

TASK A Linux Password Cracking:

1.

```
(root@kali)~#  
# sudo groupadd cyse301  
  
(root@kali)~#  
# sudo groupadd swood041  
  
(root@kali)~#  
# tail /etc/group -n 6  
=> / <=>  
tail: error reading '/': Is a directory  
tail: cannot open 'etc/group' for reading: No such file or directory  
  
(root@kali)~#  
# tail /etc/group --n 6  
xrdp:x:138:  
snort:x:139:  
syslog:x:140:  
splunk:x:1001:  
cyse301:x:1002:  
swood041:x:1003:
```

2.

```
(root@kali)~#  
# sudo useradd John -g cyse301  
  
(root@kali)~#  
# sudo useradd Danny -g cyse301  
  
(root@kali)~#  
# sudo useradd Mary -g cyse301  
  
(root@kali)~#  
# sudo useradd Tom -g swood041  
  
(root@kali)~#  
# sudo useradd Jacob -g swood041  
  
(root@kali)~#  
# sudo useradd Darla -g swood041  
  
(root@kali)~#  
# cat /etc/passwd | grep home  
kali:x:1000:1000:::/home/kali:/usr/bin/zsh  
John:x:1002:1002::/home/John:/bin/sh  
Danny:x:1003:1003::/home/Danny:/bin/sh  
Mary:x:1004:1004::/home/Mary:/bin/sh  
Tom:x:1005:1005::/home/Tom:/bin/sh  
Jacob:x:1006:1006::/home/Jacob:/bin/sh  
Darla:x:1007:1007::/home/Darla:/bin/sh
```

3.

```
(root@kali)~#  
# passwd John  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root@kali)~#  
# passwd Danny  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root@kali)~#  
# passwd Mary  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root@kali)~#  
# passwd Tom  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root@kali)~#  
# passwd Jacob  
New password:  
Retype new password:  
passwd: password updated successfully  
  
(root@kali)~#  
# passwd Darla  
New password:
```

Continues Below

CYSE 301 GROUP

- John - password
- Danny - password123
- Mary - apples123

SWOOD041 GROUP

- Tom - Apples123!
- Jacob - PURPLE_p1um5!?
- Darla - GRe3n!aPP1ez_?501

4.

```

root@kali:~# tail -n 7 /etc/shadow > lab4shadow.txt

root@kali:~# ls -lt
total 204
-rw-r--r-- 1 root root 618 Jul 12 22:20 lab4shadow.txt
drwx----- 1 root root 0 Jul 12 21:53 shared-drives
-rw-r--r-- 1 root root 77093 Jul 6 01:56 wklsu08.jpeg
-rw-r--r-- 1 root root 73802 Jul 5 23:32 smood041.exe
-rw-r--r-- 1 root root 15237 Jul 5 19:56 000031m.jpeg
drwxr-xr-x 3 root root 4096 May 31 2024 Desktop
drwxr-xr-x 2 root root 4096 May 31 2024 Public
drwxr-xr-x 2 root root 4096 May 30 2024 Downloads
drwxr-xr-x 2 root root 4096 Feb 23 2024 Documents
drwxr-xr-x 2 root root 4096 Feb 23 2024 Music
drwxr-xr-x 2 root root 4096 Feb 23 2024 Pictures
drwxr-xr-x 2 root root 4096 Feb 23 2024 Templates
drwxr-xr-x 2 root root 4096 Feb 23 2024 Videos

root@kali:~# cp /usr/share/wordlists/rockyou.txt /usr/share/wordlists/rockyou.txt
cp: making destination file overrid after "/usr/share/wordlists/rockyou.txt"
Try "cp --help" for more information.

root@kali:~# cp /usr/share/wordlists/rockyou.txt /usr/share/wordlists/rockyou.txt

root@kali:~# ls -lt
total 10684
-rw-r--r-- 1 root root 10961587 Jul 12 22:22 rockyou.txt
-rw-r--r-- 1 root root 618 Jul 12 22:20 lab4shadow.txt
drwx----- 1 root root 0 Jul 12 21:53 shared-drives
-rw-r--r-- 1 root root 77093 Jul 6 01:56 wklsu08.jpeg
-rw-r--r-- 1 root root 73802 Jul 5 23:32 smood041.exe
-rw-r--r-- 1 root root 15237 Jul 5 19:56 000031m.jpeg
drwxr-xr-x 3 root root 4096 May 31 2024 Desktop
drwxr-xr-x 2 root root 4096 May 31 2024 Public
drwxr-xr-x 2 root root 4096 May 30 2024 Downloads
drwxr-xr-x 2 root root 4096 Feb 23 2024 Documents
drwxr-xr-x 2 root root 4096 Feb 23 2024 Music
drwxr-xr-x 2 root root 4096 Feb 23 2024 Pictures
drwxr-xr-x 2 root root 4096 Feb 23 2024 Templates
drwxr-xr-x 2 root root 4096 Feb 23 2024 Videos

```

↓

```

root@kali:~# john lab4shadow.txt --wordlist=rockyou.txt --format=crypt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [7/64])
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 (John)
password123 (Danny)
2g 0:00:10:05 0.10% (ETA: 2026-07-19 16:16) 0.003305g/s 29.51p/s 120.5c/s 120.5C/s josiah1...220688
2g 0:00:10:19 0.11% (ETA: 2026-07-19 16:33) 0.003229g/s 29.45p/s 120.5c/s 120.5C/s soylomaximo...coolio1
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

```

Using John the Ripper, I was able to crack 2 passwords within roughly 10-15 minutes.

TASK B Windows Password Cracking:

1. Creating Accounts

```
meterpreter > snell
Process 3248 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user thor password /add
net user thor password /add
The command completed successfully.

C:\Windows\system32>net user batman password123 /add
net user batman password123 /add
The command completed successfully.

C:\Windows\system32>net user robin apples /add
net user robin apples /add
The command completed successfully.
```

Hashdump

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
batman:1008:aad3b435b51404eeaad3b435b51404ee:a9fdfa038c4b75ebc76dc855dd74f0da :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79cf757c09bad3139f56290e444b23 :::
robin:1009:aad3b435b51404eeaad3b435b51404ee:e2e8dc9cf11072f9a29d6b5c1c83302 :::
Sam:1003:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
thor:1007:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c :::
user1:1004:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
user2:1005:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
user3:1006:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b :::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c :::
```

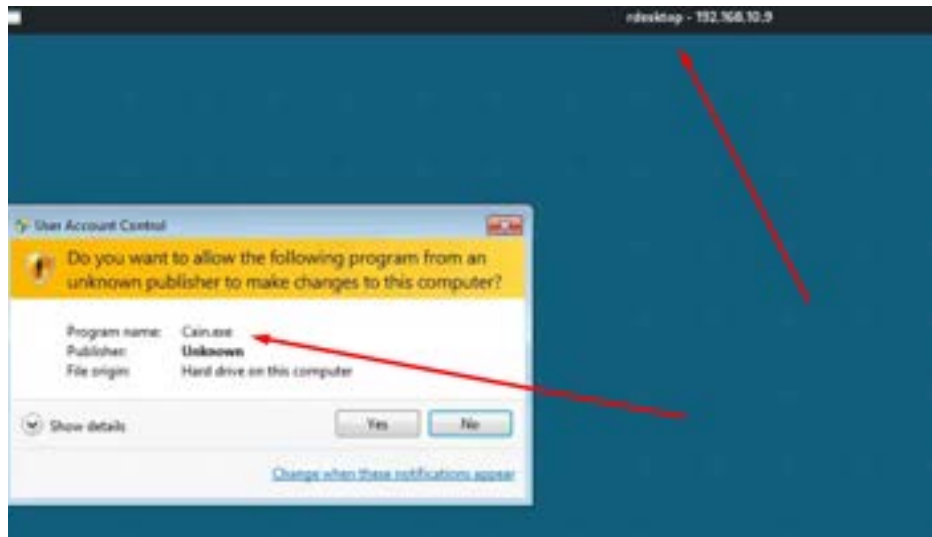
Pasting hashes into WinHash.txt

[illegible]

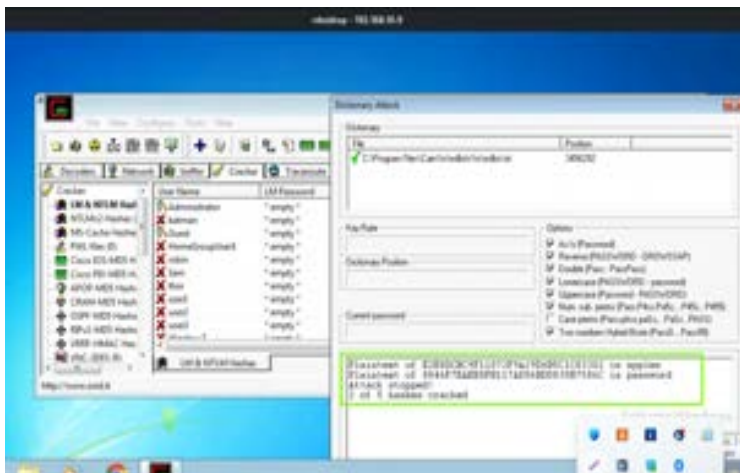
2.

```
(root@kali)~#  
# john WinHash.txt --wordlist-rockyou.txt --format-crypt  
Warning: hash encoding string length 32, type id #0  
appears to be unsupported on this system; will not load such hashes.  
Using default input encoding: UTF-8  
No password hashes loaded (see FAQ)  
  
(root@kali)~#  
# john --format-NT --wordlist-rockyou.txt WinHash.txt  
Using default input encoding: UTF-8  
Loaded 3 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
password (thor)  
apples (robin)  
password123 (batman)  
3g 0:00:00:00 DONE (2026-07-12 23:30) 60.00g/s 30720p/s 30720c/s 46080C/s 753951..mexico1  
Use the "--show --format-NT" options to display all of the cracked passwords reliably  
Session completed.
```

3. Run Cain and Able from RDP



DICTIONARY



BRUTE FORCE

