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.

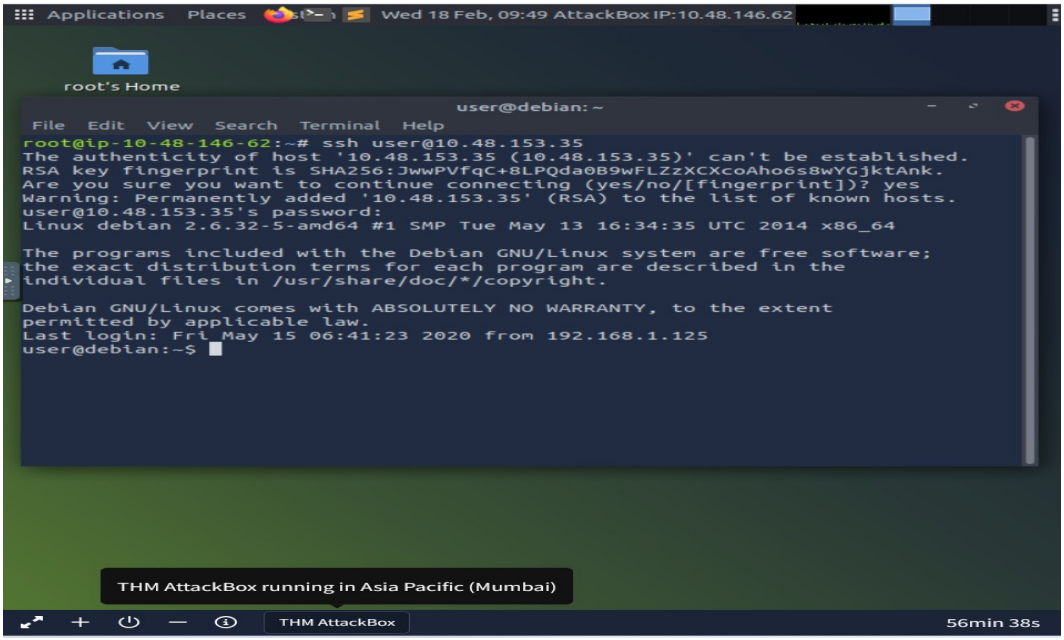
Mitigation:

Remove NOPASSWD from powerful binaries.

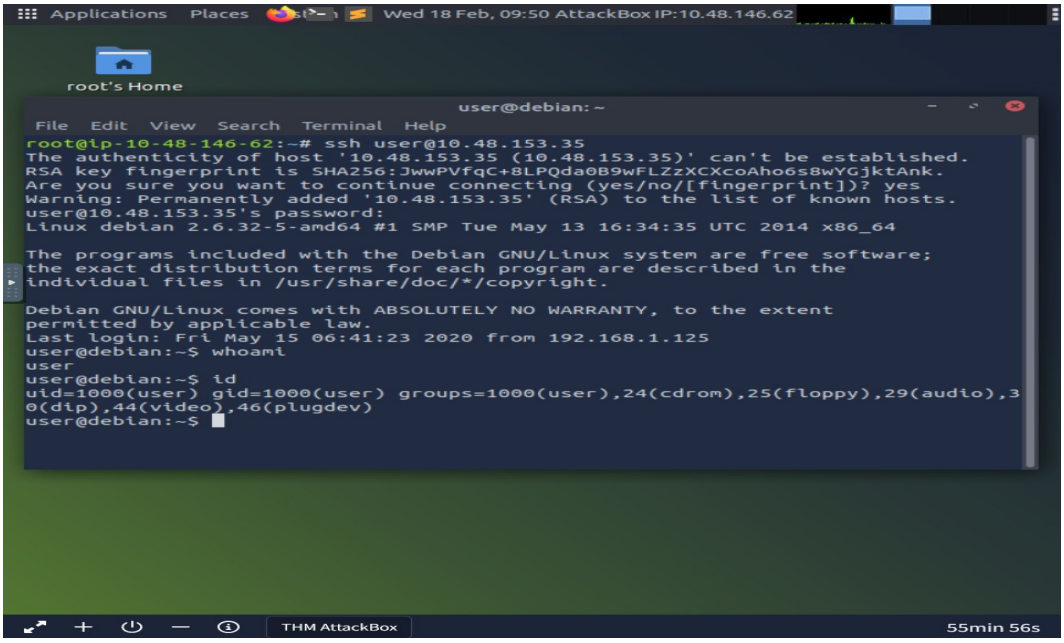
Restrict sudo commands carefully.

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

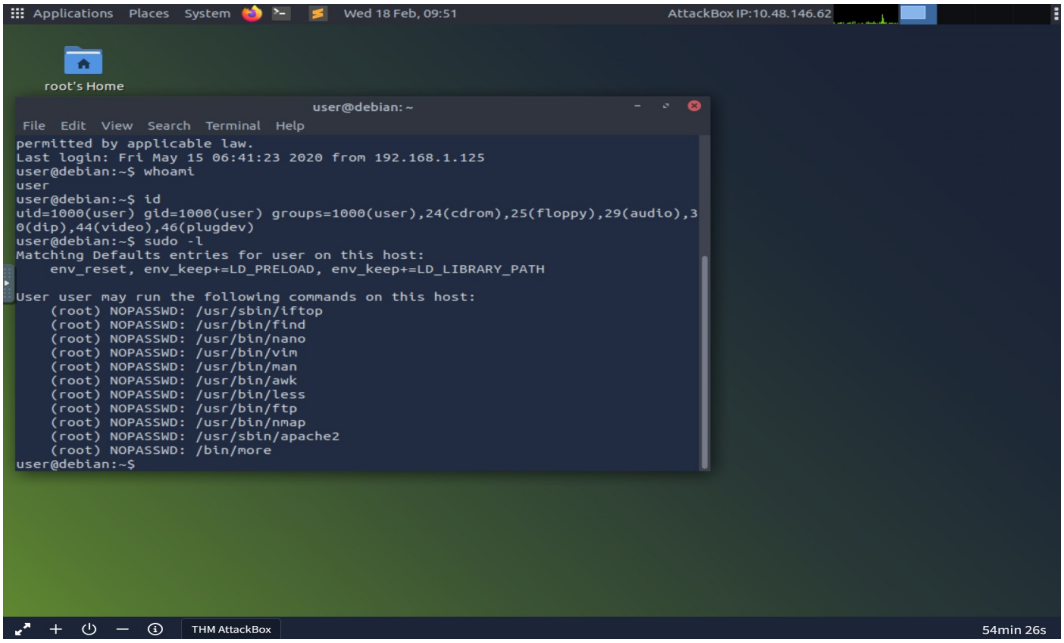
Screenshots and Evidence



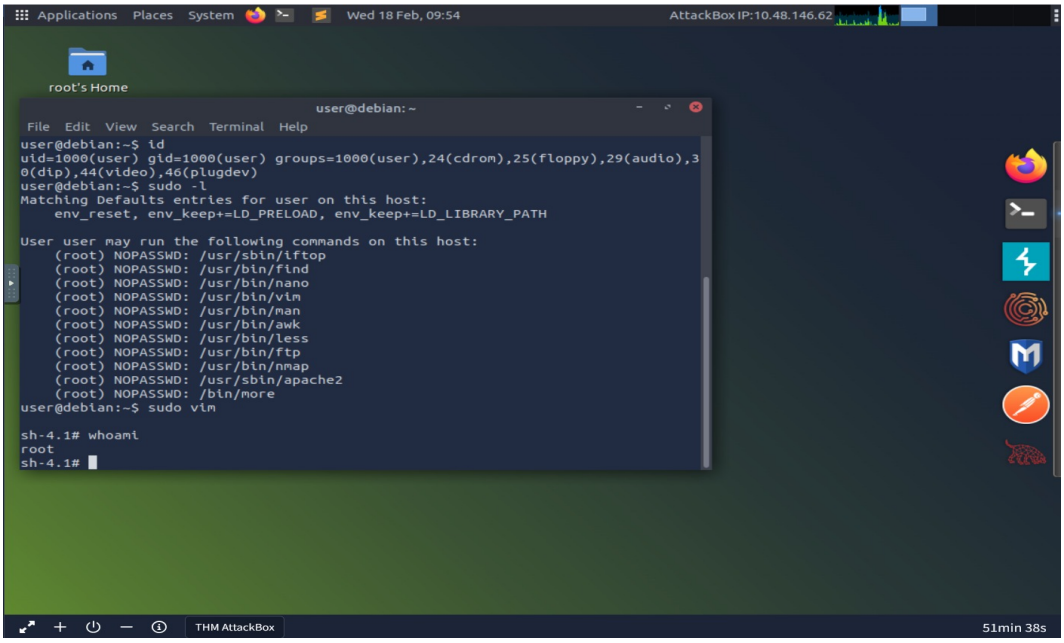
SSH login as user showing initial access.



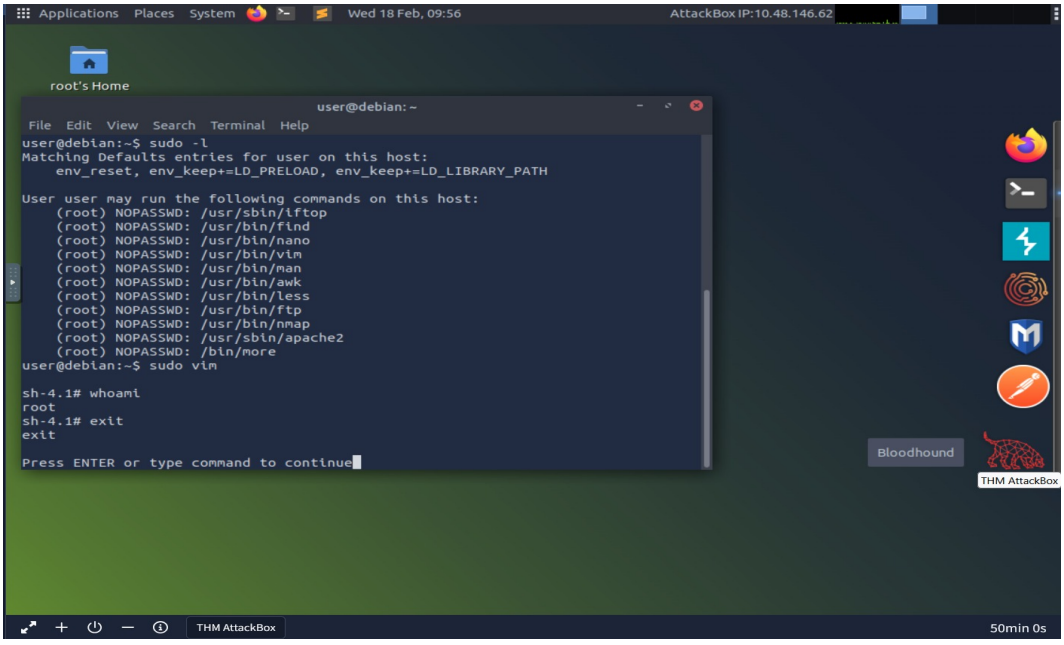
'whoami' and 'id' confirming normal user privileges.



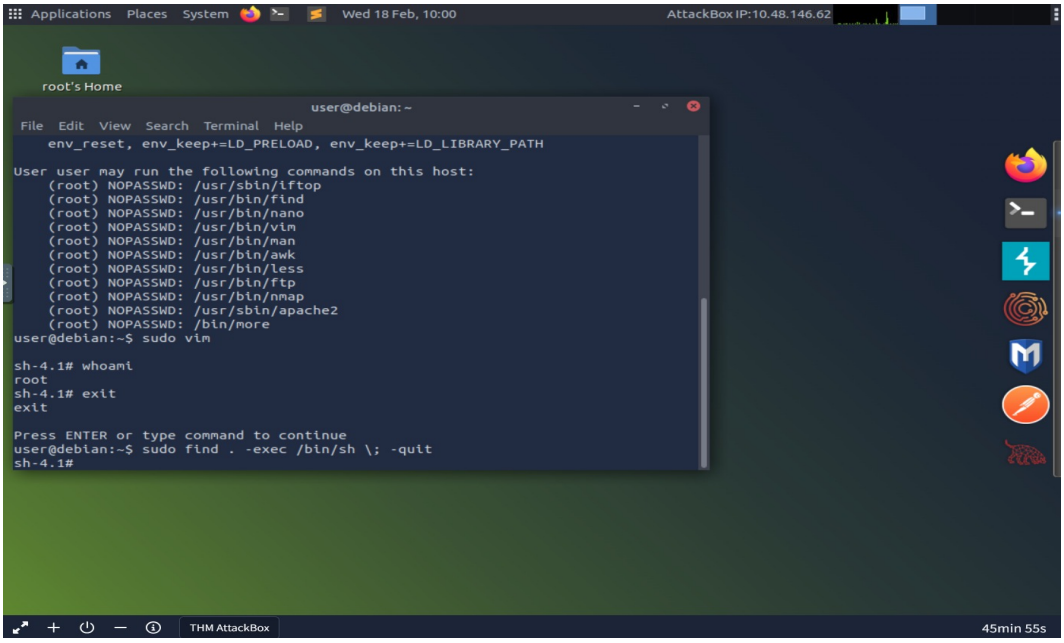
'sudo -l' output listing allowed root commands.



Running 'sudo vim' which starts vim as root.



'whoami' showing root after shell escape.



Root shell obtained using 'sudo find'.