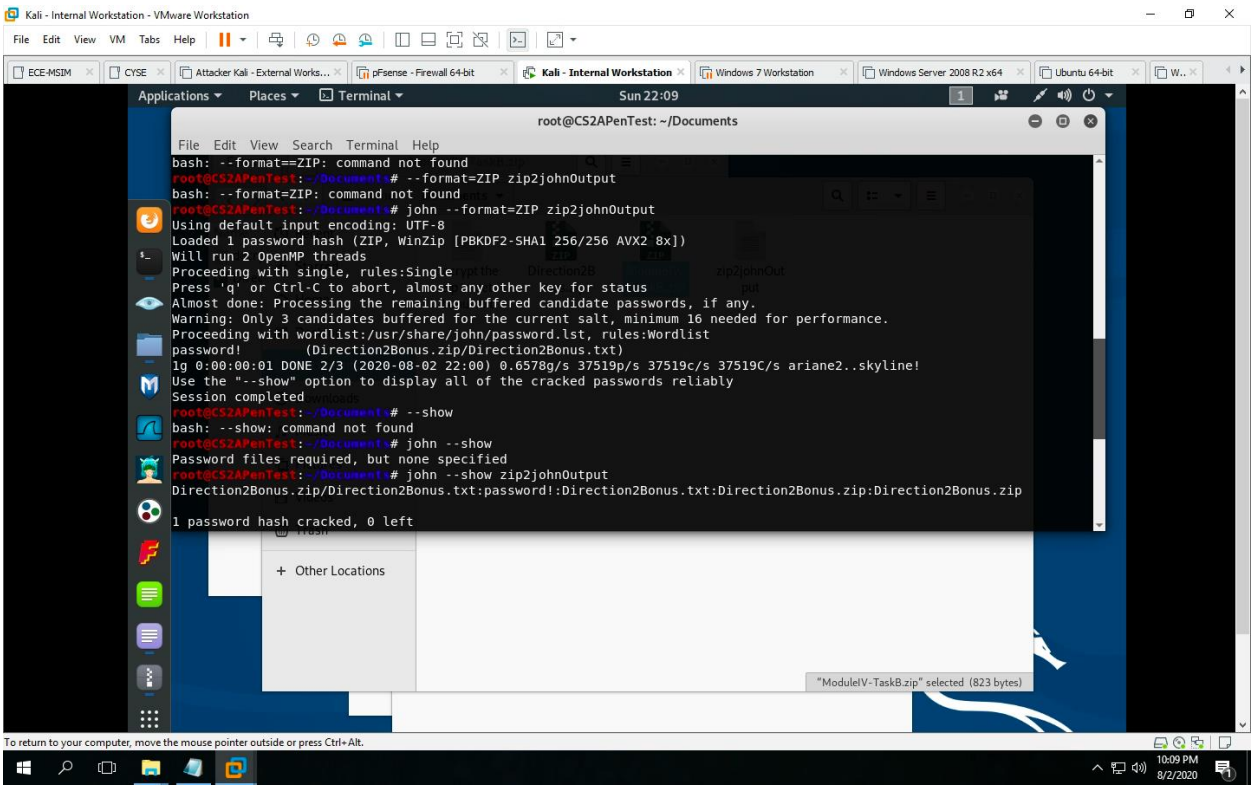


Figure 4.25 Password Extracted

- Once extracted, I used the command ***zip2john Direction2Bonus.zip***

-then I used the command ***john --format=ZIP zip2johnOuput***

-password = ***password!***

Figure 4.26 Assignment Completed