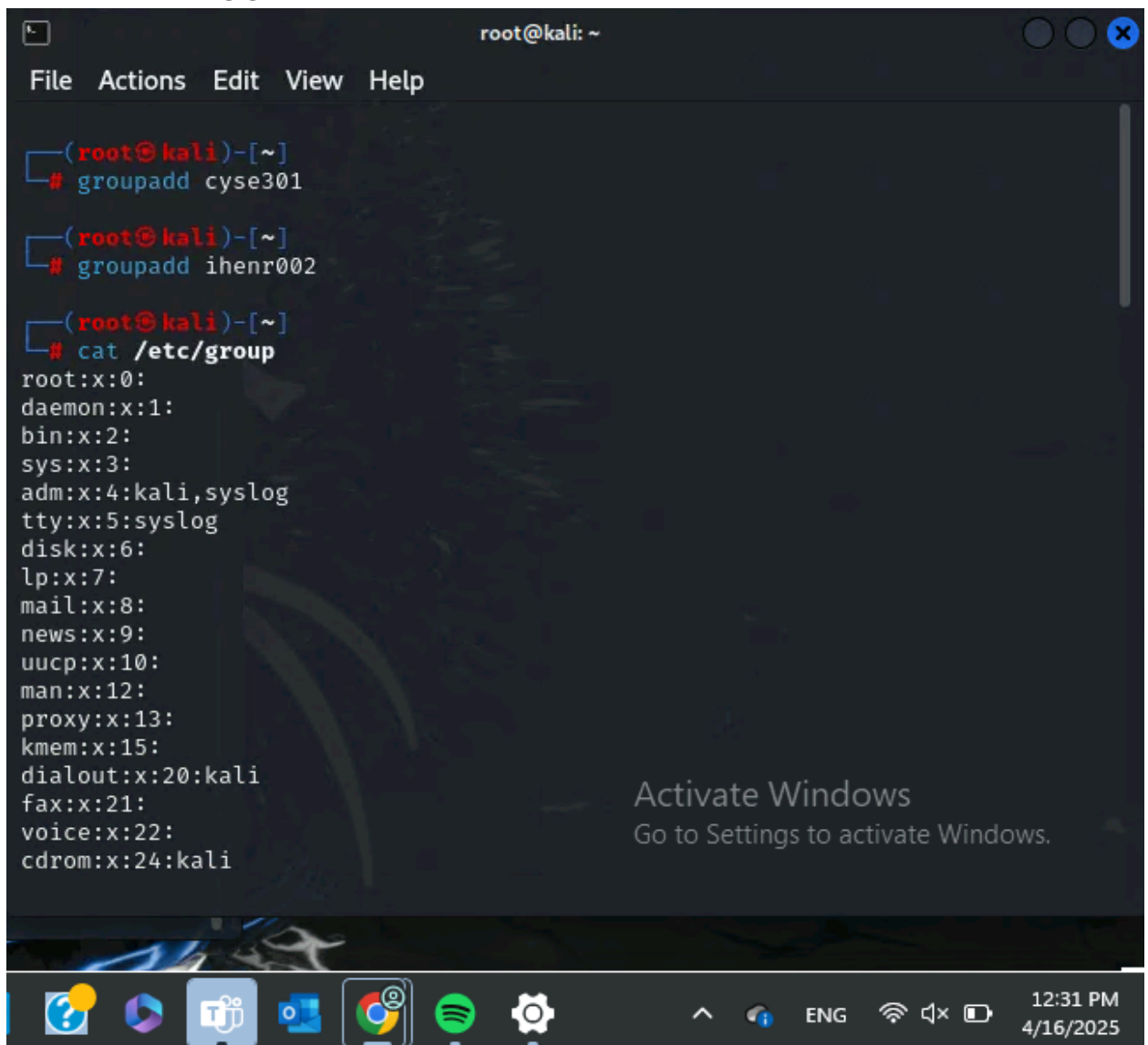


India Henry
CYSE301 - 32781
Shideh Yavary Mehr
21 April 2025 - 24 April 2025
CYSE: Cybersecurity Techniques and Operations
Assignment 5: Password & Wifi Cracking

Task A: Linux Password Cracking

1. Create two groups, one is cyse301, and the other is your MIDAS ID. Then display the corresponding group IDs.



```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)-[~]  
# groupadd cyse301  
  
(root@kali)-[~]  
# groupadd ihenr002  
  
(root@kali)-[~]  
# cat /etc/group  
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:kali,syslog  
tty:x:5:syslog  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:kali  
fax:x:21:  
voice:x:22:  
cdrom:x:24:kali
```

Activate Windows
Go to Settings to activate Windows.

12:31 PM
4/16/2025

```
root@kali: ~  
File Actions Edit View Help  
geoclue:x:122:  
Debian-snmpp:x:123:  
sslh:x:124:  
ssl-cert:x:125:postgres  
i2c:x:126:  
ntpsec:x:127:  
redsocks:x:128:  
kismet:x:129:  
_gophish:x:130:  
redis:x:131:_gvm  
postgres:x:132:  
mosquitto:x:133:  
sambashare:x:989:  
inetsim:x:134:  
wireshark:x:135:kali  
_gvm:x:136:  
kali:x:1000:  
kaboxer:x:137:kali  
xrdp:x:138:  
snort:x:139:  
syslog:x:140:  
splunk:x:1001:  
cyse301:x:1002:  
ihenr002:x:1003:  
  
# (root@kali)-[~]  
#
```

Activate Windows
Go to Settings to activate Windows.

12:32 PM
4/16/2025

Cat /etc/group

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

```
root@kali: ~
File Actions Edit View Help
splunk:x:1001:
cyse301:x:1002:
ihenr002:x:1003:

(root@kali)-[~]
# useradd user1

(root@kali)-[~]
# useradd user2

(root@kali)-[~]
# useradd user3

(root@kali)-[~]
# adduser user1 cyse301
info: Adding user `user1' to group `cyse301' ...

(root@kali)-[~]
# adduser user2 cyse301
info: Adding user `user2' to group `cyse301' ...

(root@kali)-[~]
# adduser user3 cyse301
info: Adding user `user3' to group `cyse301' ...

(root@kali)-[~]
#
```

Activate Windows
Go to Settings to activate Windows.

12:34 PM
4/16/2025

Making users 1-3 then adding them to the cyse301 group

```
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# adduser user3 cyse301
info: Adding user `user3' to group `cyse301' ...

(root@kali)-[~]
# useradd user4

(root@kali)-[~]
# useradd user5

(root@kali)-[~]
# useradd user6


(root@kali)-[~]
# adduser user4 ihenr002
info: Adding user `user4' to group `ihenr002' ...

(root@kali)-[~]
# adduser user5 ihenr002
info: Adding user `user5' to group `ihenr002' ...

(root@kali)-[~]
# adduser user6 ihenr002
info: Adding user `user6' to group `ihenr002' ...

(root@kali)-[~]
#
```

Activate Windows
Go to Settings to activate Windows.



Making users 4-6 then adding them to ihenr002 group

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# id user1
uid=1002(user1) gid=1004(user1) groups=1004(user1),1002(cyse301)

(root@kali)-[~]
# id user2
uid=1003(user2) gid=1005(user2) groups=1005(user2),1002(cyse301)

(root@kali)-[~]
# id user3
uid=1004(user3) gid=1006(user3) groups=1006(user3),1002(cyse301)

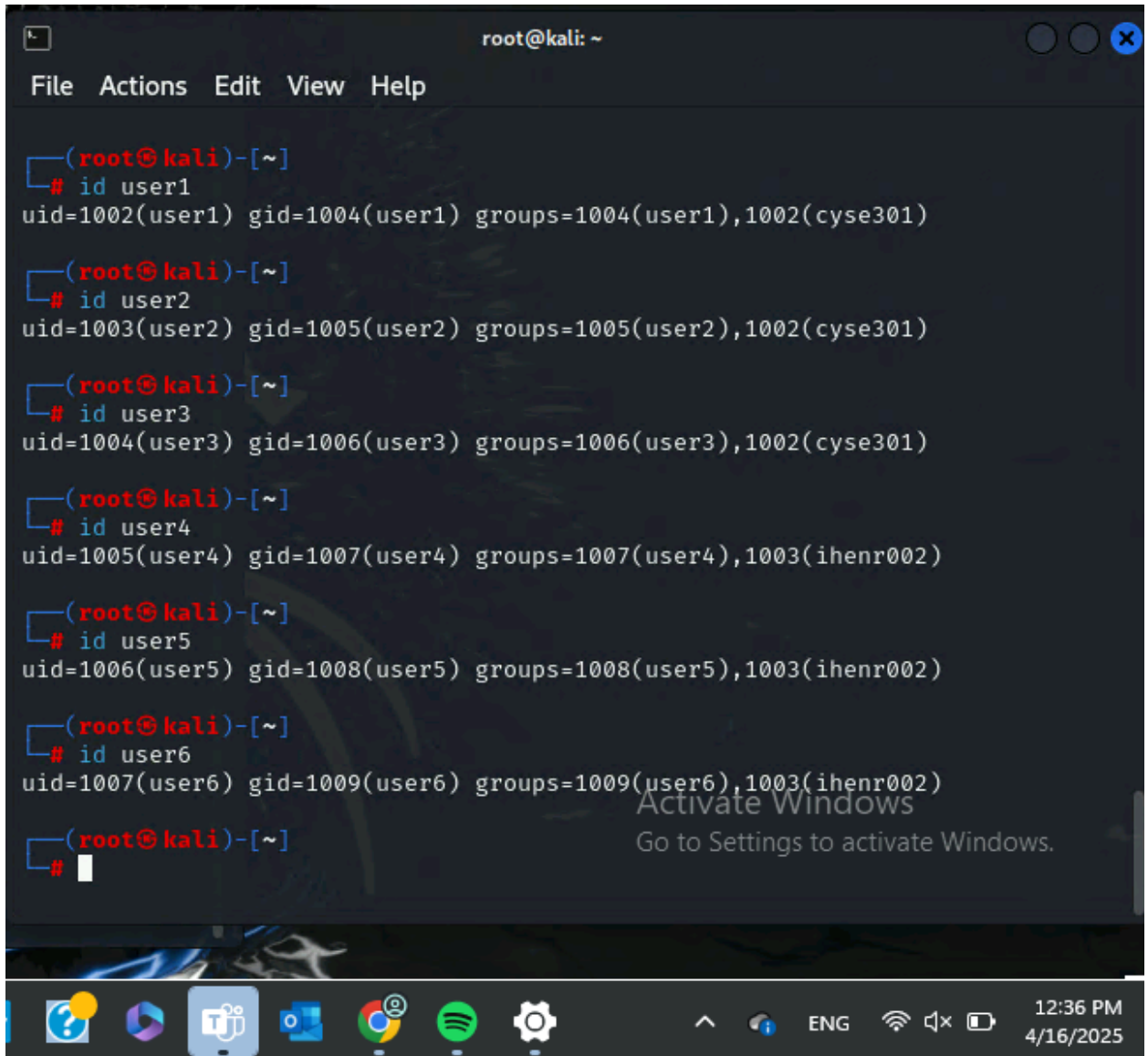
(root@kali)-[~]
# id user4
uid=1005(user4) gid=1007(user4) groups=1007(user4),1003(ihenr002)

(root@kali)-[~]
# id user5
uid=1006(user5) gid=1008(user5) groups=1008(user5),1003(ihenr002)

(root@kali)-[~]
# id user6
uid=1007(user6) gid=1009(user6) groups=1009(user6),1003(ihenr002)

(root@kali)-[~]
#
```

Activate Windows
Go to Settings to activate Windows.



IDing all of the users, and ensuring they're all in the right groups

3. Choose three new passwords, from easy to hard, and assign them to the users you created. You need to show the password you selected in your report, and do not use real passwords.

```
root@kali: ~  
File Actions Edit View Help  
└─# id user5  
uid=1006(user5) gid=1008(user5) groups=1008(user5),1003(ihenr002)  
  
└─(root@kali)-[~]  
└─# id user6  
uid=1007(user6) gid=1009(user6) groups=1009(user6),1003(ihenr002)  
  
└─(root@kali)-[~]  
└─# passwd user1  
New password:  
Retype new password:  
passwd: password updated successfully  
  
└─(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)-[~]  
└─#
```

Activate Windows
Go to Settings to activate Windows.

12:38 PM
4/16/2025

A terminal window titled 'root@kali: ~' with a menu bar containing 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows five sequential password update commands for users 3 through 6. Each command is '# passwd userX', followed by 'New password:', 'Retype new password:', and 'passwd: password updated successfully'. The sixth command is '#', with a cursor. An 'Activate Windows' watermark is visible in the bottom right of the terminal area. The Windows taskbar is at the bottom, showing icons for help, file explorer, terminal, chrome, spotify, and settings, along with system tray icons for volume, network, and battery, and the time '12:39 PM 4/16/2025'.

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

(root@kali)-[~]
└─# passwd user4
New password:
Retype new password:
passwd: password updated successfully

(root@kali)-[~]
└─# passwd user5
New password:
Retype new password:
passwd: password updated successfully

(root@kali)-[~]
└─# passwd user6
New password:
Retype new password:
passwd: password updated successfully

(root@kali)-[~]
└─#
```

User1 password: 1234
User2 password: apple567
User3 password: d!scr33t!
User4 password: beach
User5 password: forget789
User6 password: 0p3r@t!0n@!

4. Export all three users' password hashes into a file named "YourMIDAS-HASH". Then launch a dictionary attack to crack the passwords. You must crack at least one password in order to complete the assignment.

```
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
# sudo tail -6 /etc/shadow
user1:$y$j9T$J2e01B151RxCauVy.WBl4/$GRZc8mQ/VZ0k9rKu2n69c6/DeM86poo5WsRmSe7We
03:20194:0:99999:7:::
user2:$y$j9T$1xRFxQ1FZ7PqiPV77tsZI1$.9wWqp2JEm6knh6qipvGJM5iLwA.ZDDe.T2VV5Ibi
A9:20194:0:99999:7:::
user3:$y$j9T$9tlBiVEKj.WT4Ghi37m6D0$hNPrGNhC26aLs9c4ojc/KxZu59SJpwrjB84GTnnU5
f/:20194:0:99999:7:::
user4:$y$j9T$nDIH9PiAj9LHA0oBk12691$Ajs0Td/D0xnUyViaR3D2mXfKBxNoLsXTMnpI3szZz
OC:20194:0:99999:7:::
user5:$y$j9T$GcBdhwfcYXP/GsrYhHzGe.$e08e7DEtQbeBjH0sPqWzr/gW0brsLOXf6VfgSKXAM
A.:20194:0:99999:7:::
user6:$y$j9T$iRrfwBY567sZhJdFSGIu0/$Y30dhaufKDFX3gzSzpgmXPMKs3FTTJW5CnrzY80Y9
T2:20194:0:99999:7:::


(root@kali)-[~]
# sudo tail -6 /etc/shadow >ihenr002-HASH

(root@kali)-[~]
#
```

Tail -6 /etc/shadow to see new users
Putting the last 6 user's information into the ihenr002-HASH

```
root@kali: ~  
File Actions Edit View Help  
user4:$y$j9T$nDIH9PiAj9LHA0oBk12691$Ajs0Td/D0xnUyViaR3D2mXfKBxNoLsXTMnpI3szZz  
OC:20194:0:99999:7 :::  
user5:$y$j9T$GcBdhwfcYXP/GsrYhHzGe.$e08e7DEtQbeBjH0sPqWzr/gW0brsLOXf6VfgSKXAM  
A.:20194:0:99999:7 :::  
user6:$y$j9T$iRrfwBY567sZhJdFSGIu0/$Y30dhaufKDFX3gzSzpgmXPMks3FTTJW5CnrzY80Y9  
T2:20194:0:99999:7 :::  
  
(root@kali)-[~]  
# sudo tail -6 /etc/shadow >ihenr002-HASH  
  
(root@kali)-[~]  
# cat ihenr002-HASH  
user1:$y$j9T$J2e01B151RxCauVy.WBl4/$GRZc8mQ/VZ0k9rKu2n69c6/DeM86poo5WsRmSe7We  
03:20194:0:99999:7 :::  
user2:$y$j9T$1xRFxQ1FZ7PqiPV77tsZI1$.9wWqp2JEm6knh6qipvGJM5iLwA.ZDDe.T2VV5Ibi  
A9:20194:0:99999:7 :::  
user3:$y$j9T$9tLBiVEKj.WT4Ghi37m6D0$hNPrGNhC26aLs9c4ojc/KxZu59SjpwrbjB84GTnnU5  
f/:20194:0:99999:7 :::  
user4:$y$j9T$nDIH9PiAj9LHA0oBk12691$Ajs0Td/D0xnUyViaR3D2mXfKBxNoLsXTMnpI3szZz  
OC:20194:0:99999:7 :::  
user5:$y$j9T$GcBdhwfcYXP/GsrYhHzGe.$e08e7DEtQbeBjH0sPqWzr/gW0brsLOXf6VfgSKXAM  
A.:20194:0:99999:7 :::  
user6:$y$j9T$iRrfwBY567sZhJdFSGIu0/$Y30dhaufKDFX3gzSzpgmXPMks3FTTJW5CnrzY80Y9  
T2:20194:0:99999:7 :::  
  
(root@kali)-[~]  
#
```

Activate Windows
Go to Settings to activate Windows.



Checking that users are in the file

```
root@kali: ~
File Actions Edit View Help
└─# cp /usr/share/wordlists/rockyou.txt.gz
cp: missing destination file operand after '/usr/share/wordlists/rockyou.txt.gz'
Try 'cp --help' for more information.


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

(root@kali)-[~]
└─# la
.bash_history      .face.icon        .pcsc1            Videos
.bash_logout      .gnupg            Pictures          .wget-hsts
.bashrc           .ICEauthority     .profile         winhash
.bashrc.original  ihenr002-HASH    Public           .Xauthority
.BurpSuite        .java            .rnd             .xorgxrdp.1.log
.cache            .john            rockyou.txt.gz   .xorgxrdp.1.log.old
.config           .lessht         shared-drives    .xsession-errors
Desktop           .local           .smbcredentials .zsh_history
Documents         .mozilla        .splunk          .zshrc
Downloads         .msf4           .ssh
.face             Music           Templates

(root@kali)-[~]
└─# gunzip rockyou.txt.gz

(root@kali)-[~]
└─#
```

Activate Windows
Go to Settings to activate Windows.



Adding rockyou file and unzipping it

```
(root@kali)-[~]
└─# john --format=crypt -wordlist=rockyou.txt ihenr002-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) 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
beach (user4)
```

Activate Windows
Go to Settings to activate Windows.

