

## General Commands

**ls** – This command will display the contents of a directory

**cd** – This command allows you to navigate the filesystem by entering a specified directory

**cd ..** - This command allows you to navigate the filesystem by taking a step back to the parent of the current directory

**pwd** - This command displays the current working directory of the current user

**cat** – Short for concatenate, this command will output the content of a specified file to the display for review

**file** – This command will display the filetype of a specified file

**grep** – This command allows you to filter the output of a file or directory based on a specified pattern

**mkdir** – This command allows you to create a new directory with the name specified

**rm** – This command will remove the specified file

**whoami** – This command will display the username of the user running this command

**man** – This command will display the usage manual for the specified command

**find** – This command allows the user to search through the whole file system to find a specified file

**mv** – This command will move a specified file to a specified location

**cp** - This command will copy a specified file to a specified location

**kill** – This command will end a process by specified Process ID (PID)

**lsb\_release** – This command outputs distribution specific information

**uname** – This command outputs system information

**apt** – This command allows you to interact with system packages (applications)

## Review Running Processes

**ps -ef** – This command will show all current active processes

**top** - show processes w/ CPU/RAM stats

## Tool Reference: Linux Command Line



**lsof -p [pid]** - list open files associated with the specified process – **PID is an acronym for Process ID**

### Review Running Services

**systemctl list-unit-files --type=service** – This command will display all services managed by systemd

**chkconfig -list** - This command will display all services managed by sysvinit

### Review User Accounts

**/etc/passwd** - This file contains information for valid users on the system, such as, username, home directory, user shell and permissions

**w -if** – This command will show you currently logged on user accounts

**last** – This command will display a list of all users that have logged in previously

### Review OS and Application Logs

**/var/log/auth.log** - This file logs all authentication attempts on the system

**history** - This command shows the bash history (command history) of the currently logged in user

**/var/log/apache2** - This is a directory under the /var/log directory, that contains logs that are relevant to Apache Web Server

### Review Scheduled Jobs

**crontab** – This command is used to interact with cron job for individual users

**/etc/crontab** - This file is used to manage system wide cronjobs

### Review Network Information

**ifconfig** – This command shows IP information for the system (Deprecated)

**ip a** – This command shows IP information for the system (Current)

**route** - This command allows you to interact with the system's routing table

## Tool Reference: Linux Command Line



**arp** – This command allows you to interact with the system’s **Address Resolution Protocol (arp)** cache

**/etc/resolv.conf** - This file contains DNS configuration information for the system

**netstat** – This command allows you to interact with networking information on the system

### Remote Management

**ssh** – This command allows a user to establish a secure connection between two assets

**scp** – This command allows a user to securely transfer files between two assets (Deprecated)

**sftp** - This command allows a user to securely transfer files between two assets (Current)