

OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS
ASSIGNMENT #6 WI-FI PASSWORD CRACKING

Clarence V. Kimbrell Jr.
UIN 01207106

Task A Step 1

The first screenshot shows a Kali Linux virtual machine running a terminal window. The terminal displays the output of the `airdecap-ng` command, which is used to decrypt WEP/WPA packets. The output shows statistics for the captured traffic, including the number of stations, packets, and data packets. The second screenshot shows the same virtual machine with Wireshark open, displaying a detailed protocol hierarchy for the captured traffic. The Wireshark interface shows a list of protocols and their corresponding packet counts and byte sizes.

Terminal Output (airdecap-ng):

```
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security# airdecap-ng
Airdecap-ng 1.9.2 - (C) 2006-2018 Thomas d'Otreppe
https://www.aircrack-ng.org

usage: airdecap-ng [options] <pcap file>

Common options:
  -i : don't remove the 802.11 header
  -b <bssid> : access point MAC address filter
  -e <essid> : target network SSID
  -o <fname> : output file for decrypted packets (default <src>=dec)

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

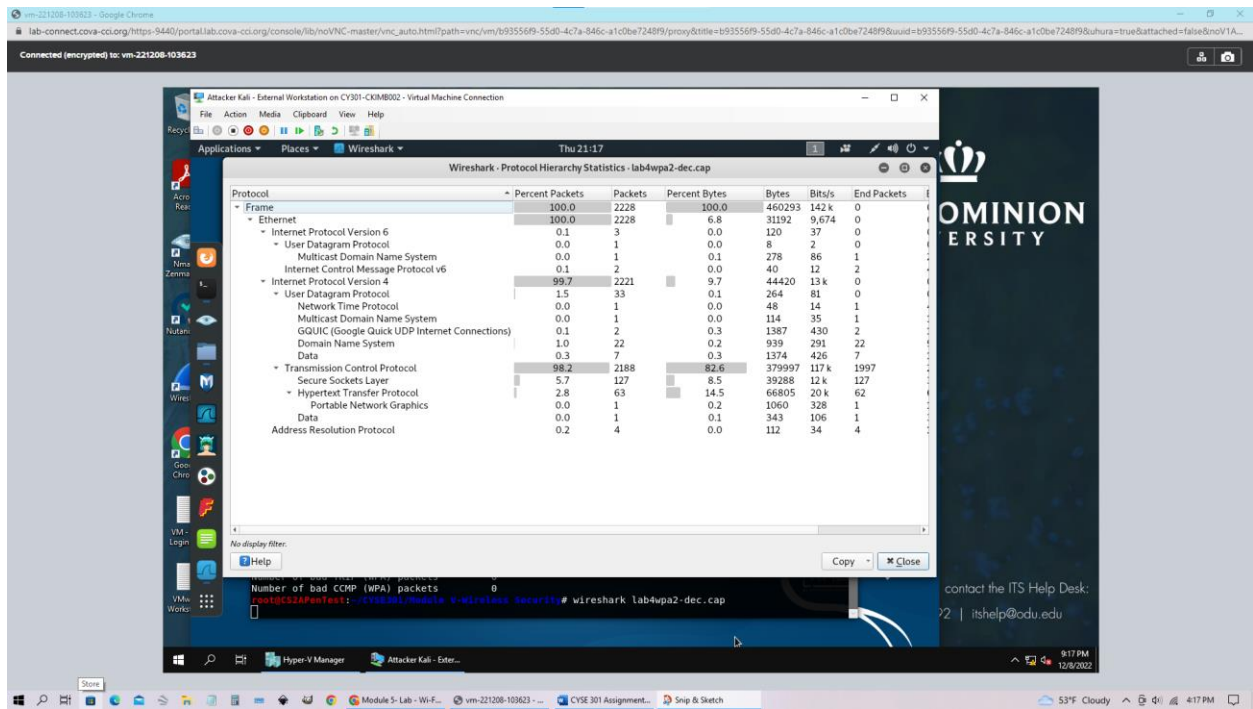
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security# airdecap-ng -w F2:C7:BB:35:B9
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security# airdecap-ng -w F2:C7:BB:35:B9 lab4wep.cap
Total number of stations seen: 37
Total number of packets read: 404693
Total number of WEP data packets: 142415
Total 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
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security#
```

Wireshark Protocol Hierarchy Statistics:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	En
Frame	100.0	142415	100.0	22356528	568 k	0	0
Ethernet	100.0	142415	8.9	1993810	50 k	0	0
Internet Protocol Version 6	0.0	60	0.0	2400	61	0	0
User Datagram Protocol	0.0	46	0.0	368	9	0	0
Multicast Domain Name System	0.0	40	0.0	5394	137	40	53
DHCPv6	0.0	6	0.0	594	15	6	59
Internet Control Message Protocol v6	0.0	14	0.0	324	8	14	32
Internet Protocol Version 4	13.7	19550	1.7	391028	9,945	0	0
User Datagram Protocol	0.1	198	0.0	1584	40	0	0
NetBIOS Name Service	0.0	20	0.0	1102	28	20	111
NetBIOS Datagram Service	0.0	3	0.0	549	13	0	0
SMB (Server Message Block Protocol)	0.0	3	0.0	303	7	0	0
SMB MailSlot Protocol	0.0	3	0.0	75	1	0	0
Microsoft Windows Browser Protocol	0.0	3	0.0	45	1	3	45
Multicast Domain Name System	0.0	30	0.0	4542	115	30	45
Dropbox LAN sync Discovery Protocol	0.0	20	0.0	2300	58	20	23
Domain Name System	0.1	80	0.0	6069	154	80	60
Bootstrap Protocol	0.0	5	0.0	1500	38	5	151
Transmission Control Protocol	13.6	19342	73.4	16399012	417 k	15644	111
Secure Sockets Layer	0.6	788	2.7	593050	15 k	785	58
Malformed Packet	0.0	12	0.0	0	0	12	0
Hypertext Transfer Protocol	0.9	1296	7.7	1715370	43 k	1238	161
MIME Multipart Media Encapsulation	0.0	2	0.0	1767	44	2	30
Media Type	0.0	18	0.0	4538	115	18	45
Line-based text data	0.0	11	0.0	7573	192	11	71
JPEG File Interchange Format	0.0	3	0.1	12178	309	3	13
JavaScript Object Notation	0.0	1	0.0	12	0	1	12
HTML Form URL Encoded	0.0	14	0.1	17314	440	14	23
CompuServe GIF	0.0	9	0.0	2734	69	9	27
FTP Data	0.0	7	0.0	9464	240	7	0
File Transfer Protocol (FTP)	0.0	22	0.0	656	16	22	0
Internet Group Management Protocol	0.0	7	0.0	56	1	7	56
Internet Control Message Protocol	0.0	3	0.0	120	3	3	121
Data	1.2	1730	9.7	2175390	55 k	1730	21
Address Resolution Protocol	86.2	122691	15.4	3435348	87 k	122691	34

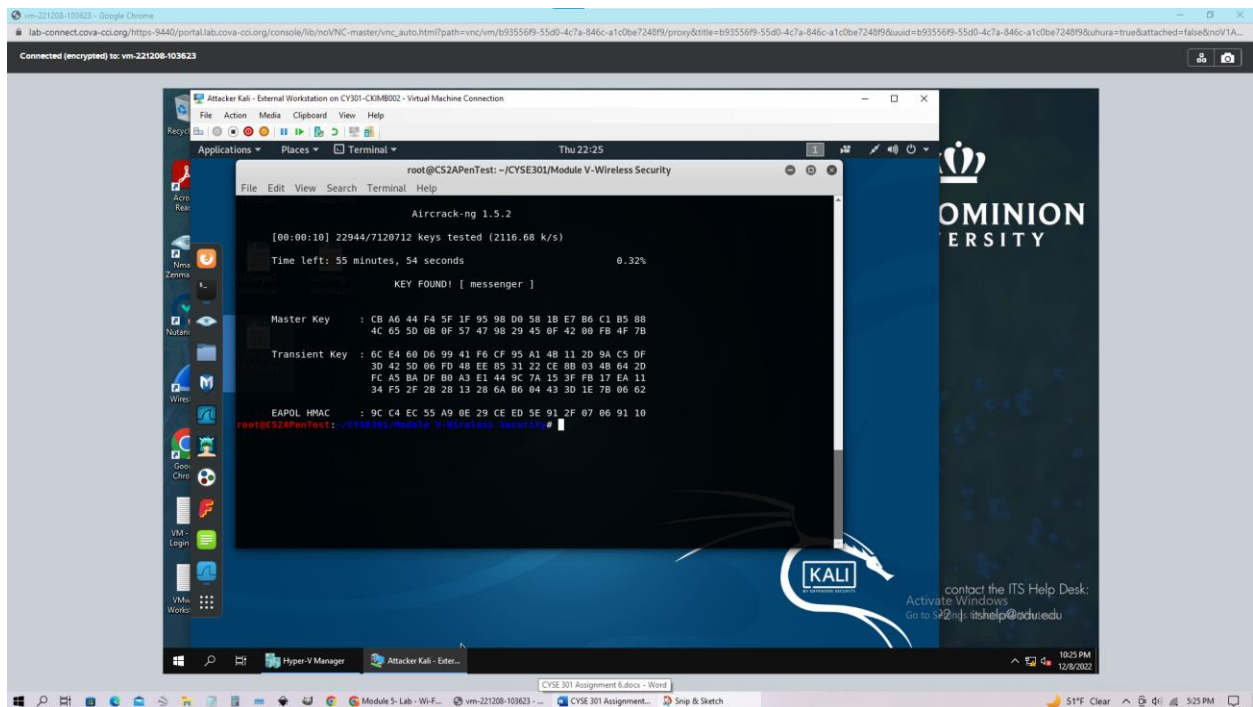
The above screenshots are detailed traffic analyses using aircrack and Wireshark. We can see that many packets are being sent to the target with Wireshark. This indicates that an attacker is trying to inject information into a user's wi-fi system.

Task A Step 2

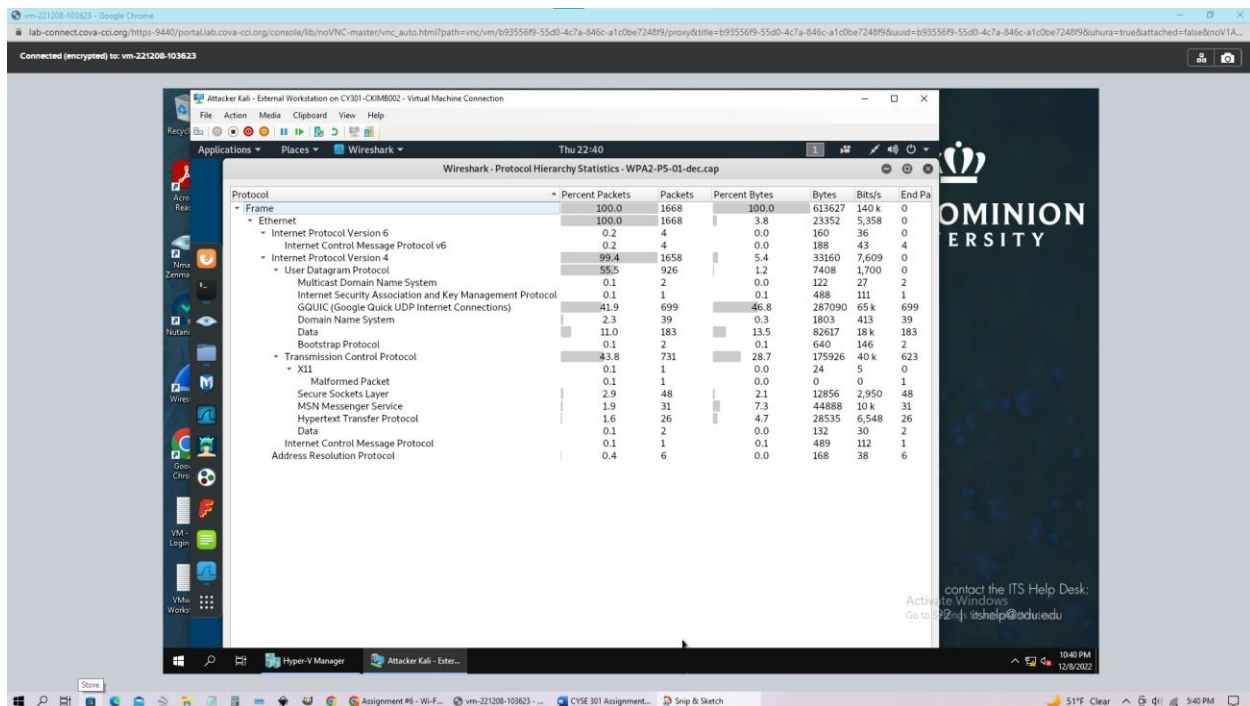


When looking at this protocol hierarchy we can see that there are significantly fewer packets being sent.

Task B Step 1



We were able to find out the password by using a dictionary attack. This was completed by using aircrack-ng followed by the file name then -w with the rockyou.txt file. It shuffled through many potential passwords until it found it using and displaying the [messenger].



When we take a closer look at the traffic analysis, we see that all but ten packets are internet protocol version 4. This indicates that a large majority of the packets were IPv4 based. So we can conclude that whoever was using this was doing many things on the internet.