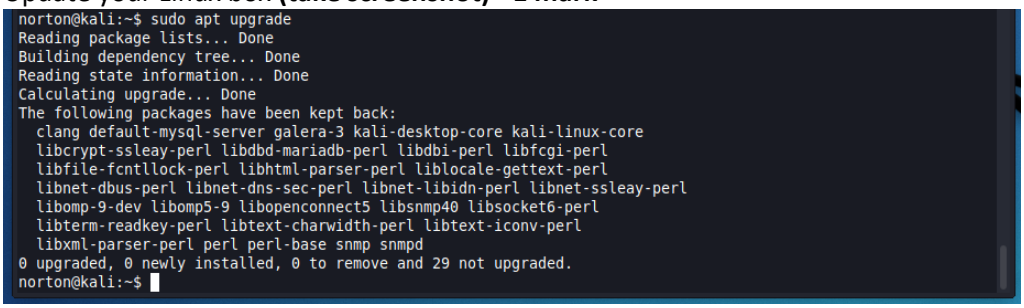
PEN TESTING ASSIGNMENT 1 (20%)

Task 1: Vulnerability assessment with Nessus

Pre-lab configuration

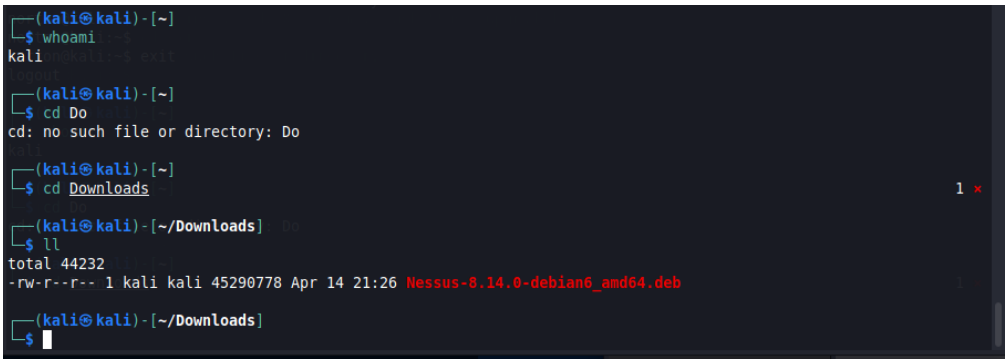
1) Make sure you have a working Linux box
2) Check your internet connection, you can either use NAT or bridge mode for this lab
3) Update your Linux box **(take screenshot) - 1 mark**



4) You need to have a working email address for this lab, either use your personal, school's one or even create one for the group.

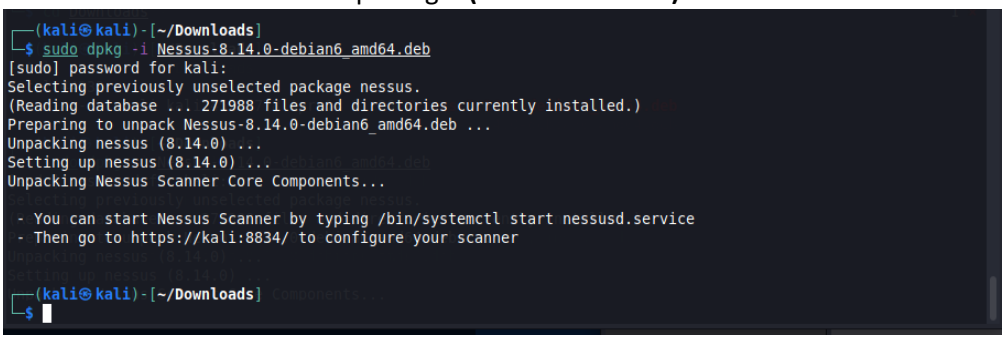
Lab

1) Use any web browser such as Firefox ESR or Ice Weasel to go to https://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code
   This is the page where you need to register a Free Home user with your email address in order to get an activation code. The activation code will be emailed to your email address.
2) Then go to the download page (https://www.tenable.com/products/nessus/select-your-operating-system#download) to download your suitable version - Debian 6, 7, 8 / Kali Linux 1 AMD64 or Debian 6, 7, 8 / Kali Linux 1 i386(32-bit) or any of your favorite Linux distribution. Download it.
3) Open up a terminal window, navigate to your Downloads folder **(take screenshot) 1 mark**

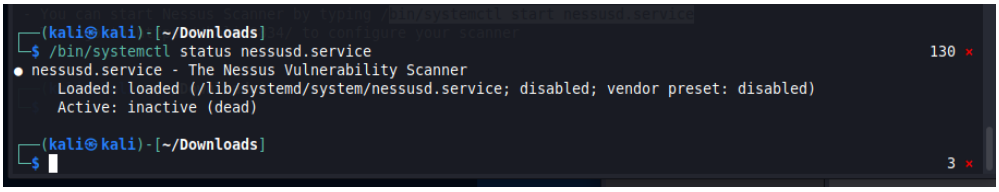


4) Use your team user account (do not use root), use "sudo dpkg -i <Nessus-6……>" to install Nessus on your system. Dpkg is the package manager in Debian system and "-

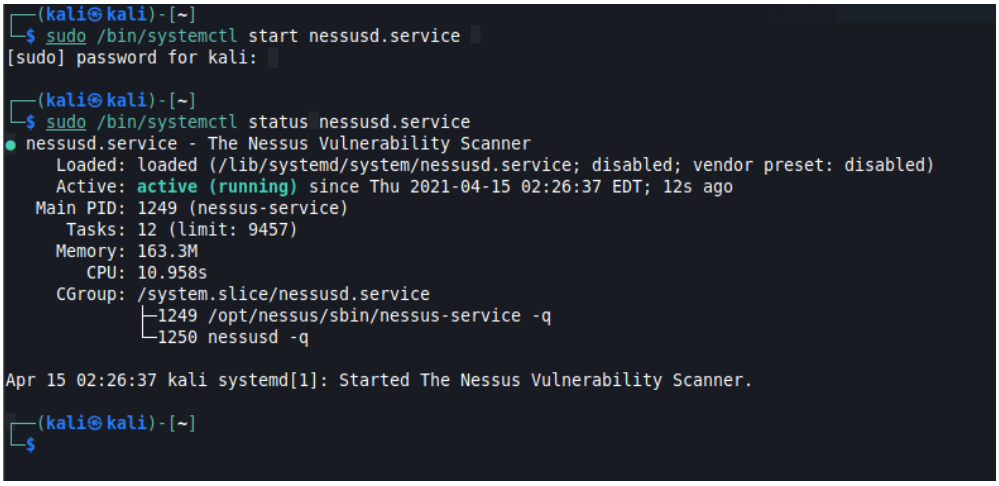
i" is the command to install a package. **(take screenshot) - 1 mark**



5) Check the status of the Nessus package on the system, use "sudo /etc/init.d/nessusd status" **(take screenshot) - 1 mark**



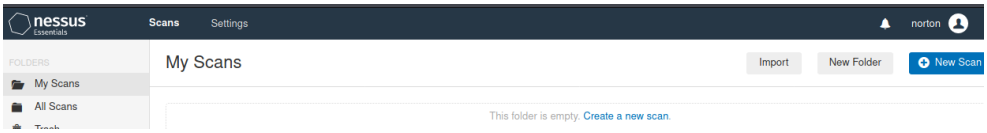
6) Now start the Nessus daemon, use "sudo /etc/init.d/nessusd start" **(take screenshot) - 1 mark**



7) Now go back to your browser, type https://127.0.0.1:8834 to login to the Nessus web interface. Please make sure you type 8834 port as Nessus by default use this port for the web interface. You might see "connection not secure" message, click "Advanced" and "Add Exception" -> "Confirm Security Exception". MWNK-TA3D-M3FX-CVC5-H42S

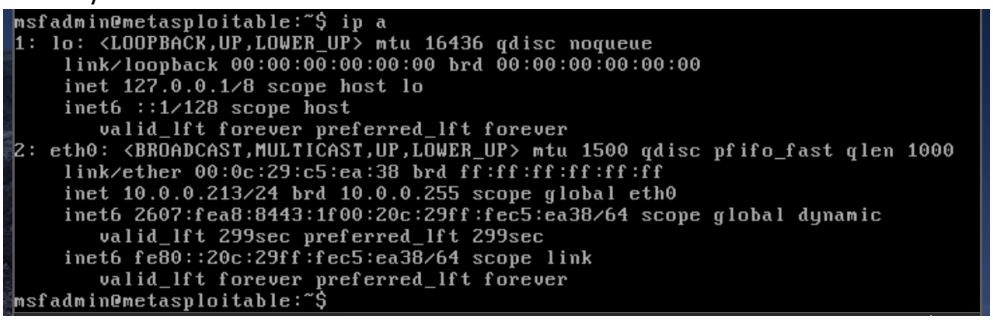
8) You will see the Nessus welcome page, click continue. Create a username and put a password. The username should be your **team name**. Now put the activation code you already received in email and put it in there. Now Nessus will start to download its essential plugins and features. It might take a while.

9) Now login to the Nessus web portal with your username and password, you will see your username on top right corner. **(take screenshot) - 1 mark**



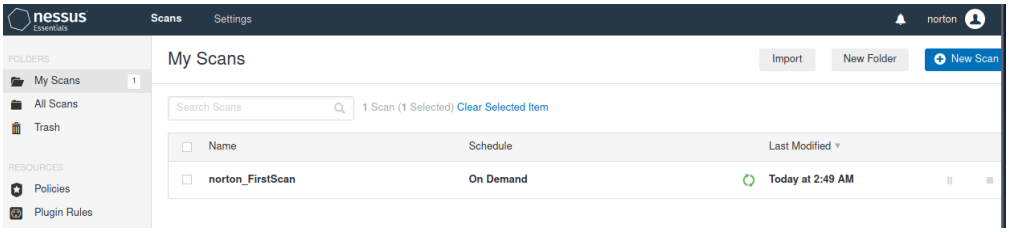
10) Before you proceed any further, we need to check the ip address of your Linux box(**Metasploitable**). We will run Nessus vulnerability scan on that. So go back to

terminal and type “sudo ifconfig -a” and note your ip address. (Usually the IP for eth0 interface, might differ though) **(take screenshot) - 1 mark** Let us assume you record your IP address to be 192.168.136.128 with netmask 255.255.255.0

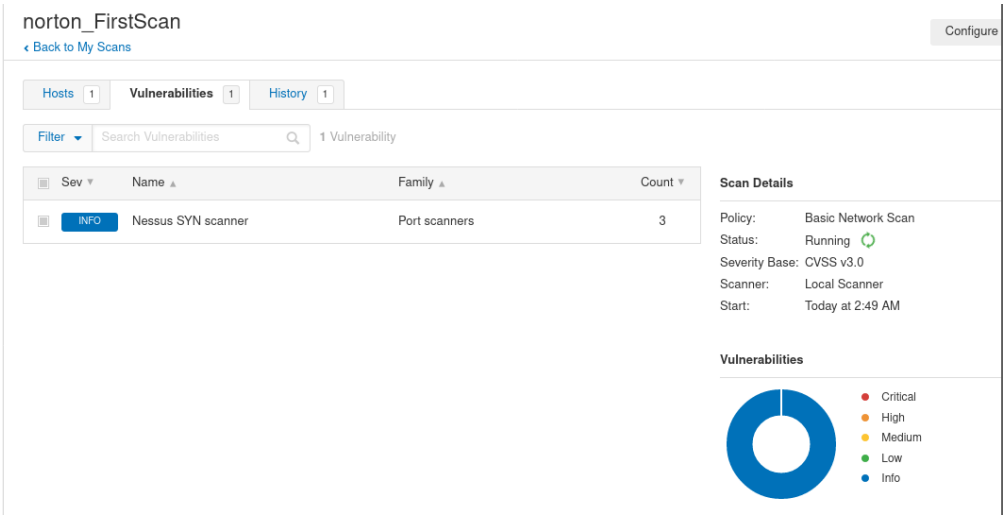


11) Go back to the Nessus web portal and click “New Scan” then choose “Basic Network Scan”.

12) Give a name to your scan. Recommended format: YourGroupName_FirstScan
13) Put the target as the IP address subnet of your Linux box. So we assumed in step 10 that the IP address of my Linux box is 192.168.136.128 with netmask 255.255.255.0. So here I will enter 192.168.136.0/24 as target machines. Save it.
14) Now click the launch button on right side of the scan to start the scan. (looks like a "play" symbol of old diskman ☺) **(take screenshot) – 1 mark**



15) Now double click on the scan, then you will see the list of Hosts with IP addresses that are scanning. Go to the next tab called "Vulnerabilities" **(take screenshot) – 1 mark**



16) Now go back to your scans and wait for the scan to finish. It might take a while. There are two green color curve arrows moving in circle that means the scan is still in progress.
17) After the scan is finished, double click on the scan. Then you will see the Export options. Export the scan in PDF with "Executive Summary" report options.

18) Send me the PDF scan report (**1 mark**) along with your actual lab report.

Task 2: Offline Cracking

1) Please perform the offline cracking task in the JTF and Hashcat lab and perform in your lab environment.

2) Add a new user "<groupname>_cracking" and password as 'password1' **(take screenshot)**

– 1 mark

```
┌──(kali㉿kali)-[~]
└─$ sudo passwd norton_cracking
New password:
Retype new password:
passwd: password updated successfully

┌──(kali㉿kali)-[~]
└─$
```

3) Add the user to Sudo group **(take screenshot) – 1 mark**

```
┌──(kali㉿kali)-[~]
└─$ sudo usermod -aG sudo norton_cracking

┌──(kali㉿kali)-[~]
└─$
```

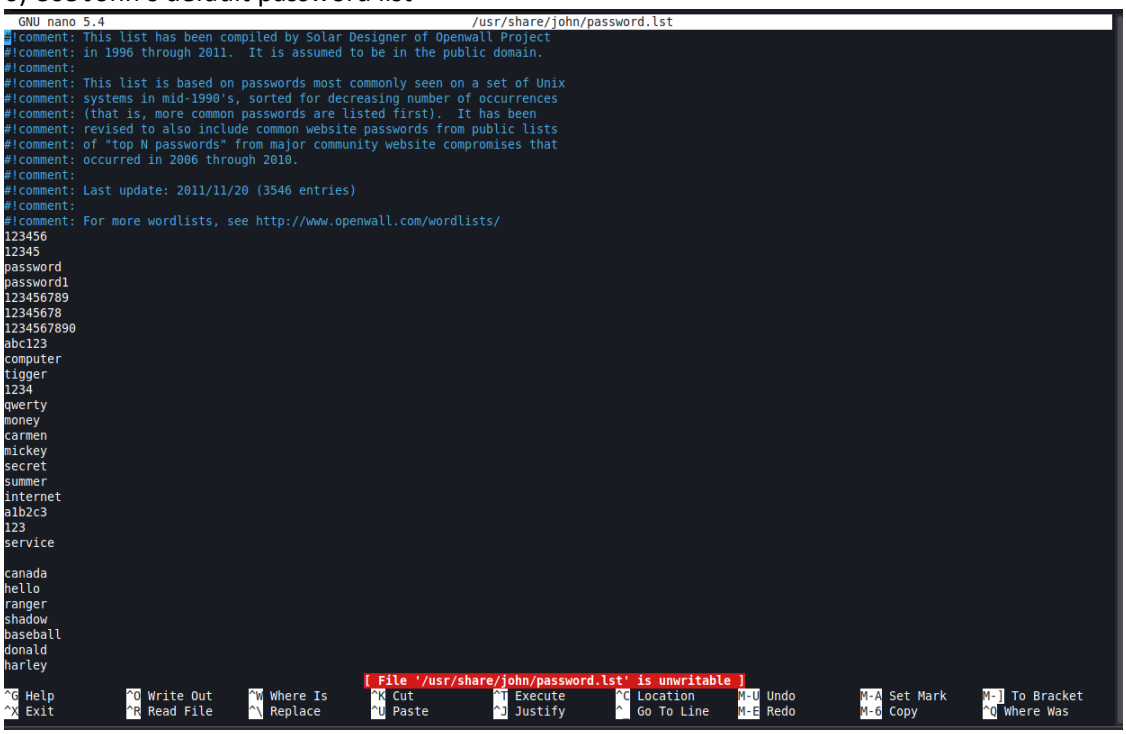
4) Change the Beep to Yes in John configuration file **(take screenshot) – 1 mark**

```
# Markov modes as well, see ../doc/MARKOV
[Options]
# Default wordlist file name (including in batch mode)
Wordlist = $JOHN/password.lst
# Use idle cycles only
Idle = Y
# Crash recovery file saving delay in seconds
Save = 60
# Beep when a password is found (who needs this anyway?)
Beep = Y
# if set to Y then dynamic format will always work with bare hashes. Normally
# dynamic only uses bare hashes if a single dynamic type is selected with
# the -format=  (so -format=dynamic_0 would use valid bare hashes).
DynamicAlwaysUseBareHashes = N

# Default Single mode rules
SingleRules = Single
```

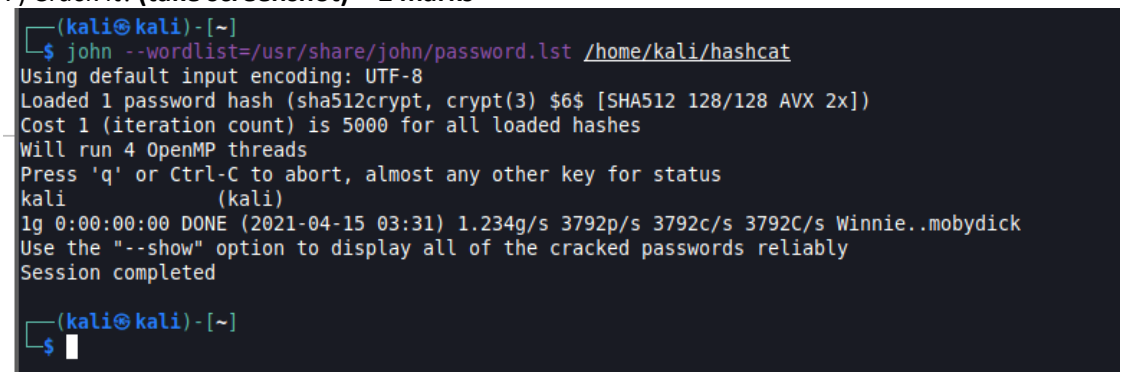
5) Use Unshadow to merge the /etc/passwd and /etc/shadow **(take screenshot) – 1 mark**

```
┌──(kali㉿kali)-[~]
└─$ sudo unshadow /etc/passwd /etc/shadow > /home/kali/hashcat
Created directory: /root/.john

┌──(kali㉿kali)-[~]
└─$ ll
```

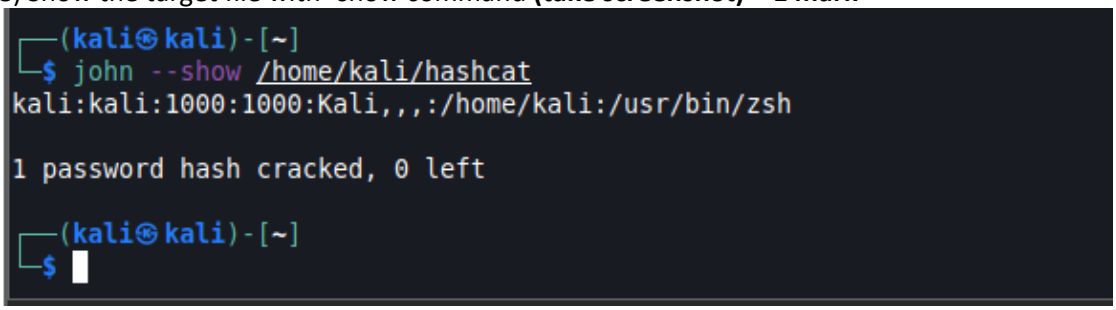
6) Use John's default password list



7) Crack it! **(take screenshot) – 2 marks**



8) Show the target file with -show command **(take screenshot) – 1 mark**

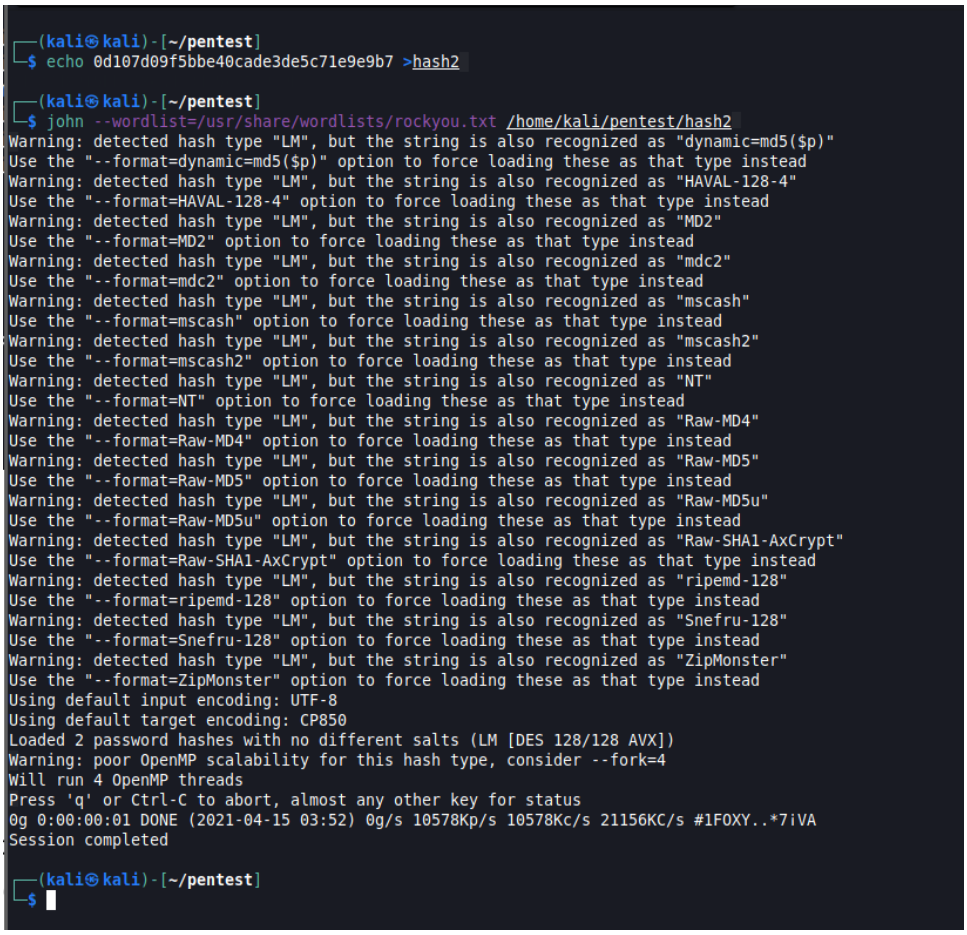


9) Use Hashcat to crack these MD5 hashes using **Rock You** word list

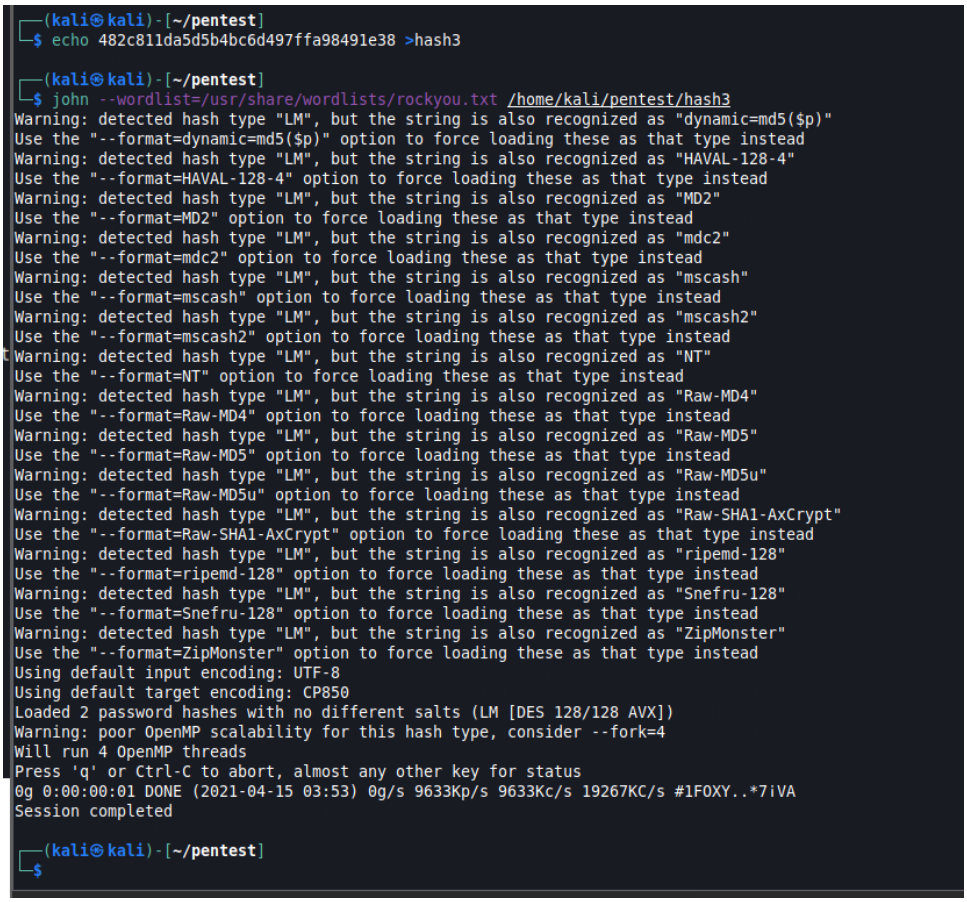
a) 827ccb0eea8a706c4c34a16891f84e7b **(take screenshot) – 1 mark**

```
┌──(kali㉿kali)-[~/pentest]
└─$ cat hash1
827ccb0eea8a706c4c34a16891f84e7b

┌──(kali㉿kali)-[~/pentest]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt /home/kali/pentest/hash1
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
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
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 2 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2021-04-15 03:51) 0g/s 9808Kp/s 9808Kc/s 19617KC/s #1FOXY..*7iVA
Session completed

┌──(kali㉿kali)-[~/pentest]
└─$
```

b) 0d107d09f5bbe40cade3de5c71e9e9b7 **(take screenshot) – 1 mark**



c)482c811da5d5b4bc6d497ffa98491e38 **(take screenshot) – 1 mark**



Post lab

1) You need to create a report in proper formatting (see #2).
2) First page of the report should have the name of the course, Lab Assignment 1, the college name, your group and group members' name. **Please use a cover page template from MS Word. Report should be in PDF format**

3) The rest of the pages should have the screenshots that you collected in the lab steps (e.g Task 1: Screenshots, Task 2: Screenshots)
4) Each team members need to submit the Lab report (in one PDF document via BB).
5) **Deadline to submit the report is on/before: EST 10 PM sharp on Thursday, April 22nd 2021.** If you have any questions/queries, you can email me or talk to me on next/following class(s)

Mark rubrics:

Task	**Marks**	**Weight**	**Percentage**
Task 1	10	1	10
Task 2	10	1	10
Total			**20%**