Elk Technologies
https://elktech.org
Scott Stephenson

Chapter 12: Mobile, Linux, and macOS Operating Systems

IT Essentials v7.0

Cisco | Networking Academy®
Mind Wide Open™

Chapter 12 - Sections & Objectives

- 12.1 Mobile Operating Systems
- Explain the purpose and characteristics of mobile operating systems.
  - Compare the Android and iOS operating systems.
  - Describe the features of the Android Touch Interface.
  - Describe the features of the iOS Touch Interface.
  - Describe the features of the Windows Touch Interface.
  - Describe operating system features that are common among mobile devices.

Chapter 12 - Sections & Objectives

- 12.2 Methods for Securing Mobile Devices
- Explain methods for securing mobile devices.
  - Explain how to configure various types of passcode locks.
  - Describe Cloud-enabled services for mobile devices.
  - Describe software security for mobile devices.

Chapter 12 - Sections & Objectives

- 12.3 Linux and Mac Operating Systems
- Explain the purpose and characteristics of Mac and Linux operating systems.
  - Describe tools and features of the Linux and Mac operating systems.
  - Describe Linux and OS X best practices.
  - Define basic CLI commands.

- 12.4 Basic Troubleshooting Process for Other Operating Systems
- Explain how to troubleshoot other operating systems.
  - Explain the six steps of troubleshooting other operating systems.
  - Describe common problems and solutions for other operating systems.

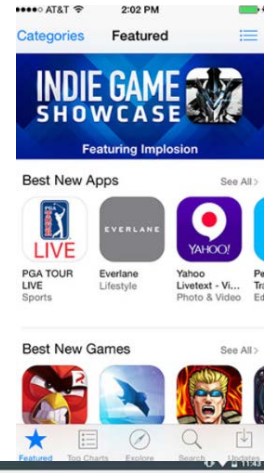
12.1 MOBILE OPERATING SYSTEMS

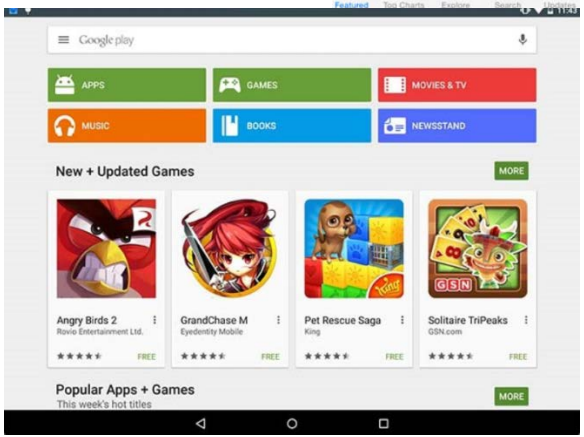
Open Source vs Closed Source

- Like desktops and laptops, mobile devices use an operating system (OS) to run software.
- Before users can analyze and modify software, they must be able to see the source code.
  - When the developer chooses to provide the source code, the software is said to be open source.
  - If the program's source code is not published, the software is said to be closed source.
- Android is developed by Google is open source, and iOS is developed by Apple is closed source.

Applications and Content Sources

- Apps are written and compiled for a specific mobile operating system such as Apple iOS, Android, or Windows.
- Mobile devices come with a number of different apps preinstalled to provide basic functionality.
  - There are apps to make phone calls, send and receive email, listen to music, take pictures, play videos, or video games.
- Instead of being installed from an optical disk, apps are downloaded from a content source.





Applications and Content Sources

- Apps for Apple iOS mobile devices are available for free or purchase from the App Store.
- Apple uses a **walled garden** model for their apps meaning the apps must be submitted to and approved by Apple before they are released to users.
  - This helps prevent the spread of malware and malicious code.
- Android apps are available from both Google Play™ and third-party sites, such as Amazon's App store
- Android apps run in a sandbox and have only the privileges enabled by the user.
- Third-party or custom programs are installed directly using an Android Application Package (apk) file.
  - This gives users the ability to directly install apps without going through the storefront interface and is known as sideloading.

Home Screen Items

- Android Main Home Screen
  - One screen is designated as the home screen.
  - Additional screens are accessed by sliding the home screen to the left or right.
- Navigation icons
  - The Android® OS uses the system **status bar** to navigate apps and screens.
    - The system bar contains the following buttons:
      - Back – return to previous screen
      - Home – go to main screen
      - Recent Apps
      - Menu

- In iOS, the icon for an app represents the app itself. Deleting the icon in iOS deletes the app. In Android, the icon on the Home screen is a shortcut to the app.

Home Screen Items

- Notification and System icons
  - Each Android® device has an area that contains system icons, such as the clock, battery status, and status for Wi-Fi and provider networks.
  - Apps such as email, text messaging, and Facebook® often display status icons to indicate communication activity.
- To open the notification area on Android® devices, swipe down from the top of the screen.
  - You can do the following when notifications are open:
    - Respond to a notification by touching it.
    - Dismiss a notification by swiping it off the screen to either side.
    - Dismiss all notifications with the icon.
    - Toggle often-used settings.
    - Adjust the brightness of the screen.
    - Open the Settings menu with the quick settings icon.

Home Screen Items

- iOS Interface
  - The iOS® interface works in much the same way as the Android® interface, but there are some very important differences:
    - No navigation icons - A physical button may have to be pressed instead of touching navigation icons.
    - No widgets - Only apps and other content can be installed on iOS® device screens.
    - No app shortcuts - The icon for an app represents the app itself. Deleting the icon in iOS deletes the app. In Android, the icon on the Home screen is a shortcut to the app.
- Home button
  - Unlike Android®, iOS® devices do not use navigation icons to perform functions.
  - Some common functions performed by the home button include:
    - Wake the device with **Touch ID** – The hash value of the user fingerprint
    - Return to the home screen.
    - Start Siri® or voice control
- Windows Phone interface apps are called **Tiles**.

Home Screen Items

- iOS Notification Center displays all alerts in one location.
- Commonly used settings
  - iOS® devices allow the user to quickly access common settings and switches, even while locked.
  - From the commonly used settings screen, a user can:
    - Toggle often used settings such as airplane mode, Wi-Fi, Bluetooth, do not disturb and screen rotation lock
    - Adjust screen brightness
    - Control the music player
    - Access **Airdrop** – Used by both macOS and Apple iOS to establish a Wi-Fi direct connection between devices to simplify file transfer
    - Access Flashlight, Clock, Calendar and Camera
- iOS Spotlight
  - Spotlight shows suggestions from many sources including the Internet, iTunes®, App Store, movie show times, and nearby locations.

Screen Orientation

- Screen Orientation
  - Most mobile devices can be used in either portrait or landscape mode.
  - A sensor inside the device known as an accelerometer, detects how it is being held and will change the screen orientation appropriately.
    - When the device is turned to landscape mode, the camera app also turns to landscape mode.
  - Some devices also have gyroscopes to provide more accurate movement readings.
    - Gyroscopes allow a device to be used as a control mechanism for driving games where the device itself acts as a steering wheel.
- Android Screen Auto-Rotation Setting
  - When using an Android device, to enable automatic rotation, go to Settings > Display > Advanced > Auto-rotate screen.
- iOS Screen Auto-Rotation Setting
  - When using an iOS device, to enable automatic rotation, swipe up from the very bottom of the screen and tap the lock icon.

Screen Calibration

- Screen Calibration
  - When bright sunlight makes the screen difficult to read, increase the brightness level.
  - Inversely, very low brightness is helpful when reading a book on a mobile device at night.
  - Some mobile devices can be configured to auto-adjust the brightness, depending on the amount of surrounding light, to conserve battery power.
    - The device must have a light sensor to use auto-brightness
- Android Brightness Menu
  - When using an Android device, to configure screen brightness, go to Settings > Display > Brightness > slide the brightness to the desired level.
- iOS Display and Brightness Menu
  - When using an iOS device, to configure screen brightness, swipe up from the very bottom of the screen > slide the brightness bar up or down to vary the brightness.

GPS

- **Global Positioning System (GPS)** is a navigation system that determines the time and geographical location of the device by using messages from satellites in space and a receiver on Earth.
- A GPS radio receiver uses at least four satellites to calculate its position.
  - Enables geocaching and geotagging.
  - GPS services allow app vendors and website to know the location of a device and offer location-specific services, which is called **geotracking**.
- Indoor Positioning Systems (IPS) can determine device location by triangulating its proximity to other radio signals such as Wi-Fi access-points.
- Android location services
  - To enable GPS on Android devices use, Settings > Location > Tap on the toggle to turn location services on
- iOS location services
  - To enable GPS on iOS devices use, Settings > Privacy > Location services > Turn location services on

Wi-Fi Calling

- Instead of using the cellular carrier's network, modern smartphones can use the internet to transport voice calls by taking advantage of a local Wi-Fi hotspot.
  - If there is no Wi-Fi hotspot within reach, the phone will use the cellular carrier's network to transport voice calls.
- Wi-Fi calling is very useful in areas with poor cellular coverage because it uses a local Wi-Fi hotspot to fill the gaps.
  - The Wi-Fi hotspot must be able to guarantee a throughput of at least 1Mbps to the internet for a good quality call.
- Wi-Fi Calling on Android
  - To enable Wi-Fi calling on Android go to Settings > More (under Wireless & networks section) > Wi-Fi Calling > Tap on the toggle to turn it on
- Enabling Wi-Fi Calling on iOS
  - To enable Wi-Fi calling on iOS go to Settings > Phone and turn on Wi-Fi Calling

NFC Payment

- Mobile payments refer to any payments made through a mobile phone.
  - **Premium SMS based transactional payments** - Consumers send an SMS message to a carrier's special phone number containing a payment request and the seller is informed the payment has been received and is cleared to release the goods.
  - **Direct Mobile Billing** - Using a mobile billing option during check-out, a user identifies their self (usually through two-factor authentication) and allows the charge to be added to the mobile service bill.
  - **Mobile Web Payments** - The consumer uses the web or dedicated apps to complete the transaction.
  - **Contactless NFC (Near Field Communication)** – This method is used mostly in physical store transactions where a consumer pays for good or services by waving the phone near the payment system.

Virtual Private Network

- A **Virtual Private Network (VPN)** is a private network that uses a public network (usually the internet) to connect remote sites or users together.
- Many companies create their own VPNs to accommodate the needs of remote employees and distant offices.
  - When a VPN is established from a client to a server, the client accesses the network behind the server as if it was connected directly to that network.
  - Because VPN protocols also allow for data encryption, the communication between client and server is secure.
- Configuring a VPN Connection on Android
  - To create a new VPN connection on Android go to Settings > More (under Wireless & networks section) > VPN > Tap on the + sign to add a VPN connection
- Configuring a VPN Connection on iOS
  - To create a new VPN connection on iOS go to Settings > General > VPN > Add VPN Configuration...

Virtual Assistants

- A digital assistant, sometimes called a virtual assistant, is a program that can understand natural conversational language and perform tasks for the end user.
  - These digital assistants rely on artificial intelligence, machine learning, and voice recognition technology to understand conversational-style voice commands.
  - By pairing simple voice requests with other inputs, such as GPS location, these assistants can perform several tasks, including playing a specific song, performing a web search, taking a note, or sending an email.
- **Google Now**
  - To access Google Now on an Android device simply say "Okay google" and Google Now will activate and start listening to requests
- **Siri**
  - To access Siri on an iOS device, press and hold the Home button and Siri will activate and start listening to requests.
  - Alternatively, Siri can be configured to start listening when it hears "Hey Siri".
- **Cortana**
  - Found on Windows Phone 8.1 or later.

12.2 METHOD FOR SECURING MOBILE DEVICES

Restrictions on Failed Login Attempts

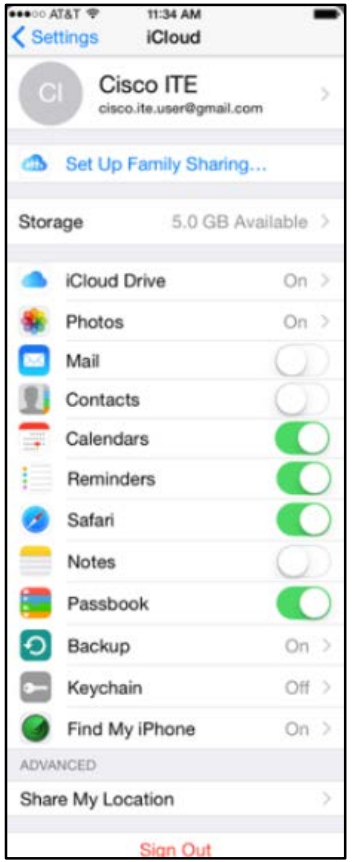
- When a passcode has been configured, unlocking a mobile device requires entering the correct PIN, password, pattern, or another passcode type.
  - In theory, a passcode, such as a PIN, could be guessed given enough time and perseverance.
- A passcode lock feature is used to:
  - Help prevent theft of private information.
  - Prevent unauthorized use of the device.
- To prevent someone from trying to guess a passcode, mobile devices can be set to perform defined actions after a certain number of incorrect attempts have been made.
  - It is common that an Android device will lock when a passcode has failed from 4 to 12 times.
    - After a device is locked, you can unlock it by entering the Gmail account information used to set up the device.

Restrictions on Failed Login Attempts

- iOS Erase Data
  - If the passcode fails 10 times, the screen goes black, and all data on the device is deleted.
    - To restore the iOS device and data, use either the Restore and Backup option in iTunes or iCloud.
- iOS GUI
  - On iOS, to increase security, the passcode is used as part of the encryption key for the entire system.

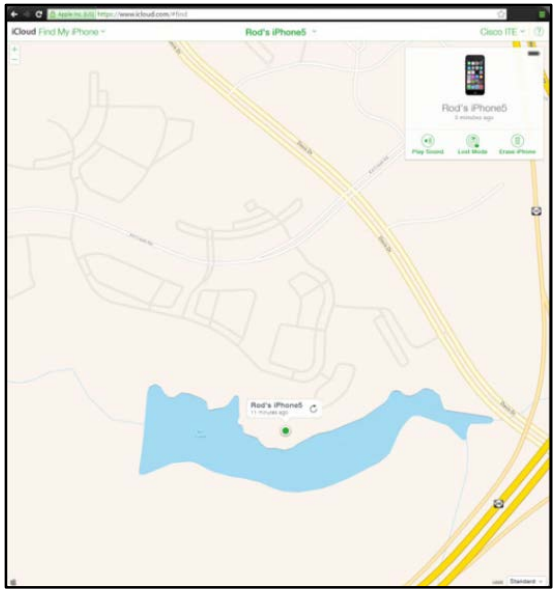
Remote Backup

- A remote backup is when a device copies its data to cloud storage using a backup app.
  - If data needs to be restored, run the backup app and access the website to retrieve the data.
- Most mobile operating systems come with a user account linked to the vendor's cloud services, such as iCloud for iOS, Google Sync for Android, and OneDrive for Microsoft.
  - The user can enable automatic backups to the cloud for data, apps, and settings.
- There are also third-party back providers, such as Dropbox, that can be used.
- Another option is to configure Mobile Device Management (MDM) software to automatically backup user devices.



Locator Applications

- If a mobile device is misplaced or stolen, it is possible to find it using a locator app.
- A locator app should be installed and configured on each mobile device before it is lost.
- Both Android and iOS have apps for remotely locating a device.
  - Android Device Manager allows a user to locate, ring, or lock a lost Android device, or to erase data from the device.
  - iOS users can use the Find My iPhone app
- After the device is located, you might be able to perform additional functions, such as sending a message or playing a sound.



Remote Lock and Remote Wipe

- If attempts to locate a mobile device have failed, there are other security features that can prevent data on the device from being compromised.
- Two of the most common remote security features are:
- Remote Lock (iOS = lost mode, Android = Lock)
  - Allows you to lock the device with a passcode, so others cannot gain access to the data in the device.
- Remote Wipe (iOS = erase phone, Android = Erase)
  - The remote wipe feature deletes all data from the device and returns it to a factory state.
  - To restore data to the device, Android users must set up the device using a Gmail account, and iOS users must synchronize their device to iTunes.

Antivirus

- Smartphones and other mobile devices are vulnerable to malicious software.
- Depending on the permissions granted to antivirus apps when they are installed on an Android device, the app might not be able to scan files automatically or run scheduled scans.
- iOS does not allow automatic or scheduled scans.
  - This is a safety feature to prevent malicious programs from using unauthorized resources or contaminating other apps or the OS.
- Mobile device apps run in a sandbox.
  - A sandbox is a location of the OS that keeps code isolated from other resources and other code.
  - It is difficult for malicious programs to infect a mobile device because apps are run inside the sandbox
  - To prevent the malicious program from infecting additional devices, a firewall can be used.

Rooting and Jailbreaking

- Mobile operating systems are usually protected by a number of software restrictions.
  - An unmodified copy of iOS, for example, will only execute authorized code and allow very limited user access to its file system.
- **Rooting** and **Jailbreaking** are two methods for removing restrictions and protections added to mobile operating systems.
  - Rooting is used on Android devices to gain privileged or root level access for modifying code or installing software that is not intended for the device.
  - Jailbreaking is typically used on iOS devices to remove manufacturer restrictions allowing them to run arbitrary user-code, grant users full access to the file system and full access to kernel modules.
- By rooting or jailbreaking a mobile device the GUI can be heavily customized, modifications can be made to the OS to improve the speed and responsiveness of the device, and apps can be installed from secondary or unsupported sources.

Patching and Updating Operating Systems

- Like the OS on a desktop or laptop, you can update or patch the OS on mobile devices.
  - Updates add functionality or increase performance.
  - Patches can fix security problems or issues with hardware and software.
- Android updates and patches use an automated process for delivery. When a carrier or manufacturer has an update for a device, a notification on the device indicates that an update is ready.
- iOS updates also use an automated process for delivery, and similar to Android, a notice to download opens if updates are available.
- There are two types of updates for mobile device radio firmware.
  - The **Preferred Roaming List (PRL)** is configuration information that a cellular phone needs to communicate on networks other than its own so that a call can be made outside of the carrier's network.
  - The **Primary Rate ISDN (PRI)** configures the data rates between the device and the cell tower. This ensures that the device is able to communicate with the tower at the correct rate.

12.3 LINUX AND MACOS OPERATING SYSTEMS

Introduction to Linux and macOS Operating Systems

- Unix
  - Unix is a proprietary operating system written in the C programming language.
  - macOS and iOS are based upon the Berkley Standard Distribution (BSD) version of Unix.
- Linux
  - Linux operating systems are used in embedded-systems, wearable devices, smartwatches, cellphones, netbooks, PCs, servers and super computers.
  - There are many different distributions (or distros) of Linux, including SUSE®, Red Hat®, CentOS®, Fedora®, Debian®, Ubuntu®, and Mint®.
  - Android, and many OS distributions rely upon the Linux kernel.
- macOS
  - The operating system for Macintosh computers is developed from the UNIX kernel, it is however, a closed source operating system.
  - macOS supports remote network installation called **NetBoot**

Linux and macSO File Systems

- Linux File Systems
  - **ext2** – Used in several Linux distributions, including Debian and Red Hat Linux.
  - **ext3** – Introduced the journaled file system to help minimize the risk of file system corruption in the event of a sudden power loss.
  - **ext4** – The latest and now default file system for must Linux distributions. Meant to extend storage limits and add other performance improvements.
- macOS File System
  - **HFS+** – Classic Mac or Mac OS Extended fie system is a metadata-rich and case-preserving but case-insensitive file system
  - **APFS** – Apple File System is the newest file system

Overview of Linux GUI

- Different Linux distributions ship with different software packages, but users decide what stays in their system by installing or removing packages.
- The graphical interface in Linux is comprised of a number of subsystems that can also be removed or replaced by the user.
  - Ubuntu Linux uses Unity as its default GUI.
  - The Linux GUI has the ability to have multiple desktops or workspaces.
- Canonical has a website that simulates Unity's UI and also provides a tour through the Unity's main features.
- To experience Unity via Canonical's website visit http://tour.ubuntu.com/en/.

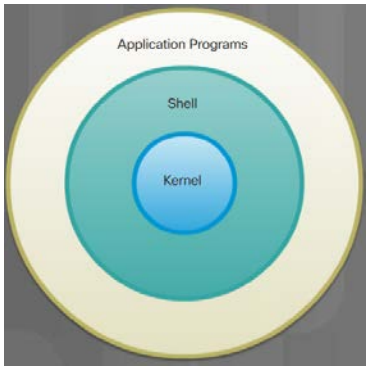
Overview of macOS GUI

- Among the major differences between older versions of OS X and macOS is the addition of the Aqua GUI.
- With macOS, Mission Control is a quick way to see everything that is currently open on your Mac.
  - Mission Control allows you to organize your apps on multiple desktops.
  - To navigate the file system, macOS includes **Finder**.
    - Finder is very similar to the Windows File Explorer.
- macOS allows screen sharing
  - Screen sharing is a feature that lets other people using Macs to be able to view your screen and even take control of your computer.

- **Force Quit** is commonly used to close an application that is unresponsive.

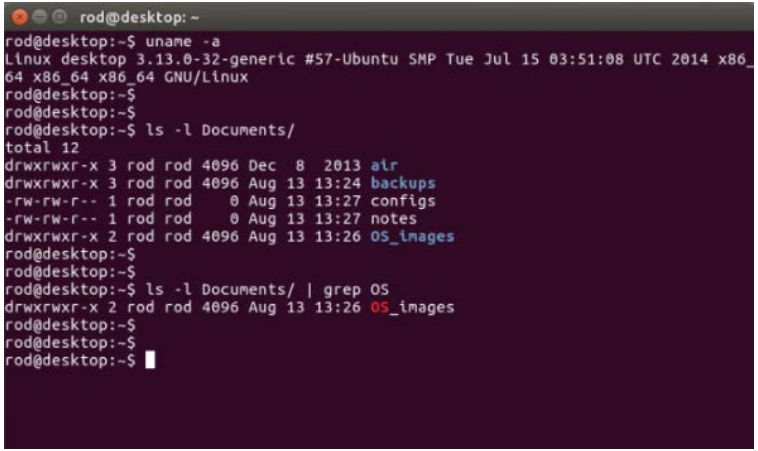
Overview of Linux and macOS CLI

- In both Linux and macOS, the user can communicate with the operating system by using the command line interface (CLI).
  - To add flexibility, commands (or tools) that support parameters, options and switches, are usually preceded by the dash (-) character.
- Most operating systems include a graphical interface.
  - Although a command line interface is still present, the OS often boots into the GUI by default, hiding the command line interface from the user.
  - One way to access the command line interface in a GUI-based operating system is through a terminal emulator application.
    - These applications provide user access to the command line interface and are often named as some variation of the word terminal.



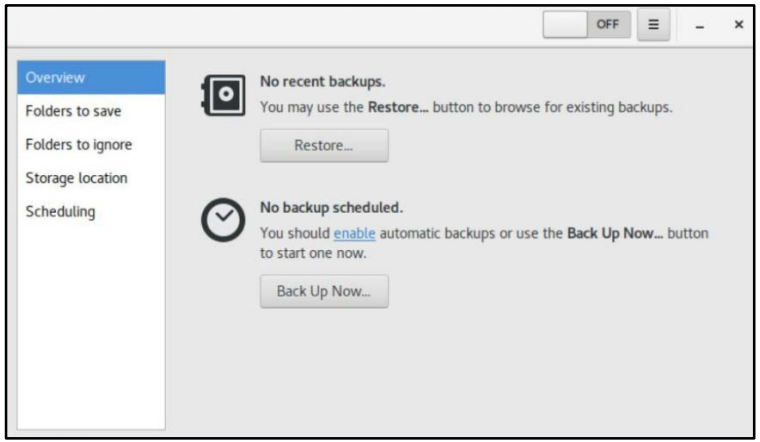
Overview of Linux and macOS CLI

- A program called a shell interprets the commands from the keyboard and passes them to the operating system.
  - When a user successfully logs in to the system, the login program starts the shell.
  - Afterwards, an authorized user can begin interacting with the OS through text-based commands.
- Users interact with the kernel through a shell.
  - The kernel is responsible for allocating CPU time and memory to processes.
  - The kernel also manages the file system and communications in response to system calls.
  - A corrupted driver may cause the kernel to freeze or exhibit kernel panic.
- macOS terminal emulator
  - macOS includes a terminal emulator called **Terminal**, but a number of third-party emulators are available.



Linux Backup and Recovery

- The process of backing up data refers to creating a copy (or multiple copies) of data for safekeeping.
- When the backing up process is complete, the copy is called a backup.
- While backups can be achieved with a simple copy command, many tools and techniques exist to make the process automatic and transparent to the user.
- Linux does not have a built-in backup tool.
  - However, there are many commercial and open source backup solutions for Linux such as Amanda, Bacula, Fwbackups, and Déjà Dup.



macOS Backup and Recovery

- macOS includes a backup tool called **Time Machine**.
  - With Time Machine, users choose an external drive to be used as a backup destination device and connect it to the Mac via USB, FireWire or Thunderbolt.
  - Time Machine will prepare the disk to receive backups and, when the disk is ready, it performs incremental backups periodically.
  - Time Machine stores some backups on your Mac, so if the Time Machine backup disk is not available, you may be able to restore a backup directly from your Mac.

Overview of Disk Utilities

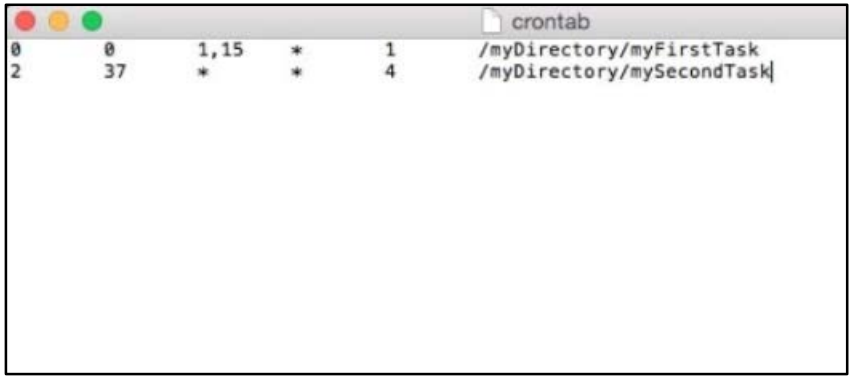
- To help diagnose and solve disk-related problems, most modern operating systems include disk utility tools.
- Ubuntu Linux includes a disk utility called Disks.
  - With Disks users can perform the most common disk-related tasks including partition management, mount or unmount, format disks and query Analysis and Reporting Technology, (S.M.A.R.T.).
- macOS includes Disk Utility.
  - In addition to supporting the main disk maintenance tasks, Disk Utility also supports Verify Disk Permissions and Repair Disk Permissions.
  - Repair Disk Permission is a common troubleshooting step in macOS.
  - Disk Utility can also be used to backup disks to image files and perform an image recovery to disk from image files.
  - To install and boot more than one OS, a boot manager is required.
  - **Netboot** is a macOS utility used to remotely boot a computer.

Overview of Disk Utilities

- Below are a few common maintenance tasks that can be performed using disk utility software:
  - **Partition management** – When working with computer disks, partitions may need to be created, deleted or resized.
  - **Mount or Unmount disk partitions** – On Unix-like systems, mounting a partition relates to the process of binding a partition of a disk or a disk image file (usually a .iso) to a folder location.
  - **Disk Format** – Before a partition can be used by the user or the system, it must be formatted.
  - **Bad Sector Check** –When a disk sector is flagged as bad, it becomes harmless to the OS because it will no longer be used to store data.
    - Many bad sectors could be an indicator of a failing disk.
  - **Query S.M.A.R.T. attributes** – S.M.A.R.T. can detect and report attributes about a disk's health.
    - The goal of S.M.A.R.T. is to anticipate disk failure, allowing the user to move the data to a healthy disk before the failing disk becomes inaccessible.

Scheduled Tasks

- Maintenance tasks should be scheduled and performed frequently to prevent or detect problems early.
  - To avoid missing maintenance tasks due to human error, computer systems can be programmed to perform tasks automatically.
- Two tasks that should be scheduled and performed automatically are backups and disk checks.
- In Linux and macOS, the cron service is responsible for scheduled tasks.
  - As a service, **cron** runs in the background and executes tasks at specific dates and times.
  - Cron uses a schedule table called a cron table that can be edited with the crontab command

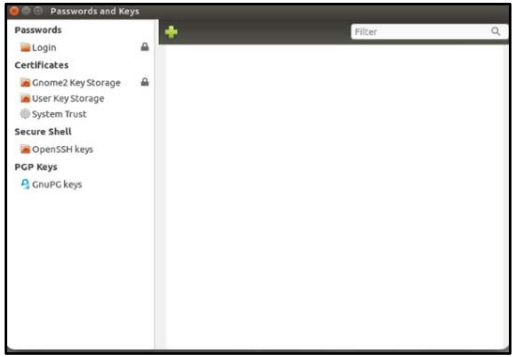


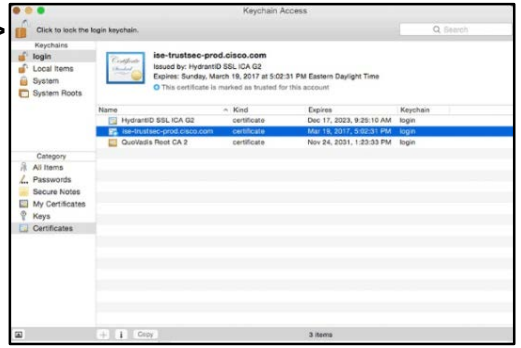
Operating System Updates

- Also known as patches, OS updates are released periodically by OS companies to address any known vulnerability in their operating systems.
  - While companies have update schedules, the release of unscheduled OS updates is common when a major vulnerability is found in the OS code.
- Firmware Updates
  - Usually held in non-volatile memory, such as ROM or Flash, firmware is a type of software designed to provide low-level functionality for a device.
- Antivirus and Antimalware
  - Antivirus and antimalware rely on code signatures to operate.
    - Signatures or signature files are files containing a sample of the code used by viruses and malware
  - New malware is created and released every day; therefore, the signature files of antivirus and antimalware programs must be updated just as frequently.

Security

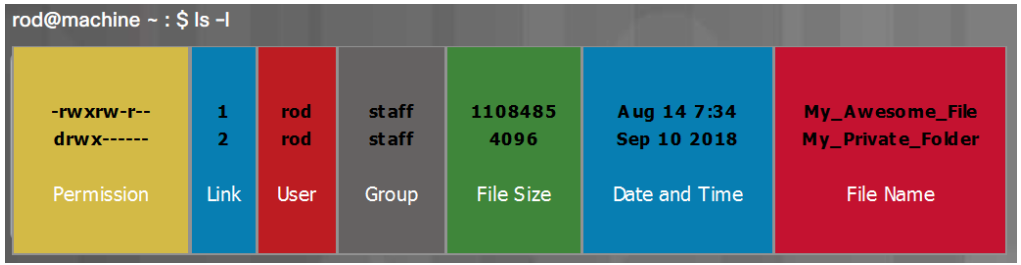
- Usernames, passwords, digital certificates, and encryption keys are just a few of the security credentials associated to a user.
- Due to the increasing number of necessary security credentials, modern operating systems include a service to manage them.
  - Applications and other services can then request and utilize the credentials stored by the security credentials manager service.
- Security Credentials Service on Ubuntu
  - Gnome-keyring is a security credentials manager for Ubuntu Linux. To access Gnome-Keyring on Ubuntu Linux, click Dash > Search for Key > Click Passwords and Keys
- Security Credentials Service on macOS
  - Keychain is a security credentials manager for macOS. To access Keychain on macOS, go to Applications > Utilities > Keychain Access





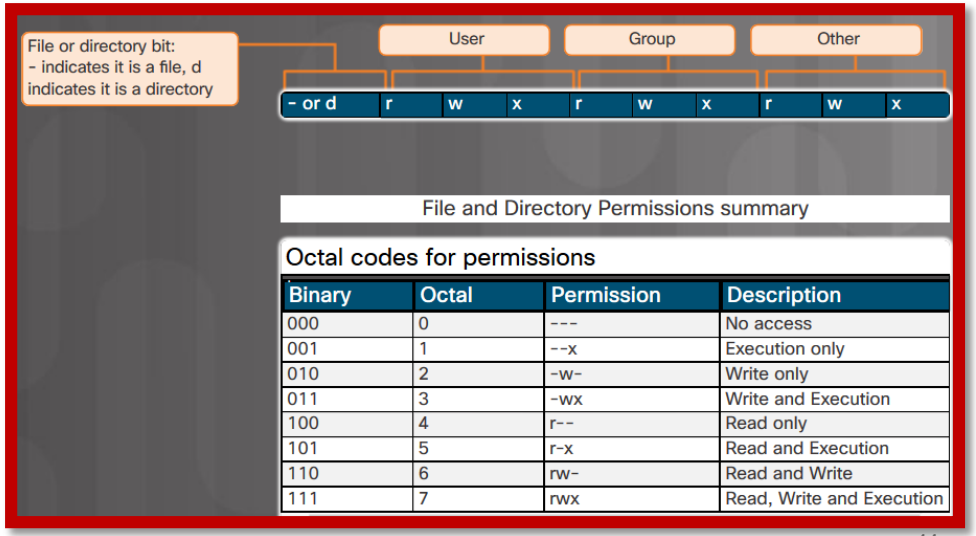
The ls –l command output

- **Permission** - Defines how the user, group, and other access the files and directories.
- **Link** - The number of links or the number of directories inside this directory
- **User** - Displays the username of the owner of the file or the directory.
- **Group** - Displays the name of the group that owns the file or the directory.
- **File Size** - Displays the file size in bytes.
- **Date and Time** - Is the data and time of the last modification.
- **File Name** - Displays the file or directory name.



Basic Unix File and Directory Permissions

- To organize the system and reinforce boundaries within the system, Unix uses file permissions.
- Every file and directory on Unix systems carries its permissions which define the actions that the **owner**, the **group**, and **others** can do with the file or directory.
- The only user who can override file permissions in Unix is the root user.
- Root access is often required before performing maintenance and administrative tasks.



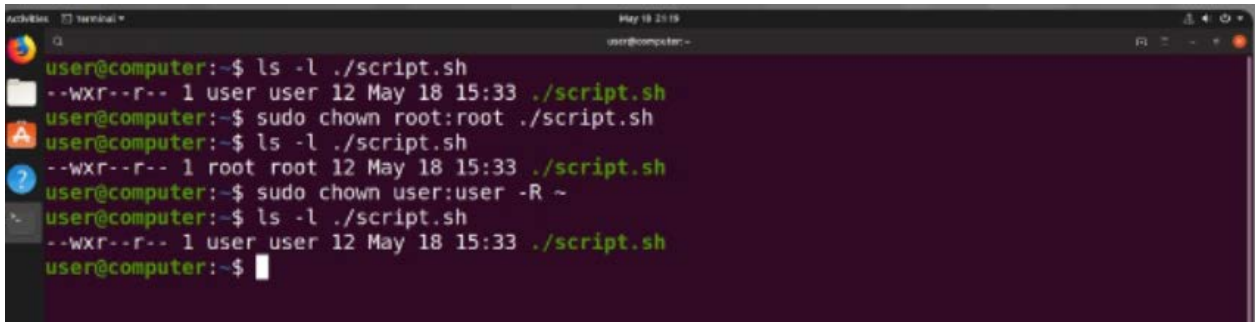
Binary	Octal	Permission	Description
000	0	---	No access
001	1	--x	Execution only
010	2	-w-	Write only
011	3	-wx	Write and Execution
100	4	r--	Read only
101	5	r-x	Read and Execution
110	6	rw-	Read and Write
111	7	rwx	Read, Write and Execution

Linux Administrative Commands

- Administrators use the terminal to monitor and control users, processes, ip addresses, and other tasks.
  - **passwd** – allows users to change their own password at the terminal.
  - **ps** – allows users to monitor their own processes.
  - **kill** – allows users to end the processes that they have started.
  - **ifconfig** – similar to the Windows ipconfig command, however this command is deprecated and the “ip address” command should be used.
  - **iwconfig** – allows users to set and view their wireless settings.
  - **chmod** – allows users to change the permissions of files that they own.
- Copy, Move, New, Edit
  - **cp** – allows users to copy or backup a file for folder.
  - **mkdir** – allows users to make a new directory.
  - **vi** – opens a text editor.

Linux Administrative Commands Requiring Root Access

- Administrators use the terminal to monitor and control users, processes, ip addresses, and other tasks.
  - **sudo** – (Super User Do) grants a user root access without actually changing their profile.
  - **chown** - allows users to switch both the owner and the group of a file or files.
  - **apt-get** – is used to install and manage software on Debian based Linux distributions.
  - **shutdown** – is used to halt and reboot the operating system.
  - **dd** - (Disk Duplicate) is used to copy files and partitions and create temporary swap files.



12.4 BASIC TROUBLESHOOTING PROCESS FOR MOBILE, LINUX, AND MACOS OPERATING SYSTEMS

The Troubleshooting Process

Most operating systems contain utilities to assist in the troubleshooting process. These utilities help a technician to determine why the computer crashes or does not boot properly. The utilities also help identify the problem and how to resolve it.

Step 1 Identify the problem

Step 2 Establish a theory of probable causes

Step 3 Test the Theory to Determine cause

Step 4 Establish a Plan of Action to Resolve the Problem and Implement the Solution

Step 5 Verify Full System Functionality and Implement Preventative Measures

Step 6 Document Findings, Actions, and Outcomes

Step 1 – Identify the Problem

Mobile Device Operating Stems	
Open-ended questions	• What is the problem you are experiencing? • What is the version of the mobile OS are you using? • What service provider do you have? • What apps have you installed recently?
Closed-ended questions	• Has this problem happened before? • Has anyone else used the mobile device? • Is your mobile device under warranty? • Have you modified the operating system on the mobile device? • Have you installed any apps from an unapproved source? • Does the mobile device connect to the Internet?

Step 1 – Identify the Problem

Linux or macOS	
Open-ended questions	• What is the problem you are experiencing? • What is the make and model of your computer? • What version of Linux or macOS is it running? • What programs or drivers have you installed recently? • What OS updates have you installed recenty? • What system configurations have you changed recently?
Closed-ended questions	• Has this problem happened before? • Has anyone else used the computer? • Is your computer under warranty? • Does the computer connect to the Internet?

Step 2 – Establish a theory of Probable Cause

Common causes of mobile device operating system problems	• The mobile device cannot send or receive email. • An app has stopped working. • A malicious app has been sideloaded. • The mobile device has stopped responding. • Mobile device software or apps are not up to date. • A user has forgotten their passcode.
Common causes of Linux or macOS problems	• The computer cannot send or receive email. • An application has stopped working. • A malicious application has been installed. • The computer has stopped responding. • The operating system is not up to date. • A user has forgotten their login credentials.

Step 3 – Test the Theory to Determine the Cause

Common steps to determine cause of mobile device operating system problem.	• Force a running app to close. • Reconfigure email account settings. • Restart the mobile device. • Restore the mobile device from a backup. • Connect an iOS device to iTunes. • Update the operating system. • Reset the mobile device to factory defaults.
Common steps to determine cause of Linux or macOS problems	• Force a running program to close. • Reconfigure email account settings. • Restart the computer. • Restore the computer from backup. • Update the computer's operating system.

Step 4 – Establish a Plan of Action to Resolve the Problem and Implement the Solution

If no solution is achieved in the previous step, further research is needed to implement the solution.	• Helpdesk Repair Logs • Other Technicians • Manufacturer FAQs • Technical Websites • Device Manual • Online Forums • Internet Search

Step 5 – Verify Full System Functionality and if Applicable, Implement Preventive Measures

Verify solution and full system functionality for mobile device operating systems.	• Reboot the mobile device. • Browse the Internet using Wi-Fi. • Browse the Internet using 4G, 3G, or another carrier network type. • Make a phone call. • Send a text message. • Open different types of apps.
Verify solution and full system functionality for Linux and macOS.	• Reboot the computer. • Browse the Internet using Wi-Fi. • Browse the Internet using a wired connection. • Send a test email. • Open different programs. • A user has forgotten their login credentials.

Step 6 – Document Findings, Actions, and Outcomes

Document your findings, actions and outcomes.	• Discuss the solution implemented with the customer. • Have the customer verify the problem has been solved. • Provide the customer with all paperwork. • Document the steps taken to solve the problem in the work order and technician's journal. • Document any components used in the repair. • Document the time spent to solve the problem.

Common Problems and Solutions for Mobile Operating Systems

The mobile device will not connect to the Internet.

Probable Causes	Possible Solutions
W-Fi is turned off.	Turn on W-Fl.
Wi-Fi settings are incorrect.	Reconfigure the W-Fi settings.
Airplane mode is turned on.	Turn off Airplane mode

Common Problems and Solutions for Mobile OS Security

A mobile device has a weak signal or the signal has been dropped.

Probable Causes	Possible Solutions
There are not enough cell towers in the area.	Move to a more populated area that will have more cell towers.
The area is between coverage areas of the carrier.	Move to an area within the range of your carrier.
The building that you are in is blocking the signal.	Relocate to a different area in the building or outside.
Your grip on the mobile device is blocking the signal.	Change your grip on the device.

Common Problems and Solutions for Linux and macOS Operating Systems

The automatic backup operation does not start.

Possible Causes	Possible Solutions
Time Machine is turned oft in macOS.	I Turn on Time Machine in macOS.
Deja Dup is turned off in Linux.	Turn on Deja Dup in Linux.

12.5 CHAPTER SUMMARY

Chapter 12: Mobile, Linux, and macOS Operating Systems

- Explain the purpose and characteristics of mobile operating systems.
- Explain methods for securing mobile devices.
- Explain the purpose and characteristics of Mac and Linux operating systems.
- Explain how to troubleshoot other operating systems.


Cisco Networking Academy
IT Essentials


Elk Technologies
https://elktech.org
SCOTT STEPHENSON