OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

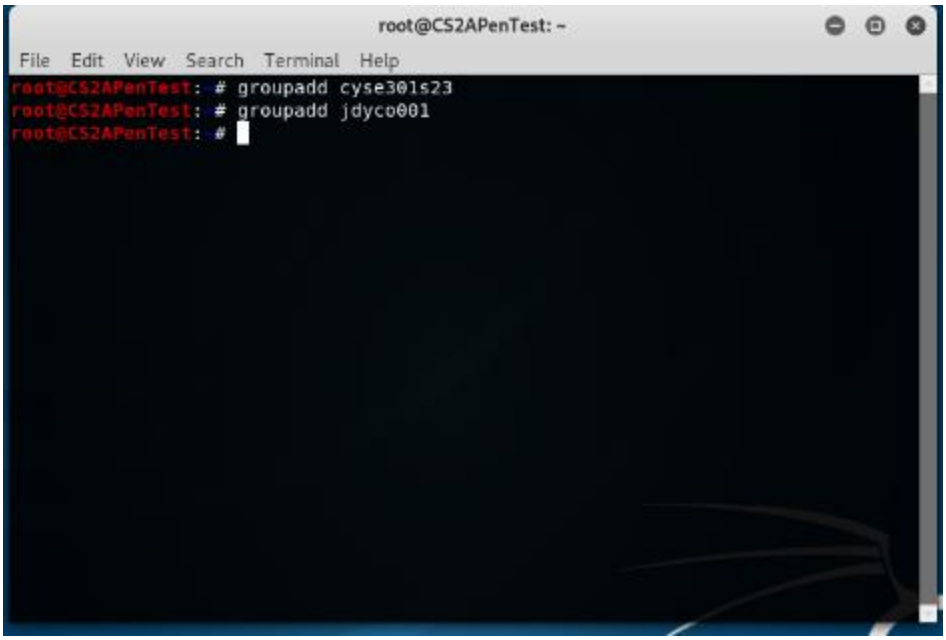
ASSIGNMENT #5 – PASSWORD CRACKING AND WIFI CRACKING

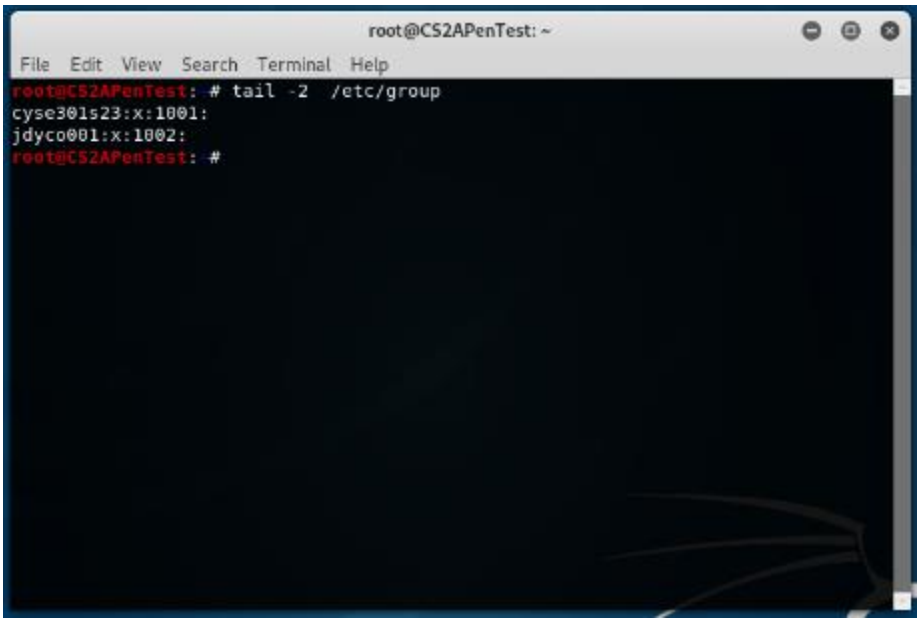
JEGGO PAOLO V. DYCOK

01242866

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.

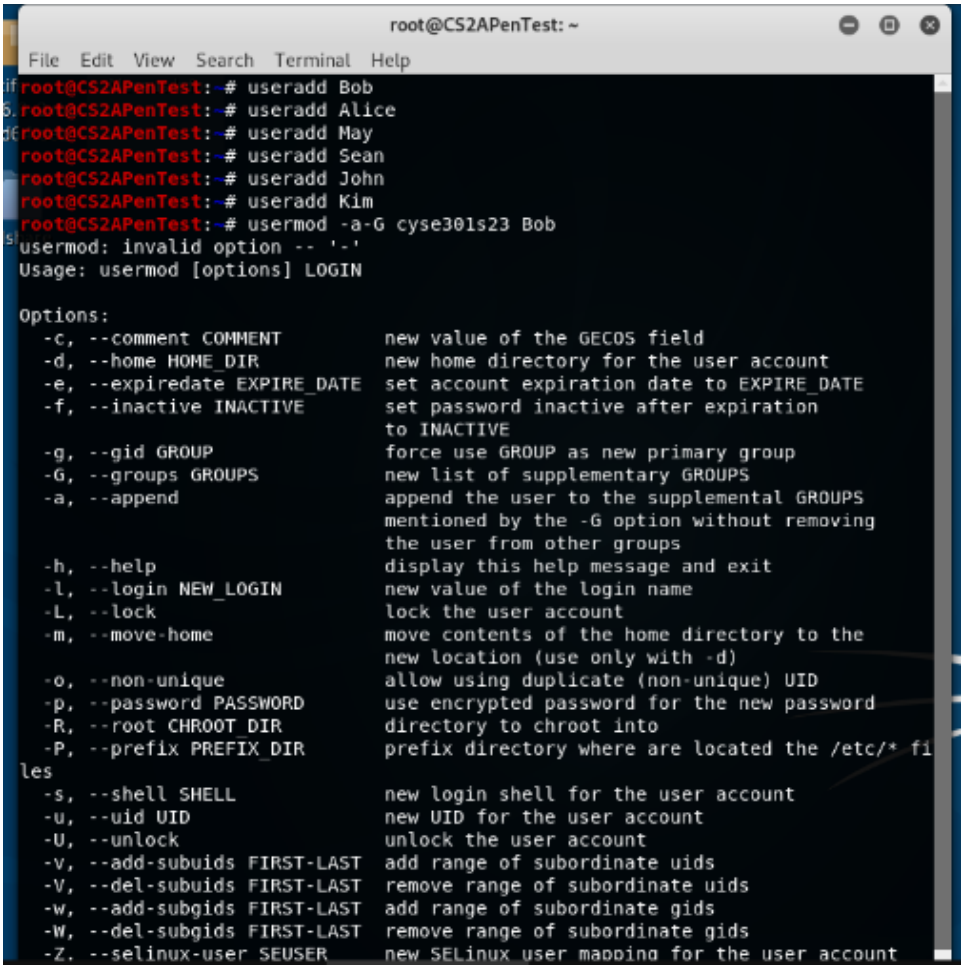


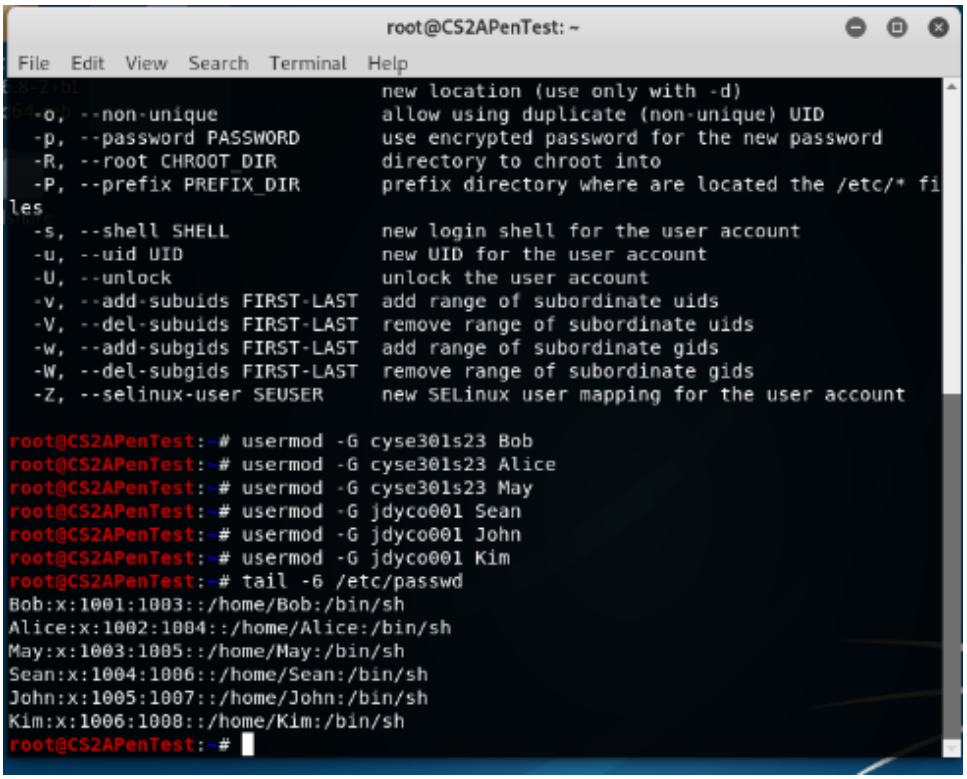


PROCEDURE:

- I created two groups, cyse301s23 and jdyco001 using groupadd command
- I used the tail command on /etc/group to show the last two groups added

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

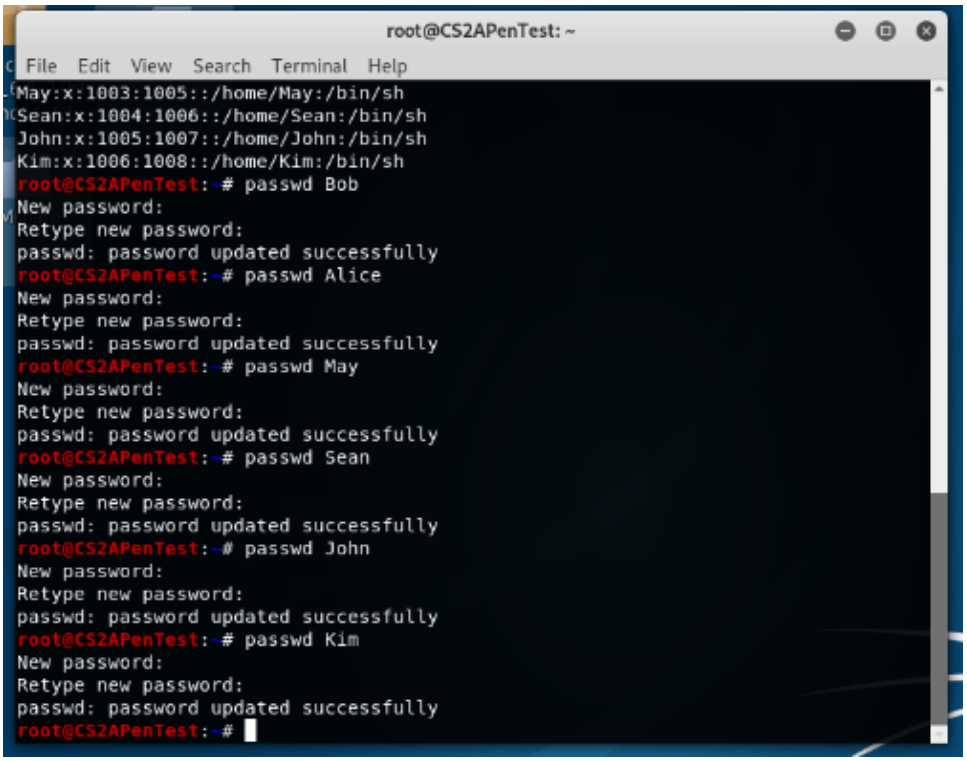




PROCEDURE:

- I created 6 users: Bob, Alice, May, Sean, John and Kim.
- I assigned Bob, Alice, and May to cyse301s23. I assigned Sean, John, and Kim to jdyco001. I then used tail –6 command to show UID and GID of all users.

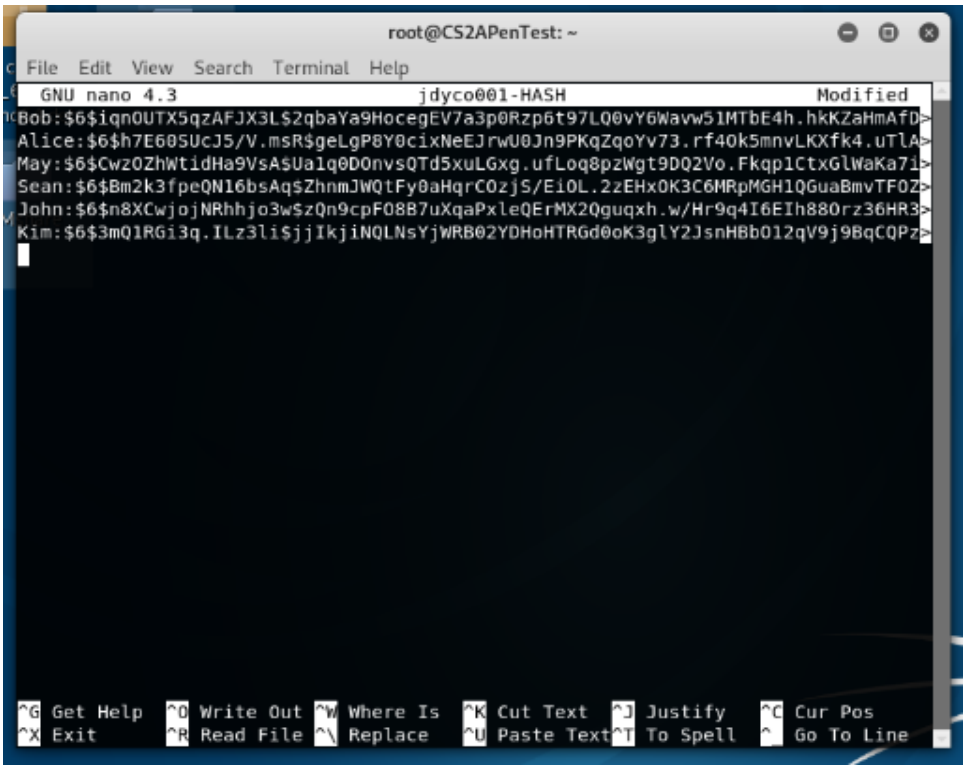
3. 5 points. Choose six new passwords, from easy to hard, and assign them to the users you created. You need to show me the password you selected in your report, and DO NOT use your real-world passwords.

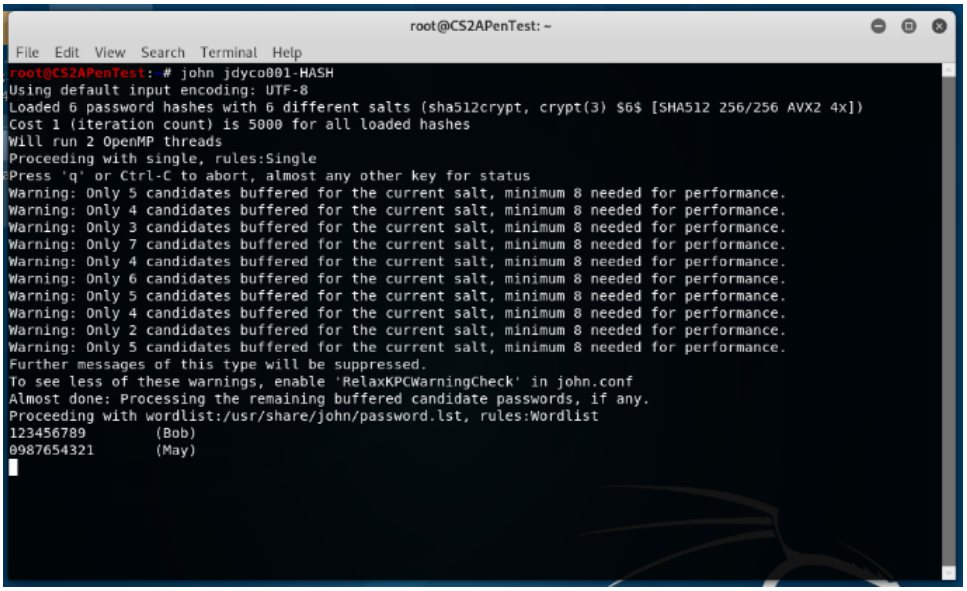


PROCEDURE:

- I used passwd command to create passwords for all 6 users.
    - Bob – pw: 123456789
    - Alice – pw: P@ssword123
    - May – pw: 0987654321
    - Sean – Apple123
    - John – KiwiStrawberry123
    - Kim – Mik1234567

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.





PROCEDURE:

- I exported all six users to jdyco001-HASH using Nano.

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

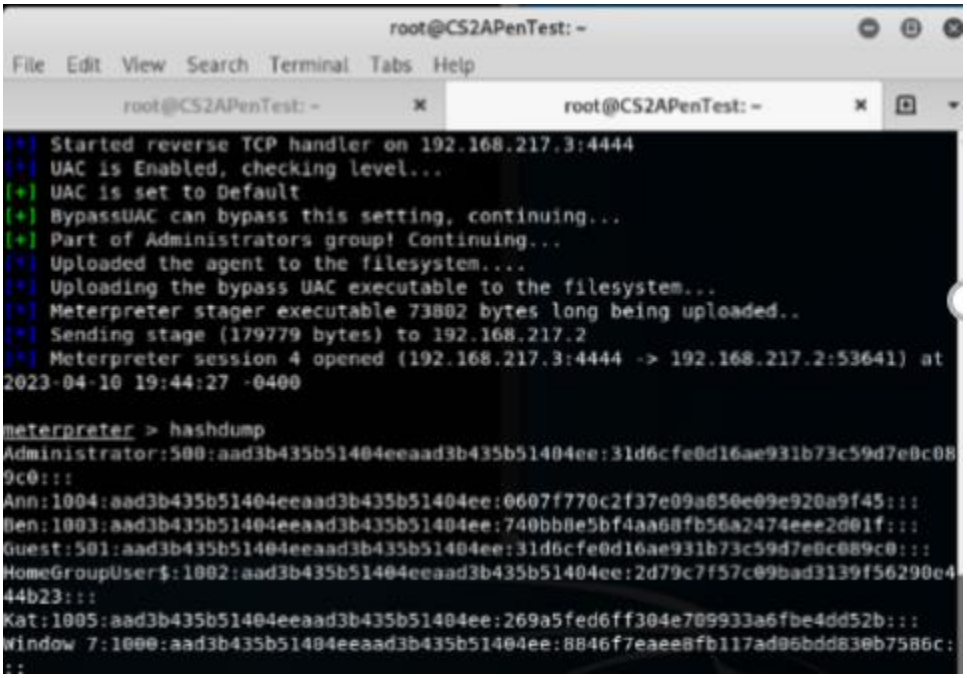
establish a reverse shell connection with the admin privilege to the target Windows 7 VM. Now, complete the following tasks:

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

Ben/P@ss12345

Ann/Abc123456

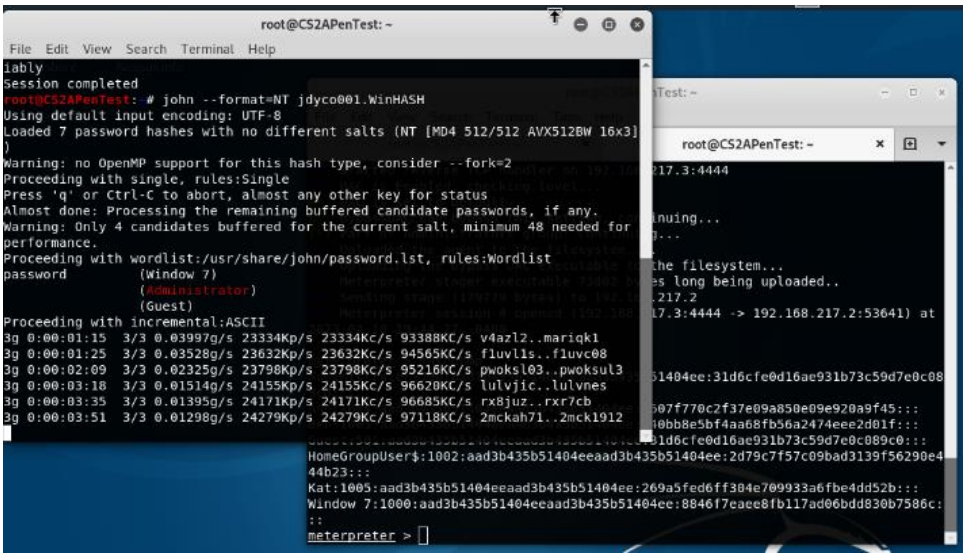
Kat/54321Apple



PROCEDURE:

- I launched a reverse TCP by setting up Kali linux as the listener and msfvenom to deliver a payload to windows 7
- I used command set session 1 and used bypassuac to get administrator access to utilize hashdump command.

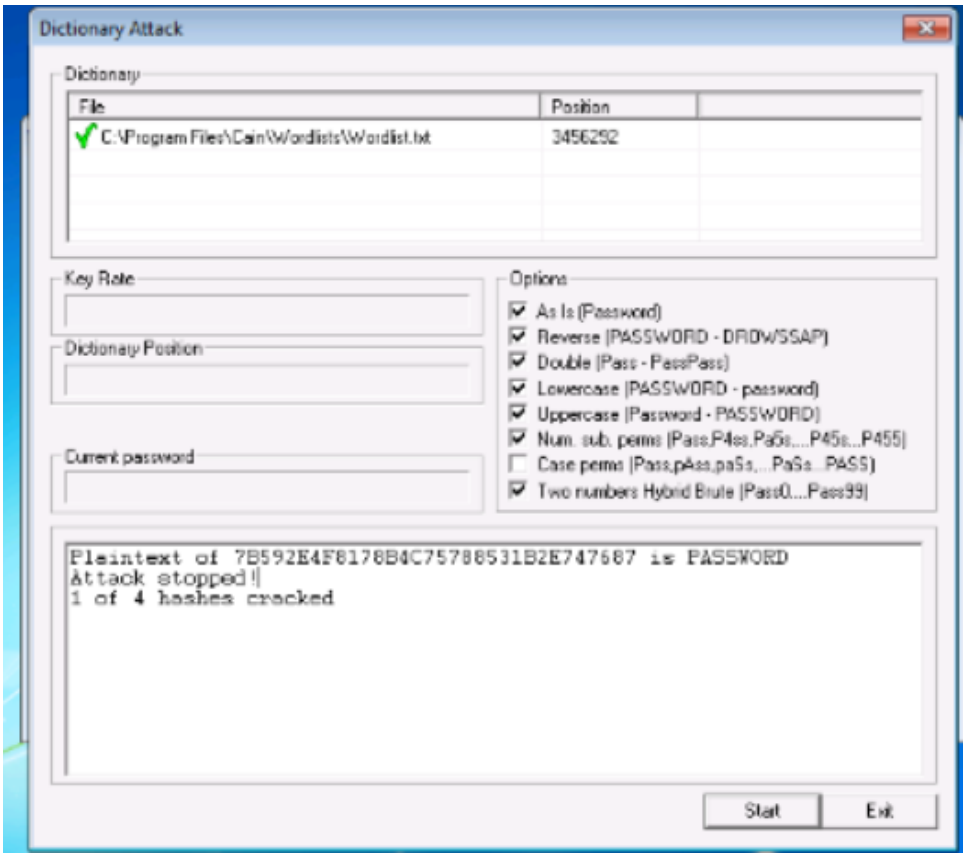
2. 10 points. Save the password hashes into a file named "your_midas.WinHASH" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).

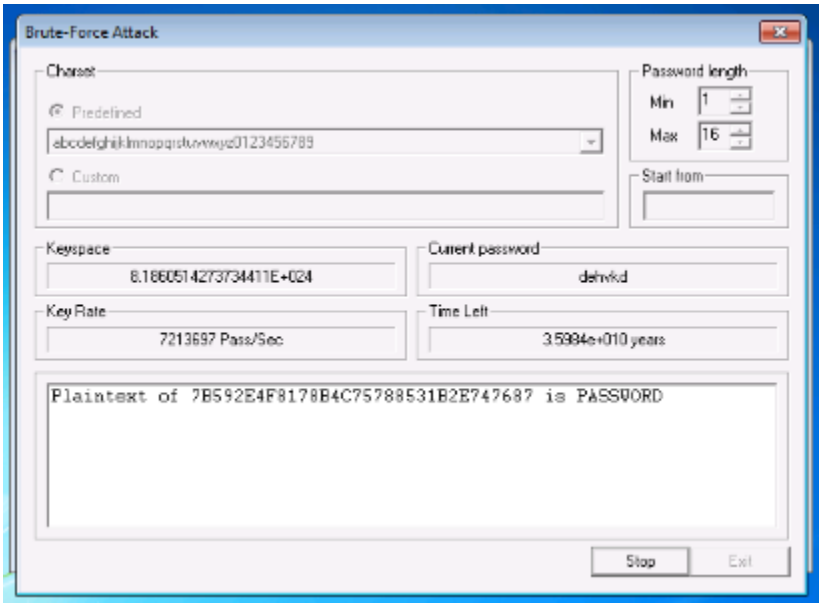


PROCEDURE:

- I saved all the hashes to jdyco001.Win-HASH and ran john the ripper for 10 minutes and got 1 password

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.).





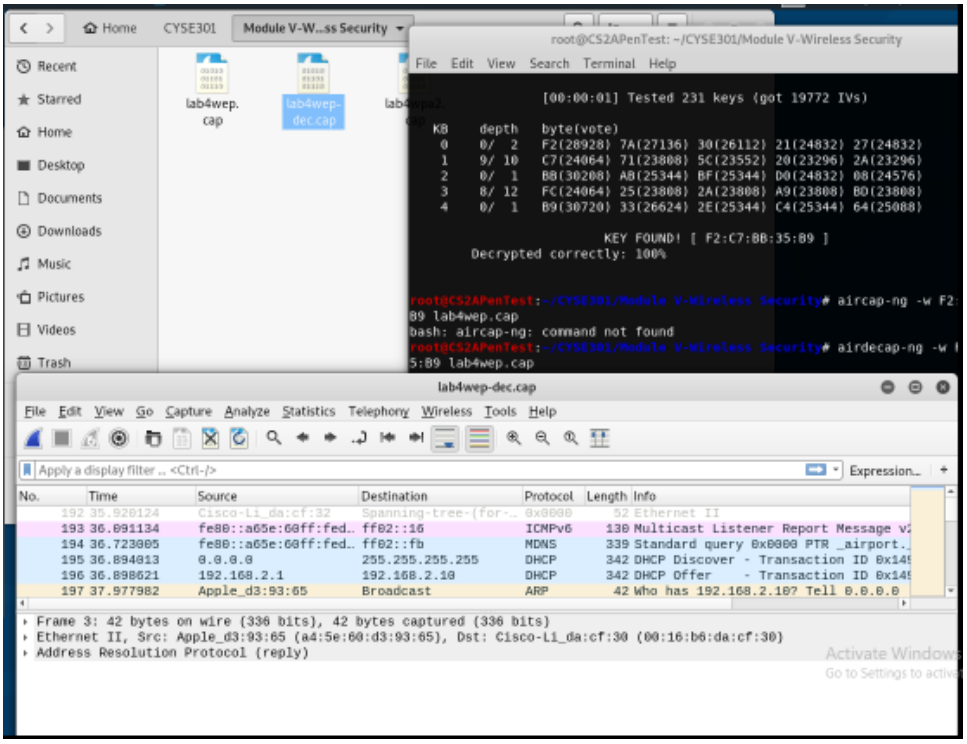
PROCEDURE:

- I uploaded the CAIN and ABEL tool using upload command to upload the setup and ran it, loading the hashes to initiate dictionary attack and brute force.

Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

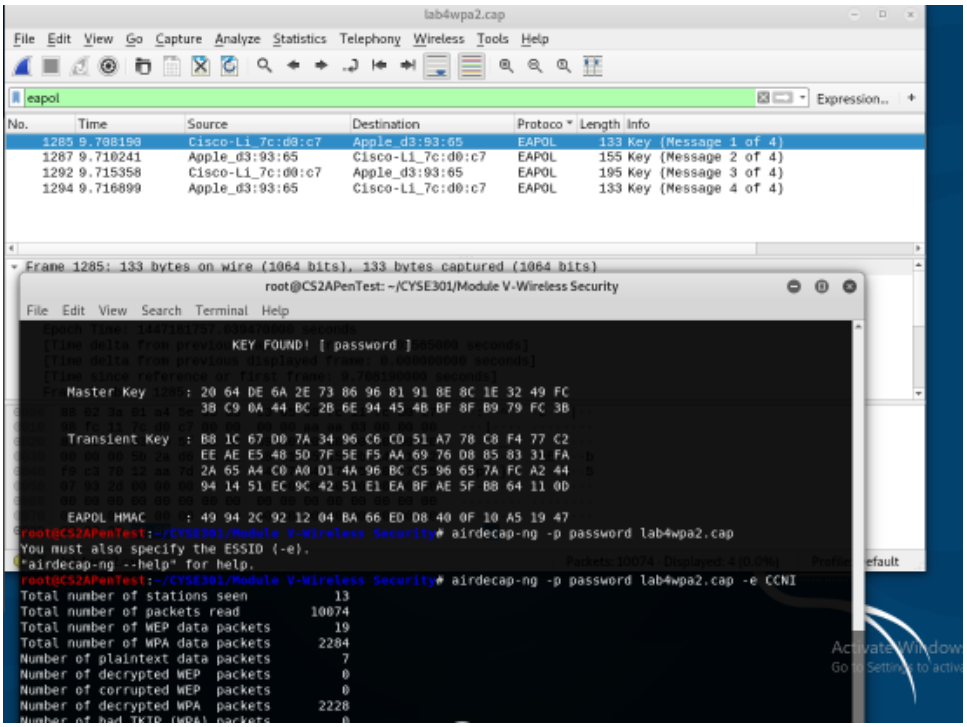
1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

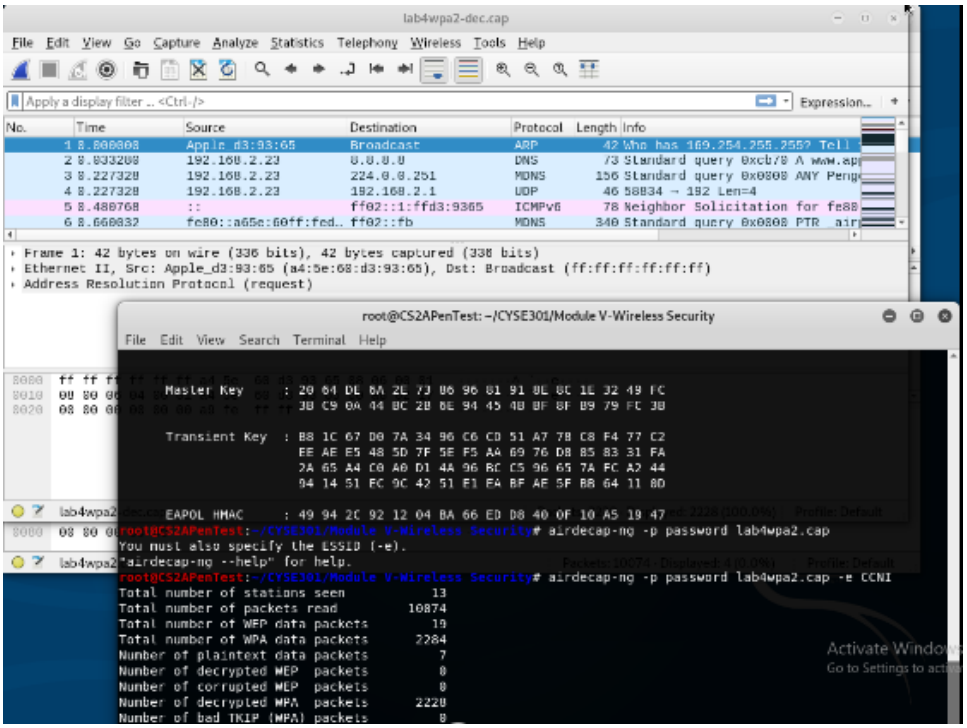


PROCEDURE:

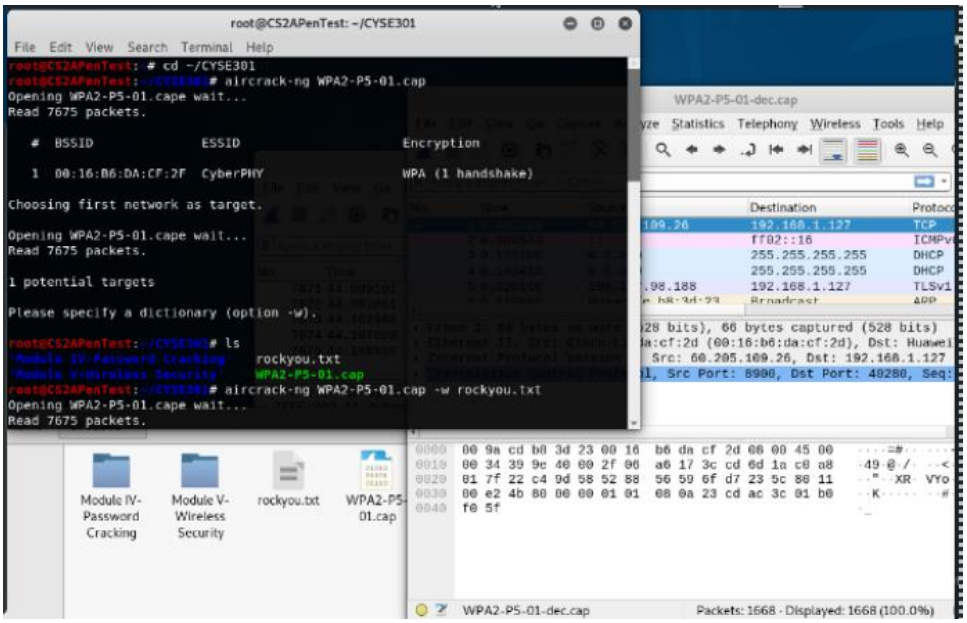
- I opened the wireshark file, used aircrack to decrypt WEP key and used airdecap-ng to create a decrypted file that shoes the protocols. Found a couple of EAP, ARP, TCP, HTTP. Although, the majority of the packets were ARP packets which make up 86% of all traffic.

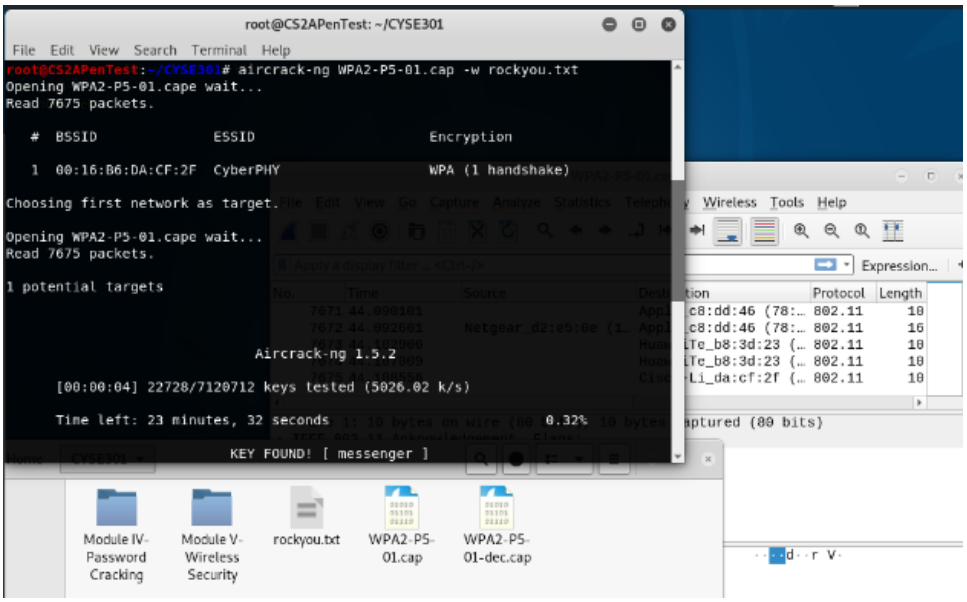
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)

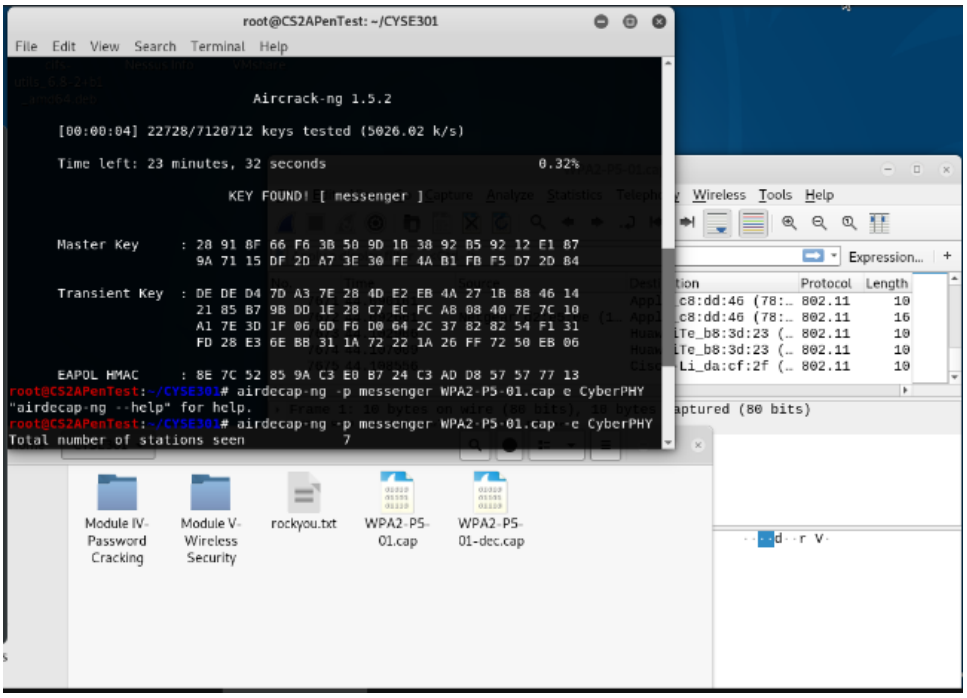

lab4wpa2.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
No. Time Source Destination Protoco Length Info
1285 9.708190 Cisco-Li_7c:d0:c7 Apple_d3:93:65 EAPOL 133 Key (Message 1 of 4)
1287 9.710241 Apple_d3:93:65 Cisco-Li_7c:d0:c7 EAPOL 155 Key (Message 2 of 4)
1292 9.715358 Cisco-Li_7c:d0:c7 Apple_d3:93:65 EAPOL 195 Key (Message 3 of 4)
1294 9.716899 Apple_d3:93:65 Cisco-Li_7c:d0:c7 EAPOL 133 Key (Message 4 of 4)
Frame 1285: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
KEY FOUND! [password]
Master Key : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B
Transient Key : B8 1C 67 D0 7A 34 96 C6 CD 51 A7 78 C8 F4 77 C2
EE AE E5 48 5D 7F 5E F5 AA 69 76 D8 B5 83 31 FA
2A 65 A4 C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44
94 14 51 EC 9C 42 51 E1 EA BF AE 5F B8 64 11 0D
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p password lab4wpa2.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p password lab4wpa2.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

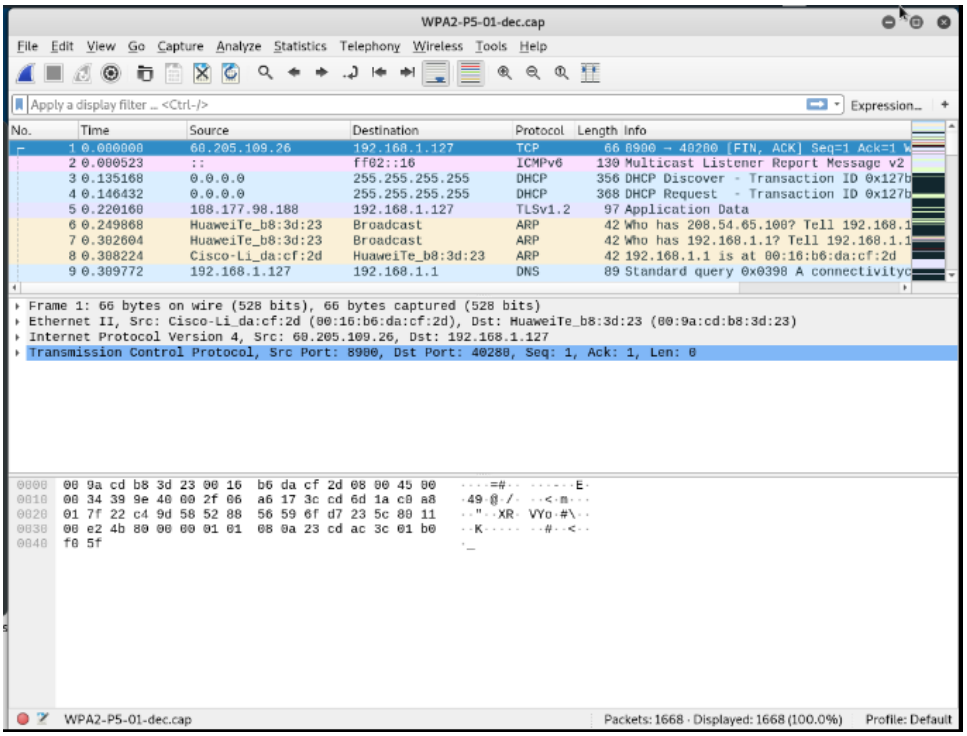

lab4wpa2-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 8.800808 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell
2 8.933208 192.168.2.23 8.8.8.8 DNS 73 Standard query 0xcb78 A www.ap
3 8.227328 192.168.2.23 224.0.0.251 MDNS 156 Standard query 0x0000 ANY Peng
4 8.227328 192.168.2.23 192.168.2.1 UDP 46 58834 → 182 Len=4
5 8.480768 :: ff02::1:ffd3:9365 ICMPv6 78 Neighbor Solicitation for fe80
6 8.660832 fe80::a65e:60ff:fed.. ff02::fb MDNS 340 Standard query 0x0000 PTR _air
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:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Master Key : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
3B C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B
Transient Key : B8 1C 67 D0 7A 34 96 C6 CD 51 A7 78 C8 F4 77 C2
EE AE E5 48 5D 7F 5E F5 AA 69 76 D8 B5 83 31 FA
2A 65 A4 C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44
94 14 51 EC 9C 42 51 E1 EA BF AE 5F B8 64 11 0D
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p password lab4wpa2.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
root@CS2APenTest:~/CYSE301/Module V-Wireless Security# airdecap-ng -p password lab4wpa2.cap -e CCNI
Total number of stations seen 13
Total number of packets read 10874
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

S


root@CS2APenTest: ~/CYSE301
File Edit View Search Terminal Help
root@CS2APenTest: ~ # cd ~/CYSE301
root@CS2APenTest: ~/CYSE301# aircrack-ng WPA2-P5-01.cap
Opening WPA2-P5-01.cape wait...
Read 7675 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:2F CyberPHY WPA (1 handshake)
Choosing first network as target.
Opening WPA2-P5-01.cape wait...
Read 7675 packets.
1 potential targets
Please specify a dictionary (option -w).
root@CS2APenTest: ~/CYSE301# ls
Module IV- Password Cracking rockyou.txt
Module V- Wireless Security WPA2-P5-01.cap
root@CS2APenTest: ~/CYSE301# aircrack-ng WPA2-P5-01.cap -w rockyou.txt
Opening WPA2-P5-01.cape wait...
Read 7675 packets.
WPA2-P5-01-dec.cap
Statistics Telephony Wireless Tools Help
Destination Protocol
192.168.1.127 TCP
ff02::16 ICMPv6
255.255.255.255 DHCP
255.255.255.255 DHCP
192.168.1.127 TLSv1
Broadcast ARP
28 bits), 66 bytes captured (528 bits)
a:cf:2d (00:16:b6:da:cf:2d), Dst: Huawei
Src: 60.205.109.26, Dst: 192.168.1.127
l, Src Port: 8990, Dst Port: 40280, Seq:
00 9a cd b0 3d 23 00 16 b6 da cf 2d 08 00 45 00
00 34 39 9c 40 00 2f 06 a6 17 3c cd 6d 1a c0 a8
01 7f 22 c4 9d 58 52 88 56 59 6f d7 23 5c 80 11
00 e2 4b 80 00 00 01 01 08 0a 23 cd ac 3c 01 b0
f0 5f
Module IV- Password Cracking
Module V- Wireless Security
rockyou.txt
WPA2-P5-01.cap
WPA2-P5-01-dec.cap
Packets: 1668 · Displayed: 1668 (100.0%)


root@CS2APenTest: ~/CYSE301
File Edit View Search Terminal Help
root@CS2APenTest:~/CYSE301# aircrack-ng WPA2-P5-01.cap -w rockyou.txt
Opening WPA2-P5-01.cape wait...
Read 7675 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:2F CyberPHY WPA (1 handshake)
Choosing first network as target.
Opening WPA2-P5-01.cape wait...
Read 7675 packets.
1 potential targets
Aircrack-ng 1.5.2
[00:00:04] 22728/7120712 keys tested (5026.02 k/s)
Time left: 23 minutes, 32 seconds 0.32%
KEY FOUND! [messenger]
Wireless Tools Help
Expression...
Protocol Length
c8:dd:46 (78:... 802.11 10
c8:dd:46 (78:... 802.11 16
LTe_b8:3d:23 (... 802.11 10
LTe_b8:3d:23 (... 802.11 10
Li_da:cf:2f (... 802.11 10
aptured (80 bits)
Module IV- Password Cracking
Module V- Wireless Security
rockyou.txt
WPA2-P5-01.cap
WPA2-P5-01-dec.cap



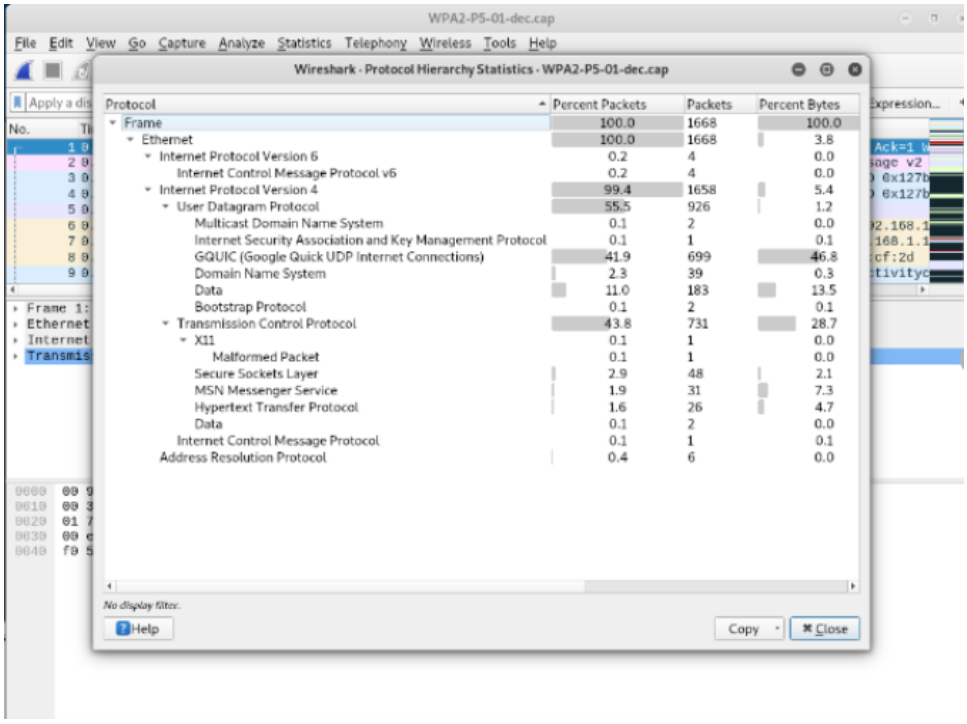


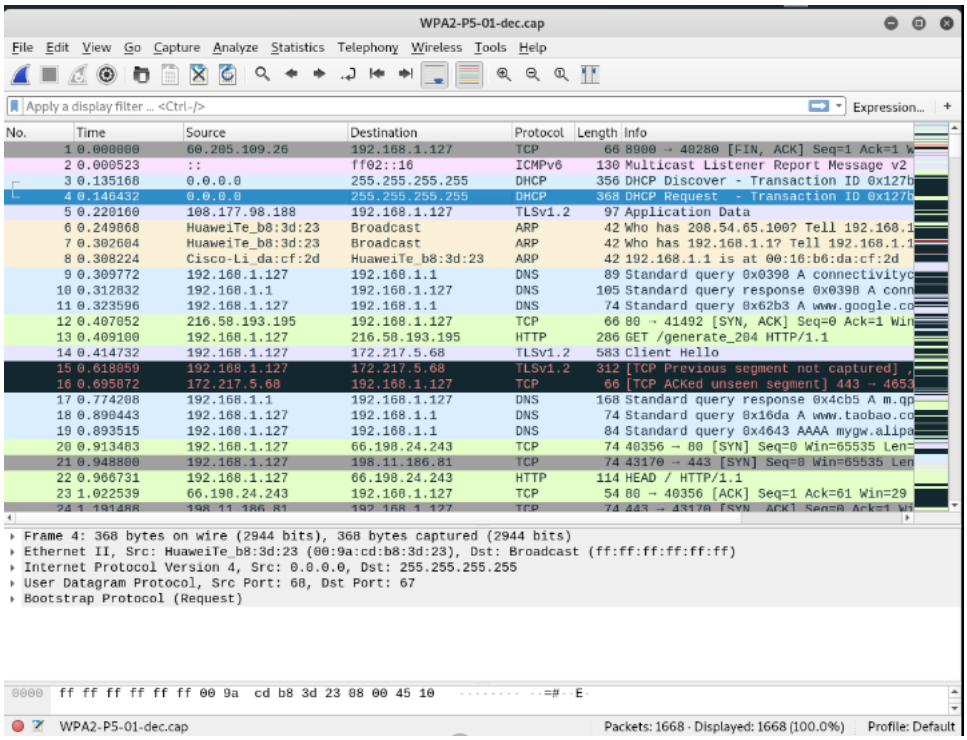
PROCEDURE:

- First, I opened the lab4wpa2.cap and see the encrypted traffic under 802.11
- I used aircrack-ng lab4wpa2.cap
- I selected “4” as an option due to WPA encryption
- I copied rockyou.txt.gz to working directory
- I unzipped rockyou.txt.gz

- I used the file to run a dictionary attack and found the password which is “password”
- I used aircdecap to create lab4wpa2-dec.cap and opened it on wireshark
- By analyzing the file, it appears that majority of the packets are TCP packets which is about 98% and IPV4 packets at 99.7%.

2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored
from this encrypted traffic file. -10 points
Last digit of your MD5 Filename
0~3 WPA2-P1-01.cap
4~5 WPA2-P2-01.cap
6~8 WPA2-P3-01.cap
9~B WPA2-P4-01.cap
C~F WPA2-P5-01.cap
Figure 1 Command to get the MD5 hash.





PROCEDURE:

- MD5 for jdyco001 is d7c49808446d3257c2ecbd70beb7271e so I used WPA2-P5-01.cap
- I used aircrack-ng to open the file
- There was only 1 option so I selected it
- I copied rockyou.txt.gz to desktop where I moved the .cap file
- I used aircrack to find the WPA key.
- I used the airdecap to create the decap file and review the traffic
- In my analysis, I noticed that IPV4 has majority of the protocols with 99.4%, UDP at 55.5%, TCP at 41.9% an TCP at 43.8% of all data packets.