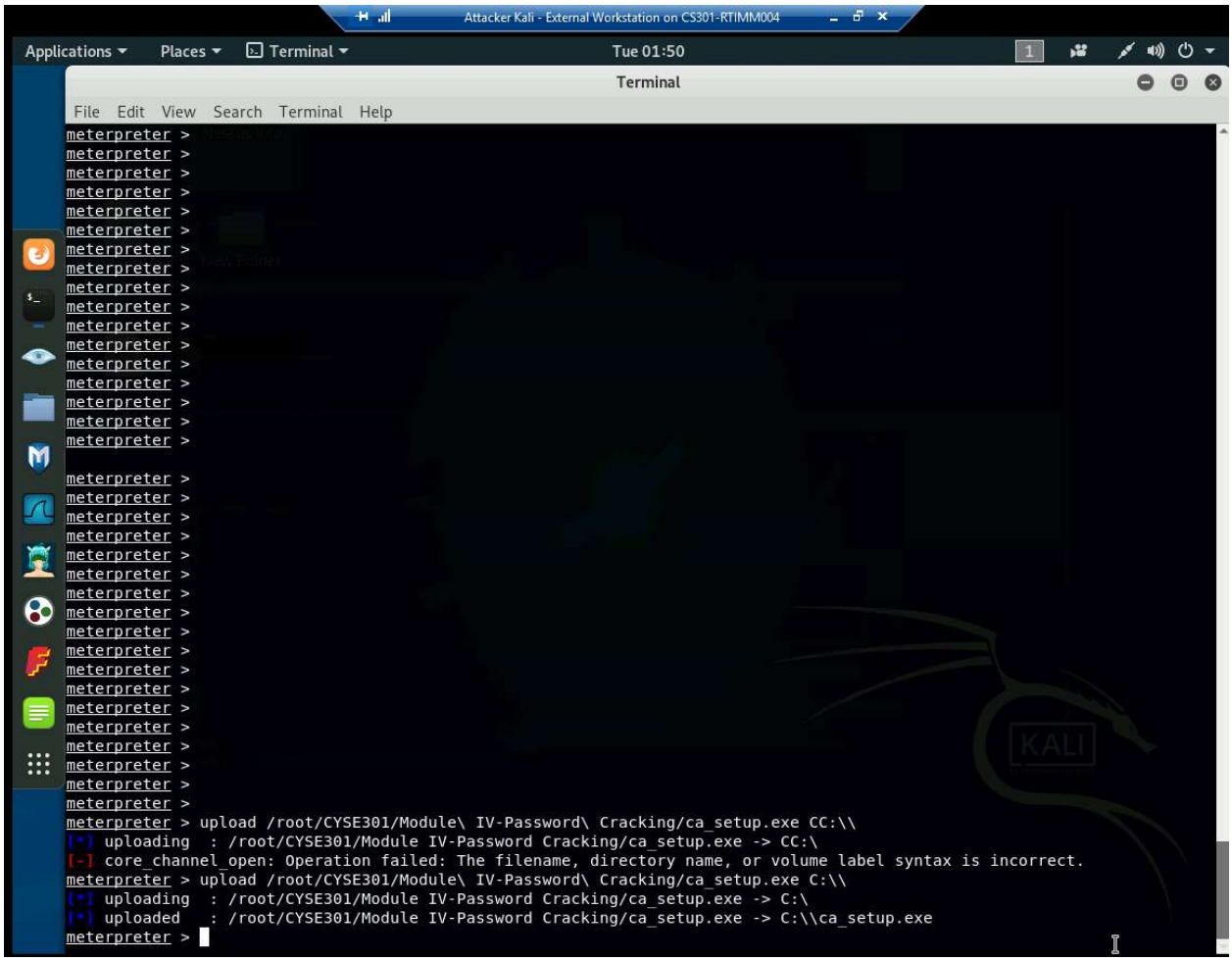
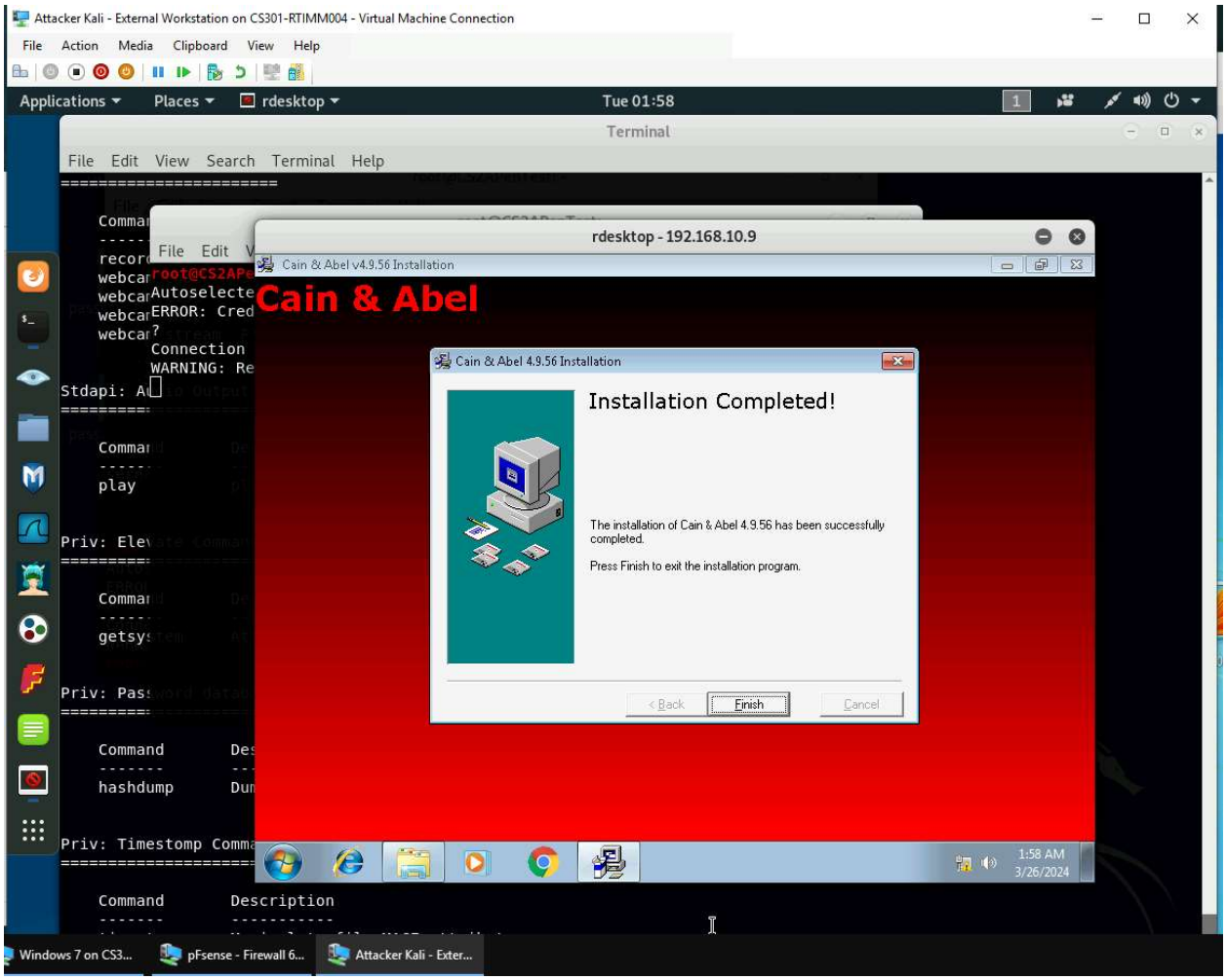
4. Upload the password cracking tool, Cain and Abel remotely to windows 7 VM, implement both brute force and dictionary attacks to crack the password on Win 7.\

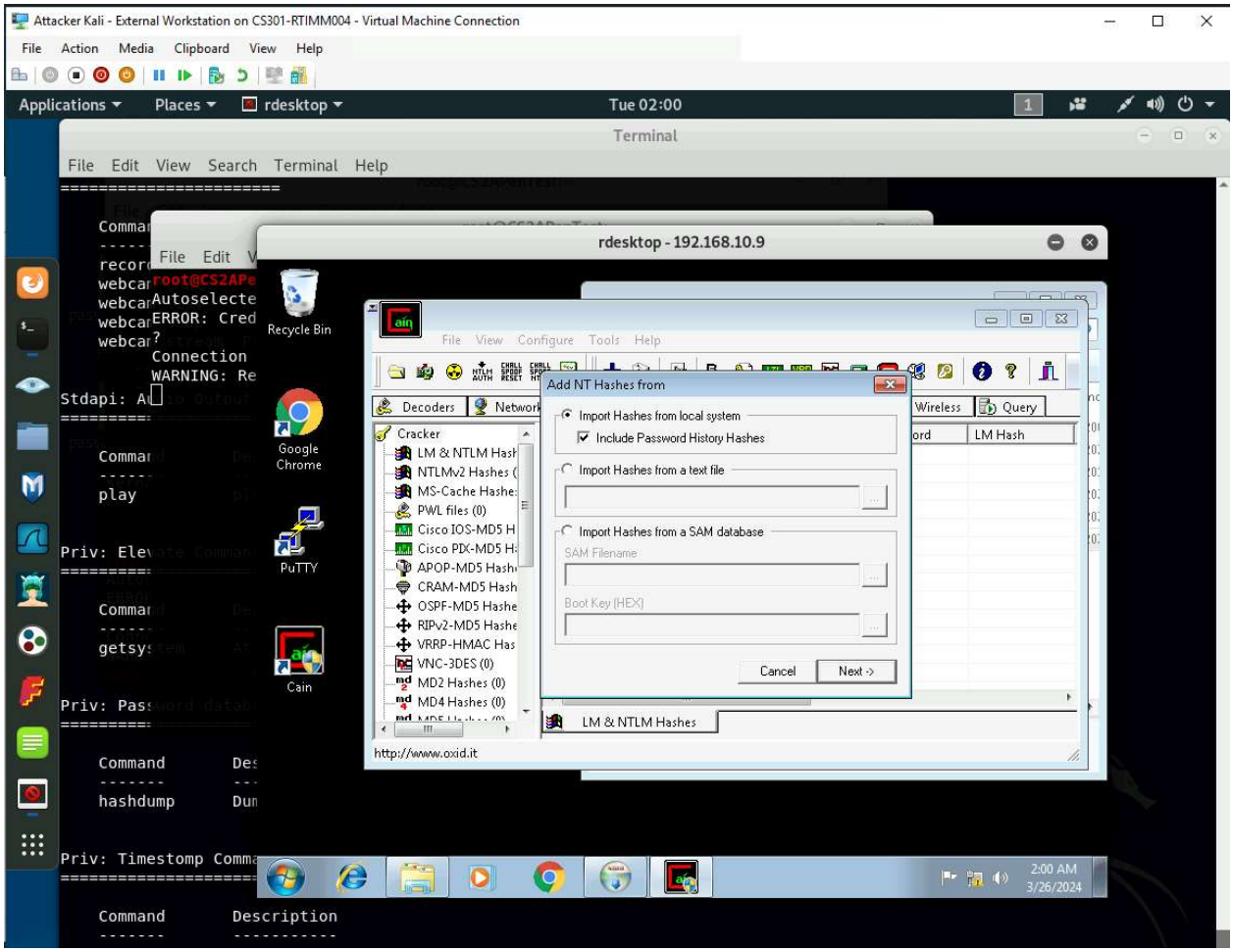
Using upload command, accidentally wrote C:\\ wrong!



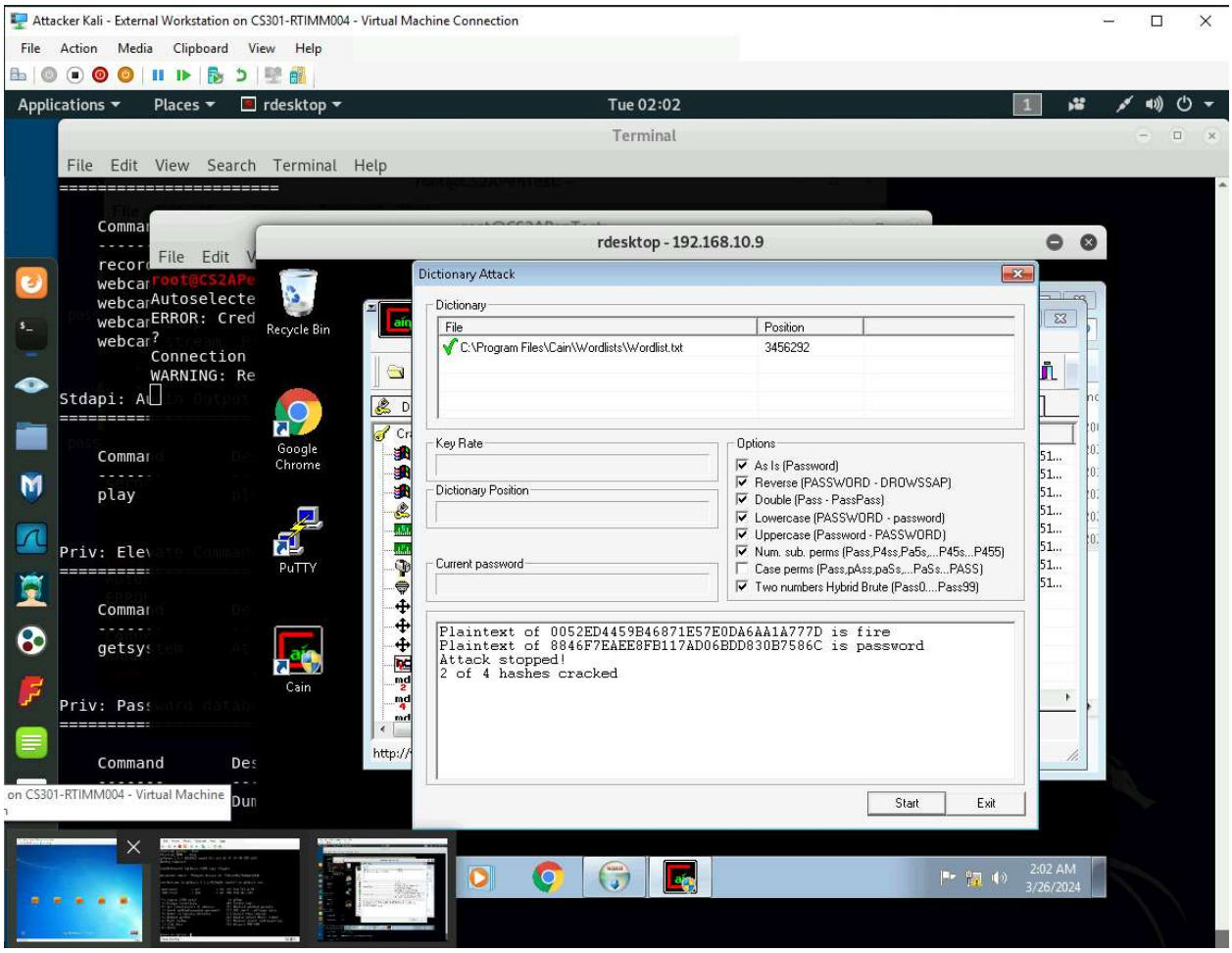
Below you can see I used rdp. Sorry I covered the command, its in the terminal behind the rdp session.



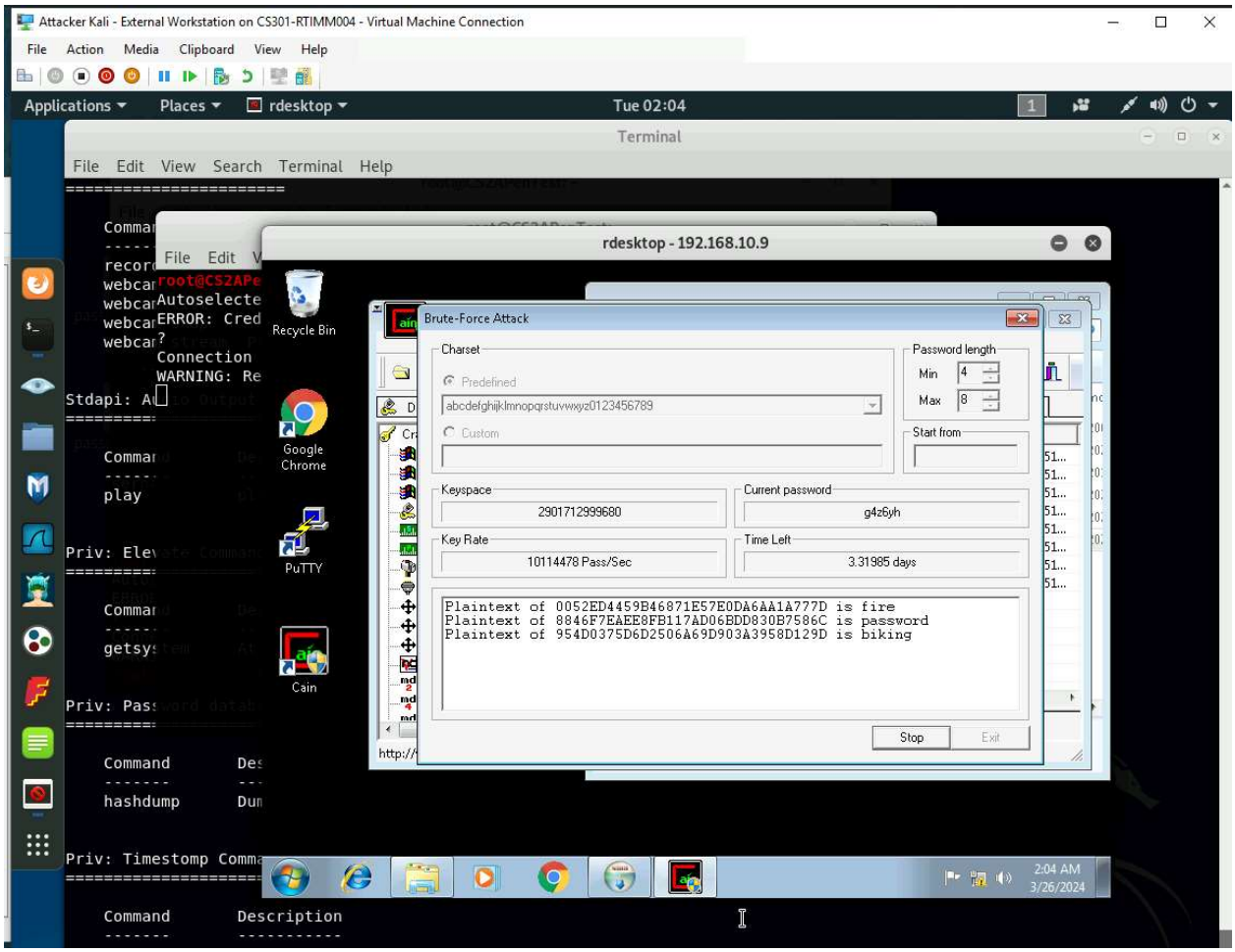
Below I am adding the hashes from the local system.



Below I do a dictionary attack, I only get two of the four passwords. How is biking not in the dictionary???



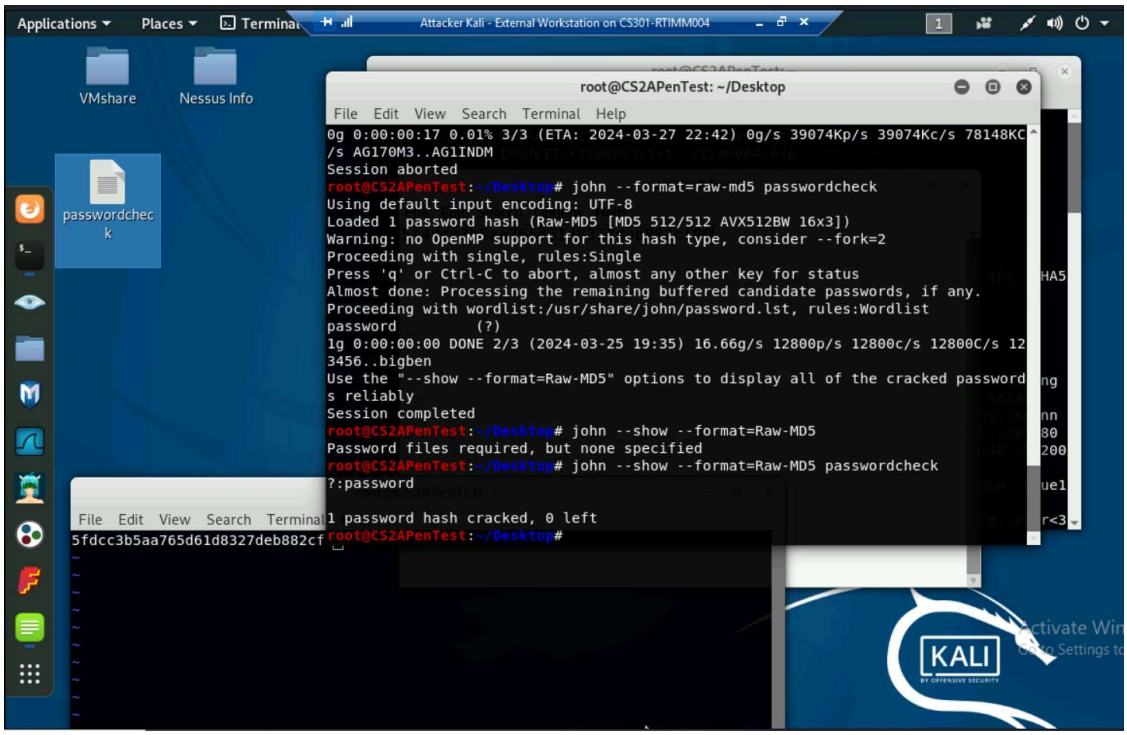
Below is my brute force attempt, it only got 3 of them, probably could've left it on overnight and it could get the last one.

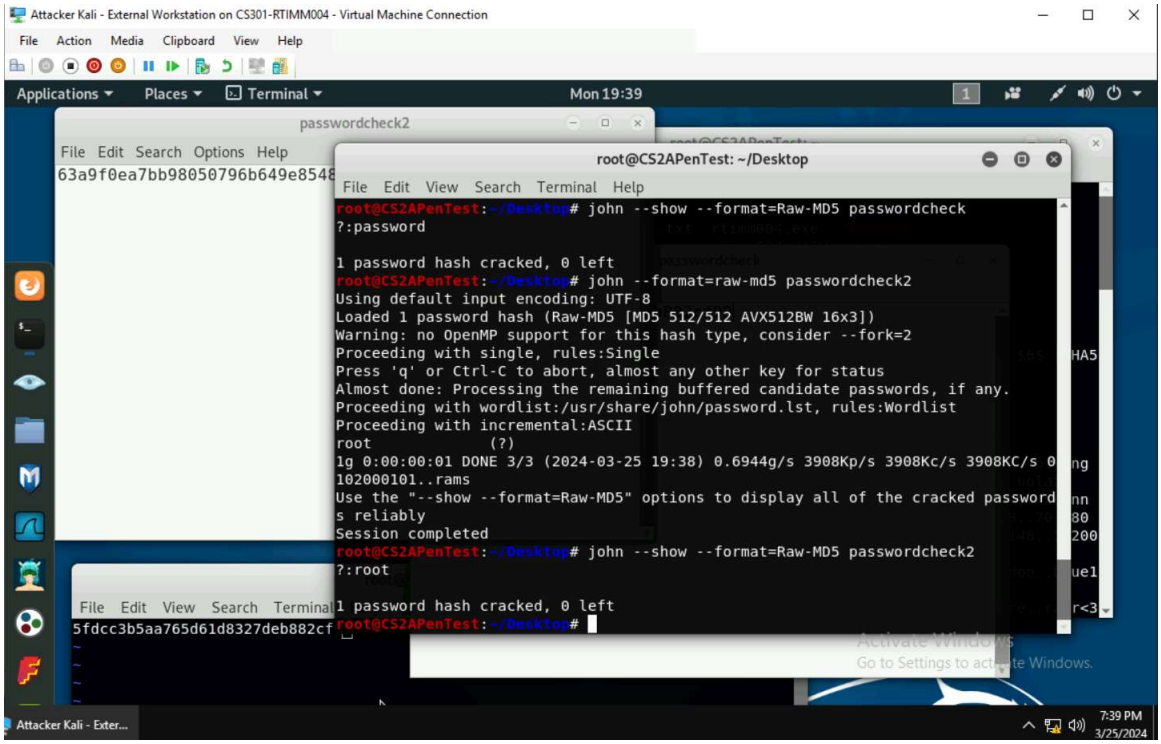


Task E (Extra Credit)

1. Crack the following hashes using proper format. Both are MD5
   5f4dcc3b5aa765d61d8327deb882cf99
   63a9f0ea7bb98050796b649e85481845

I placed both the hashes into their own individual files, passwordcheck and passwordcheck2. After setting the format to raw-md5 in john the ripper, I activated john, let it work, then did the john –show –format=Raw-MD5 to see the results. Below are the two screenshots of the results.



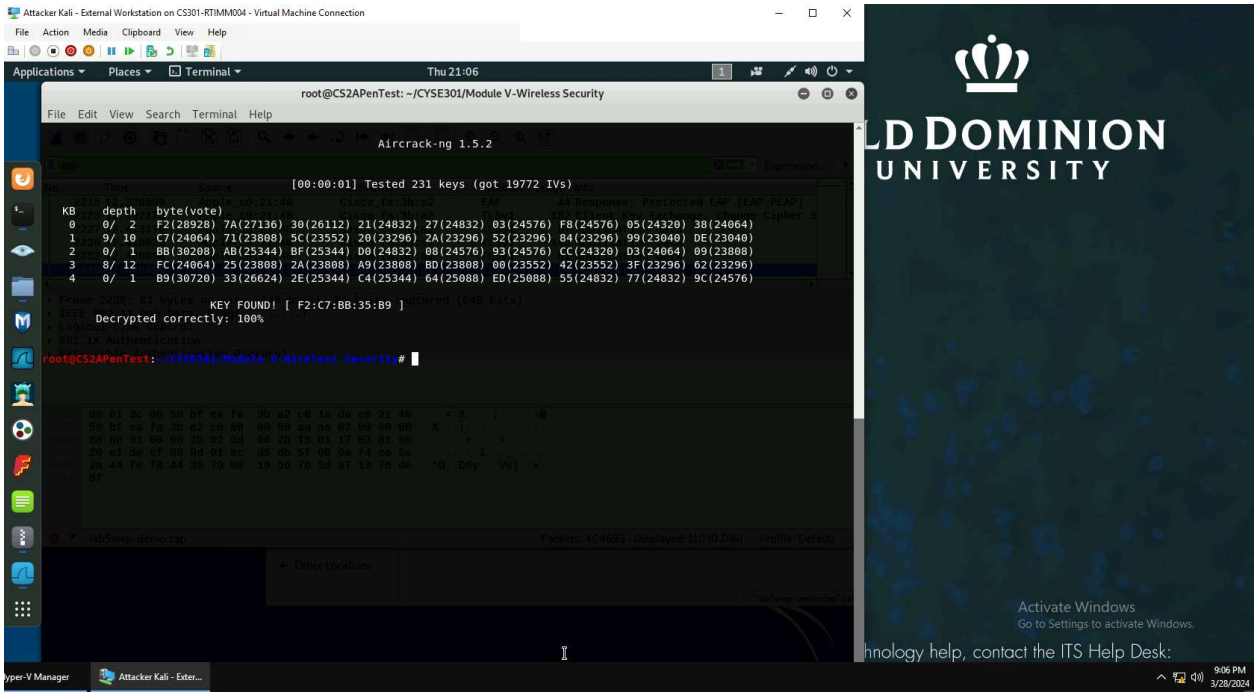


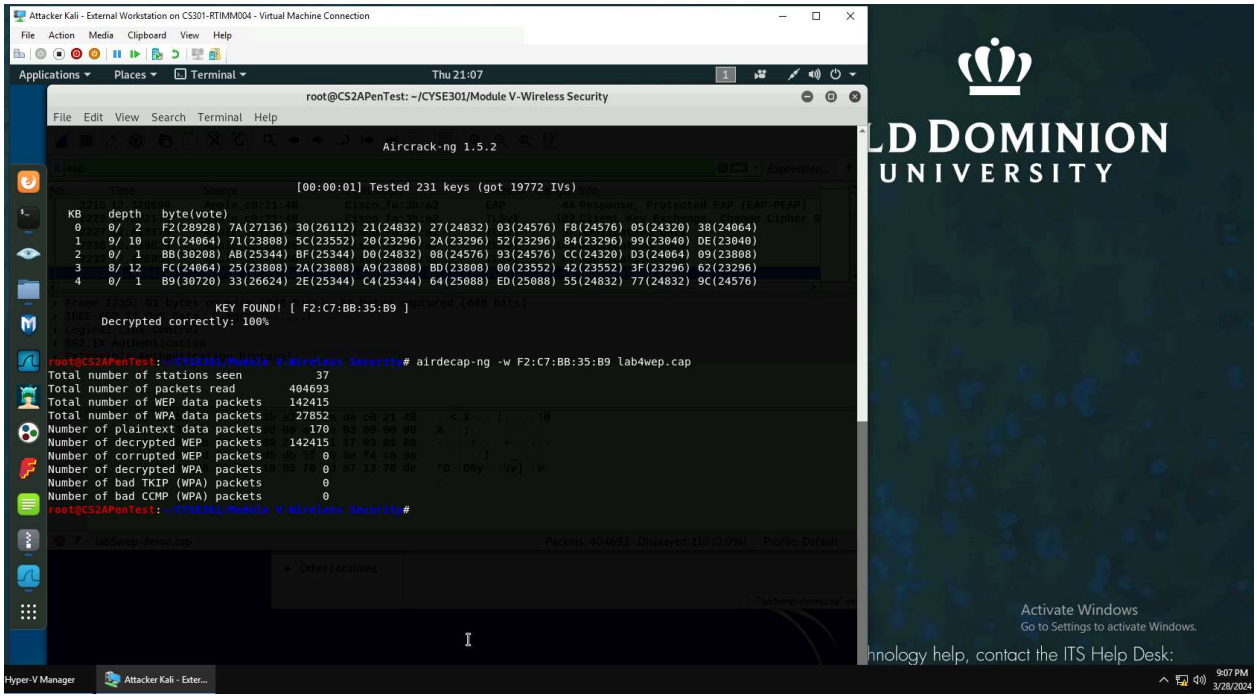
Task C

1. Decrypt the lab4wep.cap file and perform a detailed traffic analysis

After using aircrack-ng to get the decryption key and view the traffic, and using airdecap, there are a few takeaways I have garnered. I tried my best to fulfill a “detailed traffic analysis”.

First, here are the pictures of me using aircrack/airdecap respectively:

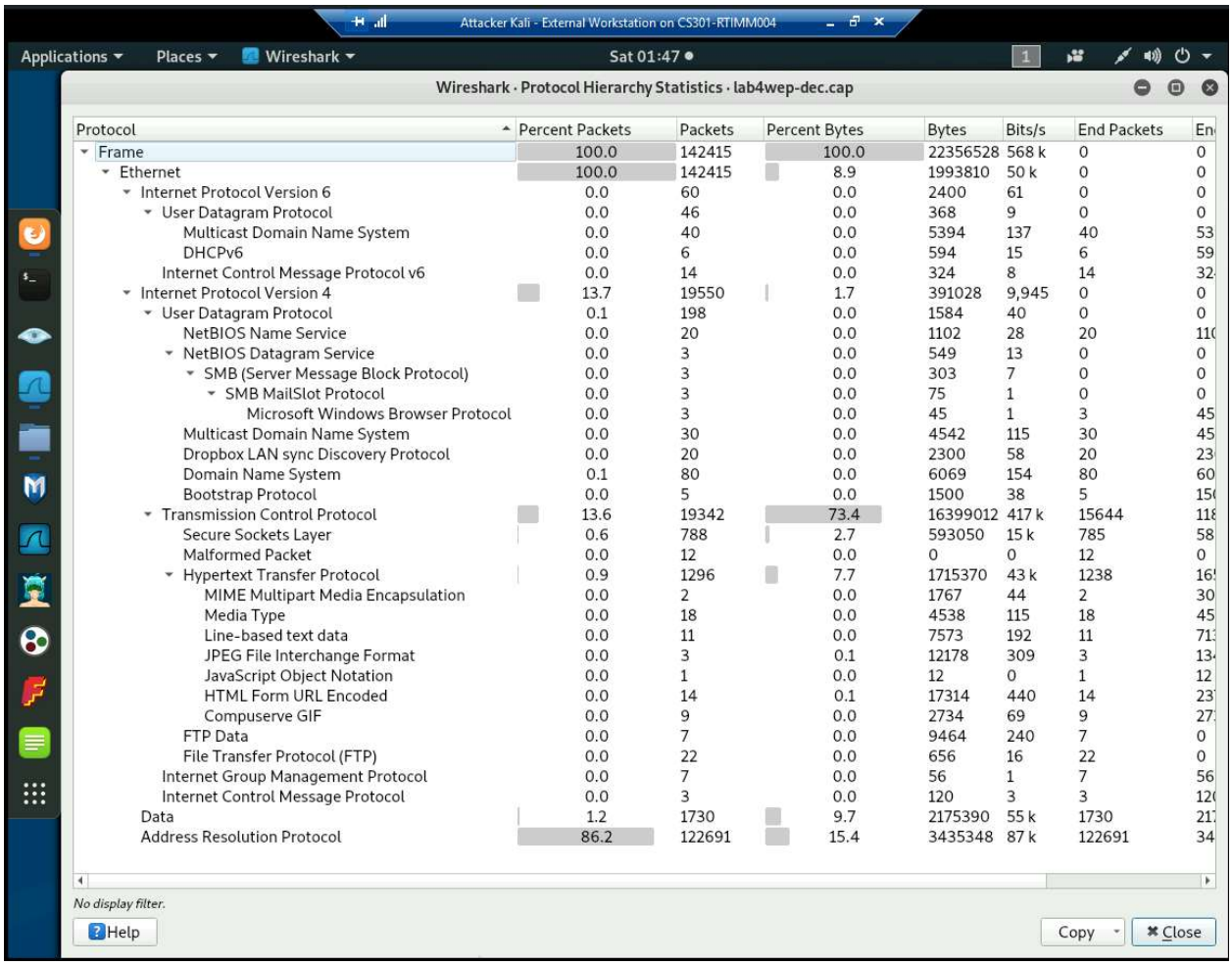

Attacker Kali - External Workstation on CS301-RTIMM004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 21:06
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security
File Edit View Search Terminal Help
Aircrack-ng 1.5.2
[00:00:01] Tested 231 keys (got 19772 IVs)
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
root@CS2APenTest: ~/CYSE301/Module V-Wireless Security#
LD DOMINION
UNIVERSITY
Activate Windows
Go to Settings to activate Windows.
hnology help, contact the ITS Help Desk:
Hyper-V Manager
Attacker Kali - Exter...
9:06 PM
3/28/2024


Attacker Kali - External Workstation on CS301-RTIMM004 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Thu 21:07
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) 03(24576) F8(24576) 05(24320) 38(24064)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040)
2 0/ 1 BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808)
3 8/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296)
4 0/ 1 B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
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#
LD DOMINION
UNIVERSITY
Activate Windows
Go to Settings to activate Windows.
hnology help, contact the ITS Help Desk:
Hyper-V Manager
Attacker Kali - Exter...
9:07 PM
3/28/2024

Takeaways from the traffic:

- 192.168.2.10 downloads DC13ATM.jpg, onto their machine using ‘get’ command. The picture is that of some band named MAKSIM (Picture below) I have reason to believe that they downloaded this off of an unsecure website using HTTP, and this may have given a malicious user a backdoor. We’ve used a similar technique when cracking into windows 7 machines, where the victim downloads a file onto their machine, causing it to be taken over through a remote connection.
- Using the FTP-data filter, 195.42.179.201 can be seen using a passive (PASV) FTP session on the 192.168.2.10 machine. The source seems like he’s in the current directory of /pub/wordlists/passwords/password.gz. I think he may be trying to do a dictionary attack using the zipped password file.
- It seems like 192.168.2.10 gets taken off the network, with ARP trying to resolve where it went. (Or, it could’ve been an ARP storm, where the STP was turned off and it looped forever)
- I did a HTTP object export of the traffic, and there’s a TON of files, all of the same size, all the same file name/file type (.m4a) being downloaded from sites like m9.music.126.net, m8music.126.net, etc.. I attempted to listen to the files, but none of them would work in their current format, and the kali virtual machine didn’t have VLC or a converter so I could listen to them.
- 195.42.179.201 continues sending some HTML that I can’t decipher. No clue what it is, but it looks like a webpage… I think it may be something regarding apple keys

Picture below shows that 86% of packets were arp, leaving me to believe it either was the storm or doing an internal search of an IP address.



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	110
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	15
Transmission Control Protocol	13.6	19342	73.4	16399012	417 k	15644	118
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	16
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	12
Data	1.2	1730	9.7	2175390	55 k	1730	21
Address Resolution Protocol	86.2	122691	15.4	3435348	87 k	122691	34

First picture, you can see 192.168.2.10 use the ‘get’ command, getting the jpg off the server.