OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Password Cracking & Wireless Security

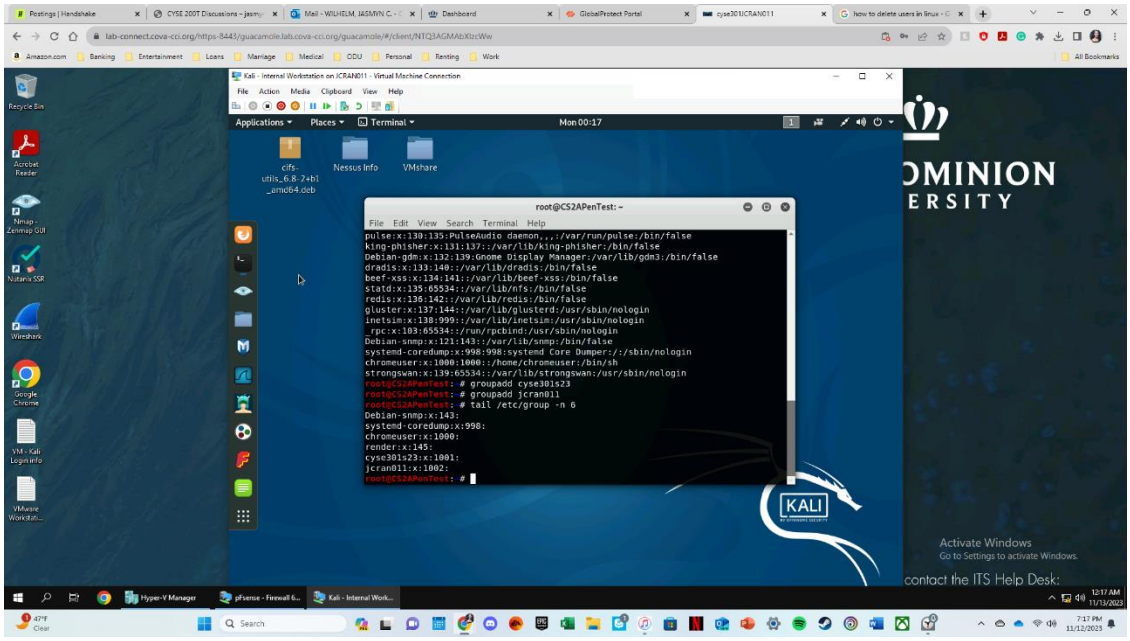
Jasmyn Wilhelm

01155323

Task A: Linux Password Cracking

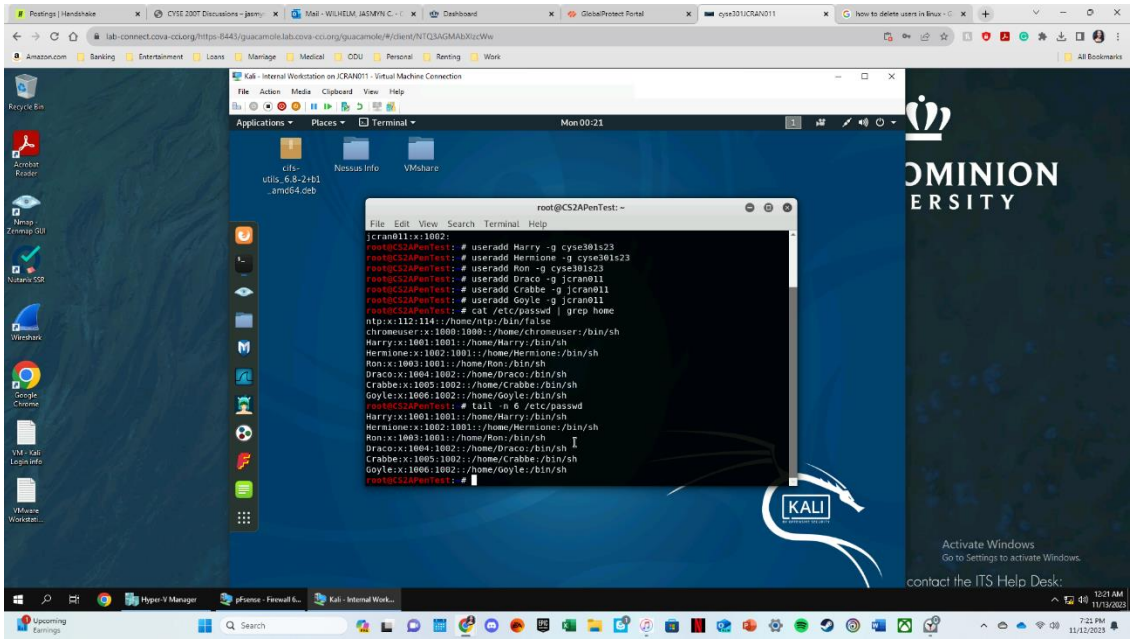
Question 1:

2 Groups were created (cyse301s23 and jcran011) using the “groupadd” command.

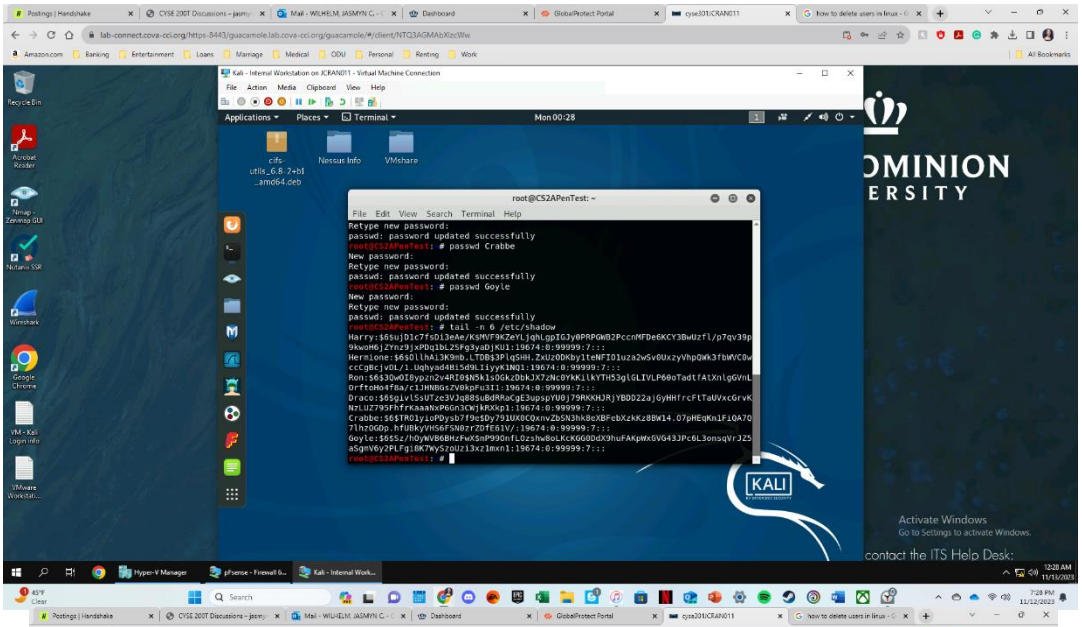


Question 2:

6 user accounts in total were added. Harry, Hermione, and Ron to group cyse301s23. Draco, Crabbe, and Goyle to jcran011.

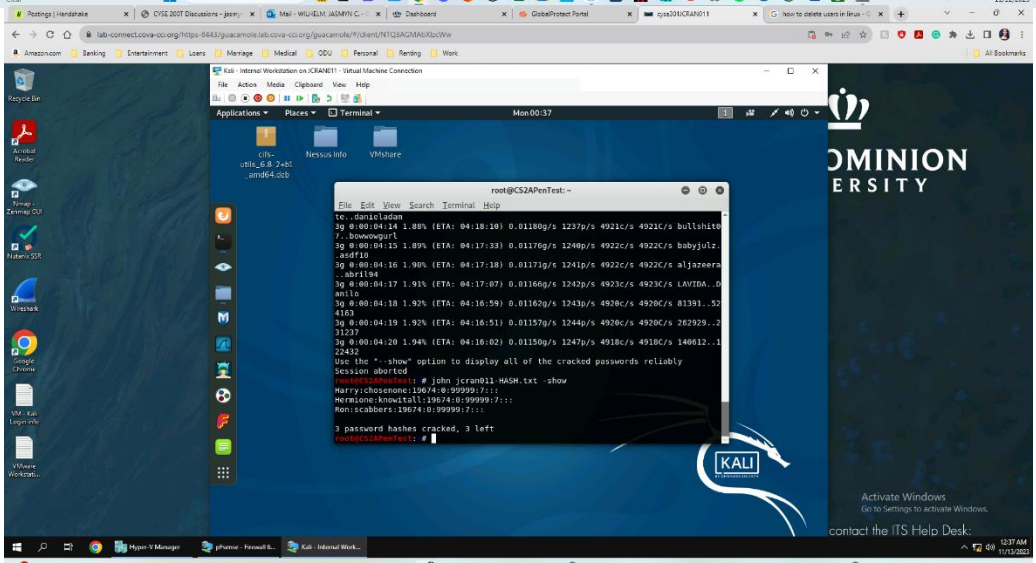


Question 3:
Unique passwords for each user were created as follows:
Harry: choseone
Hermione: knowitall
Ron: scabbers
Draco: Greenapple!
Crabbe: CuPcAkEs
Goyle: darkart$123



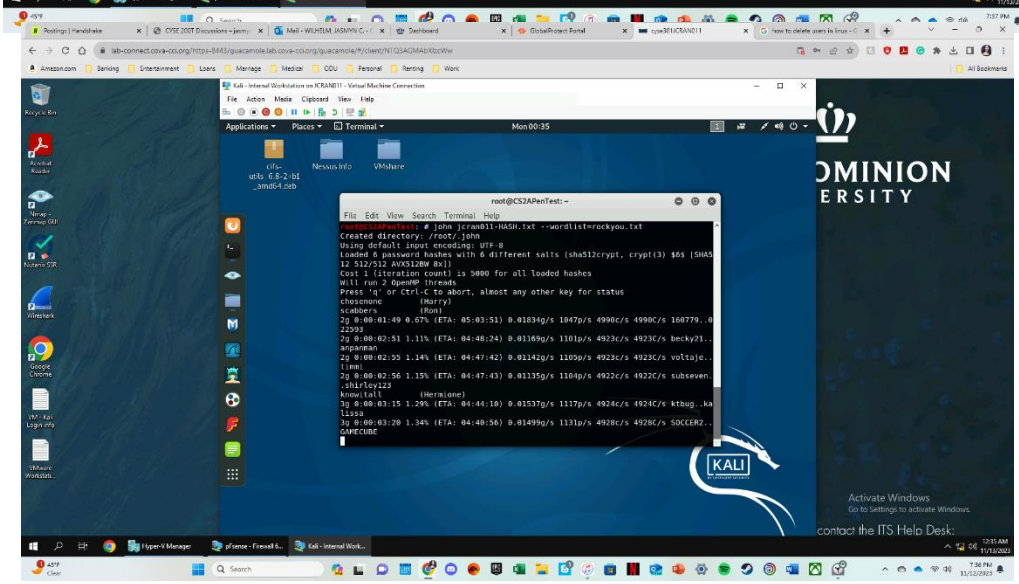
Questions 4:

This screenshot demonstrates how to use an attack to display the passwords. The passwords for Harry, Ron, and Hermione are shown after being cracked using the John the Ripper method.



Question 4 part 2:

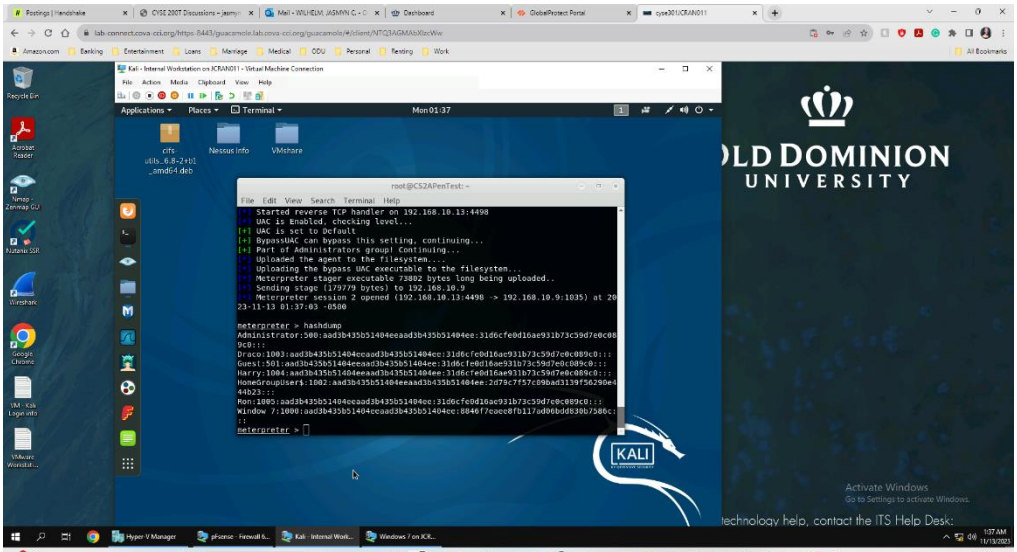
This screenshot is another view of Question 4.



Task B: Windows Password Cracking

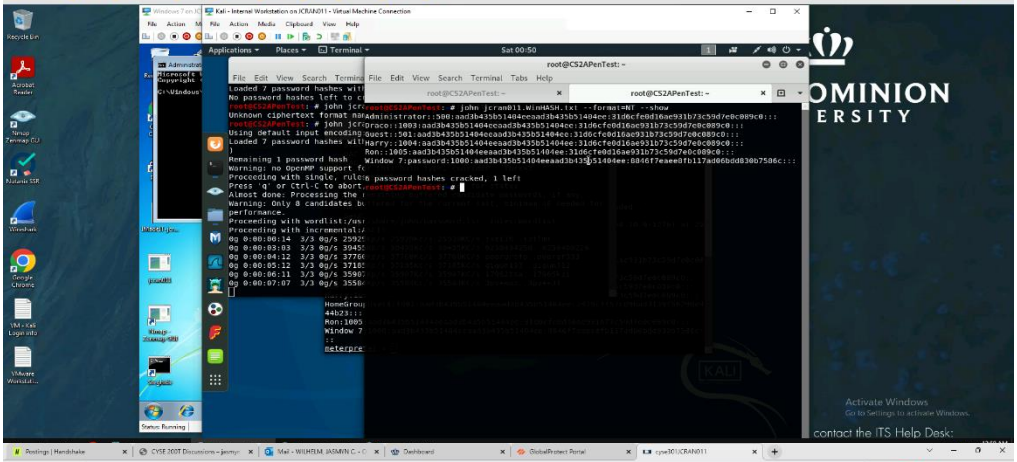
Question 1:

After accessing Metasploit and gaining administrative access onto the target, I used the Hashdump command to show the users and passwords.



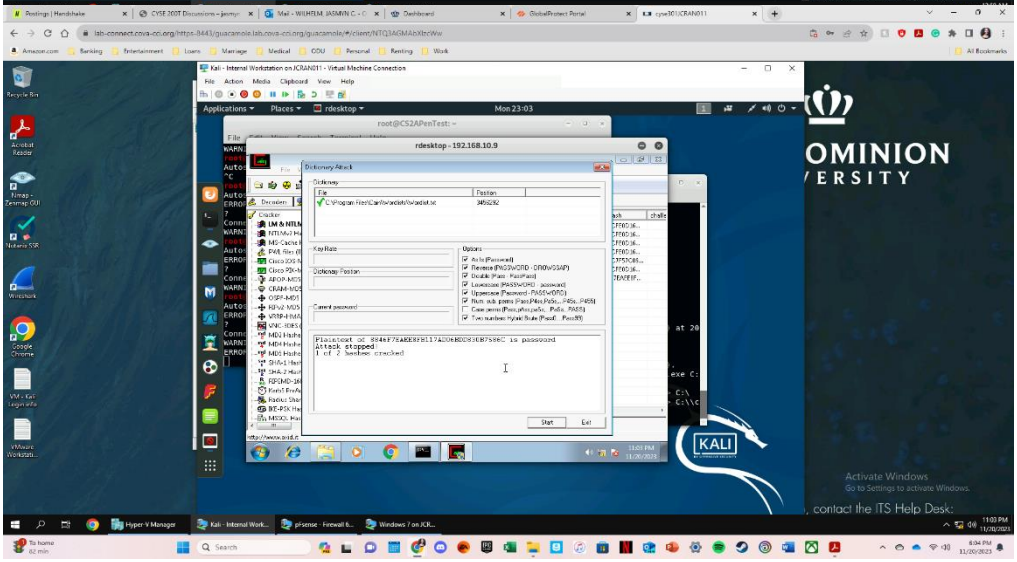
Question 2:

The passwords and user listed in the hashdump command were saved into a file labeled jcran011.WinHASH.txt. John the Ripper program was run to crack the passwords.



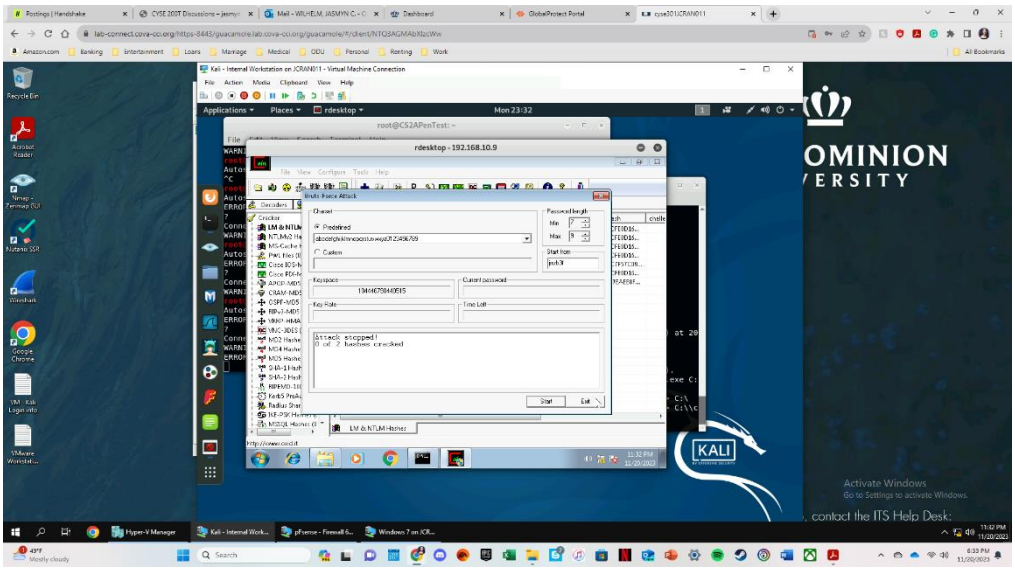
Question 3 part A:

Cain and Abel program was downloaded to the target and a Brute Force and Dictionary attack were executed. Showing at least one password cracked. This picture shows the dictionary attack.



Question 3 part 2:

This picture represents the Brute Force attack mentioned in Question 3 part A.



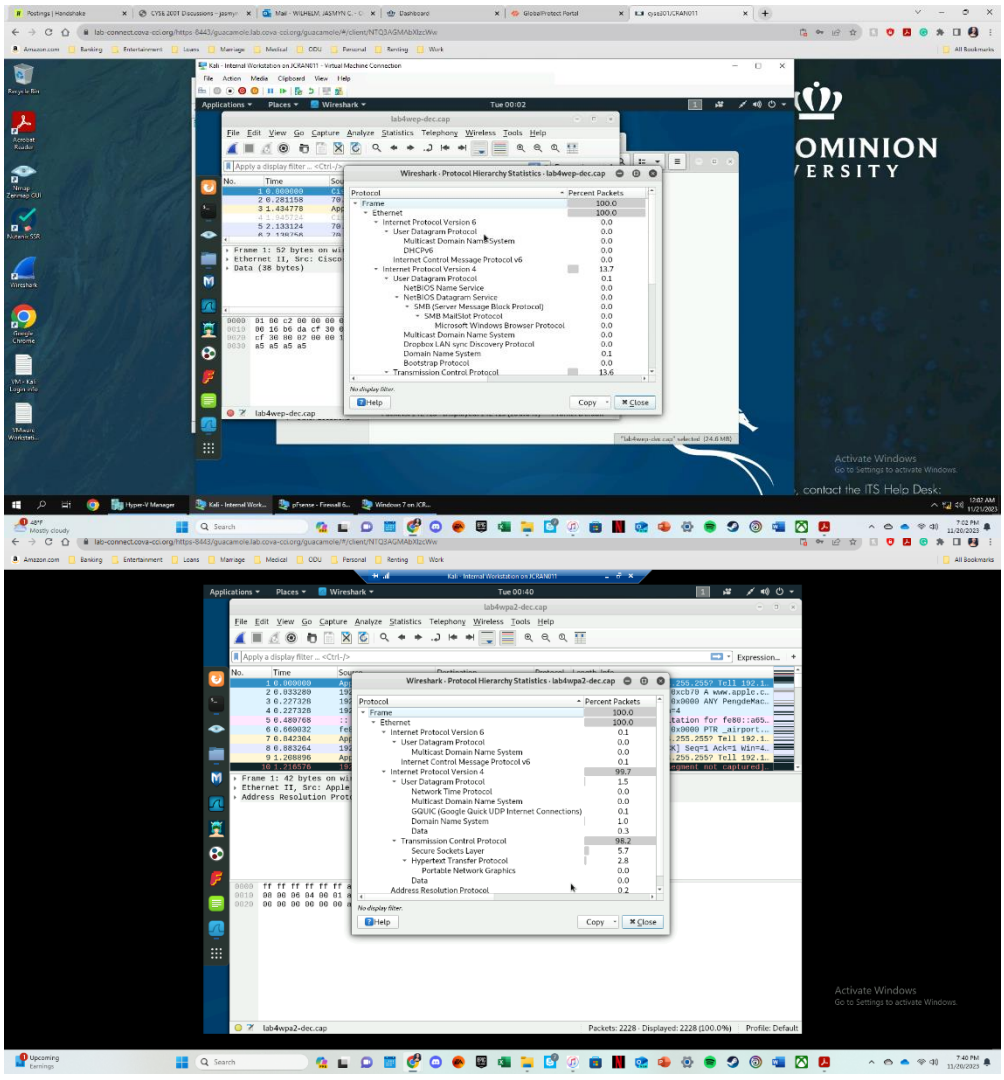
Task C: Wi-Fi Cracking

Question 1:

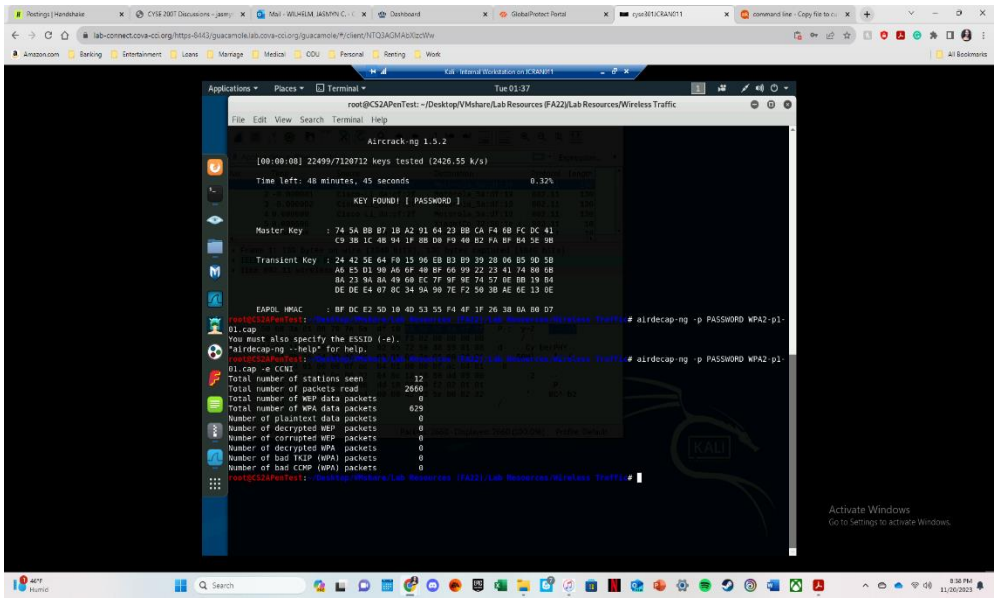
A dictionary attack was run on the Wireshark file allowing a password to be revealed to decrypt the traffic. This shows the Protocol Hierarchy of the decrypted traffic.

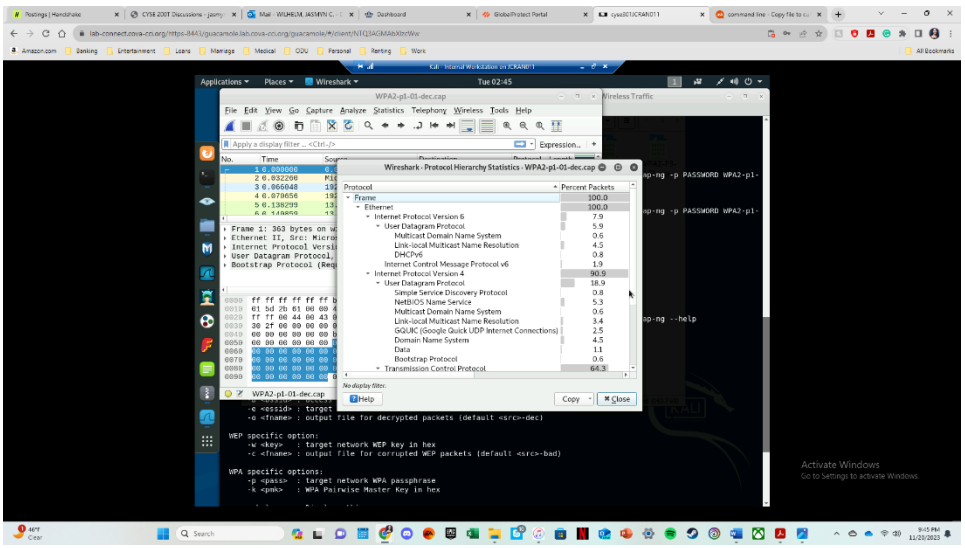
Question 2:

The same steps were run to decrypt this Wireshark file. Except, finding the passphrase require a dictionary word in which a wordlist was used to help solve. This is the result of decrypting this WPA file.



Task D: Wi-Fi Cracking





Questions 1 & 2:

This task required a specific WPA file to be used for the same process. My Midas ID of jcran011 was to be generated into a hash. The last number of the hash would determine which file I would decrypt. This process was different in the sense the same steps were in previous tasks used, but the file was in a different location requiring me to unzip the folder and access the VMshare file and specific folders in it. The same steps of figuring out the passphrase were used, but the ESSID was labeled as CyberPHY. The file was then decrypted, and the Protocol Hierarchy Statistics are shown. The difference between the encrypted and unencrypted is the amount of information given. Before the file gave very little information and categories, but once that was unraveled more categories were shown, and the percentage of packages within it. Before you could only see the traffic coming from 802.1X Authentication, but later is shown the user control and internet message protocol packets.