

# CURSO ONLINE DE CIBERSEGURIDAD

Especialidad Introducción a la  
Ciberseguridad Industrial

## Taller 3

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



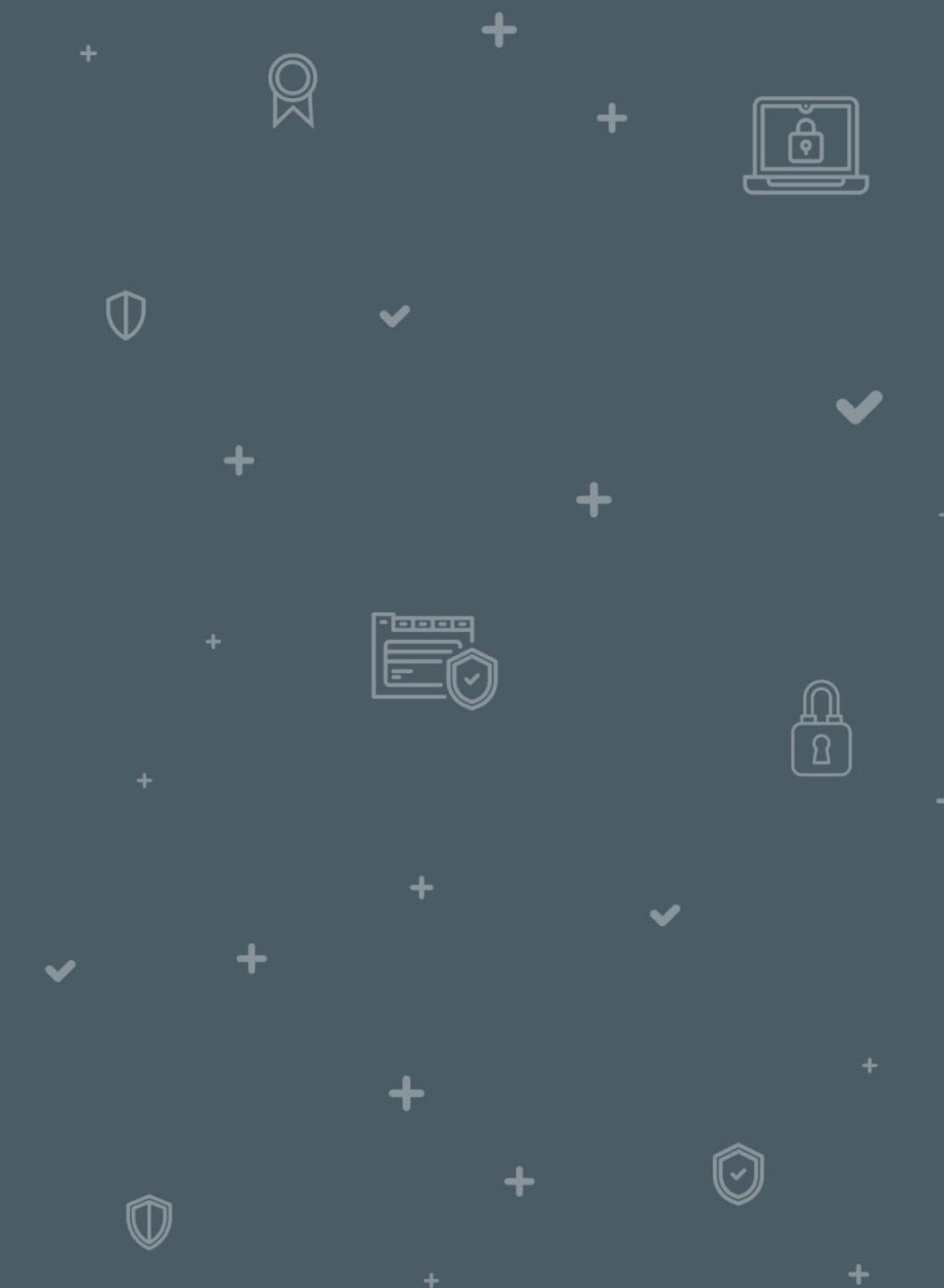
# Contenidos

- |   |  |    |
|---|--|----|
| 1 | ATAQUE POR INYECCIÓN DE CÓDIGO A PLC         | 3  |
| 2 | INSTALACIÓN Y CONFIGURACIÓN DE MBTGET        | 5  |
| 3 | INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT | 14 |
| 4 | BÚSQUEDA DE <i>EXPLOIT</i> CON SEARCHSPLOIT  | 44 |

Duración total del taller: 45 minutos

# ATAQUE POR INYECCIÓN DE CÓDIGO A PLC

# 1





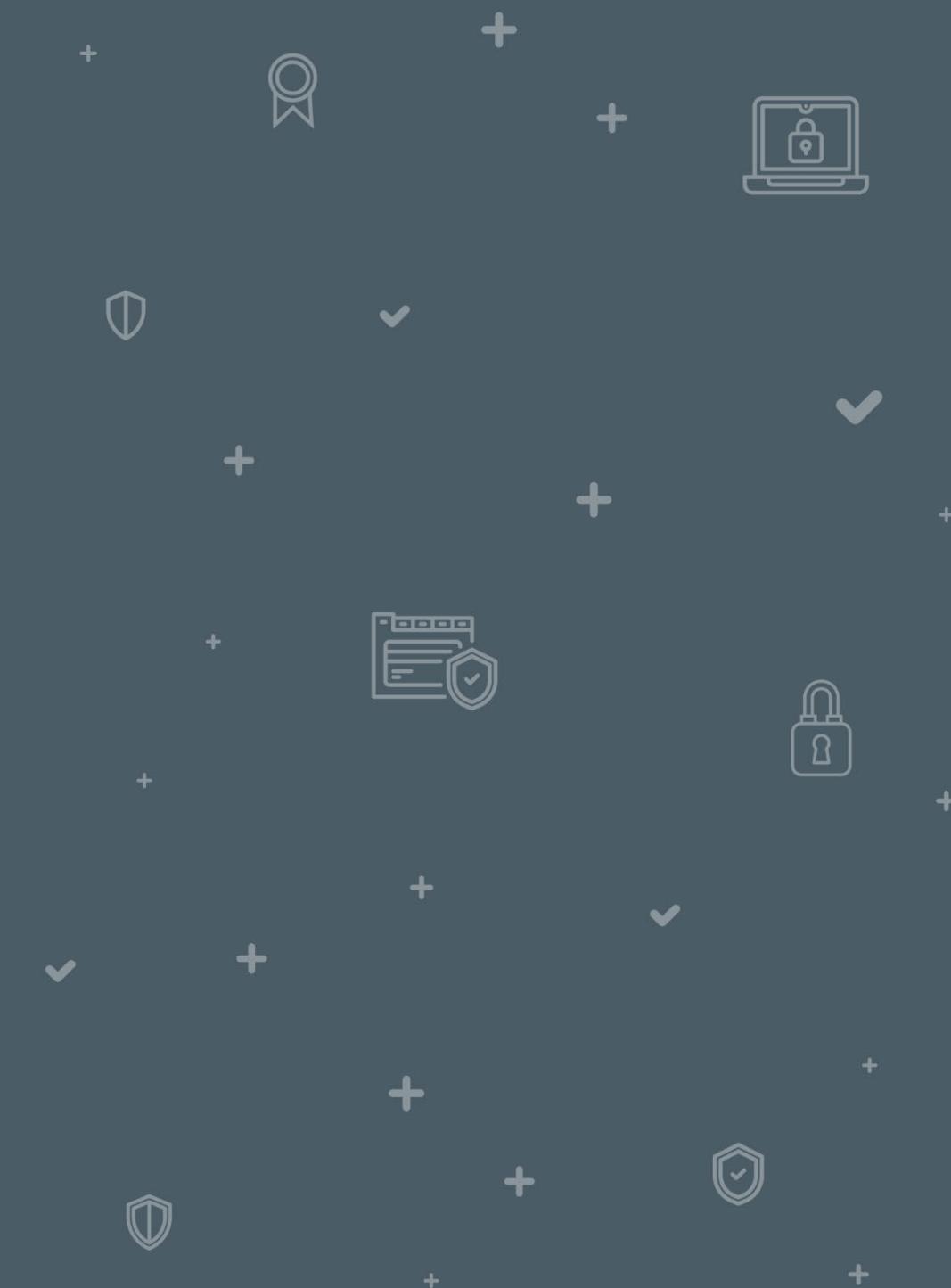
# 1 ATAQUE POR INYECCIÓN DE CÓDIGO A PLC

Ahora, aprenderás a buscar *exploits* para dispositivos industriales y utilizarlos explotando las vulnerabilidades de dispositivos Siemens. También aprenderás a utilizar las principales herramientas de explotación de vulnerabilidades enfocadas a los protocolos industriales desde la máquina atacante Kali Linux. Estas herramientas van a ser:

- **Metasploit**
- **Mbtget**
- **rodbus-client**

# INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

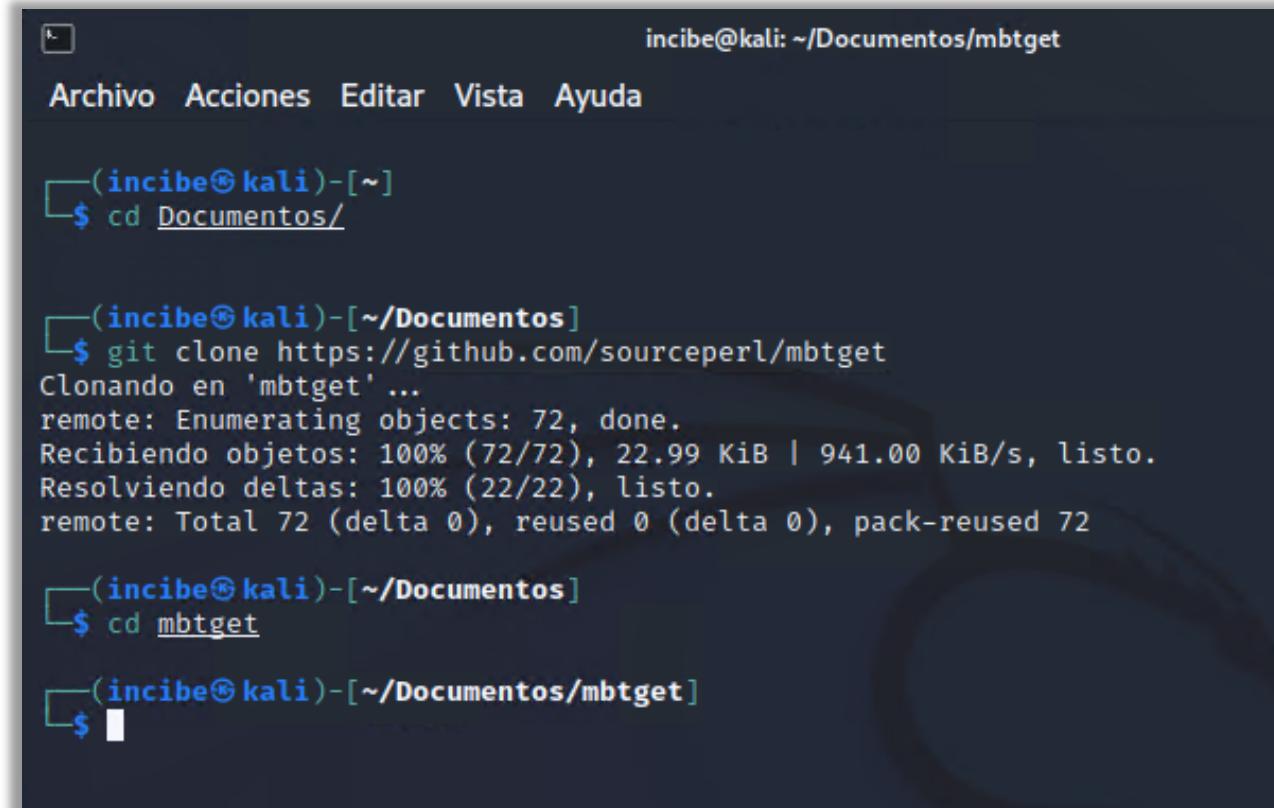
# 2



## 2

## INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Iniciamos nuestra máquina atacante Kali Linux. Abre una terminal, accede a la carpeta «Documentos» y clona el repositorio de la herramienta MBTGET.
  - cd Documentos/**
  - git clone**  
**<https://github.com/sourceperl/mbtget>**



```
incibe@kali: ~/Documentos/mbtget
Archivo  Acciones  Editar  Vista  Ayuda

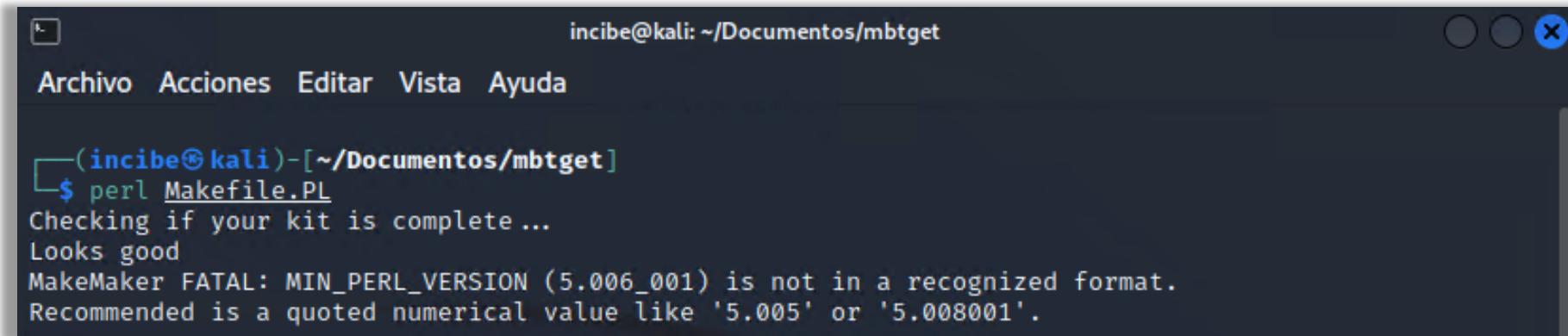
└──(incibe㉿kali)-[~]
    $ cd Documentos/
    └──(incibe㉿kali)-[~/Documentos]
        $ git clone https://github.com/sourceperl/mbtget
        Clonando en 'mbtget' ...
        remote: Enumerating objects: 72, done.
        Recibiendo objetos: 100% (72/72), 22.99 KiB | 941.00 KiB/s, listo.
        Resolviendo deltas: 100% (22/22), listo.
        remote: Total 72 (delta 0), reused 0 (delta 0), pack-reused 72
        └──(incibe㉿kali)-[~/Documentos]
            $ cd mbtget
            └──(incibe㉿kali)-[~/Documentos/mbtget]
                $
```

Ilustración 1: Inicio de máquina atacante Kali Linux. Se abre una terminal, accede a la carpeta «Documentos» y se clona el repositorio de la herramienta MBTGET.

## 2

## INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Accede a la carpeta «mbtget» y ejecuta el siguiente comando, verás que nos devuelve un error, esto es porque debes instalar PERL, un lenguaje de programación que necesitamos para poder ejecutar el comando:
  - **perl Makefile.PL**



A terminal window titled 'incibe@kali: ~/Documentos/mbtget'. The window has a dark theme with white text. The menu bar includes 'Archivo', 'Acciones', 'Editar', 'Vista', and 'Ayuda'. The title bar shows the user 'incibe@kali' and the path '("~/Documentos/mbtget")'. The terminal prompt is '\$ perl Makefile.PL'. The output shows the command executing and checking if the kit is complete, stating 'Looks good'. However, it then displays a fatal error from MakeMaker: 'MIN\_PERL\_VERSION (5.006\_001) is not in a recognized format. Recommended is a quoted numerical value like '5.005' or '5.008001''. The window has standard OS X-style close, minimize, and maximize buttons.

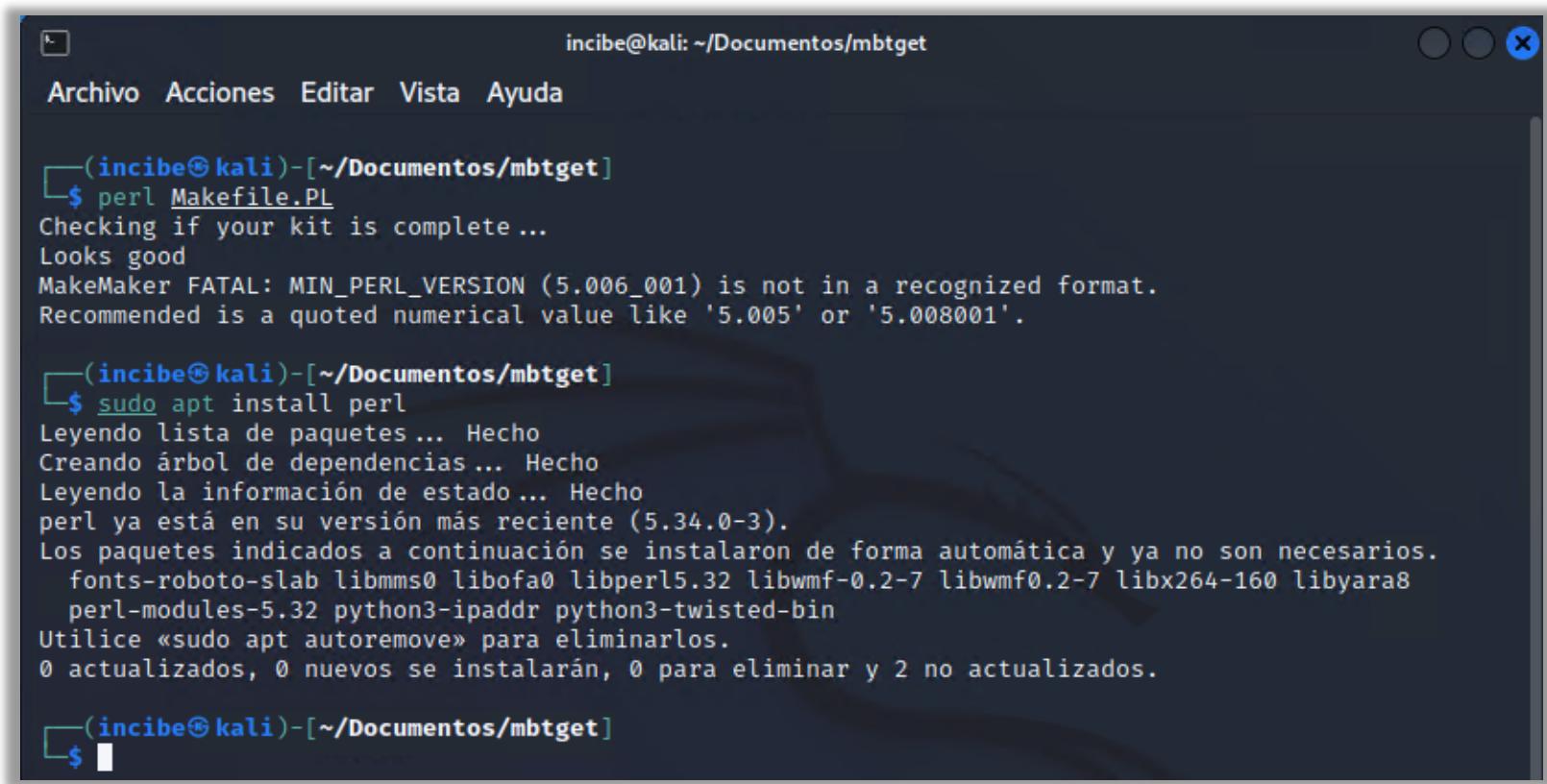
Ilustración 2: Carpeta «mbtget».

## 2

# INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- En esta situación, el primer paso es ejecutar la instalación del paquete de software Perl por si hay algún problema de dependencias y le falta alguna librería:
  - sudo apt install perl**

Pero la herramienta de gestión de paquetes APT nos informa que el paquete de software Perl está actualizado.



The screenshot shows a terminal window on a Kali Linux system. The user, incibe, is in their home directory (~/Documentos/mbtget). They run 'perl Makefile.PL' which checks for dependencies and finds them complete. However, it fails to parse the MIN\_PERL\_VERSION value. Then, they run 'sudo apt install perl', which installs the latest version (5.34.0-3) and lists other packages like fonts-roboto-slab and perl-modules-5.32 as automatically installed. Finally, they run '\$' to prompt for the next command.

```
incibe@kali: ~/Documentos/mbtget
Archivo  Acciones  Editar  Vista  Ayuda

└─(incibe㉿kali)-[~/Documentos/mbtget]
$ perl Makefile.PL
Checking if your kit is complete ...
Looks good
MakeMaker FATAL: MIN_PERL_VERSION (5.006_001) is not in a recognized format.
Recommended is a quoted numerical value like '5.005' or '5.008001'.

└─(incibe㉿kali)-[~/Documentos/mbtget]
$ sudo apt install perl
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
perl ya está en su versión más reciente (5.34.0-3).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  fonts-roboto-slab libmms0 libofa0 libperl5.32 libwmf-0.2-7 libwmf0.2-7 libx264-160 libyara8
    perl-modules-5.32 python3-ipaddr python3-twisted-bin
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 2 no actualizados.

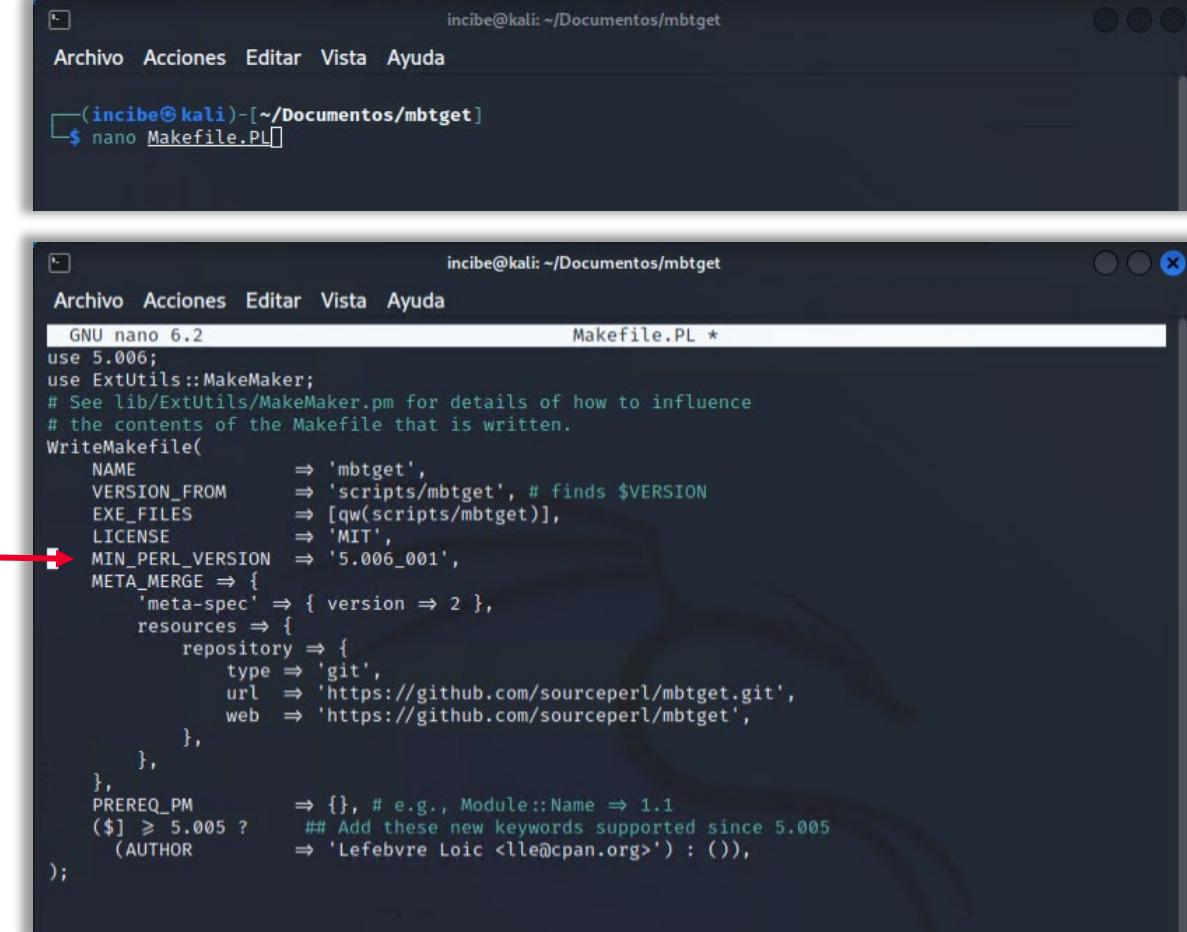
└─(incibe㉿kali)-[~/Documentos/mbtget]
$
```

Ilustración 3: Instalación software Perl.

## 2

## INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Ahora lo que debes hacer, es editar el archivo «Makefile.PL» con el editor de texto nano y modificar la entrada MIN\_PERL\_VERSION, ahí eliminar el texto \_001. Pulsa «Ctrl+X», escribe «s» para guardar los cambios y pulsa «Enter». Así se guardan los cambios en el archivo.



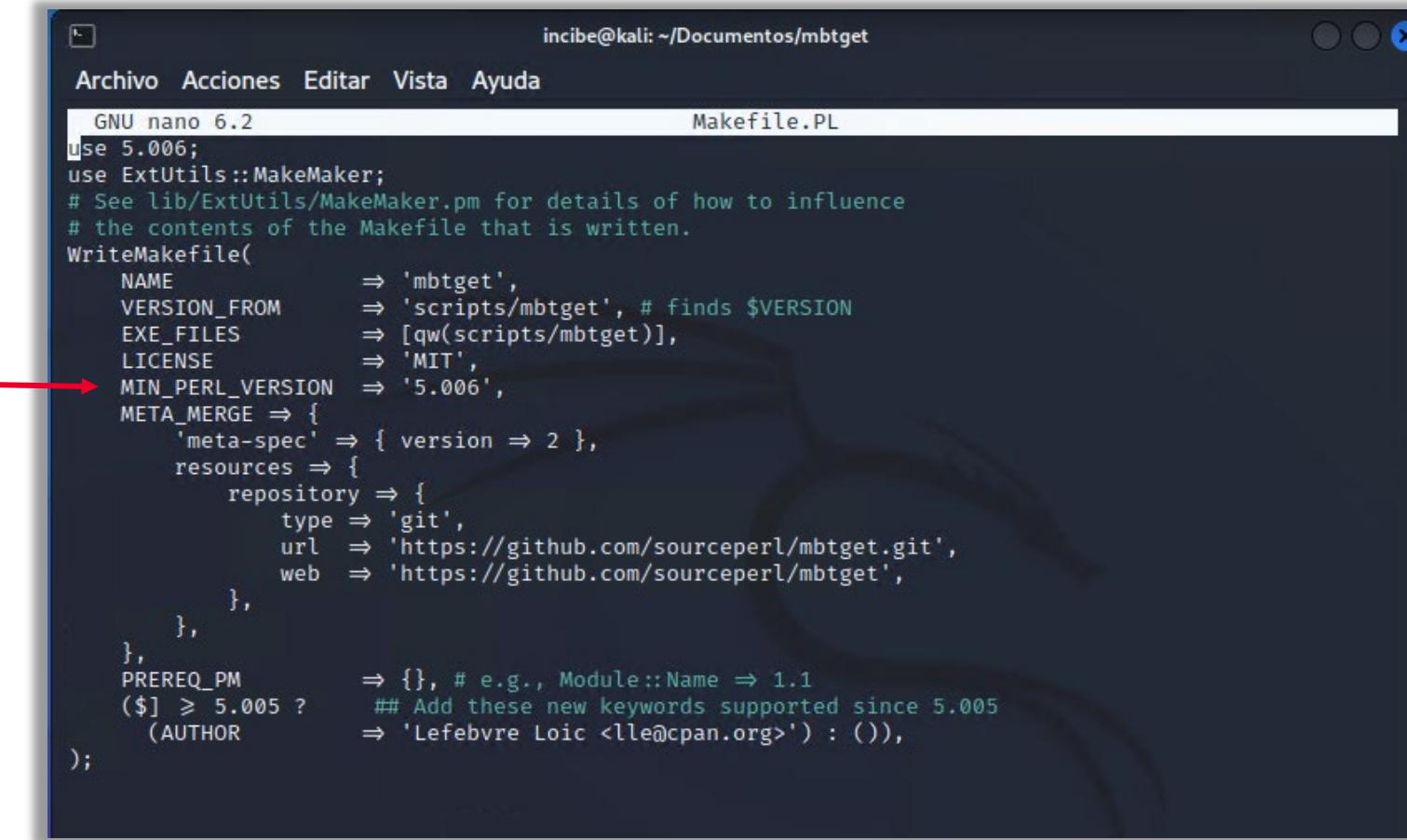
```
incibe@kali: ~/Documentos/mbtget
Archivo Acciones Editar Vista Ayuda
[incibe@kali]-(~/Documentos/mbtget)
$ nano Makefile.PL

incibe@kali: ~/Documentos/mbtget
Archivo Acciones Editar Vista Ayuda
GNU nano 6.2                                     Makefile.PL *
use 5.006;
use ExtUtils::MakeMaker;
# See lib/ExtUtils/MakeMaker.pm for details of how to influence
# the contents of the Makefile that is written.
WriteMakefile(
    NAME          => 'mbtget',
    VERSION_FROM  => 'scripts/mbtget', # finds $VERSION
    EXE_FILES     => [qw(scripts/mbtget)],
    LICENSE       => 'MIT',
    MIN_PERL_VERSION => '5.006_001',
    META_MERGE => {
        'meta-spec' => { version => 2 },
        resources => {
            repository => {
                type => 'git',
                url  => 'https://github.com/sourceperl/mbtget.git',
                web   => 'https://github.com/sourceperl/mbtget',
            },
        },
        PREREQ_PM      => {}, # e.g., Module::Name => 1.1
        ($] >= 5.005 ? ## Add these new keywords supported since 5.005
                     (AUTHOR      => 'Lefebvre Loic <lle@cpan.org>') : (()),
    );
);
```

Ilustración 4: Edición del archivo «Makefile.PL».

## 2

# INSTALACIÓN Y CONFIGURACIÓN DE MBTGET



```
incibe@kali: ~/Documentos/mbtget
Archivo  Acciones  Editar  Vista  Ayuda
GNU nano 6.2                                     Makefile.PL
use 5.006;
use ExtUtils::MakeMaker;
# See lib/ExtUtils/MakeMaker.pm for details of how to influence
# the contents of the Makefile that is written.
WriteMakefile(
    NAME          => 'mbtget',
    VERSION_FROM  => 'scripts/mbtget', # finds $VERSION
    EXE_FILES     => [qw(scripts/mbtget)],
    LICENSE       => 'MIT',
    MIN_PERL_VERSION => '5.006',
    META_MERGE => {
        'meta-spec' => { version => 2 },
        resources => {
            repository => {
                type => 'git',
                url  => 'https://github.com/sourceperl/mbtget.git',
                web   => 'https://github.com/sourceperl/mbtget',
            },
        },
        PREREQ_PM     => {}, # e.g., Module::Name => 1.1
        ($] >= 5.005 ? ## Add these new keywords supported since 5.005
                      (AUTHOR      => 'Lefebvre Loic <lle@cpan.org>') : ())
);

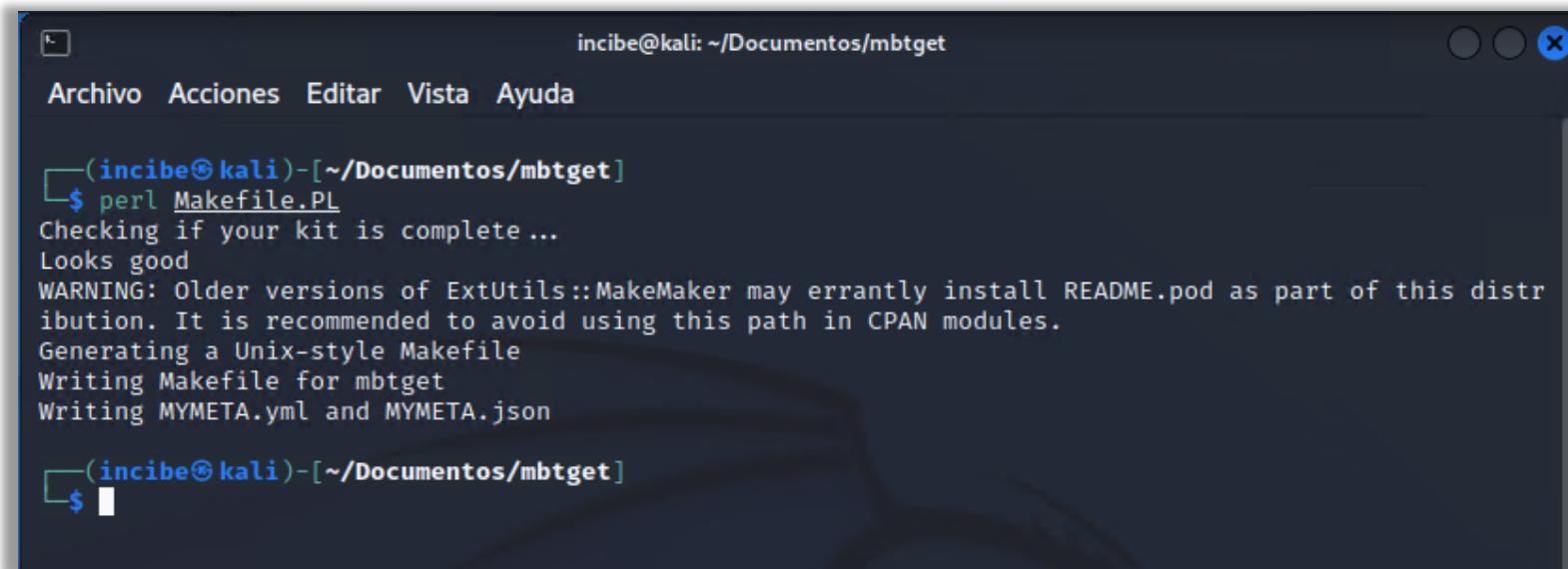
```

Ilustración 5: Modificación de la entrada MIN\_PERL\_VERSION.

## 2

# INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Volvemos a ejecutar el comando **perl Makefile.PL** y vemos que ya no nos genera error.



A screenshot of a terminal window titled "incibe@kali: ~/Documentos/mbtget". The window has a dark theme with white text. The user runs the command \$ perl Makefile.PL. The terminal output shows:

```
(incibe㉿kali)-[~/Documentos/mbtget]
$ perl Makefile.PL
Checking if your kit is complete ...
Looks good
WARNING: Older versions of ExtUtils::MakeMaker may errantly install README.pod as part of this distribution. It is recommended to avoid using this path in CPAN modules.
Generating a Unix-style Makefile
Writing Makefile for mbtget
Writing MYMETA.yml and MYMETA.json

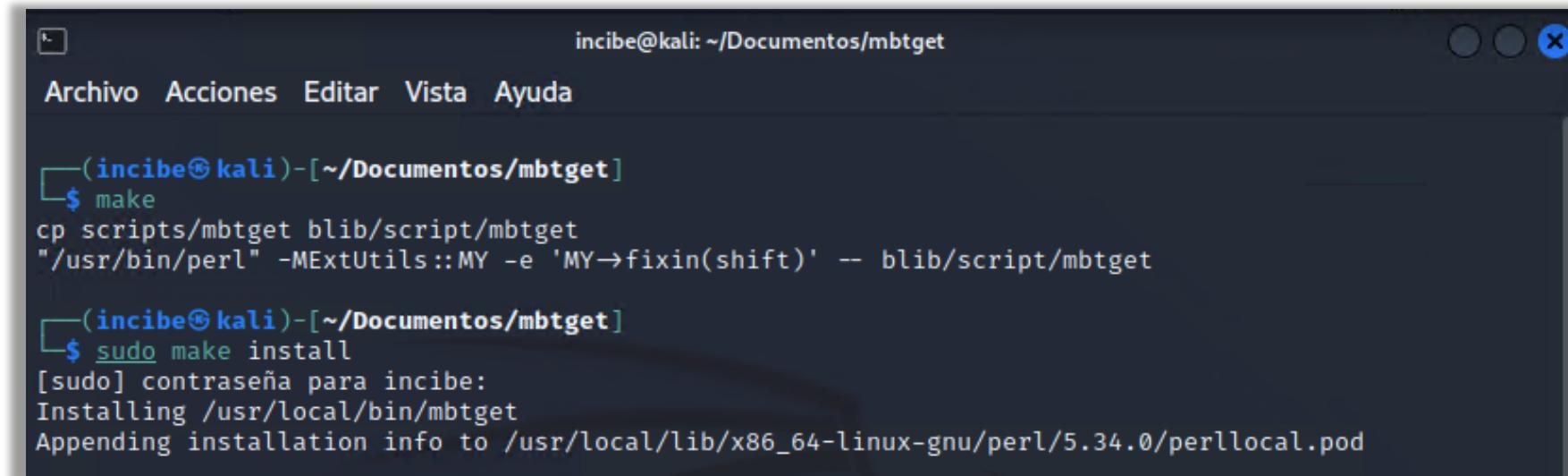
(incibe㉿kali)-[~/Documentos/mbtget]
```

Ilustración 6: Ejecución de perl Makefile.PL

## 2

## INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Ejecuta los comandos **make** y **sudo make install** (para el que nos pide contraseña) para finalizar la instalación de la herramienta.
  - **make**
  - **sudo make install**



A terminal window titled "incibe@kali: ~/Documentos/mbtget". The window shows the following command execution:

```
(incibe㉿kali)-[~/Documentos/mbtget]
$ make
cp scripts/mbtget blib/script/mbtget
"/usr/bin/perl" -MExtUtils::MY -e 'MY→fixin(shift)' -- blib/script/mbtget

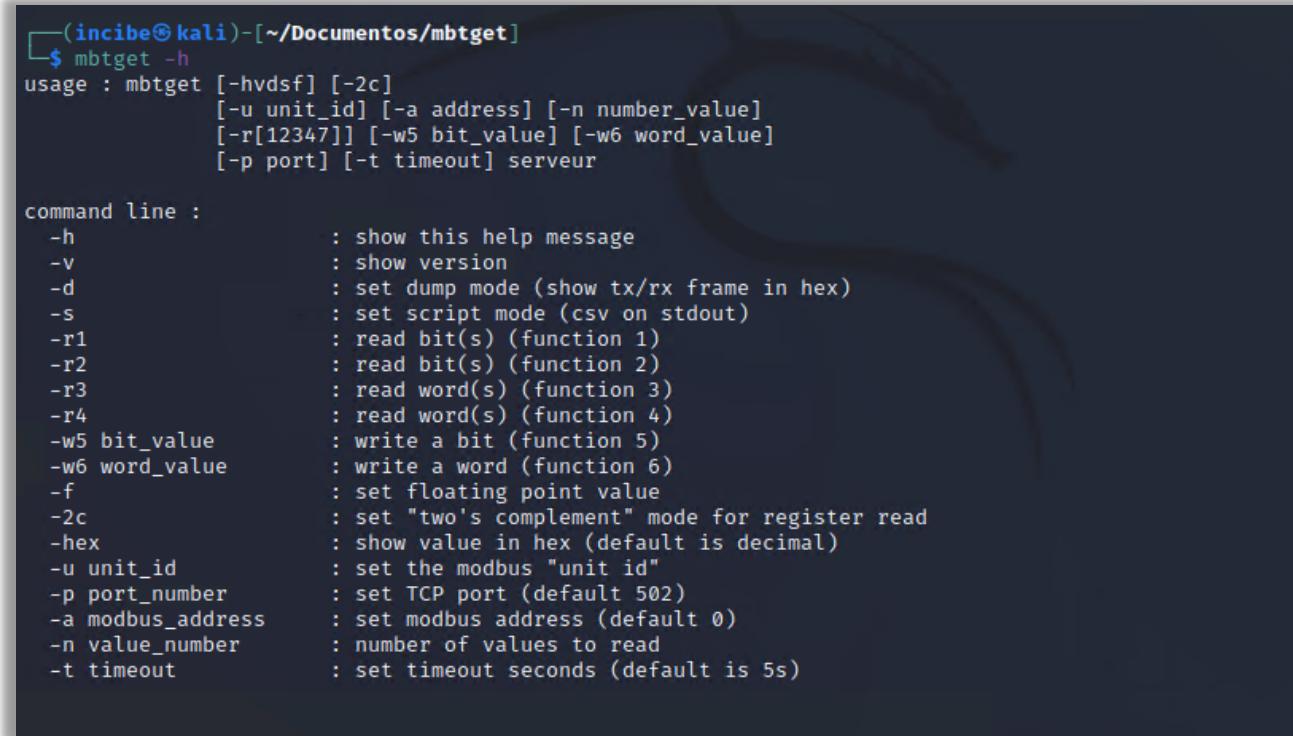
(incibe㉿kali)-[~/Documentos/mbtget]
$ sudo make install
[sudo] contraseña para incibe:
Installing /usr/local/bin/mbtget
Appending installation info to /usr/local/lib/x86_64-linux-gnu/perl/5.34.0/perllocal.pod
```

Ilustración 7: Ejecución de los comandos make y sudo make install.

## 2

# INSTALACIÓN Y CONFIGURACIÓN DE MBTGET

- Por último, ejecuta la herramienta con el parámetro -h para confirmar que la herramienta se ha instalado correctamente.



```
(incibe㉿kali)-[~/Documentos/mbtget]
$ mbtget -h
usage : mbtget [-hvdsf] [-2c]
              [-u unit_id] [-a address] [-n number_value]
              [-r[12347]] [-w5 bit_value] [-w6 word_value]
              [-p port] [-t timeout] serveur

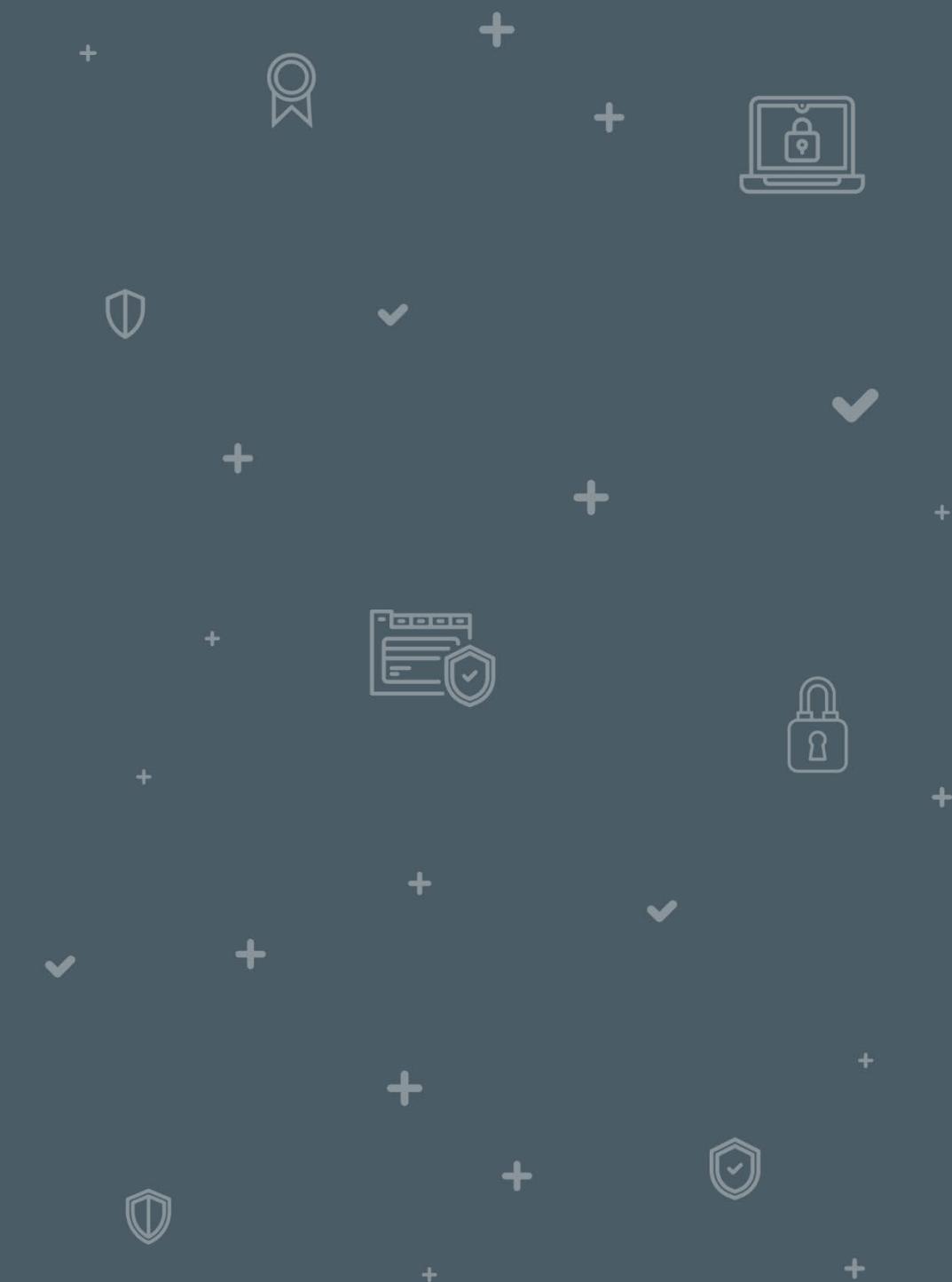
command line :
  -h          : show this help message
  -v          : show version
  -d          : set dump mode (show tx/rx frame in hex)
  -s          : set script mode (csv on stdout)
  -r1         : read bit(s) (function 1)
  -r2         : read bit(s) (function 2)
  -r3         : read word(s) (function 3)
  -r4         : read word(s) (function 4)
  -w5 bit_value : write a bit (function 5)
  -w6 word_value : write a word (function 6)
  -f          : set floating point value
  -2c         : set "two's complement" mode for register read
  -hex        : show value in hex (default is decimal)
  -u unit_id   : set the modbus "unit id"
  -p port_number : set TCP port (default 502)
  -a modbus_address : set modbus address (default 0)
  -n value_number : number of values to read
  -t timeout    : set timeout seconds (default is 5s)
```

Ilustración 8: Confirmación de que la herramienta se ha instalado correctamente.

# INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

- 3.1 Arranque de simuladores del entorno industrial 1
- 3.2 Arranque de simuladores del entorno industrial 2

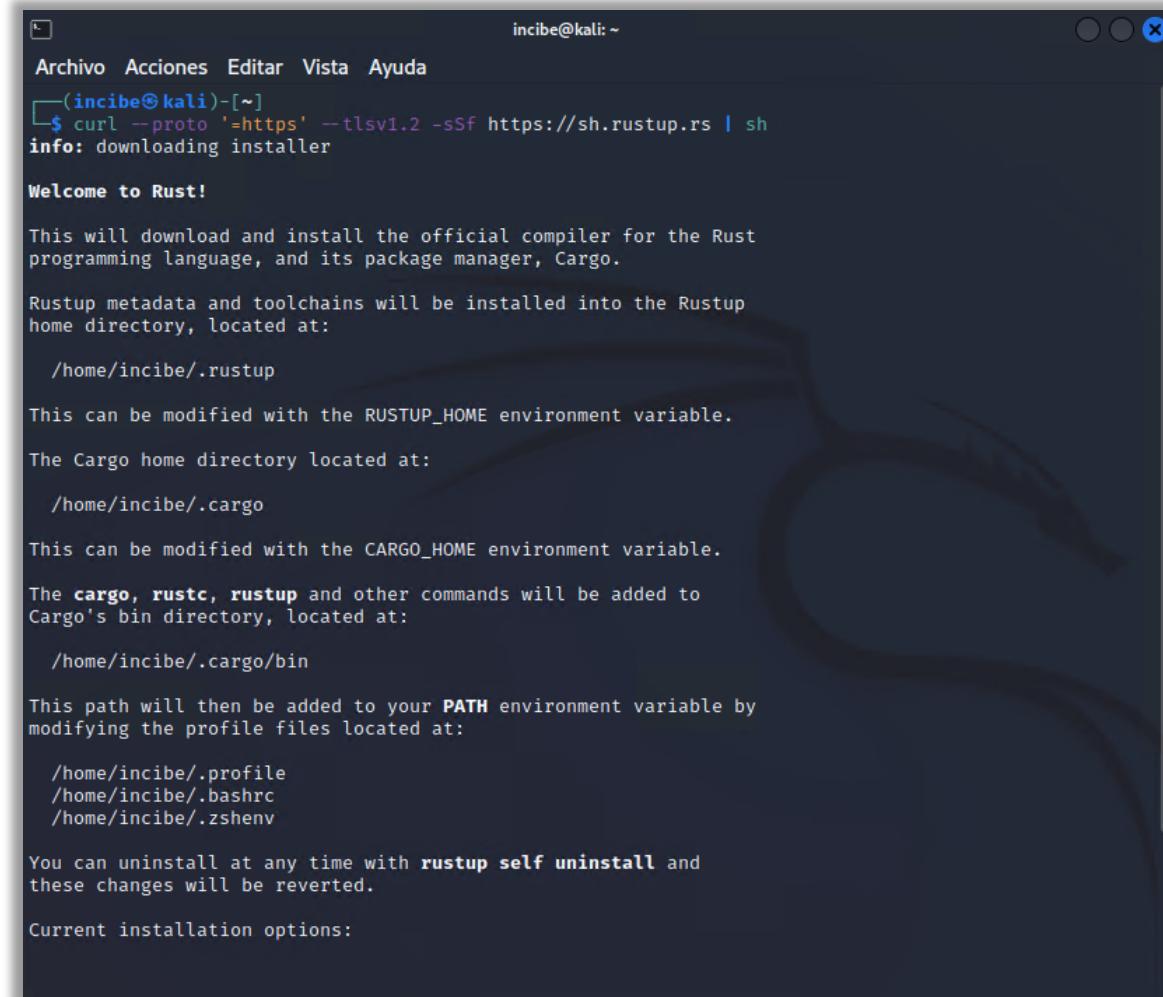
# 3



### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

Esta herramienta nos permitirá interactuar con los datos y con los distintos componentes, como los esclavos o PLC.

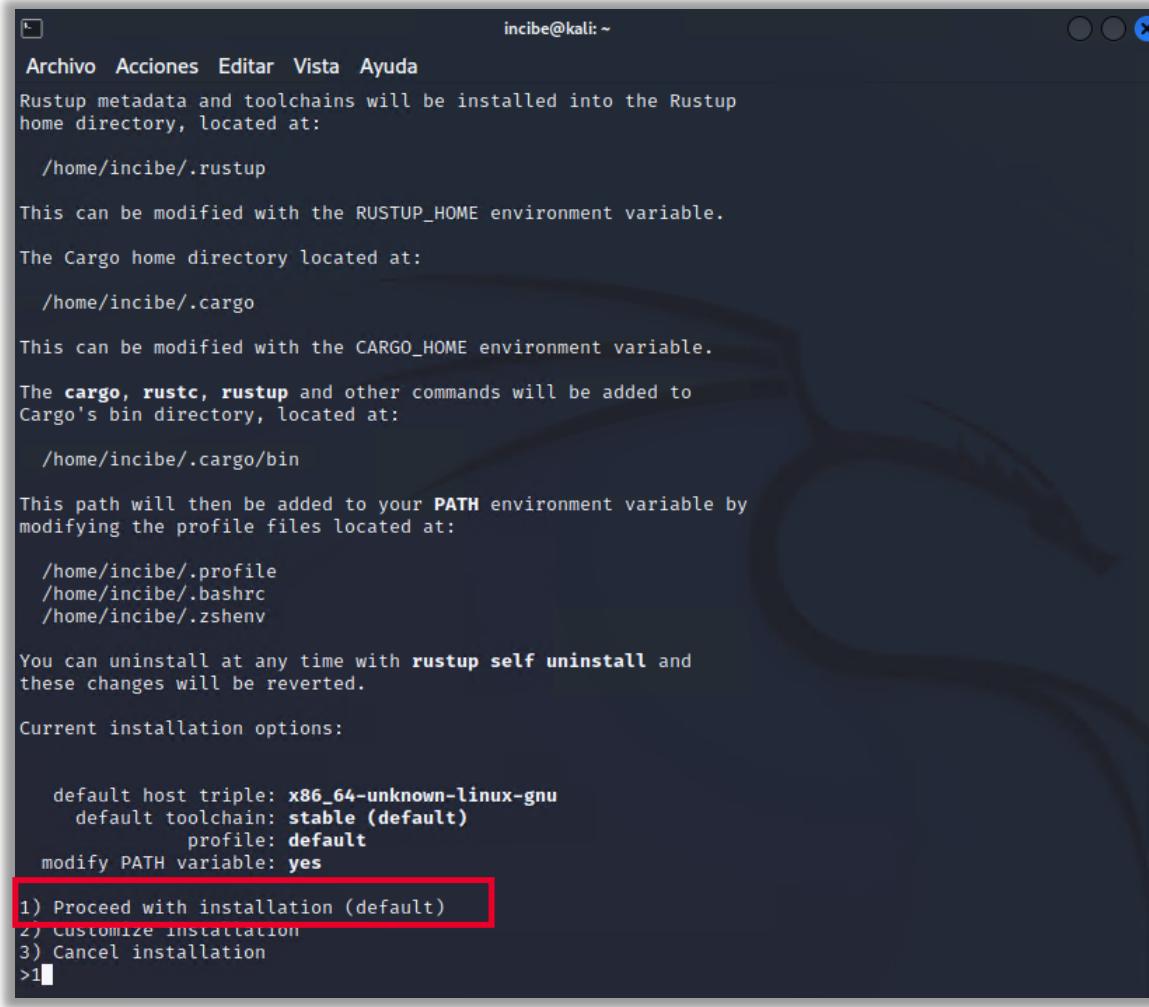
- Ejecuta el comando **curl** para descargar e instalar el compilador del lenguaje de programación «Rust», así como su gestor de paquetes «Cargo» (confirmamos escribiendo 1).
  - **curl --proto '=https' –tlsv1.2 -sSf <https://sh.rustup.rs> | sh**



A screenshot of a terminal window titled 'incibe@kali: ~'. The window shows the command \$ curl --proto '=https' -tlsv1.2 -sSf https://sh.rustup.rs | sh being run. The output includes the Rust welcome message, information about the official compiler and Cargo package manager, details about the Rustup home directory (~/.rustup), the Cargo home directory (~/.cargo), and the addition of rustc, rustup, and cargo commands to the PATH. It also mentions modifying profile files like .profile, .bashrc, and .zshenv, and provides instructions for uninstallation.

Ilustración 9: Instalación de la herramienta Rodbus-client.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT



A terminal window titled "incibe@kali: ~" displaying the Rustup installation process. The window shows the configuration of the Rustup home directory at "/home/incibe/.rustup", the Cargo home directory at "/home/incibe/.cargo", and the addition of commands to the Cargo bin directory at "/home/incibe/.cargo/bin". It also mentions modifying the PATH environment variable through profile files like ".profile", ".bashrc", and ".zshenv". A message at the bottom indicates that changes can be reverted with "rustup self uninstall". The current installation options are listed as:

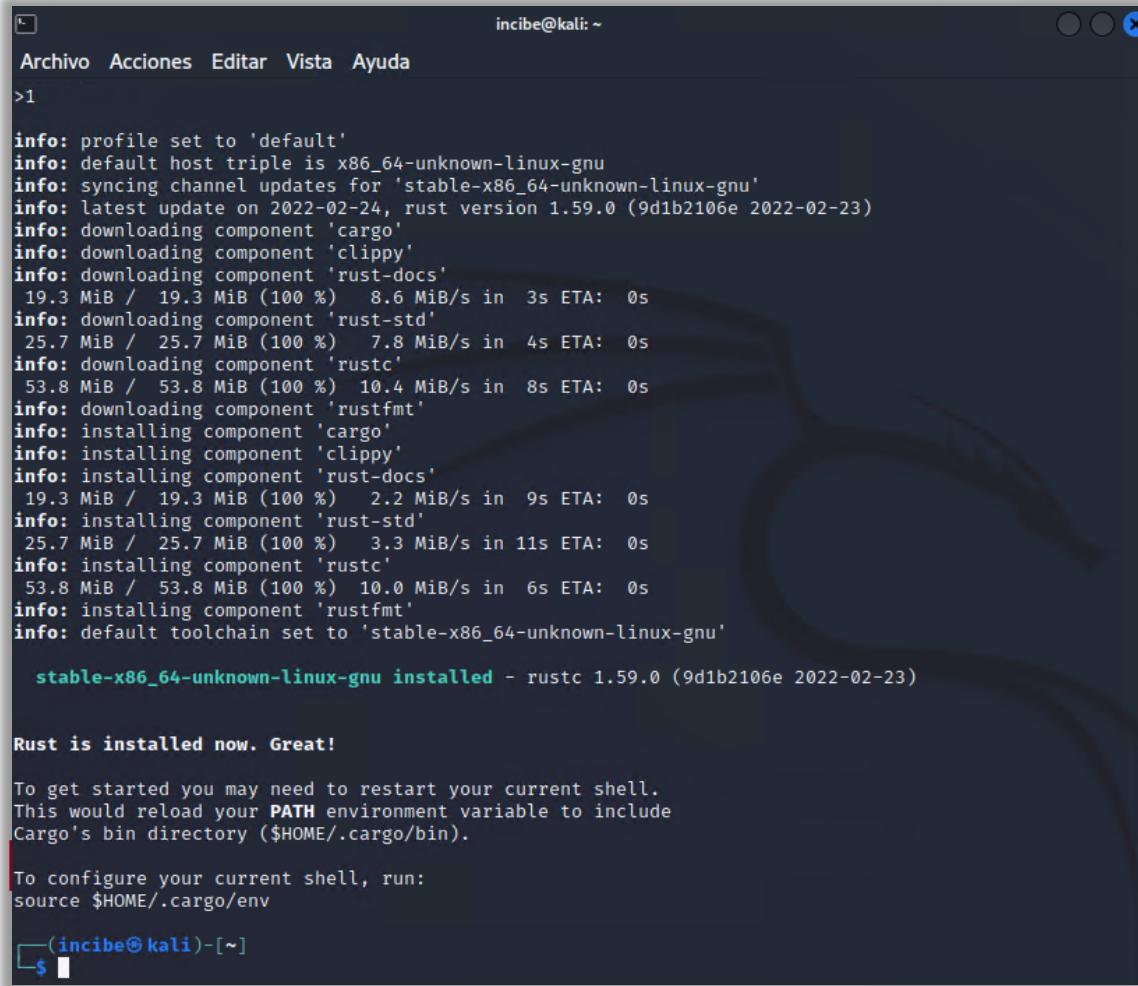
```
default host triple: x86_64-unknown-linux-gnu
  default toolchain: stable (default)
    profile: default
  modify PATH variable: yes
```

The first option, "1) Proceed with installation (default)", is highlighted with a red box.

Ilustración 10: Ejecuta el comando *curl* para descargar e instalar el compilador del lenguaje de programación «Rust».

# 3

# INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

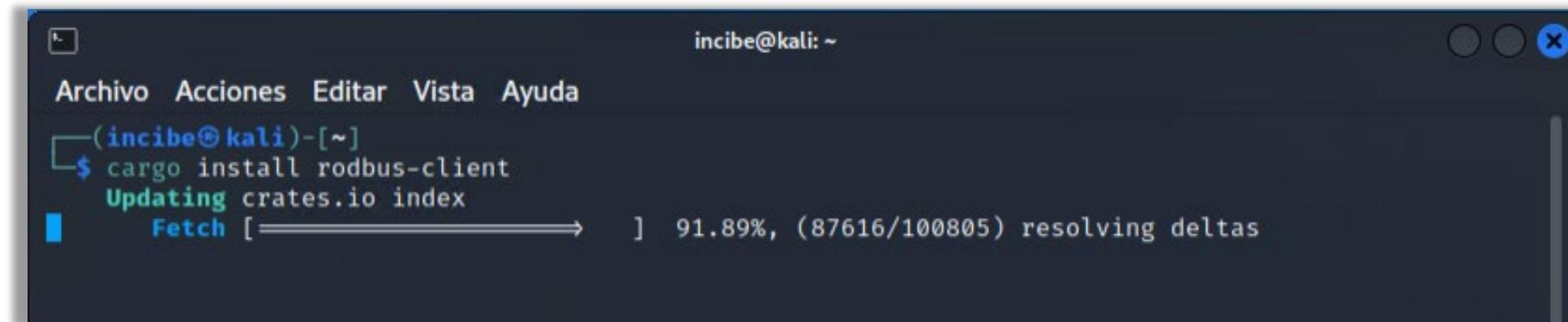


The screenshot shows a terminal window titled "incibe@kali: ~". The terminal displays the output of a command, likely "cargo install", which installs the Rust toolchain. The output includes logs for syncing channel updates, downloading components like cargo, clippy, rust-docs, rust-std, rustc, and rustfmt, and installing them. It also mentions the default host triple as x86\_64-unknown-linux-gnu and the latest update date as 2022-02-24. The Rust version installed is 1.59.0 (9d1b2106e 2022-02-23). A message at the end says "Rust is installed now. Great!" and provides instructions to restart the shell to reload the PATH environment variable. The terminal prompt at the bottom is "(incibe@kali)-[~] \$".

Ilustración 11: Gestor de paquetes «Cargo».

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

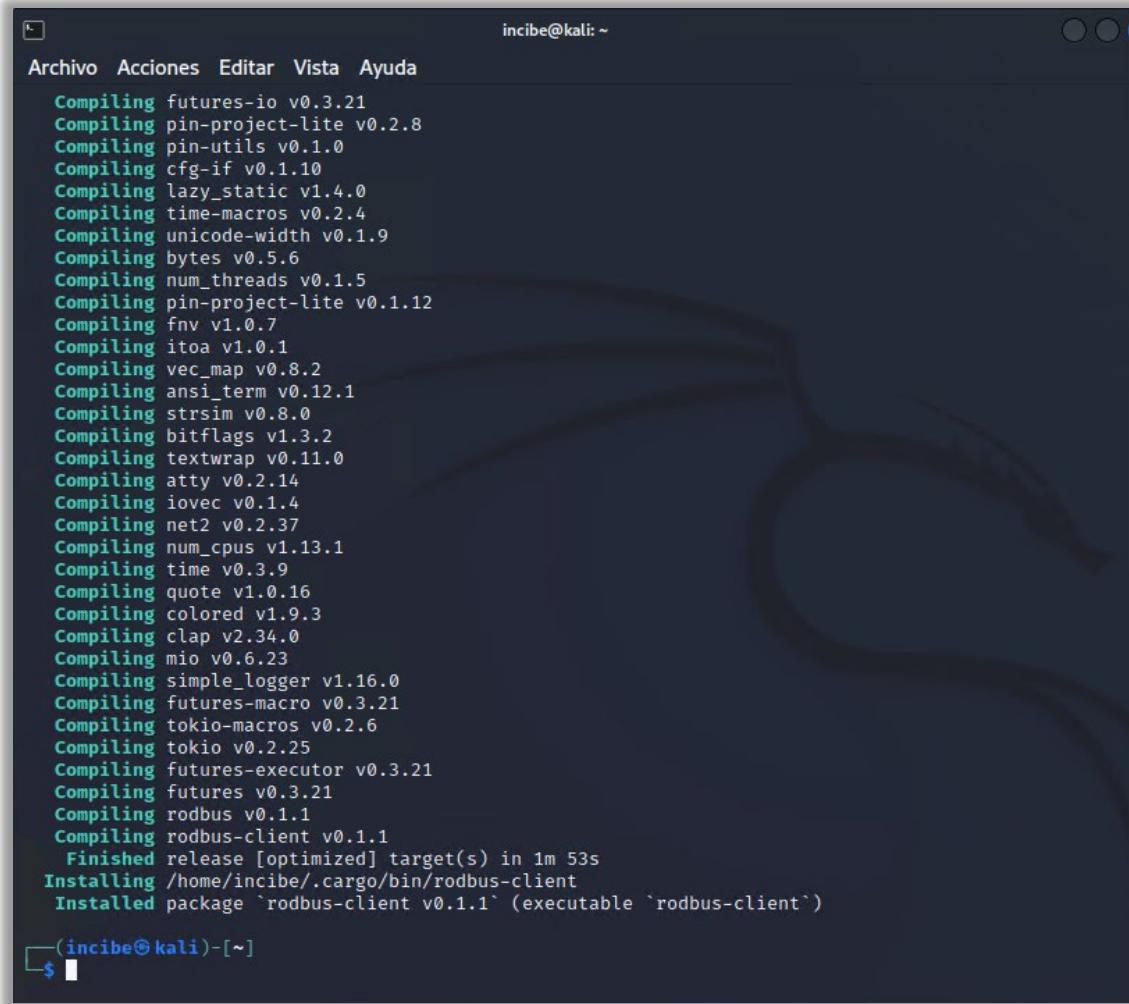
- Instala el paquete de software Rodbus-client con el gestor de paquetes «Cargo».
  - cargo install rodbus-client**



A screenshot of a terminal window titled "incibe@kali: ~". The window has a dark theme with light-colored text. The user is running the command \$ cargo install rodbus-client. The output shows the command being run, followed by "Updating crates.io index", then a progress bar indicating "Fetch [====>]" at 91.89%, with the message "(87616/100805) resolving deltas".

Ilustración 12: Paquete de software Rodbus-client con el gestor de paquetes «Cargo».

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

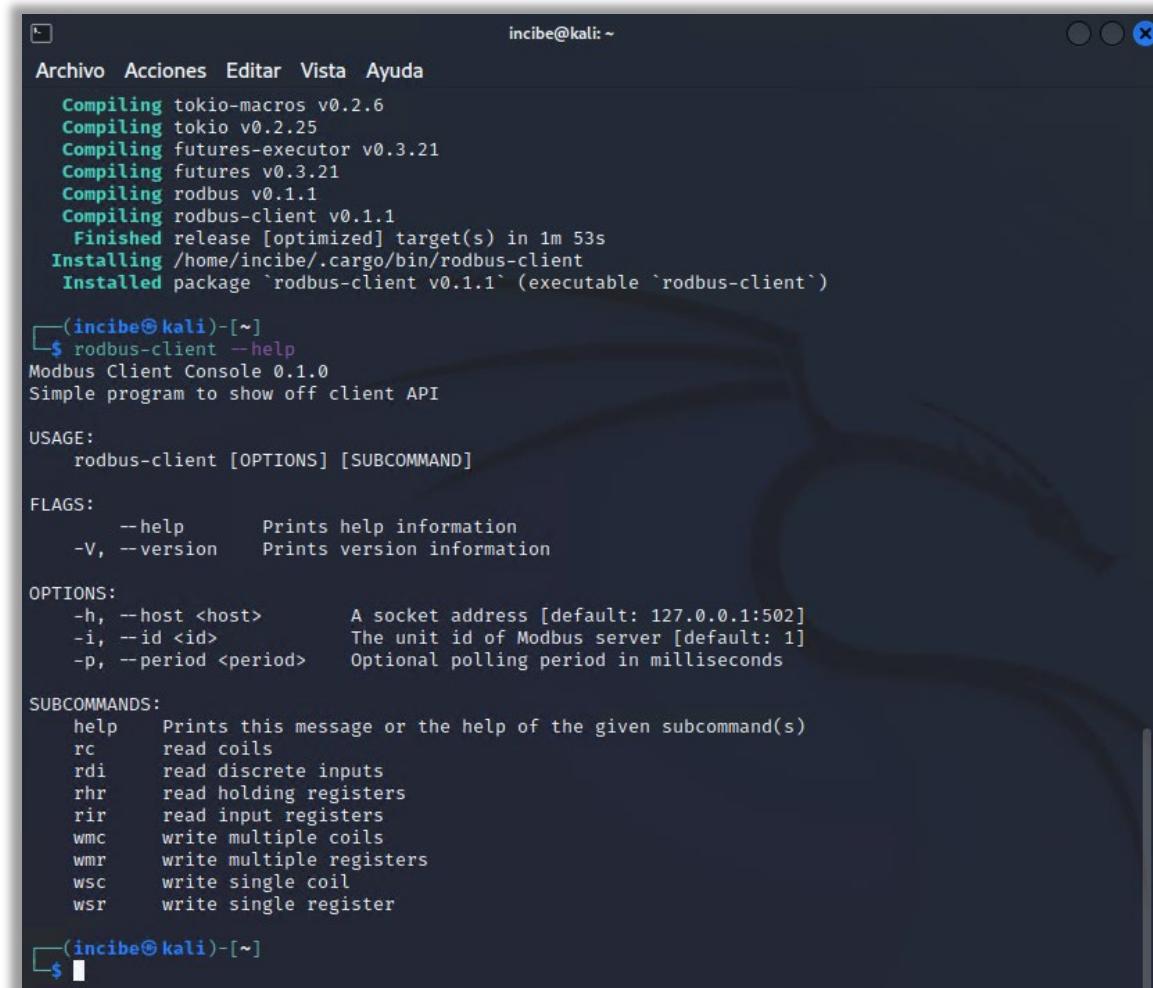


The screenshot shows a terminal window titled "incibe@kali: ~". The window displays the output of a Cargo build command. The output includes a list of dependencies being compiled, such as futures-io v0.3.21, pin-project-lite v0.2.8, pin-utils v0.1.0, cfg-if v0.1.10, lazy\_static v1.4.0, time-macros v0.2.4, unicode-width v0.1.9, bytes v0.5.6, num\_threads v0.1.5, pin-project-lite v0.1.12, fnv v1.0.7, itoa v1.0.1, vec\_map v0.8.2, ansi\_term v0.12.1, strsim v0.8.0, bitflags v1.3.2, textwrap v0.11.0, atty v0.2.14, iovec v0.1.4, net2 v0.2.37, num\_cpus v1.13.1, time v0.3.9, quote v1.0.16, colored v1.9.3, clap v2.34.0, mio v0.6.23, simple\_logger v1.16.0, futures-macro v0.3.21, tokio-macros v0.2.6, tokio v0.2.25, futures-executor v0.3.21, futures v0.3.21, rodlib v0.1.1, rodlib-client v0.1.1. The build process is completed with a message: "Finished release [optimized] target(s) in 1m 53s". It then installs the package: "Installing /home/incibe/.cargo/bin/rodlib-client" and "Installed package `rodlib-client v0.1.1` (executable `rodlib-client`)".

Ilustración 13: Instalación el paquete de software Rodbus-client con el gestor de paquetes «Cargo».

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

- Ejecuta la herramienta Rodbus-client con el parámetro --help, así confirmamos que la herramienta se ha instalado correctamente, ya que, si se ejecuta el comando, es que la herramienta está correctamente instalada y podemos utilizarla:
  - rodbus-client --help**



```
incibe@kali: ~
Archivo Acciones Editar Vista Ayuda
Compiling tokio-macros v0.2.6
Compiling tokio v0.2.25
Compiling futures-executor v0.3.21
Compiling futures v0.3.21
Compiling rodbus v0.1.1
Compiling rodbus-client v0.1.1
Finished release [optimized] target(s) in 1m 53s
Installing /home/incibe/.cargo/bin/rodbus-client
Installed package `rodbus-client v0.1.1` (executable `rodbus-client`)

└(incibe@kali)-[~]
$ rodbus-client --help
Modbus Client Console 0.1.0
Simple program to show off client API

USAGE:
  rodbus-client [OPTIONS] [SUBCOMMAND]

FLAGS:
  --help      Prints help information
  -V, --version  Prints version information

OPTIONS:
  -h, --host <host>      A socket address [default: 127.0.0.1:502]
  -i, --id <id>          The unit id of Modbus server [default: 1]
  -p, --period <period>   Optional polling period in milliseconds

SUBCOMMANDS:
  help    Prints this message or the help of the given subcommand(s)
  rc     read coils
  rdi    read discrete inputs
  rhr    read holding registers
  rir    read input registers
  wmc    write multiple coils
  wmr    write multiple registers
  wsc    write single coil
  wsr    write single register

└(incibe@kali)-[~]
$
```

Ilustración 14: Ejecución de la herramienta rodbus-client con el parámetro –help.

### 3

# INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.1 Arranque de simuladores del entorno industrial 1

- Vamos a emplear la MV del Entorno Industrial Ubuntu 20.04 LTS, para configurar las aplicaciones Snap 7 Server y Client Demo.
- Arranca la MV del Entorno Industrial Ubuntu 20.04 LTS.
- Ejecuta la aplicación de terminal Terminator y maximiza su ventana con el botón de maximizar (como en Windows). Dividimos la terminal de forma vertical.
  - Ctrl+Shift+E

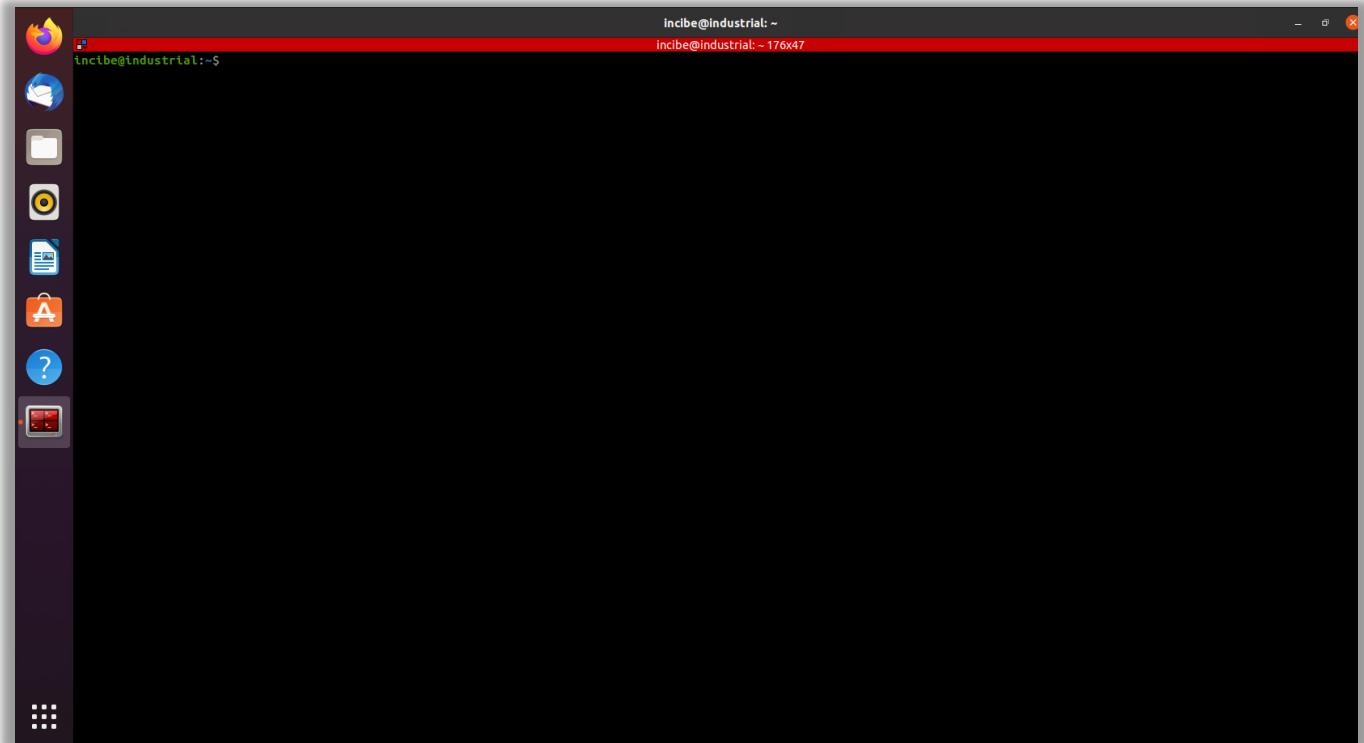


Ilustración 15: Ejecución de la aplicación de terminal Terminator.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.1 Arranque de simuladores del entorno industrial 1

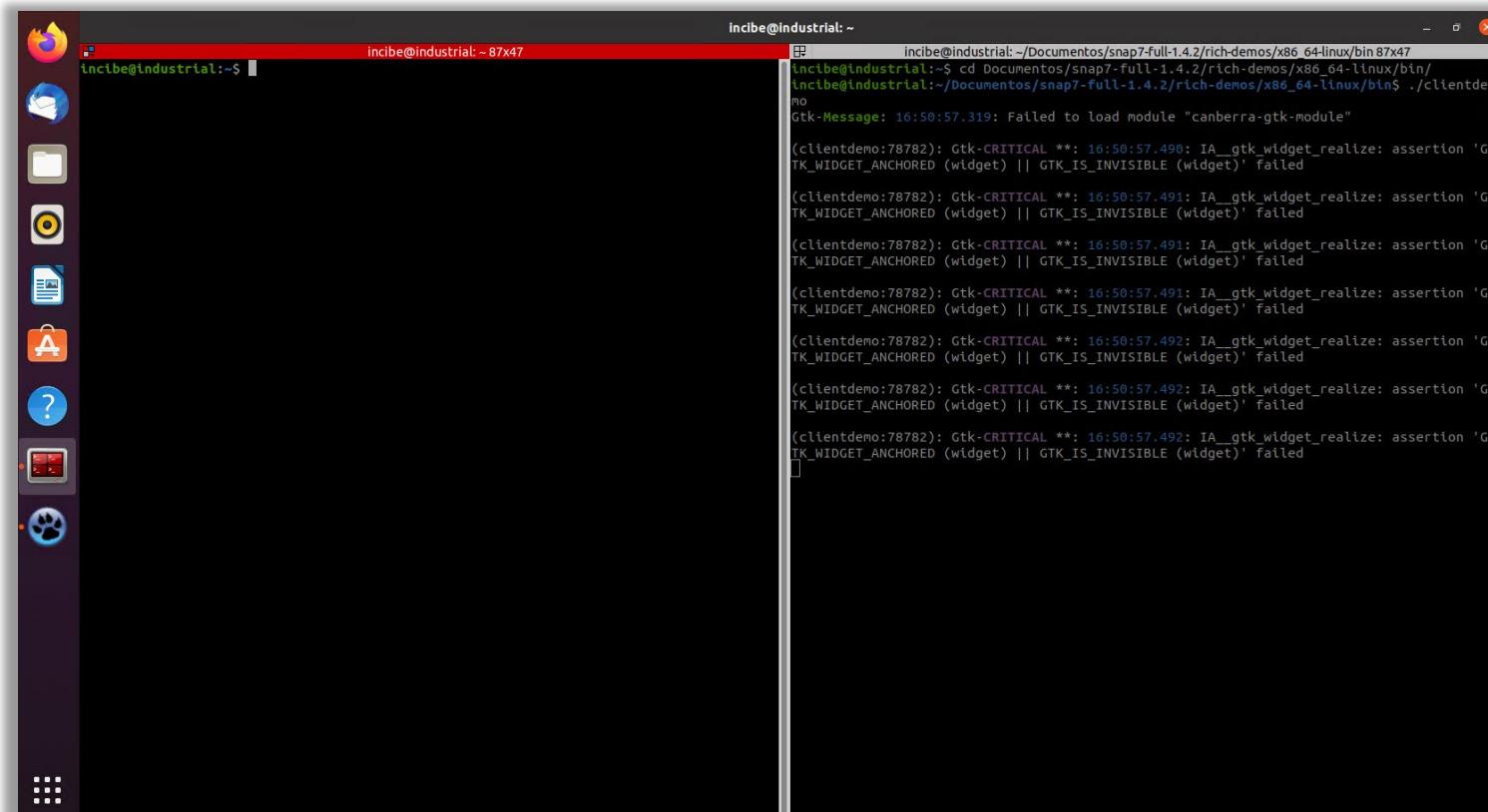


Ilustración 16: Dividir la terminal de forma vertical.

### 3 ◀ INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.1 Arranque de simuladores del entorno industrial 1

- En la terminal derecha accede a la ubicación donde se encuentra la aplicación Snap7 y ejecuta la aplicación Snap7 Client Demo.

Para ello, tenemos que acceder a la carpeta donde se encuentra la herramienta, que está en «Documentos» y ejecutar la aplicación.

- **cd Documentos/snap7-full-1.4.2/rich-demos/x86\_64-linux/bin**
- **sudo ./clientdemo**

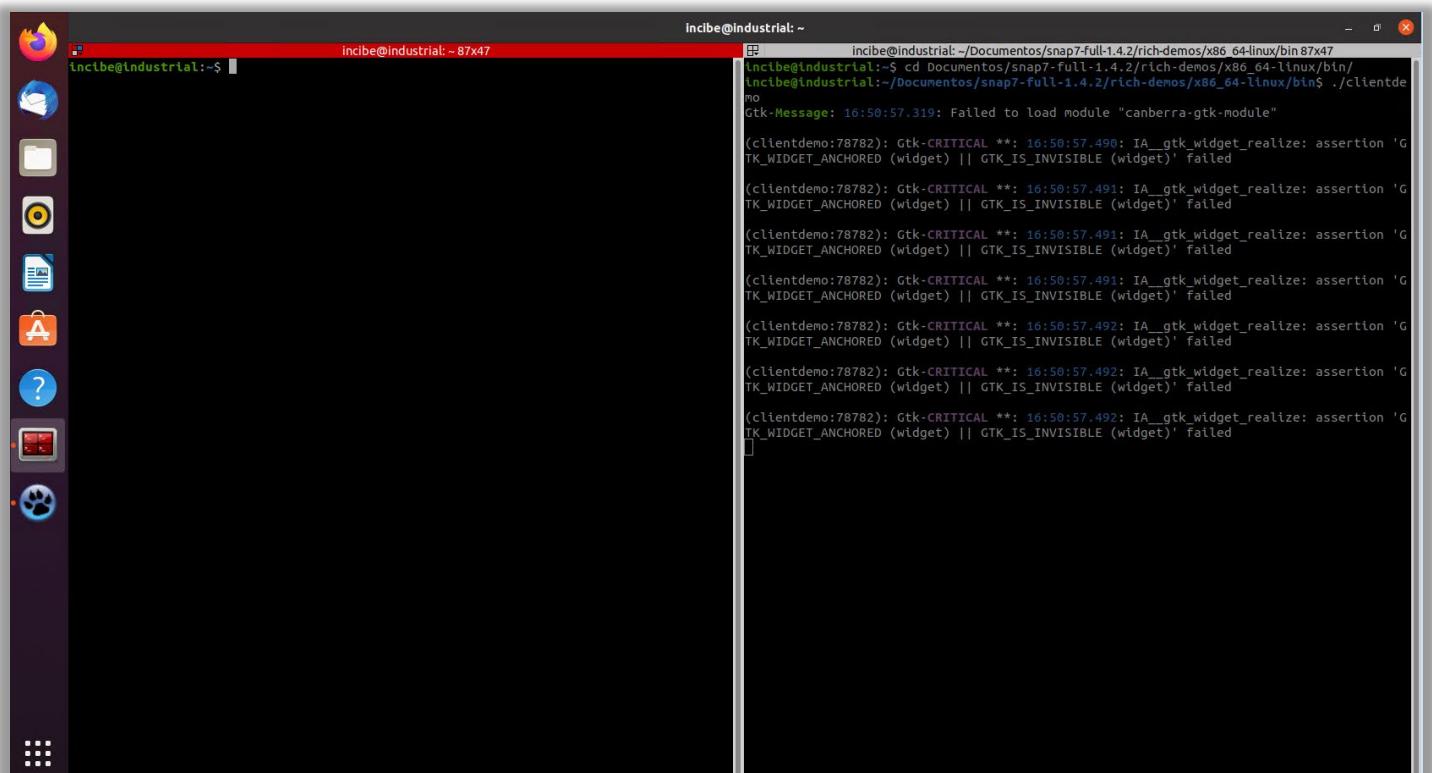


Ilustración 17: En la terminal derecha ejecuta la aplicación Snap7 Client Demo.

# **3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT**

### **3.1 Arranque de simuladores del entorno industrial 1**

- En la terminal izquierda accede a la ubicación donde se encuentra la aplicación Snap7 y ejecuta la aplicación Snap7 Server Demo.
    - **cd Documentos/snap7-full-1.4.2/rich-demos/x86\_64-linux/bin**
    - **sudo ./serverdemo**

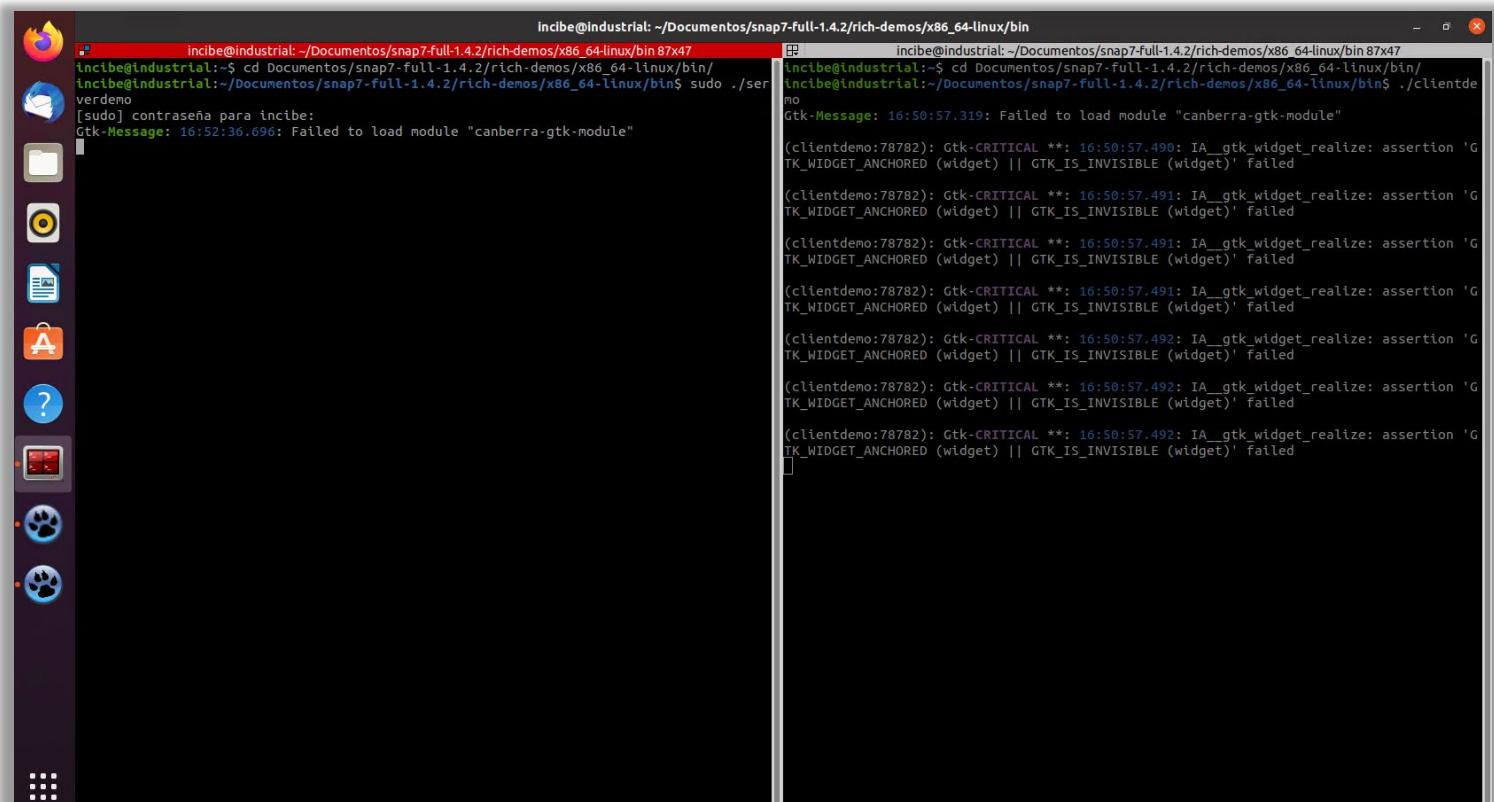


Ilustración 18: En la terminal izquierda ejecuta la aplicación Snap7 Server Demo.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.1 Arranque de simuladores del entorno industrial 1

- Una vez hecho esto, tendremos ejecutadas ambas aplicaciones.

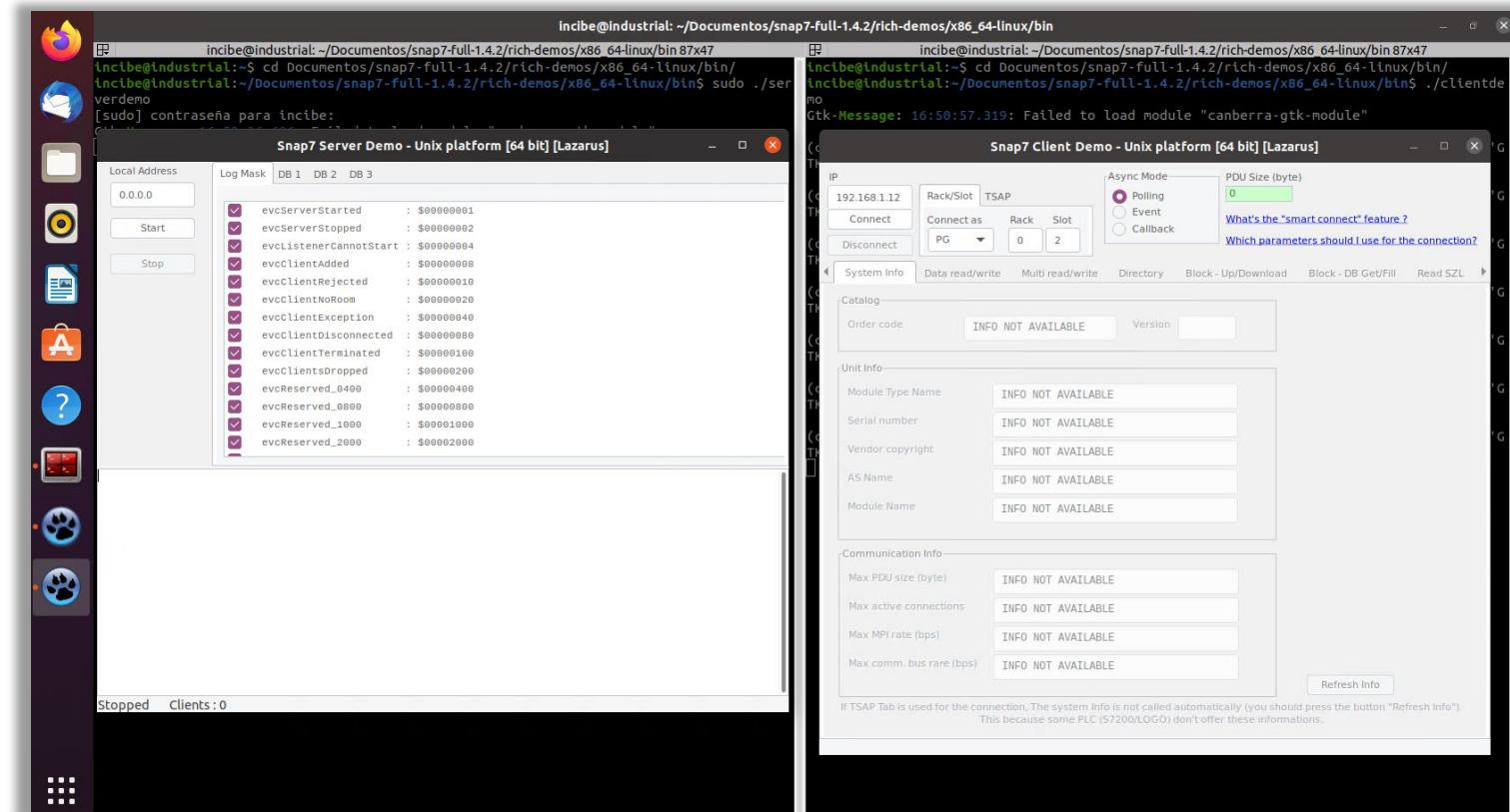


Ilustración 19: Ejecución de ambas aplicaciones.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.1 Arranque de simuladores del entorno industrial 1

- Abre una terminal nueva Terminator y ejecuta el comando **ifconfig** para conocer la dirección IP asignada al adaptador de red.

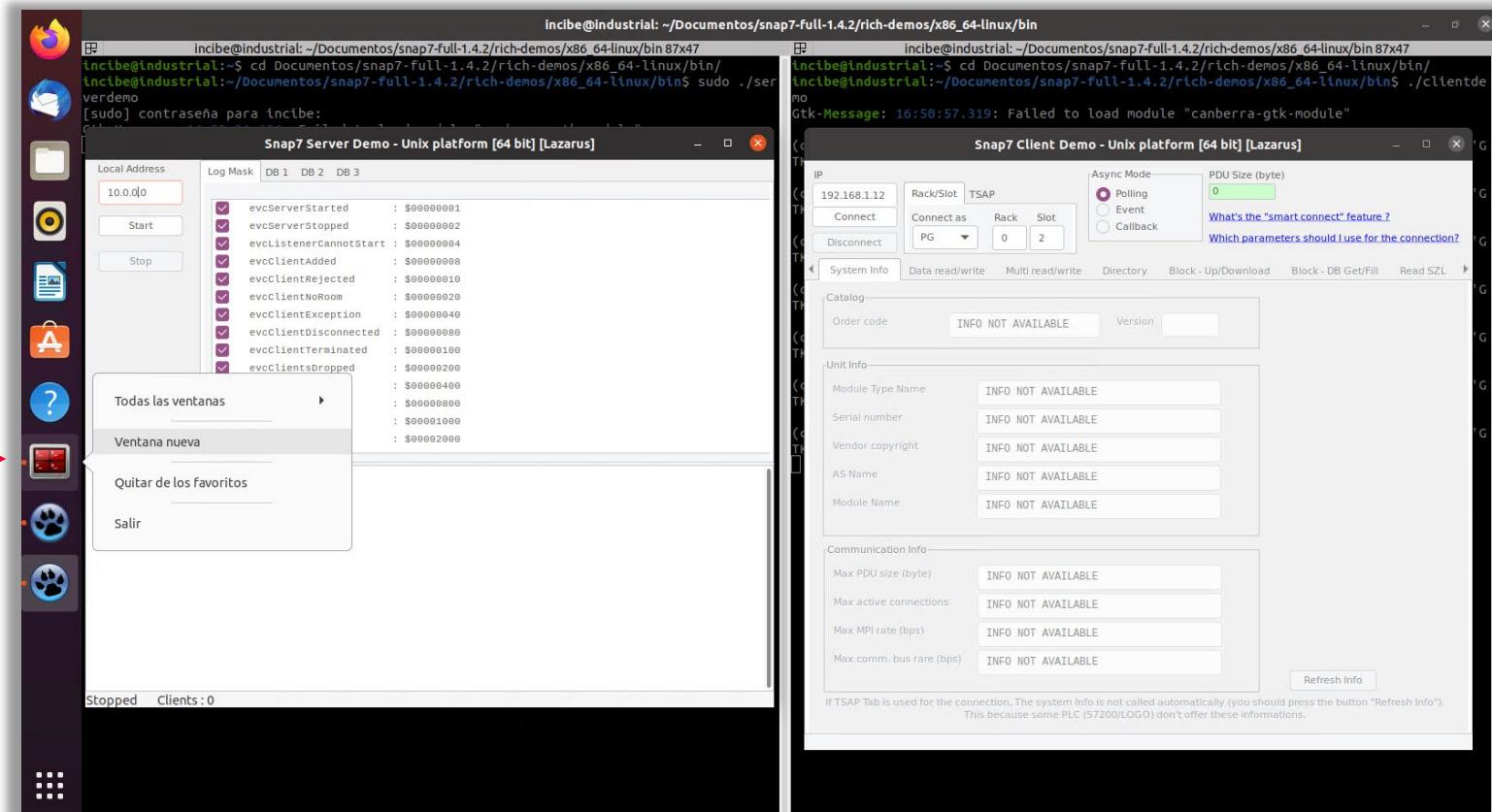
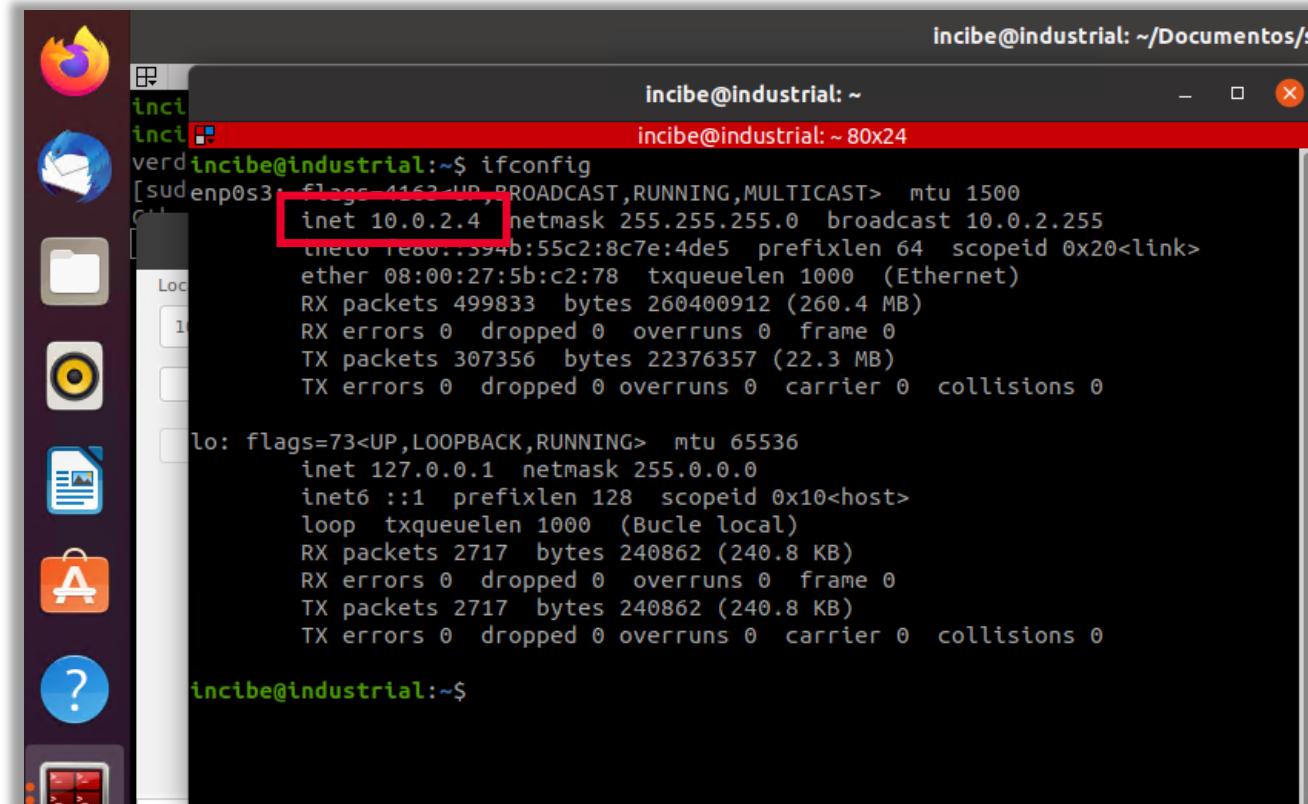


Ilustración 20: Nuevo terminal Terminator.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.1 Arranque de simuladores del entorno industrial 1

- Abre una terminal nueva Terminator y ejecuta el comando **ifconfig** para conocer la dirección IP asignada al adaptador de red.



```
incibe@industrial: ~
```

```
incibe@industrial: ~
```

```
incibe@industrial: ~ 80x24
```

```
incibe@industrial:~$ ifconfig
```

```
[sud] enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
          inet 10.0.2.4 netmask 255.255.255.0 broadcast 10.0.2.255
              ether 08:00:27:5b:c2:78 txqueuelen 1000 (Ethernet)
              RX packets 499833 bytes 260400912 (260.4 MB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 307356 bytes 22376357 (22.3 MB)
              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 2717 bytes 240862 (240.8 KB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 2717 bytes 240862 (240.8 KB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
incibe@industrial:~$
```

Ilustración 21: Ejecución del comando ifconfig.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.1 Arranque de simuladores del entorno industrial 1

- Establecemos esta misma dirección IP tanto en la aplicación Snap7 Server Demo como en la aplicación Snap7 Client Demo.  
En esta última selecciona el modo de conexión como «S7 BASIC» y pulsa en «Start», primero en Snap7 Server Demo y después «Connect» en Snap7 Client Demo.  
Comprueba como en la aplicación cliente nos aparecen todos los datos del PLC Siemens (que hace las veces de server).

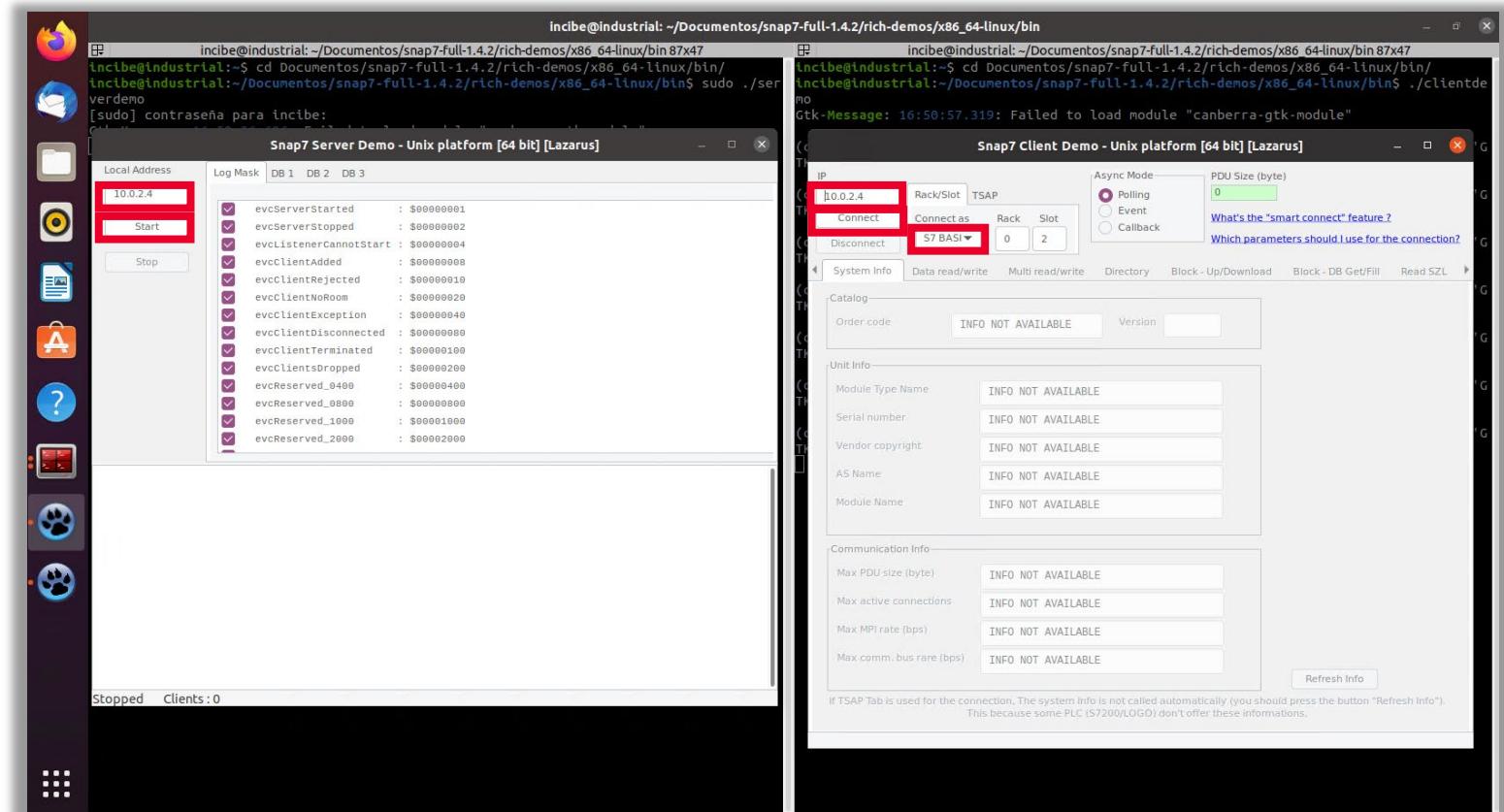


Ilustración 22: Se establece la misma dirección IP en la aplicación Snap7 Server Demo como en la aplicación Snap7 Client Demo.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.1 Arranque de simuladores del entorno industrial 1

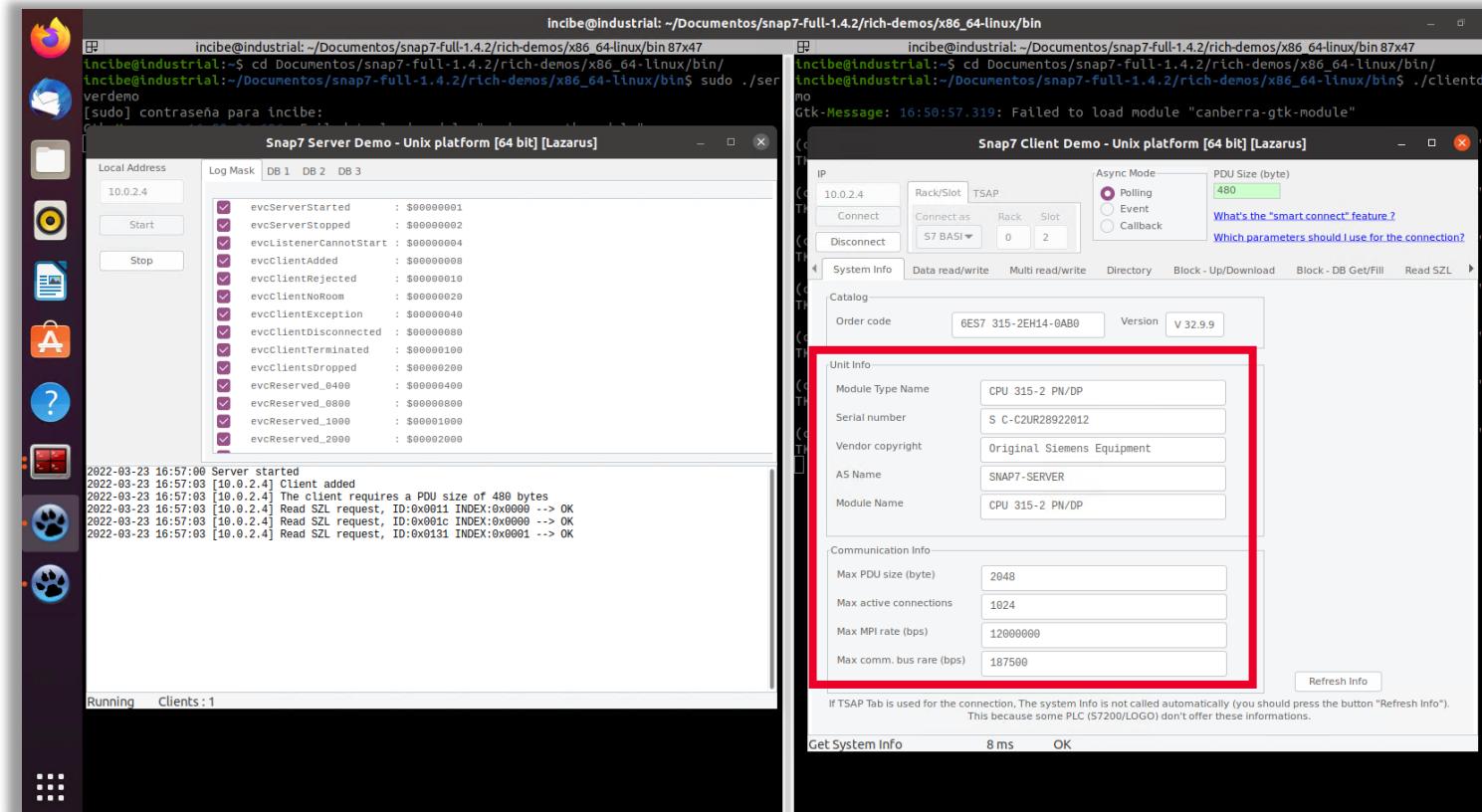


Ilustración 23: Comprobación de los datos del PLC Siemens.

### 3

# INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

### Instalación y configuración de ModbusPal

- Ejecuta la aplicación de terminal Terminator en caso de que la hubieras cerrado y maximiza su ventana con el botón de maximizar (como en Windows). Divide la terminal de forma vertical.

En la terminal derecha accede a la ubicación donde se encuentra la aplicación ModbusPal y ejecútala.

- **cd Documentos/modbuspal/**
- **sudo java -jar ModbusPal.jar**

### 3

# INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

- Puede pedir que introduzcas la contraseña en caso de que cerraras la terminal previamente.

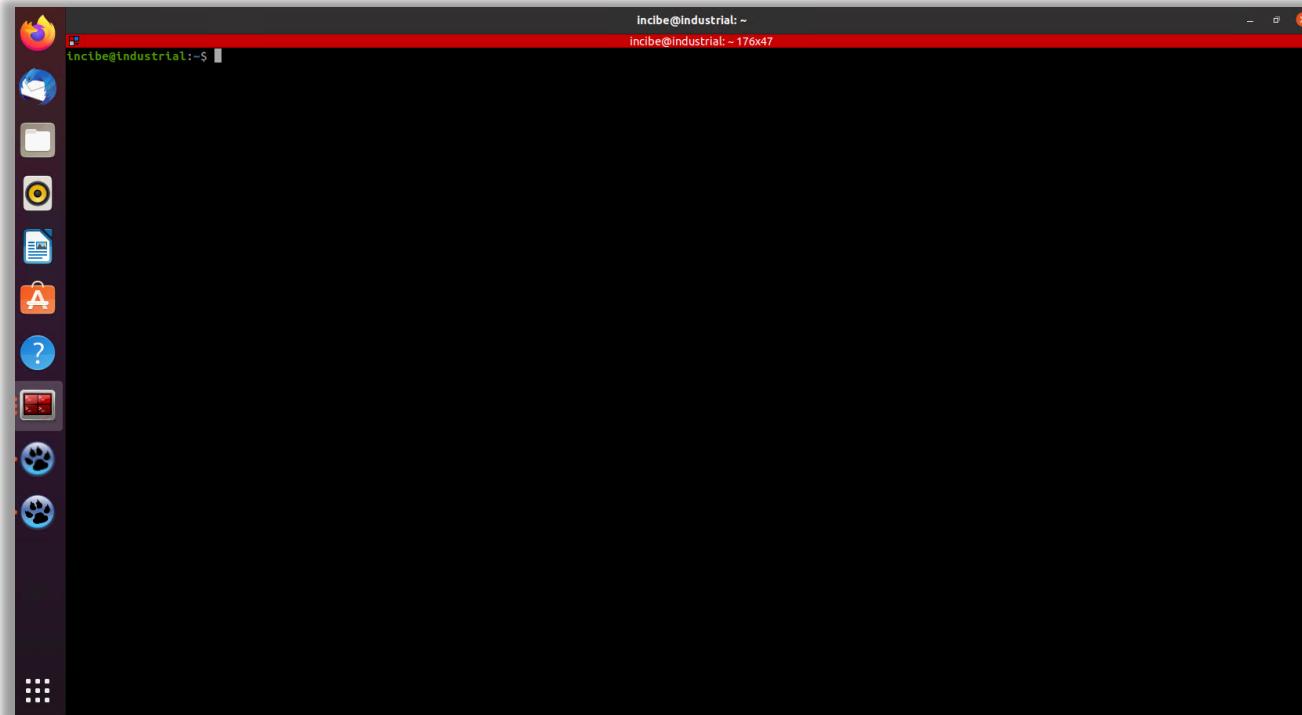


Ilustración 24: Ejecución la aplicación de terminal Terminator.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

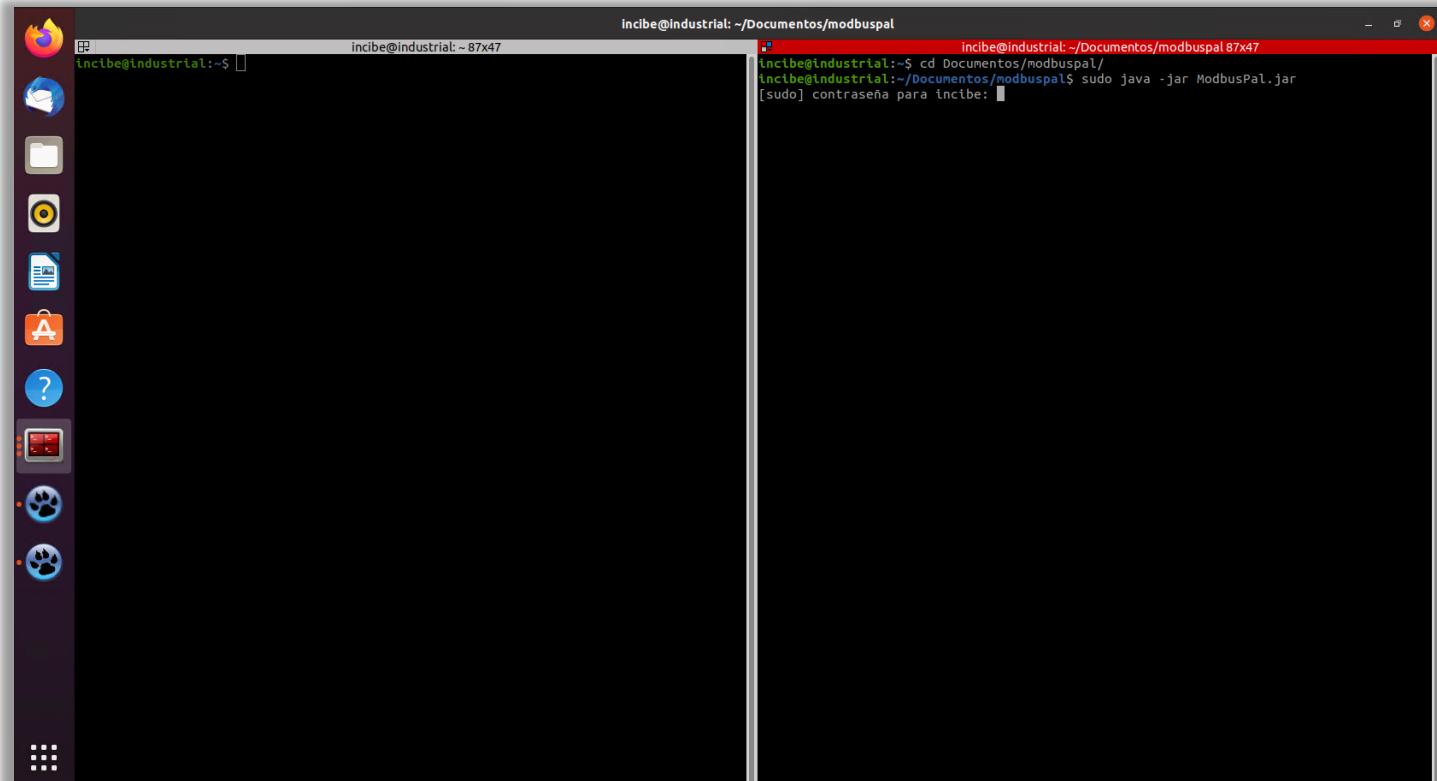


Ilustración 25: Terminal derecha: abre la aplicación ModbusPal (I).

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

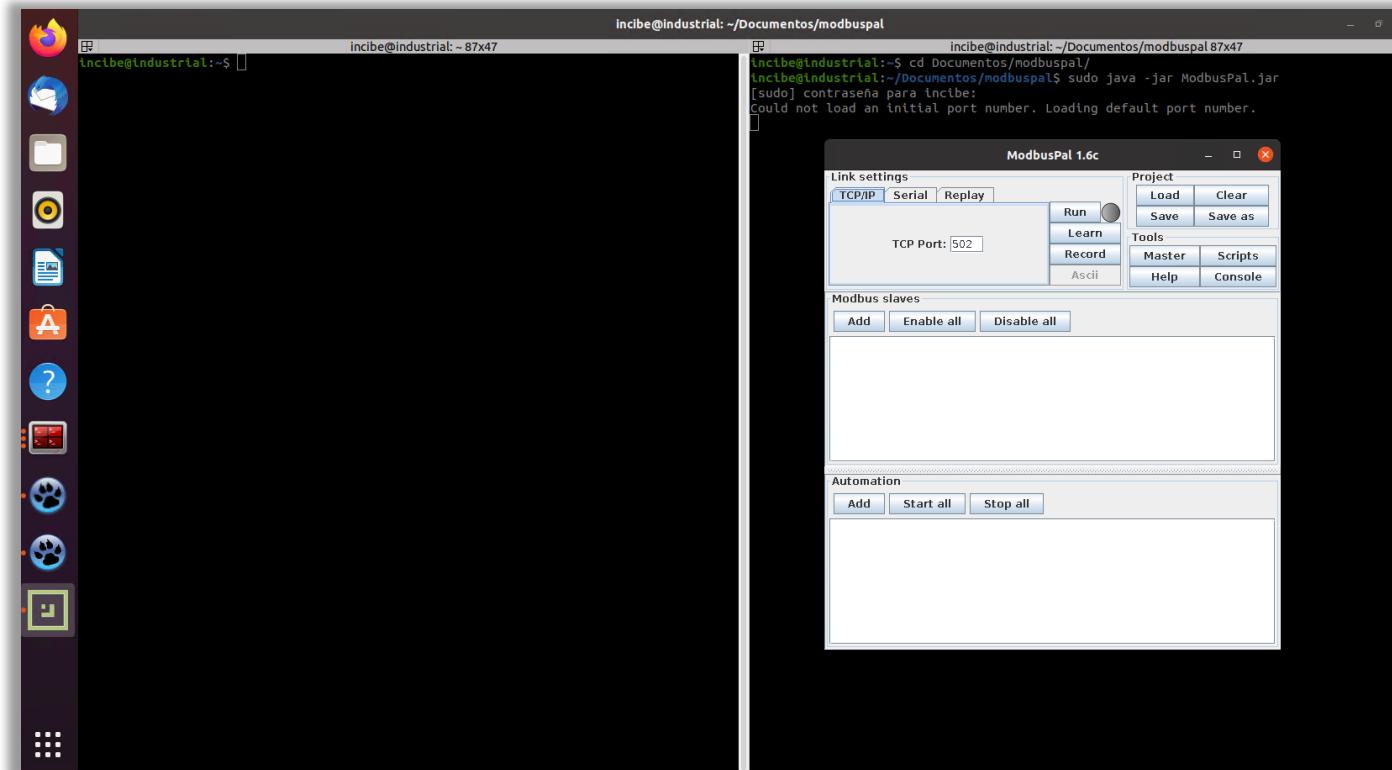


Ilustración 26: Terminal derecha: abre la aplicación ModbusPal (II).

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

- Añadimos un esclavo.

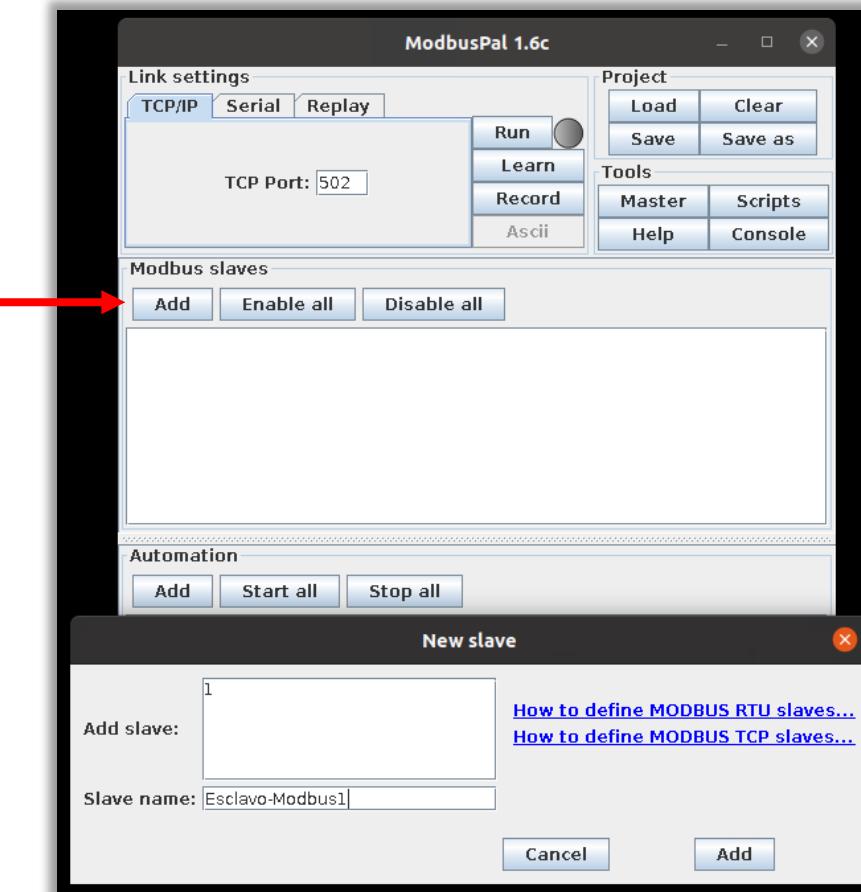


Ilustración 27: Añadir un esclavo.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

- Lo editamos pulsando en el icono que representa un ojo, y en la pestaña «*Holding Register*», añadimos 5 registros. Establecemos sus valores según aparece en la imagen (las celdas se comportan como en Excel). Selecciona la pestaña *coils* y añadimos 10 *coils*. Establecemos sus valores según como aparece en las siguientes imágenes.

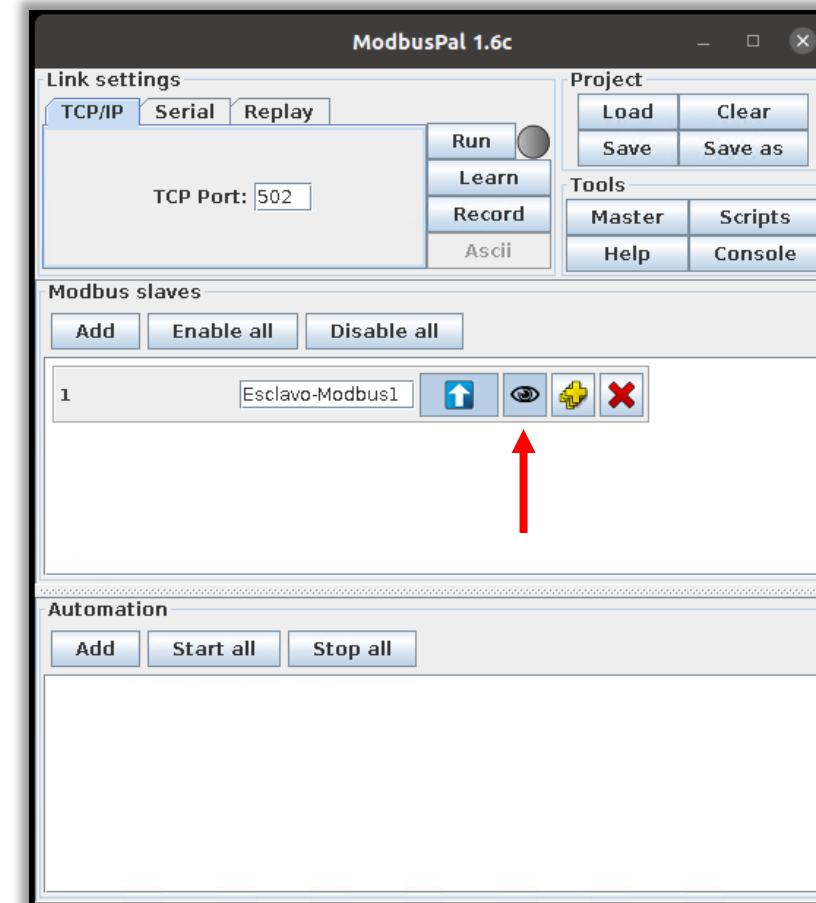


Ilustración 28: Edición del esclavo.

# 3 ◀ INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

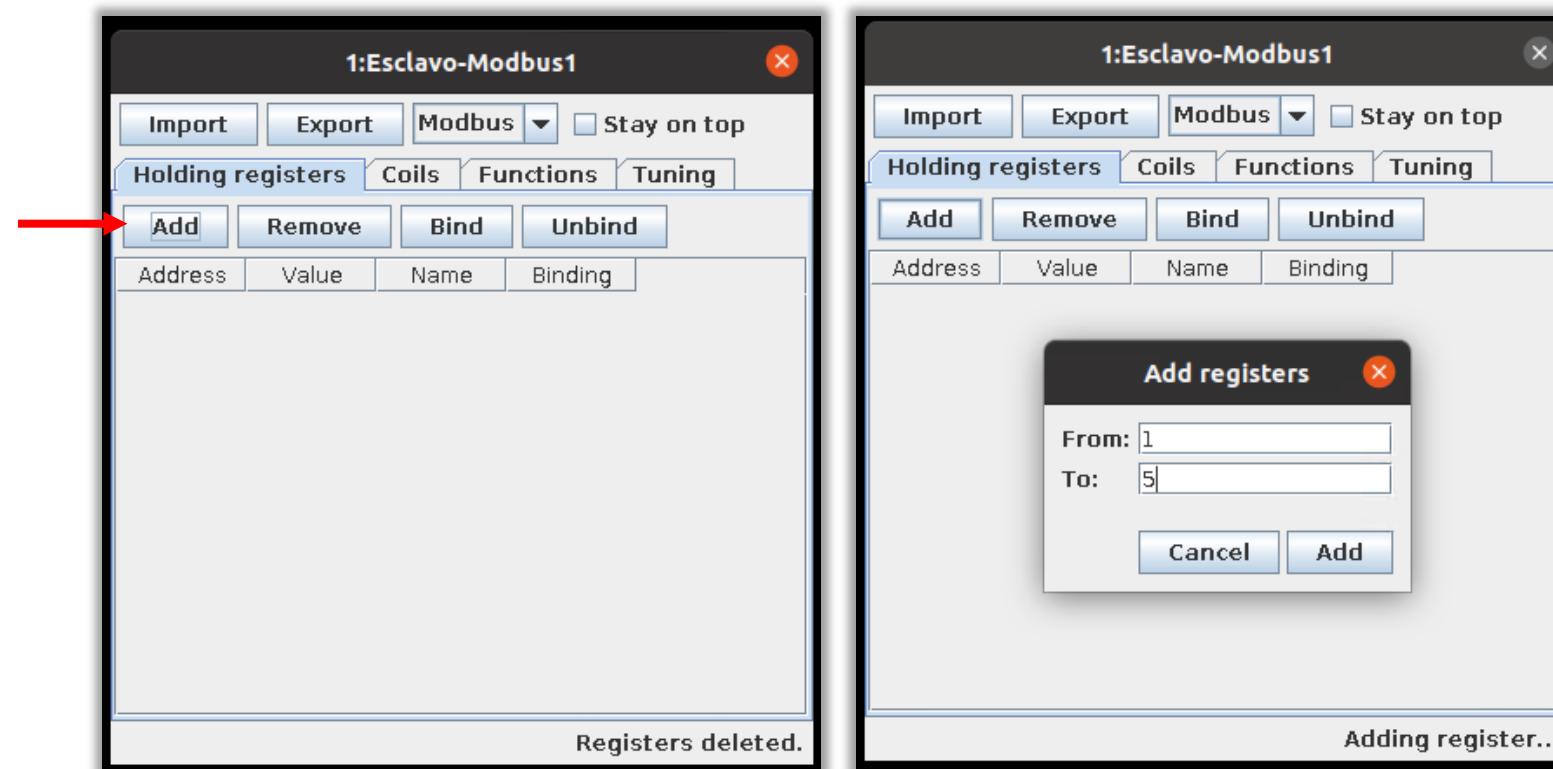


Ilustración 29: Añadir registros.

Ilustración 30: Añadir cinco registros.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

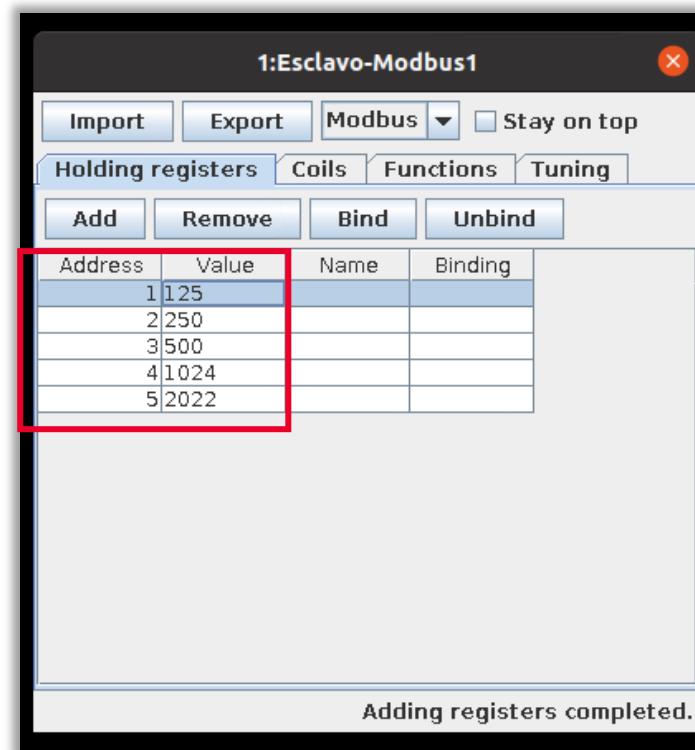


Ilustración 31: Añadir valores de los registros.

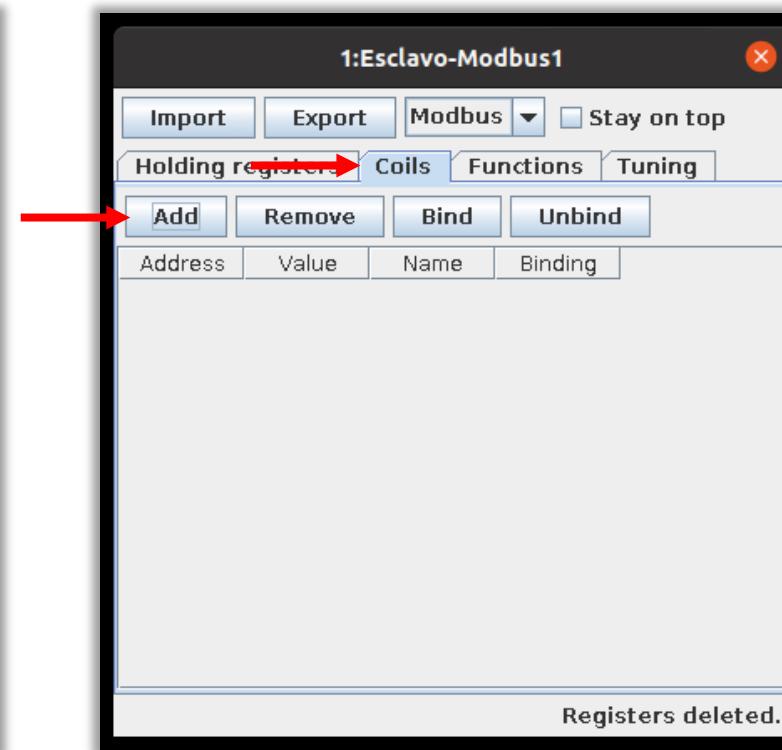


Ilustración 32: Acceso a la pestaña coils.

# 3 ◀ INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

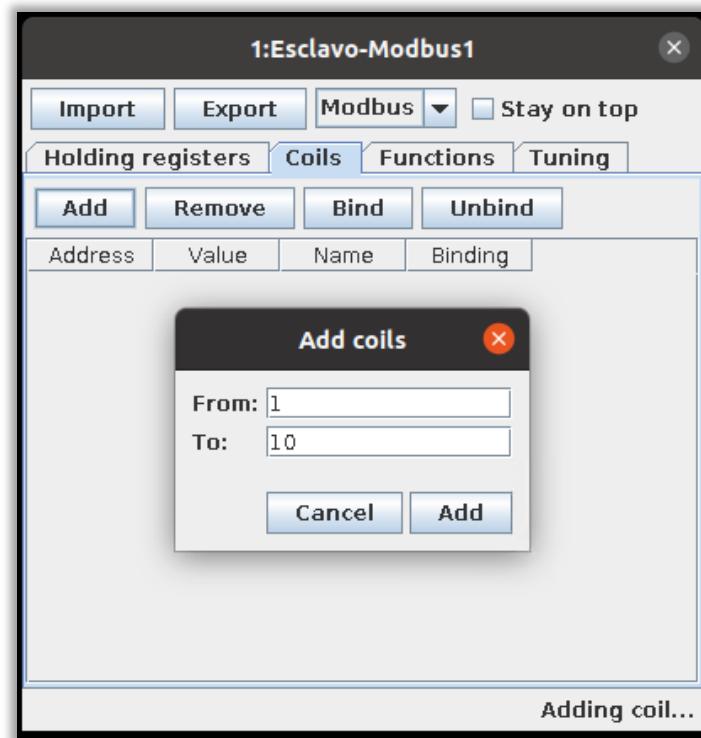


Ilustración 33: Número de *coils* que se añaden.

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

Ilustración 34: Valores dados.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

- Añadimos un segundo esclavo. Lo editamos pulsando en el icono que representa un ojo, y en la pestaña «*Holding Register*», añadimos 3 registros. Establecemos sus valores según como aparece en las siguientes imágenes.

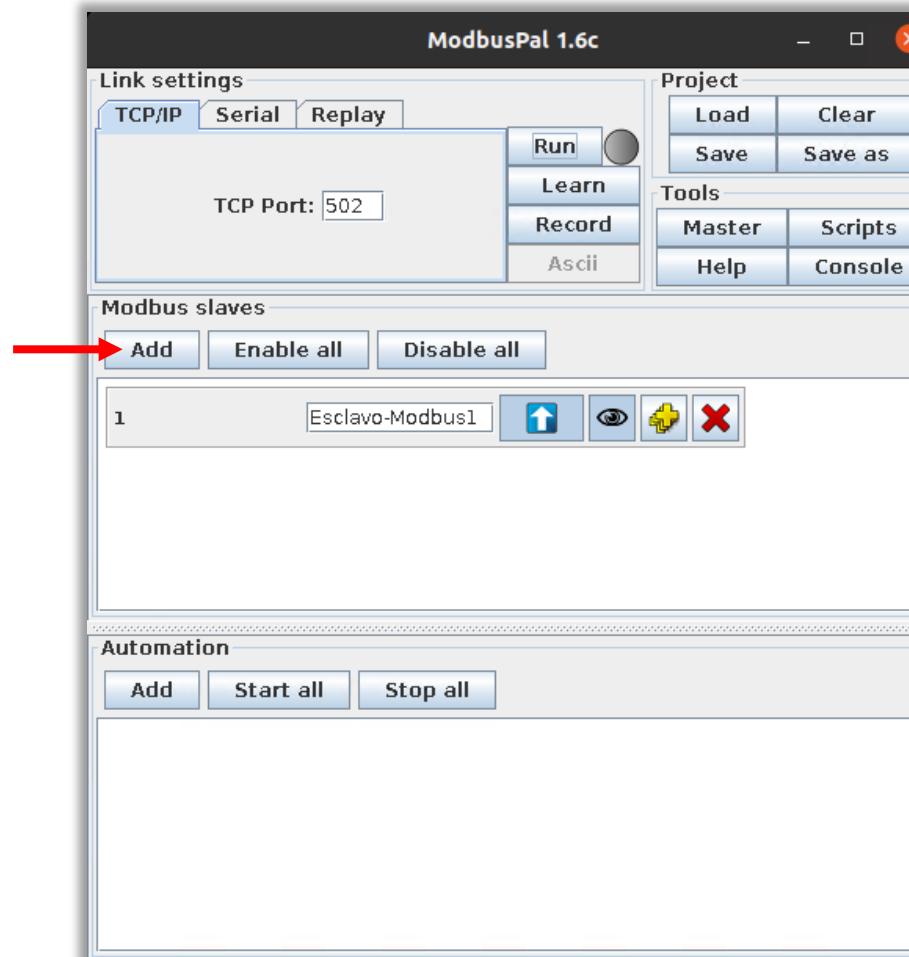


Ilustración 35: Añadir un segundo esclavo (I).

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2



Ilustración 36: Añadir un segundo esclavo (II).

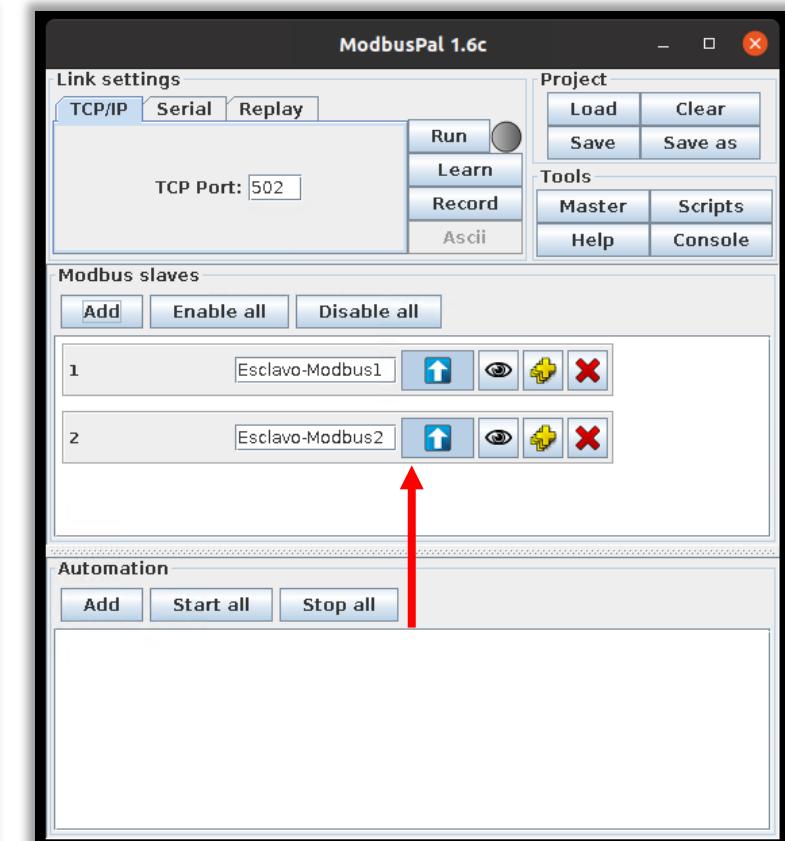


Ilustración 37: Edición del segundo esclavo.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

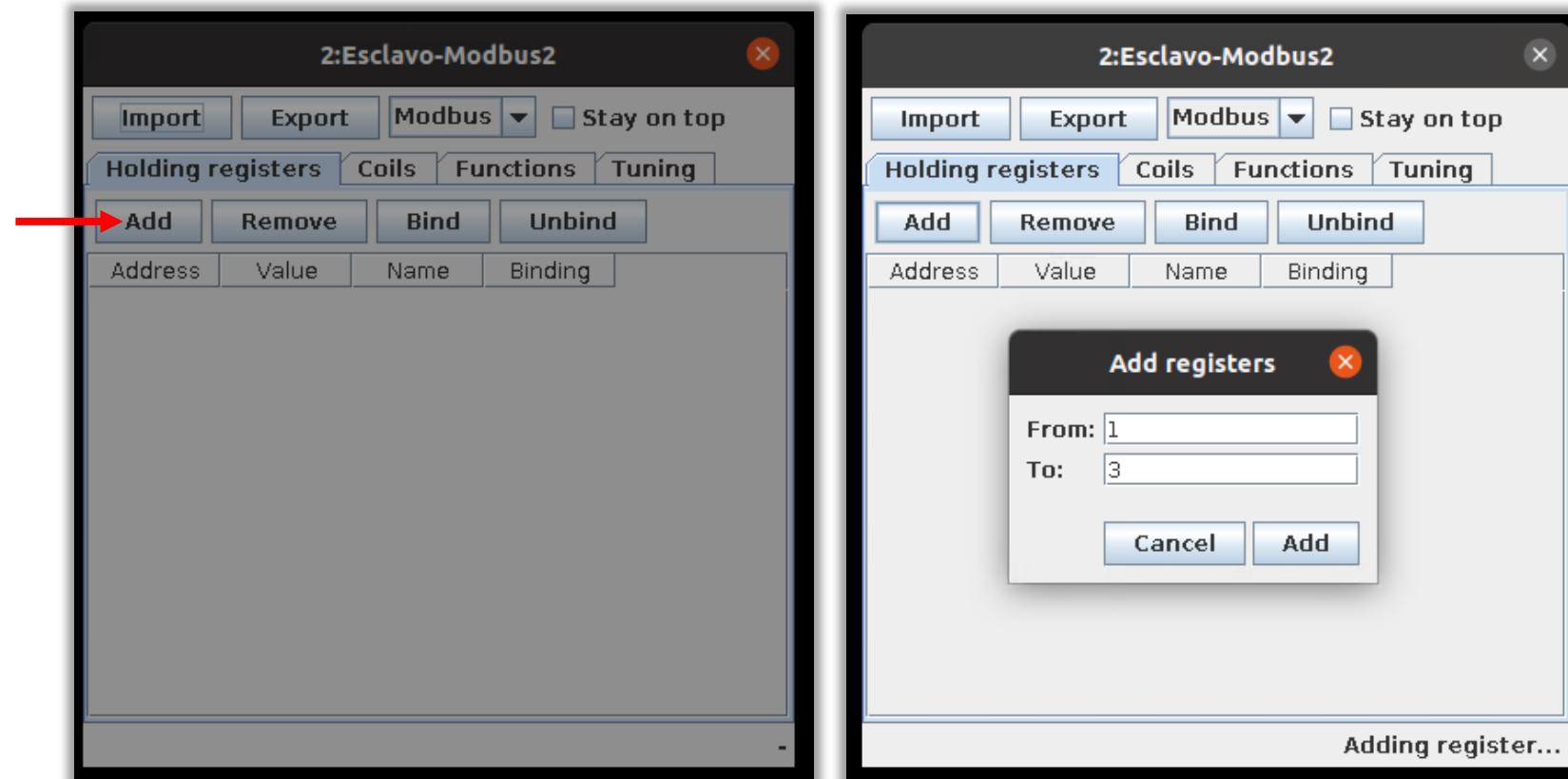


Ilustración 38: Añadir datos en «*Holding registers*».

Ilustración 39: Añadir tres registros.

### 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

#### 3.2 Arranque de simuladores del entorno industrial 2

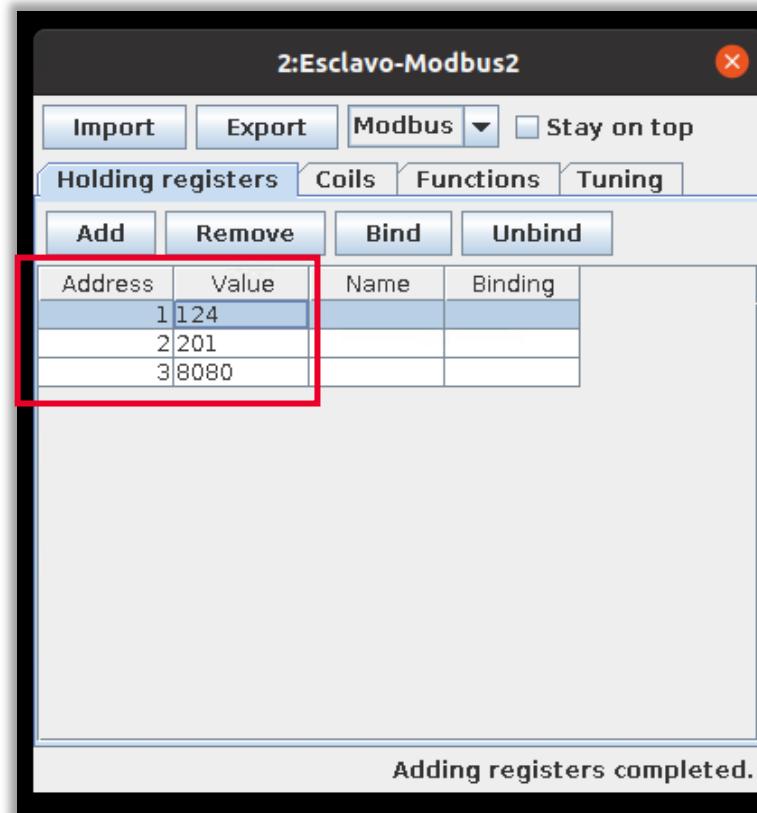


Ilustración 40: Valores de los registros añadidos.

# 3 INSTALACIÓN Y CONFIGURACIÓN DE RODBUS-CLIENT

## 3.2 Arranque de simuladores del entorno industrial 2

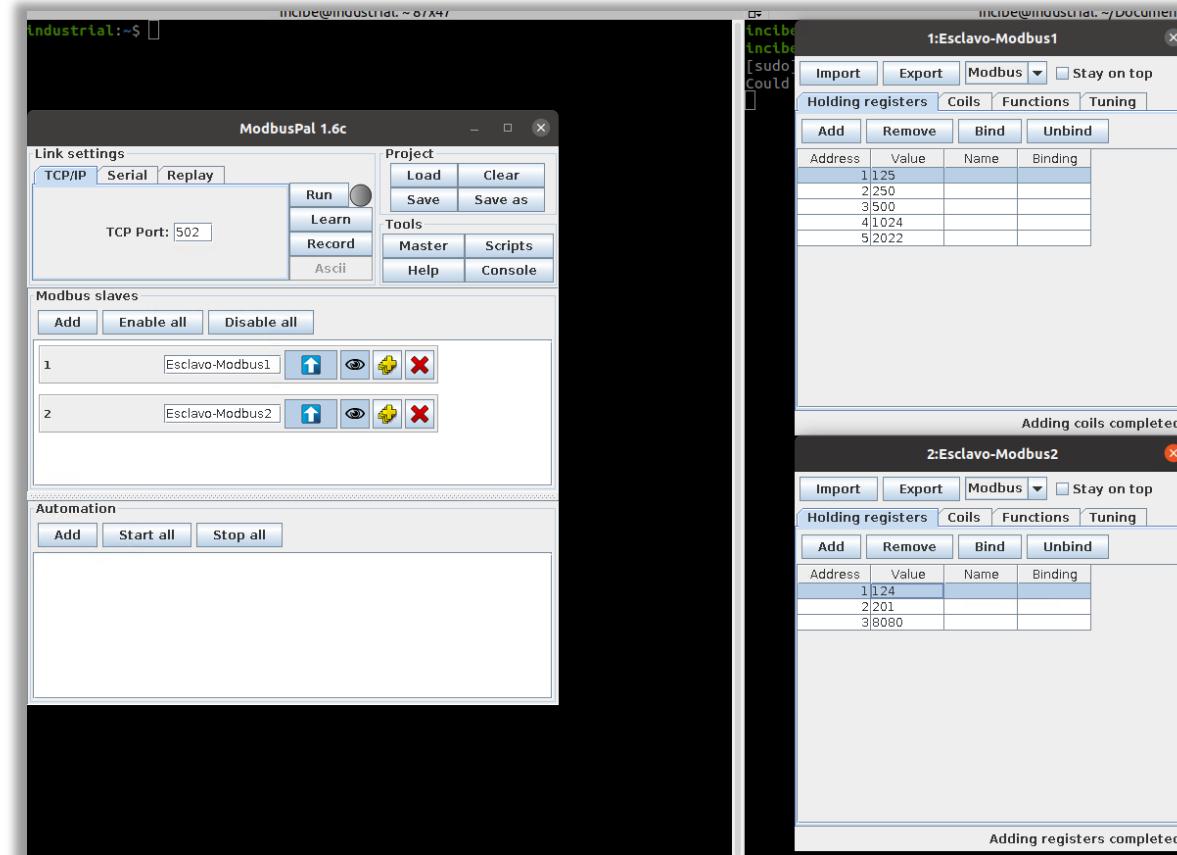


Ilustración 41: Esclavos creados.

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

# 4



## 4

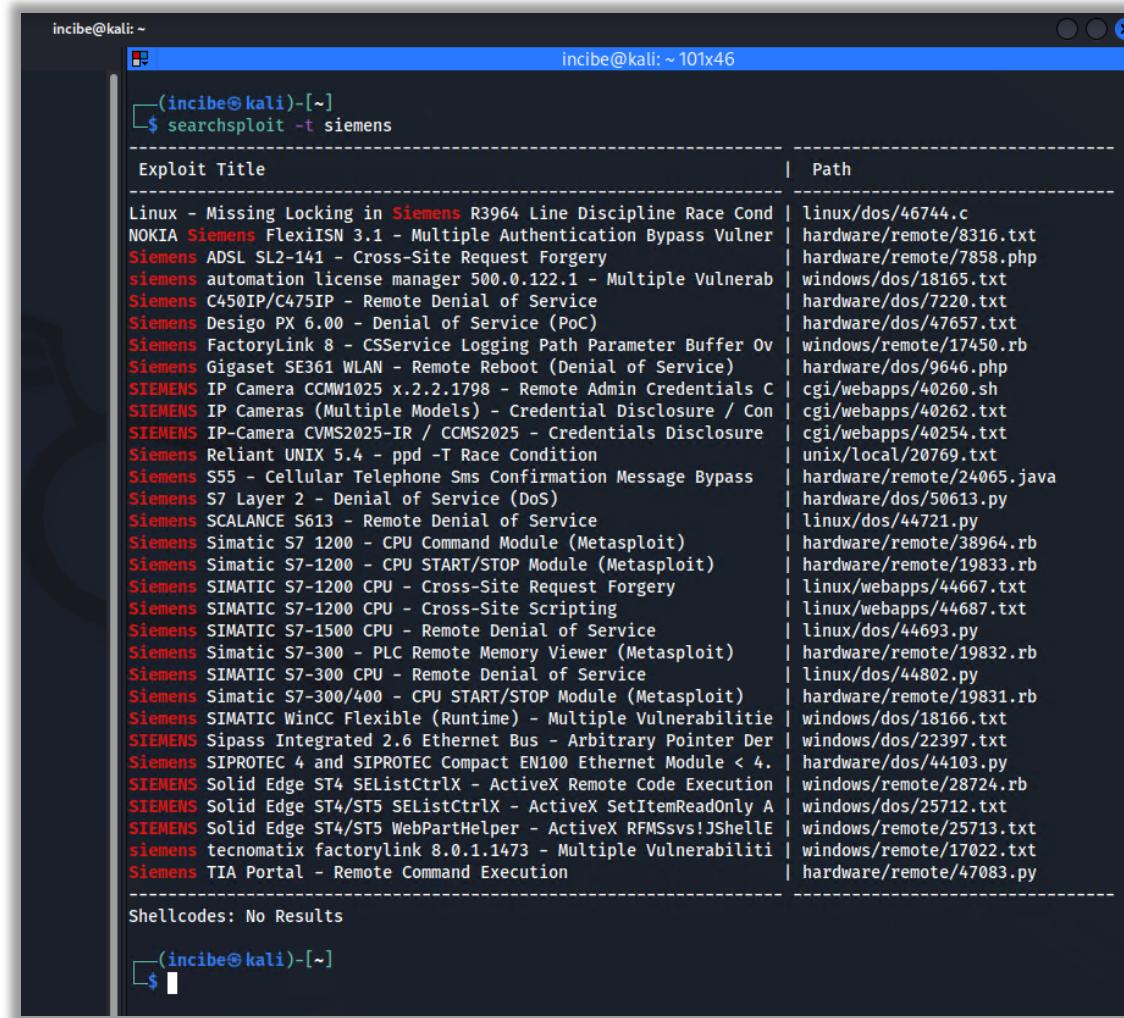
# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

En este apartado, buscaremos un *exploit* de terceros (para Metasploit Framework) y lo incorporaremos a la herramienta Searchsploit para ejecutarlo y atacar vulnerabilidades de dispositivos Siemens.

- Nos situamos en la máquina virtual Kali Linux y abre una nueva terminal. Ejecuta la herramienta Searchsploit y busca un *exploit* para dispositivos cuyo nombre de *exploit* contenga la palabra «Siemens».
  - **searchsploit -t siemens**

## 4

# BÚSQUEDA DE EXPLOIT CON SEARCHSPLOIT



```
incibe@kali: ~
incibe@kali: ~ 101x46
(incibe㉿kali)-[~]
$ searchsploit -t siemens
-----[REDACTED]-----
Exploit Title | Path
-----[REDACTED]-----
Linux - Missing Locking in siemens R3964 Line Discipline Race Condition | linux/dos/46744.c
NOKIA Siemens FlexiISN 3.1 - Multiple Authentication Bypass Vulnerability | hardware/remote/8316.txt
Siemens ADSL SL2-141 - Cross-Site Request Forgery | hardware/remote/7858.php
siemens automation license manager 500.0.122.1 - Multiple Vulnerabilities | windows/dos/18165.txt
Siemens C450IP/C475IP - Remote Denial of Service | hardware/dos/7220.txt
Siemens Desigo PX 6.00 - Denial of Service (PoC) | hardware/dos/47657.txt
Siemens FactoryLink 8 - CSService Logging Path Parameter Buffer Overflow | windows/remote/17450.rb
Siemens Gigaset SE361 WLAN - Remote Reboot (Denial of Service) | hardware/dos/9646.php
SIEMENS IP Camera CCMW1025 x.2.2.1798 - Remote Admin Credentials Disclosure | cgi/webapps/40260.sh
SIEMENS IP Cameras (Multiple Models) - Credential Disclosure / Configuration | cgi/webapps/40262.txt
SIEMENS IP-Camera CVMS2025-IR / CCMS2025 - Credentials Disclosure | cgi/webapps/40254.txt
Siemens Reliant UNIX 5.4 - ppd -T Race Condition | unix/local/20769.txt
Siemens S55 - Cellular Telephone Sms Confirmation Message Bypass | hardware/remote/24065.java
Siemens S7 Layer 2 - Denial of Service (DoS) | hardware/dos/50613.py
Siemens SCALANCE S613 - Remote Denial of Service | linux/dos/44721.py
Siemens Simatic S7 1200 - CPU Command Module (Metasploit) | hardware/remote/38964.rb
Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit) | hardware/remote/19833.rb
Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery | linux/webapps/44667.txt
Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting | linux/webapps/44687.txt
Siemens SIMATIC S7-1500 CPU - Remote Denial of Service | linux/dos/44693.py
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb
Siemens SIMATIC WinCC Flexible (Runtime) - Multiple Vulnerabilities | windows/dos/18166.txt
SIEMENS Sipass Integrated 2.6 Ethernet Bus - Arbitrary Pointer Dereferencing | windows/dos/22397.txt
Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4.0 | hardware/dos/44103.py
SIEMENS Solid Edge ST4 SEListCtrlX - ActiveX Remote Code Execution | windows/remote/28724.rb
SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX SetItemReadOnly A | windows/dos/25712.txt
SIEMENS Solid Edge ST4/ST5 WebPartHelper - ActiveX RFMssv!JShell | windows/remote/25713.txt
siemens tecnomatix factorylink 8.0.1.1473 - Multiple Vulnerabilities | windows/remote/17022.txt
Siemens TIA Portal - Remote Command Execution | hardware/remote/47083.py
-----[REDACTED]-----
Shellcodes: No Results
-----[REDACTED]-----
(incibe㉿kali)-[~]
$
```

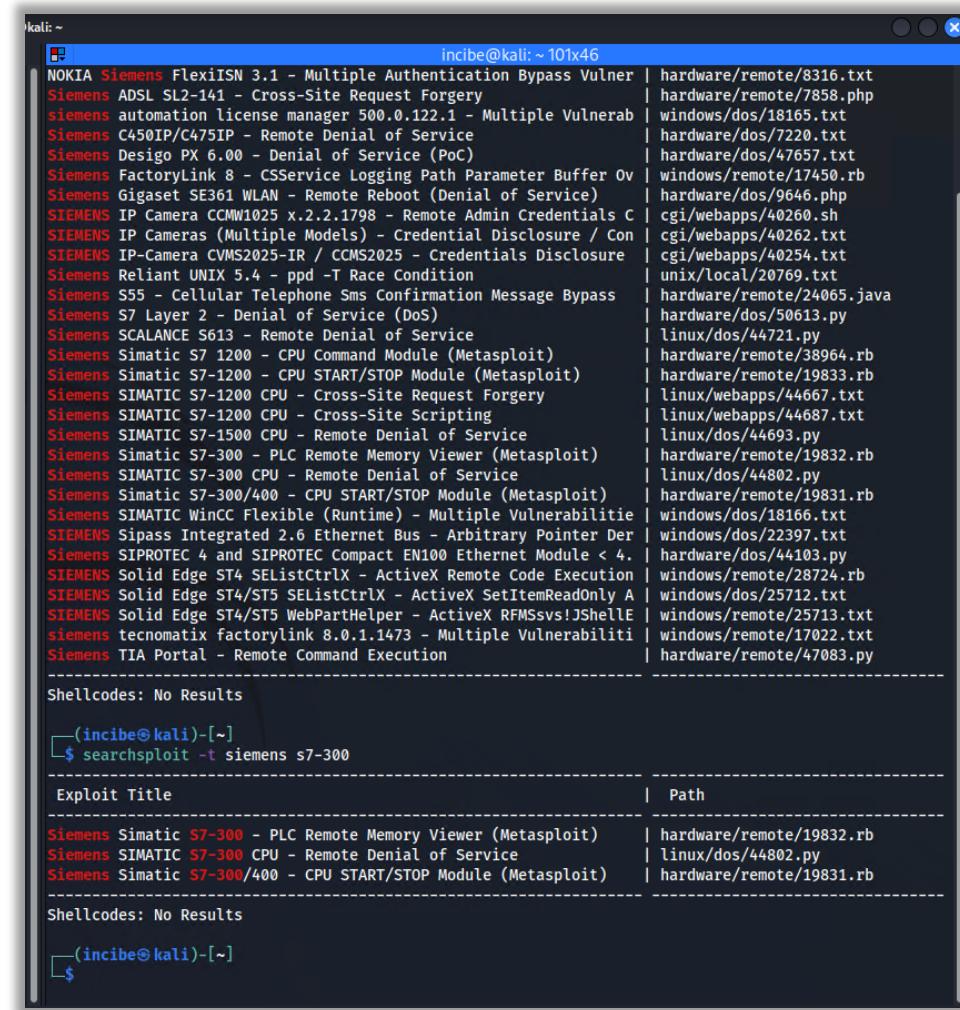
Ilustración 42: Ejecución de la herramienta Searchsploit.

## 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

- Podemos ver que han salido varios resultados, así que vamos a concretar la búsqueda para localizar los *exploit* que contentan la palabra «Siemens» y «s7-300». Ahora vemos que nos han aparecido tres resultados.

- search -t siemens s7-300**



```
incibe@kali: ~ 101x46
[Incibe] incibe@kali: ~ 101x46
NOKIA Siemens FlexiISN 3.1 - Multiple Authentication Bypass Vulner | hardware/remote/8316.txt
Siemens ADSL SL2-141 - Cross-Site Request Forgery | hardware/remote/7858.php
siemens automation license manager 500.0.122.1 - Multiple Vulnerab | windows/dos/18165.txt
Siemens C450IP/C475IP - Remote Denial of Service | hardware/dos/7220.txt
Siemens Desigo PX 6.00 - Denial of Service (PoC) | hardware/dos/47657.txt
Siemens FactoryLink 8 - CSservice Logging Path Parameter Buffer Ov | windows/remote/17450.rb
Siemens Gigaset SE361 WLAN - Remote Reboot (Denial of Service) | hardware/dos/9646.php
SIEMENS IP Camera CCMW1025 x.2.2.1798 - Remote Admin Credentials C | cgi/webapps/40260.sh
SIEMENS IP Cameras (Multiple Models) - Credential Disclosure / Con | cgi/webapps/40262.txt
SIEMENS IP-Camera CVMS2025-IR / CCMS2025 - Credentials Disclosure | cgi/webapps/40254.txt
Siemens Reliant UNIX 5.4 - pdd -T Race Condition | unix/local/20769.txt
Siemens S55 - Cellular Telephone Sms Confirmation Message Bypass | hardware/remote/24065.java
Siemens S7 Layer 2 - Denial of Service (Dos) | hardware/dos/50613.py
Siemens SCALANCE S613 - Remote Denial of Service | linux/dos/44721.py
Siemens Simatic S7 1200 - CPU Command Module (Metasploit) | hardware/remote/38964.rb
Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit) | hardware/remote/19833.rb
Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery | linux/webapps/44667.txt
Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting | linux/webapps/44687.txt
Siemens SIMATIC S7-1500 CPU - Remote Denial of Service | linux/dos/44693.py
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb
Siemens SIMATIC WinCC Flexible (Runtime) - Multiple Vulnerabilitie | windows/dos/18166.txt
SIEMENS Sipass Integrated 2.6 Ethernet Bus - Arbitrary Pointer Der | windows/dos/22397.txt
Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4. | hardware/dos/44103.py
SIEMENS Solid Edge ST4 SEListCtrlX - ActiveX Remote Code Execution | windows/remote/28724.rb
SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX SetItemReadOnly A | windows/dos/25712.txt
SIEMENS Solid Edge ST4/ST5 WebPartHelper - ActiveX RFMSsvs!JShellE | windows/remote/25713.txt
siemens tecnomatix factorylink 8.0.1.1473 - Multiple Vulnerabiliti | windows/remote/17022.txt
Siemens TIA Portal - Remote Command Execution | hardware/remote/47083.py

Shellcodes: No Results

(incibe㉿kali)-[~]
$ searchsploit -t siemens s7-300
Exploit Title | Path
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb

Shellcodes: No Results

(incibe㉿kali)-[~]
$
```

Ilustración 43: Búsqueda de los que contienen las palabras «Siemens» y «s7-300».

## 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

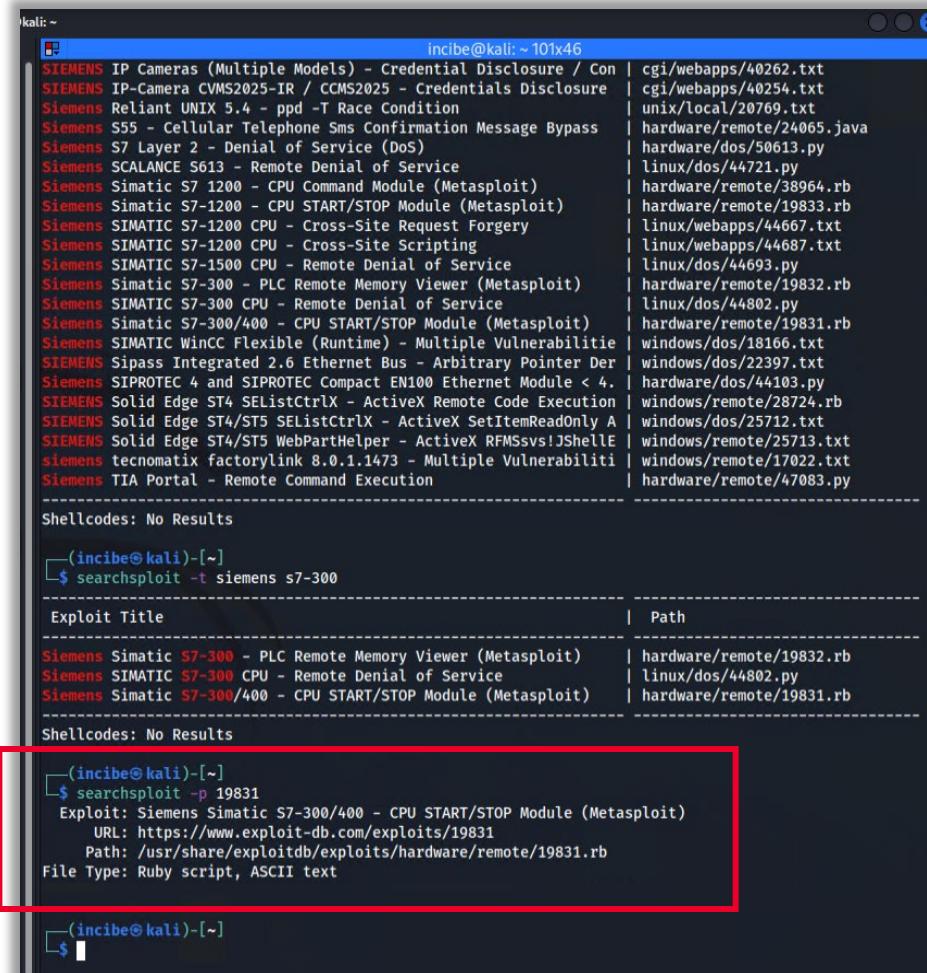
- Una vez realizado este paso, vamos a mostrar más información acerca del *exploit* elegido, que en nuestro caso será «Siemens Simatic s7-300/400 – CPU START/STOP Module (Metasploit)». Para ello, ejecuta el siguiente comando:
  - searchsploit -p 19831**

**Nota:** -p hace referencia al *path*, es decir, la ruta en la que se encuentra el *exploit*.

**Nota:** el número 19831 es el que podemos encontrar en el *path* (ruta) del *exploit* que hemos elegido y consiste en el número identificativo de la EDB (*Exploit Database*) donde se encuentran los *exploits*.

## 4

# BÚSQUEDA DE EXPLOIT CON SEARCHSPLOIT



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `$ searchsploit -t siemens s7-300`. The output lists several exploits for Siemens S7-300 devices, categorized by type (hardware/remote, linux/dos, windows/remote) and path. The results are as follows:

| Exploit Title   | Path                     |
|---|--------------------------|
| Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit)  | hardware/remote/19832.rb |
| Siemens SIMATIC S7-300 CPU - Remote Denial of Service           | linux/dos/44802.py       |
| Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb |

After selecting the exploit for Siemens Simatic S7-300/400, the user runs `$ searchsploit -p 19831`. The terminal displays the exploit details:

```
Exploit: Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)
URL: https://www.exploit-db.com/exploits/19831
Path: /usr/share/exploitdb/exploits/hardware/remote/19831.rb
File Type: Ruby script, ASCII text
```

Ilustración 44: Más información acerca del exploit elegido.



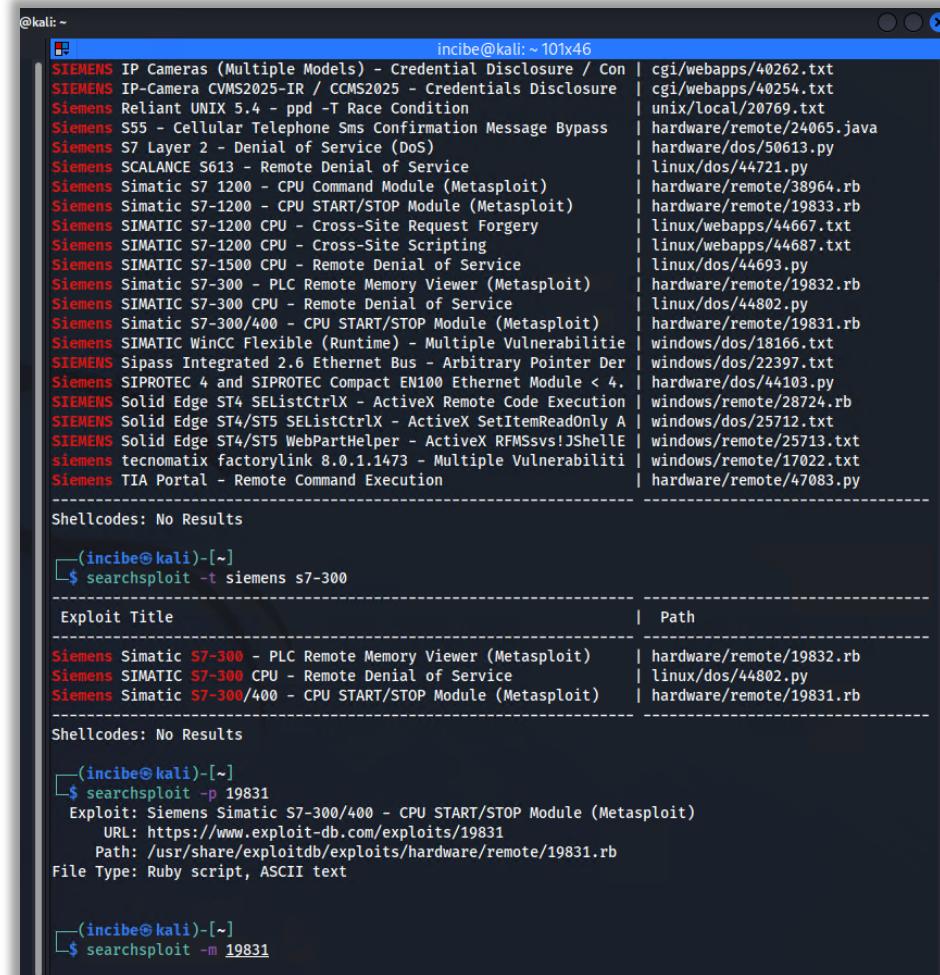
## BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

- Invocamos el comando que nos copia el *exploit* a nuestra carpeta de usuario:
  - **searchsploit -m 19831**

**Nota:** -m hace referencia a *mirror*, es decir, a copiar un *exploit* en el directorio en el que nos encontramos en ese momento.

# 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `searchsploit -t siemens s7-300`. The output lists various Siemens vulnerabilities, including S7-300 CPU Remote Denial of Service and S7-300/400 CPU START/STOP Module (Metasploit). The user then runs `searchsploit -p 19831`, which provides details about the exploit for the S7-300/400 module. Finally, the user runs `searchsploit -m 19831` to copy the exploit file to their user directory.

```
incibe@kali: ~ 101x46
[...]
SIEMENS IP Cameras (Multiple Models) - Credential Disclosure / Con | cgi/webapps/40262.txt
SIEMENS IP-Camera CVMS2025-IR / CCMS2025 - Credentials Disclosure | cgi/webapps/40254.txt
Siemens Reliant UNIX 5.4 - ppd -T Race Condition | unix/local/20769.txt
Siemens S55 - Cellular Telephone Sms Confirmation Message Bypass | hardware/remote/24065.java
Siemens S7 Layer 2 - Denial of Service (Dos) | hardware/dos/50613.py
Siemens SCALANCE S613 - Remote Denial of Service | linux/dos/44721.py
Siemens Simatic S7 1200 - CPU Command Module (Metasploit) | hardware/remote/38964.rb
Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit) | hardware/remote/19833.rb
Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery | linux/webapps/44667.txt
Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting | linux/webapps/44687.txt
Siemens SIMATIC S7-1500 CPU - Remote Denial of Service | linux/dos/44693.py
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb
Siemens SIMATIC WinCC Flexible (Runtime) - Multiple Vulnerabilitie | windows/dos/18166.txt
SIEMENS Sipase Integrated 2.6 Ethernet Bus - Arbitrary Pointer Der | windows/dos/22397.txt
Siemens SIPROTEC 4 and SIPROTEC Compact EN110 Ethernet Module < 4. | hardware/dos/44103.py
SIEMENS Solid Edge ST4 SEListCtrlX - ActiveX Remote Code Execution | windows/remote/28724.rb
SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX SetItemReadOnly A | windows/dos/25712.txt
SIEMENS Solid Edge ST4/ST5 WebPartHelper - ActiveX RFMSSvs!JShellE | windows/remote/25713.txt
siemens tecnomatix factorylink 8.0.1.1473 - Multiple Vulnerabiliti | windows/remote/17022.txt
Siemens TIA Portal - Remote Command Execution | hardware/remote/47083.py
-----
Shellcodes: No Results
[...]
(incibe㉿kali)-[~]
$ searchsploit -t siemens s7-300
-----
Exploit Title | Path
-----
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb
-----
Shellcodes: No Results
[...]
(incibe㉿kali)-[~]
$ searchsploit -p 19831
Exploit: Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)
URL: https://www.exploit-db.com/exploits/19831
Path: /usr/share/exploitdb/exploits/hardware/remote/19831.rb
File Type: Ruby script, ASCII text
[...]
(incibe㉿kali)-[~]
$ searchsploit -m 19831
```

Ilustración 45: Se ejecuta el comando que copia el *exploit* a nuestra carpeta de usuario.

## 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

```
incibe@kali: ~101x46
[incibe@kali]-(~)
$ searchsploit -t siemens s7-300
Exploit Title | Path
Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit) | hardware/remote/19832.rb
Siemens SIMATIC S7-300 CPU - Remote Denial of Service | linux/dos/44802.py
Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit) | hardware/remote/19831.rb
Siemens SIMATIC WinCC Flexible (Runtime) - Multiple Vulnerabilitie | windows/dos/18166.txt
SIEMENS Sipass Integrated 2.6 Ethernet Bus - Arbitrary Pointer Der | windows/dos/22397.txt
Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module < 4. | hardware/dos/44103.py
SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX Remote Code Execution | windows/remote/28724.rb
SIEMENS Solid Edge ST4/ST5 SEListCtrlX - ActiveX SetItemReadOnly A | windows/dos/25712.txt
SIEMENS Solid Edge ST4/ST5 WebPartHelper - ActiveX RFMSsvs!JShellE | windows/remote/25713.txt
siemens tecnomatix factorylink 8.0.1.1473 - Multiple Vulnerabiliti | windows/remote/17022.txt
Siemens TIA Portal - Remote Command Execution | hardware/remote/47083.py
-----
Shellcodes: No Results
[incibe@kali]-(~)
$ searchsploit -p 19831
Exploit: Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)
URL: https://www.exploit-db.com/exploits/19831
Path: /usr/share/exploitdb/exploits/hardware/remote/19831.rb
File Type: Ruby script, ASCII text

[incibe@kali]-(~)
$ searchsploit -m 19831
Exploit: Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)
URL: https://www.exploit-db.com/exploits/19831
Path: /usr/share/exploitdb/exploits/hardware/remote/19831.rb
File Type: Ruby script, ASCII text

Copied to: /home/incibe/19831.rb

[incibe@kali]-(~)
$
```

Ilustración 46: Se ejecuta el comando que copia el *exploit* a nuestra carpeta de usuario.

## 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

- Desde la terminal izquierda, accede a la ruta donde se almacenan los *exploit* de Metasploit Framework, en la carpeta «auxiliary» crea la estructura *hardware/remote* y copia en esta carpeta el «*exploit 19831.rb*» desde nuestra carpeta de usuario. Para ello, ejecuta los siguientes comandos:
  - **cd /usr/share/Metasploit-framework/modules/auxiliary/**
  - **sudo mkdir hardware**
  - **[Introducimos la contraseña.]**
  - **cd hardware**
  - **sudo mkdir remote**
  - **sudo cp ~/19831.rb remote**
  - **cd remote**
  - **ls -l**

## 4

# BÚSQUEDA DE *EXPLOIT* CON SEARCHSPLOIT

- Como vemos en la imagen, nos aparece el *exploit* en la carpeta.

**Nota:** Es mejor no cambiar el nombre al *exploit*, ya que puede dar problemas a la hora de que lo reconozca Metasploit Framework.

**¡Enhorabuena!**

Ya tienes el *exploit* incorporado en la herramienta Searchsploit.



```
incibe@kali:~/usr/share/metasploit-framework/modules/auxiliary/hardware$ cd /usr/share/metasploit-framework/modules/auxiliary/
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary]$ sudo mkdir hardware
[sudo] contraseña para incibe:
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary]$ cd hardware
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary/hardware]$ sudo mkdir remote
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary/hardware]$ sudo cp ~/19831.rb remote
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary/hardware]$ cd remote
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary/hardware/remote]$ ls -l
total 8
-rw-r-xr-x 1 root root 5290 mar 24 01:28 19831.rb
incibe@kali:[/usr/share/metasploit-framework/modules/auxiliary/hardware/remote]$
```

Ilustración 47: Aparece el *exploit* en la carpeta.

# ¡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

