Sudoer Specification

Introduction and/or Background

By default the su command can be used to promote a normal user account to root priviliges. In a production environment that is far from ideal. In such situations the administrator turns off su and provides sudo as the replacement.

Sudo (su "do") allows a system administrator to delegate authority to give certain users (or groups of users) the ability to run some (or all) commands as root or another user while providing an audit trail of the commands and their arguments.

what is unique about sudo is that you must use a specific editor, visudo, to make changes to the sudoers file. The sudoers file contains the accounts that are permitted to use the sudo command and what their limits are. Typical example:

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

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

If you launch visudo for the first time, it will ask which editor you wish to use. I suggest nano since you should already be familiar with it.

Note that two groups, %admin and %sudo, are permitted to have all priviliges of root user by default. Want to have a user with different priviliges? Easiest way is to create a new group, add the user to it, modify the sudoers file to only those privileges and save the file. But caution! If an account appears in both the admin group and the new group nothing has been accomplished. The admin group has full rights that supercede the new group you added to that user account!

Now there are two objects that come into play using sudo. There is the sudoer file itself (/etc/sudoer). There is also the directory sudoers.d. For this lab we will only be concerned with the sudoer file.

For those that desire the deep dive, here is the website.

Objectives

In this project/lab the student will:

- Gain familiarity with the sudo package

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Power on the Debian VM (if it isn't already).

Open a Terminal window.

Switch to the root user.

Check and if necessary install the sudo package.

```
apt install sudo
```

Create a new account and assign it a password.

```
useradd <account>
su or sudo <account>
passwd <account> provide <password>
exit
```

Create the test group.

```
groupadd test
```

Edit the /etc/sudoers file.

```
visudo
```

Allow sudo access to the users in the test group. Add the following line to the file.

8 %test ALL=(ALL) ALL

Save the file and exit. Make the new account a member of the test group.

9 usermod –aG test <account>

Switch to the new account.

10 su <account> or
11 sudo <account>

Confirm the presence of the user account in the test group.

12 grep ‘test’ /etc/group

Take a screen shot of the terminal screen. Add that to your document.

13 Enter the whoami command to verify root access.

14 Take a screenshot showing both the new account’s group memberships and root access verification.

Reflection

1 What are the benefits in granting root access using this method?
2 How could this approach help harden a server’s security?

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing new account's group memberships and root access verification (60 points)	
	Criteria #2: Show presence of user in test group (10 points)	
	Criteria #3: Show access to root privileges. (10 points)	
	Criteria #4: Answer to reflection question 1 (10 points)	
	Criteria #5: Answer to reflection question 1 (10 points)	