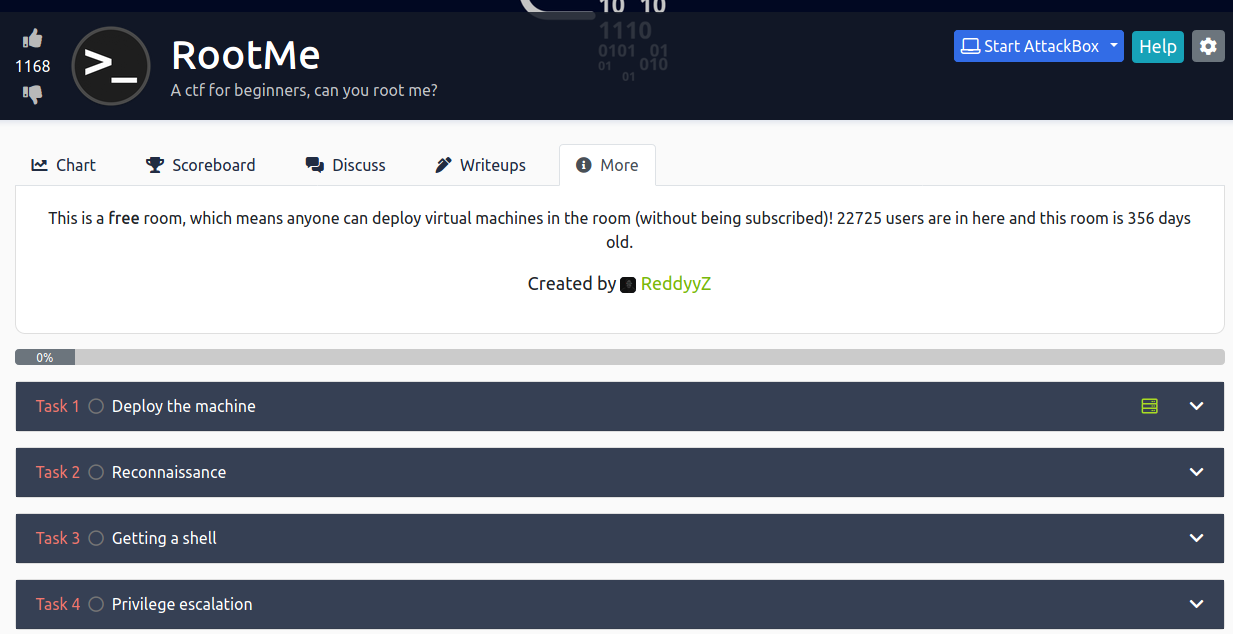
**RootMe write-up**

This is write-up for RootMe CTF in TryHackMe which is a beginner CTF that we have to exploit web server, gain access to target machine and elevate privilege to rock this box

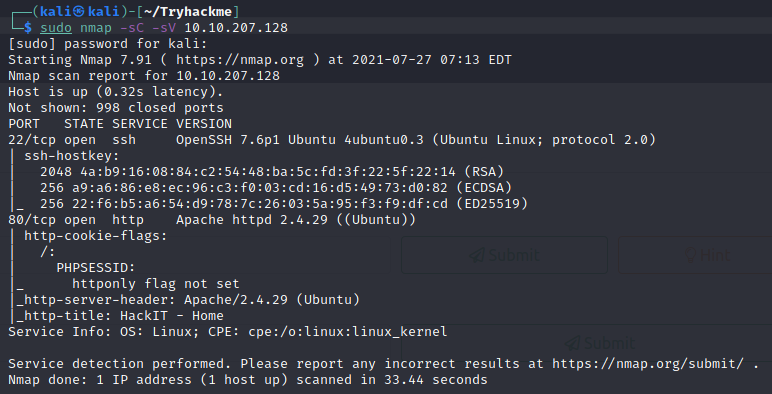
Site: <https://tryhackme.com/room/rrootme>



**Reconnaissance**

**Scan the machine, how many ports are open?**

Always start with nmap and we can see that 2 ports are opened





**What version of Apache is running?**

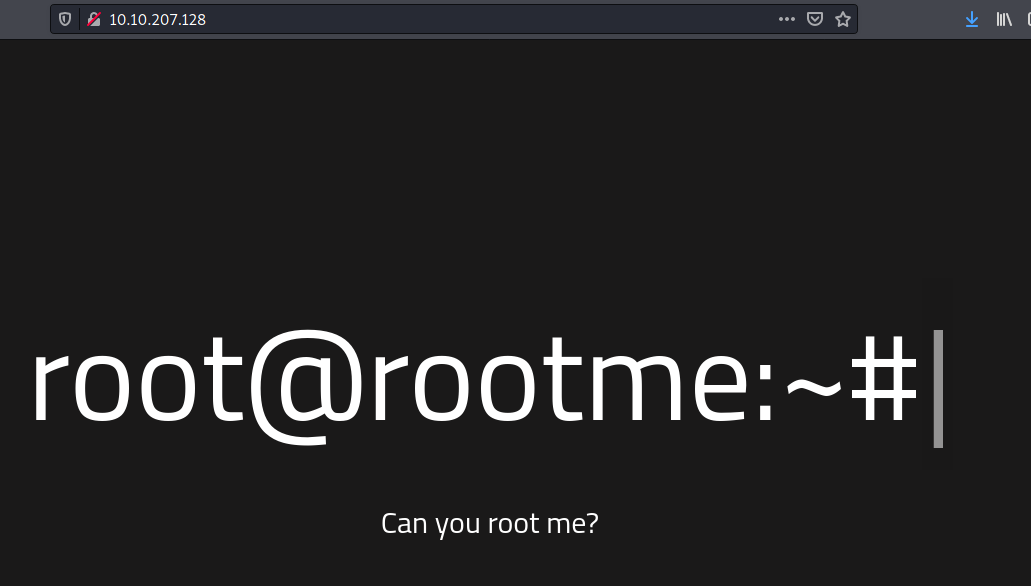


**What service is running on port 22?**

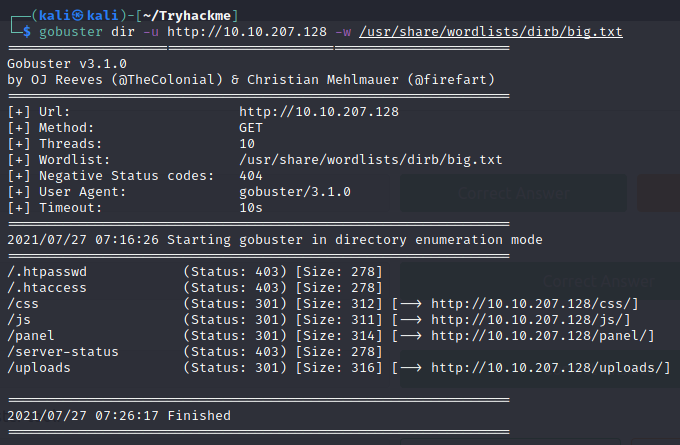


**Find directories on the web server using the GoBuster tool.**

Visit website and we can’t do anything here so it’s gobuster time

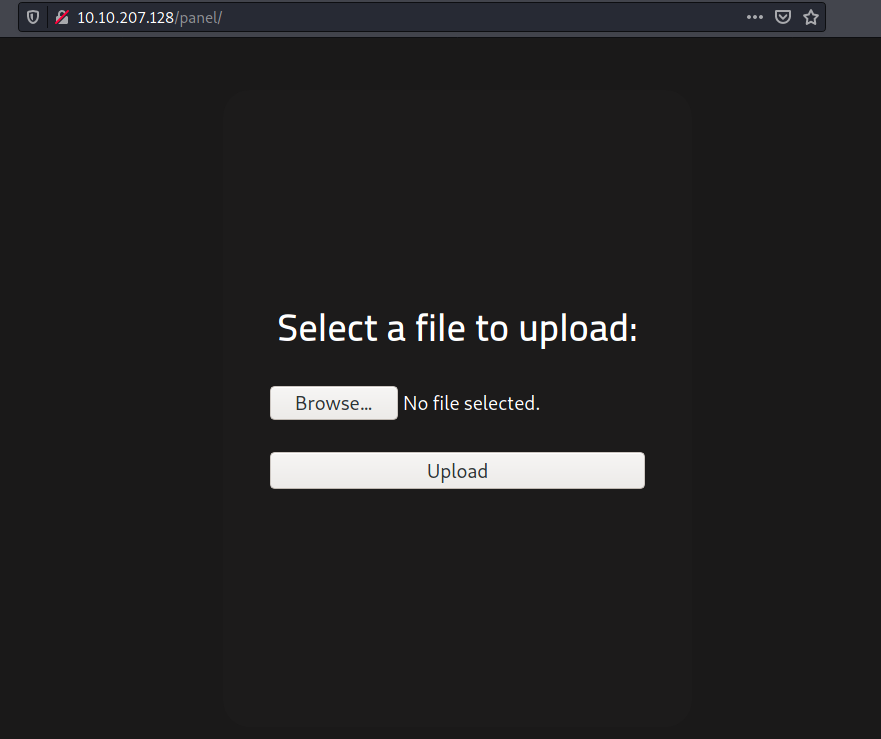


After gobuster finished it’s works we found that /panel and /uploads are stand out



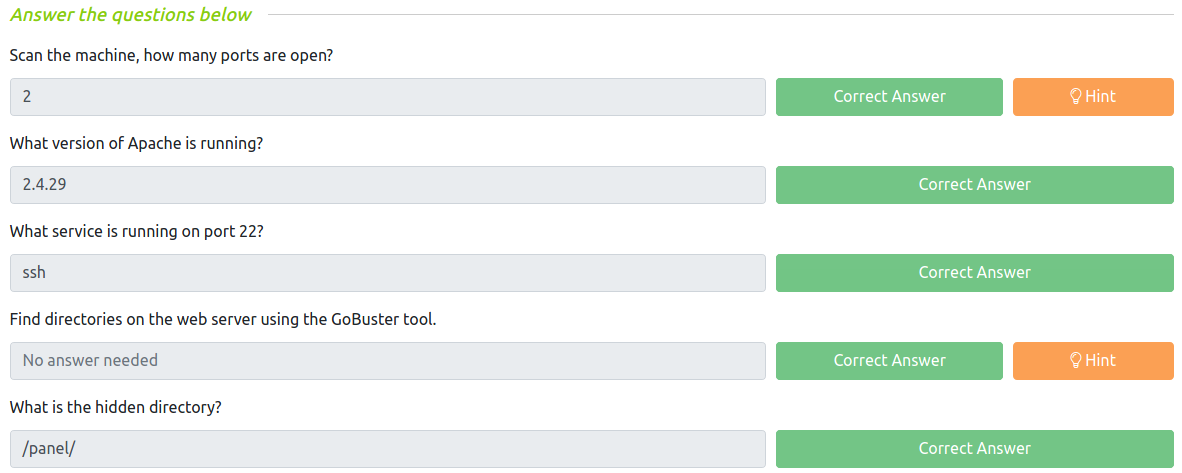
**What is the hidden directory?**

Visit panel webpage and it’s a upload file page





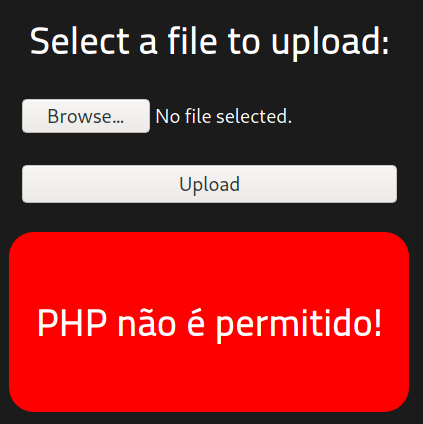
Answer – Reconnaissance



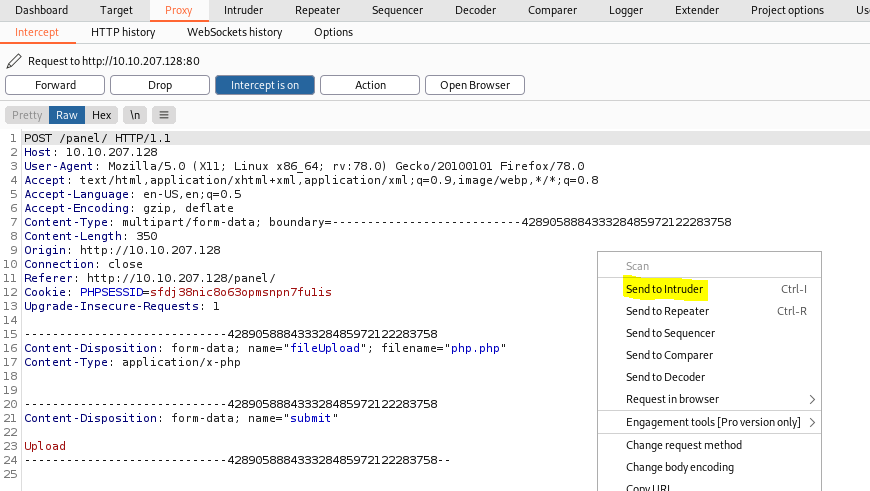
**Getting a shell**

**user.txt**

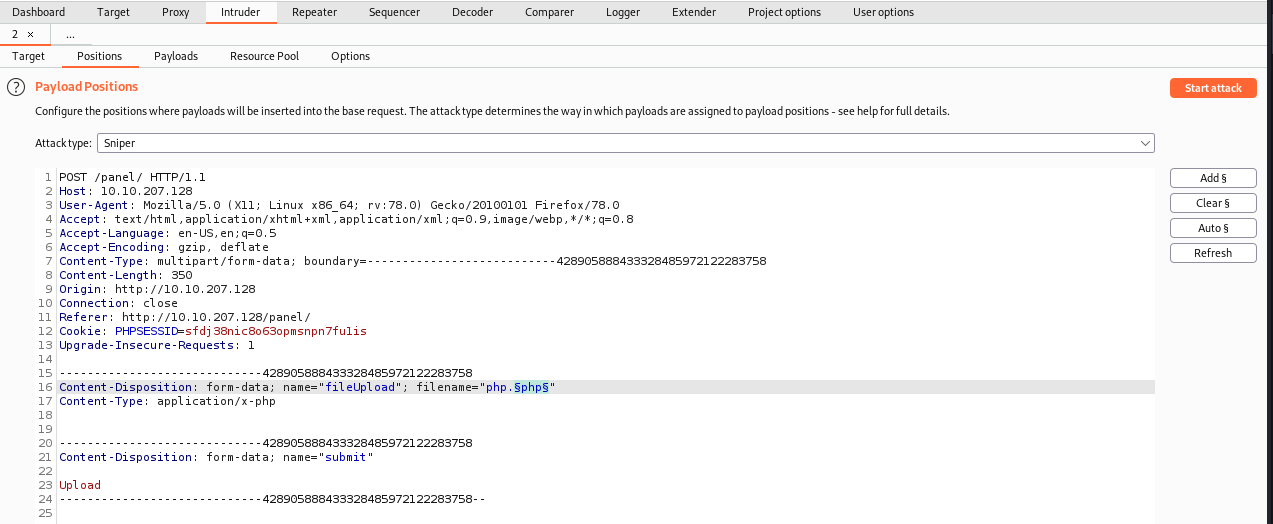
tried upload some files and it’s block .php extension

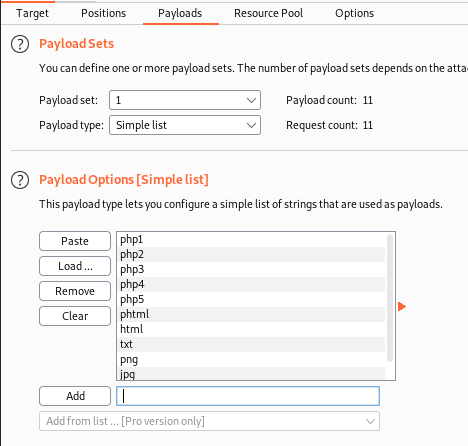


We will figure it out which extension is safe by intercept HTTP request with Burp suite and send it to Intruder

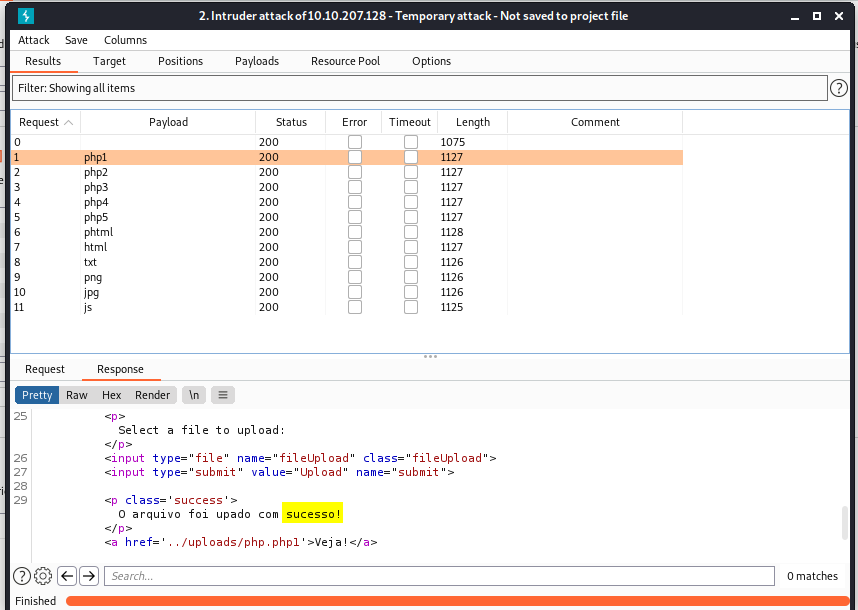


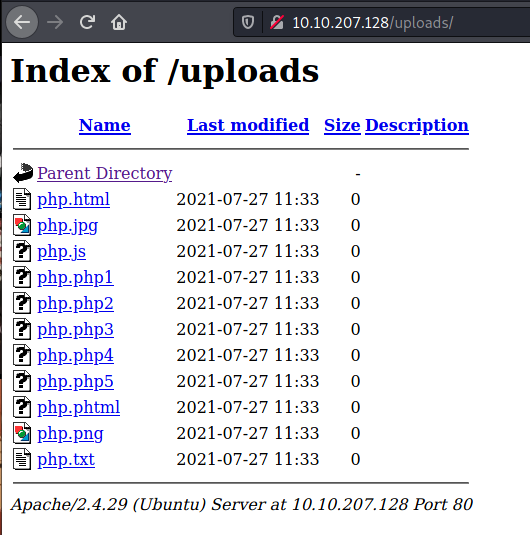
Set up everything and ready to launch



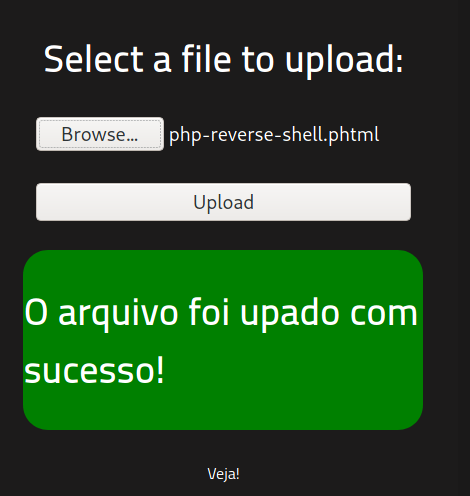


And all of this is success, it seems this website blocked only php extension

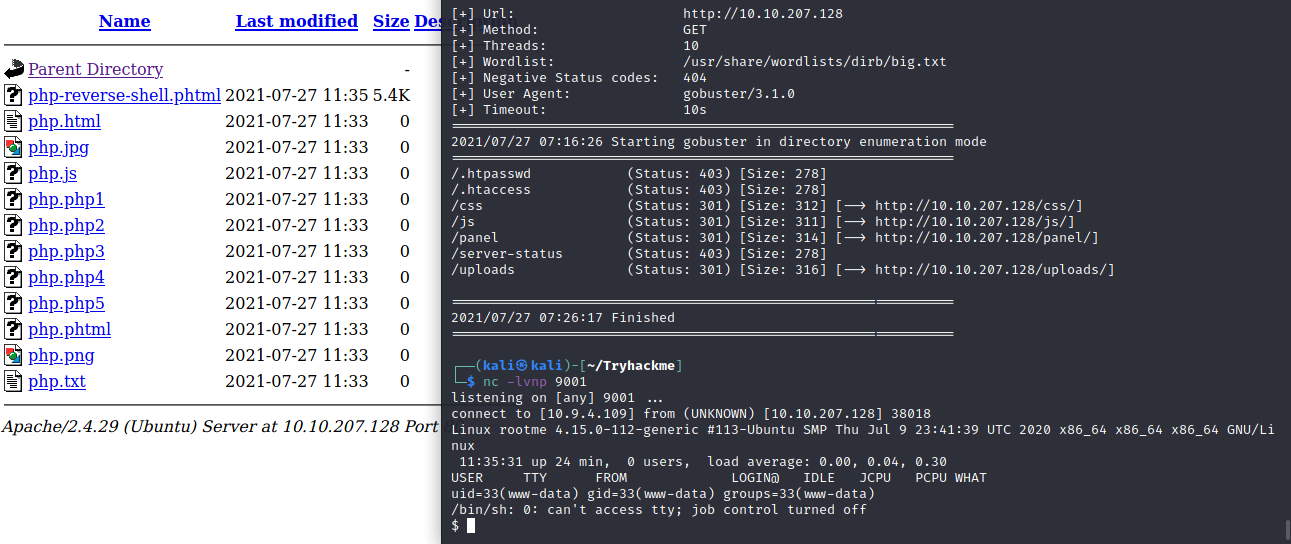




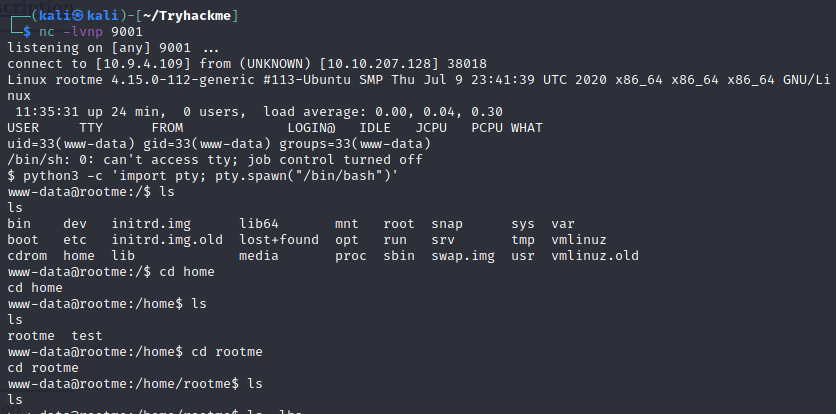
Now time to upload php reverse shell with any extension that could be executed to get the shell back



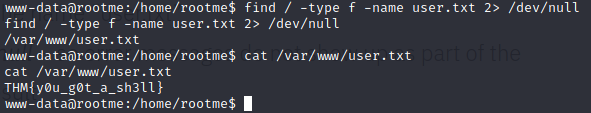
Setup Netcat listening and run reverse shell script that we uploaded earlier

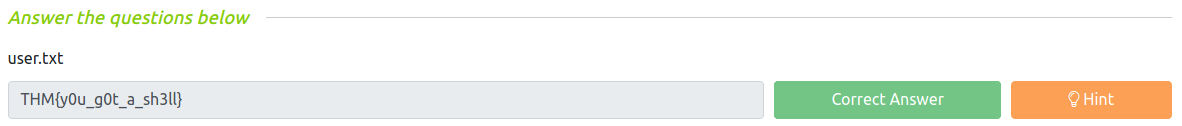


Explore file system and we found that there are 2 users in this home directory and nothing much we can do there because we don’t have permission



We don’t know password for any user, we don’t know anything so now it’s time to find a user flag and capture it

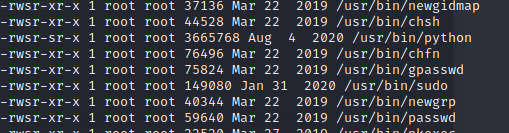




**Privilege escalation**

**Search for files with SUID permission, which file is weird?**

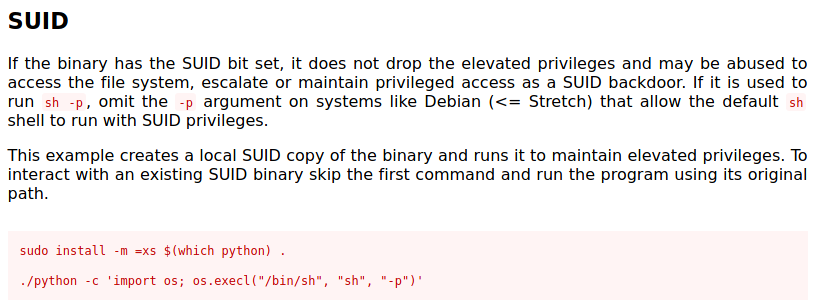
Using command **find / -user root -perm /4000 2> /dev/null** to find any executable files that we can abuse to gain root privilege and I think python is stand out there



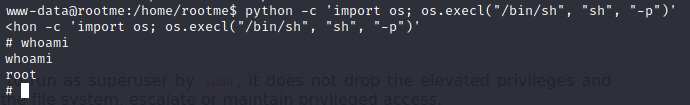


**Find a form to escalate your privileges.**

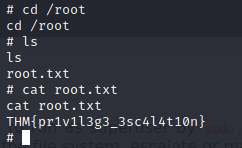
Go to GTFOBins and do what we need to



Now we got a root shell



Go to root directory and capture root flag!



**root.txt**

****

Answer – Privilege escalation

