**LINUX/UNIX**

**INFORMACIÓN DEL SISTEMA**

arch Muestra la arquitectura del ordenador

uname -a Muestra la versión del Kernel

lsmod lista los módulos del Kernel

cat /proc/cpuinfo Muestra información de la CPU

cat /proc/meminfo Muestra información de la memoria RAM

free Muestra estado y uso de la memoria

cat /proc/net/dev Muestra los adaptadores de red y sus estadísticas

cat /proc/mounts Muestra el sistema de archivos montado

top Muestra las tareas de Linux usando la mayoría de CPU

date Muestra la fecha actual del sistema

timedateclt Cambia el reloj del sistema

cal 2022 Muestra el calendario del año que indiquemos

cal 11 2022 Muestra el mes que indiquemos del año que indiquemos

clock -w Guarda los cambios de fecha en la BIOS

who Muestra quien está online

w Más información que who

whoami Muestra con que usuario estoy logado

who -a Información muy detallada de who

du Muestra el uso del espacio del directorio

df Muestra el uso de disco

history Muestra los últimos comandos

uptime Muestra cuanto tiempo lleva el equipo encendido

dmesg Muestra mensajes del reinicio del sistema

lspci -tv Muestra los dispositivos PCI

lsusb -tv Muestra los dispositivos USB

lshw Muestra información del Hardware

dmidecode Muestra información del Hardware de la BIOS

hdparm -l /dev/hda Muestra información del disco “hda”

clear Borrar la Shell

**APAGAR, REINICIAR, SALIR DEL SISTEMA**

shutdown -h now Apagar el sistema

init 0 Apagar el sistema

halt Apagar el sistema

shutdown -c Cancelar apagado planificado del sistema

shutdown -r now Reiniciar el sistema

reboot Reiniciar el sistema

logout Cerrar sesión

init 6 Reiniciar el sistema

last reboot Muestra el historial de los últimos reinicios

startx Empieza el X System

**ARCHIVOS Y DIRECTORIOS**

cd /home Entra en el directorio “home”

cd .. Retrocede un nivel en la jerarquía de directorios

cd Te lleva al directorio raíz

pwd Muestra la ruta del directorio donde me encuentro actualmente

dir Muestra directorios donde me encuentro

ls Muestra archivos y carpetas del directorio donde me encuentro

ls -l Muestra los detalles de los archivos y carpetas del directorio donde me encuentro

ls -l /etc/passwd Muestra los detalles del archivo “passwd”

ls –a Muestra los archivos ocultos y no ocultos del directorio actual

ls -lah Muestra con más detalle los archivos y directorios y más comprensiblemente

mkdir dir1 Crea una carpeta o directorio con el nombre “dir1”

mkdir dir1 dir2 Crea dos carpetas o directorios a la vez con nombre “dir1” y “dir2”

mkdir dir1 /tmp Crea una carpeta “dir1” en la ruta /tmp

rm file1 Borra el fichero “file1”

rm –r dir1 Borra la carpeta con nombre “dir1”

rm -rf / Borra el disco duro

mv file1 file2 Renombra el archivo “file1” a “file2”

cp file1 file2 Copia el contenido del archivo “file1” a “file2”

cp -r dir1 dir2 Copia recursivamente el contenido del directorio “dir1” a “dir2”

cp file1 /home/user1 Copia el archivo “file1” en la ruta /home/user1

ln -s /path/to/filename linkname Crea un enlace simbólico a “filename”

touch file1 Crea el archivo “file1”

touch {file1,file2} Crea dos archivos a la vez

nano nota1.txt Crea el archivo “nota1.txt”

wc nota1.txt Muestra el número de bytes, palabras y líneas en el archivo “nota1.txt”

cat nota1.txt Crea y edita el archivo “nota1.txt”

cat >> nota1.txt Edita el archivo “nota1.txt” desde donde se había quedado

cat > nota1.txt Edita el archivo “nota1.txt” y lo crea de nuevo

more /etc/passwd Muestra el contenido del archivo “passwd” con barra espaciadora para

seguir mostrando

head /etc/passwd Muestra el contenido del archivo “passwd” de las 10 primeras filas

tail /etc/passwd Muestra el contenido del archivo “passwd” de las 10 últimas filas

tail –n 1 /etc/passwd Muestra el contenido del archivo “passwd” de la última fila

cat /etc/passwd | tail -n 1 Muestra lo mismo que el comando de arriba

tree Muestra archivos y carpetas en forma de árbol

diff file1 file2 Elimina las cosas iguales de dos archivos

**BUSQUEDA DE ARCHIVOS**

find / -name file1 Busca fichero “file1” a partir de la raíz del sistema

find /home -name file1 Busca fichero “file1” a partir de la ruta /home

find / -user zero Busca archivos y directorios propiedad del usuario “zero”

find /home/zero -name \\*.bin Busca todos los archivos .bin en la ruta /home/zero

find / -type f -name apache2 Búsqueda del archivo apache2

whereis firefox Muestra la ubicación de un archivo binario, ayuda o fuente “firefox”

which firefox Muestra la ruta completa al binario “firefox”

locate file1 Busca todas las instancias del archivo “file1”

locate \\*.ps Busca ficheros con extensión ps

(\*) locate ofrece mucha información de golpe y solo se actualiza una vez al día en la BBDD

find /home/s4uron/Documentos | grep dir Busca en la ruta especificada archivos/directorios que tenga la palabra dir

find /home –size +10k Busca en la ruta especificada archivos de tamaño de +10kb

grep -i palabra\_a\_buscar file1.txt Busca una palabra en un archivo de texto file1.txt

sed s/mysql/MySQL/g /etc/snort/snort.conf Sustituimos en todo el archivo snort.conf MySQL por mysql

**MONTANDO UN SISTEMA DE FICHEROS**

mount /dev/hda2 /mnt/hda2 Monta un disco llamado “hda2”. Hay que verificar la existencia del directorio “/mnt/hda2”, si no está, se debe crear

umount /dev/hda2 Desmontar el disco hda2, salir primero desde el punto de montaje “/mnt/hda2”

fuser -km /mnt/hda2 Forzar el desmontaje cuando el dispositivo está ocupado

findmnt Muestra la ruta de los puntos de montaje de todos los Filesystems

**DISCO**

df -h Muestra lista de las particiones montadas

df -i Muestra los inodos libres del Filesystems

du -sh dir1 Muestra el espacio usado por el directorio “dir1”

fdisk -l Muestra las particiones de disco, tamaño y tipos

hdparm -l /dev/hda Muestra información del disco “hda”

cfdisk Particionamiento de disco

(\*) Partición Swap: Actúa como memoria virtual RAM, similar al archivo de paginación de Windows (cuando la memoria RAM es excedida). Cuando se está quedando sin memoria RAM, tirará del espacio reservado en disco que es la SWAP.

lsblk List Block Device

(\*) Comandos para ver la swap del sistema: free -h , swapon -s , top , vmstat , cat /proc/swaps

fsck Chequeo de errores en el disco (File System Check)

fsck -p /dev/sdb1 Chequeando errores y reparándolos automáticamente

**ADMINISTRACIÓN DE USUARIOS Y GRUPOS**

groupadd grupo1Crea el grupo “grupo1”

groupdel grupo1 Borra el grupo “grupo1”

useradd user1 Crea el usuario “user1”

userdel user1 Borra el usuario “user1”

useradd -c user1 -g admin -d /home/user1 -s /bin/bash Crea usuario “user1” en el grupo admin y con línea comando bash y su directorio correspondiente

(\*) useradd es un comando que ejecuta un binario del sistema.

adduser es un script enperl que utiliza el binario useradd.

La ventaja del comando adduser es que crea el directorio home del usuario creado de manera automática, cosa que no hace useradd (hay que usar la opción -m)

passwd Cambia contraseña

passwd user1 Cambia contraseña de “user1”

chage -E 2023-12-31 user1 Establece caducidad de la contraseña de “user1”

su Log in como superusuario desde log normal

(\*) su = Switch User

su - Login como superusuario desde log normal pero heredando $PATH

su usuario1 Logarte como usuario dentro de archivo sudoers

sudo Permiso de superusuario

sudo su Elevación de privilegios a root

sudo visudo edit /etc/sudoers

sudo -l Muestra si tengo algún permiso especial que me hayan puesto a mí

psu Procedimiento para el escalado de privilegios

finger usuario1 Muestra información de “usuario1”

w Muestra todos los usuarios logados en el sistema

whoami Muestra quien soy yo

getent passwd Muestra los usuarios de Linux

cat /etc/passwd Muestra los usuarios de Linux

**PERMISOS EN FICHEROS**

Binaria Octal rwx 1 = ON

0 0 0 0 - - - 0 = OFF

0 0 1 1 - - x

0 1 0 2 - w -

0 1 1 3 - w x

1 0 0 4 r - -

1 0 1 5 r - x

1 1 0 6 r w -

1 1 1 7 r w x

r=read w=write x=execution (r=4, w=2, x=1)

u= usuario

g= grupo

o= otros

777=( 2^2+2^1+2^0) ( 2^2+2^1+2^0) ( 2^2+2^1+2^0)

1 1 1 1 1 1 1 1 1

r w x r w x r w x

7 7 7

u g o

755= ( 2^2+2^1+2^0) (2^2+0+2^0) (2^2+0+2^0)

1 1 1 1 0 1 1 0 1

r w x r x r x

7 5 5

u g o

ls -l Muestra los permisos del directorio actual

ls -l /home/user1 Muestra los permisos de una ruta determinada

chmod ugo+rwx directorio1 Da permisos de lectura. escritura y ejecución sobre el usuario, grupo y otros en el “directorio1”

(\*) UGO = U (user) G (group) O (others)

(\*) Por defecto cuando te descargas una nueva herramienta, Linux asigna automáticamente permisos de 666 (archivos) y 777 (directorios). No serás capaz de ejecutar un archivo recién descargado, aparecerá algo como “Permiso Denegado”

chmod go-rwx directorio1 Quita permisos de lectura, escritura y ejecución sobre el grupo y otros en el “directorio1”

chmod 777 directorio1 Da permisos de lectura, escritura y ejecución sobre el usuario, grupo y otros en el “directorio1”

chmod 755 /data/test.c Configrua rwx para el usuario y r\_x al grupo y otros, para test.c

chmod 4775 /data/test.c Doy permisos SUID a test.c

chown user1 file1 Cambia el dueño del fichero “file1” a “user1”

chown -R user1 directorio1 Cambia el propietario del “directorio1” y de todos los ficheros y directorios contenidos dentro a “user1”

chgrp grupo1 file1 Cambia el grupo del archivo “file1” a “grupo1”

chown user1:group1 file1 Cambia el propietario usuario y grupo del archivo “file1”

chmod u+s /bin/file1 Coloca el bit SUID en el fichero “file1”. El usuario que corra el archivo “file1” adquiere los mismos privilegios que el dueño

chmod u-s /bin/file1 Deshabilita el SUID en el fichero “file1”

find / -perm -u+s Busca todos los ficheros del sistema ( / ) con SUID configurado

find \-perm -4000 2>/dev/null Búsqueda de archivos con permisos SUID

(\*) Permisos especiales en Linux:

SUID (Set user ID) bit

SGID (Set group ID) bit

Sticky bit

SUID = Cualquier usuario puede ejecutar el archivo con los permisos del propietario, pero estos permisos no se extienden más allá del uso de este archivo.

SGID = Cuando un directorio es compartido por múltiples usuarios. Todos los usuarios en el grupo pueden ejecutar los archivos.

Sticky = Muy obsoleto. Permite a un usuario borrar o renombrar archivos dentro de un directorio.

Los hackers suelen explotar el SUID bit para llegar a obtener privilegios de root.

Si en vez de una x de ejecución, hay una s, quiere decir que cualquiera que corra ese archivo tiene privilegios de root.

La mayoría de archivos cuyo propietario es el root están en /usr/bin

chmod 2644 file1 Doy permisos de SGID a file1

chattr +i file1 Convierte el archivo “file1” en invariable, no puede ser borrado ni siquiera por root

lsattr Muestra los atributos especiales

umask Configurando permisos por defecto

(\*) En Kali y en la mayoría de los Sistemas Debian, el umask está preconfigurado a 022, lo que significa que en Kali para los archivos es por defecto 644 y para los directorios 755

Archivos Nuevos Directorios Nuevos

666 777

-022 -022

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

644 755

**ARCHIVOS Y FICHEROS COMPRIMIDOS**

(\*) Los paquetes que se instalan directamente desde la fuente se empaquetan con la primitiva, pero todavía útil herramienta de tar. Luego se comprimen empleando algún tipo de formato comprimido.

(\*) Los paquetes tar.gz o tgz:

1. tar -zxvf paquete.tar.gz (desempaquetamos)

2. cd nombre\_paquete\_desempaquetado

3. ./configure

4. make

5. make install

(\*) Los paquetes tar.bz2 o tbz2:

1. tar -jxvf nombre\_paquete.tar.bz2

2. cd nombre\_paquete\_desempaquetado

3. ./configure

4. make

5. make install

(\*) Los paquetes tar sin compresión

1. tar xvf nombre\_paquete.tar

2. Ver archivo README.txt o algo similar y seguir instrucciones

(\*) Los archivos binarios .bin, se instalan así:

1. cd directorio\_donde\_está\_binario

2. ./nombre\_binario.sh

(\*) Los archivos .run, se instalan así:

1. cd directorio\_donde\_esta\_paquete

2. sh ./nombre\_paquete.run

1. sh nombre\_script.sh

(\*) Instalación de scripts .py

1. Python nombre\_script.py install

bzip2 file1 Comprime el fichero “file1”

bunzip2 file1.bz2 Descomprime el fichero “file1”

gzip file1 Comprime el fichero “file1”

gunzip file1.gz Descomprime el fichero “file1”

tar -cf archivo1.tar file1 file2 dir1 Crea un tarball “archivo1.tar” de file1, file2 y dir1

tar -xf archivo1.tar Extrae el tarball “archivo1.tar”

tar -xf archivo1.tar –C /tmp Extrae el tarball “archivo1.tar” en “/tmp”

tar -tf archivo1.tar Muestra el contenido del “archivo1.tar”

(\*) c=crea v=muestra f=archivo x=extrae

zip file1.zip file1 Comprime el fichero “file1”

zip -r file1.zip archivo1 archivo2 dir1 Comprime en zip “file1.zip” de varios archivos y directorios “archivo1”, “archivo2”, “dir1”

unzip file1.zip Descomprime el archivo zip “file1.zip”

(\*) gzip -----🡪 Extensión .tar.gz ó .tgz (entre media de los dos)

bzip2 ---🡪 Extensión .tar.bz2 (Más lento pero ocupa menos)

compress -----🡪 Extensión .tar.z (Más rápido pero ocupan más)

compress archivo1 Comprime el archivo1 con compress

uncompress archivo1.tar.z Descomprime el archivo1

**PAQUETES RPM (REDHAT, CENTOS, FEDORA, …)**

rpm -i paquete.rpm Instala el “paquete.rpm”

rpm -e paquete.rpm Elimina el “paquete.rpm”

rpm -qa Muestra todos los paquetes rpm instalados en el sistema

rpm -qi paquete.rpm Muestra información de un paquete específico

rpm –qa | grep nombrepaquete Saber si está instalado un paquete

**ACTUALIZADOR DE PAQUETES YUM (REDHAT, CENTOS, FEDORA, …)**

yum install paquete1 Descarga e Instala un paquete rpm “paquete1”

yum update paquete1 Actualiza un paquete rpm “paquete1”

yum remove paquete1 Elimina un paquete rpm “paquete1”

yum list Muestra todos los paquetes instalados en el sistema

yum search paquete1 Busca “paquete1” en repositorio rpm

yum provides \*/netstat Para saber el paquete que contiene la aplicación netstat (ejemplo)

yum update Actualización SS.OO

**PAQUETES DEB (DEBIAN, UBUNTU, KALI, …)**

dpkg -i paquete1.deb Instala/Actualiza “paquete1.deb”

dpkg -r paquete1 Elimina “paquete1.deb”

dpkg -l Muestra todos los paquetes deb instalados en el sistema

dpkg -s paquete1 Muestra información del paquete indicado “paquete1”

**ACTUALIZADOR DE PAQUETES APT (DEBIAN, UBUNTU, KALI, …)**

apt-get install paquete1 Instala/Actualiza un paquete deb “paquete1”

apt-get purge paquete1 Desinstala el paquete1 y los archivos de configuración

apt-get autoremove Borra paquetes obsoletos

apt-cdrom install paquete1 Instala/Actualiza un paquete deb “paquete1” desde el cdrom

apt-get update Actualiza la lista de paquetes

apt-get upgrade Actualiza todos los paquetes instalados. Tarda mucho

apt-get remove paquete1 Elimina un paquete deb del sistema “paquete1”

apt-get update && apt-get install sudo Actualización e instalación del paquete sudo

apt-cache search snort Para buscar un paquete de software, ejemplo snort, en mi repositorio

apt install paquete1 Instala/Actualiza un paquete deb “paquete1”

apt update Actualiza la lista de paquetes

apt upgrade Actualiza todos los paquetes instalados

apt remove paquete1 Elimina un paquete deb del sistema “paquete1”

(\*) apt es más moderna que apt-get

(\*) /etc/apt/sources.list repositorio APT

**INSTALACIÓN DE SOFTWARE CON GIT**

git clone <https://www.github.com/balle/bluediving.git> Clonación del archivo a instalar

**PIP (ADMINISTRACIÓN PAQUETES DE PYTHON)**

apt-get install python3-pip Instalación de pip

pip3 install nombre\_paquete Instalación de un paquete pip

(\*) Cuando te descargas un paquete va a /usr/local/lib/versión\_python/paquete

pip3 show pysnmp Muestra si está instalado el paquete pysnmp

**VER EL CONTENIDO DE UN FICHERO**

cat file1 Muestra el contenido de un fichero “file1”

more file1 Muestra el contenido a lo largo de un fichero “file1”

less file1 Al contrario que more

head -2 file1 Muestra las dos primeras líneas del fichero “file1”

tail -2 file1 Muestra las dos últimas líneas del fichero “file1”

**ANÁLISIS DEL SISTEMA DE FICHEROS**

fsck /dev/hda1 Chequea/Repara la integridad del fichero del sistema Linux en disco hda1

fsck.ext2 /dev/hda1 Chequea/Repara la integridad del fichero del sistema ext2 en disco hda1

**FORMATEAR UN SISTEMA DE FICHEROS**

mkfs /dev/hda1 Crea un fichero de sistema (File System) tipo Linux en la partición hda1

mke2fs /dev/hda1 Crea un fichero de sistema (File System) tipo ext2 en hda1

**TRABAJO CON SWAP**

mkswap /dev/hda3 Crea un fichero de sistema swap

swapon /dev/hda3 Activa una nueva partición swap

**BACKUP**

dump -0aj -f /tmp/home0.back /home Backup completo del directorio “/home”

dump -1aj -f /tmp/home0.back /home Backup incremental del directorio “/home”

restore -if /tmp/home0.back Restauración de Backup

rsync -rogpav -delete /home /tmp Sincronización entre directorios

rsync -rogpav -e ssh -delete /home ip\_address:/tmp Sincronización a través de SSH

rsync -a /home/apps /backup Sincroniza el contenido de /home/apps con el de /backup

(\*) rsync, copia solo los archivos cambiados, trabaja sobre SSH

dd bs=1M if=/dev/hda | gzip | ssh user@ip\_addr ‘dd of=hda.gz’ Backup de hdd en un host remoto a través de ssh

dd if=/dev/sda of=/tmp/file1 Backup de un hdd a un fichero “file1”

tar -Puf backup.tar /home/user Backup incremetal del directorio /home/user

**RED LAN Y WIFI**

ifconfig Muestra todas las interfaces de red y las ip’s

(\*) Ruta : /sbin/ifconfig

ifconfig eth0 Muestra la configuración de la tarjeta de red Ethernet “eth0”

ifconfig eth0 up Activa la interface de red “eth0”

ifconfig eth0 down Desactiva interface de red “eth0”

ifup eth0 Activa la interface de red “eth0”

ifdown eth0 Deshabilita la interface de red “eth0”

ifconfig eth0 192.168.1.10 netmask 255.255.255.0 Configuración dirección IP

ifconfig eth0 192.168.181.115 Cambiamos la dirección IP

ifconfig eth0 hw ether 00:11:22:33:44:55 Cambiamos dirección MAC

ifconfig eth0:1 10.0.0.1/8 Añade interface virtual o alias

ifconfig eth0 promisc Poner en modo promiscuo (sniffing) la interfaz “eth0”

dhclient eth0 Activa la interface “eth0” en modo dhcp. Asigna nueva IP sin tener que resetear el sistema

route -n Muestra tabla de enrutamiento

route -e Más legible

route add -net 0/0 gw IP\_Gateway Configura ruta estática

route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.1 dev ens33 Configura ruta estática para buscar la red “192.168.0.0/16”

route del 0/0 gw IP\_Gateway Elimina la ruta estática

traceroute -4 10 redeszone.net Tracea la ruta de redeszone.net

ping host Muestra si está activo el host

hostname Muestra nombre del host del sistema

hostname -i Muestra la ip local

/etc/sysconfig/network Cambiar nombre al Servidor

/etc/sysconfig/network-scripts/ifcfg-eth0 Configuración ip estática

service network restart Reinicio de red

host [www.example.com](http://www.example.com) Resuelve el nombre del host a una dirección ip

nslookup [www.example.com](http://www.example.com) Resuelve el nombre del host a una dirección ip y viceversa

ip Configuración de red y enrutamiento

ip link show Muestra el estado de enlace de todas las interfaces

ip link set eth0 up Activa interface de red “eth0”

ip link set eth0 down Desactiva interface de red “eth0”

ip link ls up Muestra información de interfaces levantadas

ip addr show Muestra las direcciones IP y todos sus interfaces de red

ip address add 192.168.0.1/24 dev eth0 Asigna dirección IP al interface “eth0”

ip address del 192.168.0.1 dev eth0 Elimina dirección ip del interface “eth0”

ip addr add 10.0.0.1/8 dev eth0 label eth0:1 Añade interface virtual o alias

ip neigh add 192.168.0.1 lladdr 00:11:22:33:44:55 nud permanent dev eth0 Añade entrada en tabla ARP

ip link set dev eth0 arp off Cambia un dispositivo ARP a off

(\*) ip es más potente y moderno que ifconfig

netstat -r Muestra la tabla de enrutamiento

netstat -i Muestra las interfaces de red

netstat -put Muestra todas las conexiones de red activas y sus PID

netstat -plunt Muestra todos los servicios de escucha de red y sus PID

(\*) Muestra conexiones de red entrantes y salientes, tablas de enrutamiento de interfaz de red

VNStat Monitoriza tráfico de red

lsof -Pin Muestra lo mismo que el anterior

arp -a Muestra todas las entradas ARP de la tabla

arp -d maquina1 Suprime una entrada de la tabla

arp -s maquina1 AA:00:BB:11:CC:22 Añade una nueva entrada a la tabla

(\*) El comando arp permite hacer la correspondencia entre direcciones ip y direcciones MAC

arp -scan 10.0.0.0/24 Escaneo de redes

arp -i eth0 -s 192.168.0.1 00:11:22:33:44:55 Añade entrada en una tabla ARP

ifconfig -arp eth0 Cambia un dispositivo ARP a off

nslookup redeszone.net Consulta registros de recursos DNS de redeszone.net

tcpdump tcp port 80 Muestra todo el tráfico HTTP

tshark Analizador de paquetes de red

iwlist scan Scanea las redes inalámbricas

iwconfig Muestra todas las interfaces de red inalámbricas y sus ip’s

iwconfig eth1 Muestra la configuración de la tarjeta de red inalámbrica “eth1”

whois [www.example.com](http://www.example.com) Busca en la BBDD Whois información del host

dig [www.example.com](http://www.example.com) Obtiene DNS para el host

dig hackers-arise.com ns Muestra información del DNS

dig hackers-arise.com mx Muestra información del Servidor de Email

dig -x [www.example.com](http://www.example.com) Lookup del host

wget -r [www.example.com](http://www.example.com) Descarga un sitio web completo

wget -c [www.example.com/file.iso](http://www.example.com/file.iso) Descarga un fichero con posibilidad de parar y reanudar más tarde

curl [www.example.com](http://www.example.com) Outputs the webpage from url. Make any HTTP request you want

(\*) Cliente URL. Sirve para verificar la conectividad a las URL y como herramienta para transferencia de datos

ssh user1@host Conexión a un host como user1

ssh –p 22 user1@host Conexión a un host usando puerto (Por defecto ssh es el 22)

ssh host Conexión al host

ssh -D port user1@host Conecta y usa el puerto bind

telnet host Conexión al host vía telnet (no seguro), por defecto el puerto es el 23

ftp host Conexión al host vía ftp, por defecto el puerto es el 21

scp file1.txt [user1@192.168.163.10:/home/user1/Desktop](mailto:user1@192.168.163.10:/home/user1/Desktop) Copia archivo file1.txt en remoto al equipo 192.168.163.10

(\*) Comando de transferencia de archivos segura (sobre ssh) entre un host remoto y uno local o entre dos ubicaciones remotas. Puerto por defecto 22

scp -p [root@192.168.1.1:/media/scp.png](mailto:root@192.168.1.1:/media/scp.png) [edward@192.168.1.2:/desktop/destination](mailto:edward@192.168.1.2:/desktop/destination) Transferencia de archivos entre dos hosts remotos

scp /users/Edward/Desktop/scp.zip [root@192.168.0.2:/writing/article](mailto:root@192.168.0.2:/writing/article) Transferencia de archivos entre un host local y otro remoto

scp -p 2322 /users/Edward/Desktop/scp.zip [root@191.162.0.2:/writing/article](mailto:root@191.162.0.2:/writing/article) Transferencia de archivos entre un host local y otro remoto en el puerto 2322

scp [root@191.162.0.2:/writing/article/scp.zip](mailto:root@191.162.0.2:/writing/article/scp.zip) users/Edward/Desktop Transferencia de archivos entre un host remoto y otro local

scp archivo.txt [usuario@example.com:/ruta/al/directorio](mailto:usuario@example.com:/ruta/al/directorio) Transferencia de archivos de un host local a otro remoto

/etc/init.d/networking restart Reinicio manual de red

/etc/init.d/network-manager restart Reinicio del controlador de red

write user1 [tty] Comunicación por chat con usuario user1

w -192.168.163.25 Quien está conectado en remoto en la máquina 192.168.163.25

iptraf Muestra ocupación de ancho de banda

iftop Muestra ocupación de ancho de banda

ntop Muestra ocupación de ancho de banda

python3 -m http server Servicio de archivo desde un directorio

ipcalc Ves fácilmente que significa 13.21.2.3/25

hciconfig Es como el ifconfig pero para dispositivos bluetooth

hcitool Muestra información de dispositivos escaneados bluetooth

hcidump Para sniffar o capturar datos bluetooth

hciconfig hci0 up Levanta un dispositivo bluetooth (hci0)

hcitool scan Scaneo de dispositivos bluetooth

hcitool inq Inquires about a device, and receives the MAC address, clock offset and class (bluetooth)

sdptool browse dirección\_MAC Búsqueda de servicios en uno de los dispositivos detectados

l2ping dirección\_MAC –c 4 Para ver si un dispositivo es accesible

**REDES MICROSOFT WINDOWS (SAMBA)**

nbtscan ip\_addr Resolución de nombre de red bios

smbclient -L ip\_addr/hostname Muestra acciones remotas de un host en Windows

**TABLAS IP (FIREWALL)**

iptables -t filter -L Muestra todas las cadenas de la tabla de filtro

iptables -t nat -L Muestra todas las cadenas de la tabla NAT

iptables -t filter -A INPUT -p tcp -dport telnet -j ACCEPT Permite conexiones telnet para entrar

iptables -t filter -A OUTPUT -p tcp -dport http -j DROP Bloquea conexiones HTTP para salir

iptables -A INPUT -s 0.0.0.0/0 -p tcp -dport 22 -j DROP Bloquea acceso al puerto 22

service iptables start Iniciamos servicio iptables

nftables Versión más moderna de iptables

ufw deny 22/tcp Bloquea acceso al puerto 22

ufw allow 22/tcp Permite acceso al puerto 22

ufw allow from 192.168.163.25 Permite el acceso desde la dirección ip 192.168.163.25

ufw allow from 192.168.163.25 to ftp to 21 Permite acceso desde la dirección ip 192.168.163.25 del protocolo ftp al puerto 21

ufw allow from 10.0.0.1 to any port 22 Permite conexión de una ip (10.0.0.1)

ufw allow 10.0.0.1:10.0.0.10/tcp Permite la conexión de un rango de ip’s

ufw allow ssh Permite la comunicación por ssh

ufw enable Habilita ufw

ufw disable Deshabilita ufw

ufw loggin on Activa el login de ufw

ufw default allow Permite conexiones por defecto

ufw default deny Deniega todas las conexiones por defecto

(\*) Rutas: /usr/sbin/ufw

/etc/ufw/ufw.conf

/etc/sysconfig/iptables

**MONITORIZACIÓN-PROCESOS**

top Muestra las tareas que usan mayor consumo de CPU

ps Muestra los procesos activos

ps aux Muestra los procesos activos con mucho detalle

ps -eo command Muestra comandos que se están ejecutando en tiempo real en el sistema

pslist -t [\\192.168.163.24](file:///\\192.168.163.24) Lista los procesos de un equipo remoto

pmap Muestra el mapa de memoria de los procesos

pstree Muestra el árbol del sistema de procesos

kill -9 ID\_Proceso Fuerza el cierre de un proceso

kill pid 4050 Mata el proceso 4050

kill -1 ID\_Proceso Fuerza el cierre de un proceso para recargar la configuración

pskill -t [\\192.168.163.24](file:///\\192.168.163.24) -u (NombreEquipo\usuario privilegiado) -p (password) (Nombre proceso/PID) Mata un proceso en remoto

lsof /home/user Muestra lista de ficheros abiertos en una ruta dada

last reboot Muestra historial de reinicio

last Muestra último login en el sistema

free -m Muestra el estado de la RAM em megas

smartctl -A /dev/hda Monitorea la fiabilidad de un hdd a través de SMART

tail /var/log/messages Muestra los eventos del sistema

bg PID Background Jobs

fg PID Foreground Jobs

fg -n Brings job n to foreground

leafpad newscript & Con el símbolo &, abrirá el editor de texto en segundo plano y el terminal volverá a un nuevo command prompt. Con esto consumen menos recursos y vas más rápido

at 7:20pm Programas un proceso en el futuro (7:20pm)

vmstat -s -S M Muestra la memoria virtual

nice -n -10 /bin/slowprocess Para configurar prioridad cuando empieza un proceso

renice 20 id\_pid Para cambiar la prioridad de un proceso en funcionamiento

(\*) Tabla de valor de prioridad de procesos:

-20 0 +19

|------------------------------|---------------------------------|

Prioridad Valor por Defecto Prioridad

Alta Baja

(\*) Solo el usuario root puede aumentar la prioridad de un proceso, pero cualquier usuario puede bajar la prioridad.

(\*) Proceso zombie = Procesos que hacen que el sistema vaya lento o que se llegue a congelar el sistema.

kill -9 proceso1 Zombie o proceso malicioso

kill -9 zombieprocess Cuando no sabemos el proceso

exec Ejecuta los comandos sin crear un nuevo proceso

**CONVERSIÓN DE FICHEROS**

dos2unix filedos.txt fileunix.txt Convertir un formato de fichero texto desde MSDOS a UNIX

unix2dos fileunix.txt filedos.txt Convertir un formato de fichero de texto desde UNIX a MSDOS

**OTROS COMANDOS ÚTILES**

chsh Cambia el comando Shell

man comando Manual del comando

./configure Ejecuta el script de preparación de la instalación de archivos para compilación

./filename1 Ejecuta el archivo o script desde el directorio actual. También dice al sistema que si hay otro archivo en otro directorio llamado filename1 lo ignore y solo ejecute el del directorio actual.

make

make install

gpg -c file1 Encripta el archivo “file1”

gpg file1.gpg Desencripta el archivo “file1”

wc Muestra el número de bytes, palabras y líneas en un archivo

xargs Ejecuta comandos desde el standard input

strings archivo\_binario Para listar caracteres que se pueden leer en un archivo binario

getcap –r / 2>/dev/null Muestra el nombre y las capabilities

/dev/null Lugar para enviar la salida para que desaparezca

shred -f -n 10 /var/log/auth.log.\* Borrado seguro de un archivo, en este caso lo borra y lo sobreescribe 10 veces

crontab -e Edita la automatización de tareas

**ARCHIVOS DE CONFIGURACIÓN**

/etc/profile Variables de entorno del sistema

/etc/fstab Lista de dispositivos y sus puntos de montaje

/etc/rc.d/rc.local Bash Script que es ejecutado al fintal del proceso de login. Similar a autoexec.bat en Windows

/etc/HOSTNAME Contiene el nombre completo, incluyendo el dominio

/etc/cron.\* Automatización de ejecución de scripts a intervalos

/etc/hosts Lista todos los equipos conocidos y sus ip’s de la máquina. Para determinar a que dirección IP va el navegador cuando navego a por ejemplo [www.microsoft.com](http://www.microsoft.com) en lugar de dejar que el Servidor DNS decida

/etc/httpd/conf Configurción del Apache Web Server

/etc/apache2/apache2.conf Configuración del Apache Web Server

/etc/phpmyadmin/apache.conf Configuración de phpmyadmin apache

/etc/php.ini Configuración de php

/var/www/html Ubicación páginas Web

/etc/nginx/sites-available/default Sitio por defecto de Nginx

/etc/inittab Especifica el nivel de booteo de la máquina

/etc/resolv.conf Define las ip’s del Servidor DNS. Lo conveniente sería poner en el archivo resolv.conf un servidor DNS local y otro servidor DNS público, como por ejemplo 8.8.8.8 de Google

/etc/smb Configuración del servidor Samba. Permite compartir archivos e impresoras con clientes Microsoft

/etc/shells Muestra los escritorios de terminal del sistema

/etc/passwd Muestra los usuarios del sistema

/etc/group Muestra los grupos del sistema

/etc/sudoers Muestra listado de usuarios con permisos de sudo

/etc/systemd/system Donde se encuentran los Demonios del Sistema

/etc/logrotate.conf Donde se configuran los archivos log

(\*) Herramienta que permite gestionar los archivos de registro (logs). Permite comprimir, mover, renombrar, eliminar, archivar, etc. Serán borrados en un periodo específico.

/var/log Donde se encuentran los archivos log

/etc/ufw/ufw.conf Archivo de configuración del firewall ufw

/etc/rsyslog.conf Configuración del Registro de Eventos

/etc/snort/snort.conf Configuración del IDS Snort

/etc/apt/sources.list Configuración de los Repositorios de instalación de paquetes

/etc/yum.repos.d Configuración de los Repositorios de instalación de paquetes

/etc/services Muestra el nombre, puerto, protocolo de todos los servicios de red

/etc/inetd.conf Fichero utilizado por el demonio inetd, conocido como el supervisor de red. El demonio inetd es el encargado de ofrecer la mayoría de servicios de nuestro equipo hacia el resto de máquinas, debemos cuidar mucho de su configuración

/etc/ssh/sshd\_config Fichero de configuración de ssh

/etc/network/interfaces Configuración manual de red

/etc/NetworkManager/NetworkManager.conf Configuración de red

/etc/init.d Servicio de Sistemas

/etc/init.d/rc Cuando se inicia Linux, un número de scripts corren en la configuración. Estos son conocidos como rc scripts. Después de que el Kernel ha inicializado y cargado sus módulos, el Kernel inicia un demonio conocido como init.d. Este demonio empieza a correr un número de scripts que están en esta ruta.

/etc/rsyslog.d Demonio que registra eventos automáticamente en el PC

/etc/sysconfig/network Cambiar el nombre al servidor, puerta enlace, etc

/etc/sysconfig/iptables Configuración de Iptables

/etc/sysconfig/network-scripts/ Configuración de ip

/etc/sysctl.conf Para tunear el Kernel. Hay que tener mucho cuidado al modificar este archivo. Los cambios que se hagan en sysctl.conf solo tienen efecto cuando reinicias el sistema.

**EDITORES DE TEXTO**

Gedit

Leafpad

Vi

Cat

Vim

Kate

Emacs

Nano

**SERVICIOS**

(\*) Demonio o Servicio es un programa que se ejecuta en segundo plano, fuera del control interactivo de los usuarios del sistema

systemctl start servicio1 Inicia el servicio “servicio1”

service servicio1 start Inicia el servicio “servicio1”

(\*) service funciona en los archivos /etc/init.d (antiguamente)

systemctl funciona en los archivos /lib/systemd (actualmente)

(\*) Si hay un archivo para su servicio en /lib/systemd, lo usará primero y, si no, volverá al archivo en /etc/init.d

(\*) Si systemctl está disponible, será mejor usarlo (más opciones de control), service es más básico

service rsyslog stop Para el servicio rsyslog (Registro de Eventos)

systemctl status cup.service Mira el estado del servicio cup.service

service mysql start Inicia el servicio mysql

/etc/init.d/servicio1 status Chequea servicio (SysV)

/etc/init.d/servicio1 start Inicia servicio (SysV)

rcconf Comando para comprobar que servicios se inician en el sistema

update-rc.d servicio1 enable Añade servicios al rc.d para que corran al inicio del sistema

**BIND**

Es el Servidor DNS más utilizado de Internet, especialmente en sistemas UNIX. Utiliza el puerto 53 para transferencias.

**ESCANEO DE PUERTOS EN EQUIPOS REMOTOS**

nmap 192.168.163.248 -p 22 Escaneo de la dirección ip 192.168.163.248 en el puerto 22

nc -zv 192.168.122.88 80 Escaneo de la dirección ip 192.168.122.88 en el puerto 80 (netcat)

**FICHEROS LOGS IMPORTANTES**

/var/log/messages (obsoleto) Autenticación de Usuarios

/var/log/syslog (actual) Logs del sistema

/var/log/dmesg Dispositivos

/var/log/auth.log Autorización

/var/log/daemon.log Servicios

/var/log/lastlog Usuarios recientes

/var/log/kern.log Kernel

/var/log/dpkg.log Instalación/Desinstalación en Debian

/var/log/btmp Intentos de autenticación fallidos

/var/log/user.log Eventos sesiones de usuarios

/var/log/wtmp Usuarios autenticados actualmente

/var/log/boot.log Mismas trazas que el sistema de arranque

/var/log/alternatives.log Cambios realizados en el software instalado

/var/log/cron Tareas programadas ejecutadas

/var/log/httpd Servidor Apache

/var/log/apache2 Servidor Apache

/var/log/lighttpd Servidor ligero Apache

/var/log/mail Correo

/var/log/samba Servidor Samba

/var/log/mysqld.log Servidor mysql

/var/log/audit Auditoria

/etc/rsyslog.d For forwarding log messages in an IP network

/etc/rsyslog.conf Configuración de rsyslog (Registro de eventos)

**SYSTEMCTL**

(\*) systemctl, es la herramienta de administración central para controlar el sistema init.

systemd es un sistema init y un administrador del sistema que se ha convertido en el nuevo estándar para las distribuciones Linux.

La finalidad principal de un sistema init es inicializar los componentes que deben iniciarse tras arrancar el kernel Linux. El sistema init también se utiliza para administrar servicios y daemons para el servidor en cualquier momento mientras se ejecuta el sistema

systemctl start servicio1 Inicia servicio1

systemctl stop servicio1 Para servicio1

systemctl restart servicio1 Reinicio servicio1

systemctl reload servicio1 Recarga servicio1

systemctl status servicio1 Estado de servicio1

systemctl enable servicio1 Habilita servicio1

systemctl disable servicio1 Deshabilita servicio1

systemctl is-enabled servicio1 Habilitado en arranque servicio1

systemctl Enumeración de unidades en ejecución

systemctl -failded Unidades fallidas

systemctl list-units -t service Enumeración de servicios activos

systemctl poweroff Apagado del sistema y máquina

systemctl halt Apaga el sistema pero no la máquina

systemctl status sshd -H [root@192.168.1.10](mailto:root@192.168.1.10) Administración de sistemas remoto

systemctl | grep running Servicios que están activos

**JOURNALCTL**

(\*) Herramienta para acceder a los registros (logs) del sistema. Equivale al viejo /var/log/messages

Journalctl es más moderno que /var/log/messages

journalctl Sistema de registro

journalctl -b Mensajes de arranque

journalctl -f Registro del sistema en tiempo real

journalctl /usr/sbin/servicio1 Verificación de registros específicos

**HOSTNAMECTL**

hostnamectl Muestra y cambia el nombre del host

**ESTRUCTURA JERARQUICA DE LINUX**

/

/bin

/boot

/etc /opt

/usr /local /share /bin /include /lib /sbin

/var /cache /lib /yp /lock /opt /run /tmp /spool /log

/sbin

/tmp

/dev

/home

/lib

/mnt

/opt

/root

/bin Comandos binarios (ejecutables) esenciales

/boot Archivos estáticos del selector de arranque

/dev Archivos de unidades

/etc Archivos de configuración de programas

/home Directorio ‘home’ de usuario

/lib Librerias esenciales compartidas y módulos del Kernel (similares a dll de Windows)

/media Punto de montaje para medios removibles

/mnt Punt de montaje temporal para archivos del sistema

/opt Agregados de paquetes de Software y Aplicaciones

/sbin Binarios del Sistema

/srv Datos para los servicios provistos por este sistema

/tmp Archivos temporales

/usr Utilidades y aplicaciones de Multi-usuario

/var Variables de archivo

/root Directorio ‘home’ del usuario root

/proc Documentación del sistema de archivos virtual del Kernel y las condiciones de los procesos en archivos de texto

**LVM**

Logical Volume Manager

LVM

File Systems /mnt/data /mnt/backup

Logical Volumes /dev/datavg/data /dev/datavg/backup

Volume Group datavg

Physical Volumes /dev/sda1 /dev/sdb1 /dev/sdc1 /dev/sdd1

Partitions /dev/sda1 /dev/sdb1 /dev/sdc1 /dev/sdd1

Hard Drives /dev/sda /dev/sdb /dev/sdc /dev/sdd

**CONEXIÓN POR RDP DE WINDOWS A LINUX DE FORMA GRÁFICA**

1. # yum install epel-release
2. # yum install xrdp
3. # nano /etc/sysconfig/iptables
4. -A INPUT -m --state NEW -m tcp -p tcp --dport 3389 -j ACCEPT
5. -A INPUT -m --state NEW -m tcp -p tcp --dport 3350 -j ACCEPT
6. # service iptables restart
7. Nos conectamos desde Windows por mstsc a la máquina CentOS y nos deja conectarnos de forma gráfica.

**INSTALACIÓN DE APACHE**

1. # yum install httpd
2. # chkconfig httpd
3. # service httpd start
4. Abrimos navegador en 127.0.0.1 para que cargue página por defecto de Apache

**INSTALACIÓN PHP**

1. # yum install php
2. # service httpd restart
3. # nano /var/www/html/test.php
4. <?php phpinfo();?>
5. Abrimos navegador en 127.0.0.1/test.php

**INSTALACIÓN MySQL**

1. # yum install mysql-server mysql
2. # service mysqld restart
3. # mysql\_secure\_installation
4. # chkconfig mysqld

**VARIABLES**

env Muestra todas las variables del Sistema

echo $SHELL Muestra terminales del Sistema

echo $PATH Muestra la ubicación (ruta) de un comando

export PATH=/tmp:$PATH Exporto /tmp a la variable PATH. Ahora se buscará primero en /tmp

(\*) Tipos de Variables:

1. Environment Variables (MAYUSCULAS. Variables de todo el Sistema)

2. Shell Variables (MINUSCULAS. Son solo válidas en la Shell en que se establecen)

set Muestra todas las variables

set | more Muestra todas las Environment Variables

set | grep HISTSIZE Filtrando para variables particulares

HISTSIZE=0 Cambiando valores de variable para una sesión

export HISTSIZE Cambiando valores de variable permanentemente

PS1=”rpuebg:#” Para cambiar el Shell Prompt en la sesión actual

export PS1=’rpuebg:#’ Para cambiar el Shell Prompt en todas las sesiones

PATH=$PATH:/root/newhackingtool Añadiendo una variable al PATH. Para poder usar la nueva herramienta desde cualquier directorio y no tener que navegar a la ruta donde se encuentra para poder ejecutarlo.

(\*) Añadir una ruta al PATH es conveniente cuando se usan directorios muy a menudo, pero no es conveniente añadir muchas porque en la búsqueda ralentizará el sistema.

MINUEVAVARIABLE=”H4ck” Creando una variable de usuario definida

echo $MINUEVAVARIABLE Muestra la nueva variable

unset MINUEVAVARIABLE Elimina una variable de usuario definida