Old Dominion University

CYSE 301 Cybersecurity Techniques and Operations

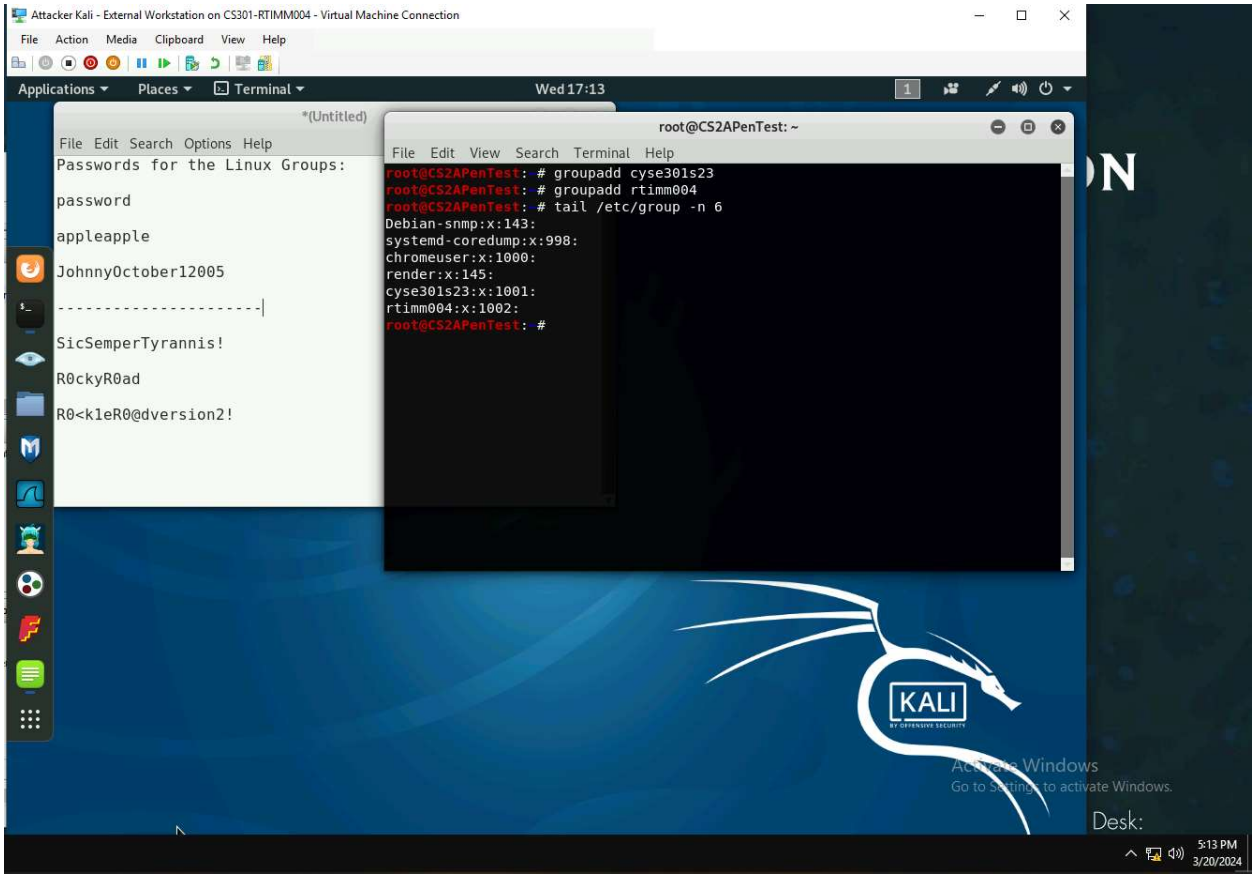
Assignment #5 Password Cracking

Robert Timmons

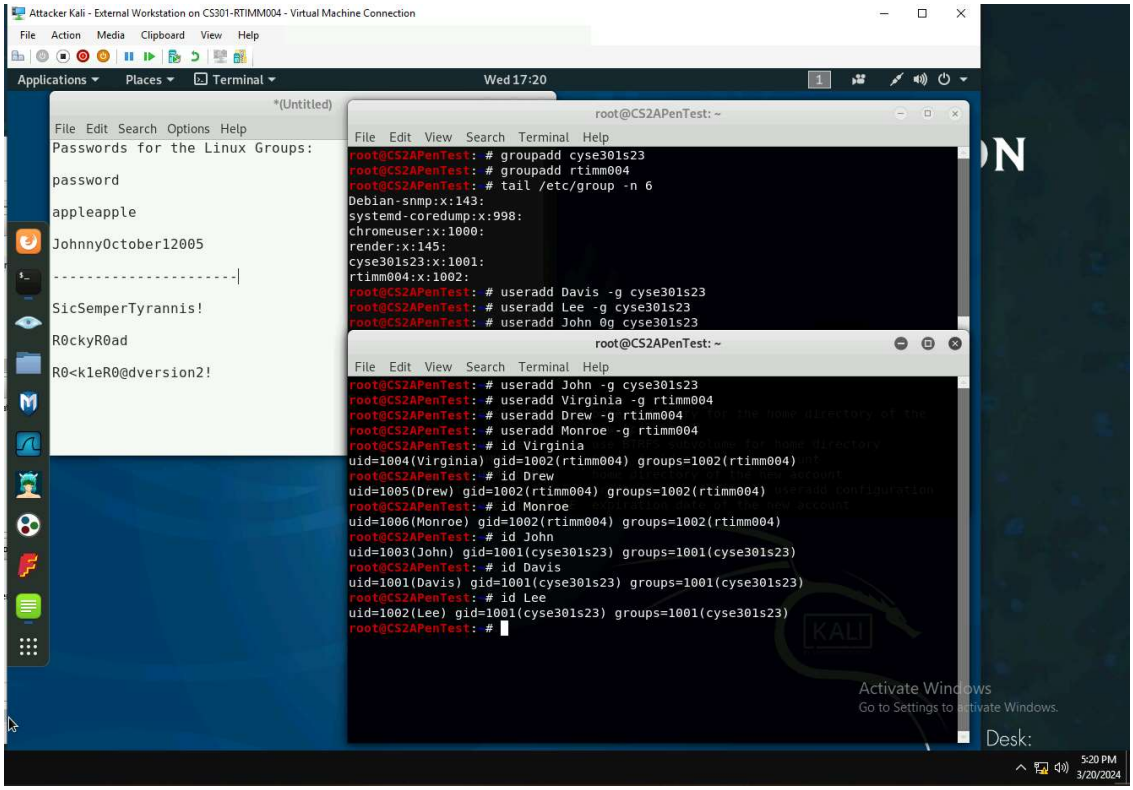
00910166

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!!!!)

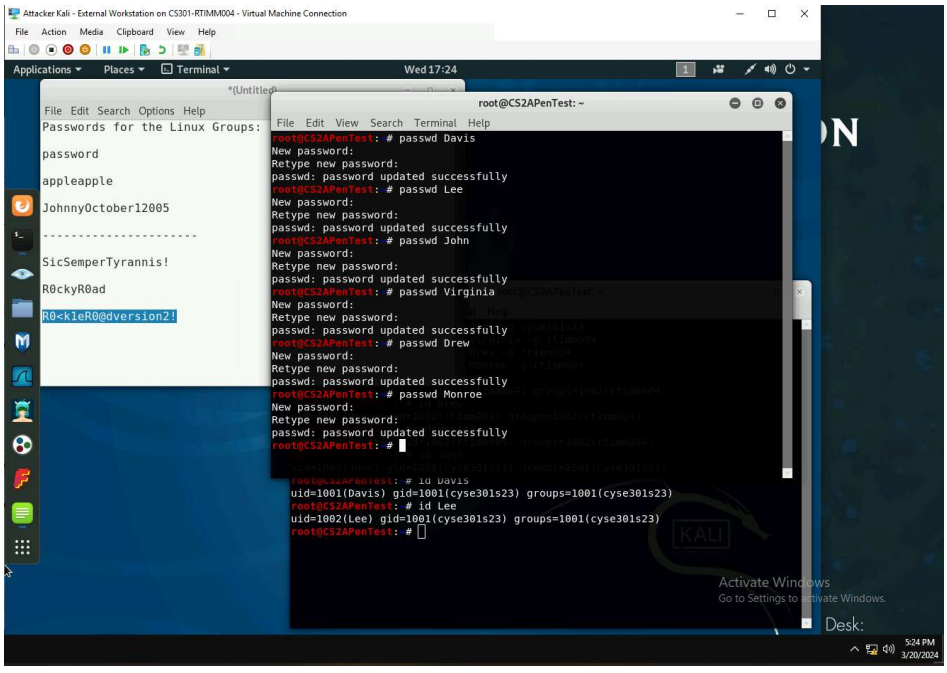


2. Create and assign three users to each group. Display UID and GID info for each user.

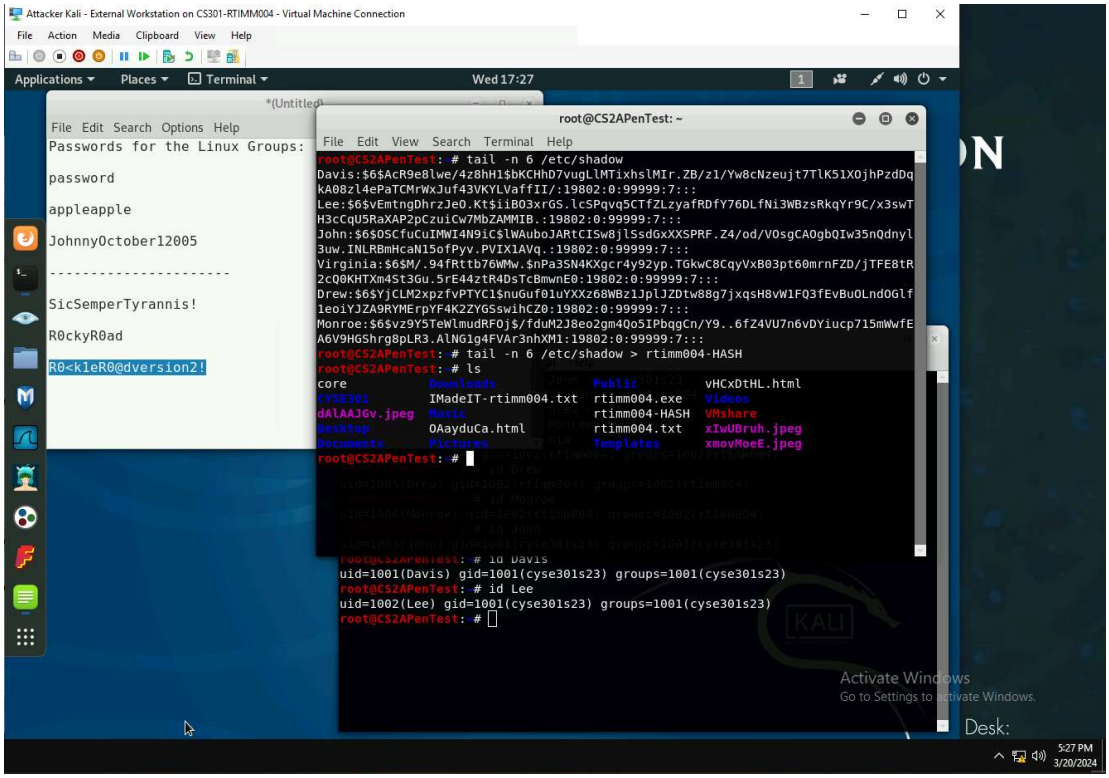


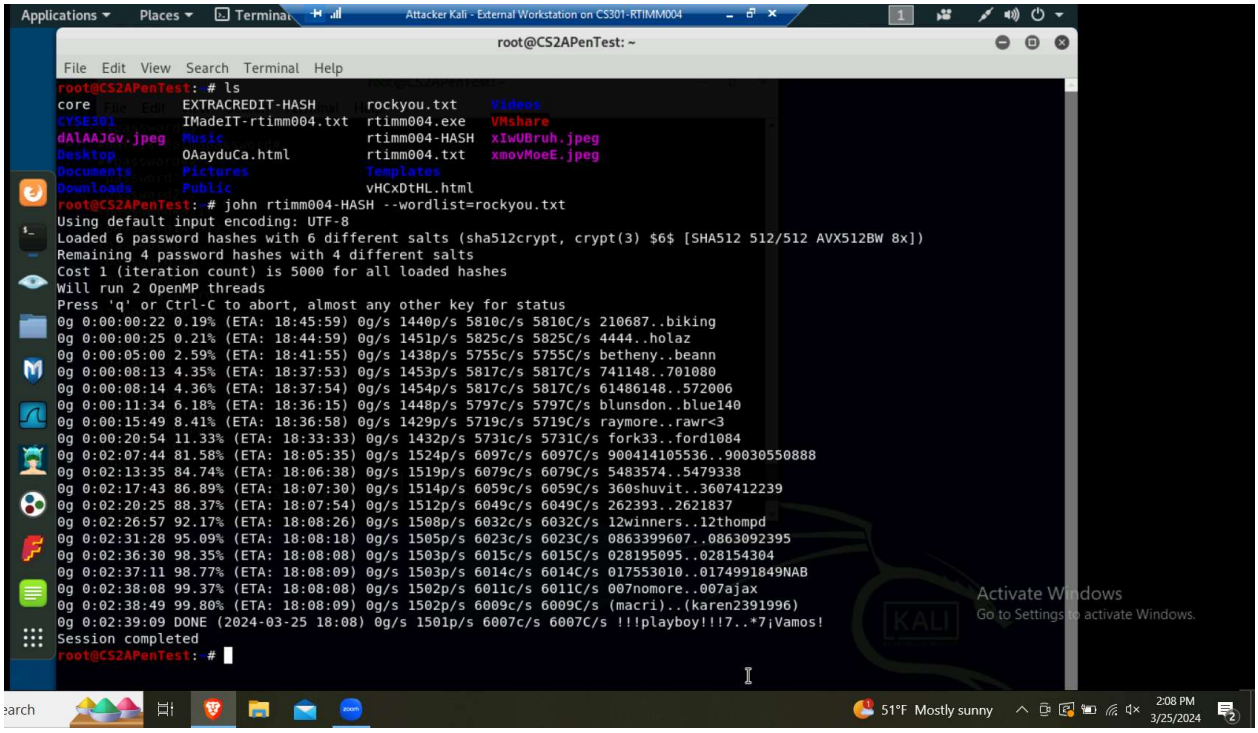
3. Choose Six new passwords, from easy to hard, and assign them to the users you created. Display passwords.

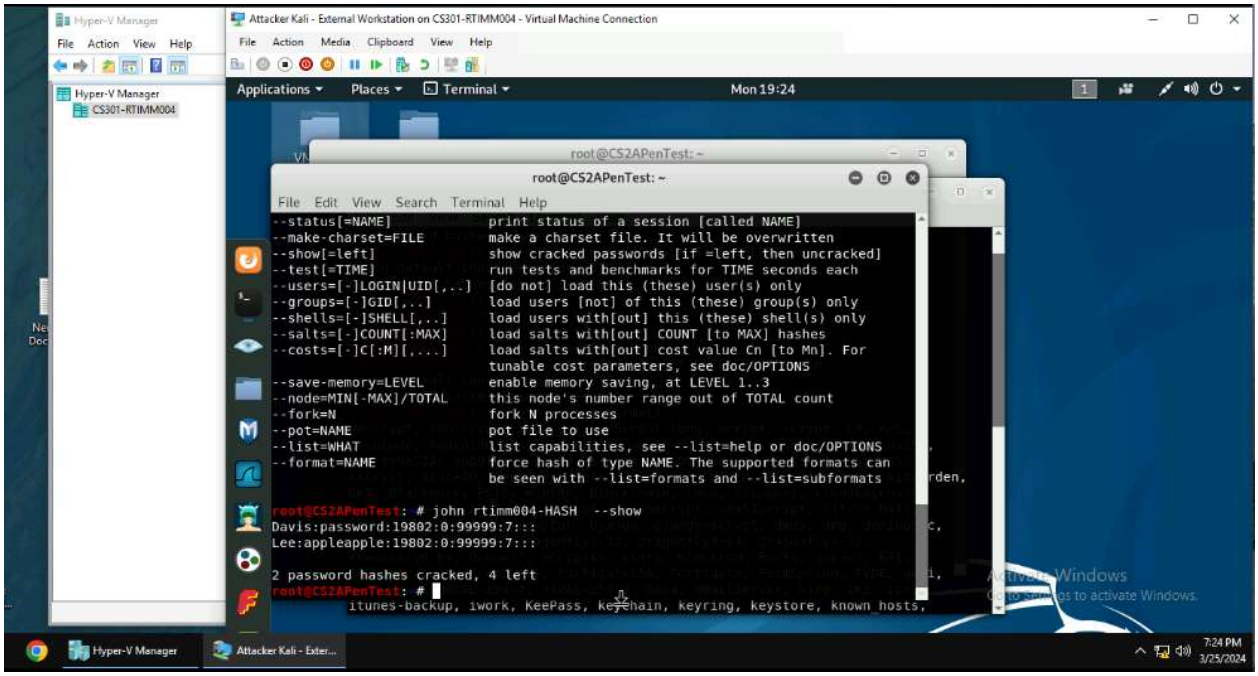
(You can see I left the passwords in a txt file on the side, just to show.)



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.)



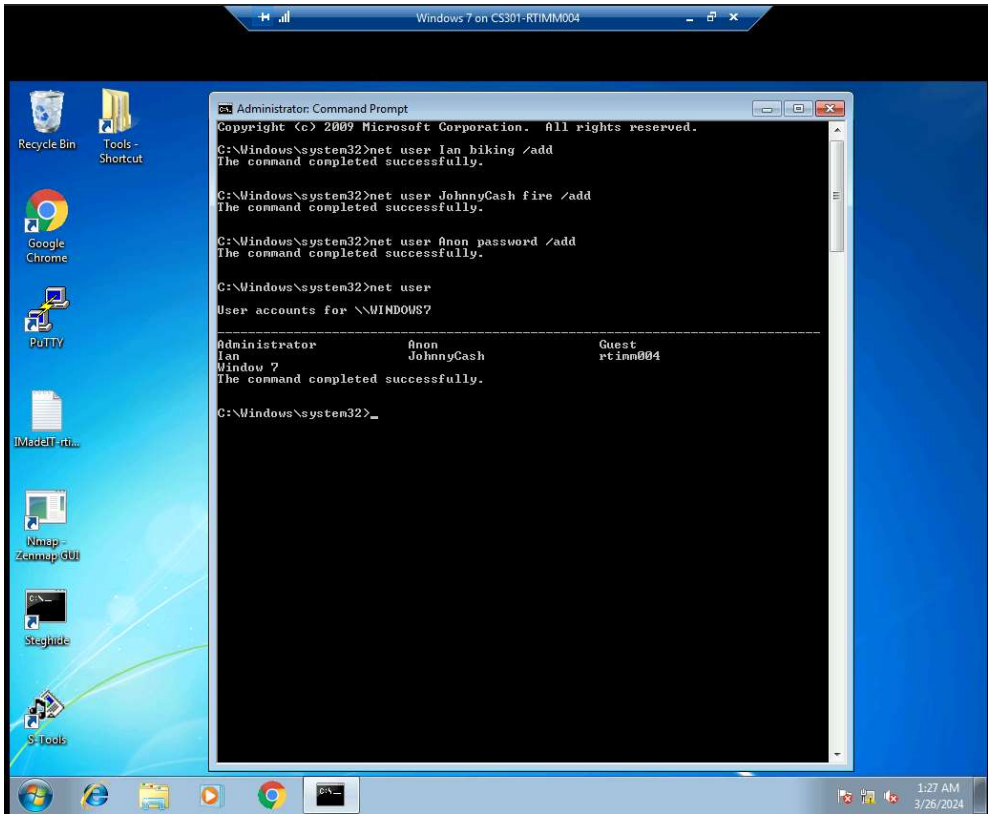

Applications
Places
Terminal
Attacker Kali - External Workstation on CS301-RTIMM004
root@CS2APenTest: ~
File Edit View Search Terminal Help
root@CS2APenTest: # ls
core EXTRACREDIT-HASH rockyou.txt Videos
CYSE301 IMadeIT-rtimm004.txt rtimm004.exe VMshare
dAlAAJGv.jpeg Music rtimm004-HASH xIwUBruh.jpeg
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 0:00:05:00 2.59% (ETA: 18:41:55) 0g/s 1438p/s 5755c/s 5755C/s betheny..beann
0g 0:00:08:13 4.35% (ETA: 18:37:53) 0g/s 1453p/s 5817c/s 5817C/s 741148..701080
0g 0:00:08:14 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 028195095..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..*7¡Vamos!
Session completed
root@CS2APenTest: #
Activate Windows
Go to Settings to activate Windows.
51°F Mostly sunny
2:08 PM
3/25/2024


Hyper-V Manager
File Action View Help
Hyper-V Manager
CS301-RTIMM004
Attacker Kali - External Workstation on CS301-RTIMM004 - Virtual Machine Connection
File Action Media Clipboard 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: #
itunes-backup, iwork, KeePass, keychain, keyring, keystore, known_hosts,
Activate Windows
Hyper-V Manager
Attacker Kali - Exter...
7:24 PM
3/25/2024

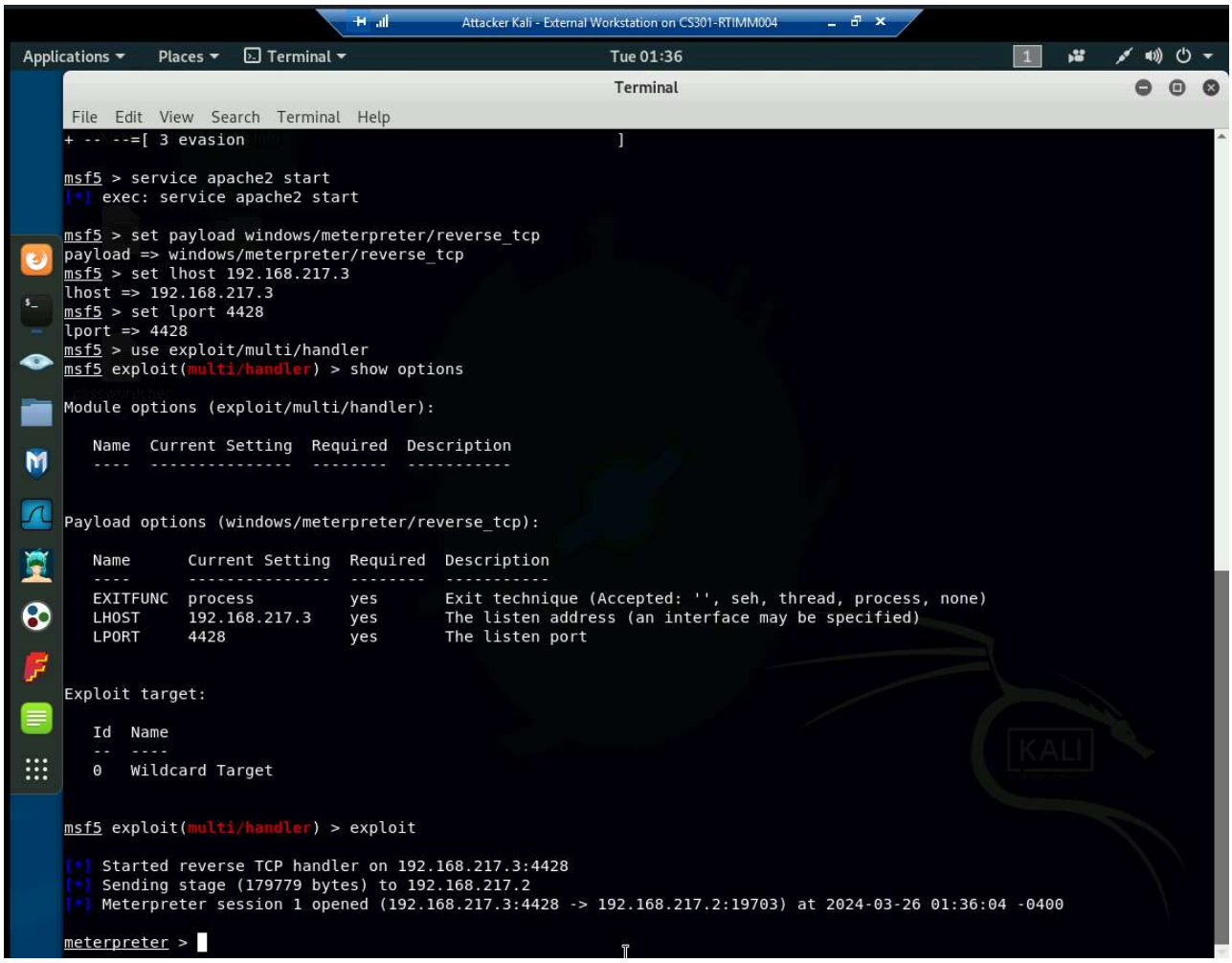
TASK B

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.

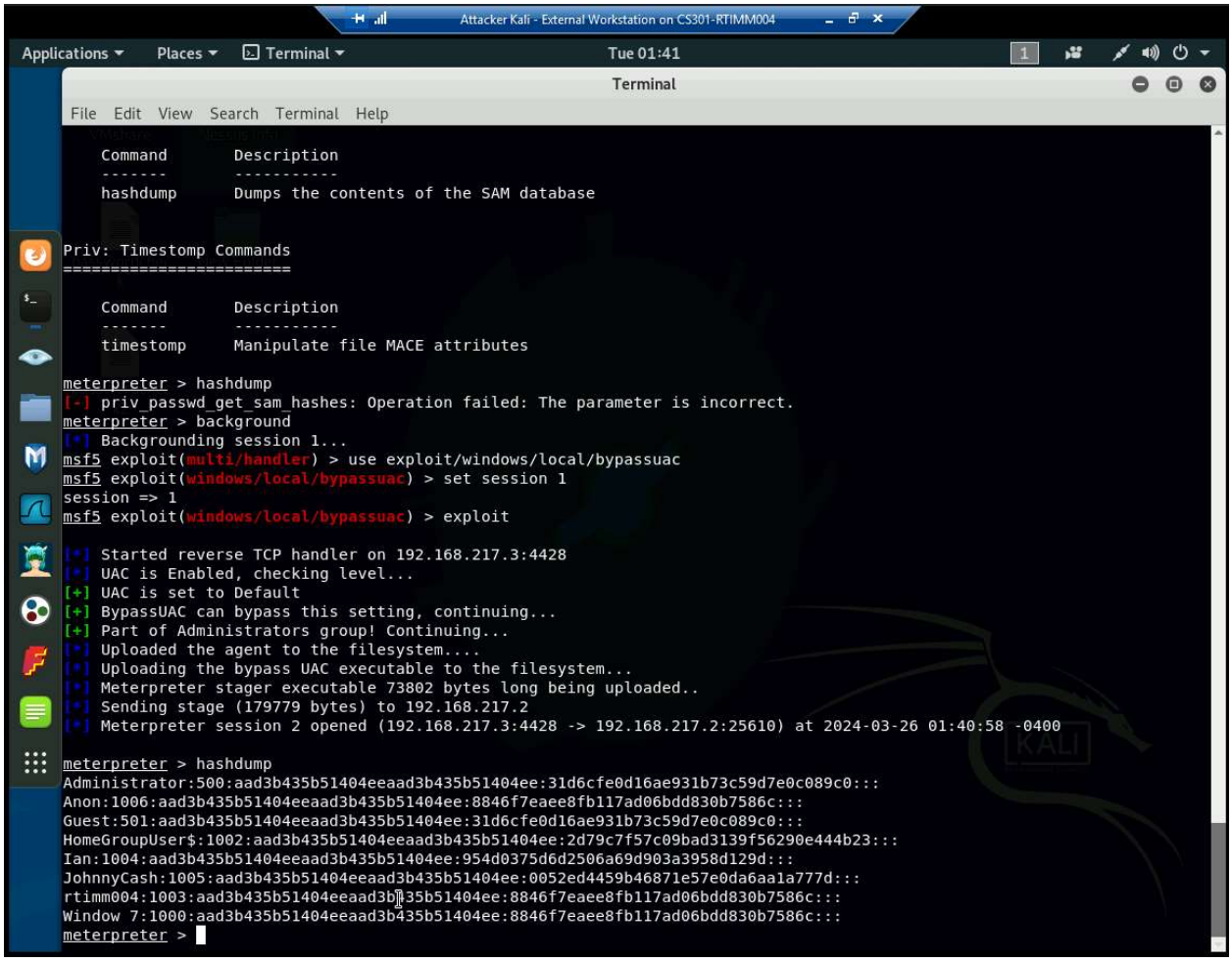


I’m using the previous exploits we learned to get into the windows 7 machine. The malicious file from the last lab is still on the device.

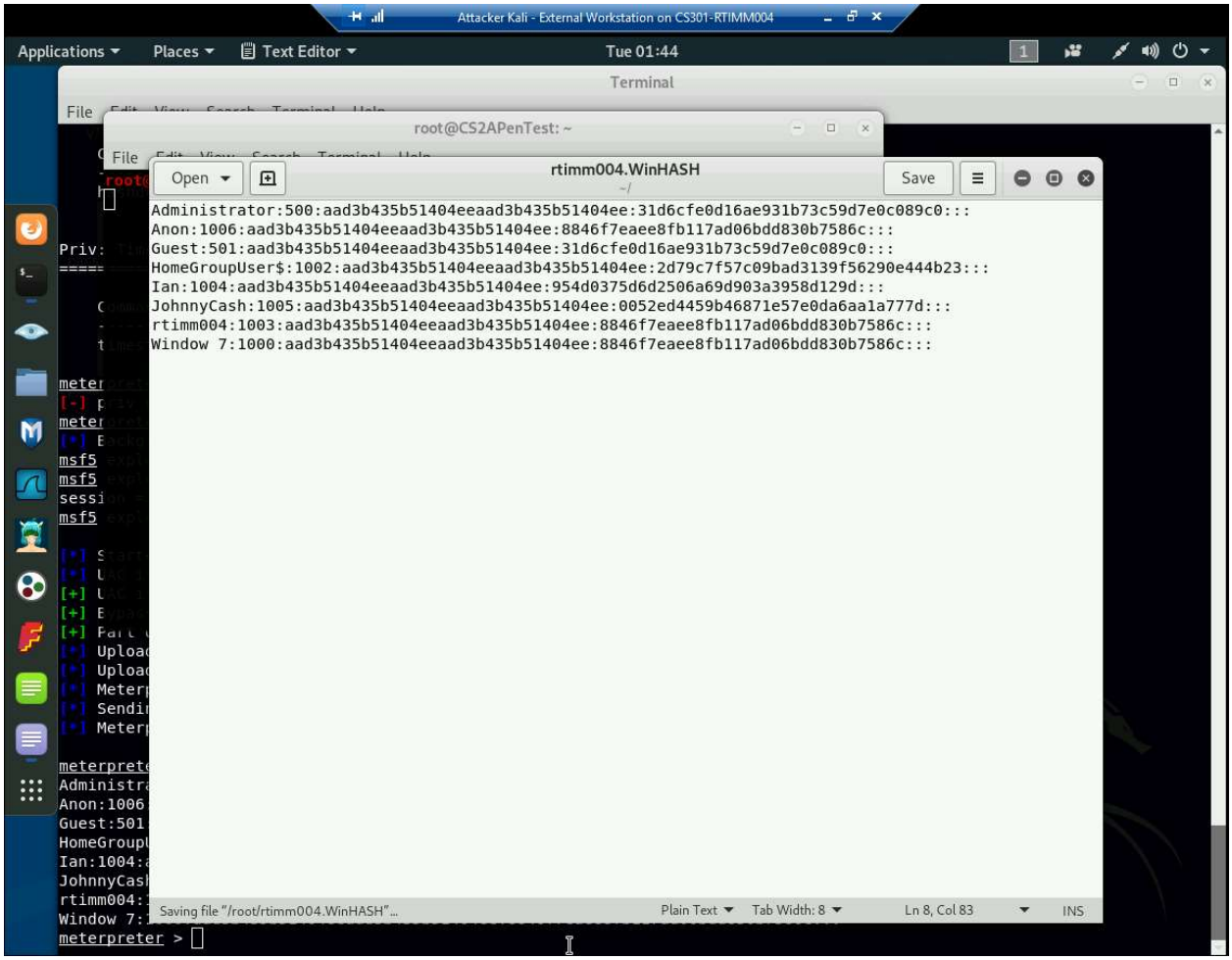


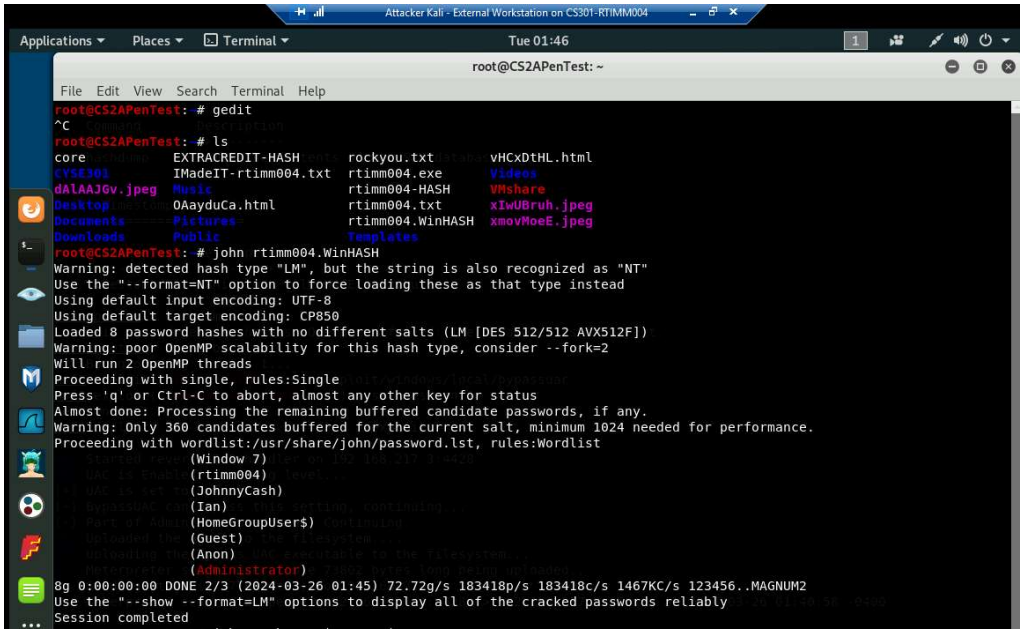
2. Display the password hashes by using the ‘hashdump’ command in the meterpreter shell

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



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 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.