Sudo and Sudoers

Give User Sudo Privileges

On Debian, the sudo group has full admin privileges. We can grant a user these same privileges by adding them to the sudo group like this:

```
 sudo usermod -aG sudo username
```

Modify the Sudoers File

Use visudo to edit the /etc/sudoers file.

```
# visudo

Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

root    ALL=(ALL:ALL) ALL

%admin ALL=(ALL) ALL
%sudo   ALL=(ALL:ALL) ALL

#includedir /etc/sudoers.d
```

Let’s take a look at what these lines do.

Default Lines

The first line, Defaults env_reset, resets the terminal environment to remove any user variables. This is a safety measure used to clear potentially harmful environmental variables from the sudo session.

The second line, Defaults mail_badpass, tells the system to mail notices of bad sudo password attempts to the configured mailto user. By default, this is the root account.

The third line, which begins with Defaults secure_path=…, specifies the PATH (the places in the filesystem the operating system will look for applications) that will be used for sudo operations. This prevents using user paths which may be harmful. User Privilege Lines

User Privilige Lines

The fourth line, which dictates the root user’s sudo privileges, is different from the preceding lines. Let’s take a look at what the different fields mean:

```
  root ALL=(ALL:ALL) ALL The first field indicates the username that the
rule will apply to (root).
  root ALL=(ALL:ALL) ALL The first “ALL” indicates that this rule applies to
all hosts.
  root ALL=(ALL:ALL) ALL This “ALL” indicates that the root user can run
commands as all users.
  root ALL=(ALL:ALL) ALL This “ALL” indicates that the root user can run
commands as all groups.
  root ALL=(ALL:ALL) ALL The last “ALL” indicates these rules apply to all
commands.
```

This means that our root user can run any command using sudo, as long as they provide their password.

Group Privilege Lines

The next two lines are similar to the user privilege lines, but they specify sudo rules for groups. Names beginning with a % indicate group names.

Here, we see the admin group can execute any command as any user on any host. Similarly, the sudo group has the same privileges, but can execute as any group as well. Included /etc/sudoers.d Line

The last line might look like a comment at first glance:

```
/etc/sudoers

. . .

#includedir /etc/sudoers.d
```

It does begin with a #, which usually indicates a comment. However, this line actually indicates that files within the /etc/sudoers.d directory will be sourced and applied as well. Files within that directory follow the same rules as the /etc/sudoers file itself. Any file that does not end in ~ and that does not have a . in it will be read and appended to the sudo configuration.

Sudo customizations

It is good practice to create seperate files for in /etc/sudoers.d for system/user specific customizations. E.g. example below illustrates the way to allow user a user to mount without root passwordt being asked.

```
# visudo /etc/sudoers.d/allowmount
```

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
oscar ALL=(ALL)   NOPASSWD: /bin/mount, /bin/umount
```

From:
https://wiki.oscardegroot.nl/ - **HomeWiki**

Permanent link:
https://wiki.oscardegroot.nl/doku.php?id=linux:system:sudoers

Last update: **2023/08/05 08:42**