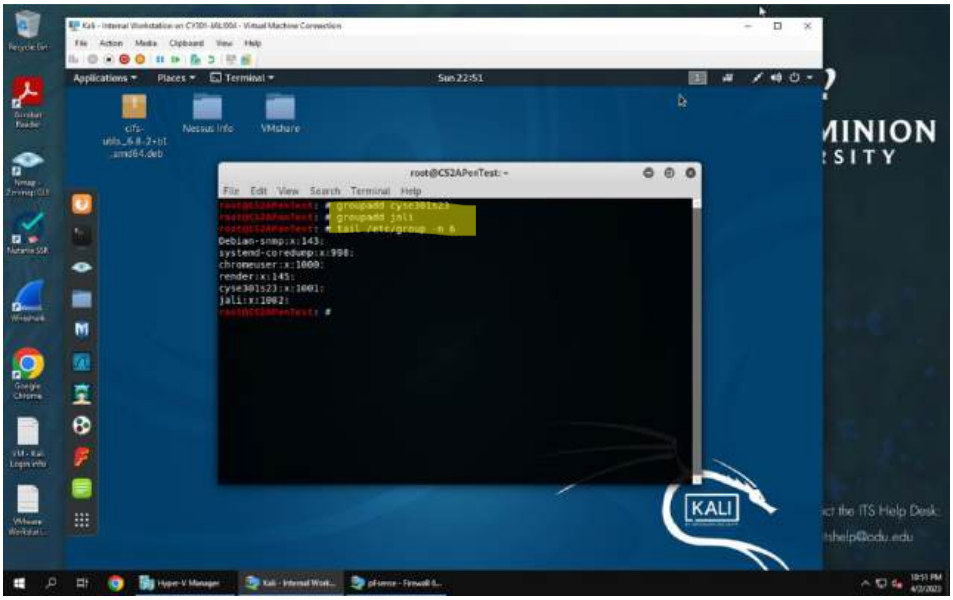
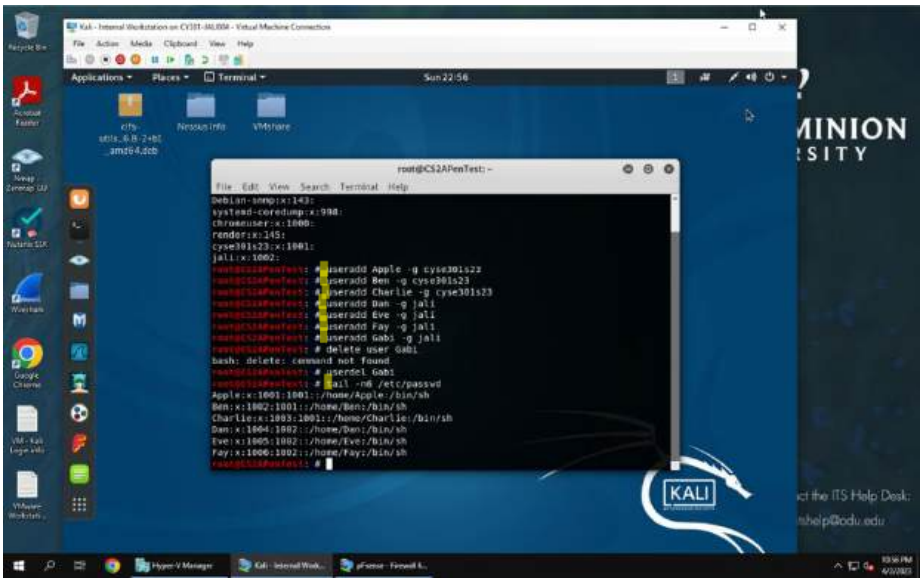
PART A

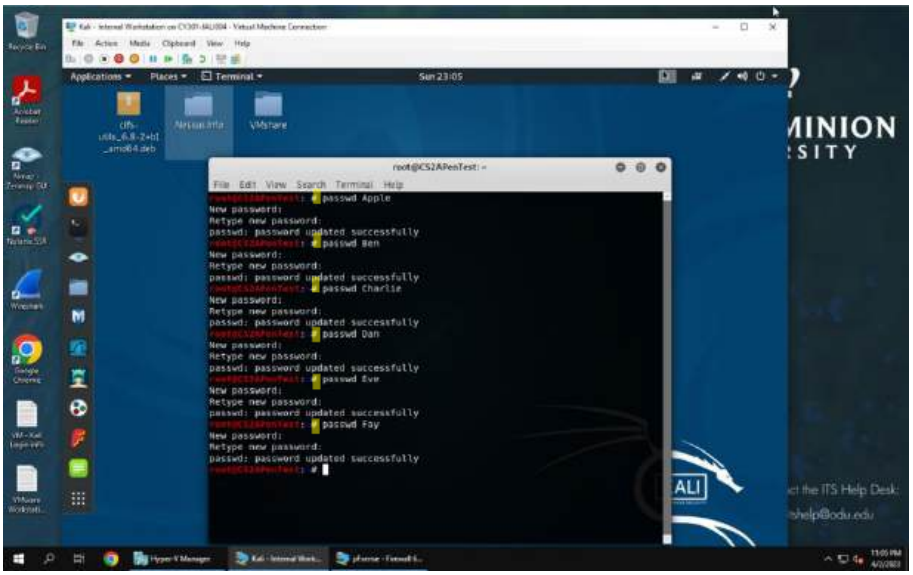
TASK A: LINUX PASSWORD CRACKING

Username & Passwords for lab task A: Apple 12345678, Ben TheSt!r8, Charlie H-h1LLzp, Dan c_c_7huk, Eve ChAnCe12, Fay !-_-h51_ .



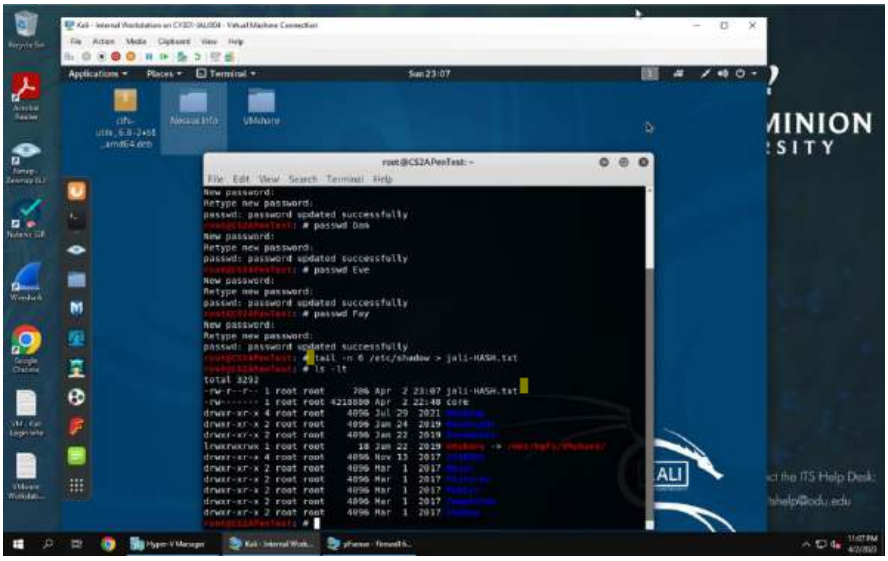
1. Created two groups, one being syse301s23 and the other being jali using the command groupadd. Then I displayed the corresponding group IDS using the command tail /etc/group -n 6. The command is telling the machine to display the last 6 lines at the end of the etc group file.



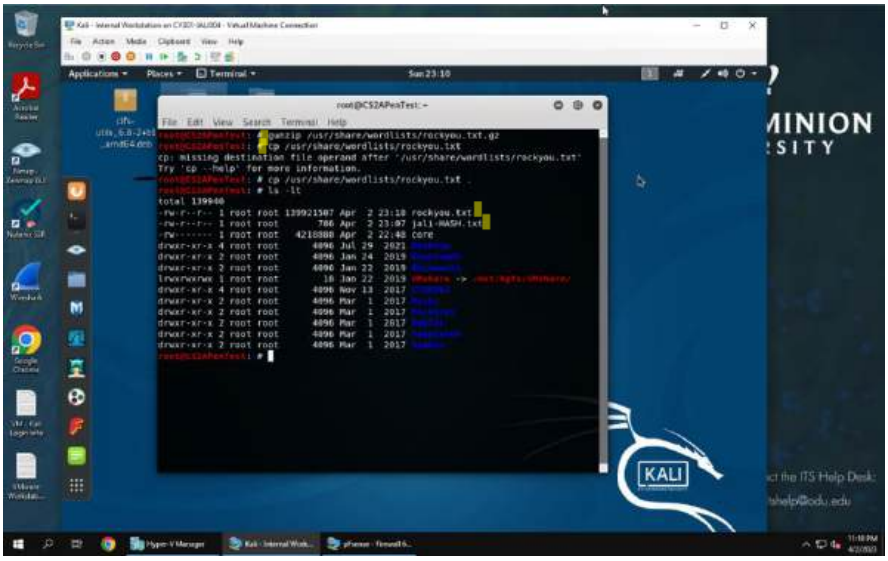


2. Created and assigned users to the groups I had previously created using the command useradd with the -g to assign that user to a group. I used the command tail -n6 /etc/passwd to display the newly created users' UID and GID information. All users match what group I put them in or the GID is correct with what I had defined.

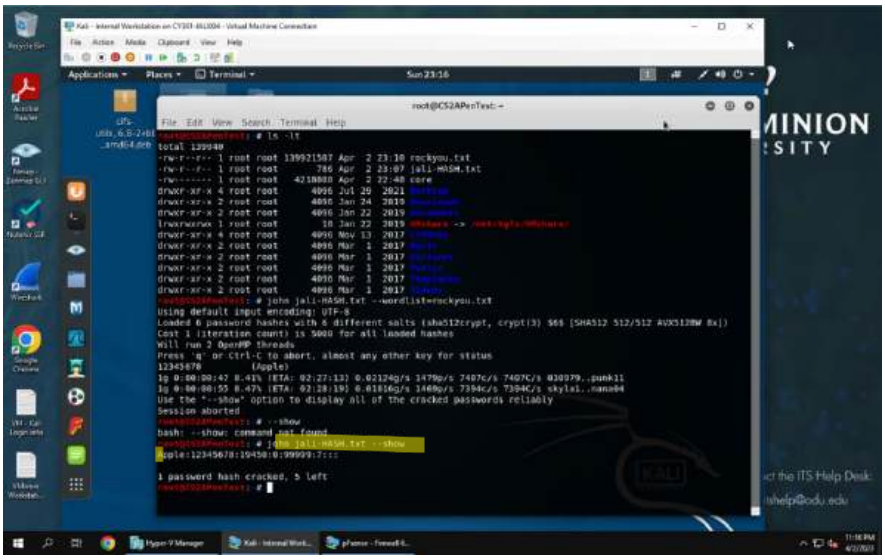
3. I then assigned each user a password with the command passwd. I also created one to many users and had to use the command userdel to delete that user.



4. Lastly I exported all six user's password hashes into a file named jali-HASH.txt with the command tail -n 6 /etc/shadow > jali.HASH.txt . I then double checked this with the command ls -lt to make sure I had exported hashes to a file correctly. I'm looking for the correct name, date, and file size.



4. Next, I need the wordlist for my dictionary attack and also unzip a file in Kali. I do this by using the command gunzip and then specify the path and what file I need to unzip. Then I want to copy this file that I just 'opened' to my current working directory, I use the command cp followed by the path and the specific file I want followed by a space and . I double check using the command ls -lt to double check that I now have this file where I need it to be so my dictionary attack has the format I specify, and the format being the rockyou file.

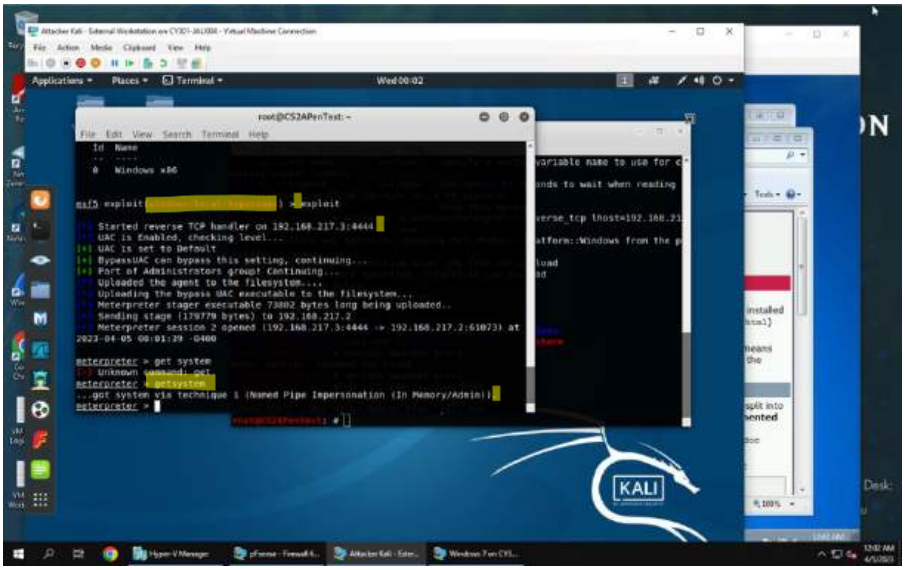


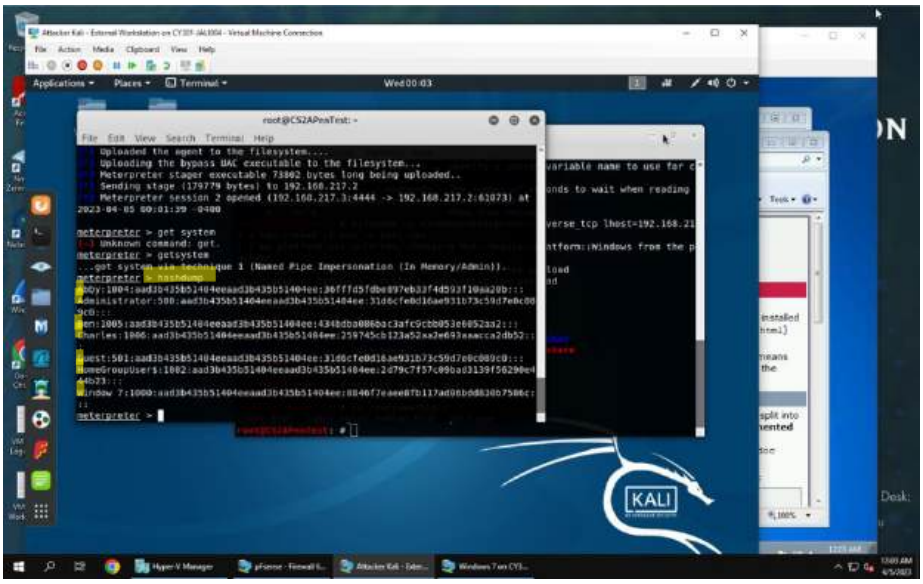
4. Now that I have double checked that the file is where it needs to be, I can move on to executing the command john so I can crack the passwords. I use the command john followed by my file with hashes jali-HASH.txt followed by my format --wordlist=rockyou.txt .I let it run for a bit and then abort and then use the command john jali-HASH.txt --show so I can see what has been found. The user Apple's password has been compromised.

TASK B: WINDOWS PASSWORD CRACKING

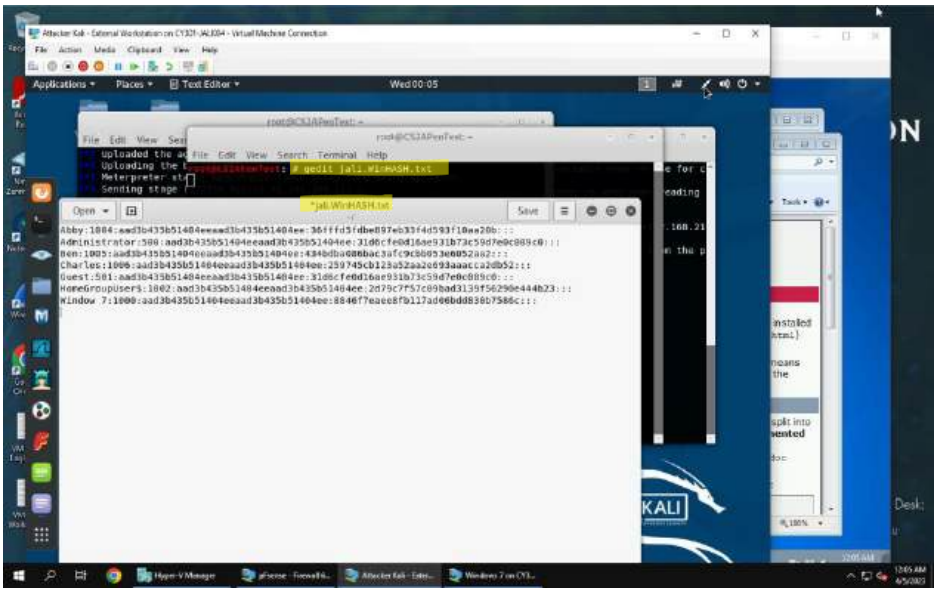
Username & Passwords for lab task A: Abby Ham12345, Ben Cheese12, Charles 12345678

Created users through Windows 7 VM with different passwords, then I moved on to establishing a reverse shell using what I learned in the previous assignment. I created a fake website with a malicious file to create a connection and then escalated that malicious connection to admin priv. level as shown below.

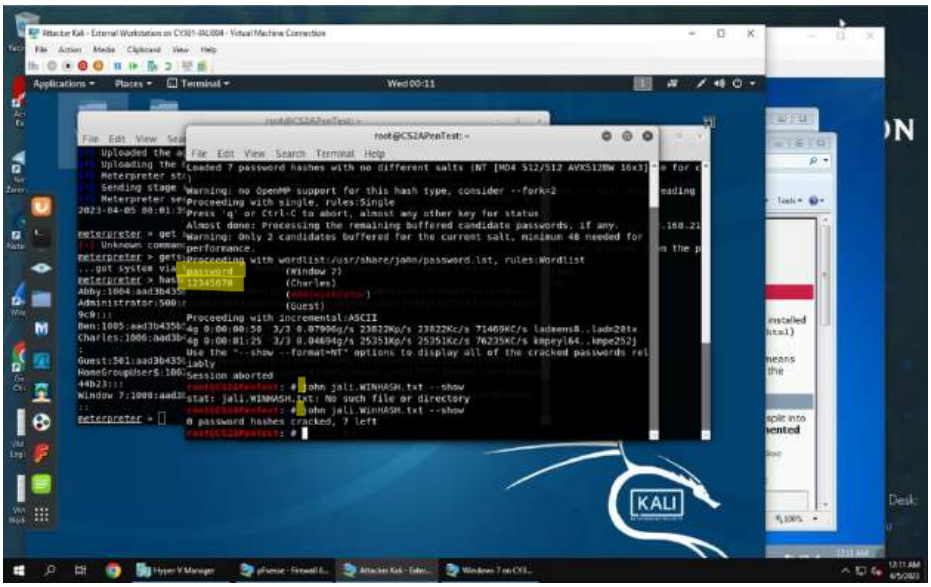




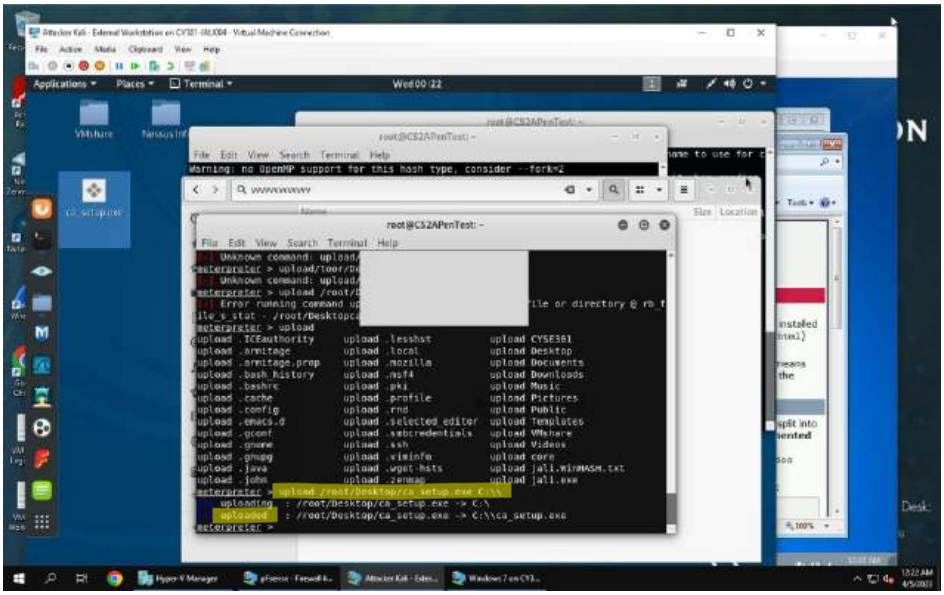
1. Once I have a successful admin level privilege reverse meterpreter shell using the command getsystem to initiate, then I use the command hashdump to display user UID and hashes. Then I copy the contents and move on to the next step below.



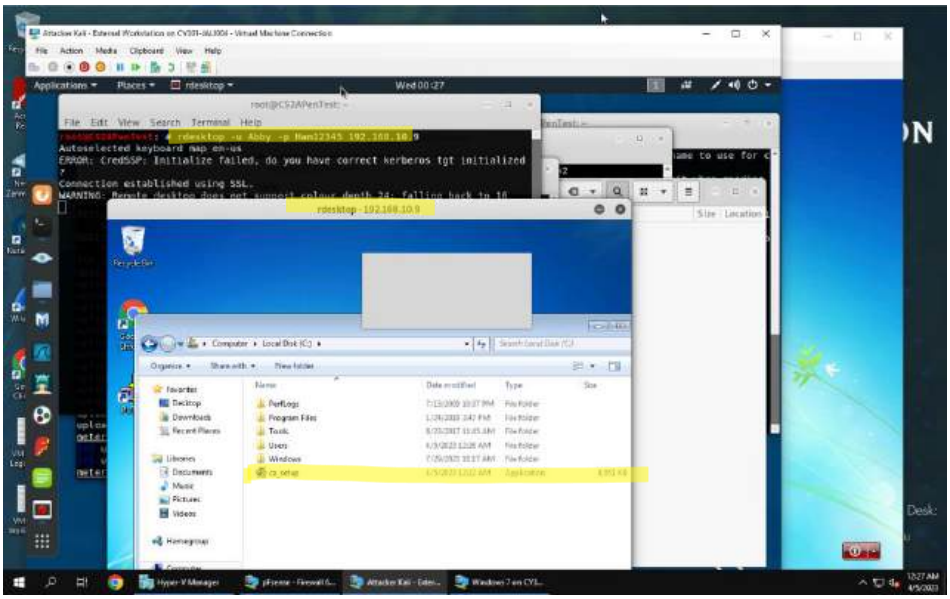
2. I use the command gedit followed my the title of the file I am creating jali.WinHASH.txt , and then paste what I had copied from the meterpreter shell. I will use this file so the John command can look through it and tell me the passwords.



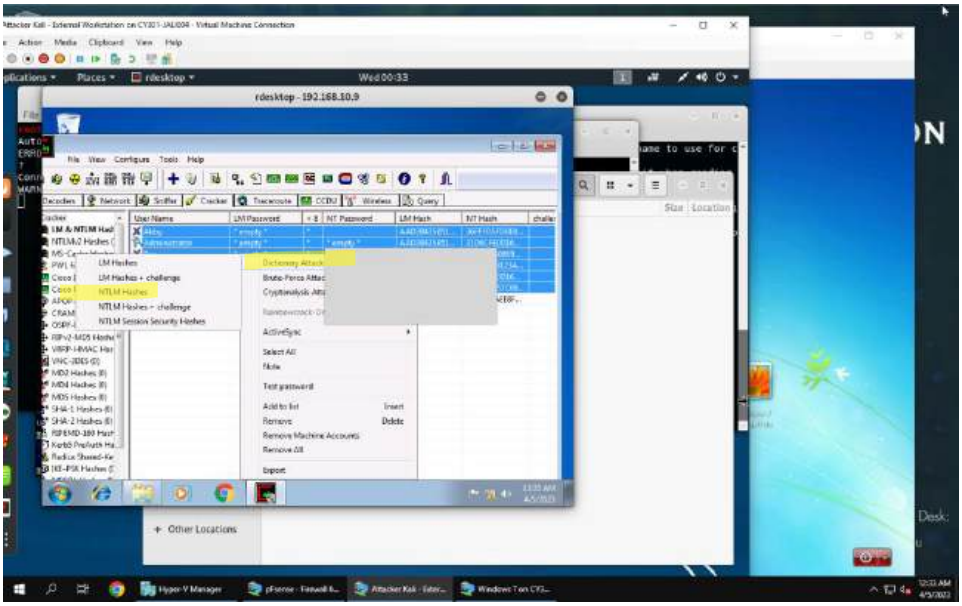
2. I start trying to crack the passwords using the command john followed by the file I just made, jali.WinHASH.txt followed by the format, --format=NT. The users Window 7 and Charles are compromised as circled above. I realized later, not shown in the screenshot that when I use the shoe command I have to specify the format as well, just like in task A. I did not here but realized, as show in the screenshot, that John already found two for me. So I moved on to the next task.

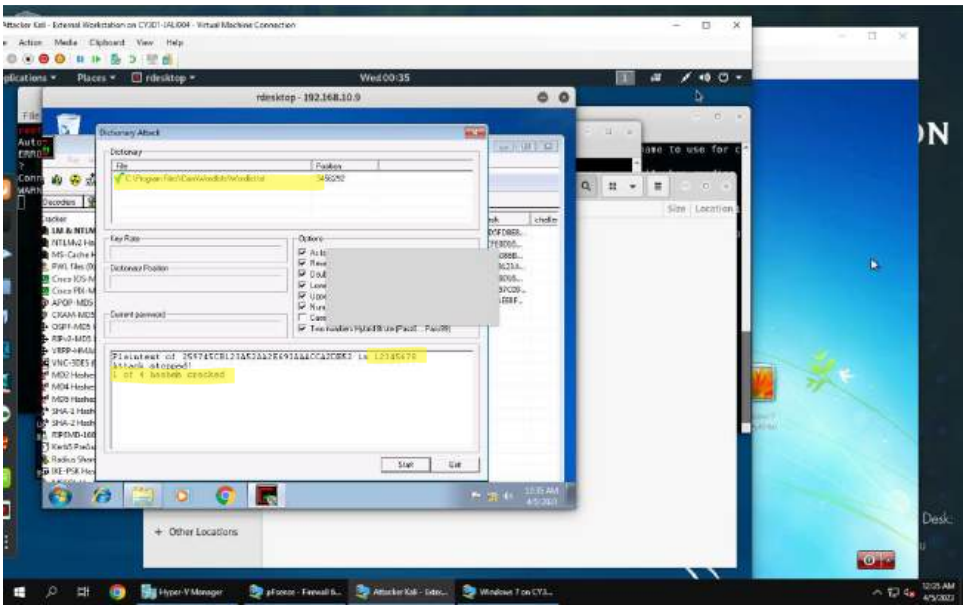


3. Shown above is me fumbling with the correct path for the ca_cetup.exe file because I had moved it to my Attacker Kali desktop, so I can upload the malicious Cain and Abel to Windows 7. Setting up so I can access it via remote desktop later. The correct command is upload followed by the path of the file I want /root/Desktop/ca_setup.exe followed by where it needs to go C:\\ . Also, this little box showed up in the middle of my VM. Next I move onto starting up a remote desktop on my infected Windows 7 VM.

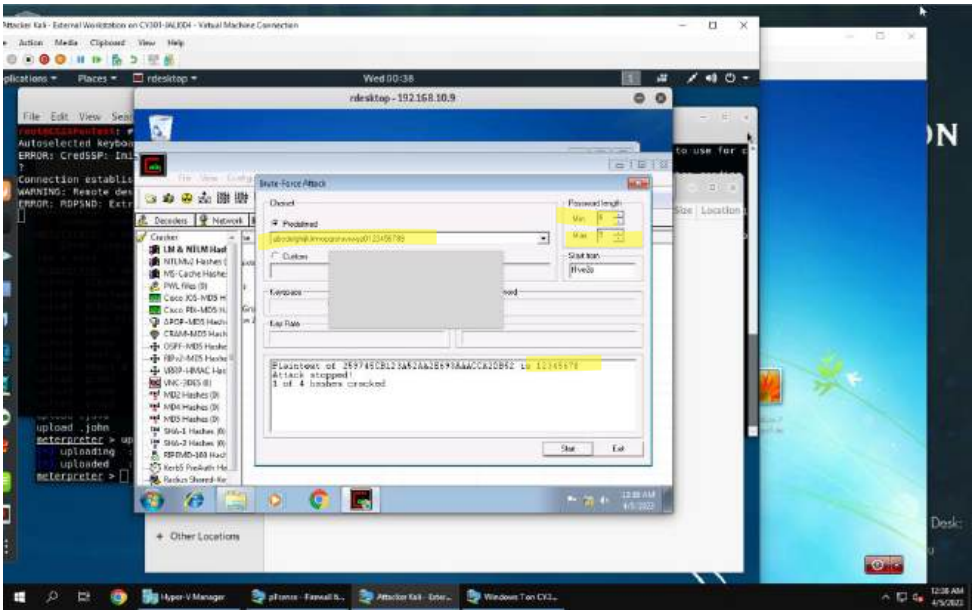


3. I use the command rdesktop followed my the user name, password, and IP of my target (windows 7, user is Abby), -u Abby, -p Ham12345, 192.168.10.9. I then click on ca_stup and download Cain and Abel. Then I begin a dictionary attack using Cain and Abel.



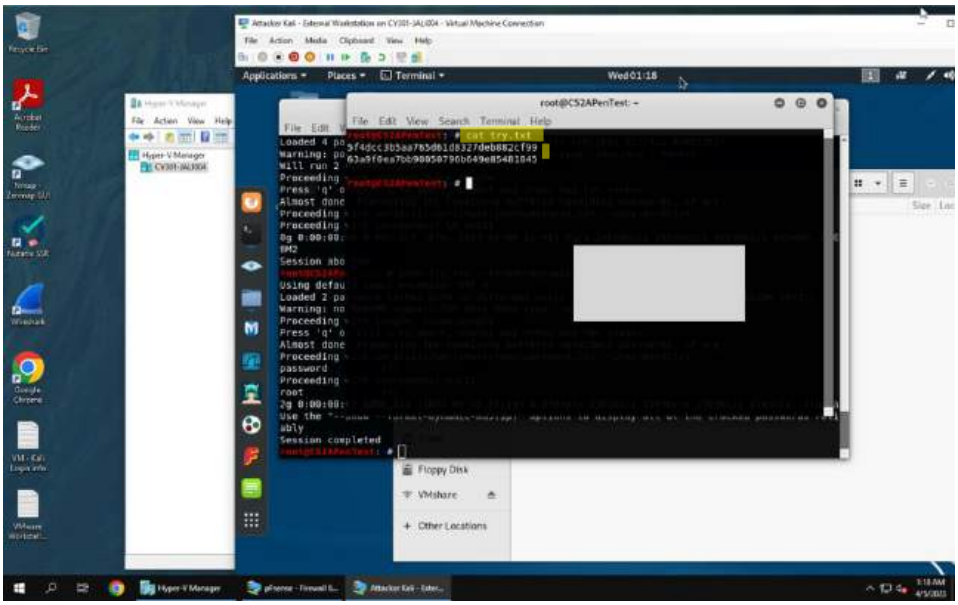


3. I right click and add the users I want based on what options I would like, and then highlight again and right lock to specify NTLM Hashes, followed by the file I would like to use, such as the wordlists file shown above and begin the dictionary attack. One user is compromised with the password 12345678.

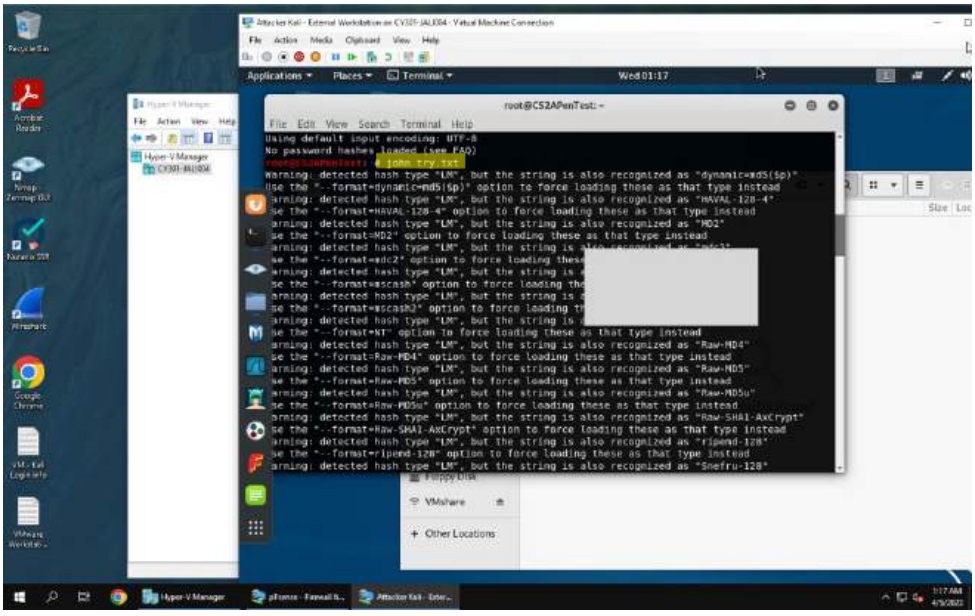


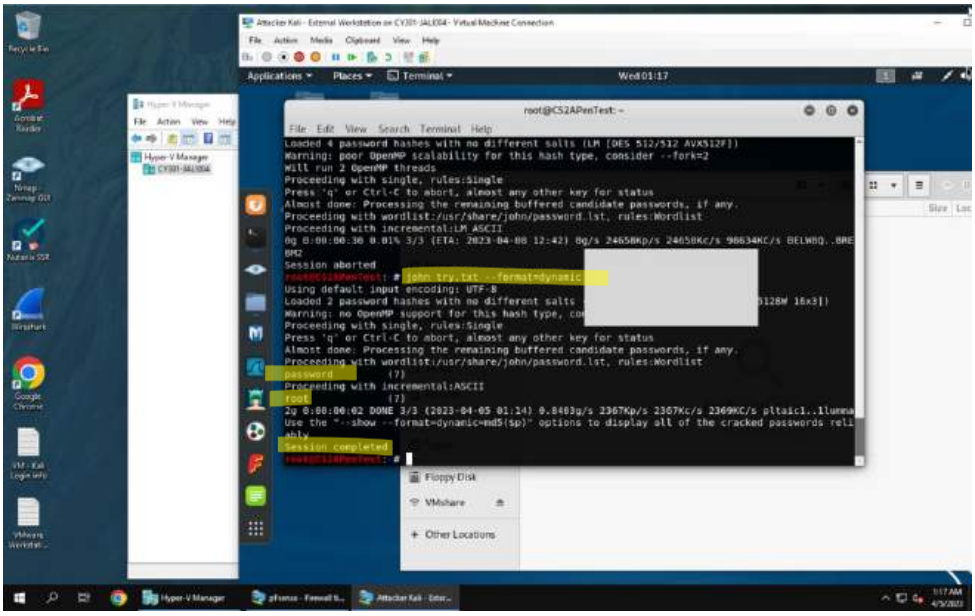
3. I do the same thing for a brute force attack, minus the specification of a wordlist file but still specifying NTLM Hashes and I limit the min and max password length to cut down on time and stop the attack once I have one cracked password. One user is compromised with the password 12345678.

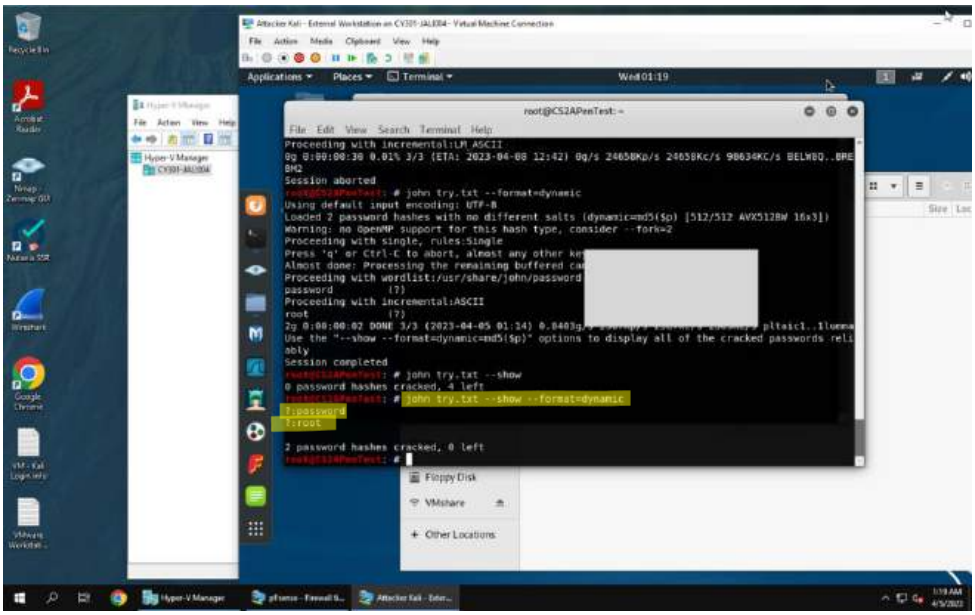
TASK C: EXTRA CREDIT



Extra Credit: I close my remote desktop and return to Attacker Kali's root shell. I then create a file with the command gedit followed by the file name I chose, try.txt . I then added the hashes from the lab assignment page. I use the command cat try.txt to double check that the file contains the hashes I want to crack. Then I use the command john try.txt so it can suggest formats. As shown below, is me fumbling through the correct formats until I figure out the best one to use is --dynamic.







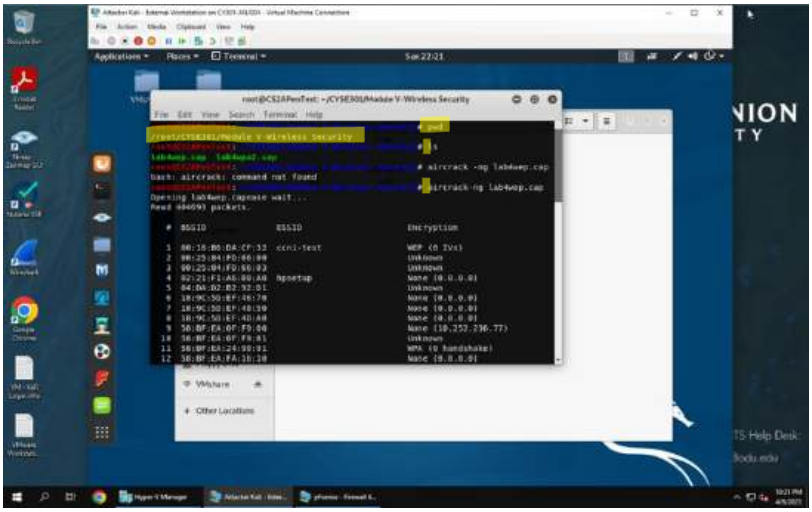
Extra Credit: I use the command john followed by the file containing the hashes, try.txt followed by the format I would like to use --format=dynamic. I then use the command john try.txt --show --format=dynamic to reveal the cracked passwords. Therefore:

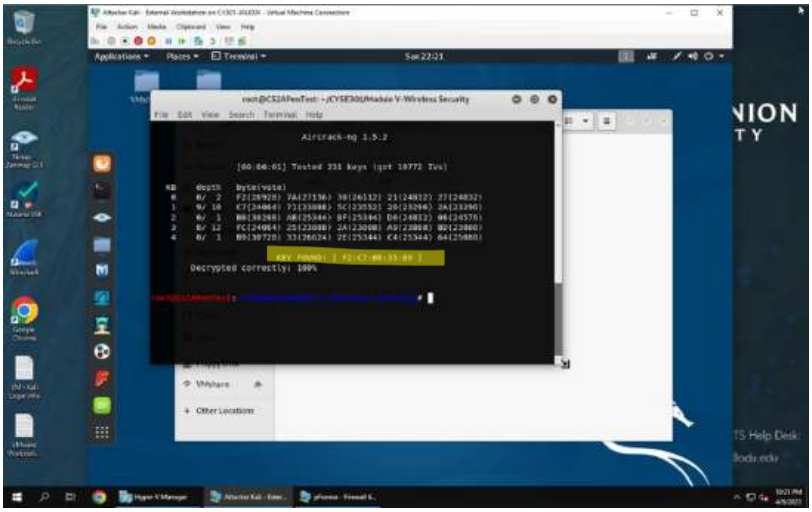
1. 5f4dcc3b5aa765d61d8327deb882cf99 = password

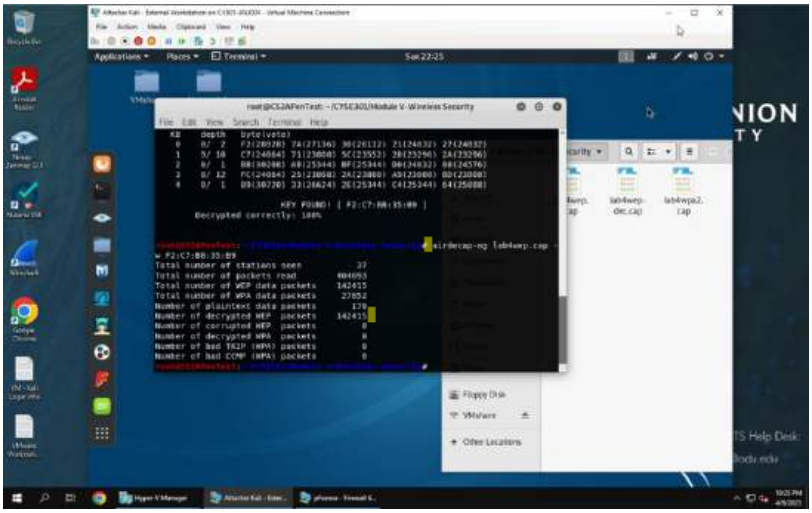
2. 63a9f0ea7bb98050796b649e85481845 = root

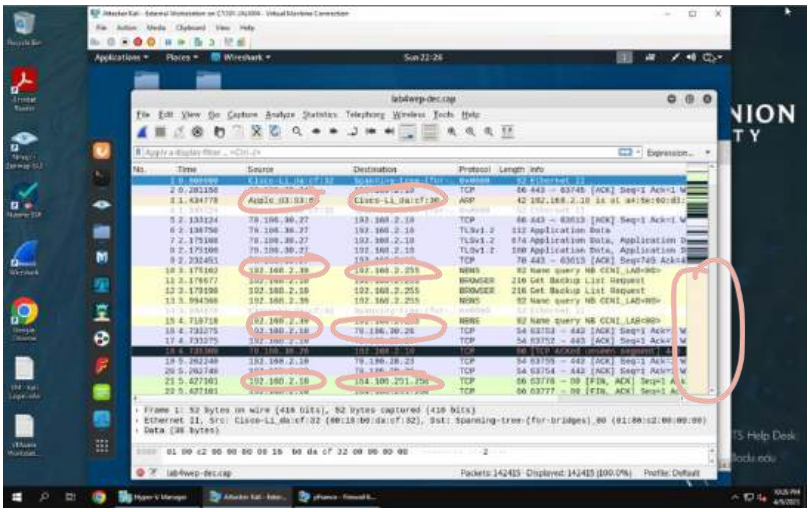
PART B: WI-FI PASSWORD CRACKING

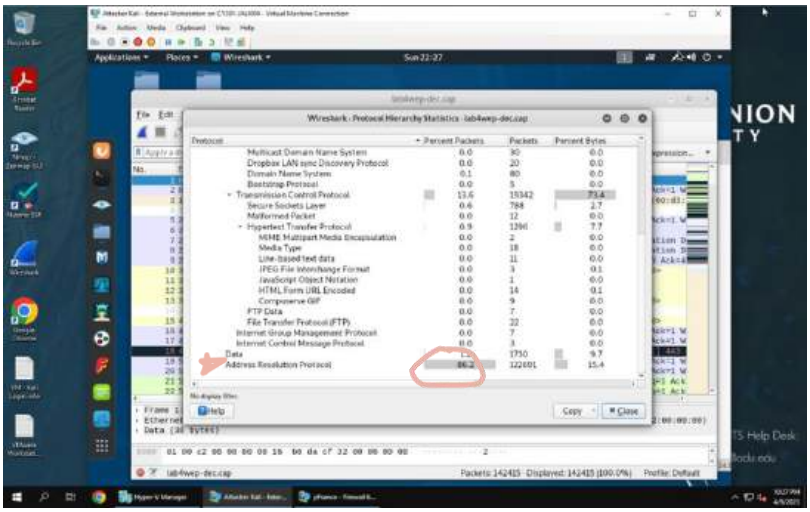
TASK C

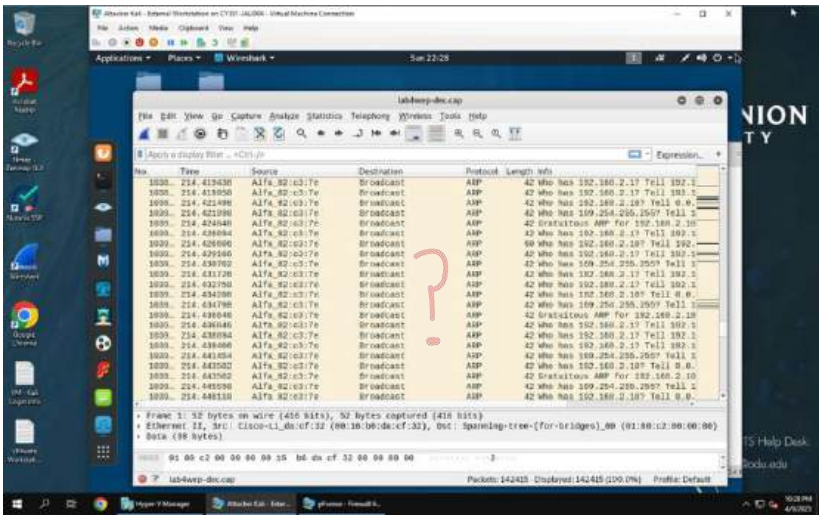


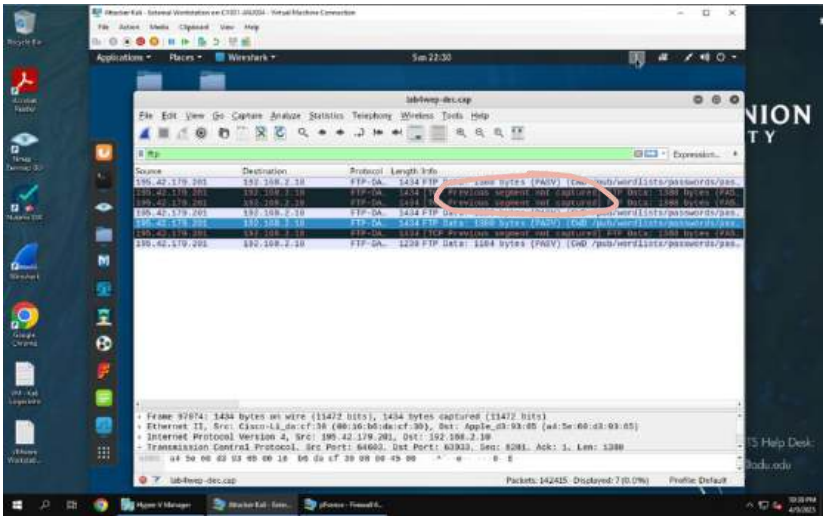


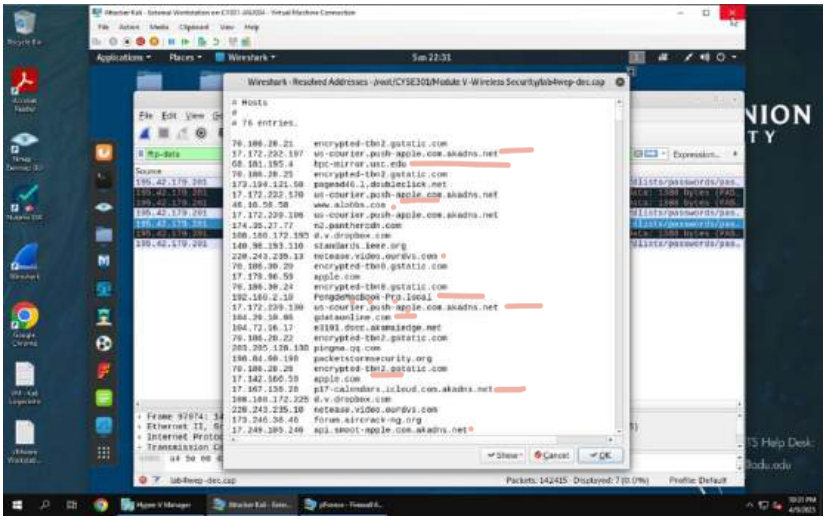

Applications
Places
Terminal
Sun 22:25
root@CSJAPenTest: ~/C7SE303/Module V-Wireless Security
File Edit View Search Terminal Help
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 98(26112) 21(24832) 27(24832)
1 5/ 10 C7(24864) 71(23808) 5C(23552) 2B(23296) 2A(23296)
2 0/ 1 B8(30208) A8(25344) BF(25344) 08(24832) 88(24576)
3 0/ 12 FC(24064) 23(23808) 2A(23808) A9(23808) 80(23808)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 84(25088)
KEY FOUND! [F2:C7:88:35:B9]
Decrypted correctly: 100%
airdecap-ng lab4wep.cap
w F2:C7:88:35:B9
Total number of stations seen 37
Total number of packets read 804093
Total number of WEP data packets 142415
Total number of WPA data packets 27852
Number of plaintext data packets 170
Number of decrypted WEP packets 142415
Number of corrupted WEP packets 0
Number of decrypted WPA packets 0
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
lab4wep-dec.cap
Floppy Disk
VMware
Other Locations


Applications
Places
Wireshark
Sun 22:26
lab4wep-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
Ethernet II, Src: Cisco-Li_da:cf:32 (00:18:0a:da:cf:32), Dst: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
Data (38 bytes)
lab4wep-dec.cap
Packets: 142415 · Displayed: 142415 (100.0%) Profile: Default


Applications
Places
Wireshark
Sun 22:27
Wireshark · Protocol Hierarchy Statistics · lab4wep-dec.cap
Protocol
Percent Packets
Packets
Percent Bytes
Multicast Domain Name System 0.0 30 0.0
Dropbox LAN sync Discovery Protocol 0.0 20 0.0
Domain Name System 0.1 80 0.0
Bootstrap Protocol 0.0 5 0.0
Transmission Control Protocol 13.6 15342 71.4
Secure Sockets Layer 0.6 788 2.7
Malformed Packet 0.0 12 0.0
Hypertext Transfer Protocol 0.9 1391 7.7
MIME Multipart Media Encapsulation 0.0 2 0.0
Media Type 0.0 18 0.0
Line-based text data 0.0 11 0.0
JPEG File Interchange Format 0.0 1 0.1
JavaScript Object Notation 0.0 1 0.0
HTML Form URL Encoded 0.0 14 0.1
Compuserve GIF 0.0 9 0.0
FTP Data 0.0 7 0.0
File Transfer Protocol (FTP) 0.0 22 0.0
Internet Group Management Protocol 0.0 7 0.0
Internet Control Message Protocol 0.0 3 0.0
Data 1.1 1710 9.7
Address Resolution Protocol 86.2 122691 15.4
Help
Copy
Close
lab4wep-dec.cap
Packets: 142415 · Displayed: 142415 (100.0%) Profile: Default



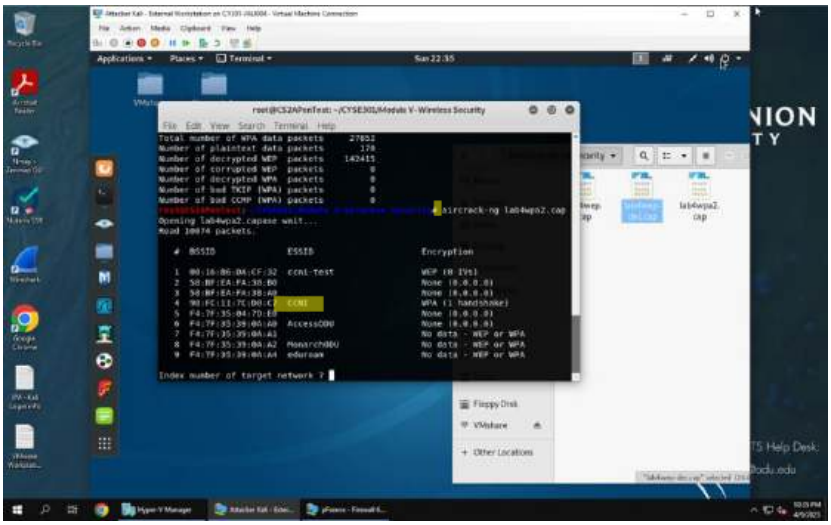


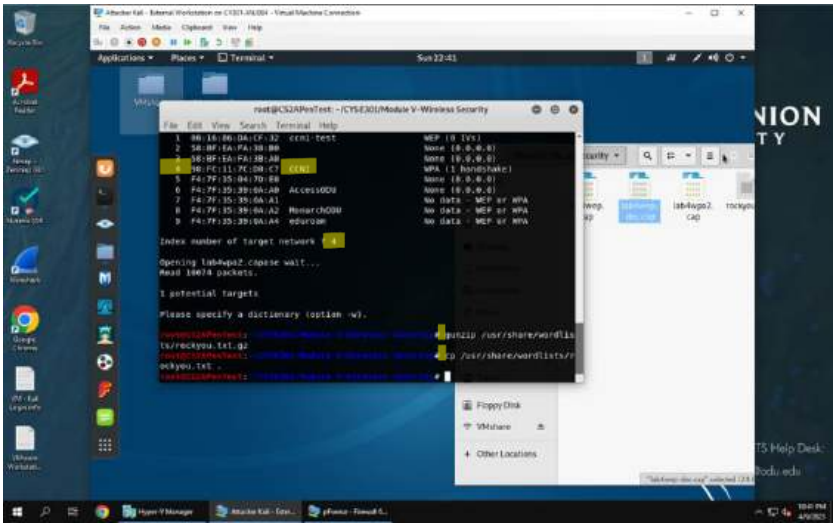


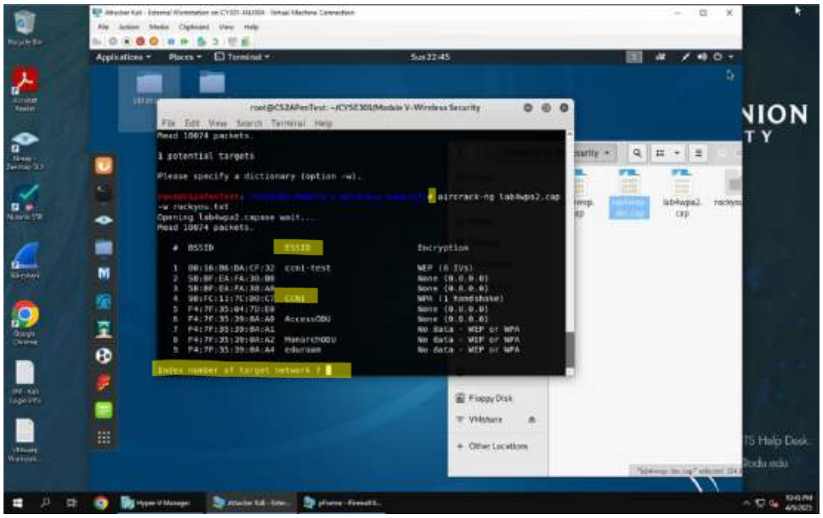
1. To decrypt the lab4wep.cap file I navigate to the file's GUI and then right click to open up a shell from this point. I then use the command pwd and ls to double check where I am at in my directory, plus the file name, and then use the command aircrack -ng followed by the file I want to decrypt, lab4wep.cap so I can

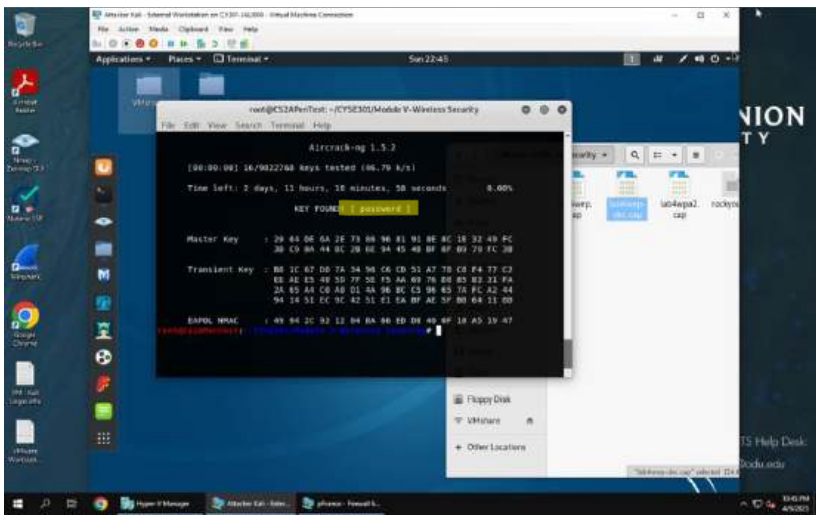
find the key. I also type in 1 for the target network. Now I have the Key and can decrypt the file. I use the command airdecap -ng then the file name lab4wep.cap followed by -w and the key, I found, and. I then analyze the decrypted file's traffic patterns.

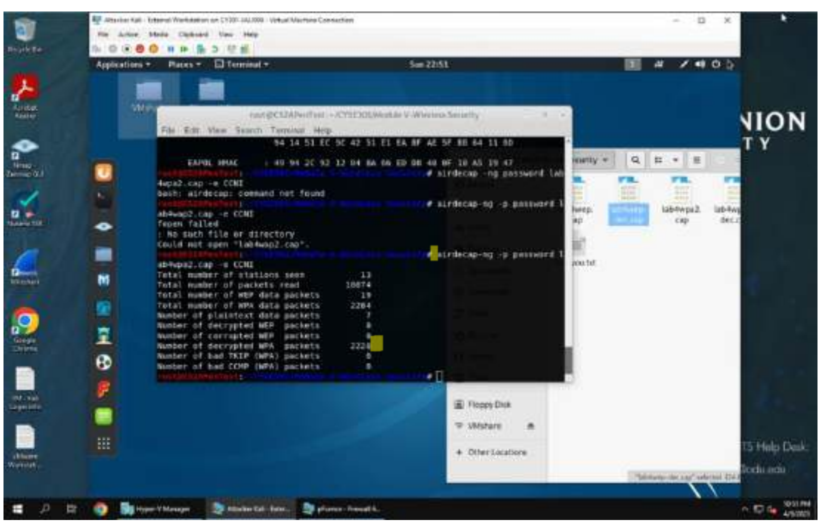
Analysis: This traffic analysis was much easier than the next two. We know from the lecture it is an ARP attack because in the protocol hierarchy a majority and overwhelming amount of the traffic is Address Resolution Protocol. I can also see IP addresses and what type of OS system certain machines are from the resolved addresses list and the ftp traffic. I also see college pages were visited and apple sites. Lastly I found it interesting this person visited packet storm security.org and then updated/accessed this person's apple calendar.

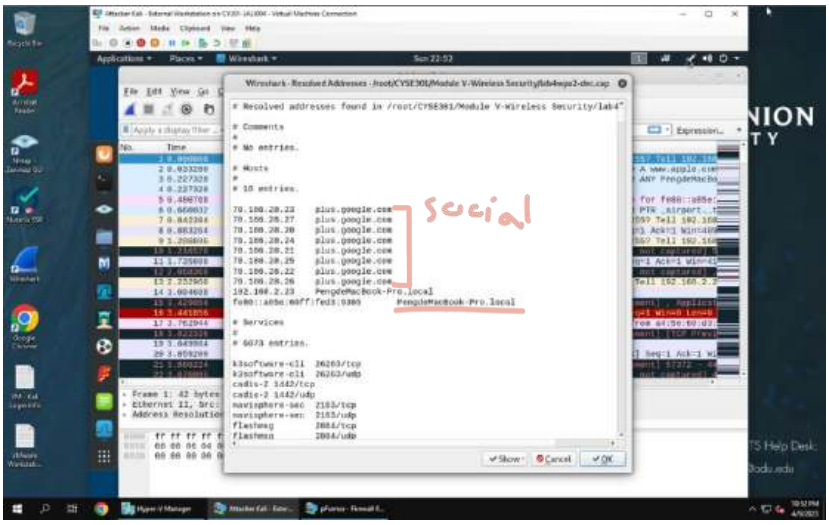


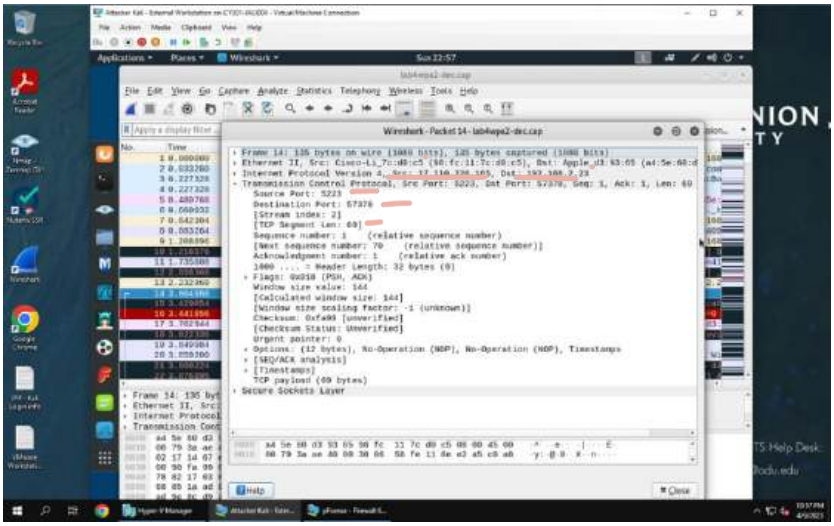



Please specify a dictionary (option -w).
Index number of target network ?


Aircrack-ng 1.5.2
KEY FOUND! [password]
Master Key
Transient Key
EAPOL HMAC







2. Next I want to decrypt another file containing traffic patterns. I the use the command aircrack -ng followed by the file I want to decrypt, lab4wpa2. cap so I can find the key. I also type in 4 for the target network because I want the network where the handshake occurs. Then I define (-w) which dictionary to use. I first unzip the file with the command gunzip followed by the absolute path name /usr/share/wordlists/rockyou.txt.gz . Then I copy this file into my current working directory (.) with the command cp /usr/share/wordlists/rockyou.txt . . I also double check this in the GUI. Then I repeat the process with the aircrack command, specify my target network (4), and define which dictionary wordlists I would like to use now that I have it copied into my current working directory. Now I have the Key and can decrypt the file. I use the command airdecap -ng, then the -p password, then the file name lab4wpa2. cap followed by the ESSID -e CCNI and. I then analyze the decrypted file's traffic patterns as before from the GUI because I now have a decrypted traffic.

Analysis: I found out that a MacBook pro was being used and accessed google +, for social networking. I also was able to find out the last name/username from the resolved address pane. The next part I anaylzed was a TCP packet. I used the source port number and googled it.

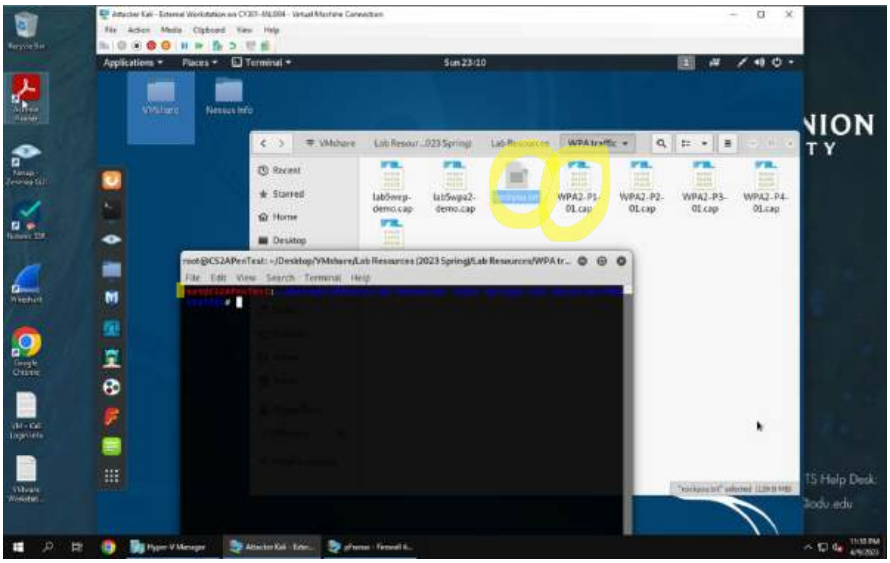
Port 5223 Details

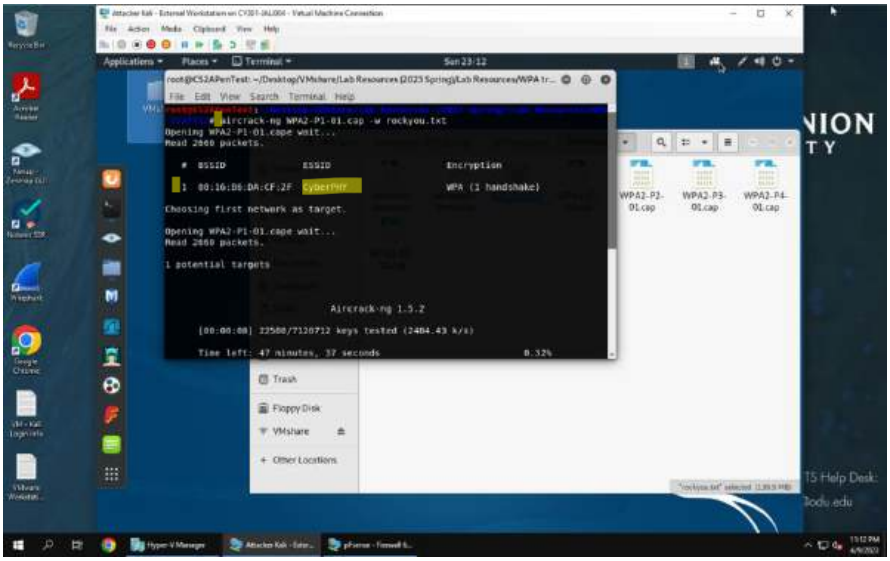
Port used by Apple to maintain a persistent connection to APNs and receive push notifications. Some Apple applications that use this port: MobileMe, FaceTime, Game Center, APNs.

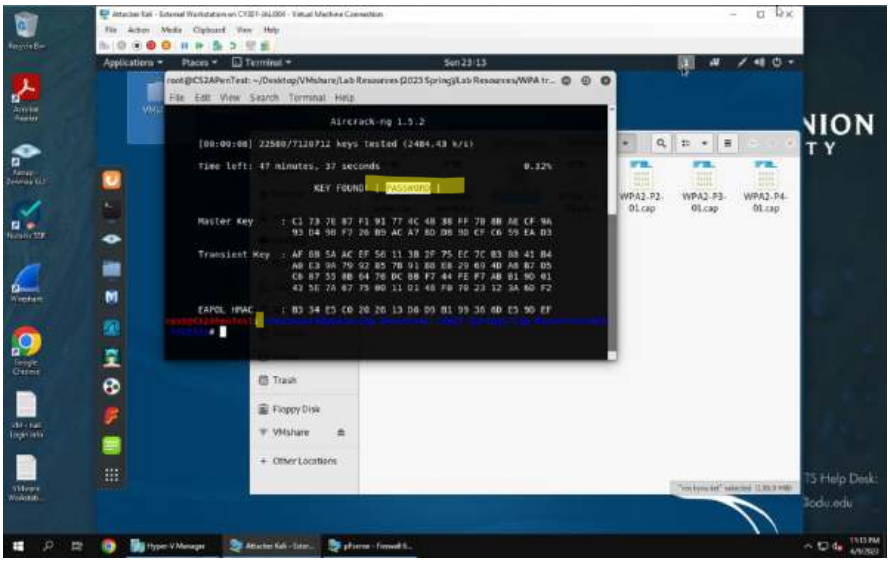
Then I also googled the source IP.

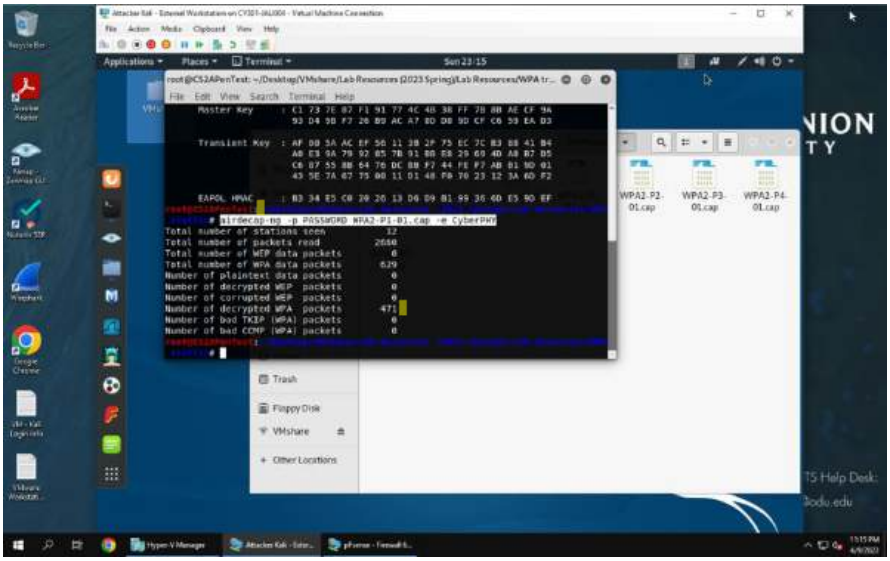
For this lab, each Task I tried to look at different areas in the traffic to try and get a better picture of the person and what they were doing.

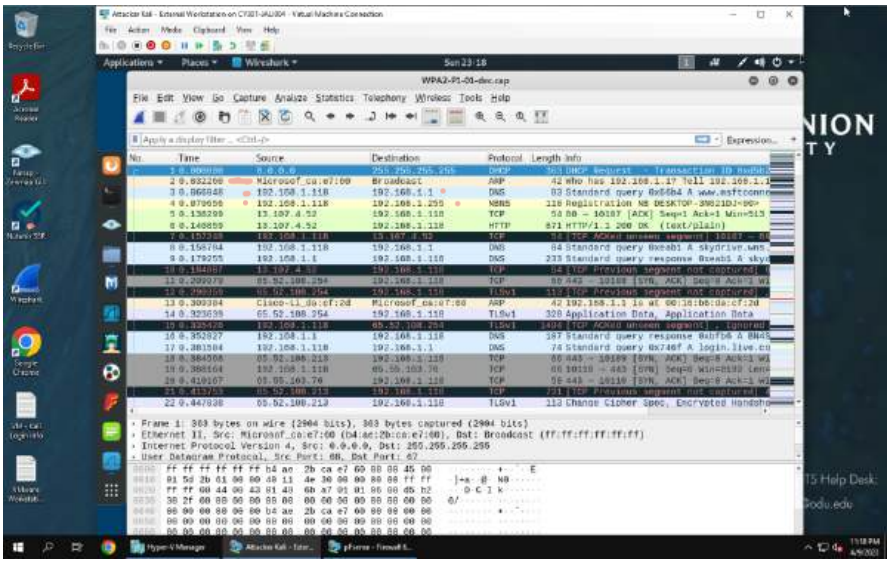
TASK D

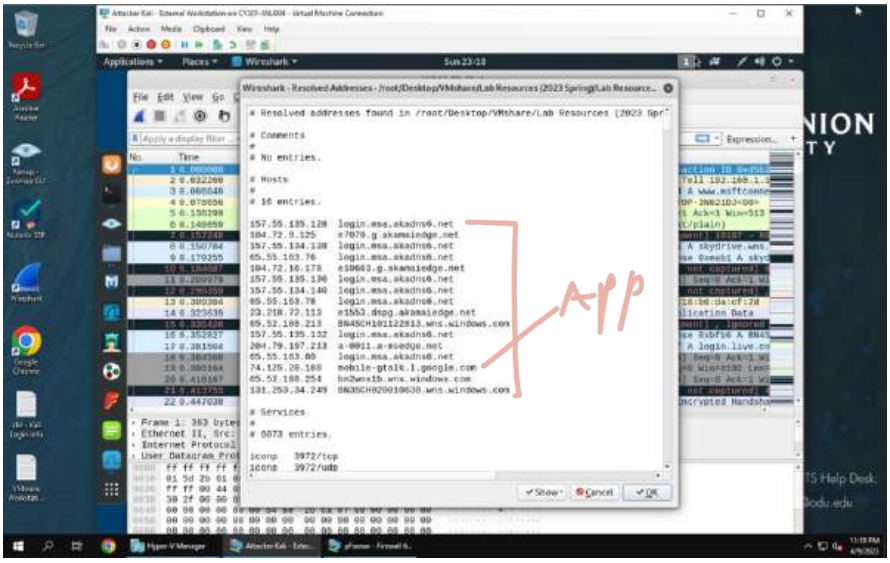


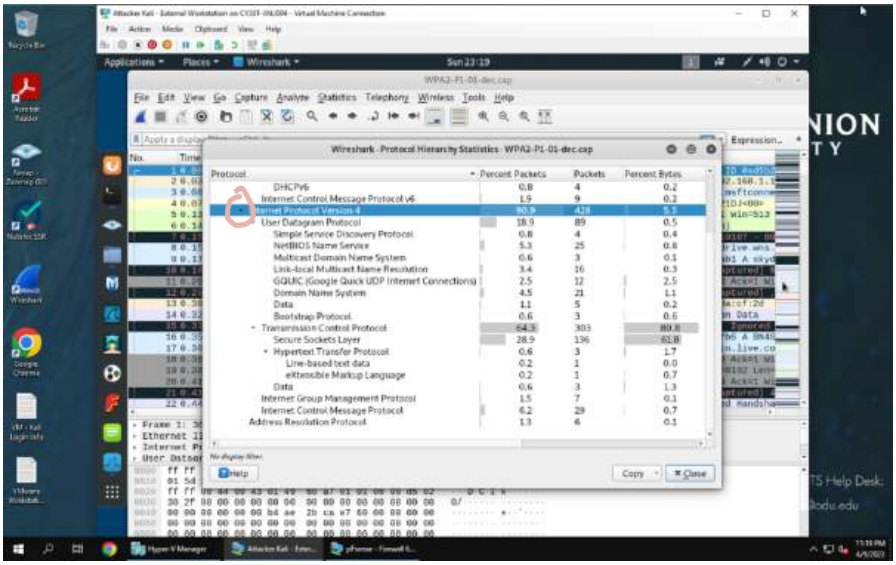

aircrack-ng WPA2-P1-01.cap -w rockyou.txt
Opening WPA2-P1-01.cap wait...
Read 2860 packets.
BSSID ESSID Encryption
1 00:16:D6:DA:CF:2F Cybernar WPA (1 handshake)
Choosing first network as target.
Opening WPA2-P1-01.cap wait...
Read 2860 packets.
1 potential targets
Aircrack-ng 1.5.2
[00:00:08] 32588/7120712 keys tested (2404.43 k/s)
Time left: 47 minutes, 37 seconds 0.32%

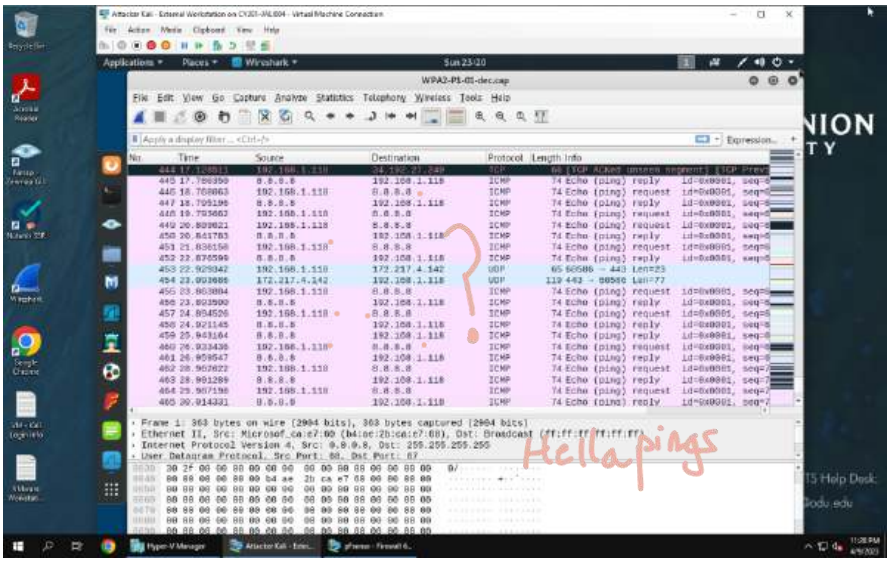

Aircrack-ng 1.5.2
[00:00:08] 22580/7128712 keys tested (2484.43 k/s)
Time left: 47 minutes, 37 seconds 0.32%
KEY FOUND! [Password]
Master Key : C1 73 7E 87 F1 91 77 4C 48 38 FF 7B 8B AE CF 9A
93 D4 9B F7 20 B9 AC A7 8D DB 9D CF C6 59 EA D3
Transient Key : AF 88 5A AC EF 56 11 38 2F 75 EC 7C B3 88 41 B4
A0 E3 9A 79 92 85 7B 91 88 E8 29 69 4D A8 B7 D5
C6 87 55 8B 64 76 DC 88 F7 44 FE F7 AB 81 9D 01
43 5E 7A 67 75 00 11 01 48 F0 70 23 12 3A 6D F2
EAPOL HMAC : B3 34 E5 C0 20 20 13 D6 D9 81 99 36 6D E5 9D EF
Trash
Floppy Disk
VMshare
Other Locations

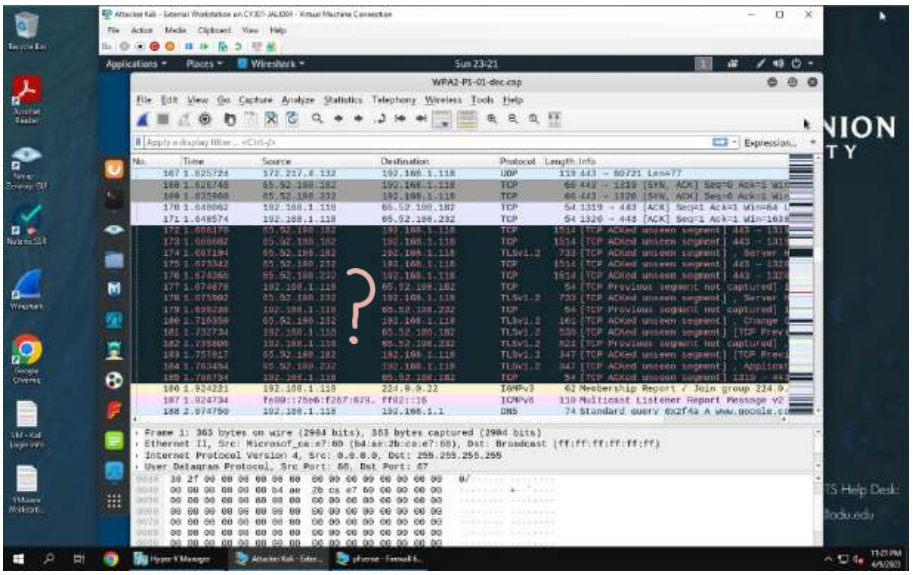

Master Key : C1 73 7E 87 F1 91 77 4C 48 38 FF 7B 8B AE CF 9A
93 D4 9B F7 20 B9 AC A7 8D DB 9D CF C6 59 EA D3
Transient Key : AF 88 5A AC EF 56 11 38 2F 75 EC 7C B3 88 41 B4
A0 E3 9A 79 92 85 7B 91 88 E8 29 69 4D A8 B7 D5
C6 87 55 8B 64 76 DC 88 F7 44 FE F7 AB 81 9D 01
43 5E 7A 67 75 00 11 01 48 F0 70 23 12 3A 6D F2
EAPOL HMAC : B3 34 E5 C0 20 20 13 D6 D9 81 99 36 6D E5 9D EF
airdecap-ng -p PASSWORD WPA2-P1-01.cap -e CyberPHY
Total number of stations seen 12
Total number of packets read 2688
Total number of WEP data packets 0
Total number of WPA data packets 629
Number of plaintext data packets 0
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 471
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
Trash
Floppy Disk
VMshare
Other Locations

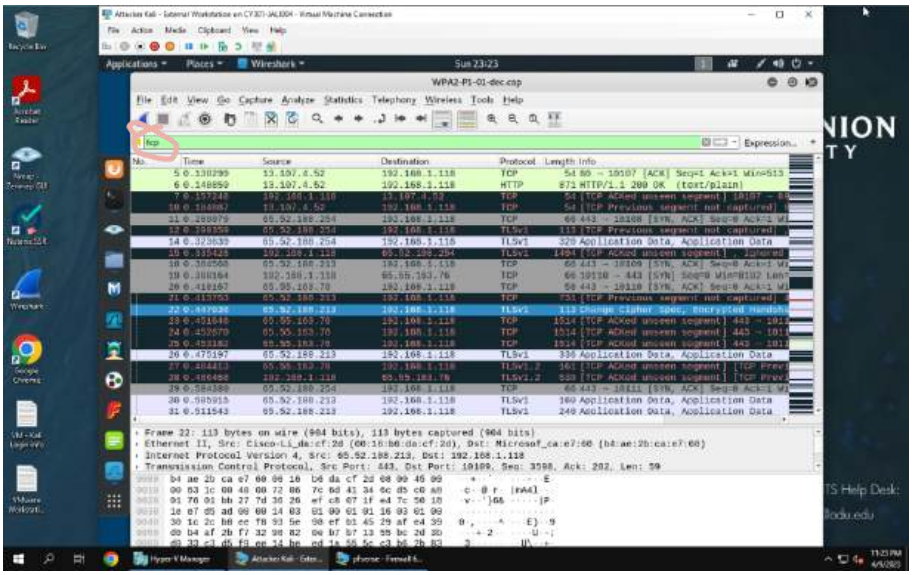

WPA2-P1-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Frame 1: 303 bytes on wire (2904 bits), 303 bytes captured (2904 bits)
Ethernet II, Src: Microsof_ca:e7:60 (b4:ae:2b:ca:e7:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Trash
Floppy Disk
VMshare
Other Locations

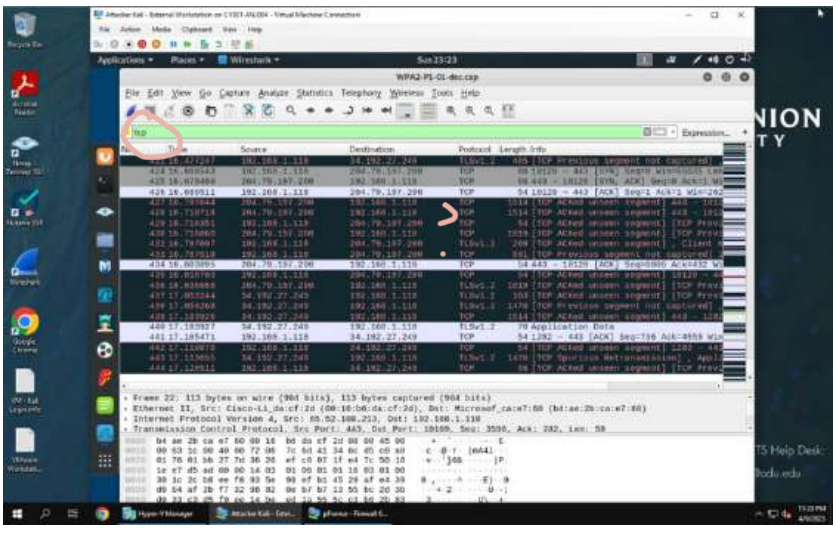

App


a


Hellapings







I first extracted or unzipped the files in the VM share folder several times until I where in the correct folder for my WPA2-P1-01.cap file. Then I right clicked and selected open in terminal, so my working directory was where I wanted it to be in my shell. Then I dragged rockyou.txt over to my new current working directory.

1. I the use the command aircrack -ng followed by the file I want to decrypt, WPA2-P1-01.cap so I can find the key. Then I define (-w) which dictionary to use because I am required to use a dictionary attack to find the password to open the file and then I also need to tell aircrack which wordlist to use.

2. I find the key and then use the command airdecap -ng followed by the key I just found, followed by the file, and then define -e, which is the network ESSID. In sum the command is airdecap-ng -p PASSWORD WPA2-P1-01-cap -e CyberPHY. I now have the traffic decrypted and I can perform my analysis.

Analysis: So this may be way off base, but I imagine someone trying to login into their google account and using the google talk app. Somehow they were infected with a ICMP flood attack which made the TCP connections fail. So their phone is compromised and possibly the network, but I lean more towards the phone. Or maybe a Chromebook?