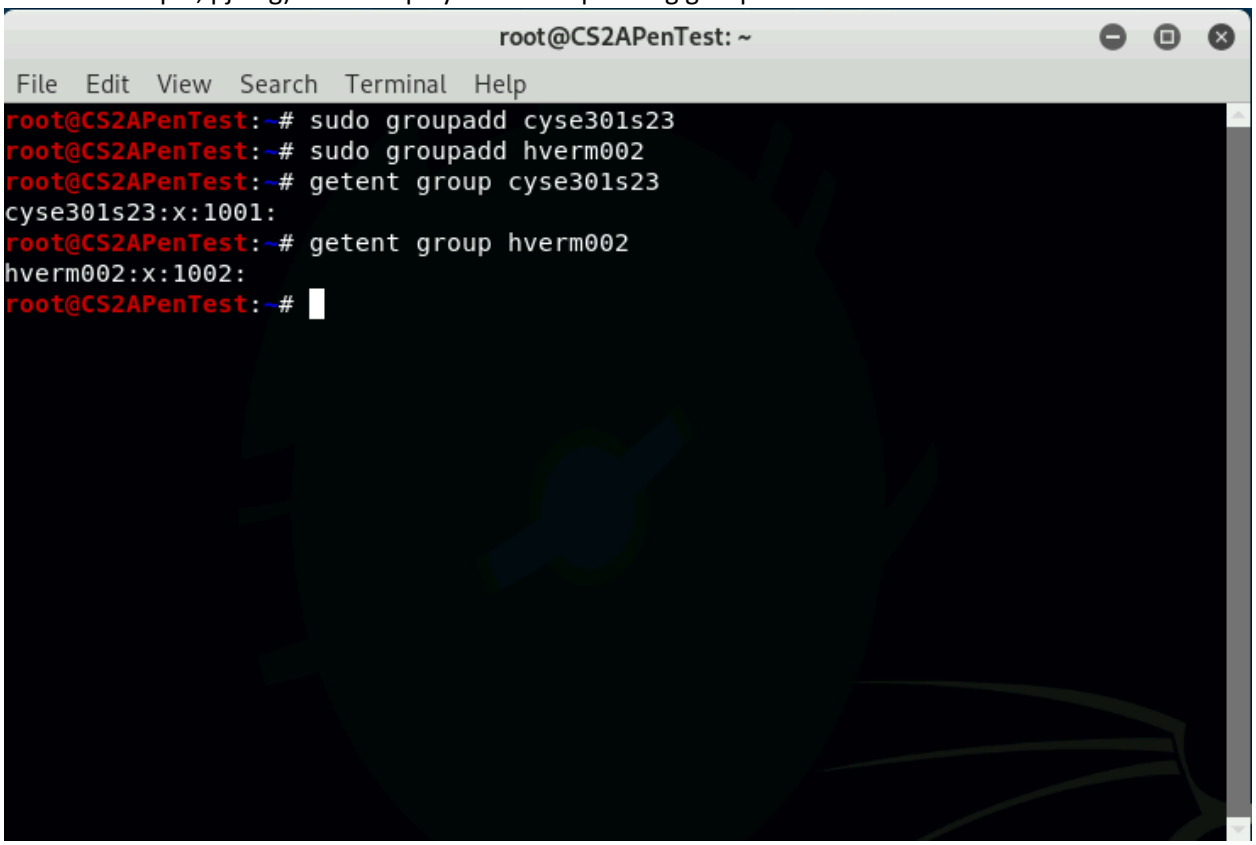
CYSE 301: Cybersecurity Technique and Operations

Assignment 4: 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 **cyse301s23**, and the other is your ODU Midas ID (for example, pjiang). 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.

```
root@CS2APenTest:~# sudo useradd -m -G cyse301s23 user1
root@CS2APenTest:~# sudo useradd -m -G cyse301s23 user2
root@CS2APenTest:~# sudo useradd -m -G cyse301s23 user3
root@CS2APenTest:~# sudo useradd -m -G hverm002 user4
root@CS2APenTest:~# sudo useradd -m -G hverm002 user5
root@CS2APenTest:~# sudo useradd -m -G hverm002 user6
root@CS2APenTest:~# grep user1 /etc/passwd
user1:x:1001:1003::/home/user1:/bin/sh
root@CS2APenTest:~# grep user2 /etc/passwd
user2:x:1002:1004::/home/user2:/bin/sh
root@CS2APenTest:~# grep user3 /etc/passwd
user3:x:1003:1005::/home/user3:/bin/sh
root@CS2APenTest:~# grep user4 /etc/passwd
user4:x:1004:1006::/home/user4:/bin/sh
root@CS2APenTest:~# gre[ user5 /etc/passwd
> ^C
root@CS2APenTest:~# grep user5 /etc/passwd
user5:x:1005:1007::/home/user5:/bin/sh
root@CS2APenTest:~# grep user6 /etc/passwd
user6:x:1006:1008::/home/user6:/bin/sh
root@CS2APenTest:~#
```

:p

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:~# echo "user1:password1" | sudo chpasswd
root@CS2APenTest:~# echo "user2:password2" | sudo chpasswd
root@CS2APenTest:~# echo "user3:P@ssw0rd3" | sudo chpasswd
root@CS2APenTest:~# echo "user4:Str0ngP@ss | sudo chpasswd
> ^C
root@CS2APenTest:~# echo "user5:c0mpL3xP@ssw0rd!" | sudo chpasswd
root@CS2APenTest:~# echo "user6:R@nd0mP@ssw0rd123" | sudo chpasswd
root@CS2APenTest:~#
```

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.

```
Proceeding with incremental:ASCII
2g 0:00:03:19  3/3 0.01004g/s 1824p/s 5339c/s 5339C/s sasink..shrisb
2g 0:00:05:13  3/3 0.006389g/s 1829p/s 5405c/s 5405C/s sheeties..mangsha1
2g 0:00:17:22  3/3 0.001919g/s 1805p/s 5391c/s 5391C/s mompiers..merreler
2g 0:00:17:25  3/3 0.001913g/s 1805p/s 5391c/s 5391C/s charkyle..chathomo
2g 0:00:18:26  3/3 0.001808g/s 1803p/s 5385c/s 5385C/s jcaris..jcatot
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
root@CS2APenTest:~# --show
bash: --show: command not found
root@CS2APenTest:~# john --show hverm002-HASH
user1:password1:19813:0:99999:7:::
user2:password2:19813:0:99999:7:::

2 password hashes cracked, 3 left
root@CS2APenTest:~#
```

Task B: Windows Password Cracking (25 points)

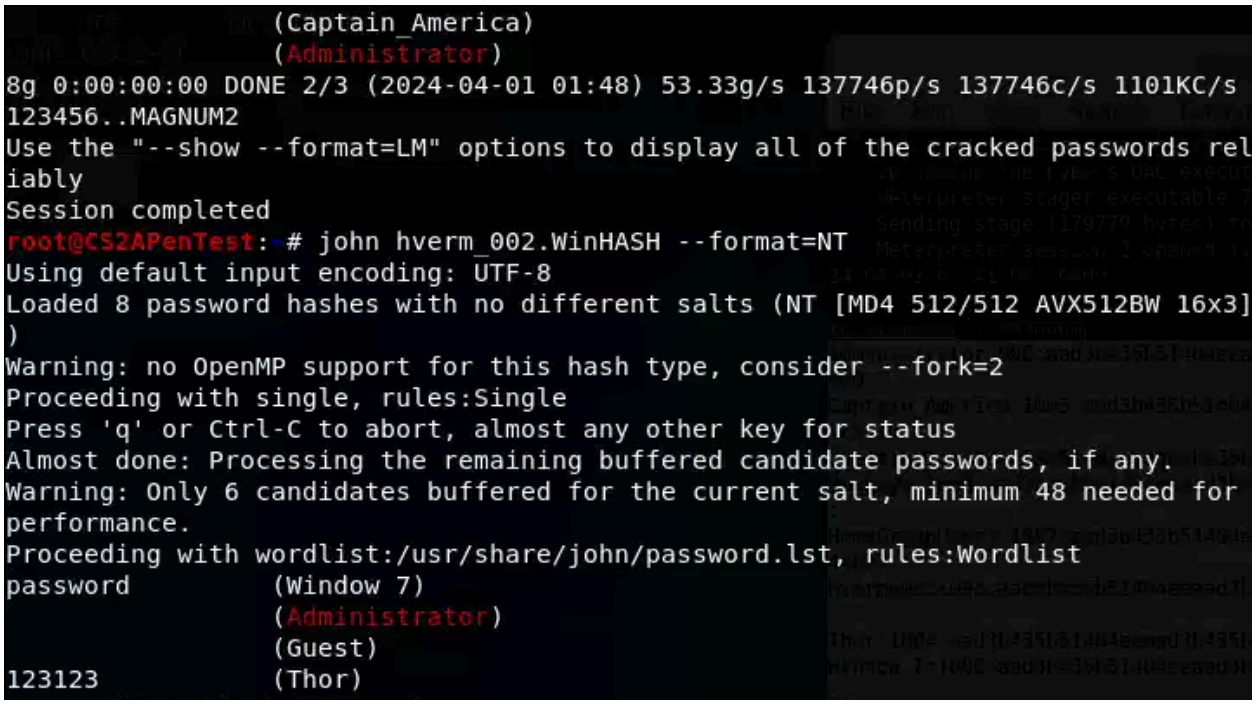
Log on to Windows 7 VM and create a list of 3 users with different passwords. Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

Now, complete the following tasks:

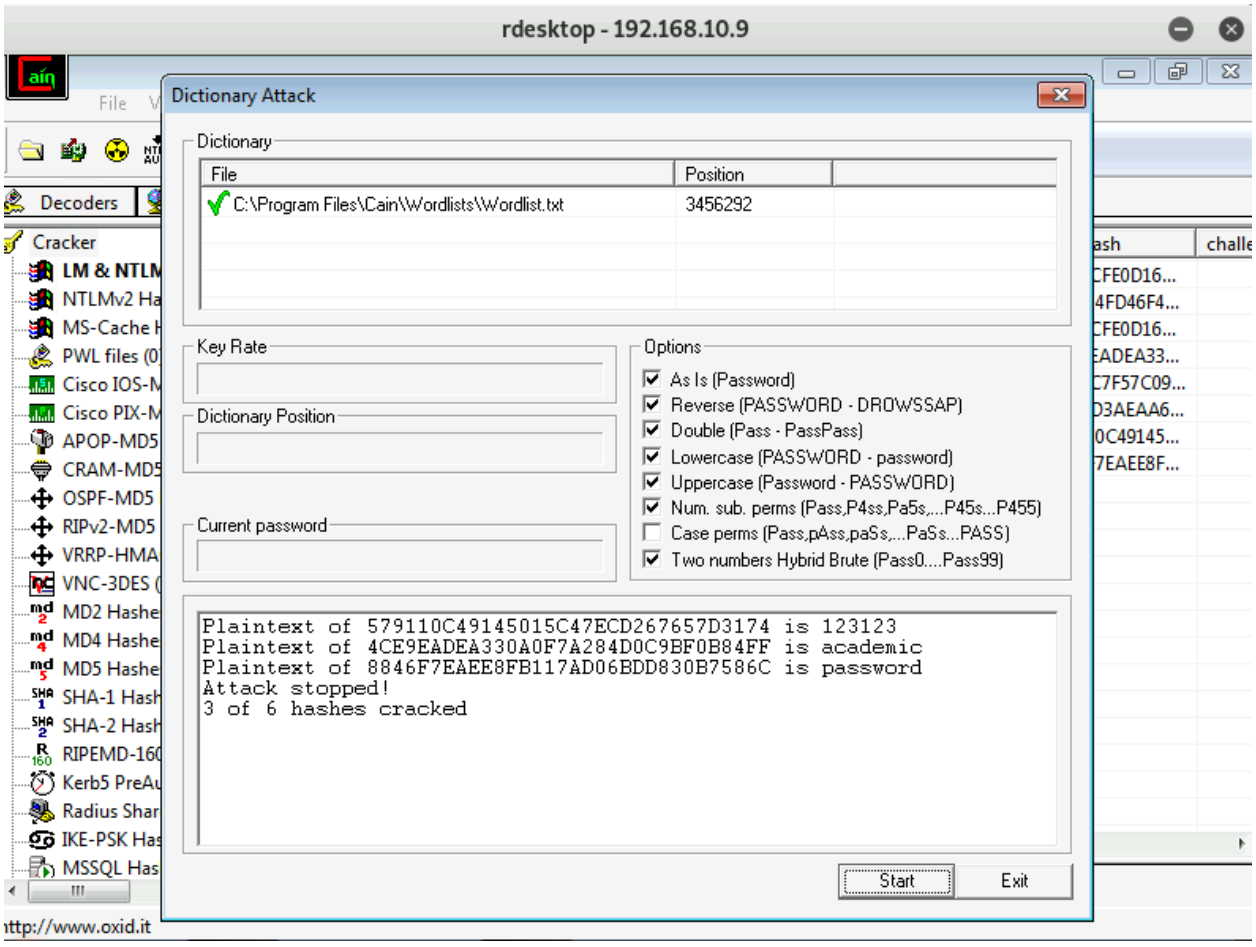
1. **5 points.** Display the password hashes by using the “hashdump” command in the meterpreter shell. Then

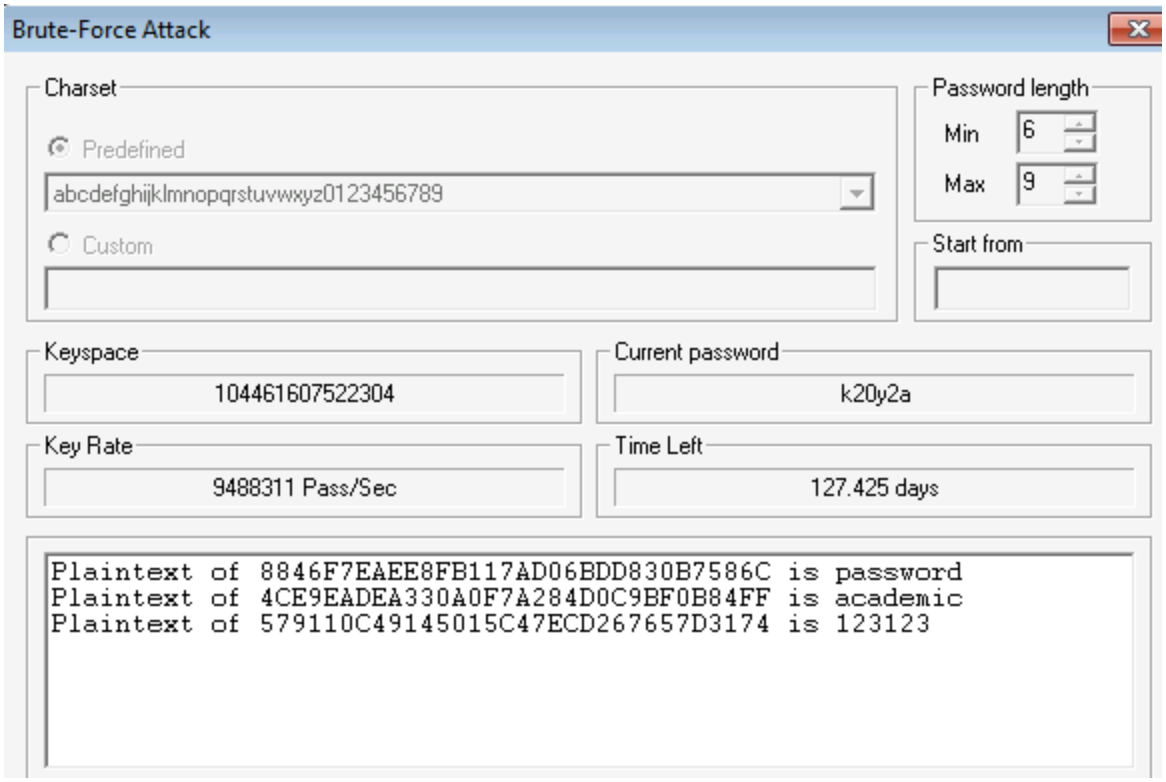
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Captain_America:1005:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb414
4c5df0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hawkeye:1006:aad3b435b51404eeaad3b435b51404ee:4ce9eadea330a0f7a284d0c9bf0b84ff::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e4
44b23:::
hverm002:1003:aad3b435b51404eeaad3b435b51404ee:b9dfd3aeaa6f43aed0cd9834b40fd484:
::
Thor:1004:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:
::
```

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.).



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.).


rdesktop - 192.168.10.9
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 579110C49145015C47ECD267657D3174 is 123123
Plaintext of 4CE9EADEA330A0F7A284D0C9BF0B84FF is academic
Plaintext of 8846F7EAEE8FB117AD06BDD830B7586C is password
Attack stopped!
3 of 6 hashes cracked
Start
Exit
Decoders
Cracker
LM & NTLM
NTLMv2 Ha
MS-Cache H
PWL files (0
Cisco IOS-M
Cisco PIX-M
APOP-MD5
CRAM-MD5
OSPF-MD5
RIPv2-MD5
VRRP-HMA
VNC-3DES (
MD2 Hashe
MD4 Hashe
MD5 Hashe
SHA-1 Hash
SHA-2 Hash
RIPEMD-160
Kerb5 PreAu
Radius Shar
IKE-PSK Has
MSSQL Has
http://www.oxid.it



Task C: Extra credit: (10 points)

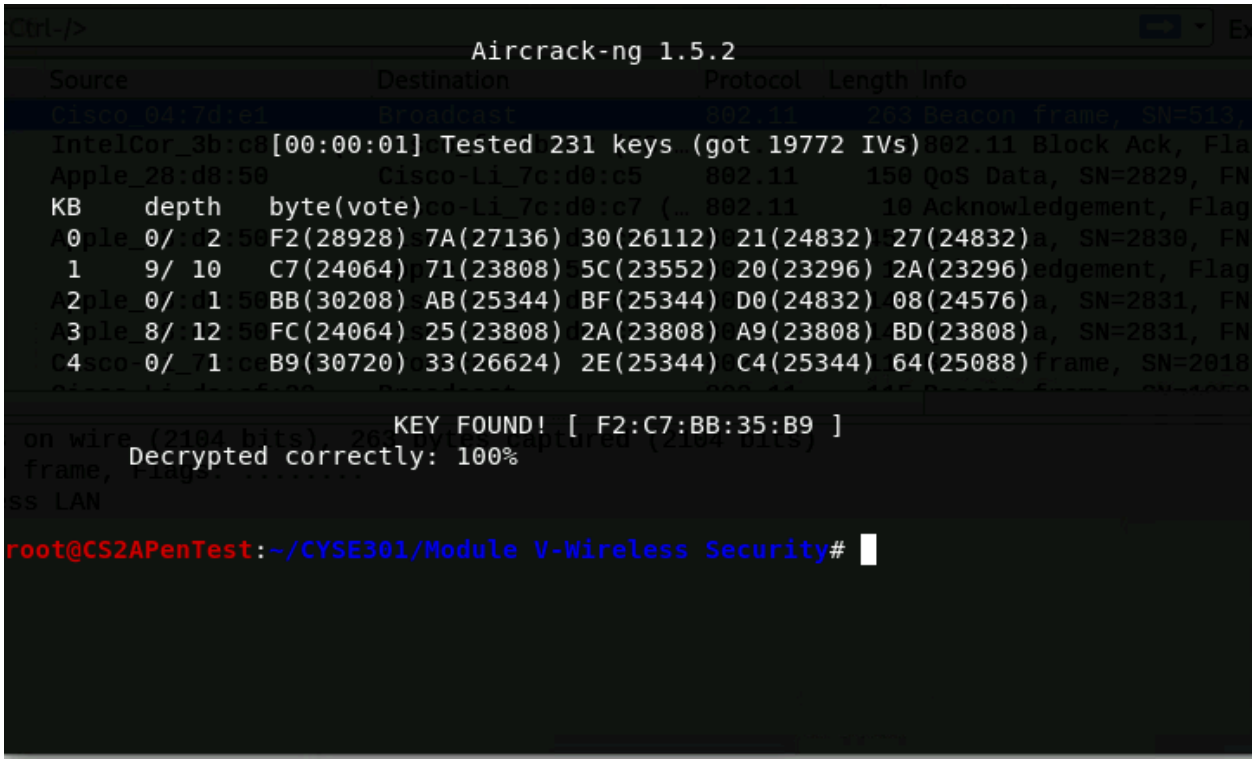
Search the proper format in John the Ripper to crack the following **MD5** hashes (use the ***--list=formats*** option to list all supported formats) . Show your steps and results.

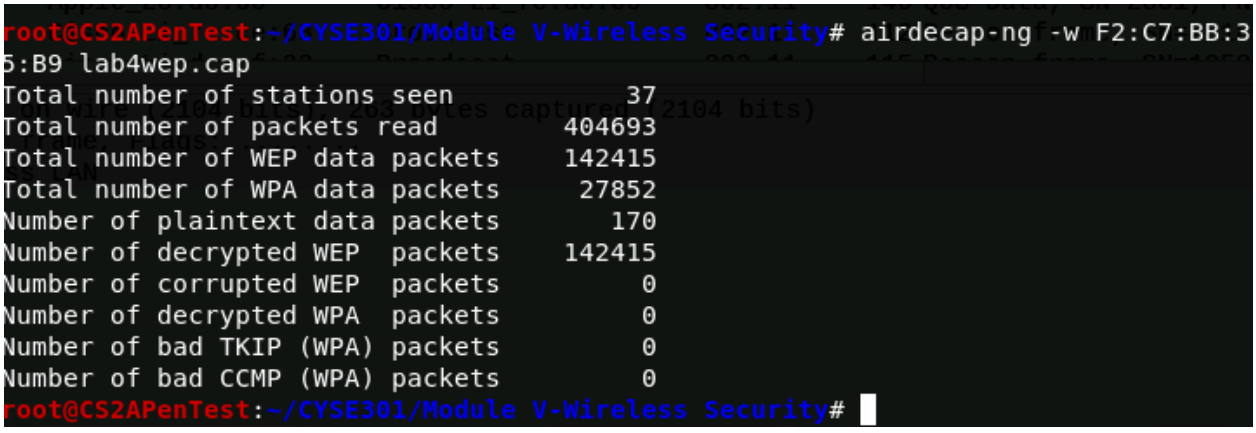
1. 5f4dcc3b5aa765d61d8327deb882cf99
2. 63a9f0ea7bb98050796b649e85481845

Task C: 20 points

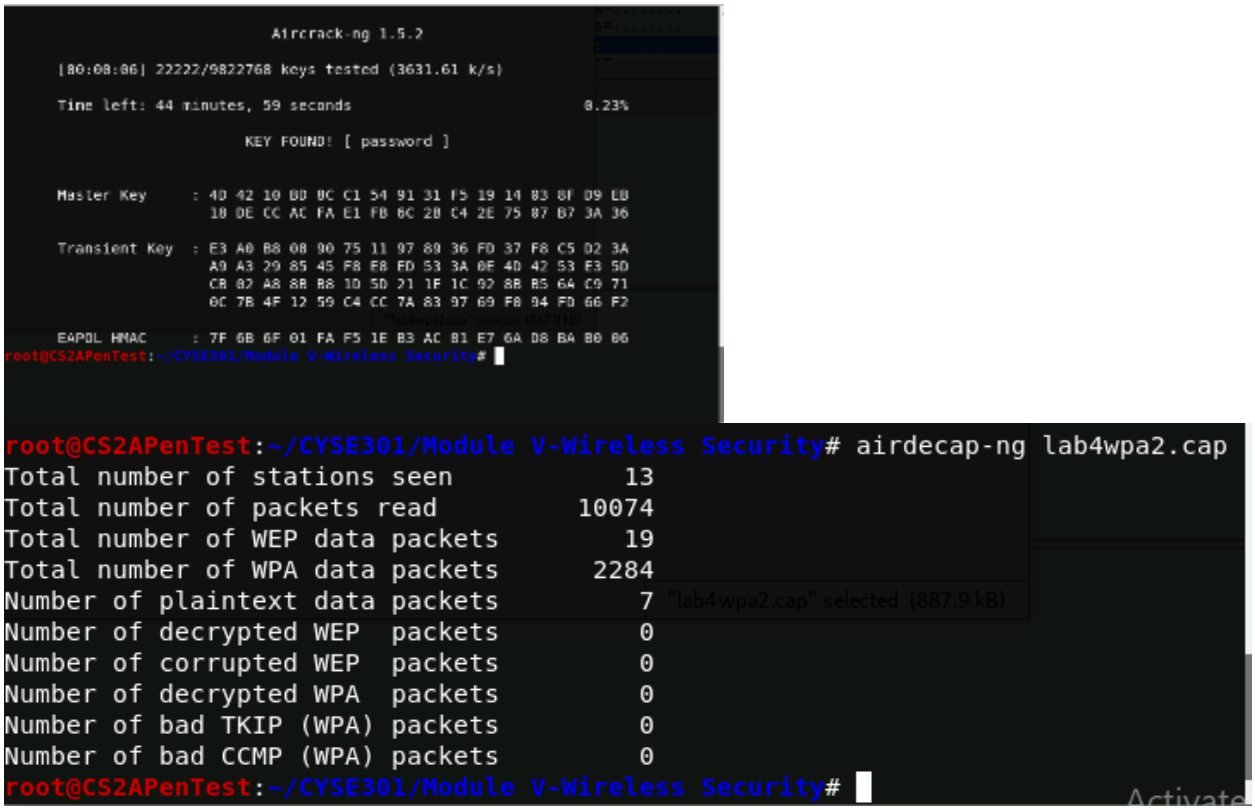
Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

Decrypt the lab4wep. cap file (**5 points**) and perform a detailed traffic analysis (**5 points**)





Decrypt the lab4wpa2. 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 pjiang is **e**. Thus, I should pick up the file "WPA2-P5-01.cap."

MD5 of pjiang is 5a618cdc3edffd8b4c661e7e9b70ce1e

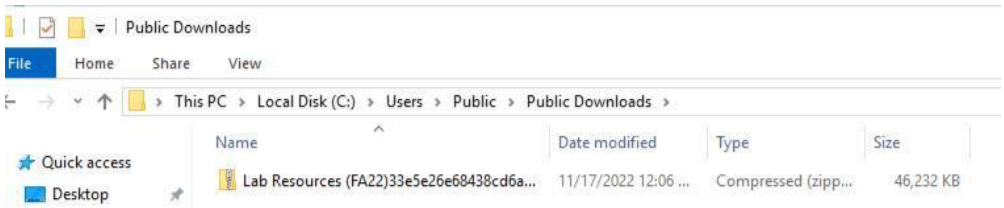
You can find an online MD5 hash generator or the following command to get the hash of a text string,

```
root@CS2APenTest:~# echo -n pjiang | md5sum
5a618cdc3edffd8b4c661e7e9b70ce1e  -
root@CS2APenTest:~#
```

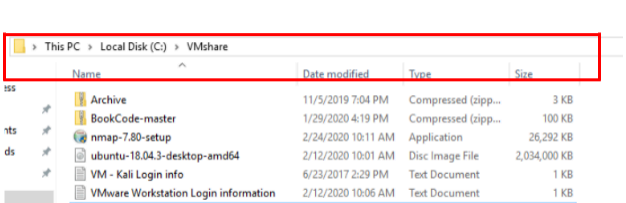
Figure 1 Command to get the MD5 hash.

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

- The above files are zipped in a folder named "Lab Resources." You can locate the zipped folder in the Windows 10 Host Machine under C:/Users/Public/Public Downloads. Then, unzip the following zipped file and find the assigned WPA file under the sub-folder "Wireless Traffic."



- Copy the file assigned to you to the "C:/VMshare" in Windows 10 Host Machine to access it from the Kali VMs (you can use either Kali to complete the assignment).



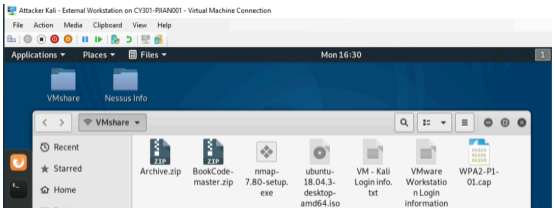
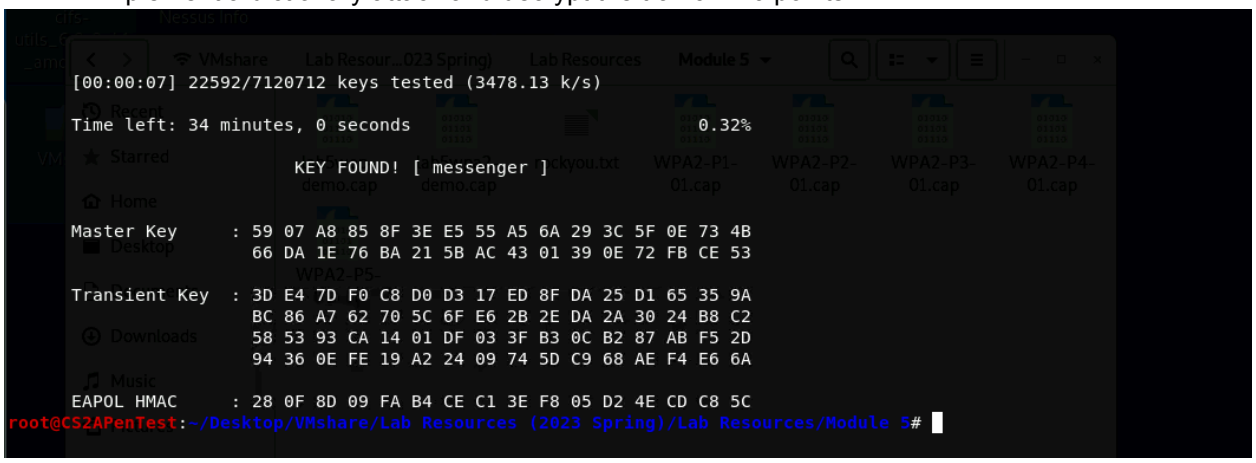


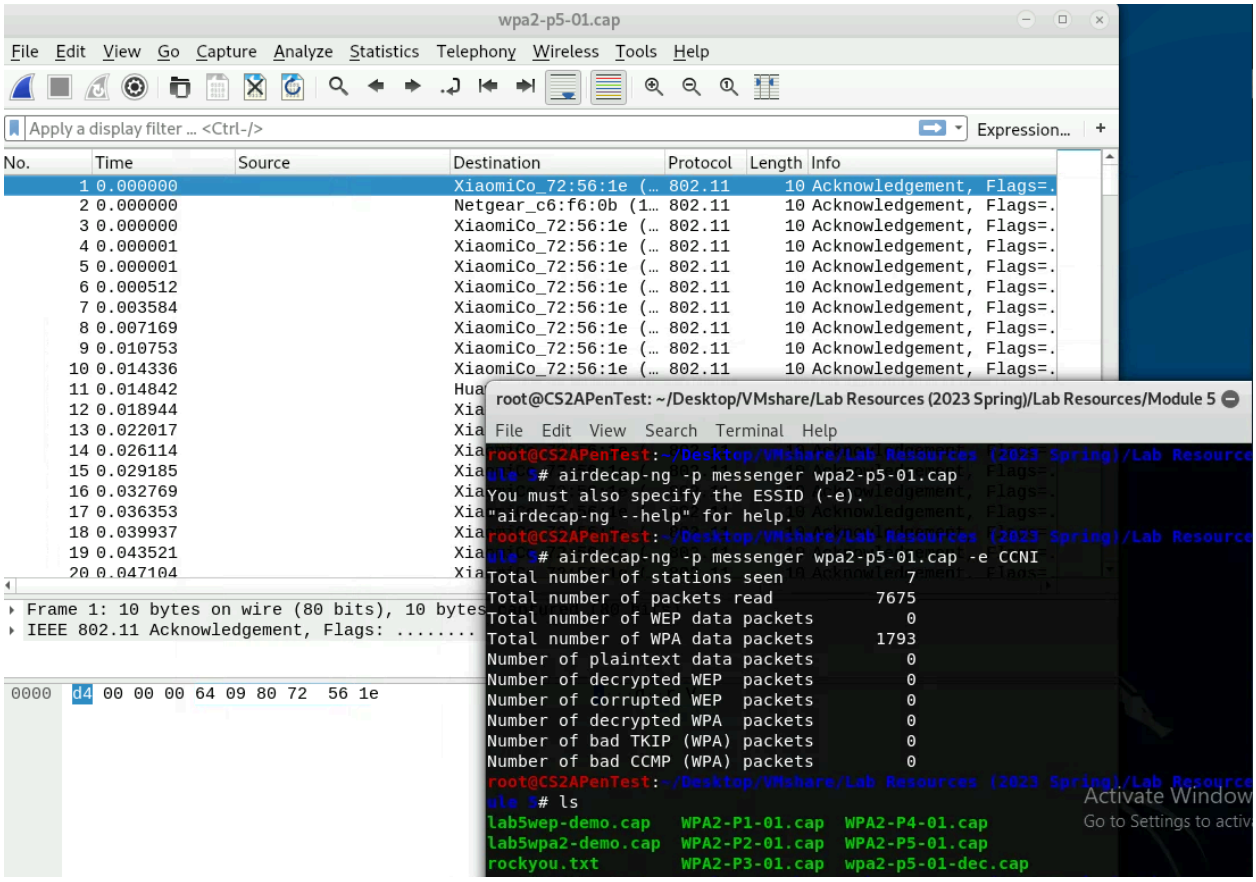
Figure left: Windows Host Machine *Figure right: VMshare folder on Kali Linux*

Then complete the following steps:

1. Implement a dictionary attack and decrypt the traffic. - 20 points



Decrypt the encrypted traffic and write a detailed summary to describe what you have explored from this encrypted traffic file. -10 points



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	7675	100.0	860960	156 k	0	0	0
IEEE 802.11 wireless LAN	102.1	7835	15.7	135555	24 k	5504	75301	13 k
Logical-Link Control	0.1	4	0.1	506	91	0	0	0
802.1X Authentication	0.1	4	0.1	474	85	4	474	85
Data	28.2	2167	82.1	707011	128 k	2167	707011	128 k

Compared to other decrypted files obtained through internet traffic, the encrypted LAN-based traffic file, primarily sourced from IEEE 802.11 wireless LAN, presents unique challenges and opportunities for analysis. Unlike internet traffic, which often utilizes TCP connections and may employ a variety of protocols such as HTTP, HTTPS, FTP, etc., this LAN-based traffic operates within a localized network environment, potentially with different communication patterns and protocols. The absence of TCP connections in the LAN-based traffic file and the use of Logical Link Control (LLC) suggest a distinct communication framework. Decryption and analysis of this LAN-based traffic file require tailored approaches, focusing on packet structures, header information, and communication endpoints specific to IEEE 802.11 wireless LAN. While insights from previous decrypted internet traffic files may inform analysis methodologies, the unique characteristics of the LAN-based traffic necessitate a customized approach to fully understand its contents and implications within the local network context.