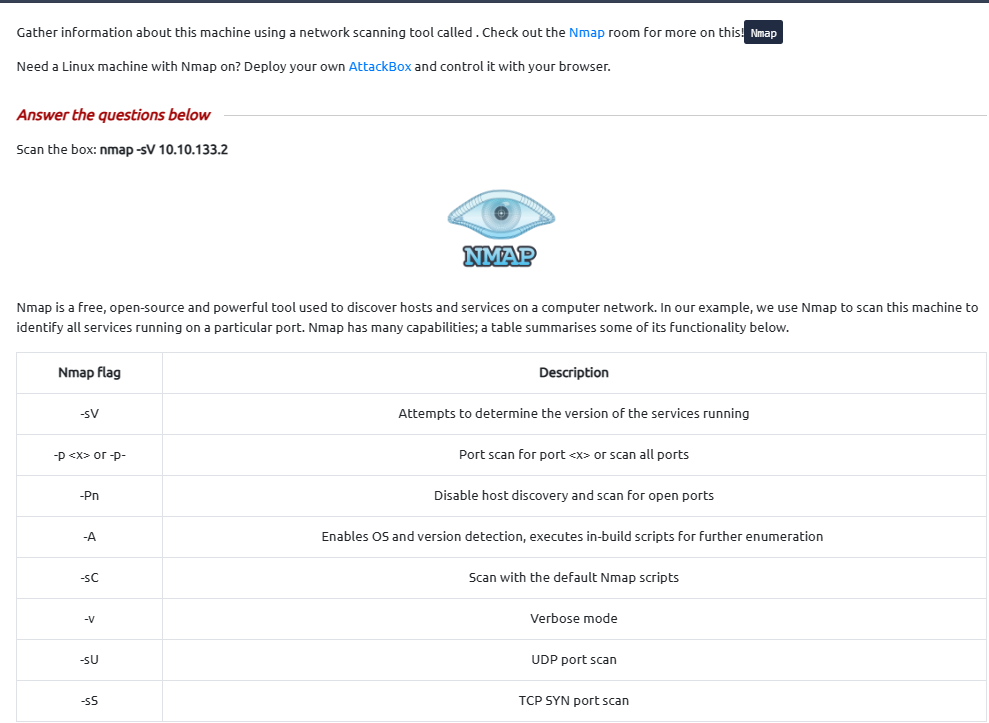
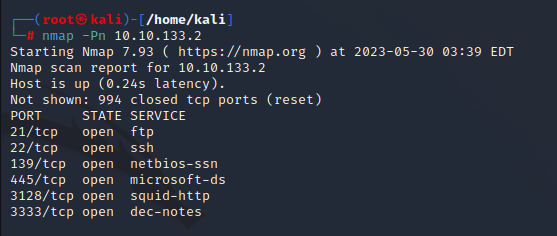
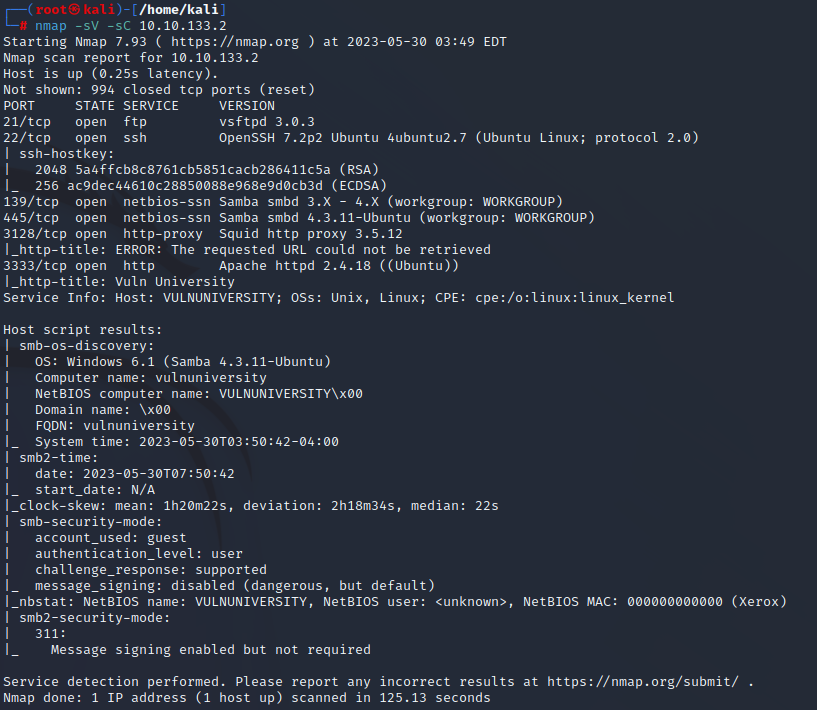
Task 2  Reconnaissance



Scan the box; how many ports are open? 6



What version of the squid proxy is running on the machine? 3.5.12



How many ports will Nmap scan if the flag -p-400 was used? 400

man nmap| less +/-p-

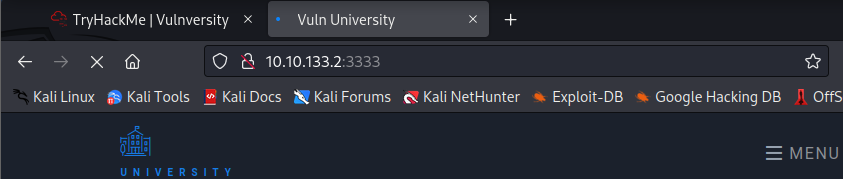
What is the most likely operating system this machine is running? Ubuntu

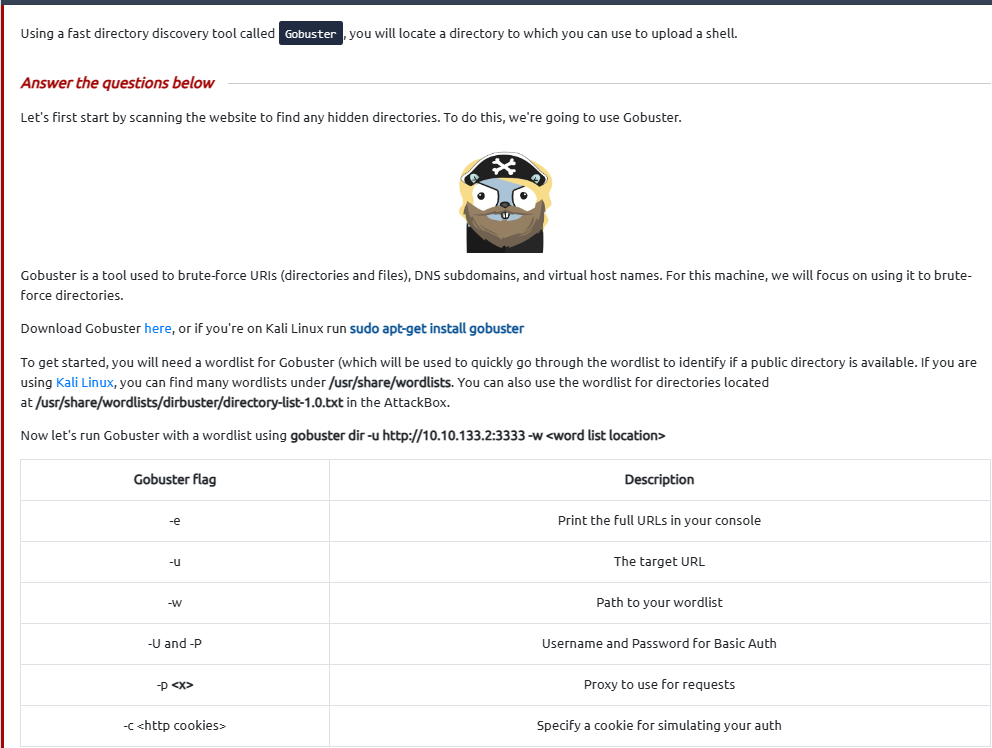
What port is the web server running on? 3333

It's essential to ensure you are always doing your reconnaissance thoroughly before progressing. Knowing all open services (which can all be points of exploitation) is very important, don't forget that ports on a higher range might be open, so constantly scan ports after 1000 (even if you leave checking in the background).

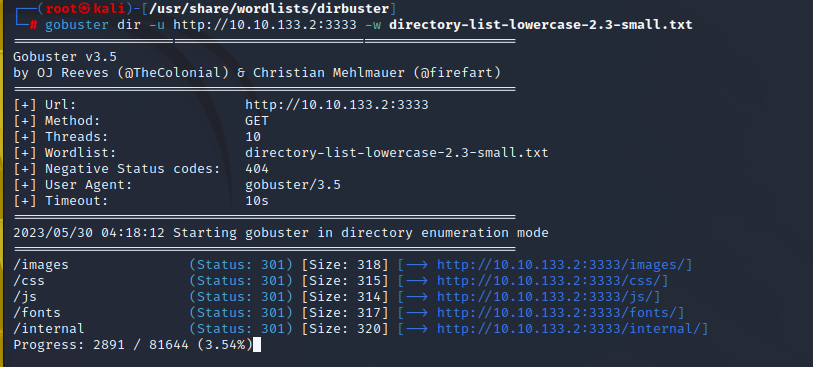
What is the flag for enabling verbose mode using Nmap? -v

Task 3  Locating directories using Gobuster

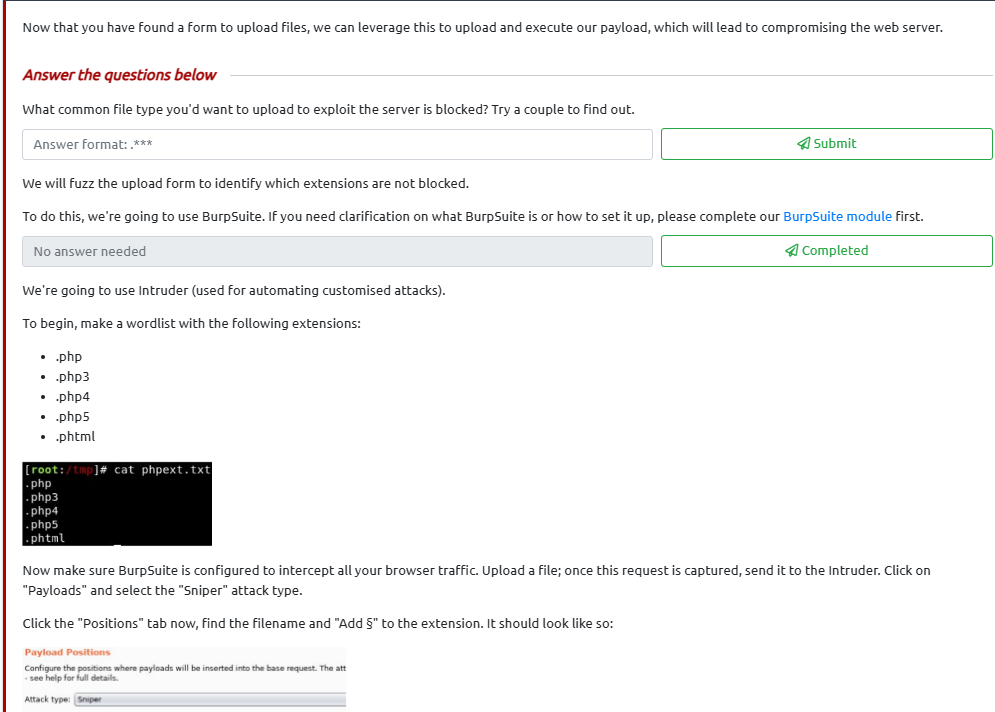




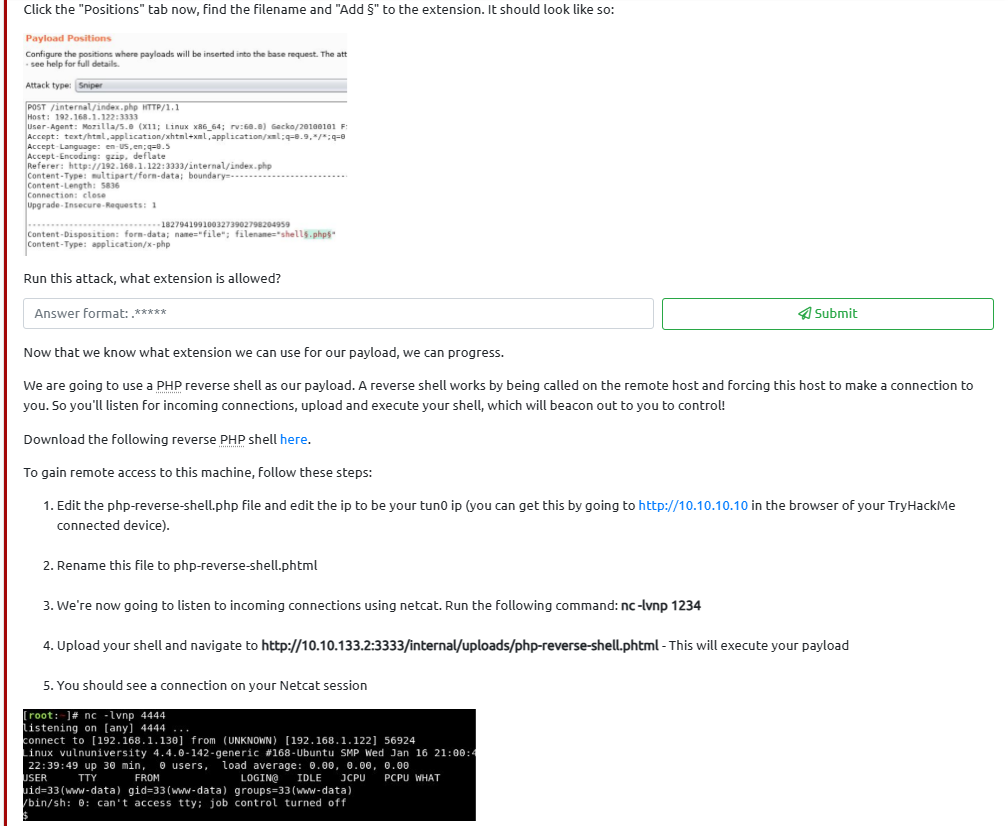
What is the directory that has an upload form page? /internal/



Task 4  Compromise the Webserver

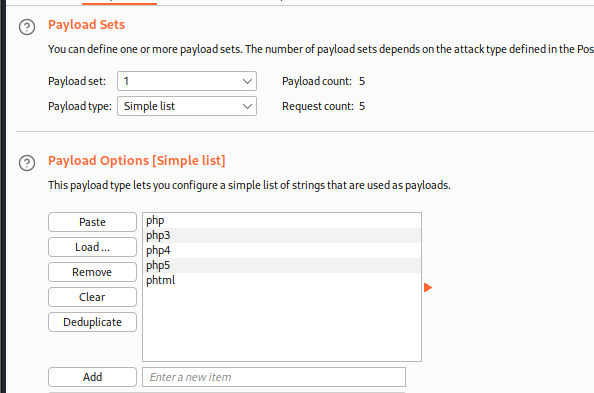


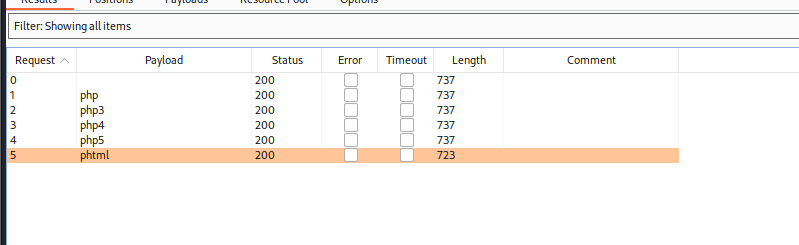
* .php



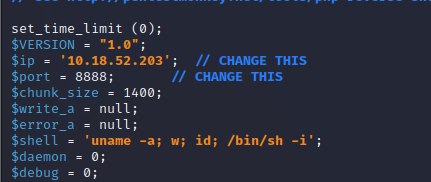
* Run this attack, what extension is allowed? .phtml

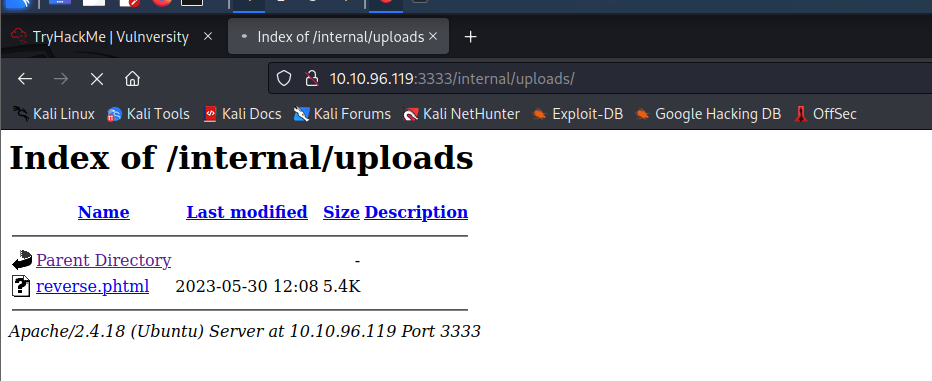


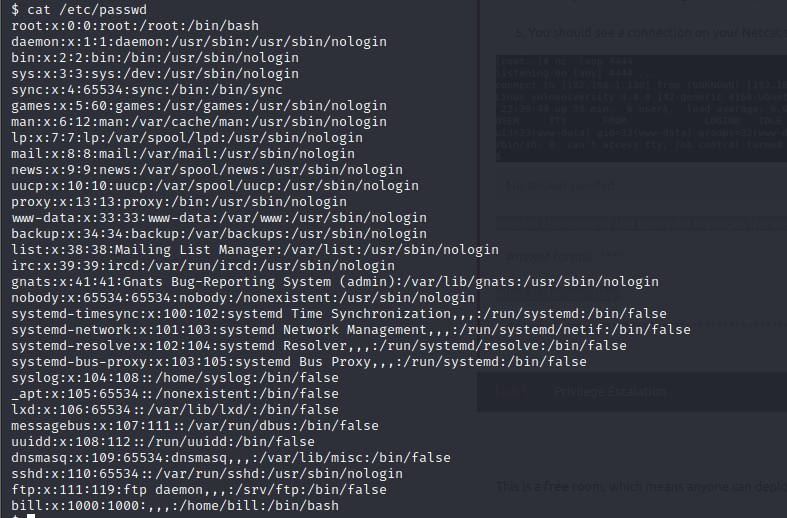




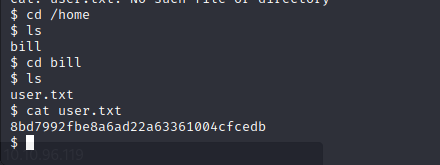
* Phtml





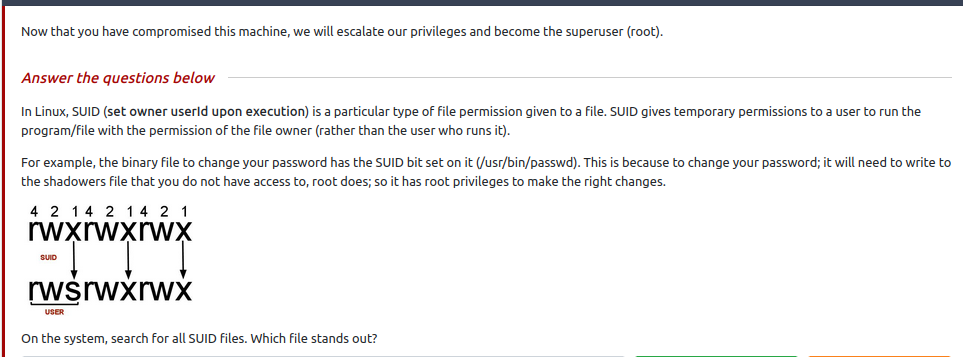


What is the name of the user who manages the webserver? bill

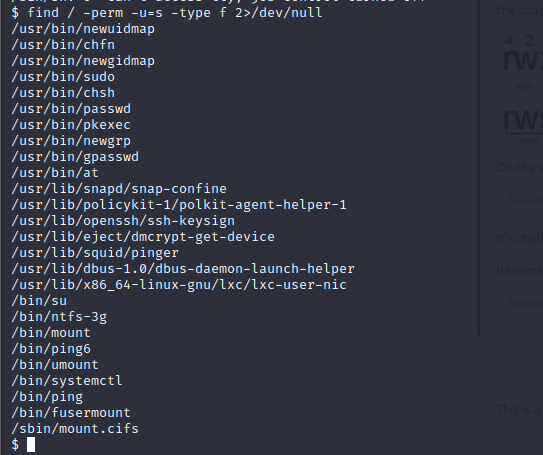


What is the user flag? 8bd7992fbe8a6ad22a63361004cfcedb

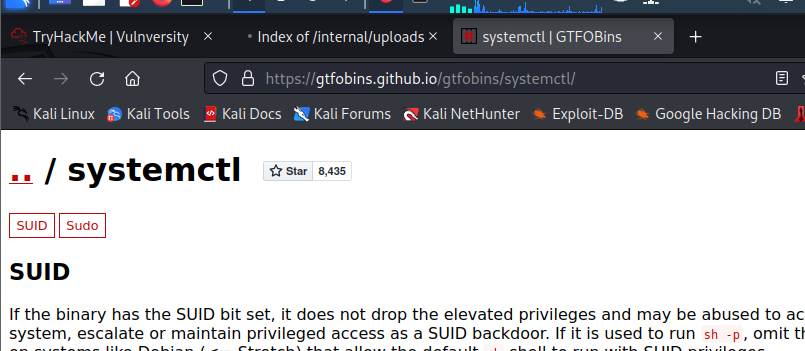
Task 5 Privilege Escalation

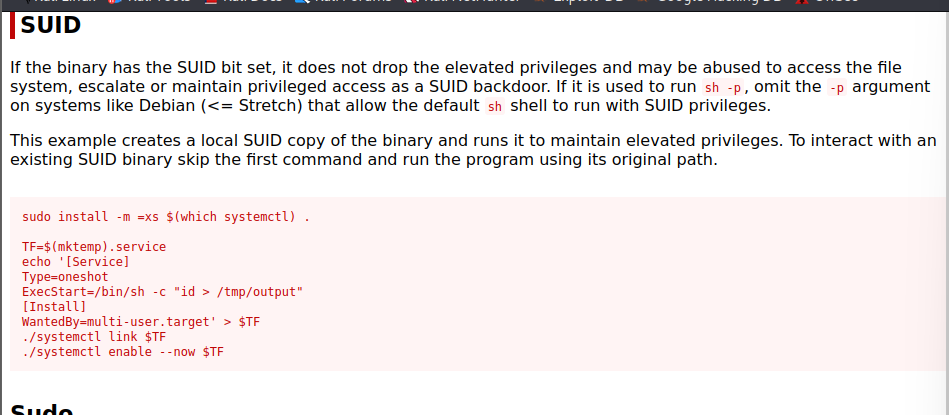


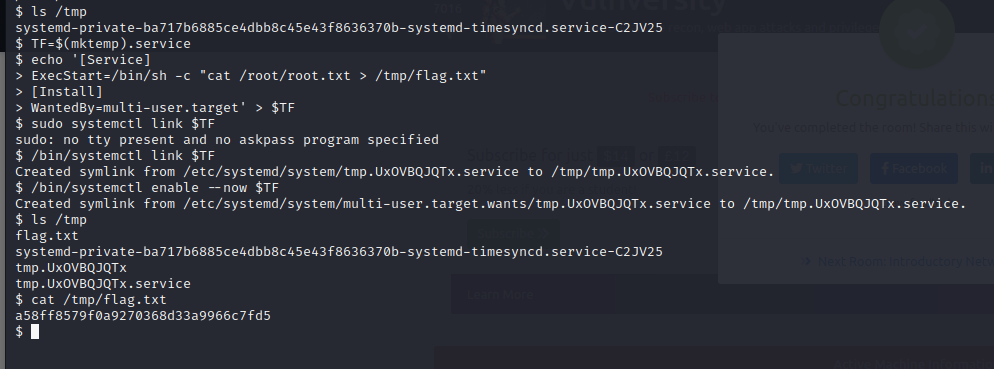
On the system, search for all SUID files. Which file stands out? /bin/systemctl



It's challenge time! We have guided you through this far. Can you exploit this system further to escalate your privileges and get the final answer?







Become root and get the last flag (/root/root.txt) :a58ff8579f0a9270368d33a9966c7fd5