CYSE 301: Cybersecurity Technique and Operations

Assignment 4: Password Cracking (Part A)

Jason Rivers

01236524

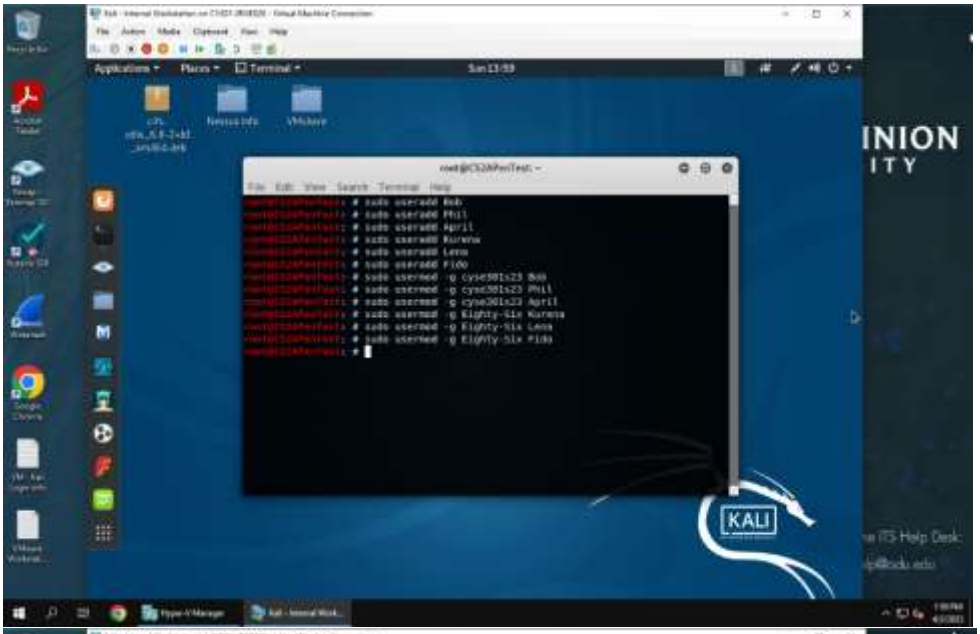
At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof.
You need to use

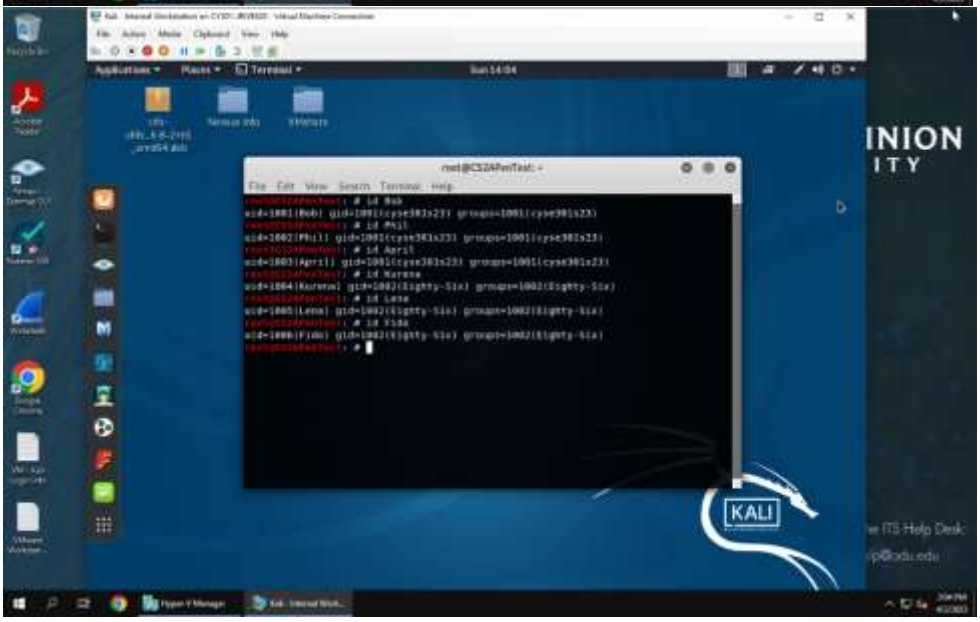
Task A: Linux Password Cracking (25 points)

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.

I forgot to use the "tail" command to show only the last 10 groups. Anyways, the group ID's are ***"cyse301s23 = 1001"*** *while my chosen group* ***"Eighty-Six = 1002"***

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

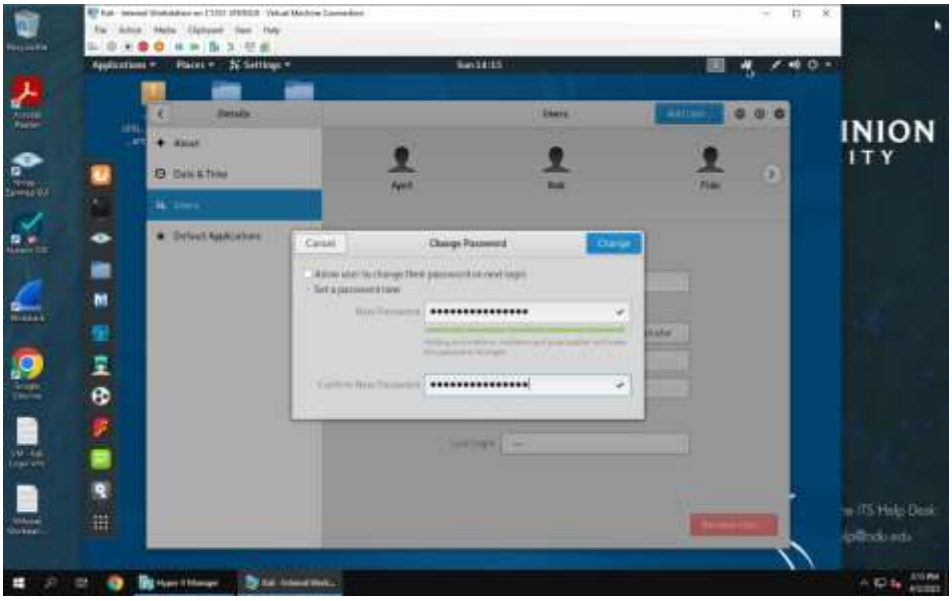




*I assigned **"Bob, Phil, and April" to the cyse301s23 group**, while **"Kurena, Lena, and Fido" are assigned to group Eighty-Six.***

The 2nd screenshot is the UID, and GID's respectively.

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.

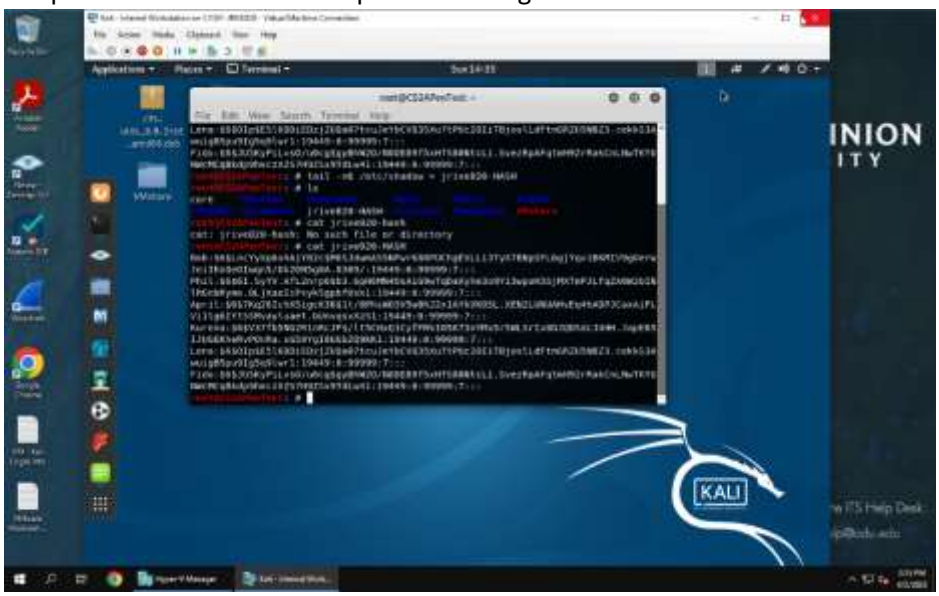


For context, I used the User modifier in settings to do the passwords to see how strong/weak they were. The characters were hidden, so I put the passwords I entered below:

Bob = yonaguni
Phil = ~~doorstopper~~ dictionary
April = 10-poundweights

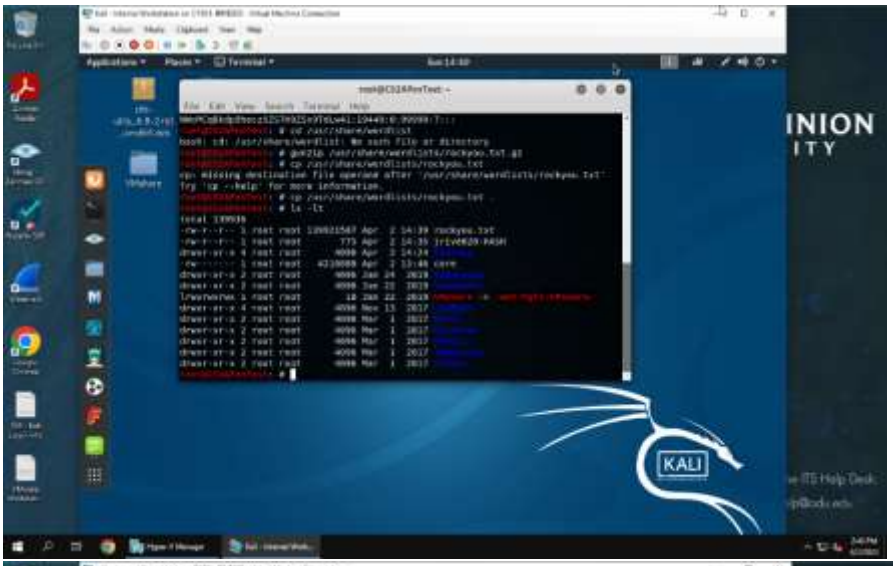
Kurena = xXbananabread505Xx
Lena = danceparty5
Fido = d0gg0goW00FBARKGRRR SNARL

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.

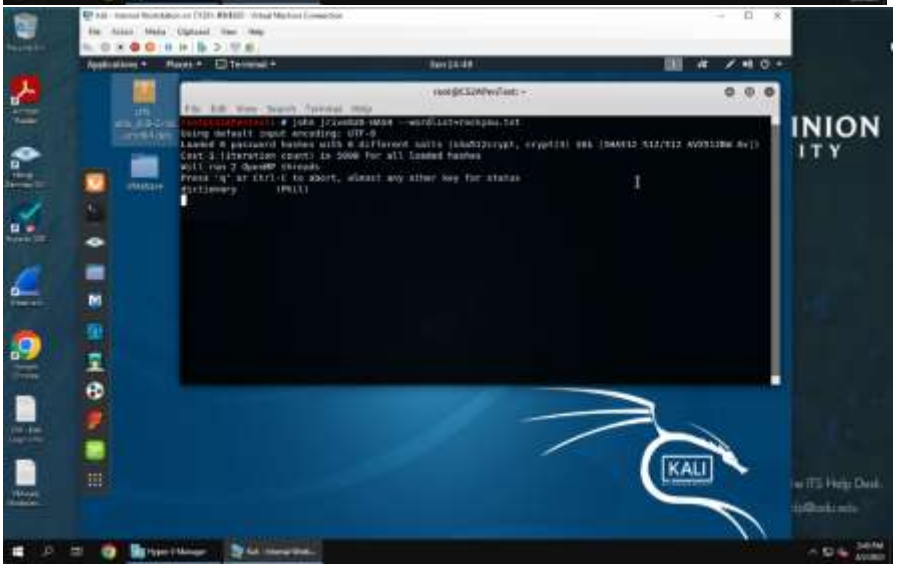


I copied the /etc/shadow file into a text file. After that, I unzipped the rockyou wordlist so we could use JohnTheRipper.

Then, I basically let it run until it cracked a password which took…..a while. I finally realized I didn't put a password that could have been in the rockyou list, so I changed Phil's password to dictionary so it would catch it.



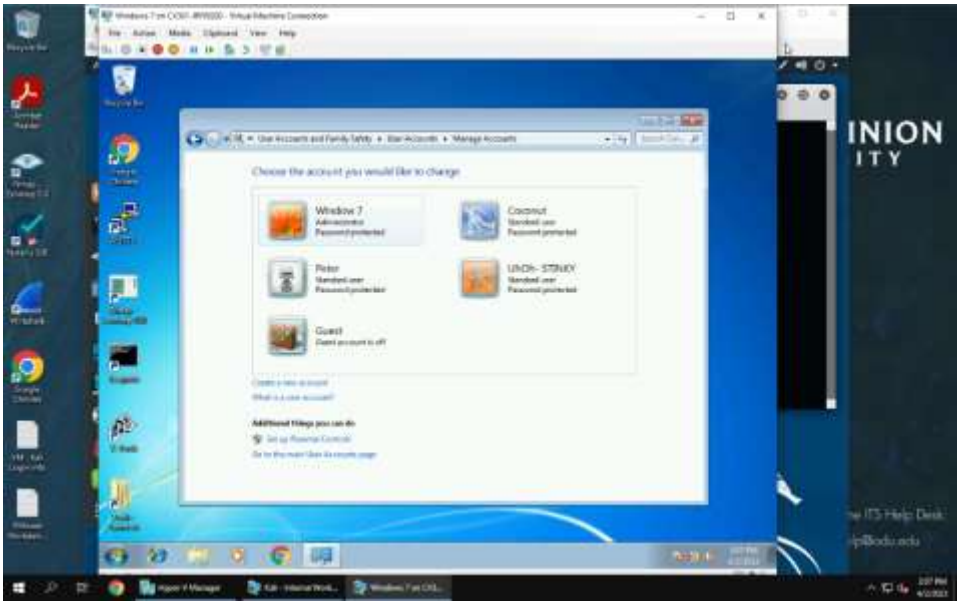
Extracting rockyou wordlist



Cracked Phil's password w/ JohnTheRipper

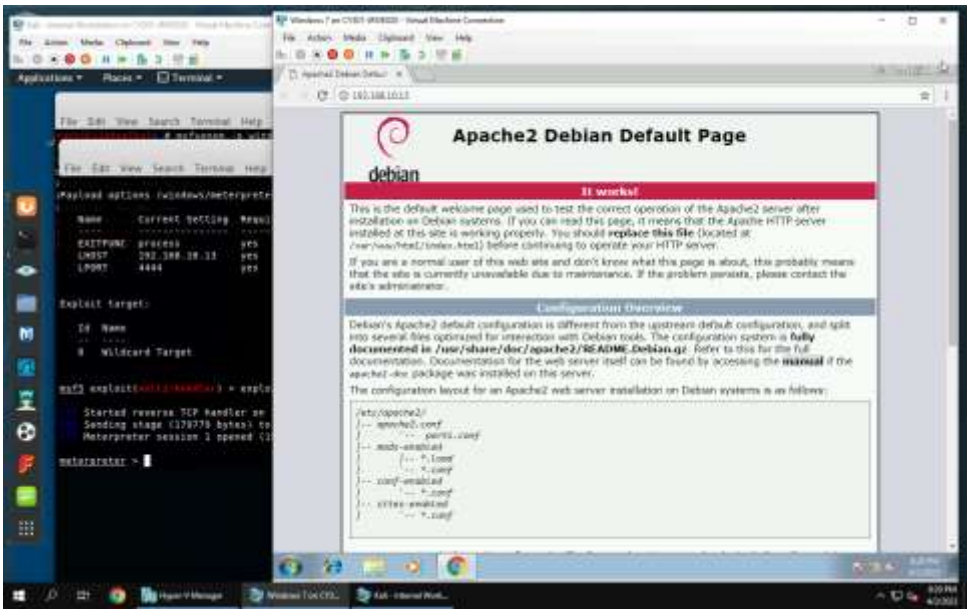
Task B: Windows Password Cracking (25 points)

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.



I added users Peter, Coconut, and Uhoh- STINKY, then I assigned them passwords easy, medium, and basically impossible to crack within a decent amount of time.

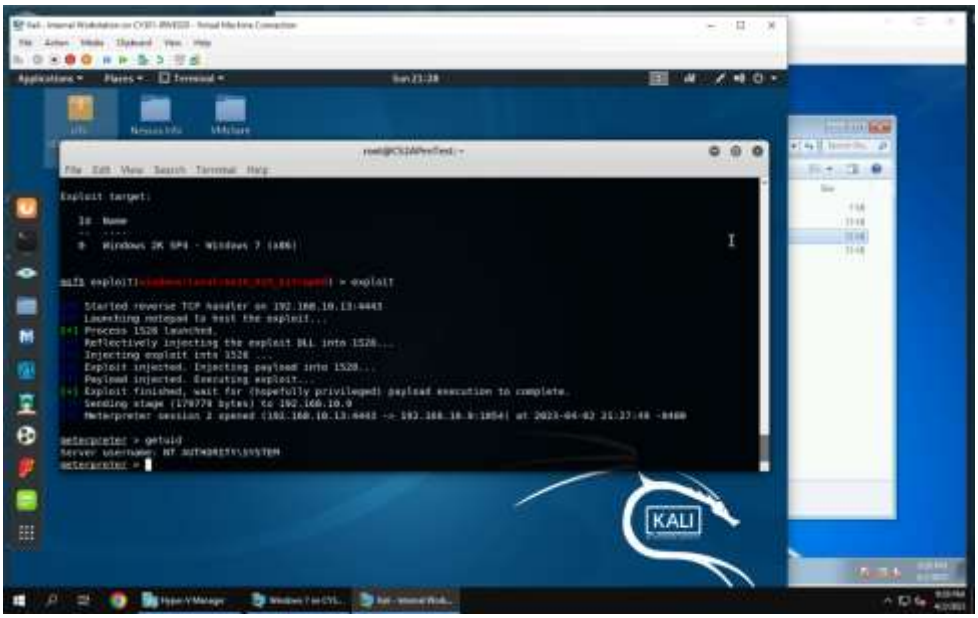
Peter: familyguy
Coconut: catcafe
Uhoh- STINKY: funny_m0nk3y



I took a break, then came back.

I spent 2 hours after this trying to do this part properly, then CCIA crashed., and ALL of my progress was just gone.

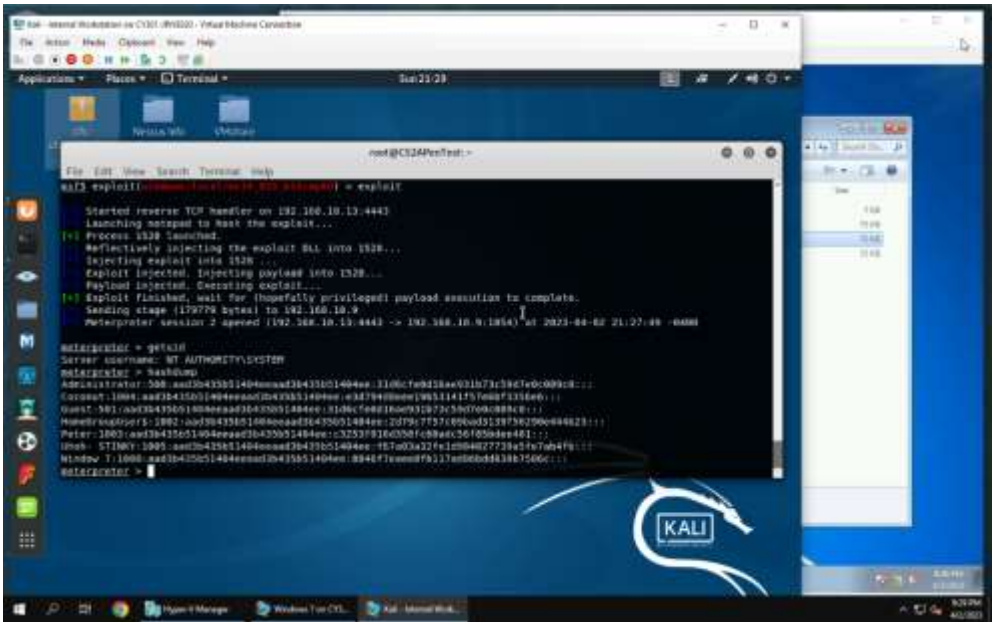
I had to reload everything from here.



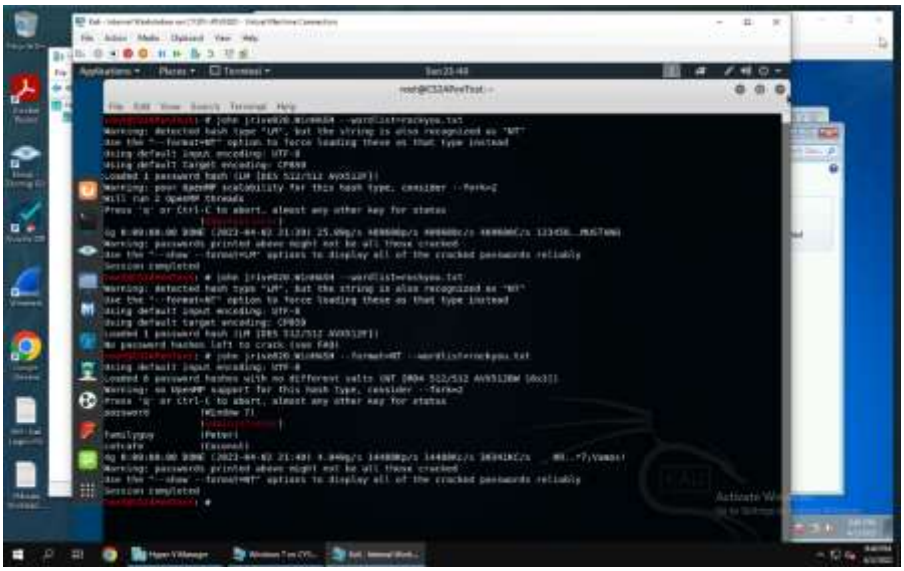
After trial and error for about 5 hours, I finally got the exploit to work, and privilege to escalate.

Now, complete the following tasks:

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

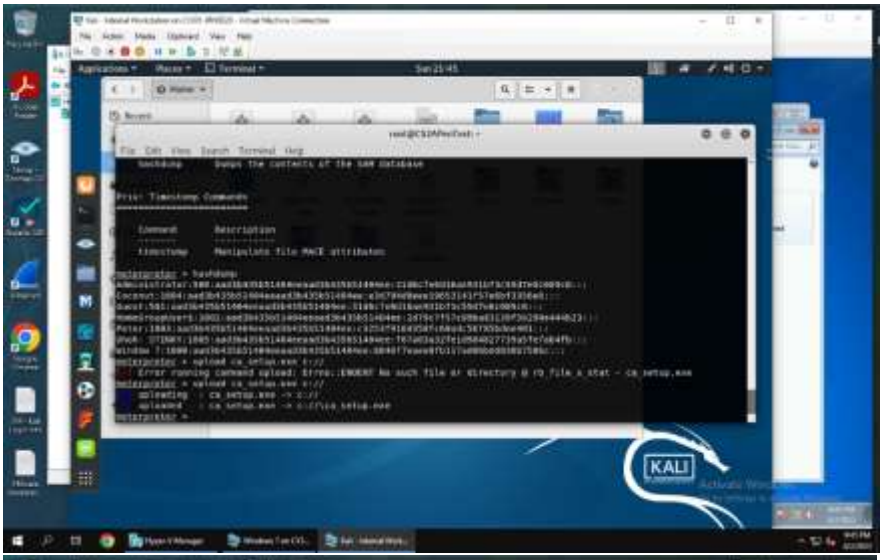


2. **10 points.** Save the password hashes into a file named “**your_midas.WinHASH**” in Kali Linux (you need to replace the “your_midas” with your university MIDAS ID). Then run John the ripper for **10 minutes** to crack the passwords (You MUST crack at least one password in order to complete this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



I didn’t need to run it for 10 minutes, it cracked both Peter, and Coconut almost immediately.

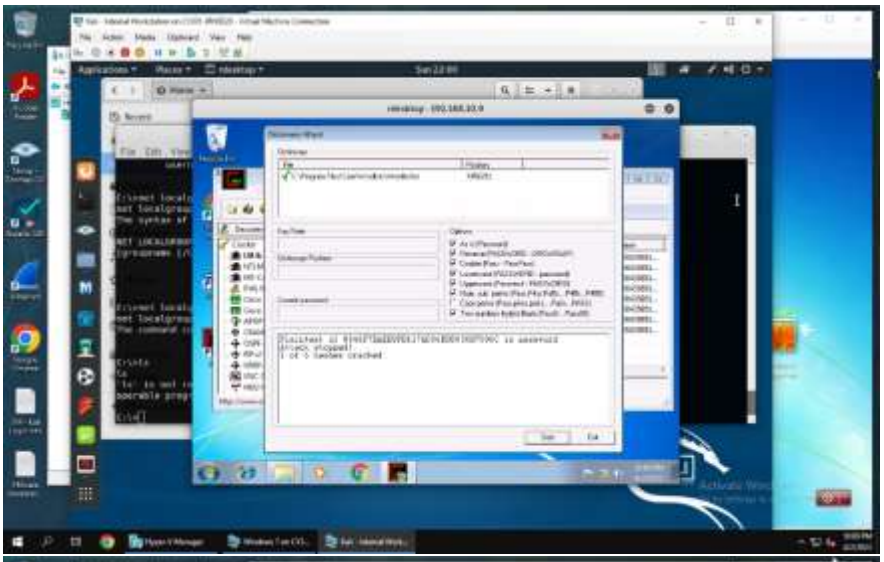
3. **10 points.** Upload the password cracking tool, **Cain and Abel,** to the remote Windows 7 VM, and install it via a remote desktop window. Then, implement **BOTH** brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).



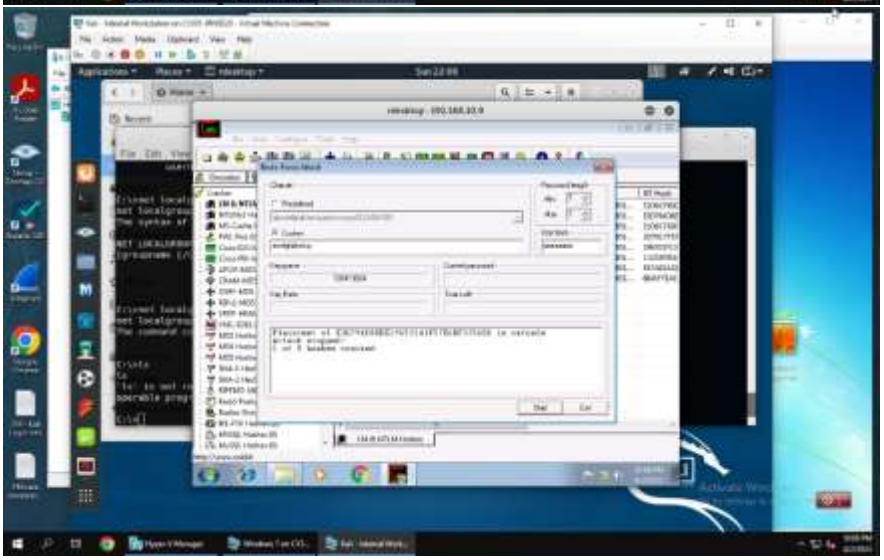
Copied ca_setup.exe from the CYSE301 folder to /root. Then I uploaded it to C://

I created a new user on the Windows 7 machine, and used Rdesktop to interface with it visually.

Installed Cain



Dictionary attack successful.



Brute-force successful.

(I did mess with the parameters for this one, but I worked on this assignment all day, so I wanted to shortcut this part!)

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