**Devel Walkthrough – HackTheBox(Easy)**

A screenshot of a computer

Description automatically generated with medium confidence

**Step 1 – Recon(Reconnaissance)**

Text

Description automatically generatedFirst, we will scan the endpoint using **Nmap**.

So, from the above scanning we figure out that the target OS is windows.

Moreover, we can notice that we have 2 open ports to make use of, 21 and 80,

FTP(through Microsoft ftpd service),HTTP(through Microsoft IIS httpd 7.5 service). We can see that FTP allows us to login anonymously, we may make use of it later…

Let us take a look at the webserver on port 80.

A screenshot of a computer

Description automatically generated with medium confidenceThis is what we get:

There is nothing unique here, except the hyper-link in the center of the page.

We will try to discover hidden endpoints through enumerating the target.

**Sub Step – Enumeration**

We will take advantage of **gobuster** tool for this purpose.

Text

Description automatically generated

Unfortunately, from this common wordlist we achieved only a single endpoint.

Trying to access this endpoint yields us the following page:

Graphical user interface, text, application, email

Description automatically generatedApparently, we do not have any access to it.

We should try to gain access through ftp.

Graphical user interface, text, application, email

Description automatically generatedAfter some digging, I found out the default login credentials for anonymous FTP login.

After trying it, we managed to access the system.

**Trying to exploit the FTP service to gain privileges**

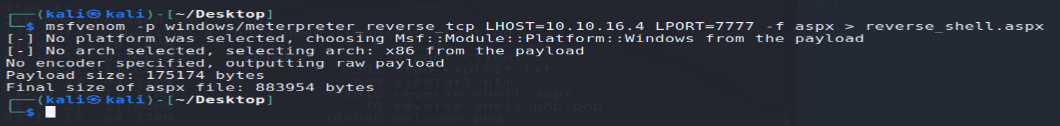
Text

Description automatically generated

By trying to upload files to the machine, we can see that some files are indeed uploaded, and can be executed through the website the machine hosts on port 80.

Once logged in ftp server anonymously tried to list the content of the ftp folder and found files iisstart.htm & welcome.png inside it. Guessed these may be webserver’s files, which is running over port 80. Ongoing to URL http://10.10.10.5/iisstart.htm and http://10.10.10.5/welcome.png it is confirmed that we have access to all the files of this folder. So, indeed these are the webserver files, but we cannot access all of them. I tried to upload a simple txt file through ftp and successfully uploaded it and uploaded file can be accessed at url http://10.10.10.5/myfile.txt . This is an example: Then tried to upload php webshell shell.php. It uploaded successfully but if we try to access, the shell at URL http://10.10.10.5/shell.php where it is supposed to present but, it gives 404 error.

This error may be due to php is not installed on the webserver. Since, it is IIS server so it generally host asp or apsx file. Tried to upload an aspx file and the uploaded file can be easily accessed directly at the url http://10.10.10.5/aspxfile.aspx. So here, we have confirmed that we can upload an aspx file and can access it. So made an aspx reverse shell using msfvenom and uploaded it on ftp server. You can get a list of reverse shell cheat sheet here.



after executing the reverse shell through **curl**, we achieved an initial foothold!

not wget, but curl…

The **curl** command transfers data from any server over to your computer. Whereas the **wget** command downloads the data as a file. This is the major difference ...

Once we have uploaded our reverse shell reverse.aspx to the webserver our next step should be to start our listener on msfconsole and set the payload. Therefore, started exploit/multi/handler on msfconsole and set the payload to it in one window. And executed the URL http://10.10.10.5/reverse.aspx in another window. You can also open the URL in the browser to access it.

Text

Description automatically generated with low confidence

Text

Description automatically generated

As we can notice, we are not granted any access to each of these folders.

Therefore, we will have to elevate/escalate our privileges in the compromised system.

Text

Description automatically generated**Intermediary Step – Privilege Escalation(Through Post Exploitation)**



It looks like that the machine is vulnerable due to the face that it has OS of WIN7 installed on it.

We will look for local exploits using the suggester exploit module in msf.

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

A picture containing graphical user interface

Description automatically generated



Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

We managed to escalate our privileges! we used our session before in order to inject a dll into the victim, results in admin capabilities

All we left to do is getting the relevant files:

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Devel has been Pwned successfully!!!!!**