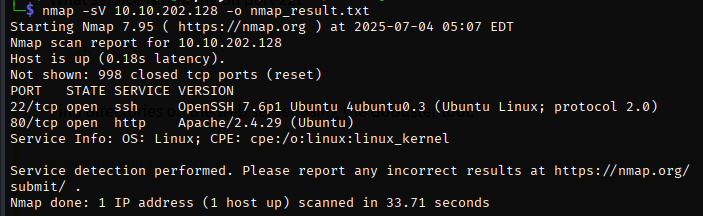
RootMe THM CTF writeUP

Nmap result



How many ports are open? **2**

What version of Apache is running? **2.4.29**

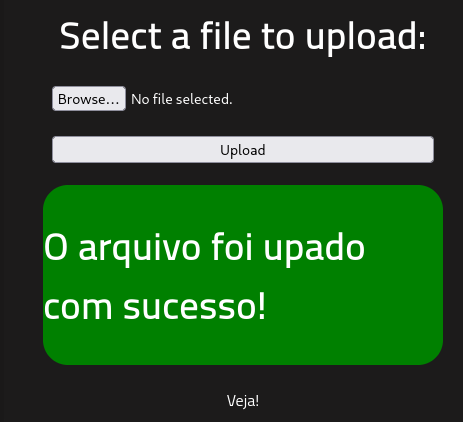
What service is running on port 22? **SSH**

Directory finding with gobuster

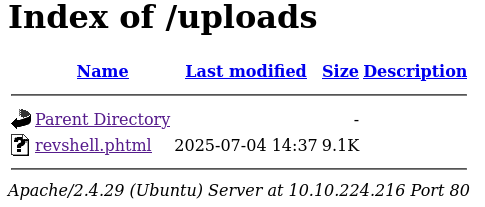


The hidden dir: /panel/

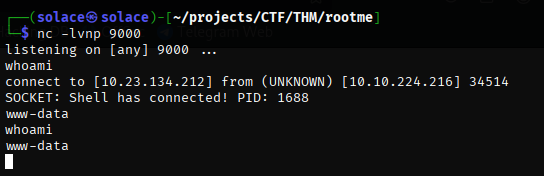
I browse http://<IP>/panel and then I uploaded a php revshell file but the allowed extension was not php, so I used another extension from google( .phtml , php3 , php4 …etc ). We’ll go in order and try changing the file extension to .phtml.



Success! The form lets us upload our shell and we can find it under the /uploads directory that we also found with Gobuster earlier.



We’ll keep it simple and utilise a basic netcat listener and execute the shell.



find -name user.txt 2> /dev/null then I got the user flag

Then, Search for files with SUID permission, which file is weird?/usr/bin/python

root.txtTHM{pr1v1l3g3\_3sc4l4t10n}

