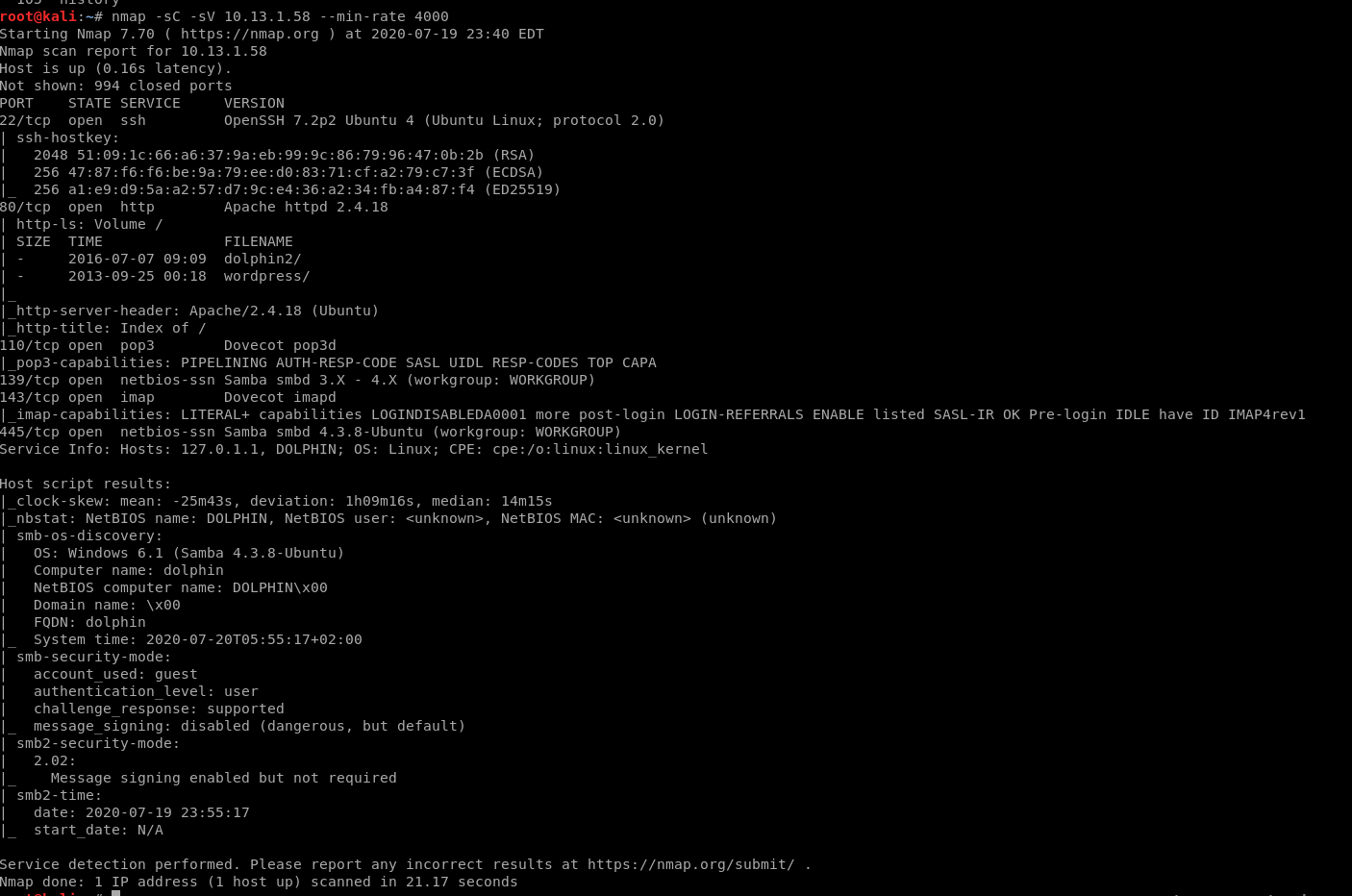
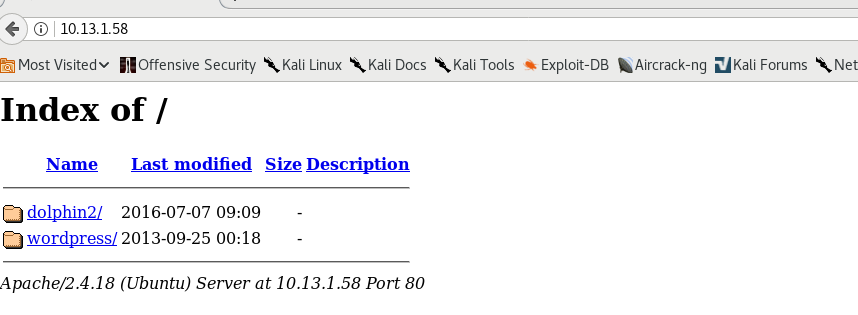
Dolphin(10.13.1.58)-GhostIA

Sarah Ferenczi

Enumeration

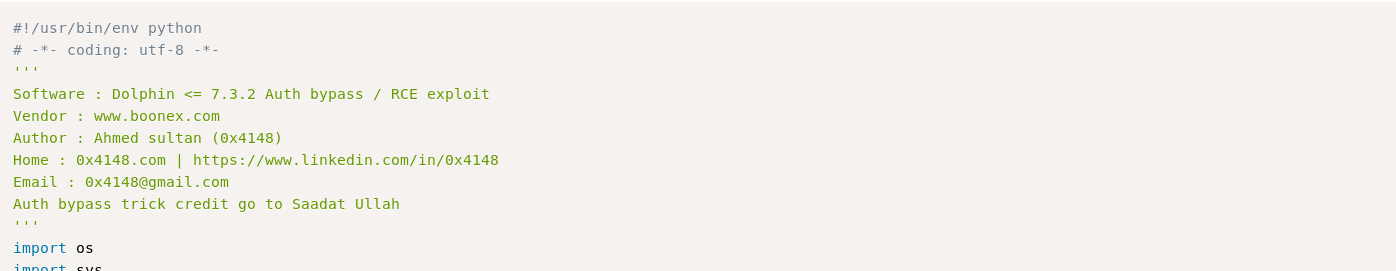


First let’s run an nmap scan. We can immediately notice port 80 is open.

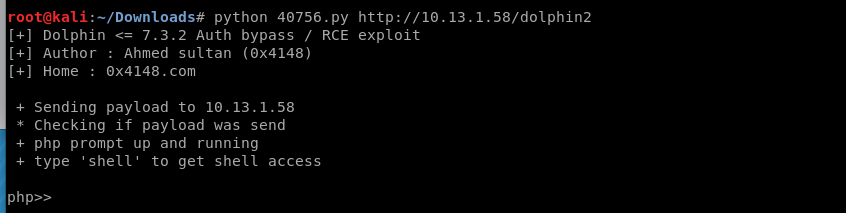


Exploitation

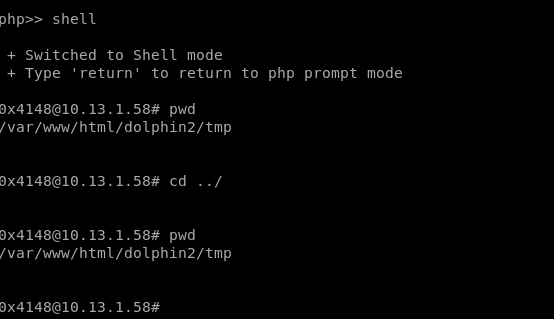
When we head there, we can see that it’s hosting 2 webservers, let’s check out dolphin2.



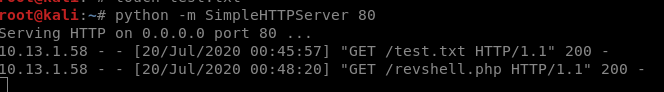
When we look up Dolphin exploits, we can see that there is an RCE that we can use for this.



When we execute it, we get a shell.

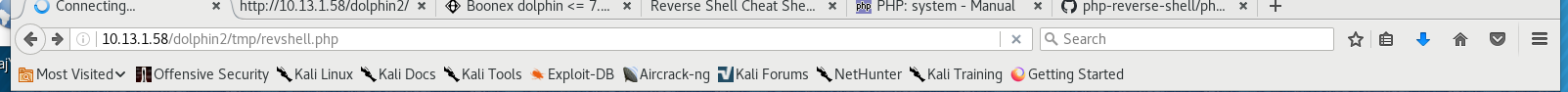


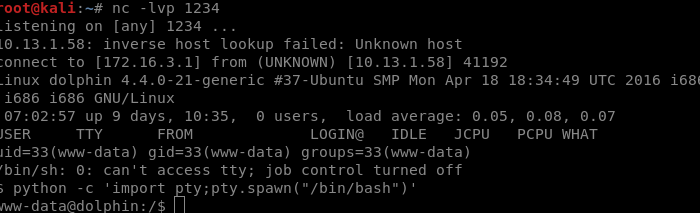
However, this shell is very limited. Let’s get a php reverse shell uploaded.



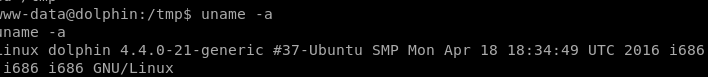
Let’s set up SimpleHTTPServer and upload a reverse shell to the tmp directory.

Privilege Escalation

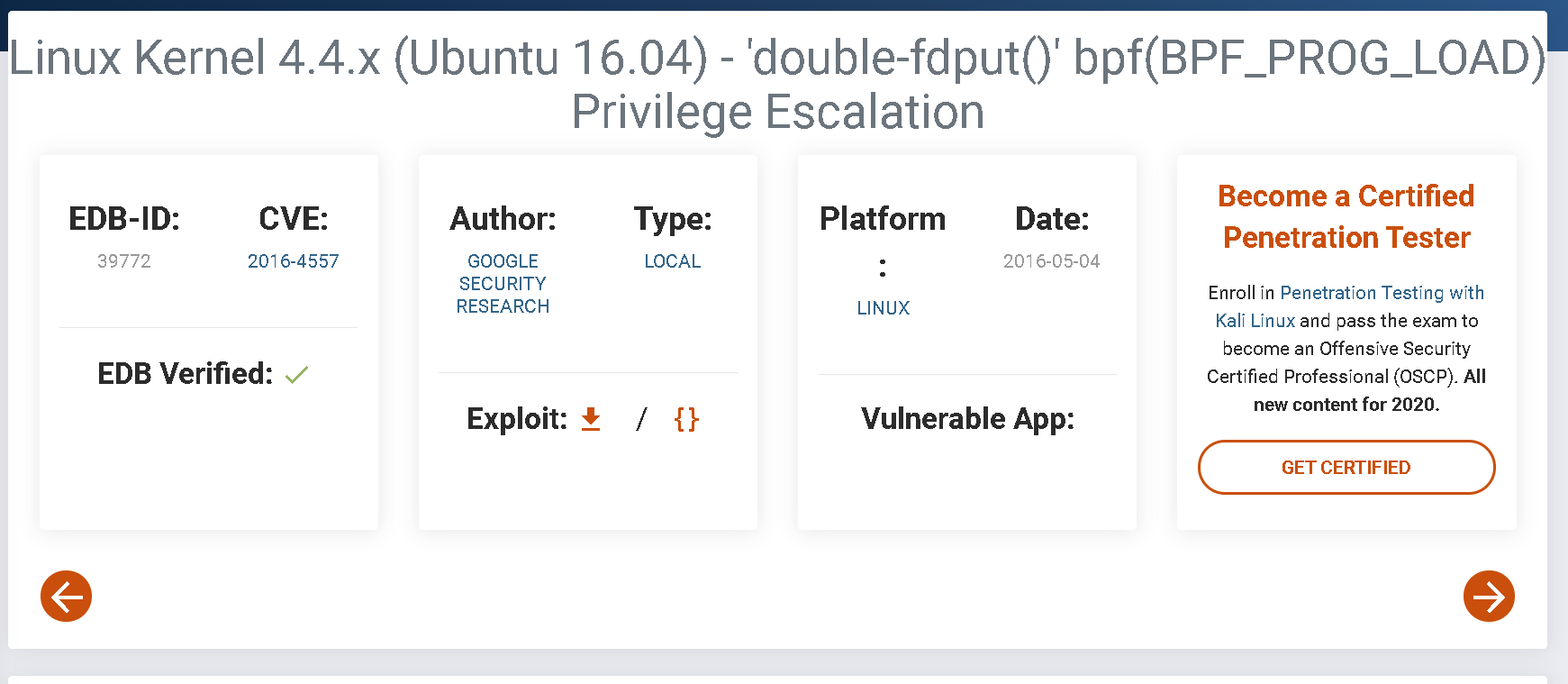




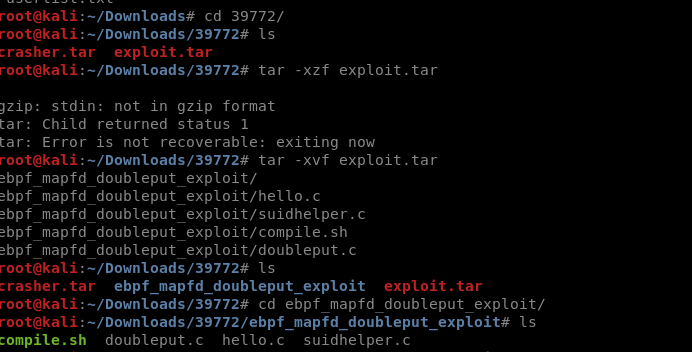
Then we can set up our reverse shell and get a real shell on the box.



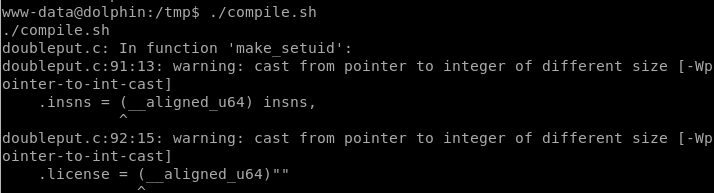
If we look at the kernel, we can see what version it is.



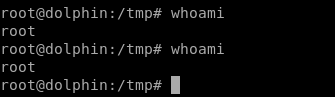
Then we can find a kernel exploit.



Then we can unzip the file



Then we transfer it over and run ./compile.sh.



Then we get root.

