**Ciberseguridad en SCI - Demos**

**4.- Descubrir dispositivos industriales en la red interna**

INDICE

**4.- Descubrir dispositivos industriales en la red interna.**

***Demo 7 - Wireshark***

***Demo 8 - NMAP***

***Demo 9 - SINEC PNI , PRONETA***

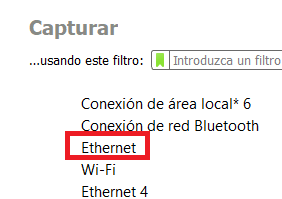
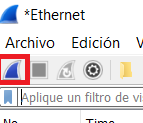
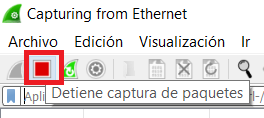
**Demo 7 - Wireshark **

**Wireshark** es un analizador de paquetes de red open-source que actualmente está disponible para plataformas Windows y Linux. Es una utilidad que captura todo tipo de información (Sniffer) que pasa a través de una conexión .Su principal objetivo es el análisis de tráfico, pero además es una excelente aplicación didáctica para el estudio de las comunicaciones , diagnosticar problemas de red, efectuar auditorías de seguridad y aprender más sobre redes informáticas.

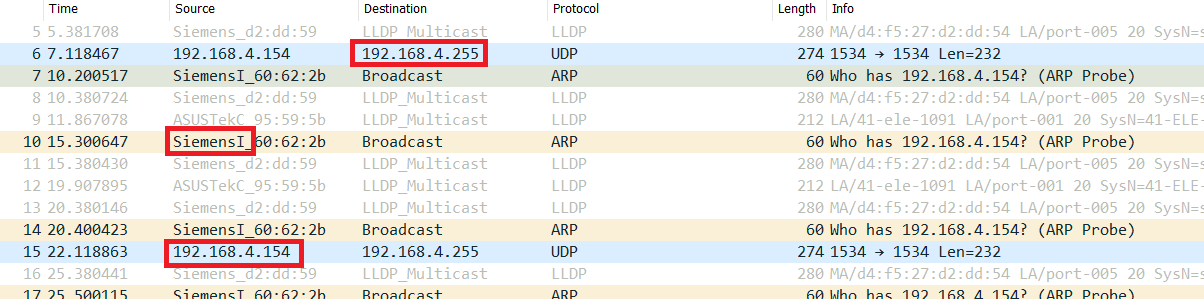
En esta demo se abordará una introducción y primer contacto con la herramienta. Volverá a ser utilizada en demos posteriores.

Abrimos la aplicación , seleccionamos el dispositivo desde el que queremos capturar los paquetes, en este caso la tarjeta de red e iniciamos la captura. Botón rojo detenemos la captura.

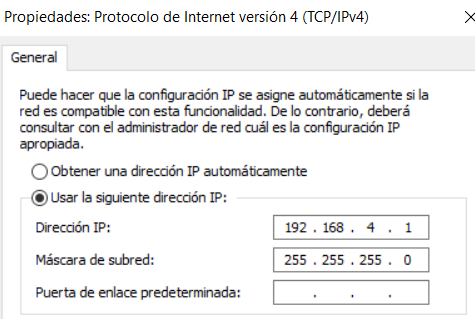
**Importante**, sólo captura el tráfico que ve nuestra tarjeta de red ( en este ejemplo). Para poder ver tráfico de una red completa hay que conectar el PC con el programa a un switch que sea capaz de visualizar el tráfico de dicha red. Más adelante aparecerá el concepto de “port mirroring” en el que un puerto del switch es capaz de ver todo el tráfico que circula por el mismo.

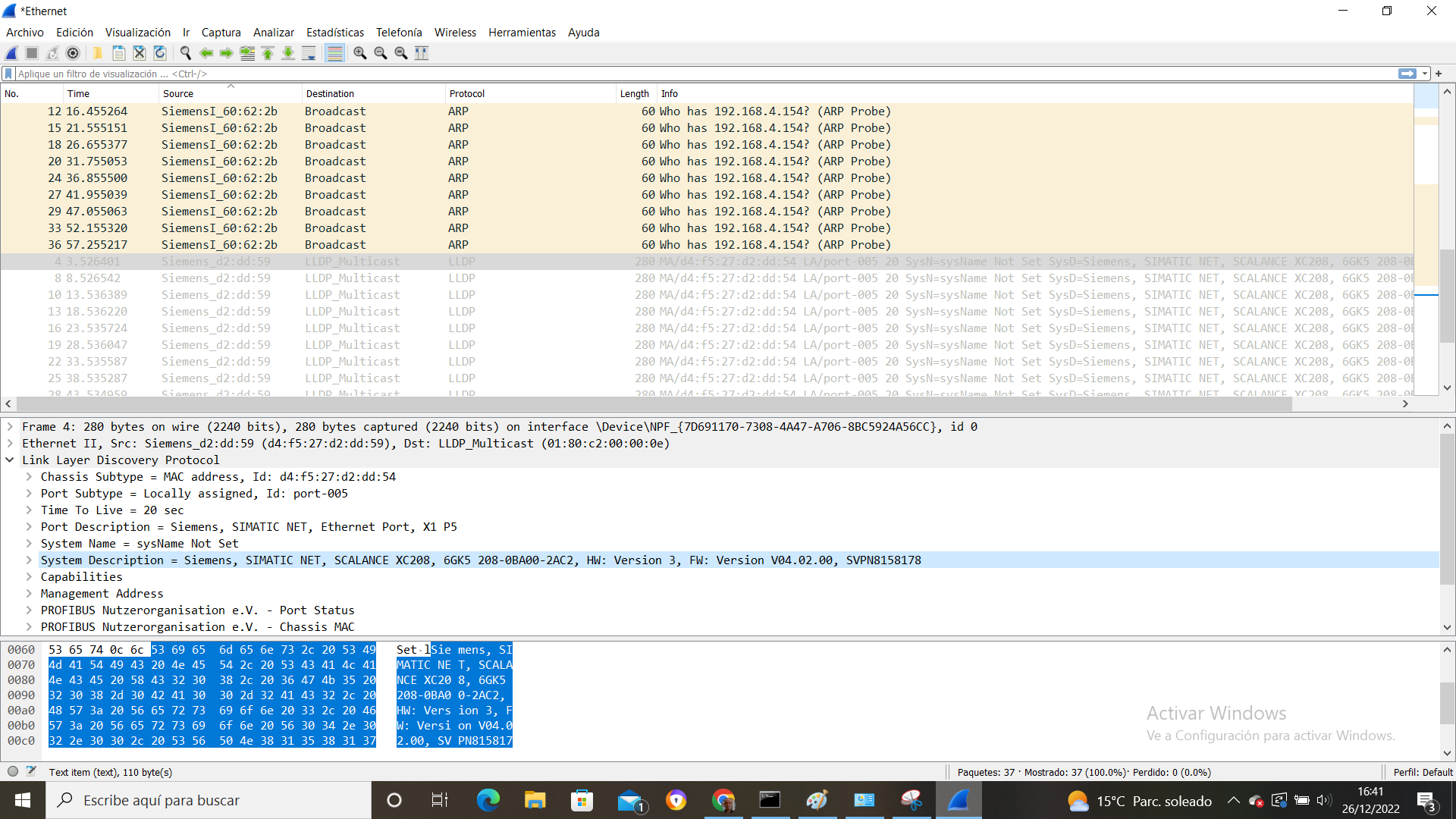
  

Aunque una interpretación técnica y detallada puede ser complicada, a simple vista ya se puede obtener información sobre algunos dispositivos que se han detectado en la red, IP de varías máquinas y marca de un PLC.



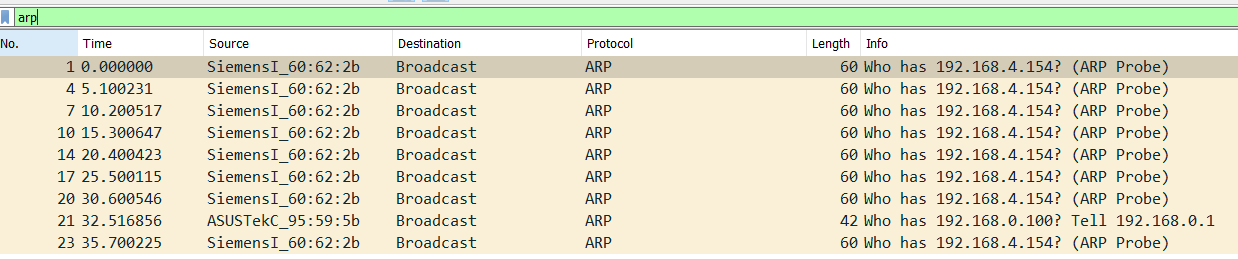
En una estrategia inicial puede servir para detectar el rango de red. En el ejemplo podemos deducir que la red es 192.168.4.0/24 aunque nuestra tarjeta de red esté en un rango diferente. Si le asignamos una IP del mismo rango y lanzamos otro escaneo podremos detectar más información.



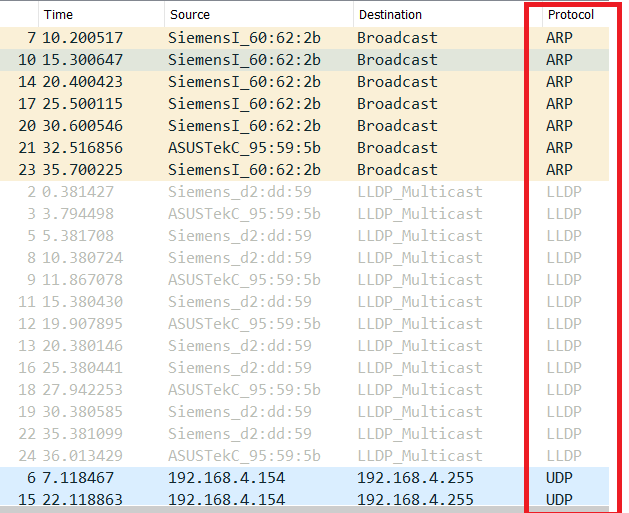


Se ha detectado , entre otros, un dispositivo de la red,System Description: Siemens, SIMATIC NET, SCALANCE XC208, 6GK5 208-0BA00-2AC2, HW: Version 3, FW: Version V04.02.00, SVPN8158178

Se pueden utilizar filtros de captura y de visualización . Un filtro práctico es el **ARP** (Address Resolution Protocol - Protocolo de resolución de direcciones). ARP convierte dinámicamente las direcciones de Internet en las direcciones de hardware exclusivas de las redes de área local.



Podemos ordenar por protocolo



Podemos ordenar por distintos valores



Al circular tantos paquetes por la red , de cara a localizar e interpretar la información, es importantísimo el utilizar filtros para “Cribar” la información. Hay cantidad de filtros. Muestra de filtros: [Filtros](https://vidatecno.net/como-usar-los-filtros-de-pantalla-en-wireshark/)

**Los filtros de captura** son los que se establecen para mostrar solo los paquetes que cumplan los requisitos indicados en el filtro. Si no establecemos ninguno, Wireshark capturará todo el tráfico y lo presentará en la pantalla principal.

### Filtros de Visualización (Display Filter).Los filtros de visualización establecen un criterio de filtro sobre los paquetes que estamos capturando y que estamos visualizando en la pantalla principal de Wireshark. Al aplicar el filtro en la pantalla principal de Wireshark aparecerá solo el tráfico filtrado a través del filtro de visualización.



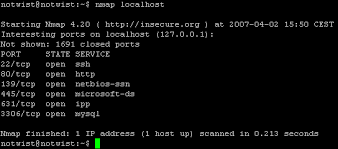
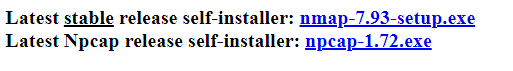
Curso completo de Wireshark: (Nota: es un curso externo compartido por un particular. No se asegura la continuidad y disponibilidad del mismo)

[Experto en wireshark - Google Drive](https://drive.google.com/drive/folders/17VyHp4--tk9Ln02ocHukntGkp3Wlatli)

**Demo 8 - NMAP **

**Nmap** *Network Mapper (mapeador de redes)* es un programa de código abierto, que sirve para realizar escaneos de redes, puertos y dispositivos. Es decir, con esta herramienta es posible determinar qué dispositivos se hallan conectados a una red, qué puertos tiene activos y qué servicios se hallan en ellos.Viene integrado por defecto en Kali Linux y puede instalarse en windows.

<https://nmap.org/download.html#windows>



### Antes de empezar…

No te pongas a lanzar escaneos con esta herramienta -ni con ninguna otra similar- sin pensar y a cualquier sitio.Si quieres practicar comandos de Nmap puedes usar tu propio equipo «localhost» como valor para los comandos más básicos. Además, los desarrolladores ponen a nuestra disposición varios servidores que permiten ser escaneados

* scanme.nmap.org
* analizame2.nmap.org

.**ATENCIÓN!! Realizar nmap contra servidores externos es intrusivo.**

Hay una gran variedad de comandos para ejecutar. Algunos son más intrusivos que otros para el dispositivo industrial. En la propia página hay una guía y se pueden encontrar infinidad de manuales, cursos y videos en internet.

<https://protegermipc.net/2018/11/07/tutorial-y-listado-de-comandos-mas-utiles-para-nmap/>

<https://www.csirtcv.gva.es/wp-content/uploads/2020/05/NMAP-6_-Listado-de-comandos.pdf>

10 Comandos Básicos de NMAP

<https://www.youtube.com/watch?v=GDZOsgYiQ44>

Tutorial de NMAP . Aprende a descubrir EQUIPOS VULNERABLES en la red . Análisis Nmap y Wireshark

<https://www.youtube.com/watch?v=apvgul-8UsM>

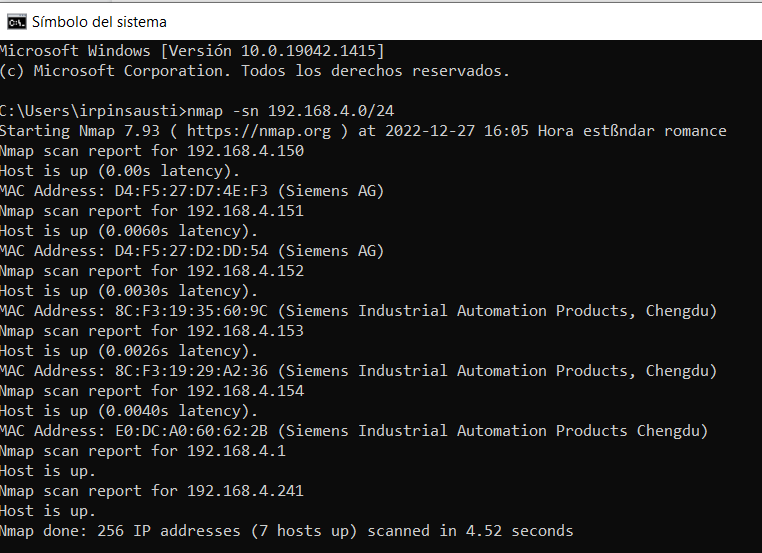
En Kali Linux acceder a la consola y en Windows abrir una ventana de consola **cmd.**

* **Escaneo de una red completa**
* **Escaneo de puertos**
* **Escaneo de servicios y versiones**
* **Escaneo de S.O**
* **Usar scripts con Nmap**
* **Guardar resultado de escaneo en un fichero**

* **Escaneo de una red completa**

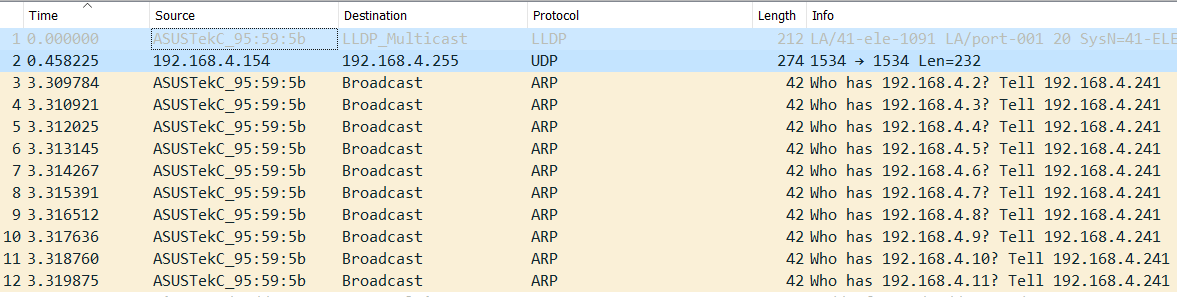
**nmap -sn(Sin escaneo de puertos)**

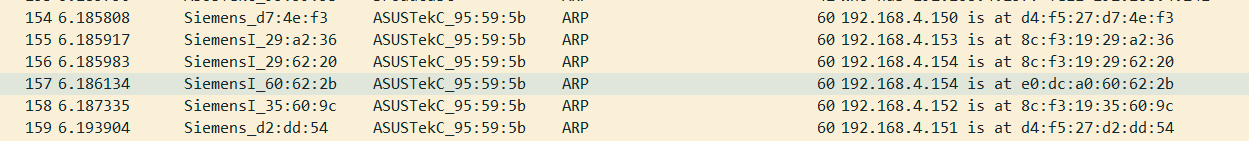
Esta opción le dice a Nmap que no realice una exploración de puertos después del descubrimiento del host y que solo imprima los hosts disponibles que respondieron a las sondas de descubrimiento del host. Esto a menudo se conoce como " **escaneo de ping** " . Permite el reconocimiento ligero de una red objetivo sin llamar mucho la atención. Saber cuántos hosts están activos es más valioso para los atacantes que la lista proporcionada por el escaneo de listas de cada IP y nombre de host. Anteriormente mediante Wireshark hemos detectado que la red de PLCs está en un rango 192.168.4.X **nmap -sn 192.168.4.0/24**



Al ser un escaneo ligero se realiza de manera rápida y es práctico para detectar los dispositivos de manera no intrusiva. Nos aporta cierta información del fabricante (Siemens) a la vez que la IP de los dispositivos.

Si ponemos wireshark a capturar el tráfico vemos la instrucción nmap -sn lanza sucesivos ping a todo el rango de IP de la red y reconoce los dispositivos que le han contestado .



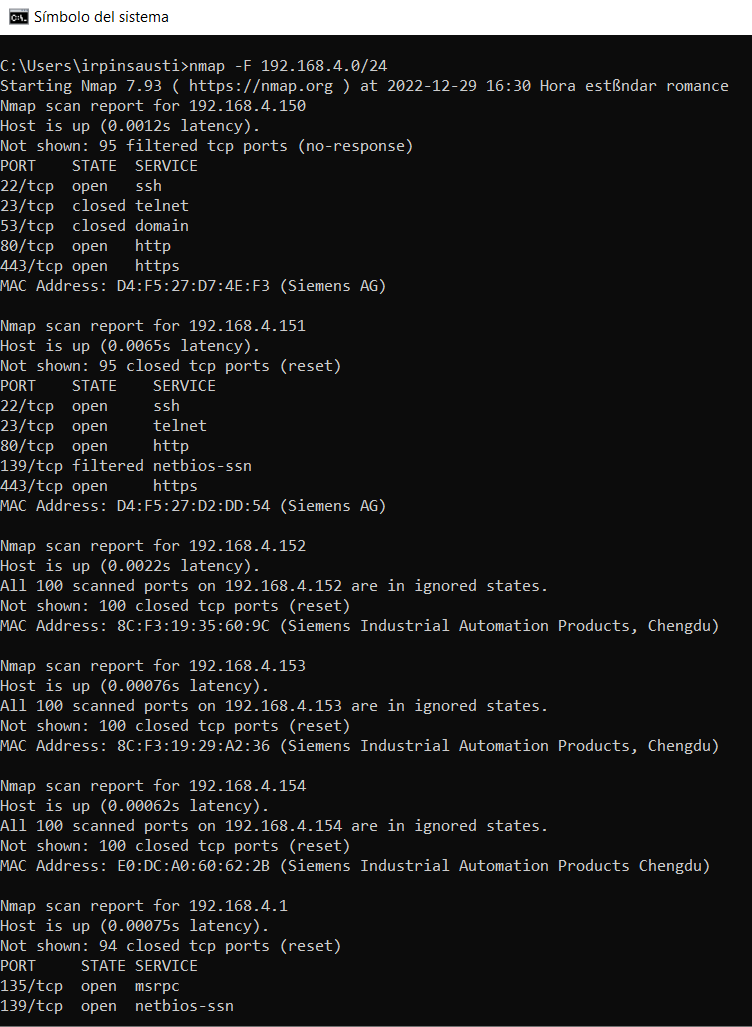


### Escaneo de toda la red con Nmap (simple) nmap -sP

Si necesitamos descubrir equipos vivos (es decir, que nos digan «oye, aquí estoy») en toda la red pero no queremos saber mucho sobre ellos, podemos lanzar un escaneo simple muy similar al anterior.

Escaneo de red + puertos (rápido) **nmap -F IP/24**

Con el siguiente comando podremos analizar toda una red o rango en busca de hosts. Se nos mostrarán los datos del ejemplo anterior y además el estado de algunos de sus puertos (los más comunes).



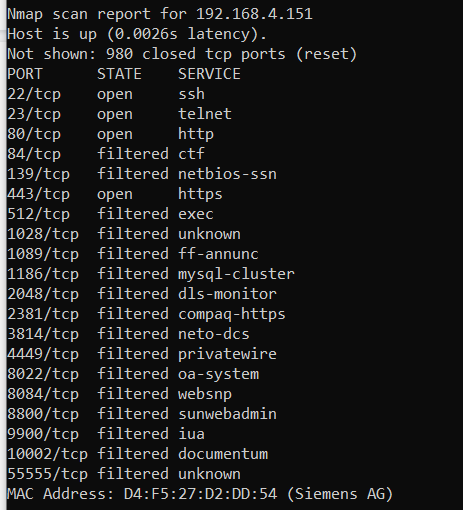
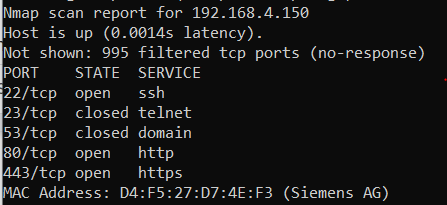




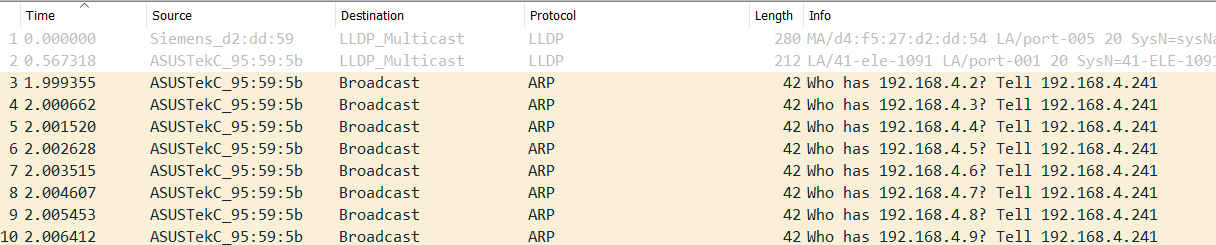


Los puertos consultados (SYN) que dan respuesta (RST) se consideran abiertos.

**nmap -Pn**(Sin ping) Esta opción omite por completo la etapa de descubrimiento del host. Normalmente, Nmap usa esta etapa para determinar las máquinas activas para un escaneo más pesado y medir la velocidad de la red. De forma predeterminada, Nmap solo realiza **sondeos intensivos,** como escaneos de puertos, detección de versiones o detección de sistemas operativos contra hosts que se encuentran activos. **nmap -Pn 192.168.4.0/24**

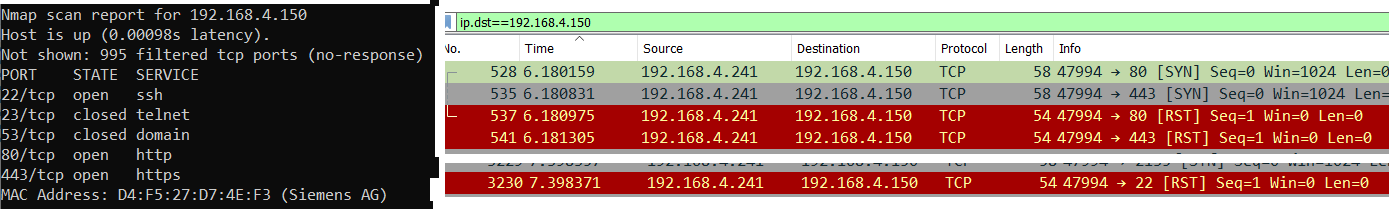
****

Si ponemos en captura wireshark comprobamos que inicialmente hace un barrido con todas las IP de la subred .



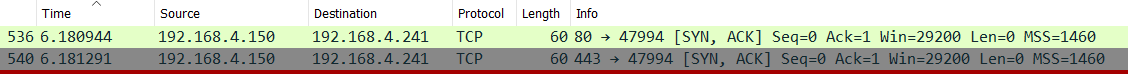
A los dispositivos que le responden, les consulta los puertos que tiene abiertos.

Filtramos por IP de destino y comprobamos que los puertos que aparecen abiertos en la consola son los que han establecido conexión y han respondido afirmativamente al requerimiento.



Observamos también como verifica que el puerto está abierto.





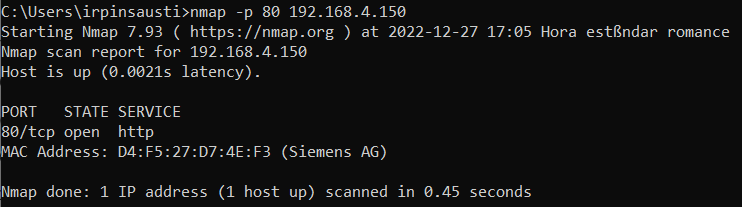


El indicador SYN sugiere al sistema remoto que está intentando establecer una conexión. Si el puerto está abierto, el objetivo dará el segundo paso de un protocolo de enlace de tres vías TCP respondiendo con un paquete SYN/ACK TCP. La máquina que ejecuta Nmap luego interrumpe la conexión naciente respondiendo con un RST en lugar de enviar un paquete ACK que completaría el protocolo de enlace de tres vías y establecería una conexión completa. El paquete RST es enviado por el núcleo de la máquina que ejecuta Nmap en respuesta al SYN/ACK inesperado, no por Nmap en sí.

* **Escaneo de puertos**

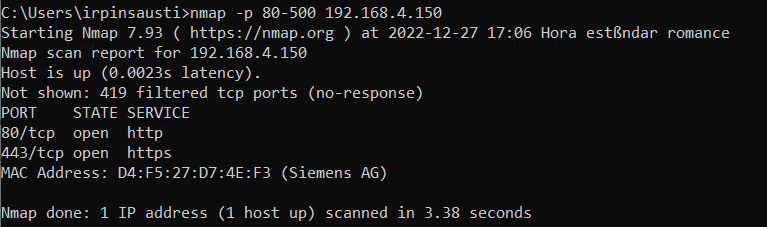
Una vez detectados los dispositivos se pueden hacer consultas a equipos específicos y a sus puertos .

**nmap -p 80 192.168.4.150**

****

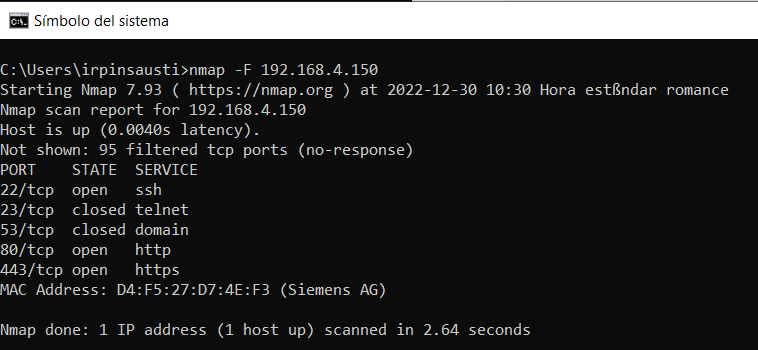
O un rango de puertos de un dispositivo.

**nmap -p 80-500 192.168.4.150**

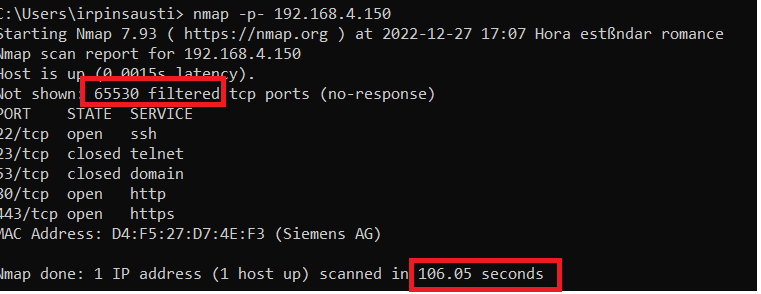


Escaneo los 100 puertos más comunes

**nmap -F 192.168.4.150**

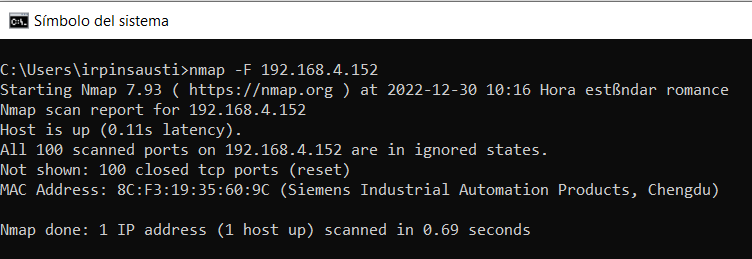
****

Se pueden escanear todos los puestos lo cual requerirá mucho tiempo y es muy intrusivo para el dispositivo. **nmap -p-** En este caso consulta los puertos más comunes.



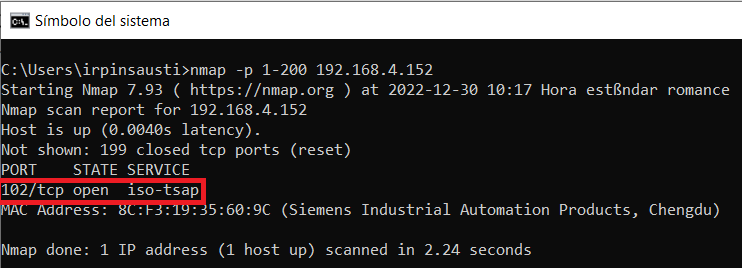
Realizamos el escaneo de puertos a un PLC Siemens , habitualmente puerto 102 y vemos que con un escaneo normal no aparece como activo.Tenemos que especificar el rango de puertos .

**nmap -F 192.168.4.150**

****

Si hacemos un escaneo específico de los puertos 1-200 si que aparece.

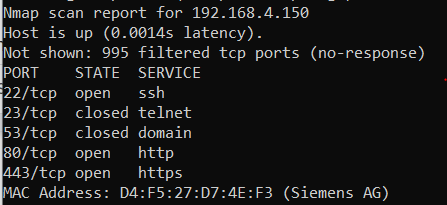
**nmap -p 1-200 192.168.4.152**



Algo similar ocurre con los PLC Omron y el puerto 9600.

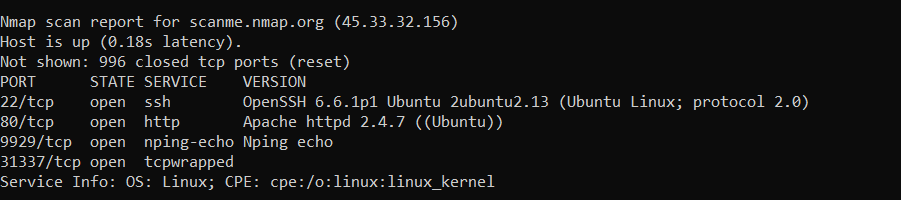
* **Escaneo de servicios y versiones.**

Al realizar un escaneo de puertos nos muestra también los servicios que tienen asociados dichos puertos. Esta asociación del número de puerto y servicio es la estándar, es decir , está normalizado. Puede ocurrir que un servicio se abra en un puerto no estándar.

****

Hay un comando específico para ver los servicios “reales” que están corriendo tras ese puerto y las versiones de los mismos.

**nmap -sV scanme.nmap.org**

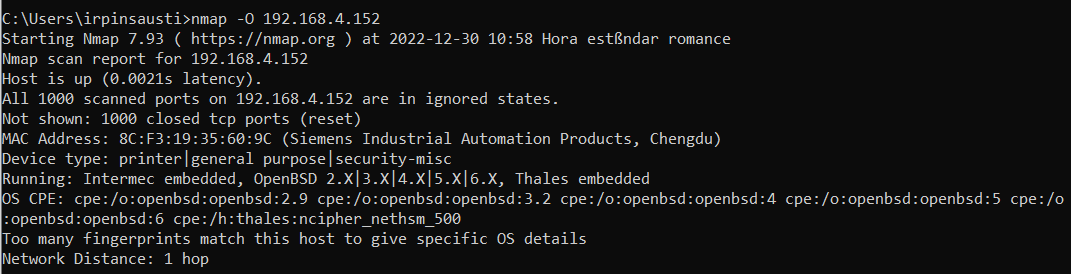
****

* **Escaneo de sistema operativo.**

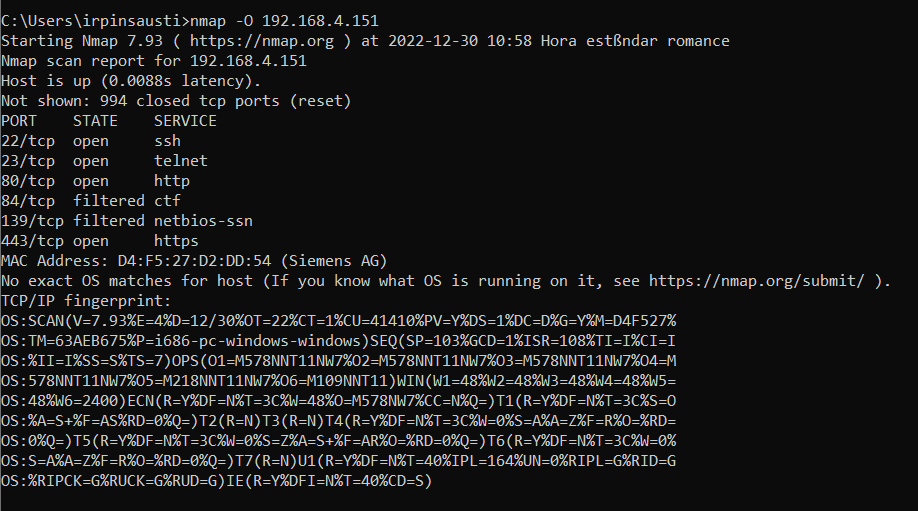
Escanear y obtener información sobre el sistema operativo del dispositivo.

Dependiendo del dispositivo mostrará diferente información.

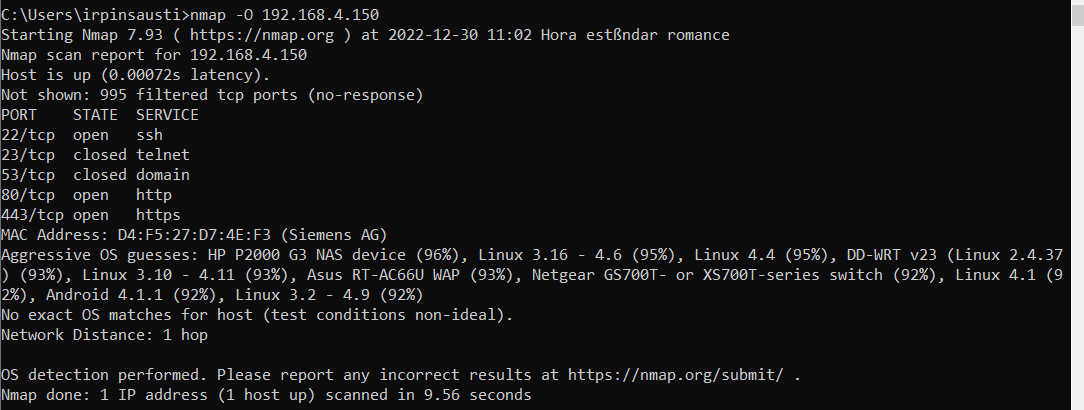
Ejemplo 1 PLC Siemens 1200 **nmap -O 192.168.4.152**

****

Ejemplo 2 PLC Switch Siemens Scalence XC208 **nmap -O 192.168.4.151**

****

Ejemplo 3 PLC Switch Router Scalence S615 **nmap -O 192.168.4.150**

****

* **Usar scripts con Nmap**

¿Qué es un script en Nmap?

Nmap incorpora un potente sistema de scripts conocido como NSE (Nmap Scripting Engine) que permite a los usuarios extender las capacidades de Nmap usando los diversos scripts que incorpora (actualmente hay más de 500 disponibles) que permiten desde la detección avanzada de versiones a la explotación de vulnerabilidades, o creando nuevos scripts que podemos compartir con el resto de usuarios (para los script se utiliza el [lenguaje de programación LUA](https://www.lua.org/)).

Manuales con información:

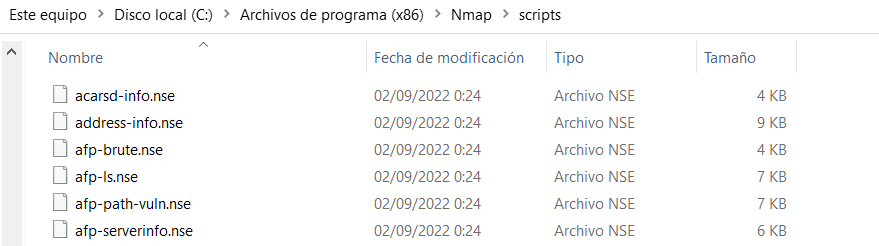
<https://clibre.io/blog/por-secciones/hardening/item/452-scripts-en-nmap>

<https://behacker.pro/como-utilizar-nmap-scripting-engine-nse/>

Ubicación de los scripts en windows y linux.

C:\Program Files (x86)\Nmap

/usr/share/nmap/scripts



Para actualizar el listado de scripts:

> sudo nmap -–scripts-updatedb

Los scripts se dividen en las siguientes categorías:

**auth**: scripts relacionados con la autenticación de usuarios.

**broadcast**: en esta categoría se engloban scripts que utilizan peticiones de transmisión para recopilar información de los host que no se listan por broadcasting.

**brute**: esta categoría es para scripts que utilizan el sistema de fuerza bruta para averiguar las credenciales de usuario en un determinado servicio.

**default**: estos son los scripts que se ejecutan cuando se ejecuta la opción -sC.

**discovery**: scripts relacionados con el descubrimiento de servicios y hosts.

**dos**: esta categoría es para scripts relacionados con ataques de denegación de servicio.

**exploit**: esta categoría es para scripts que explotan vulnerabilidades de seguridad.

**external**: esta categoría es para scripts que utilizan datos o servicios de terceros.

**fuzzer**: esta categoría es para scripts NSE que se centran en fuzzing (envían campos inesperados o aleatorios en cada paquete).

**intrusive**: esta categoría es para scripts que pueden bloquear algo o generar mucho ruido en la red.

**malware**: scripts relacionados con la detección de malware.

**safe**: esta categoría es para scripts que se consideran seguros en todas las situaciones.

**version**: esta categoría contiene scripts que extienden la funcionalidad de la detección de versiones.

**vuln**: esta categoría es para scripts relacionados con vulnerabilidades de seguridad

* Se pueden lanzar todos los scripts de una categoría sobre el objetivo:

nmap -sV --script <categoria> <objetivo>

**nmap -sV --script version scanme.nmap.org**

Ejecutamos los script de la categoría versión contra el objetivo scanme.nmap.org:

**nmap -sV --script="version,discovery" scanme.nmap.org**

Además de los script de la categoría versión también se usarán los de la categoría discovery.

* Se puede lanzar un script específico sobre el objetivo:

nmap --script <nombre de fichero> <objetivo>

**nmap --script http-title scanme.nmap.org**

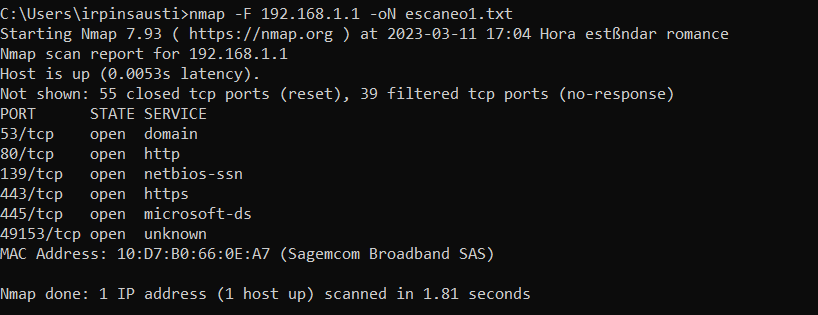
Se ejecuta el script http-title contra el objetivo scanme.nmap.org (es posible indicar varios scripts separándolos por comas).

* **Guardar resultado de escaneo en un fichero**

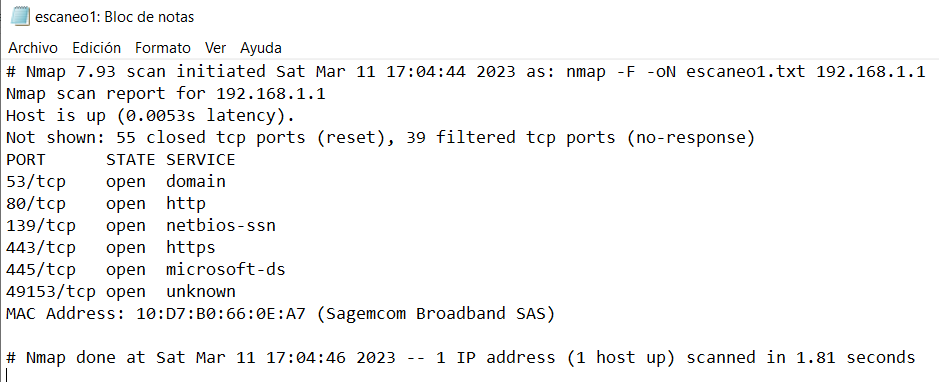
Se pueden guardar los resultados de los escaneos en un fichero (de texto por ejemplo) para su posterior análisis e incorporación a un informe final.

Existen tres formatos principales conteniendo los resultados obtenidos al utilizar nmap, desde un archivo de texto simple, hasta un formato XML, el cual potencialmente puede ser utilizado con otro programa. Los tres formatos son los siguientes, resultado normal utilizando la opción (-oN), resultado XML utilizando la opción (-oX), y formato “grep” utilizando la opción (-oG). Adicionalmente es factible utilizar la opción (-oA) para generar resultados en los tres formatos antes descritos.

**nmap scanme.nmap.org** **-nO resultado.txt**

****

El fichero resultante se ubica en la misma carpeta desde la que hemos lanzado el comando.

****

**Demo 9 -SINEC PNI-PRONETA **

**SINEC PNI Primary Network Initialization**

SINEC PNI es un programa para la inicialización de los componentes de red de Siemens, así como para la inicialización de los controladores Siemens. Además se pueden establecer parámetros específicos de red que son necesarios para la puesta en marcha de los dispositivos SCALANCE y RUGGEDCOM.

Funciones:

* Escaneo de red de todos los dispositivos PROFINET y RUGGEDCOM
* Inicialización mediante el ajuste de los siguientes parámetros en los dispositivos:
  + - Dirección IP, subred y pasarela
    - Cambio de la contraseña inicial (SCALANCE y RUGGEDCOM)
    - Nombre PROFINET (PROFINET)
    - Datos IM para la identificación del dispositivo (PROFINET)
    - SystemName, SystemContact y SystemLocation
* Activación del cliente DHCP
* Reseteo a los ajustes de fábrica
* Reseteo a los valores estándar PROFINET
* Ping
* Parpadeo de los LED
* Apertura del "Web Based Management" en los dispositivos

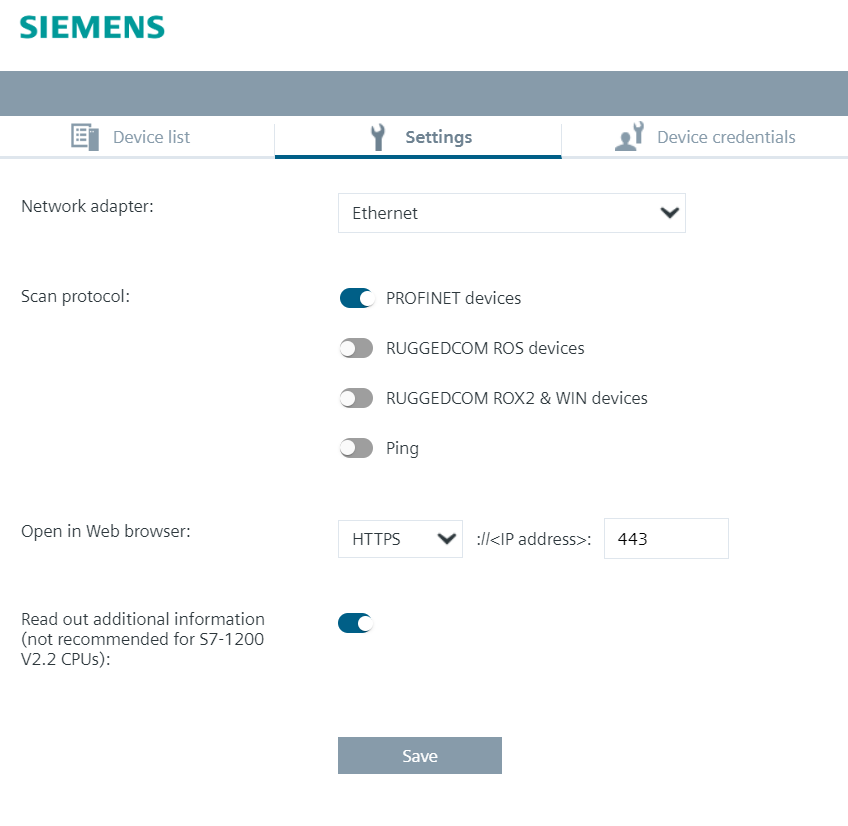
Descarga:

<https://support.industry.siemens.com/cs/document/109804190/descarga-del-software-sinec-pni-basic-v1-0-service-pack-1-update-1?dti=0&lc=es-ES>

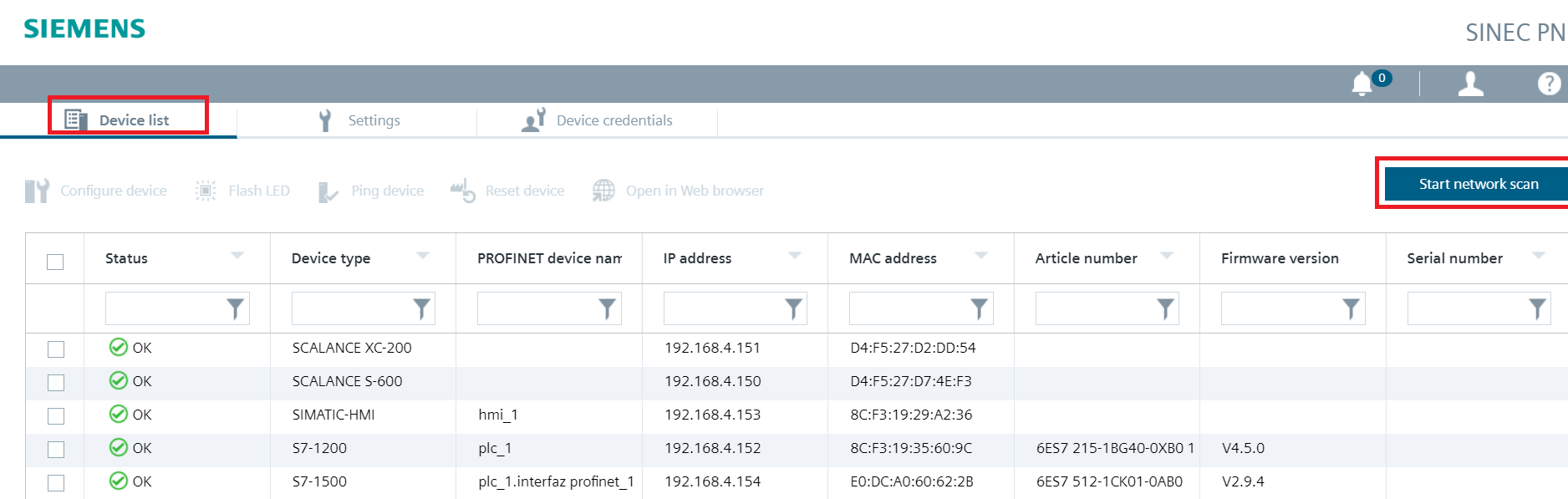
Video:

Easy and fast WLAN configuration with SINEC NMS: Part 1 - Initialization with SINEC PNI <https://www.youtube.com/watch?v=Q17ieFzegqk>

Al abrir el programa la primera vez le indicamos el adaptador por el cual “buscará” los dispositivos y el protocolo de escaneo.

****

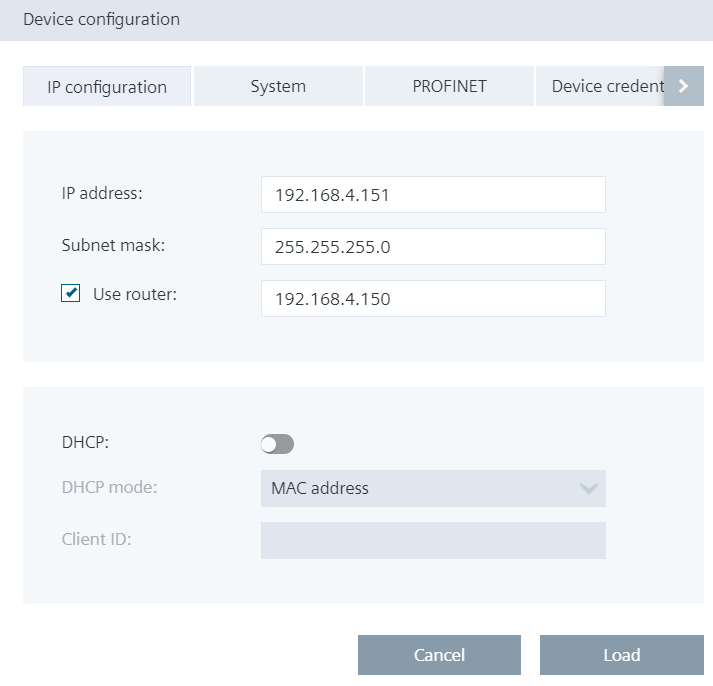
Se inicia el escaneo de la red ****

****

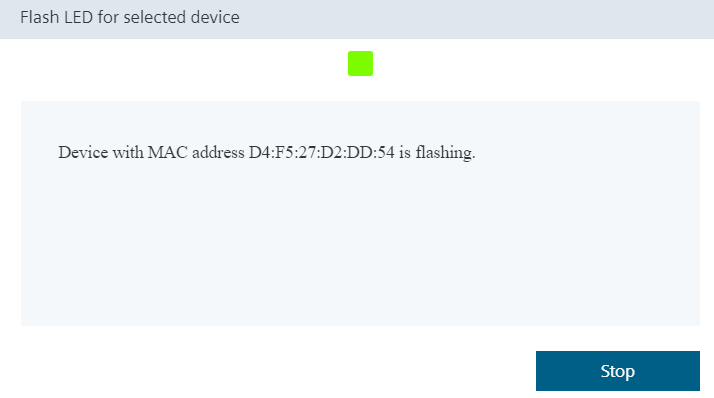
Nos muestra un listado con los dispositivos que ha descubierto. sobre ellos podremos realizar varias acciones



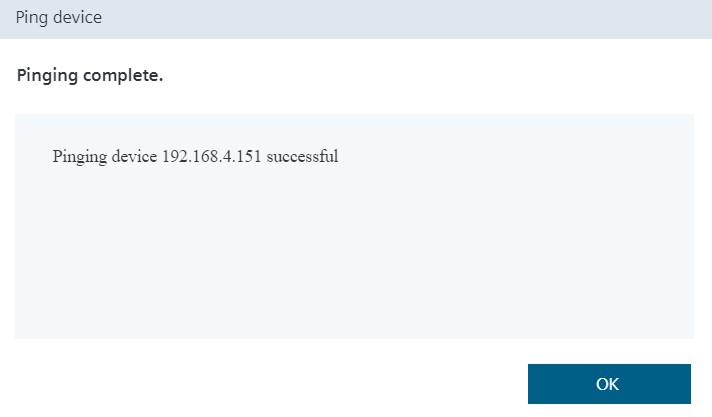
* Configurar el dispositivo 



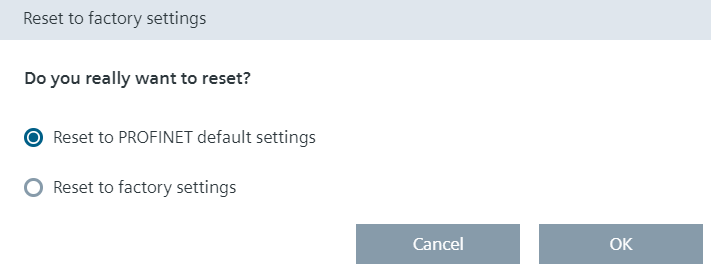
* Mostrar parpadeo para localizar físicamente el dispositivo 



* Lanzar un ping para comprobar la accesibilidad 

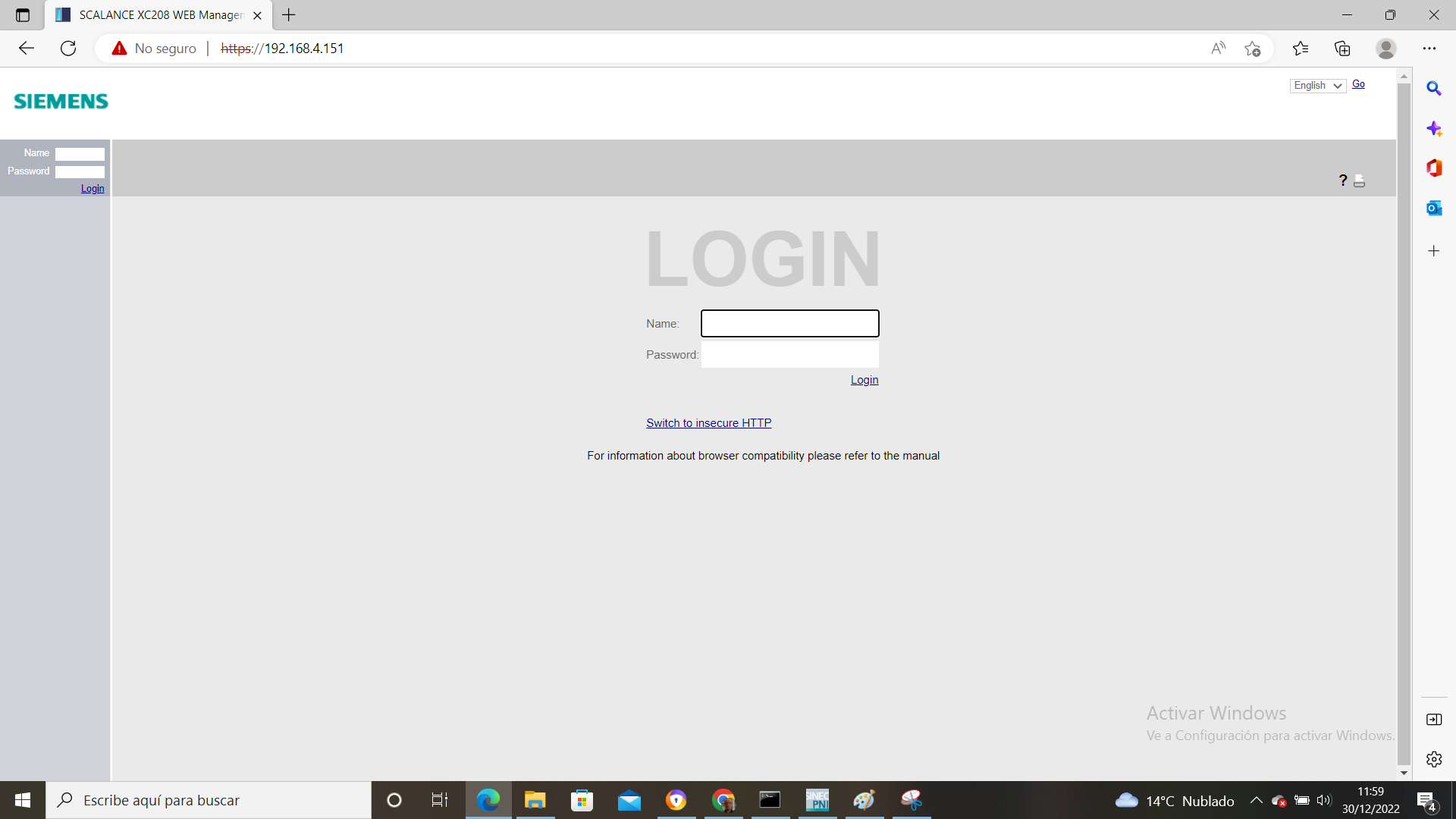


* Se puede resetear el dispositivo 

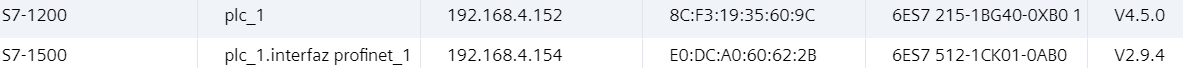
****

* Acceso a la configuración del dispositivo con el navegador web siempre que el mismo esté activo.



****

En el caso de los PLC nos aporta información valiosa : IP, MAC, Modelo CPU, versión de firmware…

****

**PRONETA**

**Herramienta de puesta en marcha y diagnóstico para PROFINET**

SIEMENS PRONETA es una herramienta software gratuito basado en PC que facilita el diagnóstico y la puesta en marcha de redes PROFINET en sistemas de automatización ofreciendo las siguientes características:

PRONETA Basic es especialmente adecuado para tareas básicas de puesta en marcha de sistemas PROFINET:

* El "**análisis de red**" proporciona una visión general rápida de los dispositivos conectados a PROFINET. Es posible realizar cambios sencillos de los parámetros de los dispositivos que forman parte de la subred a la que está conectado el PC PRONETA, por ejemplo, la configuración de red o la asignación de un nombre de red a los dispositivos. La aplicación proporciona potentes mecanismos para comparar varias topologías de red entre sí, por ejemplo, una topología "ideal" para un proyecto con la instalación real.
* La "**prueba de E/S**" es un procedimiento simple e intuitivo para probar el cableado de E/S de una instalación con un gran número de unidades de periferia. Permite verificar el cableado y crea automáticamente un registro del desarrollo de la prueba, que luego se puede exportar con fines de documentación.

Descarga:

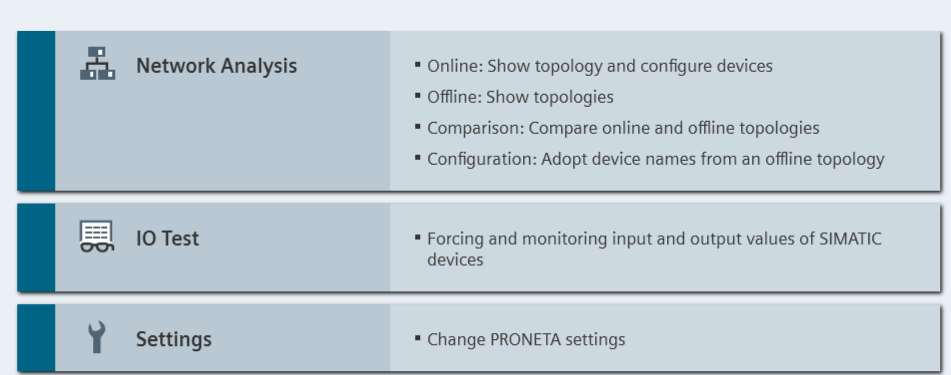
<https://support.industry.siemens.com/cs/document/67460624/proneta-basic-3-2-herramienta-de-puesta-en-marcha-y-diagn%C3%B3stico-para-profinet?dti=0&lc=es-WW>

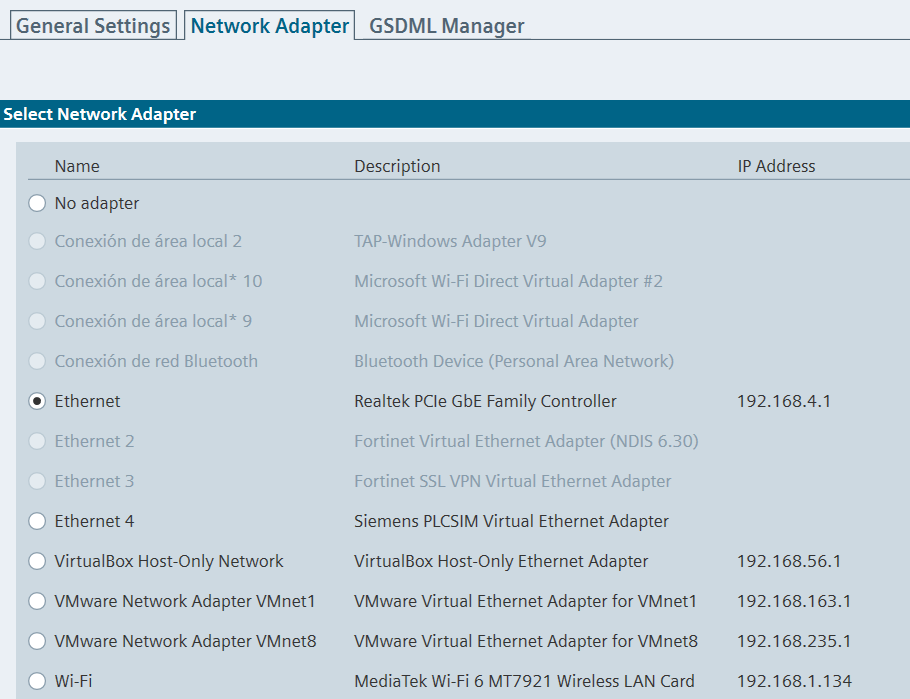
Video: PRONETA - Network analysis and IO check

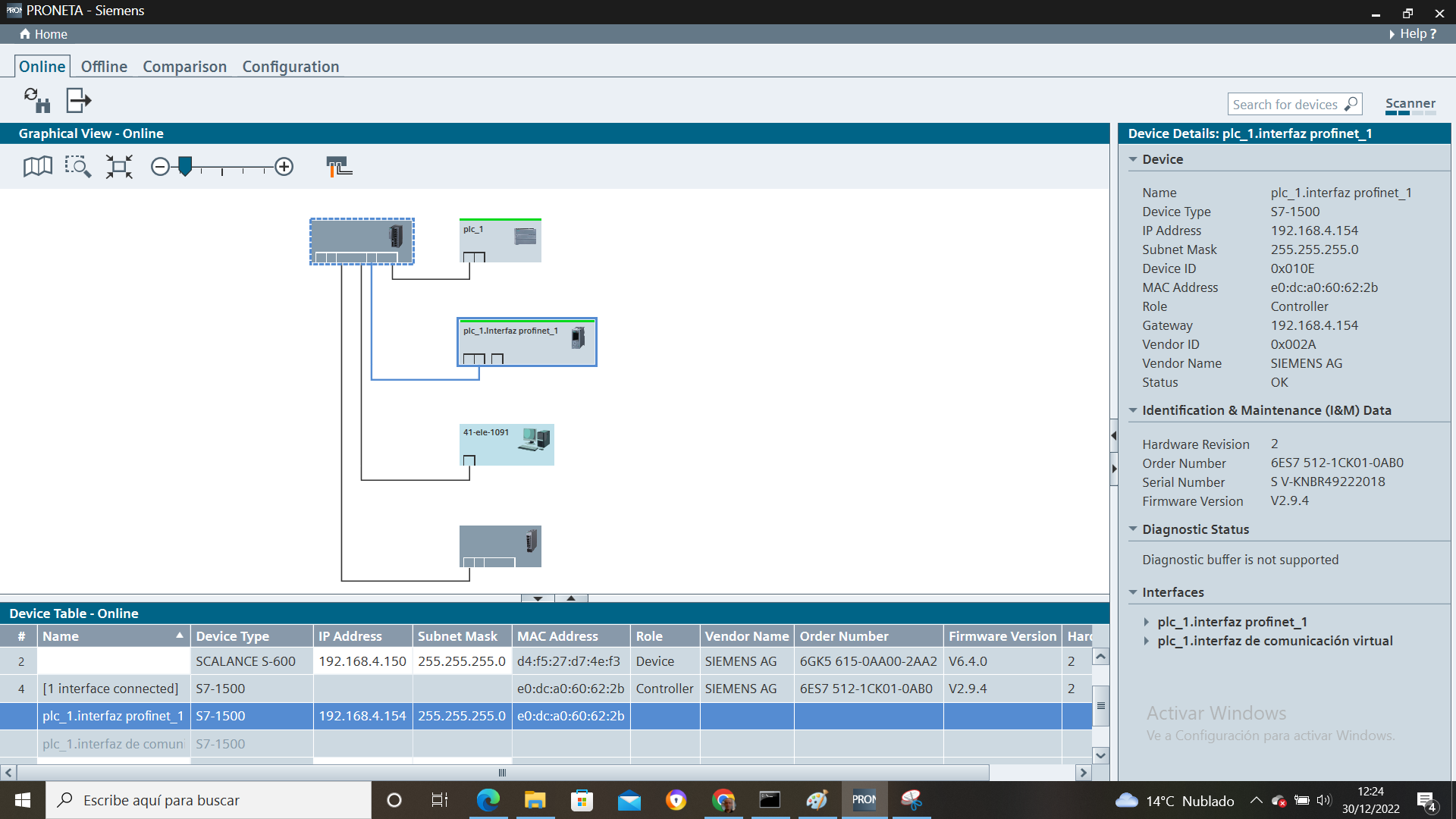
<https://www.youtube.com/watch?v=hf5h7vixcic&t=220s>

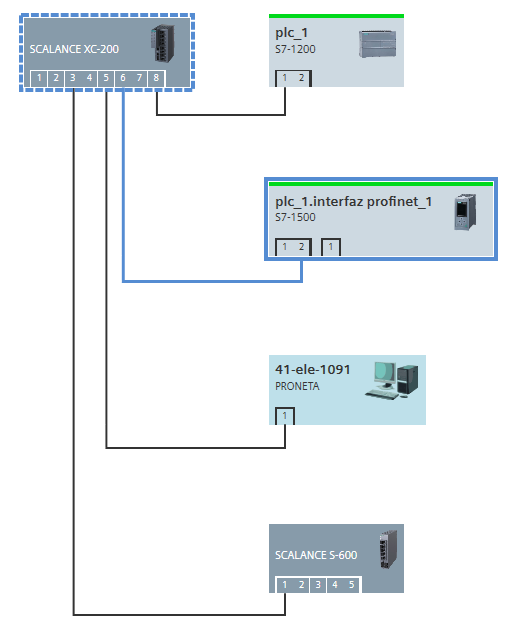
Al abrir el programa por primera vez hay que indicarle la tarjeta de red desde la que vamos a hacer el descubrimiento de dispositivos.

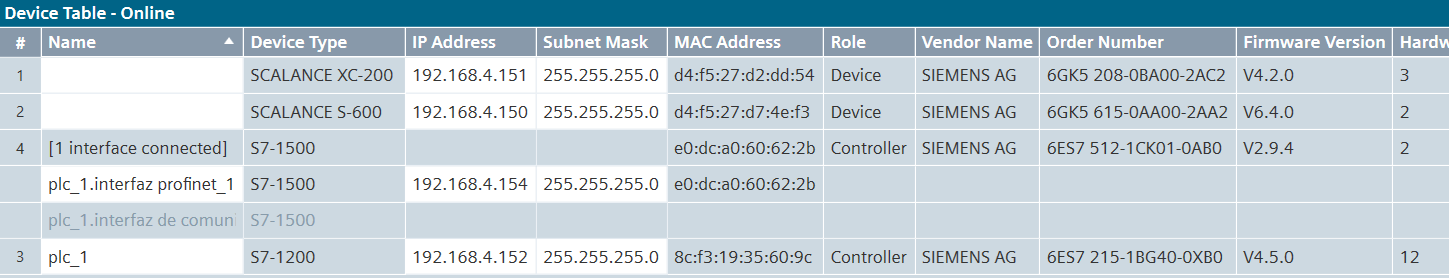


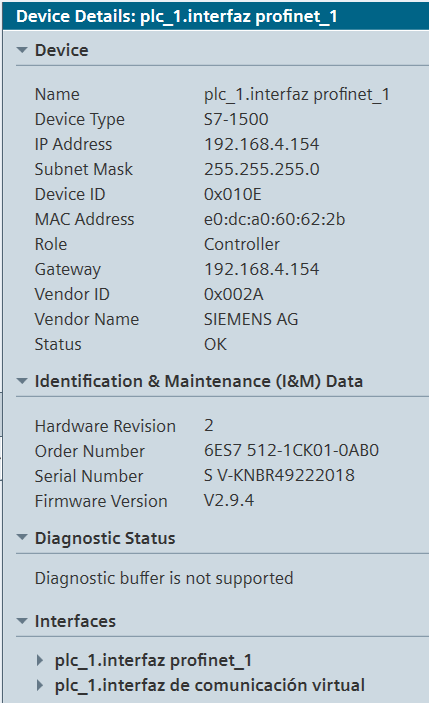




Nos muestra los dispositivos detectados, un pequeño esquema de la red y las características y datos de configuración de los elementos.







Permite configurar ciertos parámetros y realizar pruebas de conectividad.



Es posible exportar a formato pdf un informe con las características de los dispositivos de la red.

