Task 1 Deploy the Vulnerable Debian VM

This room is aimed at walking you through a variety of Linux Privilege Escalation techniques. To do this, you must first deploy an intentionally vulnerable Debian VM. This VM was created by Sagi Shahar as part of his local privilege escalation workshop but has been updated by Tib3rius as part of his Linux Privilege Escalation for OSCP and Beyond! course on Udemy. Full explanations of the various techniques used in this room are available there, along with demos and tips for finding privilege escalations in Linux.

Make sure you are connected to the TryHackMe VPN or using the in-browser Kali instance before trying to access the Debian VM!

SSH should be available on port 22. You can login to the "user" account using the following command:

ssh user@MACHINE\_IP

If you see the following message: "Are you sure you want to continue connecting (yes/no)?" type yes and press Enter.

The password for the "user" account is "password321".

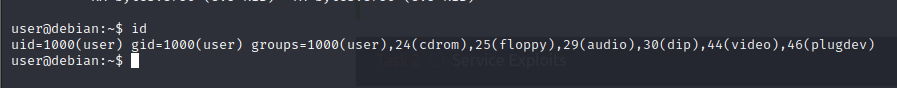
Note: If you get an error saying Unable to negotiate with <IP> port 22: no matching how to key type found. Their offer: ssh-rsa, ssh-dss this is because OpenSSH have deprecated ssh-rsa. Add -oHostKeyAlgorithms=+ssh-rsa to your command to connect.

The next tasks will walk you through different privilege escalation techniques. After each technique, you should have a root shell. Remember to exit out of the shell and/or re-establish a session as the "user" account before starting the next task!

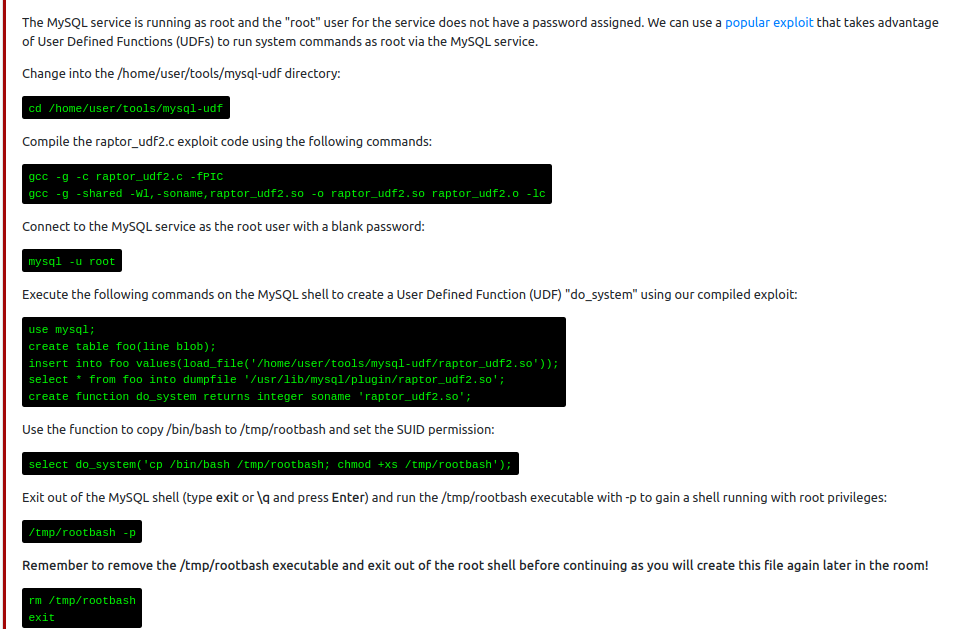
Deploy the machine and login to the "user" account using SSH.

ssh user@10.10.212.184 -oHostKeyAlgorithms=+ssh-rsa

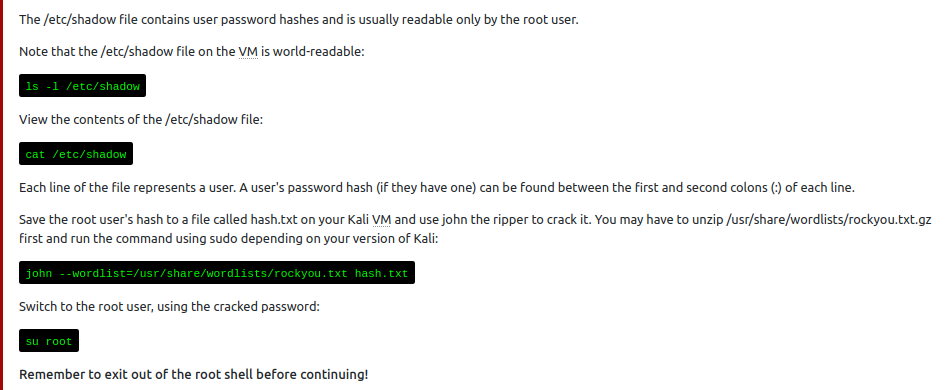
Run the "id" command. What is the result?



Task 2 Service Exploits



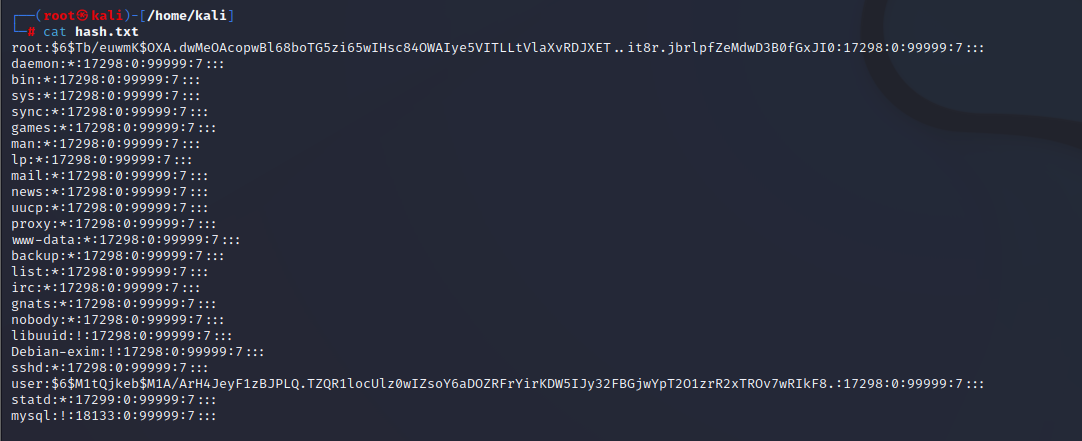
Task 3 Weak File Permissions - Readable /etc/shadow

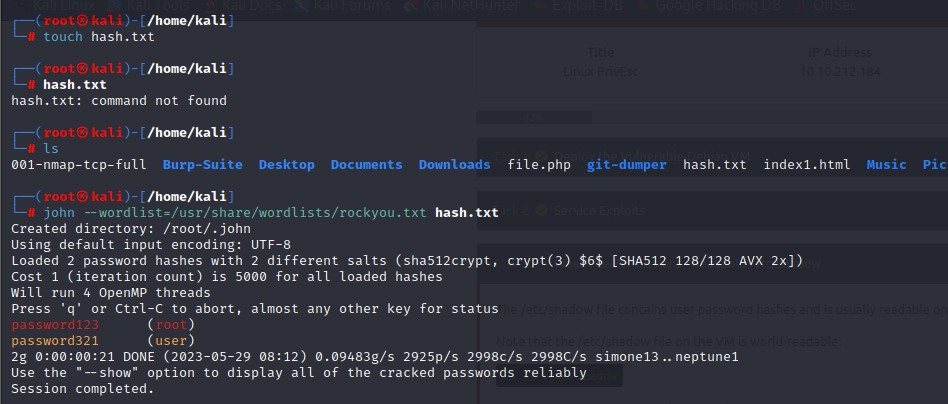


Answer the questions below

What is the root user's password hash?

6$Tb/euwmK$OXA.dwMeOAcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0





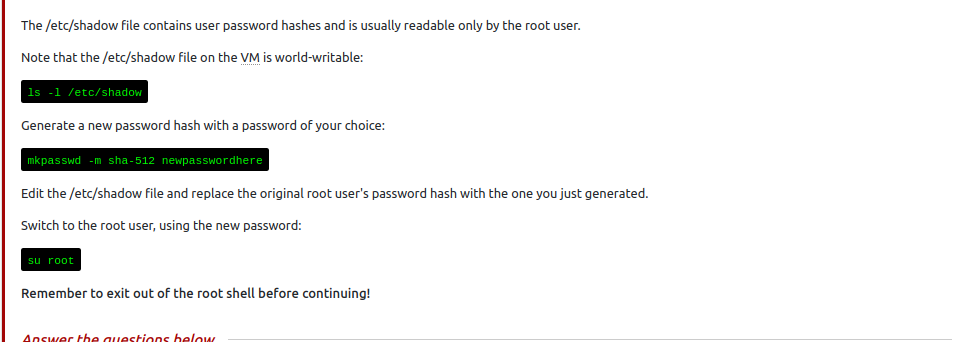
What hashing algorithm was used to produce the root user's password hash?

sha512crypt

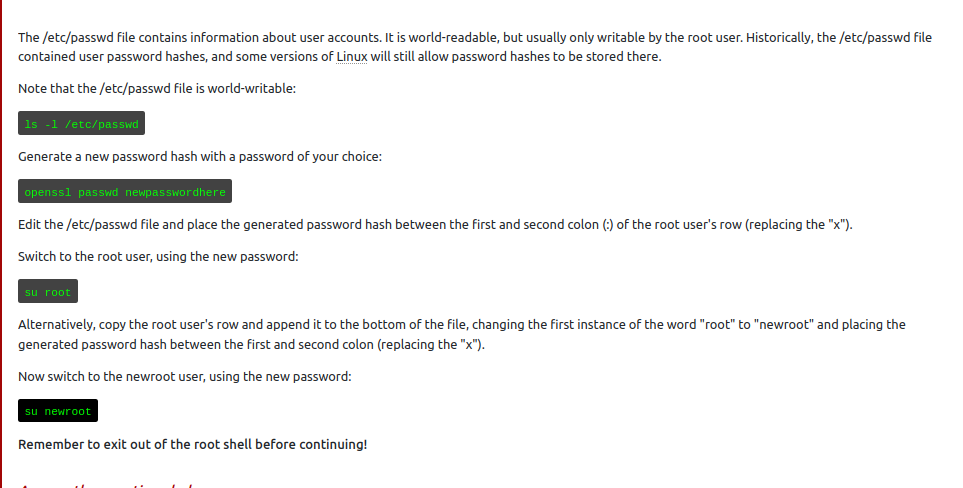
What is the root user's password?

password123

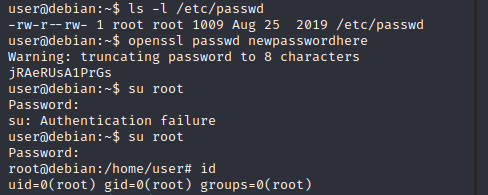
Task 4 Weak File Permissions - Writable /etc/shadow

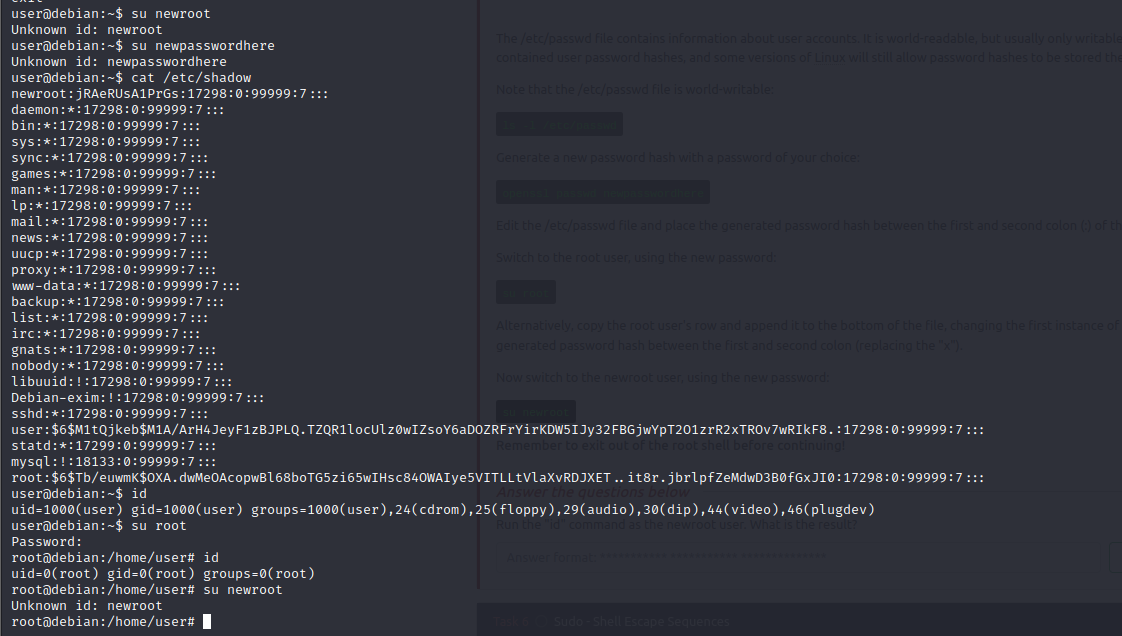


Task 5 Weak File Permissions - Writable /etc/passwd



Run the "id" command as the newroot user. What is the result?





Task 6  Sudo - Shell Escape Sequences

List the programs which sudo allows your user to run:

sudo -l

Visit GTFOBins ([https://gtfobins.github.io](https://gtfobins.github.io/)) and search for some of the program names. If the program is listed with "sudo" as a function, you can use it to elevate privileges, usually via an escape sequence.

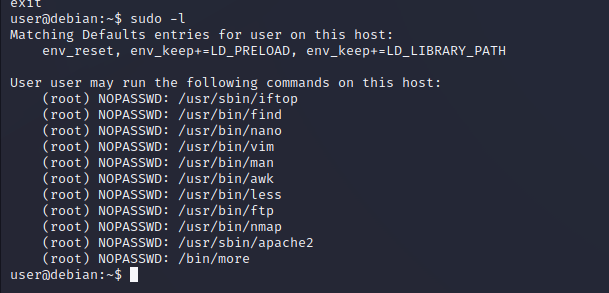
Choose a program from the list and try to gain a root shell, using the instructions from GTFOBins.

For an extra challenge, try to gain a root shell using all the programs on the list!

**Remember to exit out of the root shell before continuing!**

***Answer the questions below***

How many programs is "user" allowed to run via sudo?



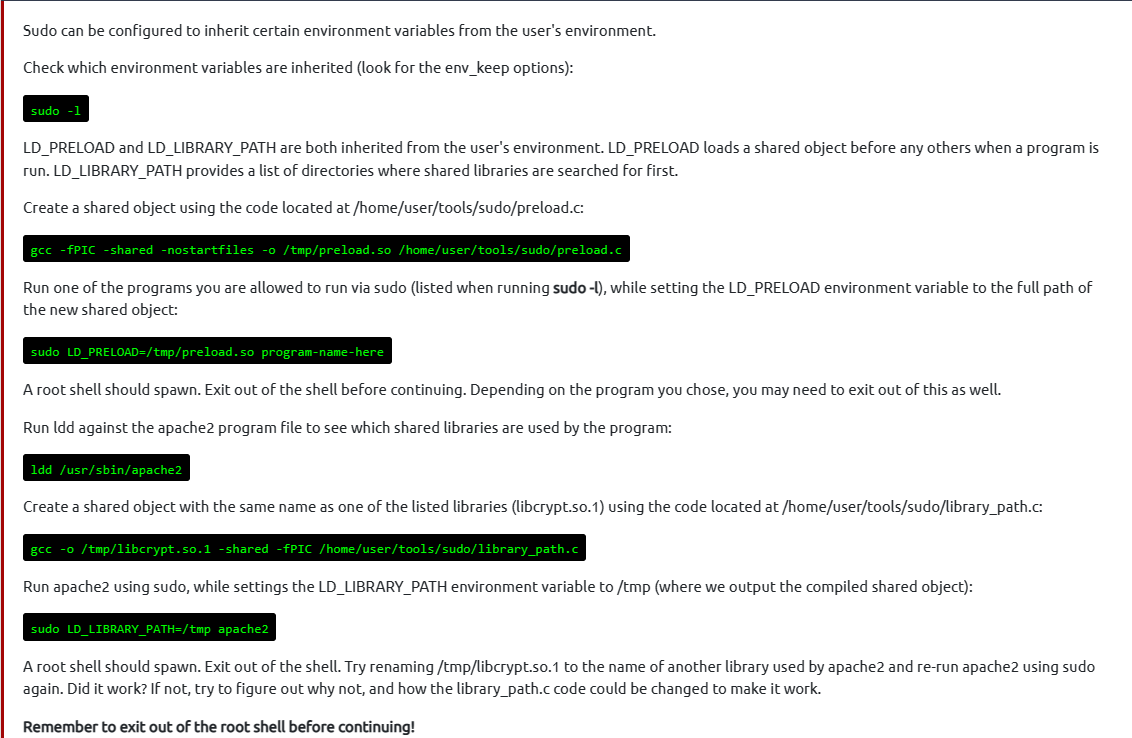
* 11

One program on the list doesn't have a shell escape sequence on GTFOBins. Which is it?

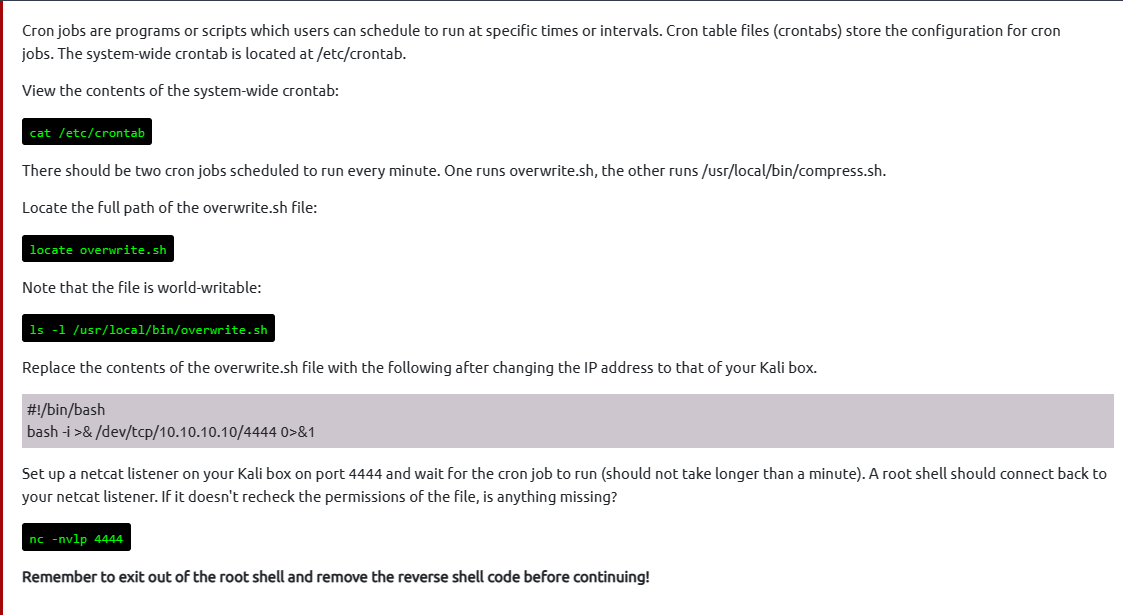
Apache2

Consider how you might use this program with sudo to gain root privileges without a shell escape sequence.

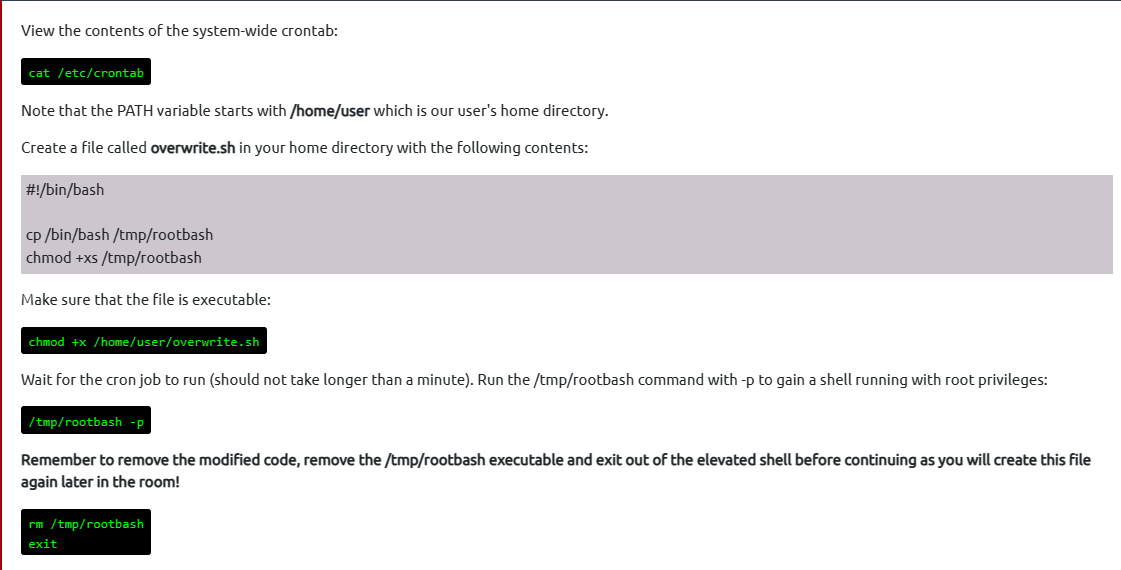
Task 7  Sudo - Environment Variables



Task 8  Cron Jobs - File Permissions



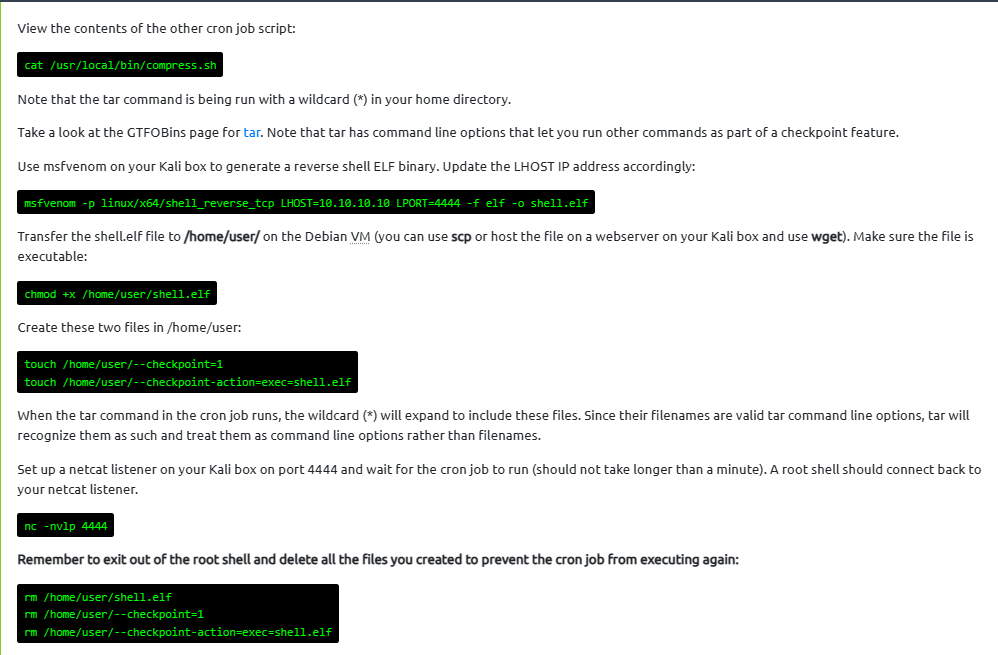
Task 9  Cron Jobs - PATH Environment Variable



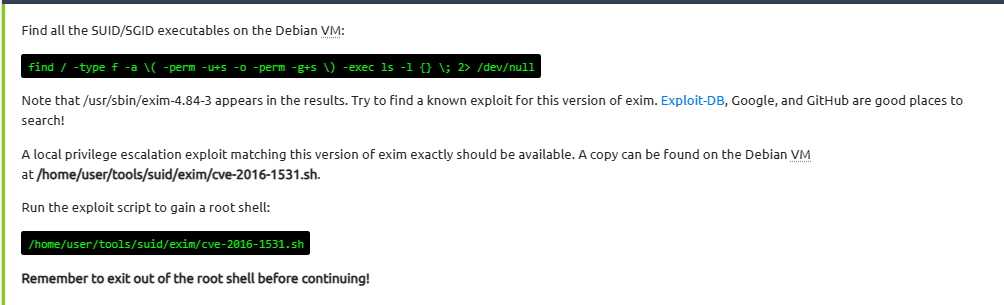
What is the value of the PATH variable in /etc/crontab?

/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

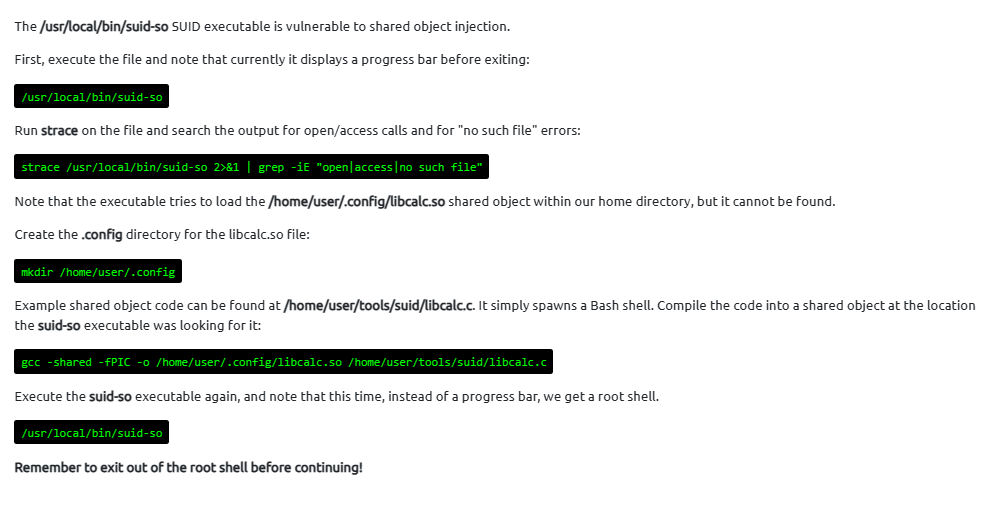
Task 10 Cron Jobs – Wildcards



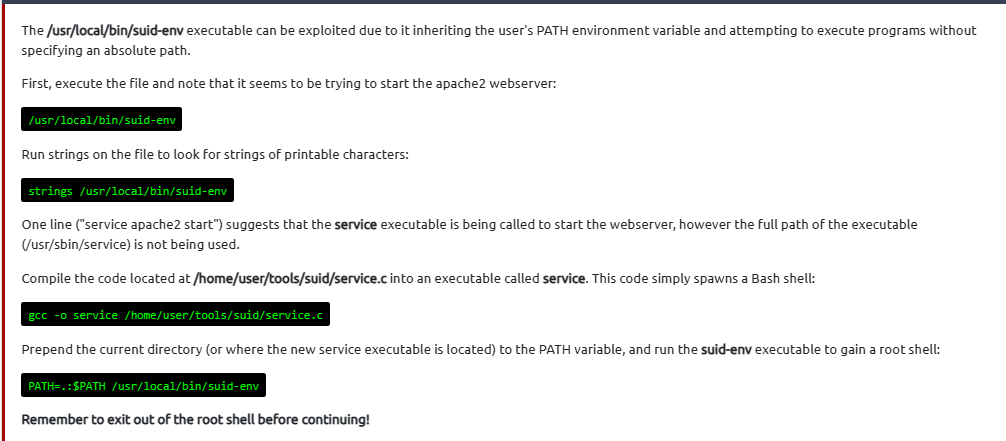
Task 11  SUID / SGID Executables - Known Exploits



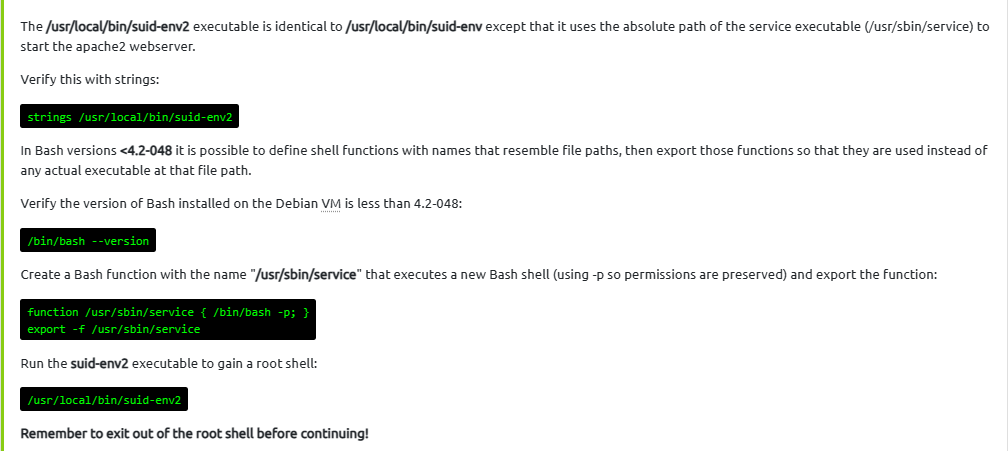
Task 12  SUID / SGID Executables - Shared Object Injection



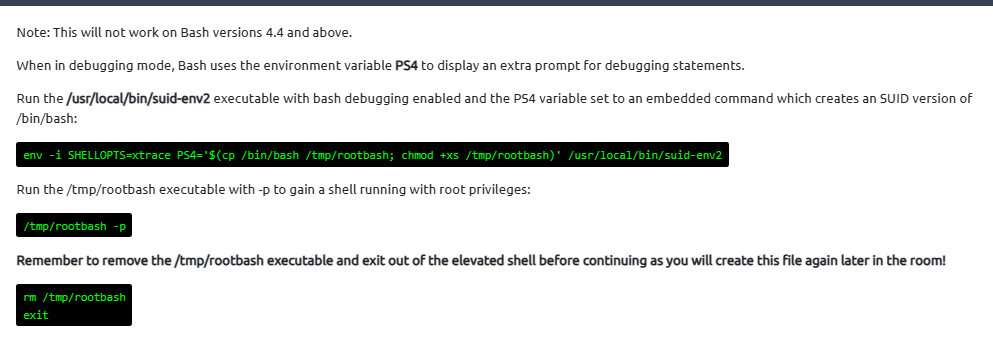
Task 13  SUID / SGID Executables - Environment Variables

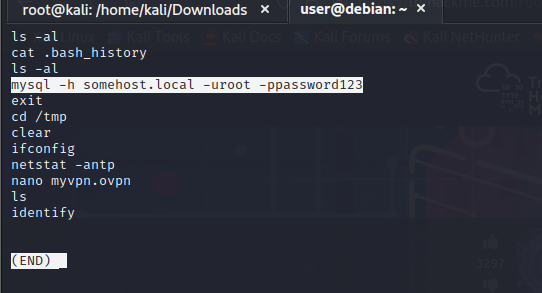


Task 14  SUID / SGID Executables - Abusing Shell Features (#1)



Task 15  SUID / SGID Executables - Abusing Shell Features (#2)

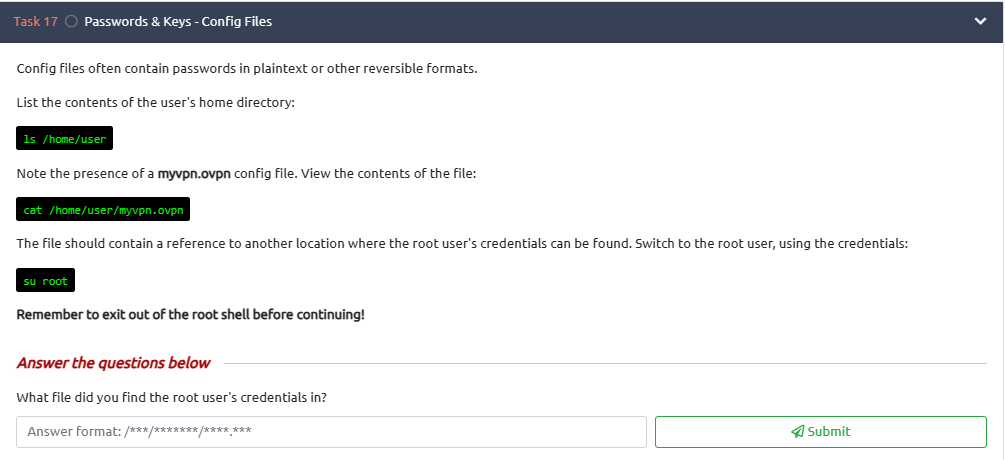




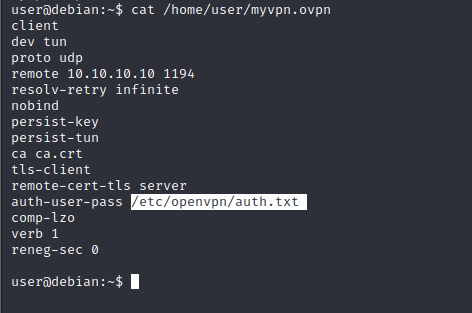
What is the full mysql command the user executed?

mysql -h somehost.local -uroot -ppassword123

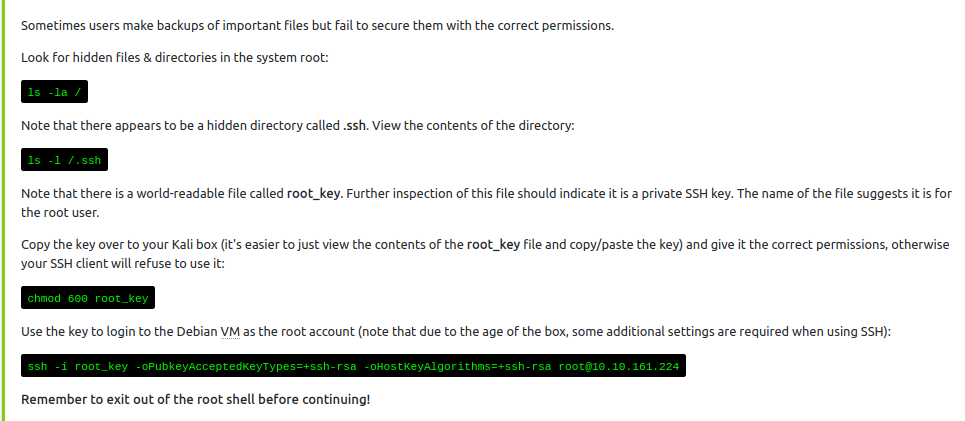
Task 17  Passwords & Keys - Config Files



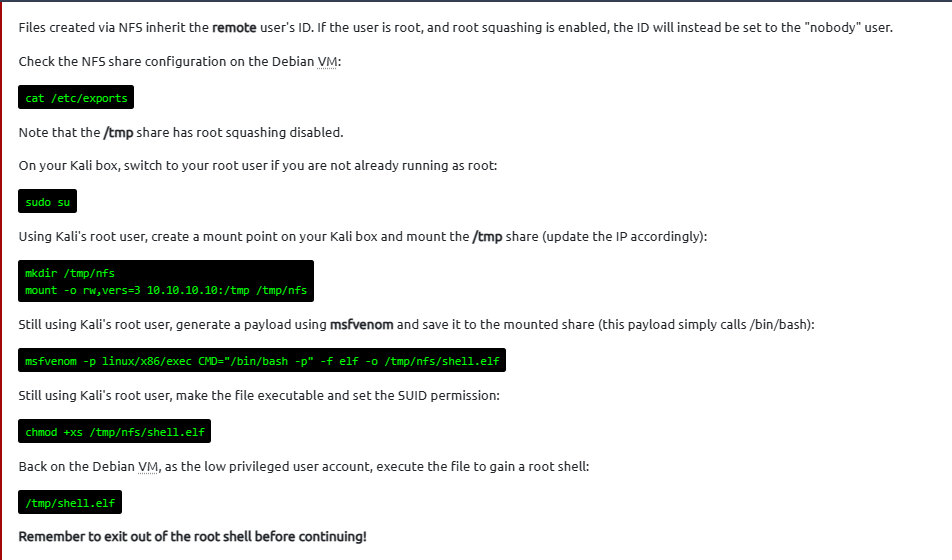
/etc/openvpn/auth.txt



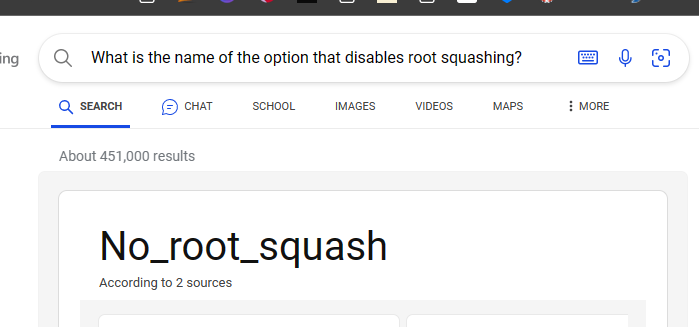
Task 18 Passwords & Keys - SSH Keys



Task 19  NFS



What is the name of the option that disables root squashing?



Task 20  Kernel Exploits

