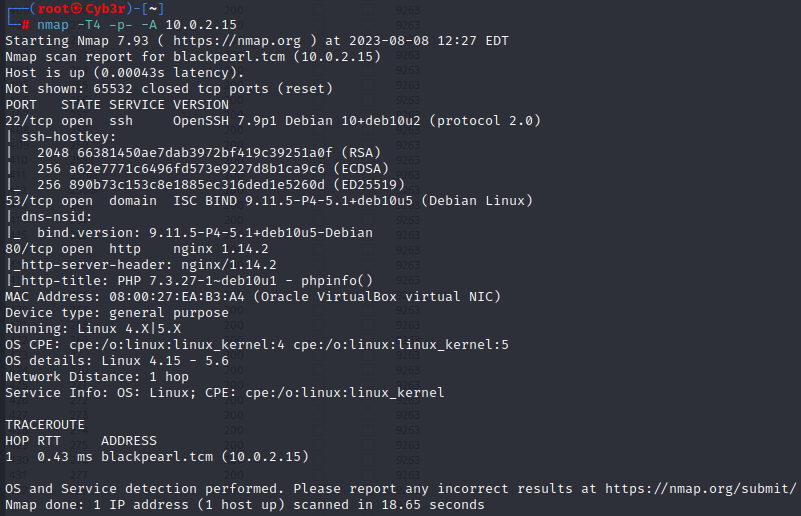
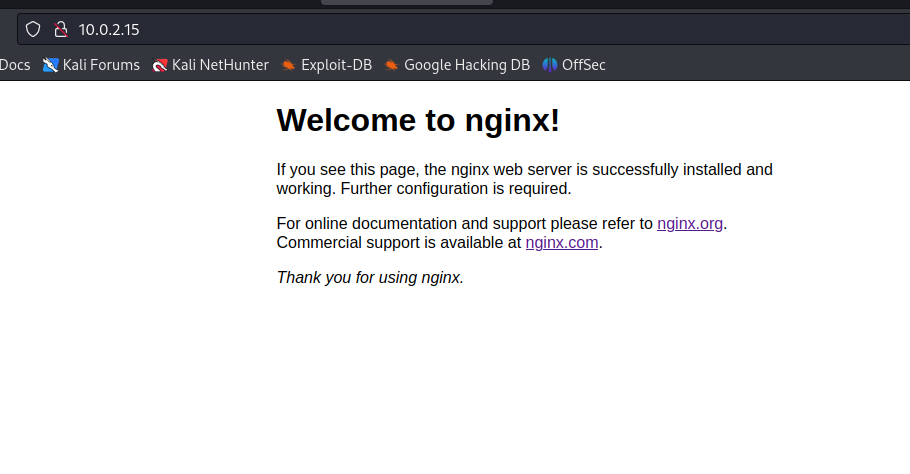
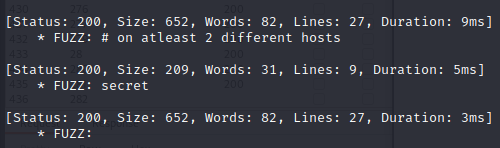
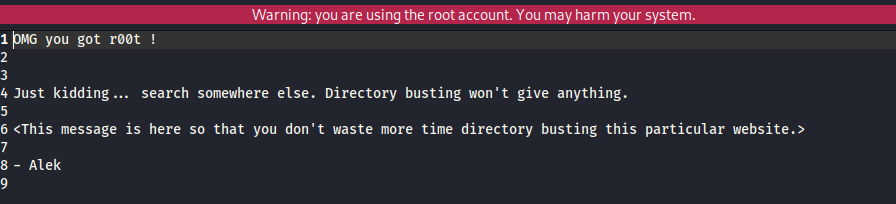
**BLACKPEARL**



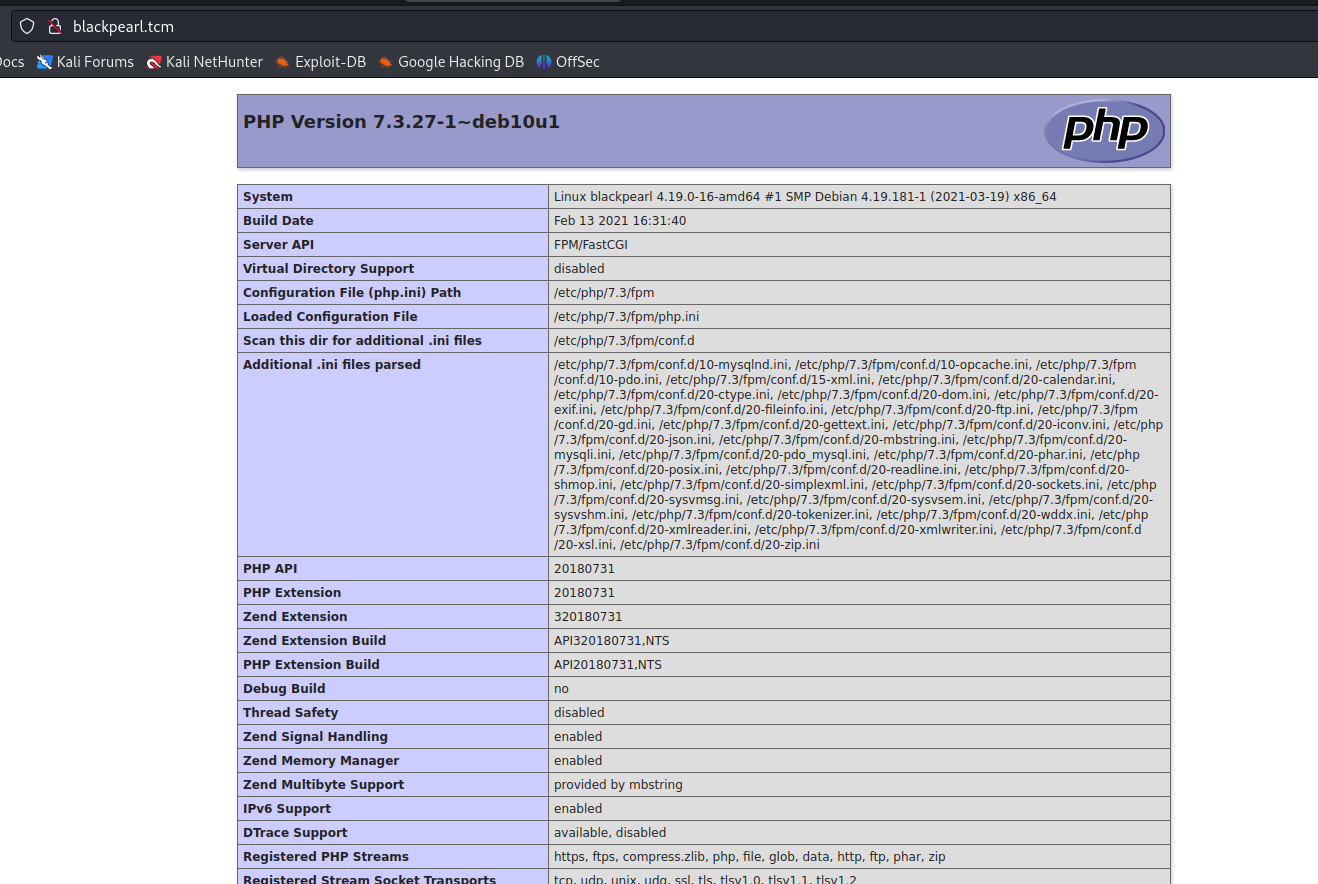


FFUF gives us a /secret and downloading the file is the output below,

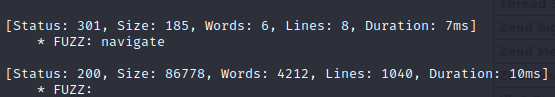


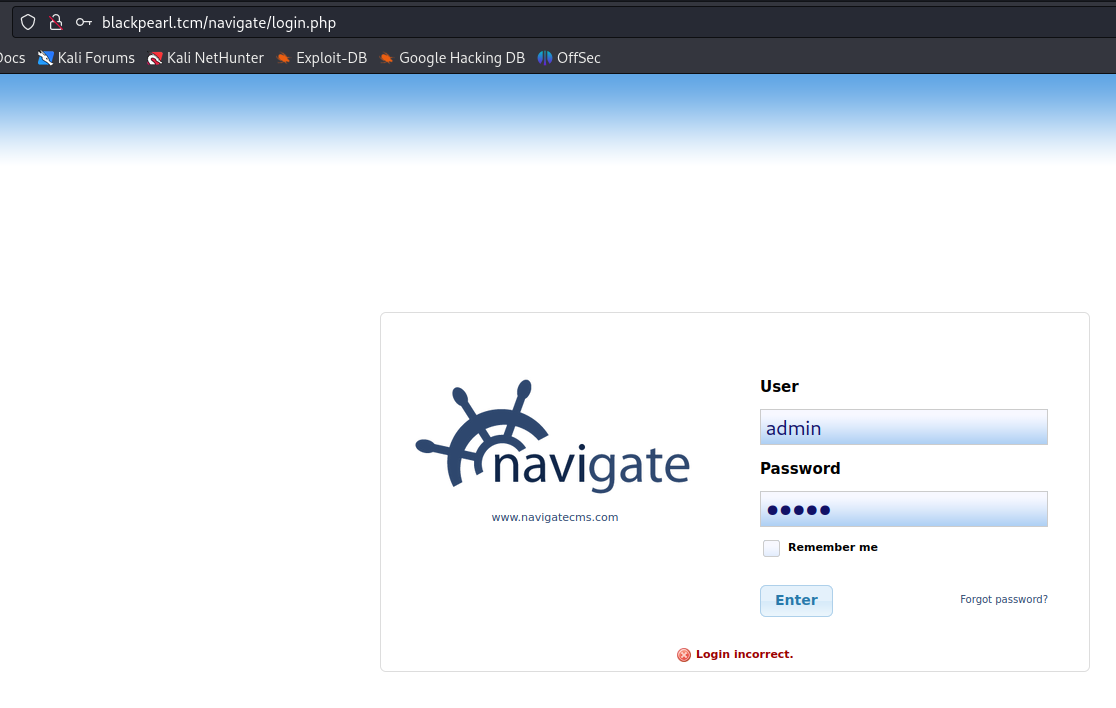


Secret told us to move on and we can see DNS service running on port 53 from nmap scan and then we add the IP and hostname to the /etc/hostname and we can go <http://blackpearl.tcm>

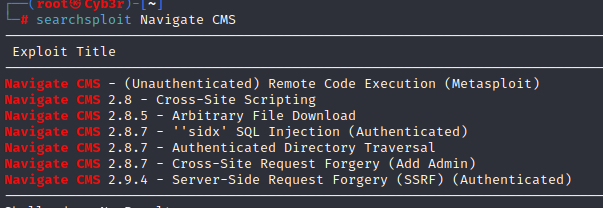


Since it opened up a webpage we decided to fuzz it again and this time we get navigate and the output when used as blackpearl/navigate is below as well

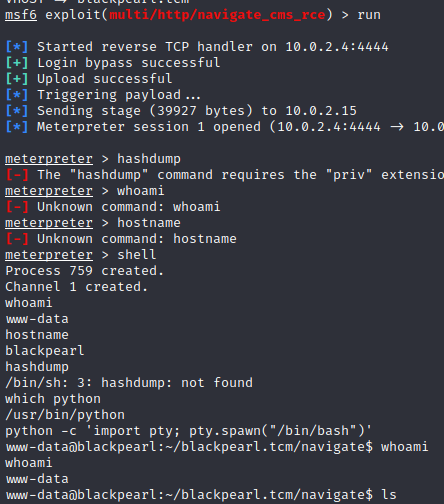




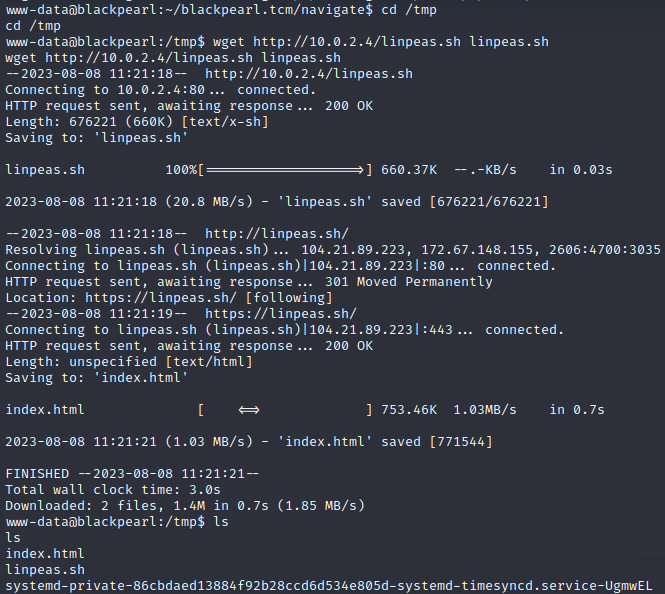
Using Exploit DB and searchsploit, we discovered that it is vulnerable



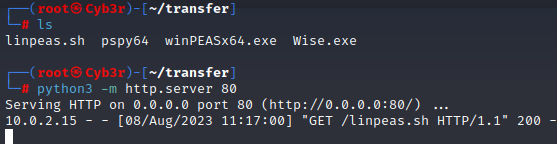
Rapid 7 had a walkthrough and we used msfconsole and we got a shell as below



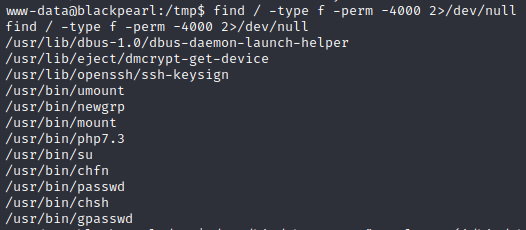
For privilege Escalation, we had to copy the Linpeas for Linux Privilege Escalation into the shell created



Don’t forget to host a python server in the same directory as the linpeas b4 running this

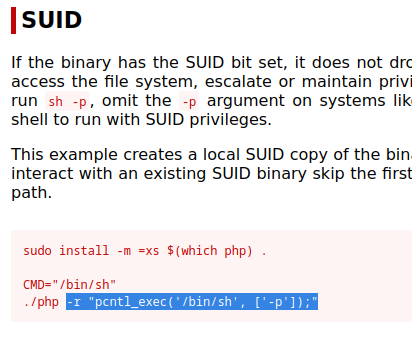




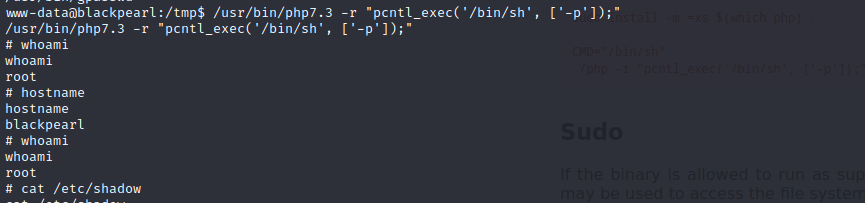


This command is used with linpease to arrange everything permissions

Then we had to go priv escalation using GTFOBIN



We edited the above from PHP in gtfobin because it had PHP and had this below,



And we are rooooooooooooooooooottttttttttttttttttt