OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #4 Penetration Testing for Windows

JaQwah Lewis

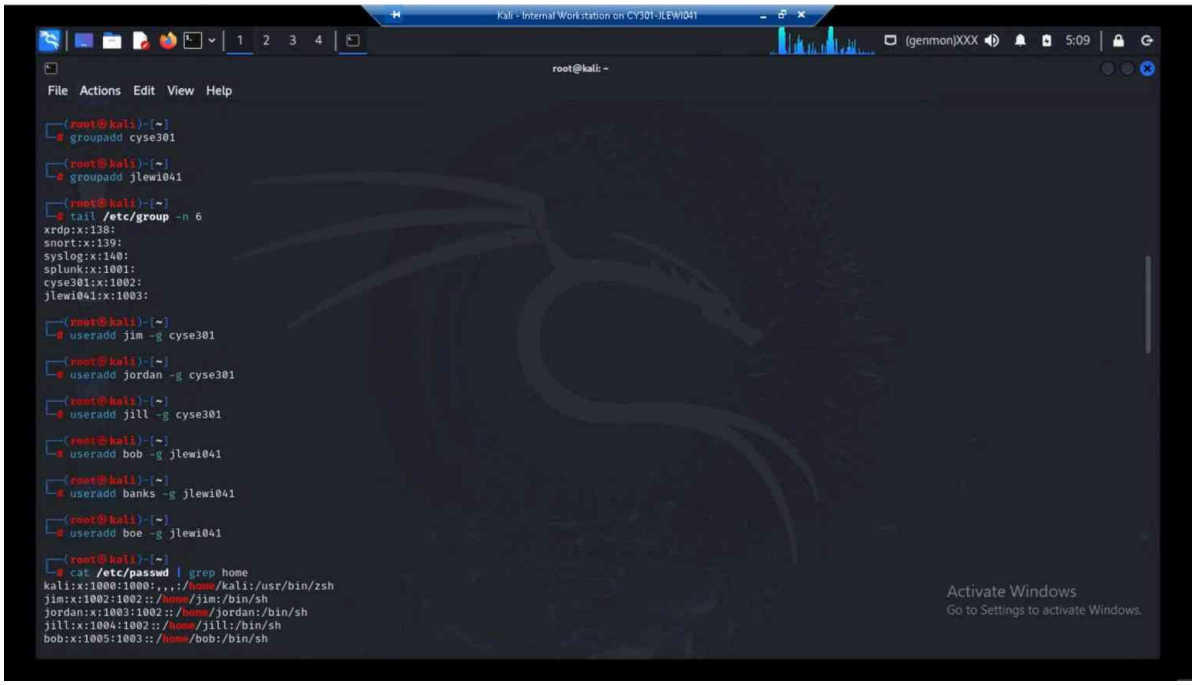
Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.

What I did to create the two groups is use the command “groupadd jlewi041” “groupadd cyse301”.Using this command was pretty easy as we used it in past assignments when creating a group.

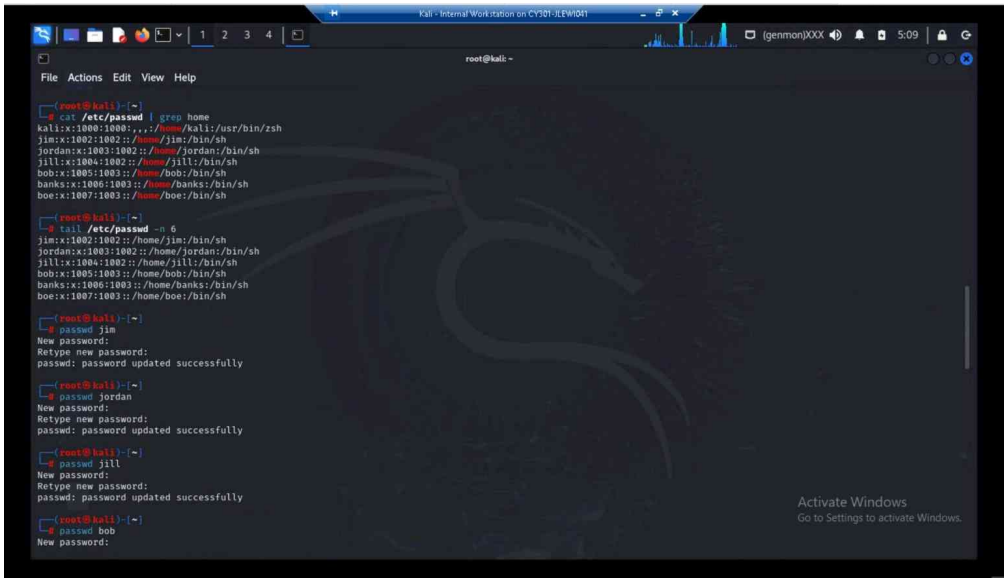
2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.

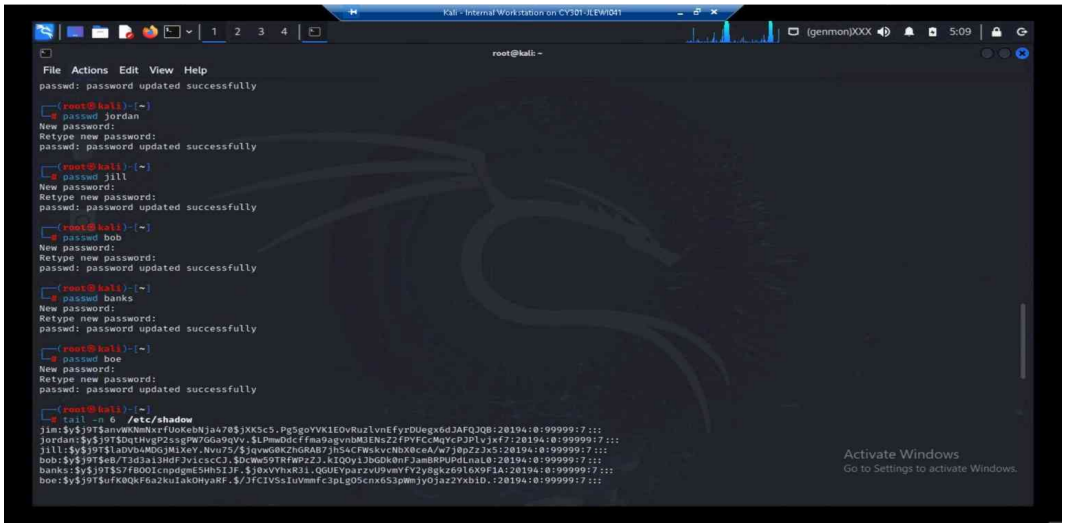
For this task I made a total of six different users and added three of them to each group. For creating the users I used the command “useradd” to create the users jim, jordan, jill, bob, banks, and boe. Following that when adding the users to the group I use the command “sudo usermod -a -G (jlewi041 or cyse301) (user’s username)”. After that to see what group the users are assigned to I used the command “ group (user’s username)”.



3. **5 points.** Choose Three 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.

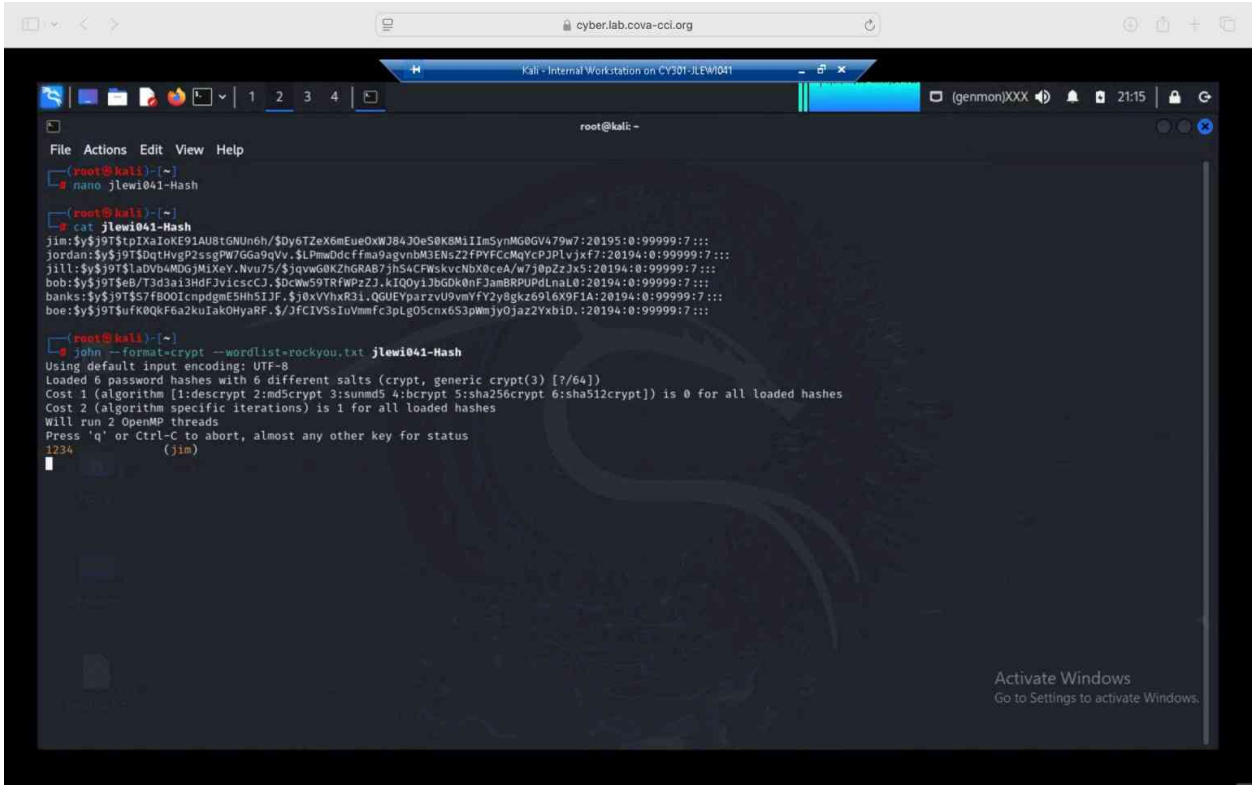
For this task I created a password for each user. The command I used to accomplish this step is “passwd (user’s username)”. The password for the user jim is 1234 and the password for jordan is 1245. The password I created for jill is pug1245. Following that, the password I created for bob is Pug1245!. The password for banks is Pug1245!0. Lastly, the password I created for boe is P5g1245!0.





4. **5 points.** Export all Three users' password hashes into a file named "**YourMIDAS-HASH**" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.

For the last step I used the command "nano jlewi041-Hash" to create a Hash file. Following that, I copied and pasted the users information from the previous step into the Hash file. To make sure the information was inside the Hash file, I used the command "cat jlewi041-Hash". Lastly, to perform a dictionary attack to gain the passwords from the users accounts I used the command "john –format=crypt –wordlist=rockyou.txt jlewi041-Hash". Within three minutes it was able to crack the password for the user jim.



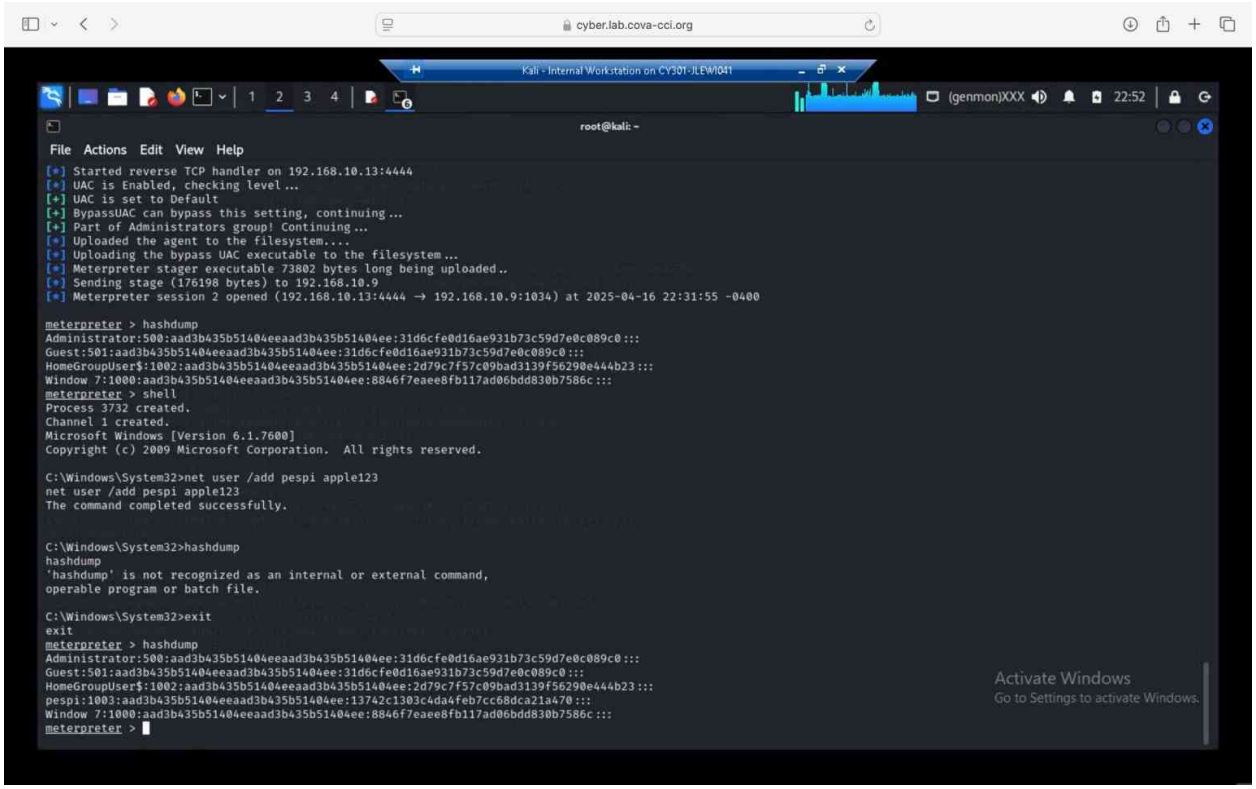
Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords (OR you may create users using net users \add command as you did in lab-4-task-c). Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

Now, complete the following tasks:

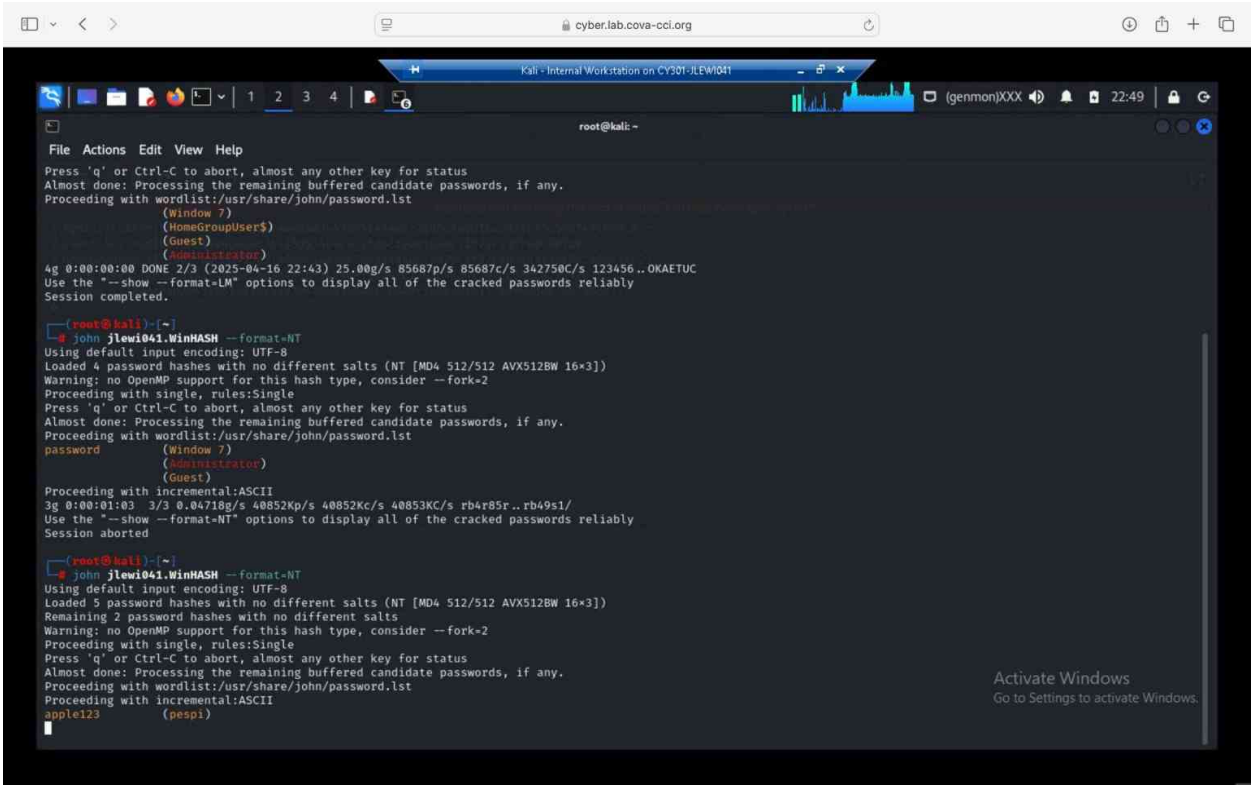
1. **5 points.** Display the password hashes by using the "hashdump" command in the meterpreter shell.

For this step I made a connection to Windows 7 by accessing it through the meterpreter by first using command "msfconsole" . Following that, I used the command "uses exploit/multi/handler" and the command "set payload windows/meterpreter/reverse_tcp". Then I used the command "exploit"to make a connection to Windows 7 by going on Windows 7 and accessing a document from the previous lab. After creating a connection I was able to use the command "hashdump" to retrieve all of the hashes from each of the users.



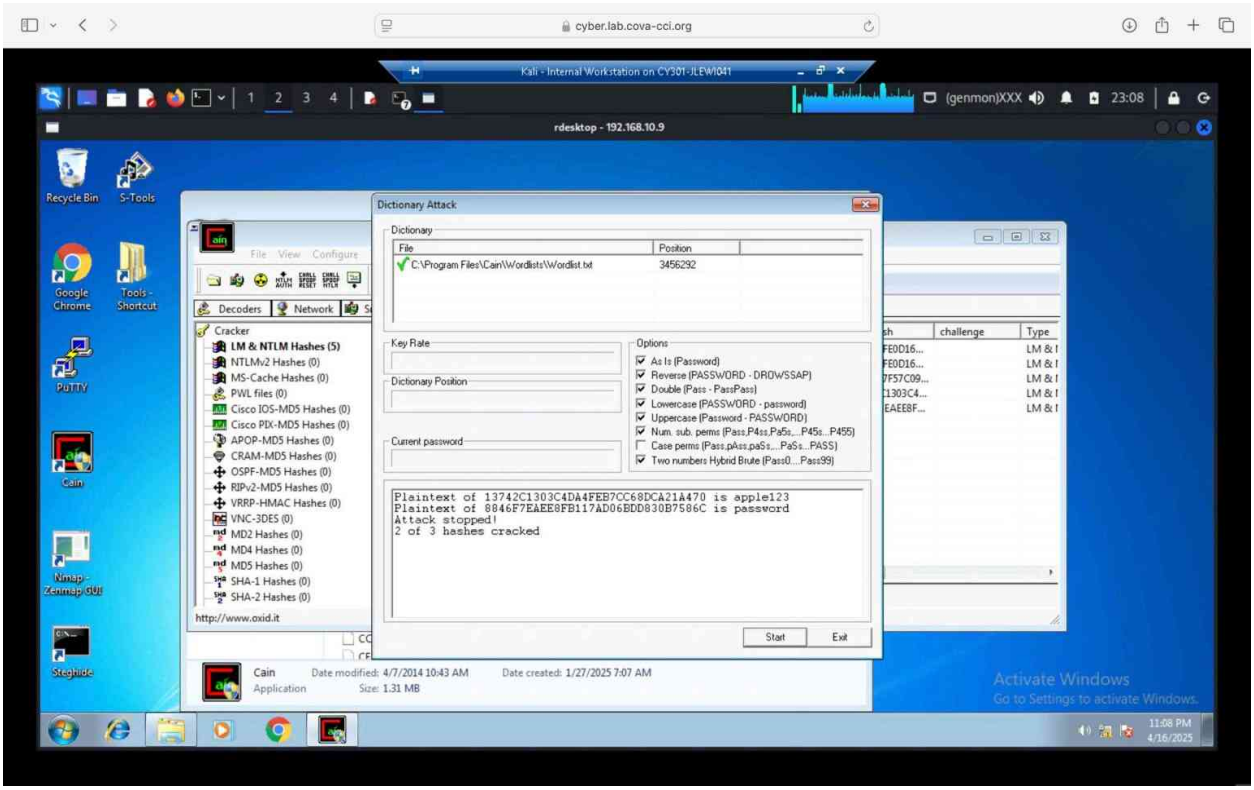
2. **10 points.** Save the password hashes into a file named "**your_midas.WinHASH**" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run **John the ripper** for **10 minutes** to crack the windows users' passwords (You MUST crack at least one password in order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

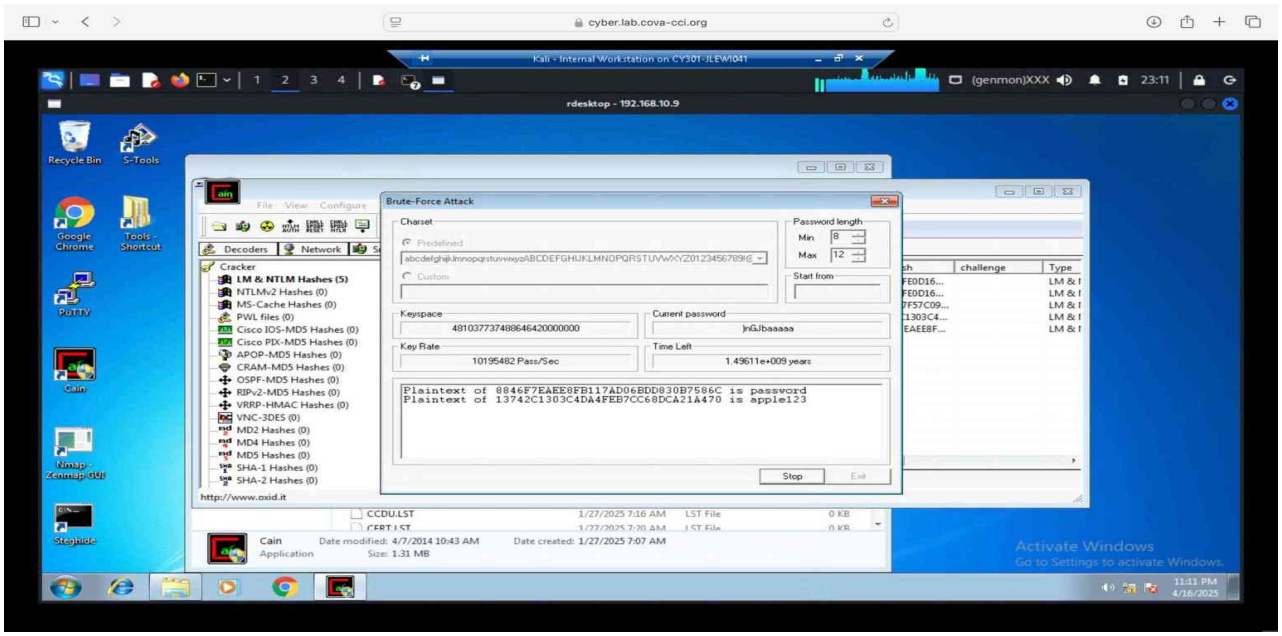
After collecting all the hashes, I made a hash file using my ODU ID using command. Following that I copied and pasted all of the hashes that were in the last step into the hash file I created titled "jlewi041.WinHASH". Next, I used the command "john jlewi041.WinHASH –format=NF" which started cracking the password. In results it gave me the password for the user pespi with the password being apple123.



10 points. Launch/open the password cracking tool, **Cain and Abel** in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).

I gained access to Windows 7 through Kali by using the command “redesk -u Windows 7 -p password 192.168.10.9”. After gaining access remotely I navigated to Cain and was able to launch both dictionary and brute force attacks to crack the passwords by watching the video you posted.

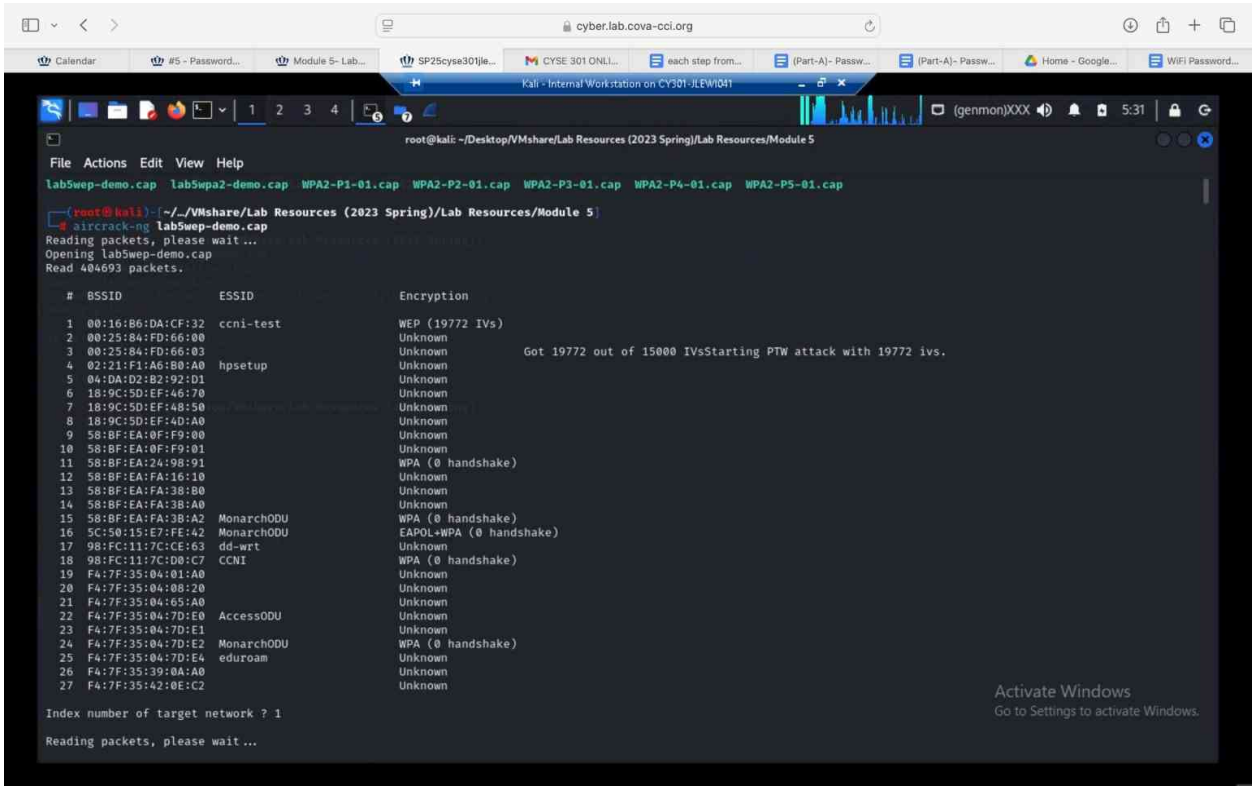


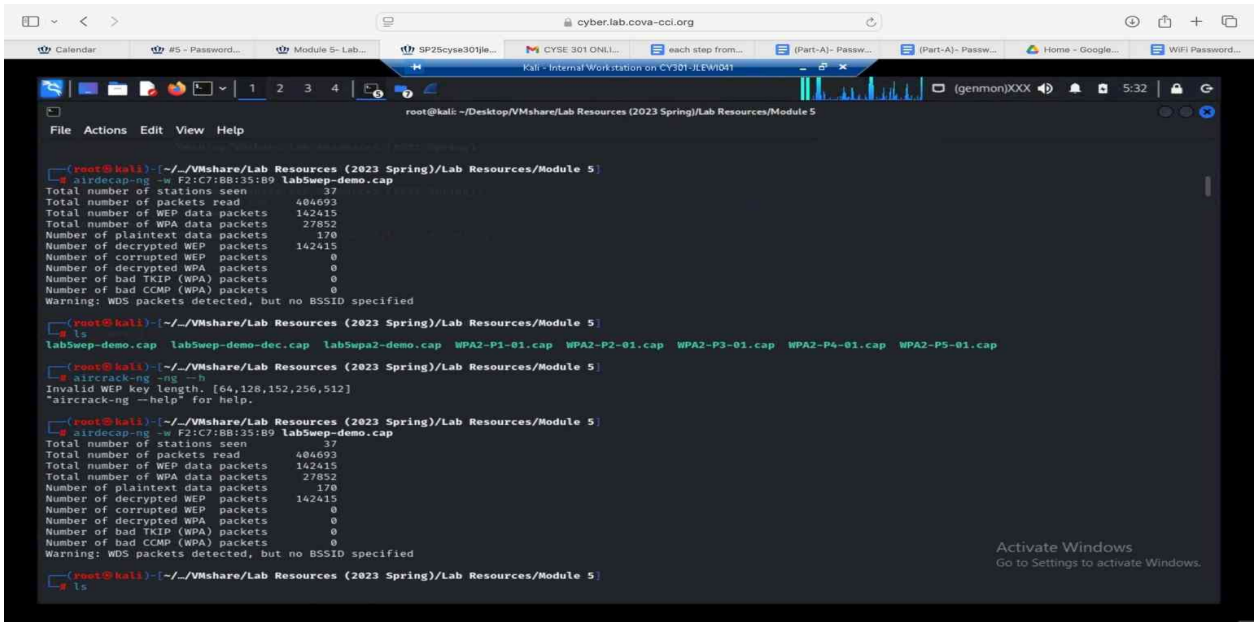

cyber.lab.cova-cci.org
Kali - Internal Workstation on CY301-JLEW1041
rdesktop - 192.168.10.9
Recycle Bin
S-Tools
Google Chrome
Tools - Shortcut
PuTTY
Cain
Nmap - Zenmap GUI
Steghide
Brute-Force Attack
Charset
Password length
Min
Max
Start from
Keyspace
Current password
Key Rate
Time Left
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Plaintext of 13742C1303C4DA4FEB7CC68DCA21A470 is apple123
Stop
Exit
Cracker
LM & NTLM Hashes (5)
NTLMv2 Hashes (0)
MS-Cache Hashes (0)
PWL files (0)
Cisco IOS-MD5 Hashes (0)
Cisco PIX-MD5 Hashes (0)
APOP-MD5 Hashes (0)
CRAM-MD5 Hashes (0)
OSPF-MD5 Hashes (0)
RIPv2-MD5 Hashes (0)
VRRP-HMAC Hashes (0)
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
http://www.oxid.it
Activate Windows
Go to Settings to activate Windows.

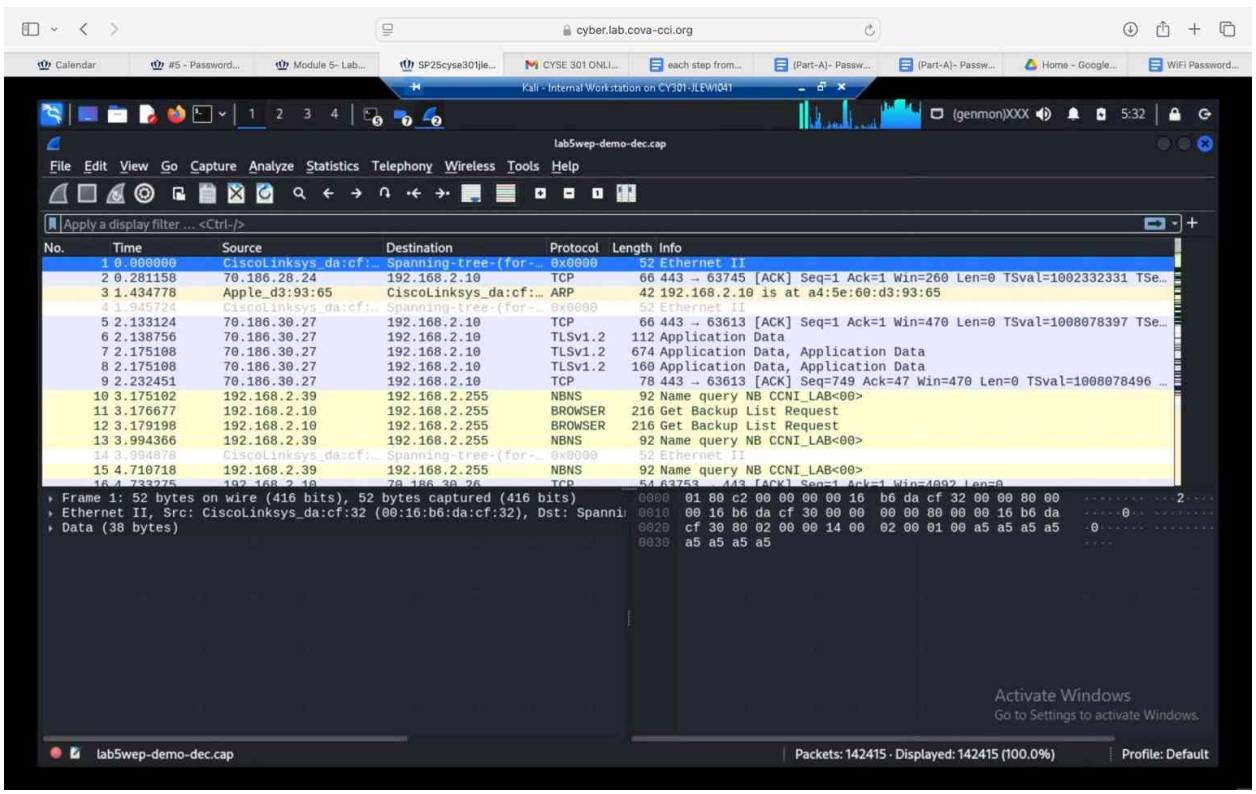
Task C: 20 points

1. Decrypt the lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

To do this task I follow the instructions in the lab manual while also watching the video. First I used the " aircrack-ng lab5wep-demo.cap" command to get the key and password. After getting the key I was able to start the decryption process. To start the decryption I used the "airdecap-ng F2:C7:BB:35:B9 labwep-demo.cap" command. After using that command it was able to decrypt the files. Lastly, I used the "wireshark labwep-demo-dec.cap" command to view the packet traffic of the decryption file version.

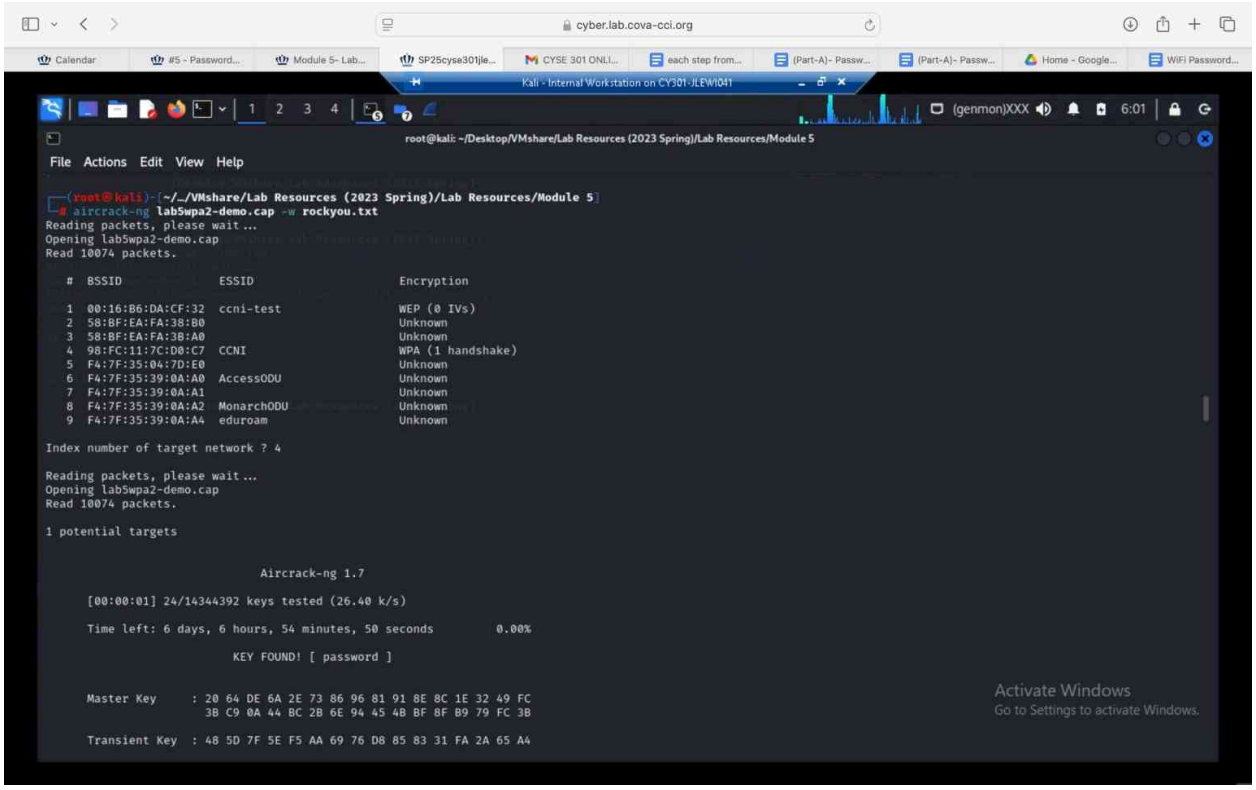


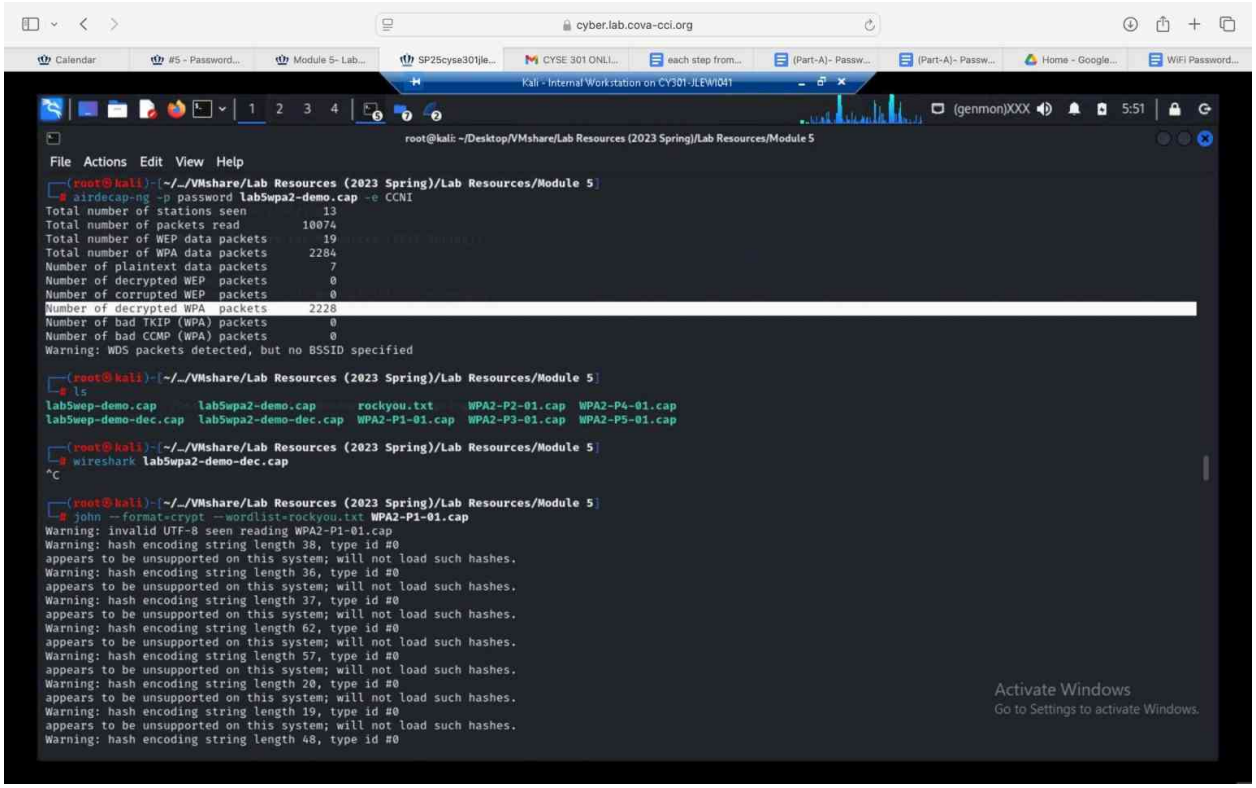

cyber.lab.cova-cci.org
Kali - Internal Workstation on CY301-JLEW1041
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
airdecap-ng -w F2:C7:8B:35:B9 lab5wep-demo.cap
Total number of stations seen 37
Total number of packets read 404693
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
Warning: WDS packets detected, but no BSSID specified
ls
lab5wep-demo.cap lab5wep-demo-dec.cap lab5wpa2-demo.cap WPA2-P1-01.cap WPA2-P2-01.cap WPA2-P3-01.cap WPA2-P4-01.cap WPA2-P5-01.cap
aircrack-ng -ng --h
Invalid WEP key length. [64,128,152,256,512]
"aircrack-ng --help" for help.
Activate Windows
Go to Settings to activate Windows.

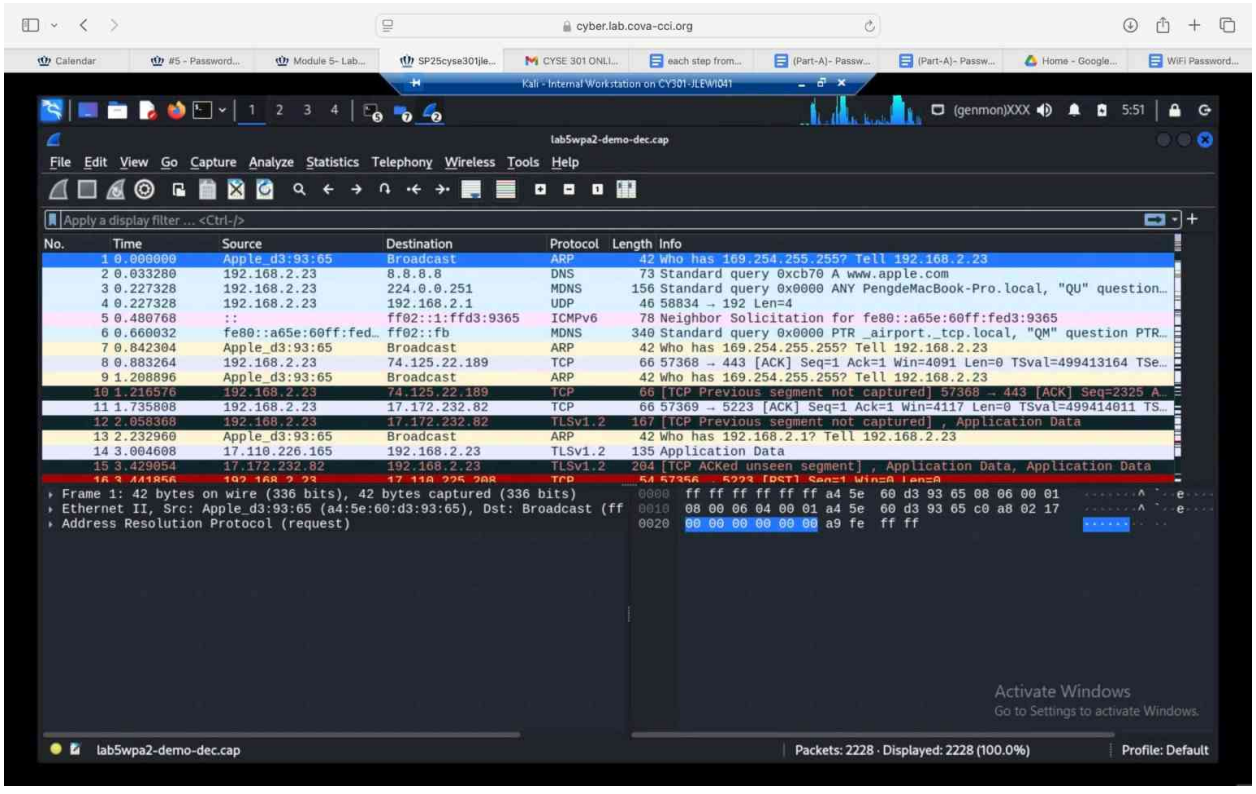

cyber.lab.cova-cci.org
Kali - Internal Workstation on CY301-JLEW1041
lab5wep-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000 52 Ethernet II
2 0.281158 70.186.28.24 192.168.2.10 TCP 66 443 → 63745 [ACK] Seq=1 Ack=1 Win=260 Len=0 TSval=1002332331 TSe…
3 1.434778 Apple_d3:93:65 CiscoLinksys_da:cf:… ARP 42 192.168.2.10 is at a4:5e:60:d3:93:65
4 1.945724 CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000 52 Ethernet II
5 2.133124 70.186.30.27 192.168.2.10 TCP 66 443 → 63613 [ACK] Seq=1 Ack=1 Win=470 Len=0 TSval=1008078397 TSe…
6 2.138756 70.186.30.27 192.168.2.10 TLSv1.2 112 Application Data
7 2.175108 70.186.30.27 192.168.2.10 TLSv1.2 674 Application Data, Application Data
8 2.175108 70.186.30.27 192.168.2.10 TLSv1.2 160 Application Data, Application Data
9 2.232451 70.186.30.27 192.168.2.10 TCP 78 443 → 63613 [ACK] Seq=749 Ack=47 Win=470 Len=0 TSval=1008078496 …
10 3.175102 192.168.2.39 192.168.2.255 NBNS 92 Name query NB CCNI_LAB<00>
11 3.176677 192.168.2.10 192.168.2.255 BROWSER 216 Get Backup List Request
12 3.179198 192.168.2.10 192.168.2.255 BROWSER 216 Get Backup List Request
13 3.994366 192.168.2.39 192.168.2.255 NBNS 92 Name query NB CCNI_LAB<00>
14 3.994878 CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000 52 Ethernet II
15 4.710718 192.168.2.39 192.168.2.255 NBNS 92 Name query NB CCNI_LAB<00>
Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
Ethernet II, Src: CiscoLinksys_da:cf:32 (00:16:b6:da:cf:32), Dst: Spanni
Data (38 bytes)
0000 01 80 c2 00 00 00 00 16 b6 da cf 32 00 00 80 00
0010 00 16 b6 da cf 30 00 00 00 00 80 00 00 16 b6 da
0020 cf 30 80 02 00 00 14 00 02 00 01 00 a5 a5 a5 a5
0030 a5 a5 a5 a5
Activate Windows
Go to Settings to activate Windows.
lab5wep-demo-dec.cap
Packets: 142415 · Displayed: 142415 (100.0%)
Profile: Default

2. Decrypt the lab5wpa2-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

When going over this step it was similar to the last step. As I used the command " aircrack-ng lab5wpa-demo.cap" to start. Following that, I used the "aircrack-ng lab5wpa-demo.cap" to get the ESSID and password. Next, I used the command " airdecaping -p password lab5wpa-demo.cap -e CCNI". This command helps decrypt and shows me the packet was decrypted. Lastly, I used "wireshark lab5wpa-demo-dec.cap" to view the traffic.




cyber.lab.cova-cci.org
Kali - Internal Workstation on CY301-JLEWI041
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen 13
Total number of packets read 10074
Total number of WEP data packets 19
Total number of WPA data packets 2284
Number of plaintext data packets 7
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 2228
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
Warning: WDS packets detected, but no BSSID specified
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
ls
lab5wep-demo.cap lab5wpa2-demo.cap rockyou.txt WPA2-P2-01.cap WPA2-P4-01.cap
lab5wep-demo-dec.cap lab5wpa2-demo-dec.cap WPA2-P1-01.cap WPA2-P3-01.cap WPA2-P5-01.cap
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
wireshark lab5wpa2-demo-dec.cap
^C
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
john --format=crypt --wordlist=rockyou.txt WPA2-P1-01.cap
Warning: invalid UTF-8 seen reading WPA2-P1-01.cap
Warning: hash encoding string length 38, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 36, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 37, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 62, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 57, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 20, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 19, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 48, type id #0
Activate Windows
Go to Settings to activate Windows.

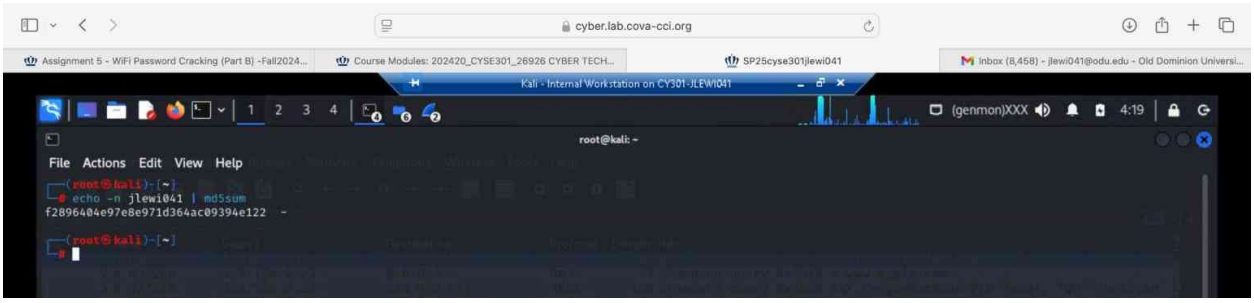

cyber.lab.cova-cci.org
Kali - Internal Workstation on CY301-JLEWI041
lab5wpa2-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell 192.168.2.23
2 0.033280 192.168.2.23 8.8.8.8 DNS 73 Standard query 0xcb70 A www.apple.com
3 0.227328 192.168.2.23 224.0.0.251 MDNS 156 Standard query 0x0000 ANY PengdeMacBook-Pro.local, "QU" question…
4 0.227328 192.168.2.23 192.168.2.1 UDP 46 58834 → 192 Len=4
5 0.480768 :: ff02::1:ff3d:9365 ICMPv6 78 Neighbor Solicitation for fe80::a65e:60ff:fed3:9365
6 0.660032 fe80::a65e:60ff:fed… ff02::fb MDNS 340 Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR…
7 0.842304 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell 192.168.2.23
8 0.883264 192.168.2.23 74.125.22.189 TCP 66 57368 → 443 [ACK] Seq=1 Ack=1 Win=4091 Len=0 TSval=499413164 TSe…
9 1.208896 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell 192.168.2.23
10 1.216576 192.168.2.23 74.125.22.189 TCP 66 [TCP Previous segment not captured] 57368 → 443 [ACK] Seq=2325 A…
11 1.735808 192.168.2.23 17.172.232.82 TCP 66 57369 → 5223 [ACK] Seq=1 Ack=1 Win=4117 Len=0 TSval=499414011 TS…
12 2.058368 192.168.2.23 17.172.232.82 TLSv1.2 167 [TCP Previous segment not captured] , Application Data
13 2.232960 Apple_d3:93:65 Broadcast ARP 42 Who has 192.168.2.1? Tell 192.168.2.23
14 3.004608 17.110.226.165 192.168.2.23 TLSv1.2 135 Application Data
15 3.429054 17.172.232.82 192.168.2.23 TLSv1.2 204 [TCP ACKed unseen segment] , Application Data, Application Data
16 3.441856 192.168.2.23 17.110.225.208 TCP 54 57356 → 5223 [RST] Seq=1 Win=0 Len=0
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Apple_d3:93:65 (a4:5e:60:d3:93:65), Dst: Broadcast (ff
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff a4 5e 60 d3 93 65 08 06 00 01
0010 08 00 06 04 00 01 a4 5e 60 d3 93 65 c0 a8 02 17
0020 00 00 00 00 00 00 a9 fe ff ff
lab5wpa2-demo-dec.cap
Packets: 2228 · Displayed: 2228 (100.0%)
Profile: Default
Activate Windows
Go to Settings to activate Windows.

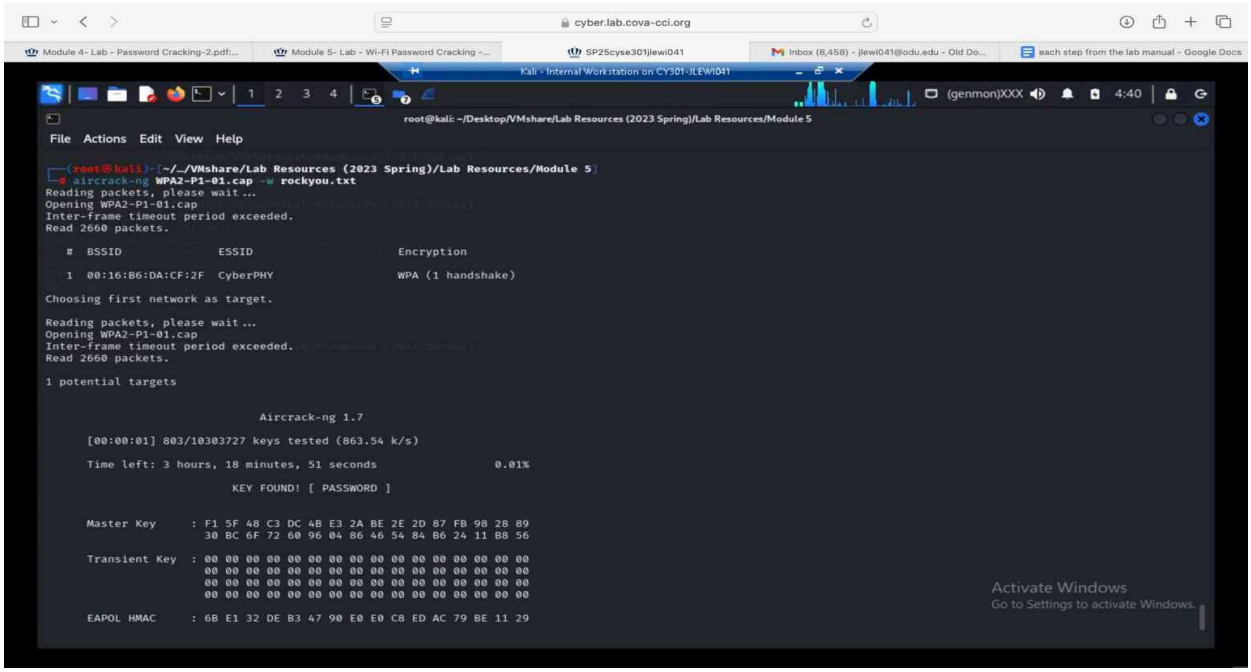
Task D: 30 points

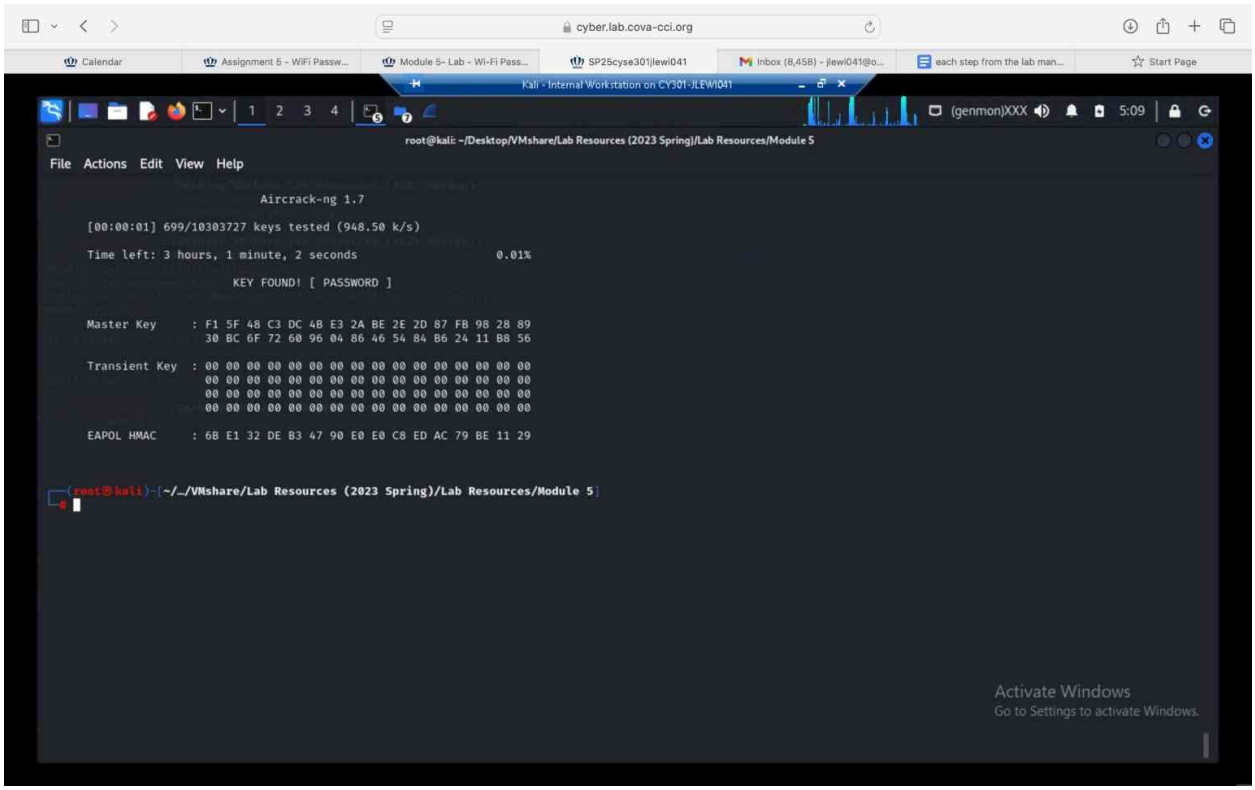
Each student will be assigned a new WPA2 traffic file for analysis. You need to refer to the table below and find the file assigned to you based on the LAST digit of the MD5 of your MIDAS ID. For example, the last digit of the hash for svatsa is **8**. Thus, I should pick up the file "WPA2-P3-01.cap."

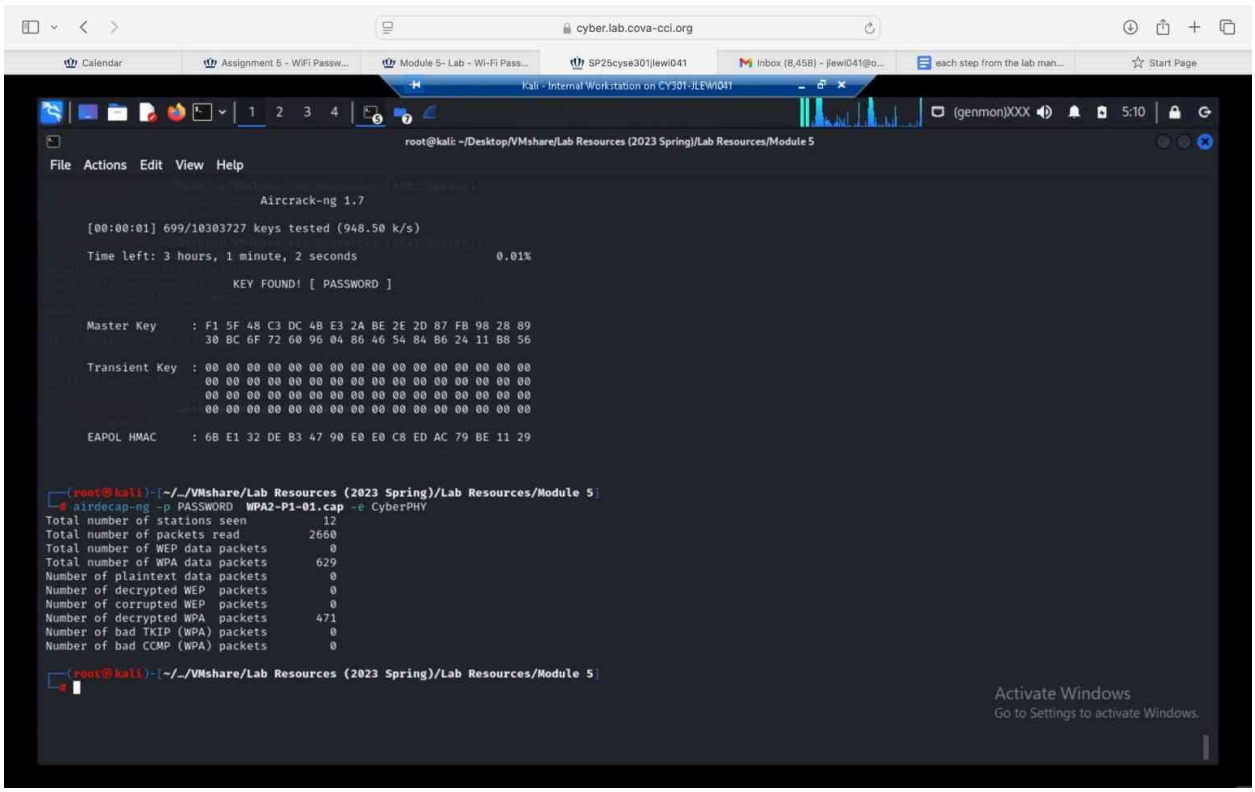
1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points

The first step I did was used the “echo -n jlewi041 | md5sum” command to figure out the last digit of my MIDAS ID, which was 2. After getting that digit I was assigned WPA2-P1-01. The next command I used was “aircrack-ng WPA2-P1-01 -w rockyou.txt” to get the ESSID and password. After getting the password I used the command “airdecap -p PASSWORD WPA2-P1-01.cap -e CyberPHY” to start the dictionary attack.






cyber.lab.cova-cci.org
Calendar
Assignment 5 - WiFi Passw...
Module 5- Lab - Wi-Fi Pass...
SP25cyse301jlewi041
Inbox (8,458) - jlewi041@o...
each step from the lab man...
Start Page
Kali - Internal Workstation on CY301-JLEWI041
(genmon)XXX
5:09
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:01] 699/10303727 keys tested (948.50 k/s)
Time left: 3 hours, 1 minute, 2 seconds 0.01%
KEY FOUND! [PASSWORD]
Master Key : F1 5F 48 C3 DC 4B E3 2A BE 2E 2D 87 FB 98 28 89
30 BC 6F 72 60 96 04 86 46 54 84 B6 24 11 B8 56
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29
(root@kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
Activate Windows
Go to Settings to activate Windows.


cyber.lab.cova-cci.org
Calendar
Assignment 5 - WiFi Passw...
Module 5- Lab - Wi-Fi Pass...
SP25cyse301jlewi041
Inbox (8,458) - jlewi041@o...
each step from the lab man...
Start Page
Kali - Internal Workstation on CY301-JLEWI041
(genmon)XXX
5:10
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:01] 699/10303727 keys tested (948.50 k/s)
Time left: 3 hours, 1 minute, 2 seconds 0.01%
KEY FOUND! [PASSWORD]
Master Key : F1 5F 48 C3 DC 4B E3 2A BE 2E 2D 87 FB 98 28 89
30 BC 6F 72 60 96 04 86 46 54 84 B6 24 11 B8 56
Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 6B E1 32 DE B3 47 90 E0 E0 C8 ED AC 79 BE 11 29
(root@kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
airdecap-ng -p PASSWORD WPA2-P1-01.cap -e CyberPHY
Total number of stations seen 12
Total number of packets read 2660
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
(root@kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
Activate Windows
Go to Settings to activate Windows.

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

To gain access to the decrypt of the encrypted traffic I used the command “wireshark WPA2-P1-01-dec.cap”. After doing so I was able to gain access to the decrypted packet traffic. While looking into the decrypted traffic I was able to see a rage of different protocols. Another thing I noticed was a lot of Pings going on at the end with the protocol ICMP. These Pings were requests and replies between two IPs which were 192.168.1.118 and 8.8.8.8. Another thing I noticed was there was no set trend with the packets. Following that, there were a lot of key exchanges going between the server and client. When looking over the ICMP protocol there were most replies and requests. However, when looking inside them I they were not a lot of information but stuff as status reports. In which majority of the status reports came back as good. When looking into the TLSv.2 protocol I learned that all of them said that they were incomplete conversations.