
Sistema Operativo Linux

A solid blue horizontal bar at the bottom of the slide.

Conceptos básicos

¿Qué es Linux?

- Linux es un sistema operativo creado en 1991.
- Linux es de código abierto, rápido, confiable y pequeño. Requiere muy pocos recursos de hardware para ejecutarse y tiene muchas opciones para ser personalizado.
- Linux es parte de varias plataformas y puede encontrarse en cualquier sitio, desde relojes hasta supercomputadora.
- Linux está diseñado para estar conectado a la red, lo cual facilita mucho la escritura y el uso de aplicaciones con base en la red.
- Una distribución de Linux es el término utilizado para describir paquetes creados por diferentes organizaciones que incluyen el Kernel de Linux con herramientas y paquetes de software personalizados.



El valor de Linux

Linux es, a menudo, el sistema operativo elegido en el centro de operaciones de seguridad (SOC). Estos son algunos de los motivos para elegir Linux:

- **Linux es de código abierto** - Cualquier persona puede adquirir Linux sin cargo y modificarlo según sus necesidades específicas.
- **La interface de línea de comandos(CLI) de Linux es muy potente** - La interfaz de línea de comandos(CLI) es extremadamente potente y permite a los analistas realizar tareas, no solo directamente en la terminal, sino que, también de manera remota.
- **El usuario tiene más control sobre el sistema operativo(OS)** - El usuario administrador en Linux, es conocido como usuario root o super-usuario, puede modificar cualquier aspecto de la computadora tecleando tan solo un poco.
- **Permite mejor control de la comunicación con la red** - El control es una parte inherente de Linux.

Linux en el SOC

- La flexibilidad proporcionada por Linux es una grandiosa característica para el SOC. Todo el sistema operativo se puede adaptar para convertirse en la plataforma perfecta para el análisis de seguridad.
- Sguil es la consola de analista de ciberseguridad en una versión especial de Linux llamada Security Onion.
- Security Onion es un conjunto de herramientas de código abierto que trabajan en conjunto para el análisis de seguridad de red.

The screenshot displays the Sguil-0.9.0 interface, which is connected to a local host. The top bar shows the application name and connection status. Below this, there are tabs for 'RealTime Events' and 'Escalated Events'. The main window is divided into several sections:

- RealTime Events Table:** A table with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. It lists various alerts such as 'ET INFO Dotted Quad Host HTA...', 'ET TROJAN Probable OneLoud...', 'ET WEB_SERVER Possible Cher...', and 'ET SCAN Suspicious inbound to...'. Each row is color-coded (yellow, red, or blue) based on the severity of the event.
- Agent Status Table:** A table with columns: Sid, Net, Hostname, Type, and Last. It shows the status of various sensors or agents, including 'seconion-os...', 'seconion-en...', and 'seconion-sn...'. The 'Last' column indicates the time of the last update.
- System Mags:** A section showing system messages and alerts, including 'alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET TROJAN Probable OneLoudner downloader (Zeus P2P)"; flow:to_server,established; content:"GET"; http_method;'. Below this, there is a detailed packet capture view showing the source and destination IP addresses, ports, and the data payload.

The bottom of the interface includes a search bar for packet payloads and options to view the data in Hex, Text, or NoCase format.

Linux en el SOC

La siguiente tabla muestra algunas herramientas que suelen encontrarse en un SOC:

Herramienta SOC	Descripción
Software de captura de paquetes	<ul style="list-style-type: none">• Una herramienta crucial para un analista del SOC, ya que permite observar y entender cada detalle de una transacción de la red.• Wireshark es una popular herramienta de captura de paquetes.
Herramientas de análisis de Malware	<ul style="list-style-type: none">• Estas herramientas permiten al analista ejecutar y observar de manera segura el funcionamiento de un malware sin poner en riesgo el sistema subyacente.
Sistemas de detección de intrusiones (Intrusion detection systems, IDSs)	<ul style="list-style-type: none">• Estas herramientas son utilizadas para el monitoreo y la inspección de tráfico en tiempo real.• Si cualquier aspecto del tráfico que fluye actualmente coincide con cualquiera de las reglas establecidas, se ejecuta una acción previamente definida.

Linux en el SOC

Herramienta SOC	Descripción
Firewalls	<ul style="list-style-type: none">• Este software se utiliza para especificar, según las reglas predefinidas, si el tráfico está permitido para entrar o salir de la red o dispositivo.
Administradores de registros	<ul style="list-style-type: none">• Los archivos de registro son usados para registrar eventos.• Dado que una red puede generar muchas entradas en el registro de eventos, los software de gestores de registro se emplean para facilitar el monitoreo de los registros.
Administración de información y eventos de seguridad (SIEM)	<ul style="list-style-type: none">• SIEM proporciona análisis en tiempo real de alertas y entradas de registro generadas por dispositivos de red, como IDSs y Firewalls
Sistema de tickets	<ul style="list-style-type: none">• La tarea de asignación, edición y registro de tickets se realiza a través de un sistema de gestión de tickets Las alertas de seguridad a menudo se asignan a los analistas a través de un sistema de tickets.

Herramientas de Linux

- Las computadoras de Linux que se utilizan en el SOC suelen tener herramientas de pruebas de penetración.
- Una prueba de penetración, también se conoce como PenTesting; es el proceso de ver la vulnerabilidad en la red o computadora a ser atacados.
- Algunos ejemplos de herramientas de PenTesting son los generadores de paquetes, los escáneres de puertos y los ataques de prueba de concepto.
- ParrotSec es una distribución Linux que contiene muchas herramientas de penetración juntas en una sola distribución Linux.
- Observar todas las categorías principales de herramientas de pruebas de penetración de Kali.



Uso de la shell

El Shell de Linux

- En Linux, el usuario se comunica con el sistema operativo mediante la CLI o GUI.
- Linux, a menudo, se inicia en la GUI de forma predeterminada. Esto oculta la CLI del usuario.
- Una manera de tener acceso a la CLI desde la GUI, es mediante una aplicación de emulación de terminales. Estas aplicaciones proporcionan al usuario acceso a la CLI y se denomina con alguna variación de la palabra terminal.
- En Linux, los emuladores de terminal comunes son: Terminator, eterm, xterm, konsole y gnome-terminal.
- Fabrice Bellard ha creado JSLinux que permite ejecutar una versión emulada de Linux en un navegador.

Nota: *El termino Shell, consola, ventana de consola, terminal de CLI y ventana terminal suelen ser usadas indistintamente.*

Comandos básicos

- Los comandos de Linux son programas creados para realizar una tarea específica.
- Dado que los comandos son programas almacenados en el disco, cuando un usuario escribe un comando, el Shell debe encontrarlo en el disco antes de que se pueda ejecutar.
- En la siguiente tabla se enlistan los comandos básicos de Linux y sus funciones:

Comando	Descripción
mv	Mueve o cambia el nombre de archivos y directorios.
chmod	Modifica los permisos de archivo.
chown	Cambia el propietario de un archivo.
dd	Copia datos de un lugar en otro.
pwd	Muestra el nombre del directorio actual.
ps	Enlista los procesos del sistema que están actualmente en ejecución
su	Simula un inicio de sesión como otro usuario o para convertirse en superusuario.

Comandos Básicos

Comando	Descripción
sudo	Ejecuta un comando como superusuario, de forma predeterminada, u otro usuario nombrado.
grep	Se utiliza para buscar cadenas de caracteres específicas dentro de un archivo o de las salidas de otros comandos.
ifconfig	Se utiliza para mostrar o configurar la información relacionada con la tarjeta de red.
apt-get	Se utiliza para instalar, configurar y eliminar paquetes en Debian y sus derivados.
iwconfig	Se utiliza para mostrar o configurar la información relacionada con la tarjeta de red inalámbrica.
shutdown	Apaga el sistema y realiza las tareas relacionadas con el apagado incluido reiniciar, detener, suspender o expulsar todos los usuarios conectados.
passwd	Se utiliza para cambiar la contraseña.
cat	Se utiliza para enumerar el contenido de un archivo y espera el nombre de archivo como parámetro.
man	Se utiliza para mostrar la documentación para un comando específico.

Comandos de archivos y directorios

Muchas herramientas de línea de comando están incluidas en Linux de manera predeterminada. La siguiente tabla enumera algunos de los más comunes comandos relacionados con archivos y directorios:

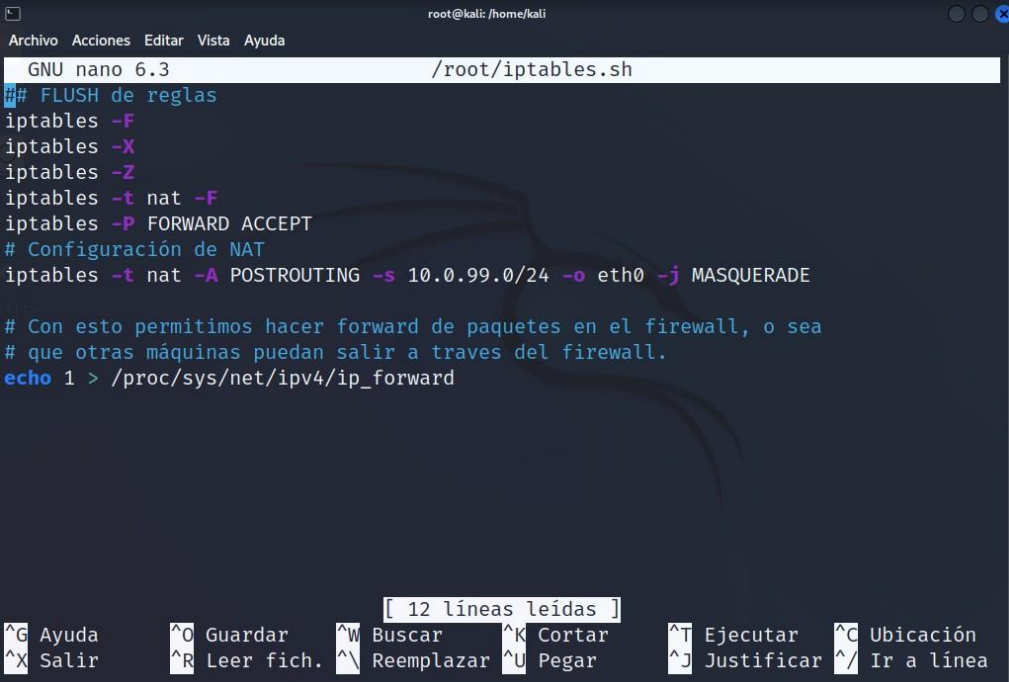
Comando	Descripción
ls	Muestra los archivos dentro de un directorio.
cd	Cambia el directorio actual.
mkdir	Crea un directorio en el directorio actual.
cp	Copia archivos de origen a destino.
mv	Desplaza archivos a otro directorio.
rm	Elimina archivos.
grep	Busca cadenas de caracteres específicas dentro de un archivo o de las salidas de otros comandos
cat	Enumera el contenido de un archivo y espera el nombre de archivo como el parámetro.

Trabajando con archivos de texto

- Linux tiene muchos editores de texto diferentes, con diversas características y funciones.
- Algunos editores de texto incluyen interfaces gráficas, mientras que otros son solamente herramientas de líneas de comando. Cada editor de texto incluye un conjunto de características diseñado para admitir una tarea específica.
- Algunos editores de texto se centran en la programación e incluyen funciones, como resaltado de sintaxis, verificación de paréntesis y otras funciones orientadas a la programación.
- Si bien los editores de texto gráficos son prácticos y fáciles de usar, los basados en la línea de comando son muy importantes para los usuarios de Linux. El principal beneficio de los editores de texto basados en la línea de comando es que permiten editar un archivo de texto desde una computadora remota.

Trabajando con Archivos de Texto

- La figura muestra **nano**, un popular editor de texto de línea de comando.
- El administrador está editando las reglas del firewall. Los editores de texto suelen utilizarse para la configuración del sistema y el mantenimiento en Linux.
- Debido a la falta de soporte gráfico, nano (o GNU nano) se puede controlar solamente con el teclado.



```
GNU nano 6.3 /root/iptables.sh
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
iptables -P FORWARD ACCEPT
# Configuración de NAT
iptables -t nat -A POSTROUTING -s 10.0.99.0/24 -o eth0 -j MASQUERADE

# Con esto permitimos hacer forward de paquetes en el firewall, o sea
# que otras máquinas puedan salir a través del firewall.
echo 1 > /proc/sys/net/ipv4/ip_forward

[ 12 líneas leídas ]
^G Ayuda      ^O Guardar    ^W Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación
^X Salir      ^R Leer fich. ^\ Reemplazar  ^U Pegar      ^J Justificar ^/ Ir a línea
```

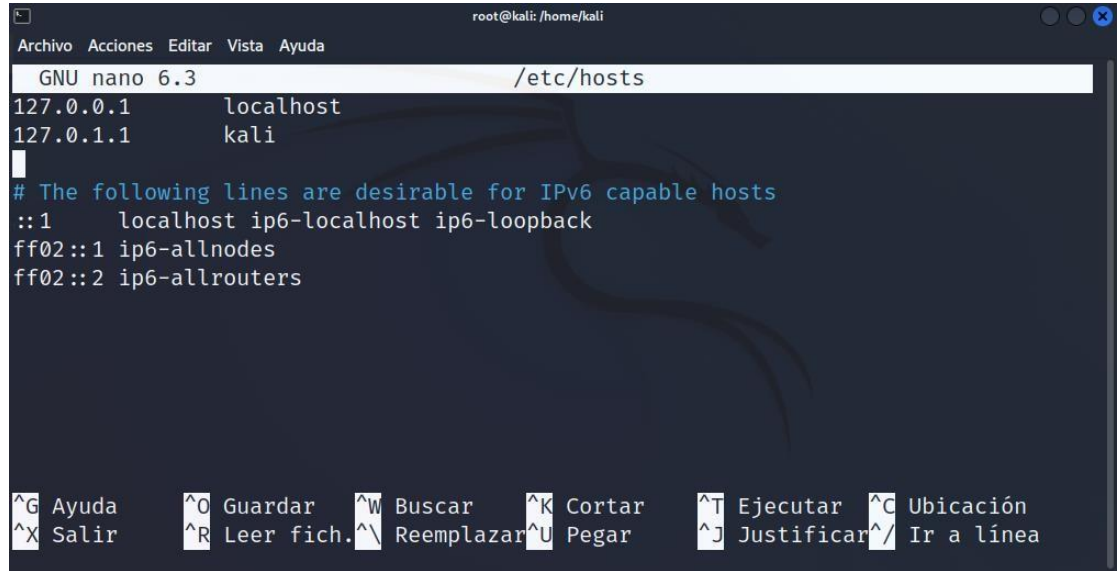
La importancia de los Archivos de Texto en Linux

- En Linux, todo se trata como un archivo. Esto incluye la memoria, los discos, el monitor y los directorios.
- Los archivos de configuración son archivos de texto los cuales son usados para almacenar ajustes y configuraciones de aplicaciones o servicios específicos.
- Los usuarios con los niveles de permisos correctos pueden usar editores de texto para cambiar el contenido de los archivos de configuración.
- Después de realizados los cambios, se guarda el archivo que ya puede ser utilizado por el servicio o la aplicación relacionados. Los usuarios pueden especificar exactamente cómo quieren que se comporte cualquier aplicación o servicio determinado. Cuando se abren, los servicios y las aplicaciones comprueban el contenido de archivos de configuración específicos para ajustar su comportamiento en consecuencia.

Nota: El administrador usa el comando **`sudo nano /etc/hosts`** para abrir el archivo. El comando **`sudo`** (Abreviatura de "superuser do") invoca los privilegios de superusuario para utilizar el editor de texto nano para abrir el archivo host.

La importancia de los archivos de texto en Linux

- En la figura, el administrador abre el archivo de configuración de host en **nano** para editar.
- El archivo host contiene asignaciones estáticas de direcciones IP de host a nombres.
- Los nombres sirven como accesos directos que permiten conectarse a otros dispositivos mediante un nombre en lugar de una dirección IP. Solamente el superusuario puede cambiar el archivo host.



```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
GNU nano 6.3 /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
```

Legend:

[^] G Ayuda	[^] O Guardar	[^] W Buscar	[^] K Cortar	[^] T Ejecutar	[^] C Ubicación
[^] X Salir	[^] R Leer fich.	[^] \ Reemplazar	[^] U Pegar	[^] J Justificar	[^] / Ir a línea

Práctica de laboratorio: Trabajar con archivos de texto en la CLI

En esta práctica de laboratorio, se familiarizará con editores de texto y archivos de configuración de la línea de comando de Linux.

Laboratorio – Familiarizar el uso de Shell de Linux

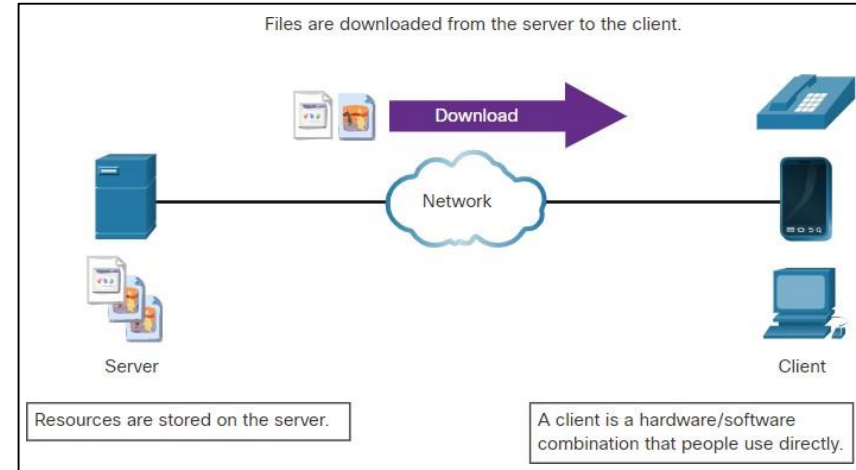
En esta práctica de laboratorio, utilizará la línea de comandos de Linux para administrar archivos y carpetas y para realizar algunas tareas administrativas básicas.

Cientes y Servidores de Linux



Una introducción a las comunicaciones entre Cliente y Servidor

- Los servidores son computadoras con software instalado que les permite ofrecer servicios a los clientes a través de la red.
- Algunos proporcionan recursos externos a los clientes cuando lo solicitan, como archivos, mensajes de correo electrónico o páginas web.
- Otros servicios ejecutan tareas de mantenimiento, como administración de registros, escaneo del disco y demás.
- Cada servicio requiere un software de servidor independiente.
- El servidor en la figura utiliza un software de servidor de archivos para proporcionar a los clientes la capacidad de recuperar y enviar archivos.



Servidores, Servicios y sus puertos

- Un puerto es un recurso de red reservado utilizado por un servicio.
- Mientras que el administrador puede decidir qué puerto utilizar con cualquier servicio, muchos clientes están configurados para utilizar un puerto específico de manera predeterminada.
- La siguiente tabla enlista algunos puertos utilizados comúnmente y sus servicios. Estos también se conocen como "Puertos conocidos(well-known ports)".

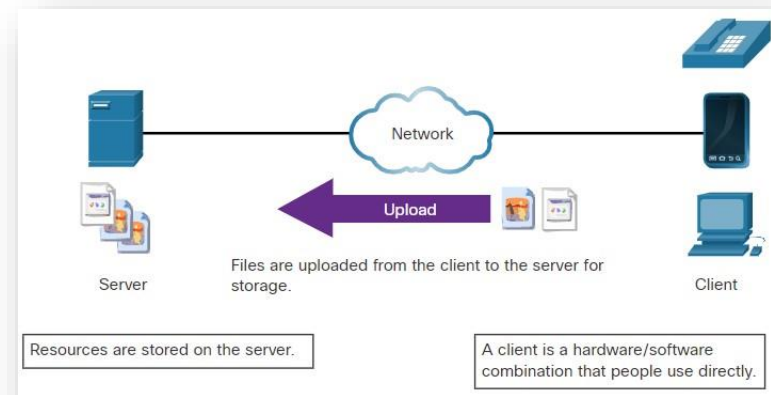
Puerto	Descripción
20/21	Protocolo de transferencia de archivos (FTP)
22	Secure Shell (SSH)
23	Servicio de inicio de sesión remoto de Telnet
25	Protocolo simple de transferencia de correo (SMTP)
53	Sistema de nombres de dominio (DNS)
67/68	Protocolo de configuración dinámica de host (DHCP)

Servidores, Servicios y sus puertos

Puerto	Descripción
69	Protocolo trivial de transferencia de archivos (TFTP)
80	Protocolo de transferencia de hipertexto (HTTP)
110	Protocolo de oficina de correos, 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)

Cientes

- Los clientes son programas o aplicaciones cuyo objetivo es comunicarse con un tipo de servidor específico.
- Los clientes usan un protocolo bien definido para comunicarse con el servidor.
- Los navegadores Web son clientes web utilizados para comunicarse con servidores web mediante el protocolo de transferencia HTTP en el Puerto 80.
- El cliente de protocolo de transferencia de archivos(File Transfer Protocol client, FTP) es un software usado para tener comunicación con un servidor FTP
- En la figura, se ve a un cliente cargando archivos a un servidor.



Laboratorio – Servicios en Linux

En este laboratorio, se pondrá en practica el uso de la línea de comando de Linux para identificar los servicios que se están ejecutando en una computadora.

ps aux (muestra todos los procesos del sistema)

ps axjf (que mostrará un árbol jerárquico con la ruta del programa al que pertenece el proceso)

ps aux | grep bash

top

man top

top -d 5 (Donde 5 es el número de segundos a transcurrir entre cada muestreo)

top -o %CPU (Donde %CPU es el valor por el que vamos a **ordenar los procesos**)

top -u pepe (Donde **pepe** es el usuario del cual queremos mostrar los procesos)

Laboratorio – Servicios en Linux

En este laboratorio, se pondrá en practica el uso de la línea de comando de Linux para identificar los servicios que se están ejecutando en una computadora.

```
htop
```

```
man htop
```

```
kill [PID del proceso]
```

```
kill -KILL [PID del proceso]
```

```
kill -9 [PID del proceso]
```

```
kill -KILL [PID del proceso]
```


```
kill -HUP [PID de Apache]
```

```
kill -1 [PID de Apache]
```

```
kill -9 3484
```

```
pkill -9 htop
```

Sistema de archivos Linux

A solid blue horizontal bar spanning the entire width of the slide at the bottom.

Los tipos de sistema de archivos de Linux

- Hay muchos tipos diferentes de sistemas de archivos, que varían en términos de velocidad, flexibilidad, seguridad, tamaño, estructura, lógica y mucho más.
- El administrador decide el tipo de sistema de archivos adecuado para el sistema operativo.
- La siguiente tabla lista algunos tipos de sistemas de archivos comúnmente encontrados y respaldado por Linux

Sistema de archivos de Linux	Descripción
ext2 (segundo sistema de archivos extendido)	<ul style="list-style-type: none">• ext2 fue el sistema de archivos predeterminado en varias distribuciones de Linux hasta que fue sustituido por ext3.• ext2 sigue siendo el sistema de archivos preferido de los medios de almacenamiento con base flash, ya que la ausencia de registros diarios aumenta el rendimiento y minimiza la cantidad de escrituras.• Dado que los dispositivos de memoria flash tienen una cantidad limitada de operaciones de escritura, reducir estas operaciones al mínimo aumenta la vida útil del dispositivo.

Los tipos sistemas de archivos en Linux

Sistema de archivos de Linux	Descripción
ext3 (tercer sistema de archivos extendido)	<ul style="list-style-type: none">• ext3 es un sistema de archivos con registro por diario diseñado para mejorar el sistema de archivos ext2 existente.• Un diario o registro, la principal característica que se agregó a ext3, es una técnica que se utiliza para minimizar el riesgo de corrupción del sistema de archivos en caso de una interrupción repentina en el suministro de corriente.• El sistema de archivos mantiene un registro de todos los cambios que están por realizarse.• Si la computadora deja de funcionar antes de que el cambio se complete, el diario puede ser usado para restaurar o corregir cualquier problema creado por la interrupción.• El tamaño máximo de archivo en sistemas de archivos ext3 es de 32 TB.
ext4 (cuarto sistema de archivos extendido)	<ul style="list-style-type: none">• ext4 se creó a partir de una serie de extensiones a ext3.• Aunque las extensiones mejoraban el rendimiento de ext3 y aumentaban el tamaño de los archivos admitidos, a los desarrolladores les preocupaba la estabilidad y se opusieron a añadir las extensiones al sistema ext3 estable.• El proyecto de ext3 se dividió en dos: un sistema se mantiene como ext3 y continúa su desarrollo normal, y el otro, llamado ext4, incorpora las extensiones mencionadas.

Los tipos de archivos de sistema en Linux

Archivos de sistema de Linux	Descripción
NFS (Sistema de archivos de red)	<ul style="list-style-type: none">• NFS es un sistema de archivos basado en la red que permite el acceso a archivos en la red.• Desde el punto de vista del usuario, no hay diferencia entre el acceso a un archivo almacenado localmente o en otra computadora en la red.• NFS es un estándar abierto que permite a cualquiera implementarlo.
CDFS (Sistema de archivos de disco compacto)	<ul style="list-style-type: none">• CDFS fue creado específicamente para medios de discos ópticos.
Sistema de intercambio de archivos	<ul style="list-style-type: none">• El sistema de archivos de intercambio es usado por Linux cuando se queda sin RAM.• Cuando Linux se queda sin RAM, el Kernel mueve el contenido inactivo de la RAM a la partición swap en el disco.• Mientras que las particiones de intercambio pueden ser útiles para computadoras Linux con una cantidad limitada de memoria, no deben considerarse una solución principal.• La partición swap se almacena en un disco que tiene velocidades de acceso mucho menores que la RAM.

Los tipos de archivos de sistema en Linux

Archivos de sistema de Linux	Descripción
HFS Plus o HSF+ (Hierarchical File System Plus)	<ul style="list-style-type: none">• Es un sistema de archivos usado por Apple en sus computadoras Macintosh.• El Kernel de Linux incluye un módulo para montar HFS+ para las operaciones de lectura y escritura.
APFS (Apple File system)	<ul style="list-style-type: none">• Sistema de archivos actualizado que utilizan los dispositivos Apple.• Proporciona un cifrado fuerte y está optimizado para unidades de estado sólido y flash.
Registro principal de arranque (MBR)	<ul style="list-style-type: none">• Situado en el primer sector de una computadora con particiones, el MBR almacena toda la información sobre la manera en que está organizado el sistema de archivos.• El MBR le cede rápidamente el control a una función de carga para que realice la carga el sistema operativo.

Roles y permisos de archivos en Linux

- Linux utiliza permisos de archivos con el objetivo de organizar el sistema y reforzar los límites de la computadora.
- Cada archivo en Linux trae sus permisos de archivo, los cuales definen las acciones que el propietario, el grupo y otros puede hacer con el archivo.
- Los posibles permisos son leer, escribir y ejecutar.
- El comando **ls** con el parámetro **-l** crea una lista detallada sobre la información del archivo.

Roles y permisos de archivos en Linux

El resultado del comando **ls -l** proporciona mucha información sobre el archivo **space.txt**:

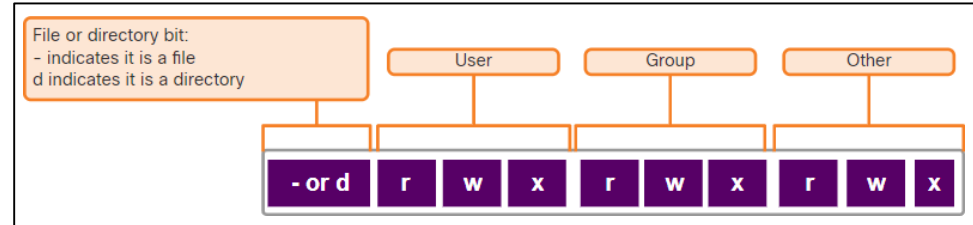
- El primer campo muestra los permisos con **space.txt** (**-rwxrw-r--**).
- El segundo campo define la cantidad de enlaces físicos hacia el archivo (el número **1** después de los permisos).
- El tercer y cuarto campo muestran el usuario (**analyst**) y el grupo (**staff**) que poseen el archivo, respectivamente.
- El quinto campo muestra el tamaño del archivo en bytes. El archivo **space.txt** tiene 253 bytes.
- El sexto campo muestra la fecha y hora de la última modificación.
- El séptimo campo muestra el nombre del archivo.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```

Roles y permisos de archivos en Linux

La figura muestra un desglose de los permisos de archivo en Linux. El archivo **space.txt** tiene los siguientes permisos:

- El guion (-) indica que se trata de un archivo.
- El primer conjunto de caracteres (**rw**x) son para permisos de usuario. El usuario (**Analyst**) que posee el archivo puede **Read** (Leer), **Write** (Escribir) y **eXecute** (ejecutar) el archivo.
- El segundo conjunto de caracteres es para los permisos de grupo (**rw**-). El grupo (**Staff**) que posee el archivo puede **Read** (Leer) y **Write** (Escribir) el archivo.
- El tercer conjunto de caracteres es para cualquier otro permiso de usuario o grupo (**r--**) los cuales solo pueden **Read** (Leer) el archivo.



Roles y permisos de archivos en Linux

- Los valores octales son utilizados para definir permisos.
- Los permisos de archivos son una parte fundamental de Linux y no se pueden eliminar.
- El único usuario que puede anular el permiso de archivo en una computadora con Linux es el usuario root.

Binario	Octal	Permiso	Descripción
000	0	---	Sin acceso
001	1	--x	Solo ejecución
010	2	-w-	Solo escritura
011	3	-wx	Escritura y ejecución
100	4	r--	Solo lectura
101	5	r-x	Lectura y ejecución
110	6	rw-	Lectura y escritura
111	7	rwX	Lectura, escritura y ejecución

Enlaces rígidos y Enlaces simbólicos

- Un enlace rígido es otro archivo que apunta a la misma ubicación que el archivo original.
- Usar el comando **ln** para crear un enlace rígido.
- El primer argumento es el archivo existente y, el segundo, el archivo nuevo.
- Como se muestra en el comando output, el archivo **space.txt** está enlazado a **space.hard.txt** y el campo de enlace ahora muestra 2.
- Ambos archivos apuntan a la misma ubicación en el sistema de archivos. Si cambia un archivo, el otro también cambia.
- El comando **echo** se utiliza para añadir algún texto a **space.txt**.

```
[analyst@secOps ~]$ ln space.txt space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.hard.txt
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "Testing hard link" >> space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.hard.txt
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ rm space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more space.txt
Space... The final frontier...
These are the voyages of the Starship Enterprise. Its continuing mission:
- To explore strange new worlds...
- To seek out new life; new civilizations...
- To boldly go where no one has gone before!
Testing hard link
[analyst@secOps ~]$
```

Enlaces rígidos y enlaces simbólicos

- Un enlace simbólico, también llamado enlace suave o symlink, es similar a un enlace físico en el sentido de que, al aplicar cambios a un enlace simbólico, también cambia el archivo original.
- Como se muestra en el comando output, utiliza el comando **ln** con la opción **-s** para crear un enlace simbólico.
- Observar que añade una línea de texto a **test.txt** también añade la línea a **mytest.txt**.

```
[analyst@secOps ~]$ echo "Hello World!" > test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ln -s test.txt mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "It's a lovely day!" >> mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more test.txt
Hello World!
It's a lovely day!
[analyst@secOps ~]$
[analyst@secOps ~]$ rm test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more mytest.txt
more: stat of mytest.txt failed: No such file or directory
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l mytest.txt
lrwxrwxrwx 1 analyst analyst 8 May  7 20:17 mytest.txt -> test.txt
[analyst@secOps ~]$
```

Enlaces rígidos y enlaces simbólicos

La siguiente tabla muestra varias ventajas de los enlaces simbólicos sobre los enlaces duros:

Enlaces rígidos	Enlaces suaves
Localizar enlaces rígidos es más difícil	Los enlaces simbólicos muestran la ubicación del archivo original en el comando <code>ls -l</code> .
Los enlaces físicos se limitan al sistema de archivos en el que se crean.	Los enlaces simbólicos pueden estar vinculados a un archivo en otro sistema de archivos.
Los enlaces rígidos no pueden estar vinculados a un directorio como el propio sistema porque utiliza enlaces rígidos para definir la jerarquía de la estructura de los directorios.	Los enlaces simbólicos pueden estar vinculados a directorios.

Laboratorio - Navegación por el sistema de archivos y la configuración de permisos

En esta práctica de laboratorio, se familiarizará con el sistema de archivos de Linux.

`-rwxrwxrwx 2 root root 4096 feb 16 15:16 seguridad.txt`

↓	↓	↓	↓	↓	↓	↓	↓	↓
Míos	Grupo	Otros	propietario		tamaño	Fecha / hora		archivo
↓								
Tipo de archivo			Cant. de enlaces físicos	grupo				

Laboratorio - Navegación por el sistema de archivos y la configuración de permisos

Dar permisos completos de lectura, escritura y ejecución a todos los roles, tanto usuario como grupo como otros:

```
chmod ugo+rwx archivoDePrueba
```

Quitar permisos de lectura, escritura y ejecución a otros usuarios:

```
chmod o-rwx archivoDePrueba
```

```
chmod 700 archivoDePrueba
```

```
chmod 666 archivoDePrueba
```

Trabajo con la GUI Linux

A solid blue horizontal bar at the bottom of the slide.

Sistema X Window

- La interfaz gráfica presente en la mayoría de las computadoras Linux tiene como base el sistema X Window.
- X window, también conocido como X o X11, es un sistema de ventanas diseñado para proporcionar el marco de trabajo básico para una GUI
- X incluye funciones para dibujar y mover ventanas en el dispositivo de visualización, e interactuar con un mouse y un teclado.
- X funciona como un servidor, el cual le permite a un usuario remoto utilizar la red para conectarse, iniciar una aplicación gráfica y mantener la ventana de gráficos abierta en el terminal remoto.
- X no especifica la interfaz de usuario y deja que otros programas, como los gestores de ventanas, definan todos los componentes gráficos.

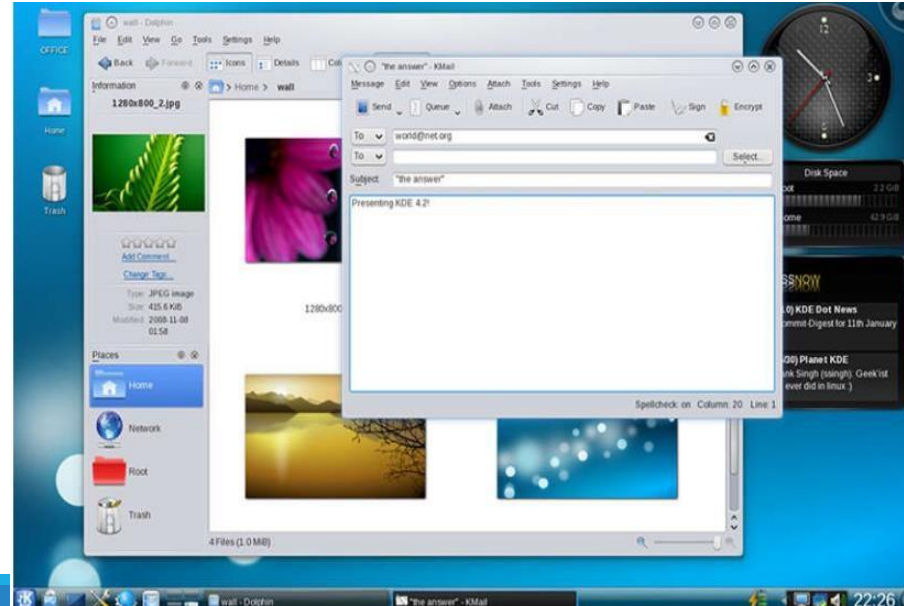
Sistema X Window

Ejemplos de gestores de ventanas son Gnome y KDE.

El Gnome Window Manager



El KDE Window Manager



Trabajo con el host Linux

A solid blue horizontal bar at the bottom of the slide.

Instalar y ejecutar aplicaciones en un host de Linux

- Muchas aplicaciones de usuario final son programas complejos, escritos en lenguajes compilados.
- Para ayudar en el proceso de instalación, Linux incluye programas llamados administradores de paquetes.
- El uso de un administrador de paquetes para instalar un paquete, permite colocar todos los archivos necesarios en la ubicación correcta en el sistema de archivos.
- Un paquete es el término utilizado para referirse a un programa y a todos sus archivos compatibles.
- El resultado del comando muestra la salida de algunos comandos **apt-get** utilizados en las distribuciones Debian.

```
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]
<output omitted>
Fetched 4,613 kB in 4s (1,003 kB/s)
Reading package lists... Done
analyst@cuckoo:~$
analyst@cuckoo:~$ sudo apt-get upgrade
Reading package lists Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
linux-generic-hwe-16.04 linux-headers-generic-hwe-16.04
linux-image-generic-hwe-16.04
The following packages will be upgraded:
firefox firefox-locale-en gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18
libwebkit2gtk-4.0-37 libwebkit2gtk-4.0-37-gtk2 libxen-4.6 libxenstore3.0 linux-libc-dev logrotate
openssh-client
qemu-block-extra qerau-kvm qemu-system-common qemu-system-x86 qemu-utils
```

Mantener el sistema actualizado

- Actualizaciones del sistema, también conocidas como parches, son publicadas periódicamente por empresas de sistemas operativos, para abordar cualquier vulnerabilidad conocida en sus sistemas operativos
- Los sistemas operativos modernos alertarán al usuario cuando las actualizaciones estén disponibles para la descarga e instalación, pero el usuario puede buscar actualizaciones en cualquier momento.
- La siguiente tabla compara los comandos de distribución Arch Linux y Debian/Ubuntu Linux para realizar operaciones básicas del sistema de paquetes.

Tarea	Arch	Debian/Ubuntu
Instalar un paquete por nombre	<code>pacman -S</code>	<code>apt install</code>
Eliminar un paquete por nombre	<code>pacman -Rs</code>	<code>apt remove</code>
Actualizar un paquete local	<code>pacman -Syy</code>	<code>apt-get update</code>
Actualizar todos los paquetes instalados actualmente	<code>pacman -Syu</code>	<code>apt-get upgrade</code>

Procesos y bifurcaciones

- Un proceso es una instancia en ejecución de un programa informático.
- La bifurcación es un método que utiliza el Kernel para permitir que un proceso cree una copia de sí mismo.
- Los procesos necesitan una manera de crear nuevos procesos en los sistemas operativos multitarea. La bifurcación es la única manera de lograr esto en Linux.
- Cuando un proceso solicita la bifurcación, el proceso que realiza la solicitud se convierte en el proceso principal y el proceso recién creado se denomina subproceso.
- Después de la bifurcación, los procesos son, hasta cierto punto, procesos independientes. Tienen diferentes identificadores de proceso pero ejecutan el mismo código de programa.

Procesos y bifurcaciones

En la siguiente tabla se enumeran tres comandos que se utilizan para administrar procesos.

Comando	Descripción
ps	<ul style="list-style-type: none">• Se utiliza para enumerar los procesos en ejecución en el sistema cuando se invoca.• Se puede indicar que muestre los procesos en ejecución que pertenecen al usuario actual o a otros usuarios.
top	<ul style="list-style-type: none">• Es utilizado para indicar procesos en ejecución, pero a diferencia de ps, top sigue mostrando los procesos en ejecución de dinámicamente.• Presione q para salir de top.
kill	<ul style="list-style-type: none">• Utilizado para modificar el comportamiento de un proceso específico.• Según el parámetro, kill removerá, reiniciará o detendrá un proceso.• En muchos casos, el usuario ejecutará ps o top antes de ejecutar kill.• Esto se hace para que el usuario adquiera la PID de un proceso antes de ejecutar kill.

Comandos Piping

- Aunque las herramientas de línea de comando suelen diseñarse para realizar una tarea específica bien definida, muchos comandos se pueden combinar para realizar tareas más complejas mediante una técnica conocida como Piping.
- El Piping consiste en vincular comandos entre sí, de manera que el resultado de un comando alimente la entrada de otro.
- Los dos comandos, **ls** y **grep**, pueden ser entubados juntos para filtrar el resultado de **ls**. Esto se muestra en la salida del comando **ls -l | grep host** y el comando **ls -l | grep file**.

```
[analyst@secOps ~]$ ls -l
total 40
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 April 2 14:44 Downloads
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 19 May 20 10:53 mytest.com
-rw-r--r-- 1 analyst analyst 228844 May 20 10:54 rkhunter-1.4.6-1-any.pkg.tar.xz
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 257 May 20 10:52 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep host
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep file
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
[analyst@secOps ~]$
```

Procesos y bifurcaciones

El comando de salida muestra el resultado del comando **top** en un computadora Linux.

```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
top - 03:10:11 up 34 min, 2 users, load average: 0,12, 0,24, 0,21
Tasks: 172 total, 1 running, 171 sleeping, 0 stopped, 0 zombie
%Cpu(s): 1,9 us, 1,4 sy, 0,0 ni, 96,1 id, 0,5 wa, 0,0 hi, 0,2 si, 0,0 st
MiB Mem : 3929,6 total, 874,9 free, 904,7 used, 2150,0 buff/cache
MiB Swap: 975,0 total, 975,0 free, 0,0 used. 2680,7 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
739	root	20	0	451128	149700	64588	S	4,0	3,7	0:17.72	Xorg
1236	kali	20	0	210320	30676	19248	S	0,7	0,8	0:11.22	panel-13-cpugra
3226	kali	20	0	433048	95876	78628	S	0,7	2,4	0:01.22	qterminal
725	root	20	0	1341572	46100	26736	S	0,3	1,1	0:01.83	containerd
1137	kali	20	0	155540	2740	2272	S	0,3	0,1	0:03.26	VBoxClient
1186	kali	20	0	931628	95164	71036	S	0,3	2,4	0:07.20	xfwm4
5940	redis	20	0	315064	224604	8440	S	0,3	5,6	0:08.15	redis-server
10332	root	20	0	0	0	0	I	0,3	0,0	0:00.02	kworker/0:0-events
10512	root	20	0	12936	4052	3268	R	0,3	0,1	0:00.03	top
1	root	20	0	166364	11400	8380	S	0,0	0,3	0:00.61	systemd
2	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kthreadd
3	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	rcu_par_gp
6	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	kworker/0:0H-events_highpri
7	root	20	0	0	0	0	I	0,0	0,0	0:00.18	kworker/0:1-events
8	root	20	0	0	0	0	I	0,0	0,0	0:00.19	kworker/u4:0-events_unbound
9	root	0	-20	0	0	0	I	0,0	0,0	0:00.00	mm_percpu_wq
10	root	20	0	0	0	0	S	0,0	0,0	0:00.00	rcu_tasks_kthre
11	root	20	0	0	0	0	S	0,0	0,0	0:00.00	rcu_tasks_rude_
12	root	20	0	0	0	0	S	0,0	0,0	0:00.00	rcu_tasks_trace
13	root	20	0	0	0	0	S	0,0	0,0	0:00.15	ksoftirqd/0
14	root	20	0	0	0	0	I	0,0	0,0	0:01.16	rcu_preempt
15	root	rt	0	0	0	0	S	0,0	0,0	0:00.01	migration/0
16	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/0
17	root	20	0	0	0	0	S	0,0	0,0	0:00.00	cpuhp/1
18	root	rt	0	0	0	0	S	0,0	0,0	0:00.28	migration/1
19	root	20	0	0	0	0	S	0,0	0,0	0:00.06	ksoftirqd/1

Malware en un host de Linux

- El malware de Linux incluye virus, troyanos, gusanos y otros tipos de malware que pueden afectar el sistema operativo.
- Un vector de ataque común en Linux son sus servicios y procesos.
- El comando de salida muestra un escaneo usando el comando nmap para probar la naturaleza y versión de un servidor ftp (Puerto 21).
- El atacante descubrió que el servidor está ejecutando vsftpd versión 2.3.4. El siguiente paso sería investigar vulnerabilidades conocidas..

```
(root@kali)-[/home/kali]
# nmap -sS -p21 172.17.0.2
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-15 12:14 CEST
Nmap scan report for 172.17.0.2
Host is up (0.000034s latency).
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.69 seconds
```

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to 172.17.0.1
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

OpenVAS. Evaluación de vulnerabilidades

- Este scanner cuenta con diversas funciones posibles, entre las que se encuentran:

- Pruebas autenticadas.

- Pruebas no autenticadas.

- Cuenta con protocolos industriales y de Internet de alto y bajo nivel.

- Ajustes personalizados de rendimiento para exploraciones a gran escala.

- Desarrollado en un potente lenguaje de programación para implementar cualquier tipo de prueba de vulnerabilidad.



Fin módulo

A solid blue horizontal bar spanning the entire width of the slide at the bottom.