Comando básicos de Linux

El comando CD (change directory - cambiar directorio)

cd /usr/local → vamos a la carpeta /usr/local
cd - → retorna a la carpeta donde estábamos antes
cd ~ → ir al directorio Home
cd .. → ir a una carpeta anterior
cd ../ ../ → en el caso que quieras subir dos niveles en las carpetas
cd /etc/f* → en el caso de olvidar una carpeta, buscamos las que empiezan con f

Ir al superusuario root

sudo su → password y abrimos una sesión como root

Listar archivos

ls -alh → a archivos ocultos, l listar, h peso
vim .bashrc alias para no tener que poner todos los argumentos >ll ejemplo

Saber en que carpeta me encuentro

#pwd

Copiar y borrar un archivos

cp archivo /carpeta
cp archivo archivo.copia
cp -a carpeta/ carpeta-destino/
rm archivo → borra el archivo
rm carpeta/archivo → borra el archivo de una carpeta especifica
rm -rf archivo → modificador -rf, hace que el borrado se ejecute recursivamente y sin pedir confirmación

Mover archivo

mv archivo carpeta/
rm -rf carpeta/ → forma recursiva
mv carpeta/ carpeta-destino/
rsync -av carpeta/ carpeta-destino/ → copia todos los archivos de una carpeta a otra

Modificar los permisos de un archivos

chmod a+rw archivo.txt → da permisos de lectura y escritura a todos los usuarios del archivo.txt

CHMOD completo en el apartado 3

Crear archivo

touch archivo.txt o #> archivo.txt

Crear y borrar una carpeta

mkdir /home/usuario1/directorio1 → crea la carpeta directorio1
mkdir directorio2 → crea la carpeta directorio2
rmdir /home/usuario1/directorio1 → borra la carpeta directorio1
rmdir directorio2 → borra la carpeta directorio2

Cuanto pesa una carpeta
du -sh directoria actual
du -sh carpeta/
du -sh carpeta/*

Saber datos específicos de un archivos
stat archivos

Comprimir y descomprimir una carpeta
zip -r images.zip carpeta/
unzip images.zip
zipinfo images.zip

Ver árbol de carpeta
tree

Buscar archivos en alguna carpeta
find . -mtime +5
find . -iname 'archivo*' → iname may y minusculas, es key sensitive

Calendario → # cal #cal 7 1977
Fecha actual → # date
Fecha mas siete dias → # date -d "+7 days"
Calculadora simple # bc

Listar procesos
ps fax
Matar un proceso
kill numero-de-proceso
Matar todos los procesos por nombre
kill nombre-de-proceso

Visitar una pagina por linea de comando
curl sitio-web → muestra el html de la pagina

Ver el contenido de un archivos
cat archivos
grep búsqueda archivo
cat archivo | grep busqueda1 | grep busqueda2 → concatenar búsquedas, grep -v es lo contrario, filtra la búsqueda

Espacio en disco

df -h

Top muestra procesos y uso de recursos de cpu, shift p usos de cpu y shift m por uso de memoria

top # htop

Ipcalc

ipcalc sirve para calcular rangos de ip y mascara

Buscar algo que ya ejecute

history
history | grep busqueda
ctrl r moverme en la linea ctrl e, ctrl a, ctrl flecha

Tab autocompleta

ping / ping6 : Envía un paquete ICMP para comprobar que el destino responde. En Linux no termina hasta que pulsemos CONTROL+C. A no ser que se use la opción -c que indica el número de paquetes a enviar.

Estadisticas de Red

netstat -nr #route -n → Muestra la tabla de roteo
netstat -i → Muestra las interfaces
netstat -natup → n no resuelve, a muestre todo, t tcp, u udp, p proceso

Mostrar el trafico de red

tcpdump -i eth0 → ver el trafico sobre eth0
tcpdump -i any tcp port 80 → ver el trafico de todas la interfaces para el port 80

traceroute / traceroute6: Parecido a trachepath pero con más opciones. Puede requerir permisos de root

Editor de texto

nano archivo → ctrl o guardar, ctrl x salir
vim o vi → i insert , q sin guardar, wq guardando, x combinación de wq
Vim completo en el apartado 2

Localizar un archivos

locate archivo → updatedb se actualiza a diario, si el archivo es nuevo no va a aparecer, salvo que corra updated

Crear una sesión en una terminal

screen

tmux

Leer un archivo

less archivo → /buscar alguna palabra, n proximo, q salir

Leer las ultimas 10 lineas de un archivo

tail /var/log/kern.log
tail -f /var/log/kern.log → y queda esperando
tail -n1 /var/log/kern.log → muestra la ultima linea
head /var/log/kern.log → muestra las primeras 10 lineas

Conectarse al otro servidor por ssh → shell remota segura

ssh users@ip

SSH completo en otro apartado 4

Ver el estado de la memoria

free -m → en megabyte
free -g → en gigabyte
free → en bit, poco usado

Ver si tu servidor esta sobre cargado

cat /proc/cpuinfo
cat /proc/loadavg

Descarga un archivo de Internet

wget pagina-web.pdf → por ejemplo

Escaneo una Red y Puertos

nmap ip → ejemplo #nmap 192.168.100.10

NMAP completo en el apartado 5

Saber el estado de las interfaces de red con su Ip, mac.

ifconfig → todas las interfaces
ifconfig eth0 → solo para la interfaz eth0

La mayoría estos comando vienen instalados, si lo no están:

sudo apt update → actualiza los repositorios
sudo apt upgrade → instala parches y nuevas versiones
sudo apt install comando → instalar el comando o aplicación

Script de shell (Shell script)

Bash es un intérprete de comandos, se trata de una interfaz de usuario con la que relacionarte con el sistema operativo con el que estás trabajando. Así, esta aplicación es capaz de leer y ejecutar instrucciones. Muy útil para automatizar procesos con menos errores. Eliminar tareas repetitivas y Ahorrar tiempo.

man bash → páginas del manual de bash
Scripts en Bash Completo en el apartado 6

Hay varios comandos que se pueden utilizar para apagar, reiniciar o cerrar Linux:

- shutdown : apaga el sistema de forma planificada
- halt : apaga el sistema sin enviar señal ACPI de apagado de alimentación eléctrica
- poweroff : apaga el sistema con señal ACPI
- reboot : reinicia el sistema

Faltan muchos mas, pero para arrancar esta mas que bien, se recomienda para conocer mas de cada uno de estos comandos, que tienen muchos mas argumentos, revisar la documentación → Ejemplo https://comandoslinux.github.io/

Gabriel O. Cendra
www.ciberseguridadgoc.com.ar