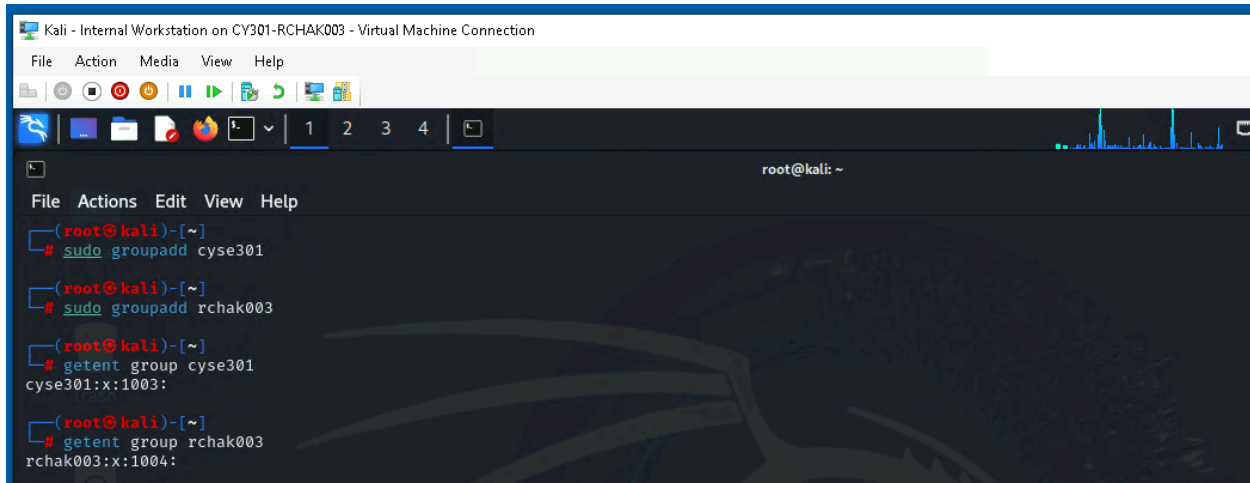


CYSE 301: Cybersecurity Technique and Operations

Assignment 5: Password Cracking (Part A)

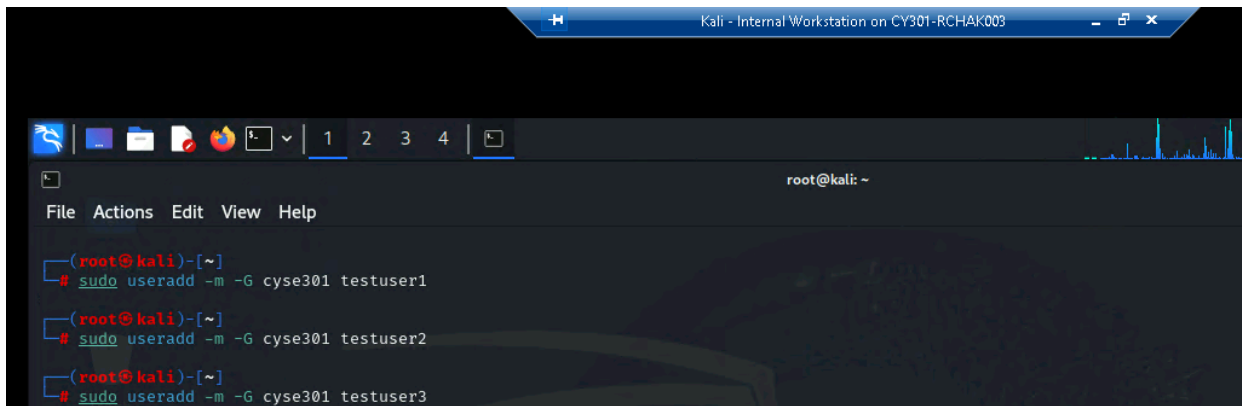
Task A: Linux Password Cracking (25 points)

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.

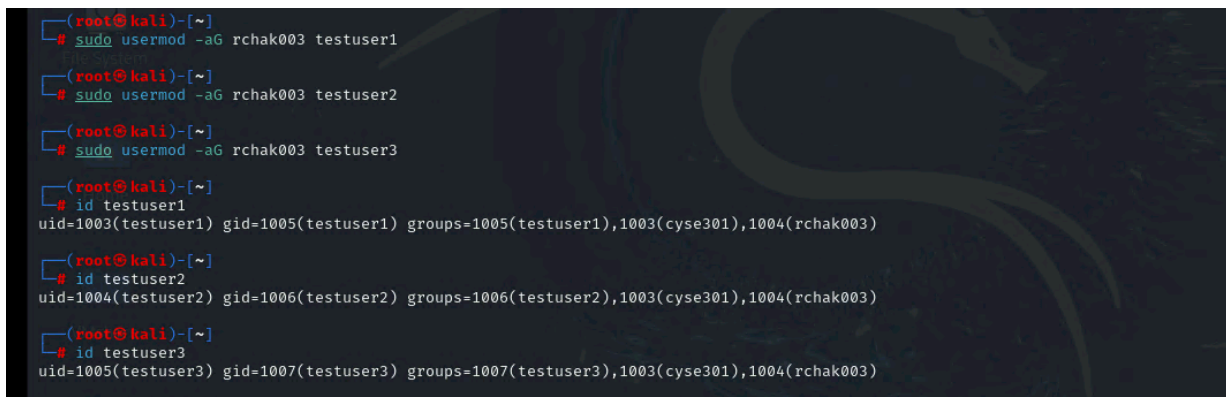


```
Kali - Internal Workstation on CY301-RCHAK003 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# sudo groupadd cyse301
(root@kali)-[~]
# sudo groupadd rchak003
(root@kali)-[~]
# getent group cyse301
cyse301:x:1003:
(root@kali)-[~]
# getent group rchak003
rchak003:x:1004:
```

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

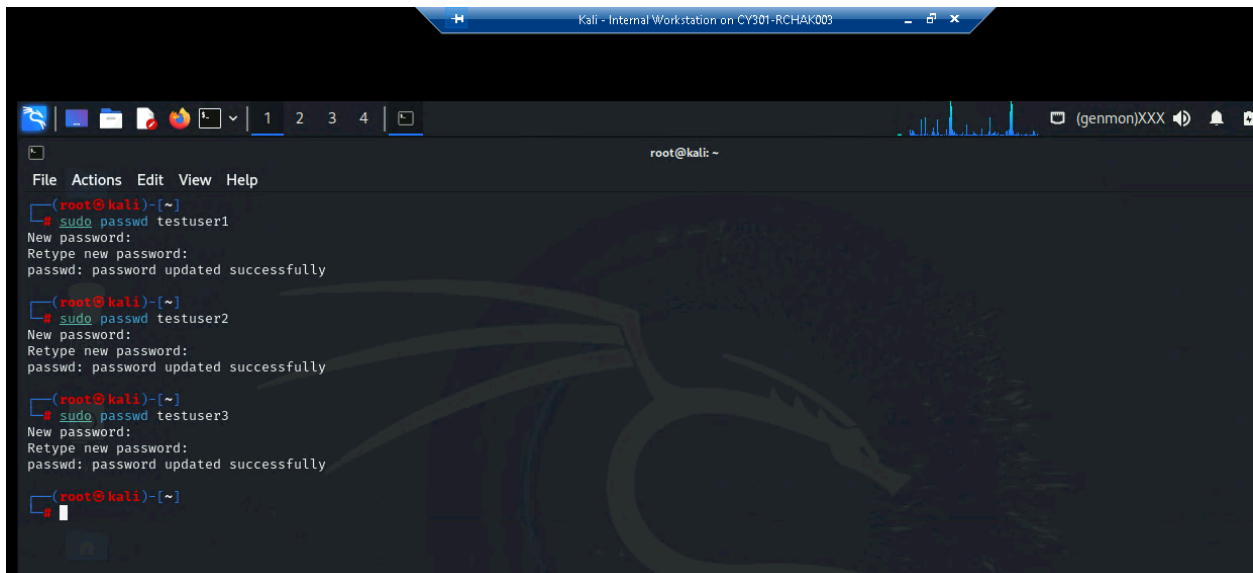


```
Kali - Internal Workstation on CY301-RCHAK003
root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# sudo useradd -m -G cyse301 testuser1
(root@kali)-[~]
# sudo useradd -m -G cyse301 testuser2
(root@kali)-[~]
# sudo useradd -m -G cyse301 testuser3
```



```
(root@kali)-[~]
# sudo usermod -aG rchak003 testuser1
(root@kali)-[~]
# sudo usermod -aG rchak003 testuser2
(root@kali)-[~]
# sudo usermod -aG rchak003 testuser3
(root@kali)-[~]
# id testuser1
uid=1003(testuser1) gid=1005(testuser1) groups=1005(testuser1),1003(cyse301),1004(rchak003)
(root@kali)-[~]
# id testuser2
uid=1004(testuser2) gid=1006(testuser2) groups=1006(testuser2),1003(cyse301),1004(rchak003)
(root@kali)-[~]
# id testuser3
uid=1005(testuser3) gid=1007(testuser3) groups=1007(testuser3),1003(cyse301),1004(rchak003)
```

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.



```
(root@kali)-[~]
└─# sudo passwd testuser1
New password:
Retype new password:
passwd: password updated successfully

(root@kali)-[~]
└─# sudo passwd testuser2
New password:
Retype new password:
passwd: password updated successfully

(root@kali)-[~]
└─# sudo passwd testuser3
New password:
Retype new password:
passwd: password updated successfully

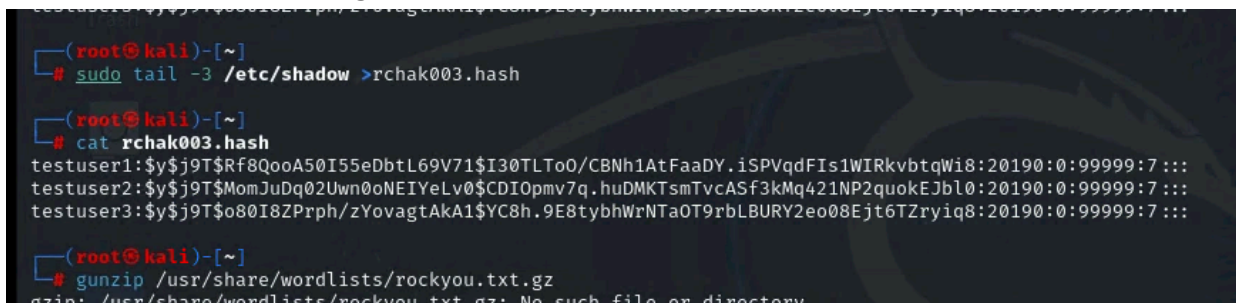
(root@kali)-[~]
└─#
```

Testuser1: password

Testuser2: password123

Testuser3: password-123

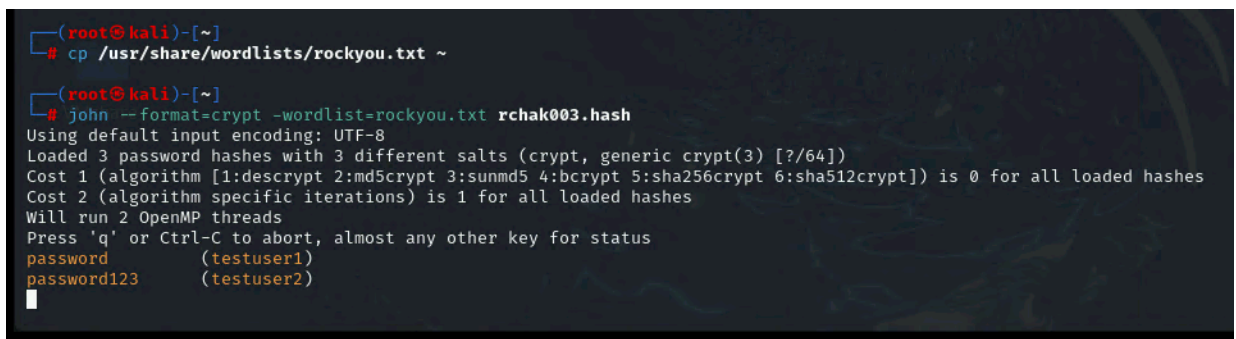
4. 5 points. Export all Three users' password hashes into a file named "YourMIDAS-HASH" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



```
(root@kali)-[~]
└─# sudo tail -3 /etc/shadow >rchak003.hash

(root@kali)-[~]
└─# cat rchak003.hash
testuser1:$y$j9T$Rf8QooA50I55eDbtL69V71$I30TLTo0/CBNh1AtFaaDY.iSPVqdFIs1WIRkvbqWi8:20190:0:99999:7:::
testuser2:$y$j9T$MomJuDq02Uwn0oNEIYeLv0$CDIOpmv7q.huDMKtSmTvcASf3kMq421NP2quoKEJbl0:20190:0:99999:7:::
testuser3:$y$j9T$o80I8ZPrph/zYovagtAkA1$YC8h.9E8tybhWrNTaOT9rbLBURY2eo08Ejt6TZryiq8:20190:0:99999:7:::

(root@kali)-[~]
└─# gunzip /usr/share/wordlists/rockyou.txt.gz
gzip: /usr/share/wordlists/rockyou.txt.gz: No such file or directory
```



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

(root@kali)-[~]
└─# john --format=crypt -wordlist=rockyou.txt rchak003.hash
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) 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
password      (testuser1)
password123   (testuser2)
```

NOTE: I was able to successfully crack 2 passwords.