

COMANDOS LINUX PARTE 1

Rosario Novelo Joahan Emmanuel

Sistemas Operativos

1. Obtén la ayuda de ping

```
akabane@debian:~$ ping -help

Usage
ping [options] <destination>

Options:
<destination>      dns name or ip address
-a                 use audible ping
-A                 use adaptive ping
-B                 sticky source address
-c <count>         stop after <count> replies
-C                 call connect() syscall on socket creation
-D                 print timestamps
-d                 use SO_DEBUG socket option
-e <identifier>    define identifier for ping session, default is random
                  SOCK_RAW and kernel defined for SOCK_DGRAM
                  Impls using SOCK_RAW (for IPv4 only for identifier 0)
```

2. Enviar un ping a 127.0.0.1 aplicando cualquier parámetro

```
akabane@debian:~$ ping -a 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.123 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.035 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=64 time=0.029 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=64 time=0.030 ms
64 bytes from 127.0.0.1: icmp_seq=10 ttl=64 time=0.028 ms
64 bytes from 127.0.0.1: icmp_seq=11 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=12 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=13 ttl=64 time=0.027 ms
64 bytes from 127.0.0.1: icmp_seq=14 ttl=64 time=0.087 ms
64 bytes from 127.0.0.1: icmp_seq=15 ttl=64 time=0.024 ms
```

3. Verificar la conectividad del equipo utilizando el comando ping, anotar conclusiones

```
akabane@debian:~$ ping -c 4 www.google.com
PING www.google.com (142.250.189.132) 56(84) bytes of data.
64 bytes from mia09s26-in-f4.1e100.net (142.250.189.132): icmp_seq=1 ttl=117
ms
64 bytes from mia09s26-in-f4.1e100.net (142.250.189.132): icmp_seq=2 ttl=117
ms
64 bytes from mia09s26-in-f4.1e100.net (142.250.189.132): icmp_seq=3 ttl=117
ms
64 bytes from mia09s26-in-f4.1e100.net (142.250.189.132): icmp_seq=4 ttl=117
ms

--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3207ms
rtt min/avg/max/mdev = 21.610/24.979/28.601/2.476 ms
```

4. Obten la ayuda de nslookup

```
C:\Windows\System32>nslookup
Servidor predeterminado: dns.google
Address: 8.8.8.8

> help
Comandos: (los identificadores se muestran en mayúsculas, [] significa opcional)
NOMBRE - imprimir información acerca de NOMBRE de host o de dominio con el
NOMBRE1 NOMBRE2 - igual que el anterior, pero se usa NOMBRE2 como servidor
help o ? - imprimir información acerca de comandos comunes
set OPCIÓN - establecer una opción
all - opciones de impresión, servidor actual y host
[no]debug - imprimir información de depuración
[no]d2 - imprimir información de depuración exhaustiva
[no]defname - anexar el nombre de dominio a cada consulta
[no]recurse - pedir respuesta recursiva a la consulta
[no]search - usar la lista de búsqueda de dominios
[no]vc - usar siempre un circuito virtual
domain=NOMBRE - establecer nombre de dominio predeterminado en NOMBRE
srchlist=N1[/N2/.../N6] - establecer dominio en N1 y lista de búsqueda en N1,N2,...,N6
root=NOMBRE - establecer servidor raíz en NOMBRE
retry=X - establecer número de reintentos en X
timeout=X - establecer intervalo de tiempo de espera inicial en X segundos
type=X - establecer tipo de consulta (p. ej., A,AAAA,A+AAAA,ANY,CNAME,DS,HTTPS,LOC,NAPTR,NS,NSID,RP,SSHFP,SPF,SRV,TLSA,TSIG,URI,WWW)
querytype=X - igual que type
class=X - establecer clase de consulta (p. ej., IN (Internet), ANY)
[no]mxfr - usar transferencia de zona rápida MS
[no]nsid - versión actual que se usará en la solicitud de transferencia de zona
```

5. Resolver la direccion https://upqroo.edu.mx / con nslookup

```
akabane@debian:~$ nslookup https://upqroo.edu.mx/
Server:      8.8.8.8
Address:     8.8.8.8#53
```

```
** server can't find https://upqroo.edu.mx/: NXDOMAIN
```

—

6. Hacer ping a la ip anterior

```
akabane@debian:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=20.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=21.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=22.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=22.2 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3339ms
rtt min/avg/max/mdev = 20.763/21.691/22.699/0.803 ms
```

7. Obtén la ayuda del comando netstat

```
akabane@debian:~$ netstat -help
usage: netstat [-vWeenNcCF] [<Af>] -r netstat {-V|--version|
netstat [-vWnNcaeol] [<Socket> ...]
netstat { [-vWeenNac] -i | [-cnNe] -M | -s [-6tuw] }

-r, --route          display routing table
-i, --interfaces     display interface table
-g, --groups          display multicast group memberships
-s, --statistics     display networking statistics (like
-M, --masquerade     display masqueraded connections

-v, --verbose        be verbose
-W, --wide           don't truncate IP addresses
-n, --numeric        don't resolve names
--numeric-hosts      don't resolve host names
--numeric-ports      don't resolve port names
--numeric-users      don't resolve user names
```

8. Mostrar todas las conexiones y puertos de escucha

```
akabane@debian:~$ netstat an
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          _gateway:bootps
udp      0      0 debian:bootpc
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State                   I-Node   Path
unix   3      [ ]                 STREAM                CONNECTED              39445    /run/user
unix   3      [ ]                 STREAM                CONNECTED              36992    /run/user
unix   3      [ ]                 STREAM                CONNECTED              18852
unix   3      [ ]                 STREAM                CONNECTED              19925
unix   3      [ ]                 STREAM                CONNECTED              18574
unix   3      [ ]                 STREAM                CONNECTED              19942    /run/user
unix   3      [ ]                 STREAM                CONNECTED              18604    /run/dbus
unix   3      [ ]                 STREAM                CONNECTED              19944
unix   3      [ ]                 STREAM                CONNECTED              19827
unix   3      [ ]                 STREAM                CONNECTED              16875
unix   3      [ ]                 STREAM                CONNECTED              40187    /run/user
```

9. Ejecutar netstat sin resolver nombres de dominio

```
akabane@debian:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
udp      0      0 debian:bootpc           _gateway:bootps         ESTABLIS
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags               Type                   State                   I-Node   Path
unix   3      [ ]                 STREAM                CONNECTED              39445    /run/user/1000/bu
unix   3      [ ]                 STREAM                CONNECTED              36992    /run/user/1000/pu
unix   3      [ ]                 STREAM                CONNECTED              18852
unix   3      [ ]                 STREAM                CONNECTED              19925
unix   3      [ ]                 STREAM                CONNECTED              18574
unix   3      [ ]                 STREAM                CONNECTED              19942    /run/user/1000/bu
unix   3      [ ]                 STREAM                CONNECTED              18604    /run/dbus/system_
unix   3      [ ]                 STREAM                CONNECTED              19944
unix   3      [ ]                 STREAM                CONNECTED              19827
unix   3      [ ]                 STREAM                CONNECTED              16875
```

10. Mostrar todas las conexiones TCP

```
akabane@debian:~$ netstat -t
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
```

11. Mostrar todas las conexiones UDP

```
akabane@debian:~$ netstat -u
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 debian:bootpc          _gateway:bootps        ESTABL
```

12. Utilizar el comando tasklist

```
akabane@debian:~$ top
top - 00:20:35 up 2:21, 1 user, load average: 1.35, 0.65, 0.30
Tareas: 171 total, 1 running, 170 sleeping, 0 stopped, 0 zombie
%Cpu(s): 3.8/4.2 8[|||||]
MiB Mem : 8177.2 total, 5398.4 free, 1561.0 used, 1496.5 buff/cache
MiB Intercambio: 975.0 total, 975.0 free, 0.0 used, 6616.2 avail

Unknown command - try 'h' for help
  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
 1243 akabane   20   0 3719.6m 286.9m 130.2m S   8.7   3.5   8:34.89 gnome
 3811 akabane   20   0 2777.0m 292.2m 133.3m S   5.5   3.6   0:14.02 firef
 1401 akabane   20   0 305.2m  13.8m   6.8m S   2.4   0.2   0:17.63 ibus-
 3347 akabane   20   0 546.8m  54.0m  38.4m S   2.4   0.7   0:15.56 gnome
 3810 akabane   20   0  11.4m   5.2m   3.3m R   1.6   0.1   0:00.23 top
 1609 akabane   20   0 157.0m   9.0m   6.4m S   0.8   0.1   0:04.91 ibus-
    1 root      20   0  164.1m  12.2m   9.0m S   0.0   0.1   0:02.09 syste
    2 root      20   0   0.0m   0.0m   0.0m S   0.0   0.0   0:00.06 kthre
    3 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 rcu_g
    4 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 rcu_g
    5 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 slab_
    6 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 netns
    8 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 kwork
   10 root      0 -20   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 mm_pe
   11 root      20   0   0.0m   0.0m   0.0m I   0.0   0.0   0:00.00 rcu_t
   12 root      20   0   0.0m   0.0m   0.0m T   0.0   0.0   0:00.00 rcu_t
```

13. Utilizar el comando taskkill

```
akabane      3539 18.6  2.3 2684860 196048 ?        Sl    00:14   0:58 /usr/lib/
akabane      3544  0.1  0.8 233516 70808 ?        S     00:14   0:00 /usr/bin/
akabane      3548  0.1  1.0 549072 83872 ?        Ssl   00:14   0:00 /usr/libe
akabane      3569  0.0  0.3 191072 25780 ?        Sl    00:14   0:00 /usr/libe
akabane      3632  0.0  0.4 208724 37080 ?        Sl    00:14   0:00 /usr/lib/
akabane      3663  0.1  0.8 2388740 75144 ?        Sl    00:14   0:00 /usr/lib/
akabane      3694  0.1  0.8 2390992 67992 ?        Sl    00:14   0:00 /usr/lib/
akabane      3701  0.0  0.7 2390992 66200 ?        Sl    00:14   0:00 /usr/lib/
akabane      3705  0.0  0.7 2390992 66136 ?        Sl    00:14   0:00 /usr/lib/
root         3769  0.0  0.0      0      0 ?        I     00:15   0:00 [kworker/
akabane      3797  0.0  0.0  11268  4888 pts/0    R+    00:19   0:00 ps aux
akabane@debian:~$ kill 3539
```

14. Utilizar el comando tracert

```
akabane@debian:~$ traceroute google.com
traceroute to google.com (142.250.217.238), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.2) 0.968 ms 0.599 ms 0.569 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * █
```

15. Utilizar el comando ARP

```
akabane@debian:~$ ip neigh show
10.0.2.2 dev enp0s3 lladdr 52:54:00:12:35:02 REACHABLE
akabane@debian:~$
```

Parte 2

1. ¿Para qué sirve el comando ping?

El comando sirve para que se pueda verificar los paquetes enviados y se detecte si funciona la conexión

2. ¿Para qué sirve el comando nslookup?

Sirve para resolver nombres de dominios que permiten entender las direcciones en cuanto a sus configuraciones DNS

3. ¿Para qué sirve el comando netstat?

Te muestra estadísticas de red que son muy comprometidas, en este caso también se pueden poner en estándares donde mejore su calidad de función.

4. ¿Para qué sirve el comando tasklist?

Ver toda la lista de procesos cuales están funcionando y si existen desconocidos

5. ¿Para qué sirve el comando taskkill?

Para detener un proceso que no se elimina o que es indeseado

6. ¿Para qué sirve el comando tracert?

Para conocer los paquetes de datos desde la computadora desde toda su conexión hasta donde es lanzada

7. ¿Cómo ayudan los primeros tres comandos para detectar problemas de red?

- ping se utiliza para verificar la conectividad básica y detectar problemas de disponibilidad.
- nslookup ayuda a solucionar problemas de resolución de nombres de dominio.
- netstat permite monitorear la actividad de red y diagnosticar conexiones y puertos problemáticos.

Parte 3

atmadm

Este comando se utiliza para administrar conexiones de red de modo asincrónico (ATM). En la mayoría de los casos, su uso es técnico y específico para la administración de redes ATM, por lo que no se usa comúnmente en situaciones cotidianas.

atmadm -c consulta

bitsadmin

Permite administrar tareas de transferencia de archivos en segundo plano (Background Intelligent Transfer Service). Un ejemplo práctico sería usarlo para descargar archivos grandes en segundo plano.

bitsadmin /transfer mi_descarga /download /priority normal http://ejemplo.com/archivo.zip C:\carpeta\archivo.zip

cmstp

Utilizado para instalar o desinstalar perfiles de conexión de red. Esto es útil principalmente en entornos corporativos para implementar configuraciones de red específicas.

cmstp /s archivo_de_configuracion.inf

ftp

El comando FTP se utiliza para transferir archivos entre sistemas a través del Protocolo de Transferencia de Archivos. Puedes conectarte a un servidor FTP y transferir archivos

ftp ejemplo.com

get

get archivo_remoto.txt

Muestra la dirección MAC (Media Access Control) de una interfaz de red. Puedes utilizarlo para obtener la dirección MAC de tu tarjeta de red, lo que es útil para la resolución de problemas de red.

hostname

Muestra el nombre del host o computadora local. Es útil para averiguar el nombre de tu propia computadora

nbstat

Proporciona información sobre la resolución de nombres de NetBIOS en una red. Se usa para diagnosticar problemas de resolución de nombres NetBIOS.

nbstat -A 192.168.1.1

net

Este comando se utiliza para administrar varias configuraciones y recursos de red. Por ejemplo, puedes usar net user para administrar cuentas de usuario y net share para administrar recursos compartidos.

net user nombre_usuario contraseña /add

net user

Permite conectar o desconectar recursos compartidos de red en tu computadora. Por ejemplo, puedes mapear una unidad de red

net user nombre_usuario contraseña /add

netsh

Es una herramienta de configuración de red versátil que permite modificar la configuración de red, firewall, VPN y más. Por ejemplo, puedes usar netsh para configurar un servidor proxy.

netsh interface ipv4 show interfaces

pathping

Combina la funcionalidad de ping y tracert. Proporciona información sobre la ruta y la latencia en una red.

pathping www.google.com

rcp

se utiliza para copiar archivos desde y hacia sistemas remotos en una red.

rcp archivo.txt usuario@servidor:/ruta/destino/

rexec

permite ejecutar comandos en un sistema remoto. Se utiliza para iniciar programas o scripts en un sistema remoto si tienes permisos para hacerlo. Por razones de seguridad, su uso se ha vuelto menos común debido a posibles vulnerabilidades.

rexec servidor comando

route

se utiliza para ver y manipular la tabla de enrutamiento en sistemas Windows. Puedes utilizarlo para agregar, eliminar o modificar rutas de red. Por ejemplo, para agregar una ruta predeterminada a través de una puerta de enlace específica

route add 0.0.0.0 mask 0.0.0.0 192.168.1.1

rpcping

Este comando se utiliza para realizar pruebas de ping a servicios RPC (Remote Procedure Call). Es útil para verificar la conectividad y la disponibilidad de servicios RPC en sistemas remotos.

rpcping -s servidor

rsh

Similar a rexec, el comando rsh (Remote Shell) permite ejecutar comandos en sistemas remotos, pero su uso también ha disminuido debido a preocupaciones de seguridad. Puede ejecutar comandos en un sistema remoto si tienes permisos para hacerlo.

rsh servidor comando

tcmsetup

Este comando se utiliza para configurar la autenticación de Trusted Platform Module (TPM) en sistemas Windows. Es una herramienta técnica utilizada para configurar la seguridad de hardware en sistemas compatibles con TPM.

tcmsetup -v -f -b 123456

telnet

El comando telnet se utiliza para conectarse a otros dispositivos o servidores a través de una sesión de terminal. Permite acceder a sistemas remotos para administrarlos o realizar pruebas

telnet servidor

tftp

El Protocolo de Transferencia de Archivos Trivial (TFTP) se utiliza para transferir archivos de manera sencilla desde y hacia sistemas remotos. Es una forma simple de copiar archivos en sistemas en red.

tftp -i servidor GET archivo.txt