LINUX FOUNDATION

TRAINING

Accessing the Root Account

A Linux Foundation Training Publication
www.training.linuxfoundation.org

Overview

One element of the Linux security model which is inherited from Unix operating system is the distinction between privileged and unprivileged (or regular) users. By default, a regular user is not permitted to run all commands or access all files in the filesystem. There are some files that regular users cannot even view. Regular users are allowed access and to run commands that change their own files, but cannot make changes to files and directories owned by other users, unless they belong to the group owner and such access has been granted to it.

While all users can be granted permissions on an as needed basis, all Linux installations include a privileged “Super User” user called the root user. The root user can run any command, including destructive ones,, and access and modify any file in the filesystem.

Given the potentially destructive ability of the root user, it is considered bad practice to use the root account for day to day tasks and activities, intentionally reserving it for potentially disruptive administrative changes. Instead, administrators are encouraged to log in to the system as regular users, changing the ownership of their session to the root user to perform administrative tasks, and then reverting to their regular user. Instead, it uses the sudo utility to grant regular users administrative privileges. To run a command with superuser privileges, preface it with the word sudo. For example:

sudo apt-get install htop

Ubuntu does not allow access to the root account directly; it is not possible to log in as the root user or become the root user.

Key Ideas

root account: A special user account with unrestricted access to all files and commands on the system. Login is root, password is set during system installation. Otherwise known as the Super User.

regular user: Any user account created for a person to use a system. Can access and perform commands on their own files (i.e. those in their own home directory).

su: The su command is used to substitute the owner of the current session (i.e. the logged in user) for another user. Given without any user name, the root user is assumed. A regular user can only switch to another user if the password for such user is known.

Example Scenario

Mounting filesystems at boot time requires changes to the /etc/fstab file. Files within the /etc directory can only be changed by a user with Super User privileges, like the root user.

Now Do It

1. Log into the system as a regular user.
2. Try and add a line the /etc/fstab file as a regular user.
3. Try and create a file in the /mnt directory.
4. Use the su command to become the root user.
5. Try and add a line to the /etc/fstab file as the root user.
6. Try and create a file in the /mnt directory
7. Substitute back to your regular user.

If you remember nothing else...

It is considered bad practice to log in and operate as the root user. You can become the root user temporarily using the su command; make sure to return to your regular user when you have completed the action that required enhanced privileges.

Answer Key

1.Using ssh to access practice virtual machine:
$ ssh USER@MACHINE
USER@MACHINE"s password:
Last login: Sun Apr 26 12:34:10 2015

2. Echo a line into /etc/fstab:
$ echo "# hey dude" >> /etc/fstab
bash: /etc/fstab: Permission denied

3. Touch /mnt/test
$ touch /mnt/test
touch: cannot touch '/mnt/test': Permission denied

4. Become root:
$ su root
Password:
#

5. Echo a line into /etc/fstab, no output on successful execution.
echo "# hey dude" >> /etc/fstab

6. Touch /mnt/test, no output on successful execution.
touch /mnt/test

7. Substitute back to your regular user:
exit
exit
$

LINUX FOUNDATION

Get Certified!

Get more information at http://training.linuxfoundation.org/certification/lfcs