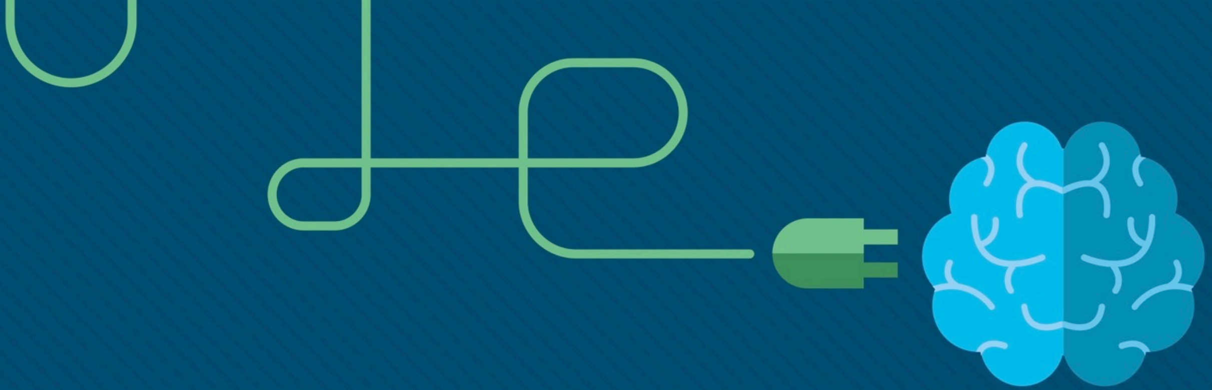


Chapter 2: Linux Operating System

Information Security

Dr. Ayman Aljarbouh

Chapter 2 - Sections & Objectives

- 2.1 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.
- 2.2 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.
- 2.3 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.

Chapter 2 - Sections & Objectives

- 2.1 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.
- 2.2 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.
- 2.3 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.

Today

2.1 Linux Overview

Module Objectives

Module Title: Linux Overview

Module Objective: Perform basic operations in the Linux shell.

Topic Title	Topic Objective
Linux Basics	Explain why Linux skills are essential for network security monitoring and investigation.
Working in the Linux Shell	Use the Linux shell to manipulate text files.
Linux Servers and Clients	Explain how client-server networks function.

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.
- Linux is part of several platforms and can be found on devices anywhere from wristwatches to supercomputers.
- Linux is designed to be connected to the network, which makes it much simpler to write and use network-based applications.
- A Some Linux distributions are free, like CentOS and Fedora. Others like RedHat Enterprise Server, cost money, but include support services.

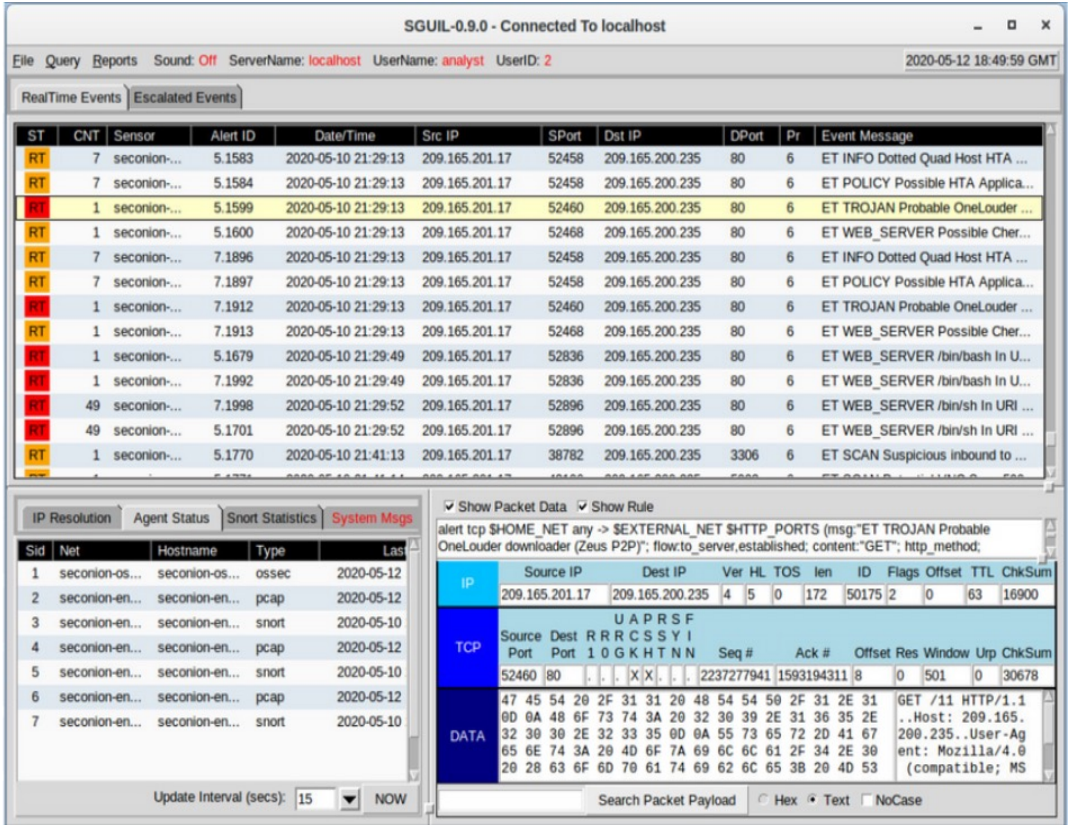
The Value of Linux

Linux is often the operating system of choice in the Security Operations Center (SOC).

- **Linux is open source -** Any person can acquire Linux at no charge and modify it to fit specific needs.
- **The Linux CLI is very powerful -** The Linux Command Line Interface (CLI) enables analysts to perform tasks remotely.
- **The user has more control over the OS -** The administrator user in Linux, known as superuser, can modify any aspect of the computer with a few keystrokes.
- **It allows for better network communication control -** Control is an inherent part of Linux.

Linux in the SOC

- The flexibility provided by Linux is a great feature for the SOC. The entire operating system can be tailored to become the perfect security analysis platform.
- Sguil is the cybersecurity analyst console in a special version of Linux called Security Onion.
- Security Onion is an open source suite of tools that work together for network security analysis.



SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: analyst UserID: 2 2020-05-12 18:49:59 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion-...	5.1583	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion-...	5.1584	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion-...	5.1599	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLouder ...
RT	1	seconion-...	5.1600	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	7	seconion-...	7.1896	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion-...	7.1897	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion-...	7.1912	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLouder ...
RT	1	seconion-...	7.1913	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	1	seconion-...	5.1679	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	1	seconion-...	7.1992	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash In U...
RT	49	seconion-...	7.1998	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	49	seconion-...	5.1701	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh In URI ...
RT	1	seconion-...	5.1770	2020-05-10 21:41:13	209.165.201.17	38782	209.165.200.235	3306	6	ET SCAN Suspicious inbound to ...

IP Resolution | Agent Status | Snort Statistics | System Msgs

Sid	Net	Hostname	Type	Las
1	seconion-os...	seconion-os...	ossec	2020-05-12
2	seconion-en...	seconion-en...	pcap	2020-05-12
3	seconion-en...	seconion-en...	snort	2020-05-10
4	seconion-en...	seconion-en...	pcap	2020-05-12
5	seconion-en...	seconion-en...	snort	2020-05-10
6	seconion-en...	seconion-en...	pcap	2020-05-12
7	seconion-en...	seconion-en...	snort	2020-05-10

Update Interval (secs): 15 NOW

☑ Show Packet Data ☑ Show Rule

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN Probable
OneLouder downloader (Zeus P2P)"; flow:to_server,established; content:"GET"; http_method;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
	209.165.201.17	209.165.200.235	4	5	0	172	50175	2	0	63	16900

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
	52460	80	.	.	.	X	X	.	.	.	2237277941	1593194311	8	0	501	0	30678

DATA

```
47 45 54 20 2F 31 31 20 48 54 54 50 2F 31 2E 31   GET /11 HTTP/1.1
0D 0A 48 6F 73 74 3A 20 32 30 39 2E 31 36 35 2E   ..Host: 209.165.
32 30 30 2E 32 33 35 0D 0A 55 73 65 72 2D 41 67   200.235..User-Ag
65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 30   ent: Mozilla/4.0
20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D 53    (compatible; MS
```

Search Packet Payload ○ Hex ● Text □ NoCase

Linux in the SOC (Contd.)

The following table lists a few tools that are often found in a SOC:

SOC Tool	Description
Network packet capture software	• A crucial tool for a SOC analyst as it makes it possible to observe and understand every detail of a network transaction. • Wireshark is a popular packet capture tool.
Malware analysis tools	• These tools allow analysts to safely run and observe malware execution without the risk of compromising the underlying system.
Intrusion detection systems (IDSs)	• These tools are used for real-time traffic monitoring and inspection. • If any aspect of the currently flowing traffic matches any of the established rules, a pre-defined action is taken.

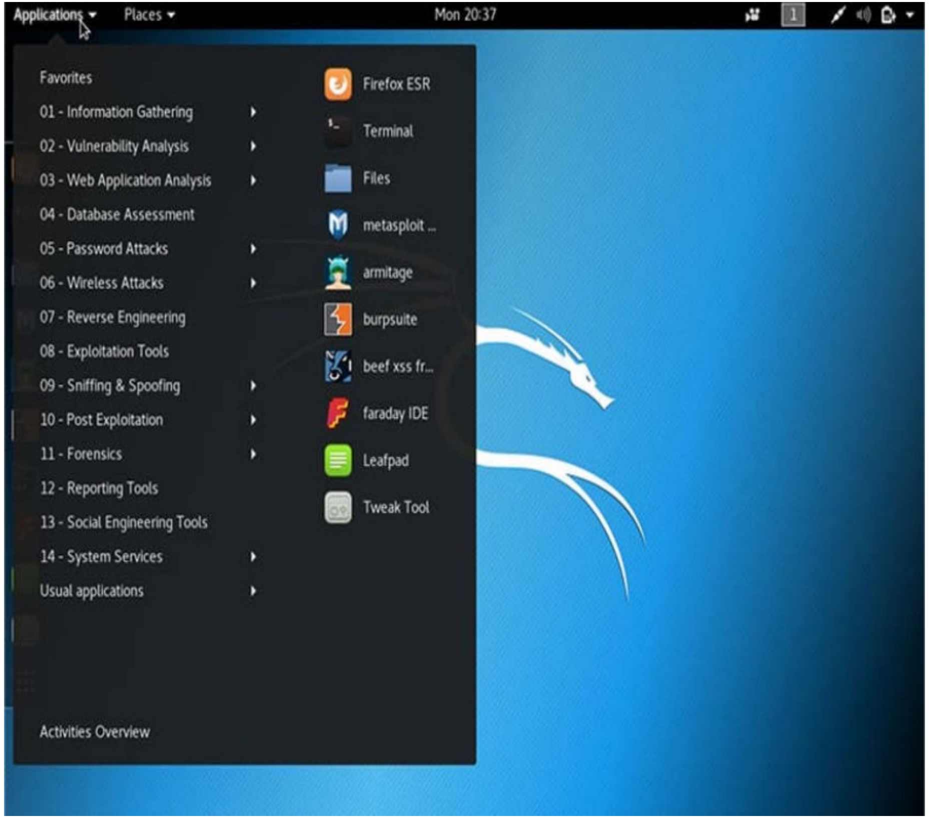
Linux Basics

Linux in the SOC (Contd.)

SOC Tool	Description
Firewalls	• This software is used to specify, based on pre-defined rules, whether traffic is allowed to enter or leave a network or device.
Log managers	• Log files are used to record events. • Because a network can generate a very large number of log entries, log manager software is employed to facilitate log monitoring.
Security information and event management (SIEM)	• SIEMs provide real-time analysis of alerts and log entries generated by network appliances such as IDSs and firewalls.
Ticketing systems	• Task ticket assignment, editing, and recording is done through a ticket management system. Security alerts are often assigned to analysts through a ticketing system.

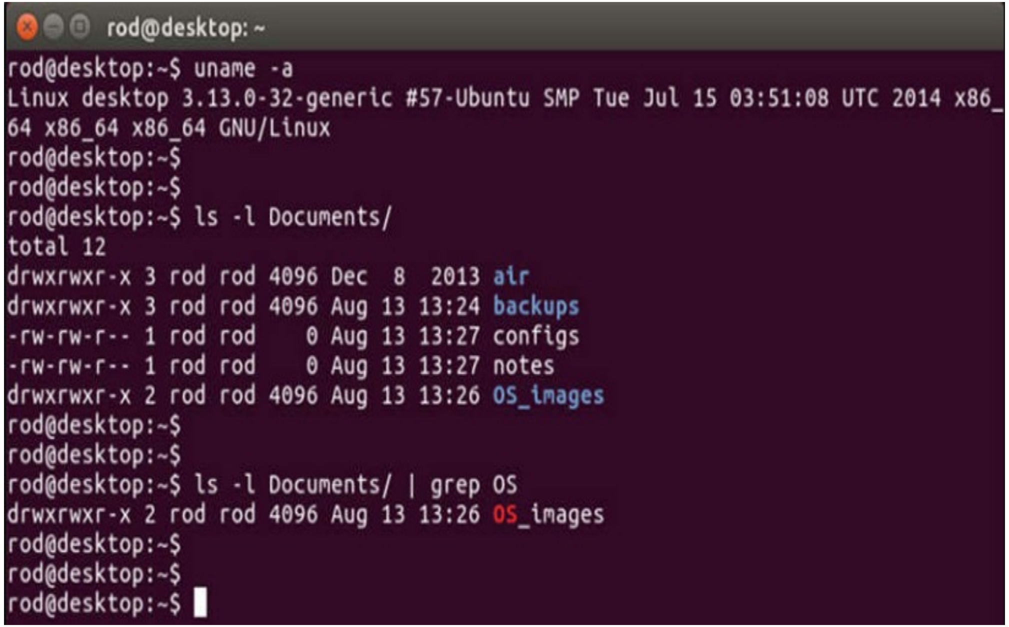
Linux Tools

- Linux computers that are used in the SOC often contain penetration testing tools.
- A penetration test, also known as PenTesting, is the process of looking for vulnerabilities in a network or computer by attacking it.
- Packet generators, port scanners, and proof-of-concept exploits are examples of PenTesting tools.
- Kali Linux distribution groups many penetration tools.



The Linux Shell

- User communicates with the OS by using the CLI or the GUI.
- Terminal emulator applications provide user access to the CLI :
  - terminator
  - eterm
  - xterm
  - konsole
  - gnome-terminal



```
rod@desktop:~$ uname -a
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_
64 x86_64 x86_64 GNU/Linux
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$ ls -l Documents/
total 12
drwxrwxr-x 3 rod rod 4096 Dec  8  2013 air
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups
-rw-rw-r-- 1 rod rod    0 Aug 13 13:27 configs
-rw-rw-r-- 1 rod rod    0 Aug 13 13:27 notes
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$ ls -l Documents/ | grep OS
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images
rod@desktop:~$
rod@desktop:~$
rod@desktop:~$
```

gnome-terminal

Working in the Linux Shell

Basic Commands

- Linux commands are programs created to perform a specific task.
- As the commands are programs stored on the disk, when a user types a command, the shell must find it on the disk before it can be executed.
- The following table lists basic Linux commands and their functions:

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.

Basic Commands (Contd.)

Command	Description
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.
ifconfig	Used to display or configure network card related information.
apt-get	Used to install, configure and remove packages on Debian and its derivatives.
iwconfig	Used to display or configure wireless network card related information.
shutdown	Shuts down the system and performs shut down related tasks including restart, halt, put to sleep or kick out all currently connected users.
passwd	Used to change the password.
cat	Used to list the contents of a file and expects the file name as the parameter.
man	Used to display the documentation for a specific command.

Working in the Linux Shell

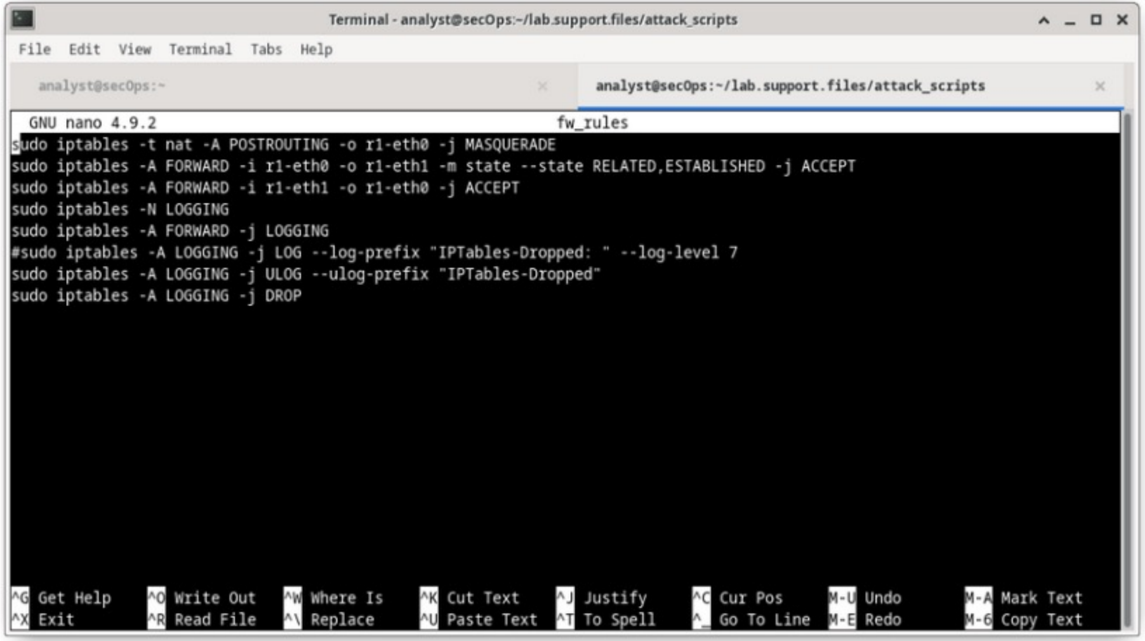
File and Directory Commands

Many command line tools are included in Linux by default. The following table lists a few of the most common commands related to files and directories:

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.

Working with Text Files

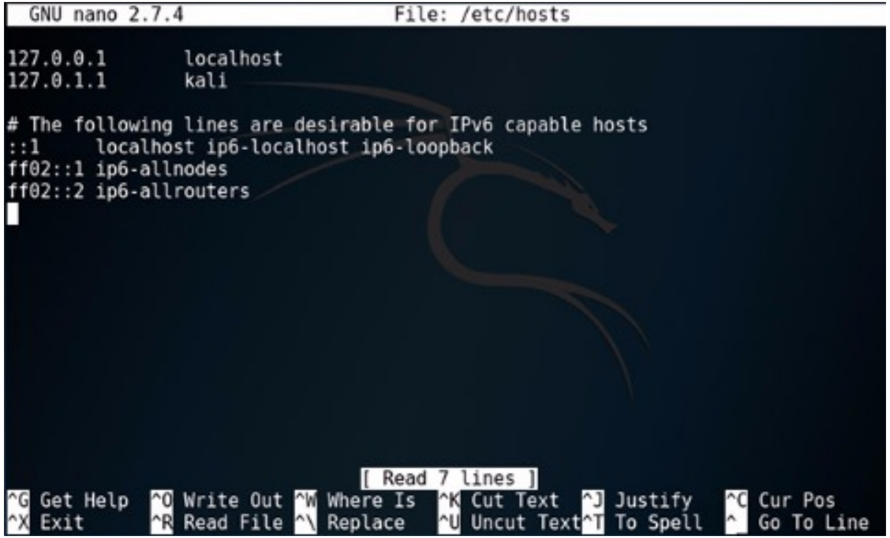
- There are many text editors available in Linux.
- Some text editors are for the CLI only, like vi, vim, and nano.
- Other text editors, like gedit, are GUI-based.
- CLI text editors allow system management remotely, such as via SSH.


Terminal - analyst@secOps:~/lab.support.files/attack_scripts
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~/lab.support.files/attack_scripts

```
  GNU nano 4.9.2                                         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

^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text
```

The Importance of Text Files in Linux

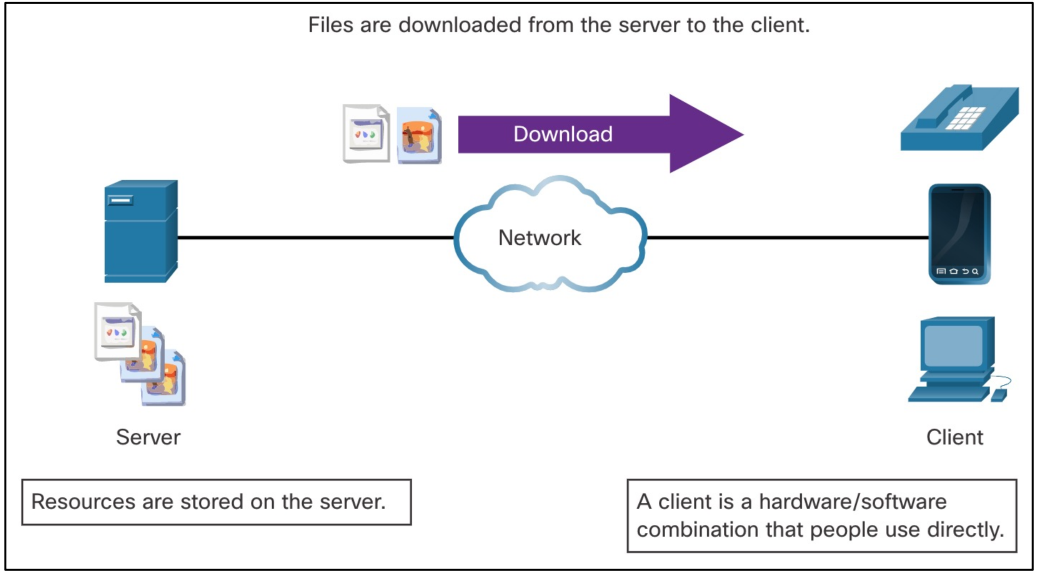
- In Linux, everything is treated as a file, this includes the memory, the disks, the monitor, the files, and the directories.
- The operating system as well as most programs are configured by editing the configuration files which are text files.
- Editing system or application configuration files requires 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
```

An Introduction to Client-Server Communications

- Servers are computers with software installed that enables them to provide services to clients across the network.
- Some provide external resources such as files, email messages, or web pages to clients upon request.
- Other services run maintenance tasks such as log management, disk scanning and so on.
- Each service requires separate server software.


Files are downloaded from the server to the client.
Download
Network
Server
Client
Resources are stored on the server.
A client is a hardware/software combination that people use directly.

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.

Port	Description
20/21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet remote login service
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
67/68	Dynamic Host Configuration Protocol (DHCP)

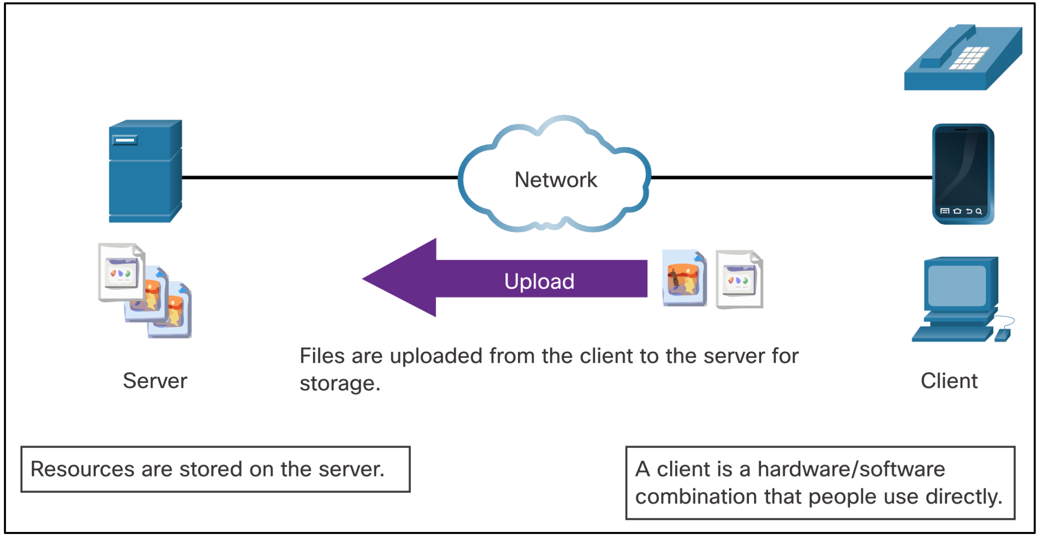
Linux Servers and Clients

Servers, Services, and Their Ports (Contd.)

Port	Description
69	Trivial File Transfer Protocol (TFTP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP)
161/162	Simple Network Management Protocol (SNMP)
443	HTTP Secure (HTTPS)

Clients

- Clients are programs or applications designed to communicate with a specific type of server.
- Clients use a well-defined protocol to communicate with the server:
  - File Transfer Protocol (FTP)
  - Hyper Text Transfer Protocol (HTTP)



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

Resources are stored on the server.

A client is a hardware/software combination that people use directly.

Linux Operating System

New Terms and Commands

- Security Operations Center (SOC)
- Security information and event management (SIEM)
- Intrusion detection systems (IDSs)

- configuration file
- port
- server
- PenTesting

Linux Operating System

Lab 5 – Working with Text Files in the CLI

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