CCDC Notes

**Linux Permissions and Attributes**

Linux files and folders (directories) have permission settings and attribute settings.

The following command will view Linux permission settings

ls -l

The following command will view Linux attribute settings

lsattr

The “man lsattr” will explain all the possible options for Linux attributes

The following command will change Linux permissions

chmod

The following command will change Linux attributes

chattr +i file.txt

Note: The previous command makes the “file.txt” immutable. The file cannot be changed until the “immuntable” setting is removed.

The following command will change Linux attributes

chattr -i file.txt

Note: The previous command removes the immutable setting from “file.txt”. If the login has permission, the file may be changed.

**Message of the Day**

The contents of this file is displayed by the login command. Edit the following file with the content you desire for every login.

“/etc/motd”

**Sudo definitions**

The file controlling the behavior of sudo is “/etc/sudoers”

Items to note in the file “/etc/sudoers”

## User privilege specifications

root ALL=(ALL) ALL

preuss ALL=(ALL) All

Note: Both root and preuss are able to run any command. Changing this to just root would be good.

## Uncomment to allow members of group wheel to execute any command

# %wheel ALL=(ALL) ALL

Note: wheel is the traditional group. Another group may be listed.

## Same thing without a password

# %wheel ALL=(ALL) NOPASSWD: ALL

Note: This allows all members of “wheel” to execute any command without a password.

## Uncomment to allow members of group sudo to execute any command

# %sudo ALL=(ALL) ALL

Note: This is just like the wheel line earlier.

## Uncomment to allow any user to run sudo if they know the password

## of the user they are running the command as (root by default).

# Defaults targetpw # Ask for the password of the target user

# ALL ALL=(ALL) ALL # WARNING: only use this together with 'Defaults targetpw'

Note: This requires knowledge of the other password.

## Read drop-in files from /etc/sudoers.d

## (the '#' here does not indicate a comment)

#includedir /etc/sudoers.d

Note: This allows the definitions to be in another file. If uncommented, the file in this example would “/etc/sudoers.d”

**Sshd configuration**

The primary configuration file controlling the sshd (server accepting ssh connections) is /etc/ssh/sshd\_config.

#PermitRootLogin prohibit-password

Note: This line should be commented or have a # at the beginning. This means the login root may not use ssh over the network. Another account must be used to login over the network. This is the recommended operation.

**Log File Searches**

Linux is currently in two camps, systemd and not-systemd. The not-systemd is found on older systems.

How to test if the Linux distribution is running systemd or not.

systemctl

Note: This will list all services on the Linux system. If the command fails, the distribution does not use systemd.

This command will list all active and running systemd services

systemctl - -type=service - -state=active

The command to view log files in systemd is journalctl

This command will open the end of the log file and “follow” or update as events happen. This should be opened in a dedicated terminal session

journalctl -ef

Non-systemd log files

/var/log/messages

This log file is generic system activity.

/var/log/auth.log

This is authentication events

/var/log/secure

This is security related including secure authentication

/var/log/boot

This is boot information

dmesg (application)

This is kernel ring messages

/var/log/kern.log

This is kernel information

/var/log/faillog

This is failed login information

/var/log/cron

This is information about cron job that run automatically.

/var/log/mail.log

This mail information messages

/var/log/httpd

This is web server information

/var/log/mysqld or /var/log/mysql.log

This is mysql information

**DNS resolution**

The DNS servers used by Linux is found in

“/etc/resolv.conf”

Cron

The file that defines when cron jobs or programs/scripts will run is

“/etc/crontab”

Some systems may have a folder/directory for programs/scripts to run. Every file in /etc/cron.hourly will run every hour.