OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

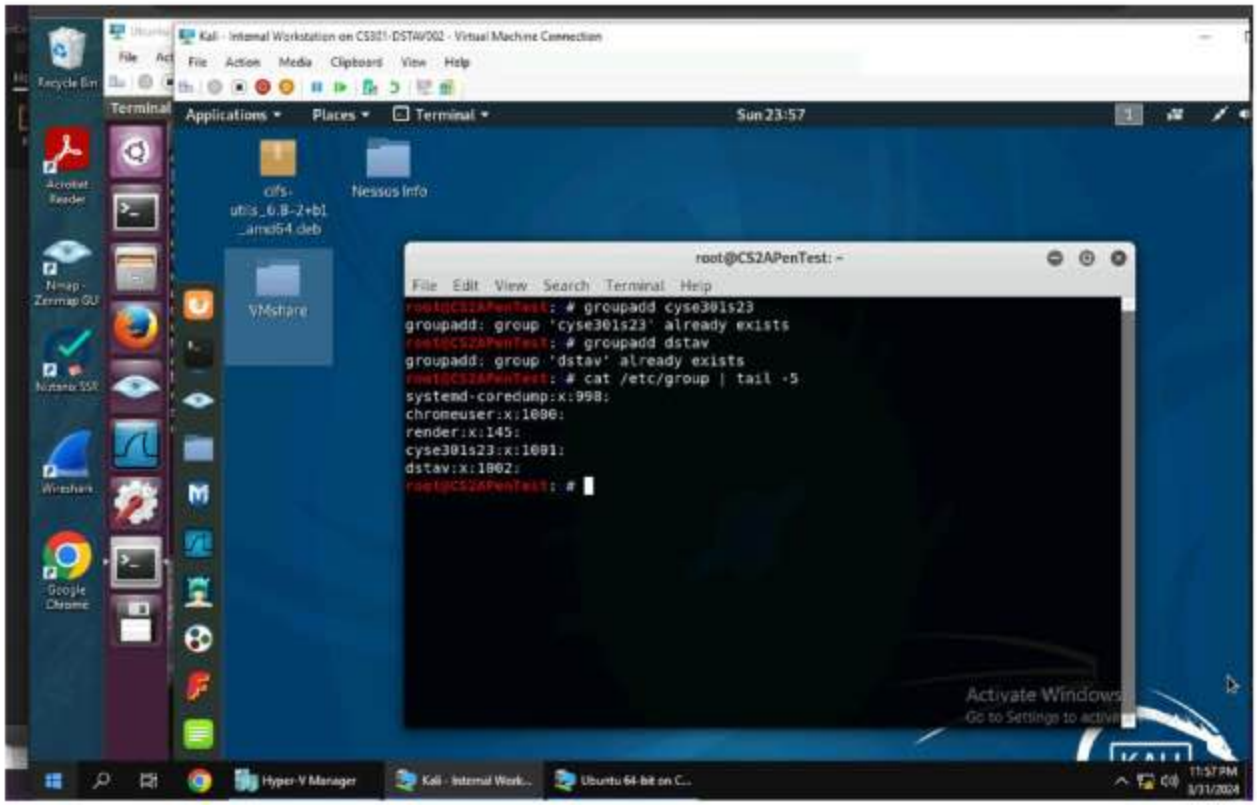
Assignment #5 Password Cracking

Donte Staves

01171770

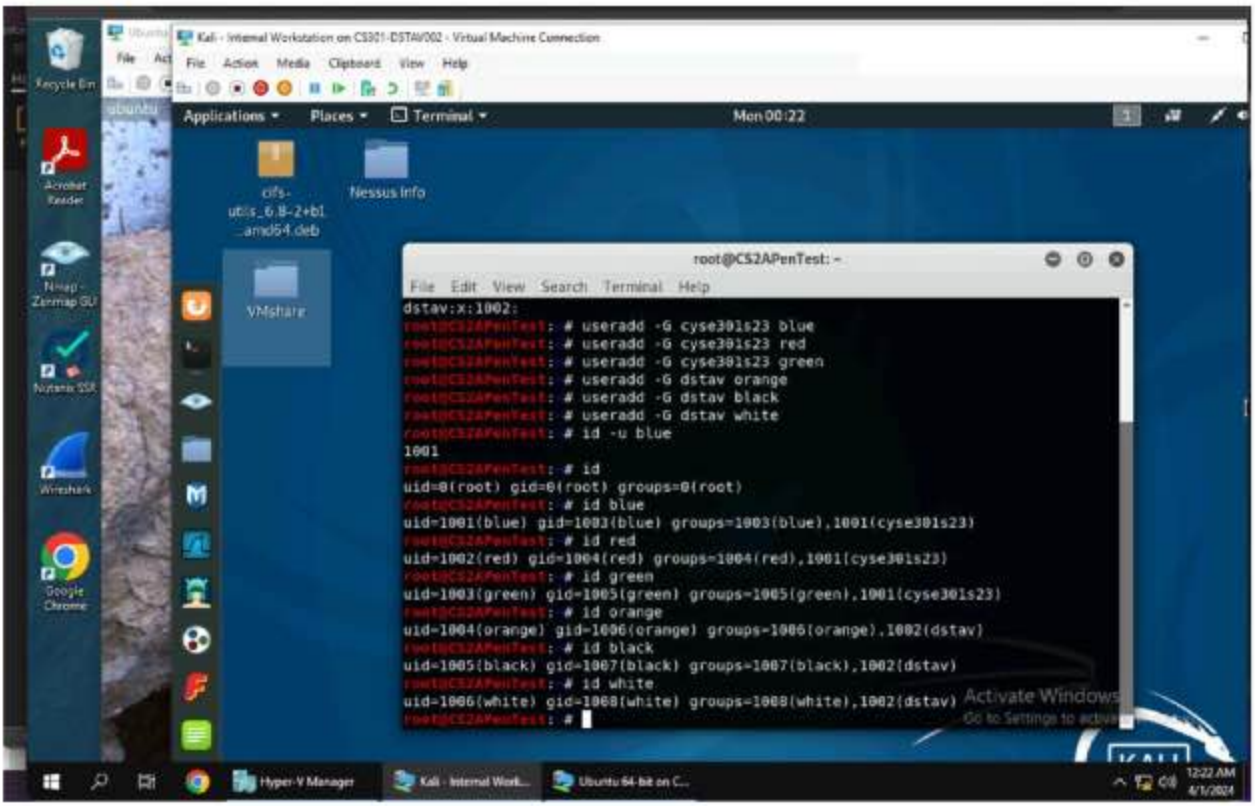
TASK A

1. Create two groups, one is cyse301s23, and the other is your ODU Midas ID (for example,
pjiang). Then display the corresponding group IDs.

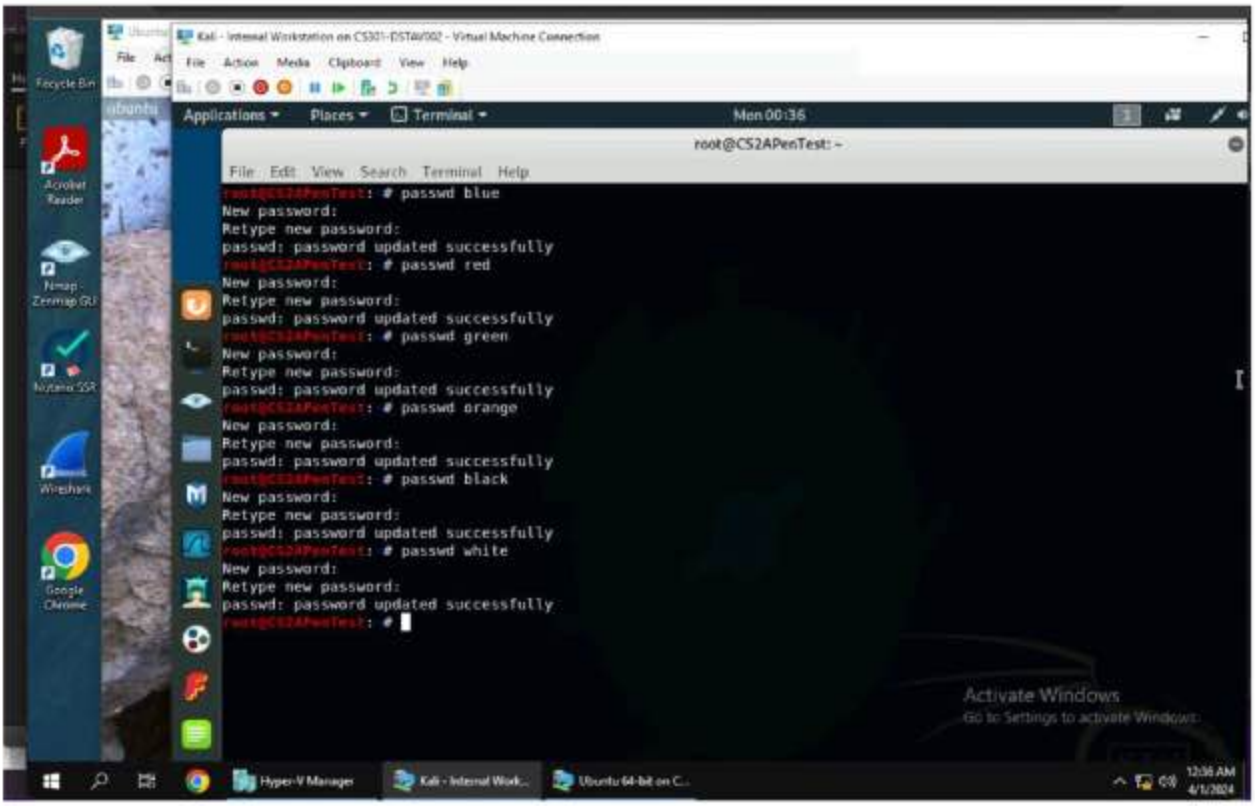


In this screenshot I used the “groupadd” command followed by “cyse301s23” and “dstav” to create groups. I then used the command “cat /etc/groups | tail -5” to display the group IDs.

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



3. 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.



blue – sky

red – car1

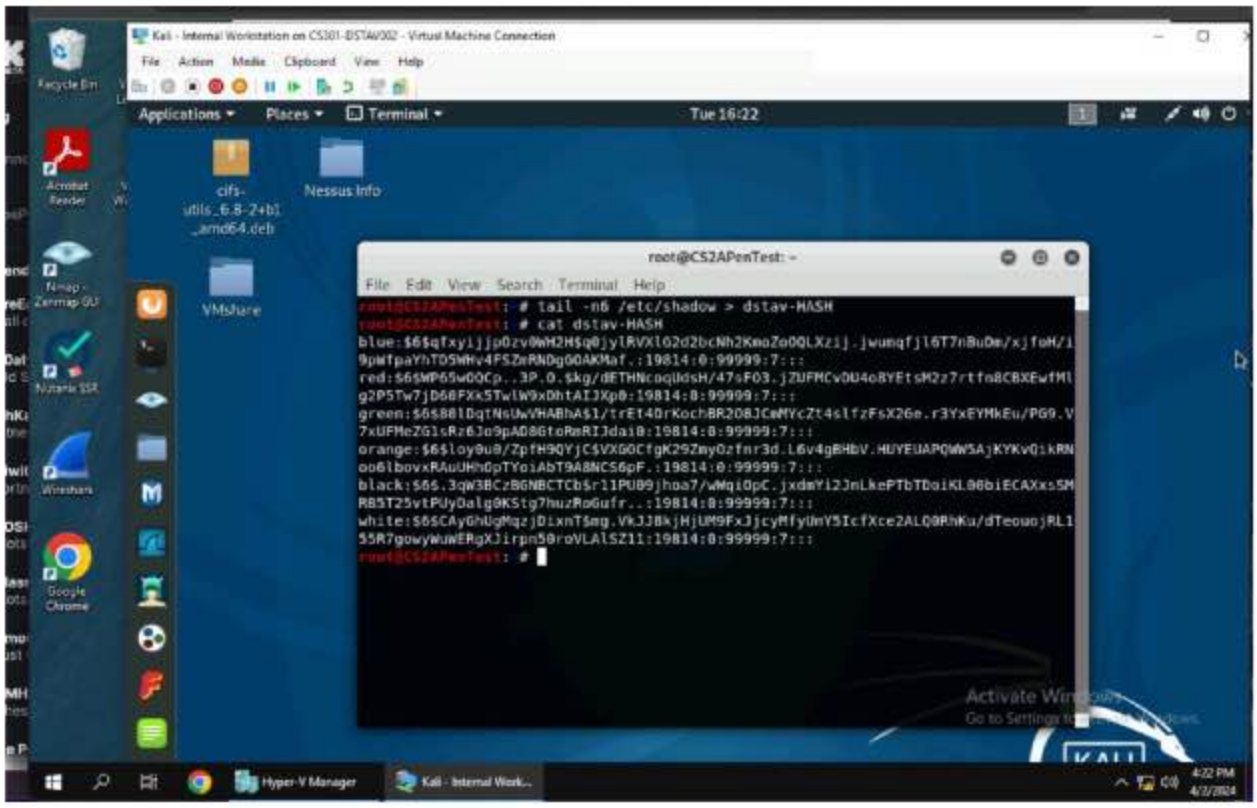
green – Grass10

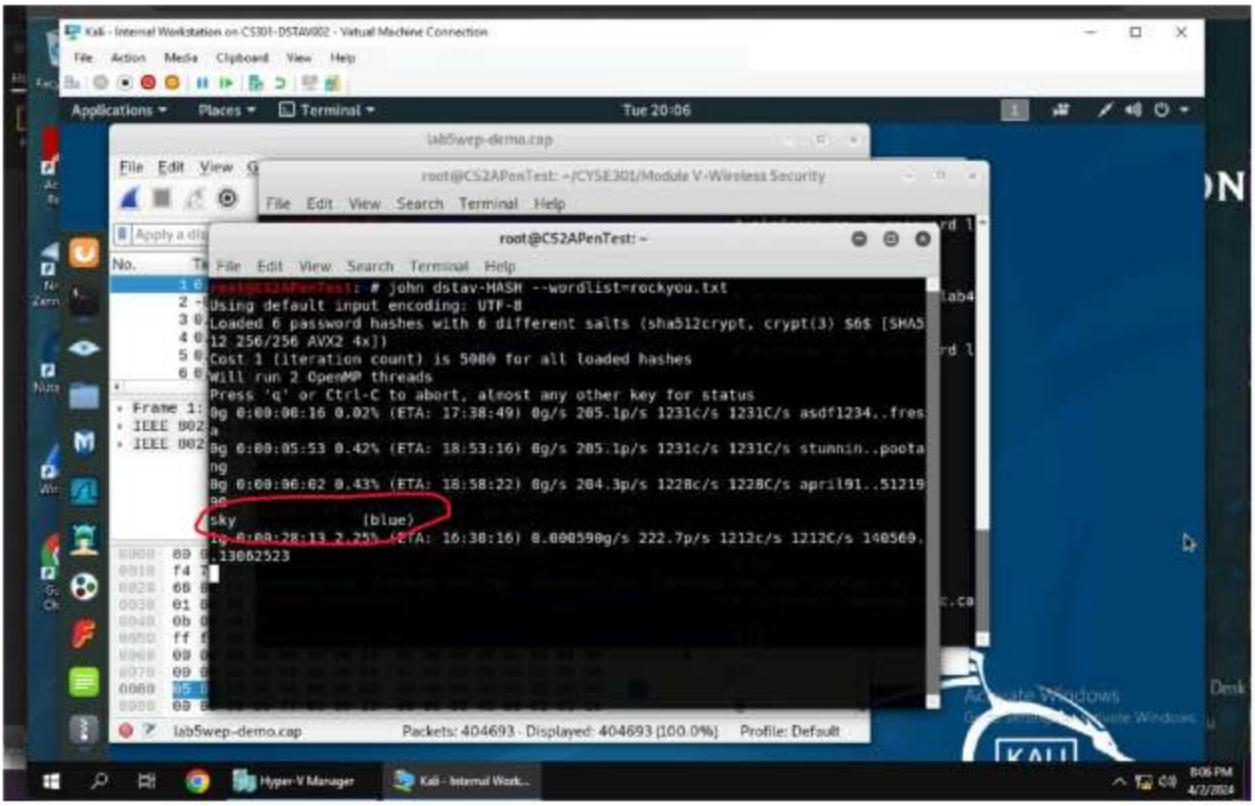
orange – Football11

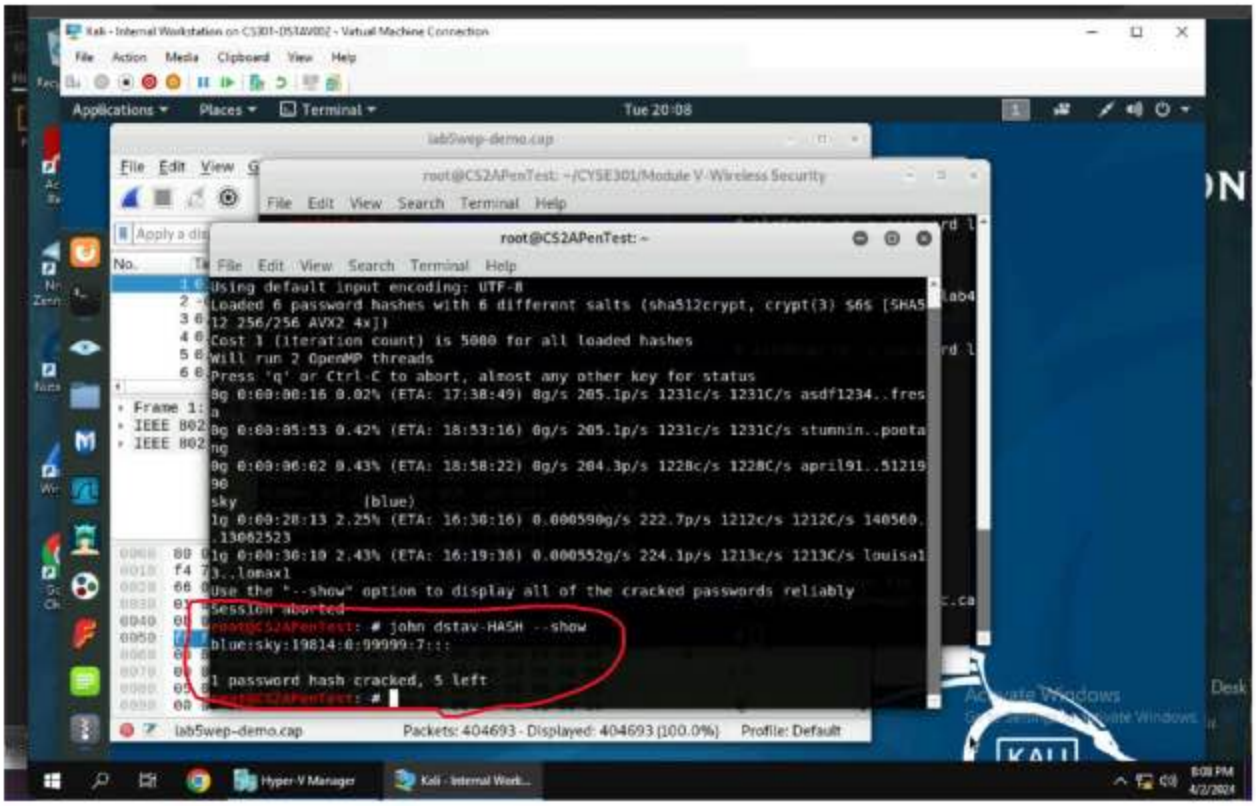
black – Baseball$12

white – BasketBall$%13

4. 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.

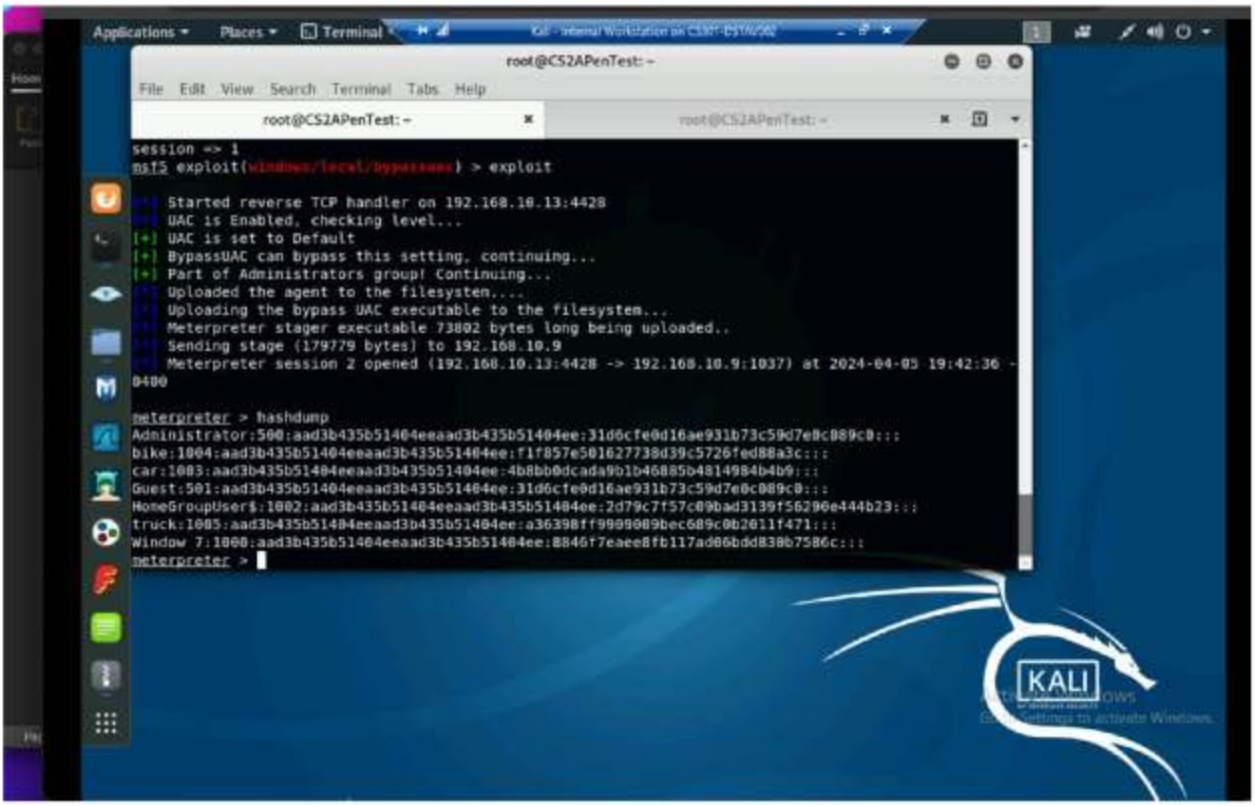



root@CS2APenTest: ~
root@CS2APenTest: # john dstav-HASH --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) 6 [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:16 0.02% (ETA: 17:38:49) 0g/s 205.1p/s 1231c/s 1231C/s asdf1234..fres
a
0g 0:00:05:53 0.42% (ETA: 18:53:16) 0g/s 205.1p/s 1231c/s 1231C/s stunnin..poota
ng
0g 0:00:06:62 0.43% (ETA: 18:58:22) 0g/s 204.3p/s 1228c/s 1228C/s april91..51219
90
sky (blue)
1g 0:00:28:13 2.25% (ETA: 16:38:16) 0.000590g/s 222.7p/s 1212c/s 1212C/s 140560.
.13062523
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default

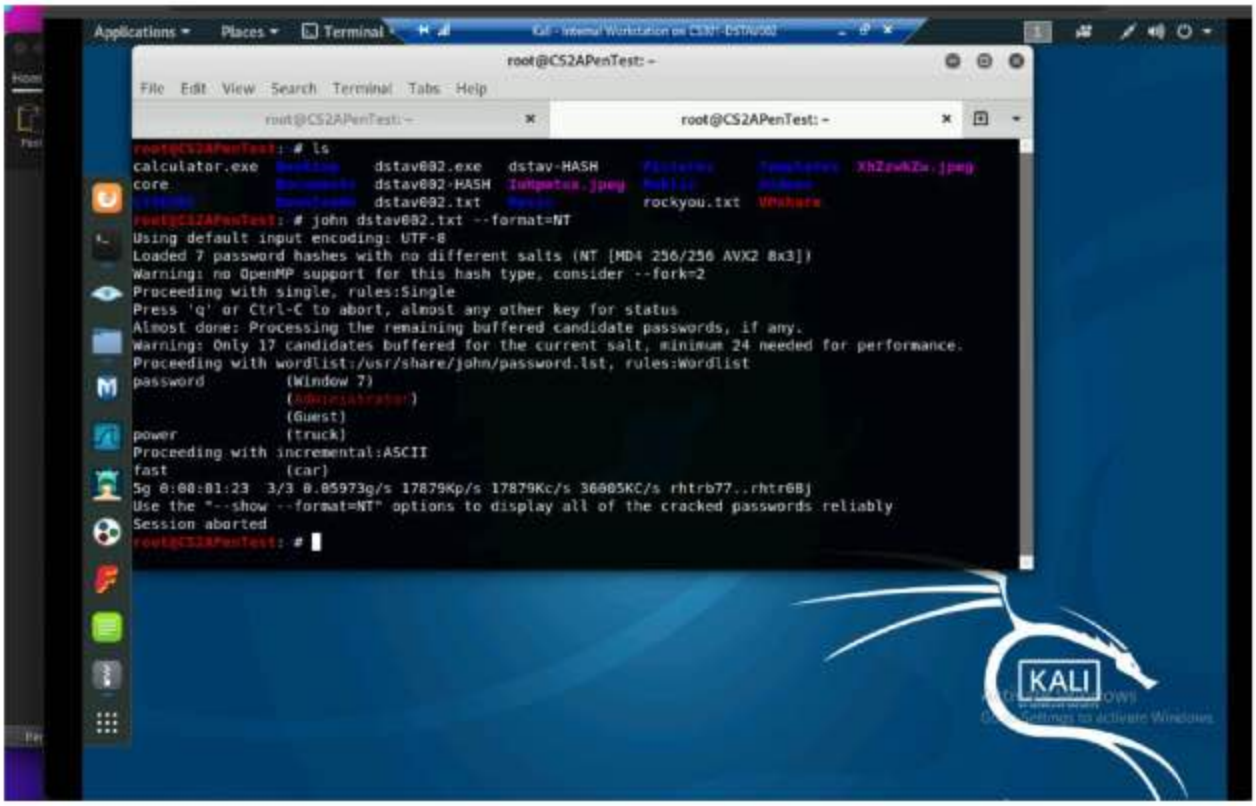

root@CS2APenTest: ~
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) 6 [SHA5
12 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:16 0.02% (ETA: 17:38:49) 0g/s 205.1p/s 1231c/s 1231C/s asdf1234..fres
a
0g 0:00:05:53 0.42% (ETA: 18:53:16) 0g/s 205.1p/s 1231c/s 1231C/s stunnin..poota
ng
0g 0:00:06:62 0.43% (ETA: 18:58:22) 0g/s 204.3p/s 1228c/s 1228C/s april91..51219
90
sky (blue)
1g 0:00:28:13 2.25% (ETA: 16:38:16) 0.000590g/s 222.7p/s 1212c/s 1212C/s 140560.
.13062523
1g 0:00:36:10 2.43% (ETA: 16:19:38) 0.000552g/s 224.1p/s 1213c/s 1213C/s louisal
3..lonaxl
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest: # john dstav-HASH --show
blue:sky:19814:0:99999:7:::
1 password hash cracked, 5 left
root@CS2APenTest: #
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default

Task B

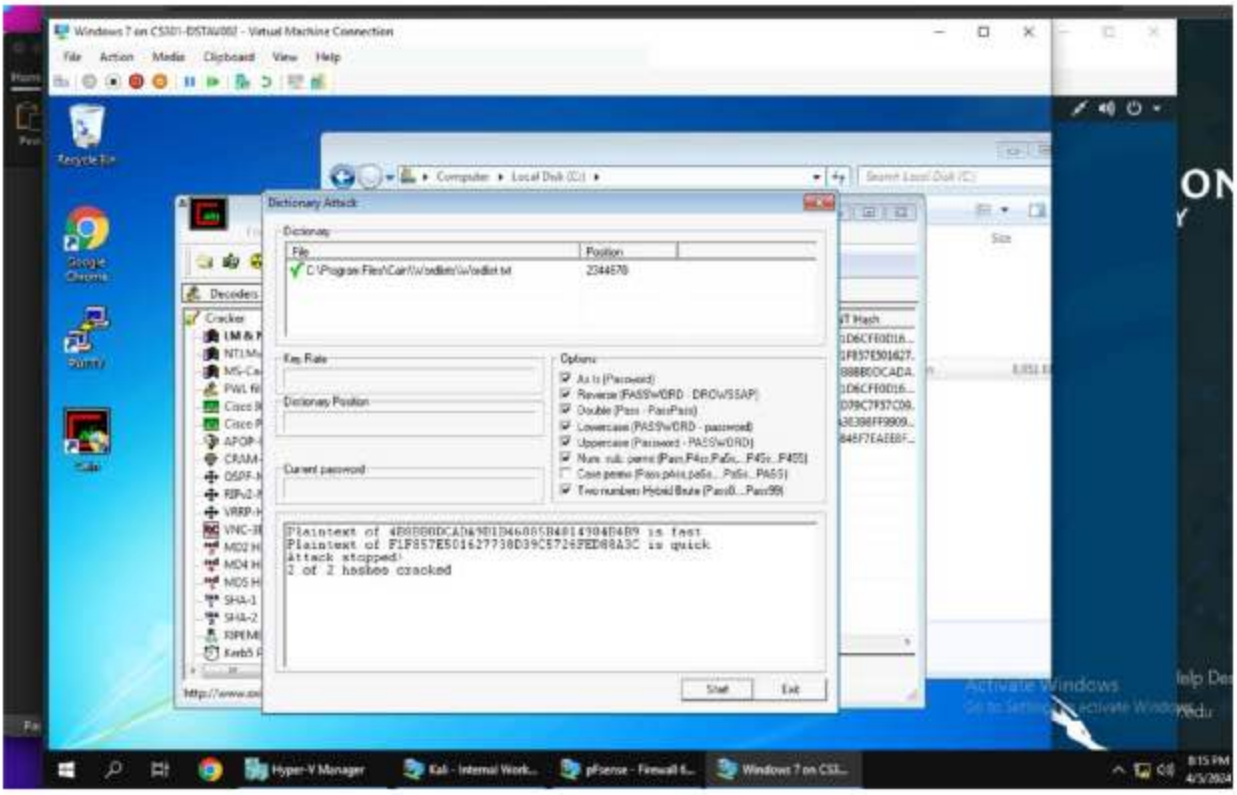
1. 5 points. Display the password hashes by using the “hashdump” command in the meterpreter
   shell. Then



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.).



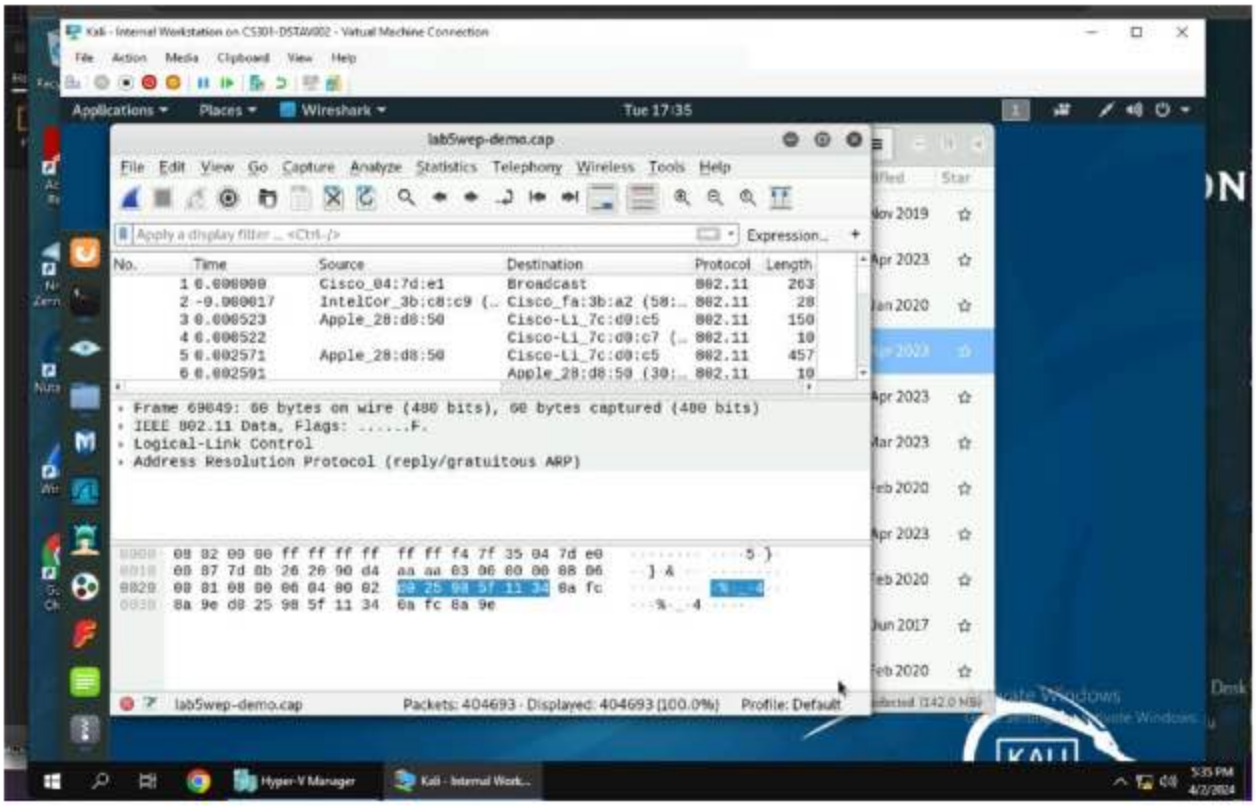
3. 10 points. Upload the password cracking tool, Cain and Abel, to the remote Windows 7 VM, and
install it via a remote desktop window. Then, implement BOTH brute force and dictionary
attacks to crack the passwords. (You MUST crack at least one password in order to complete this
assignment.)

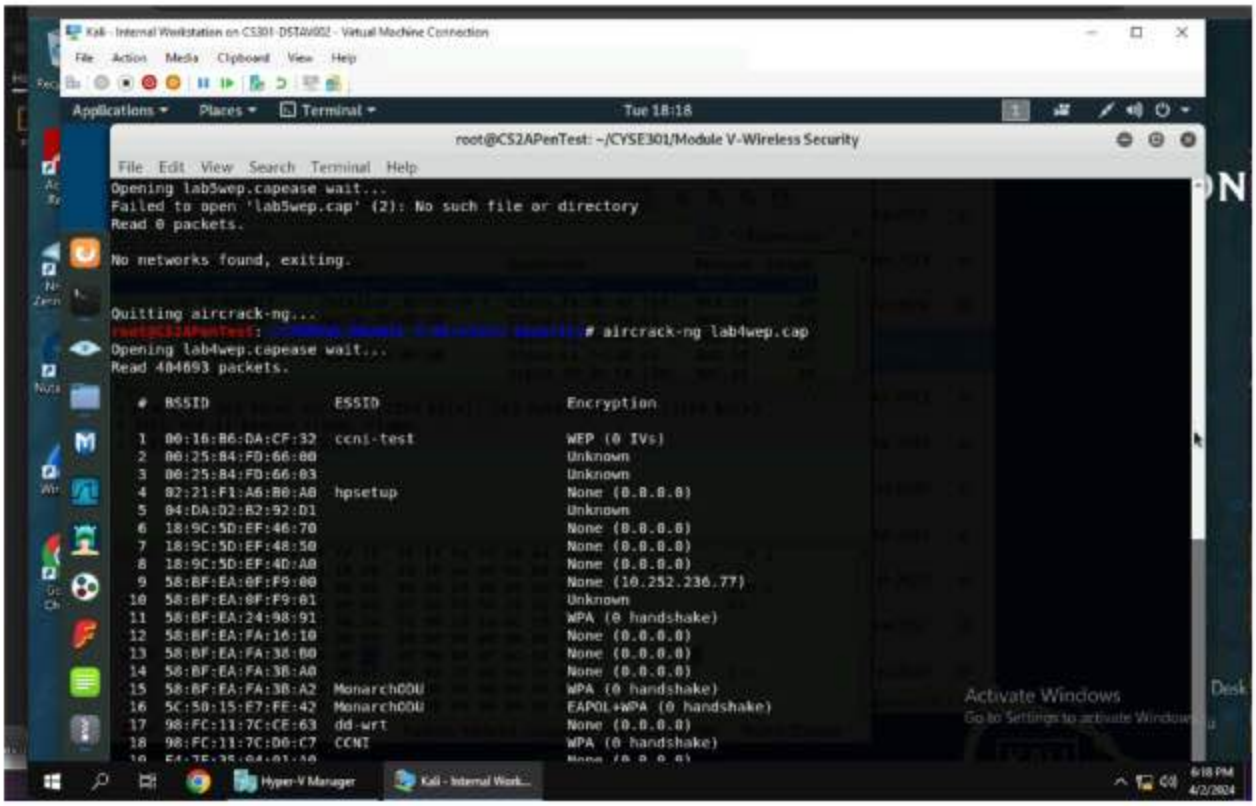


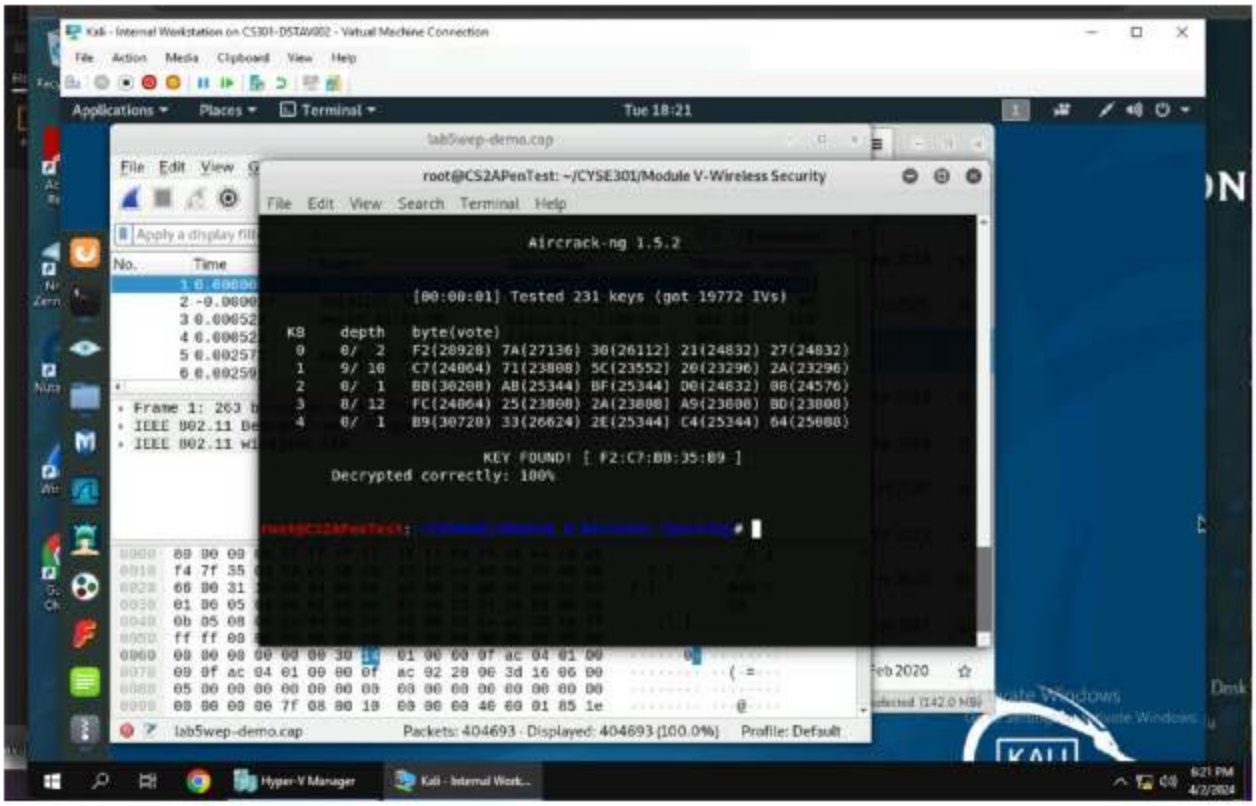
Part B

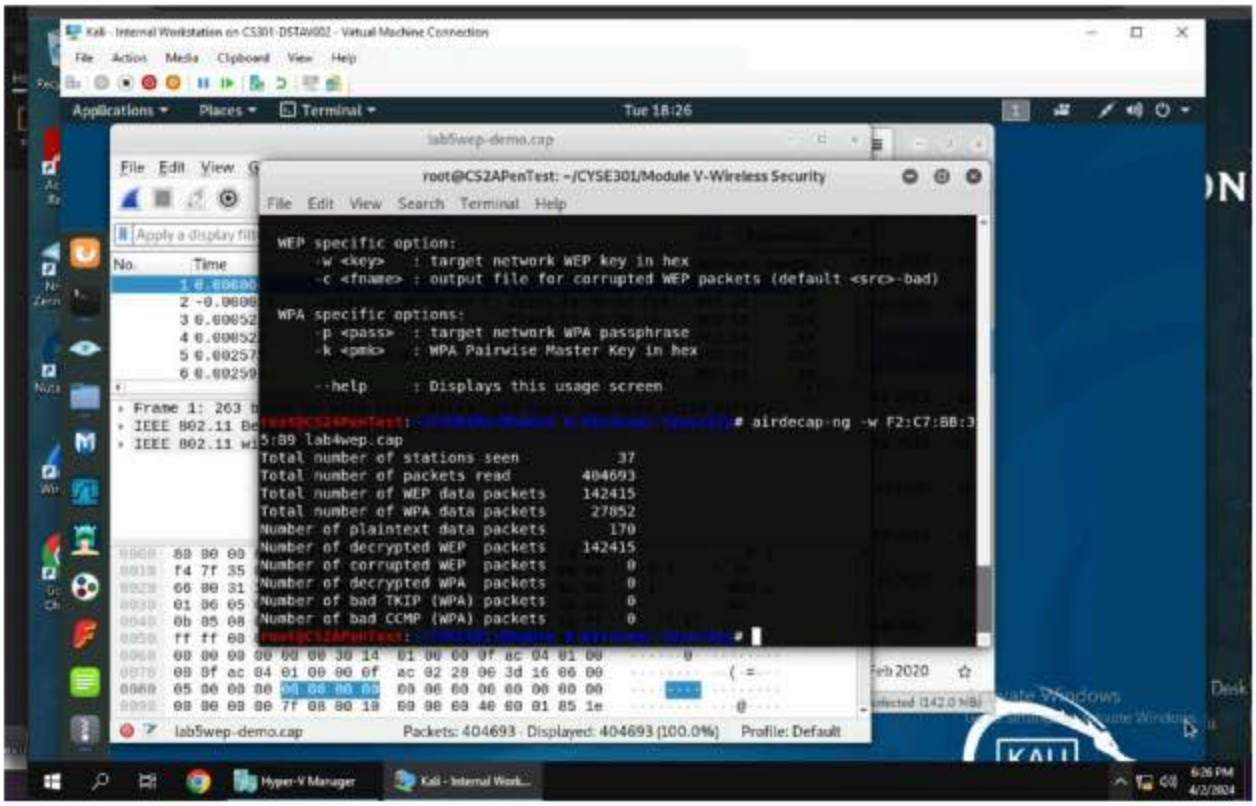
Task C

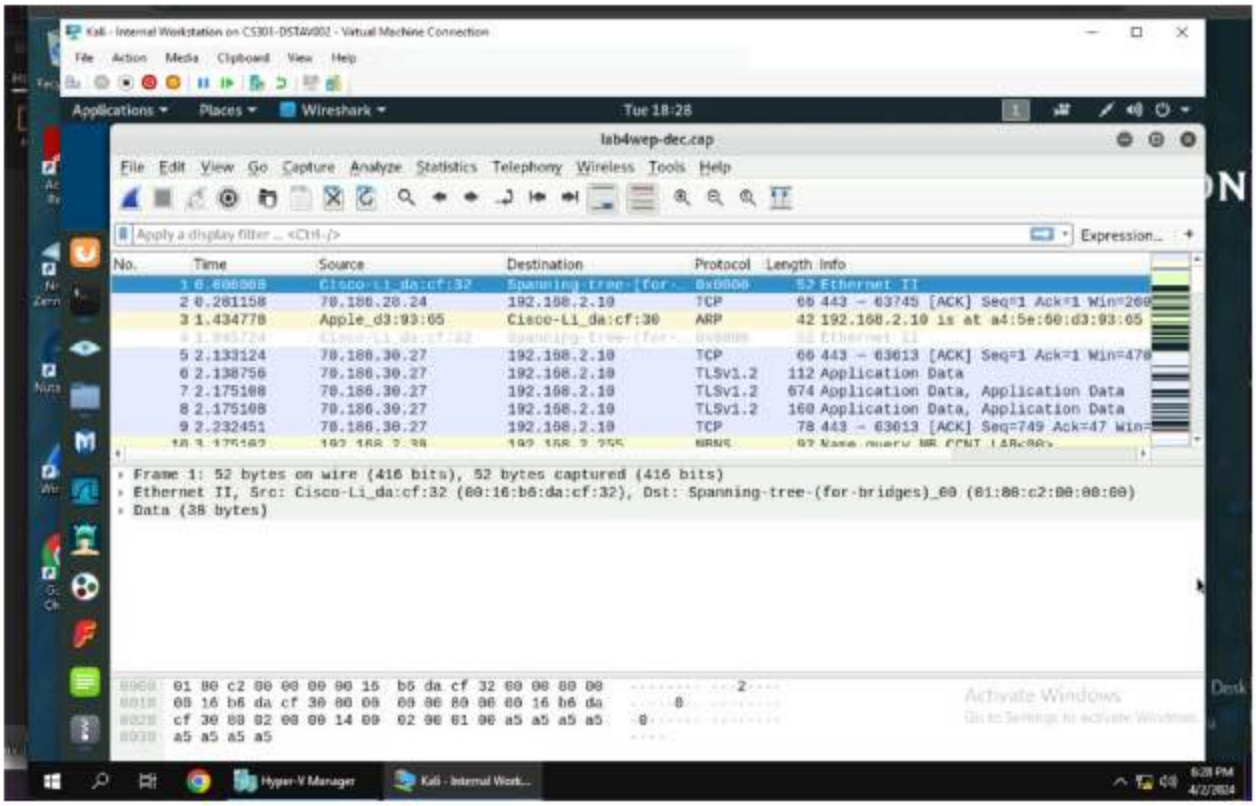
1. Decrypt the lab4wep. cap file (5 points) and perform a detailed traffic analysis (5 points)

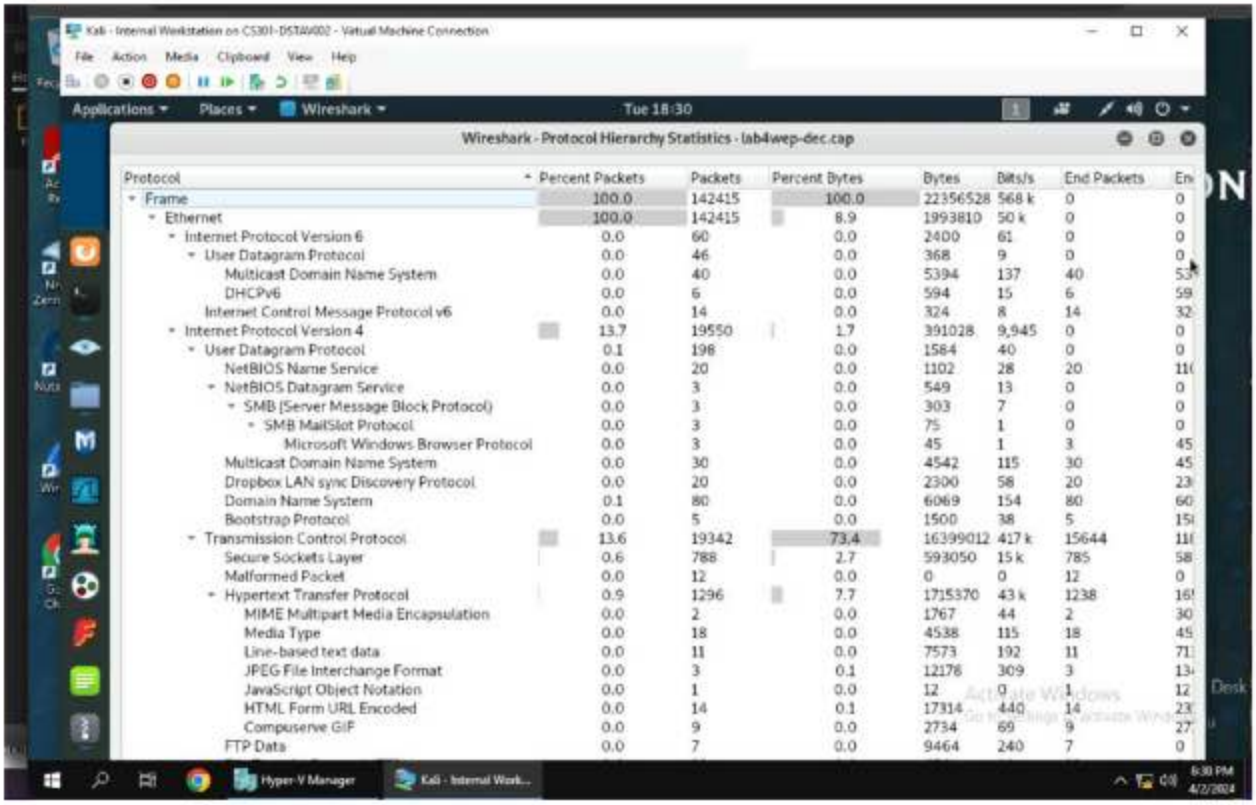

Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Tue 17:35
lab5wep-demo.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length
1 0.000000 Cisco_04:7d:e1 Broadcast 802.11 263
2 -9.000017 IntelCor_3b:c8:c9 (... Cisco_fa:3b:a2 (58:... 802.11 28
3 0.000523 Apple_28:d8:50 Cisco-Li_7c:d0:c5 802.11 150
4 0.000522 Cisco-Li_7c:d0:c7 (... 802.11 10
5 0.002571 Apple_28:d8:50 Cisco-Li_7c:d0:c5 802.11 457
6 0.002591 Apple_28:d8:50 (30:... 802.11 10
Frame 60649: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.11 Data, Flags: .....F.
Logical-Link Control
Address Resolution Protocol (reply/gratuitous ARP)
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default
Hyper-V Manager
Kali - Internal Work...
5:35 PM
4/2/2024


Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 18:18
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Opening lab5wep.capease wait...
Failed to open 'lab5wep.cap' (2): No such file or directory
Read 0 packets.
No networks found, exiting.
Quitting aircrack-ng...
aircrack-ng lab4wep.cap
Opening lab4wep.capease wait...
Read 404693 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:32 ccni-test WEP (0 IVs)
2 00:25:84:FD:66:00 Unknown
3 00:25:84:FD:66:03 Unknown
4 02:21:F1:A6:B0:A8 hpsetup None (0.0.0.0)
5 04:DA:D2:B2:92:D1 Unknown
6 18:9C:5D:EF:46:70 None (0.0.0.0)
7 18:9C:5D:EF:48:50 None (0.0.0.0)
8 18:9C:5D:EF:4D:A0 None (0.0.0.0)
9 58:BF:EA:0F:F9:00 None (10.252.236.77)
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 None (0.0.0.0)
13 58:BF:EA:FA:38:00 None (0.0.0.0)
14 58:BF:EA:FA:38:A0 None (0.0.0.0)
15 58:BF:EA:FA:38:A2 MonarchODU WPA (0 handshake)
16 5C:50:15:E7:FE:42 MonarchODU EAPOL+WPA (0 handshake)
17 98:FC:11:7C:CE:63 dd-wrt None (0.0.0.0)
18 98:FC:11:7C:D0:C7 CCNI WPA (0 handshake)
Activate Windows
Hyper-V Manager
Kali - Internal Work...
6:18 PM
4/2/2024

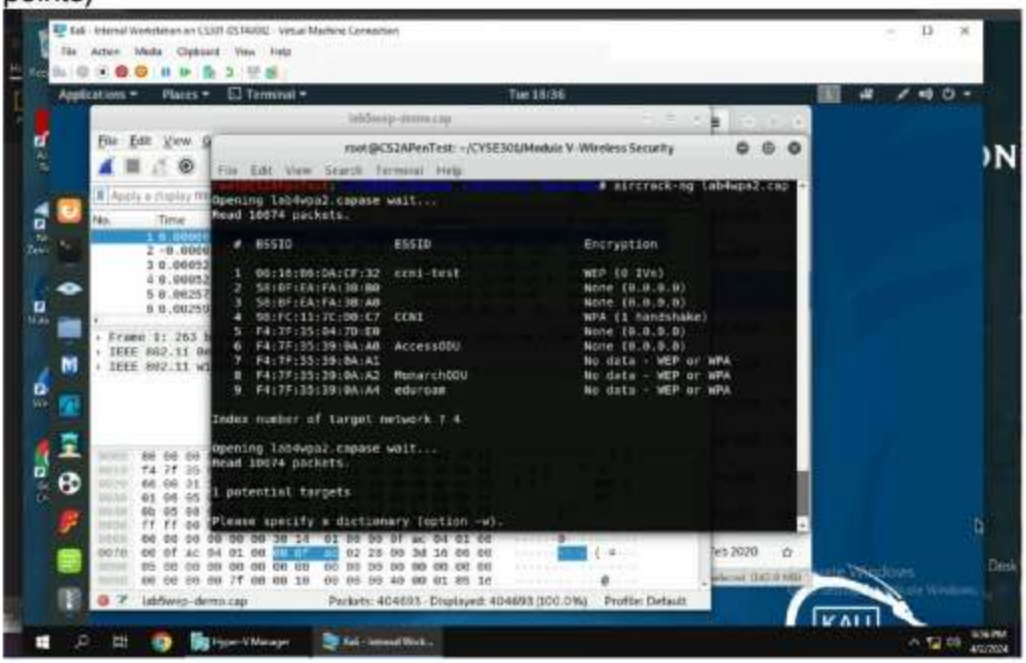

Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 18:21
lab5wep-demo.cap
File Edit View
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
[00:00:01] 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(24632) 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%
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default
Hyper-V Manager
Kali - Internal Work...
6:21 PM
4/2/2024

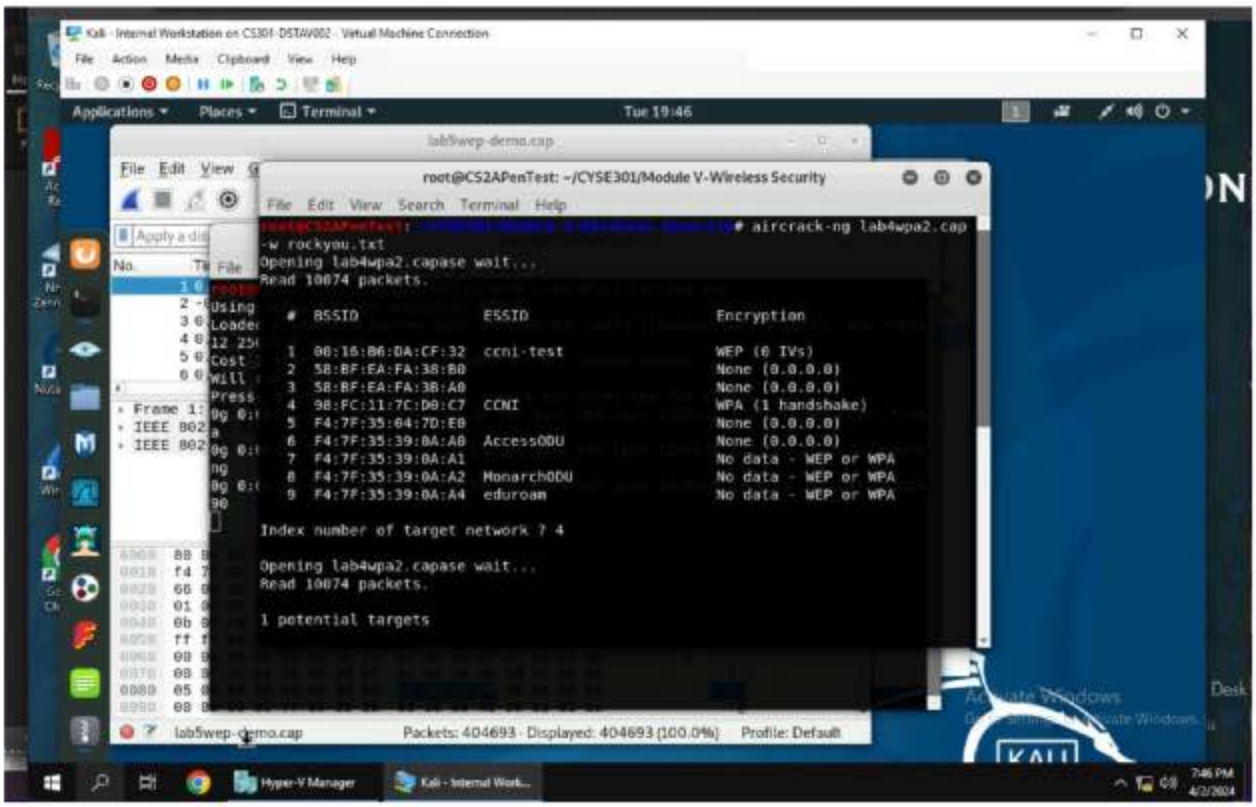

Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 18:26
lab5wep-demo.cap
File Edit View
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
WEP specific option:
-w <key> : target network WEP key in hex
-c <fname> : output file for corrupted WEP packets (default <src>-bad)
WPA specific options:
-p <pass> : target network WPA passphrase
-k <pmk> : WPA Pairwise Master Key in hex
--help : Displays this usage screen
airdecap-ng -w F2:C7:BB:35:B9 lab4wep.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
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default
Hyper-V Manager
Kali - Internal Work...
6:26 PM
4/2/2024

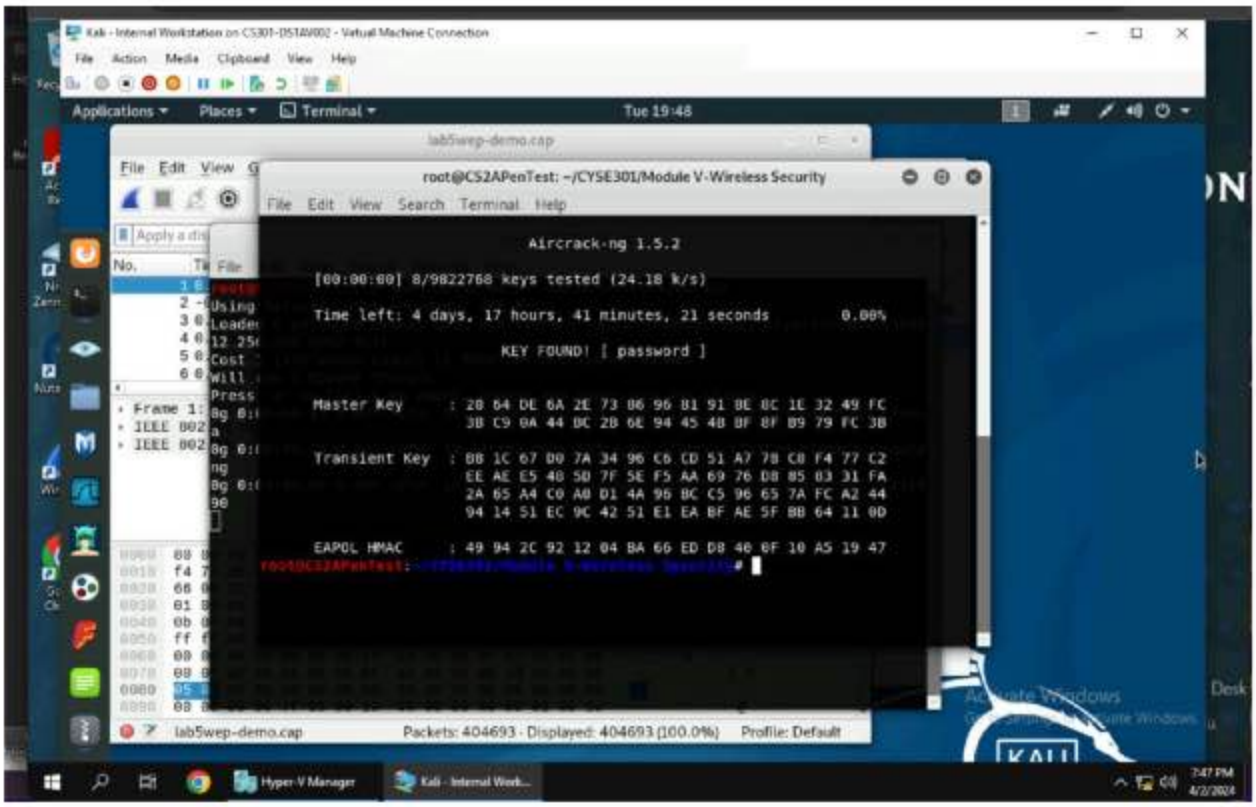

Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Tue 18:28
lab4wep-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 Cisco-Li_da:cf:32 Spanning-tree-(for-... 0x0000 52 Ethernet II
2 0.281158 70.186.28.24 192.168.2.10 TCP 60 443 → 63745 [ACK] Seq=1 Ack=1 Win=260
3 1.434778 Apple_d3:93:65 Cisco-Li_da:cf:30 ARP 42 192.168.2.10 is at a4:5e:60:d3:93:65
5 2.133124 70.186.30.27 192.168.2.10 TCP 60 443 → 63613 [ACK] Seq=1 Ack=1 Win=470
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=
Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
Ethernet II, Src: Cisco-Li_da:cf:32 (60:16:b6:da:cf:32), Dst: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
Data (38 bytes)
0000 01 80 c2 00 00 00 00 15 b5 da cf 32 00 08 00 00
0010 08 16 b6 da cf 30 00 00 00 00 00 16 b6 da
0020 cf 30 00 02 00 00 14 00 02 00 01 00 a5 a5 a5 a5
0030 a5 a5 a5 a5
Activate Windows
Hyper-V Manager
Kali - Internal Work...
6:28 PM
4/2/2024

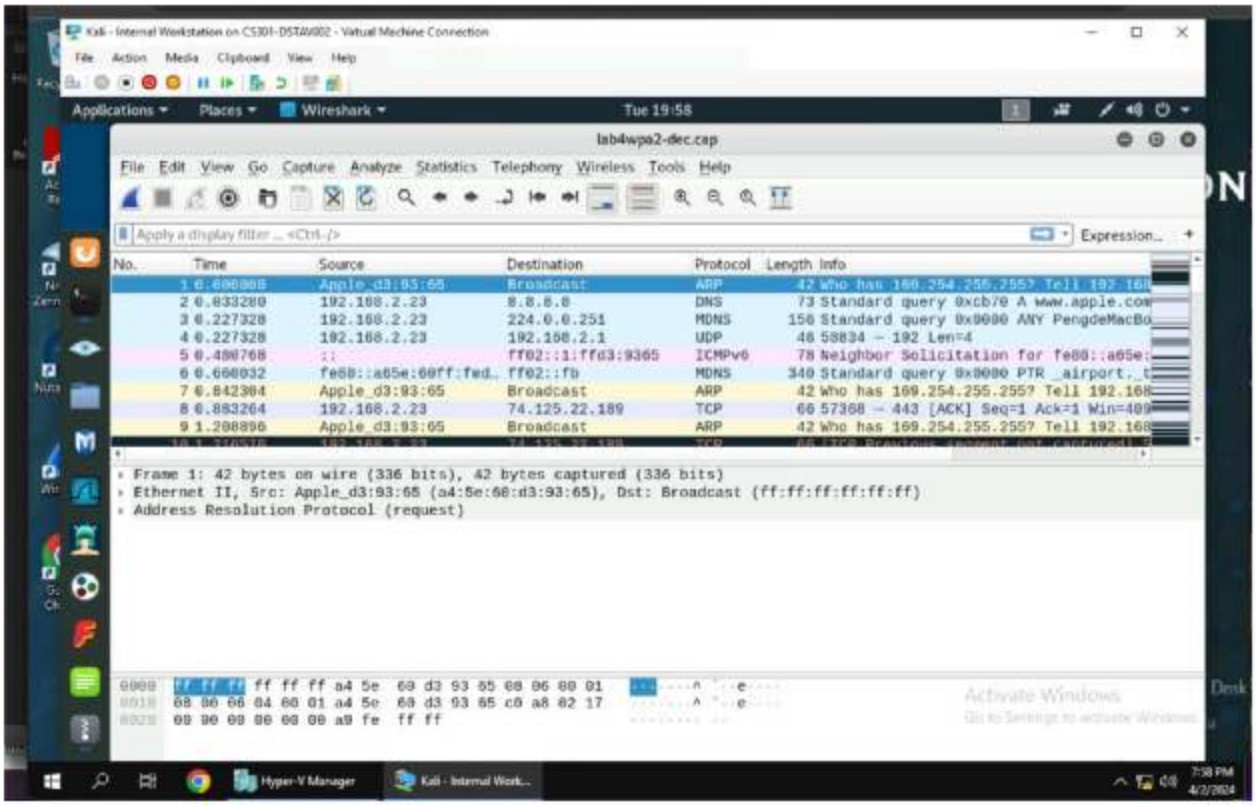

Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Tue 18:30
Wireshark · Protocol Hierarchy Statistics · lab4wep-dec.cap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets
Frame 100.0 142415 100.0 22356528 568 k 0
Ethernet 100.0 142415 8.9 1993810 50 k 0
Internet Protocol Version 6 0.0 60 0.0 2400 61 0
User Datagram Protocol 0.0 46 0.0 368 9 0
Multicast Domain Name System 0.0 40 0.0 5394 137 40
DHCPv6 0.0 6 0.0 594 15 6
Internet Control Message Protocol v6 0.0 14 0.0 324 8 14
Internet Protocol Version 4 13.7 19550 1.7 391028 9,945 0
User Datagram Protocol 0.1 198 0.0 1584 40 0
NetBIOS Name Service 0.0 20 0.0 1102 28 20
NetBIOS Datagram Service 0.0 3 0.0 549 13 0
SMB (Server Message Block Protocol) 0.0 3 0.0 303 7 0
SMB MailSlot Protocol 0.0 3 0.0 75 1 0
Microsoft Windows Browser Protocol 0.0 3 0.0 45 1 3
Multicast Domain Name System 0.0 30 0.0 4542 115 30
Dropbox LAN sync Discovery Protocol 0.0 20 0.0 2300 58 20
Domain Name System 0.1 80 0.0 6069 154 80
Bootstrap Protocol 0.0 5 0.0 1500 38 5
Transmission Control Protocol 13.6 19342 73.4 16399012 417 k 15644
Secure Sockets Layer 0.6 788 2.7 593050 15 k 785
Malformed Packet 0.0 12 0.0 0 0 12
Hypertext Transfer Protocol 0.9 1296 7.7 1715370 43 k 1238
MIME Multipart Media Encapsulation 0.0 2 0.0 1767 44 2
Media Type 0.0 18 0.0 4538 115 18
Line-based text data 0.0 11 0.0 7573 192 11
JPEG File Interchange Format 0.0 3 0.1 12178 309 3
JavaScript Object Notation 0.0 1 0.0 12 0 1
HTML Form URL Encoded 0.0 14 0.1 17314 440 14
Compuserve GIF 0.0 9 0.0 2734 69 9
FTP Data 0.0 7 0.0 9464 240 7
Activate Windows
Hyper-V Manager
Kali - Internal Work...
6:30 PM
4/2/2024

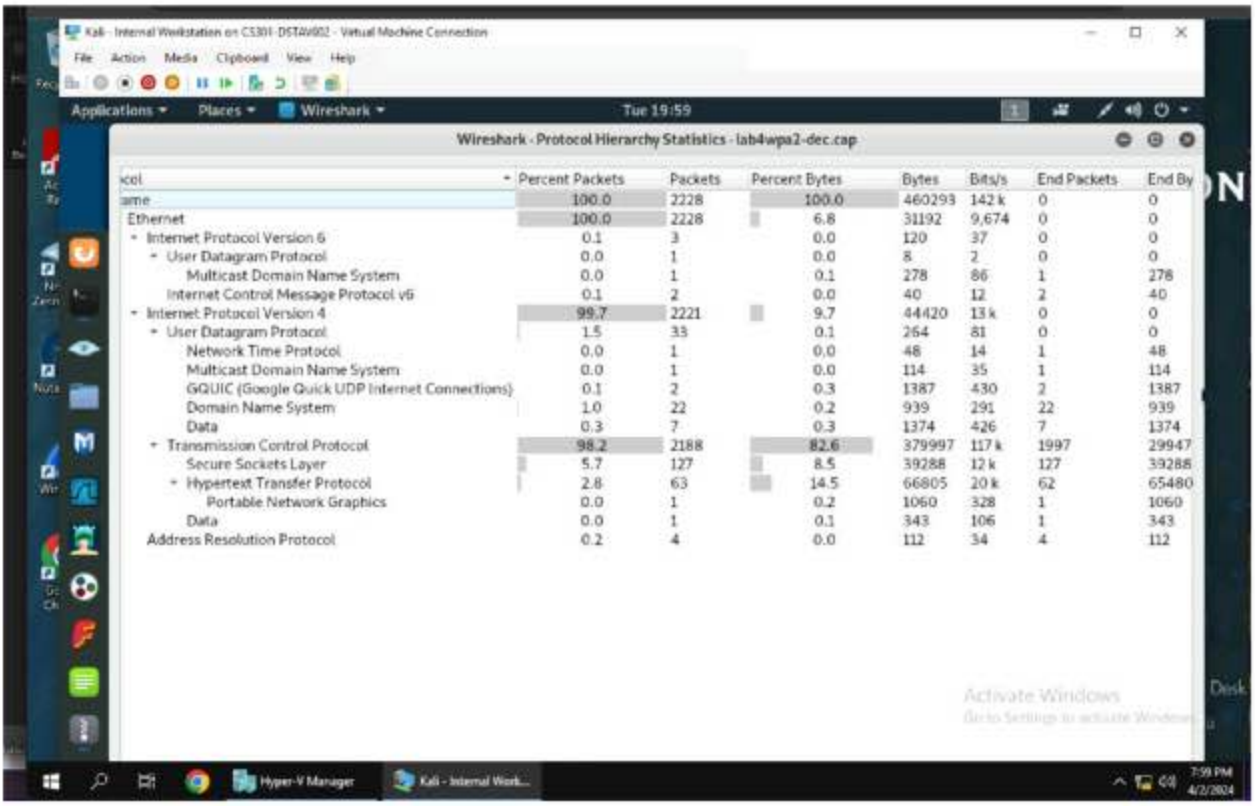
2. Decrypt the lab4wpa2. cap file (5 points) and perform a detailed traffic analysis (5 points)






Kali - Internal Workstation on CS301-DSTAW002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Tue 19:48
lab5wep-demo.cap
File Edit View Search Terminal Help
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
Aircrack-ng 1.5.2
[00:00:00] 8/9822768 keys tested (24.18 k/s)
Time left: 4 days, 17 hours, 41 minutes, 21 seconds 0.00%
KEY FOUND! [password]
Master Key : 20 64 DE 6A 2E 73 06 96 81 91 0E 8C 1C 32 49 FC
3B C9 0A 44 0C 2B 6E 94 45 40 0F 0F 09 79 FC 3B
Transient Key : 80 1C 67 D0 7A 34 96 C6 CD 51 A7 78 C0 F4 77 C2
EE AE E5 40 5D 7F 5E F5 AA 69 76 D8 85 03 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 BB 64 11 0D
EAPOL HMAC : 49 94 2C 92 12 04 BA 66 ED D8 40 0F 10 A5 19 47
lab5wep-demo.cap
Packets: 404693 · Displayed: 404693 (100.0%)
Profile: Default
Hyper-V Manager
Kali - Internal Work...
7:47 PM
4/2/2024

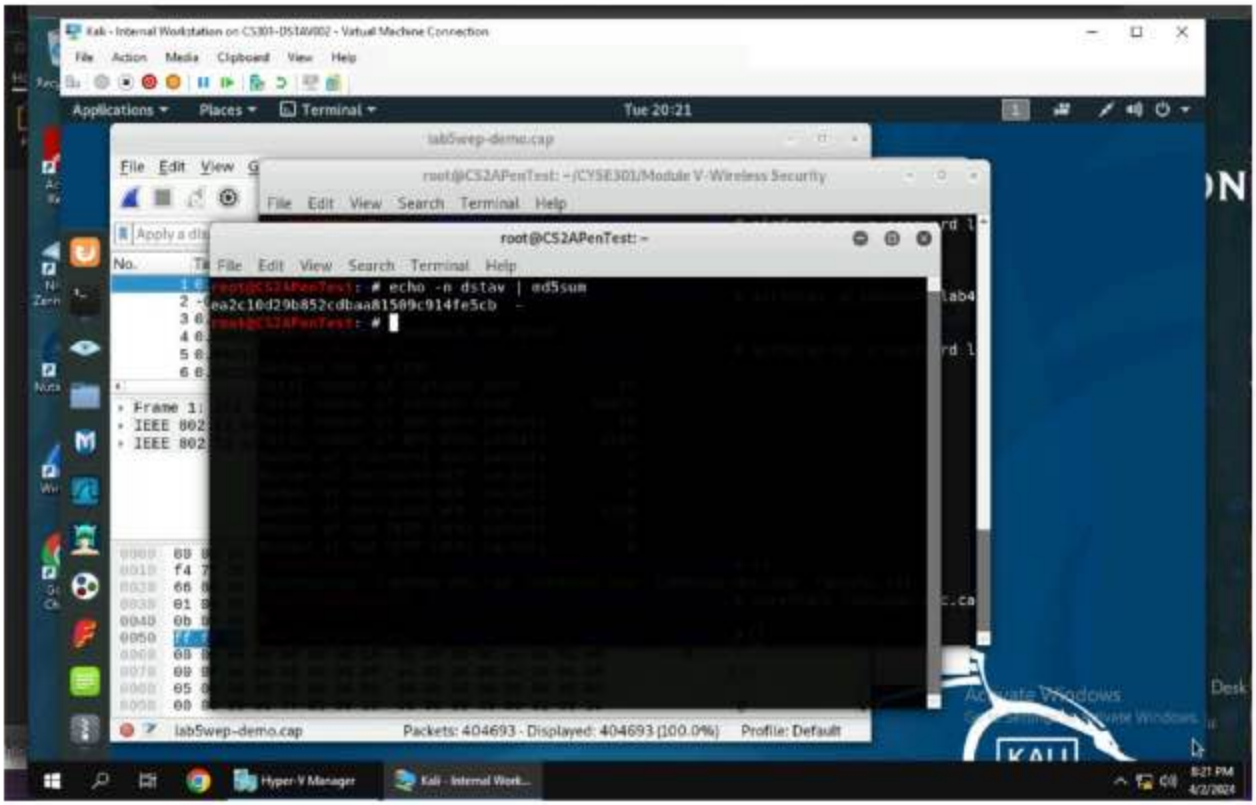

Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Tue 19:58
lab4wpa2-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time 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 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 PengdeMacBo
4 0.227328 192.168.2.23 192.168.2.1 UDP 46 58834 → 192 Len=4
5 0.480768 :: ff02::1:ffd3:9365 ICMPv6 78 Neighbor Solicitation for fe80::a65e:
6 0.660032 fe80::a65e:60ff:fed... ff02::fb MDNS 340 Standard query 0x0000 PTR _airport._t
7 0.842304 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell 192.168
8 0.883264 192.168.2.23 74.125.22.189 TCP 66 57368 → 443 [ACK] Seq=1 Ack=1 Win=409
9 1.208896 Apple_d3:93:65 Broadcast ARP 42 Who has 169.254.255.255? Tell 192.168
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)
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
Activate Windows
Hyper-V Manager
Kali - Internal Work...
7:58 PM
4/2/2024

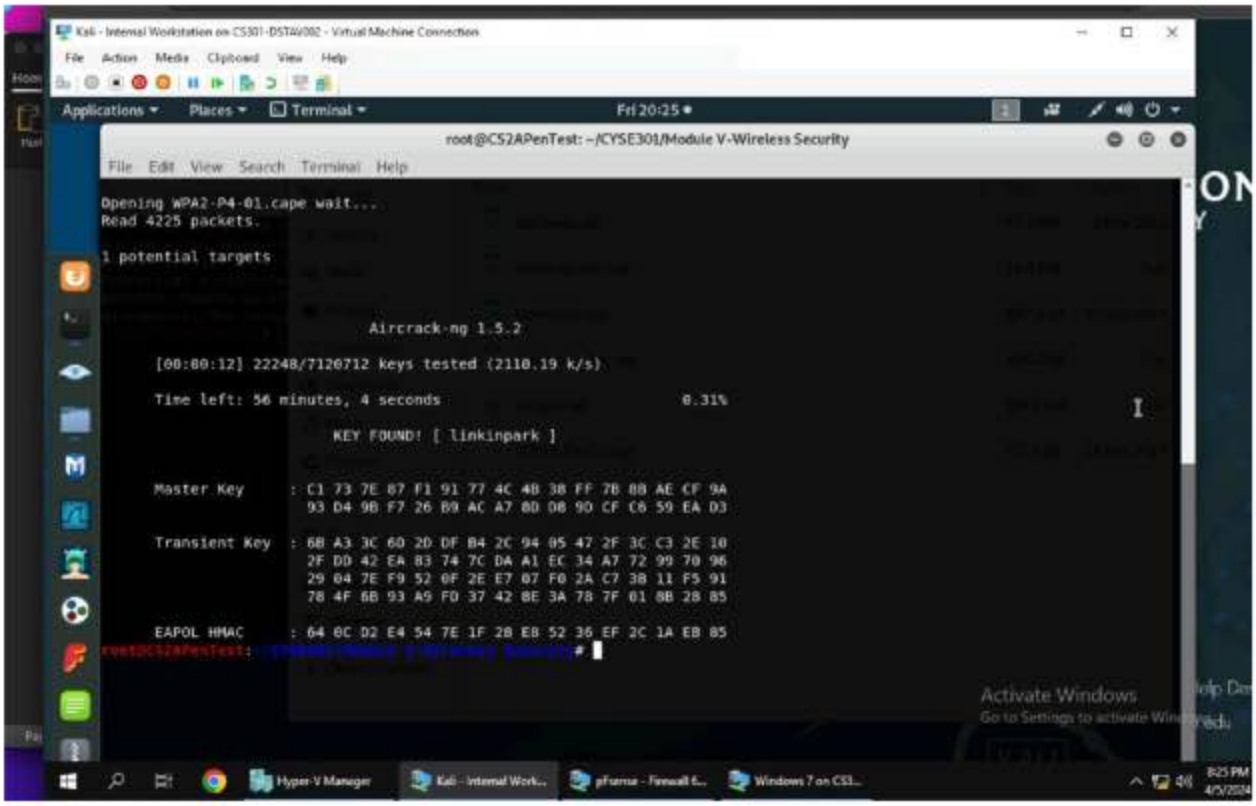

Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Tue 19:59
Wireshark · Protocol Hierarchy Statistics · lab4wpa2-dec.cap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End By
frame 100.0 2228 100.0 460293 142 k 0 0
Ethernet 100.0 2228 6.8 31192 9,674 0 0
Internet Protocol Version 6 0.1 3 0.0 120 37 0 0
User Datagram Protocol 0.0 1 0.0 8 2 0 0
Multicast Domain Name System 0.0 1 0.1 278 86 1 278
Internet Control Message Protocol v6 0.1 2 0.0 40 12 2 40
Internet Protocol Version 4 99.7 2221 9.7 44420 13 k 0 0
User Datagram Protocol 1.5 33 0.1 264 81 0 0
Network Time Protocol 0.0 1 0.0 48 14 1 48
Multicast Domain Name System 0.0 1 0.0 114 35 1 114
GQUIC (Google Quick UDP Internet Connections) 0.1 2 0.3 1387 430 2 1387
Domain Name System 1.0 22 0.2 939 291 22 939
Data 0.3 7 0.3 1374 426 7 1374
Transmission Control Protocol 98.2 2188 82.6 379997 117 k 1997 29947
Secure Sockets Layer 5.7 127 8.5 39288 12 k 127 39288
Hypertext Transfer Protocol 2.8 63 14.5 66805 20 k 62 65480
Portable Network Graphics 0.0 1 0.2 1060 328 1 1060
Data 0.0 1 0.1 343 106 1 343
Address Resolution Protocol 0.2 4 0.0 112 34 4 112
Activate Windows
Hyper-V Manager
Kali - Internal Work...
7:59 PM
4/2/2024

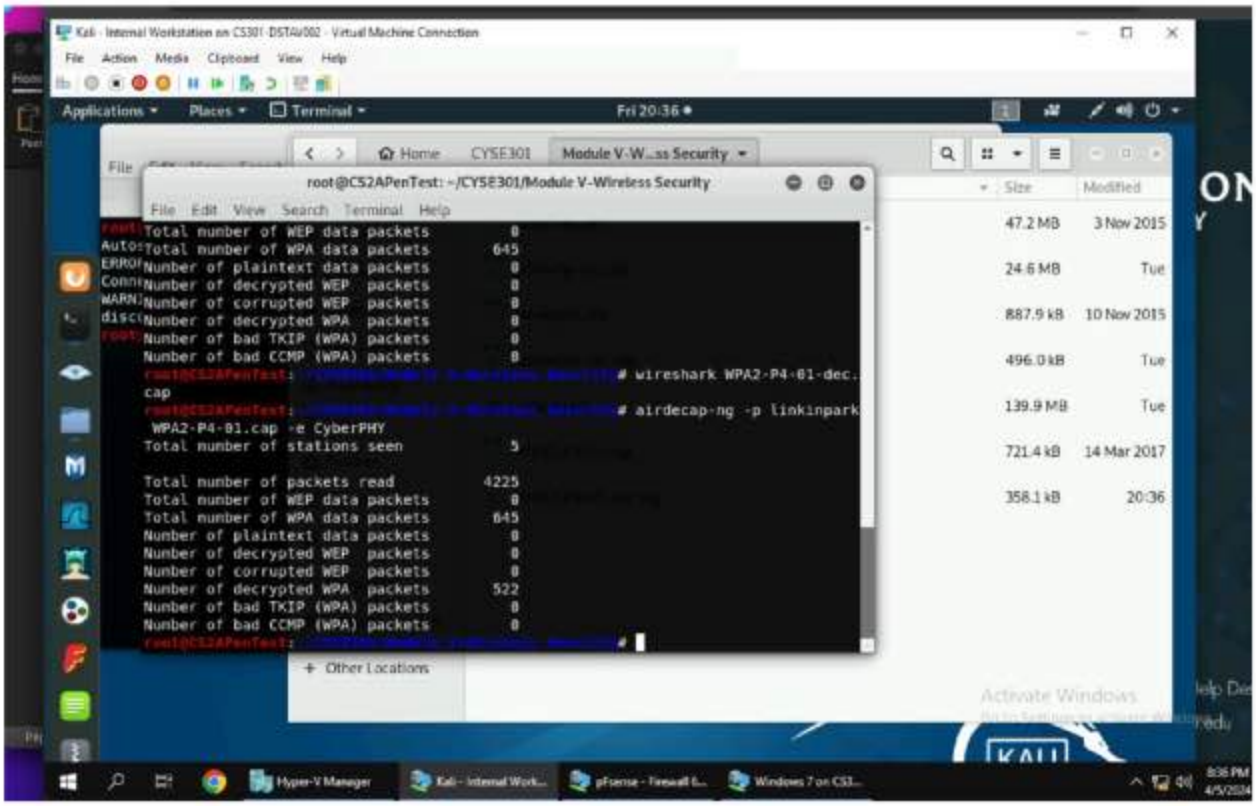
Task D

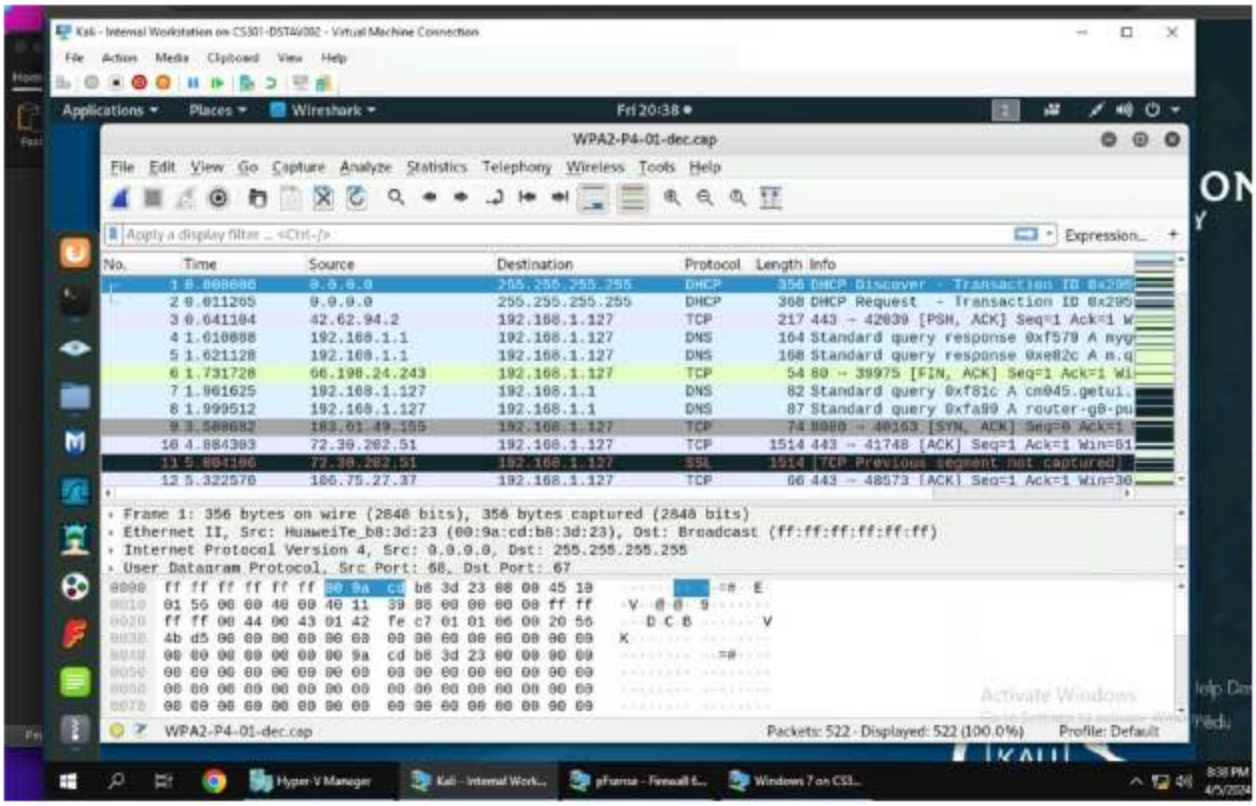
1. Implement a dictionary attack and decrypt the traffic. - 20 points

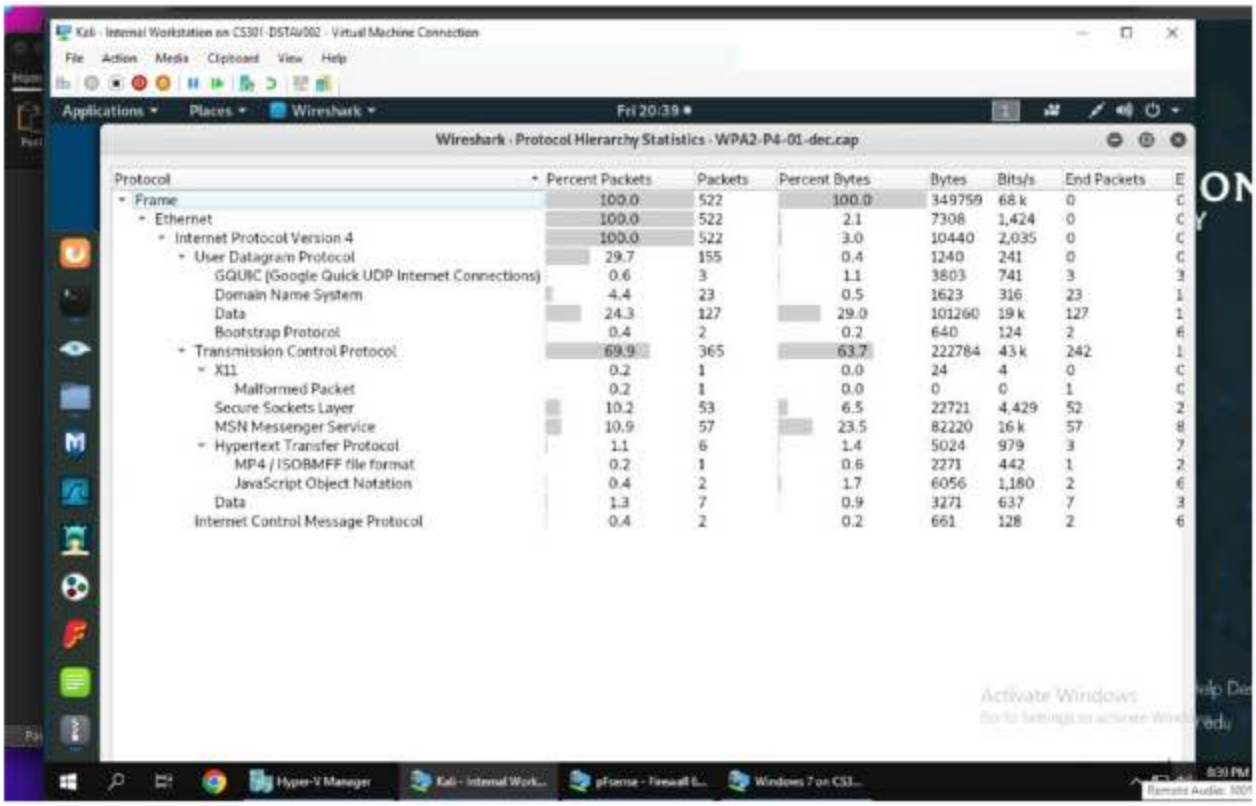
2. Decrypt the encrypted traffic and write a detailed summary to describe what you have explored
   from this encrypted traffic file. -10 points
   Last digit of your MD5 Filename
   0~3 WPA2-P1-01.cap
   4~5 WPA2-P2-01.cap
   6~8 WPA2-P3-01.cap
   9~B WPA2-P4-01.cap
   C~F WPA2-P5-01.cap
   Figure 1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




Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Fri 20:25
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Opening WPA2-P4-01.cape wait...
Read 4225 packets.
1 potential targets
Aircrack-ng 1.5.2
[00:00:12] 22248/7120712 keys tested (2110.19 k/s)
Time left: 56 minutes, 4 seconds 0.31%
KEY FOUND! [linkinpark]
Master Key : C1 73 7E 87 F1 91 77 4C 4B 3B FF 7B 8B AE CF 9A
93 D4 9B F7 26 B9 AC A7 8D 08 9D CF C6 59 EA D3
Transient Key : 6B A3 3C 60 2D DF B4 2C 94 05 47 2F 3C C3 2E 10
2F DD 42 EA 83 74 7C DA A1 EC 34 A7 72 99 70 96
29 04 7E F9 52 0F 2E E7 07 F0 2A C7 3B 11 F5 91
78 4F 6B 93 A9 F0 37 42 8E 3A 78 7F 01 8B 28 85
EAPOL HMAC : 64 0C D2 E4 54 7E 1F 2B E8 52 36 EF 2C 1A EB 85
Activate Windows
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows 7 on CS3...
8:25 PM
4/5/2024


Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Fri 20:36
Home CYSE301 Module V-W...ss Security
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Total number of WEP data packets 0
Total number of WPA data packets 645
Number of plaintext data packets 0
Number of decrypted WEP packets 0
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
wireshark WPA2-P4-01-dec.cap
airdecap-ng -p linkinpark WPA2-P4-01.cap -e CyberPHY
Total number of stations seen 5
Total number of packets read 4225
Total number of WEP data packets 0
Total number of WPA data packets 645
Number of plaintext data packets 0
Number of decrypted WEP packets 0
Number of corrupted WEP packets 0
Number of decrypted WPA packets 522
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets 0
Size Modified
47.2 MB 3 Nov 2015
24.6 MB Tue
887.9 kB 10 Nov 2015
496.0 kB Tue
139.9 MB Tue
721.4 kB 14 Mar 2017
358.1 kB 20:36
Other Locations
Activate Windows
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows 7 on CS3...
8:36 PM
4/5/2024


Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Fri 20:38
WPA2-P4-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 0.0.0.0 255.255.255.255 DHCP 356 DHCP Discover - Transaction ID 0x20
2 0.011265 0.0.0.0 255.255.255.255 DHCP 308 DHCP Request - Transaction ID 0x20
3 0.641104 42.62.94.2 192.168.1.127 TCP 217 443 → 42039 [PSH, ACK] Seq=1 Ack=1 W
4 1.610888 192.168.1.1 192.168.1.127 DNS 104 Standard query response 0xf579 A myg
5 1.621128 192.168.1.1 192.168.1.127 DNS 108 Standard query response 0xe82c A m.q
6 1.731728 66.198.24.243 192.168.1.127 TCP 54 80 → 39975 [FIN, ACK] Seq=1 Ack=1 Wi
7 1.961625 192.168.1.127 192.168.1.1 DNS 82 Standard query 0xf81c A cm045.getui.
8 1.999512 192.168.1.127 192.168.1.1 DNS 87 Standard query 0xfa99 A router-g0-pu
9 3.508682 183.61.49.155 192.168.1.127 TCP 74 8080 → 40163 [SYN, ACK] Seq=0 Ack=1
10 4.884303 72.30.202.51 192.168.1.127 TCP 1514 443 → 41748 [ACK] Seq=1 Ack=1 Win=61
11 5.884186 72.30.202.51 192.168.1.127 SSL 1514 [TCP Previous segment not captured]
12 5.322570 186.75.27.37 192.168.1.127 TCP 66 443 → 48573 [ACK] Seq=1 Ack=1 Win=30
Frame 1: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits)
Ethernet II, Src: HuaweiTe_b8:3d:23 (00:9a:cd:b8:3d:23), 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
WPA2-P4-01-dec.cap
Packets: 522 · Displayed: 522 (100.0%)
Profile: Default
Activate Windows
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows 7 on CS3...
8:38 PM


Kali - Internal Workstation on CS301-DSTAV002 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Wireshark Fri 20:39
Wireshark · Protocol Hierarchy Statistics · WPA2-P4-01-dec.cap
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets
Frame 100.0 522 100.0 349759 68 k 0
Ethernet 100.0 522 2.1 7308 1,424 0
Internet Protocol Version 4 100.0 522 3.0 10440 2,035 0
User Datagram Protocol 29.7 155 0.4 1240 241 0
GQUIC (Google Quick UDP Internet Connections) 0.6 3 1.1 3803 741 3
Domain Name System 4.4 23 0.5 1623 316 23
Data 24.3 127 29.0 101260 19 k 127
Bootstrap Protocol 0.4 2 0.2 640 124 2
Transmission Control Protocol 69.9 365 63.7 222784 43 k 242
X11 0.2 1 0.0 24 4 0
Malformed Packet 0.2 1 0.0 0 0 1
Secure Sockets Layer 10.2 53 6.5 22721 4,429 52
MSN Messenger Service 10.9 57 23.5 82220 16 k 57
Hypertext Transfer Protocol 1.1 6 1.4 5024 979 3
MP4 / ISOBMFF file format 0.2 1 0.6 2271 442 1
JavaScript Object Notation 0.4 2 1.7 6056 1,180 2
Data 1.3 7 0.9 3271 637 7
Internet Control Message Protocol 0.4 2 0.2 661 128 2
Activate Windows
Hyper-V Manager
Kali - Internal Work...
pFsense - Firewall 6...
Windows 7 on CS3...
8:39 PM

In the encrypted traffic file, you can see many IPs in conversation with each other and you can also see some of the traffic is coming from websites. There are also various protocols being used in this traffic file as well such as DNS which used being used for these domain names. As well TCP to ensure the integrity of it.