**Ciberseguridad en SCI - Demos**

**6.- Ataques a SCI**

INDICE

**6.- Ataques a SCI.**

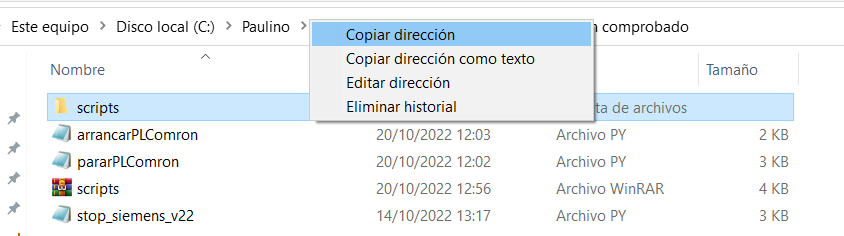
**Demo 13- Ataques a SCI. 6.2 Scripts**

**Demo 13 -Ataques a SCI. 6.2 Scripts** 

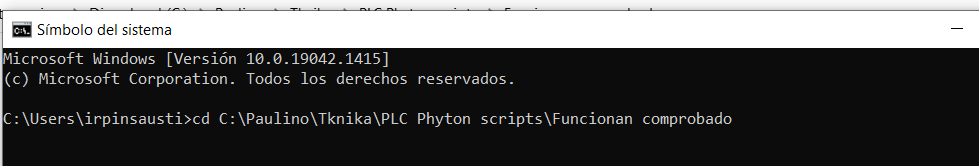
Instalar el complemento para poder ejecutar scripts en python

<https://www.python.org/downloads/>

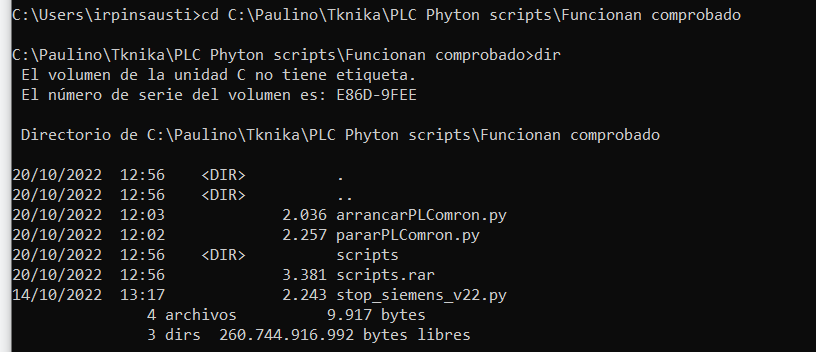
Abrir la consola cmd y ubicarse en la carpeta donde están los scripts. La forma más cómoda es copiar la dirección en el navegador



Pegar la dirección en la consola tras cd ( se usa para entrar en carpetas)



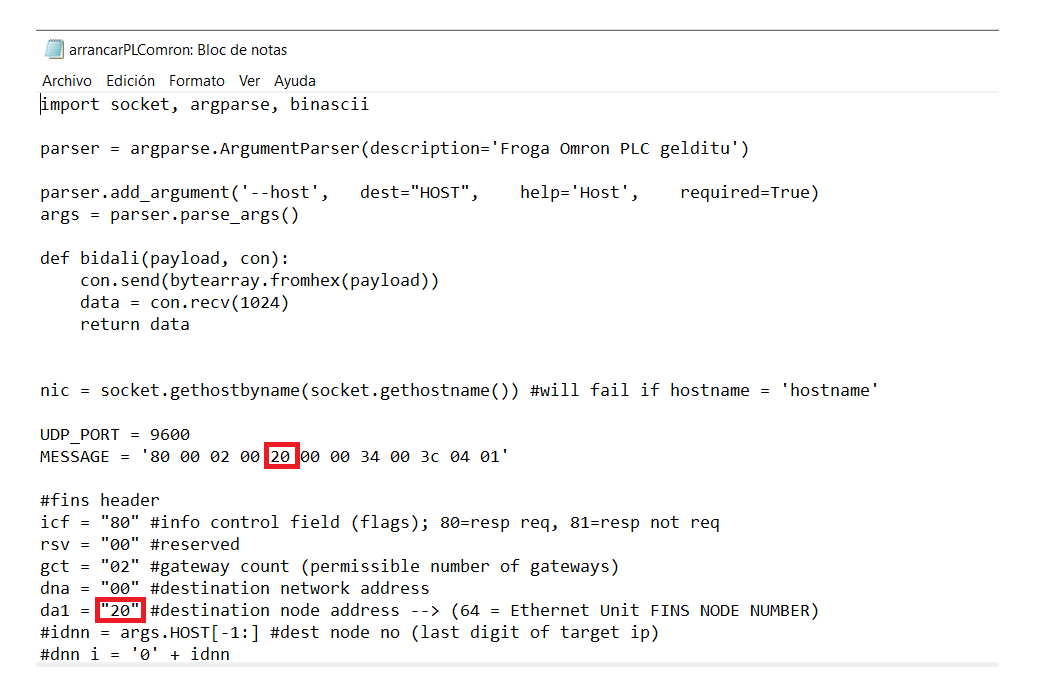
Comprobar que los scripts están accesibles **dir**

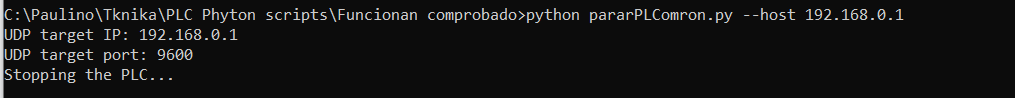
****

Ejecutar el scripts siguiendo el ejemplo:

**python nombrescript.py - - host 192.168.0.1** (Poner IP del PLC)

**Atención!!! Los scripts de Omron hay que editarlos con el bloc de notas y poner el número de nodo del PLC (mirar en el PLC Omron en el display o en la posición de los switches)**

Al ejecutarlo no tiene que dar errores.



Nota: Los scripts están comprobados con PLC Omron CJ2M CPU31 y CP1L Siemens S7 1200 Firmware V2.2

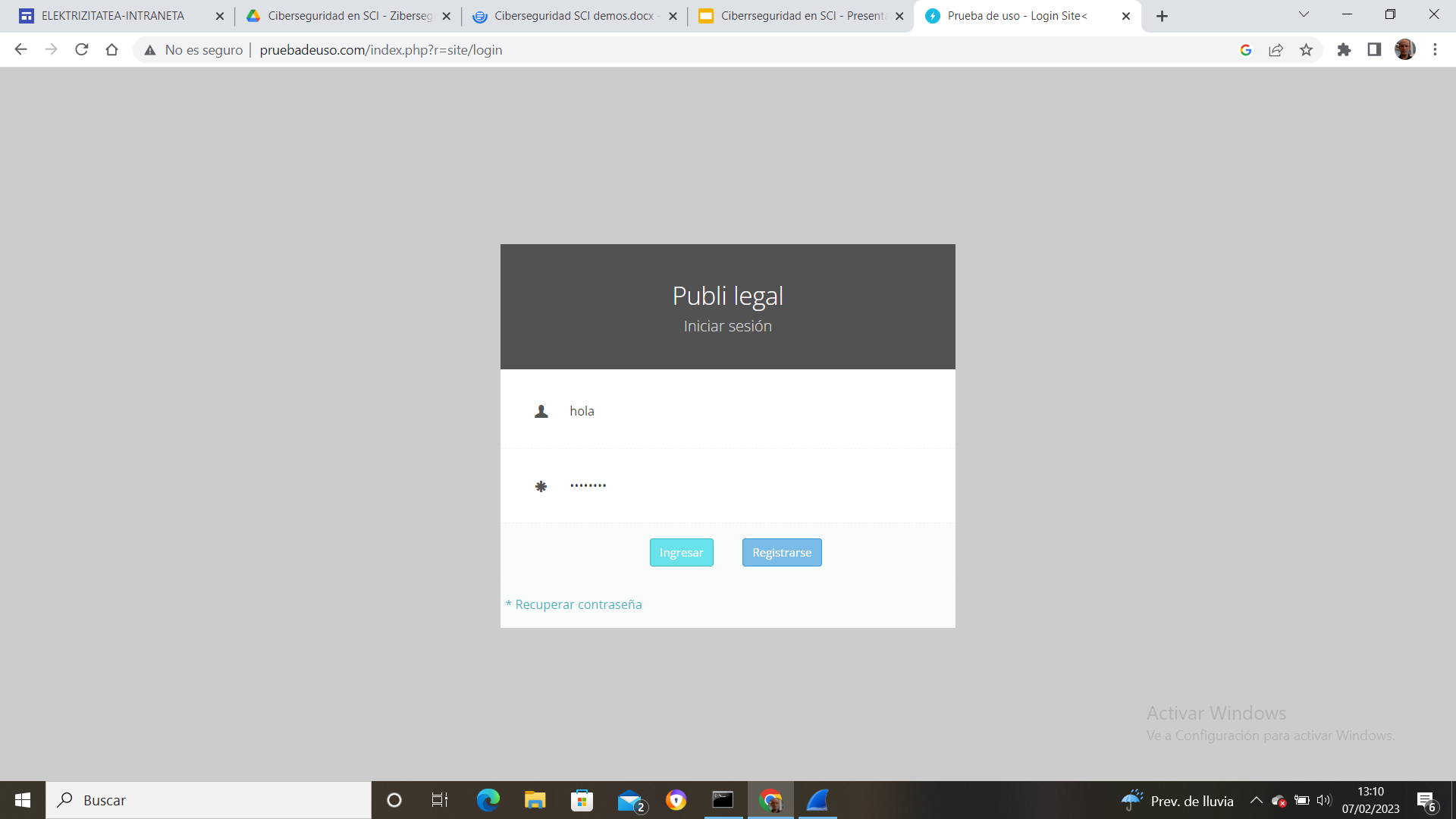
**Demo 14 -Ataques a SCI.**

**6.3 Captura credenciales hmi (http)**

Ponemos en captura Wireshark (Tener en cuenta si salimos por wifi o por cable para seleccionar de donde capturar) .

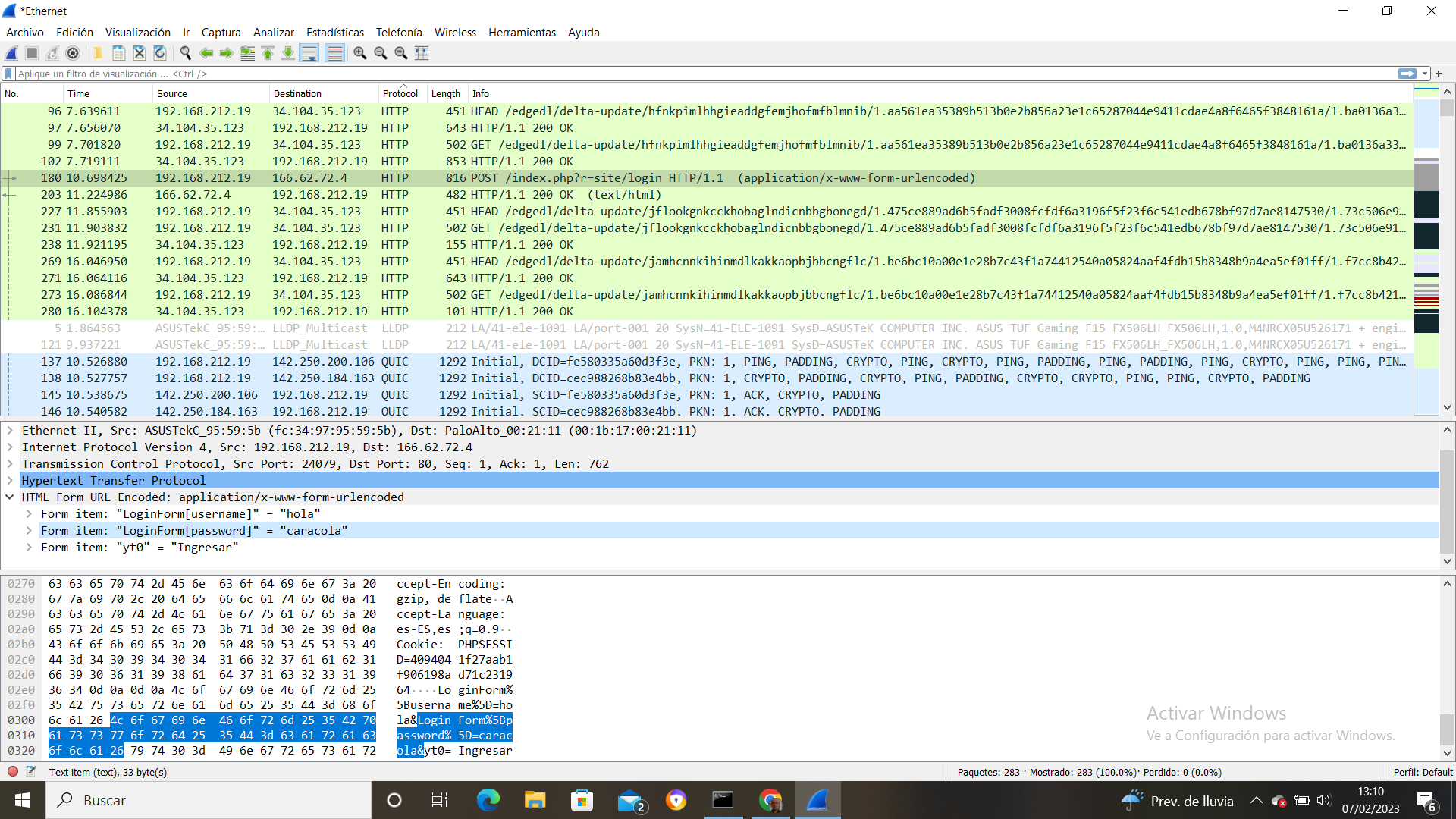
Nos conectamos a una página http e intentamos logearnos. Utilizamos un usuario y password ficticios pues luego se verán en wireshark.Evidentemente no accederemos .

<http://pruebadeuso.com/index.php?r=site/login>

****

Paramos wireshark y localizamos en el protocolo **HTTP** en el campo Info una línea **POST. (** CRTL +F para abrir buscador)

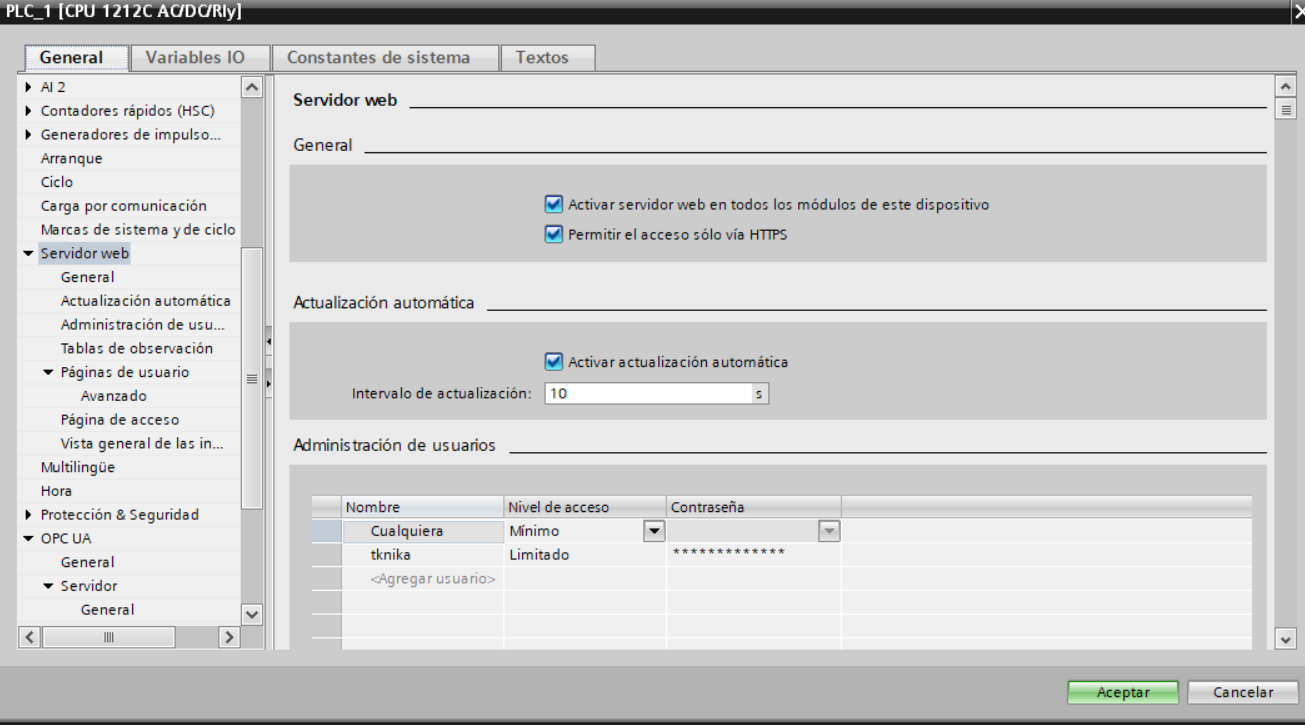


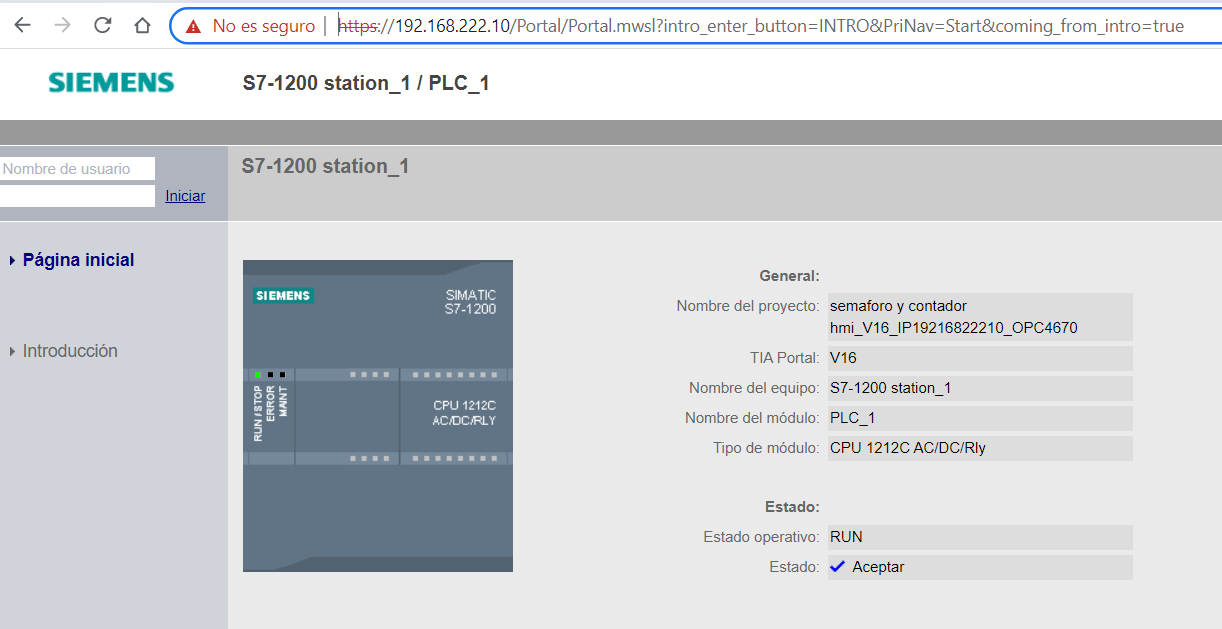


Siemens webserver pasahitza lortu (https) . Webserverra klonatu eta pishing bidez kredentzialak lapurtu Wireshark erabiliaz

**6.4 Captura credenciales hmi (https)**

Webserver aktibatu PLC propietateetan https moduan eta PLC ari kargatu



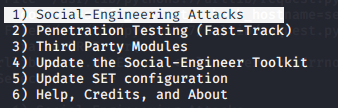


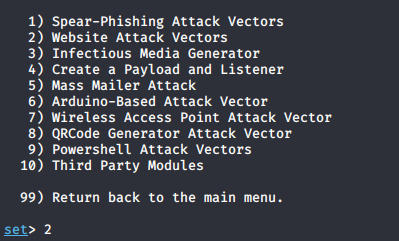
Kali makina (Erasotzailea) eta Siemenseko PLCa (192.168.222.10) sare berean egon behar dira. .

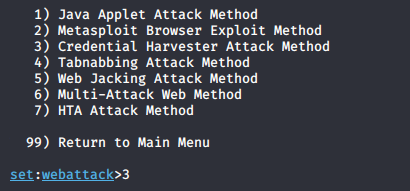
Erasoaren prozesua hau da:

* Kali makinan
  + Siemens PLCaren kudeaketa-webgunearen login-orria klonatu. Web orri bat klonatzeko Kaliko tresnak erabili.





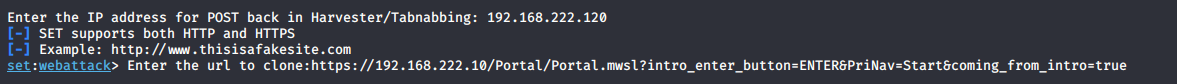




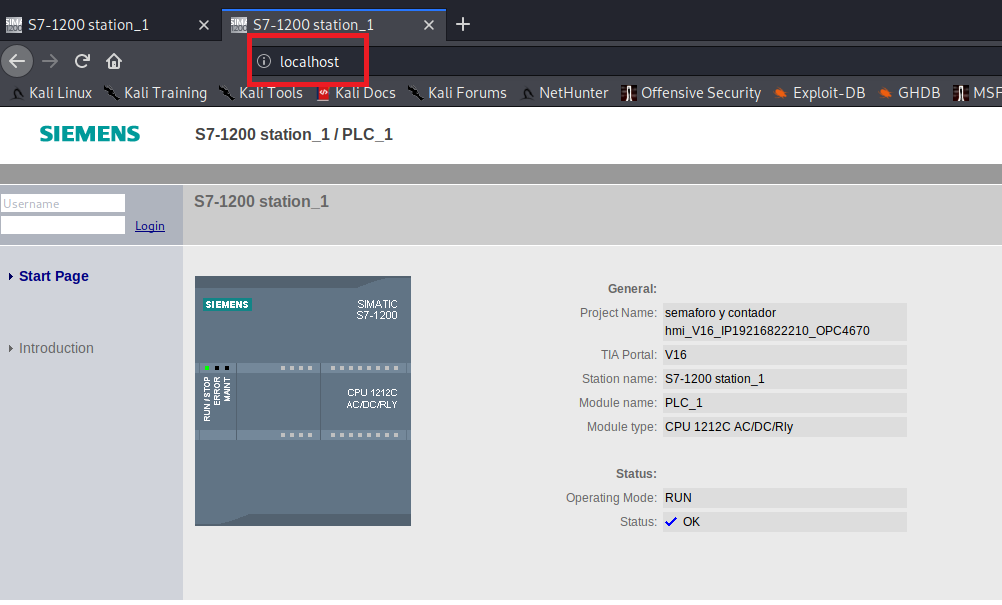


Kali makinaren IP jarri (bertan klonatuko du web zerbitzaria)

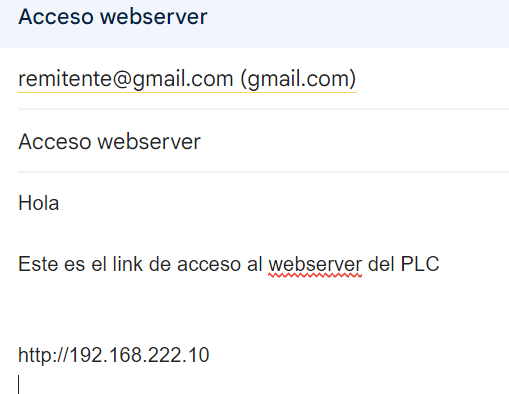
PLC aren webserver helbidea jarri.(Klonatu nahi dena)

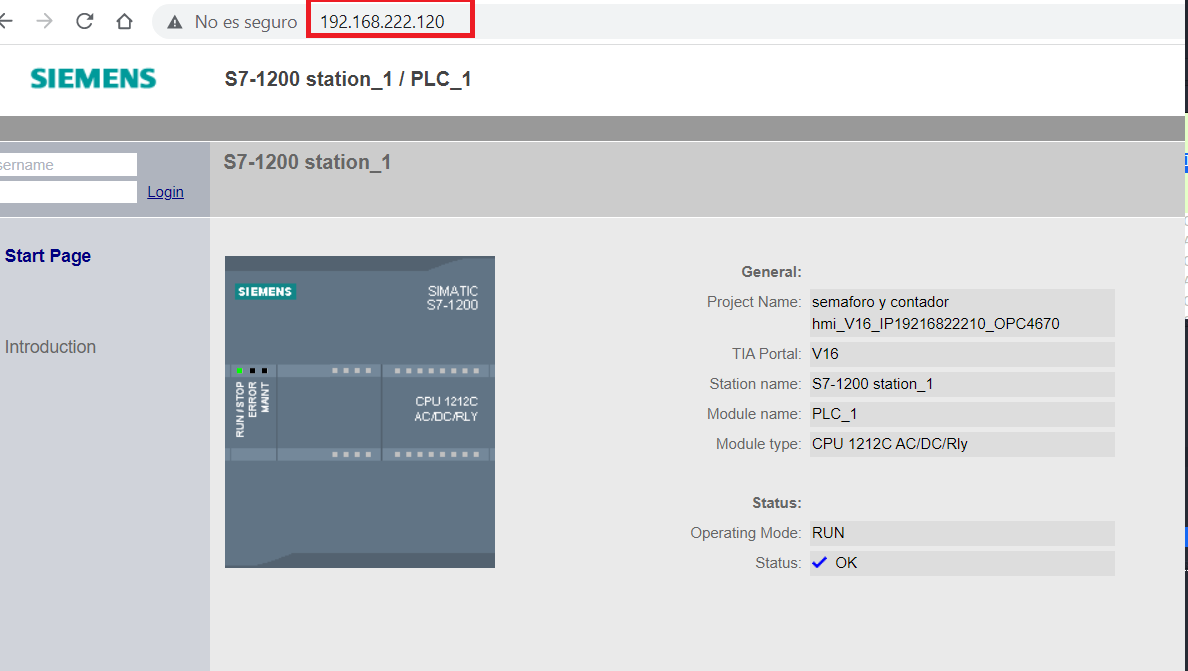


Konprobatu kali makinan **localhost** moduan webserver aren kopia sortua dagoela.



* + Emailez esteka-gisa bidali Kali makinaren IPa Siemenseko PLCarena balitz bezala.

****

* + Wireshark entzuten jarri.
* Biktimak emaila jaso eta esteka sakatzen du. Ondoren, logeatu egiten da.
* 
* Kali makinako Wiresharken kredentzialak agertzen dira.horiek erabilita, web orrian logeatuko gara.
* 