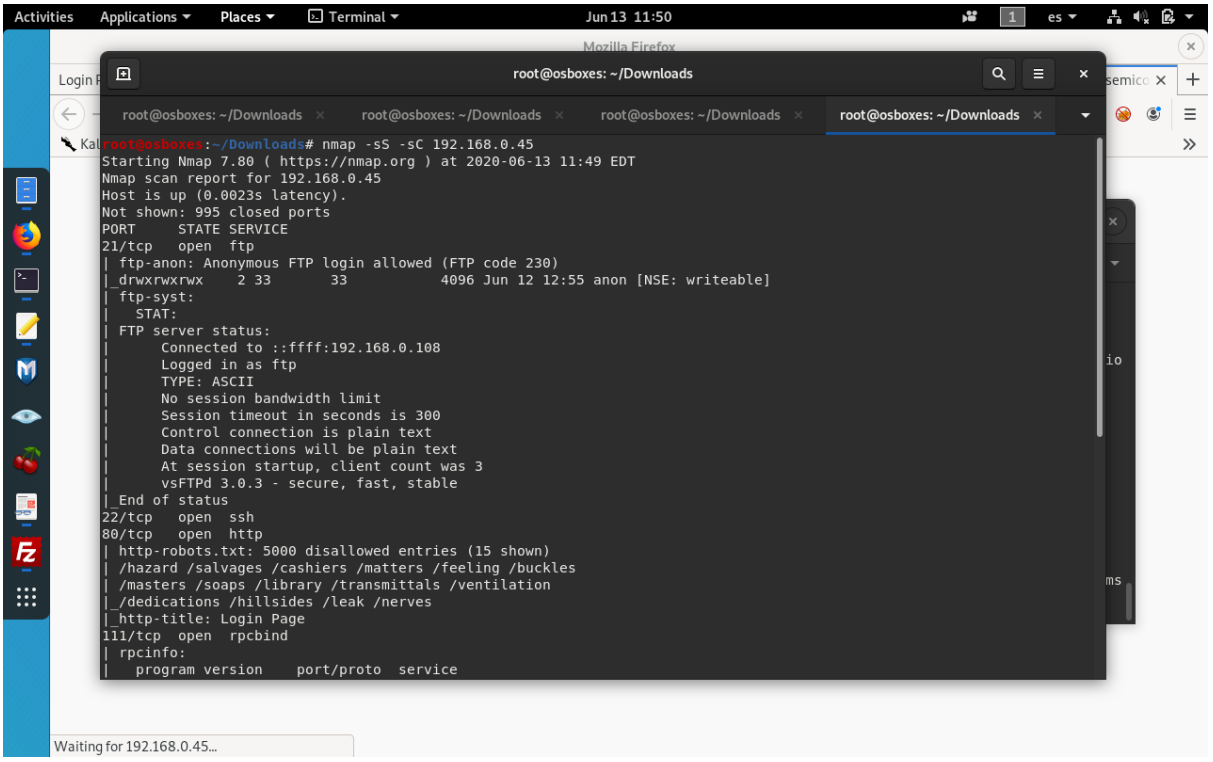
Jorge Amoros

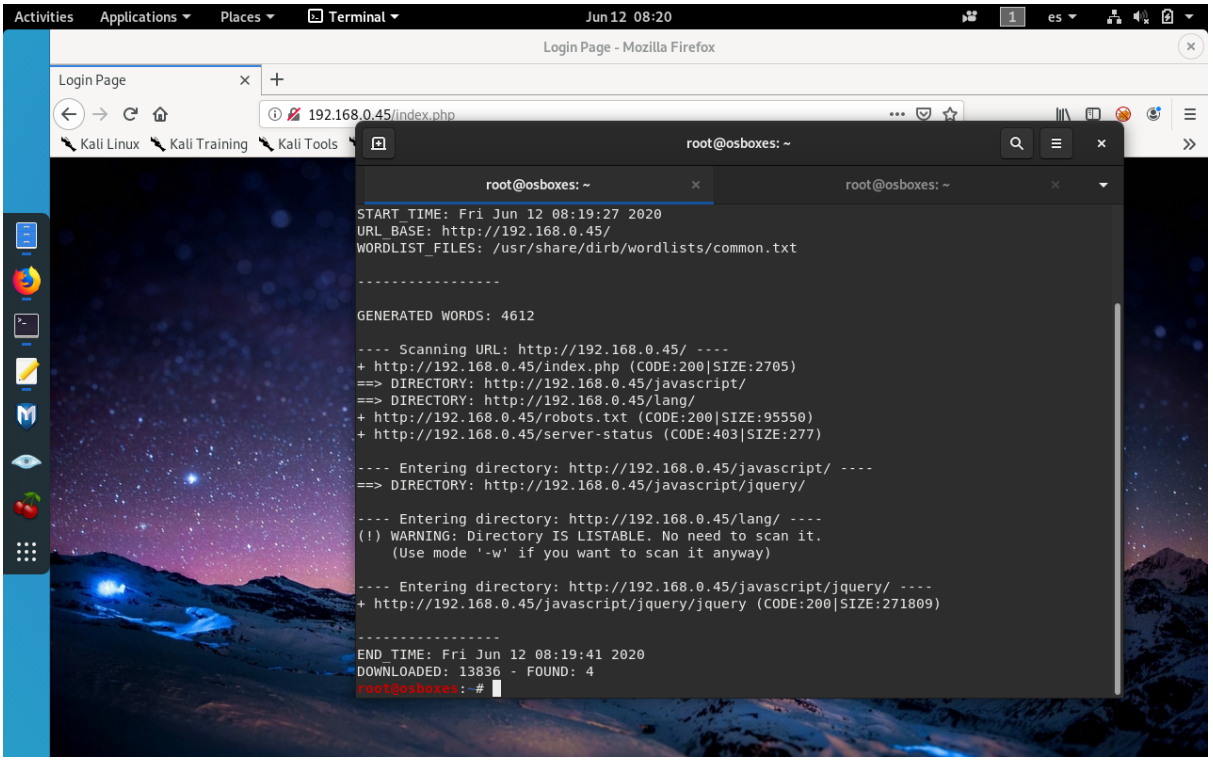
Walkthrough HayStack machine

The very first step as usual is running nmap to look for services running on the machine. On this one we can see several of them, like FTP with anonymous login accepted. SSH version 2.0 so we will forget about it. Http as usual and NFS also available for mounting.

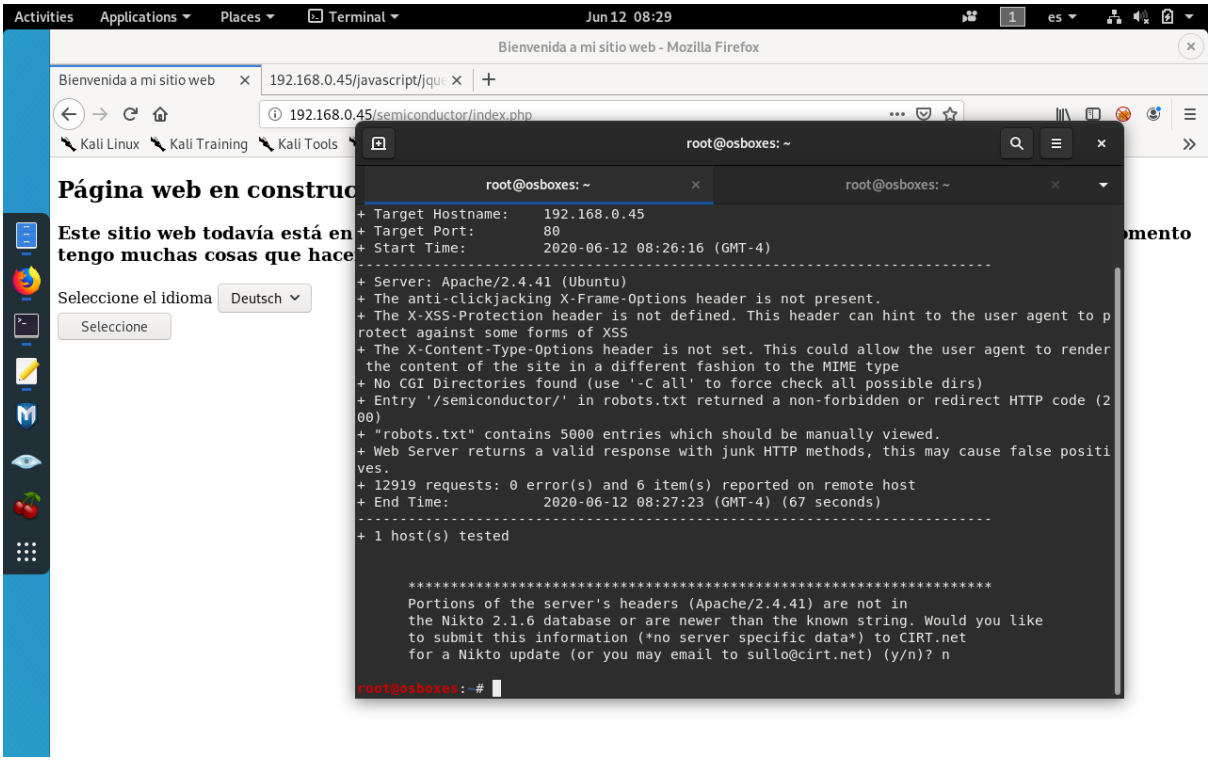


Since I like taking a look to HTTP first I execute Dirb and Nikto in order to know where to start looking for. We see the index.php (Good to know its using PHP as backend language) and also some directories than can be browsed like javascript/Jquery which is not relevant and semiconductor. This one looks interesting since is the only one found by Nikto.

Jorge Amoros

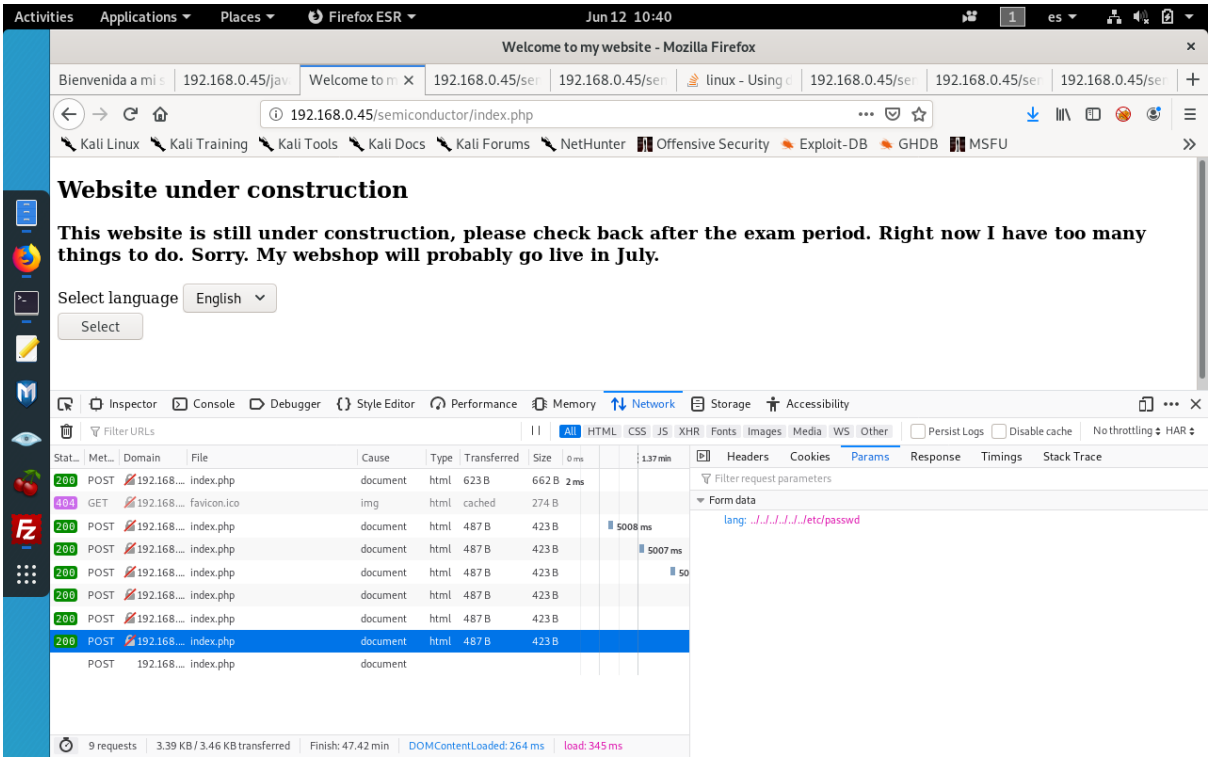


On this subdirectory found by Nikto we see that is sending and Http Post request to reload the web in the language you select.

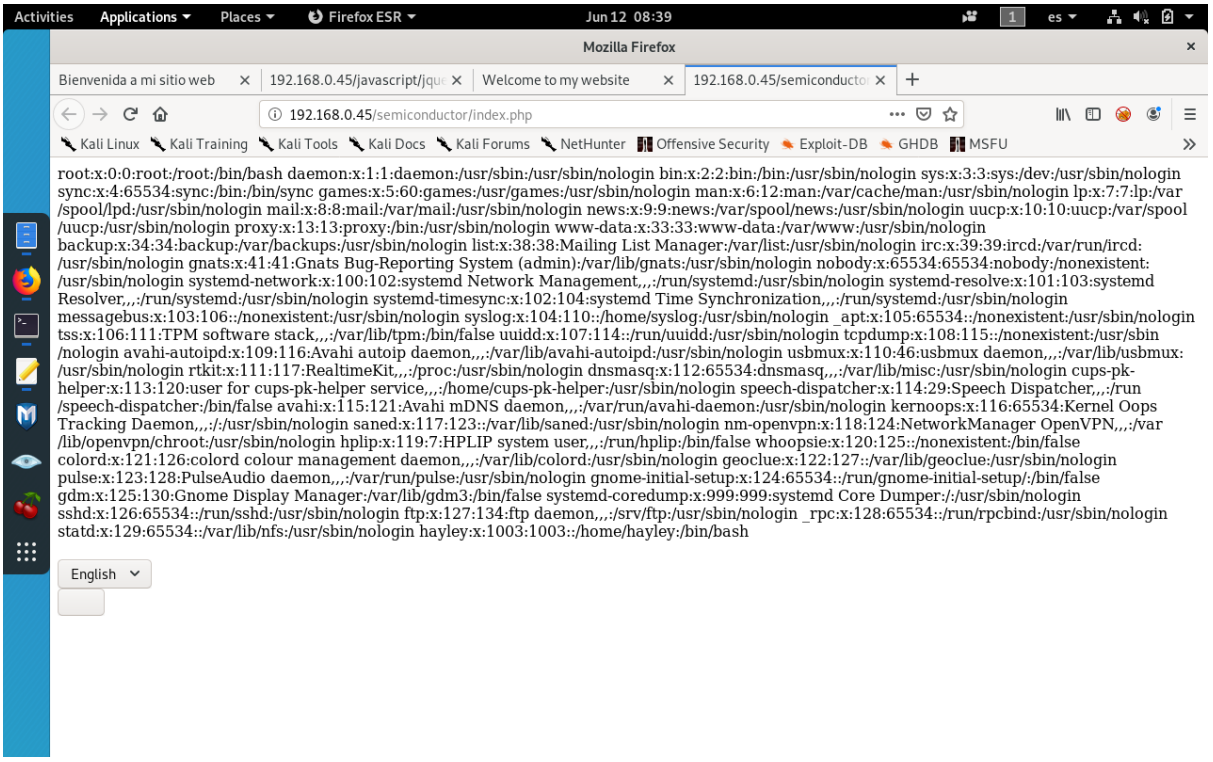


Jorge Amoros

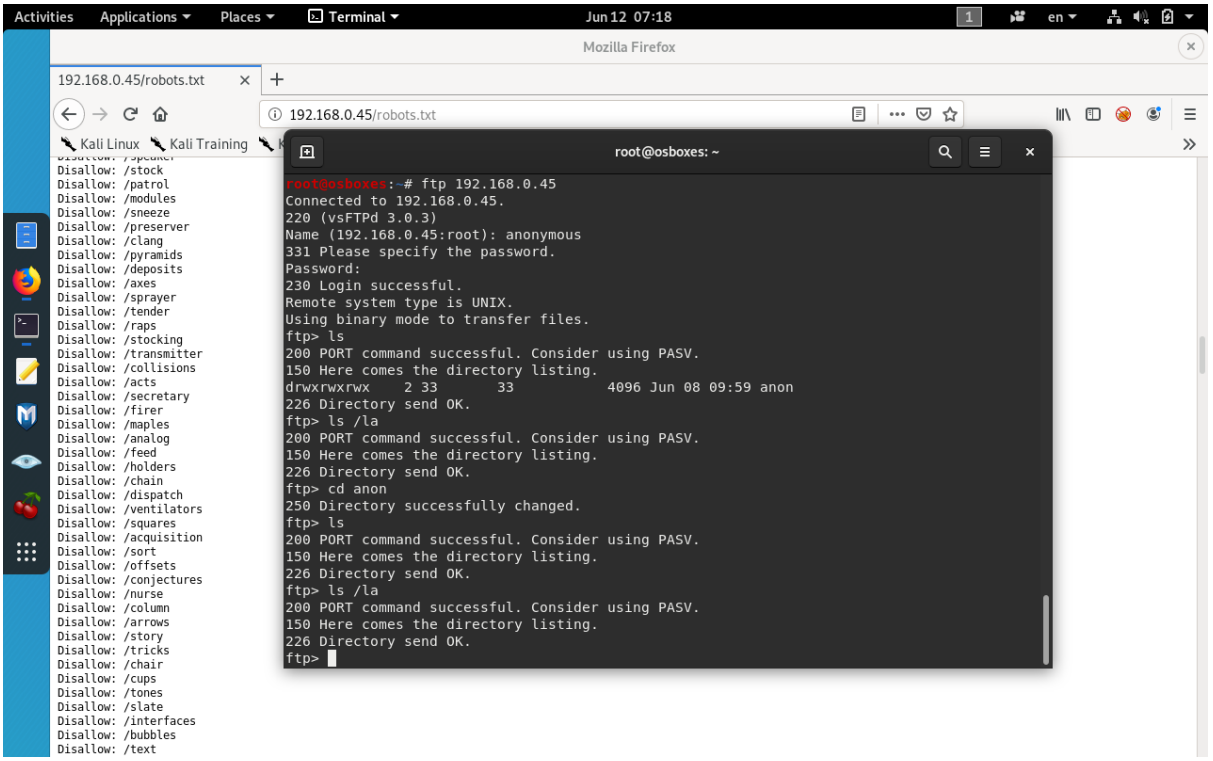
We try to path Transveral and see if we can read /etc/passwd. Probably reading this file wont be really usefull but it will tell us that the system is not secure against path transveral vulnerabilities.



Which is definitely not prepared for it.

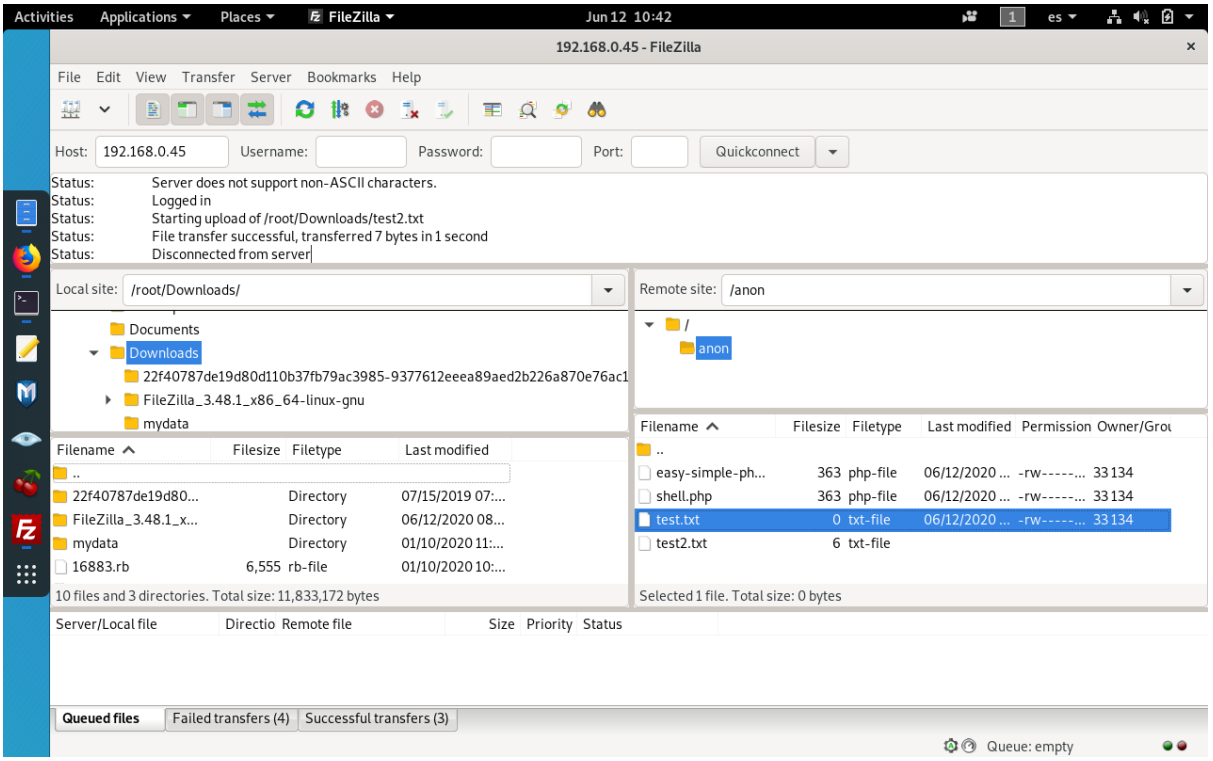


At this point we cannot keep digging in since we cannot upload anything and we dont knoe how is organised the server. But, if it vulnerable to path transveral we could execute a reverse shell. So we go to the FTP service.



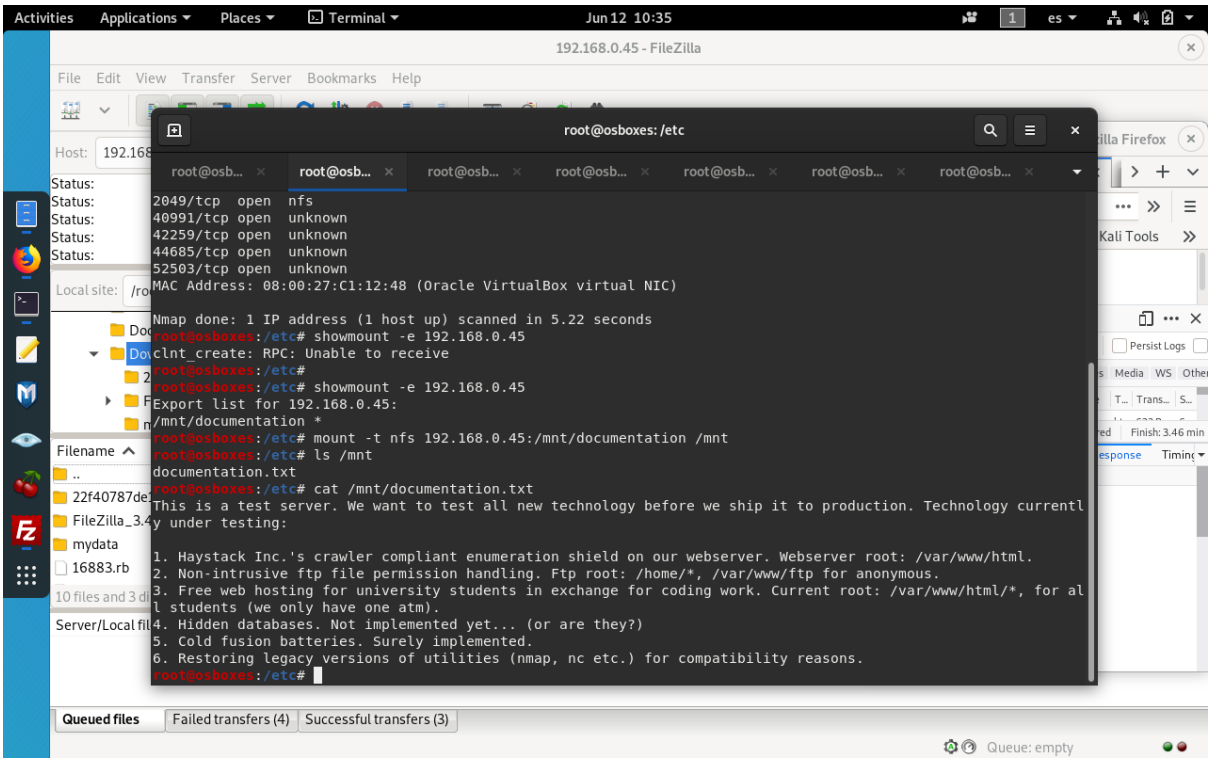
For simplicity, we will download filezilla and use the web interface. The FTP allows to upload files on it, but not rename or delete them. Since is not checking anything we create a simple reverse shell executing a whoami order to see if we succeed and some .txt files.

Jorge Amoros



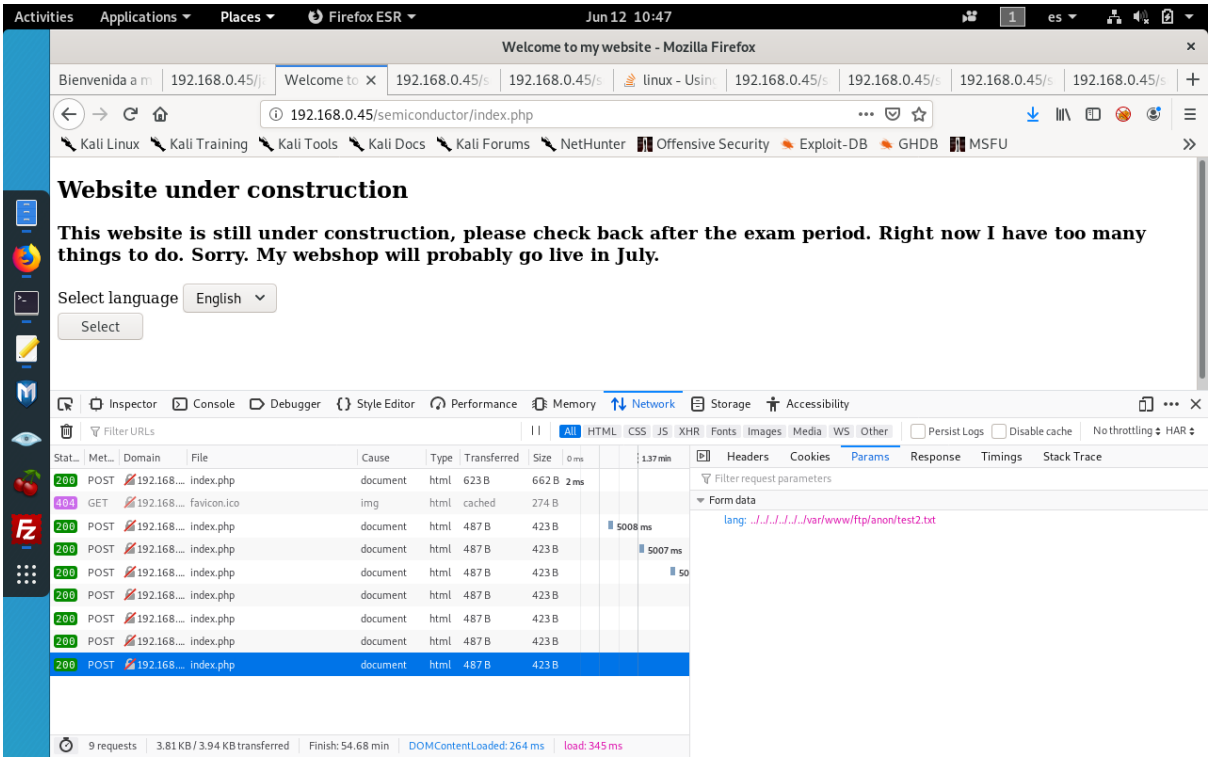
But first, we need to know where FTP is located. We could try and error but is quite boring. WE remember about the NFS and we look into it after mounting.

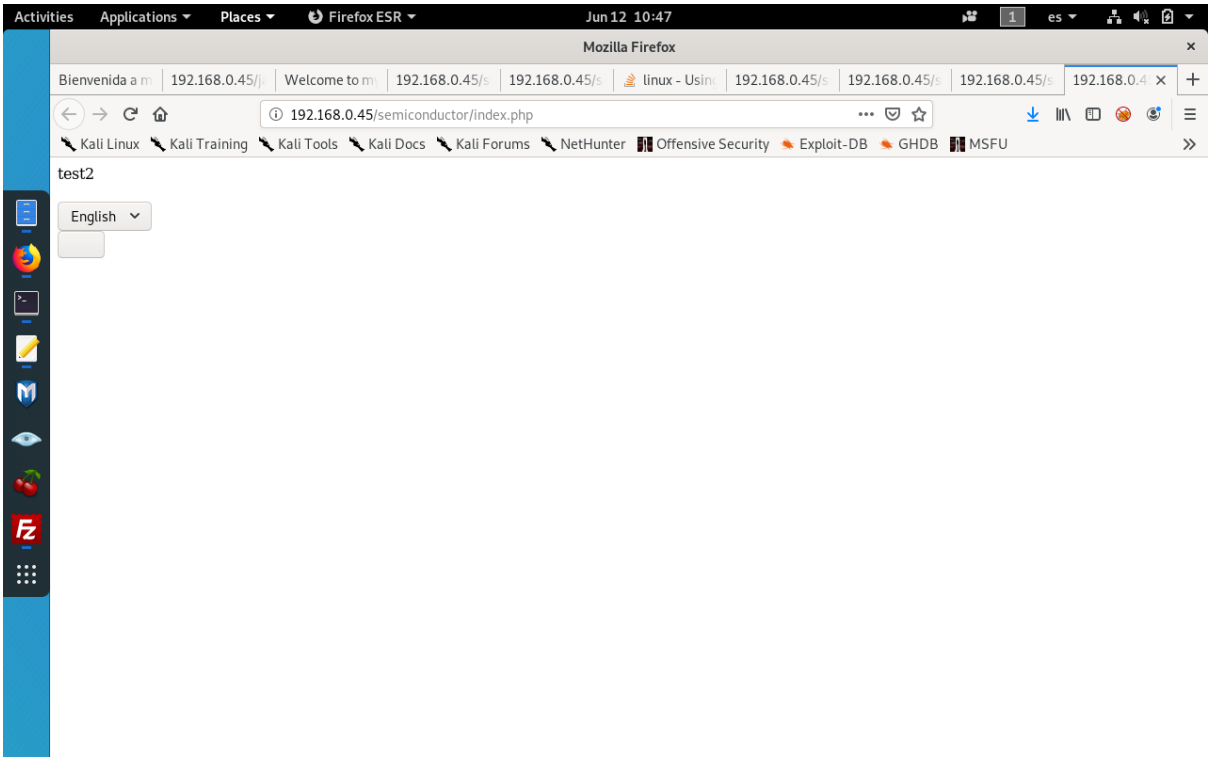
Where there is some documentation.txt telling us where the data is located. Also saying something about databases which could be implemented but hidden.



Jorge Amoros

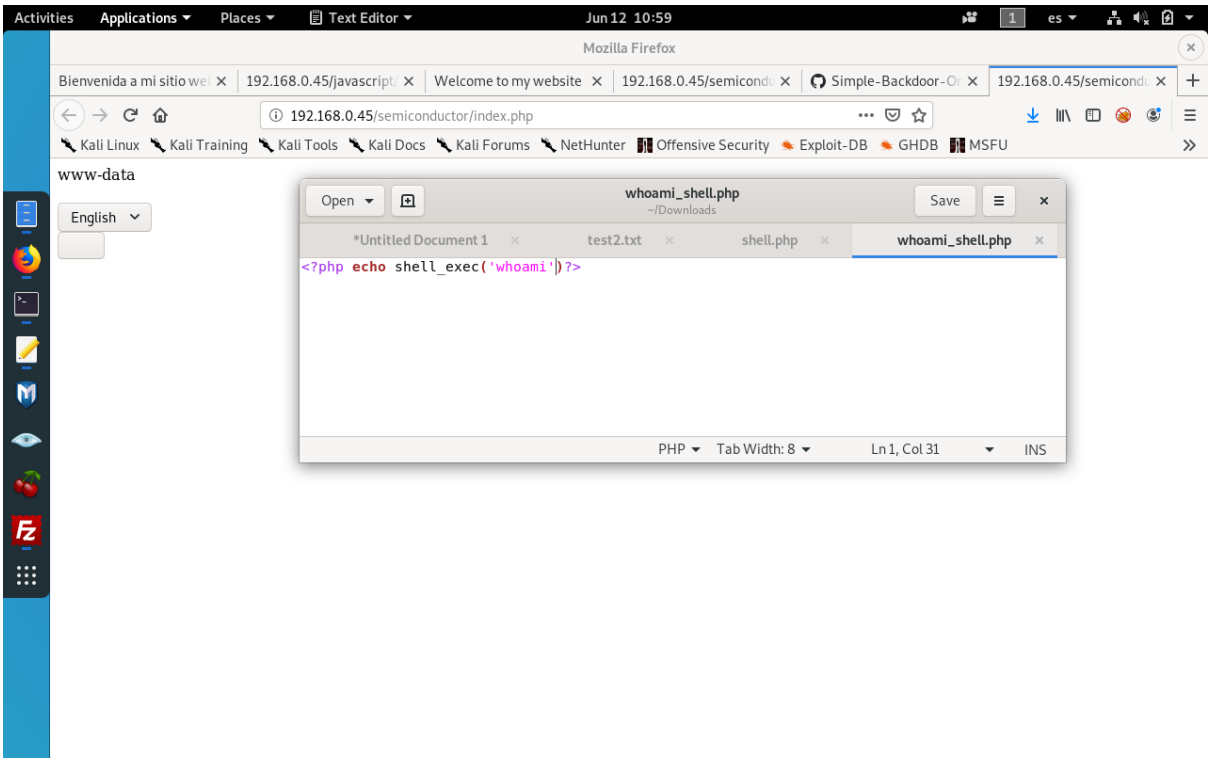
Now we can go back to the HTTP and execute, for testing porpuses our test2.txt to see that we know the location now.



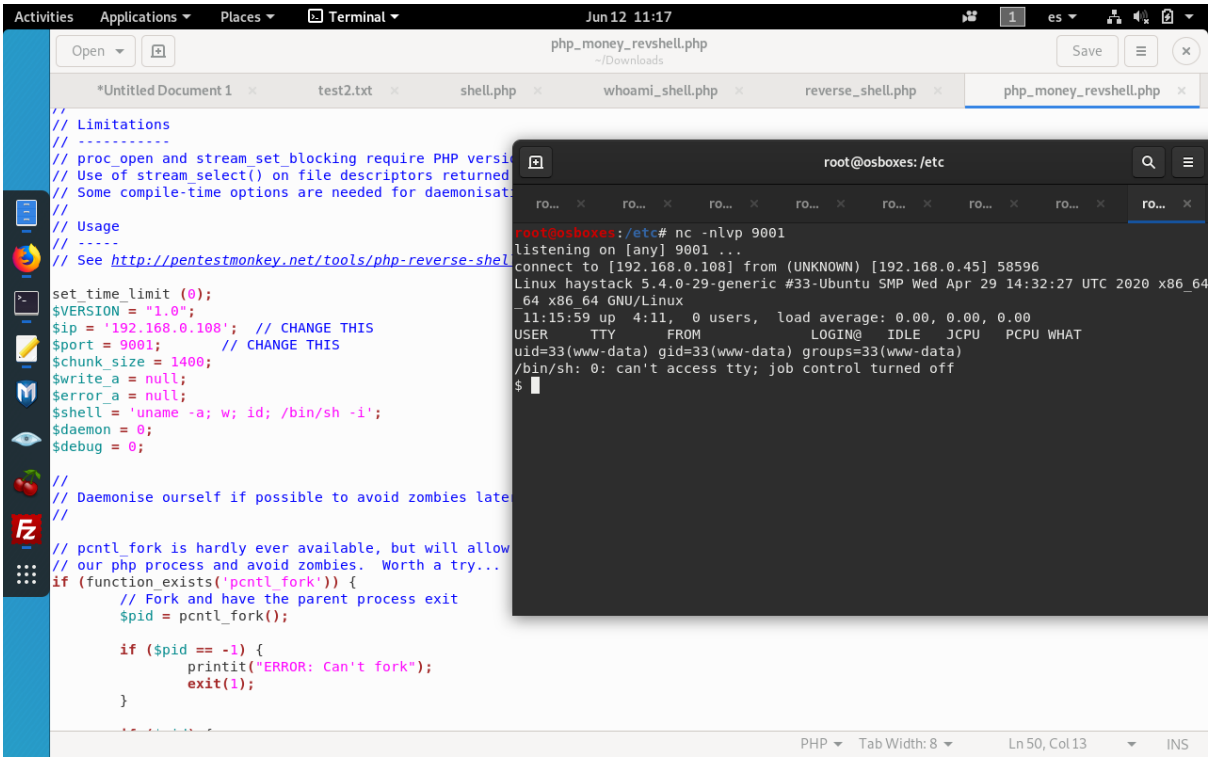


we execute also the reverse shell with whoami.

Jorge Amoros



Finally we download a nice reverse shell who will open a connection on port 9001 and execute it.

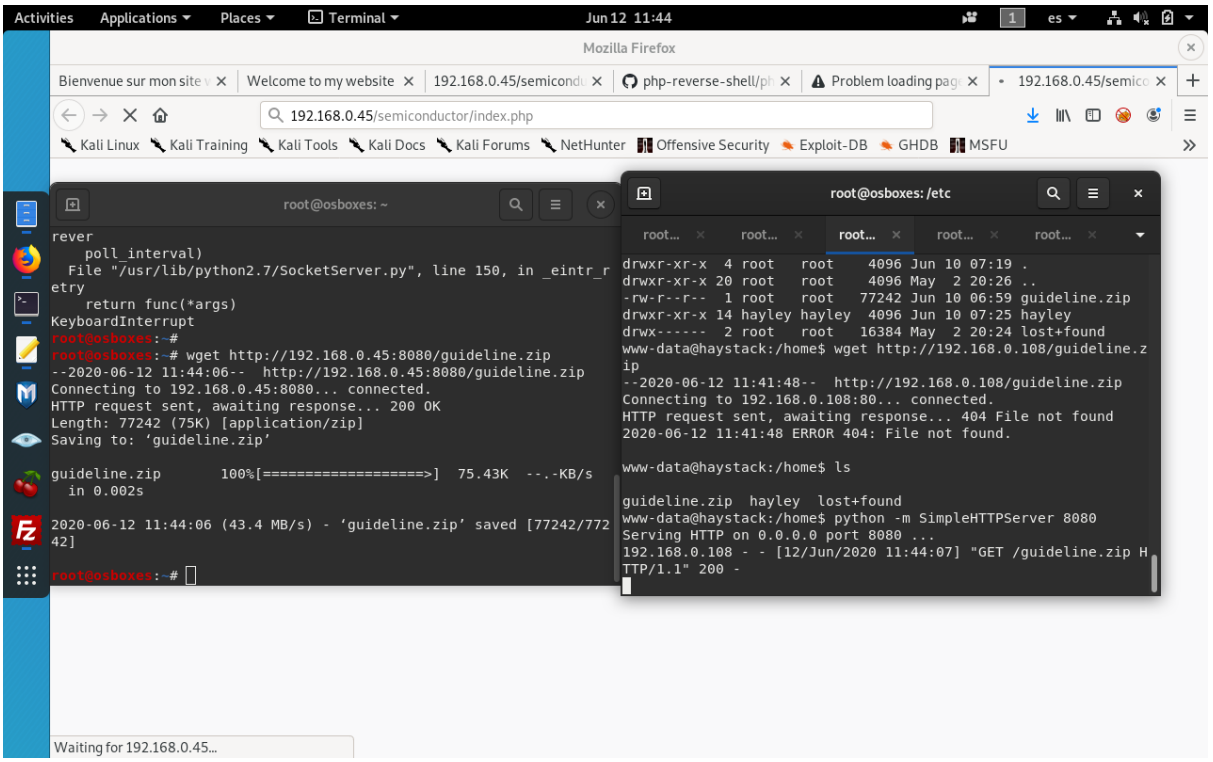


Once inside we start trying things.

Jorge Amoros

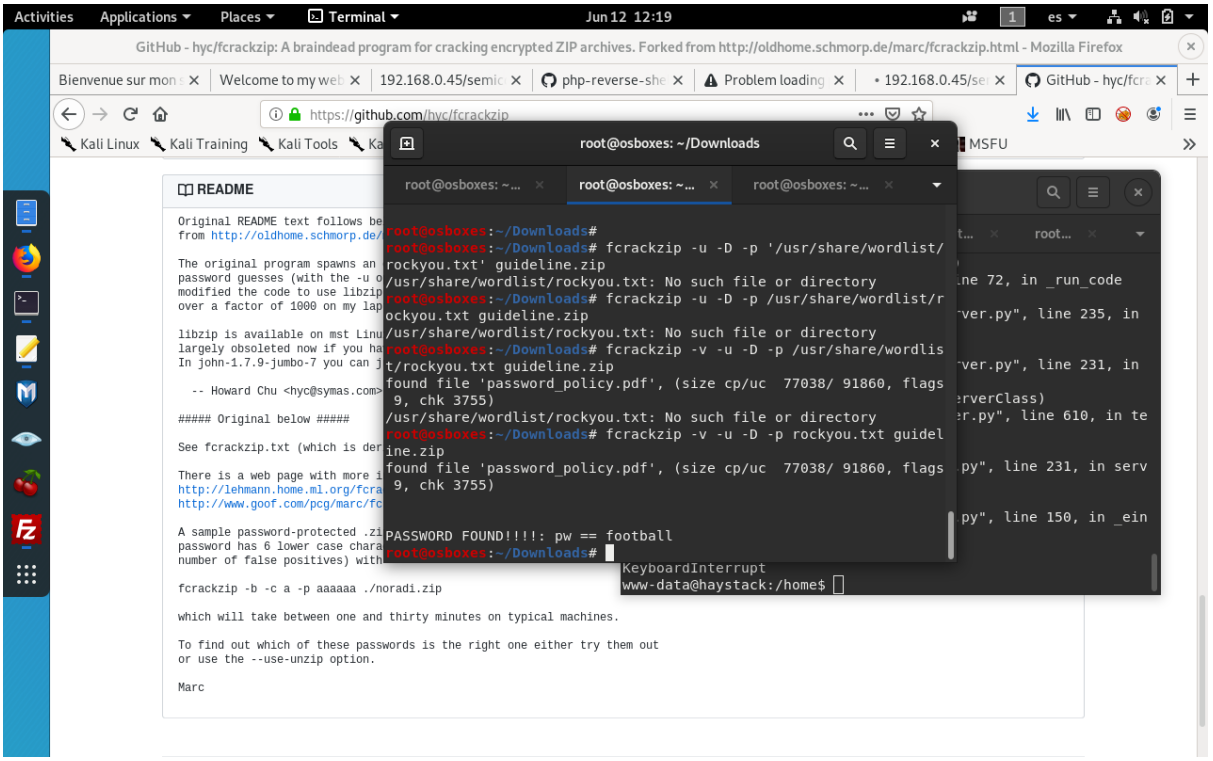
Bash_hystory denied.

We discover an interesting file called guidelines.zip so we download it using python webserver on the host machine and wget on attacker machine.



And we crack it using fcrackzip (downloaded) with rockyou.txt file.

Jorge Amoros

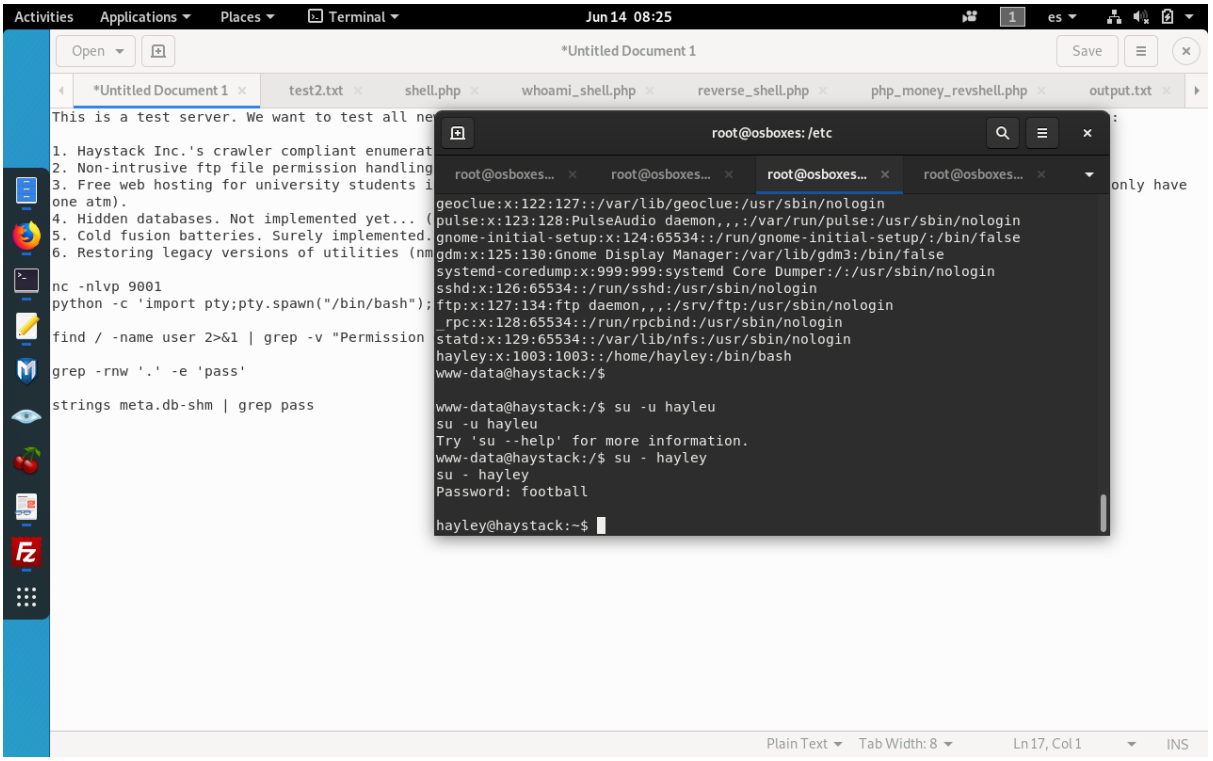


We try so passwords here to log in as root but no luck.
Says something about a database. So we confirm that there is probably a hidden database somewhere…

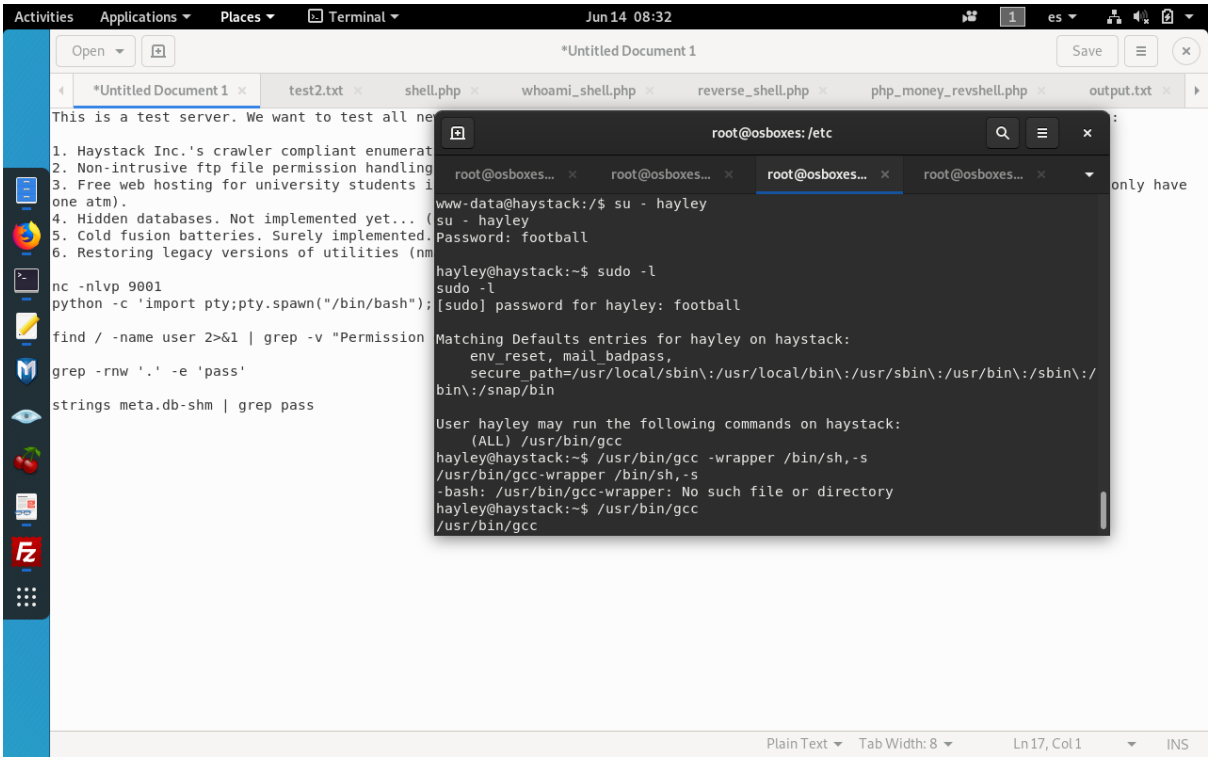
After trying several things, password of the machine is betteruseamagnet so maybe inside .cache , there is a tracker folder with several binary files. Trying to find something inside with strings is not giving any pass or result.

We see there is a user call hayley, we try pass football (pdf encrypted) on it and suceed.

Jorge Amoros



Once we are here, we try to see our privileges with sudo -l



We see there is saying something about the compiter gcc. So we look into GTFO Bins to see if it is exploitable.

Jorge Amoros

.. / gcc

Star 2,874

Shell Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

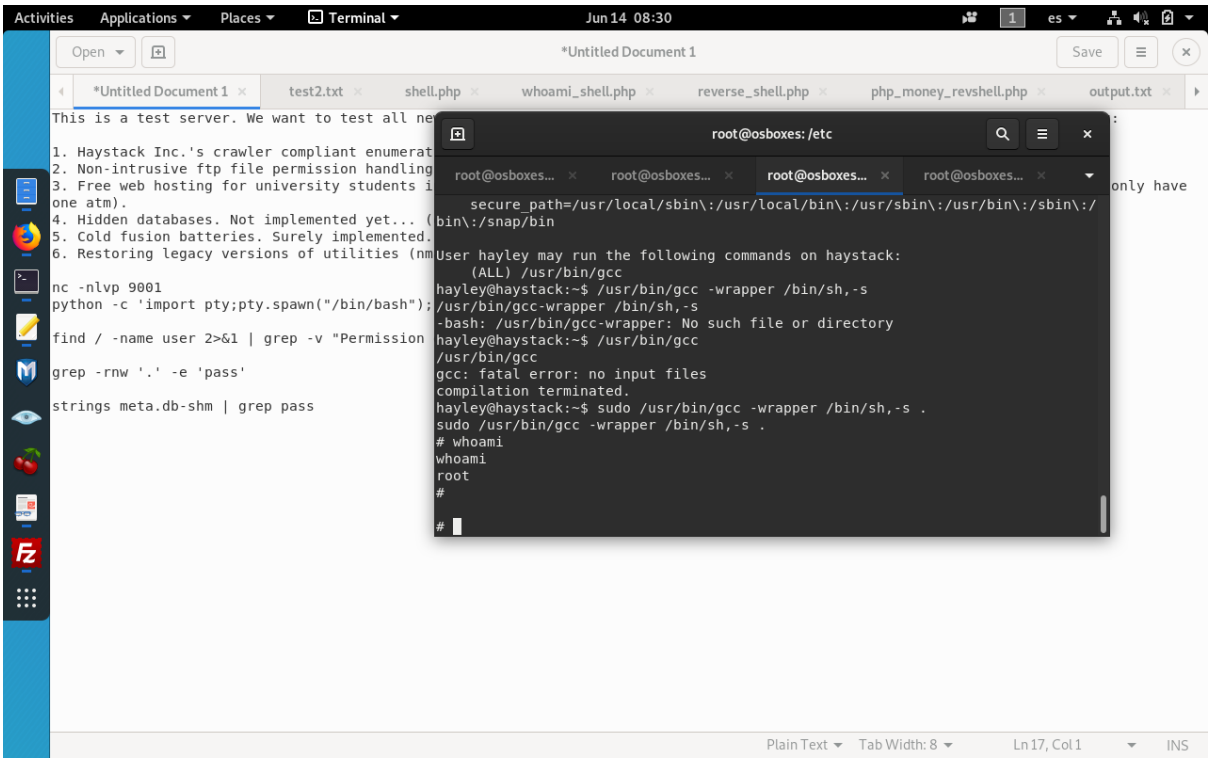
```
gcc -wrapper /bin/sh,-s .
```

Sudo

It runs in privileged context and may be used to access the file system, escalate or maintain access with elevated privileges if enabled on `sudo`.

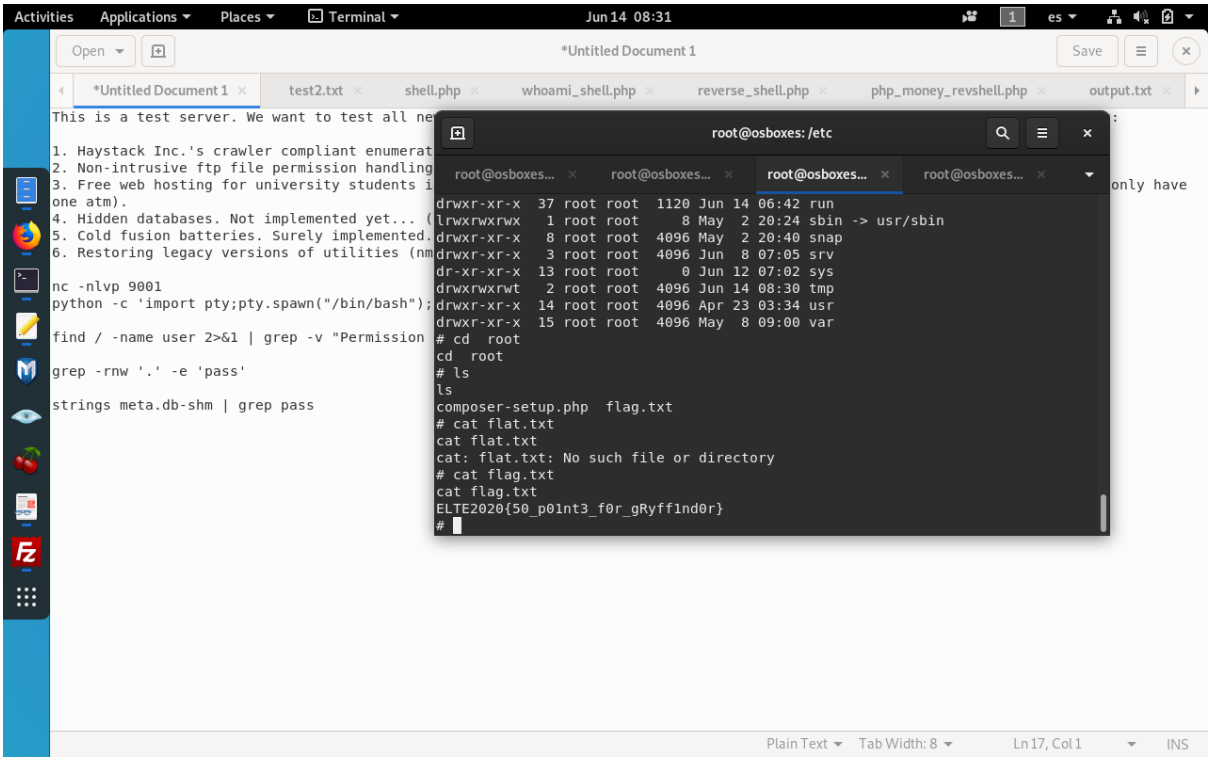
```
sudo gcc -wrapper /bin/sh,-s .
```

We will try with the sudo command



And bingo.
Now we can search for the flag.

Jorge Amoros



And we get 50 points for Gryffindor. Sadly, I am more into Ravenclaw :D