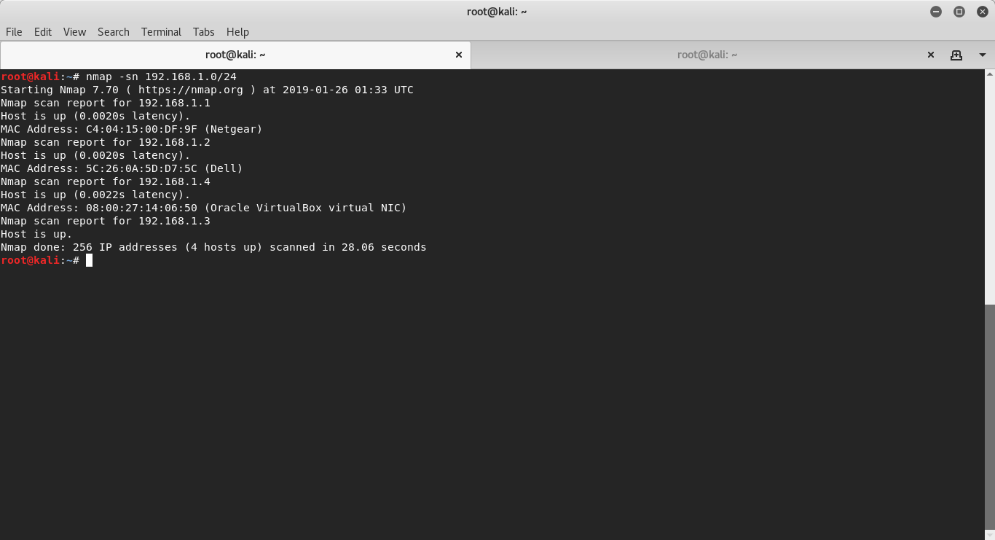
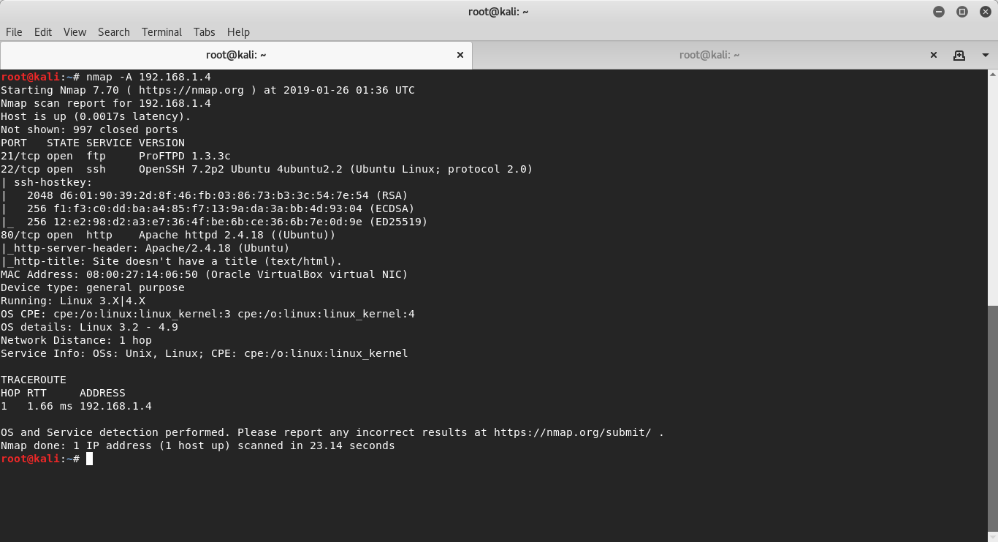
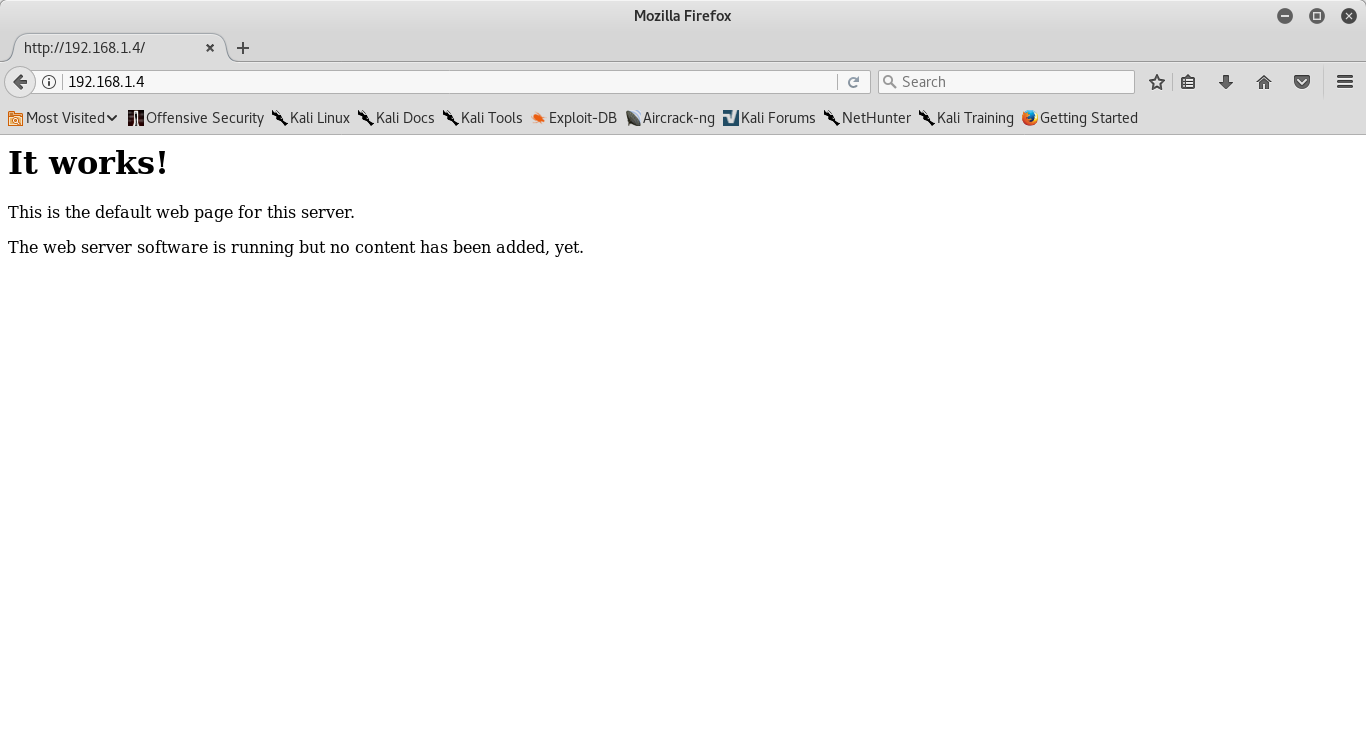
This is my writeup for the ctf box. I was on an isolated network, so there was only a few devices. Host discovery was simple.



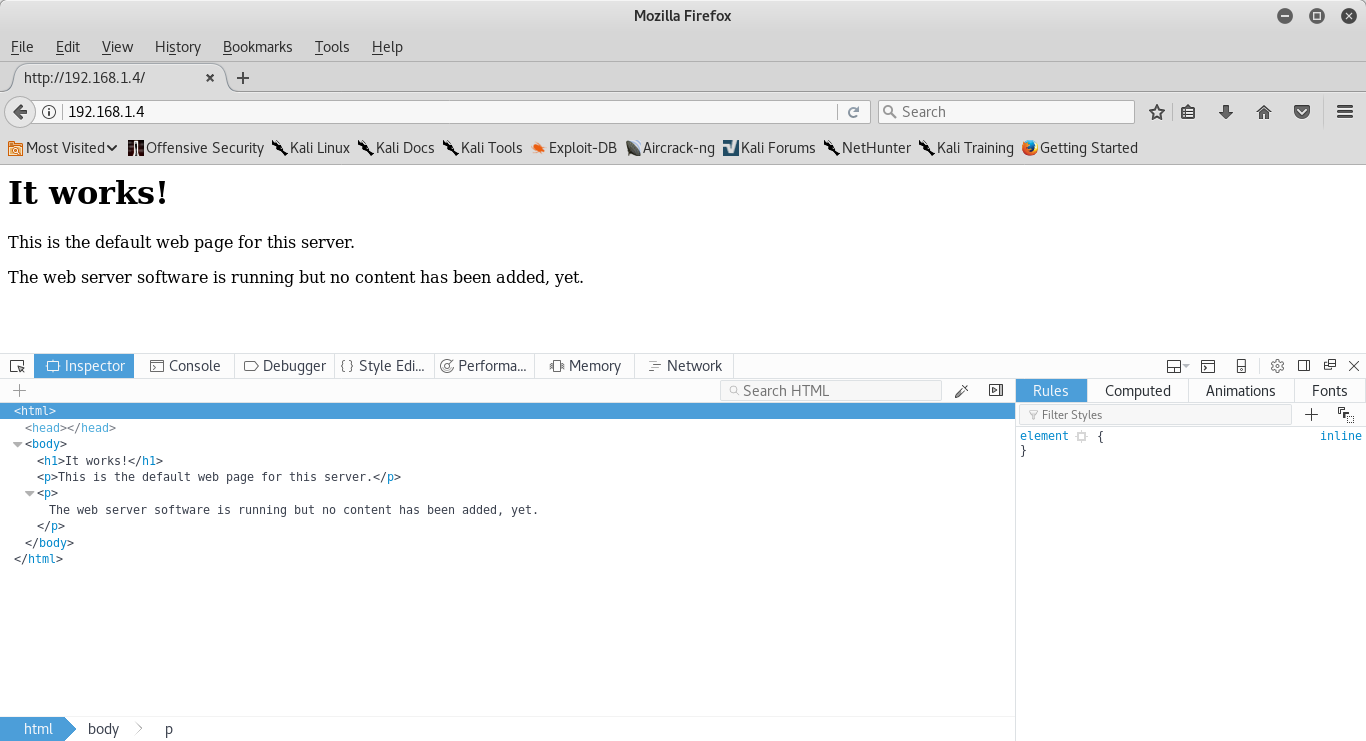
From here a did a more refined nmap search to find a bit more about what services the box has.

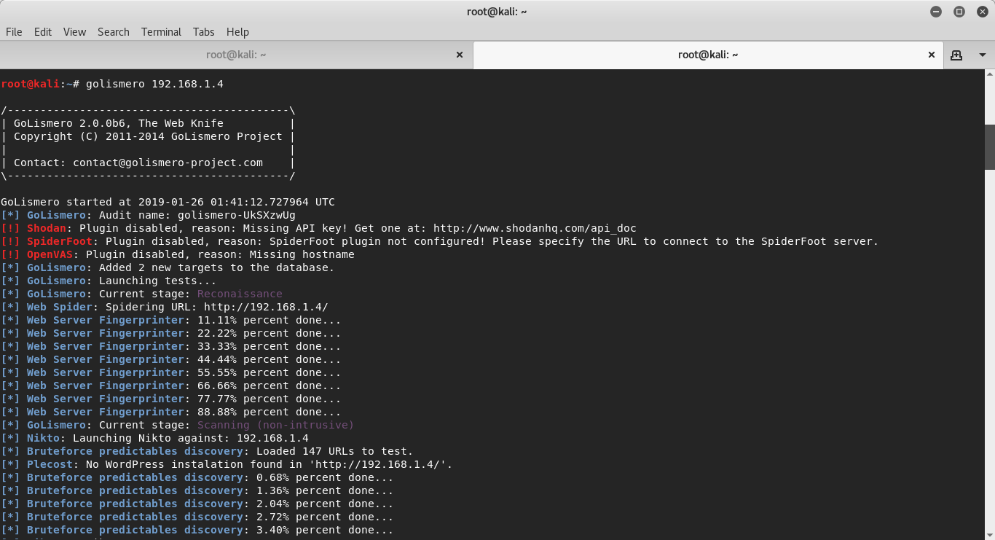


We find that port 80 is open with an Apache 2.4.18 server. We also find the box is Ubuntu, and a virtual box (I’m running it as a vm on an old dell laptop). Let’s check the website out.

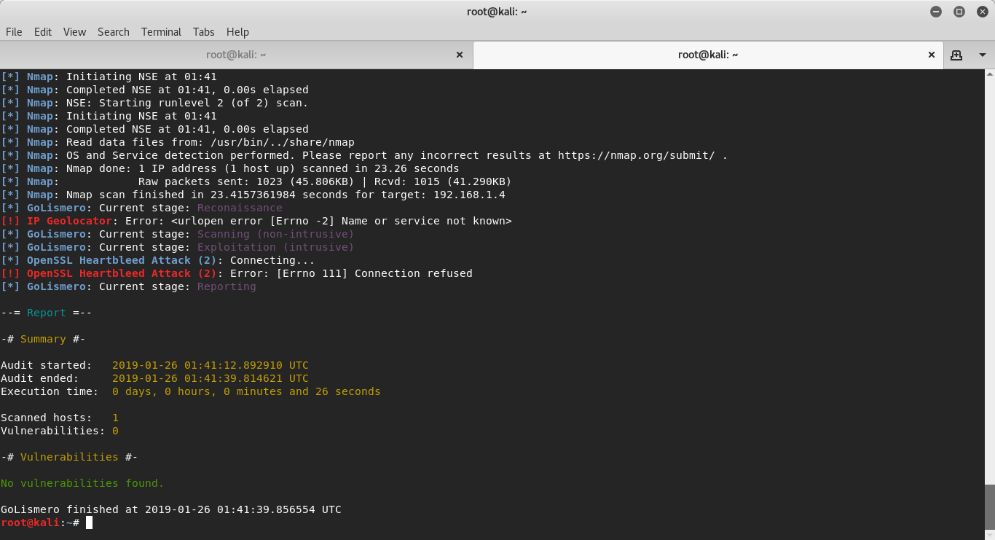


The website doesn’t have anything interesting, even after looking through the html.

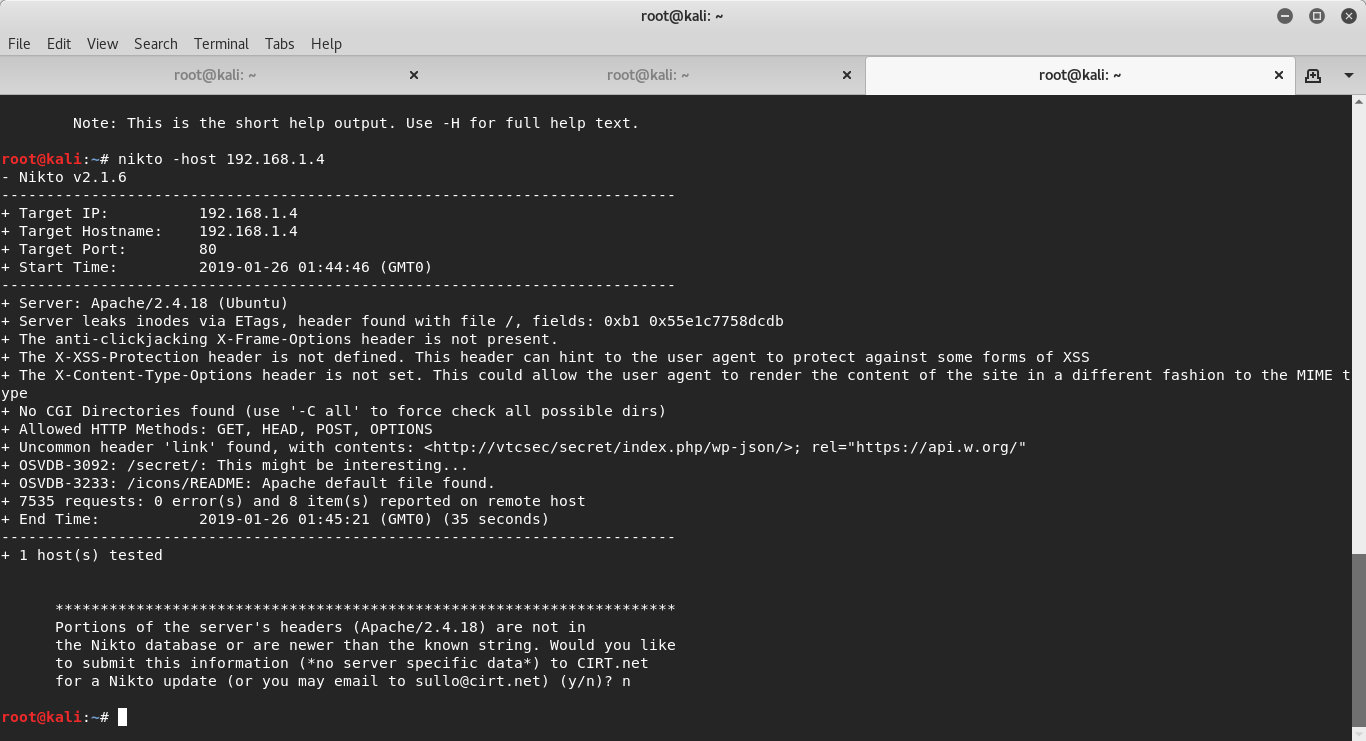


I decided to run golismero to find out anything I could about the website. 

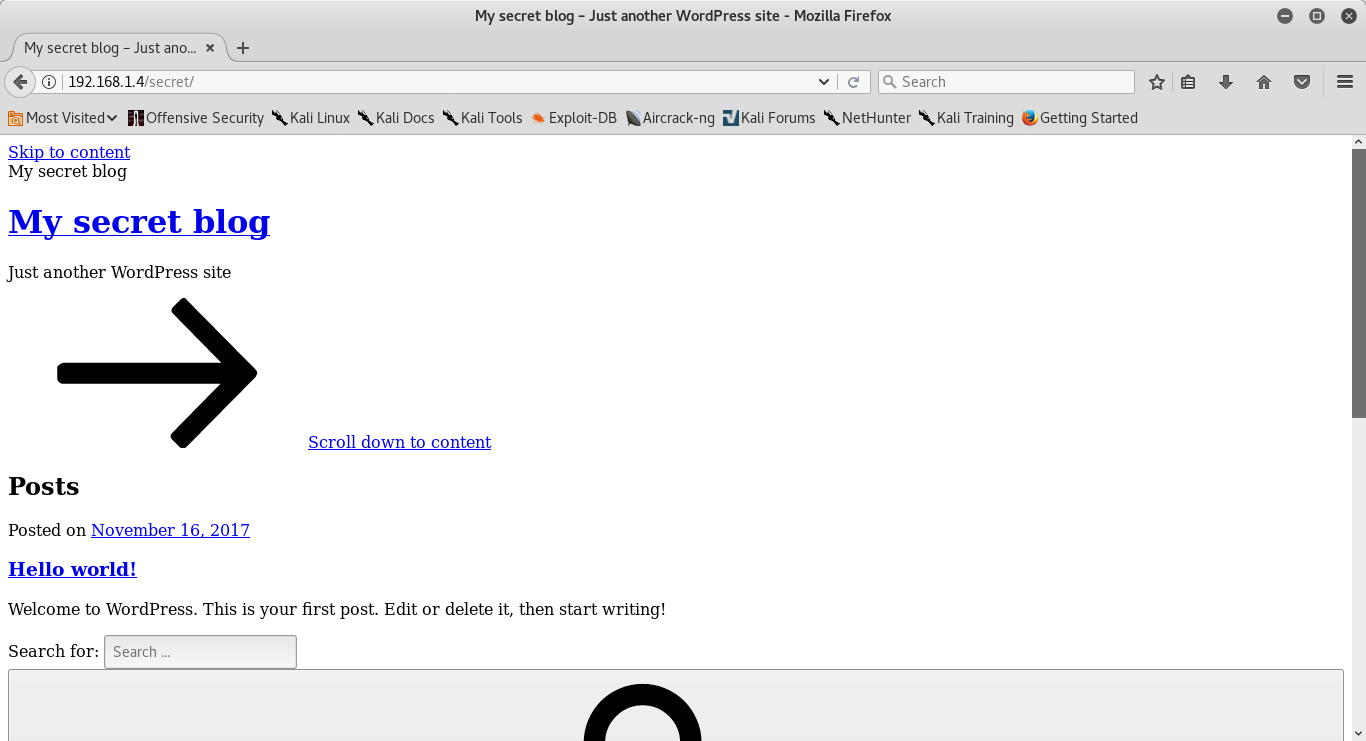
..snip



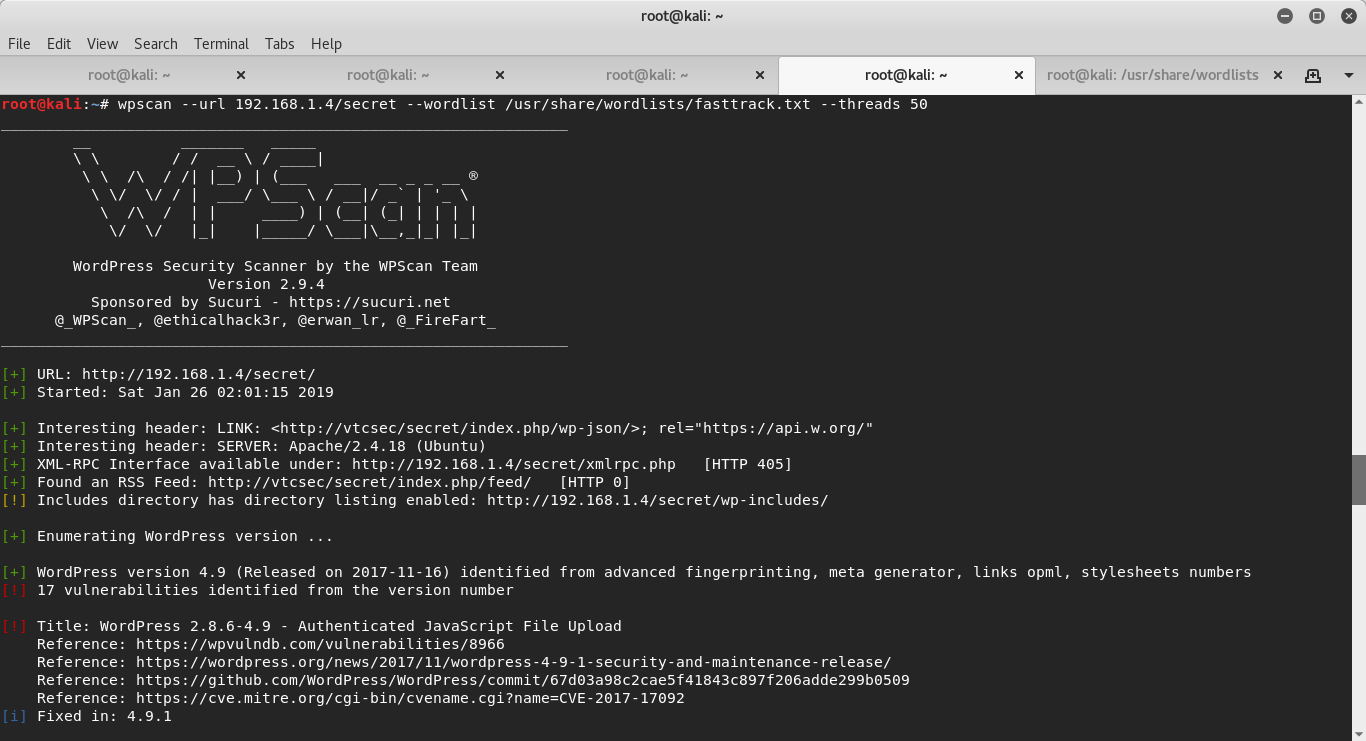
This couldn’t find anything at all that could help with the investigation. I decided to retry with nikto.



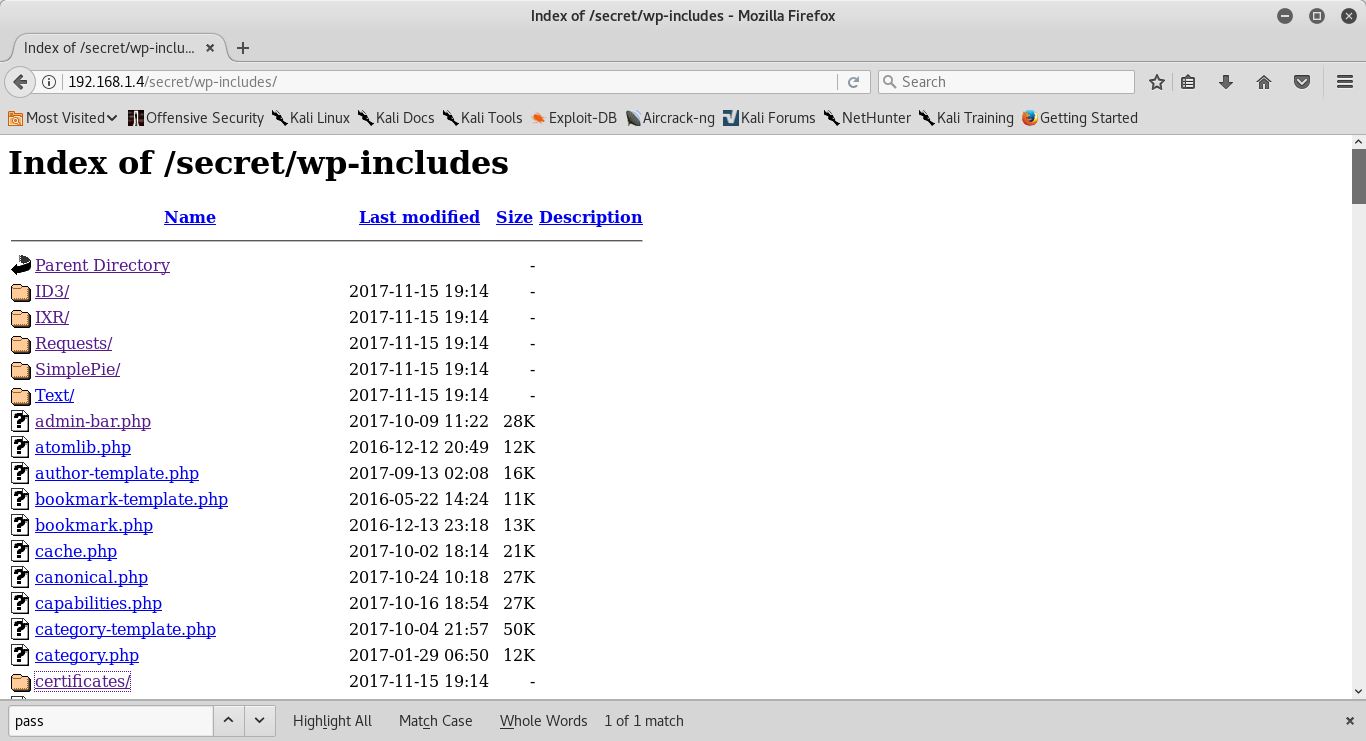
Here we get the /secret part of the webserver.



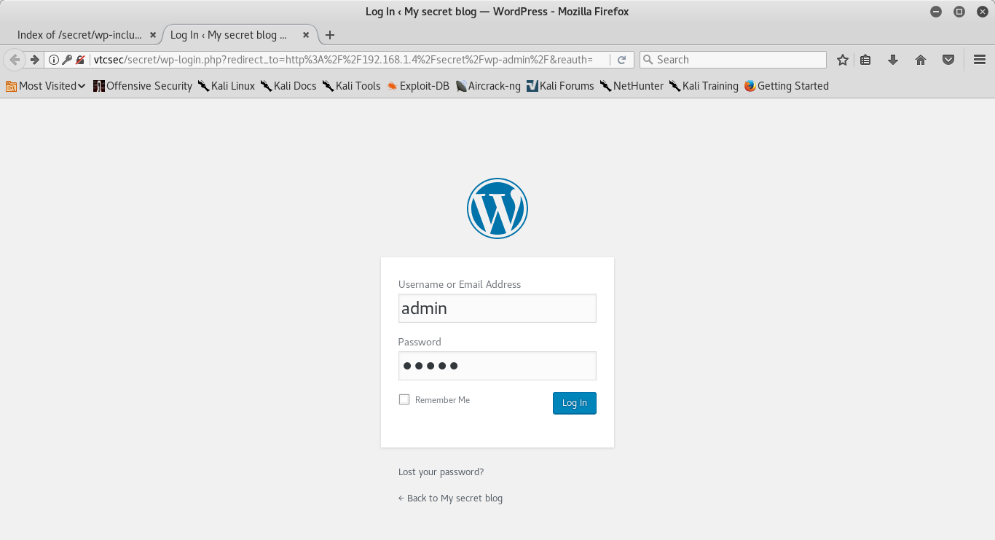
It looks a little weird because it reverences some other website for a style sheet, but we don’t need it to look nice. Let’s run it through wpscan because the title reveals it’s a WordPress site.



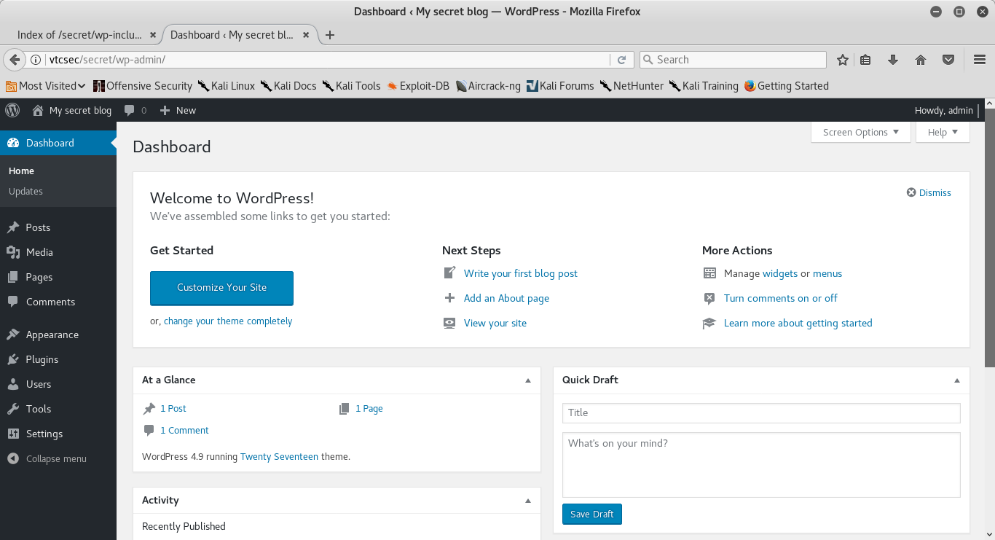
We get a directory listing. Let’s check it out.



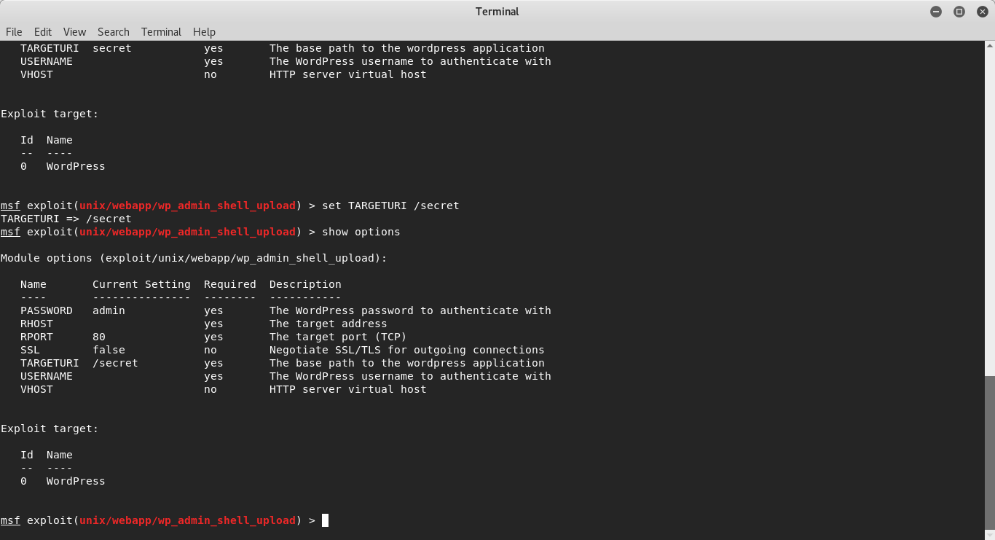
After looking for a while through the site, I couldn’t find anything. I decided to just tried a login for the admin page.



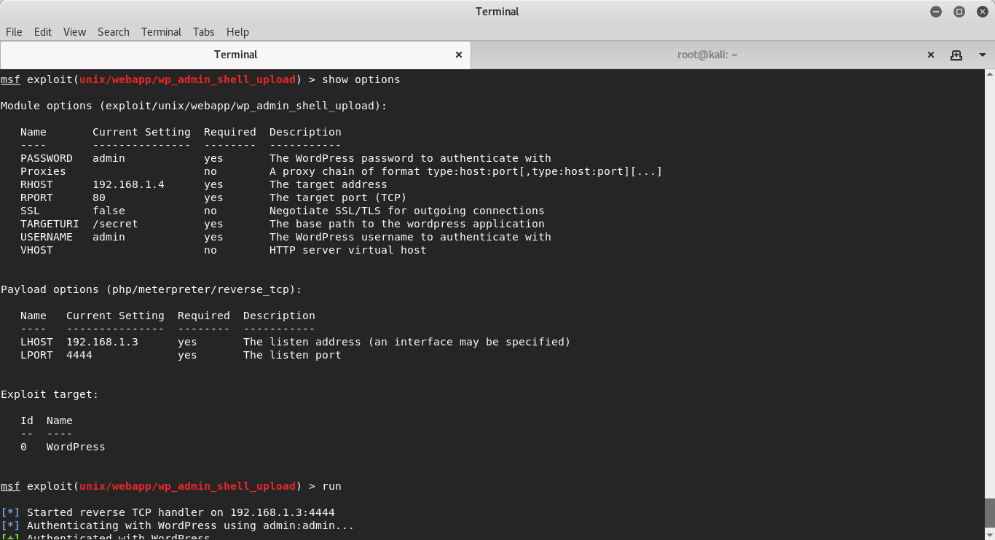
It worked! The login creds were just ‘admin’ ‘admin’.

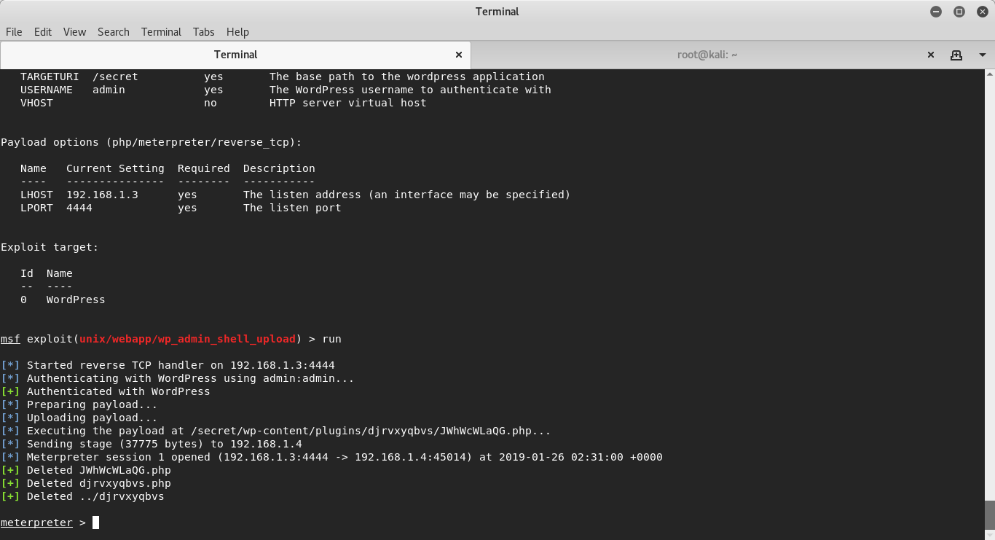


The admin panel doesn’t have much, but now that we have the login, we can upload the shell.

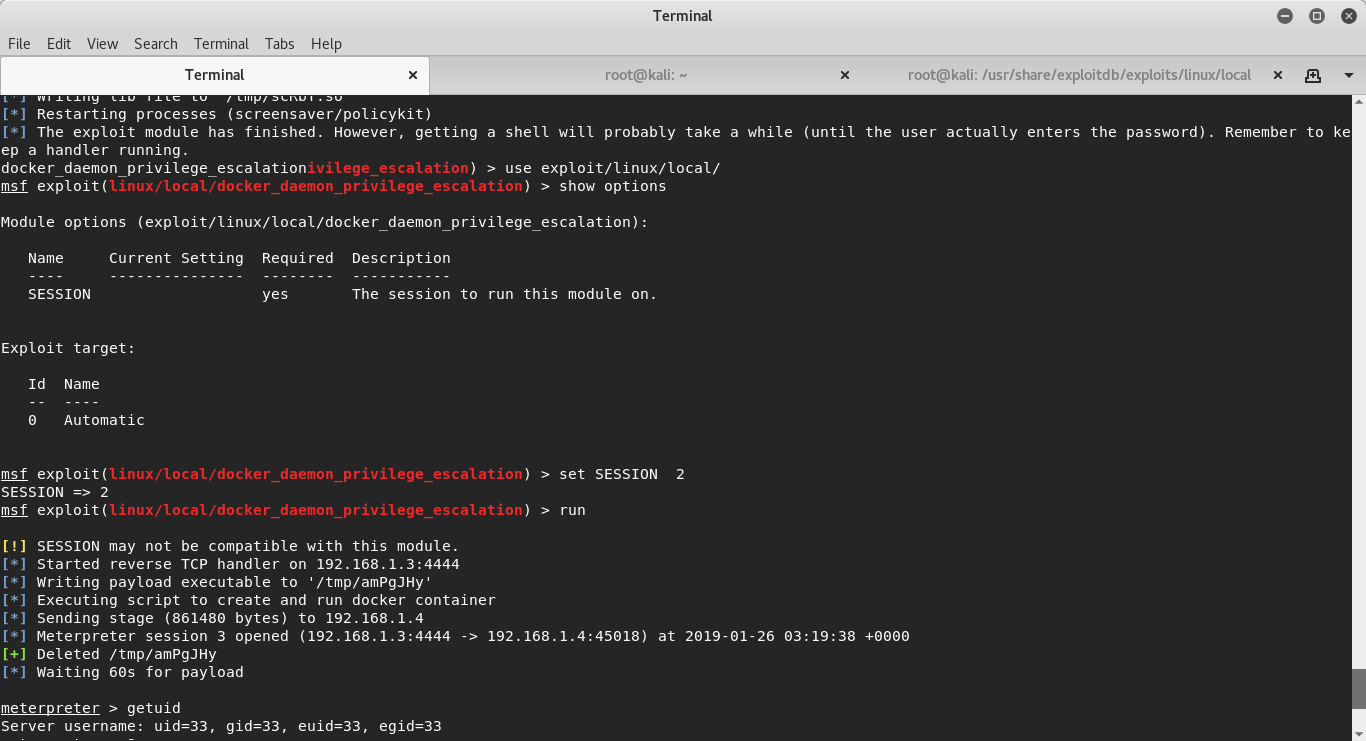


The Metasploit exploit is very simple, and exactly what we need. I set the payload to a the php meterpreter reverse tcp shell.





It worked! We have a meterpreter session!



We backgrounded the session and ran a priv esc module on it. We got the admin shell and thus ends the challenge.