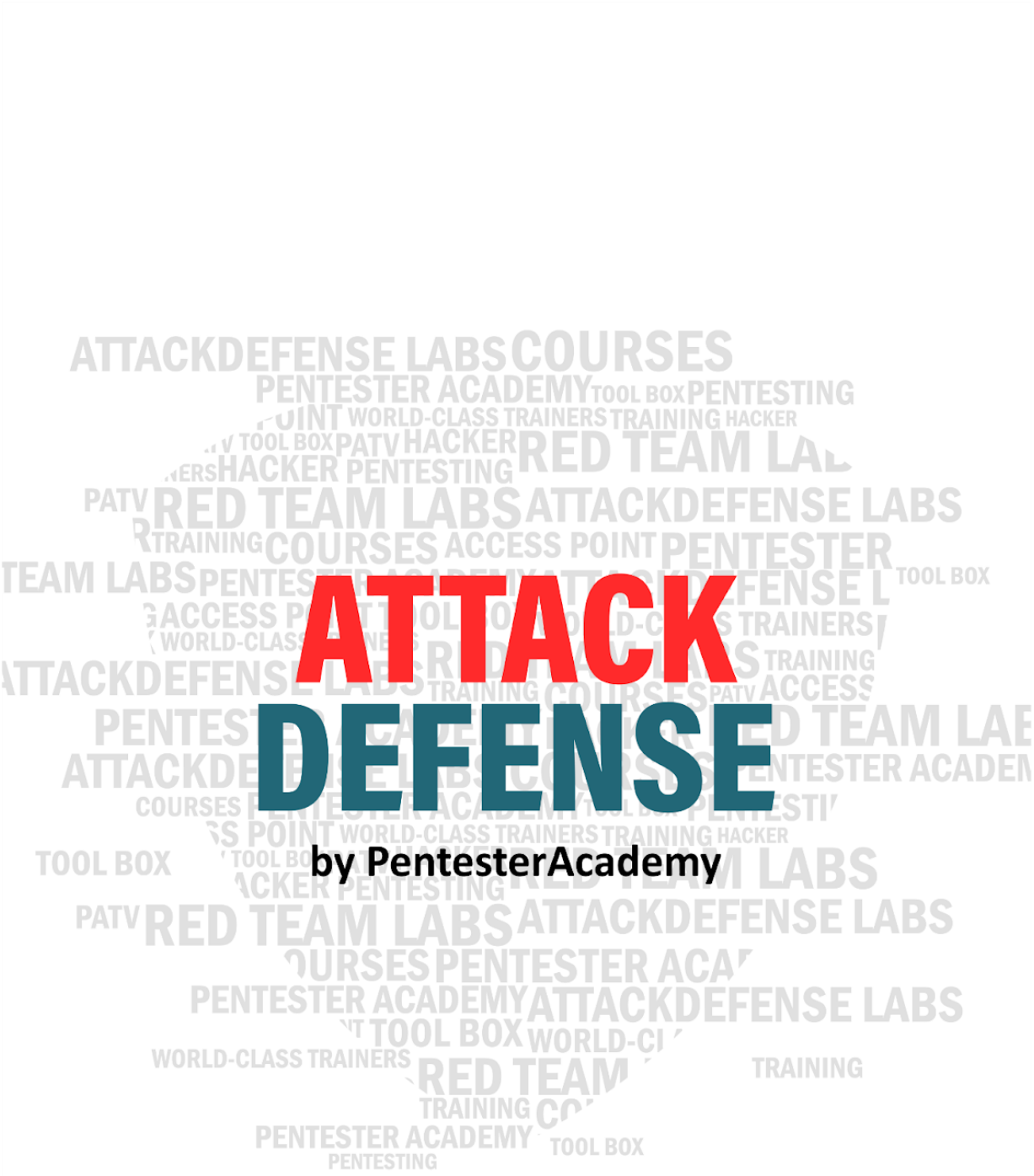
ATTACK
DEFENSE
by PentesterAcademy

Name	Switching Users
URL	https://attackdefense.com/challengedetails?cid=1807
Type	Beginner Skills : Linux For Pentesters

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: Learn about switching users by doing the following activities and answering questions

1. How many non-system/daemon users are present on the machine?
2. What is the default shell for the student user?
3. Which user is a member of the sudoers group?
4. Does the user teacher have any sudo capabilities?
5. Use sudo command to start SSH service from the student user.
6. Switch to root user.
7. As root user, add a new user “john” and add john to sudo group.
8. As root user, add a new user “lara” and add entry in sudoers file to allow lara start SSH service without being prompted for password.
9. As root user, launch a bash shell as user john (using su command).
10. As root user, delete user “john”.

Theoretical Explanation:

Su stands for substitute user. The su command is used to switch the user. It also allows the user to run a command as another user.

Examples:
su root // Switch to root user
su -c

Sudo command allows the user to run a command as any user, with the default generally being the root.

Examples:
sudo vim /etc/shadow // Running vim command as root

The difference between both is the duration or objective. If the task is short then sudo can be used and if the task is long which requires multiple commands to be fired, su can be used to switch the user first.

Solution:

Q 1. How many non-system/daemon users are present on the machine (including root)?

Check /etc/passwd file

Command: cat /etc/passwd

```
student@attackdefense:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:106::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
student:x:999:999:student:/home/student:/bin/sh
teacher:x:998:997:teacher:/home/teacher:/bin/sh
student@attackdefense:~$
```

There are three non-system/daemon users i.e. student, teacher and root.

Answer: 3

Q 2. What is the default shell for the student user?

From /etc/passwd, one can observe that the sh shell (bourne shell) is the default shell of the student user.

Answer: Bourne shell

Q 3. Which user is a member of the sudoers group?

Check the /etc/group file and look for sudo group entry

Command: cat /etc/group | grep sudo

```
student@attackdefense:~$
student@attackdefense:~$ cat /etc/group | grep sudo
sudo:x:27:student
student@attackdefense:~$
```

The user student is a member of sudo group.

Answer: student

Q 4. Does the user teacher have any sudo capabilities?

User teacher is not in the sudo group. However, the sudo related capabilities can also be defined in the sudoers file. Check that file.

Command: sudo cat /etc/sudoers

```
student@attackdefense:~$ sudo cat /etc/sudoers
[sudo] password for student:
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
```

The password for student user is “student”

```
# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
teacher ALL=NOPASSWD: /etc/init.d/cron
student@attackdefense:~$
```

User teacher can start/stop cron service.

However, on taking a deeper look at it, one can observe that the members of “admin” group can also use sudo.

```
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

On checking the /etc/group file, it can be observed that the “teacher” is member of the “admin” group.

Command: cat /etc/group | grep teacher

```
student@attackdefense:~$ cat /etc/group | grep teacher
admin:x:998:teacher
teacher:x:997:
student@attackdefense:~$
```

Hence, the user “teacher” can use “sudo” for other work too.

Q 5. Use sudo command to start SSH service from the student user.

Start SSH service

Command: sudo /etc/init.d/ssh start

```
student@attackdefense:~$ sudo /etc/init.d/ssh start
 * Starting OpenBSD Secure Shell server sshd
student@attackdefense:~$
```

Q 6. Switch to root user.

Use su command to switch to root

Command: sudo su

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

Alternative command: sudo su root

Q 7. As root user, add a new user “john” and add john to sudo group.

Add a new user john

Command: adduser john

```
root@attackdefense:/home/student# adduser john
Adding user `john' ...
Adding new group `john' (1000) ...
Adding new user `john' (1000) with group `john' ...
Creating home directory `/home/john' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for john
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@attackdefense:/home/student#
```

Add the user to sudo group

Command: usermod -a -G sudo john

```
root@attackdefense:/home/student# usermod -a -G sudo john
root@attackdefense:/home/student#
```

Verify that the user john is now a member of sudo group

Command: cat /etc/group | grep sudo

```
root@attackdefense:/home/student# cat /etc/group | grep sudo
sudo:x:27:student,john
root@attackdefense:/home/student#
```

The user john is added to the machine and is a part of sudo group.

Q 8. As root user, add a new user “lara” and add entry in sudoers file to allow lara start SSH service without being prompted for password.

Add a new user lara

Command: adduser lara

```
root@attackdefense:/home/student# adduser lara
Adding user `lara' ...
Adding new group `lara' (1001) ...
Adding new user `lara' (1001) with group `lara' ...
Creating home directory `/home/lara' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for lara
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
root@attackdefense:/home/student#
```

Open /etc/sudoers file for modification.

Command: vim /etc/sudoers

Add the following line

lara ALL=NOPASSWD: /etc/init.d/ssh

```
 24
 25 # Allow members of group sudo to execute any command
 26 %sudo   ALL=(ALL:ALL) ALL
 27
 28 # See sudoers(5) for more information on "#include" directives:
 29
 30 #includedir /etc/sudoers.d
 31 teacher ALL=NOPASSWD: /etc/init.d/cron
 32 lara ALL=NOPASSWD: /etc/init.d/ssh
"/etc/sudoers" [Modified][readonly] 32 lines --100%--
```

The user lara can now start/stop SSH service without have to provide the password.

Q 9. As root user, launch a bash shell as user john (using su command).

Launch a bash shell as user john

Command: su -c bash - john

```
root@attackdefense:/home/student# su -c bash - john
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

john@attackdefense:~$
john@attackdefense:~$
```

Q 10. As root user, delete user “john”.

Delete the user john.

Command: userdel -r john

```
root@attackdefense:/home/student# userdel  -r john
userdel: john mail spool (/var/mail/john) not found
root@attackdefense:/home/student#
```

Verify the deletion by trying to run a bash command as user john.

Command: su -c bash - john

```
root@attackdefense:/home/student# su -c bash - john
su: user john does not exist
root@attackdefense:/home/student#
root@attackdefense:/home/student#
```