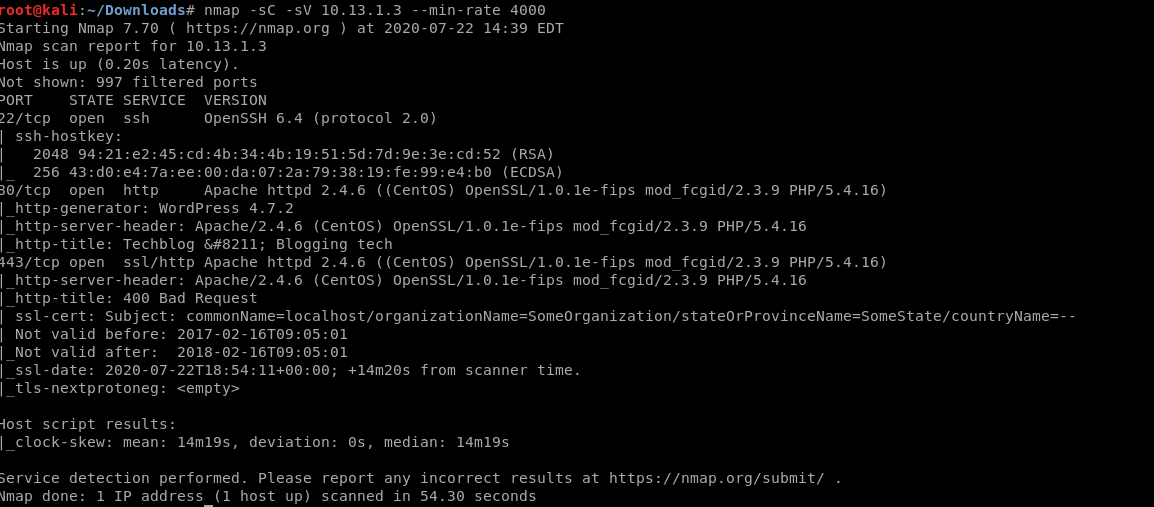
Techblog(10.13.1.3)-GhostIA

Sarah Ferenczi

Enumeration

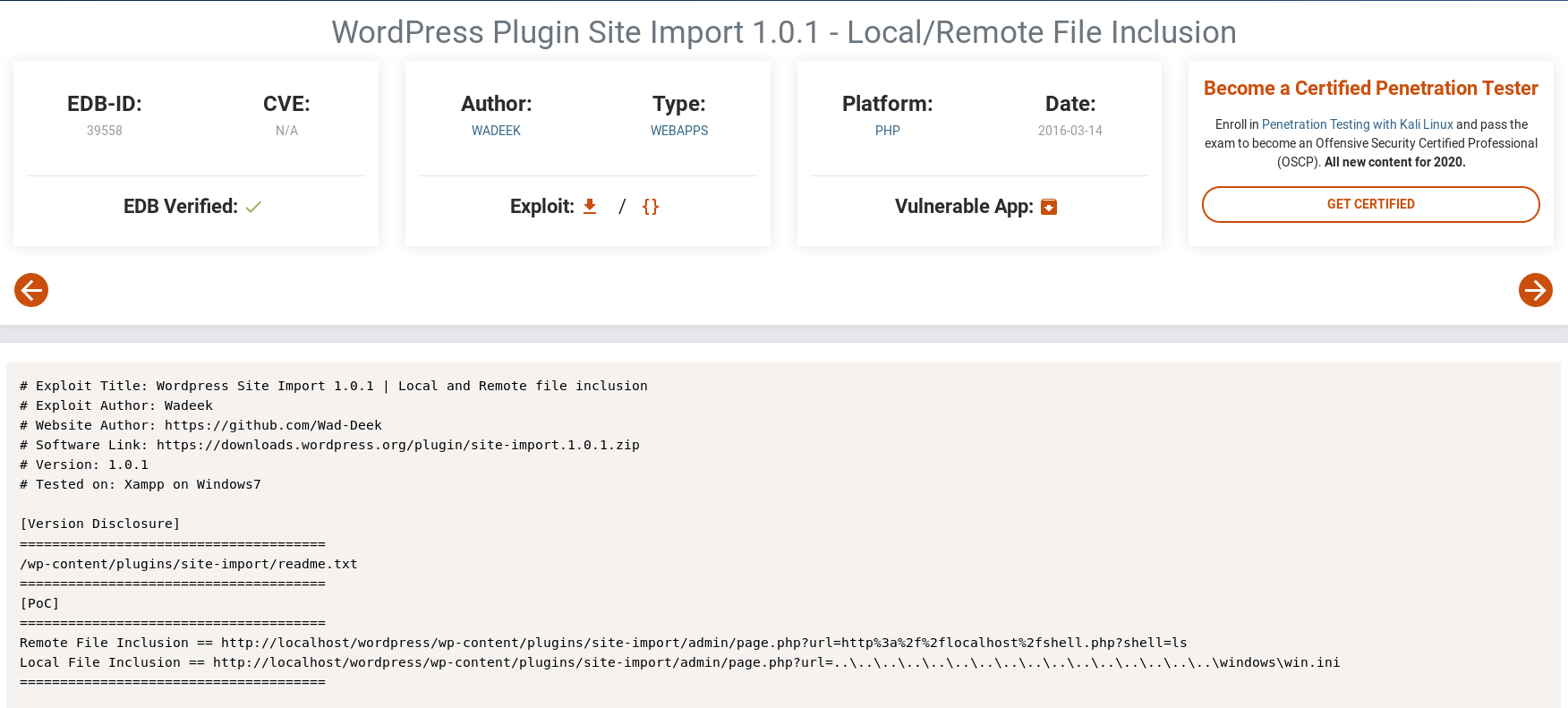


First we run an nmap scan and we immediately can notice port 80 is open, meaning there is a webserver running, specifically Wordpress.

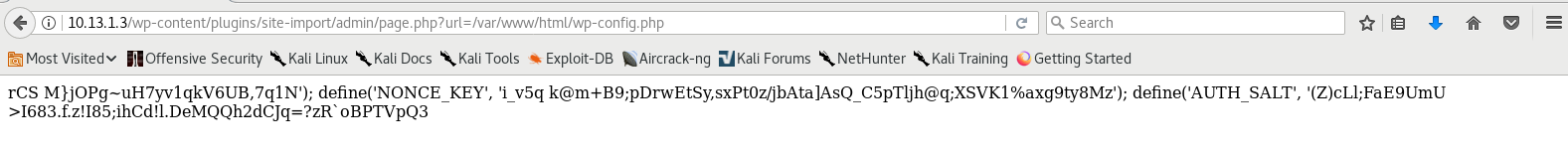


If we look around the website, we can notice that siteimport is a plugin that is being used on this server, let’s look up some stuff related to that

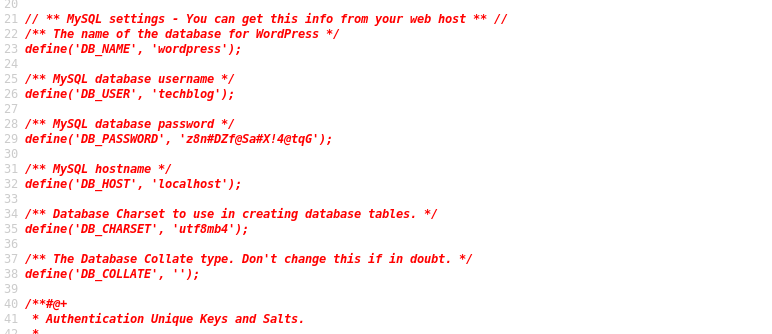
Exploitation



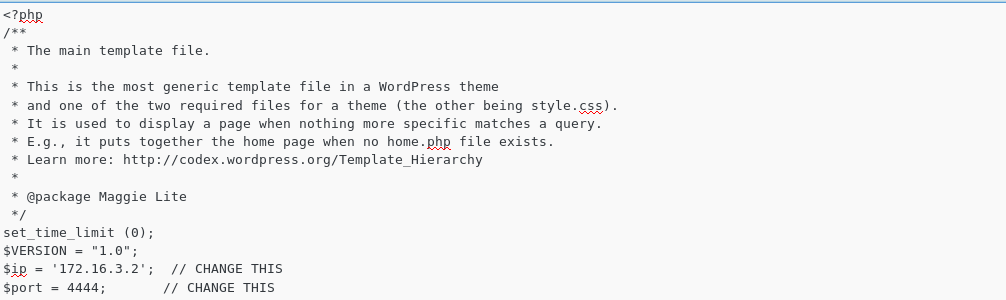
If we look up exploits related to siteimport, we can find this proof of concept for the exploit that is going to be used.



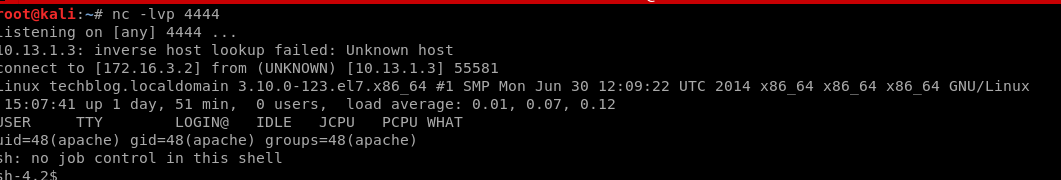
We can try accessing wp-config.php, since credentials are stored in there. Nothing comes up, but let’s go ahead and view the page source.



Immediately, we can find credentials for the user within this file. Let’s use those to log in.



If we navigate to Appearance>Editor>Main Index Template, we can edit the page to put in a php reverse shell payload.

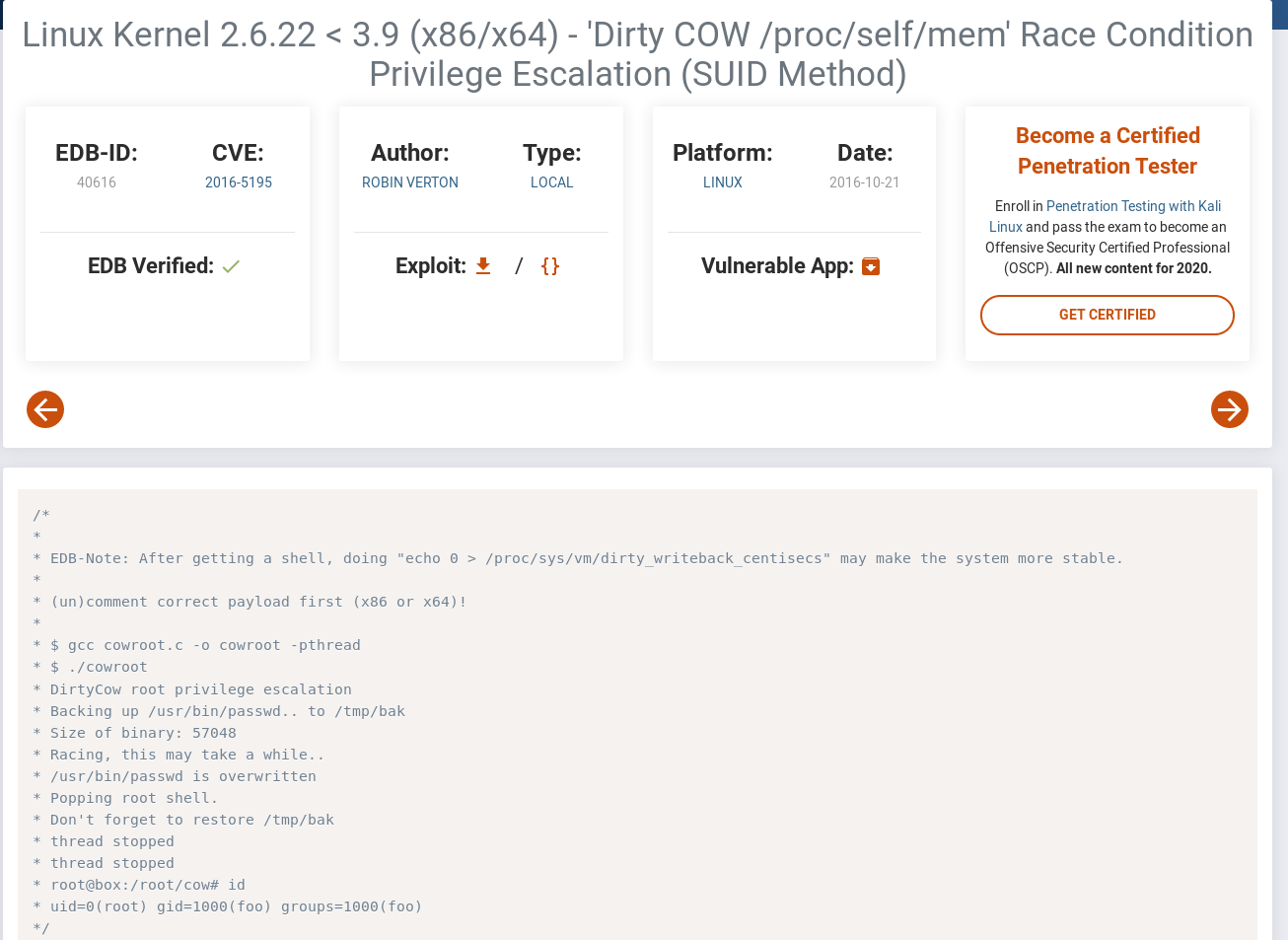


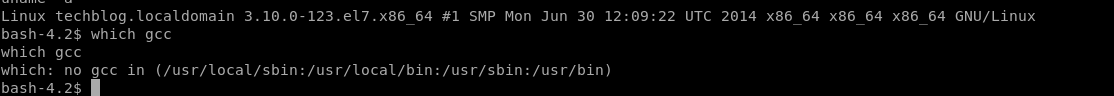
Privilege Escalation

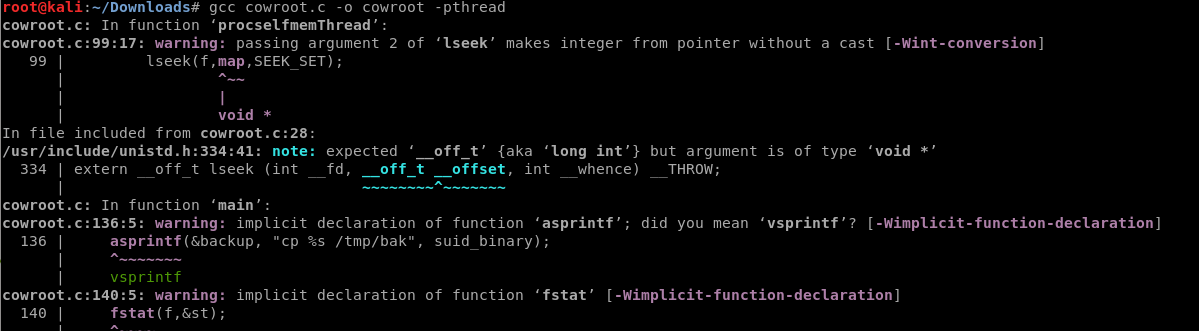
Once we navigate to the main page after setting up our listener, we can catch the reverse shell.

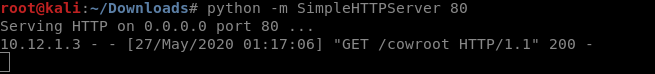


After poking around, we notice the kernel that is being run on this system

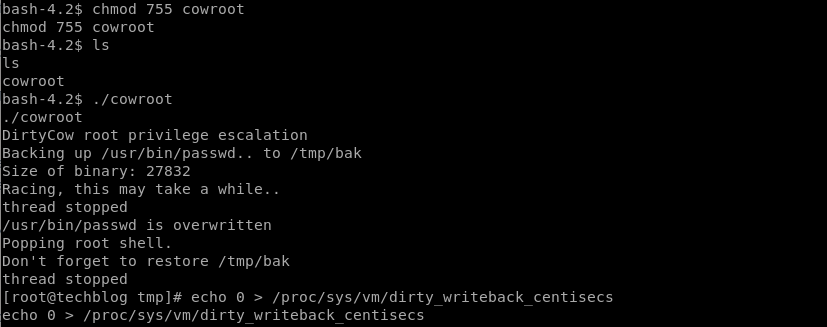


This kernel is vulnerable to the cowroot exploit, however, gcc cannot be found on the system





However, we can still compile it locally and transfer it over



And then we get root.

