Chapter 1

1.0 Introduction:

- [ ] Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- [ ] Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- [ ] Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
- [ ] Explain the features and characteristics of the Linux Operating System.
- [ ] Analyze the operation of network protocols and services.
- [ ] Explain the operation of the network infrastructure.
- [ ] Classify the various types of network attacks.
- [ ] Use network monitoring tools to identify attacks against network protocols and services.
- [ ] Explain how to prevent malicious access to computer networks, hosts, and data.
- [ ] Explain the impacts of cryptography on network security monitoring.
- [ ] Explain how to investigate endpoint vulnerabilities and attacks.
- [ ] Evaluate network security alerts.
- [ ] Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- [ ] Apply incident response models to manage network security incidents.
- [ ] Threat Actors: Explain the motivations of the threat actors behind specific security incidents.
- [ ] Threat Impact: Explain the potential impact of network security attacks.

Resources:

Two virtual machines:

1. CyberOps Workstation
2. Security Onion

Packet Tracer

Our community

Get a Job!

Ethical Hacking Statement:

Using the knowledge in sandboxed and this a course for create professionals in cybersecurity.

Why should I take this Module?

Protect your information and find out more about the threats and threat actors.

Activity Class.

a. What is the vulnerability being exploited?
b. What information, data, or control can be gained by a hacker exploiting this vulnerability?
c. How is the hack performed?
d. What about this particular hack interested you specifically?
e. How do you think this particular hack could be mitigated?

1.1 War Stories: Explain why networks and data are attacked.

Hijacked People:

- evil twin hotspots
- Connect devices in Wi-Fi

Ransomed Companies

- Ransomware: use a email to encrypt important data and the goal is financial gain

Targeted Nations:

- Only a nation have the resources to create a malware.
- Stuxnet worm: This is a malware, which infected USB drives.
- [ ] WATCH: Zero Days, a film released in 2016
- [x] Anatomy of an IoT Attack ~ The anatomy of an IoT Attack

Lab installing the virtual machines

Resources

- Host computer with a minimum of 8 GB of RAM and 40GB of free disk space
- High speed internet access to download Oracle VirtualBox and the virtual machine image files

Lab Cybersecurity Case Studies

Who were the victims of the attacks?
What technologies and tools were used in the attack?
When did the attack happen within the network?
What systems were targeted?
What was the motivation of the attackers in this case? What did they hope to achieve?
What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

1.2 Threat Actors

a. *Amateurs (script kiddies): No skills, but they can cause big damage*
b. *Hacktivists: they use DDoS to public information about organizations and governments.*
c. *Financial Gain: Use this for win money and cash flow*
d. *Trade Secrets and Global politics*

Lab - Learning the Details of Attacks IoT

Who were the victims of the attacks?
What technologies and tools were used in the attack?
When did the attack happen within the network?
What systems were targeted?
What was the motivation of the attackers in this case? What did they hope to achieve?
What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

1.3 Threat Impact

PII: *Personally identifiable information*
Ej: Name, Last name, birthdate, Credit Card numbers, ID, etc.
PHI: *protected health information*
Ej: blood, rh+, disease
PSI: ***Personal security information:***
Ej: Id in a social networks, Password, etc.

ABSTRACT ABOUT THE CHAPTER

War Stories

Threat actors can hijack banking sessions and other personal information by using "evil twin" hotspots. Threat actors can target companies, as in the example where opening a pdf on the company computer can install ransomware. Entire nations can be targeted. This occurred in the Stuxnet malware attack.

Threat Actors

Threat actors include, but are not limited to, amateurs, hacktivists, organized crime groups, state sponsored, and terrorist groups. The amateur may have little to no skill and often use information found on the internet to launch attacks. Hacktivists are hackers who protest against a variety of political and social ideas. Much of the hacking activity is motivated by financial gain. Nation states are interested in using cyberspace for industrial espionage. Theft of intellectual property can give a country a significant advantage in international trade. As the Internet of Things (IoT) expands, webcams, routers, and other devices in our homes are also under attack.

Threat Impact

It is estimated that businesses will lose over $5 trillion annually by 2024 due to cyberattacks. Personally identifiable information (PII), protected health information (PHI), and personal security information (PSI) are forms of protected information that are often stolen. A company can lose its competitive advantage when this information is stolen, including trade secrets. Also, customers lose trust in the company's ability to protect their data. Governments have also been victims of hacking.

2.0 Introduction

SOC and becoming a defender

2.1 The Modern Security Operations Center

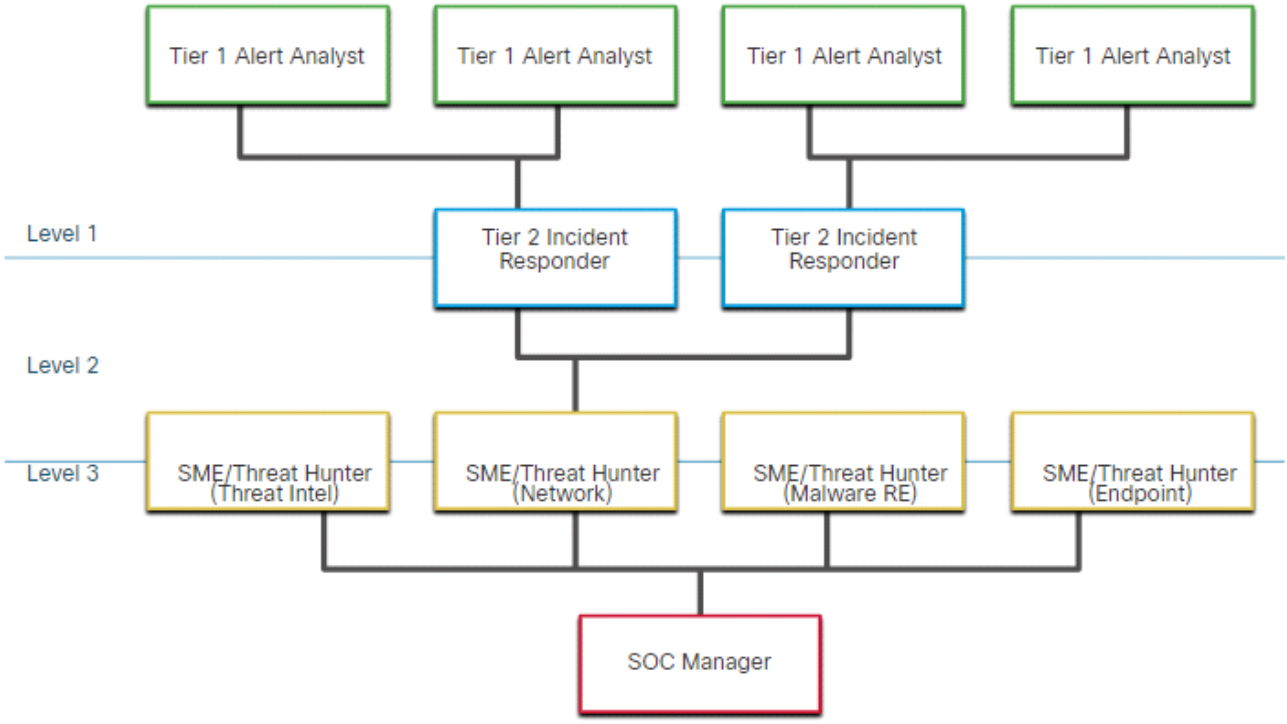
Elements of a security Operations Center

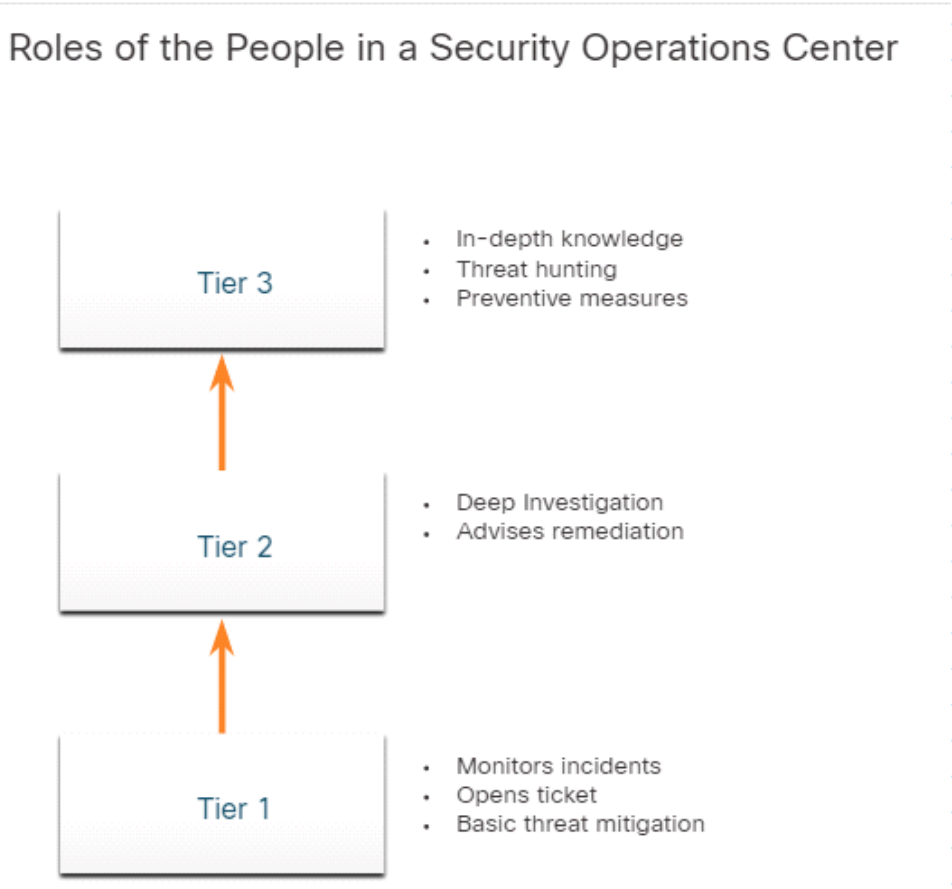
- Process
- Technology
  - SIEM:
    - → Event collection, correlation, and analysis
    - → Security monitoring
    - → Security control
    - → Log management
    - → Vulnerability assessment
    - → Vulnerability tracking
    - → Threat intelligence
  - SOAR:
    - → Gather alarm data from each component of the system.
    - → Provide tools that enable cases to be researched, assessed, and investigated.
    - → Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies.
    - → Include pre-defined playbooks that enable automatic response to specific threats. Playbooks

can be initiated automatically based on predefined rules or may be triggered by security personnel.

- SOC (security operations center):
  - → Dwell Time – the length of time that threat actors have access to a network before they are detected, and their access is stopped.
  - → Mean Time to Detect (MTTD) – the average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network.
  - → Mean Time to Respond (MTTR) – the average time that it takes to stop and remediate a security incident.
  - → Mean Time to Contain (MTTC) – the time required to stop the incident from causing further damage to systems or data.
  - → Time to Control – the time required to stop the spread of malware in the network.

- People
  - Alert Analyst
  - Incident Responder
  - Threat Hunter
  - SOC Manager





2.2 Becoming a defender

Certifications:

- Cisco Certified CyberOps Associate
- CompTIA Cybersecurity Analyst Certification
- (ISC)² Information Security Certifications
- Global Information Assurance Certification (GIAC)

Further Education

- Degrees
- Python Programming
- Linux Skills

Sources of Career Information

- Indeed.com
- CareerBuilder.com
- USAJobs.gov
- Glassdoor
- LinkedIn

2.3 Fighters in the war against cybercrime summary

ABSTRACT ABOUT THE CHAPTER

The Modern Security Operations Center

Major elements of the SOC include people, processes, and technologies. Job roles are rapidly evolving and include tiers based on expertise and experience. These roles include a Tier 1 Alert Analyst, a Tier 2 Incident Responder, a Tier 3 Threat hunter, and an SOC Manager. A Tier 1 Analyst will monitor incidents, open tickets, and perform basic threat mitigation.

SEIM systems are used for collecting and filtering data, detecting and classifying threats, and analyzing and investigating threats. SEIM and SOAR are often paired together. SOAR is similar to SIEM. SOAR goes a step further by integrating threat intelligence and automating incident investigation and response workflows based on playbooks developed by the security team. Key Performance Indicators (KPI) are devised to measure different aspects of SOC

incident investigation and response workflows based on playbooks developed by the security team. Key Performance Indicators (KPI) are devised to measure different aspects of SOC performance. Common metrics include Dwell Time, Meant Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), and Time to Control.

There must be a balance between security and availability of the networks. Security cannot be so strong that it interferes with employees or business functions.

Becoming a Defender

A variety of cybersecurity certifications that are relevant to careers in SOCs are available from different organizations. They include Cisco Certified CyberOps Associate, CompTIA Cybersecurity Analyst Certification, (ISC)2 Information Security Certifications, Global Information Assurance Certification (GIAC), and others. Job sites include Indeed.com, CareerBuilder.com, USAJobs.gov, Glassdoor, and LinkedIn. You may also want to consider internships and temporary agencies to gain experience and begin your career. In addition, Linux and Python programming skills will add to your desirability in the job market.

Windows Operating system

Module Objective: Explain the security features of the Windows operating system.

3.1 Windows History

DOS => Only to read and write data

Windows bought DOS and they created MS-DOS

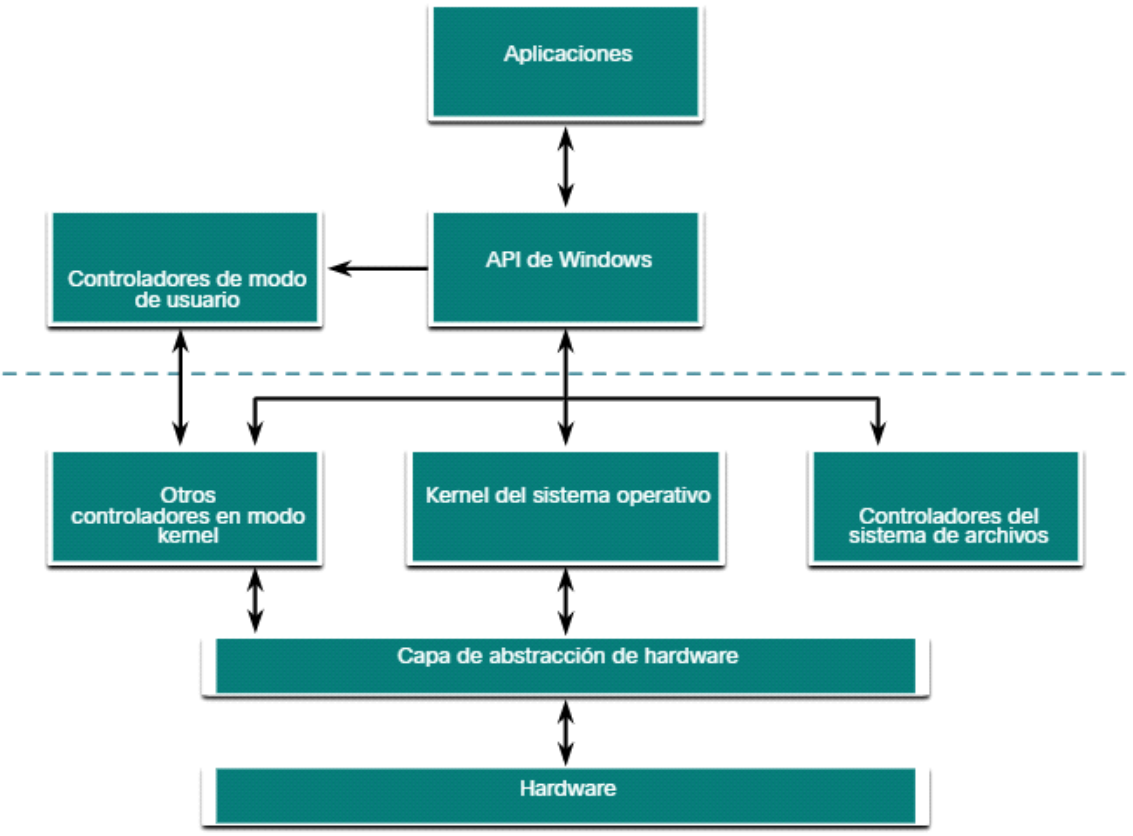
Comands in MS-DOS

- → **dir**
- → **cd** , cd .., cd, cd directory,
- → **del** filename
- → **find**
- → **Mkdir** directory
- → **ren** oldname newname
- → **Help**
- → **Help** command

Operating System Vulnerabilities

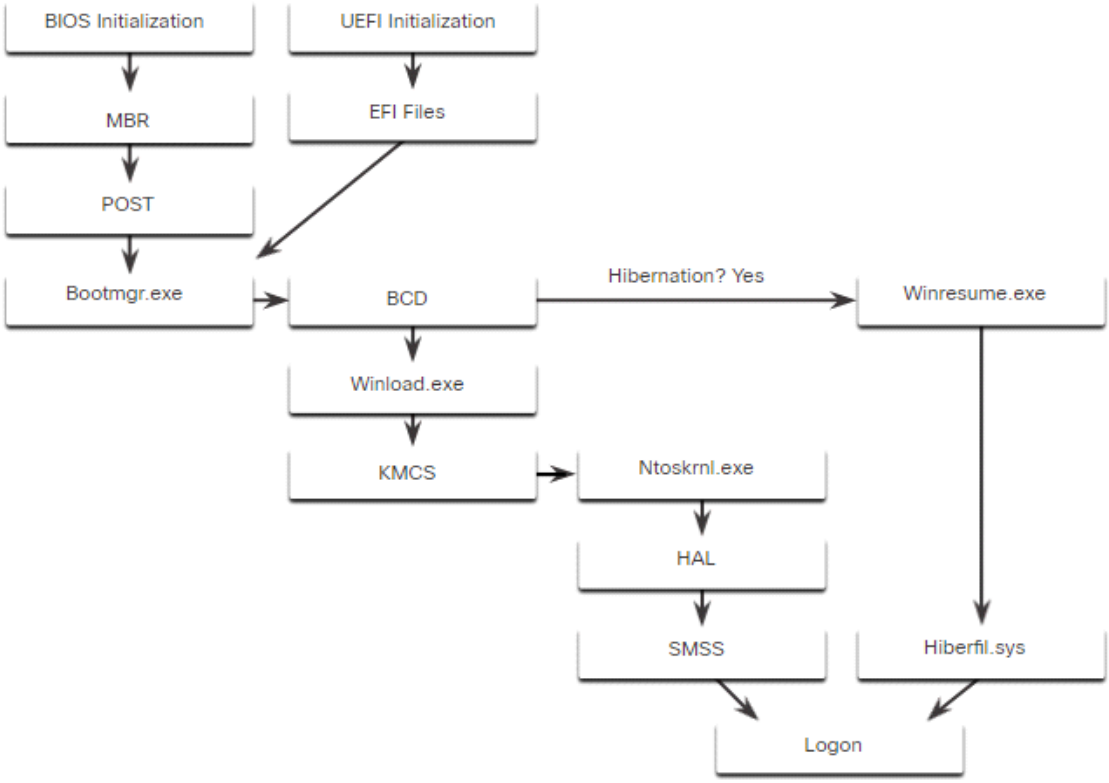
- → Virus or malware protection
- → Unknown or unmanaged services
- → Encryption
- → Security policy
- → Firewall
- → File and share permissions
- → Weak or no password
- → Login as Administrator

3.2 Windows Arquitecture and operations



Basic model OS

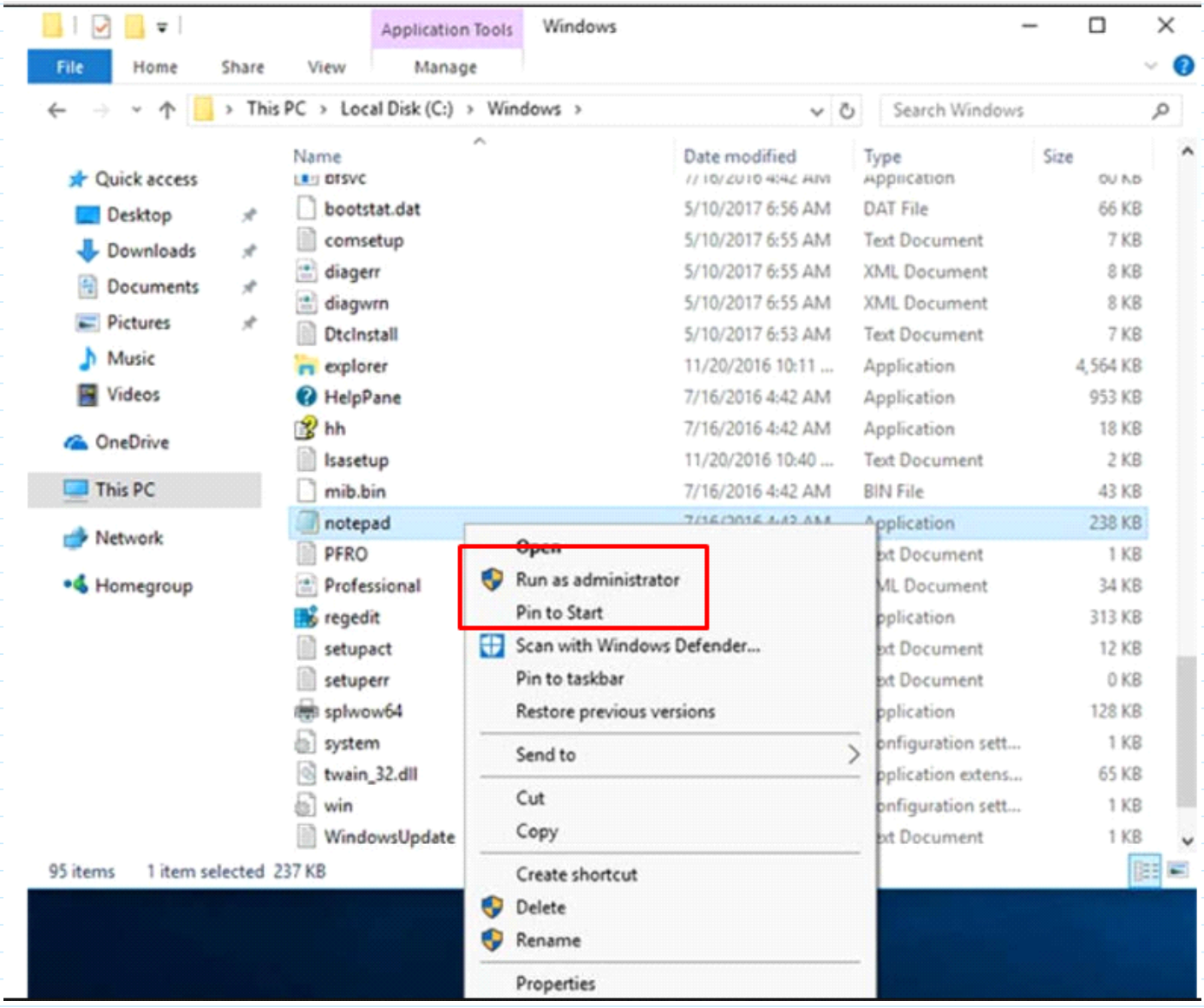
- **Hal:** hardware abstraction layer
  → communication between the hardware and the kernel.
- Windows File Systems
  → exFAT
  → Hierarchical File System Plus (HFS+)
  → Extended File System (EXT)
  → New Technology File System (NTFS)

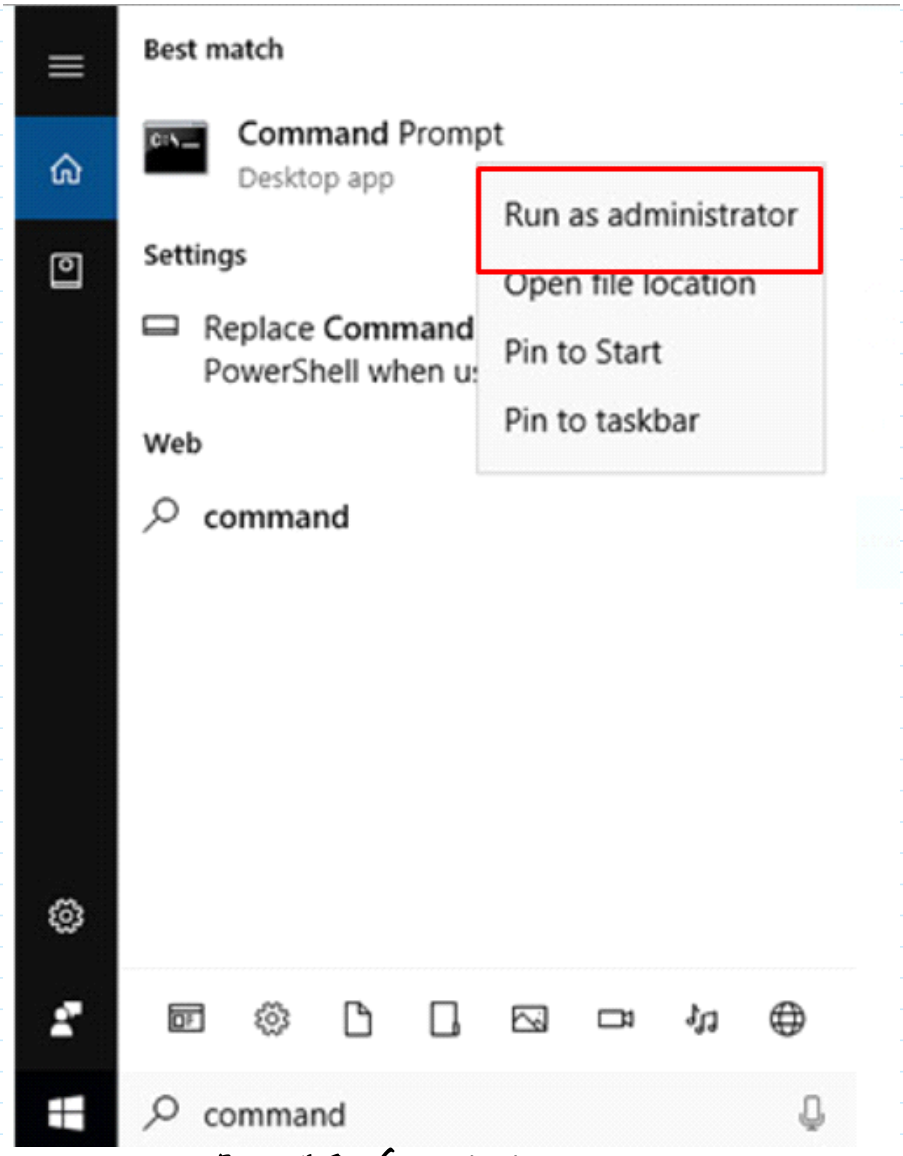


→

Windows Boot Process

3.3 Windows configuration and monitoring


Application Tools
Windows
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Windows ›
Search Windows
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Homegroup
Name
Date modified
Type
Size
bootstat.dat 5/10/2017 6:56 AM DAT File 66 KB
comsetup 5/10/2017 6:55 AM Text Document 7 KB
diagerr 5/10/2017 6:55 AM XML Document 8 KB
diagwrn 5/10/2017 6:55 AM XML Document 8 KB
DtcInstall 5/10/2017 6:53 AM Text Document 7 KB
explorer 11/20/2016 10:11 ... Application 4,564 KB
HelpPane 7/16/2016 4:42 AM Application 953 KB
hh 7/16/2016 4:42 AM Application 18 KB
lsasetup 11/20/2016 10:40 ... Text Document 2 KB
mib.bin 7/16/2016 4:42 AM BIN File 43 KB
notepad Application 238 KB
PFRO
Professional
regedit
setupact
setuperr
splwow64
system
twain_32.dll
win
WindowsUpdate
Open
Run as administrator
Pin to Start
Scan with Windows Defender...
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties
95 items
1 item selected 237 KB



Run AS administrator

Comands in power shell

→ get-help

These are the four tabs in the Windows Management Instrumentation*(WMI) *Control Properties window:

- *General - Summary information about the local computer and WMI*
- *Backup/Restore - Allows manual backup of statistics gathered by WMI*
- *Security - Settings to configure who has access to different WMI statistics*
- *Advanced - Settings to configure the default namespace for WMI*

Comands to use windows

- Net : which is used in the administration and maintenance of the OS

Command	Description
net accounts	Sets password and logon requirements for users
net session	Lists or disconnects sessions between a computer and other computers on the network
net share	Creates, removes, or manages shared resources
net start	Starts a network service or lists running network services
net stop	Stops a network service
net use	Connects, disconnects, and displays information about shared network resources
net view	Shows a list of computers and network devices on the network

3.4 Windows Security

netstat command can be used to look for inbound or outbound connections that are not authorized. When used on its own, the netstat command will display all of the active TCP connections.

Event Viewer

ABSTRACT ABOUT THE CHAPTER

Windows History

The first computers required a Disk Operating System (DOS) to create and manage files. Microsoft developed MS-DOS as a command line interface (CLI) to access the disk drive and load the operating system files. Early versions of Windows consisted of a Graphical User Interface (GUI) that ran over MS-DOS. However, modern Windows versions are in direct control of the computer and its hardware and support multiple user processes. This is much different than the single process, single user MS-DOS. Since 1993, there have been more than 20 releases of Windows that are based on the NT operating system. Users use a Windows GUI to work with data files and software. The GUI has a main area that is known as the Desktop and a Task Bar situated below the desktop. The Task Bar includes the Start menu, quick launch icons, and a notification area. Windows has many vulnerabilities. Recommendations to secure the Windows OS include use of virus or malware protection, use of strong passwords, use of firewall, and limited use of the administrator account, among others.

Windows Architecture and Operations

Windows consists of a hardware abstraction layer (HAL) that is software that handles all of the communication between the hardware and the kernel. The kernel has control over the entire computer and handles input and output requests, memory, and all of the peripherals connected to the computer. Windows operates in two different modes. The first is user mode. Most Windows programs run

and the kernel. The kernel has control over the entire computer and handles input and output requests, memory, and all of the peripherals connected to the computer. Windows operates in two different modes. The first is user mode. Most Windows programs run in user mode. The second is kernel mode. It allows operating system code direct access to the computer hardware. Windows supports several different file systems, but NTFS is the most widely used. NTFS volumes include the partition boot sector, master file table, system files and the file area. When a computer boots, it first accesses system information and code that is stored in BIOS hardware. The BIOS boot code performs a system self-test called POST, locates and loads the Windows OS, and loads other associated programs to start the operating system. Windows should always be shutdown properly.

A computer works by storing instructions in RAM until the CPU processes them. Each process in a 32-bit Windows computer supports a virtual address space that enables addressing up to 4 gigabytes. Each process in a 64-bit Windows computer supports a virtual address space of up to 8 terabytes. Windows stores all of the information about hardware, applications, users, and system settings in a large database known as the registry. The registry is a hierarchical database where the highest level is known as a hive, below that there are keys, followed by subkeys. There are five registry hives that contain data regarding the configuration and operation of Windows. There are hundreds of keys and subkeys.

Windows Configuration and Monitoring

For security reasons, it is not advisable to log on to Windows using the Administrator account or an account with administrative privileges. Do not give standard users administrative privileges. Do not enable the Guests account unless the computer is going to be used by many different people who do not have accounts. Use Windows groups to make administration of users easier. Local users and groups are managed with the lusrmgr.msc control panel applet.

You can use the CLI or the Windows PowerShell to execute commands. PowerShell can be used to create scripts to automate tasks that the regular CLI is unable to automate. Windows Management Instrumentation (WMI) is used to manage remote computers. The net command can be combined with switches to focus on specific output. Task Manager provides a lot of information about what is running, and the general performance of the computer. The Resource Monitor provides more detailed information about resource usage. The Network and Sharing Center is used to configure Windows networking properties and test networking settings. The Server Message Block (SMB) protocol is used to share network resources such as files on remote hosts. The Universal Naming Convention (UNC) format is used to connect to resources. Windows Server is an edition of Windows that is mainly used in data centers. It provides network, file, web, and management services to a Windows network or domain.

Windows Security

Malware can open communication ports to communicate and spread. The Windows netstat command displays all open communication ports on a computer and can also display the software processes that are associated with the ports. This enables unknown potentially malicious software to be identified and shutdown. Windows Event Viewer provides access to numerous logged events regarding the operation of a computer. Windows logs Windows events and applications and services events. Logged event severity levels range through the information, warning, error, or critical levels. It is very import to keep Windows up to date to guard against new security threats. Software patches, updates, and service packs address security vulnerabilities as they are discovered. Windows should be configured to automatically download and install updates as they become available. Windows can be configured to only install and restart a computer at specified times of day.

Introduction:

What is Linux

Linux is an operating system that was created in 1991. Linux is open source, fast, reliable, and small. It requires very little hardware resources to run and is highly customizable. Unlike other operating systems such as Windows and Mac OS X, Linux was created, and is currently maintained by, a community of programmers. Linux is part of several platforms and can be found on devices anywhere from "wristwatches to supercomputers".

Kali linux

Kali Linux is a Linux distribution groups many penetration tools together in a single Linux distribution. Kali contains a great selection of tools. The figure shows a screenshot of Kali Linux. Notice all the major categories of penetration testing tools.

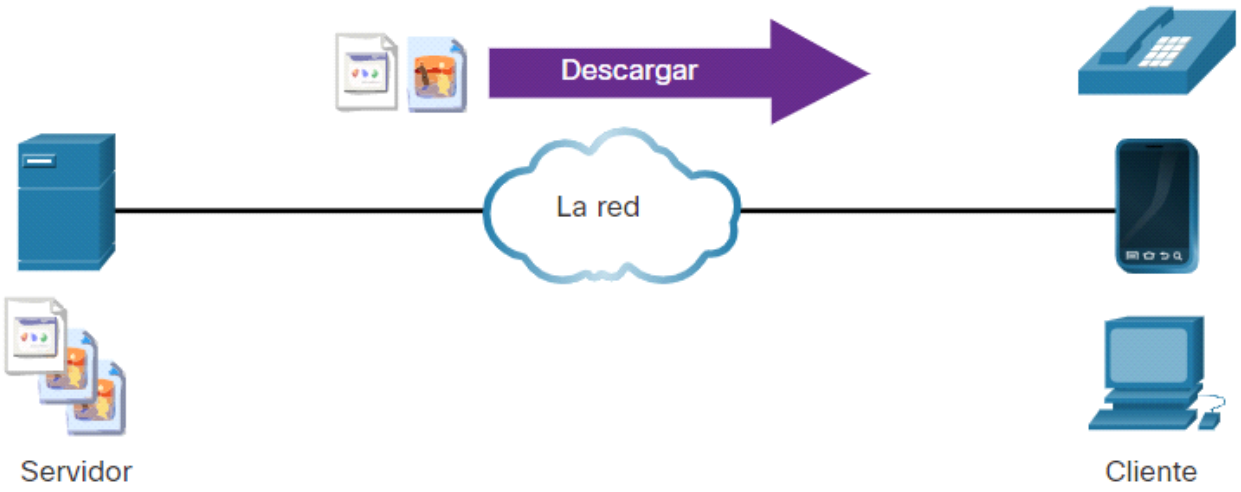
Tutorial Commands linux
https://ubuntu.com/tutorials/command-line-for-beginners#3-opening-a-terminal

Command	Description
mv	Moves or renames files and directories
chmod	Modifies file permissions
chown	Changes the ownership of a file
dd	Copies data from an input to an output
pwd	Displays the name of the current directory
ps	Lists the processes that are currently running in the system
su	Simulates a login as another user or to become a superuser
sudo	Runs a command as a super user, by default, or another named user
grep	Used to search for specific strings of characters within a file or other command outputs. To search through the output of a previous command, **grep** must be piped at the end of the previous command.
ifconfig	Used to display or configure network card related information. If issued without parameters, **ifconfig** will display the current network card(s) configuration. Note: While still widely in use, this command is deprecated. Use **ip address** instead.
apt-get	Used to install, configure and remove packages on Debian and its derivatives. Note: **apt-get** is a user-friendly command line front-end for **dpkg**, Debian's package manager. The combo **dpkg** and **apt-get** is the default package manager system in all Debian Linux derivatives, including Raspbian.
iwconfig	Used to display or configure wireless network card related information. Similar to **ifconfig**, **iwconfig** will display wireless information when issued without parameters.
shutdown	Shuts down the system, **shutdown** can be instructed to perform a number of shut down related tasks, including restart, halt, put to sleep or kick out all currently connected users.
passwd	Used to change the password. If no parameters are provided, **passwd** changes the password for the current user.
cat	Used to list the contents of a file and expects the file name as the parameter. The **cat** command is usually used on text files.
man	Used to display the documentation for a specific command.

Command	Description
ls	Displays the files inside a directory
cd	Changes the current directory
mkdir	Creates a directory under the current directory
cp	Copies files from source to destination
mv	Moves files to a different directory
rm	Removes files
grep	Searches for specific strings of characters within a file or other commands outputs
cat	Lists the contents of a file and expects the file name as the parameter

Client-Server Communications

Los archivos se descargan del servidor al cliente.



Los recursos se almacenan en el servidor.

Un cliente es una combinación de hardware / software que la gente usa directamente.

Ports "well-known ports".

Puerto	Descripción
20/21	Protocolo de transferencia de archivos (FTP)
22	Shell seguro (SSH)
23	Servicio de inicio de sesión remoto Telnet
25	Protocolo simple de transferencia de correo (SMTP)
53	Sistema de nombres de dominio (DNS)
67/68	Protocolo de configuración dinámica de host (DHCP)
69	Protocolo de transferencia de archivos trivial (TFTP)
80	Protocolo de transferencia de hipertexto (HTTP)
110	Protocolo de oficina postal versión 3 (POP3)
123	Protocolo de tiempo de red (NTP)
143	Protocolo de acceso a mensajes de Internet (IMAP)
161/162	Protocolo simple de administración de redes (SNMP)
443	HTTP seguro (HTTPS)

Hardening Devices

The following are basic best practices for device hardening.

- Ensure physical security
- Minimize installed packages
- Disable unused services
- Use SSH and disable the root account login over SSH
- Keep the system updated
- Disable USB auto-detection
- Enforce strong passwords
- Force periodic password changes
- Keep users from re-using old passwords

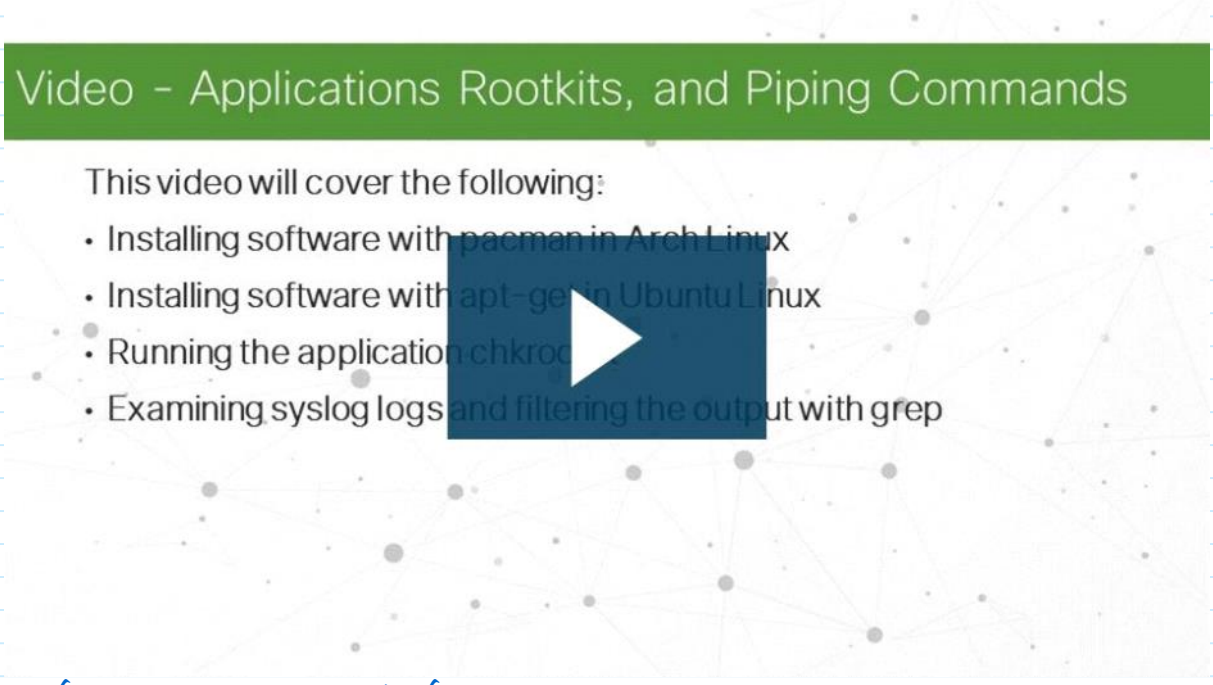
Use octal values to define permissions.

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

Keeping the System Up to Date

Task	Arch	Debian / Ubuntu
Install a package by name	pacman -S	apt install
Remove a package by name	pacman -Rs	apt remove
Update a local package	pacman -Syy	apt-get update
Upgrade all currently installed packages	pacman -Syu	apt-get upgrade

Video - Applications, Rootkits, and Piping Commands



[CyberOps Associate - Working on a Linux Host]

ABSTRACT ABOUT THE CHAPTER

Linux Basics

Linux is a fast, reliable, and small open-source operating system. It requires few hardware resources to run and is highly customizable. It is designed to be used on networks. The Linux kernel is distributed by different organizations with different tools and software packages. A customized version of Linux that is called Security

networks. The Linux kernel is distributed by different organizations with different tools and software packages. A customized version of Linux that is called Security Onion contains software and tools that are designed for use in network security monitoring by cybersecurity analysts. Kali Linux is another customized Linux distribution that has numerous tools that are designed for network security penetration testing.

Working in the Linux Shell

In Linux, the user communicates with the operating system through a GUI or a command-line interface (CLI), or shell. If a GUI is running, the shell is accessed through at terminal application such as xterm or gnome terminal. Linux commands are programs that perform a specific task. The man command, followed by a specific command, provides documentation for that command. It is important to know at least basic Linux commands, file and directory commands, and commands for working with text files. In Linux everything is treated is if it were a file, including the memory, disks, monitor, and directories.

Linux Servers and Clients

Servers are computers that have software installed that enables them to provide services to client computers across the network. Some services provide access to external resources such as files, email, and web pages, to clients upon request. Other services run internally and perform tasks such as log management, memory management, or disk scanning. To enable a computer to provide multiple services, ports are used. A port is a reserved network resource that "listens" for requests by clients. While the port number that is used by a service can be configured, most services listen on default "well-known" ports. Client software applications are designed to communicate with specific types of servers. Web browsers are designed to communicate with web servers by using the HTTP protocol on port 80. FTP

to communicate with web servers by using the HTTP protocol on port 80. FTP clients communicate with FTP servers to transfer files.

Basic Server Administration

In Linux, servers are managed by using configuration files. Various settings can be modified and saved in configuration files. When a service is started, it looks at its configuration file(s) to know how it should run. There is no rule for the way configuration files are written. Configuration file formatting depends on the creator of the server software. Linux devices should be secured by using proven methods to protect the device and administrative access. This is known as hardening devices. One way to harden a device is to maintain passwords, configure enhanced login features, and implement secure remote login with SSH. It is also very important to keep the operating system up to date. Other ways to harden a device are to force periodic password changes, enforce strong passwords, and to prevent reuse of passwords. Finally, Linux clients and servers use logfiles to record the operation of the system and important events. A number of different logfiles are maintained including application logs, event logs, service logs, and system logs. Server logs record activities that are conducted by remote users who access system services. It is important to know the location of different logs in the Linux file system so that they can be accessed and monitored for problems.

The Linux File System

Linux supports a number of different file systems that vary by speed, flexibility, security, size, structure, logic, and more. Some of the file systems that are supported by Linux are ext2, ext3, ext4, NFS, and CDFS. File systems are mounted on partitions and accessed through mounting points, or directories. Windows drive letters are examples of mounting points. The mount command can be used to display details of the file systems that are currently mounted on a Linux computer

letters are examples of mounting points. The mount command can be used to display details of the file systems that are currently mounted on a Linux computer. The root file system is represented by the "/" symbol. It contains all of the files in the computer by default. Linux uses file permissions to control who is permitted to have different types of access to files and directories. Permissions include read (r), write (w), and execute (x). Files and directories have permissions that are assigned for users, groups, and others. The permissions for files and folders are displayed with the ls -l command. This command also displays the links for a file. Hard links create another file with a different name that is linked to the same place in the file system. The owner of the file and the group for the file are also displayed along with the date and time of the last modification to the file. File permissions are powerful features of the Linux file system and can't be violated. Only the root user can override file permissions. Because of the power of the root user, root access should be carefully controlled. Hard links are created with the ln command. Changes to one of the hard-linked files are also made to the original file. Symbolic links, or symlinks, are similar to hard links in that a change to the linked file is reflected in the original file. Symbolic links have several advantages over hard links.

Working with Linux GUI

The X Windows, or X11, system is a basic software framework that includes functions for creating, controlling, and configuring a windows GUI in a point-and-click interface. Different vendors use the X Windows system to create different windows manager GUIs for Linux. Examples of windows managers are Gnome and KDE. The Ubuntu Linux distribution uses Gnome 3 by default. The Gnome 3 desktop consists of the Apps Menu, Ubuntu Dock, Top Bar, Calendar and System Message tray, the Activities area, and the Status Menu.

Working on a Linux Host

Working on a Linux Host

In order to install applications on Linux hosts, programs called package managers are used. Packages are software applications and all of their supporting files. Package managers are extremely helpful for installing complex software applications from centralized package repositories that are accessible over the internet. Different Linux distributions use different package managers. For example, Arch Linux uses pacman, Debian uses dpkg as the base package manager and apt to communicate with dpkg. Ubuntu also uses apt. Package manager CLI commands are used to install, remove, and update software packages. Upgrade commands upgrade all currently installed packages. Package management can also be performed in a GUI. Software processes are instances of computer programs that are running. Multitasking operating systems can run many processes at the same time. Forking is a method that the kernel uses to allow a running process to copy itself. The ps command lists the running processes, top displays information about running processes dynamically, and kill is used to remove, restart, or pause running processes. While Linux is considered to be better protected against malicious software (malware) than other operating systems, it is still susceptible to Trojan horses, worms, and other types of malware. Linux is usually attacked through its services and processes. Out of date software is often vulnerable to attack. Threat actors can probe a device for open ports that are linked to out of date server processes. With this knowledge, attacks can be launched. It is important to keep the operating system and its components and applications up to date. The chkrootkit program is designed to detect rootkit malware. Rootkits are deep level malware programs that are very difficult to detect and remove. They can change the fundamental operation of the operating system itself and can be used to create unauthorized access to systems. Piping commands uses the "|" symbol to chain different commands together by using the output of one command as the input for another.

lunes, 12 de julio de 2021 7:02 p. m.

Chapter 4

lunes, 12 de julio de 2021 7:02 p. m.