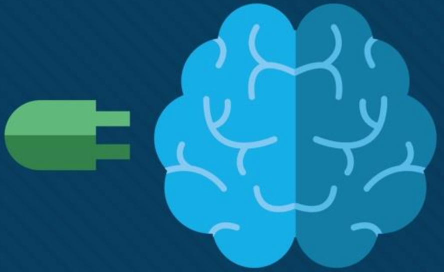


Chapter 3: Linux Operating System

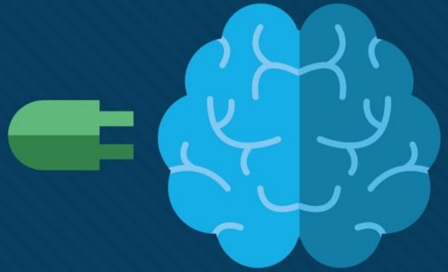
Instructor Materials

Cybersecurity Operations v1.1

Chapter 3: Linux Operating System

Cybersecurity Operations v1.1
Planning Guide

Chapter 3: Linux Operating System



Cybersecurity Operations v1.1

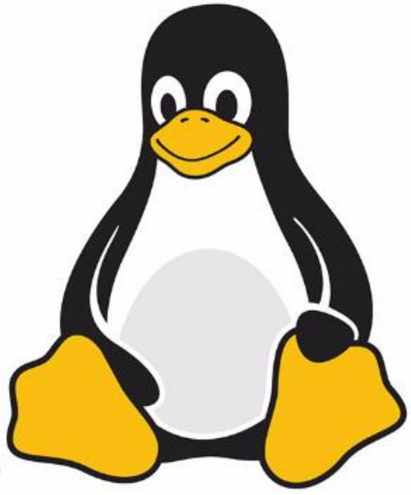
Chapter 3 - Sections & Objectives

- 3.1 Linux Overview
  - Perform basic operations in the Linux shell.
    - Explain why Linux skills are essential for network security monitoring and investigation.
    - Use the Linux shell to manipulate text files.
    - Explain how client-server networks function.
- 3.2 Linux Administration
  - Perform basic Linux administration tasks.
    - Explain how a Linux administrator locates and manipulates security log files..
    - Manage the Linux file system and permissions.
- 3.3 Linux Hosts
  - Perform basic security-related tasks on a Linux host.
    - Explain the basic components of the Linux GUI.
    - Use tools to detect malware on a Linux host.

3.1 Linux Overview

What is Linux?

- Linux is an Open Source operating system created in 1991 and maintained by a community of programmers.
- Open Source means the source programming files, including the kernel, shell, and applications are available for downloading, viewing and modification.
- Linux was designed as a network operating system and is widely used on different platforms including embedded systems.
- There are many different versions or distributions of Linux. A distribution is defined by its kernel, as well as its programs and software packaging.
- Some Linux distributions are free, like CentOS and Fedora. Others like RedHat Enterprise Server, cost money, but include support services.

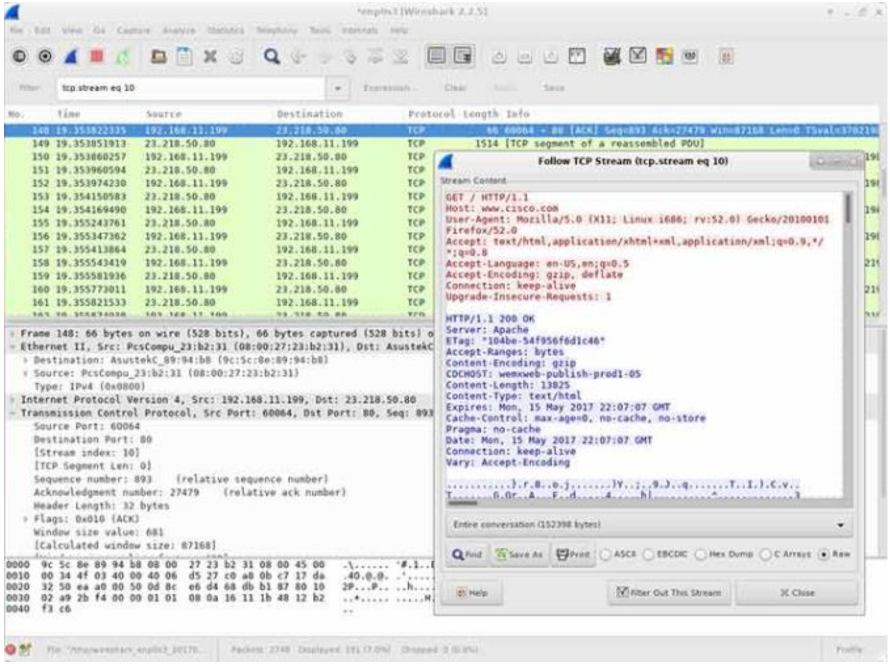


The Value of Linux

- Linux is an operating system of choice in Security Operations Center (SOC).
  - Open source
    - Allows analysts and administrators to tailor-build the OS.
  - Command Line Interface (CLI) is very powerful
    - Enables analysts to perform tasks directly or remotely on a terminal.
  - More user control over the OS
    - Root user or superuser has absolute power over the computer.
      - Modify any aspect of the computer.
      - Precise control over the functions of the computer.
  - Better network communication control
    - Great platform for creating network application.

Linux in the SOC

- A custom security distribution of Linux can be created for the SOC with just the tools needed for the job.
  - Packet Capture (Wireshark)
  - Malware Analysis Tools
  - Intrusion Detection Systems (IDSs)
  - Firewalls
  - Log Managers
  - Security Information and Event Management (SIEM)
  - Ticketing Systems



```
No.  Time          Source          Destination     Protocol Length Info
148 19.353822335  192.168.11.199  23.218.50.80    TCP        66 60064 → 80 [ACK] Seq=893 Ack=27479 Win=87168 Len=0 TSval=370219
149 19.353851913  23.218.50.80    192.168.11.199  TCP      1514 [TCP segment of a reassembled PDU]
150 19.353860257  192.168.11.199  23.218.50.80    TCP
151 19.353960594  23.218.50.80    192.168.11.199  TCP
152 19.353974230  192.168.11.199  23.218.50.80    TCP
153 19.354150583  23.218.50.80    192.168.11.199  TCP
154 19.354169490  192.168.11.199  23.218.50.80    TCP
155 19.355243761  23.218.50.80    192.168.11.199  TCP
156 19.355347362  192.168.11.199  23.218.50.80    TCP
157 19.355413864  23.218.50.80    192.168.11.199  TCP
158 19.355543419  192.168.11.199  23.218.50.80    TCP
159 19.355581936  23.218.50.80    192.168.11.199  TCP
160 19.355773011  192.168.11.199  23.218.50.80    TCP
161 19.355821533  23.218.50.80    192.168.11.199  TCP
```

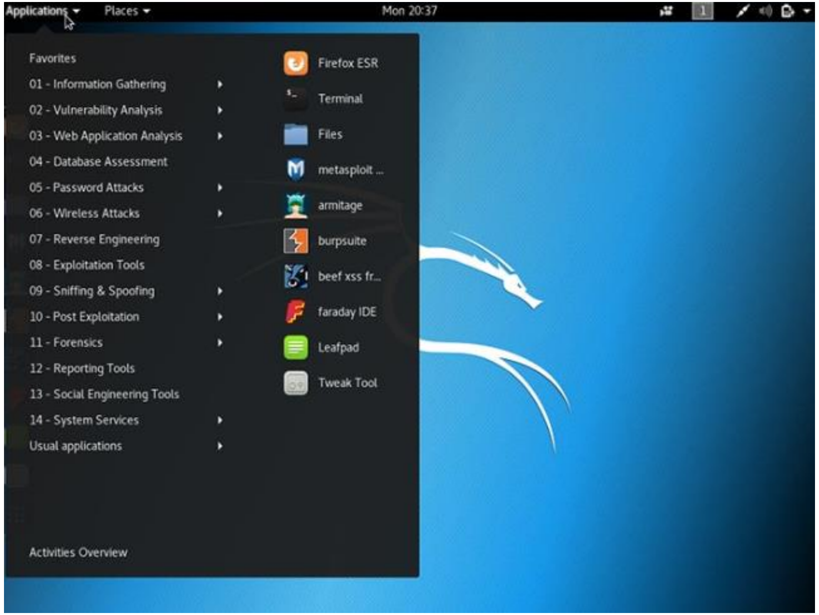
```
Frame 148: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) o
Ethernet II, Src: PcsCompu_23:b2:31 (08:00:27:23:b2:31), Dst: AsustekC
  Destination: AsustekC_89:94:b8 (9c:5c:8e:89:94:b8)
  Source: PcsCompu_23:b2:31 (08:00:27:23:b2:31)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.11.199, Dst: 23.218.50.80
Transmission Control Protocol, Src Port: 60064, Dst Port: 80, Seq: 893
  Source Port: 60064
  Destination Port: 80
  [Stream index: 10]
  [TCP Segment Len: 0]
  Sequence number: 893    (relative sequence number)
  Acknowledgment number: 27479    (relative ack number)
  Header Length: 32 bytes
  Flags: 0x010 (ACK)
  Window size value: 681
  [Calculated window size: 87168]
```

```
0000  9c 5c 8e 89 94 b8 08 00  27 23 b2 31 08 00 45 00   .\...... '#.1..E
0010  00 34 4f 03 40 00 40 06  d5 27 c0 a8 0b c7 17 da   .4O.@.@. .'......
0020  32 50 ea a0 00 50 0d 8c  e6 d4 68 db b1 87 80 10   2P...P.. ..h.....
0030  02 a9 2b f4 00 00 01 01  08 0a 16 11 1b 48 12 b2   ..+..... .....H..
0040  f3 c6                                              ..
```

```
GET / HTTP/1.1
Host: www.cisco.com
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:52.0) Gecko/20100101
Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache
ETag: "104be-54f956f6d1c46"
Accept-Ranges: bytes
Content-Encoding: gzip
CDCHOST: wemxweb-publish-prod1-05
Content-Length: 13825
Content-Type: text/html
Expires: Mon, 15 May 2017 22:07:07 GMT
Cache-Control: max-age=0, no-cache, no-store
Pragma: no-cache
Date: Mon, 15 May 2017 22:07:07 GMT
Connection: keep-alive
Vary: Accept-Encoding

............}.r.8..o.j.......]Y..;..9.J..q.......T..I.).C.v..
```

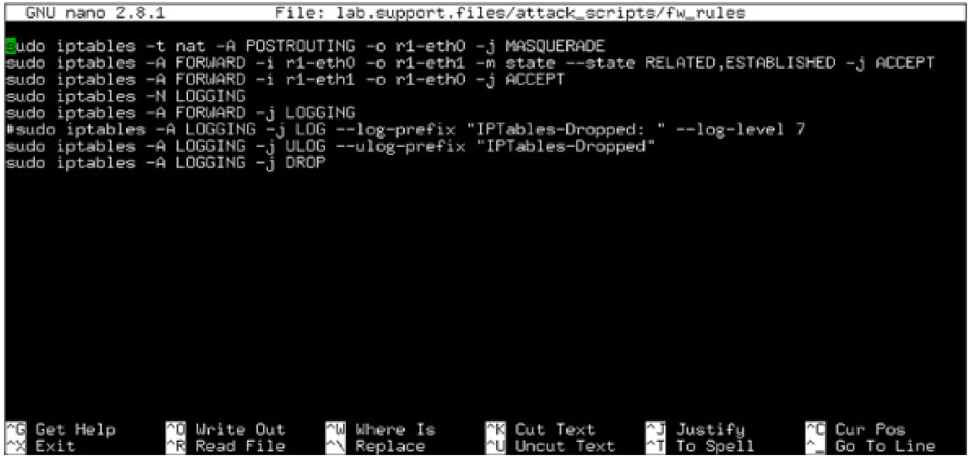
Linux Tools

- Penetration testing tools
  - Process of looking for vulnerabilities.
  - Tool examples:
    - Packet generators
    - Port scanners
    - Proof-of-concept exploits
- Kali Linux distribution groups many penetration tools.



Working with Text Files

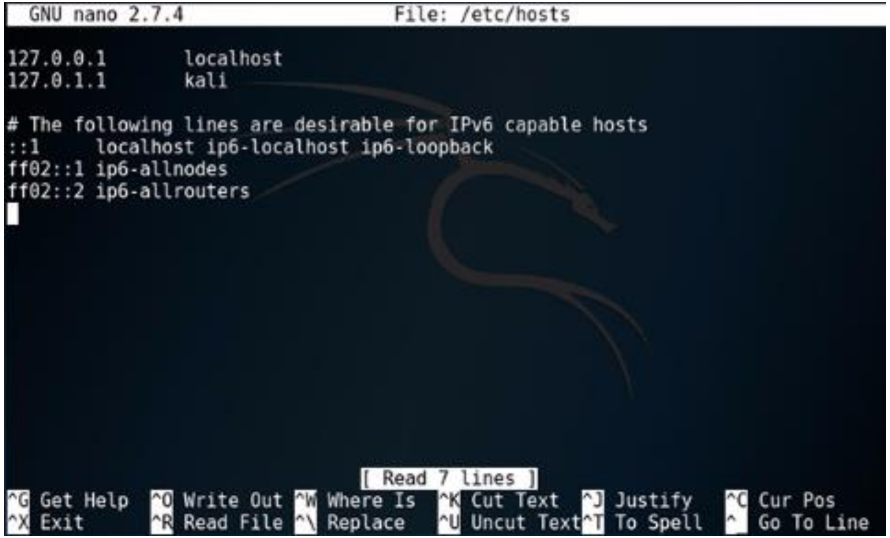
- There are many text editors available in Linux.
- Some text editors are for the CLI only, like vi, vim, and nano.
- Other text editors, like gedit, are GUI-based.
- CLI text editors allow system management remotely, such as via SSH.



```
  GNU nano 2.8.1              File: lab.support.files/attack_scripts/fw_rules

sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i r1-eth1 -o r1-eth0 -j ACCEPT
sudo iptables -N LOGGING
sudo iptables -A FORWARD -j LOGGING
#sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped: " --log-level 7
sudo iptables -A LOGGING -j ULOG --ulog-prefix "IPTables-Dropped"
sudo iptables -A LOGGING -j DROP
```

The Importance of Text Files in Linux

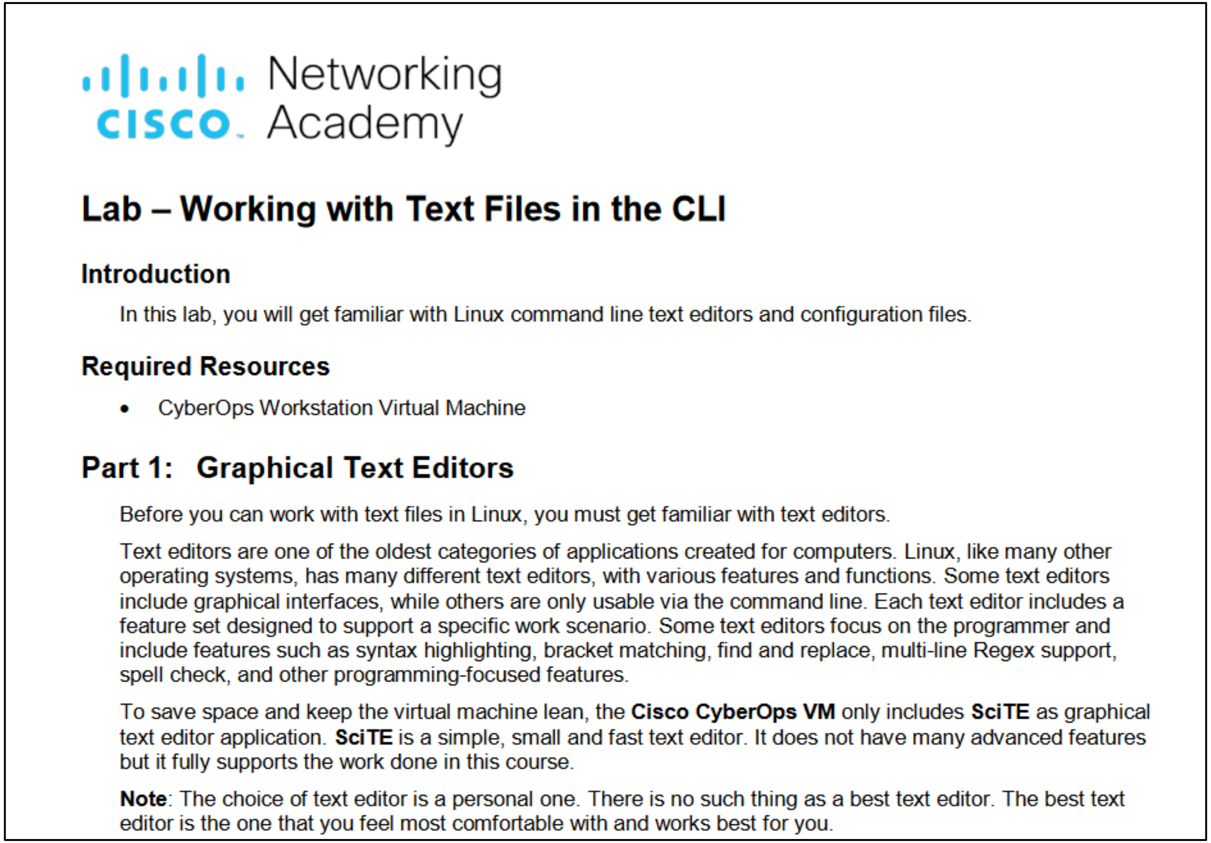
- In Linux, everything is treated as a file, this includes the memory, the disks, the monitor, the files, and the directories.
- The operating system as well as most programs are configured by editing the configuration files which are text files.
- Editing system or application configuration files requires super user (root) privileges. This can be accomplished with the sudo command.



```
  GNU nano 2.7.4                  File: /etc/hosts

127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


                           [ Read 7 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Spell  ^  Go To Line
```

Working in the Linux Shell

Lab – Working with Text Files in the CLI



Networking Academy

Lab – Working with Text Files in the CLI

Introduction

In this lab, you will get familiar with Linux command line text editors and configuration files.

Required Resources

- CyberOps Workstation Virtual Machine

Part 1: Graphical Text Editors

Before you can work with text files in Linux, you must get familiar with text editors.

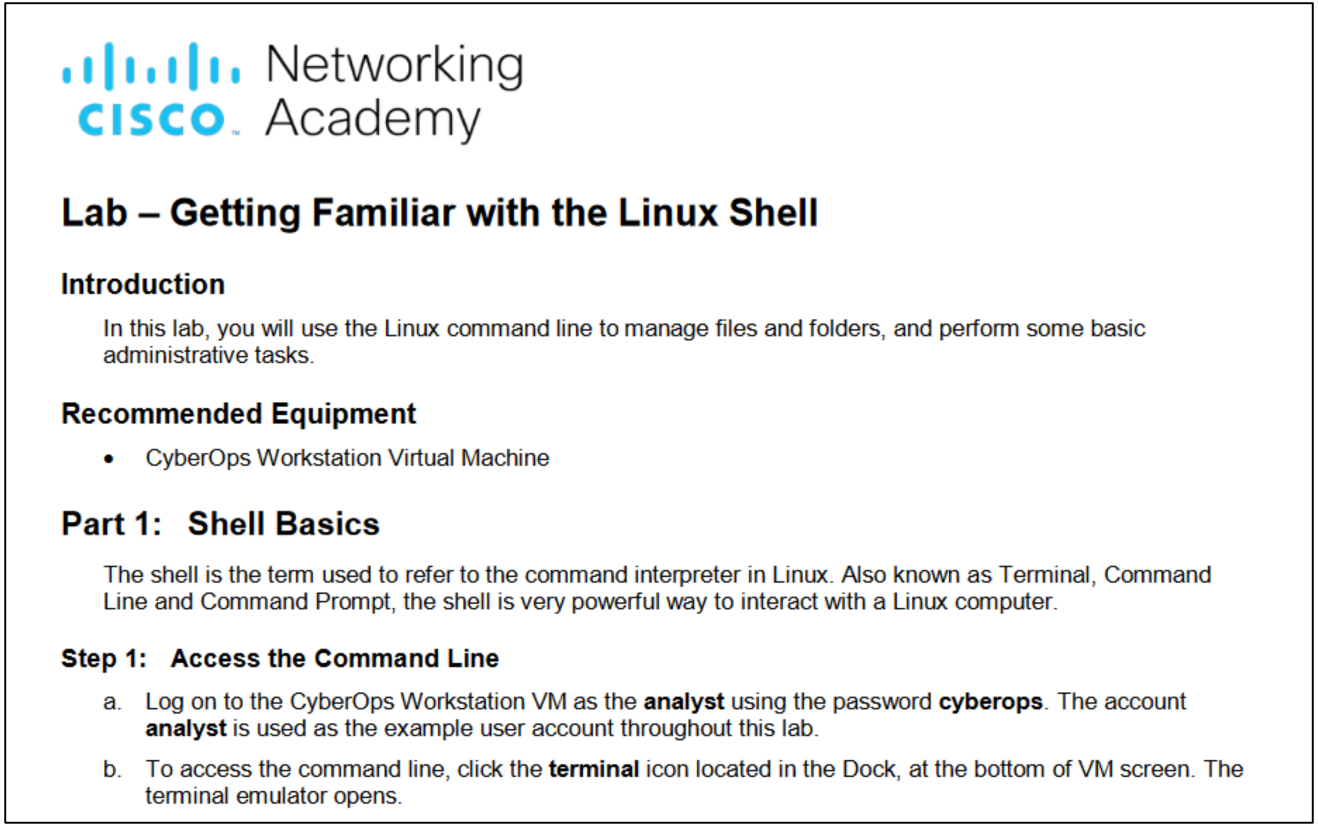
Text editors are one of the oldest categories of applications created for computers. Linux, like many other operating systems, has many different text editors, with various features and functions. Some text editors include graphical interfaces, while others are only usable via the command line. Each text editor includes a feature set designed to support a specific work scenario. Some text editors focus on the programmer and include features such as syntax highlighting, bracket matching, find and replace, multi-line Regex support, spell check, and other programming-focused features.

To save space and keep the virtual machine lean, the **Cisco CyberOps VM** only includes **SciTE** as graphical text editor application. **SciTE** is a simple, small and fast text editor. It does not have many advanced features but it fully supports the work done in this course.

Note: The choice of text editor is a personal one. There is no such thing as a best text editor. The best text editor is the one that you feel most comfortable with and works best for you.

Working in the Linux Shell

Lab – Getting Familiar with the Linux Shell



Networking Academy

Lab – Getting Familiar with the Linux Shell

Introduction

In this lab, you will use the Linux command line to manage files and folders, and perform some basic administrative tasks.

Recommended Equipment

- CyberOps Workstation Virtual Machine

Part 1: Shell Basics

The shell is the term used to refer to the command interpreter in Linux. Also known as Terminal, Command Line and Command Prompt, the shell is very powerful way to interact with a Linux computer.

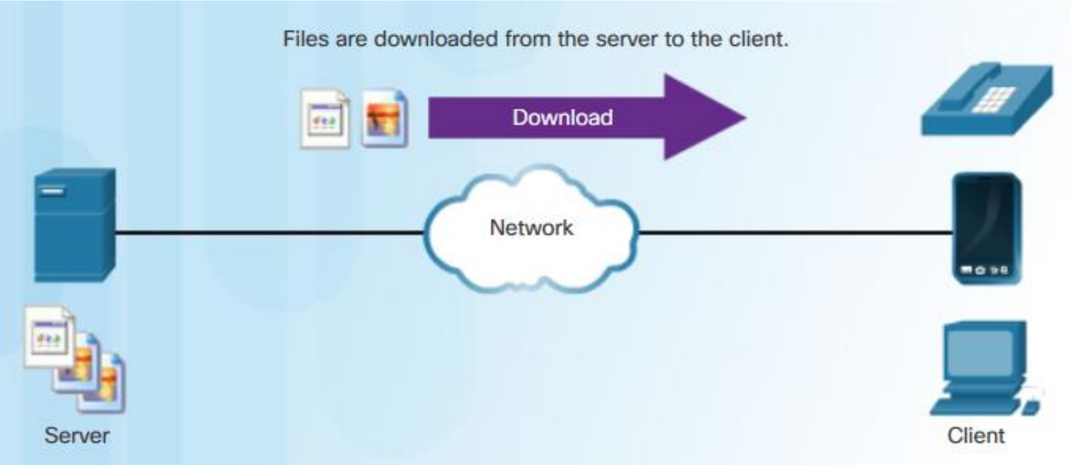
Step 1: Access the Command Line

a. Log on to the CyberOps Workstation VM as the **analyst** using the password **cyberops**. The account **analyst** is used as the example user account throughout this lab.

b. To access the command line, click the **terminal** icon located in the Dock, at the bottom of VM screen. The terminal emulator opens.

An Introduction to Client-Server Communications

- Servers are computers with software installed that enable them to provide services to clients.
- Resources, such as files, email messages, or web pages, are stored on the server.
- Servers can also provide services, such as log management, memory management, and disk scanning.
- The client software is designed to communicate with the server.



Linux Servers and Clients

Servers, Services, and Their Ports

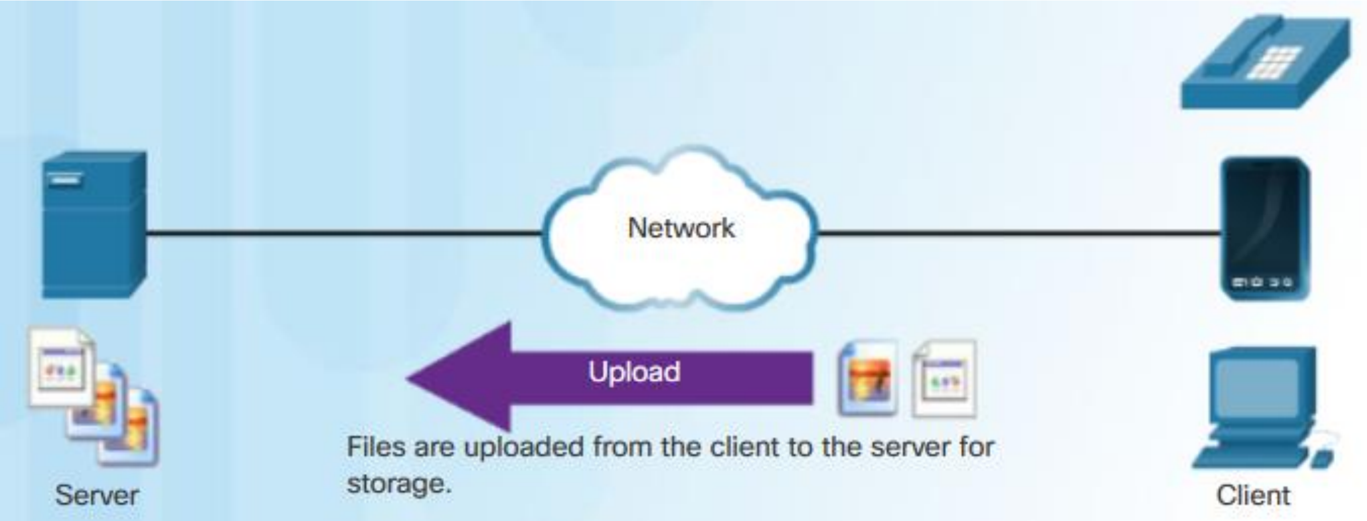
- A port is a reserved network resource used by a service.
- An administrator can assign a port to a specific service or use the default port number.

Default Port Number	Service
21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet remote login service
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
123	Network Time Protocol (HTTP)
143	Internet Message Access Protocol (NTP)
161/162	Simple Network Management Protocol (SNMP)
443	HTTP Secure (HTTPS)

Linux Servers and Clients

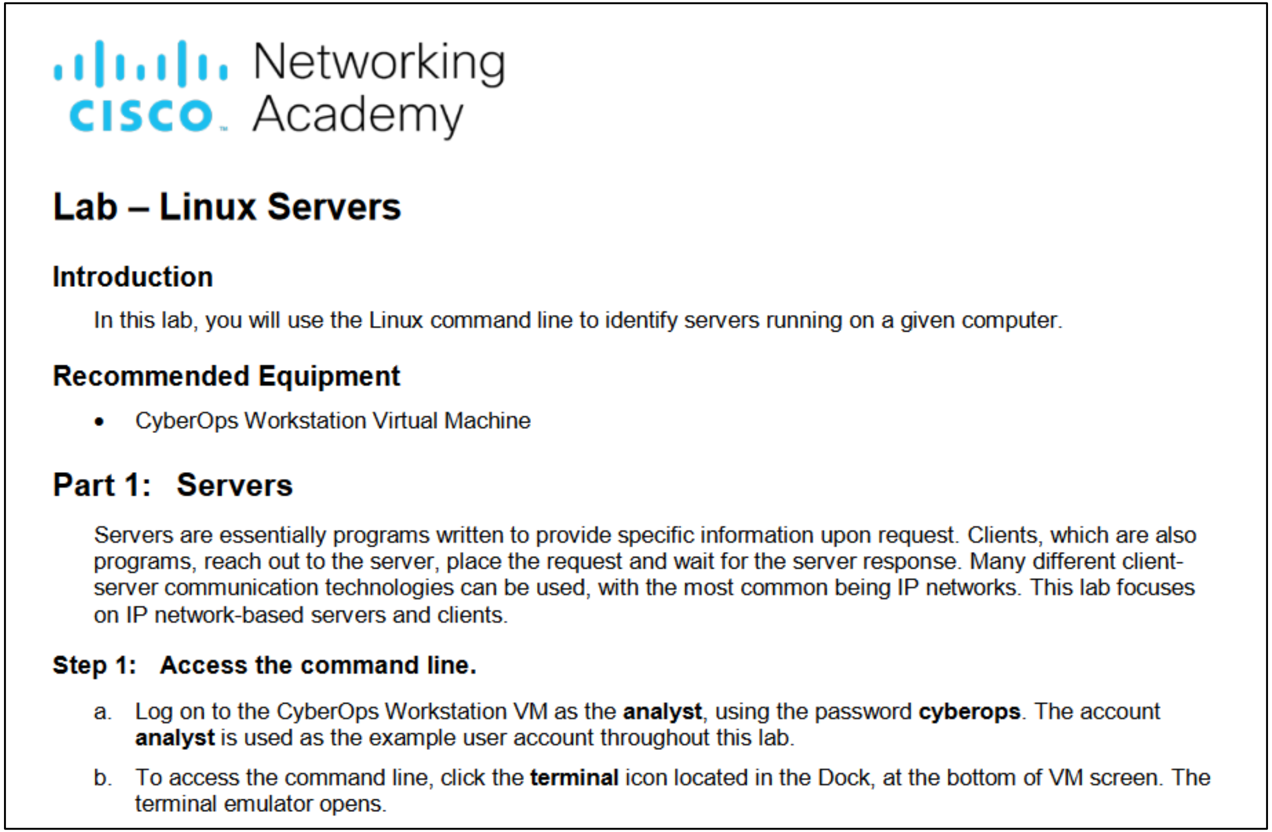
Clients

- Clients are programs or applications designed to communicate with a specific server.
- Client applications are used for a well-defined protocol:
  - File Transfer Protocol (FTP)
  - Hyper Text Transfer Protocol (HTTP)



Files are uploaded from the client to the server for storage.

Lab – Linux Servers



Networking Academy

Lab – Linux Servers

Introduction

In this lab, you will use the Linux command line to identify servers running on a given computer.

Recommended Equipment

- CyberOps Workstation Virtual Machine

Part 1: Servers

Servers are essentially programs written to provide specific information upon request. Clients, which are also programs, reach out to the server, place the request and wait for the server response. Many different client-server communication technologies can be used, with the most common being IP networks. This lab focuses on IP network-based servers and clients.

Step 1: Access the command line.

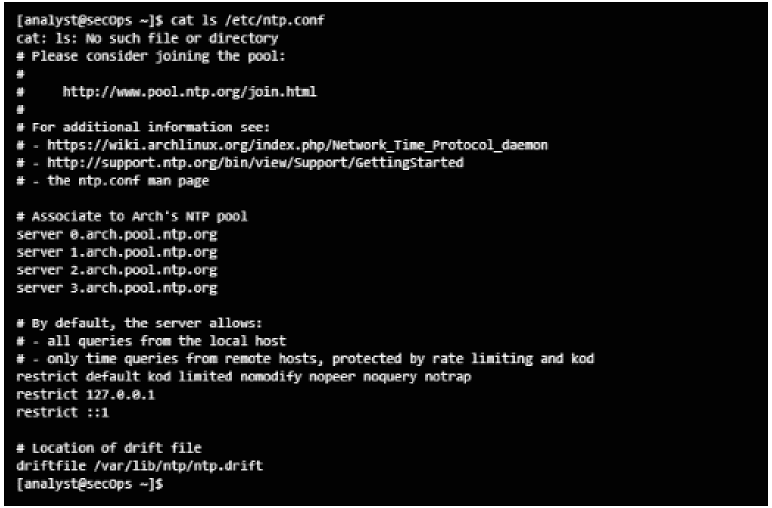
a. Log on to the CyberOps Workstation VM as the **analyst**, using the password **cyberops**. The account **analyst** is used as the example user account throughout this lab.

b. To access the command line, click the **terminal** icon located in the Dock, at the bottom of VM screen. The terminal emulator opens.

3.2 Linux Administration

Service Configuration Files

- Linux Servers are typically configured with text-based configuration files.
- The configuration file defines options for the service, such as port number, location of hosted resources, and client authorization details.
- A server configuration file often consists of important server settings in the form of variables in key=value pairs.
- A server configuration file usually has instructions that begin with a comment like a hash #. Comments are ignored by the software.



```
[analyst@secOps ~]$ cat ls /etc/ntp.conf
cat: ls: No such file or directory
# Please consider joining the pool:
#
#     http://www.pool.ntp.org/join.html
#
# For additional information see:
# - https://wiki.archlinux.org/index.php/Network_Time_Protocol_daemon
# - http://support.ntp.org/bin/view/Support/GettingStarted
# - the ntp.conf man page

# Associate to Arch's NTP pool
server 0.arch.pool.ntp.org
server 1.arch.pool.ntp.org
server 2.arch.pool.ntp.org
server 3.arch.pool.ntp.org

# By default, the server allows:
# - all queries from the local host
# - only time queries from remote hosts, protected by rate limiting and kod
restrict default kod limited nomodify nopeer noquery notrap
restrict 127.0.0.1
restrict ::1

# Location of drift file
driftfile /var/lib/ntp/ntp.drift
[analyst@secOps ~]$
```

Hardening Devices

- 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
- Review logs regularly

Basic Server Administration

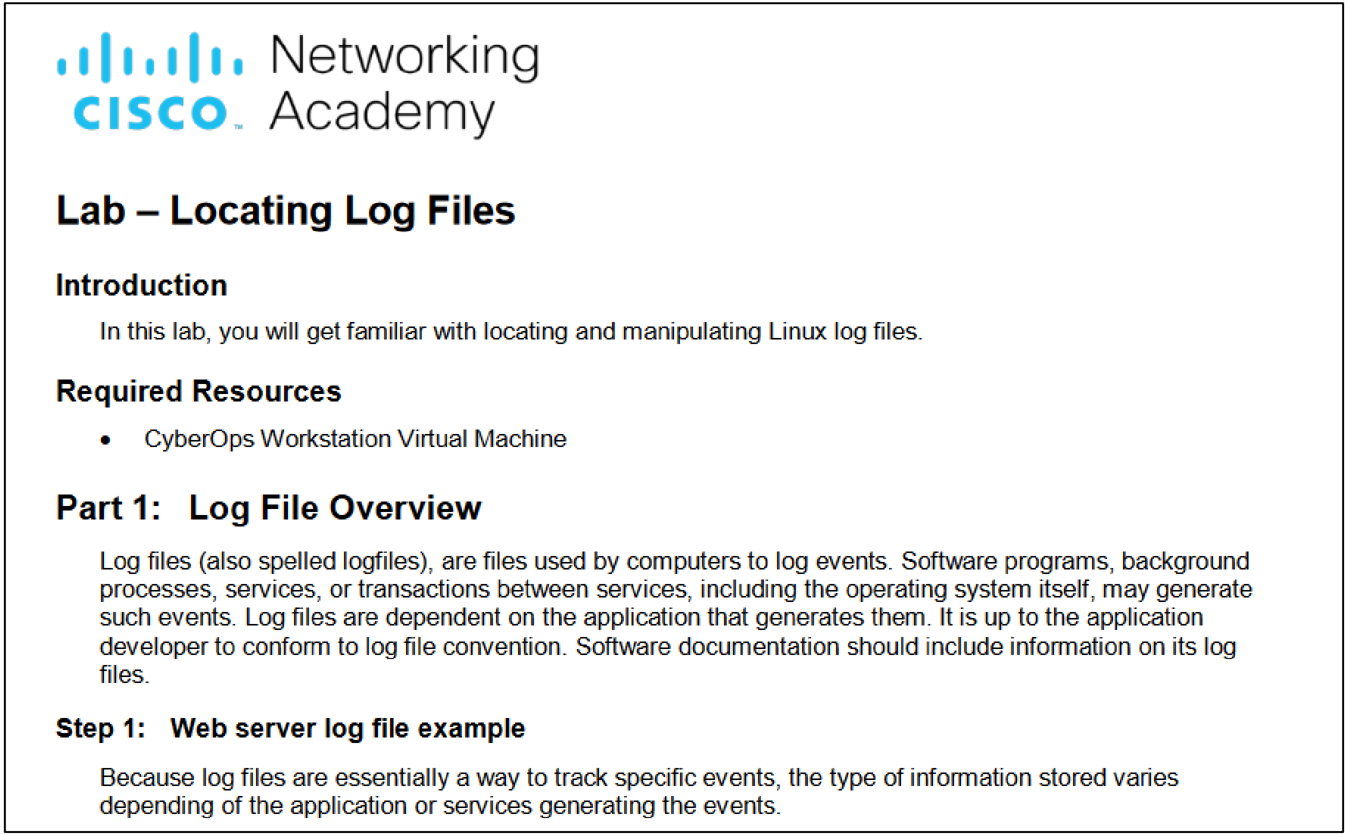
Monitoring Service Logs

- Log files are records to keep track of important computer events.
- Linux has the following types of logs:
  - Application Logs
  - Event Logs
  - Service Logs
  - System Logs

Log	Purpose
/var/log/messages	Used to store informational and non-critical system messages
/var/log/auth.log	Stores all authentication-related events
/var/log/secure	Used by RedHat and CentOS and tracks sudo logins, SSH logins, and errors logged by SSSD
/var/log/boot.log	Stores boot related messages during startup
/var/log/dmesg	Contains kernel ring bugger messages
/var/log/kern.log	Contains information logged by the kernel
/var/log/cron	A service used for scheduling automated tasks in Linux
/var/log/mysqld.log or /var/log/mysql.log	Logs all debug, failure and success messages related to the mysql process and mysqld_safe daemon

Basic Server Administration

Lab – Locating Log Files



Networking Academy

Lab – Locating Log Files

Introduction

In this lab, you will get familiar with locating and manipulating Linux log files.

Required Resources

- CyberOps Workstation Virtual Machine

Part 1: Log File Overview

Log files (also spelled logfiles), are files used by computers to log events. Software programs, background processes, services, or transactions between services, including the operating system itself, may generate such events. Log files are dependent on the application that generates them. It is up to the application developer to conform to log file convention. Software documentation should include information on its log files.

Step 1: Web server log file example

Because log files are essentially a way to track specific events, the type of information stored varies depending of the application or services generating the events.

The Linux File System

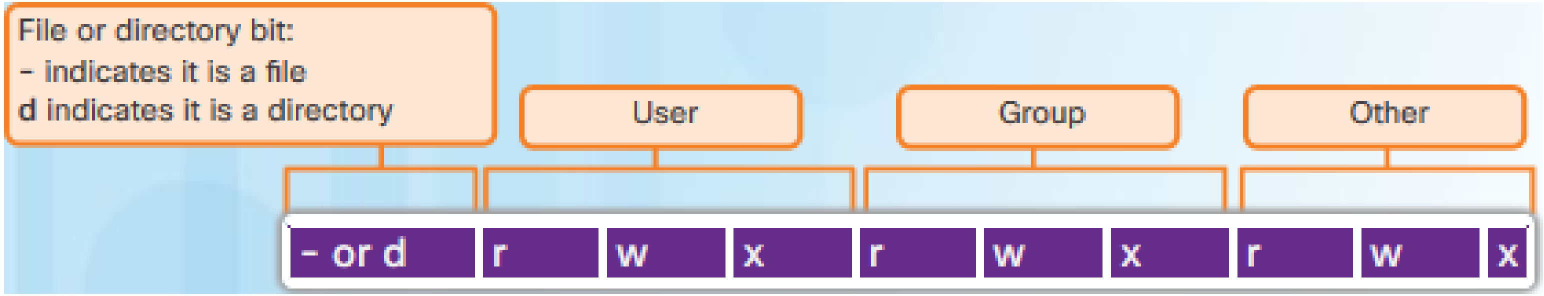
The File System Types in Linux

File System Type	Description
ext2 (second extended file system)	Is the file system of choice for flash-based storage media.
ext3 (third extended file system)	Is an improved successor to ext2 with the additional feature of journaling of all the file system changes.
ext4 (fourth extended file system)	Is designed as a successor to ex3 with increased support file sizes and better performance than ext3.
NFS (Network File System)	Is a network-based file system, allowing file access over the network.
CDFS (Compact Disc File System)	Was created specifically for optical disk media.
Swap File System	Is used when the system runs out of RAM.
HFS+ (Hierarchical File System Plus)	Is the primary file system used by Apple in its Macintosh computers.
APFS (Apple File System)	An updated file system used by Apple devices that provides strong encryption and is optimized for flash and solid state drives.
Master Boot Record (MBR)	Is located in the first sector of a partitioned computer and stores all the information about the way the file system is organized.

Linux Roles and File Permissions

In octal (3bits), per permission (i.e. 111 is a 7 for read, write and execute)

- **User** - the file owner's permission
- **Group** - a group's permission to a file
- **Other** – any user, non-owner's permission to a file
- **Read** – the ability to look at a file's contents
- **Write** – the ability to change a files contents
- **Execute** – the ability to run or launch a file (scripts and programs)



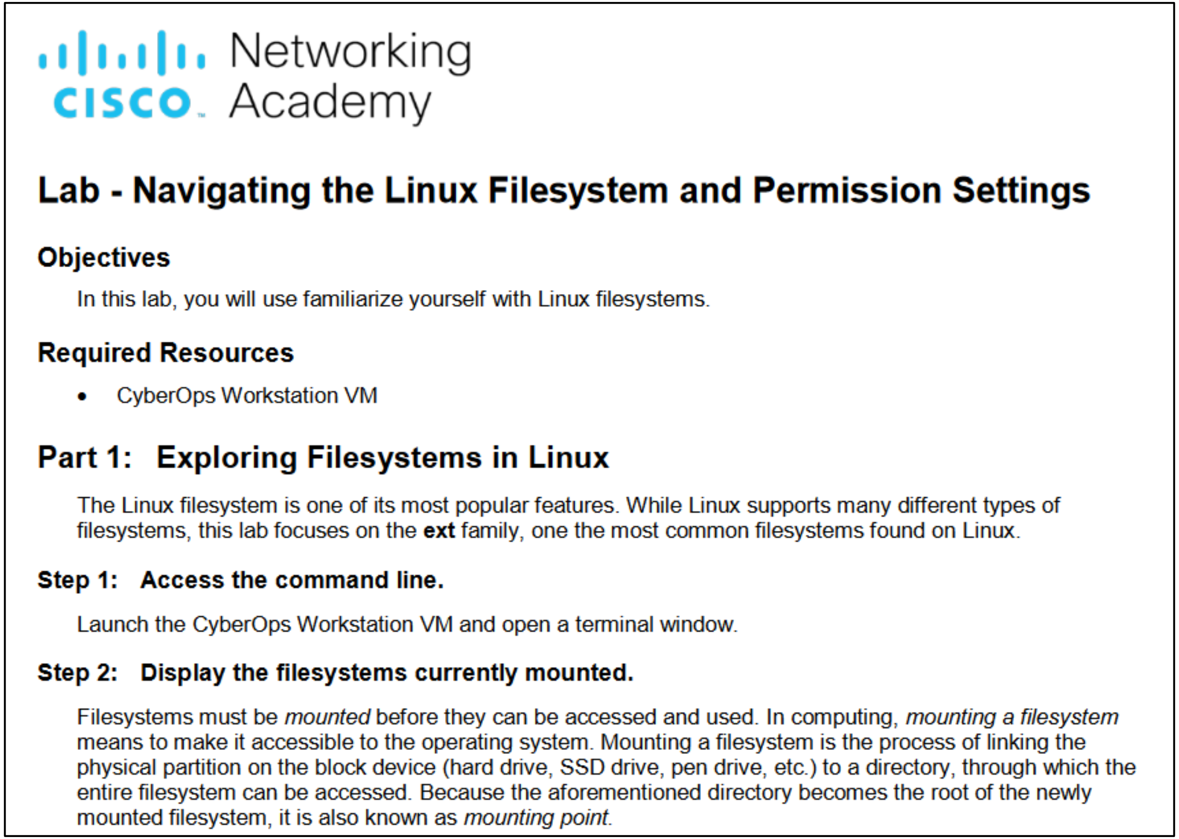
The Linux File System

Hard Links and Symbolic Links

- The *ln* command make links between files.
- Hard Links:
  - Points to the same location as the original file.
  - Changes one file, the other one also changes.
- Symbolic or Soft Links:
  - Uses the *-s* option in the command to create the symbolic link.
  - Delete the original file, the soft link is link to the original file that no longer exists.
- Advantages to symbolic link:
  - Locating hard links is more difficult.
  - Hard links are limited to the file system in which they are created. Symbolic links can link to a file in another file system.
  - Hard links cannot link to a directory, but symbolic links can.

The Linux File System

Lab – Navigating the Linux Filesystem and Permission Settings



Networking Academy

Lab - Navigating the Linux Filesystem and Permission Settings

Objectives

In this lab, you will use familiarize yourself with Linux filesystems.

Required Resources

- CyberOps Workstation VM

Part 1: Exploring Filesystems in Linux

The Linux filesystem is one of its most popular features. While Linux supports many different types of filesystems, this lab focuses on the **ext** family, one the most common filesystems found on Linux.

Step 1: Access the command line.

Launch the CyberOps Workstation VM and open a terminal window.

Step 2: Display the filesystems currently mounted.

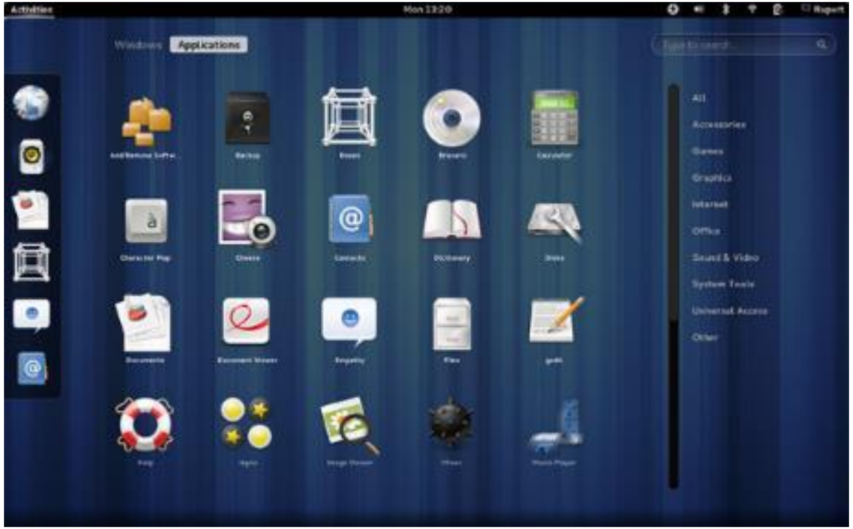
Filesystems must be *mounted* before they can be accessed and used. In computing, *mounting a filesystem* means to make it accessible to the operating system. Mounting a filesystem is the process of linking the physical partition on the block device (hard drive, SSD drive, pen drive, etc.) to a directory, through which the entire filesystem can be accessed. Because the aforementioned directory becomes the root of the newly mounted filesystem, it is also known as *mounting point*.

3.3 Linux Hosts

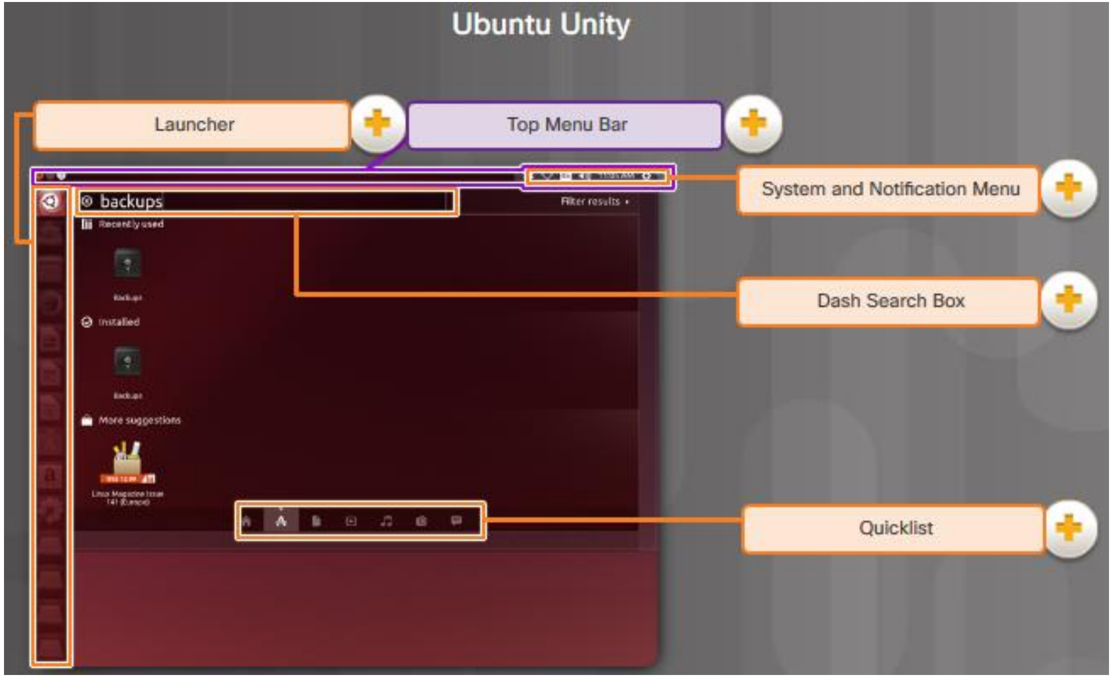
Working with the Linux GUI

X Windows System

- X Window System is the framework for the Linux GUI also known as X and X11.
- Functions for drawing and moving the window, as well as interacting with the mouse and keyboard.
- X works as a server and can send the graphical window over a network to a remote computer.
- X does not specify the user interface or desktop. That is left to a window manager to define the look and feel of the GUI.
- Gnome and KDE are examples of popular Linux window managers.



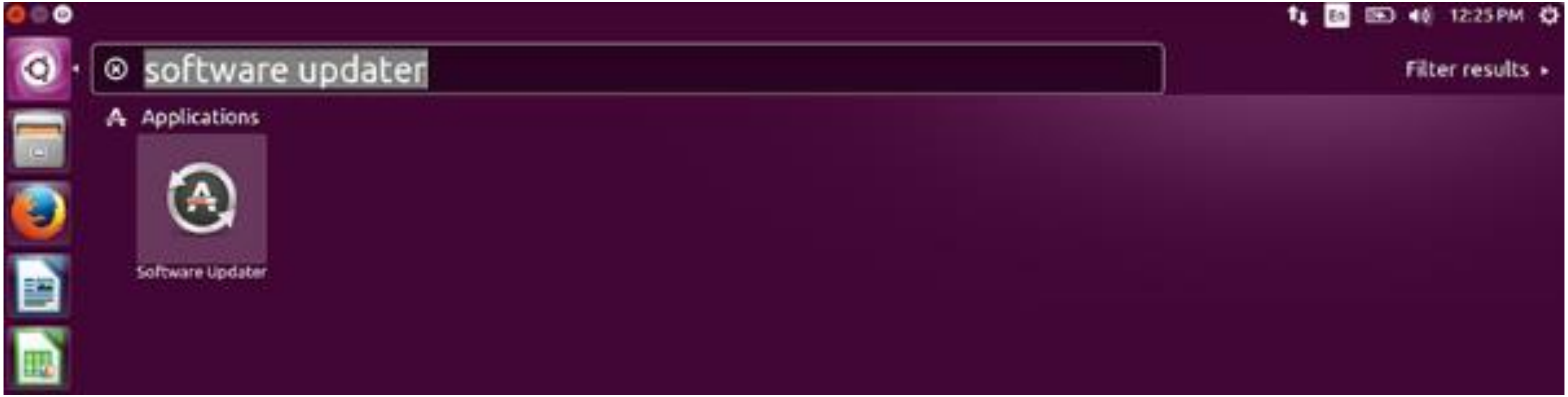
The Linux GUI



- **Top Menu Bar** – currently running application
- **Launcher** – serves as the application launcher and switcher
- **Quicklist** - Right-click any application hosted on the Launcher to access a short list of tasks the application can perform.
- **Dash Search Box** - holds the Search tool and a list of recently used applications.
- **System and Notification Menu** – Can be used to switch users, shut down your computer, control the volume level, or change network settings.

Installing and Running Applications on a Linux Host

- The Installation and removal of programs in Linux is simplified by using a package manager.
- Linux package managers maintain lists of available software and their dynamic library dependencies and requirements.
- Popular package managers are APT for Debian packages (dpkg) and Yum for RedHat packages (rpm).



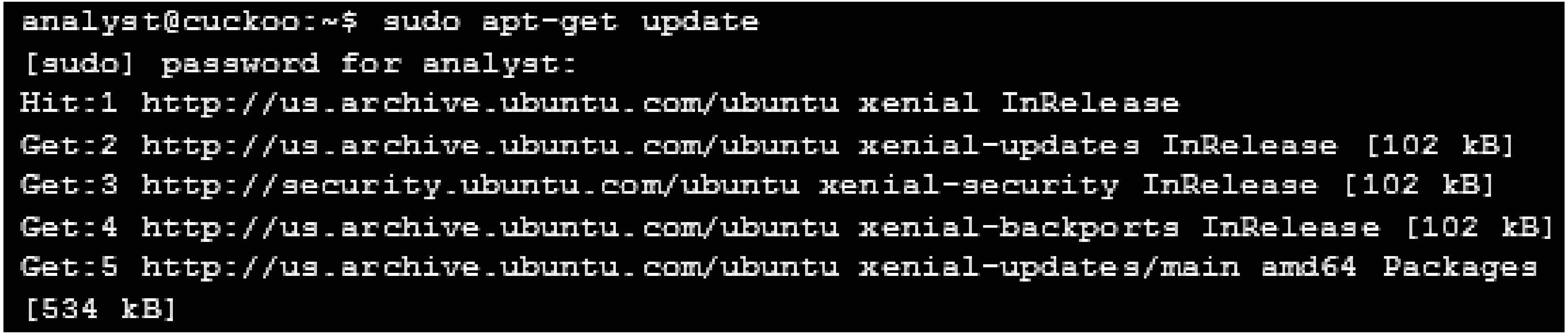
software updater

Working on a Linux Host

Keeping the System Up to Date

- **apt-get update** – downloads the list of available software from the distribution repository and updates the local package database.

- **apt-get upgrade** – downloads and upgrades all of the installed software applications on the system.



```
analyst@cuckoo:~$ sudo apt-get update
[sudo] password for analyst:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages
[534 kB]
```

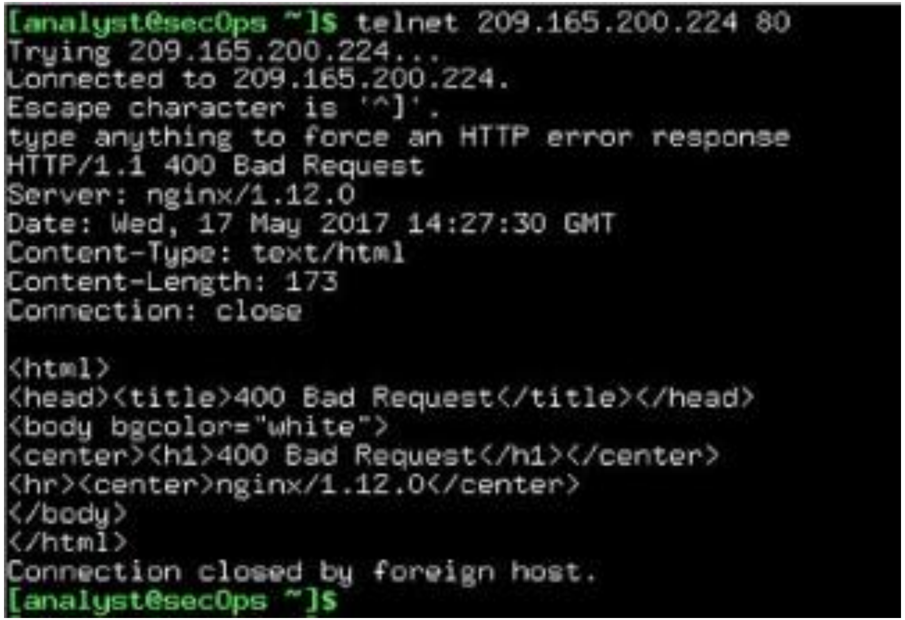
Working on a Linux Host

Processes and Forks

- A process is a running instance of a computer program. Multitasking operating systems can execute many processes at the same time.
- Forking is a method that the kernel uses to allow a process to create a copy of itself to provide process scalability.
- Some commands to manage processes:
  - **ps** – list processes running on the system
  - **top** – list running processes dynamically
  - **kill** – modify the behavior of a specific process, such as remove, restart or pause a process

Malware on a Linux Host

- Linux is generally considered more resistant to malware than other operating systems but it is still not immune.
- A Linux server is only as secure as the programming behind its services and applications.

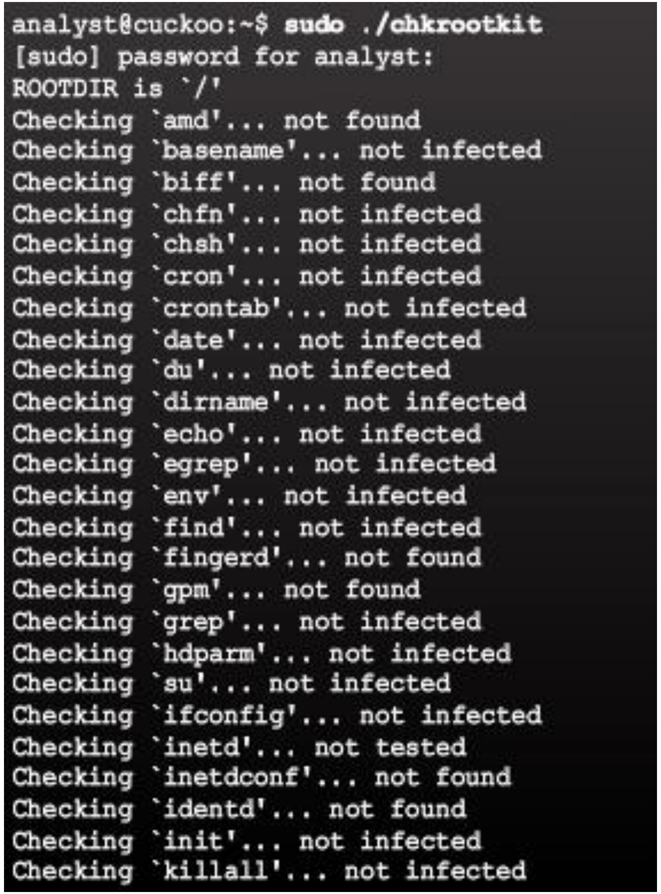


```
[analyst@secOps ~]$ telnet 209.165.200.224 80
Trying 209.165.200.224...
Connected to 209.165.200.224.
Escape character is '^]'.
type anything to force an HTTP error response
HTTP/1.1 400 Bad Request
Server: nginx/1.12.0
Date: Wed, 17 May 2017 14:27:30 GMT
Content-Type: text/html
Content-Length: 173
Connection: close

<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.12.0</center>
</body>
</html>
Connection closed by foreign host.
[analyst@secOps ~]$
```

Working on a Linux Host

Rootkit Check

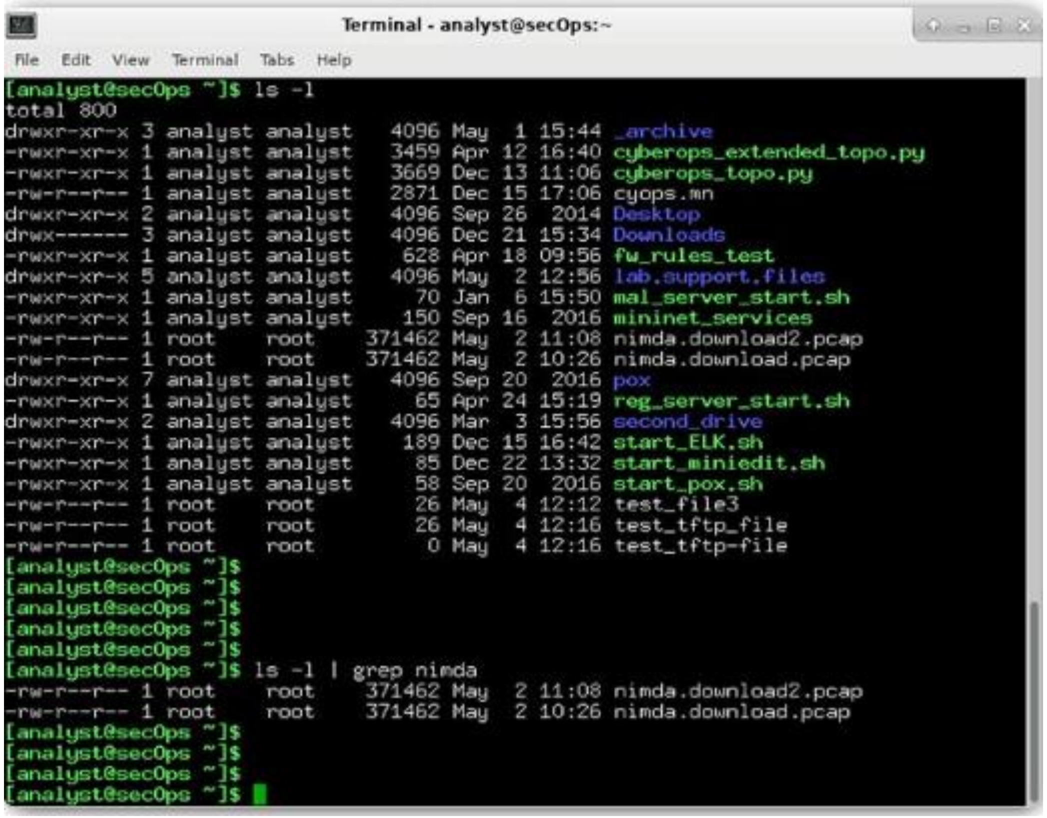
- Rootkits are installed into the operating system kernel and are often used to establish hidden backdoors.
- chkrootkit is a program that will check for rootkits and remove them.
- Rootkit removal can be complicated and often impossible, especially in cases where the rootkit resides in the kernel; re-installation of the operating system is usually the only real solution to the problem.



```
analyst@cuckoo:~$ sudo ./chkrootkit
[sudo] password for analyst:
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
```

Piping Commands

- Many commands can be combined to perform more complex tasks by a technique known as piping.
- the pipe (|)
- Piping consists of chaining commands together, feeding the output of one command into the input of another.



```
[analyst@secOps ~]$ ls -l
total 800
drwxr-xr-x 3 analyst analyst   4096 May  1 15:44 .archive
-rwxr-xr-x 1 analyst analyst   3459 Apr 12 16:40 cyberops_extended_topo.py
-rwxr-xr-x 1 analyst analyst   3669 Dec 13 11:06 cyberops_topo.py
-rw-r--r-- 1 analyst analyst   2871 Dec 15 17:06 cyops.mn
drwxr-xr-x 2 analyst analyst   4096 Sep 26  2014 Desktop
drwx------ 3 analyst analyst   4096 Dec 21 15:34 Downloads
-rwxr-xr-x 1 analyst analyst    628 Apr 18 09:56 fw_rules_test
drwxr-xr-x 5 analyst analyst   4096 May  2 12:56 lab.support.files
-rwxr-xr-x 1 analyst analyst     70 Jan  6 15:50 mal_server_start.sh
-rwxr-xr-x 1 analyst analyst    150 Sep 16  2016 mininet_services
-rw-r--r-- 1 root    root    371462 May  2 11:08 nimda.download2.pcap
-rw-r--r-- 1 root    root    371462 May  2 10:26 nimda.download.pcap
drwxr-xr-x 7 analyst analyst   4096 Sep 20  2016 pox
-rwxr-xr-x 1 analyst analyst     65 Apr 24 15:19 reg_server_start.sh
drwxr-xr-x 2 analyst analyst   4096 Mar  3 15:56 second_drive
-rwxr-xr-x 1 analyst analyst    189 Dec 15 16:42 start_ELK.sh
-rwxr-xr-x 1 analyst analyst     85 Dec 22 13:32 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst     58 Sep 20  2016 start_pox.sh
-rw-r--r-- 1 root    root        26 May  4 12:12 test_file3
-rw-r--r-- 1 root    root        26 May  4 12:16 test_tftp_file
-rw-r--r-- 1 root    root         0 May  4 12:16 test_tftp-file
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep nimda
-rw-r--r-- 1 root    root    371462 May  2 11:08 nimda.download2.pcap
-rw-r--r-- 1 root    root    371462 May  2 10:26 nimda.download.pcap
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$
[analyst@secOps ~]$
```

Video Demonstration- Applications, Rootkits and Piping Commands

- Arch Linux uses the pacman package manager.
  - The command mlocate helps with file searching.
- Ubuntu Linux uses APT package manager.
  - chkrootkit – program to check for rootkits
- Pipe is useful for taking the output from one program, and sending it to the input for another program.

Video Demonstration | Applications, Rootkits, and Piping Commands

3.4 Chapter Summary

Chapter Summary

Summary

- Linux is open source operating system that can be customized and was designed to be connected to the network.
- Linux operation system is used in a SOC environment because it allows for more user and network control.
- Linux tools, such as packet capture, analysis, and penetration testing, are used for security monitoring and investigation.
- Using the Linux shell to work with directories and files including: create, modify, copy, and move files.
- Command line text editors allow users to perform administrative tasks remotely.
- Super user or root access is required to manage system configuration files. All the configuration files are text files.
- Servers are computers with software installed that allows them to provide services to clients.

Summary (Cont.)

- A port is a reserved network resource used by a service.
- Clients are programs or applications designed to communicate with a specific server.
- Services are managed with text-based configuration files.
- Device hardening involves using proven methods of securing devices and protect administrative access.
- The types and location of services logs used for monitoring purposes.
- Linux file system types include: ext2, ext3, ext4, NFS, CDFS, and HFSF+.
- A file permissions consist of the user's, group's and other's, and whether or not they have read, write, and execute permissions.
- A hard link is a type of file that points to the same inode as the original file. A symbolic link, is similar to a hard link except that it points to another file's filename.

Summary (Cont.)

- X Window System is the framework for the Linux GUI also known as X and X11. X works a server.
- The GUI is not required on a Linux system but is considered more user friendly.
- Installing and running applications is made easy using a package manager.
- The system is kept up to date with apt-get update and apt-get upgrade.
- Viewing the current processes and forks running in memory.
- A Linux server is only as secure as the programming behind its services and applications.
- Using chkrootkit to check the computer for known rootkits.
- Using piping to chain commands together, feeding one command output into the input of another command.

Chapter 3

New Terms and Commands

- client
- Compact Disc File System (CDFS)
- configuration file
- device hardening
- distro
- ext2
- ext3
- ext4
- forking
- hard link
- Hierarchical File System Plus (HFS+)
- intrusion detection system (IDS)
- journal
- Kali Linux
- Linux
- log files
- mounting
- Network File System (NFS)
- patch
- PenTesting
- piping
- port
- rookit
- server
- Snort
- superuser
- swap file system
- symbolic link
- terminal emulator
- X Window System

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECFND - Understanding Cisco Cybersecurity Fundamentals:

- Domain 4: Host Based Analysis
  - 4.2 Define the following terms as they pertain to Linux:
    - Processes
    - Forks
    - Permissions
    - Symlinks
    - Daemon
  - 4.4 Interpret the following operating system log data to identify an event:
    - Unix based syslog
    - Apache Access Logs
    - IIS Access Logs

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-255 SECOPS - Implementing Cisco Cybersecurity Operations:

- Domain 1: Endpoint Threat Analysis & Computer Forensics
  - 1.5 Define the following terms as they pertain to the Linux file system:
    - EXT4
    - Journaling
    - MBR
    - Swap File System
    - MAC

cisco