**Nibble Walkthrough (Hack the Box)**

1.make the directory of that particular box- mkdir –

2.ping 10.10.10.?- to check that host is up or not,

3.nmap scan- nmap -sc -sv -oa nmap 10.10.10.? -to just check what ports are open

Here we can see few of the ports are open like 22 and 80

4.Now just fire up the firefox -10.10.10.75- we went on that found hello world and the by checking its source code we got the nibbleblog directory,

5.by putting 10.10.10.75/nibbleblog- we have got some of the results.

6.so after doing that we look more into directory (the one which we found initially) by using gobuster- gobuster dir -u [http://10.10.10.75/nibbleblog -w /usr/share/wordlists/dirb/common.txt](http://10.10.10.75/nibbleblog%20-w%20/usr/share/wordlists/dirb/common.txt) -x txt,php

7. we can also do nikto to find important directories- nikto -h <http://10.10.10.75/nibbleblog/>

8.After getting results from gobuster we found some of the directories like admin.php, admin, contents and all by searching the we got some results out of it too, and in contents one we got user.xml, by clicking on it we have got admin there which is a username so we just need to find password to get in,

9.we can find passowrds by brute forcing through hydra but it can give us some false positives, so by searching on google we found the password of the box.

10.by going on /admin.php, and after entering the credentials we got in

11.we can search the nibble blog and its versions exploits, and we found one from packet strom where we need to follow the proof of concept, after copying that URL and also don’t forget to edit the URL and paste it on your firefox and you will get some result.

12. we can see image folder and configure it but before that you have to follow some steps,

13 we have to locate php-revese-shell.php (this tool designed for those situations during pen-test where you have upload access to a web server that’s running php, upload the script to somewhere in the web root then run it by accessing the appropriate URL in your browser.

14.cp it to your convenient directory and then we have rename it to image.php by mv php-reverse-shell.php image.php, we are dong this because we can upload the file in that form only.

15.we will do nano image.php by this we can edit the ip address and port and save that,

16.we will set up a nc -lvnp 1234 (netcat lister to get the shell)

17 now we will upload that file (first we need to verify the file by cat image.php) and also in proof of concept they said that ignore the warning now go to the last URL in proof of concept and paste it in firefox by refresh it we will see we get the shell.(nc-lvnp 1234)

18.then we do python3 -c ‘import pty;pty.spawn(“/bin/bash’)’

And the ctrl z and do stty raw -echo start the netcat listener again and you are in perfectly,

* cd /home,
* ls,
* cat user.txt

19.

Now we are moving forward for root file,

Cd /root -permission denied then sudo -l, we got some information,

We can run some file here with root permission so we will first do ls and then we found two files one is personal.zip so we can do unzip it by unzip personal.zip.

20, so now we can change the directory = cd personal/stuff/

Do ls we will get monitor.sh

21.so we know that in this file/script we have a root access, we will mv monitor.sh temp.sh first and then we will create reverse shell,(reverse-shell is an integral part of any hacking/pen testing operation, it helps us in firewall evasion and enable us to execute commands on the remote target system)

22.search pentest monkey and revershell cheat sheets, we will use rm one from pentestmonkey

23 we will put one file called vi monitor.sh and then paste that command (insert it)

First line should be #! /bin/sh and then past that command form pentest monkey and change the port to 9999 and the tun0 add it and save it and then do ls,

24, make it executable chmod +x monitor.sh

Cat monitor.sh

25now start the nc listener nc -lvnp 9999 then going on to the tab where we executed that script sudo the path which we had got initially as a sudo

26, give it some time we got shell again

cd /root,

ls,

cat root.txt.

Done (Pwned)