Kunal Patel

CYSE 301: Cybersecurity Technique and Operations

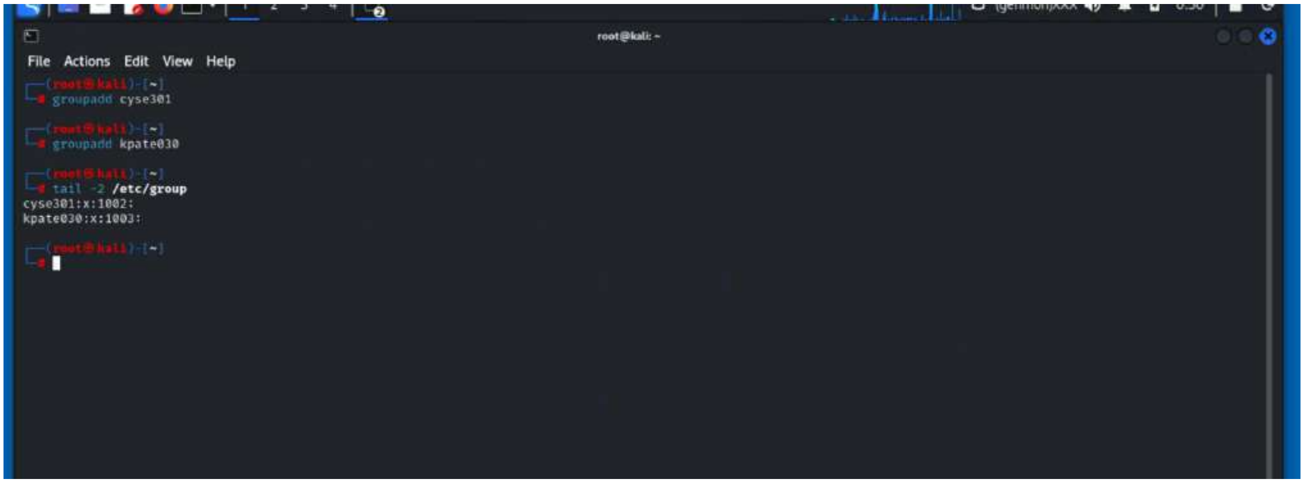
Assignment 5: Password Cracking (Part A &B)

Kunal Patel

At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof.
You need to use

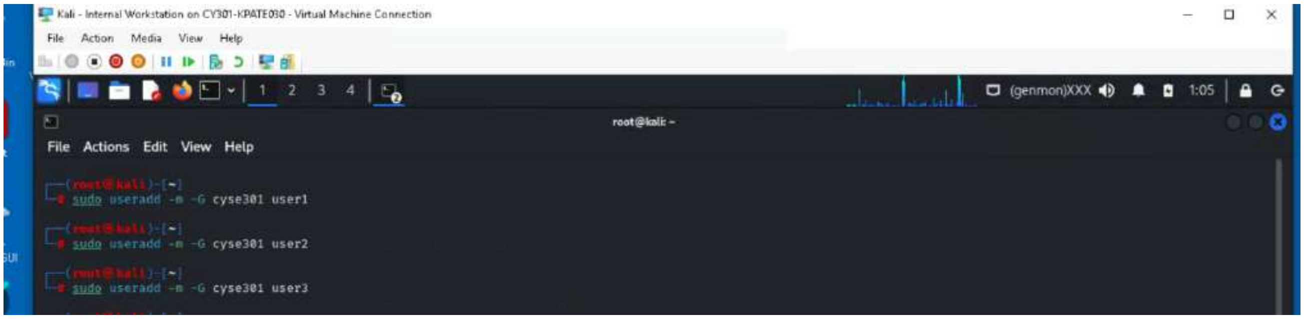
Task A: Linux Password Cracking (25 points)

1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.



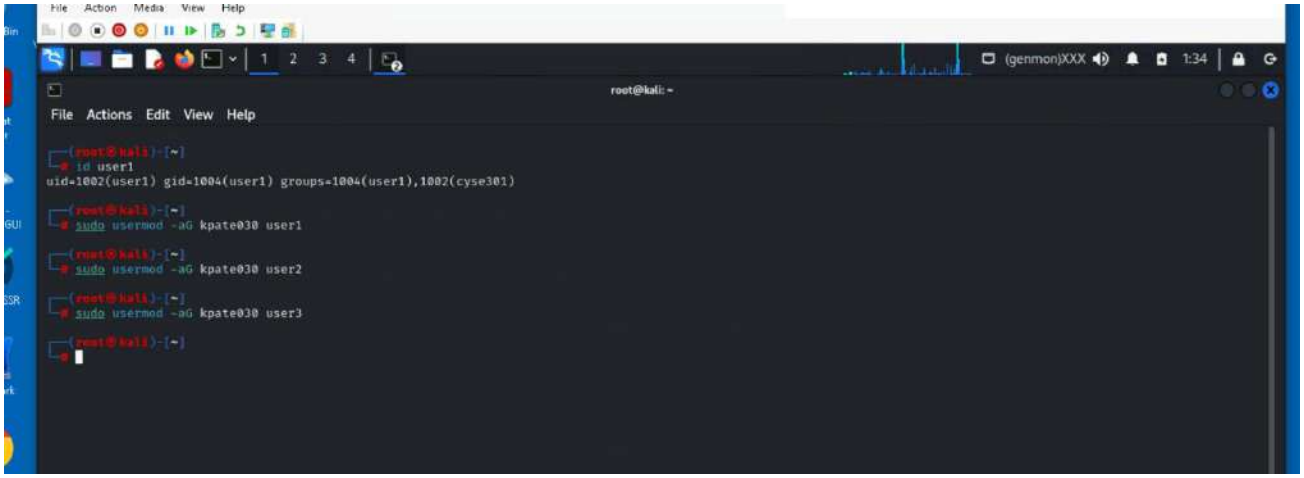
```
┌──(root㉿kali)-[~]
└─# groupadd cyse301

┌──(root㉿kali)-[~]
└─# groupadd kpate030

┌──(root㉿kali)-[~]
└─# tail -2 /etc/group
cyse301:x:1002:
kpate030:x:1003:

┌──(root㉿kali)-[~]
└─# 
```

2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.



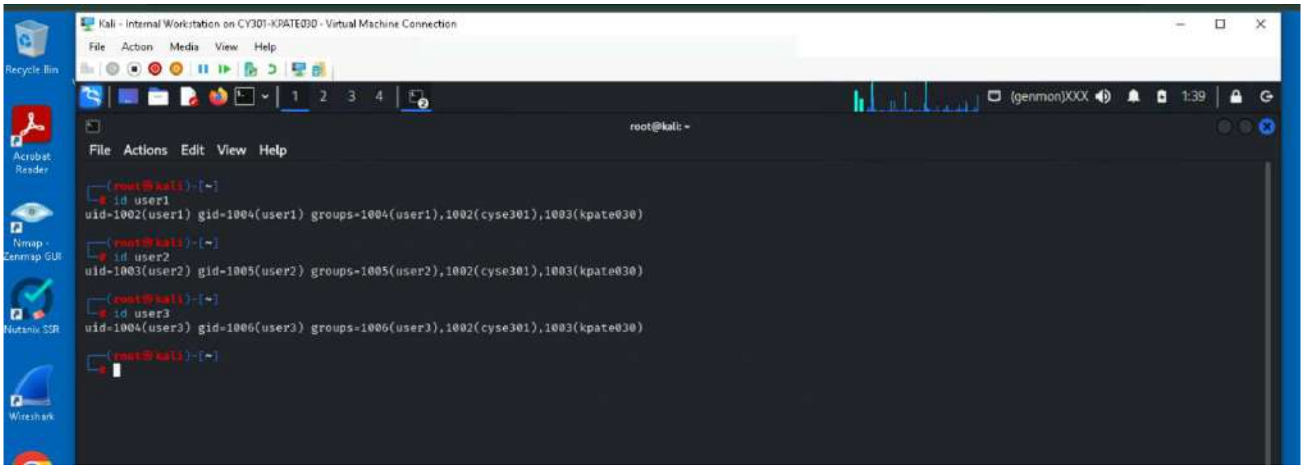
Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
(genmon)XXX
1:05
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 user1

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 user2

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 user3
```



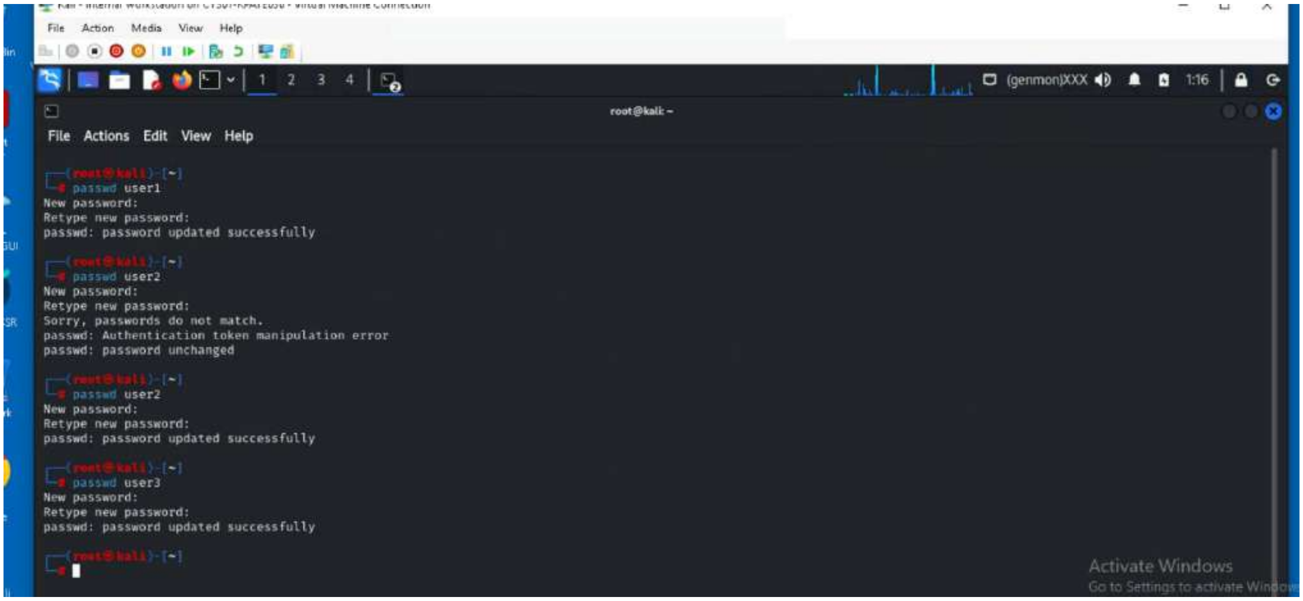
```
┌──(root㉿kali)-[~]
└─# id user1
uid=1002(user1) gid=1004(user1) groups=1004(user1),1002(cyse301)

┌──(root㉿kali)-[~]
└─# sudo usermod -aG kpate030 user1

┌──(root㉿kali)-[~]
└─# sudo usermod -aG kpate030 user2

┌──(root㉿kali)-[~]
└─# sudo usermod -aG kpate030 user3

┌──(root㉿kali)-[~]
└─# 
```

Kunal Patel


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
(genmon)XXX 1:39
root@kali: ~
File Actions Edit View Help

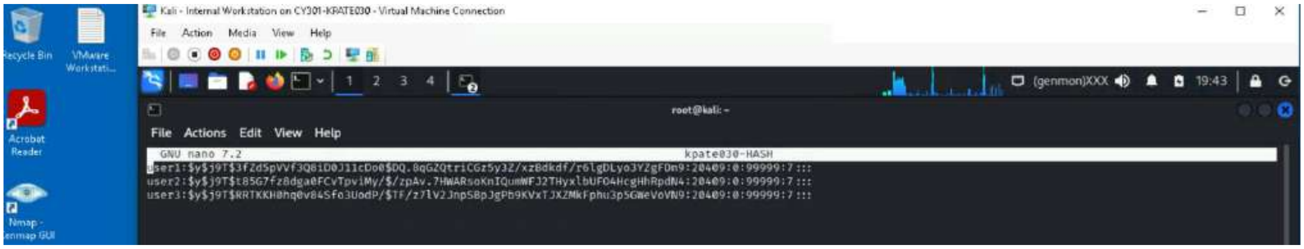
```
┌──(root㉿kali)-[~]
└─# id user1
uid=1002(user1) gid=1004(user1) groups=1004(user1),1002(cyse301),1003(kpate030)

┌──(root㉿kali)-[~]
└─# id user2
uid=1003(user2) gid=1005(user2) groups=1005(user2),1002(cyse301),1003(kpate030)

┌──(root㉿kali)-[~]
└─# id user3
uid=1004(user3) gid=1006(user3) groups=1006(user3),1002(cyse301),1003(kpate030)

┌──(root㉿kali)-[~]
└─# 
```

3. **5 points.** Choose Three 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.
   Password user1: 1234
   Password user2: Cyber2025
   Password user3: Hacking@9999


File Action Media View Help
(genmon)XXX 1:16
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows

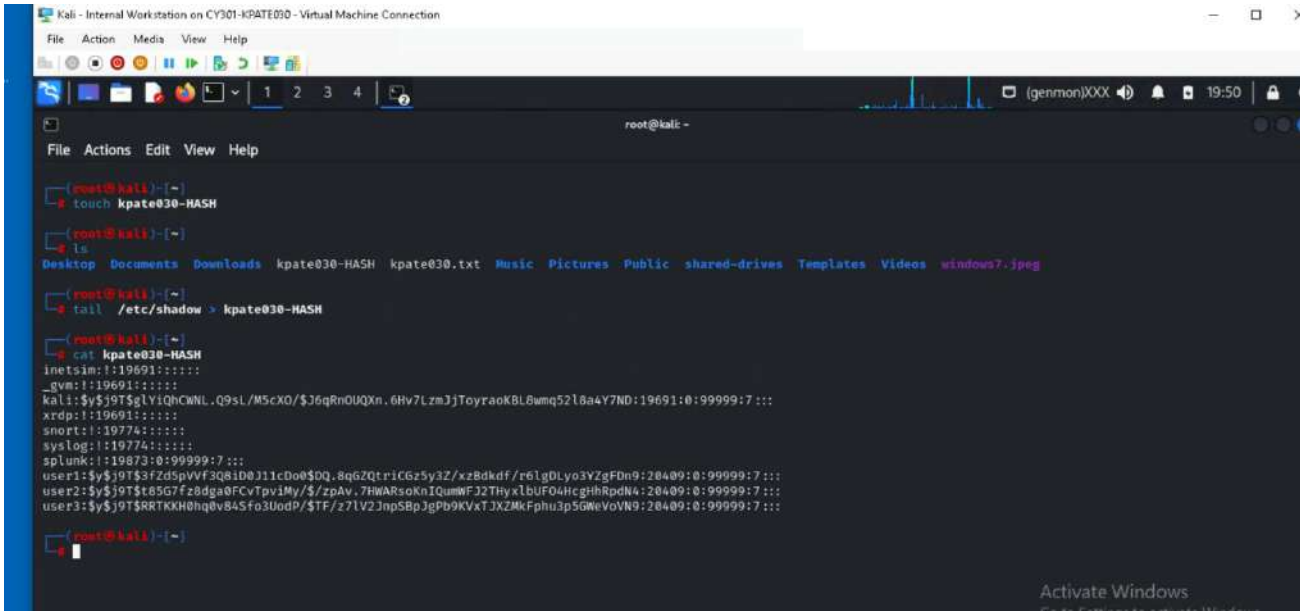
```
┌──(root㉿kali)-[~]
└─# passwd user1
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd user2
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged

┌──(root㉿kali)-[~]
└─# passwd user2
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# passwd user3
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# 
```

4. **5 points.** Export all Three users' password hashes into a file named "**YourMIDAS-HASH**" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.

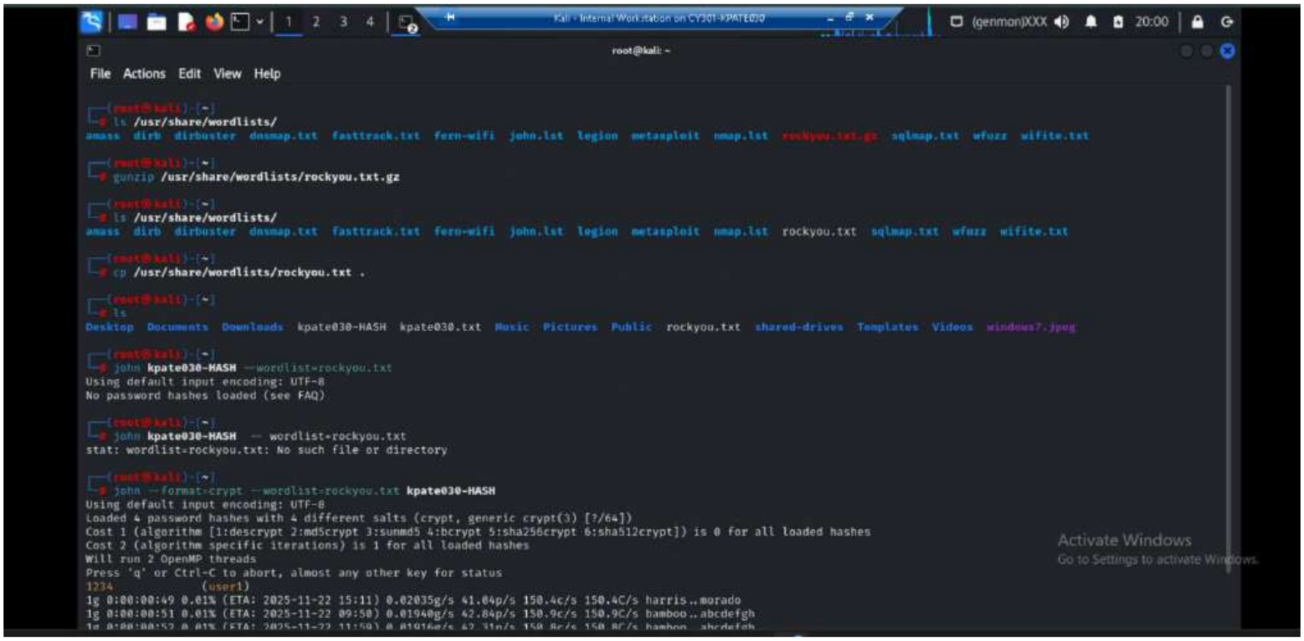

Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
(genmon)XXX 19:43
root@kali: ~
File Actions Edit View Help

```
  GNU nano 7.2                                                   kpate030-HASH
user1:$y$j9T$3fZd5pVVf3Q8iD0J11cDo0$DQ.8qGZQtriCGz5y3Z/xz8dkdf/r6lgDLyo3YZgFDm9:20409:0:99999:7:::
user2:$y$j9T$t85G7fz8dga0FCvTpviMy/$/zpAv.7HWARsoKnIQumWFJ2THyxlbUFO4HcgHhRpdN4:20409:0:99999:7:::
user3:$y$j9T$RRTKKH0hq0v84Sfo3UodP/$TF/z7lV2JnpS8pJgPb9KVxTJXZMkFphu3p5GWeVoVN9:20409:0:99999:7:::
```

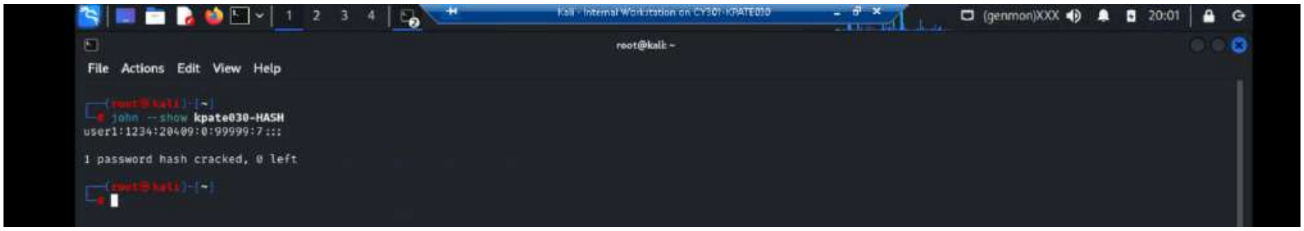
Kunal Patel


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
(genmon)XXX 19:50
root@kali: ~
File Actions Edit View Help
Activate Windows

```
┌──(root㉿kali)-[~]
└─# touch kpate030-HASH

┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  kpate030-HASH  kpate030.txt  Music  Pictures  Public  shared-drives  Templates  Videos  windows7.jpeg

┌──(root㉿kali)-[~]
└─# tail  /etc/shadow > kpate030-HASH

┌──(root㉿kali)-[~]
└─# cat kpate030-HASH
inetsim:!:19691::::::
_gvm:!:19691::::::
kali:$y$j9T$glYiQhCWNL.Q9sL/M5cXO/$J6qRnOUQXn.6Hv7LzmJjToyraoKBL8wmq52l8a4Y7ND:19691:0:99999:7:::
xrdp:!:19691::::::
snort:!:19774::::::
syslog:!:19774::::::
splunk:!:19873:0:99999:7:::
user1:$y$j9T$3fZd5pVVf3Q8iD0J11cDo0$DQ.8qGZQtriCGz5y3Z/xzBdkdf/r6lgDLyo3YZgFDn9:20409:0:99999:7:::
user2:$y$j9T$t85G7fz8dga0FCvTpviMy/$/zpAv.7HWARsoKnIQumWFJ2THyxlbUFO4HcgHhRpdN4:20409:0:99999:7:::
user3:$y$j9T$RRTKKH0hq0v84Sfo3UodP/$TF/z7lV2JnpSBpJgPb9KVxTJXZMkFphu3p5GWeVoVN9:20409:0:99999:7:::

┌──(root㉿kali)-[~]
└─# █
```


Kali - Internal Workstation on CY301-KPATE030
1 2 3 4
(genmon)XXX 20:00
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
┌──(root㉿kali)-[~]
└─# ls /usr/share/wordlists/
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt.gz  sqlmap.txt  wfuzz  wifite.txt

┌──(root㉿kali)-[~]
└─# gunzip /usr/share/wordlists/rockyou.txt.gz

┌──(root㉿kali)-[~]
└─# ls /usr/share/wordlists/
amass  dirb  dirbuster  dnsmap.txt  fasttrack.txt  fern-wifi  john.lst  legion  metasploit  nmap.lst  rockyou.txt  sqlmap.txt  wfuzz  wifite.txt

┌──(root㉿kali)-[~]
└─# cp /usr/share/wordlists/rockyou.txt .

┌──(root㉿kali)-[~]
└─# ls
Desktop  Documents  Downloads  kpate030-HASH  kpate030.txt  Music  Pictures  Public  rockyou.txt  shared-drives  Templates  Videos  windows7.jpeg

┌──(root㉿kali)-[~]
└─# john kpate030-HASH --wordlist=rockyou.txt
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(root㉿kali)-[~]
└─# john kpate030-HASH  -- wordlist=rockyou.txt
stat: wordlist=rockyou.txt: No such file or directory

┌──(root㉿kali)-[~]
└─# john --format=crypt --wordlist=rockyou.txt kpate030-HASH
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234             (user1)
1g 0:00:00:49 0.01% (ETA: 2025-11-22 15:11) 0.02035g/s 41.04p/s 150.4c/s 150.4C/s harris..morado
1g 0:00:00:51 0.01% (ETA: 2025-11-22 09:50) 0.01940g/s 42.84p/s 150.9c/s 150.9C/s bamboo..abcdefgh
1g 0:00:00:52 0.01% (ETA: 2025-11-22 11:59) 0.01916g/s 42.31p/s 150.8c/s 150.8C/s bamboo..abcdefgh
```


Kali - Internal Workstation on CY301-KPATE030
1 2 3 4
(genmon)XXX 20:01
root@kali: ~
File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# john --show kpate030-HASH
user1:1234:20409:0:99999:7:::

1 password hash cracked, 0 left

┌──(root㉿kali)-[~]
└─# █
```

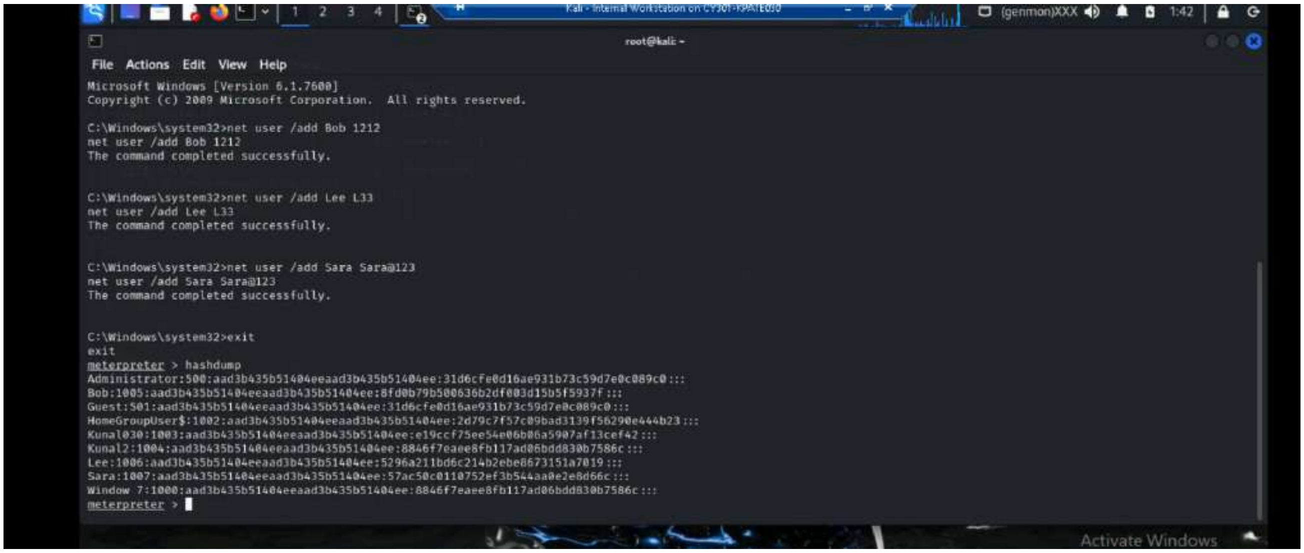
Kunal Patel

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords (OR you may create users using net users \add command as you did in lab-4-task-c). Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

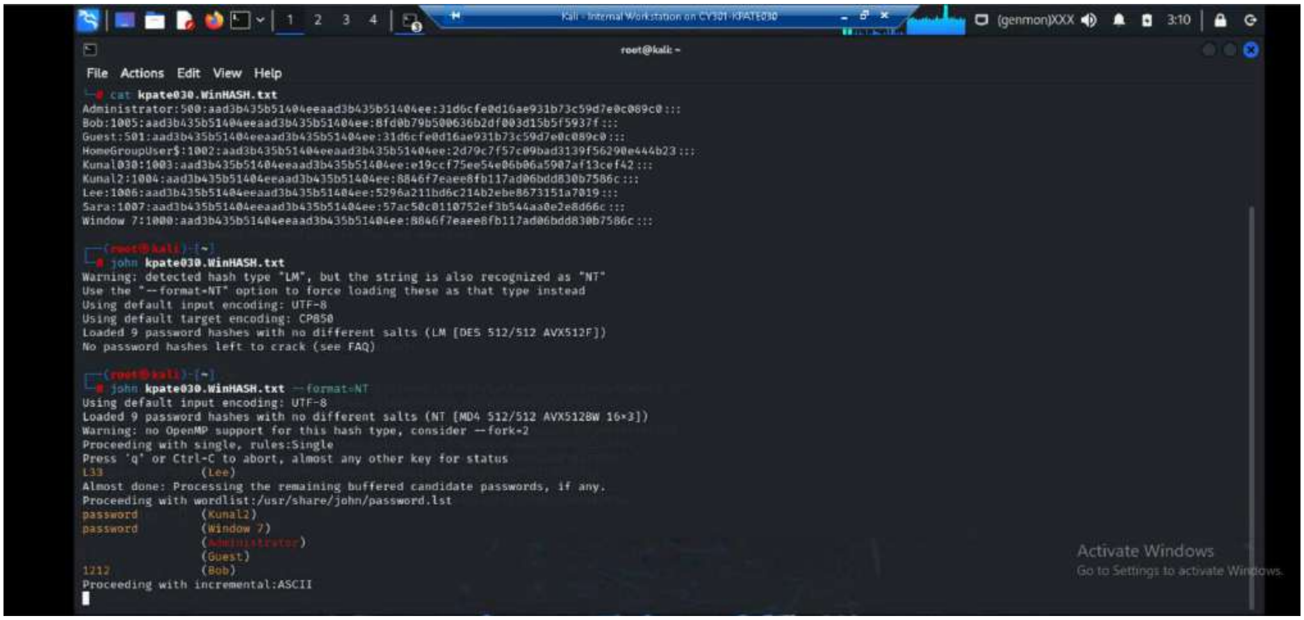
Now, complete the following tasks:

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


Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
1:42
root@kali: ~
File Actions Edit View Help
Activate Windows

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net user /add Bob 1212
net user /add Bob 1212
The command completed successfully.


C:\Windows\system32>net user /add Lee L33
net user /add Lee L33
The command completed successfully.


C:\Windows\system32>net user /add Sara Sara@123
net user /add Sara Sara@123
The command completed successfully.


C:\Windows\system32>exit
exit
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bob:1005:aad3b435b51404eeaad3b435b51404ee:8fd0b79b500636b2df003d15b5f5937f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Kunal030:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Kunal2:1004:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Lee:1006:aad3b435b51404eeaad3b435b51404ee:5296a211bd6c214b2ebe8673151a7019:::
Sara:1007:aad3b435b51404eeaad3b435b51404ee:57ac50c0110752ef3b544aa0e2e8d66c:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > █
```

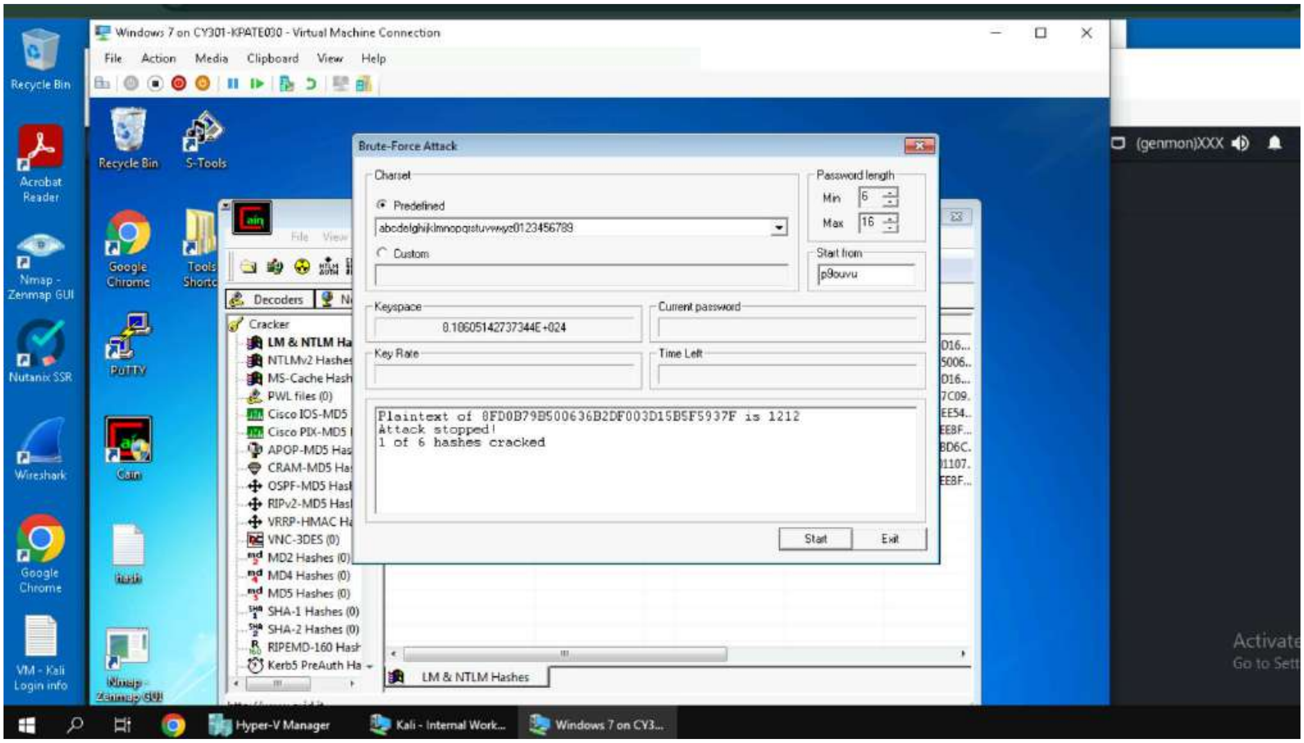
2. **10 points.** Save the password hashes into a file named "**your_midas.WinHASH**" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run **John the ripper** for **10 minutes** to crack the windows users' passwords (You MUST crack at least one password in order to complete this assignment.).


Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
3:10
root@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
└─# cat kpate030.WinHASH.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Bob:1005:aad3b435b51404eeaad3b435b51404ee:8fd0b79b500636b2df003d15b5f5937f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Kunal030:1003:aad3b435b51404eeaad3b435b51404ee:e19ccf75ee54e06b06a5907af13cef42:::
Kunal2:1004:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Lee:1006:aad3b435b51404eeaad3b435b51404ee:5296a211bd6c214b2ebe8673151a7019:::
Sara:1007:aad3b435b51404eeaad3b435b51404ee:57ac50c0110752ef3b544aa0e2e8d66c:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::

┌──(root㉿kali)-[~]
└─# john kpate030.WinHASH.txt
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 9 password hashes with no different salts (LM [DES 512/512 AVX512F])
No password hashes left to crack (see FAQ)

┌──(root㉿kali)-[~]
└─# john kpate030.WinHASH.txt --format=NT
Using default input encoding: UTF-8
Loaded 9 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
L33              (Lee)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (Kunal2)
password         (Window 7)
                 (Administrator)
                 (Guest)
1212             (Bob)
Proceeding with incremental:ASCII
█
```

Kunal Patel

3. 10 points. Launch/open the password cracking tool, **Cain and Abel** in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).



Windows 7 on CY301-KPATE030 - Virtual Machine Connection

Brute-Force Attack

Charset: ● Predefined abcdefghijklmnopqrstuvwxyz0123456789 ○ Custom

Password length: Min 6 Max 16

Start from: p9ouvu

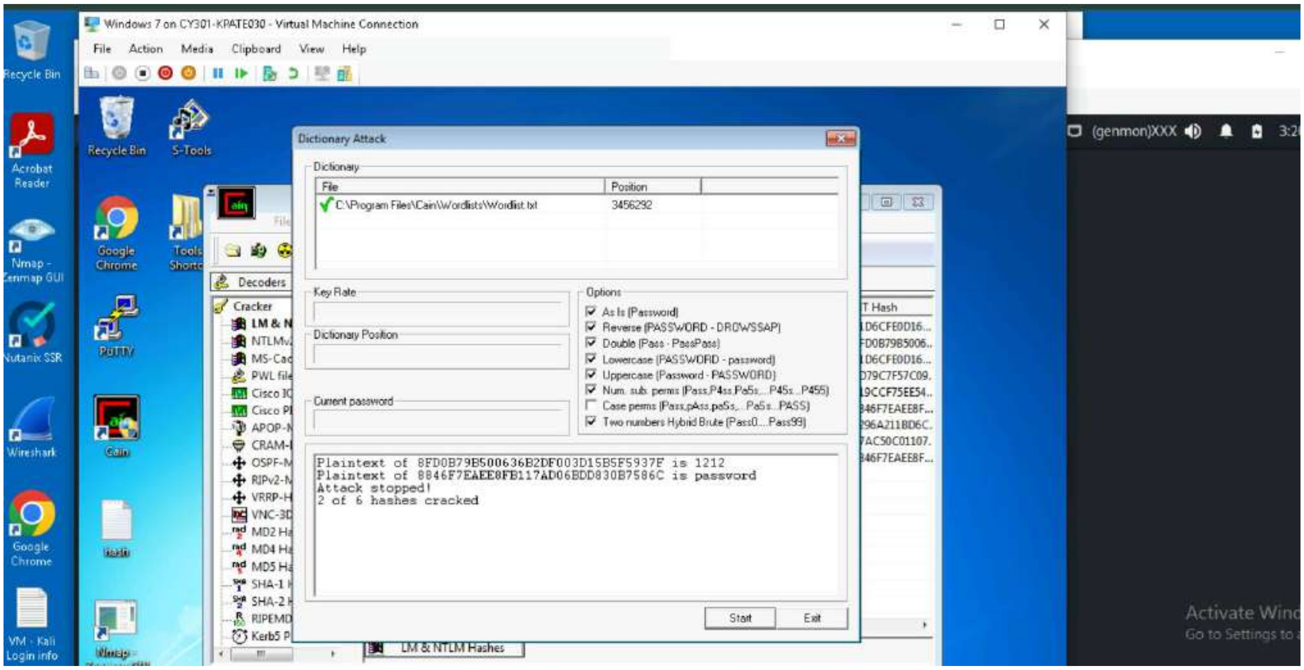
Keyspace: 8.18605142737344E+024

Current password:

Key Rate:

Time Left:

```
Plaintext of 8FD0B79B500636B2DF003D15B5F5937F is 1212
Attack stopped!
1 of 6 hashes cracked
```



Windows 7 on CY301-KPATE030 - Virtual Machine Connection

Dictionary Attack

Dictionary

File	Position
✓ C:\Program Files\Cain\Wordlists\Wordlist.txt	3456292

Key Rate:

Dictionary Position:

Current password:

Options
- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- □ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0...Pass99)

```
Plaintext of 8FD0B79B500636B2DF003D15B5F5937F is 1212
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Attack stopped!
2 of 6 hashes cracked
```

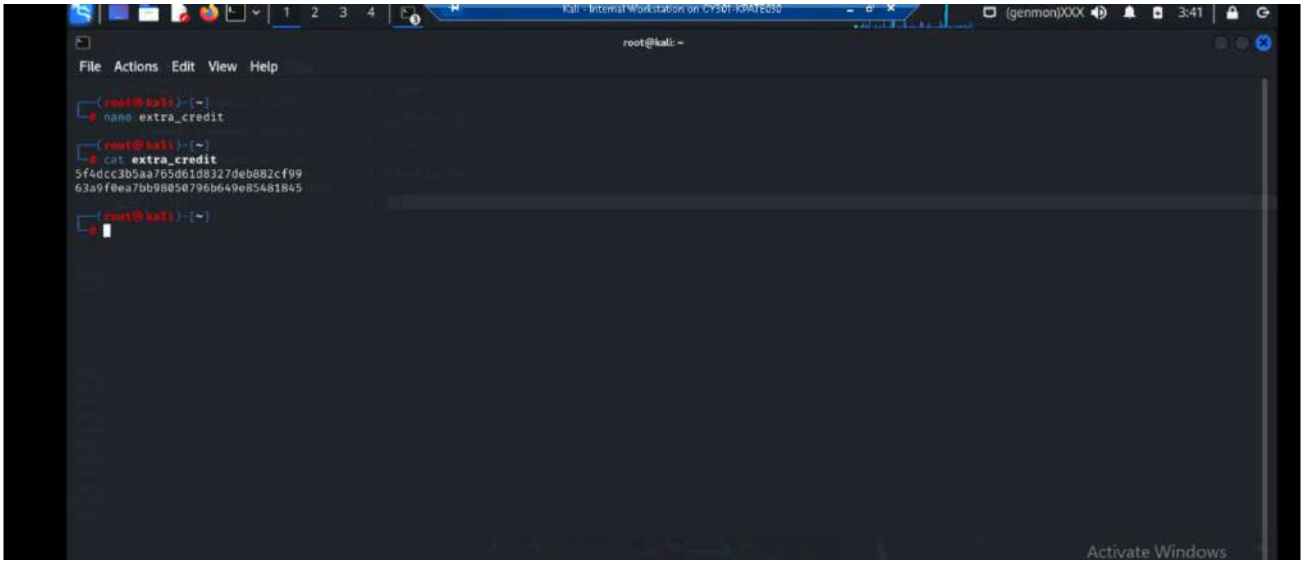
NOTE: Please refer to the class lecture to learn how to add users in windows7 and using Cain tool for windows password cracking.

Kunal Patel

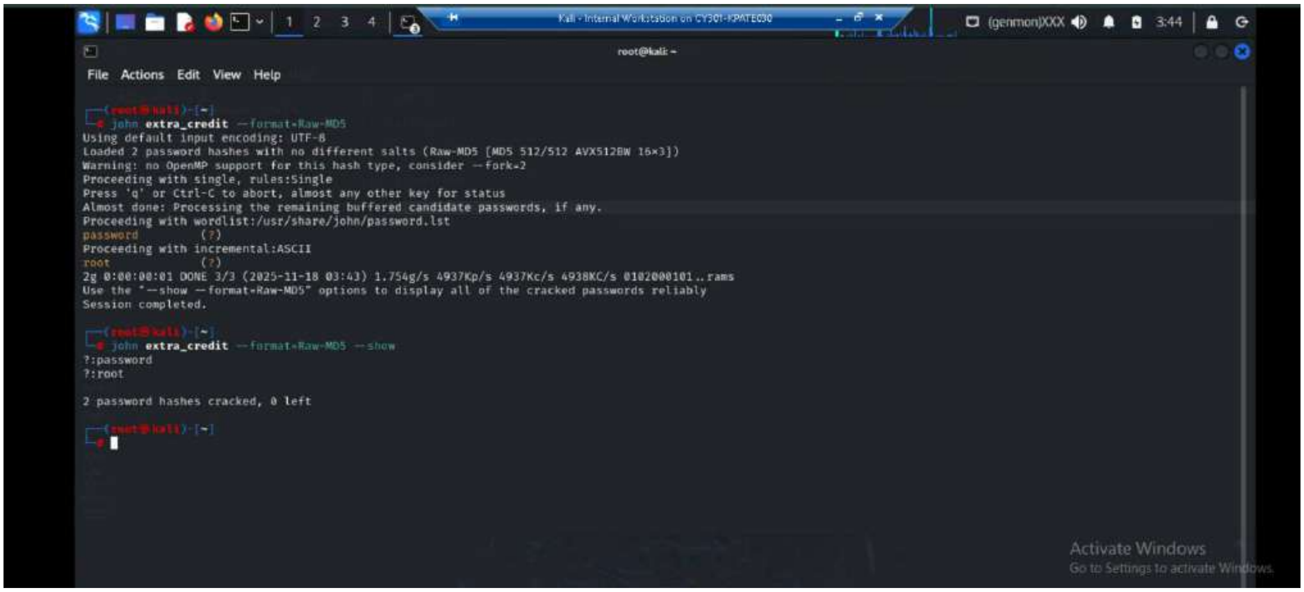
Extra credit: (10 points)

Search the proper format in John the Ripper to crack the following **MD5** hashes (use the ***--list=formats*** option to list all supported formats). Show your steps and results.

1. 5f4dcc3b5aa765d61d8327deb882cf99 = **password**
2. 63a9f0ea7bb98050796b649e85481845 = **root**



```
┌──(root㉿kali)-[~]
└─# nano extra_credit

┌──(root㉿kali)-[~]
└─# cat extra_credit
5f4dcc3b5aa765d61d8327deb882cf99
63a9f0ea7bb98050796b649e85481845

┌──(root㉿kali)-[~]
└─# 
```

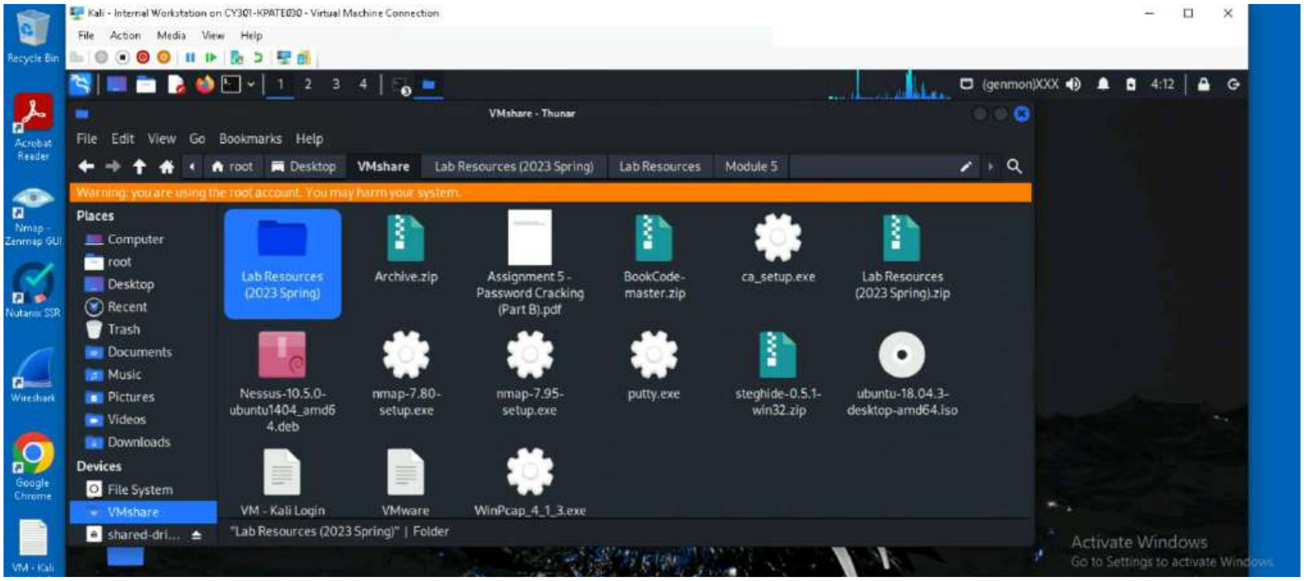

Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
3:44
root@kali: ~
File
Actions
Edit
View
Help
Activate Windows
Go to Settings to activate Windows.

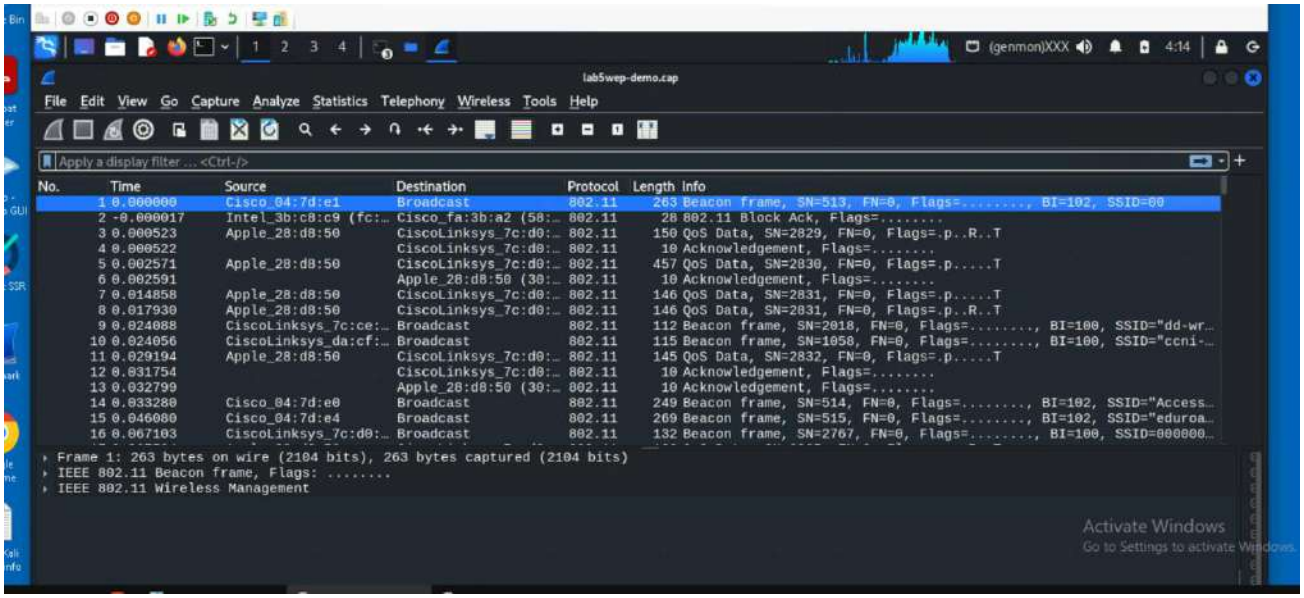
```
┌──(root㉿kali)-[~]
└─# john extra_credit --format=Raw-MD5
Using default input encoding: UTF-8
Loaded 2 password hashes with no different salts (Raw-MD5 [MD5 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (?)
Proceeding with incremental:ASCII
root             (?)
2g 0:00:00:01 DONE 3/3 (2025-11-18 03:43) 1.754g/s 4937Kp/s 4937Kc/s 4938KC/s 0102000101..rams
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[~]
└─# john extra_credit --format=Raw-MD5 --show
?:password
?:root

2 password hashes cracked, 0 left

┌──(root㉿kali)-[~]
└─# 
```

Kunal Patel

Assignment 5 – Part-2: Wi-Fi Password Cracking

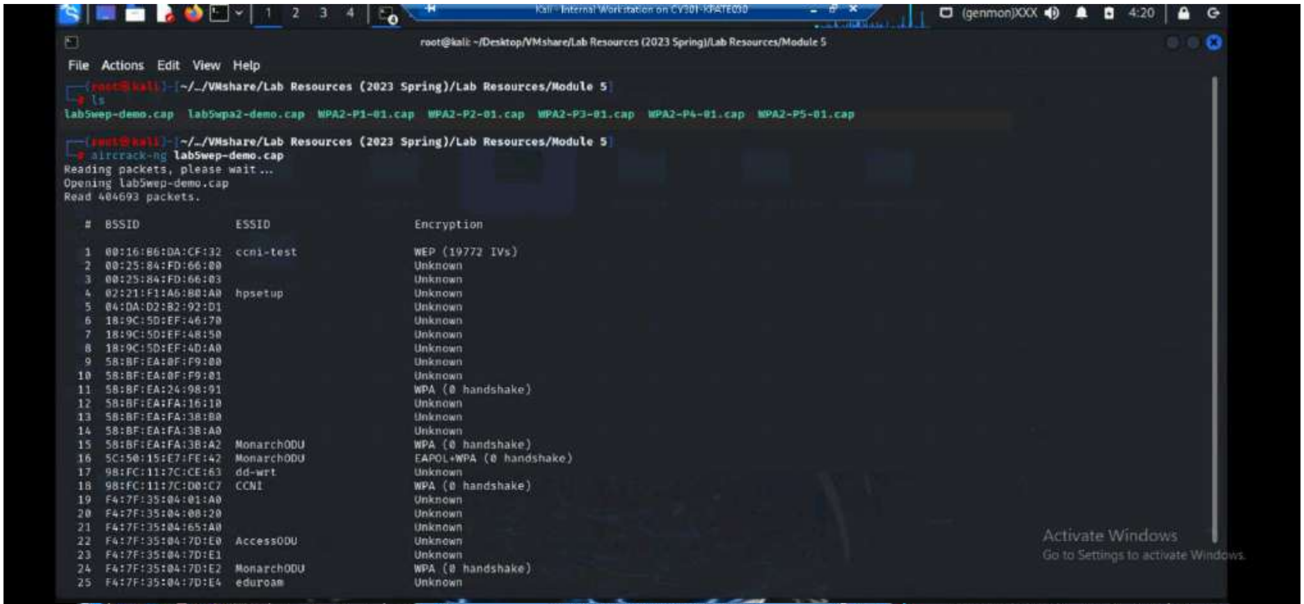
Task C: 20 points
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected
traffic.
1. Decrypt the lab5wep-demo. cap file (5 points) and perform a detailed traffic analysis (5 points)


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
VMshare - Thunar
File Edit View Go Bookmarks Help
root Desktop VMshare Lab Resources (2023 Spring) Lab Resources Module 5
Warning: you are using the root account. You may harm your system.
Places
Computer
root
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
VMshare
shared-dri...
Lab Resources (2023 Spring)
Archive.zip
Assignment 5 - Password Cracking (Part B).pdf
BookCode-master.zip
ca_setup.exe
Lab Resources (2023 Spring).zip
Nessus-10.5.0-ubuntu1404_amd64.deb
nmap-7.80-setup.exe
nmap-7.95-setup.exe
putty.exe
steghide-0.5.1-win32.zip
ubuntu-18.04.3-desktop-amd64.iso
VM - Kali Login
VMware
WinPcap_4_1_3.exe
"Lab Resources (2023 Spring)" | Folder
(genmon)XXX 4:12
Activate Windows
Go to Settings to activate Windows.

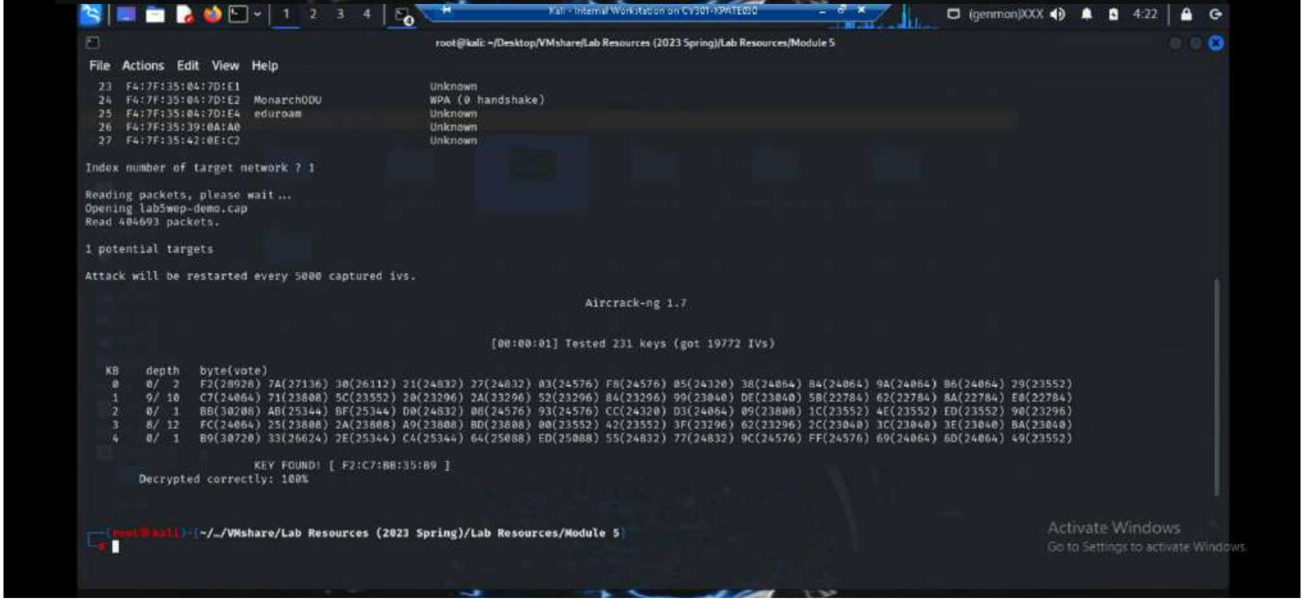

lab5wep-demo.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
(genmon)XXX 4:14
Activate Windows
Go to Settings to activate Windows.

```
No.   Time        Source                  Destination              Protocol Length Info
    1 0.000000    Cisco_04:7d:e1          Broadcast                802.11     263 Beacon frame, SN=513, FN=0, Flags=........, BI=102, SSID=00
    2 -0.000017   Intel_3b:c8:c9 (fc:…    Cisco_fa:3b:a2 (58:…     802.11      28 802.11 Block Ack, Flags=........
    3 0.000523    Apple_28:d8:50          CiscoLinksys_7c:d0:…     802.11     150 QoS Data, SN=2829, FN=0, Flags=.p..R..T
    4 0.000522                            CiscoLinksys_7c:d0:…     802.11      10 Acknowledgement, Flags=........
    5 0.002571    Apple_28:d8:50          CiscoLinksys_7c:d0:…     802.11     457 QoS Data, SN=2830, FN=0, Flags=.p.....T
    6 0.002591                            Apple_28:d8:50 (30:…     802.11      10 Acknowledgement, Flags=........
    7 0.014858    Apple_28:d8:50          CiscoLinksys_7c:d0:…     802.11     146 QoS Data, SN=2831, FN=0, Flags=.p.....T
    8 0.017930    Apple_28:d8:50          CiscoLinksys_7c:d0:…     802.11     146 QoS Data, SN=2831, FN=0, Flags=.p..R..T
    9 0.024088    CiscoLinksys_7c:ce:…    Broadcast                802.11     112 Beacon frame, SN=2018, FN=0, Flags=........, BI=100, SSID="dd-wr…
   10 0.024056    CiscoLinksys_da:cf:…    Broadcast                802.11     115 Beacon frame, SN=1058, FN=0, Flags=........, BI=100, SSID="ccni-…
   11 0.029194    Apple_28:d8:50          CiscoLinksys_7c:d0:…     802.11     145 QoS Data, SN=2832, FN=0, Flags=.p.....T
   12 0.031754                            CiscoLinksys_7c:d0:…     802.11      10 Acknowledgement, Flags=........
   13 0.032799                            Apple_28:d8:50 (30:…     802.11      10 Acknowledgement, Flags=........
   14 0.033280    Cisco_04:7d:e0          Broadcast                802.11     249 Beacon frame, SN=514, FN=0, Flags=........, BI=102, SSID="Access…
   15 0.046080    Cisco_04:7d:e4          Broadcast                802.11     269 Beacon frame, SN=515, FN=0, Flags=........, BI=102, SSID="eduroa…
   16 0.067103    CiscoLinksys_7c:d0:…    Broadcast                802.11     132 Beacon frame, SN=2767, FN=0, Flags=........, BI=100, SSID=000000…

› Frame 1: 263 bytes on wire (2104 bits), 263 bytes captured (2104 bits)
› IEEE 802.11 Beacon frame, Flags: ........
› IEEE 802.11 Wireless Management
```

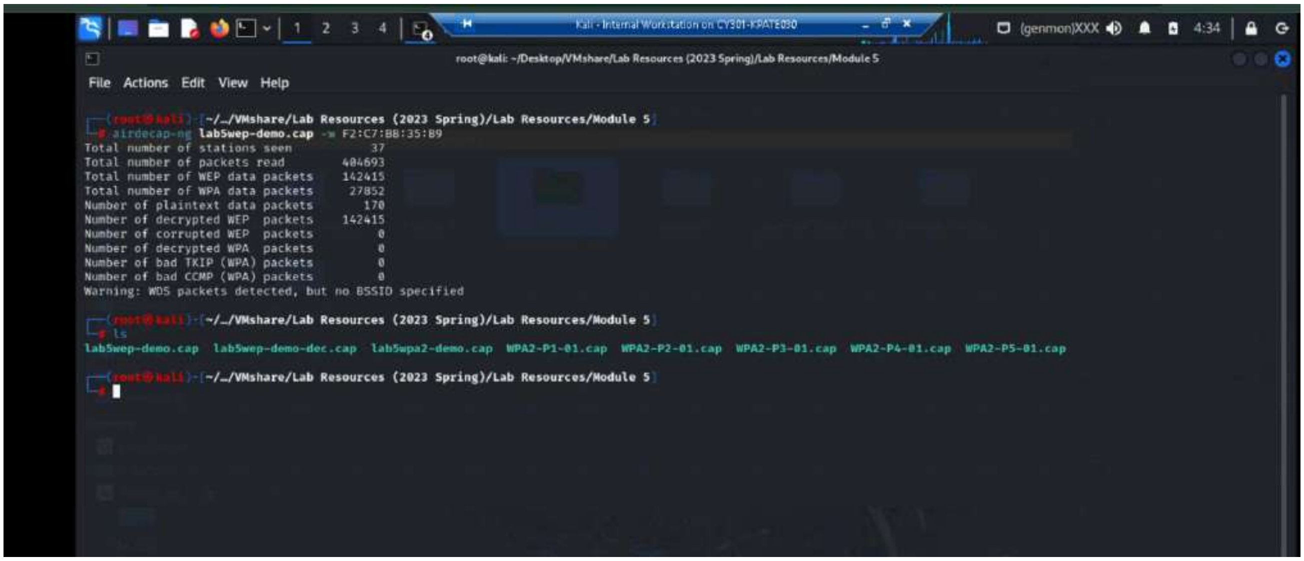
Kunal Patel


Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
4:20
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap  lab5wpa2-demo.cap  WPA2-P1-01.cap  WPA2-P2-01.cap  WPA2-P3-01.cap  WPA2-P4-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/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
  13  58:BF:EA:FA:38:B0                            Unknown
  14  58:BF:EA:FA:3B:A0                            Unknown
  15  58:BF:EA:FA:3B: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                    Unknown
  18  98:FC:11:7C:D0:C7  CCNI                      WPA (0 handshake)
  19  F4:7F:35:04:01:A0                            Unknown
  20  F4:7F:35:04:08:20                            Unknown
  21  F4:7F:35:04:65:A0                            Unknown
  22  F4:7F:35:04:7D:E0  AccessODU                 Unknown
  23  F4:7F:35:04:7D:E1                            Unknown
  24  F4:7F:35:04:7D:E2  MonarchODU                WPA (0 handshake)
  25  F4:7F:35:04:7D:E4  eduroam                   Unknown
```

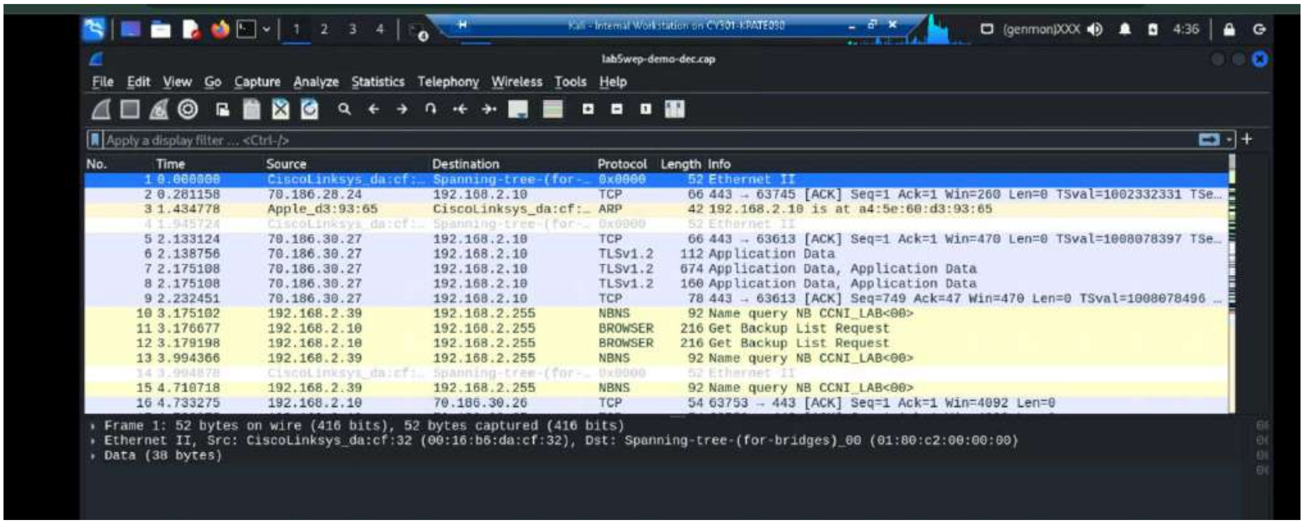

Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
4:22
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
  23  F4:7F:35:04:7D:E1                            Unknown
  24  F4:7F:35:04:7D:E2  MonarchODU                WPA (0 handshake)
  25  F4:7F:35:04:7D:E4  eduroam                   Unknown
  26  F4:7F:35:39:0A:A0                            Unknown
  27  F4:7F:35:42:0E:C2                            Unknown

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


                              [00:00:01] 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) B4(24064) 9A(24064) B6(24064) 29(23552)
    1    9/ 10   C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040) 5B(22784) 62(22784) 8A(22784) E0(22784)
    2    0/  1   BB(30208) AB(25344) BF(25344) D0(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808) 1C(23552) 4E(23552) ED(23552) 90(23296)
    3    8/ 12   FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 00(23552) 42(23552) 3F(23296) 62(23296) 2C(23040) 3C(23040) 3E(23040) BA(23040)
    4    0/  1   B9(30720) 33(26624) 2E(25344) C4(25344) 64(25088) ED(25088) 55(24832) 77(24832) 9C(24576) FF(24576) 69(24064) 6D(24064) 49(23552)

                        KEY FOUND! [ F2:C7:BB:35:B9 ]
        Decrypted correctly: 100%


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# 
```


Kali - Internal Workstation on CY301-KPATE030
(genmon)XXX
4:34
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help

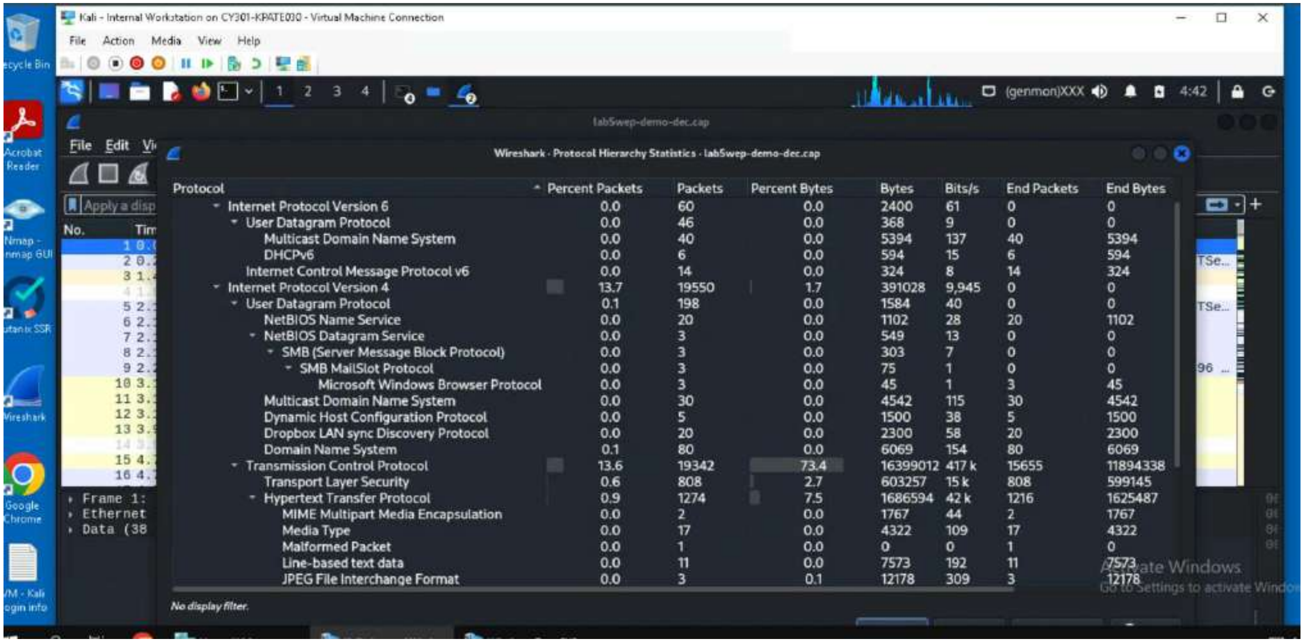
```
┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng lab5wep-demo.cap -w F2:C7:BB:35:B9
Total number of stations seen            37
Total number of packets read         404693
Total number of WEP data packets     142415
Total number of WPA data packets      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)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap  lab5wep-demo-dec.cap  lab5wpa2-demo.cap  WPA2-P1-01.cap  WPA2-P2-01.cap  WPA2-P3-01.cap  WPA2-P4-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# 
```

Kunal Patel



lab5wep-demo-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 0.000000   CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000     52 Ethernet II
   2 0.281158   70.186.28.24         192.168.2.10         TCP        66 443 → 63745 [ACK] Seq=1 Ack=1 Win=260 Len=0 TSval=1002332331 TSe…
   3 1.434778   Apple_d3:93:65       CiscoLinksys_da:cf:… ARP        42 192.168.2.10 is at a4:5e:60:d3:93:65
   4 1.945724   CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000     52 Ethernet II
   5 2.133124   70.186.30.27         192.168.2.10         TCP        66 443 → 63613 [ACK] Seq=1 Ack=1 Win=470 Len=0 TSval=1008078397 TSe…
   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=470 Len=0 TSval=1008078496 …
  10 3.175102   192.168.2.39         192.168.2.255        NBNS       92 Name query NB CCNI_LAB<00>
  11 3.176677   192.168.2.10         192.168.2.255        BROWSER   216 Get Backup List Request
  12 3.179198   192.168.2.10         192.168.2.255        BROWSER   216 Get Backup List Request
  13 3.994366   192.168.2.39         192.168.2.255        NBNS       92 Name query NB CCNI_LAB<00>
  14 3.994878   CiscoLinksys_da:cf:… Spanning-tree-(for-… 0x0000     52 Ethernet II
  15 4.710718   192.168.2.39         192.168.2.255        NBNS       92 Name query NB CCNI_LAB<00>
  16 4.733275   192.168.2.10         70.186.30.26         TCP        54 63753 → 443 [ACK] Seq=1 Ack=1 Win=4092 Len=0

› Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)
› Ethernet II, Src: CiscoLinksys_da:cf:32 (00:16:b6:da:cf:32), Dst: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
› Data (38 bytes)
```



Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
lab5wep-demo-dec.cap
Wireshark · Protocol Hierarchy Statistics · lab5wep-demo-dec.cap

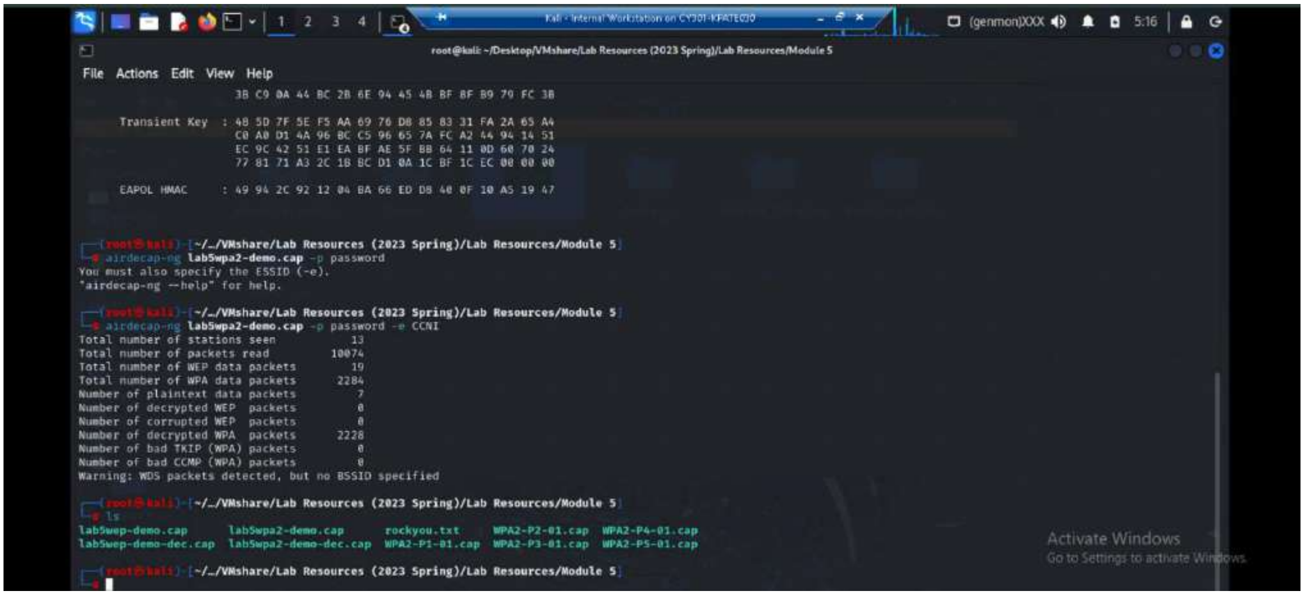
Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes
Internet Protocol Version 6	0.0	60	0.0	2400	61	0	0
User Datagram Protocol	0.0	46	0.0	368	9	0	0
Multicast Domain Name System	0.0	40	0.0	5394	137	40	5394
DHCPv6	0.0	6	0.0	594	15	6	594
Internet Control Message Protocol v6	0.0	14	0.0	324	8	14	324
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	1102
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	4542
Dynamic Host Configuration Protocol	0.0	5	0.0	1500	38	5	1500
Dropbox LAN sync Discovery Protocol	0.0	20	0.0	2300	58	20	2300
Domain Name System	0.1	80	0.0	6069	154	80	6069
Transmission Control Protocol	13.6	19342	73.4	16399012	417 k	15655	11894338
Transport Layer Security	0.6	808	2.7	603257	15 k	808	599145
Hypertext Transfer Protocol	0.9	1274	7.5	1686594	42 k	1216	1625487
MIME Multipart Media Encapsulation	0.0	2	0.0	1767	44	2	1767
Media Type	0.0	17	0.0	4322	109	17	4322
Malformed Packet	0.0	1	0.0	0	0	1	0
Line-based text data	0.0	11	0.0	7573	192	11	7573
JPEG File Interchange Format	0.0	3	0.1	12178	309	3	12178

No display filter.

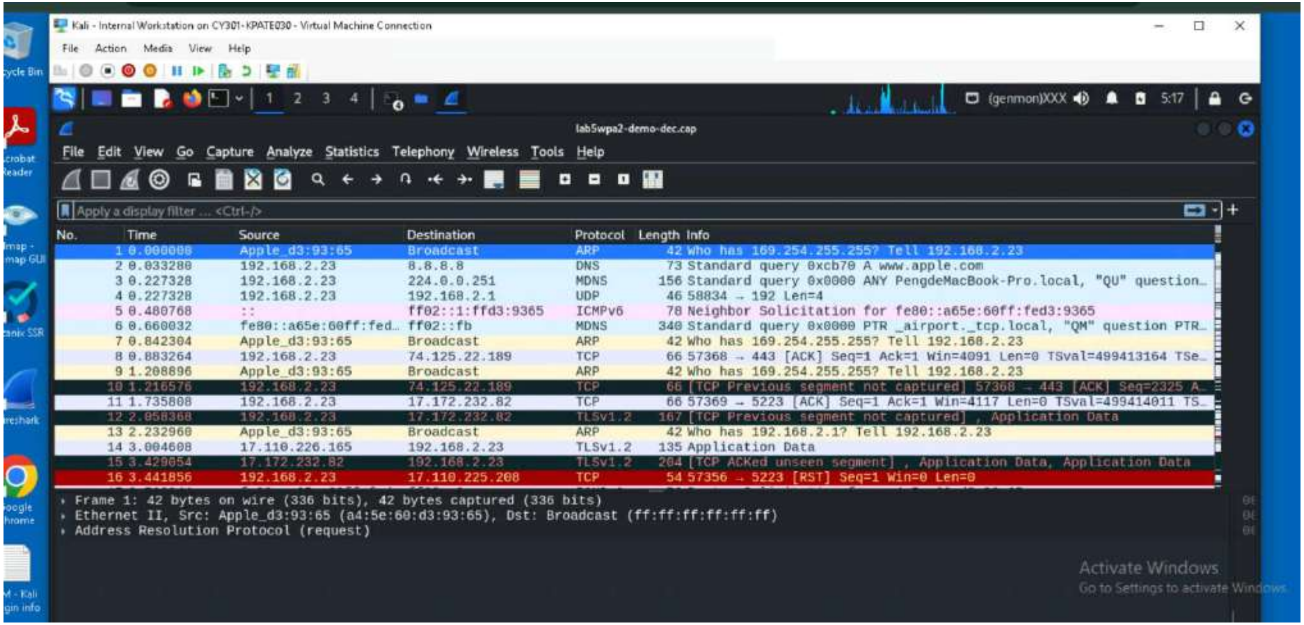
To decrypt the file, I first copied the Lab Resources folder onto my internal Kali VM desktop. I opened the **lab5wep-demo.cap** file in Wireshark and ran a **Protocol Hierarchy Statistics** analysis to see what packets were visible in the encrypted capture. Then, using the cd and ls commands, I navigated to the correct directory and ran aircrack-ng lab5wep-demo.cap to analyze the traffic. After setting the network index to **1**, I obtained the WEP key. I then used the command airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap to decrypt the capture file. Once the file was decrypted, I opened it in Wireshark, enabled the display of decrypted traffic, and ran another Protocol Hierarchy Statistics analysis.

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

Kunal Patel

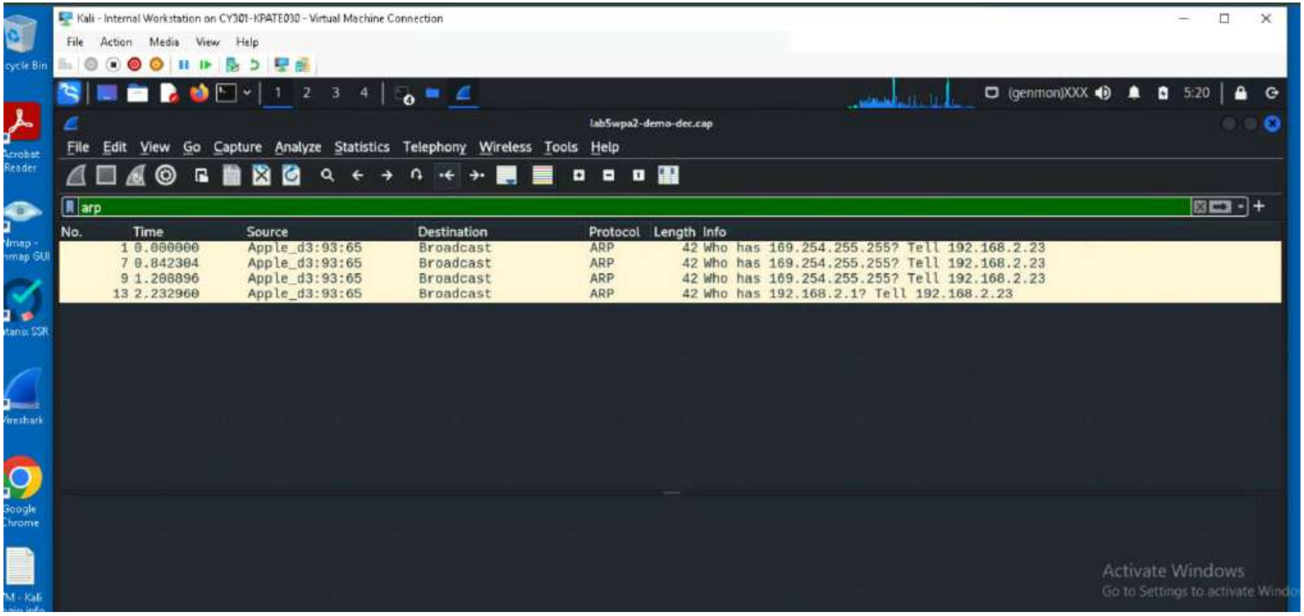

root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.

```
                   3B C9 0A 44 BC 2B 6E 94 45 4B BF BF 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 BB 64 11 0D 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 BA 66 ED D8 40 0F 10 A5 19 47


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng lab5wpa2-demo.cap -p password
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng lab5wpa2-demo.cap -p password -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
Number of bad CCMP (WPA) packets          0
Warning: WDS packets detected, but no BSSID specified

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# ls
lab5wep-demo.cap      lab5wpa2-demo.cap      rockyou.txt      WPA2-P2-01.cap  WPA2-P4-01.cap
lab5wep-demo-dec.cap  lab5wpa2-demo-dec.cap  WPA2-P1-01.cap   WPA2-P3-01.cap  WPA2-P5-01.cap

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# 
```


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
lab5wpa2-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
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 PengdeMacBook-Pro.local, "QU" question…
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:60ff:fed3:9365
6	0.660032	fe80::a65e:60ff:fed…	ff02::fb	MDNS	340	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR…
7	0.842304	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
8	0.883264	192.168.2.23	74.125.22.189	TCP	66	57368 → 443 [ACK] Seq=1 Ack=1 Win=4091 Len=0 TSval=499413164 TSe…
9	1.208896	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
10	1.216576	192.168.2.23	74.125.22.189	TCP	66	[TCP Previous segment not captured] 57368 → 443 [ACK] Seq=2325 A…
11	1.735808	192.168.2.23	17.172.232.82	TCP	66	57369 → 5223 [ACK] Seq=1 Ack=1 Win=4117 Len=0 TSval=499414011 TS…
12	2.058368	192.168.2.23	17.172.232.82	TLSv1.2	167	[TCP Previous segment not captured] , Application Data
13	2.232960	Apple_d3:93:65	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.23
14	3.004608	17.110.226.165	192.168.2.23	TLSv1.2	135	Application Data
15	3.429054	17.172.232.82	192.168.2.23	TLSv1.2	204	[TCP ACKed unseen segment] , Application Data, Application Data
16	3.441856	192.168.2.23	17.110.225.208	TCP	54	57356 → 5223 [RST] Seq=1 Win=0 Len=0

```
› 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)
```


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
lab5wpa2-demo-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Activate Windows
Go to Settings to activate Windows

arp

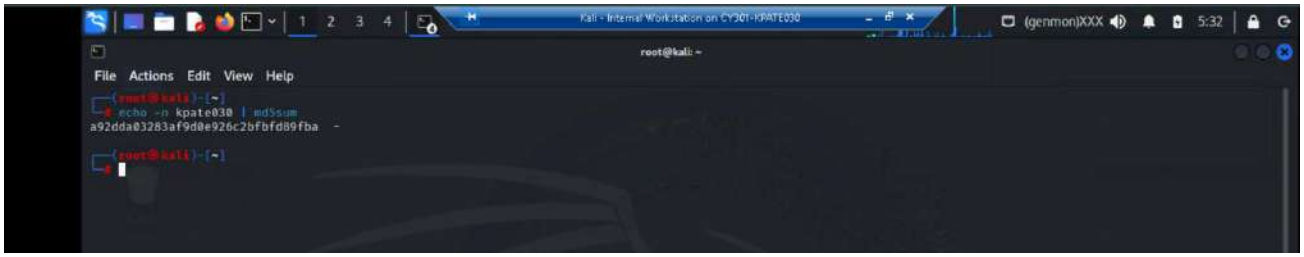
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
7	0.842304	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
9	1.208896	Apple_d3:93:65	Broadcast	ARP	42	Who has 169.254.255.255? Tell 192.168.2.23
13	2.232960	Apple_d3:93:65	Broadcast	ARP	42	Who has 192.168.2.1? Tell 192.168.2.23

Kunal Patel

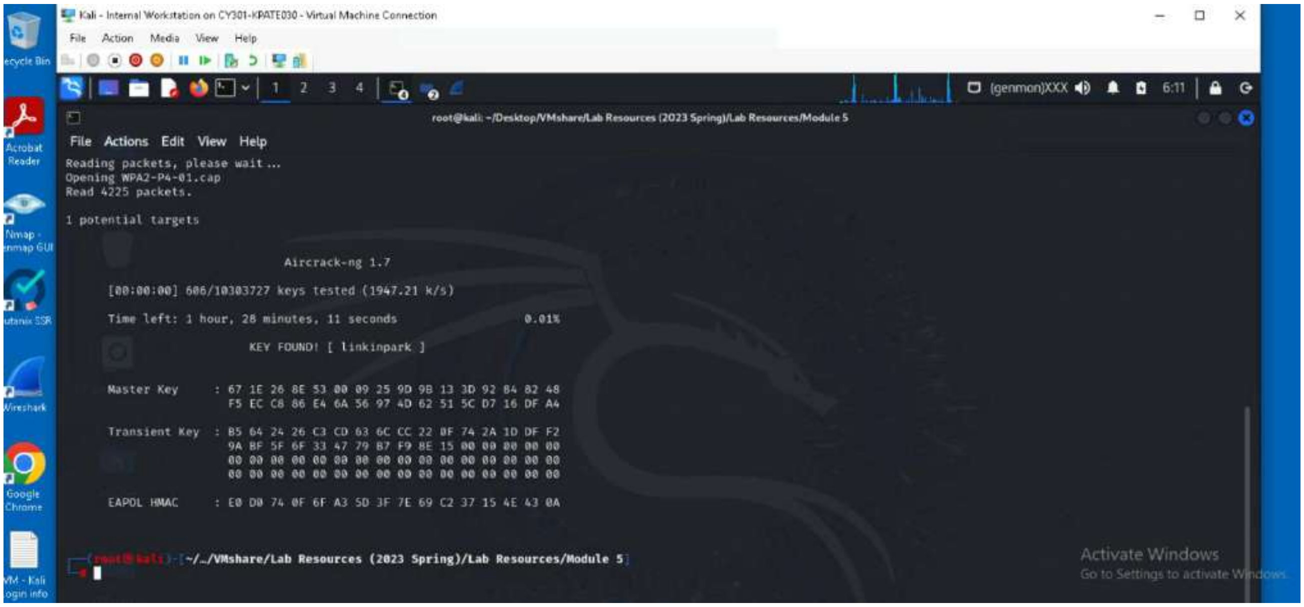
To begin, I opened Wireshark and loaded the **lab5wpa2-demo.cap** file to view the encrypted traffic, then performed a Protocol Hierarchy Statistical Analysis, which showed that the packets were classified under IEEE 802.11 Wireless LAN. After switching back to the terminal, and already being in the correct directory, I used the ls command to review the files and ran aircrack-ng lab5wpa2-demo.cap, setting the index number to 4. I then copied the default wordlist into the directory using cp / root/rockyou.txt and attempted to crack the key again with aircrack-ng lab5wpa2-demo.cap -w rockyou.txt. Using ls to check my progress, I set the index to 4 again and successfully retrieved the WPA2 key, which was “password.” I proceeded with decryption using the command airdecap-ng -p password lab5wpa2-demo.cap -e CCNI, then confirmed my files with ls and opened the decrypted capture in Wireshark using wireshark lab5wpa2-demo-dec.cap. Once opened, I examined the decrypted traffic and performed another Protocol Hierarchy Statistical Analysis to review the packet structure. Lastly, I filter the arp result to be curious about it.

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."

My hash file end with letter A, so I am picking up WPA2-P4-01.cap

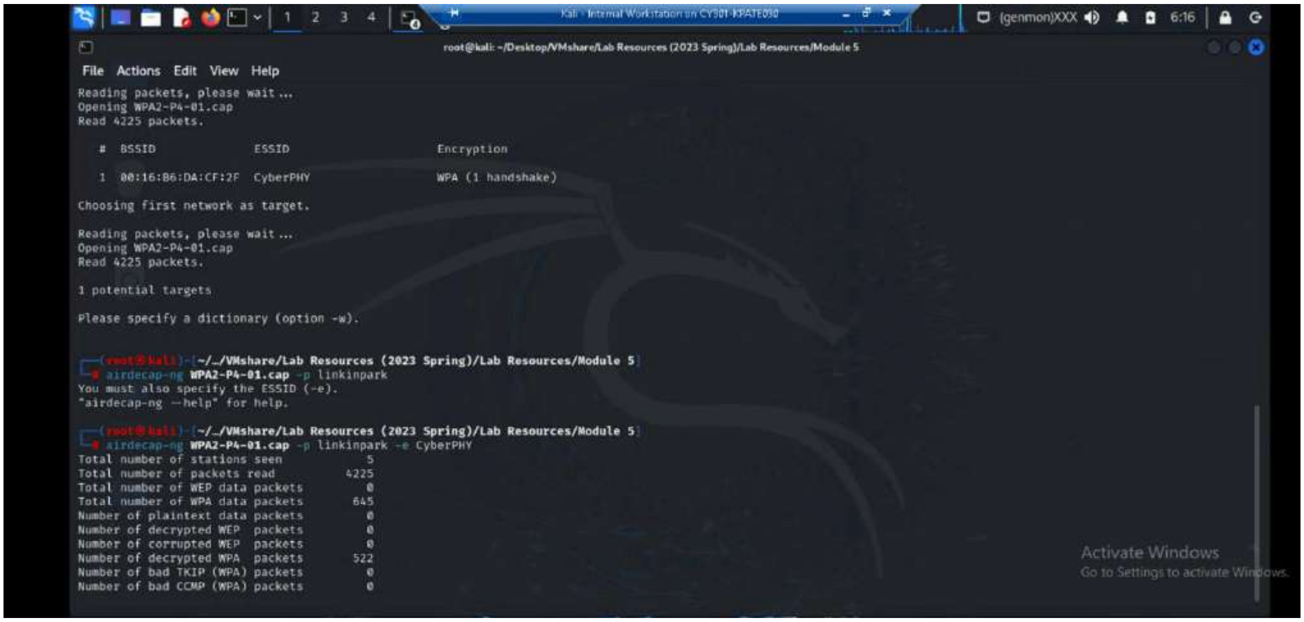


```
┌──(root㉿kali)-[~]
└─# echo -n kpate030 | md5sum
a92dda03283af9d0e926c2bfbfd89fba  -

┌──(root㉿kali)-[~]
└─# 
```



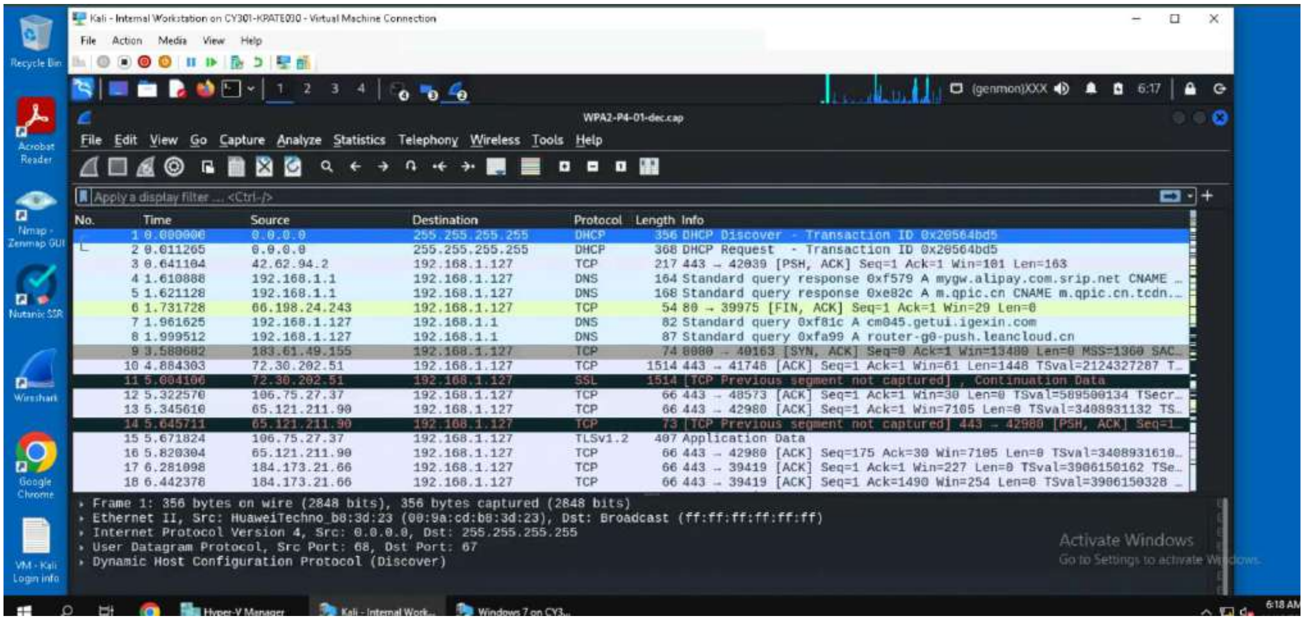
```
Reading packets, please wait...
Opening WPA2-P4-01.cap
Read 4225 packets.

1 potential targets


                               Aircrack-ng 1.7

      [00:00:00] 606/10303727 keys tested (1947.21 k/s)

      Time left: 1 hour, 28 minutes, 11 seconds                 0.01%

                          KEY FOUND! [ linkinpark ]


      Master Key     : 67 1E 26 8E 53 00 09 25 9D 9B 13 3D 92 84 82 48
                       F5 EC C8 86 E4 6A 56 97 4D 62 51 5C D7 16 DF A4

      Transient Key  : B5 64 24 26 C3 CD 63 6C CC 22 0F 74 2A 1D DF F2
                       9A BF 5F 6F 33 47 79 B7 F9 8E 15 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : E0 D0 74 0F 6F A3 5D 3F 7E 69 C2 37 15 4E 43 0A


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# 
```

Kunal Patel



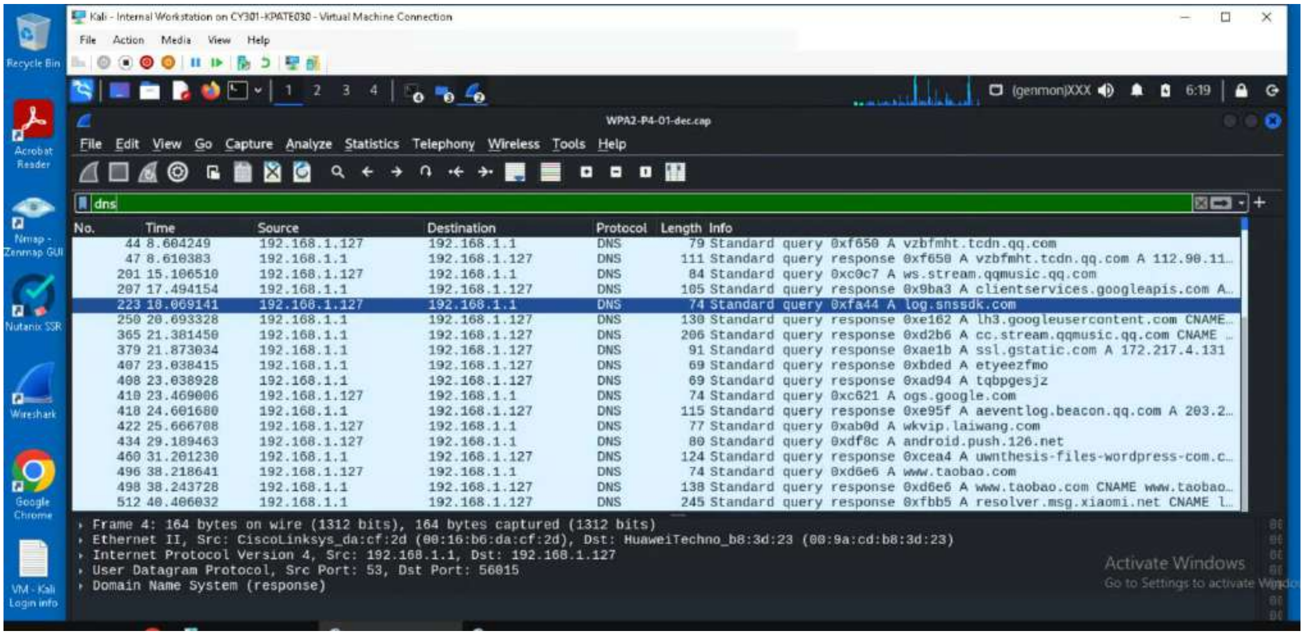
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help

```
Reading packets, please wait ...
Opening WPA2-P4-01.cap
Read 4225 packets.

   #  BSSID              ESSID                     Encryption

   1  00:16:B6:DA:CF:2F  CyberPHY                  WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait ...
Opening WPA2-P4-01.cap
Read 4225 packets.

1 potential targets

Please specify a dictionary (option -w).


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng WPA2-P4-01.cap -p linkinpark
You must also specify the ESSID (-e).
"airdecap-ng --help" for help.

┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# airdecap-ng WPA2-P4-01.cap -p linkinpark -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
```



Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
WPA2-P4-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Kali - Internal Work...
Windows 7 on CY3...

```
No.   Time       Source          Destination      Protocol  Length Info
    1 0.000000   0.0.0.0         255.255.255.255  DHCP       356 DHCP Discover - Transaction ID 0x20564bd5
    2 0.011265   0.0.0.0         255.255.255.255  DHCP       368 DHCP Request  - Transaction ID 0x20564bd5
    3 0.641104   42.62.94.2      192.168.1.127    TCP        217 443 → 42039 [PSH, ACK] Seq=1 Ack=1 Win=101 Len=163
    4 1.610888   192.168.1.1     192.168.1.127    DNS        164 Standard query response 0xf579 A mygw.alipay.com.srip.net CNAME …
    5 1.621128   192.168.1.1     192.168.1.127    DNS        168 Standard query response 0xe82c A m.qpic.cn CNAME m.qpic.cn.tcdn.…
    6 1.731728   66.198.24.243   192.168.1.127    TCP         54 80 → 39975 [FIN, ACK] Seq=1 Ack=1 Win=29 Len=0
    7 1.961625   192.168.1.127   192.168.1.1      DNS         82 Standard query 0xf81c A cm045.getui.igexin.com
    8 1.999512   192.168.1.127   192.168.1.1      DNS         87 Standard query 0xfa99 A router-g0-push.leancloud.cn
    9 3.580682   183.61.49.155   192.168.1.127    TCP         74 8080 → 40163 [SYN, ACK] Seq=0 Ack=1 Win=13480 Len=0 MSS=1360 SAC…
   10 4.884303   72.30.202.51    192.168.1.127    TCP       1514 443 → 41748 [ACK] Seq=1 Ack=1 Win=61 Len=1448 TSval=2124327287 T…
   11 5.004106   72.30.202.51    192.168.1.127    SSL       1514 [TCP Previous segment not captured] , Continuation Data
   12 5.322570   106.75.27.37    192.168.1.127    TCP         66 443 → 48573 [ACK] Seq=1 Ack=1 Win=30 Len=0 TSval=589500134 TSecr…
   13 5.345610   65.121.211.90   192.168.1.127    TCP         66 443 → 42980 [ACK] Seq=1 Ack=1 Win=7105 Len=0 TSval=3408931132 TS…
   14 5.645711   65.121.211.90   192.168.1.127    TCP         73 [TCP Previous segment not captured] 443 → 42980 [PSH, ACK] Seq=1…
   15 5.671824   106.75.27.37    192.168.1.127    TLSv1.2    407 Application Data
   16 5.820304   65.121.211.90   192.168.1.127    TCP         66 443 → 42980 [ACK] Seq=175 Ack=30 Win=7105 Len=0 TSval=3408931610…
   17 6.281098   184.173.21.66   192.168.1.127    TCP         66 443 → 39419 [ACK] Seq=1 Ack=1 Win=227 Len=0 TSval=3906150162 TSe…
   18 6.442378   184.173.21.66   192.168.1.127    TCP         66 443 → 39419 [ACK] Seq=1 Ack=1490 Win=254 Len=0 TSval=3906150328 …

› Frame 1: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits)
› Ethernet II, Src: HuaweiTechno_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
› Dynamic Host Configuration Protocol (Discover)
```


Kali - Internal Workstation on CY301-KPATE030 - Virtual Machine Connection
File Action Media View Help
Recycle Bin
Acrobat Reader
Nmap - Zenmap GUI
Nutanix SSR
Wireshark
Google Chrome
VM - Kali Login info
1 2 3 4
(genmon)XXX
6:19
WPA2-P4-01-dec.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Activate Windows
Go to Settings to activate Windo

```
dns
```

```
No.     Time        Source          Destination     Protocol  Length Info
   44 8.604249    192.168.1.127   192.168.1.1     DNS        79 Standard query 0xf650 A vzbfmht.tcdn.qq.com
   47 8.610383    192.168.1.1     192.168.1.127   DNS       111 Standard query response 0xf650 A vzbfmht.tcdn.qq.com A 112.90.11…
  201 15.106510   192.168.1.127   192.168.1.1     DNS        84 Standard query 0xc0c7 A ws.stream.qqmusic.qq.com
  207 17.494154   192.168.1.1     192.168.1.127   DNS       105 Standard query response 0x9ba3 A clientservices.googleapis.com A…
  223 18.069141   192.168.1.127   192.168.1.1     DNS        74 Standard query 0xfa44 A log.snssdk.com
  250 20.693328   192.168.1.1     192.168.1.127   DNS       130 Standard query response 0xe162 A lh3.googleusercontent.com CNAME…
  365 21.381450   192.168.1.1     192.168.1.127   DNS       206 Standard query response 0xd2b6 A cc.stream.qqmusic.qq.com CNAME …
  379 21.873034   192.168.1.1     192.168.1.127   DNS        91 Standard query response 0xae1b A ssl.gstatic.com A 172.217.4.131
  407 23.038415   192.168.1.1     192.168.1.127   DNS        69 Standard query response 0xbded A etyeezfmo
  408 23.038928   192.168.1.1     192.168.1.127   DNS        69 Standard query response 0xad94 A tqbpgesjz
  410 23.469006   192.168.1.127   192.168.1.1     DNS        74 Standard query 0xc621 A ogs.google.com
  418 24.601680   192.168.1.1     192.168.1.127   DNS       115 Standard query response 0xe95f A aeventlog.beacon.qq.com A 203.2…
  422 25.666708   192.168.1.127   192.168.1.1     DNS        77 Standard query 0xab0d A wkvip.laiwang.com
  434 29.189463   192.168.1.127   192.168.1.1     DNS        80 Standard query 0xdf8c A android.push.126.net
  460 31.201230   192.168.1.1     192.168.1.127   DNS       124 Standard query response 0xcea4 A uwnthesis-files-wordpress-com.c…
  496 38.218641   192.168.1.127   192.168.1.1     DNS        74 Standard query 0xd6e6 A www.taobao.com
  498 38.243728   192.168.1.1     192.168.1.127   DNS       138 Standard query response 0xd6e6 A www.taobao.com CNAME www.taobao…
  512 40.406032   192.168.1.1     192.168.1.127   DNS       245 Standard query response 0xfbb5 A resolver.msg.xiaomi.net CNAME l…
```

```
› Frame 4: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits)
› Ethernet II, Src: CiscoLinksys_da:cf:2d (00:16:b6:da:cf:2d), Dst: HuaweiTechno_b8:3d:23 (00:9a:cd:b8:3d:23)
› Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.127
› User Datagram Protocol, Src Port: 53, Dst Port: 56015
› Domain Name System (response)
```

After learning about the file’s key, I entered the command “**airdecap-ng -p linkinpark WPA2- P4-01.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-P4-01-dec.cap.”** I had access to the general traffic and performed a Protocol Hierarchy Statistical Analysis. Right above screenshot I filter the traffic specifically for “DNS”. I glad I found amazing results. I also specify **packet no. 223**, which is standard query with source and destination address (Source: 192.168.1.127, Destination: 192.168.1.1)