Actividad #: 4

Autor/es: Ariana González Pinto

Carrera: Tecnología Superior en Desarrollo de Software

Docente: Ing.: Edison Espinoza

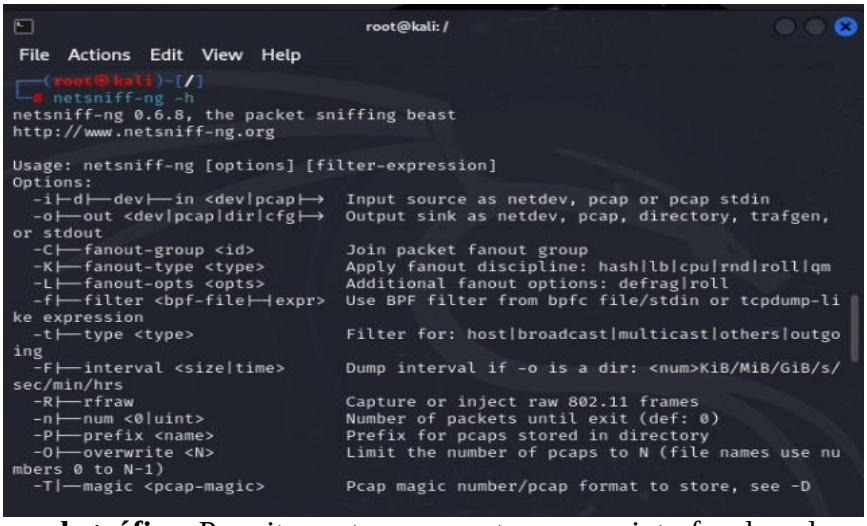
-Fecha:10/11/2024

Explicación del comando

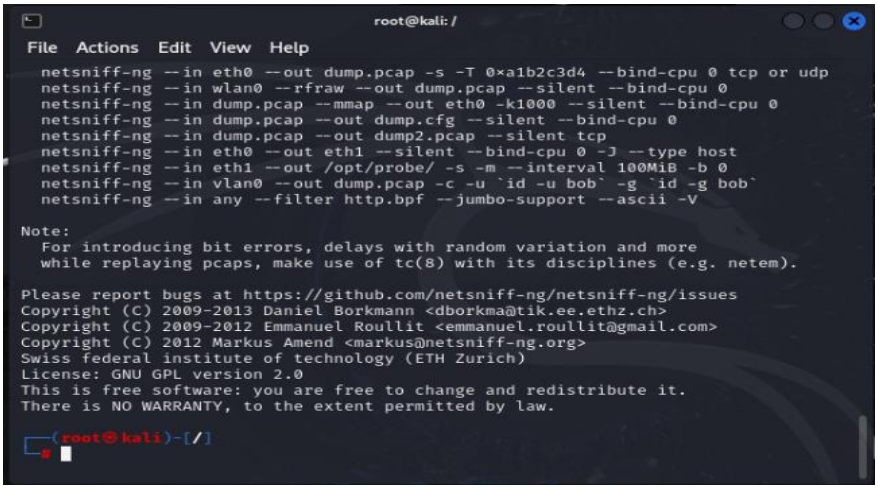
netsniff-ng: Es la herramienta principal que se usa para capturar, analizar y reproducir tráfico de red en tiempo real o en archivos de captura.

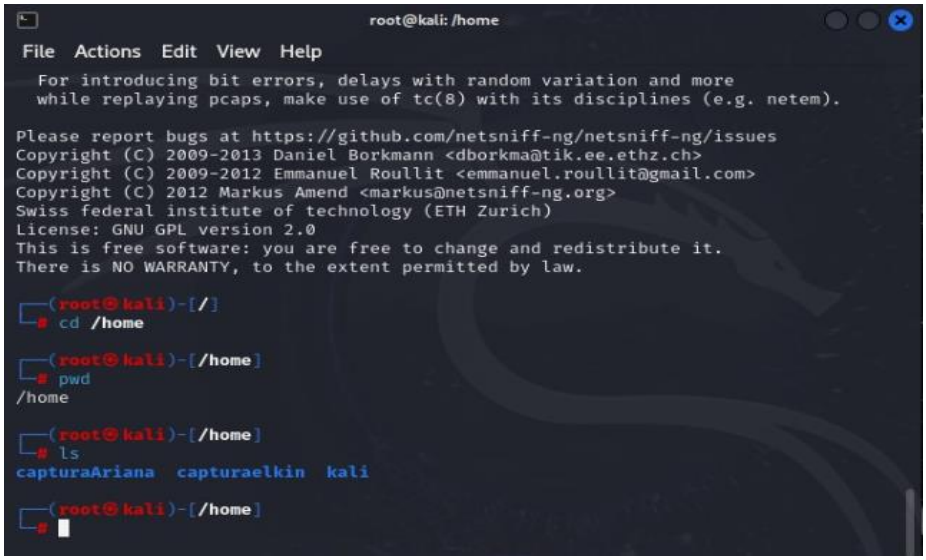
-h: Muestra el menú de ayuda o la lista de opciones disponibles para utilizar con netsniff-ng.

Al ejecutar netsniff-ng -h, saldra un listado de las opciones y parámetros que se usa con netsniff-ng. Esta información incluye opciones para:



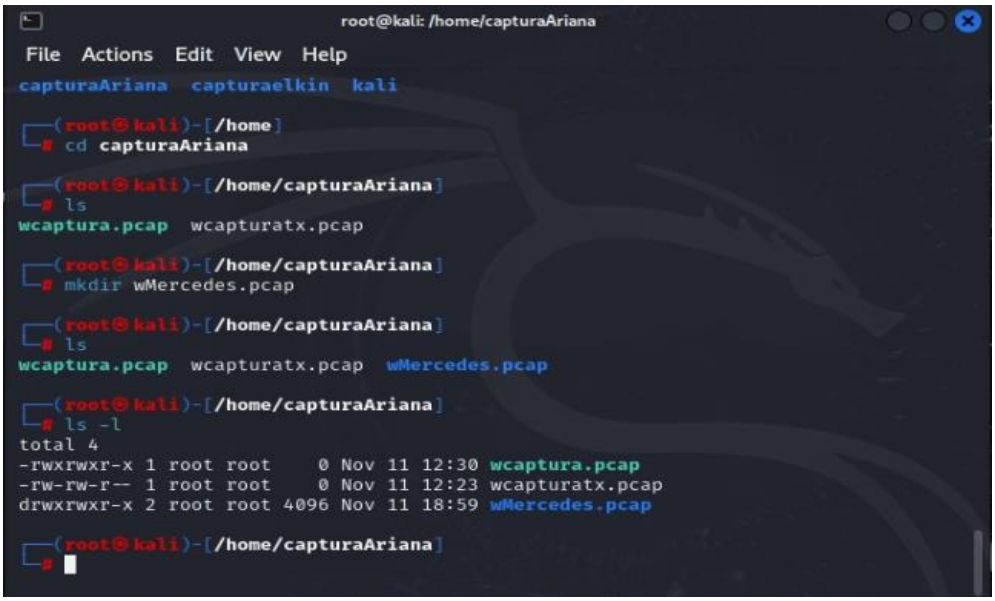
1. **Captura de tráfico**: Permite capturar paquetes en una interfaz de red específica.
2. **Reproducción de tráfico**: Puedes enviar tráfico previamente capturado a través de una interfaz de red.
3. **Filtrado de tráfico**: Filtra paquetes específicos según ciertos criterios (como puertos o protocolos).
4. **Opciones de salida**: Especifica el formato y ubicación de los archivos de captura.
5. **Modos avanzados**: Como el modo de captura de baja latencia, análisis detallado de tráfico, estadísticas de red, entre otros.





Cuando se ejecuta cd /home, el terminal cambia tu ubicación al directorio /home. Después de este comando, mostrará como directorio actual /home, y desde allí se puede ver los directorios de los usuarios o navegar a otros subdirectorios.

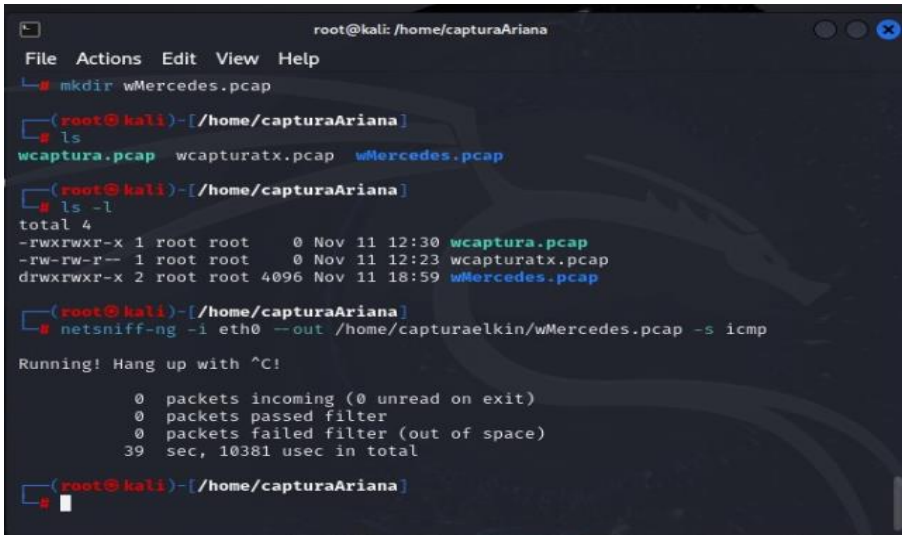
Si después se ejecuta el comando ls, saldra una lista de carpetas de usuarios, como:



El comando mkdir wMercedes.ccap se usa para **crear un nuevo directorio (carpeta)** con el nombre wMercedes.ccap en el directorio actual.

- **mkdir**: Es el comando para "make directory" (crear un directorio).
- **wMercedes.ccap**: Es el nombre del nuevo directorio que se está creando. En este caso, wMercedes.ccap es solo un nombre y no tiene ningún significado especial. Aunque

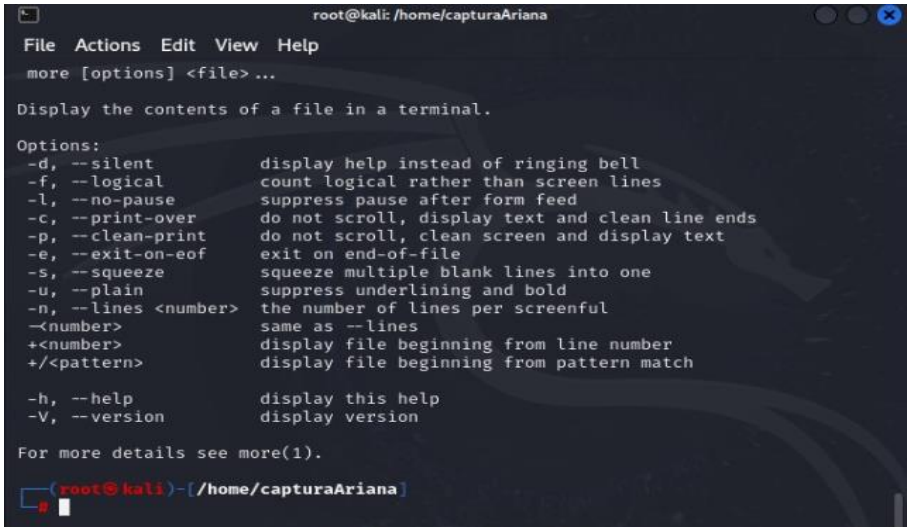
termina en .ccap, el sistema de archivos lo interpretará simplemente como una carpeta, a menos que tenga otro contexto en el sistema.



Se ejecuta el comando ls -l dentro de la ruta donde se creo el directorio wMercedes.ccap, se verá un listado detallado de los archivos y directorios que están en ese directorio.

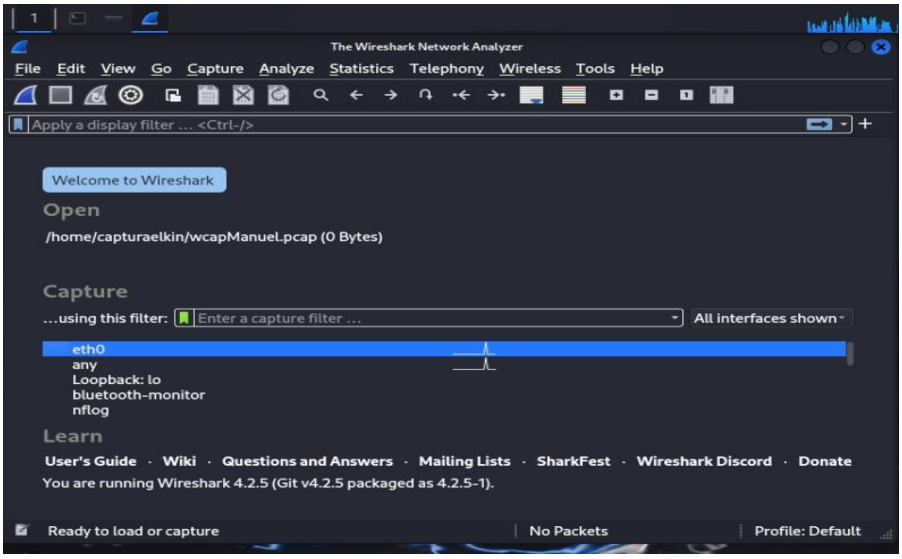
ls: Lista el contenido del directorio actual.

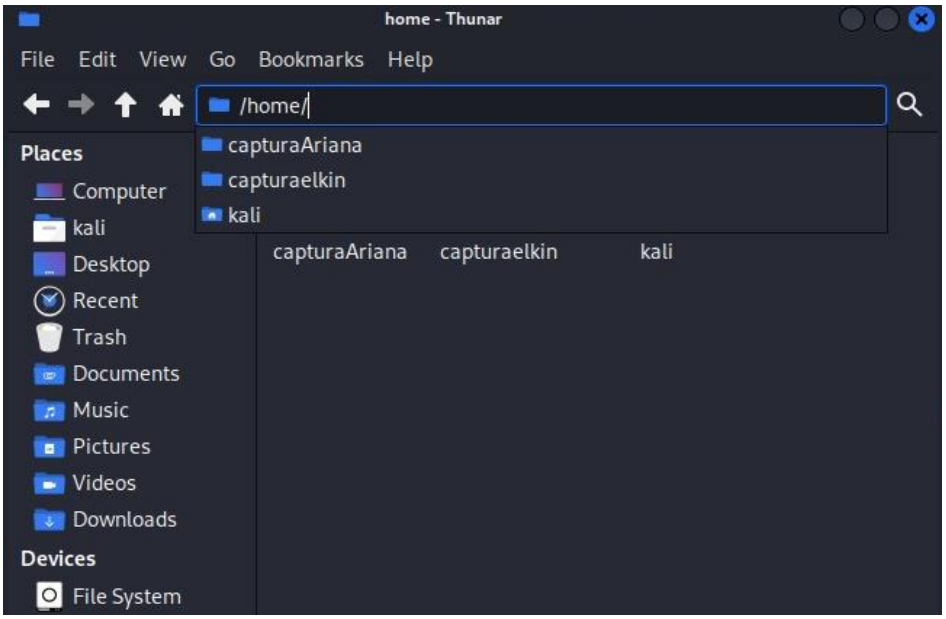
-l: Muestra los detalles de cada archivo o carpeta en formato de lista larga.

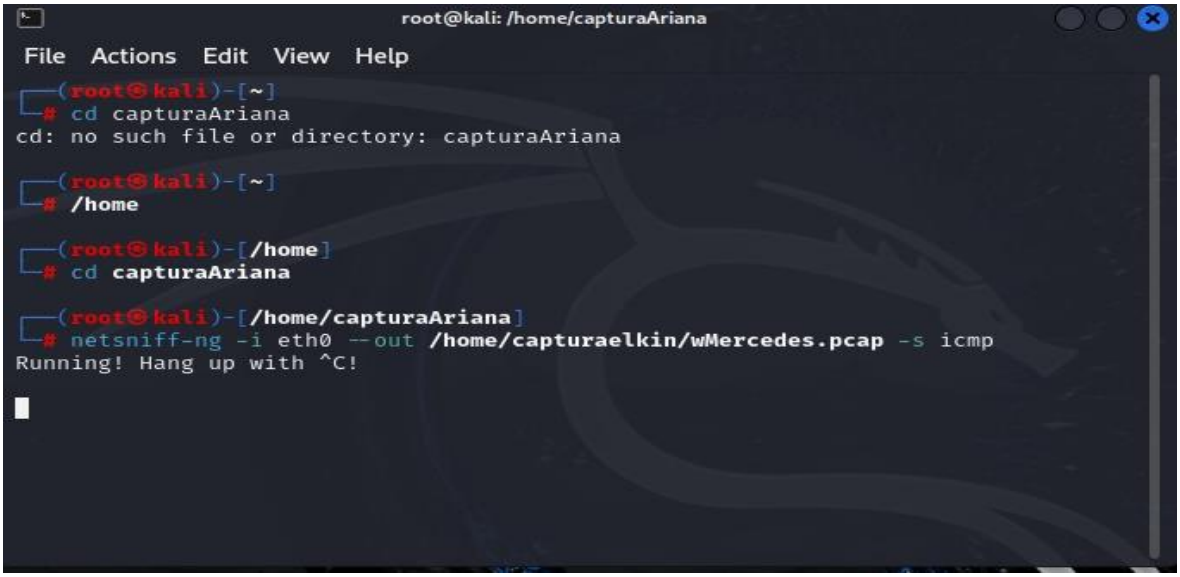


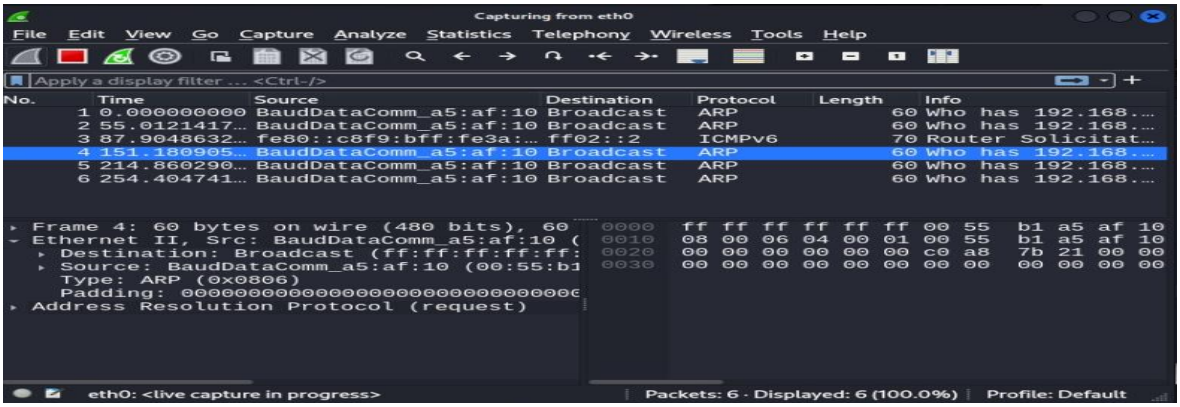
Este comando de **netsniff-ng** se usa para capturar tráfico de red en la interfaz eth0, filtrando solo paquetes ICMP (como el tráfico de ping), y guardar la captura en un archivo llamado wMercedes.pcap dentro del directorio /home/capturaelkin.

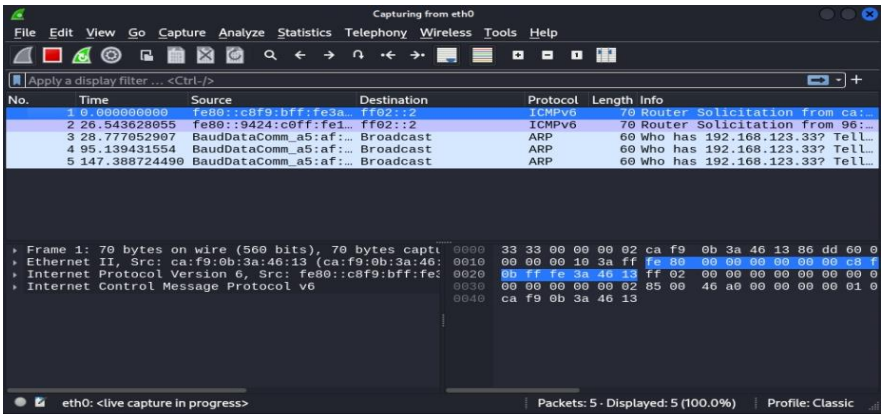
- **-i eth0**: Especifica la interfaz de red a capturar. En este caso, es eth0 (puede ser diferente en otros sistemas, por ejemplo, wlan0 en caso de Wi-Fi).
- **--out /home/capturaelkin/wMercedes.pcap**: Define la ubicación y el nombre del archivo donde se guardarán los datos capturados. Aquí se guardarán en /home/capturaelkin/wMercedes.pcap.
- **-s icmp**: Filtra la captura de paquetes para que incluya solo tráfico ICMP (Internet Control Message Protocol), que es el protocolo usado por herramientas como ping.






root@kali: /home/capturaAriana
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# cd capturaAriana
cd: no such file or directory: capturaAriana
┌──(root㉿kali)-[~]
└─# /home
┌──(root㉿kali)-[/home]
└─# cd capturaAriana
┌──(root㉿kali)-[/home/capturaAriana]
└─# netsniff-ng -i eth0 --out /home/capturaelkin/wMercedes.pcap -s icmp
Running! Hang up with ^C!


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 BaudDataComm_a5:af:10 Broadcast ARP 60 Who has 192.168.…
2 55.0121417… BaudDataComm_a5:af:10 Broadcast ARP 60 Who has 192.168.…
3 87.9048632… fe80::c8f9:bff:fe3a:… ff02::2 ICMPv6 70 Router Solicitat…
4 151.180905… BaudDataComm_a5:af:10 Broadcast ARP 60 Who has 192.168.…
5 214.860290… BaudDataComm_a5:af:10 Broadcast ARP 60 Who has 192.168.…
6 254.404741… BaudDataComm_a5:af:10 Broadcast ARP 60 Who has 192.168.…
Frame 4: 60 bytes on wire (480 bits), 60
Ethernet II, Src: BaudDataComm_a5:af:10 (
Destination: Broadcast (ff:ff:ff:ff:ff:
Source: BaudDataComm_a5:af:10 (00:55:b1
Type: ARP (0x0806)
Padding: 000000000000000000000000000000
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 55 b1 a5 af 10
0010 08 00 06 04 00 01 00 55 b1 a5 af 10
0020 00 00 00 00 00 00 c0 a8 7b 21 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
eth0: <live capture in progress>
Packets: 6 · Displayed: 6 (100.0%)
Profile: Default


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 fe80::c8f9:bff:fe3a… ff02::2 ICMPv6 70 Router Solicitation from ca:…
2 26.543628055 fe80::9424:c0ff:fe1… ff02::2 ICMPv6 70 Router Solicitation from 96:…
3 28.777052907 BaudDataComm_a5:af:… Broadcast ARP 60 Who has 192.168.123.33? Tell…
4 95.139431554 BaudDataComm_a5:af:… Broadcast ARP 60 Who has 192.168.123.33? Tell…
5 147.388724490 BaudDataComm_a5:af:… Broadcast ARP 60 Who has 192.168.123.33? Tell…
Frame 1: 70 bytes on wire (560 bits), 70 bytes capti
Ethernet II, Src: ca:f9:0b:3a:46:13 (ca:f9:0b:3a:46:
Internet Protocol Version 6, Src: fe80::c8f9:bff:fe3
Internet Control Message Protocol v6
0000 33 33 00 00 00 02 ca f9 0b 3a 46 13 86 dd 60 0
0010 00 00 00 10 3a ff fe 80 00 00 00 00 00 00 c8 f
0020 0b ff fe 3a 46 13 ff 02 00 00 00 00 00 00 00 0
0030 00 00 00 00 00 02 85 00 46 a0 00 00 00 00 01 0
0040 ca f9 0b 3a 46 13
eth0: <live capture in progress>
Packets: 5 · Displayed: 5 (100.0%)
Profile: Classic


root@kali: /var/www/html
File Actions Edit View Help
cd /root
pwd
/root
cd /var/www/html
service dvwa start
mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 37
Server version: 11.4.2-MariaDB-4 Debian n/a
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>