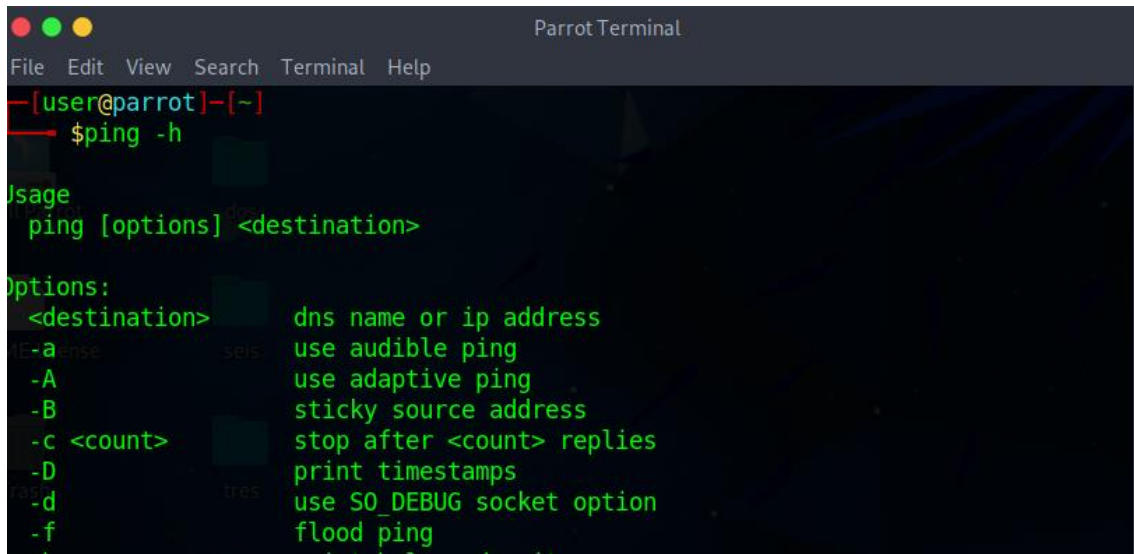


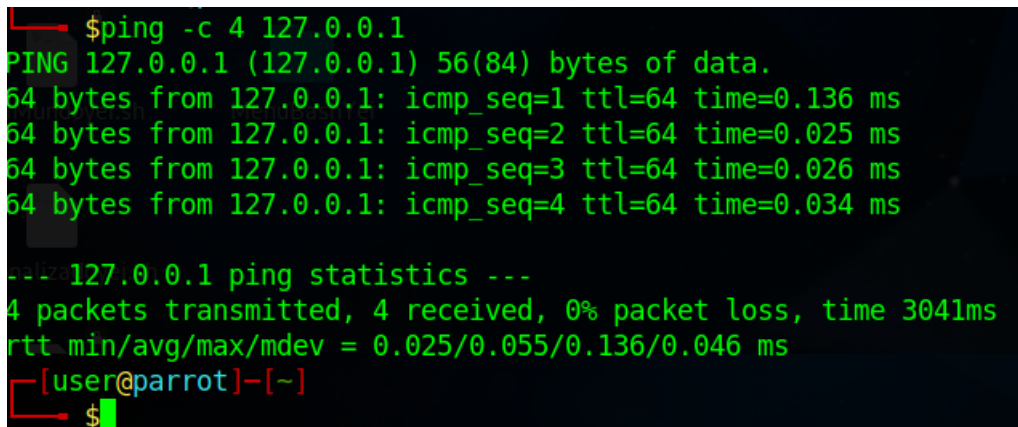
A) Anotar los comandos necesarios para ejecutar las siguientes instrucciones desde la consola de 1.- Obtener La Ayuda del comando ping (ping -h)



```
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~$ ping -h
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
  -D             print timestamps
  -d             use SO_DEBUG socket option
  -f             flood ping
```

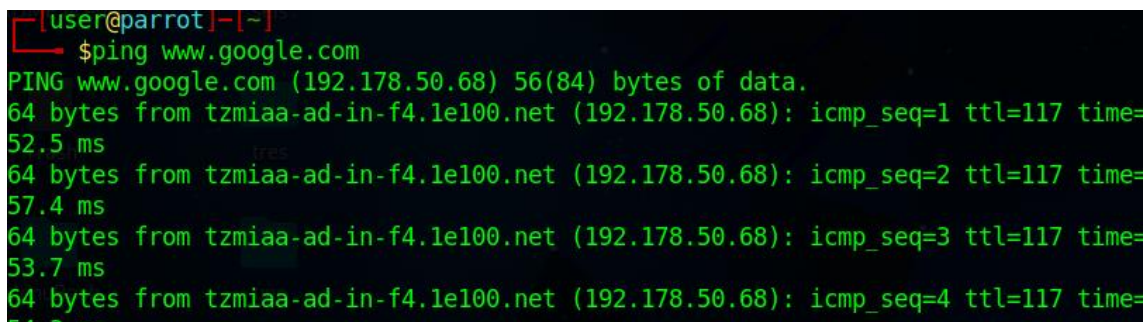
2.- Enviar un ping a 127.0.0.1 aplicando cualquier parámetro



```
[user@parrot]~$ ping -c 4 127.0.0.1
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=0.136 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.025 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.026 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.034 ms

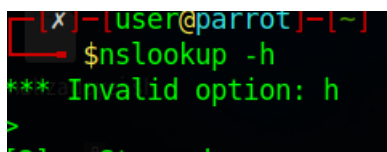
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/mdev = 0.025/0.055/0.136/0.046 ms
[user@parrot]~$
```

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



```
[user@parrot]~$ ping www.google.com
PING www.google.com (192.178.50.68) 56(84) bytes of data.
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=1 ttl=117 time=52.5 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=2 ttl=117 time=57.4 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=3 ttl=117 time=53.7 ms
64 bytes from tzmiaa-ad-in-f4.1e100.net (192.178.50.68): icmp_seq=4 ttl=117 time=54.2 ms
```

4.-Obtener la ayuda del comando nkslookup



```
[x]-[user@parrot]~$ nkslookup -h
***Invalid option: h
>
```

5- Resolver la dirección ip de <https://upgrooo.edu.mx/> usando nslookup

```
$nslookup upgroo.edu.mx
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   upgroo.edu.mx
Address: 77.68.126.20
; communications error to 192.168.1.254#53: timed out
; communications error to 192.168.1.254#53: timed out
; communications error to 192.168.1.254#53: timed out
; no servers could be reached
```

6.-Hacer ping a la ip obtenido en el paso anterior anotar conclusiones

```
[user@parrot]~$ ping 142.250.217.238
PING 142.250.217.238 (142.250.217.238) 56(84) bytes of data.
64 bytes from 142.250.217.238: icmp_seq=1 ttl=117 time=306 ms
64 bytes from 142.250.217.238: icmp_seq=2 ttl=117 time=56.6 ms
64 bytes from 142.250.217.238: icmp_seq=3 ttl=117 time=57.0 ms
64 bytes from 142.250.217.238: icmp_seq=4 ttl=117 time=54.4 ms
64 bytes from 142.250.217.238: icmp_seq=5 ttl=117 time=52.4 ms
64 bytes from 142.250.217.238: icmp_seq=6 ttl=117 time=52.8 ms
^Z
```

7.- Obtener la ayuda del comando netstat

```
$netstat -h
Usage: netstat [-vWeenNcCF] [<Af>] -r          netstat {-V|--version|-h|--help}
       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 SNMP)
-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

```
[user@parrot]~$ netstat -anp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
ID/Program name
tcp        0      0 0.0.0.0:22               0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 10.0.2.15:68            10.0.2.2:67            ESTABLISHED
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
```

## 9.- Ejecutar netstat sin resolver nombres de dominio o puerto

```
[user@parrot]~$ netstat -anp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
ID/Program name
tcp        0      0 0.0.0.0:22               0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
udp        0      0 10.0.2.15:68            10.0.2.2:67            ESTABLISHED
raw        0      0 0.0.0.0:1               0.0.0.0:*               7
```

## 10.- Mostrar las conexiones TCP

```
[user@parrot]~$ netstat -tn
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

## 11.- Mostrar las conexiones UDP

```
[user@parrot]~$ netstat -un
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 10.0.2.15:68            10.0.2.2:67            ESTABLISHED
```

12.- Utilizar el comando tasklist

```
[user@parrot]~$ ps
  PID TTY          TIME CMD
 18422 pts/0    00:00:00 bash
 18481 pts/0    00:00:00 ping
 18483 pts/0    00:00:00 nslookup
```

13.- Utiliza el comando taskkill

```
[user@parrot]~$ killall 1010
1010: no process found
[x]-[user@parrot]~$
```

14.- Utilizar el comando tracer

```
[user@parrot]~$ traceroute www.google.com
traceroute to www.google.com (192.178.50.68), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.564 ms  0.172 ms  0.183 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  *
```

15.- Utilizar el comando ARP

```
[user@parrot]~$ arp -a
? (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
[user@parrot]~$
```

### **1.- ¿Para qué sirve el comando ping?**

El Ping es como el intermediario de la red. Les manda mensajes a otros aparatos y espera respuestas para ver si están en línea. Si tardan mucho en contestar, es señal de que algo anda mal.

### **2.-¿Para qué sirve el comando nslookup?**

Nslookup es como el traductor de nombres de la red. Le preguntas sobre un sitio web y te dice la dirección secreta (IP) o viceversa.

### **3.-¿Para qué sirve el comando netstat?**

Netstat muestra todo sobre quién está hablando con quién y qué puertos están abiertos.

### **4.-¿Para qué sirve el comando tasklist?**

Tasklist es como la lista de información de estado de los integrantes o componentes. Te muestra cuánto espacio ocupan y qué tanto están rindiendo.

### **5.-¿Para qué sirve el comando taskkill?**

Taskkill es como el guardaespaldas digital. Si hay algún proceso que se está portando mal y persiste Taskkill termina a la fuerza. Es como echar a alguien que está causando problemas en la PC.

### **6.-¿Para qué sirve el comando tracert?**

Tracert te muestra el camino que toma un mensaje desde tu computadora hasta su destino, marcando todos los lugares donde hace escalas.

### **7.-¿Cómo ayudan los primeros 3 comandos para detectar problemas en la red?**

Ping es como el detective de la red, confirmando si los dispositivos están disponibles. Nslookup arregla líos con nombres, como cuando alguien cambia su apodo. Y Netstat es chequea el estado de tu internet, buscando cualquier problema en las conexiones y puertos.

Investigar los siguientes comandos y anota ejemplos prácticos:

**atmadm:**

Descripción: Controla las conexiones de interfaz de servicios de acceso a banda ancha (BAS).

Ejemplo Práctico: `atmadm show` con muestra información sobre las conexiones ATM en el sistema.

**bitsadmin:**

Descripción: Administra trabajos de transferencia de archivos en segundo plano.

Ejemplo Práctico: `bitsadmin /transfer myDownloadJob /download /priority normal http://example.com/file.zip C:\Downloads\file.zip` descarga un archivo utilizando BITS.

**cmstp:**

Descripción: Instala o desinstala un perfil de conexión.

Ejemplo Práctico: `cmstp.exe /au VPN_Profile.inf` instala un perfil VPN.

**ftp:**

Descripción: Transfiere archivos a través del Protocolo de Transferencia de Archivos.

Ejemplo Práctico: `ftp example.com` inicia una sesión FTP con el servidor example.com.

**getmac:**

Descripción: Muestra las direcciones MAC de los adaptadores de red.

Ejemplo Práctico: `getmac` muestra las direcciones MAC de los adaptadores en tu sistema.

**hostname:**

Descripción: Muestra o establece el nombre del host de la computadora.

Ejemplo Práctico: `hostname` muestra el nombre del host de la máquina.

**nbstat:**

Descripción: Muestra estadísticas del protocolo NetBIOS sobre TCP/IP.

Ejemplo Práctico: `nbstat -n` muestra las estadísticas de NetBIOS.

**net:**

Descripción: Muestra información o configura recursos compartidos y conexiones de red.

Ejemplo Práctico: `net view` muestra una lista de recursos compartidos en la red.



**net use:**

Descripción: Conecta o desconecta una computadora de un recurso compartido en la red.

Ejemplo Práctico: net use Z: \\server\share conecta la unidad Z: a un recurso compartido de red.

**netsh:**

Descripción: Configura interfaces de red, firewall, y otros servicios de red.

Ejemplo Práctico: netsh interface ip show config muestra la configuración de red actual.

**pathping:**

Descripción: Combina las funciones de tracer y ping, mostrando detalles de la ruta y la latencia.

Ejemplo Práctico: pathping example.com realiza un seguimiento de ruta y mide la latencia a example.com.

**rcp:**

Descripción: Copia archivos entre sistemas utilizando el Protocolo de Copia Remota.

Ejemplo Práctico: rcp file.txt user@remote:/path copia el archivo file.txt a un sistema remoto.

**rexec:**

Descripción: Ejecuta comandos en sistemas remotos.

Ejemplo Práctico: rexec -l username -p password hostname command ejecuta el comando en el host remoto.

**route:**

Descripción: Muestra o manipula la tabla de enrutamiento.

Ejemplo Práctico: route print muestra la tabla de enrutamiento.

**rpcping:**

Descripción: Realiza pruebas de ping a un punto de conexión RPC.

Ejemplo Práctico: rpcping -t ncacn\_ip\_tcp -o portqry -p 135 target realiza una prueba RPC a un objetivo específico.

**rsh:**

Descripción: Ejecuta comandos en sistemas remotos.

Ejemplo Práctico: rsh hostname command ejecuta el comando en el host remoto.

**tcmsetup:**

Descripción: Configura servicios de administración de claves de confianza.

Ejemplo Práctico: `tcmsetup /ec /server:ServerName` configura el servicio de administración de claves de confianza.

**telnet:**

Descripción: Establece una sesión de comunicación con un host remoto.

Ejemplo Práctico: `telnet example.com 80` establece una conexión Telnet al puerto 80 de example.com.

**tftp:**

Descripción: Transfiere archivos utilizando el Protocolo de Transferencia de Archivos Trivial.

Ejemplo Práctico: `tftp -i get filename` descarga un archivo utilizando TFTP.