OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 – Password Cracking

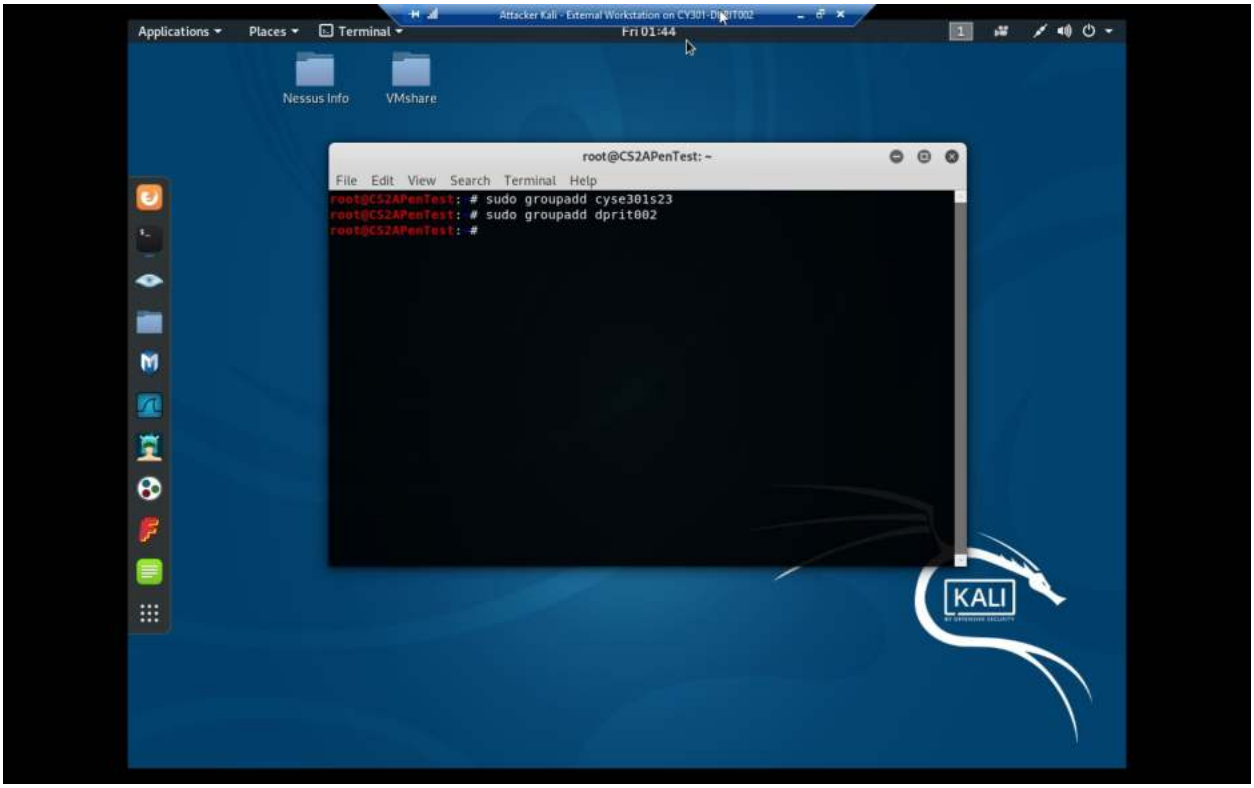
Darren Pritchard

01241796

Password Cracking (Part A)

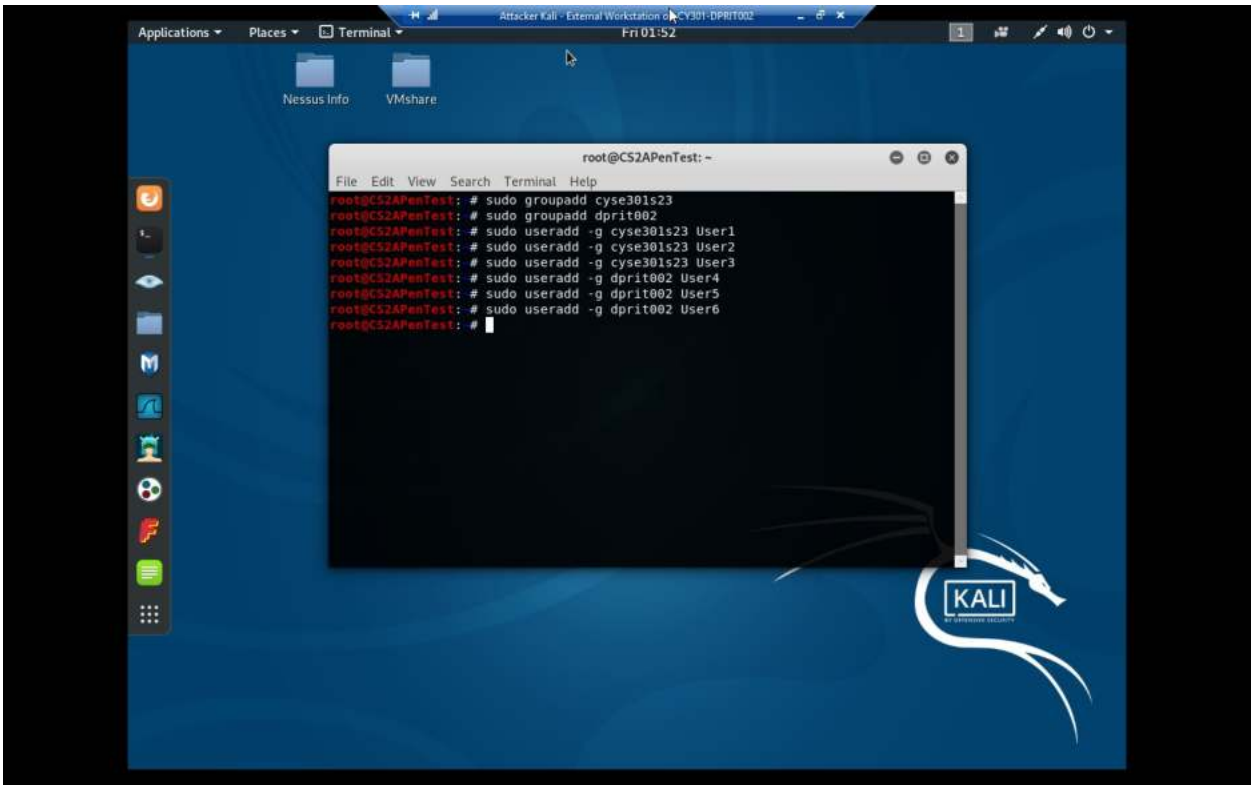
Task A: Linux Password Cracking (25 points)

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.



Explanation: Here we add both groups, one named cyse301s23 and the other named dprit002, my Midas ID.

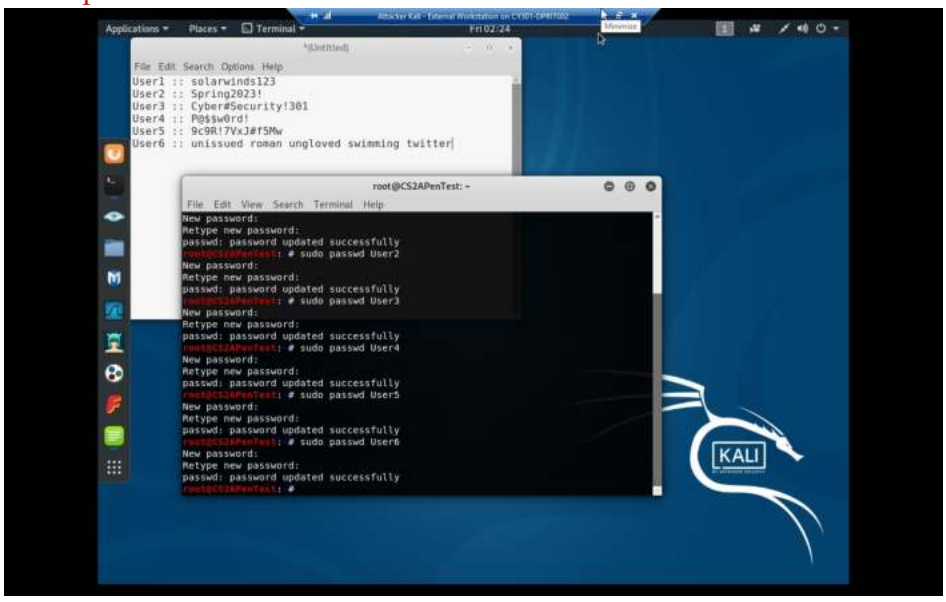
2. 5 points. Create and assign three users to each group. Display related UID and GID information of each user.



Explanation: Here 6 users are created, with User1 through User3 assigned to cyse301s23, and User4 through User6 is assigned to dprit002.

3. 5 points. Choose six new passwords, from easy to hard, and assign them to the users you created.

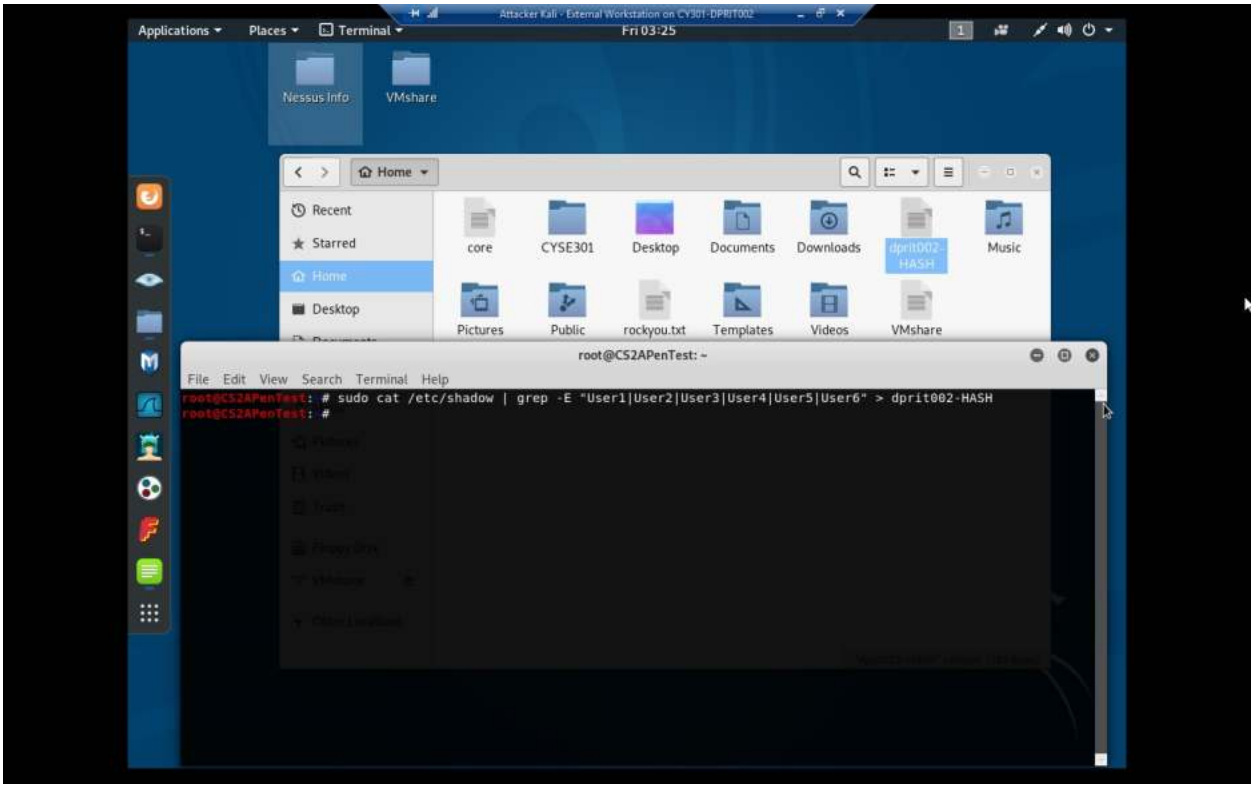
You need to show me the password you selected in your report, and DO NOT use your real world passwords.



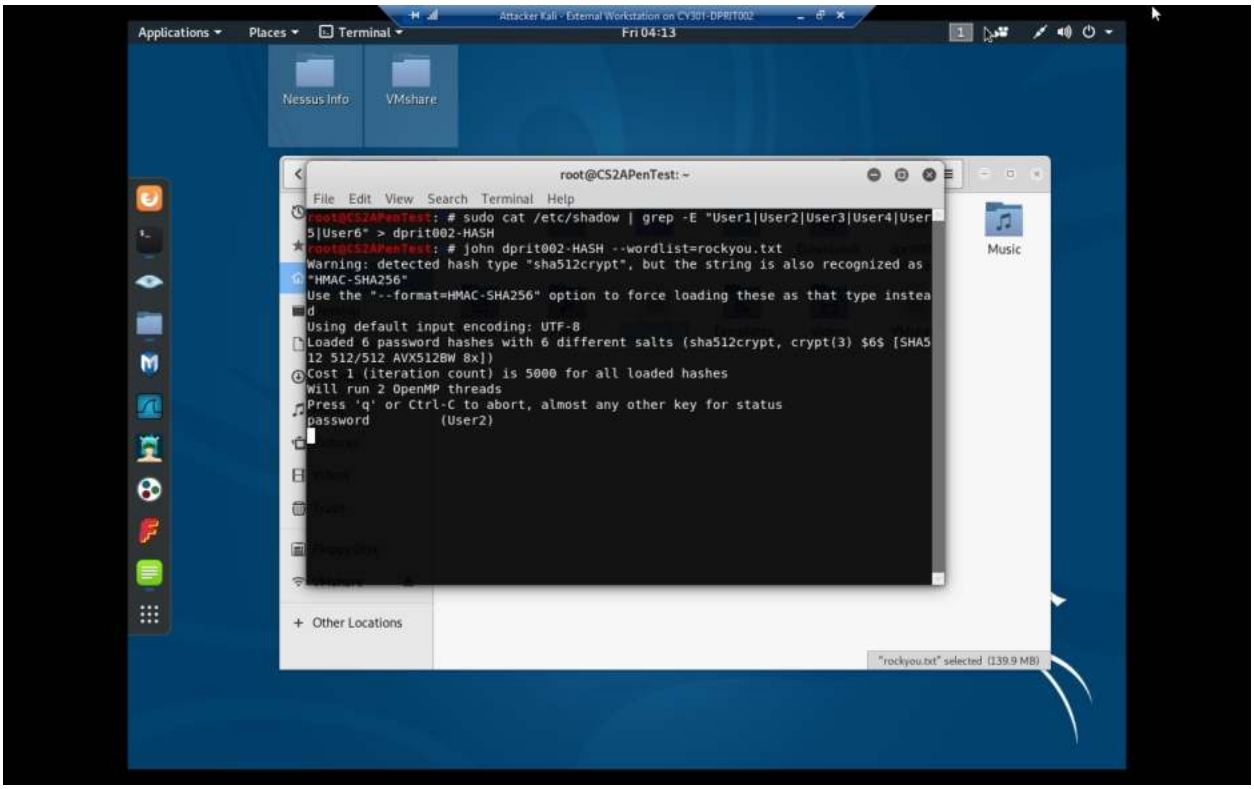
Explanation: As shown, this is after updating all 6 users with passwords ranging from very easy to very hard, with solarwinds123 being the easiest password, and the last password being a diceware passphrase using the EFF wordlist, which is the hardest.

EDIT: For the speed of the next step of the process, the password for User2 has been changed to "password".

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.



Explanation: This is the command used to export all 6 passwords to a file called "dprit002-HASH". You can see, in the background, that the file has been made in the home directory.

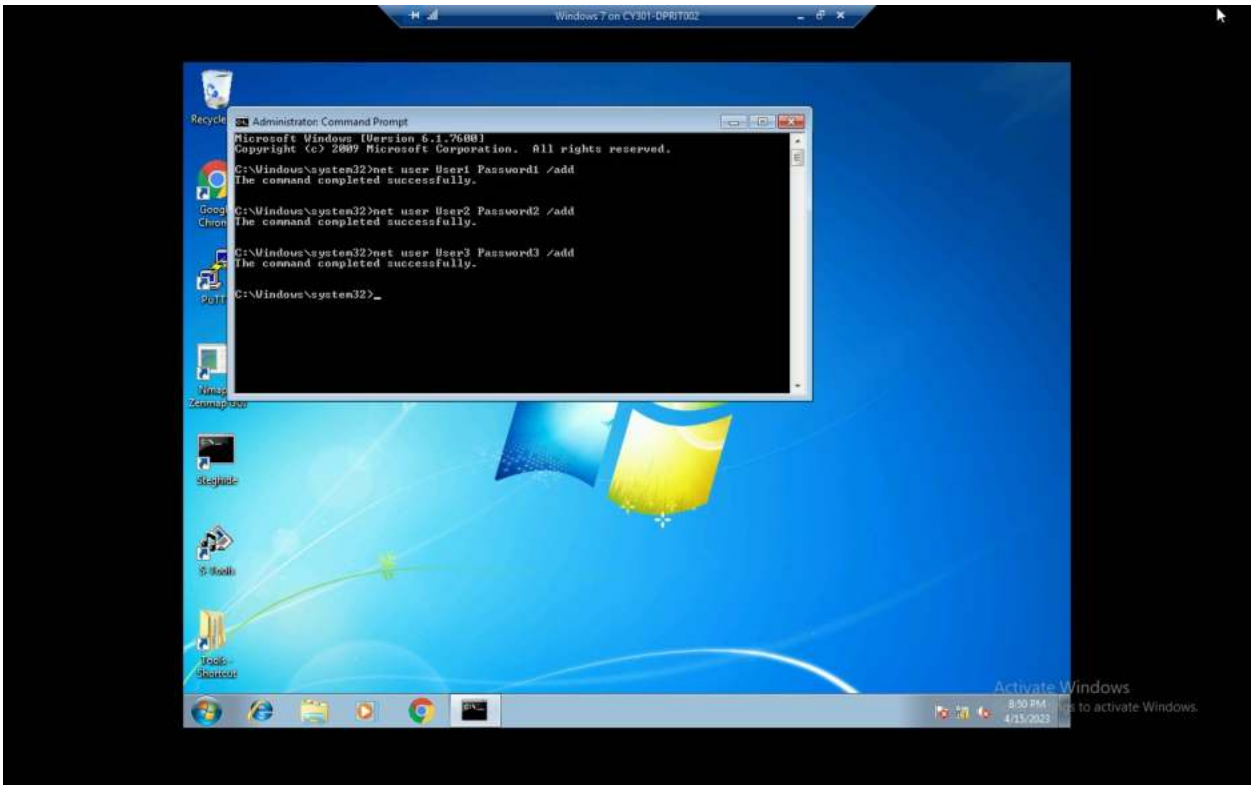


Explanation: After running the command “john dprit002-HASH –wordlist=rockyou.txt” for less than a minute, the password for User2, “password”, is found.

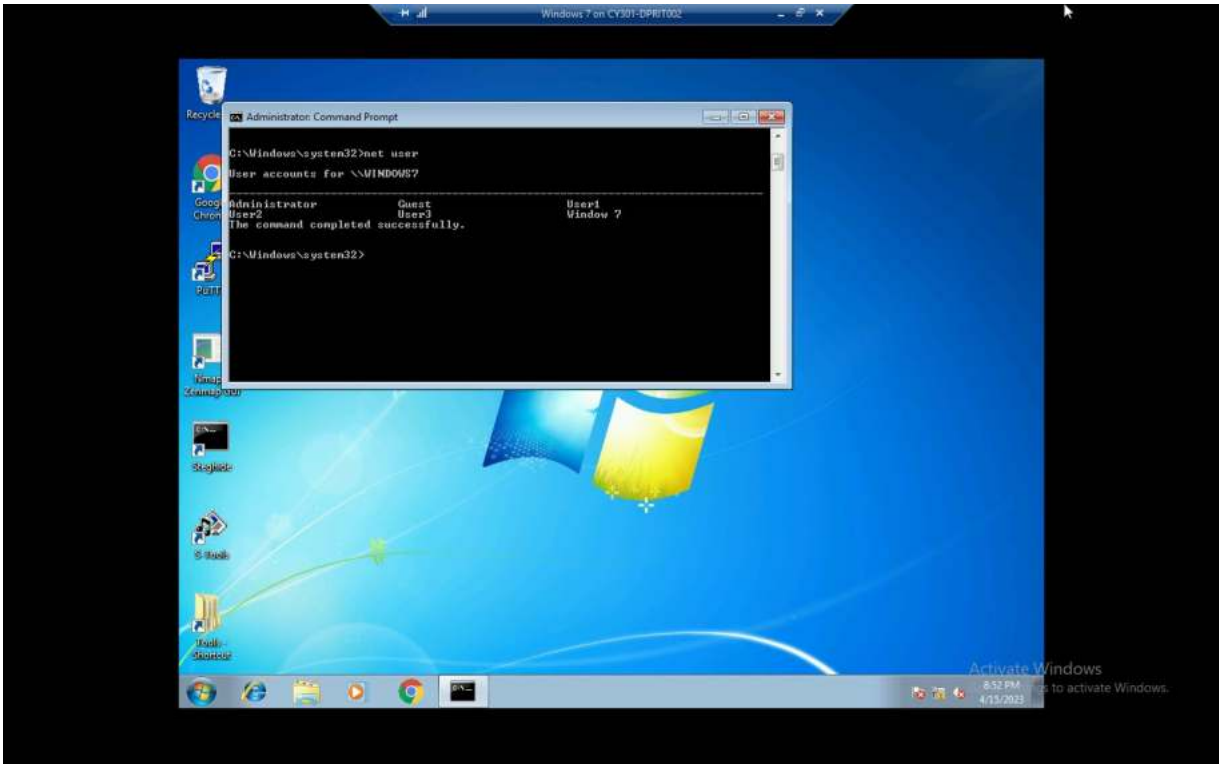
Task B: Windows Password Cracking (25 points)

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.

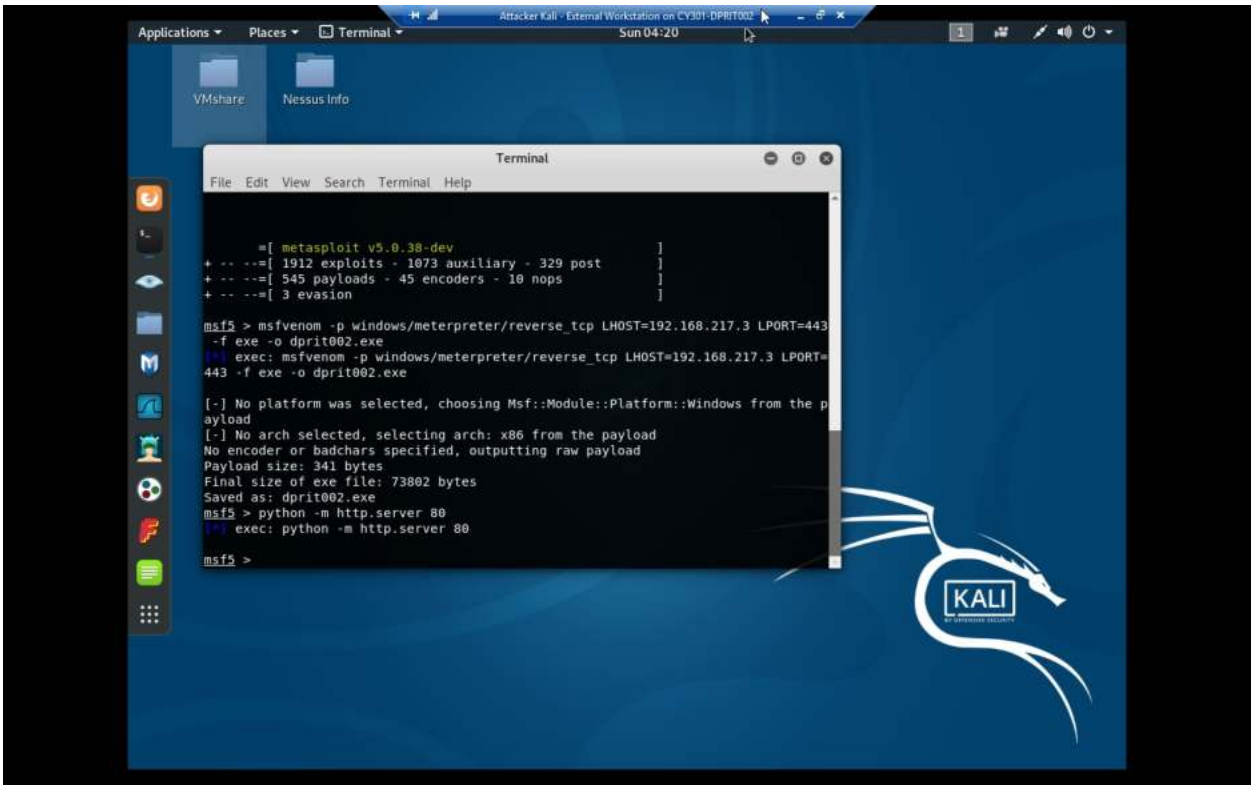
Now, complete the following tasks:



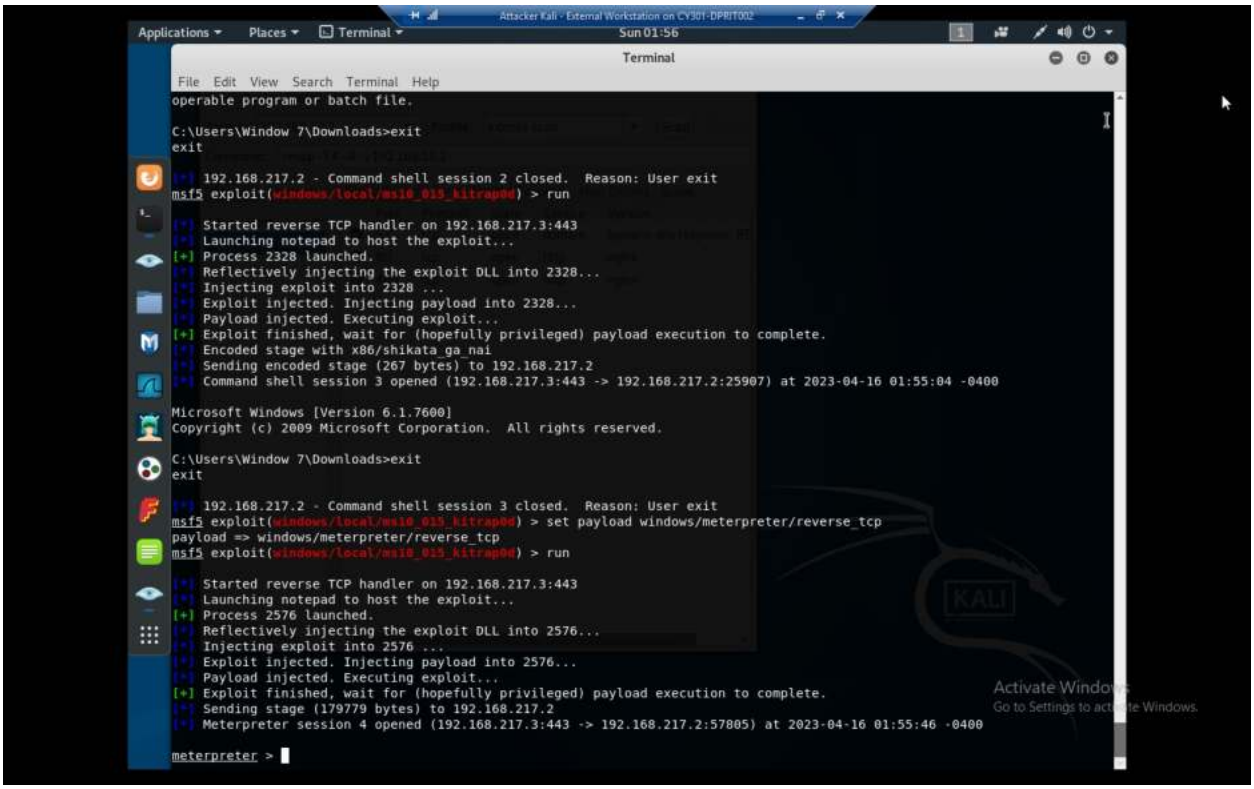
Explanation: Here we have the commands used in command prompt to create 3 users and their corresponding passwords.



Explanation: And here we see that all users have been made correctly.

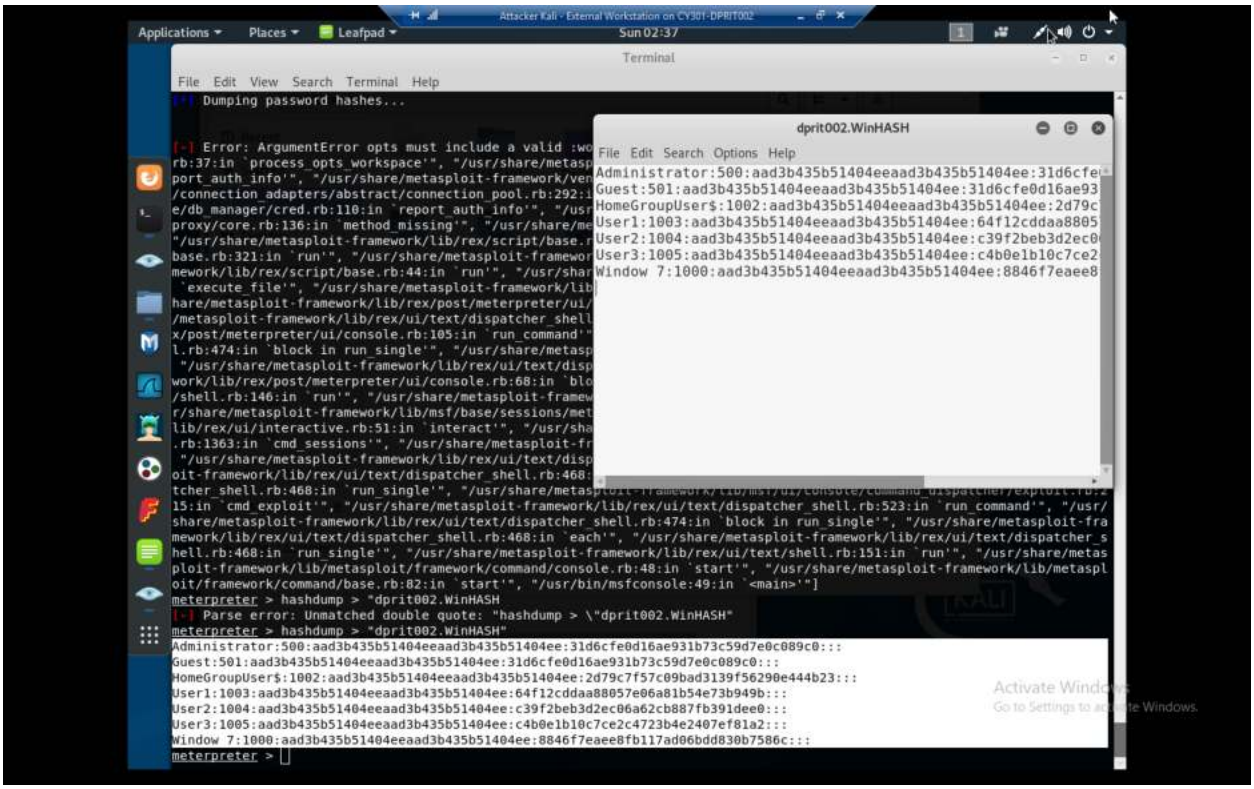


Explanation: Rather than reinventing the wheel, I will be using the same method as the previous assignment to establish a reverse shell.



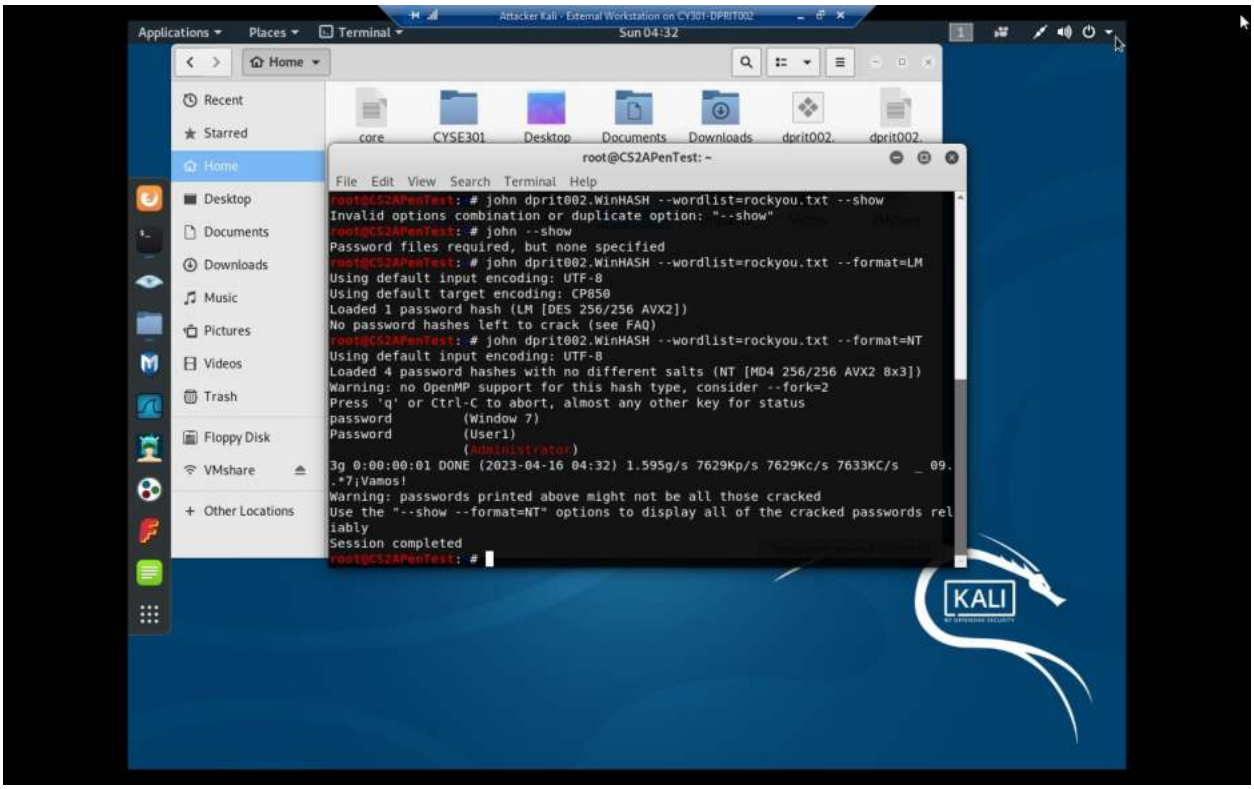
Explanation: And then to perform privilege escalation, we background the original session and use ms10_015_kitrap0d.

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



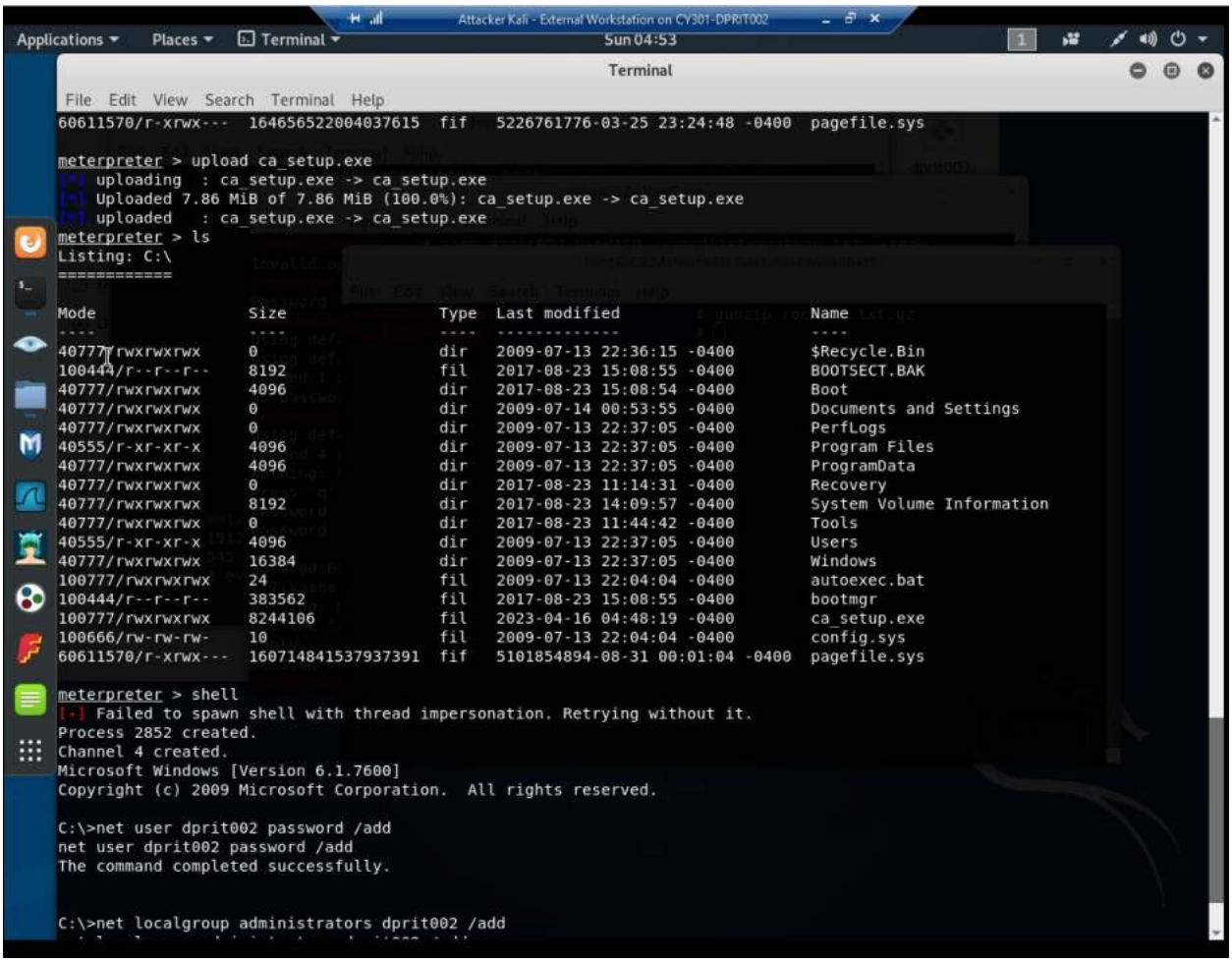
Explanation: This is after running hashdump, failing for some reason to directly write to a file named "dprit002.WinHASH" and just copy-pasting it to leafpad and saving the file as "dprit002.WinHASH."

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.).

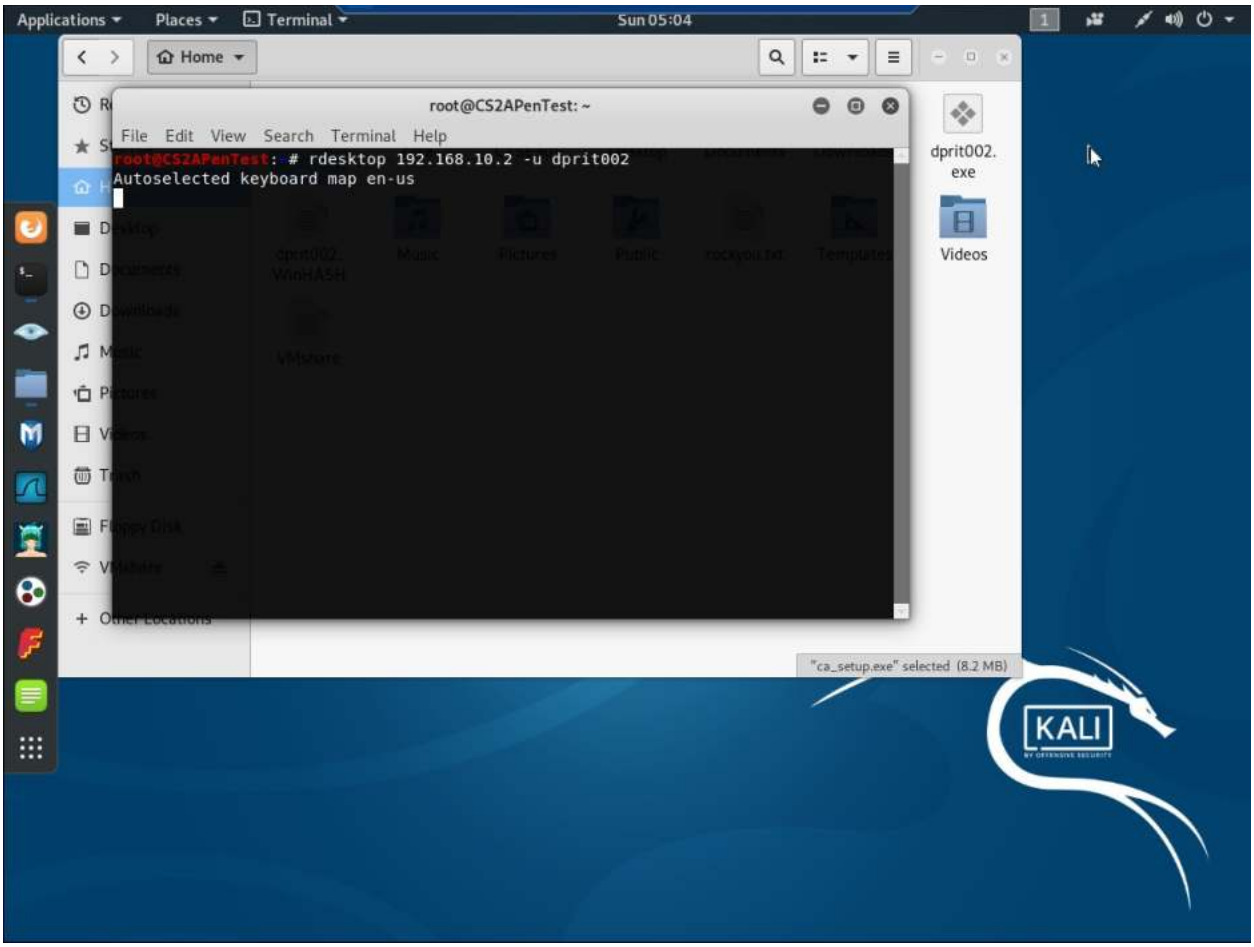


explanation: After the VM getting deleted, I repeated all the steps but instead made all the passwords “password” for every user, hence there is only one hash to crack.

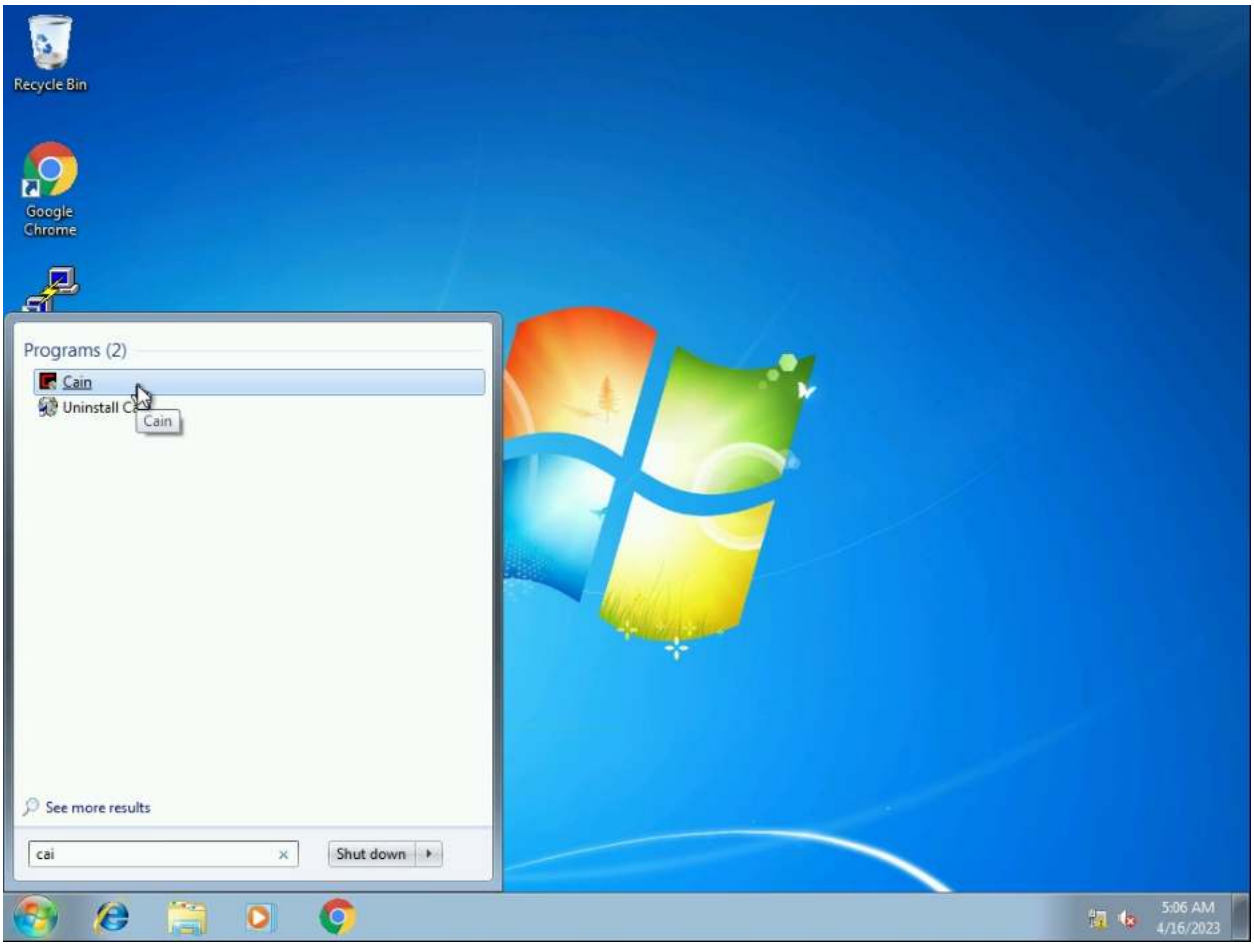
3. 10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and
install it via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords. (You MUST crack at least one password in order to complete this assignment.).



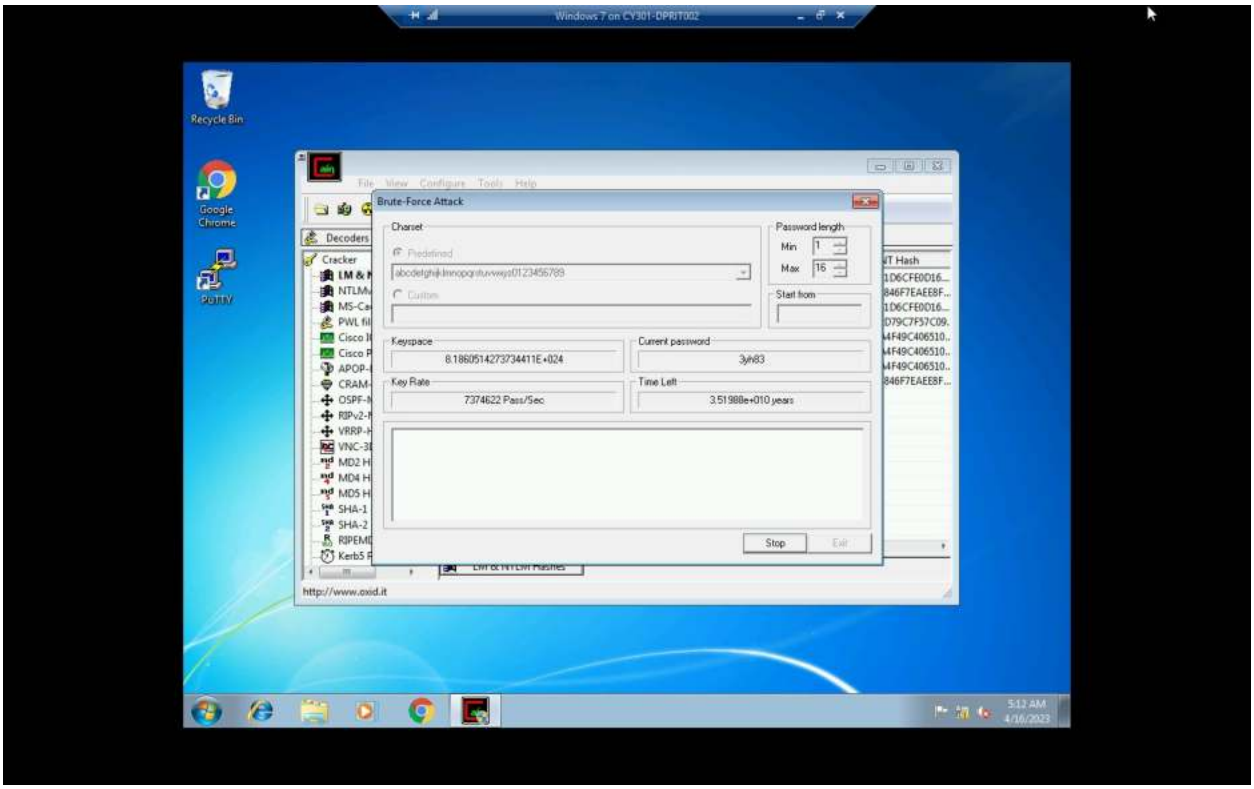
explanation: after uploading ca_setup.exe we add my MIDAS as a user and elevate it to administrator-level privileges



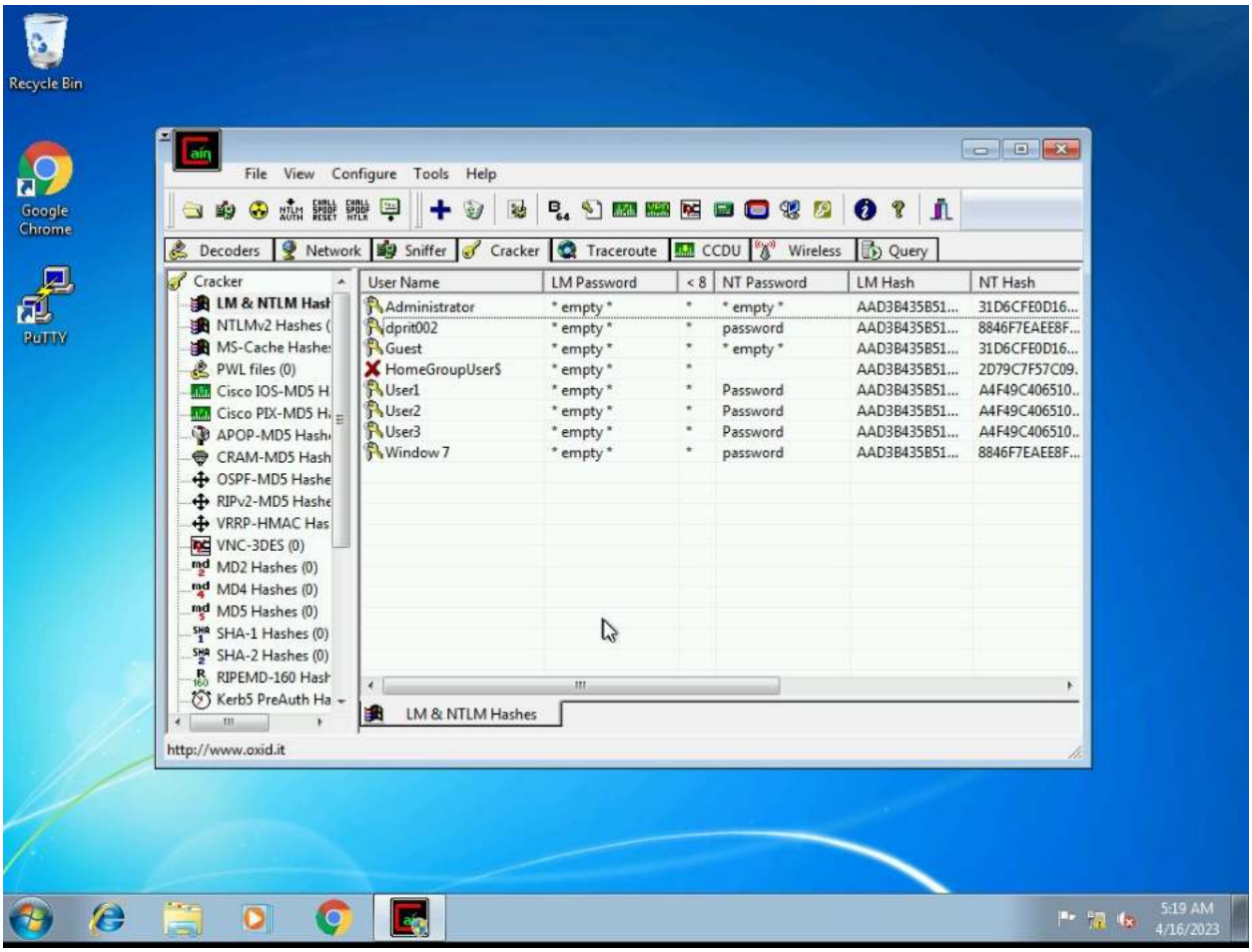
Explanation: me starting up rdesktop, yet failing to actually launch it for an absolutely unknown reason



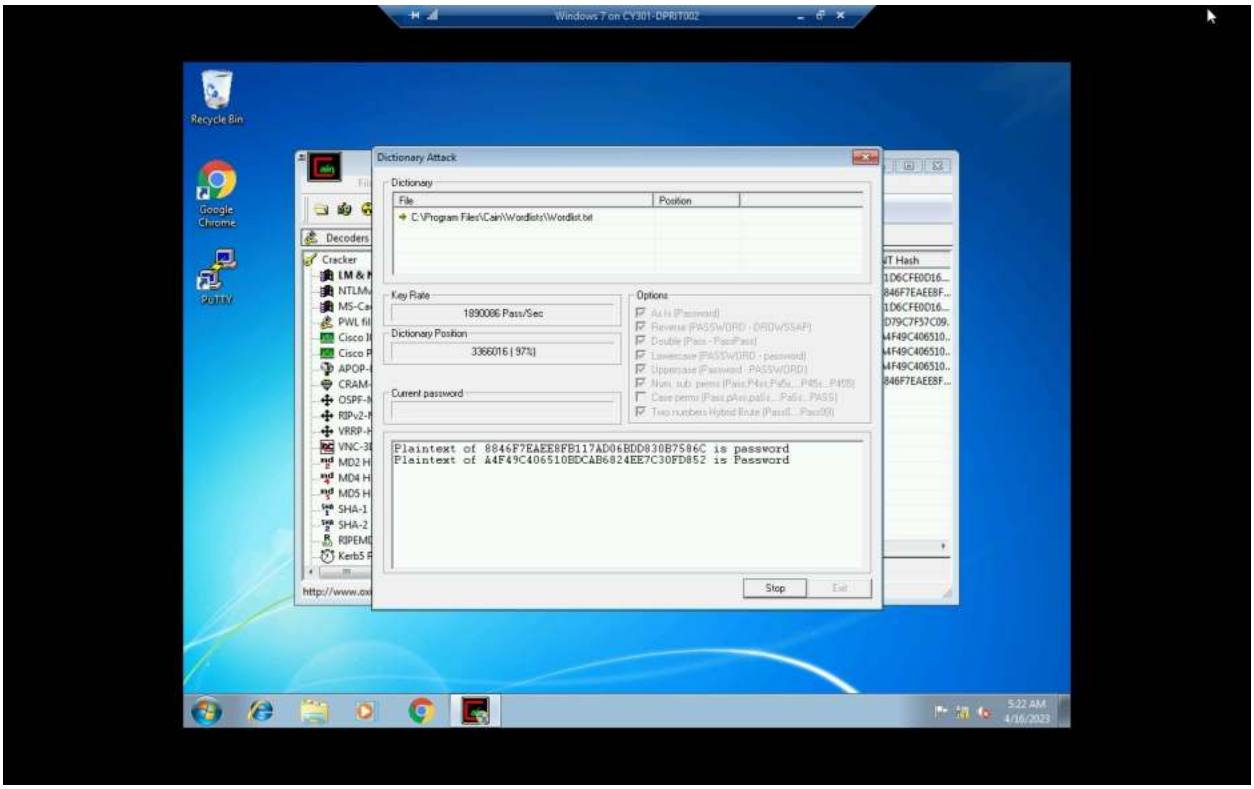
explanation: due to repeated technical errors I just went to the windows 7 VM, logged in, installed CA. This is generally the same steps as what it would be otherwise, just not using rdesktop



Explanation: and this is me bruteforcing passwords

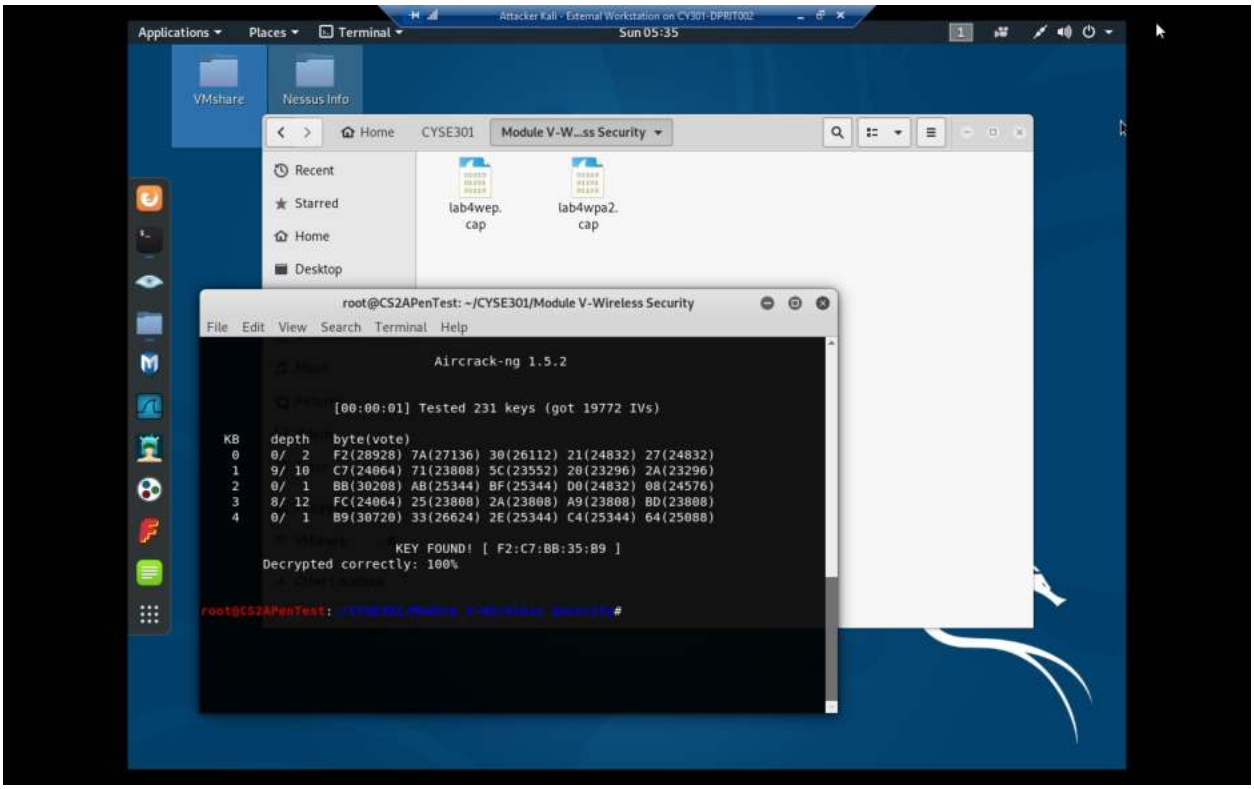


explanation: after restarting the bruteforce attack and starting from “password,” thus automatically cracking all of the passwords at once

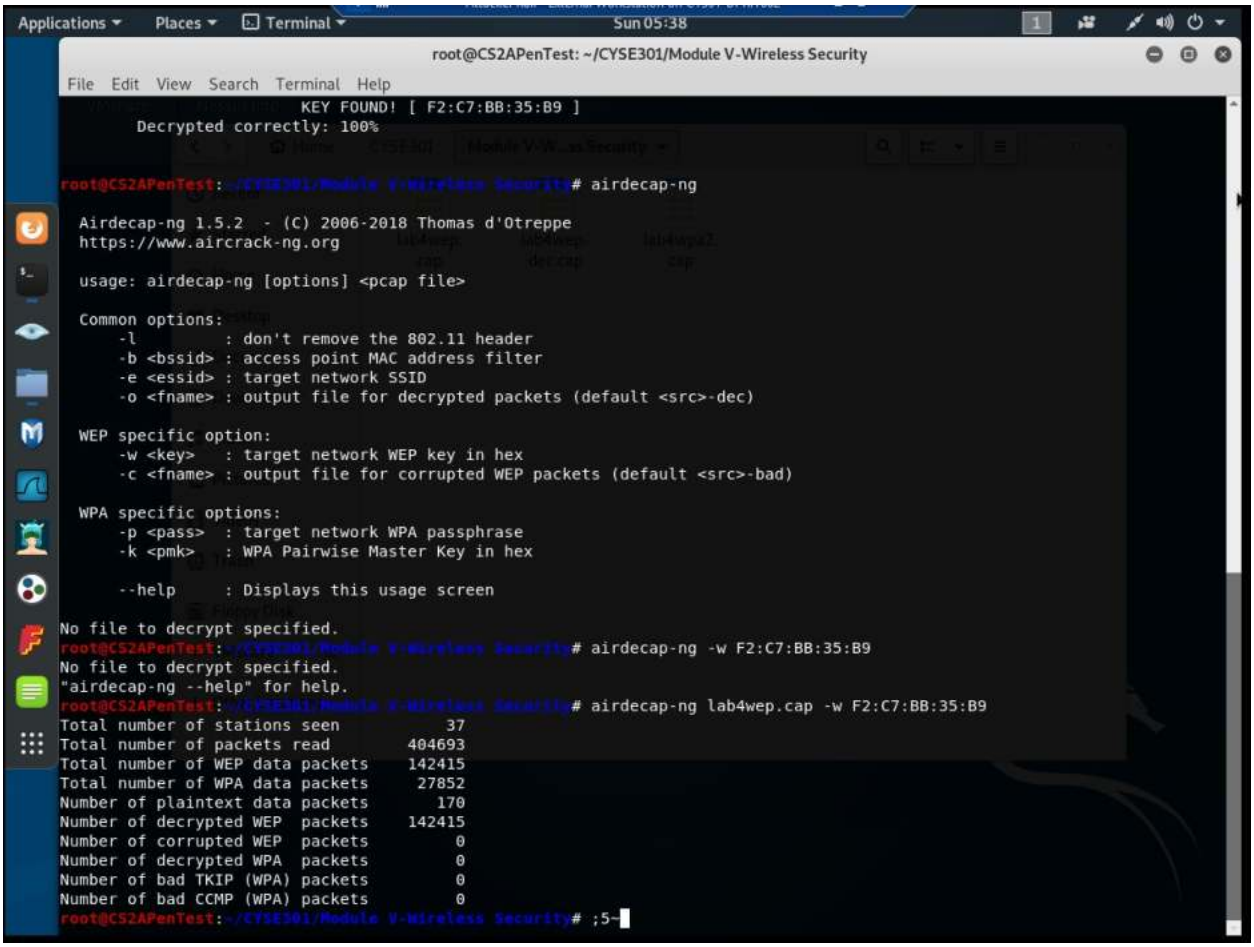


explanation: dictionary attack, using the wordlist.txt in CA

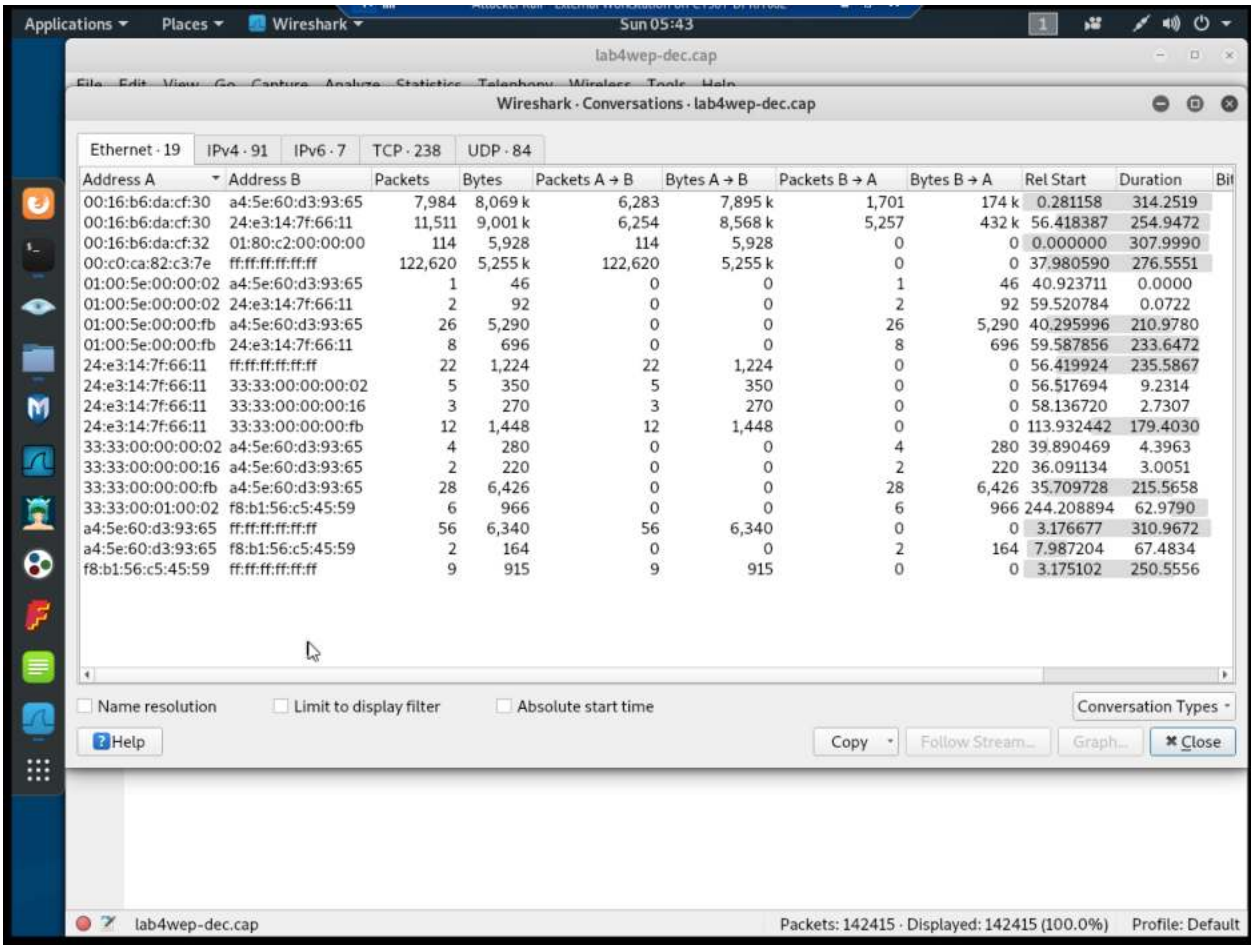
Task C: 20 points
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected
traffic.
1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)



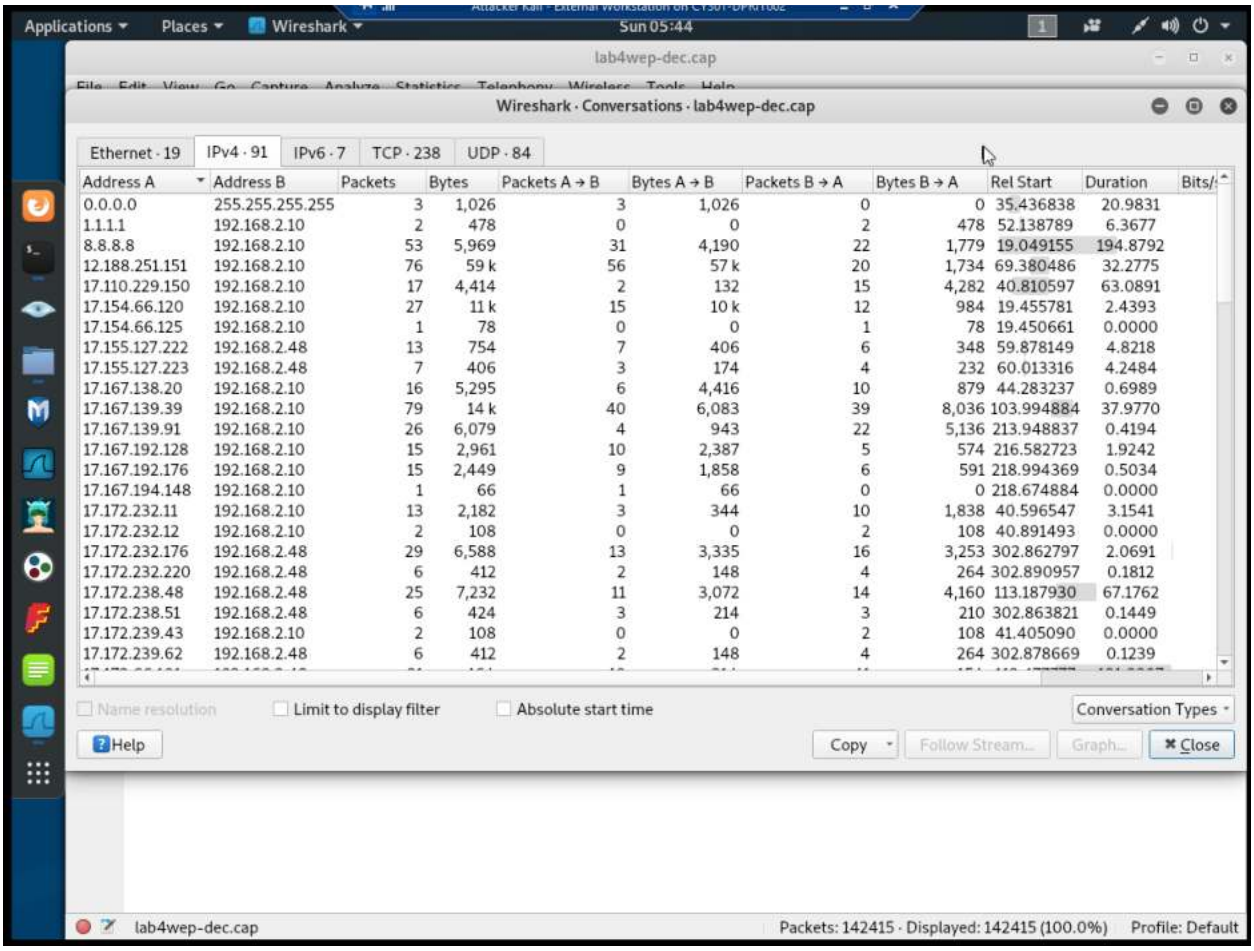
explanation: after using aircrack-ng on lab4wep.cap and selecting network 1, which is the only WEP one, we get a key of F2:C7:BB:35:B9



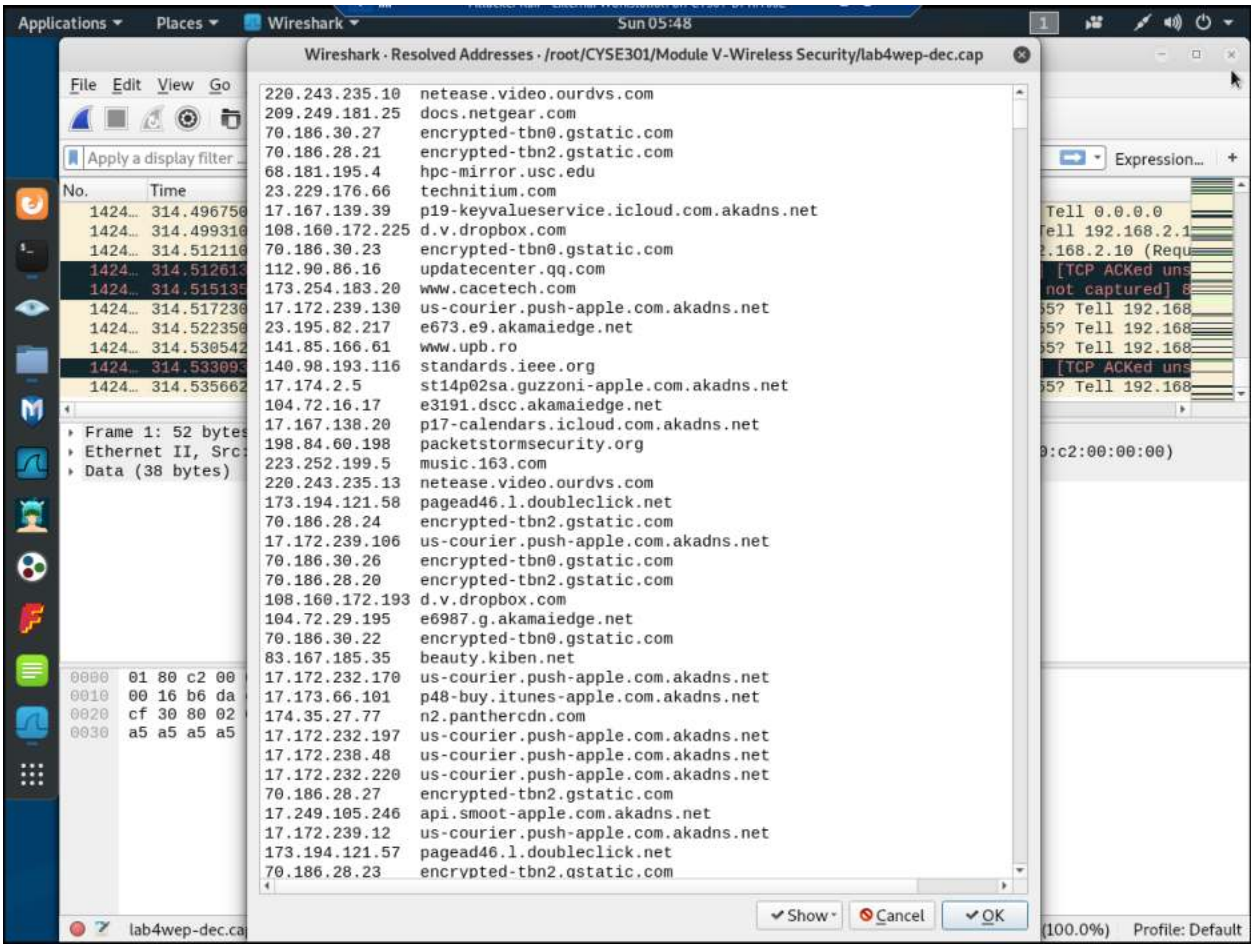
explanation: And after using airdecap we have 142,415 decrypted WEP packets



explanation: And looking at the conversations in the decrypted cap file, we see the ethernet conversations that took place in this capture

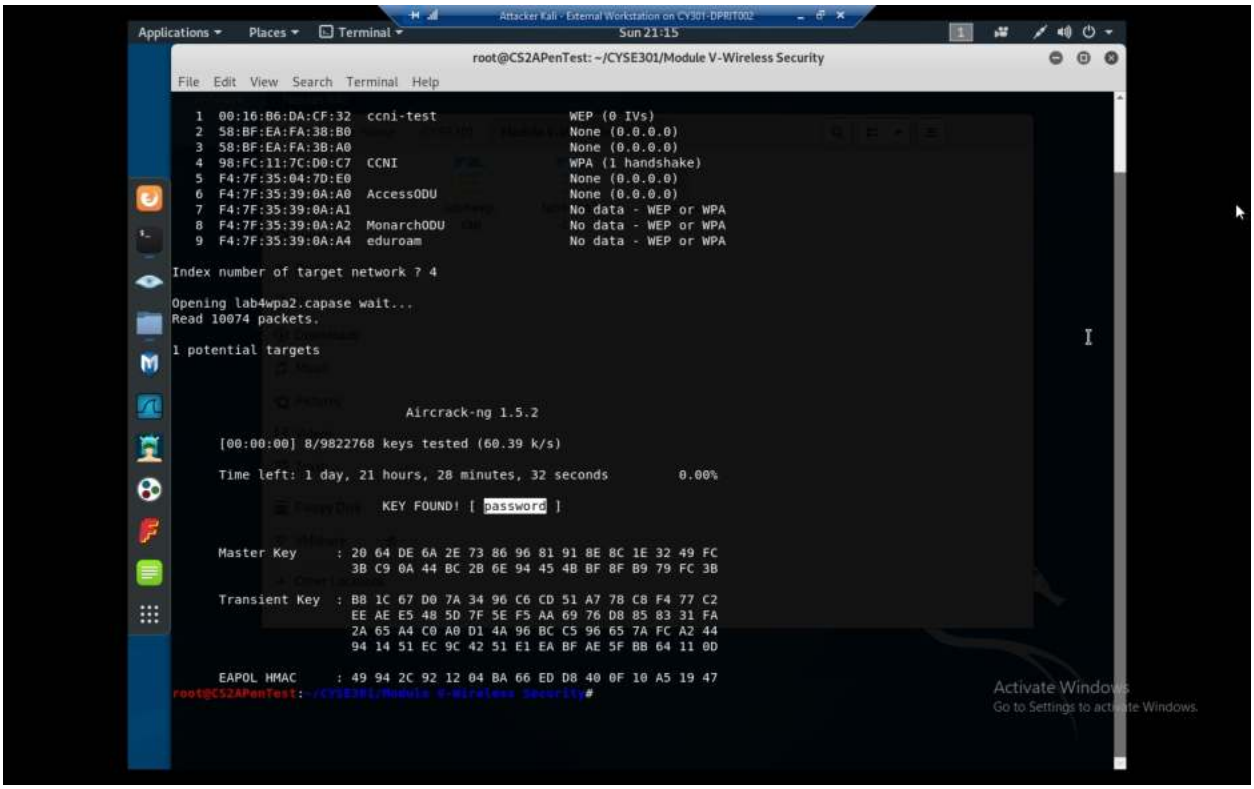


explanation: As we can see, much of this traffic is from 192.168.2.10

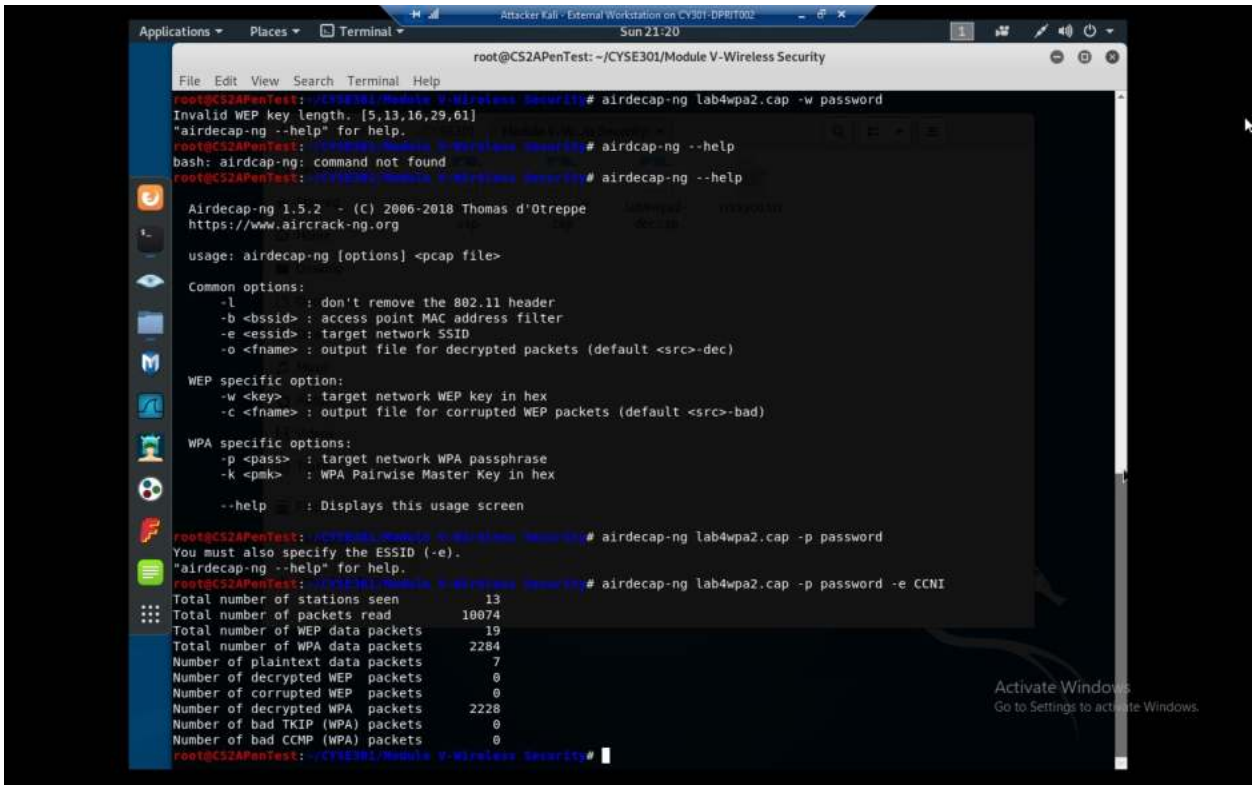


Explanation: And here we can see some of the resolved addresses, including music.163.com, apple.com, and dropbox.com

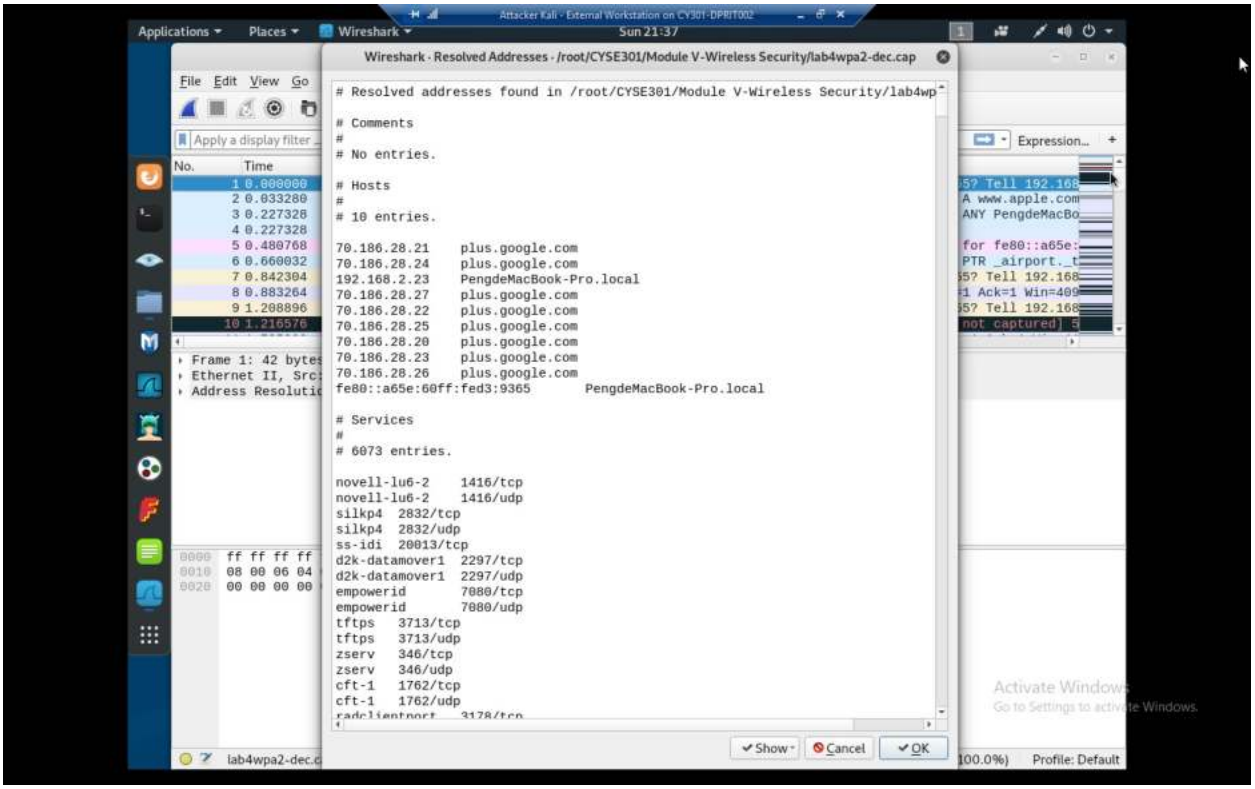
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)



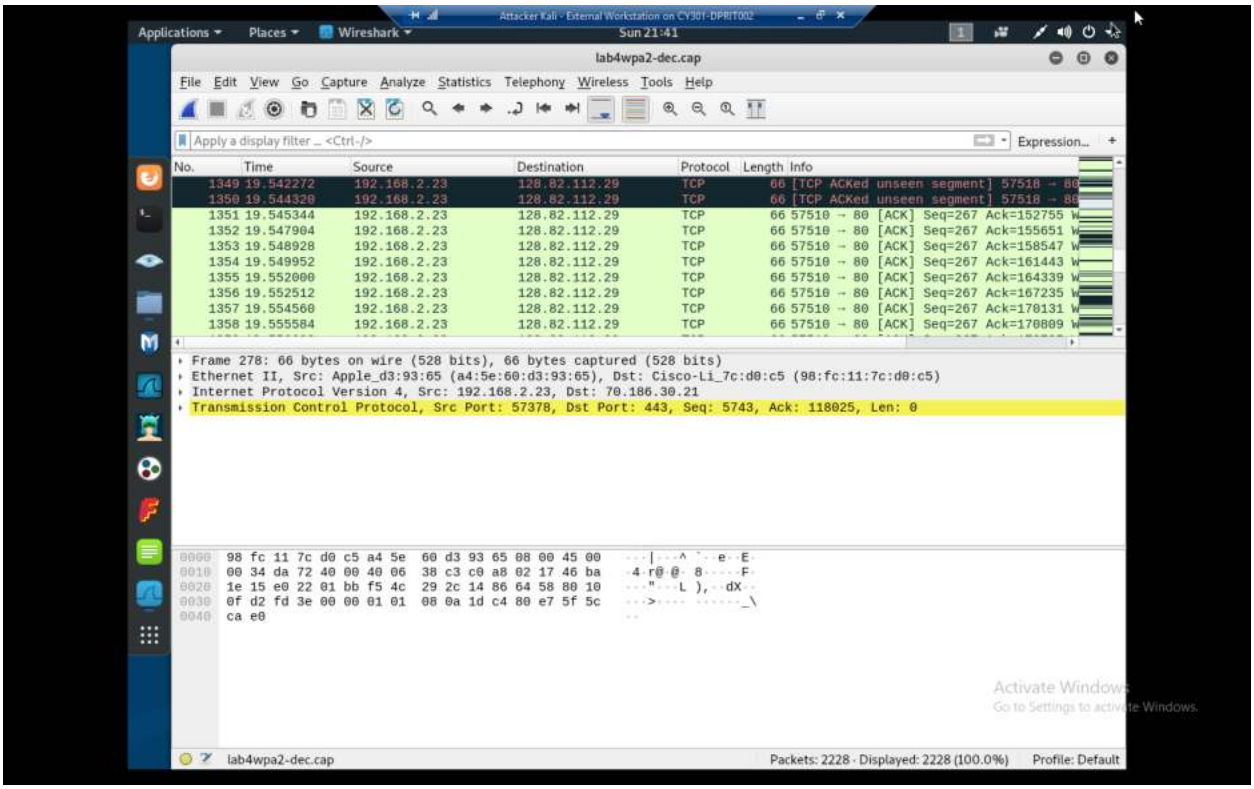
Explanation: Similar process to before, decrypting using the rockyou.txt dictionary and aircrack-ng



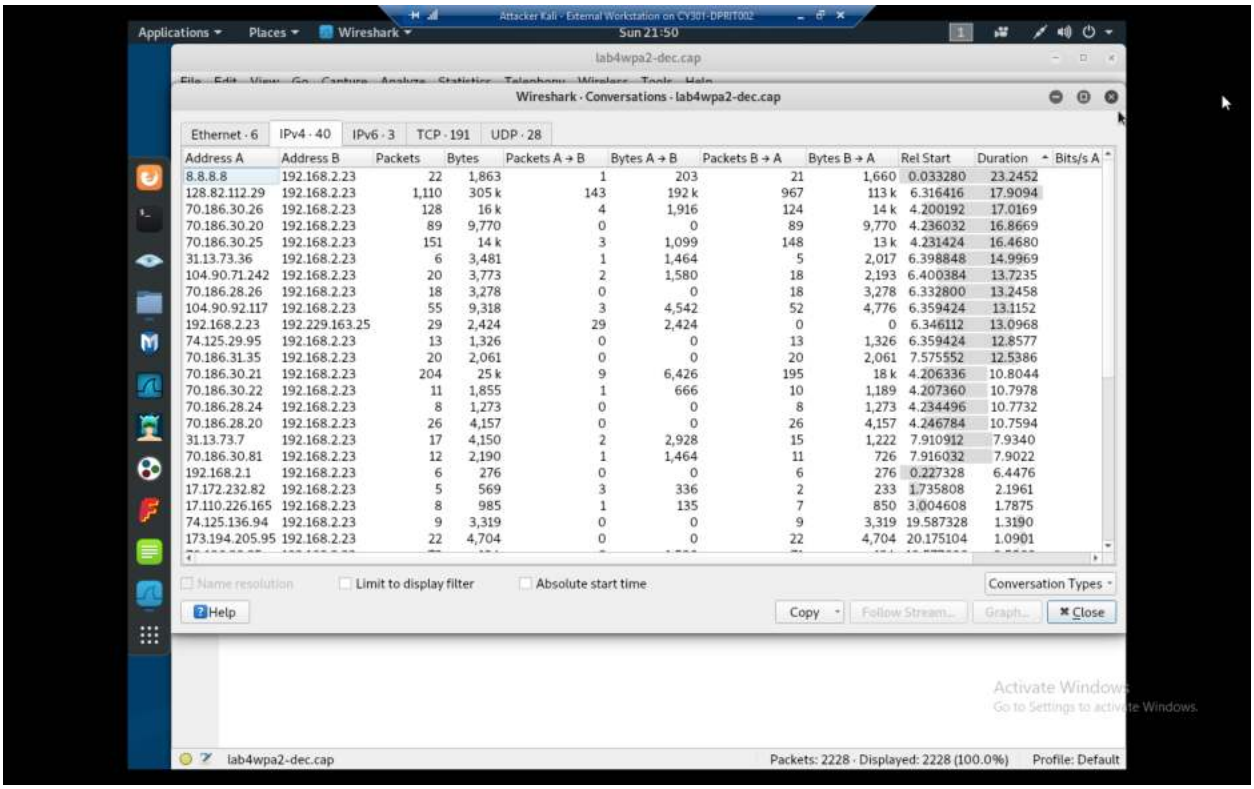
Explanation: After decrypting the traffic with airdecap, using the passphrase of "password" and the WPA ESSID



explanation: Resolved addresses of this traffic, mostly google plus traffic.



Explanation: Most of this traffic is also from 192.168.2.23



We can see here that while most of the time was spent in communication with 8.8.8.8 (google DNS) the next most communicated with address is 128.82.112.29

Task D: 30 points

Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below

and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the

last digit of the hash for pjiang is e. Thus, I should pick up the file "WPA2-P5-01.cap."

MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

You can find an online MD5 hash generator or the following command to get the hash of a text string,

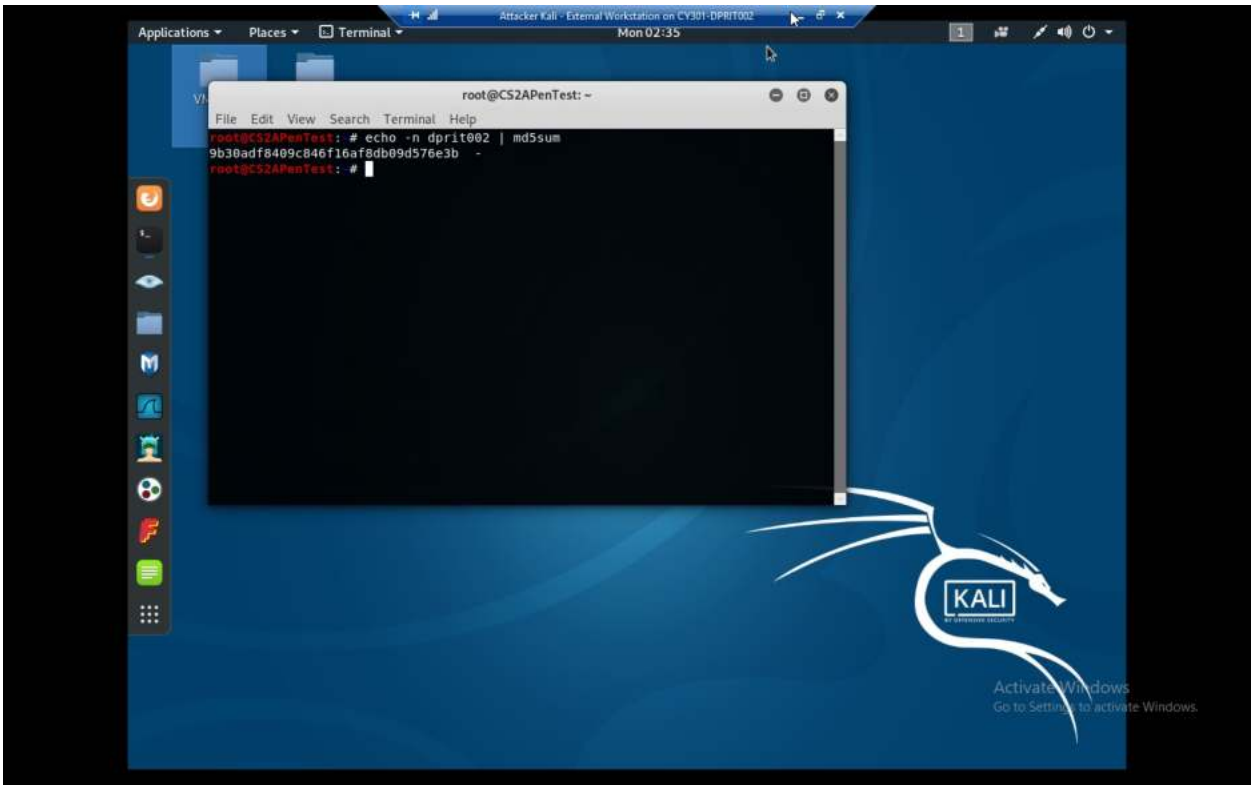
• The above files are zipped in a folder named "Lab Resources." You can locate the zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under the sub-folder "Wireless Traffic."

• Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine to access it from

the Kali VMs (you can use either Kali to complete the assignment).

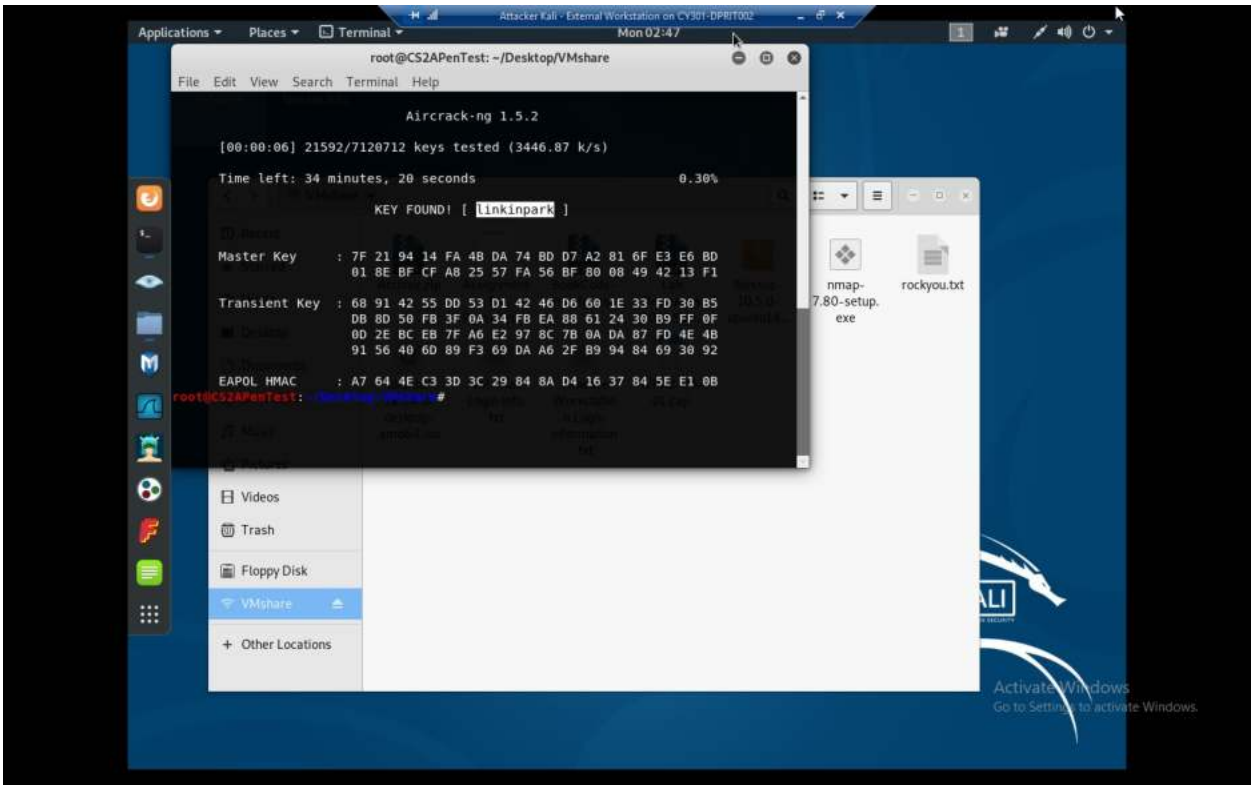
Figure left: Windows Host Machine Figure right: VMshare folder on Kali Linux

Then complete the following steps:

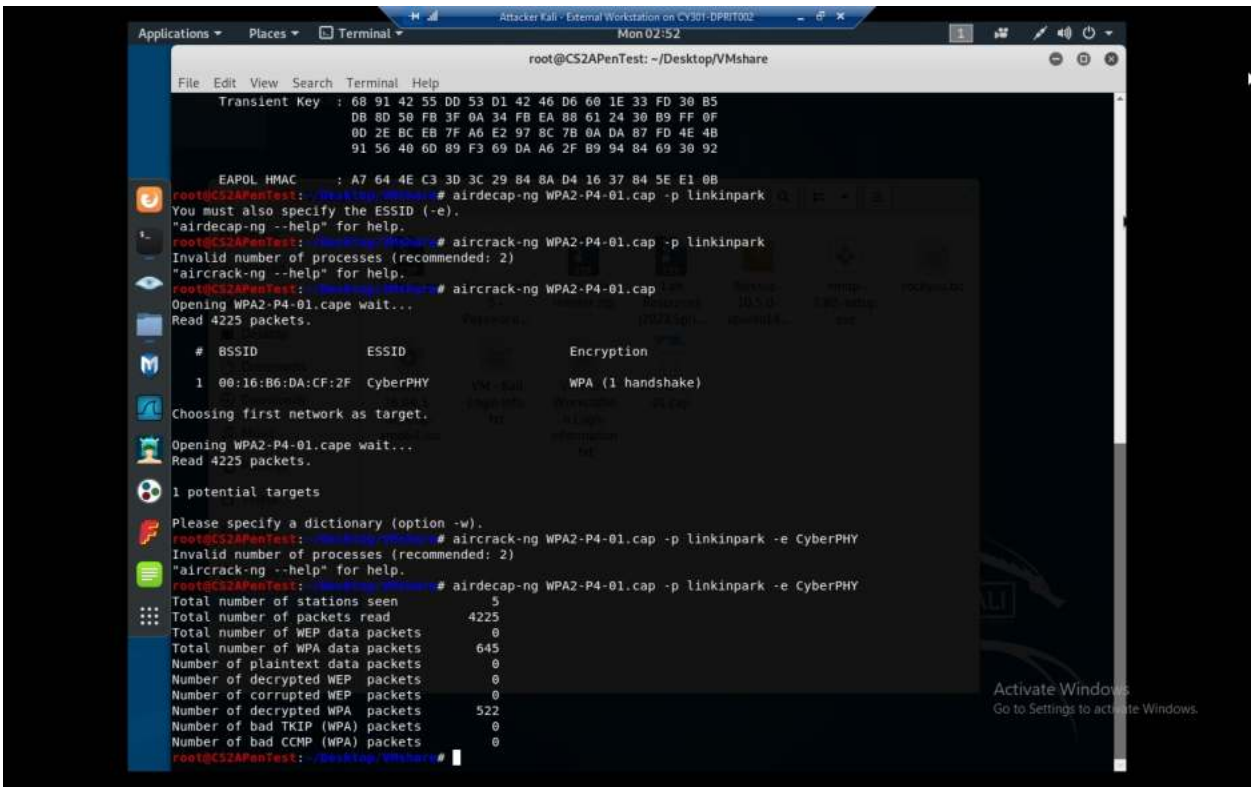


Explanation: the MD5 of my MIDAS ID is as shown and ends in “b” so my file is “WPA2-P4-01.cap “

1. Implement a dictionary attack and decrypt the traffic. - 20 points

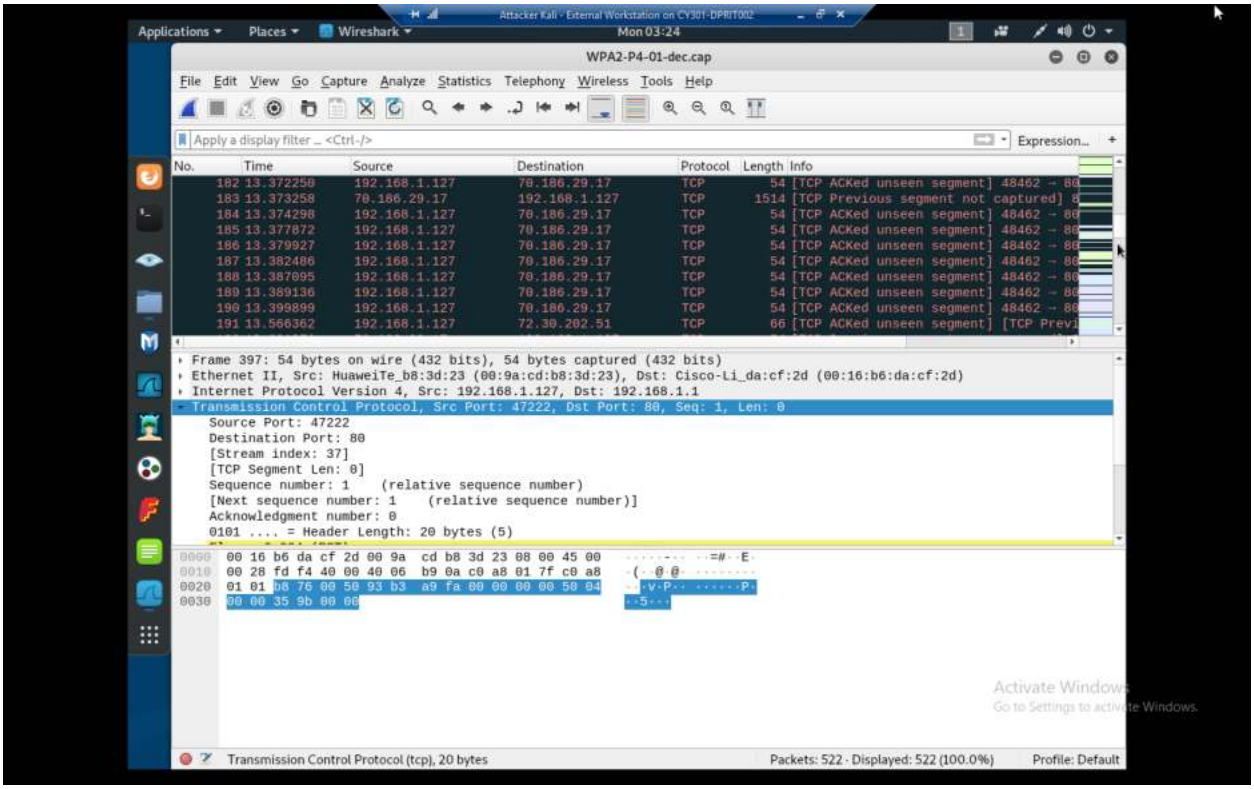


Explanation: after the dictionary attack we see the passphrase is linkinpark, rest in peace chester

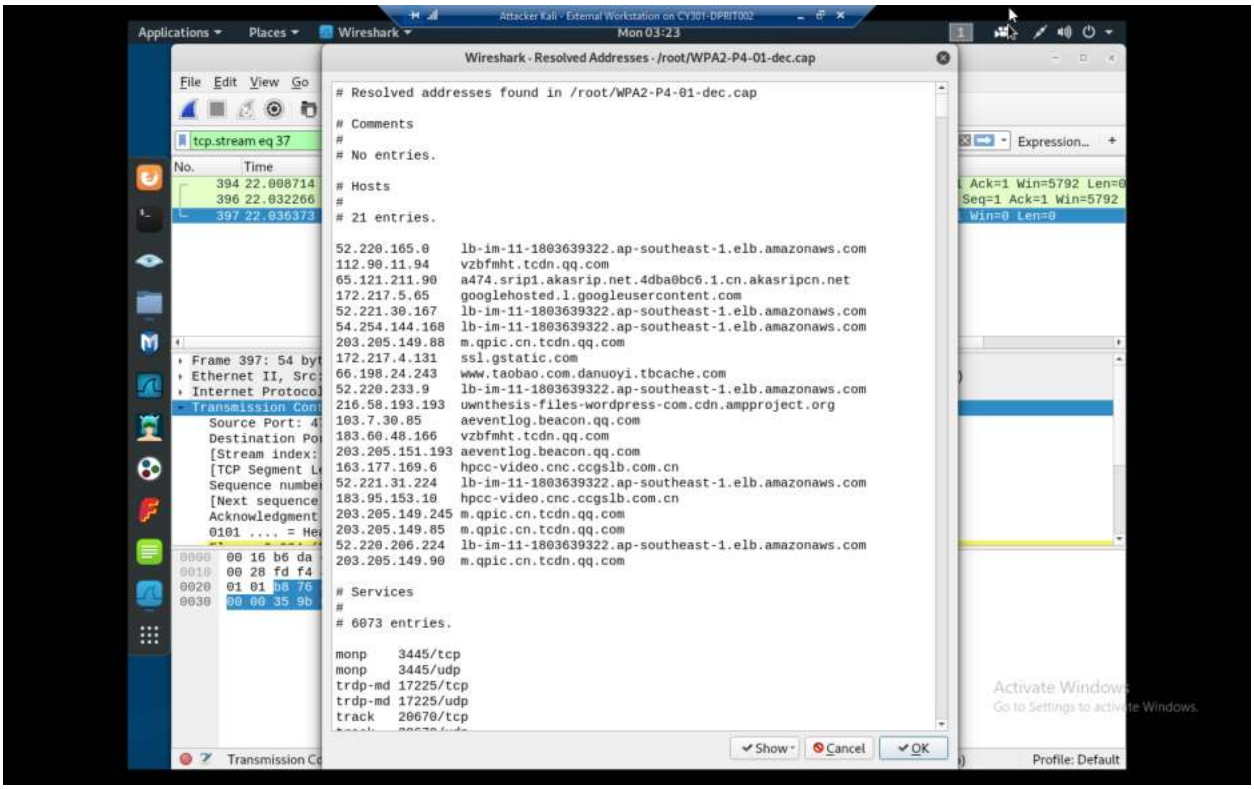


explanation: after cracking

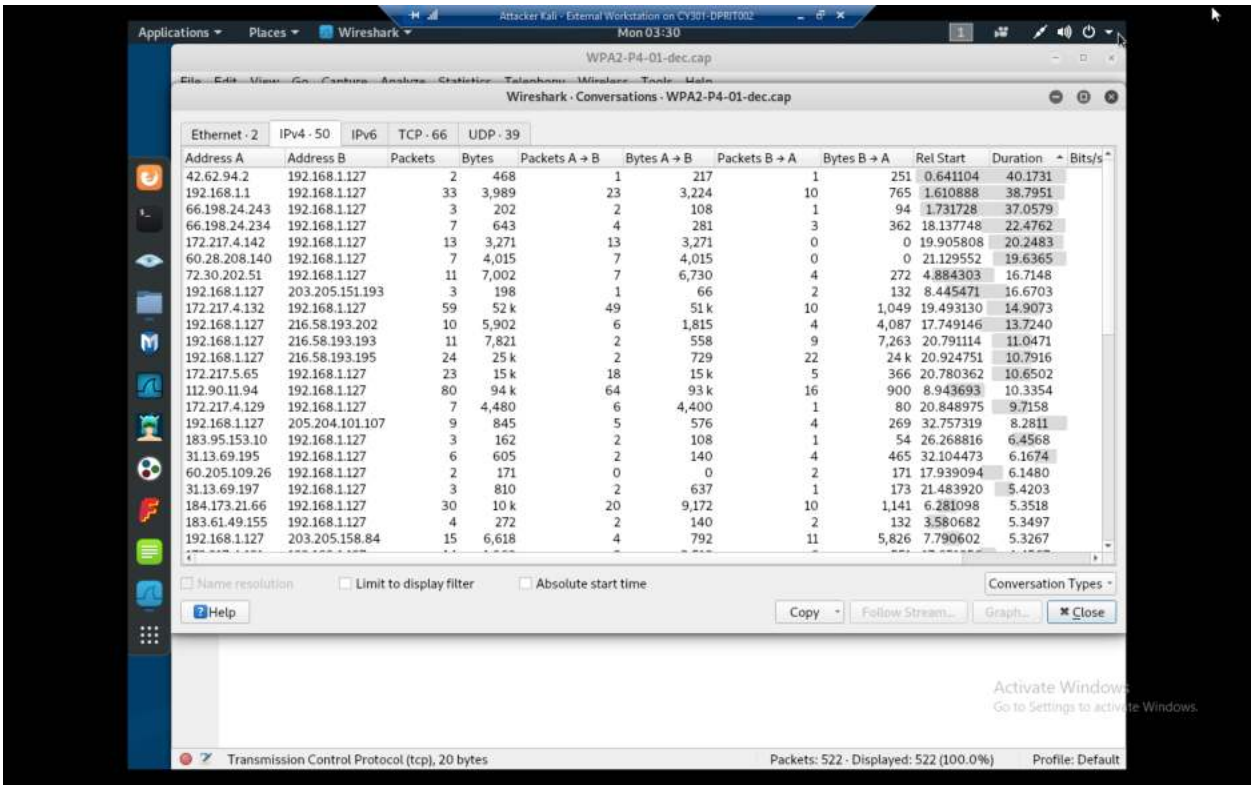
2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored
from this encrypted traffic file. -10 points



Explanation: the suspicious traffic in this file mostly comes from 192.168.1.127 and seems to have a large number of destinations. In particular here I'm looking at the traffic to 70.186.29.17, though there are many other addresses that have been communicated with by 192.168.1.127.



We can see here the resolved addresses in this capture file, seemingly a lot of interaction with AWS servers. Though, imaginably, it's probably because ODU uses AWS.



Explanation: We see here that 192.168.1.127 spent the most time talking to 42.62.94.2, followed by 192.168.1.1, but 192.168.1.127 looks like it's talking to everyone. I think 192.168.1.127 was doing a thorough nmap scan of the network.