OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Wi-Fi Password Cracking (Part B)

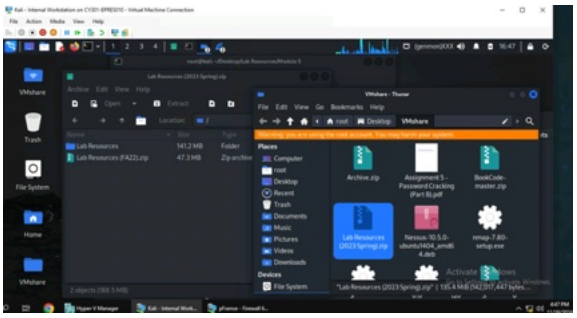
Eric Mung'aũ Preston

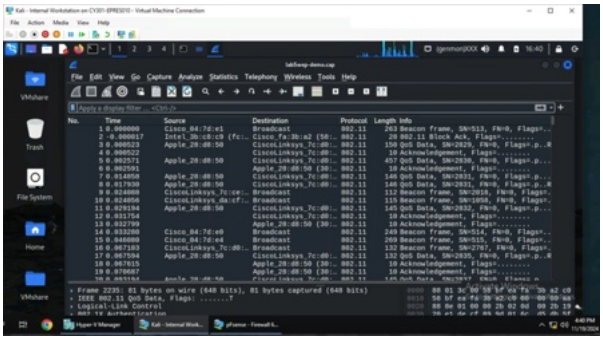
01228601

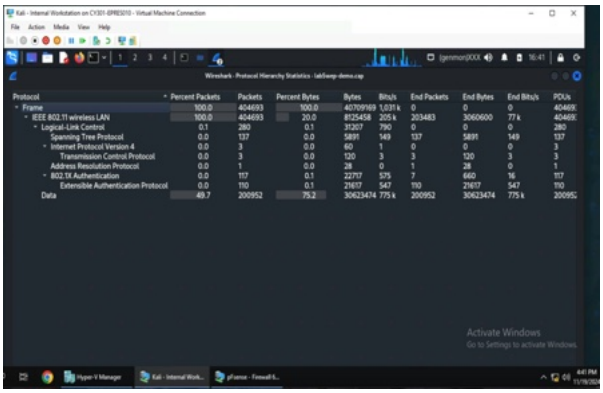
Task C: 20 points

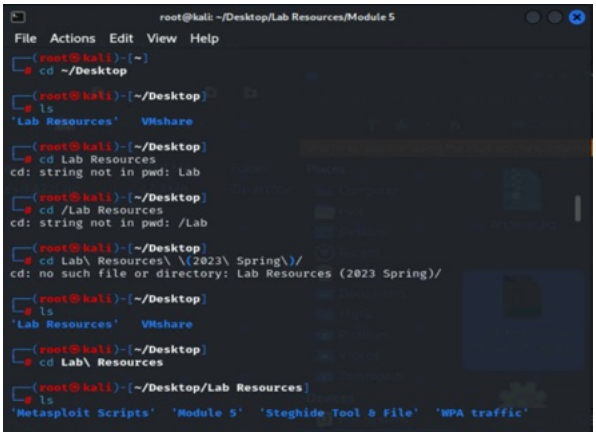
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

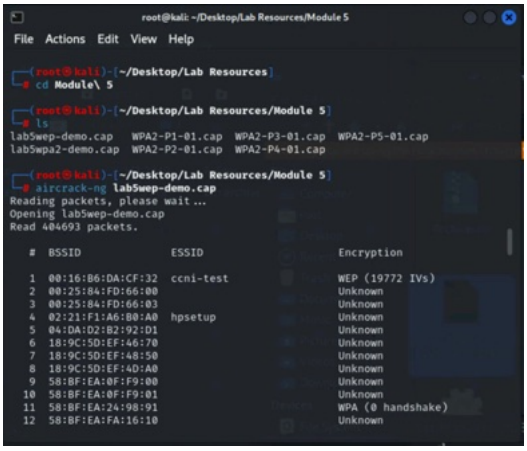
1. Decrypt the lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

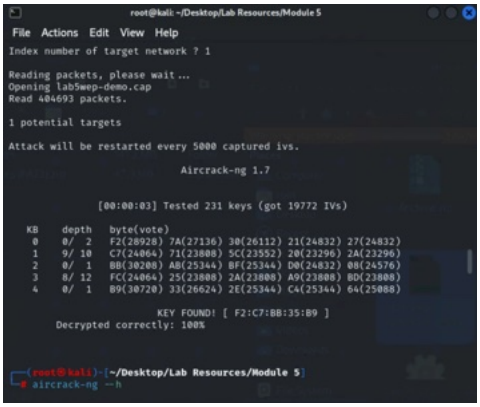


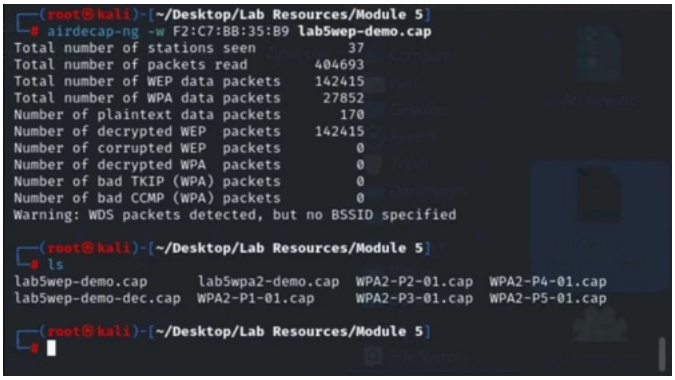


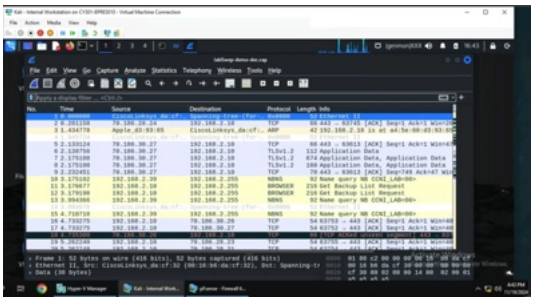


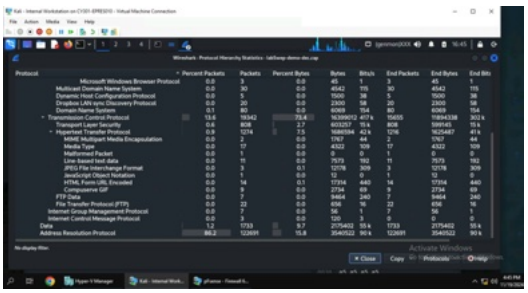

root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# cd ~/Desktop
┌──(root㉿kali)-[~/Desktop]
└─# ls
'Lab Resources'   VMshare
┌──(root㉿kali)-[~/Desktop]
└─# cd Lab Resources
cd: string not in pwd: Lab
┌──(root㉿kali)-[~/Desktop]
└─# cd /Lab Resources
cd: string not in pwd: /Lab
┌──(root㉿kali)-[~/Desktop]
└─# cd Lab\ Resources\ \(2023\ Spring\)/
cd: no such file or directory: Lab Resources (2023 Spring)/
┌──(root㉿kali)-[~/Desktop]
└─# ls
'Lab Resources'   VMshare
┌──(root㉿kali)-[~/Desktop]
└─# cd Lab\ Resources
┌──(root㉿kali)-[~/Desktop/Lab Resources]
└─# ls
'Metasploit Scripts' 'Module 5' 'Steghide Tool & File' 'WPA traffic'


root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
┌──(root㉿kali)-[~/Desktop/Lab Resources]
└─# cd Module\ 5
┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap   WPA2-P1-01.cap WPA2-P3-01.cap WPA2-P5-01.cap
lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P4-01.cap
┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─# aircrack-ng lab5wep-demo.cap
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:32 ccni-test WEP (19772 IVs)
2 00:25:84:FD:66:00 Unknown
3 00:25:84:FD:66:03 Unknown
4 02:21:F1:A6:B0:A0 hpsetup Unknown
5 04:DA:D2:B2:92:D1 Unknown
6 18:9C:5D:EF:46:70 Unknown
7 18:9C:5D:EF:48:50 Unknown
8 18:9C:5D:EF:4D:A0 Unknown
9 58:BF:EA:0F:F9:00 Unknown
10 58:BF:EA:0F:F9:01 Unknown
11 58:BF:EA:24:98:91 WPA (0 handshake)
12 58:BF:EA:FA:16:10 Unknown


root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
Index number of target network ? 1
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.
1 potential targets
Attack will be restarted every 5000 captured ivs.
Aircrack-ng 1.7
[00:00:03] Tested 231 keys (got 19772 IVs)
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─# aircrack-ng --h

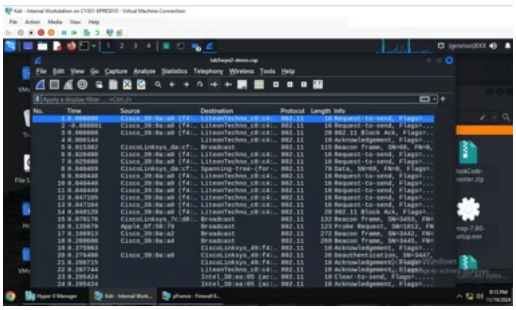

┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─# airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen 37
Total number of packets read 404693
Total number of WEP data packets 142415
Total number of WPA data packets 27852
Number of plaintext data packets 170
Number of decrypted 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
┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P4-01.cap
lab5wep-demo-dec.cap WPA2-P1-01.cap WPA2-P3-01.cap WPA2-P5-01.cap
┌──(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
└─#

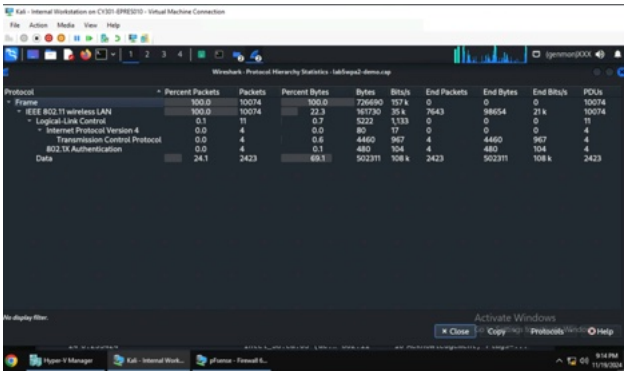


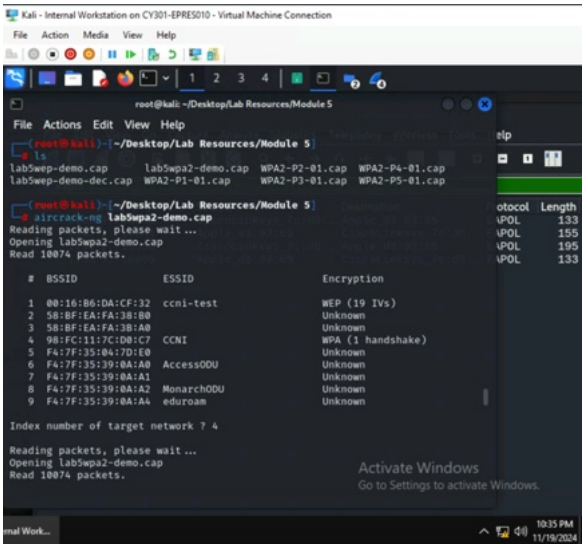


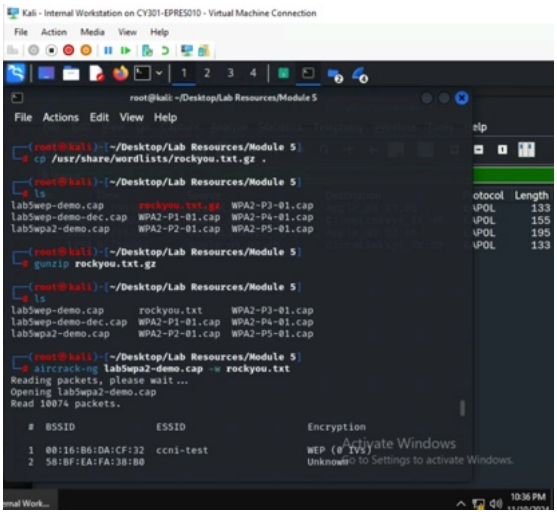
To decrypt the file, I first copied the Lab Resources file onto my Internal Kali VM desktop. I then opened the “lab5wep-demo.cap” file in Wireshark and performed a Protocol Hierarchy Statistical Analysis to look at what packets were viewable from the encrypted file. Using the cd and ls commands, I worked my way up to the correct directory to then use “aircrack-ng lab5wep-demo.cap” to better look at the traffic. After setting my index network to 1, I got the WEP key, and then entered the “airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap” command to decrypt the file. I went back to Wireshark, opened the decrypted file, show the decrypted traffic, and performed another Protocol Hierarchy Statistical Analysis. 86.2% of the packets were under Address Resolution Protocol, and the other 13.6% were using Transmission Control Protocol with Internet Protocol Version 4. Looking through the traffic there were a significant amount of ARP packets broadcasting for the IP address 192.168.20.10.

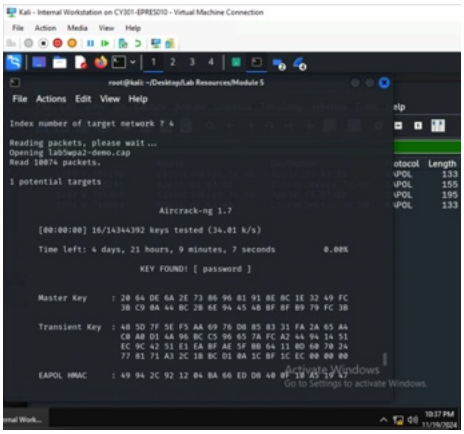
2. Decrypt the lab5wpa2-demo. cap file (5 points) and perform a detailed traffic analysis (**5 points**)

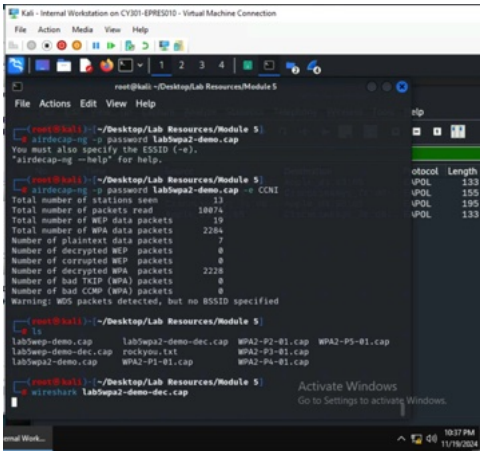


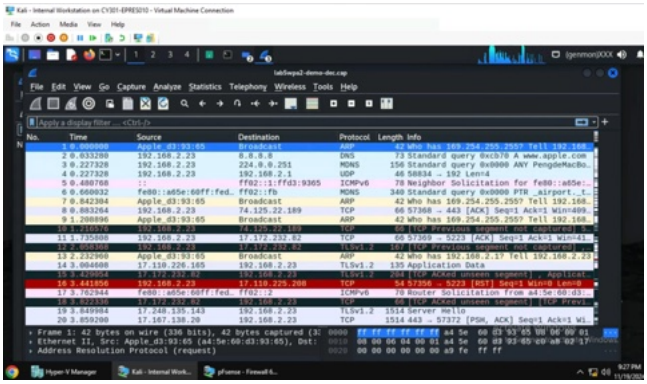

Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
Wireshark · Protocol Hierarchy Statistics · lab5wpa2-demo.cap
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
PDUs
Frame 100.0 10074 100.0 726690 157 k 0 0 0 10074
IEEE 802.11 wireless LAN 100.0 10074 22.3 161730 35 k 7643 98654 21 k 10074
Logical-Link Control 0.1 11 0.7 5222 1133 0 0 0 11
Internet Protocol Version 4 0.0 4 0.0 80 17 0 0 0 4
Transmission Control Protocol 0.0 4 0.6 4460 967 4 4460 967 4
802.1X Authentication 0.0 4 0.1 480 104 4 480 104 4
Data 24.1 2423 69.1 502311 108 k 2423 502311 108 k 2423
Activate Windows
Close
Copy
Protocols
Help

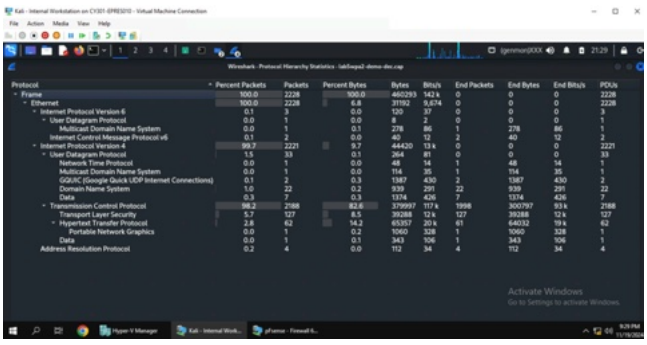

Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
ls
lab5wep-demo.cap lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P4-01.cap
lab5wep-demo-dec.cap WPA2-P1-01.cap WPA2-P3-01.cap WPA2-P5-01.cap
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
aircrack-ng lab5wpa2-demo.cap
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:32 ccni-test WEP (19 IVs)
2 58:BF:EA:FA:38:B0 Unknown
3 58:BF:EA:FA:3B:A0 Unknown
4 98:FC:11:7C:D0:C7 CCNI WPA (1 handshake)
5 F4:7F:35:04:7D:E0 Unknown
6 F4:7F:35:39:0A:A0 AccessODU Unknown
7 F4:7F:35:39:0A:A1 Unknown
8 F4:7F:35:39:0A:A2 MonarchODU Unknown
9 F4:7F:35:39:0A:A4 eduroam Unknown
Index number of target network ? 4
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.
Activate Windows
Go to Settings to activate Windows.
10:35 PM
11/19/2024


Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
cp /usr/share/wordlists/rockyou.txt.gz .
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
ls
lab5wep-demo.cap rockyou.txt.gz WPA2-P3-01.cap
lab5wep-demo-dec.cap WPA2-P1-01.cap WPA2-P4-01.cap
lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P5-01.cap
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
gunzip rockyou.txt.gz
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
ls
lab5wep-demo.cap rockyou.txt WPA2-P3-01.cap
lab5wep-demo-dec.cap WPA2-P1-01.cap WPA2-P4-01.cap
lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P5-01.cap
(root㉿kali)-[~/Desktop/Lab Resources/Module 5]
aircrack-ng lab5wpa2-demo.cap -w rockyou.txt
Reading packets, please wait...
Opening lab5wpa2-demo.cap
Read 10074 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:32 ccni-test WEP (0 IVs)
2 58:BF:EA:FA:38:B0 Unknown
Activate Windows
Go to Settings to activate Windows.
10:36 PM


Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
Index number of target network ? 4
Reading packets, please wait ...
Opening lab5wpa2-demo.cap
Read 10074 packets.
1 potential targets
Aircrack-ng 1.7
[00:00:00] 16/14344392 keys tested (34.01 k/s)
Time left: 4 days, 21 hours, 9 minutes, 7 seconds 0.00%
KEY FOUND! [password]
Master Key : 20 64 DE 6A 2E 73 86 96 81 91 8E BC 1E 32 49 FC
3B C9 8A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B
Transient Key : 48 5D 7F 5E F5 AA 69 76 D8 85 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 8D 60 70 24
77 81 71 A3 2C 1B BC D1 0A 1C BF 1C EC 00 00 00
EAPOL HMAC : 49 94 2C 92 12 04 8A 66 ED D8 40 0F 10 A5 14 47
Activate Windows
Go to Settings to activate Windows.


Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~/Desktop/Lab Resources/Module 5
File Actions Edit View Help
(root@kali)-[~/Desktop/Lab Resources/Module 5]
airdecap-ng -p password lab5wpa2-demo.cap
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.
(root@kali)-[~/Desktop/Lab Resources/Module 5]
airdecap-ng -p password lab5wpa2-demo.cap -e CCNI
Total number of stations seen 1)
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)-[~/Desktop/Lab Resources/Module 5]
ls
lab5wep-demo.cap lab5wpa2-demo-dec.cap WPA2-P2-01.cap WPA2-P5-01.cap
lab5wep-demo-dec.cap rockyou.txt WPA2-P3-01.cap
lab5wpa2-demo.cap WPA2-P1-01.cap WPA2-P4-01.cap
(root@kali)-[~/Desktop/Lab Resources/Module 5]
wireshark lab5wpa2-demo-dec.cap
Activate Windows
Go to Settings to activate Windows.


Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured
Ethernet II, Src: Apple_d3:93:65 (a4:5e:60:d3:93:65), Dst:
Address Resolution Protocol (request)


Kali - Internal Workstation on CY301-EPRES010 - Virtual Machine Connection
Wireshark · Protocol Hierarchy Statistics · lab5wpa2-demo-dec.cap
Protocol
Frame
Ethernet
Internet Protocol Version 6
User Datagram Protocol
Multicast Domain Name System
Internet Control Message Protocol v6
Internet Protocol Version 4
User Datagram Protocol
Network Time Protocol
Multicast Domain Name System
QUIC (Google Quick UDP Internet Connections)
Domain Name System
Data
Transmission Control Protocol
Transport Layer Security
Hypertext Transfer Protocol
Portable Network Graphics
Data
Address Resolution Protocol
Activate Windows
Go to Settings to activate Windows.

To start, I switched to Wireshark and opened the “lab5wpa2-demo.cap” to see the encrypted traffic and performed a Protocol Hierarchy Statistical Analysis to see that the traffic was under IEEE 802.11 Wireless LAN. Going back to my terminal, since I was still in the necessary directory, I used the ls command to see all file options, and then used “aircrack-ng lab5wpa2-demo.cap” with the index number set to 4. I copied the default wordlist to the current directory with “cp /usr/share/wordlists/rockyou.txt.gz .”, unzipped the wordlist with “gunzip rockyou.txt.gz”, started cracking again with “aircrack-ng lab5wpa2-demo.cap -w rockyou.txt” and used ls to check my progress. I set the index number to 4 again and got the key as “password”. Afterwards, I started the decryption process with the command “airdecap-ng -p password lab5wpa2-demo.cap” with an added “-e CCNI” for specification. I then used ls to check my files, used the command “wireshark lab5wpa2-demo-dec.cap” to switch to Wireshark with the decrypted file to look at its traffic, and performed another Protocol Hierarchy Statistical Analysis. Looking at the analysis, there are significantly fewer packets than the WEP file at 2,228 compared to over 100,000. 98.2% percent of packets were TCP packets and 99.7% were under IPv4 Protocol. With the traffic, the most prominent IP addresses were 192.168.2.23 and 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 svatsa is **8**. Thus, I should pick up the file "WPA2-P3-01.cap."

*MD5 of svatsa is fe2943715a4e07c670b242559f5974f**8***

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 (2023 Spring)." You can locate the zipped folder in your VMshare in any Kali Linux VM. Then, extract the zipped file and find the assigned WPA file under the sub-folder "WPA traffic."

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

• Please note that - it is recommended to copy the zip file to your local folder before extracting the whole file in the VMshare folder.

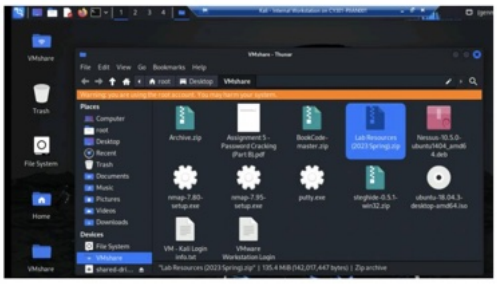


Figure 1 Location of Lab Resource (2023 Spring) in the VMshare folder.

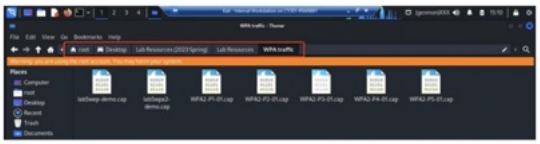
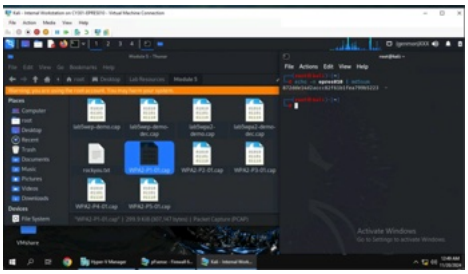
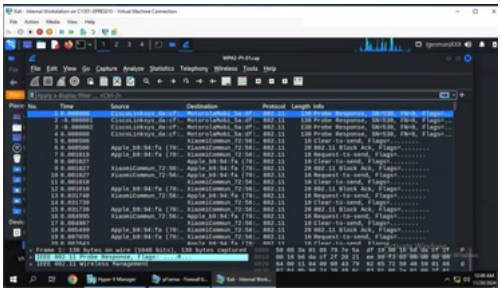


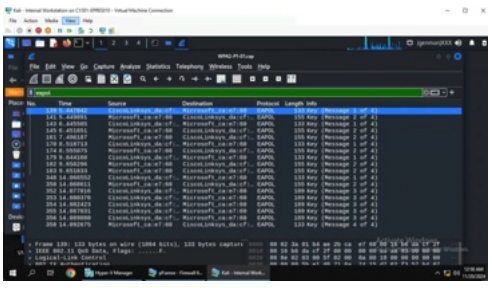
Figure 2 I copied the zip file to the Desktop and then extracted it to access the WPA traffic folder.

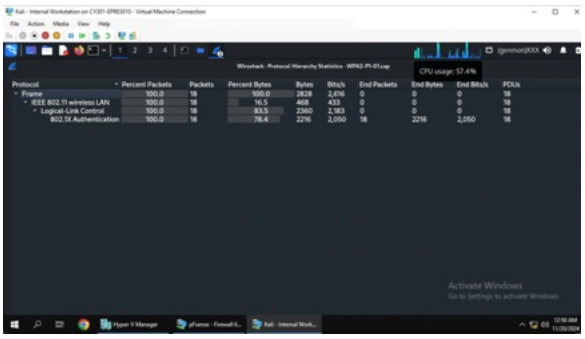
Then complete the following steps:

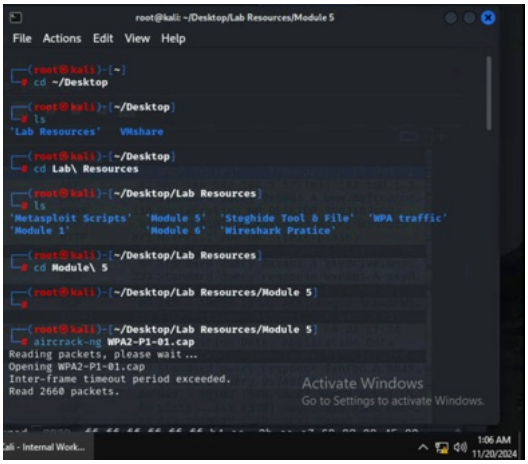
1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points

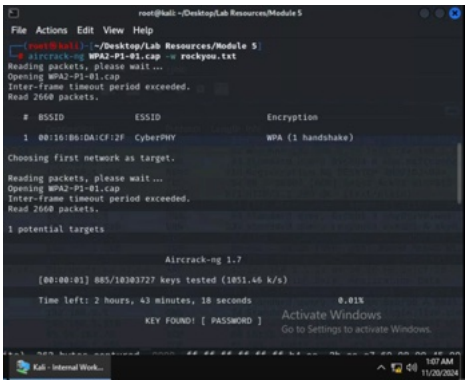






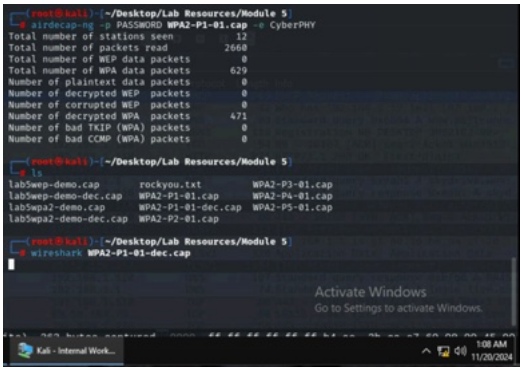


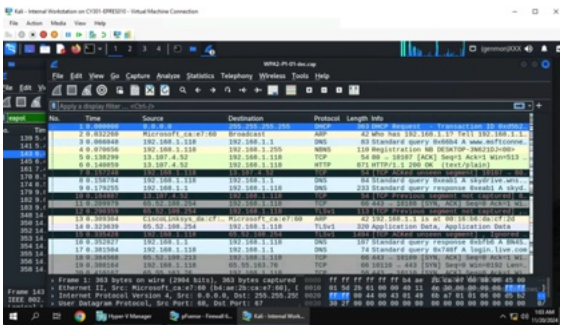


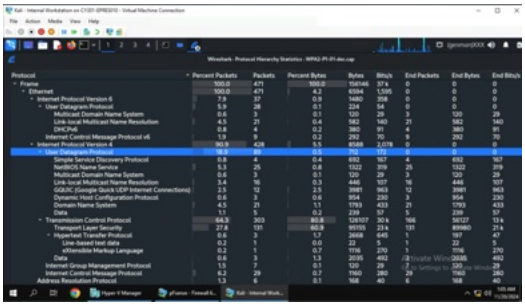


With my MD5 hash being 872dde14d2accc82f61b1fea799b5223 after epres010, I opened the "WPA2-P1-01.cap" file in Wireshark and looked at the main traffic with and without the "eapol" filter for seeing the 4-way handshakes and general traffic, and performed a Protocol Hierarchy Statistical Analysis. I then used the cd and ls commands to move up to the right directory and used the "aircrack-ng WPA2-P1-01.cap" to get access to the key, but later added "-w rockyou.txt" to add the wordlist and for the command to function properly. Finally, I managed to crack the file and got the "PASSWORD" key.

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







After learning about the file's key, I entered the command "airdecap-ng -p PASSWORD WPA2-P1-01.cap -e CyberPHY" due to CyberPHY being the only additional information to put into the command, decrypting most of the packets in the file. I then used the ls command to see all files, and then changed back to Wireshark with "wireshark WPA2-P1-01-dec.cap." I had access to the general traffic and performed a Protocol Hierarchy Statistical Analysis. From the analysis, the most significant factors are that 90.0% of packets are under IPv4, 64.3% are using TCP, 27.8% are under TLS, and 18.9% are using UDP. Another point is that TCP packets take up 80.8% of the percent bytes and TLS packets take up 60.9%. There are also 471 packets in total. Looking at the overall traffic, there were also a decent quantity of GQUIC packets, LLMNR packets, and ICMP packets. There were also TCK and TLSv1.2 packets that had segments not captured. GQUIC packets remained encrypted despite the decryption command. Finally, the traffic ended with ICMP packets ping requesting and replying in between the IP addresses 192.168.1.118 and 8.8.8.8.