**Vulnhub Hemisphere-Gemini CTF writeup**

**by TecnoLinux**

**Twitter:@tecnolinux\_user**

**Thanks to:**

* Author-d4t4s3c-Twitter:@d4t4s3c

**Tools that i use for this challenge:**

* nmap
* gobuster
* enum4linux

**Note**

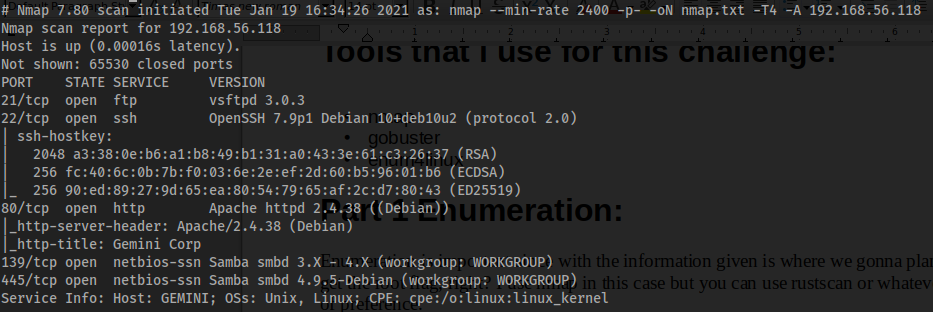
When you see the simbols <> on a commmand you dont need to add them thank you

**Part 1 Enumeration:**

Enumeration is important since with the information given is where we gonna plan to get the root flag, right? I use nmap in this case but you can use rustscan or whatever tool of preference.

* export IP=<The IP of the VM machine>
* nmap -A --min-rate 2400 -p- -T4 $IP -vv

When the nmap scan finish I find 5 services FTP,SSH,Apache and SMB, as you can see the FTP not success on finding a exploit for that version also the same thing for Apache.

We have SSH and SMB, so let’s start for enumerating SMB.

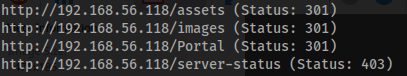
When enumerating SMB i find a interesting username called william using enum4linux, i did try bruteforcing for the password but no success so i take it as a clue for the SSH username.

* enum4linux -r <your ip>

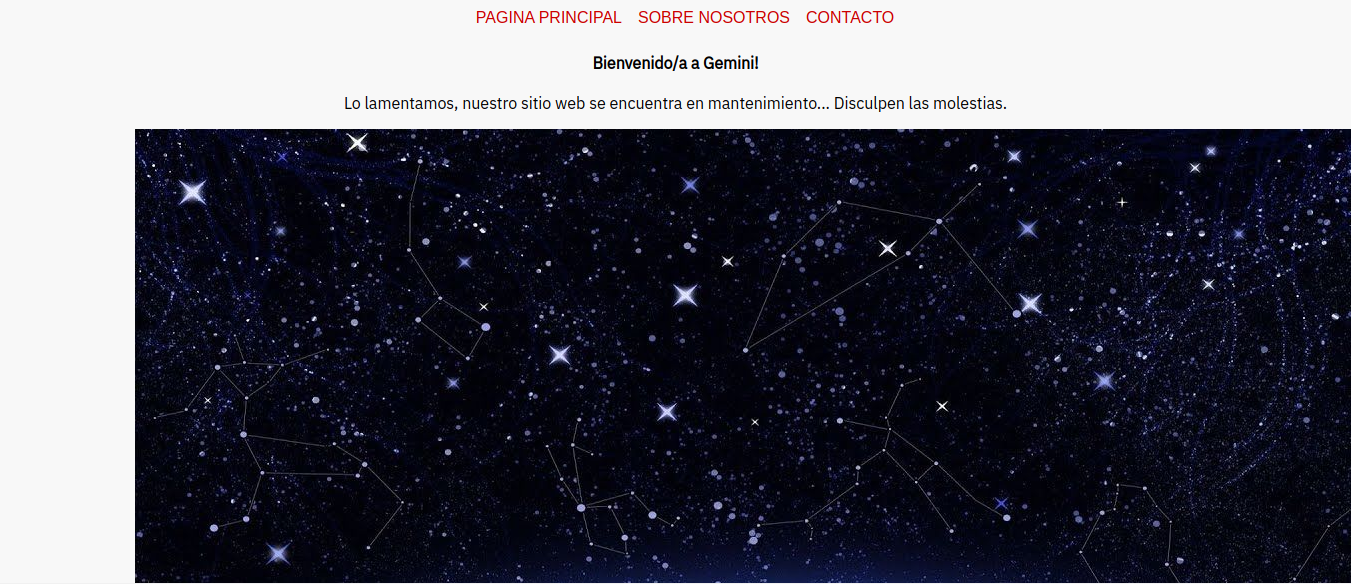
Now let’s go to the enumeration of the website.

For website enumerating i use gobuster to list the path of the website in this case we find something interesting path called Portal, if you put only the ip it show something like this. But if you add /Portal at the back of the url it show you another webpage.

* gobuster dir -e -u http://<your ip>/ -w <your wordlist> -t 100 -q







**Part 2 Gaining Access**

In Gaining Access as you can see from the /Portal website is under maintenance. When i clicked on Sobre Nosotros i did look at the back of the URL at it looks like this.



Whe i see the URL like that it reminds me of a vulnerability called LFI

or Local file inclusion especially directory trasversal attack, But what is LFI? On acutenix they have a definition for it that it is like this,LFI is a web vulnerability caused by mistakes made by a programmer of a website or web application. If an LFI vulnerability exists in a website or web application, an attacker can include malicious files that are later run by this website or web application. Lets see if the webpage is vulnerable to LFI.

Now that we have the definition of LFI now let’s define directory trasversal attack,is an HTTP attack which allows attackers to access restricted directories and execute commands outside of the web server’s root directory.i test it out by navigation to the /etc/passwd like this.



When you press enter it will show the usernames of the machine,if you right click> view source code, to get a better view of the file if you scroll down you will see the username william that means we can use it to get SSH access but we have one part of the SSH credentials so what we could do at this point you can bruteforce credentials but that takes time and remember hackers looks for “the lowest hanging fruit” meaning that hackers goes to the easy route, yeah you got it directory trasversal attack, you can navigate to the id\_rsa directory of william to get SSH private key.

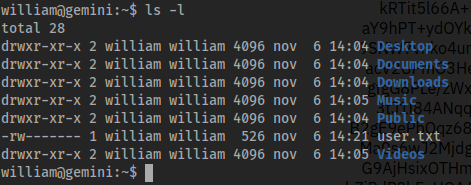


And you will get the private key of william, right click and view source code and copy the -----BEGIN OPENSSH PRIVATE KEY----- all the way including -----END OPENSSH PRIVATE KEY----- create a file with nano called id\_rsa and change file permissions with chmod like this.

* nano id\_rsa
* chmod 400 id\_rsa

Now all that you need is to access the machine like this

* ssh -i "id\_rsa" william@<your ip>



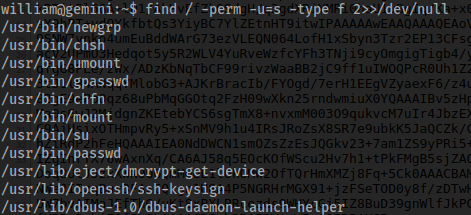
We have successfully enter to the machine and get the user flag. Now let’s move on to the third part of getting the root flag.

**Part 3 Getting the root flag**

In case of getting the root flag i didn’t use linpeas because i look for basic stuff manually, and this machine doesn’t have sudo in it so i did take another step is in fiding SUID binaries and i find it using the find command.

* find / -perm -u=s -type f 2>>/dev/null

Once the command finishes i find something interesting and it is the passwd binary.



passwd allows you to set a password or change it, when i see the binary i look at the /etc/passwd permissions and the permissions are not good.



That means that every user can change the file and creates a user with password and have root access. Let’s first generate a user and a password using openssl.

* openssl passwd -1 -salt <your username> <your password>

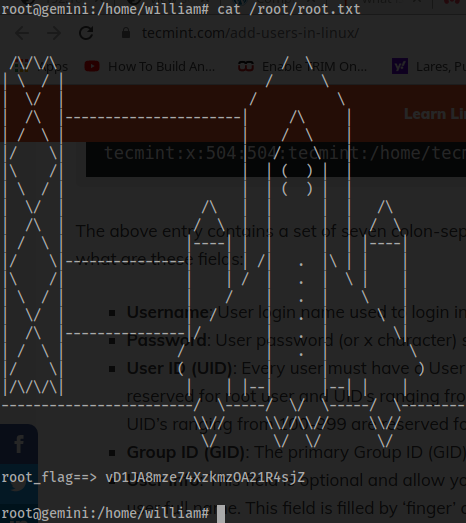


Now let’s add the user and password hash in this case the type of hash is a md5 unix hash if you want to know more examples about unix hashes enter here https://hashcat.net/wiki/doku.php?id=example\_hashes, in order to add a user on that file you need to follow a structure to add it if you want to know more info enter here https://www.tecmint.com/add-users-in-linux/ this is the command for adding a user.

* echo "<your username>:<password hash>:0:0:/root:/bin/bash" >> /etc/passwd



Once you complete it you have to use su command and the username that you create it enter the password and you will have root access and get the flag.



*I hope that you enjoy this writeup, I enjoy this challenge a lot and I learn few things on the way. Thanks to the author for creating this room. Dont feel yourself bad when you check a writeup it’s okay doing it but learn from them, correct your mistakes and improve. Dont give up and the next time try harder.*

