Trabajo Fin de Grado
Grado en Ingeniería de las Tecnologías de Telecomunicación

Ciberseguridad en Sistemas de Control Industrial

Autor: Estrella Hernández Candelario
Tutor: Juan Manuel Escaño González

Dpto. Ingeniería de Sistemas y Automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2024

Trabajo Fin de Grado
Ingeniería de Telecomunicación

Ciberseguridad en Sistemas de Control Industrial

Autor:
Estrella Hernández Candelario

Tutor:
Juan Manuel Escaño González
Profesor titular

Dpto. de Ingeniería de Sistemas y Automática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2024

Proyecto Fin de Grado: Ciberseguridad en Sistemas de Control Industrial

Autor: Estrella Hernández Candelario

Tutor: Juan Manuel Escaño González

El tribunal nombrado para juzgar el Proyecto arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2024

El Secretario del Tribunal

A mi familia

Agradecimientos

En primer lugar, agradecer a Juan Manuel Escaño su colaboración y guía en este Trabajo de Fin de Grado y por haberme brindado la oportunidad de sumergirme en este fascinante y emergente campo. Su entusiasmo ha despertado en mí una curiosidad insaciable por el mundo de la investigación y me ha enseñado que el aprendizaje es un viaje que nunca termina.

A mi familia, gracias por ser mi refugio y mi guía. A mis abuelos, Rosa, José, Eduarda y Lorenzo, gracias por enseñarme el valor del trabajo duro y la constancia. A mis padres y a mi hermano, gracias por su amor y apoyo diario. Son la razón de todo lo que he logrado y mi mayor inspiración. Gracias de corazón.

A mis amigos, tanto a aquellos que he conocido durante esta etapa universitaria, que han compartido conmigo momentos que siempre recordaré, como a los amigos de toda la vida que han sido pilares fundamentales en mi crecimiento personal.

Finalmente, agradezco a Alberto su apoyo constante, su paciencia y amor, que hacen de cada día un momento especial.

A todos, gracias por acompañarme en esta etapa, por vuestro apoyo y por creer en mí.

Estrella Hernández Candelario

Sevilla, 2024

Resumen

Este Trabajo de Fin de Grado aborda la ciberseguridad en los Sistemas de Control Industrial (SCI), un área crítica en la era de la Industria 4.0 y el Internet de las Cosas (IoT).

Se analiza la evolución de los ciberataques dirigidos a infraestructuras industriales, destacando la necesidad urgente de medidas robustas de seguridad cibernética. Se presentan estudios de casos prácticos, incluyendo un pentesting en redes Modbus, para identificar vulnerabilidades y proponer mejoras en los sistemas industriales. Además, se discuten estrategias de mitigación basadas en normativas como la IEC-62443 y la evaluación de protocolos como Modbus y DNP3.

Este estudio proporciona un marco integral para fortalecer la seguridad en los SCI, orientado tanto a profesionales del sector como a entidades reguladoras, con el objetivo de garantizar la continuidad operativa y proteger los activos industriales.

Abstract

This bachelor's Thesis delves into cybersecurity within Industrial Control Systems (ICS), a critical area in the era of Industry 4.0 and the Internet of Things (IoT).

It examines the evolution of cyberattacks targeting industrial infrastructures, underlining the urgent need for robust cybersecurity measures. Case studies, including a Modbus network pentesting, are presented to identify vulnerabilities and propose enhancements. Furthermore, mitigation strategies based on standards like IEC-62443 and the evaluation of protocols such as Modbus are discussed.

This study provides a comprehensive framework for enhancing security in ICS, aimed at both industry professionals and regulatory bodies, with the aim of ensuring operational continuity and safeguarding industrial assets.

Índice

ÍNDICE DE FIGURAS

Introducción

"La desconfianza es la madre de la seguridad"

Actualmente, estamos viviendo un crecimiento exponencial de nuevas tecnologías que transforman nuestra forma de vida y de producción. Cada día nos encontramos con nuevas inteligencias artificiales que simplifican tareas, automatismos que posibilitan la reducción de trabajos manuales y labores repetitivas, y un largo etcétera de avances que están en desarrollo y aún están por venir. En este contexto, la adaptación a los cambios tecnológicos es imprescindible para mantener la competitividad y la eficiencia operativa.

Las tecnologías de la información han experimentado un vertiginoso avance en las últimas décadas en áreas como la computación en la nube, la inteligencia artificial, el aprendizaje automático y el análisis de datos, entre otras. La flexibilidad y la escalabilidad inherentes en las tecnologías de la información permiten una adopción relativamente rápida de estas soluciones en los sectores empresariales.

Por otro lado, las tecnologías de la operación, referentes a la industria y a la producción, enfrentan desafíos que provocan que estos cambios sean más complejos y costosos. La maquinaria e instrumentación industrial en la fabricación suele tener una vida útil prolongada y requieren de grandes inversiones, por lo que el reemplazo continuo de los sistemas ante un nuevo cambio tecnológico no es una opción. Además, detener la producción en infraestructuras criticas (industrias eléctricas, de agua, gas, etc.), donde la continuidad del proceso es vital, supone grandes riesgos tanto a nivel económico como a nivel humanitario.

A pesar de estos desafíos, las industrias están integrando paulatinamente estas tecnologías emergentes como la computación en la nube para facilitar la gestión de datos en tiempo real entre equipos conectados remotamente y la robótica y automatización para mejorar la eficiencia y seguridad de los entornos de producción.

La integración de estas tecnologías en la industria es lo que se conoce como Industria 4.0, un término que describe una organización de los procesos de producción basada en la tecnología y en dispositivos que se comunican entre ellos de forma autónoma a lo largo de la cadena de valor. Se busca un modelo de "fabrica inteligente", donde sistemas computacionales se encargan de supervisar los procesos físicos, crean una copia virtual del mudo físico y toman decisiones descentralizadas basadas en mecanismos de autoorganización [1].

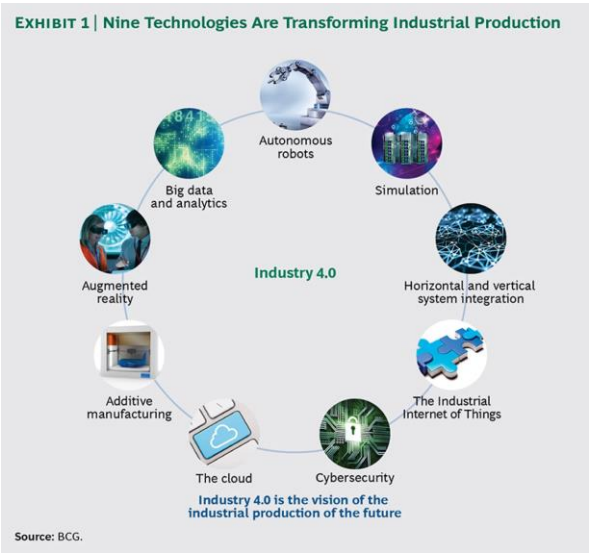


Figura 1. Tecnologías claves en la Industria 4.0 [1]

Sin embargo, a medida que las industrias avanzan hacia sistemas conectados a Internet y dispositivos inteligentes (IoT), dejando en un papel secundario las redes físicas aisladas, surge un importante desafío, proteger la industria de ataques cibernéticos.

Esto plantea una serie de retos que deben superarse para garantizar una industria eficiente y segura frente a posibles ataques cibernéticos. Proteger la producción en todo momento es crucial para mantener el funcionamiento ininterrumpido del complejo sistema industrial. Es necesario implementar medidas sólidas de seguridad cibernética que salvaguarden los activos críticos y garanticen la integridad de los procesos industriales.

El propósito de este trabajo es destacar la importancia de la ciberseguridad industrial al ofrecer una visión general de los aspectos más relevantes que deben considerarse. Se busca establecer una base que pueda servir como punto de partida para investigaciones y proyectos futuros en este campo emergente.

Para ello, se estructura el trabajo en una serie de capítulos descritos brevemente a continuación:

- **Capítulo 1. Línea Temporal de Ciberataques Industriales**: En este capítulo se ofrece una visión histórica citando ataques que han tenido especial relevancia en el ámbito industrial. Estos ataques pueden servir como base para futuros incidentes y su estudio puede ser clave para aplicar las medidas de seguridad correspondientes y mitigar los efectos de ataques futuros.
- **Capítulo 2. Retos y Factores Críticos de la Ciberseguridad Industrial**: Como se ha anticipado en la introducción de este trabajo, la ciberseguridad en la industria se enfrenta a retos que no aparecen en otros ámbitos tecnológicos. En esta sección, se resaltan algunas de las características propias de la industria a las que se deben adaptar las medidas de seguridad aplicadas.
- **Capítulo 3. Tecnologías de la Operación**: Se describe la estructura de los sistemas de control industrial y de las redes de comunicación utilizadas en los mismos. El estudio de estos es clave para comprender la infraestructura y, por tanto, defender el sistema industrial.
- **Capítulo 4. Estudio de Ciberataques y Amenazas**: En este capítulo se detallan las fases que conforman un ciberataque y se presentan algunos de los tipos de ataques más comunes dirigidos contra los sistemas industriales. La comprensión de los métodos y técnicas empleados por los atacantes permite desarrollar estrategias de defensa proactivas y más efectivas.
- **Capítulo 5. Medidas de Seguridad**: En esta sección se describen medidas a llevar a cabo para proteger los sistemas de control, como pueden ser la aplicación de la normativa referente a este campo, la realización de auditorías de seguridad y la implantación de sistemas de detección y prevención de ataques.
- **Capítulo 6. Caso Práctico. Pentesting a Redes Modbus en Sistemas de Control Industrial**: En esta sección práctica del trabajo, se ejecuta el proceso de pentesting, siguiendo la estructura convencional de estos análisis y haciendo uso de herramientas de auditoría empleadas por profesionales de seguridad. Se configura un escenario industrial de pruebas con un PLC real y se establece comunicación mediante el protocolo Modbus. Los objetivos de este caso práctico son:
    - Describir de manera práctica las fases que un auditor de seguridad lleva a cabo para determinar el nivel de seguridad de una infraestructura.
    - Presentar las herramientas más efectivas en el mercado para realizar pruebas de penetración.
    - Construcción de un escenario de pruebas que posibilite realizar auditorías preliminares sin impactar directamente en la producción.
    - Evaluar la seguridad del protocolo Modbus, identificando sus vulnerabilidades inherentes y proponiendo medidas para mitigar posibles fallos de seguridad.
- **Capítulo 7**. **Conclusiones y Líneas Futuras:** En este último capítulo, se resumen las conclusiones obtenidas de los capítulos anteriores y se plantean posibles áreas para investigaciones futuras en ciberseguridad industrial.

Todos los archivos empleados en el desarrollo de este trabajo han sido depositados en un repositorio de GitHub,

al que se puede acceder mediante el siguiente enlace:
https://github.com/estrellahc/ICSPentesting.git

1 LÍNEA TEMPORAL DE CIBERATAQUES INDUSTRIALES

"Quien no conoce la historia está condenado a repetirla"

-George Santayana

En este capítulo se busca ofrecer una visión histórica, trazando una línea temporal de ataques que han comprometido a la industria, ocasionando importantes daños tanto económicos como humanos. Con esta información, se pretende adquirir conocimiento sobre las organizaciones criminales más destacadas en ataques contra sistemas industriales, las técnicas llevadas a cabo y los daños producidos. La frase "Quien no conoce la historia está condenado a repetirla", atribuida a George Santayana, se aplica en este ámbito, ya que muchos de los ataques que actualmente comprometen los sistemas industriales son evoluciones de los que se mencionan a continuación.

En enero de 2010 un "gusano" tomó el control de la central nuclear de Bushehr, en Irán. Este consiguió reprogramar el funcionamiento de las máquinas industriales de Siemens y alterar el funcionamiento de las centrifugadoras, las cuales recibieron instrucciones de autodestrucción [2]. Este ataque, basado en el uso de una serie de vulnerabilidades Zero Day [1]en el sistema operativo Windows y dirigido al sistema de supervisión y adquisición de datos (SCADA), fue el primero que alteró el funcionamiento de la maquinaria industrial en un entorno de alta seguridad [3]. Fue conocido como *Struxnet* y marcó un antes y un después en lo que se conoce como ciberseguridad de las operaciones, ciberseguridad OT.

En el año 2012, se descubrió el troyano *BlackEnergy*, el cual se empleó para llevar a cabo ataques DDoS,[2] ciberespionaje y destrucción de información. *BlackEnergy* se utilizó en contra de diversas organizaciones, incluyendo sectores gubernamentales, diplomáticos, de medios de comunicación y transporte. No obstante, el incidente más destacado tuvo lugar el 23 de diciembre de 2015, cuando se perpetró un ataque significativo contra la red eléctrica de Ucrania. Aproximadamente la mitad de los hogares en la región ucraniana de Ivano-Frankivsk se vieron privados de electricidad durante varias horas [4]. El grupo responsable de *BlackEnergy* es conocido como SandWorm. A este grupo de ciberatacantes se les atribuye la utilización de la amenaza *BlackEnergy* en diversas campañas de ciberataques y ciberespionaje, con gran interés en Ucrania y otros países de Europa del Este [5].

En 2014 se identifica un nuevo malware destinado al ataque de sistemas industriales y maquinaria de determinados fabricantes en Europa y Estados Unidos. Esta amenaza, conocida como *Havex*, consiste en un troyano de acceso remoto, RAT[3] capacidad de recolectar datos de los sistemas de control industrial con la intención de llevar a cabo posteriores ataques contra este hardware [6].

En 2016, *Industroyer*, la mayor amenaza para sistemas de control industrial desde Struxnet según los investigadores de ESET, dejó sin suministro eléctrico a parte de la capital ucraniana, Kiev. Este malware es capaz de controlar los interruptores de una subestación eléctrica. Para ello, utiliza algunos de los protocolos de comunicación industrial más utilizados en sistemas de infraestructura crítica como suministro de agua, gas y

[1] Una vulnerabilidad de día cero o Zero Day, es una vulnerabilidad que acaba de ser descubierta y aún no se conocen las medidas de seguridad a aplicar. El principal riego de estas vulnerabilidades es que hasta que se encuentra el parche de seguridad, los atacantes tienen vía libre para explotar la vulnerabilidad [64].

[2] Un ataque de Denegación Distribuida de Servicio (DDoS) tiene como objetivo desactivar o derribar un servicio, proceso u otro recurso en línea sobrecargándolo con solicitudes de conexión sin sentido, paquetes falsos u otro tráfico malicioso. Al no poder manejar el volumen de tráfico ilegítimo, el objetivo se ralentiza o se bloquea por completo, por lo que no está disponible para los usuarios legítimos.

[3] Un troyano de acceso remoto, o RAT, es un tipo de software malicioso que permite a un atacante controlar de forma remota un sistema infectado, accediendo y manipulando información sin el conocimiento del usuario.

electricidad [7].

En 2016, el grupo de ciberatacantes Electrum ejecutó un ataque a una subestación eléctrica en Ucrania, denominado *Crashoverrider* [8]Este ataque se distinguió por su modus operandi, que incorporó varias técnicas basadas en ataques anteriores: envía comandos directamente a las RTU utilizando protocolos industriales, entre los que se incluye la apertura y cierre de "breakers" (interruptores de las subestaciones) de forma rápida y continuada al igual que BlackEnergy, bloquea los puertos series de equipos Windows, impidiendo las comunicaciones de los dispositivos legítimos con los equipos afectados y también tiene capacidad para explotar una vulnerabilidad conocida de los relés de Siemens SIPROTEC, que puede provocar denegaciones de servicio [9].

Trisis, o *Triton*, es un malware dirigido a sistemas de seguridad industrial diseñado para manipular los Sistemas Instrumentados de Seguridad (SIS) Triconex de Schneider Electric, permitiendo la sustitución de la lógica en los elementos de control finales [10]. Este ciberataque se identificó en 2017, cuando afectó a una planta petroquímica en Oriente Medio.

En 2022, se ha detectado una amenaza APT [4]dirigida a sistemas de control industrial, que ha afectado a dispositivos clave como PLCs de Schneider Electric y OMRON Sysmac NEX. Se ha denominado *Pipedream* (Dragos [11]) o *Incontroller* (Mandiant [8]). Este malware modular explota funciones estándar de protocolos como Codesys, Modbus y OPC UA, con el fin de causar interrupciones y sabotajes. Las medidas de mitigación por parte de Mandiant, Dragos, CISA, y fabricantes como ABB y Schneider Electric, recomiendan la actualización de los productos [12].

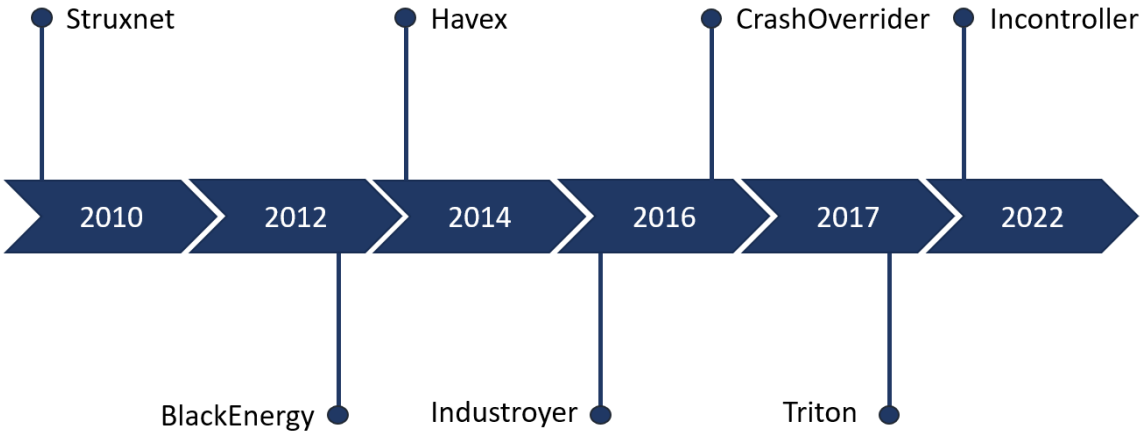


Figura 2. Línea temporal de ataques relevantes a Sistemas de Control Industrial

[4] Una amenaza avanzada persistente (APT) utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas [65].

2 RETOS Y FACTORES CRÍTICOS DE LA CIBERSEGURIDAD INDUSTRIAL

"El conocimiento es poder, pero la información es la clave"

-Aaron Levie

En este capítulo, se exploran los principales desafíos que enfrenta la ciberseguridad industrial, destacando su diferencia con las redes de tecnología de la información (IT) y cómo la evolución de las redes industriales plantea nuevos riesgos.

Como se ha mencionado previamente en este trabajo, la continuidad de la producción representa un aspecto crítico en el entorno industrial. Los sistemas de control industrial constituyen la columna vertebral de numerosas infraestructuras críticas, donde la interrupción de los procesos de producción no es una alternativa viable. Por consiguiente, todas las medidas de ciberseguridad deben implementarse para preservar la continuidad operativa.

Si bien la aplicación de parches de seguridad es una práctica habitual para mitigar vulnerabilidades en sistemas informáticos, su implementación en el ámbito industrial puede resultar compleja y arriesgada. Esto se debe a que la aplicación de parches podría ocasionar interrupciones en la producción que tendrían repercusiones económicas significativas o podrían provocar escasez de suministros. Esta situación deja a los sistemas vulnerables ante amenazas cibernéticas y plantea un dilema constante entre la seguridad y la continuidad operativa.

Anteriormente, las redes industriales solían ser redes locales aisladas que utilizaban protocolos propios de cada fabricante. Esto implicaba un cierto nivel de seguridad inherente al no comunicarse con el exterior. Sin embargo, la evolución en tecnologías como la automatización, robótica o IoT ha resultado en la conexión de los sistemas industriales a Internet. Esta integración expone a los sistemas a ciberataques.

Cuando se diseñaron los protocolos de campo, no se anticiparon problemas de ciberseguridad, por lo que carecen de medidas necesarias como encriptación, autenticación, entre otros aspectos cruciales. Actualmente, la mayoría de las comunicaciones se realizan a través de estos protocolos poco seguros. Sin embargo, sustituirlos por otros más seguros seria económica y logísticamente inviable [13].

Además, el sector industrial se caracteriza por la necesidad de maquinaria, sistemas e infraestructuras de alto coste que tienen tiempos de vida prolongados. Por ejemplo, en una planta de fabricación de piezas automotrices, una sola máquina especializada puede costar cientos de miles o incluso millones de euros. Estas máquinas suelen ser diseñadas para durar décadas y están integradas con sistemas de control específicos que pueden no ser compatibles con las últimas medidas de seguridad cibernética. Aunque se descubran vulnerabilidades en estos sistemas, cambiarlos por otros más seguros puede resultar imposible tanto en términos de coste como de tiempo. Además del gasto directo en la actualización de la maquinaria, también se enfrentarían a interrupciones en la producción y a la necesidad de volver a capacitar al personal para trabajar con las nuevas tecnologías. Por tanto, muchas empresas industriales están en una encrucijada entre asegurar la protección de sus sistemas y las limitaciones financieras de su funcionamiento [14].

En conclusión, las industrias se enfrentan al reto de proteger sus sistemas sin descuidar las limitaciones financieras y técnicas propias del sector. Además, es crucial que el personal esté bien capacitado en ciberseguridad, ya que necesitan aplicar medidas de protección y estar preparados para responder ante posibles

amenazas cibernéticas. Esta situación resalta la importancia y la urgencia de abordar los desafíos de seguridad digital en la industria.

3 TECNOLOGÍAS DE LA OPERACIÓN

Las grandes oportunidades nacen de haber sabido aprovechar las pequeñas.

-Bill Gates-

Comprender la estructura de los sistemas de control industriales es esencial para su protección. Esto nos ayuda a detectar vulnerabilidades en cada dispositivo y aplicar medidas para proteger tanto los activos individuales como el sistema en su conjunto. Al comprender cómo se integran las piezas, logramos entender su funcionamiento y, en consecuencia, protegerlo de manera más efectiva.

En este capítulo, se describen los componentes fundamentales de un sistema de control industrial y como se interconectan a través de las redes de comunicaciones industriales.

3.1 Sistema de Control Industrial

Un sistema de control industrial (ICS) representa un conjunto de componentes tanto hardware como softwares diseñados para supervisar y regular operaciones dentro de entornos industriales. Estos sistemas desempeñan un papel vital en sectores críticos como centrales energéticas, industria alimentaria, nuclear y petroquímica, donde su correcto funcionamiento es esencial para la seguridad y la eficiencia operativa.

El objetivo fundamental de un sistema de control industrial es garantizar la monitorización y regulación de los procesos industriales, asegurando su ejecución de manera segura y eficiente. Estos sistemas se encargan de controlar una amplia gama de variables, que van desde la temperatura y la presión hasta el caudal, la velocidad y otras condiciones específicas que varían según el tipo de proceso industrial. A continuación, se describen los elementos fundamentales que están presentes en la mayoría de los sistemas de control industrial:

- **Sensores y Actuadores**: los sensores son dispositivos que registran y convierten magnitudes físicas como temperatura, presión o luz en señales eléctricas, mientras que los actuadores son dispositivos que interpretan señales eléctricas para realizar acciones físicas, como mover un motor o abrir una válvula.
- **Programmable Logic Controller (PLC)**: un PLC es un microcontrolador utilizado en el ámbito industrial para automatizar procesos y realizar funciones de control. Los PLCs son físicamente más robustos (amplio rango de temperaturas, inmunidad al ruido, resistencia ante vibraciones) que una computadora común, lo que los hace adecuados para un entorno industrial. Además, cuentan con numerosas entradas y salidas para conectar múltiples sensores y actuadores.

  Un PLC es programado para generar salidas en función de las entradas, es decir, activar o desactivar los actuadores conectados (motores, válvulas, bombas, compresores, etc.) en función del estado de los sensores (sensores de presión, vacío, temperatura, fotoeléctricos, ópticos, etc.). Los PLC pueden ser programados en una serie de estándares definidos en la norma IEC-61131-3[5]. Para realizar la conexión de sensores y actuadores con el PLC normalmente se utilizan buses de campo como Modbus, Profibus, EtherNet/IP, Interbus, etc. [15]

[5] IEC 61131-3:2013 establece la sintaxis y semántica de un conjunto unificado de lenguajes de programación para controladores programables (CP). Este conjunto incluye dos lenguajes textuales (IL y ST) así como dos lenguajes gráficos (LD y FBD) [66]

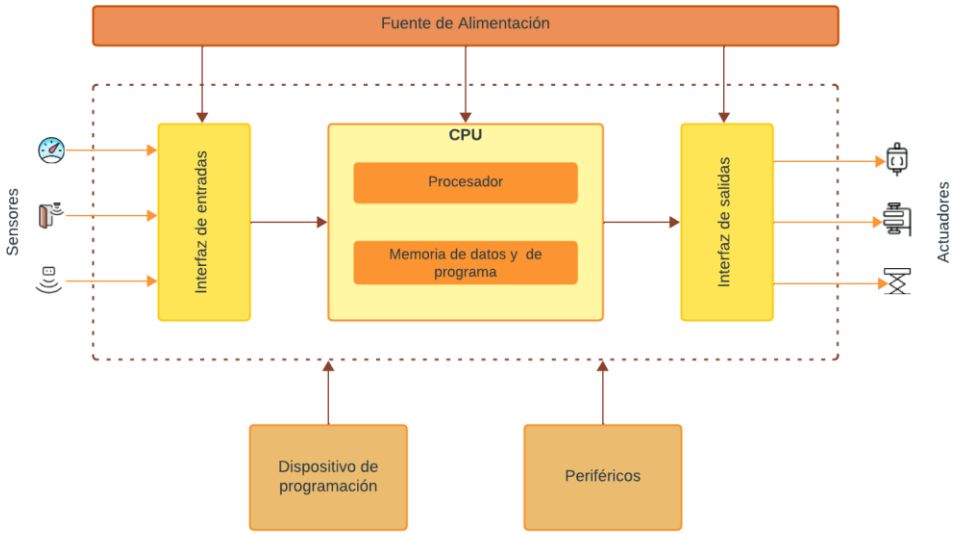


Figura 3. Estructura interna de un controlador lógico programable (PLC)

- **Remote Terminal Unit (RTU)**: un RTU es un dispositivo que se encuentra en una subestación o estación remota. La función de estos dispositivos es monitorizar los parámetros de planta y transmitirlos a una estación central conocida como unidad terminal maestra (MTU). Un PLC o un HMI pueden realizar las funciones de MTU. Para realizar la comunicación remota utilizan tecnologías de comunicación como GPRS/3G/4G[6], radio, vía MQTT[7] o OPC UA [8][16].
- **Human Machine Interface (HMI):** las interfaces hombre-máquina son el medio de comunicación entre el operario y los PLCs y RTUs. Esta interfaz proporciona al operario funciones para interactuar con un proceso de control como iniciar y detener procesos, ajustar variables y visualización de gráficos informativos sobre el estado del área controlada. La HMI interactúa directa o indirectamente, a través de un servidor ICS, con uno o varios controladores utilizando protocolos industriales como OPC o protocolos de buses de campo como Modbus, Profibus, EtherNet/IP, Interbus, etc.
- **Supervisory Control and Data Acquisition (SCADA)**: se utiliza este término para describir el conjunto de sistemas de control industrial y dispositivos que trabajan simultáneamente para supervisar y controlar procesos industriales en tiempo real [17]. Recopilan datos de sensores y actuadores, registrando toda la información generada y activando alarmas ante comportamientos anómalos. La integración con otros sistemas de control industrial permite una gestión eficiente de las operaciones en entornos industriales.

[6] GPRS (General Packet Radio Service) es un estándar de comunicación inalámbrica que permite la transmisión eficiente de datos a través de redes móviles.
[7] MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería ligero y eficiente diseñado para la comunicación entre dispositivos en redes de baja potencia y ancho de banda limitado, es comúnmente utilizado en el Internet de las Cosas (IoT).
[8] OPC UA (Open Platform Communications Unified Architecture) es un estándar de comunicación industrial diseñado para facilitar la interoperabilidad y la integración de sistemas en entornos industriales.

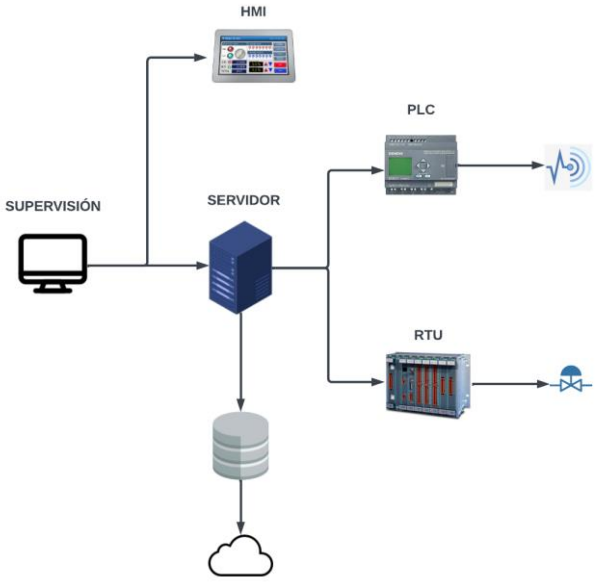


Figura 4. Esquema Sistema de Control y Adquisición de Datos (SCADA)

- **Distributed Control System (DCS)**: el Sistema de Control Distribuido está estrechamente relacionado con un sistema SCADA, las diferencias entre ambos son bastante sutiles y, con el tiempo, se vuelven cada vez más difíciles de distinguir. Tradicionalmente, los sistemas SCADA se han utilizado para llevar a cabo tareas de automatización que abarcan un área geográfica más extensa, mientras que un DCS se emplea con mayor frecuencia en una sola planta o instalación.

  Un DCS es un sistema de gran envergadura, diseñado para cumplir una tarea muy específica. Este sistema utiliza una unidad de supervisión centralizada que puede controlar puntos de entrada y salida. Además, se aplica redundancia en todos los niveles de la instalación para garantizar un funcionamiento ininterrumpido y confiable [17].

- **Safety Instrumented System (SIS)**: el Sistema de Seguridad Instrumentado es un conjunto de sensores, actuadores y lógica de control encargado de proteger los sistemas de control y garantizar la seguridad de las personas, el medio y la maquinaria. Este sistema cuenta con numerosos sensores que miden variables criticas como temperatura o presión y toma las acciones necesarias en caso de detectar valores anómalos (altas temperaturas, altos niveles de gases, etc.) que puedan provocar situaciones peligrosas.

3.2 Protocolos de comunicación industriales

Las redes de comunicación son indispensables en un sistema de control industrial, pues posibilitan la transmisión de señales entre dispositivos y sistemas dentro de una planta industrial. Los protocolos industriales están diseñados para operar en tiempo real y soportar operaciones de alta precisión.

A continuación, se describen algunos de los protocolos más utilizados en las redes industriales y que tienen un gran impacto en este entorno.

3.2.1 Modicon Communication Bus

El protocolo Modbus fue desarrollado por Modicon Industrial Automation Systems en 1979 para su gama de controladores lógicos programables (PLC). A partir de ese momento, el

protocolo Modbus se ha ido extendiendo hasta llegar a estar presente en la mayoría de los sistemas de control industriales.

Figura 5. Logo Modbus

Modbus comenzó utilizándose como protocolo de comunicación serie, posteriormente surgieron otras versiones para adaptarse a las redes industriales sobre TCP/IP. Modbus TCP se utiliza para Ethernet, y Modbus RTU y Modbus ASCII para los puertos serie [18].

- El protocolo Modbus serie emplea el estándar HDLC para la tecnología de transmisión. Cuando se implementa en modo maestro-esclavo, utiliza interfaces RS232 o RS485.
- Modbus/TCP utiliza la arquitectura TCP/IP para transmitir información.

Actualmente, con la integración de las fábricas a Internet, el protocolo Modbus sobre TCP gana más implementación que la conexión serie. Sin embargo, es importante destacar que esta implementación conlleva una mayor vulnerabilidad a ataques de red. Por esta razón, en este capítulo se analiza detalladamente el funcionamiento del protocolo Modbus TCP, centrándose en su estructura y operatividad.

Modbus TCP proporciona una comunicación cliente/servidor entre dispositivos conectados en una red Ethernet TCP/IP. En una comunicación cliente/servidor el cliente es el encargado de iniciar la comunicación, realizando peticiones. La función del servidor es esperar el recibo de peticiones por parte del cliente y responder a estas peticiones con la acción requerida. Por defecto, el puerto TCP de escucha para comunicaciones Modbus es el 502. Este modelo cliente/servidor se basa en cuatro tipos de mensajes: [19]

- MODBUS Request: mensaje enviado por el cliente para iniciar una transacción.
- MODBUS Confirmation: mensaje de respuesta recibido en el lado del cliente.
- MODBUS Indication: mensaje de solicitud recibido en el lado del servidor.
- MODBUS Response: mensaje de respuesta enviado por el servidor.

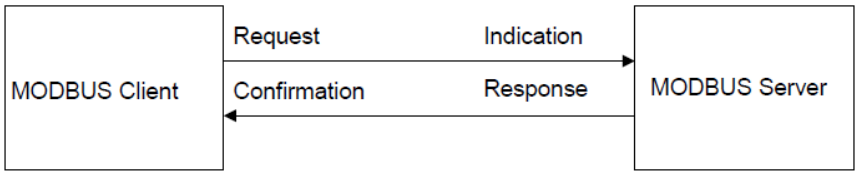


Figura 6. Modelo cliente servidor Modbus [18]

El protocolo Modbus TCP se define como un sistema de mensajería de aplicación situado en el séptimo nivel del modelo OSI[9]. En este protocolo, la comunicación entre dispositivos sigue la pila de protocolos TCP/IP como se muestra en la siguiente imagen. TCP proporciona un intercambio confiable de datos entre dispositivos, asegurando que los mensajes enviados sean

[9] El Modelo OSI (Open Systems Interconnection) es un marco conceptual que describe y estandariza la comunicación entre sistemas de computadoras. Fue desarrollado por la Organización Internacional de Normalización (ISO) en la década de 1980 con el objetivo de facilitar la comunicación entre diferentes sistemas de computadoras, independientemente de su arquitectura y fabricante [67].

recibidos correctamente y en el orden correcto.

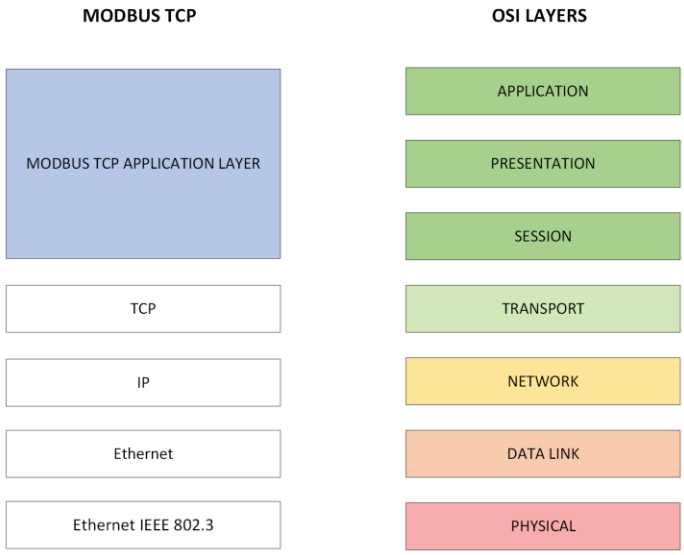


Figura 7. Pila de protocolos Modbus TCP (izquierda) vs Modelo OSI (derecha)

El intercambio de tramas en Modbus TCP se realiza según el siguiente procedimiento:

- **Establecimiento de la conexión**: en primer lugar, se establece una conexión TCP entre el cliente y el servidor Modbus. Esto implica un proceso de tres vías de sincronización (*handshake*) para establecer la comunicación.

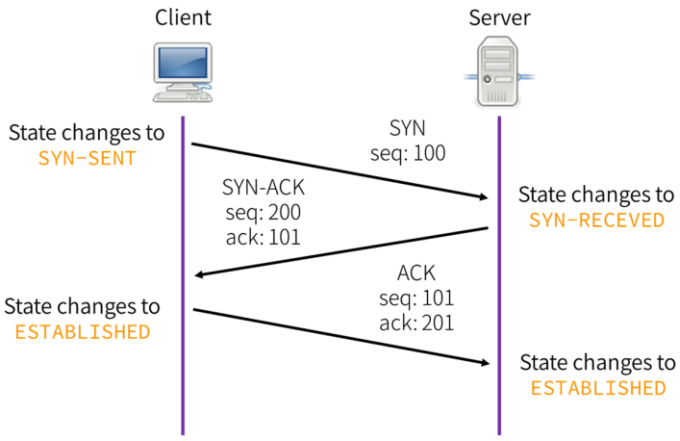


Figura 8. Handshake Modbus TCP [20]

- **Intercambio de datos entre cliente y servidor Modbus**: Una vez que se establece la conexión, el cliente Modbus envía solicitudes al servidor Modbus. Estas solicitudes contienen información sobre la acción que se desea realizar, como leer o escribir datos en un dispositivo. El servidor Modbus responde a estas solicitudes con la información solicitada o un código de error si la solicitud no se puede completar. Las tramas enviadas entre cliente y servidor siguen el formato especificado en la norma Modbus [19] que se describen en el siguiente párrafo de este capítulo.
- **Cierre de la conexión**: Una vez que se completa la comunicación o se detecta un tiempo de inactividad, se cierra la conexión TCP con el envío de tramas de cierre de conexión.

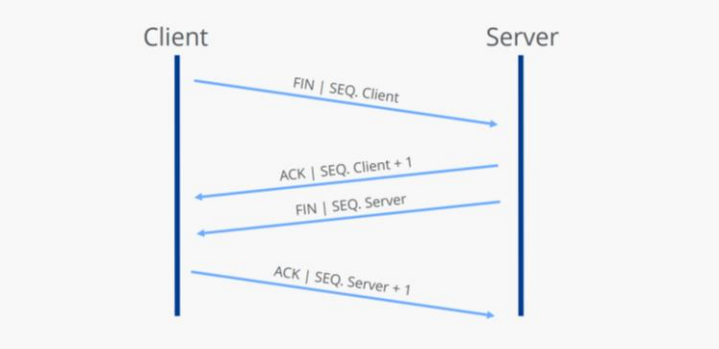


Figura 9. Cierre conexión Modbus TCP [21]

A continuación, se estudian las tramas intercambiadas por cliente y servidor para comunicarse, esto permite comprender el protocolo y encontrar posibles vulnerabilidades que puedan comprometer las redes Modbus.

La trama *Modbus TCP ADU (Modbus TCP Application Data Unit)* está compuesta por una cabecera, *MBAP header (Modbus Application Protocol header)* seguida de la *PDU (Protocol Unit Data)* como se muestra en la figura. El tamaño de la PDU es variable, aunque tiene una longitud máxima de 253 bytes. Por tanto, el límite máximo de la trama TCP ADU es de 260 bytes, 253 bytes de PDU más la cabecera MBAP (7 bytes) [19].

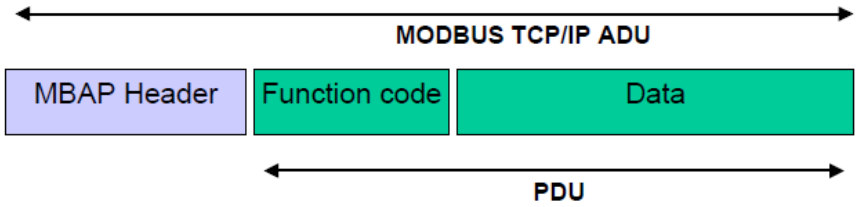


Figura 10. Trama Modbus TCP [18]

La cabecera MBAP header se compone de los siguientes campos:

- Transaction Identifier, identificador de la transacción (2 bytes): Permite identificar los pares solicitud/respuesta en una transacción. Este campo debe contener el mismo valor tanto en la trama del cliente como en la del servidor.
- Protocol Identifier, identificador del protocolo (2 bytes): Identifica el protocolo encapsulado en la trama, útil para la multiplexación dentro del sistema. El valor reservado para Modbus es el 0.
- Length, longitud (2 bytes): Indica la longitud en bytes de los campos siguientes, Unit Identifier y PDU.
- Unit Identifier, identificador de la unidad (1 byte): Este campo es utilizado para el enrutamiento dentro del sistema. Se utiliza para comunicarse con Modbus o con un esclavo de línea serie a través de una puerta de enlace entre una red Ethernet TCP/IP y una línea serie Modbus. Este campo se establece por el cliente en la solicitud y debe ser devuelto en la respuesta con el mismo valor.

La unidad de datos del protocolo (PDU) está compuesta por dos campos:

- Function code, código de función (1 byte): Indica al servidor el tipo de acción a realizar. Se pueden encontrar tres tipos de códigos de función: códigos de función públicos (*public function codes*), códigos de función definidos por el usuario (*user-defined function codes*) y códigos de función reservados (*reserved function codes*).

  Además, este campo proporciona un mecanismo de detección de errores. Si no hay

errores, el servidor envía en la respuesta el código de función. Si hubiera error, al código de función se suma 128 en decimal.

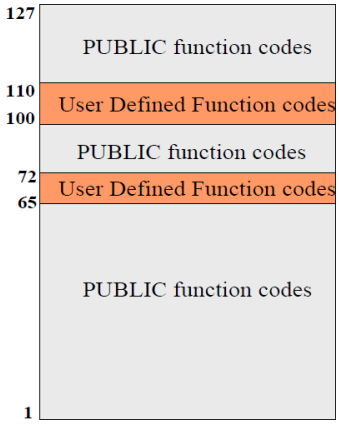


Figura 11. Rango de códigos de función Modbus

En la siguiente tabla se muestran algunos de los códigos de función más utilizados:

				Function Codes			
				code	*Sub code*	*(hex)*	*Section*
Data Access	**Bit access**	Physical Discrete Inputs	Read Discrete Inputs	**02**		**02**	6.2
		Internal Bits Or Physical coils	Read Coils	**01**		**01**	6.1
			Write Single Coil	**05**		**05**	6.5
			Write Multiple Coils	**15**		**0F**	6.11
	16 bits access	Physical Input Registers	Read Input Register	**04**		**04**	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	**03**		**03**	6.3
			Write Single Register	**06**		**06**	6.6
			Write Multiple Registers	**16**		**10**	6.12
			Read/Write Multiple Registers	**23**		**17**	6.17
			Mask Write Register	**22**		**16**	6.16
			Read FIFO queue	**24**		**18**	6.18
	File record access		Read File record	**20**		**14**	6.14
			Write File record	**21**		**15**	6.15
Diagnostics			Read Exception status	**07**		**07**	6.7
			Diagnostic	**08**	**00-18,20**	**08**	6.8
			Get Com event counter	**11**		**OB**	6.9
			Get Com Event Log	**12**		**0C**	6.10
			Report Server ID	**17**		**11**	6.13
			Read device Identification	**43**	**14**	**2B**	6.21
Other			Encapsulated Interface Transport	**43**	**13,14**	**2B**	6.19
			CANopen General Reference	**43**	**13**	**2B**	6.20

Figura 12. Códigos de función Modbus más utilizados [18]

- Data (longitud variable): Información adicional sobre la acción a realizar. Si el código de función solo especifica la acción este campo no existirá.

En el capítulo 6 se presenta un estudio práctico que implica la auditoría del protocolo mencionado para identificar vulnerabilidades en su diseño y funcionamiento, que podrían

explotarse en ciberataques. Se recomienda encarecidamente revisar este capítulo para comprender dichas vulnerabilidades y, por ende, poder planificar e implementar las medidas de seguridad correspondientes.

3.2.2 PROFIBUS

PROFIBUS es un protocolo de comunicación industrial de tipo estándar que se distingue por su robustez y su habilidad para conectar múltiples dispositivos dentro de sistemas de automatización. Fue creado en la década de 1980 por un consorcio de empresas junto a la colaboración del gobierno alemán. PROFIBUS responde a la necesidad de simplificar las instalaciones industriales, reduciendo así los costos y aumentando la eficiencia de los procesos [22].

Figura 13. Logo Profibus/Profinet

Este protocolo opera bajo el modelo maestro-esclavo o maestro-maestro y utiliza el estándar RS-485 en su capa física.

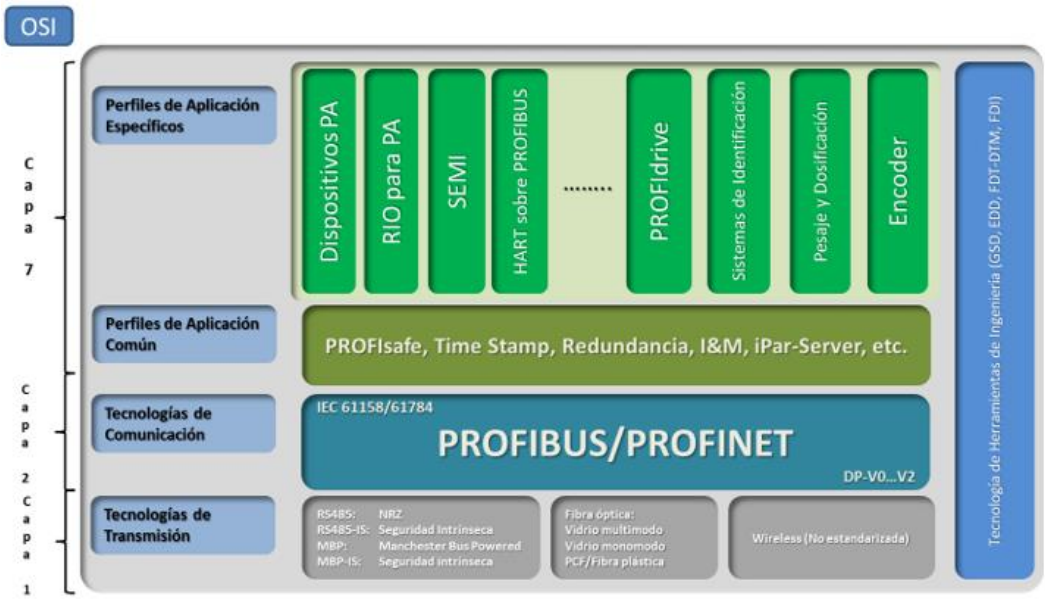


Figura 14. Estructura del protocolo PROFIBUS [22]

Ofrece tres variantes principales para adaptarse a diferentes necesidades industriales [23]:

- Profibus DP: Utilizado principalmente para conectar sensores y actuadores con PLCs o terminales, ofrece altas velocidades y eficiencia, siendo una alternativa a los sistemas de transmisión de 4 a 20 mA.
- Profibus FMS: Empleado para la comunicación entre células de proceso o equipos de

automatización, permite la transmisión de datos comunes en entornos industriales y soporta un sistema multimaestro.

- Profibus PA: Destinado al control de procesos en industrias como la química y la petrolera, funciona a 31.2 Kbits/s y se basa en la tecnología IEC 1158-2, también sustituyendo sistemas de transmisión de 4 a 20 mA y utilizando cables trenzados de dos hilos con protección RS485.

Una de las características clave de PROFIBUS es su flexibilidad en la configuración, que permite múltiples topologías como anillo, línea y estrella. Soporta altas velocidades de transmisión, hasta 12 Mbps para la variante Profibus DP, que son suficientes para la mayoría de las aplicaciones industriales.

Baud rate kbit/s	Max longitud de cable
9,6	1200 m
19,2	1200 m
45,45	1200 m
93,75	1200 m
187,5	1000 m
500	400 m
1500	200 m
3000	100 m
6000	100 m
12000	100 m

Figura 15. Relación velocidad de transmisión frente a longitud del cableado Profibus [22]

Más adelante surge PROFINET, un sucesor de PROFIBUS que se adapta a las necesidades de la automatización industrial mediante la tecnología Ethernet industrial. PROFINET aprovecha el estándar Ethernet para comunicaciones en tiempo real y la gestión integrada de operaciones de IT y OT en una misma red.

Sin embargo, la naturaleza accesible de PROFINET lo vuelve vulnerable a exposiciones en línea, enfatizando la necesidad de reforzar la ciberseguridad en las redes donde se implementa.

El documento "PROFINET Security Guideline" de PROFIBUS Internacional [24] y el documento sobre "Protocolos y seguridad de red en infraestructuras SCI" de INCIBE, proponen estrategias clave para proteger entornos industriales que emplean PROFINET [25] :

- Establecer protecciones contra errores y funcionamientos incorrectos, y gestionar incidentes mediante protocolos previamente definidos.
- Implementar controles para prevenir accesos no autorizados que podrían resultar en alteraciones de la red o actividades de espionaje.
- Utilizar estándares y equipos de seguridad que hayan sido rigurosamente probados y certificados, incluyendo cortafuegos, redes privadas virtuales (VPN) y sistemas de detección y prevención de intrusiones (IDS/IPS).
- Mejorar la infraestructura de red: Las redes planas, aunque simplifican la comunicación entre dispositivos y sistemas, también plantean desafíos para mantener

la red estable, disponible y segura. La segmentación de la red mediante VLANs, routers y cortafuegos es fundamental para reducir estos riesgos.

3.2.3 Distributed Network Protocol

El protocolo de red distribuida (DNP) fue creado por Westronic en la década de los 90 con el objetivo de lograr interoperabilidad entre dispositivos en una red de control distribuido perteneciente a la industria eléctrica. Su uso se extiende principalmente por Estados Unidos y Canadá.

Figura 16. Logo DNP3

Este protocolo tiene algunas características que lo hacen más robusto y eficiente que otros protocolos industriales como Modbus. Está compuesto por tres capas según el modelo OSI: capa de enlace, capa de transporte y capa de aplicación [26].

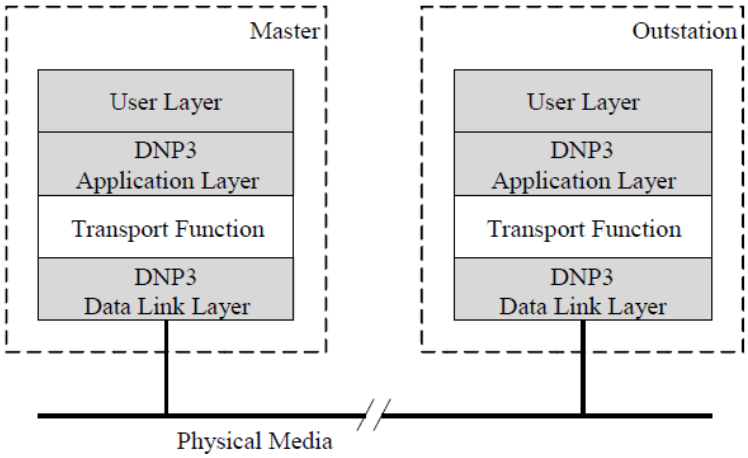


Figura 17. Pila de protocolos DNP3

Capa de enlace

La capa de enlace de datos actúa como puente entre la capa de transporte y la interfaz física. Los datos se transforman en paquetes llamados tramas, con un tamaño máximo de 292 bytes cada una.

Esta capa desempeña dos roles fundamentales. Primero, facilita el transporte de datos en ambas direcciones a lo largo del canal de comunicación, llevando la información desde la capa de aplicación hasta el dispositivo de destino. En segundo lugar, se encarga de aspectos cruciales como la sincronización de las tramas de datos, el control del flujo para evitar sobrecargas, el control de errores para garantizar la integridad de los datos y proporcionar información sobre el estado de la conexión.

Cada trama finaliza con un campo llamado CRC (Cyclic Redundancy Check), un código de 16 bits que sirve para detectar cualquier posible error en la transmisión de datos. Este mecanismo de verificación es esencial para asegurar la fiabilidad de la comunicación y mantener la integridad de los datos transmitidos a través del enlace de datos.

Capa de transporte

En este nivel de comunicación, los mensajes intercambiados se conocen como segmentos, con un límite máximo de tamaño de 149 bytes cada uno. Sin embargo, en ocasiones, los fragmentos de datos generados en la capa de aplicación pueden exceder este límite. Para resolver esto, la capa de transporte divide estos fragmentos en unidades más pequeñas, del tamaño adecuado para la transmisión a través de la capa de enlace. Posteriormente, agrega la información de encabezado correspondiente a nivel de transporte antes de enviarlos. En el extremo receptor, estos segmentos se vuelven a ensamblar para reconstruir los datos originales. Este proceso garantiza una comunicación fluida y eficiente entre las diferentes capas del sistema de comunicación.

Capa de aplicación

En el protocolo DNP3, un fragmento en la capa de aplicación representa un conjunto de datos que se transmiten entre un dispositivo maestro y una estación remota. Estos fragmentos contienen información esencial para la comunicación, como solicitudes de datos o respuestas a esas solicitudes. Cada fragmento contiene un código de función que indica cómo el receptor debe interpretar la información recibida.

El tamaño máximo de un fragmento en DNP3 es de 1014 bytes. Además, cada fragmento comienza con una cabecera que contiene detalles de control de mensajes, facilitando la correcta interpretación y procesamiento de la información por parte del receptor. Es importante destacar que, en el caso de los fragmentos de respuesta, se agrega un campo adicional denominado "indicaciones internas". Este campo proporciona información adicional sobre el estado interno del dispositivo, pero no está presente en los fragmentos de solicitud.

Message type	Code	Name	Brief description
Confirmation	0 0x00	CONFIRM	Confirm Function Code: Master sends this to an outstation to confirm the receipt of an Application Layer fragment. Reference: 4.4.1
Request	1 0x01	READ	Read Function Code: Outstation shall return the data specified by the objects in the request. Reference: 4.4.2
Request	2 0x02	WRITE	Write Function Code: Outstation shall store the data specified by the objects in the request. Reference: 4.4.3
Request	3 0x03	SELECT	Select Function Code: Outstation shall select (or arm) the output points specified by the objects in the request in preparation for a subsequent operate command. The outstation shall not activate the outputs until a request with a matching Operate function code is received. Reference: 4.4.4
Request	4 0x04	OPERATE	Operate Function Code: Outstation shall activate the output points selected (or armed) by a previous select function code command. Reference: 4.4.4
Request	5 0x05	DIRECT_OPERATE	Direct Operate Function Code: Outstation shall immediately actuate the output points specified by the objects in the request. A prior matching select command is not required. Reference: 4.4.5
Request	6 0x06	DIRECT_OPERATE_NR	Direct Operate—No Response Function Code: Same as function code 5 but outstation shall not send a response. Reference: 4.4.5
Request	7 0x07	IMMED_FREEZE	Immediate Freeze Function Code: Outstation shall copy the point data values specified by the objects in the request to a separate freeze (or holding) buffer (or register). Reference: 4.4.6

Figura 18. Códigos de función DNP3

La realización de auditorías y simulaciones sobre este protocolo excede los objetivos establecidos para este trabajo. En cambio, a continuación, se mencionan algunos métodos de seguridad que se han incorporado en este protocolo.

En cuanto a seguridad, el protocolo DNP3 se orienta hacia la maximización de la disponibilidad del sistema, aunque puede reducir la confidencialidad e integridad de los datos.

La capa de enlace, por ejemplo, implementa un mecanismo de detección de errores a través de CRC. Esto no es una medida de seguridad absoluta, ya que una inyección de datos falsos podría modificar el CRC de la trama.

Desde el año 2020, la capa de aplicación ha integrado un estándar de autenticación segura conocido como DNP3 security versión 6 [27]. Este estándar proporciona autenticación y confidencialidad a nivel de aplicación, garantizando así una comunicación segura de extremo a extremo.

La autenticación segura (DNP3-SA) se introduce como una capa adicional entre las capas de aplicación y transporte del protocolo DNP3. Esta capa utiliza códigos de autenticación de

mensajes (MAC) para garantizar una comunicación segura.

Además, el protocolo de gestión de autorizaciones (AMP) se utiliza en conjunto con la capa de aplicación de DNP3 y DNP3-SA para gestionar qué dispositivos están autorizados para autenticarse.

Estos estándares de seguridad abordan varios problemas potenciales, incluyendo ataques de suplantación de identidad, escucha de mensajes durante la comunicación y ataques de inyección de tráfico, que implican la transmisión maliciosa o fraudulenta de datos válidos.

4 ESTUDIO DE CIBERATAQUES Y AMENAZAS

En este capítulo, se explora la ciberseguridad desde la perspectiva del atacante, desentrañando las fases que atraviesa para realizar un ataque con éxito. A su vez, se identifican y analizan vulnerabilidades y puntos de ataque comunes en los sistemas de control industrial. Comprender la metodología del atacante es esencial para resguardar los activos críticos y añadir una capa adicional de protección a aquellos que sean más vulnerables ante un potencial ataque.

4.1 Ciclo de vida de un ciberataque

En la literatura sobre ciberseguridad industrial, hay diversas formas de clasificar las fases realizadas durante un ataque. Dos de las más mencionadas son la clasificación del Certified Ethical Hacker (CEH), también usada en el ámbito de la ciberseguridad IT [28], y la "Cyber Kill Chain", desarrollada por Lockheed Martin, una empresa de seguridad y defensa [29].

En la siguiente imagen se muestran las etapas en las que distribuyen los ataques ambas clasificaciones y después se describe el objetivo de cada una de las cinco fases definidas por el CEH.

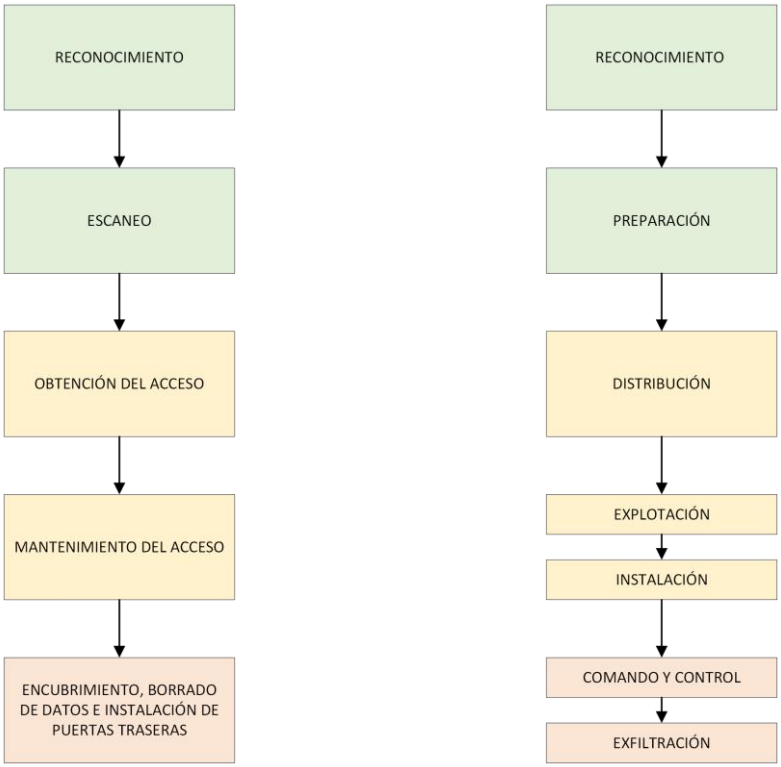


Figura 19. Fases de un ciberataque CEH (izquierda) vs "Ciber Kill Chain" (derecha)

En el contexto del CEH (Certified Ethical-Hacker) del British Council se describen las siguientes fases:

1) Reconocimiento

   La etapa de reconocimiento, también conocida como fase de preparación, es la primera etapa de un ciberataque en la cual un atacante busca recopilar datos y obtener información relevante del objetivo deseado que pueda ser utilizada en fases posteriores del ataque. El objetivo de esta fase es revelar

debilidades e identificar información susceptible para explotar vulnerabilidades. En los sistemas de control industriales la fase de reconocimiento también incluye la investigación de vulnerabilidades técnicas y características de los sistemas de control y el análisis de la susceptibilidad a ataques del proceso y el modelo operativo. [30]

2) Escaneo

El escaneo es el paso previo que precede al ataque real y consiste en adquirir información detallada basada en los datos obtenidos en la fase anterior, el reconocimiento.

En esta fase, también conocida como enumeración, se obtiene información sobre posibles puntos de entrada, cuentas de usuario válidas en el sistema, y mecanismos de seguridad implementados, como firewalls, sistemas de detección de intrusiones y políticas de seguridad.

3) Obtención de Acceso

En esta fase, el hacker intenta explotar las vulnerabilidades encontradas en la fase de enumeración para ganar acceso al sistema o red objetivo. Para llevar a cabo su propósito, el hacker realiza ataques de fuerza bruta como los ataques de contraseña, ataques de inyección, usa puertos y servicios abiertos y explota fallos de configuración de los sistemas.

4) Mantenimiento del Acceso

Cuando el hacker accede al sistema objetivo comienza una de las fases más importantes de un ataque que consiste en mantener el acceso obtenido de forma prolongada sin detectarse. Cuando el hacker obtiene el acceso crea mecanismos de persistencia como la instalación de troyanos[10] o modificación de la configuración del sistema.

Si el hacker ha penetrado el sistema mediante contraseñas, debe asegurarse de mantenerlas, ya sea realizando un cambio de estas o la escalada de privilegios para crear nuevas cuentas de usuario.

5) Encubrimiento, Borrado de Rastros e Instalación de Puertas Traseras

Es fundamental que el atacante se asegure de que nadie tenga conocimiento de sus actividades maliciosas no autorizadas en los sistemas de control. Para lograrlo, pueden utilizar rootkits [11]con el objetivo de encubrir las huellas dejadas por sus acciones. Además, el atacante podría eliminar o modificar archivos de registro para ocultar eventos perjudiciales o inusuales que pudieran generar sospechas.

4.2 Vectores de Ataques y Vulnerabilidades

Un vector de ataque se define como una vía o método específico que los atacantes emplean para comprometer un sistema o proceso [31]. A continuación, se detallan algunos de los puntos críticos y vulnerabilidades identificados en sistemas de control industrial, destacando los vectores de ataques más comunes. En este contexto, es común hacer referencia a los sistemas, dispositivos o activos críticos susceptibles de ser atacados como “target” u “objetivo” [28]

[10] Un troyano, también conocido como caballo de Troya, es un tipo de archivo informático malicioso que simula ser legítimo e inofensivo.
[11] Un rootkit es un software malicioso que se oculta en un ordenador o en otro software y que permite a los atacantes acceder y controlar el sistema de forma remota sin ser detectados.

- **Manipulación del medio físico**: este vector implica la manipulación de sensores y actuadores en entornos industriales para enviar información falsa o comandos maliciosos.
- **Malware:** software malicioso diseñado para infiltrarse en sistemas de control industrial. Los objetivos del malware pueden incluir el robo de información confidencial, la interrupción de la operación de los sistemas o la provocación de daños físicos a la infraestructura industrial.
- **Manipulación de comunicaciones**: este vector implica interferir en las comunicaciones entre dispositivos industriales y sistemas de control. Los atacantes buscan interceptar o modificar los datos transmitidos, lo que les permite obtener información confidencial o incluso tomar el control de los sistemas industriales.
- **Escalado de privilegios**: en este tipo de ataque, los atacantes buscan obtener acceso a niveles de autorización más altos de lo que se les permite inicialmente. Al escalar sus privilegios, los atacantes pueden obtener un mayor control sobre el sistema comprometido, lo que les permite realizar acciones maliciosas adicionales o acceder a información confidencial.
- **Inyección de código**: este vector implica la inserción de código malicioso con el objetivo de alterar su funcionamiento o realizar acciones no autorizadas.
- **Denegación de servicio**: los atacantes inundan un sistema o red con tráfico malicioso con la intención de impedir el acceso a usuarios legítimos. La denegación de servicio puede causar interrupciones significativas en los procesos industriales, lo que puede resultar en pérdidas económicas y de producción considerablemente graves.
- **Compromiso de credenciales**: Permite a un atacante obtener credenciales para funciones del dispositivo, generalmente debido a almacenamiento o transmisión insegura.
- **Phishing:** técnica de ingeniería social que implica enviar correos electrónicos o mensajes fraudulentos para engañar a los usuarios y obtener información confidencial o acceso no autorizado a sistemas industriales. Los ataques de phishing son una preocupación importante en entornos industriales debido a la vulnerabilidad de los empleados a las tácticas de manipulación psicológica.
- **Ingeniería social**: se refiere a la manipulación psicológica de las personas con el objetivo de obtener información confidencial o persuadirlas para que realicen acciones que beneficien al atacante. Los ataques de ingeniería social pueden ser extremadamente efectivos en entornos industriales donde la concienciación sobre seguridad cibernética puede ser menor, lo que los convierte en una preocupación significativa en este entorno.

En el entorno industrial, numerosos dispositivos están expuestos a los vectores de ataque mencionados. En el informe titulado "OT:ICEFALL" elaborado por Verdere Labs [32] se reporta un conjunto de 56 vulnerabilidades que afectan a dispositivos de 10 proveedores de tecnología operativa. Se incluyen proveedores reconocidos en la industria como Emerson, Siemens, Omron o Honeywell.

Las vulnerabilidades encontradas se clasifican en cuatro categorías principales: protocolos de ingeniería inseguros, criptografía débil o ausencia de medidas de autenticación, actualizaciones de firmware inseguras y ejecución remota de código a través de funcionalidades nativas.

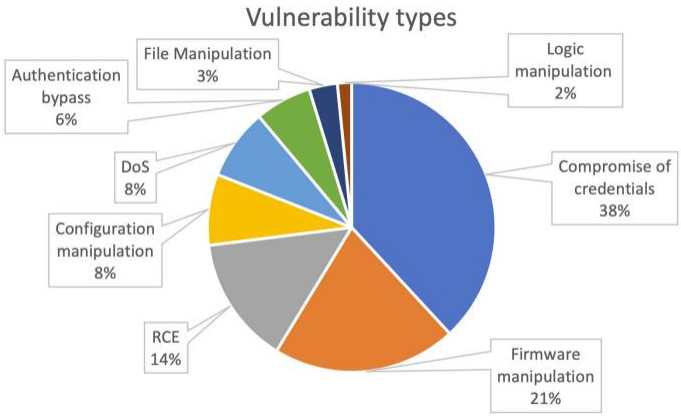


Figure 3 – Vulnerability Types in OT:ICEFALL

Figura 20. Tipos de vulnerabilidades según el informe OT:ICEFALL [32]

Por tanto, es crucial examinar los vectores de ataque a los que un sistema de control podría exponerse, para implementar las medidas de seguridad pertinentes y reducir los posibles daños por ciberataques. En el próximo capítulo de este estudio, se examinan algunas de las medidas de seguridad fundamentales para resguardar tanto los sistemas como la producción de las amenazas y ataques mencionados.

5 MEDIDAS DE SEGURIDAD

En esta sección se detallan diversas medidas destinadas a salvaguardar los sistemas de control industrial. Se incluye la aplicación de normativas específicas en el campo de la ciberseguridad y se enfatiza la importancia de realizar auditorías de seguridad periódicas, que permiten identificar posibles vulnerabilidades y evaluar la efectividad de las medidas de protección existentes.

Otro aspecto clave abordado en esta sección es la implementación de sistemas de detección y prevención de ataques. Estos sistemas, que van desde firewalls avanzados hasta soluciones de análisis de comportamiento, son fundamentales para identificar y mitigar amenazas en tiempo real.

5.1 Estándares y Buenas Prácticas

Actualmente, gobiernos e industrias imponen varias normativas, directrices y regulaciones de ciberseguridad, abarcando desde documentos de "buenas prácticas" hasta requisitos estrictos con sanciones y multas para quienes incumplan la normativa. Aunque el número de directrices en comparación con el ámbito de la tecnología de la información es menor, se observa un aumento significativo en las normativas y regulaciones específicas de ciberseguridad industrial.

En Europa, se aplican normativas y directrices clave como la EU M/490 y la SGCG, que proporcionan orientación para energía moderna, junto con una amplia gama de publicaciones de la Agencia de la Unión Europea para la Seguridad de Redes y de la Información (ENISA). Por otro lado, en Estados Unidos se siguen las recomendaciones generales del Instituto Nacional de Normas y Tecnología (NIST) en la Publicación Especial 800-82, además de normativas específicas para las infraestructuras críticas, como las Normas de Fiabilidad de Protección de Infraestructuras Críticas (CIP) de NERC y los Estándares Antiterroristas de Instalaciones de Instalaciones Químicas (CFATS) del DHS. A nivel internacional, la serie de normas ISO/IEC 27000 desempeña un papel fundamental en la seguridad de la información [33].

La norma más destacada en seguridad industrial es la ISA 62443 (antes conocida como ISA 99), desarrollada por la Sociedad Internacional de Automatización. Esta norma se centra en garantizar la seguridad de los sistemas de automatización y control industrial, siendo aplicable a cualquier organización o industria que utilice este tipo de sistemas. Además, la ISA 62443 se alinea con la norma internacional IEC 62443 y está siendo revisada y reestructurada para ser aceptada por la Organización Internacional de Normalización (ISO) como ISO 62443.

En este capítulo, se busca presentar algunas de las normas relevantes, con especial énfasis en la IEC 62443.

5.1.1 ISO/IEC 27000

El conjunto de normas ISO/IEC 27000 es la norma de referencia para la seguridad de la información y la gestión de riesgos. Aunque estas normas estén especializadas en los sistemas de la información pueden servir para orientar y mejorar la seguridad de los sistemas de control industrial [34].

A continuación, se nombran algunas normas de este conjunto que pueden ser útiles para asegurar los sistemas industriales:

- ISO/IEC 27001: establece un marco para gestionar la seguridad de la información aplicado a cualquier organización, incluidas las industriales.
- ISO/IEC 27002: ofrece controles y buenas prácticas que pueden implementar las organizaciones para mejorar la seguridad de la información. Aunque no es específica

para sistemas de control industrial, muchas de las recomendaciones son aplicables a este contexto.

- ISO/IEC 27019: ofrece directrices específicas para la seguridad de la información en sistemas de control industrial del sector energético.
- ISO/IEC TR 27008: incluye directrices para la auditoría de seguridad de la información, aplicables en auditorias para sistemas de control industrial.

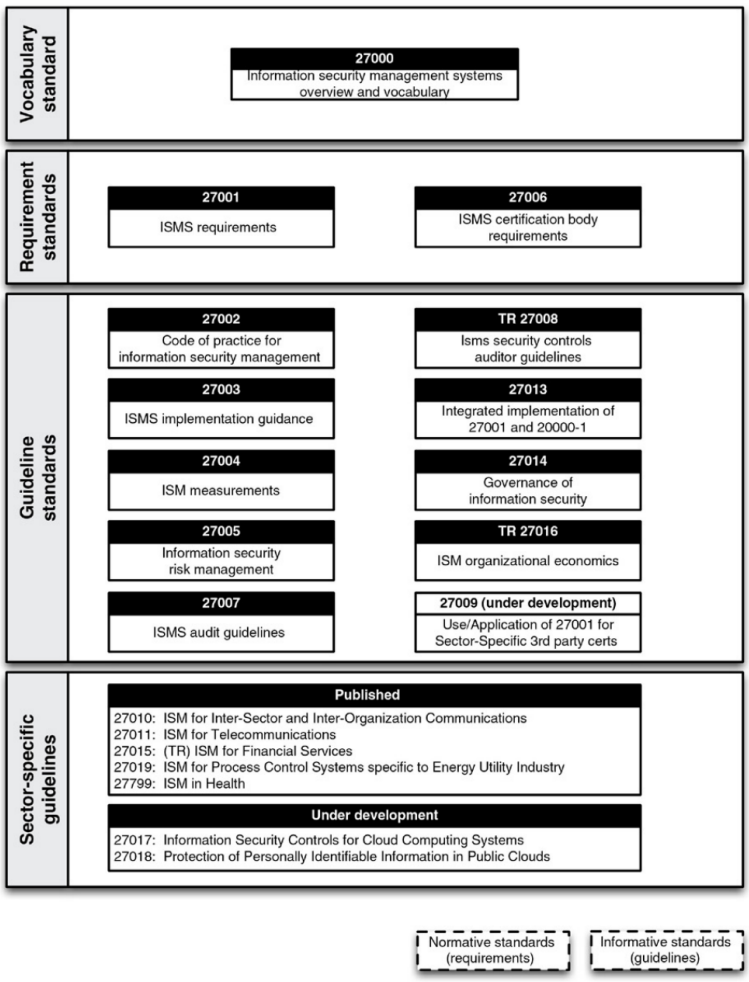


Figura 21. Estructura normativa ISO 27000 [33]

5.1.2 NIST SP 800-82

El documento técnico NIST SP 800-82 ofrece una guía detallada para implementar un entorno seguro en tecnologías de la operación (OT), abarcando sistemas de control industrial como SCADA y distribuidos, usados ampliamente en entornos industriales e infraestructuras críticas. La norma destaca cuatro aspectos fundamentales:

- Evaluación del riesgo: se recomienda encarecidamente a las organizaciones definir un método para evaluar la probabilidad de eventos de ciberseguridad, considerando varios factores como la intención y la capacidad de adversarios e históricos de datos [35].
- Respuesta al riesgo: la norma destaca que en entornos de tecnología operativa (OT), las acciones para hacer frente a los riesgos pueden estar restringidas por requisitos del sistema, efectos en la operación o cumplimiento normativo. Se sugiere considerar

estrategias como compartir el riesgo mediante acuerdos de colaboración entre organizaciones.

- Monitorización del riesgo: se aconseja establecer una frecuencia de monitoreo de las actividades cibernéticas en función del riesgo detectado.
- Seguridad física y cibernética: se resalta la importancia de poseer una estrategia de "defensa en profundidad" combinando técnicas de seguridad física y cibernética para proteger el sistema en su conjunto [35].

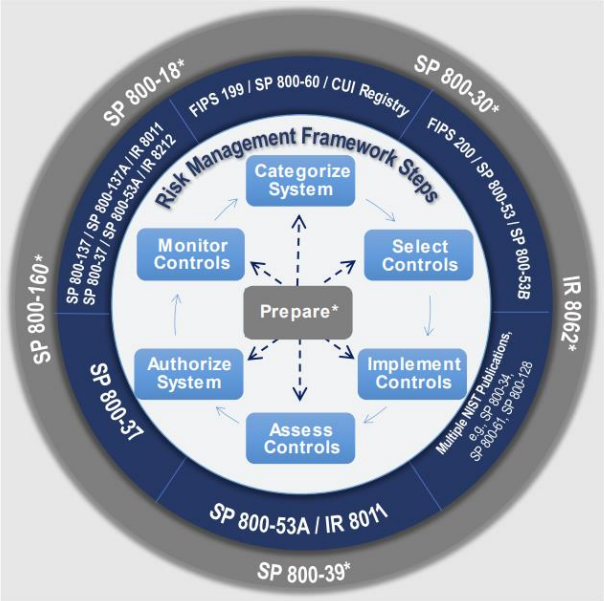


Figura 22. Estructura normativa NIST [36]

En resumen, la normativa NIST SP 800-82 proporciona una orientación integral sobre como evaluar, responder y monitorear los riesgos de seguridad en entornos industriales, enfocándose en los sistemas críticos de control industrial [35].

5.1.3 NERC CIP

La Corporación de Confiabilidad Eléctrica de América del Norte, establece un conjunto de estándares llamados NERC-CIP para la Protección de Infraestructuras Críticas. Estos estándares están diseñados para los sistemas de transmisión de energía de las empresas de servicios públicos [37]. Hasta la fecha, NERC-CIP ha establecido más de 80 estándares, de los cuales 11 son de obligado cumplimiento para las entidades de EE. UU y Canadá.

Esta normativa representa un marco integral para fortalecer la seguridad cibernética en el sector energético. Además de compartir ciertos elementos con la norma IEC 62443, también aborda aspectos como planes de recuperación, capacitación del personal y gestión de visitantes [38]. Luego, se describe cada estándar en la tabla adjunta, mientras que la lista completa se puede consultar en el siguiente enlace de referencia [39].

Estándar CIP	**Título**
CIP-002-5. 1a	Seguridad cibernética – Categorización del sistema cibernético BES
CIP-003-6	Ciberseguridad: controles de gestión de seguridad

CIP-005-5	Ciberseguridad: perímetro (s) de seguridad electrónica
CIP-006-6	Ciberseguridad: seguridad física de los sistemas cibernéticos de BES
CIP-007-6	Ciberseguridad: administración de seguridad del sistema
CIP-008-5	Ciberseguridad: informe de incidentes y planificación de respuesta
CIP-009-6	Ciberseguridad: planes de recuperación para Sistemas Cibernéticos BES

Tabla 1. Partes estándar CIP [38]

5.1.4 IEC-62443

Es un conjunto internacional de estándares que abordan la ciberseguridad para la tecnología operativa en sistemas de automatización y control. Su propósito es asegurar los sistemas de automatización y control industrial (IACS) a lo largo de su ciclo de vida [40]. La norma comprende nueve estándares, informes técnicos (TR) y especificaciones técnicas (TS). Los estándares se organizan en cuatro partes: General, Políticas y Procedimientos, Sistema y Componentes [41].

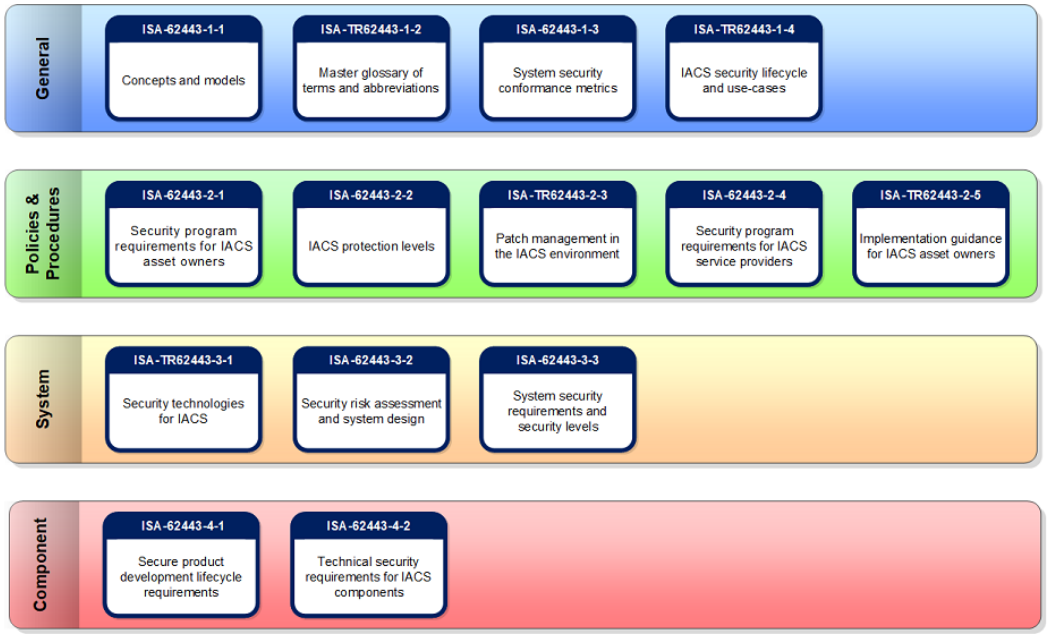


Figura 23. Estructura normativa IEC-62443 [41]

5.1.4.1 Parte 1: General

La primera de la norma ISA 62443 (ISA 62443-1-x) se enfoca en establecer una base sólida de términos estandarizados y referencias en el ámbito de la seguridad de sistemas de control industrial. Su principal objetivo es garantizar una comprensión común y unificada de los conceptos básicos, lo cual sirve de referencia para los otros grupos relacionados [33].

Actualmente, se están desarrollando activamente cuatro documentos dentro de este grupo, entre ellos, un glosario principal (62443-1-2) y definiciones sobre el ciclo de vida de seguridad de los sistemas de control industrial (62443-1-4). Uno de los

aspectos más interesantes es el documento 62443-1-3, que establece métricas de conformidad útiles para evaluar el cumplimiento de prácticas de seguridad en estos sistemas.

5.1.4.2 Parte 2: Políticas y Procedimientos

En la parte dos de la norma ISA 62443 (ISA 62443-2-x) se describen las políticas y procedimientos necesarios para establecer medidas efectivas de seguridad para Sistemas de Control Industrial. Dentro de este grupo se encuentra el documento 62443-2-1, que detalla los requisitos necesarios para un sistema de gestión de seguridad. El documento 62443-2-3 aborda la gestión de parches dentro de arquitecturas industriales y el documento 62443-2-4 proporciona requisitos para la certificación de proveedores de sistemas de control industrial [33].

5.1.4.3 Parte 3: Sistema

La parte tres de la norma ISA 62443 (ISA 62443-3-x) estudia las tecnologías relacionadas con la ciberseguridad. Los documentos incluidos en esta norma describen las tecnologías disponibles, los métodos de evaluación y los requisitos de seguridad.

El documento 62443-3 proporciona recomendaciones sobre la estructuración de las redes de comunicación y medidas para evaluar los riesgos asociados. Por otro lado, el documento 62443-3-3 actúa como un catálogo de controles de seguridad específicos para los Sistemas de Control Industrial, con un esquema similar a las normas ISO 27002 y NIST 800-53.

5.1.4.4 Parte 4: Componentes

El Grupo 4 de la norma ISA 62443 (ISA 62443-4-x) se enfoca en el desarrollo seguro de componentes para Sistemas de Control Industrial (SCI). Establece requisitos detallados para implementar un Ciclo de Desarrollo Seguro (SDLC) específico para estos componentes. Esto abarca desde el diseño y la planificación hasta el desarrollo del código, la revisión de vulnerabilidades y las pruebas a nivel de componente [33].

La norma ISA 62443 representa un avance fundamental en la seguridad de los sistemas de control industrial a nivel mundial. Al abordar aspectos clave como términos estandarizados, políticas y procedimientos, tecnologías de sistemas y desarrollo de componentes seguros, esta norma proporciona un marco integral para salvaguardar los sistemas de automatización y control industrial a lo largo de su ciclo de vida. Su importancia radica en establecer una comprensión común, implementar medidas efectivas de seguridad y promover mejores prácticas en la industria, lo que contribuye significativamente a la protección de infraestructuras críticas y la prevención de ciberataques en entornos industriales.

5.2 Securización de zonas

Cuando se diseña una red OT, es esencial adoptar un enfoque integral que garantice la protección y confiabilidad de los sistemas en entornos industriales. No se trata solo de implementar medidas de seguridad, sino de optimizar la eficacia y el rendimiento de la red en su conjunto [42].

Un elemento clave para conseguir una red industrial eficiente y segura es la segmentación de la red. La segmentación de la red OT consiste en dividirla en segmentos más pequeños y aislados entre sí, para mejorar el flujo de tráfico y evitar que se propague una vulnerabilidad a la red [43]

La segmentación de redes ofrece ventajas en seguridad y cumple con los requisitos del estándar

ISA/IEC 62443. Una de estas ventajas es un mayor control sobre el acceso a los recursos. Al limitar el acceso solo a los usuarios o dispositivos que realmente necesitan interactuar con una determinada parte de la red, se reduce la superficie de ataque y se disminuyen las posibilidades de intrusiones no autorizadas.

La normativa IEC-62443, mencionada en el capítulo 0 establece las bases para la segmentación en el apartado IEC-62443-3-2, titulado "Estándar para la evaluación de riesgos de seguridad y el diseño de sistemas para IACS". Este estándar introduce los conceptos de *zonas* y *conductos*.

En este contexto, las *zonas de seguridad* se definen como "agrupaciones de activos físicos o lógicos que comparten requisitos de seguridad comunes y tienen límites claramente definidos, ya sea físicamente o de manera lógica". Los enlaces que conectan estas zonas se denominan *conductos* y deben incluir medidas de seguridad para controlar el acceso, resistir ataques de denegación de servicio, prevenir la propagación de otros tipos de ataques, actuar como una barrera de protección para otros sistemas en la red y garantizar la integridad y confidencialidad de las comunicaciones [44]

La norma IEC 62264 también sugiere la aplicación de un modelo particular denominado Modelo de Purdue para la segmentación de las redes industriales. Este modelo divide el sistema industrial en zonas de seguridad y las conecta mediante conductos, los cuales restringen el flujo de información entre ellas mediante el uso de firewalls. Si la seguridad de la red se compromete, esta disposición minimiza la superficie expuesta.

El modelo de Purdue divide la red en cinco niveles principales insertando una barrera entre la red IT y el entorno OT. El modelo sigue el siguiente esquema [45]:

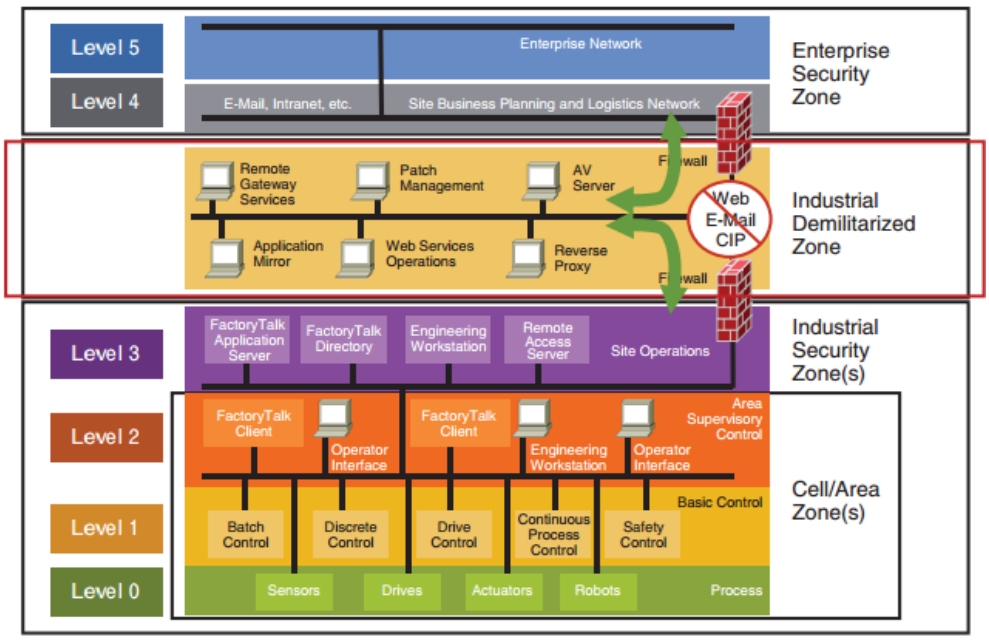


Figura 24. Modelo de Purdue [17]

- **Nivel 0 (Nivel de Proceso)**: este nivel incluye los componentes físicos que realizan el proceso. Está compuesto por sensores y actuadores como motores, bombas, válvulas, etc. Estos dispositivos generan los datos de la planta que posteriormente se procesarán y monitorizarán.
- **Nivel 1 (Nivel de Control)**: esta capa posee las funciones de detección y control del proceso físico, realizadas por equipos de control como los PLC (Controladores Lógico-Programables) y los RTU (Unidades de Telemetría Remota), entre otros. El propósito de estos dispositivos es controlar las variables del proceso indicando instrucciones como, por ejemplo: accionar actuadores, arrancar motores, abrir válvulas, etc.
- **Nivel 2 (Nivel de Supervisión y Control)**: este nivel tiene la función de supervisar el entorno

de ejecución y el funcionamiento de un área dentro de una instalación de producción. Incluye las interfaces hombre-máquina (HMI), los SCADA y los sistemas distribuidos (DCS).

- **Nivel 3 (Nivel de Control de Operaciones)**: el objetivo de los componentes involucrados en este nivel es el de gestionar el flujo para lograr la producción deseada. Incluyen sistemas de gestión de lotes o MES, bases de datos y sistemas de gestión de calidad.
- **Zona Industrial Desmilitarizada (DMZ)**: esta zona permite la conexión de redes distintas conforme a los requisitos de seguridad. Es una capa de intercambio de información entre los sistemas empresariales (IT), ubicados en los niveles cuatro y cinco, y los sistemas de producción, nivel tres e inferiores. En esta zona se encuentran los servidores de automatización, los servidores de supervisión y control y los servidores de bases de datos.

  En caso de que las redes IT de la empresa sufran un ciberataque, se procede al cierre de la DMZ para contener la amenaza y salvaguardar el sistema OT. Esta acción permite que la producción continúe sin interrupciones significativas.
- **Nivel 4 (Nivel de Planificación Comercial y Logística)**: este nivel alberga todos los sistemas de tecnología de la información (IT) que están detrás de los procesos de producción en una planta industrial. Estos sistemas tienen la función de monitorizar tiempos, unidades producidas y otros datos con fines corporativos y comerciales.
- **Nivel 5 (Nivel de Red Empresarial)**: este nivel está ubicado a nivel corporativo y es común que abarque múltiples instalaciones y plantas. Se encargan de recolectar los datos de cada subsistema y utilizar estos datos para informar sobre el estado de producción, inventario y demanda. Los sistemas encargados de este nivel son los ERP (Enterprise Resource Planning).

La segmentación en redes OT es una estrategia que permite dividir las redes que forman parte del sistema de control en diferentes zonas de seguridad conectadas mediante conductos que implementan medidas para controlar el flujo entre zonas. El Modelo de Purdue, recomendado en la norma IEC- 62443, implementa esta filosofía para limitar la capacidad de los atacantes para realizar ataques de movimiento lateral, que les permita comprometer la red en su totalidad. Además, la segmentación de redes mejora la eficiencia de la red al poder priorizar en tráfico de la red y tener mayor control sobre cada una de las zonas en las que se divide el sistema.

5.3 Auditoria y Pentesting

Las auditorias y el pentesting son dos herramientas fundamentales para asegurar la integridad, confidencialidad y disponibilidad de los sistemas de control industrial.

En auditoria se llevan a cabo procesos de evaluación exhaustiva de los sistemas, procesos y normativa de seguridad. Esta evaluación permite identificar las vulnerabilidades a las que se expone el sistema, asegurar que los dispositivos y redes cumplen con la normativa aplicable a la seguridad en entornos industriales y obtener una visión completa de la situación de la seguridad en el sistema [46].

Las pruebas de penetración (pentesting) se centran en realizar ataques reales controlados para identificar y explotar una vulnerabilidad concreta. Mediante estas pruebas se pretende comprobar la resistencia del sistema ante ataques para integrar nuevas técnicas y mejoras en las partes más deficientes y vulnerables de la industria [47].

A continuación, se describen las fases recorridas durante el proceso de pentesting:

1. Planificación
    - Definición del alcance: En esta etapa inicial, se define de forma clara y concisa el alcance del proceso de pentesting. Esto implica la descripción detallada de los dispositivos, redes y protocolos que serán evaluados. Esta fase es fundamental para establecer límites precisos durante el proceso, lo que ayuda a prevenir riesgos en la

producción y a mejorar la eficiencia de este.

- Análisis de riesgos: En esta etapa se busca minimizar cualquier impacto negativo y asegurar la continuidad de los sistemas industriales durante el proceso de pentesting. Esto incluye la formación y la comunicación anticipada sobre las pruebas al personal requerido, la definición de procedimientos de respuesta, la limitación del alcance de las pruebas y la realización de pruebas en entornos controlados. Estas acciones buscan minimizar cualquier impacto negativo y asegurar la continuidad de los sistemas industriales durante el proceso de pentesting.

2. Evaluación de Vulnerabilidades
    - Reconocimiento: Recopilación de información relevante sobre el sistema de control objetivo.
    - Escaneo de vulnerabilidades: Se utilizan herramientas para explorar y analizar el sistema en busca de posibles puntos débiles. Esta etapa puede incluir la búsqueda de puertos abiertos, servicios expuestos, configuraciones incorrectas o desactualizadas, y otras debilidades que podrían ser aprovechadas por un atacante.
3. Explotación: Se llevan a cabo simulaciones de diversos tipos de ataques dirigidos a los sistemas de control industrial en el mundo real. Esto ayuda a evaluar la capacidad del sistema para resistir diferentes tipos de amenazas e identificar posibles puntos débiles que deben ser fortalecidos.
4. Documentación y Análisis de Resultados: Se elabora un informe detallado documentando los hallazgos obtenidos. Incluye información sobre las vulnerabilidades identificadas, su gravedad y se proponen medidas de seguridad para mitigar el riesgo.

Figura 25. Fases pentesting [48]

Además, existen distintos enfoques de *pentesting* diferenciados por el alcance que cubren: caja negra, caja gris y caja blanca [49].

- Caja negra o *black box*: Se compromete el sistema sin previo conocimiento interno. Esto permite detectar errores y fallos de seguridad que puedan ser explotados por un atacante que realice ataques externos, sin acceso al sistema.
- Caja gris o *grey box*: Se proporciona cierta información confidencial sobre el sistema, como la arquitectura del sistema o formas de acceso. Esto permite al *pentester* tener un conocimiento parcial del sistema, lo que puede facilitar la identificación de vulnerabilidades.
- Caja blanca o *whithe box*: Se proporciona toda la información confidencial del sistema, diseño

de la arquitectura del sistema, credenciales de acceso, información de cada dispositivo, etc. Este enfoque brinda al *pentester* un conocimiento completo del sistema, lo que facilita la identificación exhaustiva de vulnerabilidades y riesgos de seguridad.

Tanto las auditorías como las pruebas de penetración (pentesting) desempeñan roles cruciales en la protección de los sistemas de control industrial. Mientras que las auditorías proporcionan una evaluación exhaustiva de los sistemas, procesos y normativas de seguridad, las pruebas de penetración se centran en simular ataques reales para identificar y explotar vulnerabilidades específicas. Ambas prácticas, complementarias entre sí, contribuyen a garantizar la integridad, confidencialidad y disponibilidad de los sistemas industriales. Además, el enfoque de pentesting, ya sea caja negra, caja gris o caja blanca, ofrece flexibilidad para adaptarse a las necesidades de seguridad y proporciona una visión detallada de las vulnerabilidades y riesgos, permitiendo así la implementación de medidas de seguridad efectivas para proteger los sistemas críticos de la industria.

5.4 Sistemas de detección y prevención: IDS, IPS y SIEM

Para mitigar posibles ataques e intrusiones en los sistemas industriales, se han desarrollado técnicas y sistemas especializados que detectan y previenen de manera efectiva accesos no autorizados, anomalías y actividades ilegítimas. Entre estas soluciones, se destacan los Sistemas de Detección de Intrusiones (IDS), concebidos inicialmente para su aplicación en entornos de tecnologías de la información (IT), los cuales son adaptados para analizar el tráfico de las redes industriales y detectar cualquier actividad sospechosa. Con el tiempo, se introdujeron los Sistemas de Prevención de Intrusiones (IPS) y los Sistemas de Información y Gestión de Eventos de Seguridad (SIEM), ampliando así las herramientas disponibles para preservar la integridad y disponibilidad de los sistemas industriales.

En este capítulo, se describen los dispositivos mencionados y se enumeran algunos de los softwares disponibles en el mercado que se pueden ser útiles en la industria.

Un IDS (Sistema de Detección de Intrusiones) es un sistema que monitorea el tráfico y los eventos de red para encontrar comportamientos anómalos que puedan indicar una intrusión. Estos sistemas son configurados con reglas y algoritmos para detectar actividades maliciosas en el sistema de control y generar alertas al operario o al administrador de seguridad de la planta [50].

En la Figura 26 se determina la posición que debe tomar el dispositivo IDS en la red de control industrial. Por lo general, el IDS se coloca en puntos clave de la red como puede ser la entrada o salida de datos hacia Internet o cerca de servidores críticos [51].

Los sistemas IPS (Sistema de Prevención de Intrusiones) son los encargados de reaccionar ante las intrusiones detectadas por los IDS. Estos toman medidas para mitigar el impacto de las actividades maliciosas detectadas como filtrado de paquetes, bloqueo de direcciones IP o modificaciones en tiempo real dentro del sistema de control para evitar que las intrusiones comprometan la integridad y disponibilidad del sistema.

Estos sistemas funcionan activamente por lo que debemos colocar los dispositivos en medio del tráfico. Por ello, la configuración de las reglas debe ser adecuada para que no se interrumpa el flujo de tráfico de la red de control y únicamente se bloqueen en caso de fallos de seguridad [50].

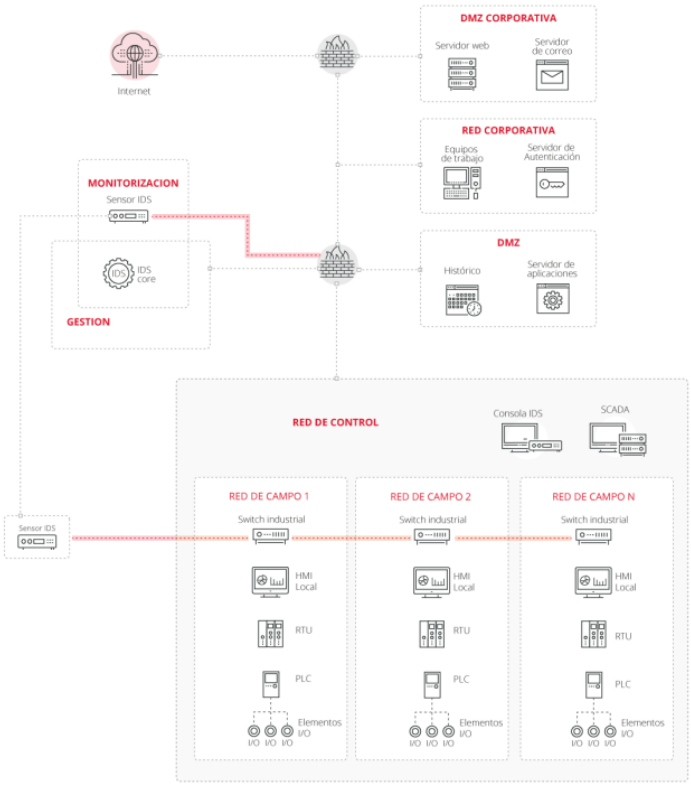


Figura 26. Sistema de Detección de Intrusiones en Sistema de Control Industrial [52]

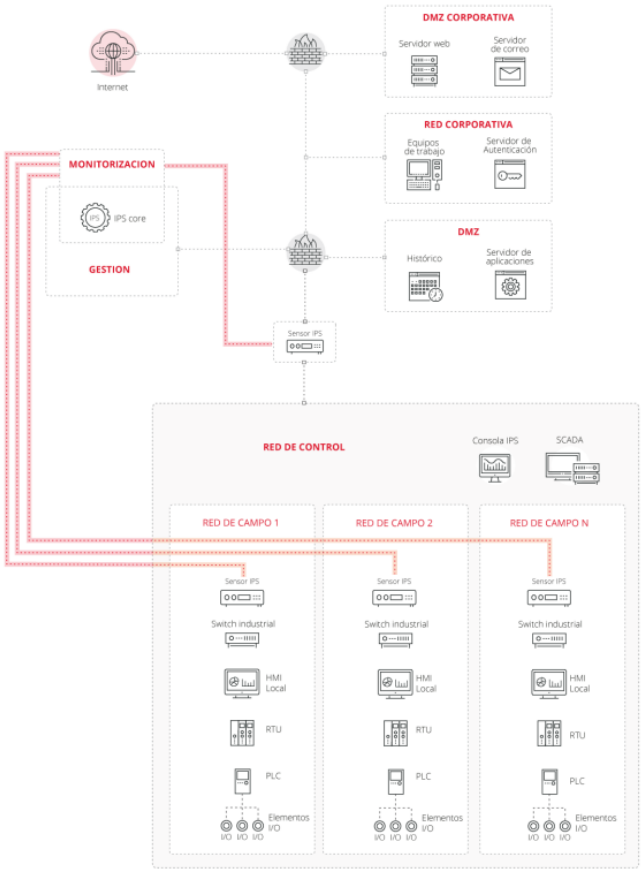


Figura 27. Figura 23. Sistema de Detección de Intrusiones en Sistema de Control Industrial [52]

La principal diferencia entre un IPS y un IDS radica en sus acciones. Un IDS puede detectar actividades maliciosas o inusuales y notificar a los administradores, pero no toma medidas directas para bloquearlas. Por otro lado, un IPS no solo detecta amenazas, sino que también desempeña acciones para prevenirlas o bloquearlas en tiempo real, como el bloqueo, rechazo, limitación o modificación del tráfico malicioso, brindando una capa adicional de protección proactiva para la seguridad de la red [47].

Un sistema SIEM recopila y correlaciona eventos de seguridad de diferentes fuentes para generar alertas. Estas fuentes incluyen información de dispositivos, registros de los sistemas IDS e IPS, registros y otros datos relacionados con la seguridad. Permite la supervisión integral de la seguridad además de detección de patrones y amenazas en tiempo real. También aportan la inteligencia necesaria para reducir falsos positivos.

El despliegue de un SIEM ofrece ventajas clave en la seguridad de los sistemas industriales. Permite la detección temprana de incidentes en tiempo real, permitiendo bloquear amenazas antes de causar daños. Facilita el análisis forense al almacenar eventos pasados para identificar el origen de incidentes. Centraliza la información de seguridad de la red y otros elementos. Ahorra recursos al recopilar datos de manera automática y centralizada. Además, identifica fácilmente anomalías en el comportamiento de los equipos, alertando sobre posibles problemas o incidentes en redes estables [53].

En el mercado se encuentran soluciones de código abierto como Snort[12] y Suricata[13] que funcionan tanto como Sistemas de Detección de Intrusiones (IDS) como Sistemas de Prevención de Intrusiones (IPS).

La adecuada configuración y uso de los IDS, IPS y SIEM permiten detectar posibles ataques y tomar medidas efectivas para mitigar sus efectos, protegiendo la producción y garantizando la disponibilidad siempre. Este enfoque es fundamental en la industria, como se ha subrayado en este trabajo.

[12] Snort - Network Intrusion Detection & Prevention System
[13] Home - Suricata

6 PENTESTING EN SISTEMAS DE CONTROL INDUSTRIAL

The quieter you come, the more you are able to hear.

-Ram Dass-

Como se ha descrito en apartados anteriores, las pruebas de penetración son una herramienta indispensable para garantizar la seguridad en los sistemas automatizados actuales. Estas pruebas permiten la detección de vulnerabilidades e identificación de posibles vectores de ataque en el sistema mediante la realización de pruebas que simulan un ataque real controlado. En el siguiente capítulo, se pretende replicar el proceso de pruebas de penetración en un sistema simulado y controlado utilizando las herramientas más populares en este campo.

6.1 Fase I. Planificación

La planificación es esencial en las pruebas de penetración, ya que define los objetivos y límites del proceso. En este estudio, la fase inicial asegura una evaluación precisa de la seguridad del protocolo Modbus en sistemas industriales, lo que permite identificar vulnerabilidades, evaluar riesgos y proponer medidas de protección adecuadas.

6.1.1 Definición del Alcance

Como se ha estudiado en el capítulo 3.2.1, Modbus es uno de los estándares más utilizados en la comunicación industrial y en infraestructuras criticas debido a su simplicidad y eficiencia. Sin embargo, su diseño original carece de medidas de seguridad robustas, lo que lo hace vulnerable a ataques cibernéticos. Por ello, es importante evaluar la seguridad ofrecida por este protocolo para aplicar las medidas necesarias que garanticen la integridad, confidencialidad y disponibilidad de los sistemas de control industrial.

El propósito de este estudio es evaluar la seguridad proporcionada por el protocolo Modbus en comunicaciones habituales en sistemas industriales. Para ello, se analizan las vulnerabilidades y debilidades del sistema, para identificar posibles puntos de entrada para un atacante externo o interno.

Los objetivos específicos son los siguientes:

- Construir un entorno de pruebas con componentes reales utilizados en la industria para llevar a cabo análisis controlados.
- Identificar y evaluar las vulnerabilidades en la comunicación mediante el protocolo Modbus.
- Emplear herramientas de pentesting y explotación de vulnerabilidades conocidas para evaluar su impacto en el sistema.
- Determinar el nivel de riesgo asociado a los puntos de ataque identificados.
- Proporcionar recomendaciones para garantizar un nivel adecuado de protección de los sistemas de control.

El alcance del pentesting comprende:

- Recopilación de información y aplicación de técnicas OSINT para obtener información sensible sobre los dispositivos objeto de estudio.
- Aplicación de herramientas de escaneo y enumeración de servicios y puertos para obtener una visión de la estructura del sistema.
- Empleo de *exploits* para la lectura y escritura de datos en los dispositivos.
- Inspección y obtención de paquetes y tramas, así como el análisis de comunicaciones.

Este estudio excluye:

- Técnicas de intrusión en la red de control: se adopta un enfoque de caja blanca, donde el atacante tiene conocimiento completo del sistema.
- Ingeniería social y ataques de intrusión: se asume que el *pentester* ya ha obtenido acceso a la red y está presente en ella para explotar la comunicación Modbus.
- Explotación de vulnerabilidades que puedan causar daños irreparables a los dispositivos utilizados.

6.1.2 Análisis de Riesgos

A continuación, se enumeran las implicaciones que este estudio puede tener:

- **Consideraciones Éticas y Legales**: es esencial destacar que este estudio se lleva a cabo con fines educativos y dentro de un entorno controlado. Se prohíbe el uso de la información obtenida con propósitos maliciosos o ilegales. El objetivo principal es analizar las vulnerabilidades del protocolo Modbus sin comprometer la confidencialidad, integridad o disponibilidad de los sistemas y datos.
- **Recomendaciones de Seguridad**: al finalizar las pruebas, se proporcionarán recomendaciones y buenas prácticas para asegurar la seguridad de los sistemas y reducir la exposición de los dispositivos a posibles amenazas.
- **Capacitación y Concienciación**: estas pruebas buscan promover la formación y la concienciación sobre los riesgos que enfrentan los sistemas industriales.

6.2 Fase I. Configuración del entorno de pruebas

Para realizar esta evaluación, se ha configurado un escenario de pruebas que simula una comunicación industrial mediante el protocolo Modbus. Este escenario está compuesto por un PLC real del fabricante Schneider, Modicon M221, que se comunica con una planta industrial virtualizada con el software Factory IO. En este entorno, el PLC actúa como el controlador principal, gestionando la lógica de control y comunicándose con los diferentes dispositivos de la planta a través del protocolo Modbus.

Se han llevado a cabo pruebas de penetración utilizando una máquina equipada con el sistema operativo Kali Linux, una distribución de Linux de código abierto basada en Debian. Kali Linux está especialmente diseñada para actividades relacionadas con la seguridad, pruebas de penetración, investigación forense y seguridad informática. Ofrece una amplia variedad de herramientas y utilidades, como Nmap, Metasploit o Wireshark. Esta instalación se ha realizado virtualizando el sistema operativo mediante el entorno VMWare Workstation Pro-17.

Para recrear una planta industrial en el software Factory IO, se ha empleado una escena sencilla que simula acciones de "Pick and Place", comunes en las industrias reales. "Pick and Place" consiste en el

proceso automatizado de recoger un objeto de un lugar determinado y colocarlo en otro, generalmente en una posición específica. En el contexto de la industria, esto puede implicar la transferencia de productos entre diferentes puntos de la línea de producción, como mover componentes de una cinta transportadora a otra o colocar artículos en envases.

El software Factory IO permite simular elementos industriales, como sensores, actuadores, cintas transportadoras, cajas, palets, entre otros, para recrear situaciones lo más cercanas posible a la vida real. Para obtener más detalles sobre cómo se ha configurado y montado la escena de la planta en Factory IO, se puede consultar el Anexo I.

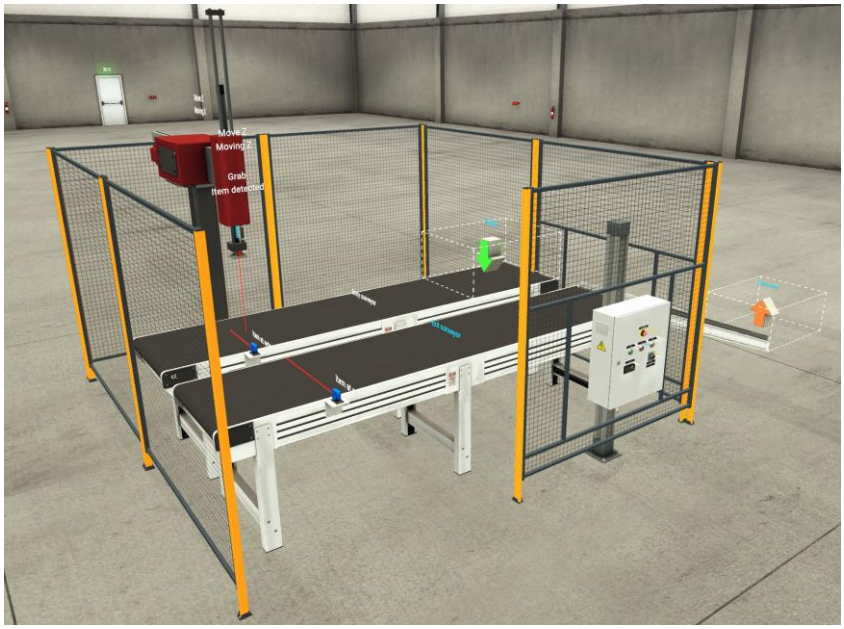


Figura 28. Software virtualización planta industrial

Se ha elegido un PLC de Schneider, el Modicon 221 (TM221CE16T), para el control y operación de la planta recreada. Este modelo ofrece una amplia gama de funcionalidades, capacidad de entrada/salida y facilidad de programación, lo que lo convierte en la opción adecuada para supervisar los procesos simulados en la planta virtual. Su diseño compacto facilita su integración en el escenario construido, permitiendo una instalación portátil.

Este autómata se programa utilizando el software Schneider EcoStruxure Control Basic, que proporciona una plataforma intuitiva para el desarrollo de la lógica de control. Este programa admite varios lenguajes de programación como Ladder, FBD, ST, SFC o LI.

Además, el autómata TM221CE16R puede conectarse con otros dispositivos a través del protocolo Modbus. También cuenta con conectividad Ethernet para facilitar la comunicación en red y la supervisión de la planta.

En ese caso, se ha programado la lógica mediante el lenguaje Ladder o lenguaje de contactos. En la Figura 30 se muestra un esquema del funcionamiento que ilustra el proceso para realizar el control de la escena “Pick and Place”.

Figura 29. Controlador Lógico Programable Schneider Modicon 221

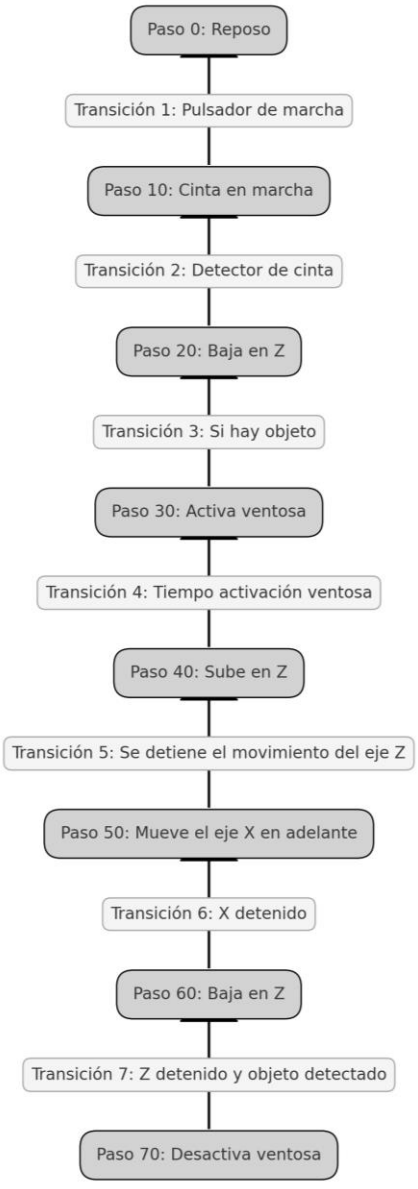


Figura 30. Diagrama Grafcet. Lógica funcionamiento programación Pick&Place

En la fase de planificación, se parte del supuesto de que el atacante ya ha obtenido acceso a la red de control y al sistema. En consecuencia, se configura la máquina atacante para integrarse en red con el autómata y la planta virtual. Se utiliza un cable Ethernet para conectar el PLC al equipo que aloja el software de virtualización de la planta, ya que el autómata Schneider M221 permite la conexión a través de Ethernet. Posteriormente, mediante el software EcoStruxure, se asigna una dirección IP estática al PLC y se carga la programación necesaria para controlar la planta, utilizando en este caso la dirección IP 192.254.103.100. Los pasos detallados para esta configuración y programación del PLC se describen en el Anexo II. A continuación, se conecta la planta al PLC utilizando la configuración de Factory IO, especificando la dirección IP del PLC como la dirección a la que debe conectarse la planta. Por último, se configura la red de la máquina atacante en modo bridge, permitiendo así que la máquina virtual acceda a la red del host físico como si estuviera conectada directamente a ella. En este modo, la máquina virtual utiliza la misma red física que el host y puede comunicarse directamente con otros dispositivos en esa red, obteniendo una dirección IP del mismo rango que los dispositivos físicos conectados al host. En este caso, se asigna a la máquina virtual una dirección IP estática del mismo rango que la del PLC (192.254.103.50). Los detalles para esta configuración se especifican en el Anexo III.

Figura 31. Configuración escenario de pentesting

6.3 Fase III. Reconocimiento

La primera etapa del proceso de *pentesting*, se centra en el reconocimiento mediante la búsqueda y recopilación de datos utilizando técnicas de Open Source Intelligence (OSINT). Cabe resaltar que esta fase se lleva a cabo de manera pasiva y conforme a las normativas legales, evitando cualquier actividad ilícita.

En esta fase, el objetivo es recopilar exhaustivamente toda la información relevante sobre el sistema objetivo. Se emplea una variedad de fuentes, desde motores de búsqueda como Google, Bing y Shodan, hasta exploración de sitios web públicos de la organización objetivo. Se busca obtener detalles como la estructura de la red, tecnologías utilizadas, información de contacto y perfiles de empleados. Además, se examinan las redes sociales asociadas con la empresa para identificar empleados, sus roles y posibles puntos débiles de seguridad. Se realiza un análisis minucioso de la documentación técnica disponible, incluyendo manuales de productos, especificaciones de hardware y software, así como informes de vulnerabilidad y notas de seguridad, con el fin de comprender la infraestructura tecnológica y evaluar riesgos potenciales.

Figura 32. Proceso OSINT [54]

En este apartado se detallan algunas de las herramientas más reconocidas y empleadas en esta fase para recopilar información valiosa de manera pasiva y se aplican al escenario de pruebas construido.

6.3.1 Listas de Credenciales y Documentación Sensible.

En la industria, la falta de concienciación en ciberseguridad a menudo conduce al uso de contraseñas por defecto en dispositivos de campo, lo que los deja vulnerables a ataques de diccionario o de fuerza bruta. Un ataque de diccionario es un método utilizado para intentar descifrar contraseñas probando una lista de palabras comunes o predefinidas. En los ataques de fuerza bruta, los atacantes intentan descifrar la contraseña probando combinaciones posibles de caracteres, desde números y letras hasta símbolos, para encontrar la contraseña correcta.

En GitHub y otros repositorios, se pueden encontrar varios registros de contraseñas por defecto organizadas por fabricante y producto.

- ICS Master
- SCADAPASS

En este escenario, se ha hecho una búsqueda en la lista llamada "SCADAPASS" para obtener información sobre el fabricante de nuestro PLC objetivo, Schneider Electric. Como se ilustra en la imagen adjunta, dicha lista revela varias contraseñas utilizadas en PLCs, servidores en Internet o módulos Ethernet. Aunque el PLC específico utilizado en este proyecto, el Modicon 221, no figura en dicha lista, los atacantes podrían emplear combinaciones de las credenciales listadas para deducir las credenciales del PLC, lo que podría facilitar un posible ataque.

Vendor	Device	Default Password	Port	Device type	Protocol	Source
Schneider Electric	PowerLogic Series 800 Power Meter	0000		PLC		http://www.powerlogi
Schneider Electric	PowerLogic ION7550 / ION7650 / IOI		0	Energy and power meter		http://www2.schneide
Schneider Electric	PowerLogic Ethernet Gateway EGX3C	Administrator:Gateway	80/tcp	Integrated gateway-server	http	http://azzo.com.au/w
Schneider Electric	POWERLOGIC EGX200 / EGX400 with	Administrator:admin, User 1:n	80/tcp	gateway-server	http	http://www.powerlogi
Schneider Electric	Modicon Quantum	ftpuser/password, qbf77101/I	21/tcp, 23/tcp, 8	PLC	HTTP, FTP, Telnet	http://www.digitalbon
Schneider Electric	Modicon M340 for Ethernet	ntpupdate:ntpupdate (Using a	21/tcp, 80/tcp	PLC	FTP, HTTP	https://dariusfreamon
Schneider Electric	Modicon Premium	FTP: sysdiag:factorycast@schn	21/tcp, 80/tcp	PLC	FTP, HTTP	https://github.com/ITI
Schneider Electric	PM8000, PM8240, PM8243, PM8244	Physical: 0, FTP: 8000:<display	21/tcp, 80/tcp	PLC	FTP, HTTP	http://www2.schneide
Schneider Electric	TSX ETG 1000	HTTP Server, PAP Protocol: USI	21 TCP	PLC	FTP, PAP, HTTP	http://www.is-com.ru/
Schneider Electric	ETG100	Administrator:Gateway		PLC		http://www.schneider-
Schneider Electric	M258	adm:adm	80/tcp	PLC	http	http://ewon.biz/sites/
Schneider Electric	Quantum NOE 771 xx	pcfactory:pcfactory, loader:fw	21/tcp, 80/tcp	Ethernet Modules	ftp, http	https://igate.alamedae

Figura 33. Listado de credenciales por defecto para el fabricante Schneider Electric

Además, para ejecutar un ataque de manera efectiva, es fundamental comprender a fondo la estructura y el funcionamiento de los dispositivos objetivo. Esta información detallada suele estar disponible en los manuales técnicos proporcionados por los fabricantes. Estos manuales contienen descripciones de las especificaciones del dispositivo, su configuración, protocolos de comunicación y posibles vulnerabilidades. Para acceder a estos manuales, se puede recurrir a diversas fuentes, como los sitios web oficiales de los fabricantes, bibliotecas digitales

especializadas o incluso comunidades en línea de profesionales en seguridad informática, donde suelen compartirse recursos y conocimientos relevantes.

Para obtener esta información de nuestro objetivo, se ha realizado una búsqueda en la propia web del fabricante (Modicon M221 | Schneider Electric España (se.com)) donde se encuentran documentos como la guía de usuario, guía de programación y una biblioteca de funciones avanzadas. Este proceso permite acceder a información valiosa que contribuye a comprender en profundidad el dispositivo y sus capacidades.

6.3.2 Google Dorks

Google Dorks, también conocidos como Google Hacks, son comandos de búsqueda específicos que utilizan consultas avanzadas para acceder a información oculta en Google. Cuando Google rastrea la web para indexar páginas, puede ver partes de los sitios web que no se muestra en una búsqueda regular. Los comandos Google Dorks permiten consultar información confidencial de organizaciones, empresas y propietarios de sitios web.

Algunos ejemplos de comandos Google Dorks incluyen:

- *site:example.com*: limita la búsqueda a un sitio web específico.
- *intitle:"index of"*: restringe los resultados de la búsqueda a páginas que contienen un título específico.
- *filetype:pdf*: filtra resultados por tipo de archivo.
- *inurl:admin*: encuentra páginas que contienen "admin" en la URL.

A continuación, se realiza una búsqueda empleando la directiva *intitle,* que restringe los resultados de la búsqueda a páginas que contienen el término “Schneider Electric Telecontrol” para encontrar sitios webs relacionados con esta plataforma.

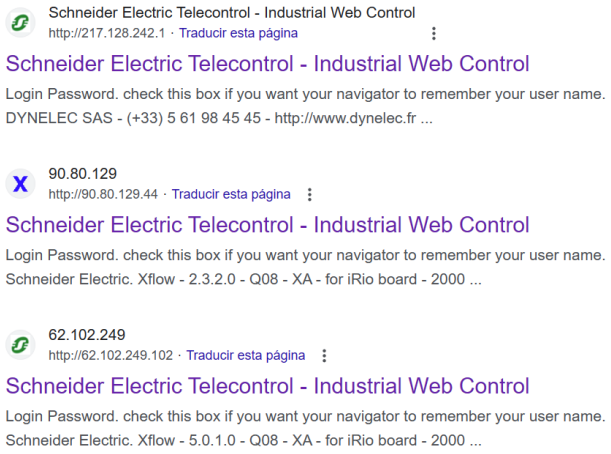


Figura 34. Google Dorks. Resultados búsqueda con directiva “intitle”

Como se ve en la web obtenida, encontramos servidores de proveedores frecuentemente utilizados que no se configuraron con las medidas de seguridad adecuadas y están expuestos en internet.

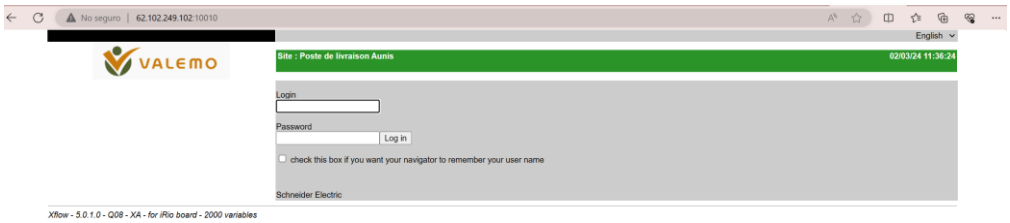


Figura 35. Google Dorks. Servidor accesible públicamente

Si se logra obtener acceso a uno de estos sistemas mediante credenciales predeterminadas, como las proporcionadas anteriormente, esto podría suponer una vulnerabilidad para sistemas industriales. Con el acceso a la plataforma de telecontrol, un atacante potencial tendría la capacidad de monitorizar y controlar dispositivos industriales críticos.

6.3.3 Shodan

Shodan[14] es un motor de búsqueda especializado que explora y recopila información sobre dispositivos conectados a Internet [55].

Lo que distingue a Shodan es su capacidad para indexar registros específicos sobre los dispositivos, como cámaras de seguridad, routers, servidores, PLCs, sistemas de supervisión y dispositivos de Internet de las cosas (IoT), entre otros. Estos registros pueden incluir información sobre el software que están ejecutando, puertos abiertos, protocolos utilizados y, en algunos casos, datos más sensibles si la configuración de seguridad no es adecuada.

Es importante destacar que el uso de Shodan para buscar información en Internet es completamente legal. Sin embargo, acceder a los servidores mostrados en los resultados podría ser ilegal y considerarse ciberdelincuencia.

Shodan permite realizar búsquedas filtradas por número de puerto, protocolo e incluso incorpora una sección dedicada a sistemas de control industrial.

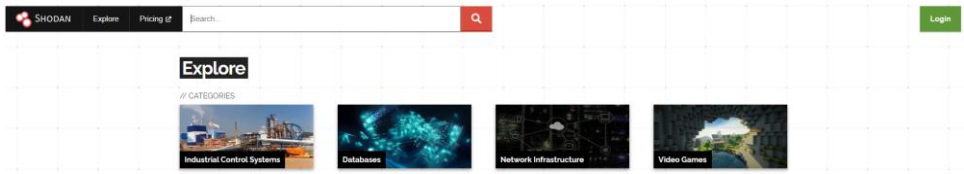


Figura 36. Shodan. Sección Industrial Control Systems

En este estudio se realizan varias búsquedas para obtener información sobre el PLC Schneider Modicon 221 y el protocolo utilizado, Modbus.

En primer lugar, se realiza una búsqueda filtrando por la referencia del PLC objetivo, “TM221CE16T”. Como se muestra en la imagen a continuación, la búsqueda arroja 189 resultados de PLCs y proporciona información detallada, incluyendo las direcciones IP y los puertos utilizados por estos dispositivos.

[14] Shodan Search Engine

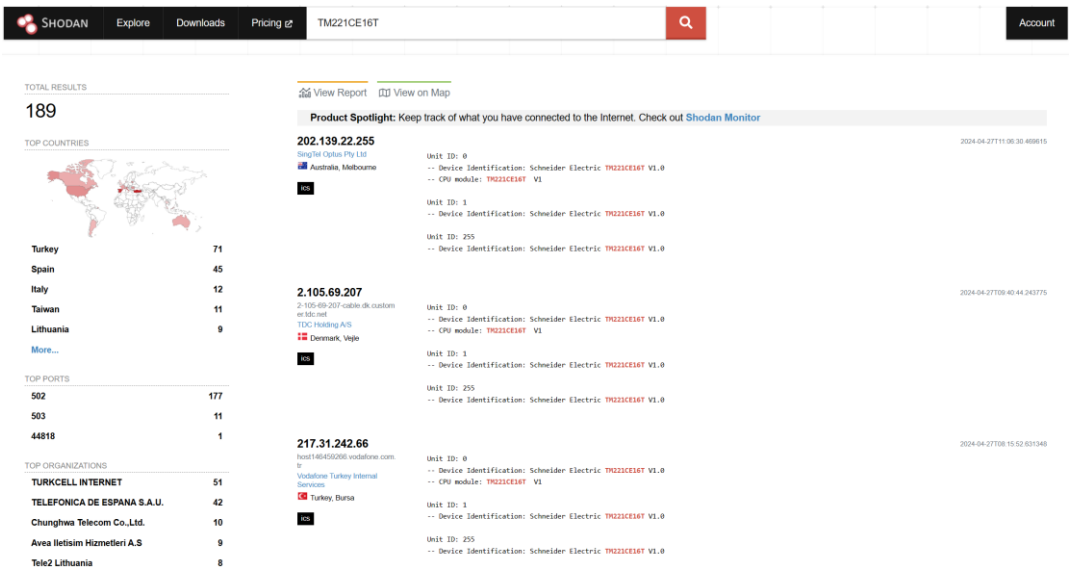


Figura 37. Shodan. Resultados búsqueda TM221CE16T

La siguiente búsqueda muestra dispositivos que utilizan el protocolo Modbus. Dado que el puerto estándar asignado para este protocolo es el 502, la búsqueda se enfoca en encontrar dispositivos que tengan este puerto abierto y estén activamente utilizando Modbus. Como resultado, se obtienen numerosas entradas que corresponder a dispositivos que podrían estar utilizando este protocolo.

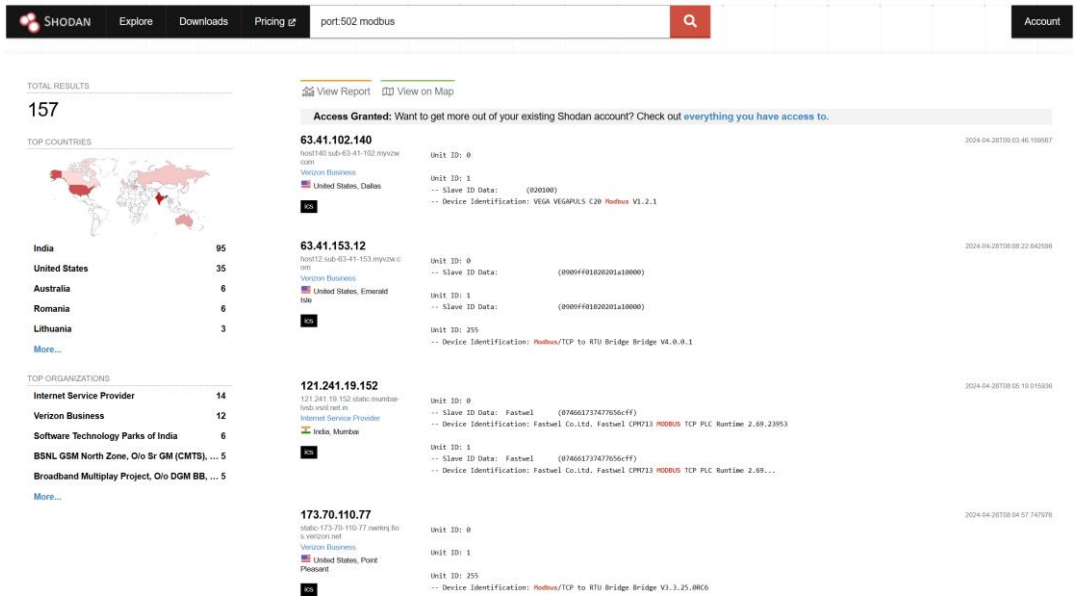


Figura 38. Shodan. Resultados búsqueda port 502 modbus

En el siguiente repositorio, se recopilan listas con directivas útiles para obtener información valiosa sobre dispositivos de campo a través de Shodan y Google Dorks:

- ICS IoT Shodan Dorks

6.3.4 Exploit DB

Exploit DB es un repositorio que información sobre fallos de software, exploits, shellcode, vulnerabilidades zero-days, así como informes de seguridad y vulnerabilidades de diversos dispositivos. Alberga una gran cantidad de datos provenientes de numerosas fuentes, lo que lo convierte en una herramienta esencial para identificar y comprender las vulnerabilidades que pueden afectar a una amplia gama de dispositivos y sistemas.

Las siguientes imágenes presentan las vulnerabilidades detectadas para el fabricante de dispositivos objetivo, Schneider, y el protocolo utilizado, Modbus. Cada resultado de búsqueda está acompañado de tres columnas: "D", "A" y "V", que permiten descargar el exploit, la aplicación afectada, y verificar si la vulnerabilidad ha sido confirmada o no, respectivamente.

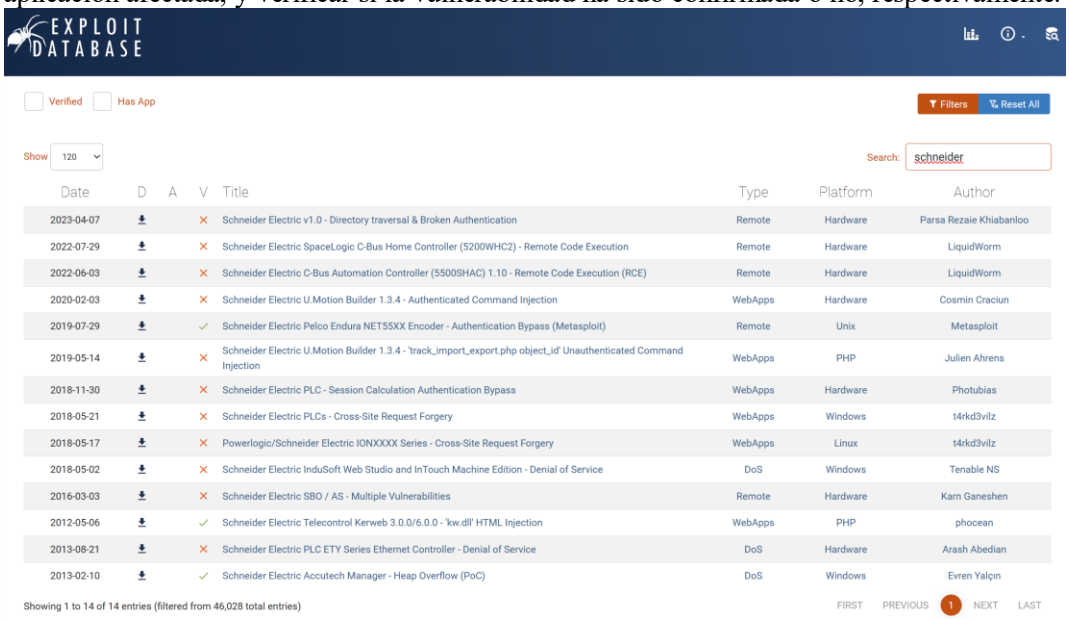


Figura 39. Exploit DB. Resultados búsqueda schneider

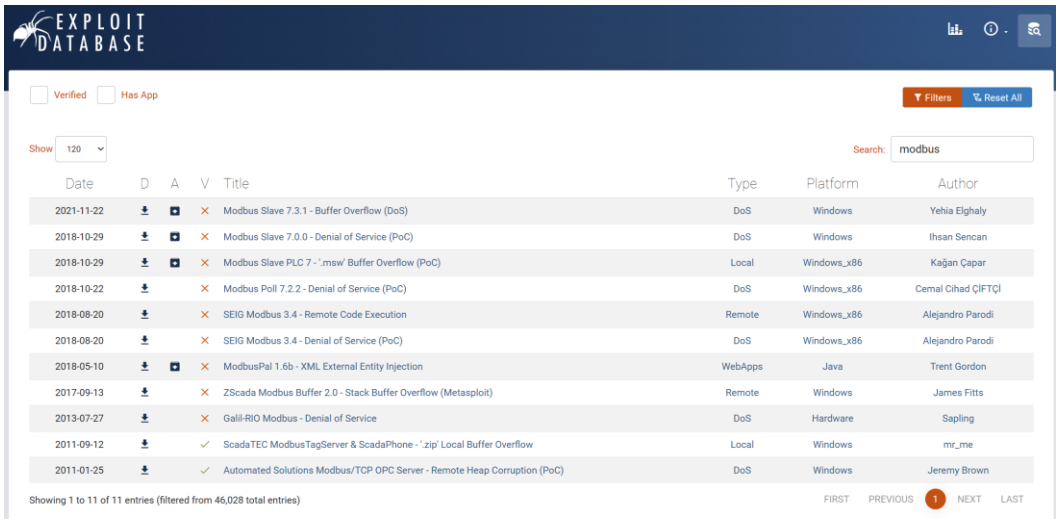


Figura 40. Exploit DB. Resultados búsqueda modbus

La fase inicial del pentesting es crucial ya que proporciona una base sólida para todo el proceso. A través del reconocimiento pasivo, se recopila información valiosa que permite comprender a fondo el sistema objetivo y evaluar los posibles riesgos. Esta información es fundamental para planificar estratégicamente los pasos siguientes e identificar posibles vulnerabilidades en la seguridad del sistema. En conclusión, una fase de reconocimiento bien ejecutada es esencial para el éxito del pentesting y para garantizar la efectividad de las acciones posteriores.

6.4 Fase IV. Escaneo

La segunda fase de este proceso consiste en la obtención de información sobre el sistema objetivo con un enfoque activo. Mientras que la fase de reconocimiento se centra en la recopilación de datos de forma pasiva y legal, el escaneo implica la exploración activa para identificar activos, puertos abiertos y servicios.

En el escaneo se utilizan escáneres de puertos y exploradores de vulnerabilidades para detectar posibles puntos de entrada al sistema y planificar los vectores de ataque. En este capítulo, se presentan algunas de las herramientas útiles para llevar a cabo esta fase en el escenario configurado.

6.4.1 Nmap

Nmap es una de las herramientas de código abierto más populares para la exploración de redes y las auditorías de seguridad. Nmap puede identificar los dispositivos activos en una red, así como los servicios que ofrecen (incluyendo el nombre y la versión de la aplicación), los sistemas operativos y sus versiones, y los diversos tipos de filtros de paquetes o cortafuegos utilizados. Esta herramienta proporciona una visión integral de la infraestructura de red y de los posibles riesgos de seguridad asociados [55].

En la documentación oficial de Nmap[15] se puede encontrar toda la información detallada acerca del funcionamiento de la herramienta. Sin embargo, en este capítulo de detallan algunos de los comandos más útiles para pruebas de penetración en entornos industriales:

- *-sL* (sondeo de lista): realiza un listado de sistemas sin enviar paquetes. Utiliza una resolución inversa DNS para obtener los nombres de los equipos. Esta táctica permite obtener información valiosa sin "hacer ruido", ya que no se envía ningún paquete al objetivo.
- *-PU* [lista de puertos] (Ping UDP): esta táctica envía un paquete UDP vacío a los puertos especificados. Si el puerto está cerrado, responde con un mensaje ICMP de "puerto no alcanzable", si no se recibe este mensaje, Nmap supone que el puerto está abierto.
- *-PS* [lista de puertos] (Ping TCP Syn): esta opción envía un paquete TCP vacío con la bandera SYN activa, indicando al sistema objetivo que quiere establecer una conexión. Si el puerto está cerrado, enviará un paquete de reset (RST), si el puerto está abierto, responderá al saludo. Nmap lista todos los sistemas que respondan con RST o SYN/ACK.
- *-sV* (Version Detection): determina la versión que se está ejecutando de los servicios con puertos abiertos. La información recolectada durante la fase de descubrimiento, como vulnerabilidades en versiones de dispositivos de fabricantes industriales, sumada a los detalles de los servicios obtenidos mediante el comando de Nmap, podría ser utilizada por un atacante para ejecutar ataques dirigidos hacia componentes críticos como PLCs, SCADAs y HMIs.
- *--script* (Script Scanning): ejecuta scripts Nmap predefinidos para realizar pruebas de seguridad específicas en los sistemas objetivos. A continuación, se enumeran algunos scripts útiles para el escaneo de diversos protocolos ampliamente utilizados en sistemas industriales, junto con las URL de los repositorios desde donde se pueden descargar.
    - **modbus-discover.nse**: escanea dispositivos Modbus y direcciones IP y puertos utilizados

      https://github.com/nmap/nmap/blob/master/scripts/modbus-

[15] Nmap Documentation - Free Security Scanner For Network Exploration & Security Audits

discover.nse

- **s7-info.nse:** proporciona información de dispositivos Siemens S7.

  https://github.com/nmap/nmap/blob/master/scripts/s7-info.nse

- **enip-info.nse:** detecta dispositivos Ethernet/IP y obtiene información sensible como nombres de dispositivos, direcciones IP e información del fabricante.

  https://github.com/nmap/nmap/blob/master/scripts/enip-info.nse

En la siguiente imagen se muestra un ejemplo de uso del script *modbus-discover,* en este caso se ha añadido la opción *-A* que realiza un ataque más agresivo.

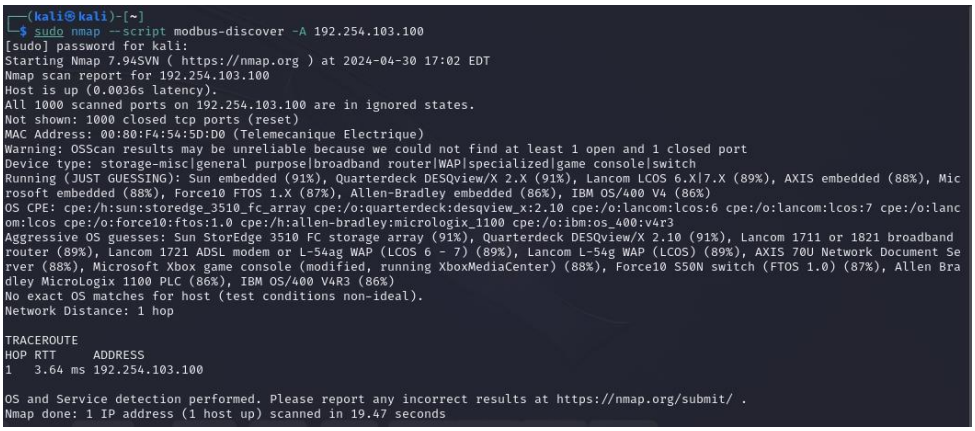


Figura 41. Nmap. Resultado ejecución script modbus-discover

El análisis de la red proporciona una serie de hallazgos significativos sobre el host 192.254.103.100, correspondiente al PLC Schneider. Revela la presencia de un dispositivo con todos sus 1000 puertos en un estado ignorado, posiblemente debido a medidas de seguridad como un firewall. Se detecta una amplia variedad de sistemas operativos potenciales, desde dispositivos embebidos de Sun hasta equipos de redes de fabricantes como Lancom, Force10, Allen-Bradley, e IBM. Aunque se identifica un dispositivo asociado con Telemecanique Electrique, la información sobre el tipo de dispositivo es ambigua, incluyendo almacenamiento misceláneo, enrutador de banda ancha, punto de acceso inalámbrico (WAP), consola de juegos, entre otros.

Además, se identifica la dirección MAC del host, lo que resulta útil para identificar el fabricante del dispositivo. Herramientas como *Mac Lookup*[16] permiten obtener información detallada sobre el fabricante a partir de la dirección MAC extraída. Conocer el fabricante del dispositivo puede ayudar al atacante a dirigir ataques específicos a vulnerabilidades asociadas con ese fabricante o utilizar esta información para ataques de suplantación de identidad.

[16] MAC Address Vendor Lookup | MAC Address Lookup (maclookup.app)

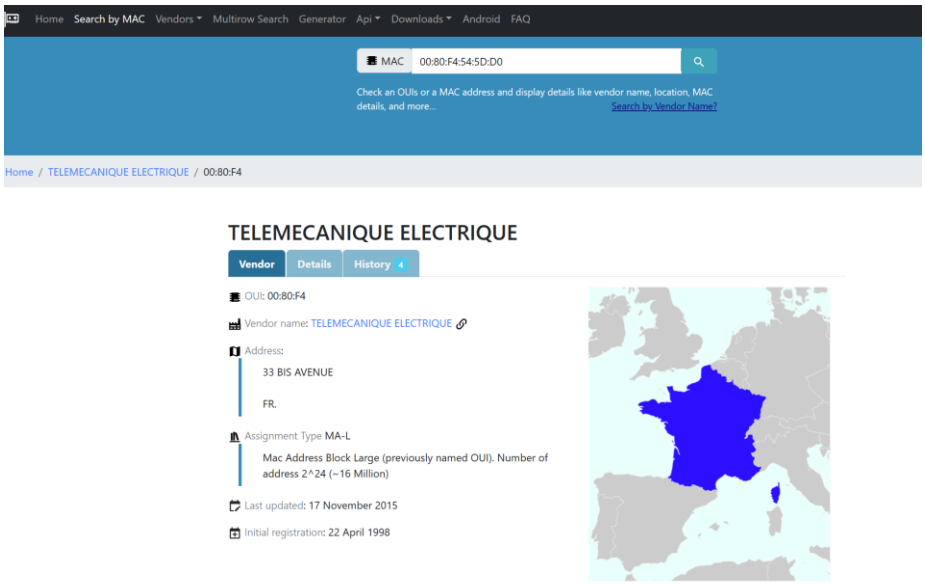


Figura 42. Resultados búsqueda MAC dispositivo en MAC Look up

Por otro lado, el escaneo realizado por Nmap revela múltiples coincidencias de *fingerprints* para el sistema operativo en el host, lo que dificulta proporcionar detalles específicos sobre el sistema operativo en uso.

Finalmente, se destaca que la distancia de red indica que el host objetivo está a un salto de distancia del host de origen, indicando una conexión directa con un tiempo de ida y vuelta (RTT) de 3,64 ms. Este dato es importante para comprender la topología de la red y la proximidad física entre los dispositivos.

6.4.2 Wireshark

Wireshark[17] es una herramienta de análisis de paquetes que captura y muestra el tráfico de datos en una red. Esta herramienta ofrece las siguientes opciones útiles para realizar pruebas de penetración y también para detectar fallos de seguridad o un posible ataque en ejecución.

- Captura de paquetes: Wireshark permite interceptar y registrar el tráfico de red en tiempo real, lo que facilita el análisis de los datos transmitidos entre dispositivos en la red.
- Aplicación de filtros de captura: los filtros de captura permiten especificar qué tipo de tráfico se desea observar, lo que ayuda a enfocarse en paquetes específicos y a reducir el volumen de datos capturados para un análisis más eficiente.
- Identificación de dispositivos y protocolos: Wireshark puede identificar los dispositivos conectados a la red y los protocolos utilizados para comunicarse. Esto es útil para comprender la topología de la red y detectar dispositivos desconocidos o no autorizados.
- Identificación de paquetes sospechosos y tráfico no autorizado: mediante el análisis del tráfico capturado, Wireshark puede detectar patrones inusuales o comportamientos sospechosos que podrían indicar un posible ataque o actividad maliciosa en la red. Esto ayuda a los administradores de red a identificar y mitigar posibles amenazas de seguridad.

[17] Wireshark · Go Deep

En el contexto de este estudio, se supone que el atacante se infiltra en la red y accede, colocándose en la misma red que los dispositivos objetivo: el cliente y el servidor de comunicación Modbus. Ante esta situación, se procede a iniciar Wireshark en la máquina del atacante para llevar a cabo un análisis del tráfico de red. Siempre que la comunicación entre el PLC y la planta este activa, Wireshark intercepta todo el tráfico intercambiado, permitiendo la visualización de las tramas y su contenido. Este proceso se ilustra en la imagen adjunta.

Para reducir la búsqueda a la comunicación objetivo, se filtra por paquetes con puerto fuente o destino 502, puerto por defecto de las comunicaciones Modbus. Así, podemos examinar la comunicación completa intercambiada, analizando cada paquete para observar la estructura estudiada del protocolo. A través de la última capa, podemos identificar la acción que se está realizando, como escritura o lectura de registros.

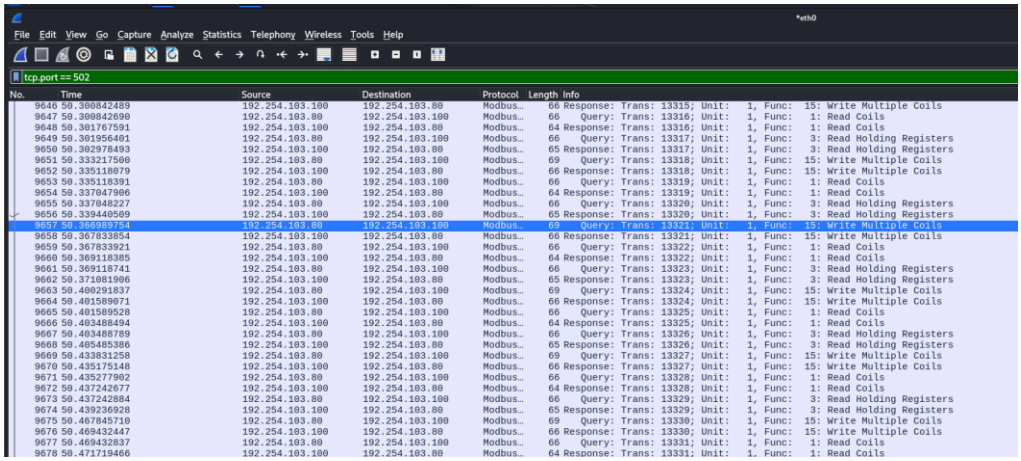


Figura 43. Wireshark. Captura comunicación PLC - planta

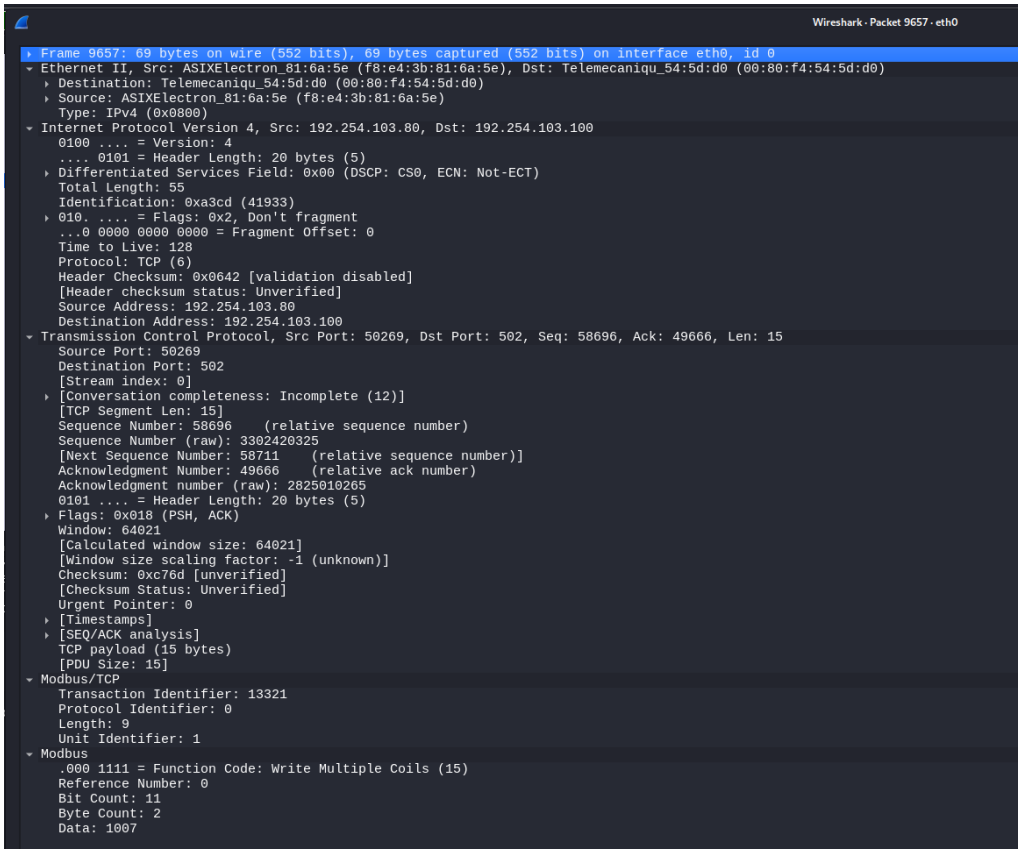


Figura 44. Wireshark. Paquete Modbus capturado

6.5 Fase V. Explotación

Una vez recopilada toda la información del sistema de control objetivo del ataque como se detalla en las fases anteriores, se procede con la fase de explotación. Esta fase, núcleo del proceso de pentesting, consiste en explotar las vulnerabilidades detectadas con el objetivo de simular un ataque real. Esto permite evaluar las posibles consecuencias de una intrusión, detectar los puntos débiles del sistema y valorar la efectividad de las medidas de seguridad implementadas para protegerlo. Es una etapa crítica para evaluar el nivel de vulnerabilidad del sistema y determinar las acciones necesarias para reforzar su seguridad.

Durante esta fase, al igual que en las anteriores etapas del pentesting, se describirán las herramientas disponibles para llevar a cabo la explotación de los sistemas de control industrial. Estas herramientas serán aplicadas específicamente al escenario construido, permitiendo la evaluación de las vulnerabilidades de este sistema y su impacto.

6.5.1 Lectura y Escritura de Datos

En este capítulo, se utilizan herramientas conocidas de explotación de vulnerabilidades y pentesting para obtener información crítica del sistema de control y perturbar su funcionamiento. En primer lugar, se ejecutan varios exploit para obtener información sobre los dispositivos que están haciendo uso de Modbus en la red y posteriormente se procede a la lectura y escritura de datos en los registros del autómata.

La lectura de datos puede exponer información sensible sobre el funcionamiento y la configuración de la planta, lo que podría ser aprovechado para obtener una comprensión detallada de los procesos industriales en curso. Por otro lado, la capacidad de escribir datos con este módulo es aún más preocupante. Al modificar los valores de los registros y bobinas en un sistema de control, un atacante podría provocar cambios no autorizados en la operación de la planta [56].

6.5.1.1 Metasploit

Metasploit Framework [18]es un marco de código abierto basado en Ruby utilizado tanto por profesionales de la seguridad de la información como por ciberdelincuentes para identificar, explotar y validar vulnerabilidades en sistemas y redes. Este conjunto de herramientas ofrece a los usuarios la capacidad de realizar pruebas de penetración y piratería ética, así como de remediar vulnerabilidades en las redes de una organización. Además, los equipos de seguridad de la información emplean Metasploit para llevar a cabo pruebas de penetración y corregir vulnerabilidades. Dada su naturaleza de código abierto, Metasploit puede ser personalizado y utilizado fácilmente en una amplia variedad de sistemas operativos [57].

Dado que Metasploit viene preinstalado en el sistema Kali Linux, basta con abrir una terminar y ejecutar el comando '*msfconsole'*.

Una vez dentro de Metasploit, se buscan módulos relacionados con Modbus (> *search modbus*). Esta búsqueda proporciona varios módulos relacionados con dicho protocolo, incluidos algunos dirigidos a Schneider Modicon. Estos recursos pueden ser útiles para explotar vulnerabilidades en el PLC del escenario de estudio.

[18] Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit

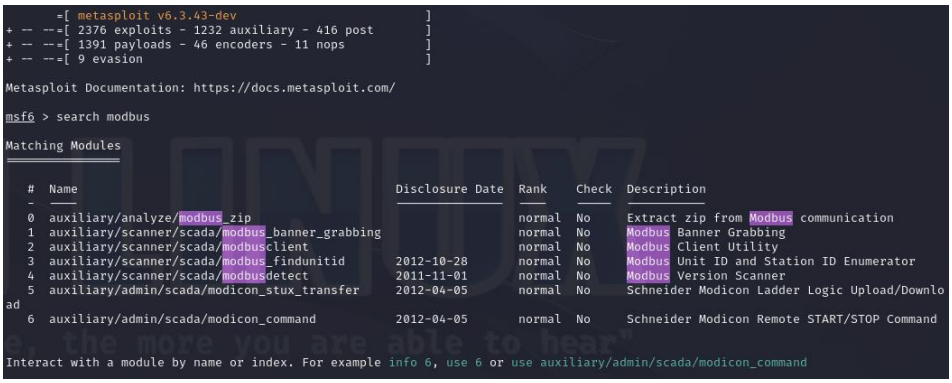


Figura 45. Metasploit. Listado de módulos relacionados con el protocolo Modbus

En primer lugar, se utiliza el módulo ***modbusdetect***. Este módulo emplea técnicas de escaneo de red para identificar dispositivos que utilizan el protocolo Modbus. Para ejecutarlo, se selecciona el módulo mediante el comando "*use",* seguido de la ruta específica proporcionada en la imagen anterior. En este caso:

> use auxiliary/scanner/scada/modbusdetect

Una vez dentro del módulo correspondiente, el comando '*> show options'* muestra los parámetros necesarios para la explotación. En este caso, es necesario determinar la IP del dispositivo objetivo mediante el comando '*> set RHOSTS [IP_target]'*.

En la siguiente imagen, se muestra la ejecución del exploit contra el PLC objetivo (IP 192.254.103.100) y los resultados obtenidos. Se observa que Metasploit ha detectado un dispositivo haciendo uso de Modbus en esa dirección.

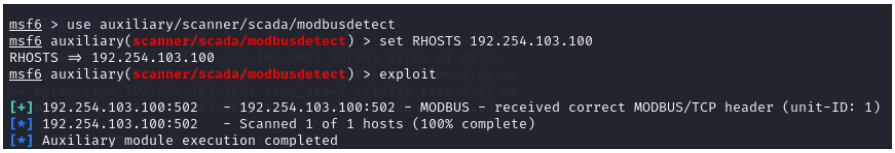


Figura 46. Metasploit. Ejecución módulo modbusdetect

Luego, se ejecuta el módulo ***modbus _findunitid***. En Modbus los "identificadores de unidad" son números asignados a cada dispositivo Modbus en una red para direccionar solicitudes específicas. El módulo analiza la respuesta del dispositivo al enviar un comando de lectura de registro de entrada (0x04) a dispositivos en la red. Si el dispositivo en la dirección IP especificada responde con el mismo ID, significa que el comando fue enviado al ID de unidad correcto. El escaneo puede ajustarse con parámetros como el puerto y la IP, con la opción de ralentizarlo (*BENICE)* para evitar problemas de rendimiento en la red.

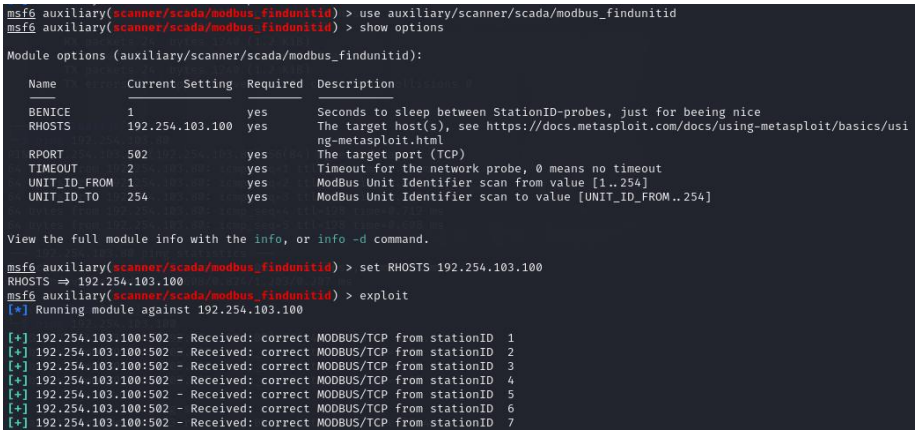


Figura 47. Metasploit. Ejecución módulo modbus_findunitid

El siguiente módulo que se estudia en este capítulo es ***modbusclient.*** Dicho módulo permite interactuar con el protocolo Modbus para realizar operaciones de lectura y escritura en registros y bobinas.

Al igual que en los anteriores módulos, el primer paso es cargar el módulo mediante el comando: '> *use auxiliary/scanner/scada/modbusclient'.* Después, se muestran las variables necesarias para su ejecución. Como se ve en la imagen a continuación este módulo tiene varias variables que deben ser configuradas según la acción que se desee tomar. En primer lugar, se pueden seleccionar cuatro acciones diferentes:

- READ_REGISTERS
- WRITE_REGISTERS
- READ_COILS
- WRITE_COILS

Es importante tener en cuenta que, de forma predeterminada, las acciones solo se aplican al primer registro o bobina de la primera unidad. Para cambiar este comportamiento, se pueden ajustar los parámetros UNIT_NUMBER y NUMBER.

En primer lugar, se leen los 100 primeros registros del PLC, ejecutando los comandos mostrados en la imagen a continuación. Esto nos devuelve el valor actual de cada uno. Si ejecutamos este comando con la planta en funcionamiento, el valor de los registros varía según la acción que este tomando el PLC.

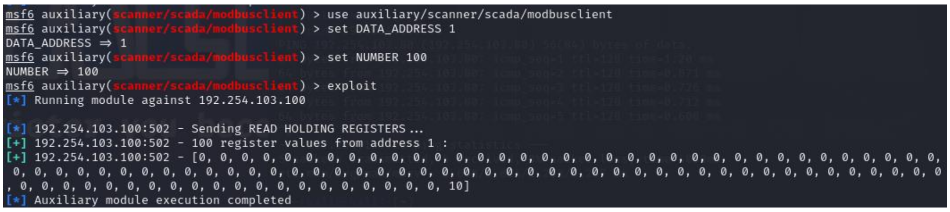


Figura 48. Metasploit. Resultado lectura de registros

Figura 49. Metasploit. Evolución lectura de registros

Después, se modifica la acción para leer el valor de las bobinas, utilizando la función READ_COILS. Al ejecutar los comandos que se muestran en la imagen, obtenemos el valor de cada una de las bobinas durante el proceso. Esto proporciona información relevante para un atacante, como el número de bobinas que se activan durante el proceso, lo que podría sugerir los valores críticos y cómo causar fallos en la planta si se altera su valor.

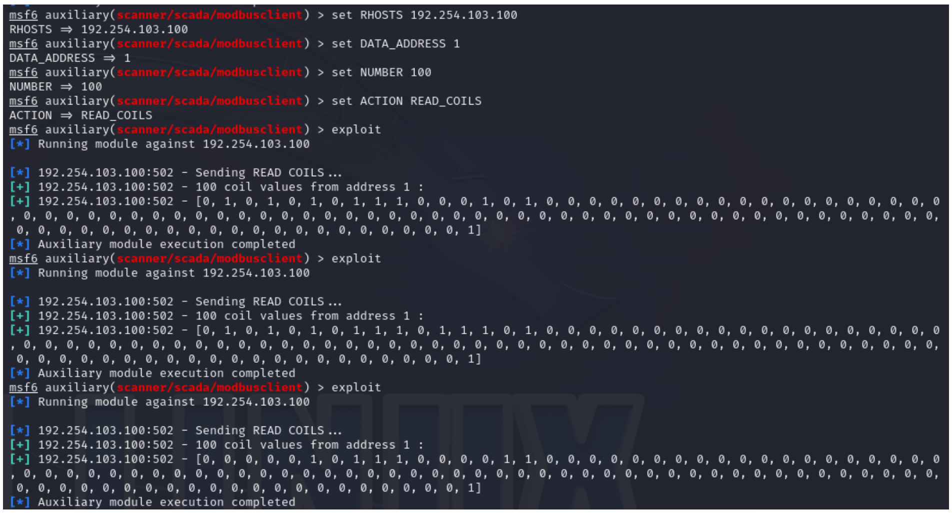


Figura 50. Metasploit. Lectura de bobinas

Finalmente, se lleva a cabo la escritura en las bobinas para perturbar el funcionamiento de la planta. Para ello, se ajusta el valor de la acción mediante el comando 'set ACTION WRITE_COIL', se especifica el número de bobinas en las que tendrá efecto la acción, en este caso 10, y se determina el valor a introducir, estableciéndolo en 1.

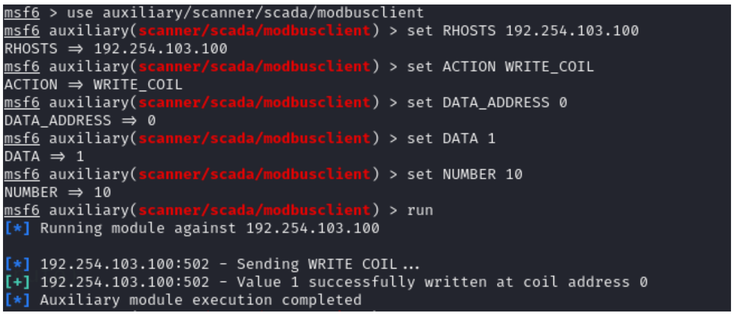


Figura 51. Metasploit. Escritura de datos en bobinas

En el escenario construido la frecuencia del PLC es elevada, por lo que es necesario ejecutar varias veces el exploit para alterar el funcionamiento de la planta. Para ello se ha realizado un script que toma las siguientes acciones:

- En primer lugar, se realiza una lectura de bobinas para comprobar el funcionamiento de la planta.
- Posteriormente, durante dos minutos se realiza consecutivamente la escritura del valor uno en las diez primeras bobinas.
- Tras esos dos minutos, se leen las bobinas para mostrar el efecto en el PLC.

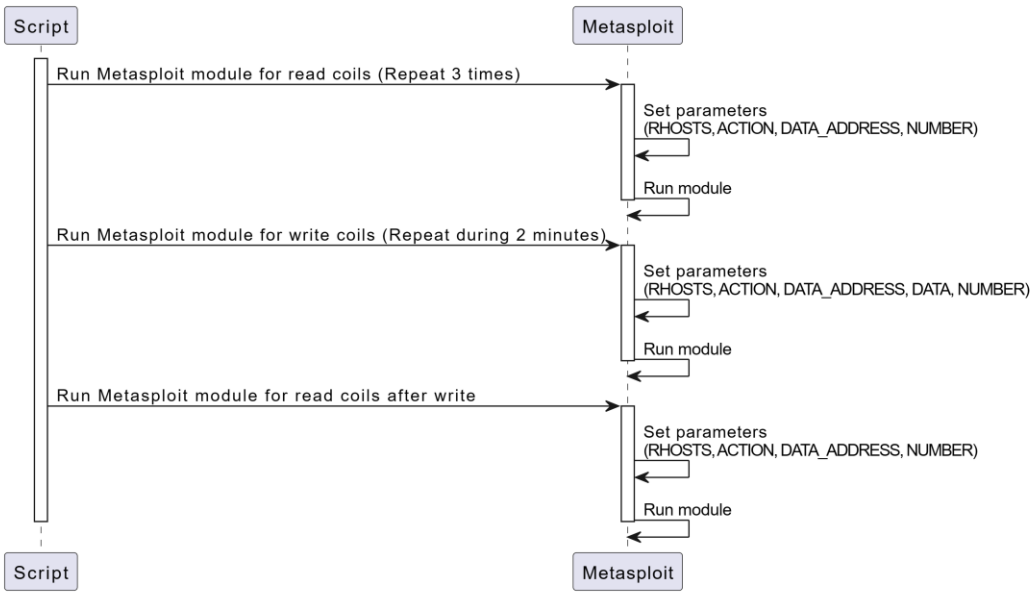


Figura 52. Metasploit. Script ejecución en bucle para modificación de datos

En el repositorio de github (ICSPentesting/Simulación Factory IO at main · estrellahc/ICSPentesting (github.com)) pueden encontrar un video donde se evidencia el impacto de la ejecución del script en la planta. Se observa cómo el brazo robot queda bloqueado después de realizar una escritura en las bobinas. Este ejemplo resalta los riesgos asociados con la manipulación remota de los sistemas industriales a través de protocolos como Modbus. La alteración no autorizada de las bobinas podría resultar en consecuencias graves, como el bloqueo de maquinaria crítica, deteniendo procesos de producción o incluso causando daños físicos a equipos y personal.

6.5.2 Man In the Middle (MITM)

Este estudio se centra en analizar uno de los ataques más preocupantes en el ámbito de la ciberseguridad: el "Man in the Middle" (MITM). Este tipo de ataque habilita a un intruso para interceptar y manipular la comunicación entre un cliente y un servidor, en este caso, entre un autómata y una planta industrial, comprometiendo así la confidencialidad e integridad de los datos transmitidos.

El proceso general de estos ataques sigue los siguientes pasos:

1. Intercepción: el atacante busca posicionarse entre cliente y servidor, interceptando todas las comunicaciones entre ambos. Esto puede lograrse mediante varias técnicas como el envenenamiento de tabla ARP, ataques basados en manipulaciones de servidores DHCP o DNS.
2. Redireccionamiento: una vez que el atacante ha interceptado el tráfico, debe redirigirlo a través de la infraestructura para que la comunicación cliente/servidor permanezca inalterada y sin cortes de conexión.
3. Manipulación de datos: en esta fase el atacante puede llevar a cabo acciones maliciosas para manipular los datos transmitidos como la modificación de los mensajes o la inserción de datos maliciosos.
4. Reenvío de datos legítimos: después de manipular los datos, el atacante reenvía al destinatario datos legítimos para que la comunicación parezca que no ha sido alterada.

En este capítulo, se realiza el primer paso del ataque, la intercepción, utilizando la técnica *"ARP Poisoning"*. Para llevar a cabo esta técnica es imprescindible conocer el funcionamiento del protocolo ARP.

El protocolo ARP lleva a cabo la traducción de direcciones IP a direcciones físicas de red. Un dispositivo envía una solicitud ARP a toda la red preguntando *"¿Quién tiene esta dirección IP?"*, y el dispositivo con esa IP especifica responde con su dirección MAC. Este dispositivo almacena esta información temporalmente en la tabla caché ARP.

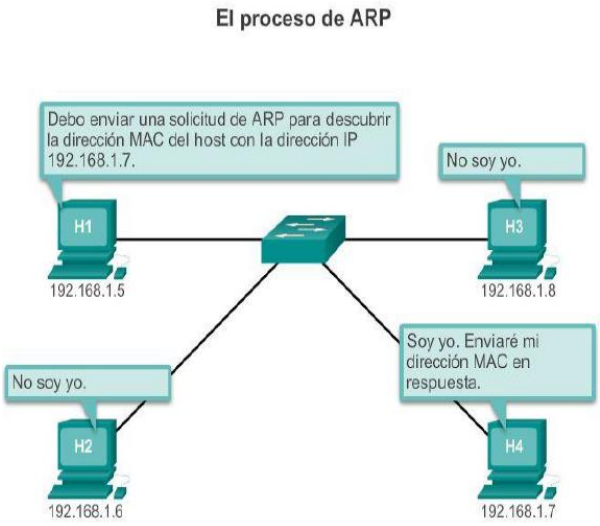


Figura 53. Funcionamiento protocolo ARP [58]

La técnica *ARP Spoofing* aprovecha la falta de autenticación del protocolo ARP. De esta forma, el atacante envía respuestas falsas a la red fingiendo poseer una dirección IP específica. Los dispositivos a los que llegan estos mensajes actualizan su tabla ARP asociando la MAC del atacante a la dirección IP en cuestión. Esto permite que el tráfico se desvíe hacia el atacante en lugar de llegar al destinatario de la comunicación.

Como se muestra en la siguiente imagen, en el escenario construido el atacante envía mensajes ARP con su dirección MAC periódicamente tanto al cliente como al servidor. El cliente y el servidor al recibir estas tramas añaden la dirección MAC del atacante a su tabla ARP, asumiendo que es la correspondiente al servidor y cliente, respectivamente. Una vez, que el ataque tenga éxito, el atacante se situará en medio de la comunicación y recibirá todas las tramas enviadas por cliente y servidor.

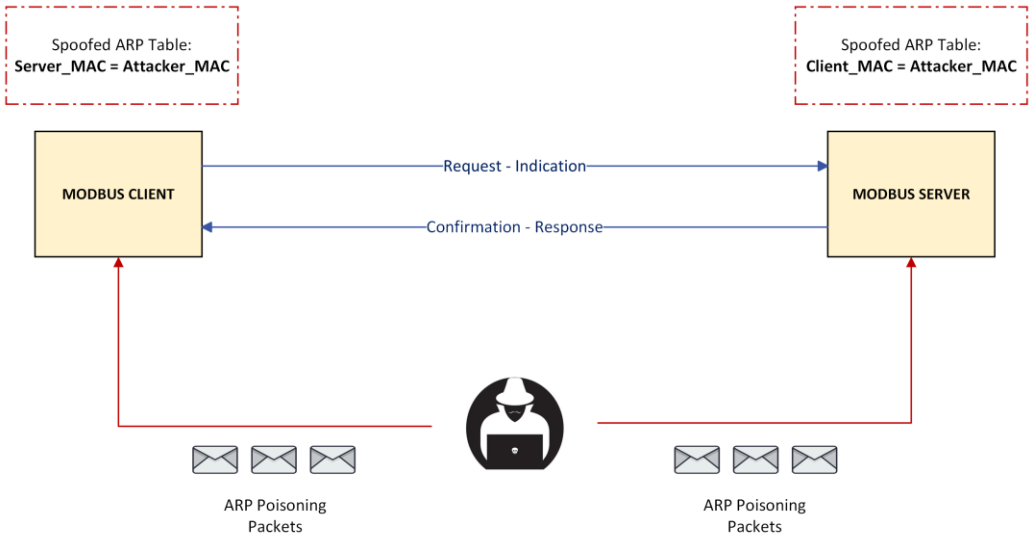


Figura 54. Diagrama ataque ARP Spoofing

La técnica ARP Spoofing se ha implementado haciendo uso de la herramienta Ettercap. Ettercap es una herramienta gratuita y de código abierto que puede lanzar ataques Man-in-the-Middle, además de analizar el tráfico de red, capturar contraseñas, etc. Esta herramienta se utiliza para análisis de redes y auditorias de seguridad y puede ejecutarse en varios sistemas operativos [59].

La herramienta Ettercap s ejecuta en la máquina atacante Kali Linux escribiendo en consola el comando: *sudo Ettercap -G*

Una vez que está abierta la interfaz de usuario de la aplicación se selecciona la interfaz de red que se desea inspeccionar, en este caso se selecciona *eth0*, ya que en la arquitectura construida el PLC y la planta se encuentran conectados a esta tarjeta de red.

Figura 55. Interfaz Ettercap

Tras pulsar en "Accept", se obtienen los resultados del escaneo de la red seleccionada, en este caso aparecen los dispositivos cliente y servidor (PLC y planta) identificados por su dirección IP y MAC.

Figura 56. Ettercap - Escaneo red

A continuación, se asignan servidor y cliente al objetivo uno y al objetivo dos pulsando en *"Add to Target 1"* y en *"Add To Target 2"* respectivamente. Esto permite determinar los dispositivos entre los que se situará el atacante.

Una vez que se han asignado los objetivos del ataque, se selecciona la opción *"ARP Poisoning"* como se muestra en la siguiente imagen, y se marca la opción *"Sniff remote connections"*.

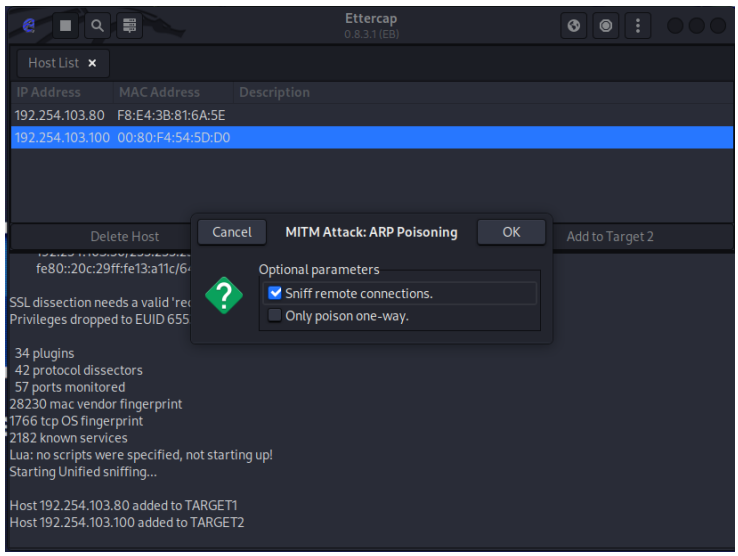


Figura 57. Ettercap - Configuración ARP Poisoning

Al hacer click en "Ok" comienza el ataque y las peticiones enviadas por el cliente Modbus son enviadas al atacante. Se debe tener en cuenta que, si el atacante no reenvía estos mensajes al servidor Modbus, la comunicación cliente/servidor se interrumpe, lo que puede resultar en cortes en el servicio y en la operación, con graves consecuencias en el entorno industrial.

Tras realizar este ataque con Ettercap, se analiza el tráfico de red utilizando la herramienta Wireshark, como se muestra en la figura siguiente. Se confirma que la conexión cliente/servidor se interrumpe en varias ocasiones, provocando la retrasmisión de tramas y pérdidas de datos.

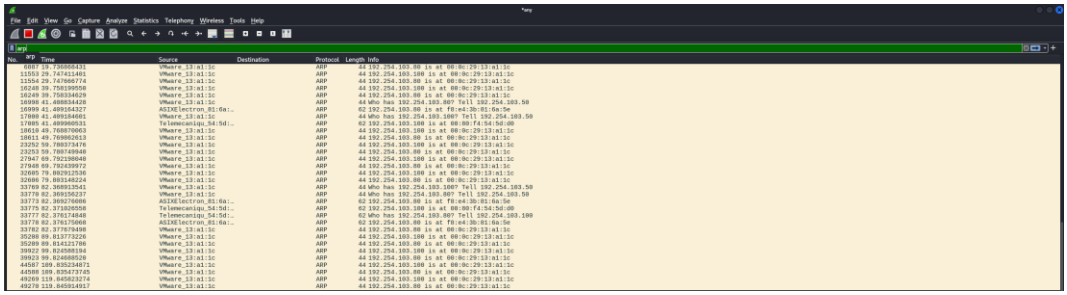


Figura 58. Wireshark - Mensajes enviados ARP Spoofing

Figura 59. Wireshark - Mensajes retransmitidos por ARP Spoofing

6.5.3 Análisis y Sniffing del Tráfico de Red

En las últimas etapas del ataque "Man in The Middle", como se ha mencionado previamente, el atacante procede a reenviar al destinatario datos legítimos con el fin de evitar que las víctimas detecten la alteración en la comunicación. Para lograr esto, el atacante primero debe obtener un conocimiento exhaustivo de la comunicación entre el autómata y la planta industrial. Esta comprensión detallada se puede adquirir interceptando los mensajes de una comunicación estándar entre cliente y servidor, permitiendo al atacante analizar las tramas intercambiadas para entender su estructura y contenido.

Para espiar la comunicación se utilizan herramientas de análisis de tráfico como Wireshark o Scapy. En este caso se ha optado por utilizar Scapy, una potente biblioteca de manipulación de paquetes escrita en Python. Scapy permite codificar y decodificar paquetes de multitud de protocolos, enviarlos por la red, capturarlos y encontrar solicitudes y respuestas [60].

Se ha desarrollado un script utilizando esta herramienta para capturar todos los mensajes dirigidos al puerto 502, el puerto estándar para las comunicaciones Modbus. Este script, tras identificar si la trama pertenece al protocolo Modbus, procede a extraer cada uno de los campos que la componen, siguiendo las especificaciones documentadas del protocolo Modbus. Es importante destacar que esta documentación es de conocimiento público y accesible. Una vez que se obtiene toda esta información, se almacena trama por trama en una base de datos, y los datos de cada campo se organizan en columnas correspondientes.

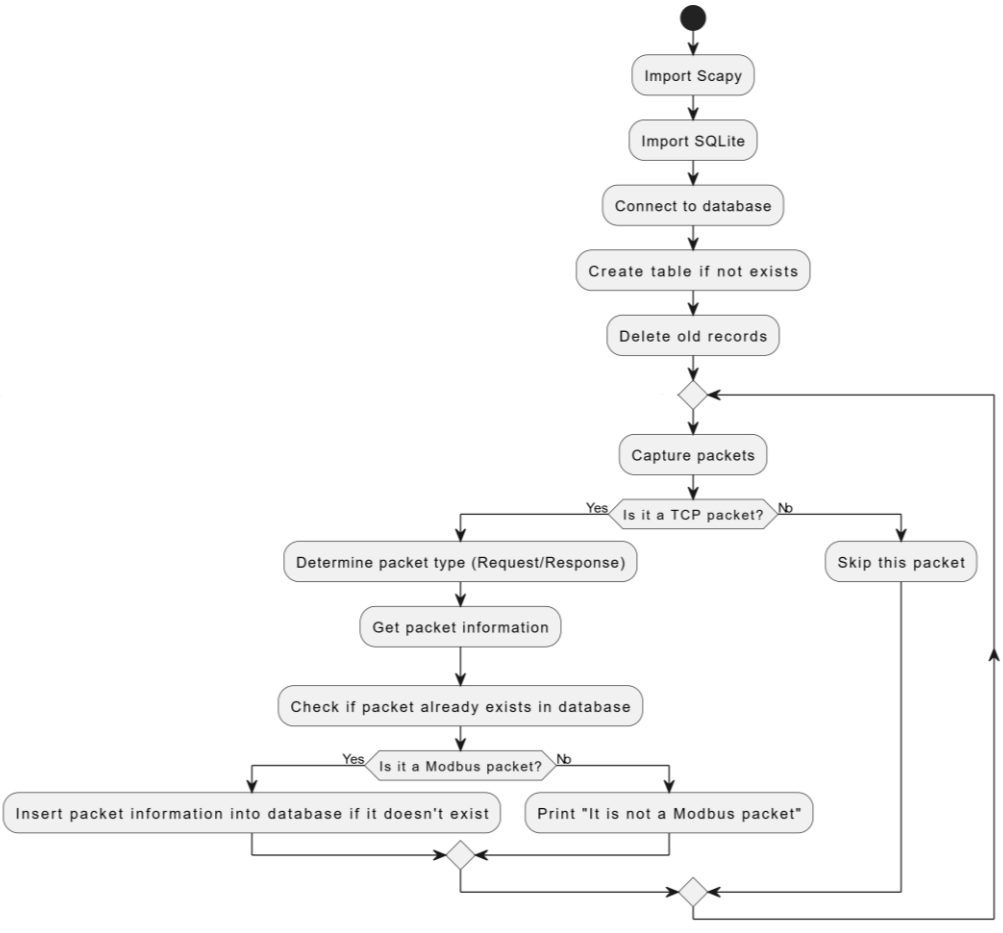


Figura 60. Diagrama UML script "Sniffing"

Este script se ejecuta durante un periodo de tiempo prolongado que permita capturar todos los mensajes disponibles en la red.

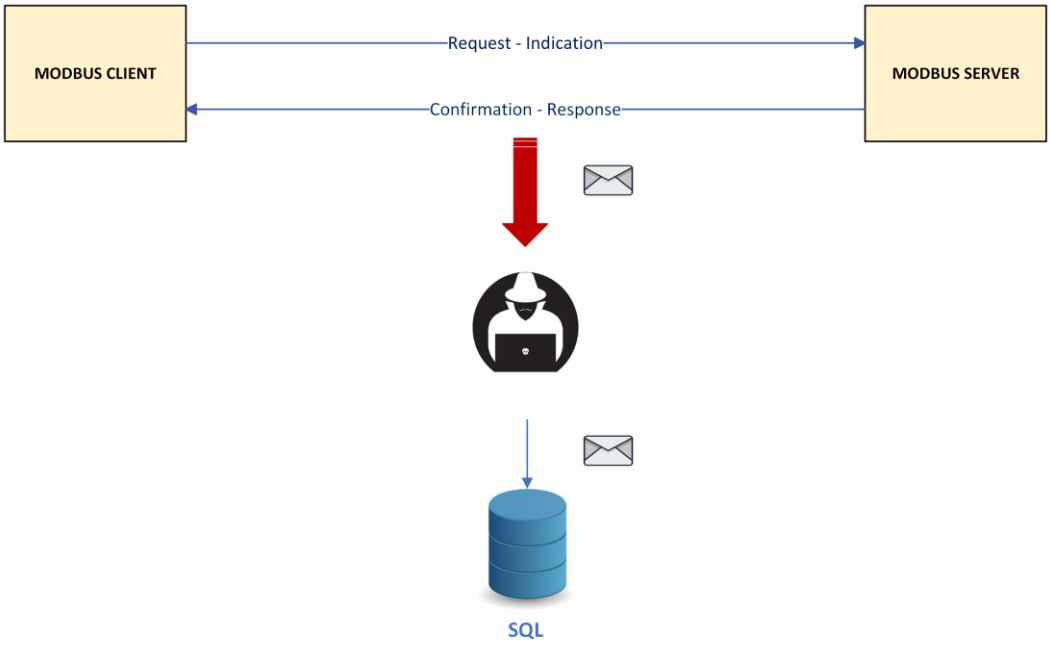
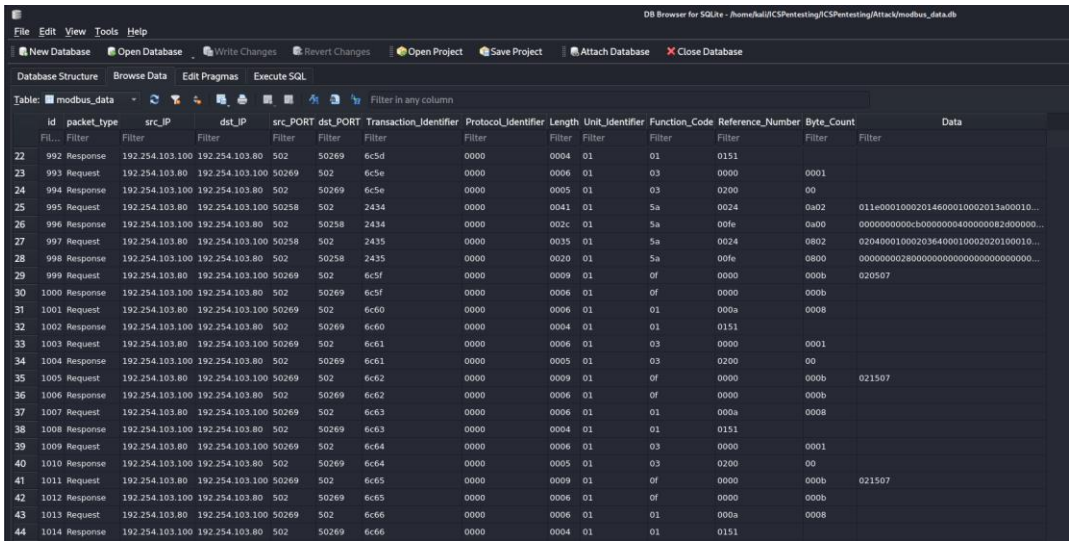


Figura 61. Diagrama funcionamiento Sniffing

Después de esto toda la información referente a la comunicación del PLC con la planta estará almacenada en la base de datos.



	id	packet_type	src_IP	dst_IP	src_PORT	dst_PORT	Transaction_Identifier	Protocol_Identifier	Length	Unit_Identifier	Function_Code	Reference_Number	Byte_Count	Data
22	992	Response	192.254.103.100	192.254.103.80	502	50269	6c5d	0000	0004	01	01	0151		
23	993	Request	192.254.103.80	192.254.103.100	50269	502	6c5e	0000	0006	01	03	0000	0001	
24	994	Response	192.254.103.100	192.254.103.80	502	50269	6c5e	0000	0005	01	03	0200	00	
25	995	Request	192.254.103.80	192.254.103.100	50258	502	2434	0000	0041	01	5a	0024	0a02	011e0001000201460001000201 3a00010...
26	996	Response	192.254.103.100	192.254.103.80	502	50258	2434	0000	002c	01	5a	00fe	0a00	0000000000cb0000000400000082d00000...
27	997	Request	192.254.103.80	192.254.103.100	50258	502	2435	0000	0035	01	5a	0024	0802	0204000100020364000100020201000 10...
28	998	Response	192.254.103.100	192.254.103.80	502	50258	2435	0000	0020	01	5a	00fe	0800	0000000028000000000000000000000...
29	999	Request	192.254.103.80	192.254.103.100	50269	502	6c5f	0000	0009	01	0f	0000	000b	020507
30	1000	Response	192.254.103.100	192.254.103.80	502	50269	6c5f	0000	0006	01	0f	0000	000b	
31	1001	Request	192.254.103.80	192.254.103.100	50269	502	6c60	0000	0006	01	01	000a	0008	
32	1002	Response	192.254.103.100	192.254.103.80	502	50269	6c60	0000	0004	01	01	0151		
33	1003	Request	192.254.103.80	192.254.103.100	50269	502	6c61	0000	0006	01	03	0000	0001	
34	1004	Response	192.254.103.100	192.254.103.80	502	50269	6c61	0000	0005	01	03	0200	00	
35	1005	Request	192.254.103.80	192.254.103.100	50269	502	6c62	0000	0009	01	0f	0000	000b	021507
36	1006	Response	192.254.103.100	192.254.103.80	502	50269	6c62	0000	0006	01	0f	0000	000b	
37	1007	Request	192.254.103.80	192.254.103.100	50269	502	6c63	0000	0006	01	01	000a	0008	
38	1008	Response	192.254.103.100	192.254.103.80	502	50269	6c63	0000	0004	01	01	0151		
39	1009	Request	192.254.103.80	192.254.103.100	50269	502	6c64	0000	0006	01	03	0000	0001	
40	1010	Response	192.254.103.100	192.254.103.80	502	50269	6c64	0000	0005	01	03	0200	00	
41	1011	Request	192.254.103.80	192.254.103.100	50269	502	6c65	0000	0009	01	0f	0000	000b	021507
42	1012	Response	192.254.103.100	192.254.103.80	502	50269	6c65	0000	0006	01	0f	0000	000b	
43	1013	Request	192.254.103.80	192.254.103.100	50269	502	6c66	0000	0006	01	01	000a	0008	
44	1014	Response	192.254.103.100	192.254.103.80	502	50269	6c66	0000	0004	01	01	0151		

Figura 62. Mensajes almacenados en la base de datos tras espiar la comunicación

Al analizar las tramas, se observa que un par de petición y respuesta comparten tres parámetros de la trama: *"Transaction_Identifier"*, *"Unit_Identifier"* y *"Function_Code"*. Estos parámetros sirven para identificar una transacción única entre un cliente y un servidor Modbus, señalar al dispositivo esclavo al que el cliente desea comunicarse e indicar al dispositivo esclavo qué tipo de operación se está solicitando en la comunicación Modbus, respectivamente.

Estos mensajes no solo proporcionan información sobre las operaciones realizadas en la operación, sino que también permiten agrupar las solicitudes con sus respectivas respuestas, lo que permite al atacante cumplir su objetivo de hacerse pasar por los dispositivos víctimas del

ataque.

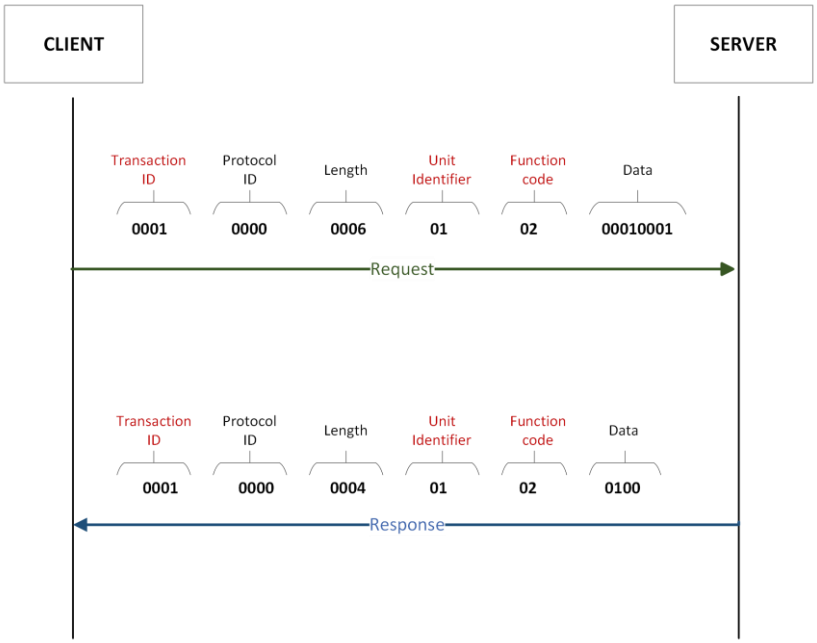


Figura 63. Estructura de mensajes petición- respuesta en comunicación Modbus

Con esta información en la base de datos, cuando un atacante se interponga en la comunicación, esperará hasta que el cliente envíe una solicitud. Luego, el atacante inspeccionará el paquete y, basándose en los parámetros identificativos, determinará el paquete de respuesta correspondiente.

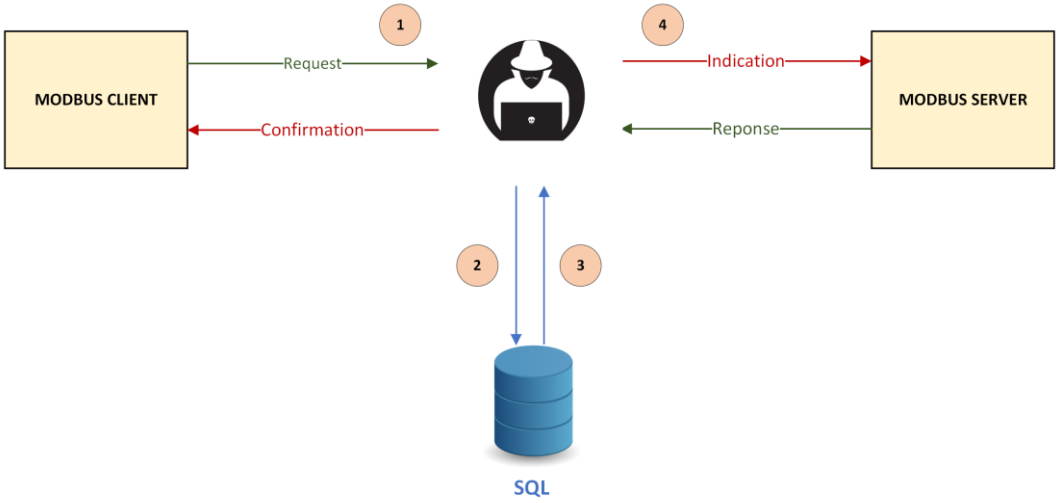


Figura 64. Diagrama funcionamiento MITM

En esta fase, el atacante intercepta el tráfico de red para capturar las tramas intercambiadas entre el autómata y la planta. El objetivo principal es espiar toda la comunicación, extrayendo y examinando cada parámetro de las tramas, esto puede ser realmente útil para replicar la comunicación y suplantar la identidad de las víctimas sin perturbar la comunicación normal.

Los paquetes recopilados durante este proceso podrían ser inspeccionados para detectar que campos podrían ser manipulados. Luego, Scapy permite modificar estos paquetes o construir nuevos paquetes desde cero, cambiando campos específicos como identificadores de

transacción, códigos de función o cualquier otro dato relevante en el protocolo Modbus.

Durante este proceso, los paquetes capturados se someten a un escrutinio detallado para identificar qué campos son susceptibles de ser manipulados. Utilizando Scapy, el atacante tiene la capacidad de alterar estos paquetes o incluso de crear nuevos desde cero, modificando aspectos específicos como los identificadores de transacción, los códigos de función o cualquier otro dato pertinente dentro del protocolo Modbus.

6.6 Fase VI. Documentación y Análisis de Resultados

En este capítulo se describen los resultados obtenidos tras el estudio realizado durante el proceso de pruebas de penetración. A lo largo de esta investigación, se han identificado múltiples vulnerabilidades inherentes en el protocolo Modbus. A partir de los hallazgos del estudio, se proponen diversas medidas de seguridad enfocadas en fortalecer las redes industriales que utilizan este protocolo, con el objetivo de proteger los dispositivos y sistemas implicados frente a potenciales amenazas y explotaciones maliciosas.

Durante las etapas iniciales del estudio de seguridad sobre el protocolo Modbus, se ha descubierto una gran cantidad de equipos industriales que aún mantienen configuraciones con contraseñas por defecto. Esta práctica común representa una debilidad significativa, ya que permite el acceso no autorizado a dispositivos y sistemas, que podría conllevar una alteración en el funcionamiento de estos.

Además, la utilización de herramientas de búsqueda avanzada como Google Dorks y Shodan ha revelado una alarmante cantidad de dispositivos y servidores industriales expuestos a Internet. Este hallazgo es particularmente preocupante porque proporciona a los atacantes información valiosa que podría ser explotada para lanzar ataques dirigidos.

Posteriormente, se ha procedido a una fase más técnica de enumeración y escaneo utilizando Nmap, una herramienta esencial en el arsenal de cualquier auditor de seguridad. Esta fase ha permitido identificar detalles críticos de la infraestructura de red, como los puertos abiertos, direcciones IP activas y direcciones MAC de los dispositivos conectados. Conocer esta información es fundamental, ya que establece las bases para las etapas de explotación y manipulación de la red y sus componentes.

En la fase de explotación, se ha mostrado cómo las inherentes debilidades del protocolo Modbus pueden ser aprovechadas para comprometer la seguridad de un sistema de control. Se han realizado pruebas efectivas que han permitido tanto la lectura como la escritura en los registros del controlador con la herramienta Metasploit. Esto no solo ha revelado información sobre el funcionamiento y las acciones controladas por el PLC, sino que también ha permitido alterar directamente el funcionamiento de la planta. Además, se han explotado las vulnerabilidades del protocolo ARP para realizar ataques de inundación, permitiendo al atacante posicionarse estratégicamente en la comunicación entre dispositivos para manipularla a su favor.

Una de las debilidades más críticas identificadas en el protocolo Modbus es su falta de encriptación. Las comunicaciones se realizan en texto plano, facilitando ataques de interceptación y manipulación como los de tipo Man In The Middle (MITM). Estos ataques han permitido no solo capturar información en tránsito sino también modificarla, lo que podría tener consecuencias devastadoras en un entorno industrial. La ausencia de un sistema robusto de autenticación y de verificación de integridad de las tramas permite a los atacantes alterar y replicar comandos, mientras que la falta de marcas de tiempo en las tramas deja a los dispositivos incapaces de discernir si las respuestas recibidas son recientes o han sido maliciosamente retrasadas o replicadas.

A raíz de estos hallazgos, se considera necesario adoptar medidas de seguridad robustas para proteger las redes industriales que utilizan este protocolo. A continuación, se detallan algunas recomendaciones clave diseñadas para mitigar los riesgos identificados y fortalecer la seguridad de los dispositivos y sistemas implicados:

- **Establecimiento de políticas de contraseñas**: es necesario reemplazar las contraseñas por defecto por credenciales seguras y únicas en cada dispositivo dentro de la red. Se aconseja el uso de contraseñas complejas que incluyan mayúsculas, minúsculas, símbolos y números. Es necesario realizar actualizaciones periódicas de estas contraseñas para evitar accesos no autorizados.
- **Restricciones de acceso**: esta medida consiste en permitir el acceso a determinadas partes de Internet únicamente a los dispositivos y usuarios que lo requieran. Para ello, se recomienda la utilización de firewalls con reglas restrictivas que limiten el acceso de los dispositivos tanto desde dentro como desde fuera de la red industrial. Además, como se ha detallado en el capítulo 5.4, es muy recomendable la implementación de sistemas de detección y prevención de intrusiones (IPS/IDS) para controlar el tráfico entre dispositivos y zonas del sistema de control.
- **Implementación de Redes Privadas Virtuales (VPN)**: las VPNs son necesarias para asegurar las conexiones remotas, proporcionando un canal de comunicación cifrado que protege contra ataques externos al sistema.
- **Segmentación de la red**: como se ha visto en el capítulo 5.2, esta medida divide la red en segmentos más pequeños, limitando así la propagación de ataques y reduciendo la superficie de exposición. Al restringir el movimiento lateral de posibles amenazas, se mitigan los riesgos asociados a los ataques cibernéticos.
- **Mantenimiento y actualización de sistemas**: es importante aplicar parches de seguridad siempre que sea posible sin alterar la producción para proteger el sistema de vulnerabilidades ya conocidas.
- **Monitorización y auditorias frecuentes**: la implementación de herramientas de monitoreo de red que detecten actividades sospechosas o inusuales es fundamental. Asimismo, se deben realizar auditorías de seguridad periódicas para evaluar la robustez de las medidas de seguridad y descubrir nuevas vulnerabilidades potenciales.
- **Formación del personal implicado en las operaciones**: informar y capacitar a los empleados sobre las mejores prácticas de seguridad, incluidas las estrategias para reconocer intentos de phishing y otras técnicas de ingeniería social, es crucial. La formación continua puede prevenir brechas de seguridad que se originen por errores humanos.

A pesar de la aplicación de todas estas medidas, es importante reconocer que ningún sistema es completamente seguro, como afirmó Gene Spafford: *"El único sistema informático seguro es aquel que está apagado, en el interior de un bloque de hormigón y protegido dentro de una habitación sellada rodeada por guardias armados. E incluso así tengo mis dudas"*. Sin embargo, la implementación de estas recomendaciones reduce significativamente la probabilidad de sufrir un ataque y limita el riesgo al sistema. En caso de un incidente, estas medidas aseguran la aplicación de protocolos de respuesta adecuados para minimizar el impacto en el sistema, sobre todo para el factor más crítico en estos sistemas, la producción.

7 CONCLUSIONES Y LÍNEAS FUTURAS

En conclusión, se considera que este estudio ha cumplido con sus objetivos al combinar un análisis teórico detallado con pruebas prácticas de *pentesting* para abordar la ciberseguridad en sistemas de control industrial.

A lo largo del trabajo, se ha llevado a cabo una revisión precisa de la literatura existente y las normativas relevantes como la ISA 62443, estableciendo un marco teórico sólido que resalta la importancia de proteger la infraestructura industrial frente a amenazas cibernéticas. Los hallazgos teóricos han proporcionado la comprensión profunda de los retos y vulnerabilidades específicas que enfrentan estos sistemas.

Complementando la teoría, las pruebas de *pentesting* realizadas han permitido identificar vulnerabilidades prácticas y evaluar la eficacia de las medidas de seguridad actuales. Estas pruebas han revelado brechas significativas que pueden ser explotadas, subrayando la necesidad de implementar estrategias de seguridad más robustas y adaptativas. Se pretende que ambos enfoques construyan una base para futuras investigaciones y mejoras, con el objetivo de fortalecer la resiliencia de los sistemas de control industrial contra ataques cibernéticos, asegurando así la continuidad operativa y la integridad de infraestructuras críticas.

A continuación, se proponen algunas líneas futuras que pueden usar este trabajo como base para desarrollar tecnologías y aplicar técnicas que aseguren la protección de los sistemas de control industrial. Estas propuestas buscan no solo mitigar los riesgos existentes sino también preparar los sistemas para responder de manera proactiva y autónoma ante futuras amenazas.

- ***Machine Learning y Deep Learning***: se recomienda explorar el uso de técnicas avanzadas de Machine Learning y Deep Learning para la creación de sistemas de detección avanzados. Estos sistemas no solo identificarán ataques de manera precoz, sino que también facilitarán respuestas automáticas y adecuadas a las amenazas detectadas. Mediante la implementación de estos métodos, es posible desarrollar modelos predictivos que aprendan de interacciones pasadas y ajusten dinámicamente la configuración de seguridad, como el cierre automático de tráfico de red sospechoso [61].
- ***Fuzzy Control Systems***: los sistemas de control borroso utilizan lógica difusa para procesar datos que son ambiguos o imprecisos, permitiendo decisiones basadas en grados de verdad en lugar de binarios absolutos. Esta capacidad los hace ideales para la ciberseguridad industrial, donde la detección precisa de amenazas a menudo involucra interpretar señales sutiles o parcialmente verdaderas. Al aplicar sistemas de control borroso, se puede mejorar significativamente la detección de comportamientos sospechosos y la respuesta a incidentes, adaptando las medidas de seguridad en tiempo real y con gran sensibilidad a la naturaleza dinámica de las amenazas cibernéticas. Esta tecnología promete transformar las estrategias de defensa, haciendo que los sistemas de control industrial no solo sean más seguros, sino también más inteligentes y proactivos ante las amenazas emergentes [62].
- ***Tecnología Blockchain***: esta es una tecnología de registro distribuido que crea una cadena segura y verificable de bloques de datos, cada uno cifrado y conectado al anterior. En entornos industriales, donde los protocolos de comunicación pueden ser vulnerables a ataques debido a la falta de robustas medidas de seguridad como la autenticación avanzada y la integridad de los datos, el blockchain ofrece soluciones esenciales. Permite la autenticación segura de dispositivos en la red, garantizando que solo los actores verificados y autorizados puedan acceder y operar dentro del sistema. Además, mejora la auditabilidad y la transparencia, asegurando que todas las transacciones y comunicaciones sean rastreables y resistentes a manipulaciones. Al implementar blockchain, las redes industriales pueden mejorar significativamente su seguridad, mitigando riesgos y fortaleciendo la gestión de las comunicaciones entre dispositivos [63].

REFERENCIAS

[1] "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries." Accessed: Mar. 04, 2024. [Online]. Available: https://www.bcg.com/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries

[2] "El virus que tomó control de mil máquinas y les ordenó autodestruirse - BBC News Mundo." Accessed: Jun. 03, 2023. [Online]. Available: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[3] "Gusano informático Stuxnet: ¿cuál es el legado actual?" Accessed: Jun. 03, 2023. [Online]. Available: https://www.stormshield.com/es/noticias/stuxnet-que-lecciones-podemos-aprender-doce-anos-despues/

[4] "Ciberataques a infraestructuras críticas: los coletazos de un conflicto." Accessed: Dec. 16, 2023. [Online]. Available: https://www.welivesecurity.com/la-es/2022/12/21/ciberataques-infraestructuras-criticas-tendencias-ciberseguridad/

[5] "Sandworm Team, ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, Voodoo Bear, IRIDIUM, Group G0034 | MITRE ATT&CK®." Accessed: Dec. 16, 2023. [Online]. Available: http://attack.mitre.org/groups/G0034/

[6] "ICS Focused Malware | CISA." Accessed: Dec. 16, 2023. [Online]. Available: https://www.cisa.gov/news-events/ics-advisories/icsa-14-178-01

[7] "Industroyer: la mayor amenaza para sistemas de control industrial desde Stuxnet | WeLiveSecurity." Accessed: Jun. 04, 2023. [Online]. Available: https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/

[8] "Threat Intelligence Solutions | Cyber Security Services & Training." Accessed: May 22, 2024. [Online]. Available: https://www.mandiant.com/

[9] "CrashOverride: El malware para SCI ataca de nuevo | INCIBE-CERT | INCIBE." Accessed: Dec. 16, 2023. [Online]. Available: https://www.incibe.es/incibe-cert/blog/crashoverride-el-malware-sci-ataca-nuevo

[10] "TRISIS Malware Analysis of Safety System Targeted Malware", Accessed: Dec. 16, 2023. [Online]. Available: www.dragos.com

[11] "Industrial Cybersecurity Technology for ICS/OT Asset Visibility | Dragos." Accessed: May 22, 2024. [Online]. Available: https://www.dragos.com/

[12] "INCONTROLLER/PIPEDREAM: amenaza APT dirigida a dispositivos SCI/SCADA | INCIBE-CERT | INCIBE." Accessed: Dec. 16, 2023. [Online]. Available: https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/incontrollerpipedream-amenaza-apt-dirigida-dispositivos-sciscada

[13] "Retos de ciberseguridad para la digitalización industrial | Seguridad | IT Trends." Accessed: Mar. 05, 2024. [Online]. Available: https://www.ittrends.es/seguridad/2022/09/retos-de-ciberseguridad-para-la-digitalizacion-industrial

[14] "Ciberseguridad industrial: principales desafíos en este año 2021." Accessed: Mar. 05, 2024. [Online]. Available: https://www.redseguridad.com/sectores/industria/principales-desafios-de-la-ciberseguridad-industrial-en-2021_20210125.html

[15] C. J. Brooks and P. A. Craig, Jr., Practical Industrial Cybersecurity: ICS, Industry 4.0, and IIoT. 1st ed. Hoboken, NJ, USA: John Wiley & Sons, 2022.

[16] "Qué es una RTU | Becolve digital." Accessed: Oct. 30, 2023. [Online]. Available:

https://becolve.com/blog/que-es-una-rtu/

[17] P. Ackerman and an O. M. Company. Safari, *Industrial cybersecurity : efficiently monitor the cybersecurity posture of your ICS environment*.

[18] "MODBUS Application Protocol Specification V1.1b3 Modbus," 2012. [Online]. Available: http://www.modbus.org

[19] Modbusorg, "MODBUS Messaging on TCP/IP Implementation Guide V1.0b Modbus Organization," 2006. [Online]. Available: http://www.Modbus.org

[20] F. H. Hsu, Y. L. Hwang, C. Y. Tsai, W. T. Cai, C. H. Lee, and K. W. Chang, "TRAP: A Three-Way Handshake Server for TCP Connection Establishment," *Applied Sciences 2016, Vol. 6, Page 358*, vol. 6, no. 11, p. 358, Nov. 2016, doi: 10.3390/APP6110358.

[21] "TCP: How the Transmission Control Protocol works - IONOS." Accessed: Mar. 15, 2024. [Online]. Available: https://www.ionos.co.uk/digitalguide/server/know-how/introduction-to-tcp/

[22] "PROFIBUS: Qué es y cómo funciona - Cursos Centro de Entrenamiento Internacional de PROFIBUS & PROFINET." Accessed: May 22, 2024. [Online]. Available: https://profibus.com.ar/profibus_que_es_y_como_funciona/

[23] P. José, A. Espada, R. Capilla, L. Co-, and C. Sánchez Díaz, "DISEÑO PLACA DE COMUNICACIÓN POR BUSES INDUSTRIALES PARA ARDUINO®".

[24] "Download - www.profibus.com." Accessed: May 22, 2024. [Online]. Available: https://www.profibus.com/download/profinet-security-guideline/

[25] Instituto Nacional de Ciberseguridad (INCIBE), "Protocolos y seguridad de red en infraestructuras SCI," https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe_protocolos_seguridad_red_sci.pdf.

[26] D. Committee, S. Committee of the IEEE Power, and E. Society, "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3) Sponsored by the Transmission and Distribution Committee and Substations Committee IEEE Power and Energy Society," 2012.

[27] Overview of DNP3 Security, Version 6, [Online]. Available: https://es.scribd.com/document/562698812/Overview-of-DNP3-Security-Version-6-2020-01-21. Accessed on May 23, 2024.

[28] R. L. Krutz and R. D. Vines, "The CEH ™ Prep Guide: The Comprehensive Guide to Certified Ethical Hacking."

[29] "Cyber Kill Chain® | Lockheed Martin." Accessed: May 21, 2024. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[30] M. J. Assante and R. M. Lee, "The Industrial Control System Cyber Kill Chain," 2015, Accessed: Oct. 01, 2023. [Online]. Available: www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[31] "¿Qué es un vector de ataque en ciberseguridad?" Accessed: Nov. 01, 2023. [Online]. Available: https://keepcoding.io/blog/que-es-un-vector-de-ataque-en-ciberseguridad/#Que_es_un_vector_de_ataque_en_ciberseguridad

[32] "OT ICEFALL: The legacy of 'insecure by design' and its implications for certifications and risk management," Thales Group, 07 Dec. 2023. [Online]. Available: https://cds.thalesgroup.com/en/node/321. Accessed on May 23, 2024.

[33] E. D. Knapp and J. T. Langill, *Industrial network security : securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*.

[34] "ISO - ISO/IEC 27000 family — Information security management." Accessed: Mar. 17, 2024.

[Online]. Available: https://www.iso.org/standard/iso-iec-27000-family

[35] K. Stouffer *et al.*, "NIST Special Publication NIST SP 800-82r3 Guide to Operational Technology (OT) Security", doi: 10.6028/NIST.SP.800-82r3.

[36] "Implementing the NIST Risk Management Framework - TalaTek, LLC." Accessed: May 06, 2024. [Online]. Available: https://talatek.com/solutions/integrated-risk-management-services-public-sector/

[37] "RELIABILITY | RESILIENCE | SECURITY CIP Definitions Modifications to CIP Standards," 2016.

[38] "Desglosando las normas de Ciberseguridad Industrial | Anixter." Accessed: Mar. 19, 2024. [Online]. Available: https://www.anixter.com/es_mx/resources/literature/techbriefs/breaking-down-industrial-cybersecurity-standards.html

[39] "Reliability Standards." Accessed: Mar. 19, 2024. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[40] "Understanding IEC 62443." Accessed: Nov. 09, 2023. [Online]. Available: https://www.iec.ch/blog/understanding-iec-62443

[41] "The Essential Guide to the IEC 62443 industrial cybersecurity standards - Industrial Cyber." Accessed: Nov. 09, 2023. [Online]. Available: https://industrialcyber.co/features/the-essential-guide-to-the-iec-62443-industrial-cybersecurity-standards/

[42] "Segmentación de la red OT como medida de seguridad en ICS." Accessed: Mar. 07, 2024. [Online]. Available: https://www.mytra.es/blog-post/segmentacion-de-redes-ot-mejores-practicas-de-implementacion-y-consideraciones-clave

[43] "Segmentación de la red OT como medida de seguridad en ICS." Accessed: May 06, 2024. [Online]. Available: https://www.mytra.es/blog-post/segmentacion-de-redes-ot-mejores-practicas-de-implementacion-y-consideraciones-clave

[44] "Zonas y conductos, protegiendo nuestra red industrial | INCIBE-CERT | INCIBE." Accessed: Nov. 07, 2023. [Online]. Available: https://www.incibe.es/incibe-cert/blog/zonas-y-conductos-protegiendo-nuestra-red-industrial

[45] P. Ackerman, *Industrial cybersecurity : efficiently secure critical infrastructure systems*.

[46] by Paul Baybutt Primatech Inc, "AUDIT PROTOCOLS FOR INDUSTRIAL CYBER SECURITY," 2003, Accessed: Nov. 11, 2023. [Online]. Available: www.primatech.com

[47] E. D. Knapp and J. T. Langill, *Industrial network security : securing critical infrastructure networks for Smart Grid, SCADA, and other industrial control systems*.

[48] "PenTest: testes de penetração – TI para seus negócios." Accessed: May 07, 2024. [Online]. Available: https://cybergo.com.br/pentest-testes-de-penetracao/

[49] "Pentesting o Prueba de Penetración: Qué Es y Tipos." Accessed: May 04, 2024. [Online]. Available: https://www.deltaprotect.com/blog/que-es-pentesting

[50] "incibe_protocolos_seguridad_red_sci".

[51] "Catalyst Switched Port Analyzer (SPAN) Configuration Example - Cisco." Accessed: Jun. 10, 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html#anc6

[52] "Diseño y configuración de IPS, IDS y SIEM en Sistemas de Control Industrial | INCIBE-CERT | INCIBE." Accessed: May 12, 2024. [Online]. Available: https://www.incibe.es/incibe-cert/guias-y-estudios/guias/diseno-y-configuracion-de-ips-ids-y-siem-en-sistemas-de-control-industrial

[53] "Despliegue de SIEM en entornos TO | INCIBE-CERT | INCIBE." Accessed: Nov. 07, 2023. [Online]. Available: https://www.incibe.es/incibe-cert/blog/despliegue-de-siem-en-entornos

[54] “Que es OSINT - Servicios Informáticos profesionales.” Accessed: May 12, 2024. [Online]. Available: https://laeliteweb.com/que-es-osint/

[55] “Shodan Search Engine.” Accessed: Jan. 24, 2024. [Online]. Available: https://www.shodan.io/dashboard

[56] “Metasploit Basics, Part 16: Metasploit SCADA Hacking.” Accessed: May 01, 2024. [Online]. Available: https://www.hackers-arise.com/post/2018/10/22/Metasploit-Basics-Part-16-Metasploit-SCADA-Hacking

[57] “¿Qué es Metasploit Framework y cómo funciona? | Ciberseguridad.” Accessed: Apr. 28, 2024. [Online]. Available: https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

[58] “Ingeniería Systems: Introducción a ARP y funciones del protocolo ARP - CCNA1 V5 - CISCO C5.” Accessed: May 12, 2024. [Online]. Available: https://www.ingenieriasystems.com/2016/12/Introduccion-a-ARP-y-funciones-del-protocolo-ARP-CCNA1-V5-CISCO-C5.html

[59] “Tutorial de Ettercap con Ejemplos de Ataques » EsGeeks.” Accessed: Mar. 10, 2024. [Online]. Available: https://esgeeks.com/tutorial-ettercap-ejemplos/

[60] “Scapy.” Accessed: Mar. 10, 2024. [Online]. Available: https://scapy.net/

[61] A. Jaramillo-Alcazar, J. Govea, and W. Villegas-Ch, “Anomaly Detection in a Smart Industrial Machinery Plant Using IoT and Machine Learning,” *Sensors 2023, Vol. 23, Page 8286*, vol. 23, no. 19, p. 8286, Oct. 2023, doi: 10.3390/S23198286.

[62] M. Noguera, B. Millán, A. J. Barragán, M. A. Martínez, F. Segura, and J. M. Andújar, “Detección de ataques de inyección de datos falsos en turbinas eólicas mediante sistemas neuro-borrosos,” *XVII Simposio CEA de Control Inteligente. 27-29 de junio de 2022, León.*, pp. 66–77, 2022, doi: 10.18002/simceaci.

[63] “Construyendo comunicaciones seguras, Blockchain en la industria 4.0 | INCIBE-CERT | INCIBE.” Accessed: May 12, 2024. [Online]. Available: https://www.incibe.es/incibe-cert/blog/construyendo-comunicaciones-seguras-blockchain-industria-40

[64] “¿Qué es una vulnerabilidad Zero Day? | Ciudadanía | INCIBE.” Accessed: Dec. 15, 2023. [Online]. Available: https://www.incibe.es/ciudadania/blog/que-es-una-vulnerabilidad-zero-day

[65] “¿Qué es una amenaza avanzada persistente (APT)?” Accessed: Dec. 16, 2023. [Online]. Available: https://latam.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[66] “IEC 61131-3:2013 | Normas AENOR.” Accessed: Dec. 15, 2023. [Online]. Available: https://tienda.aenor.com/norma-iec-61131-3-2013-4552

[67] J. F. Kurose, *Computer networking : a top-down approach*, Eight edition. Gl... Harlow, England: Pearson Education, 2022.

Anexo I: Guía Usuario Factory IO

Esta guía proporciona una descripción detallada del software de virtualización de plantas industriales Factory IO. Se incluye una breve descripción del software y se explica cómo obtenerlo. Además, se detalla el proceso de conexión de la planta, estableciendo una comunicación mediante el protocolo Modbus para controlar la planta desde un controlador lógico programable.

Factory IO es un software desarrollado por Real Games para la virtualización de plantas industriales. Permite crear entornos virtuales que replican procesos industriales reales, lo que facilita la formación, el diseño y la realización de pruebas de sistemas de automatización industrial. Este software se encuentra disponible para su descarga en la web propia del producto (Download Archive - Factory I/O (factoryio.com)) y proporciona un periodo de prueba gratuito durante treinta días.

Una vez instalado Factory IO, al navegar a la sección "Scenes" en el menú izquierdo, se encuentran varias escenas preconstruidas por Factory IO. Sin embargo, también es posible crear una escena desde cero y personalizarla según se requiera.

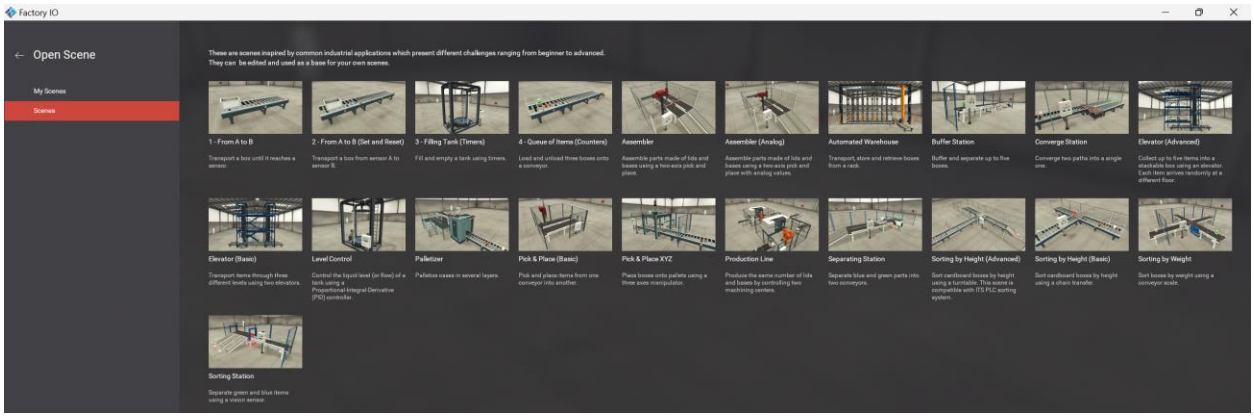


Figura 65. Catálogo de escenas preconstruidas en Factory IO

En este proyecto, se ha empleado la escena "Pick and Place", la cual ofrece un escenario simple pero práctico y aplicable a la industria real. Esta escena proporciona elementos comunes en la industria, como cintas transportadoras, robots de posición, sensores de presencia, paneles de control, entre otros.

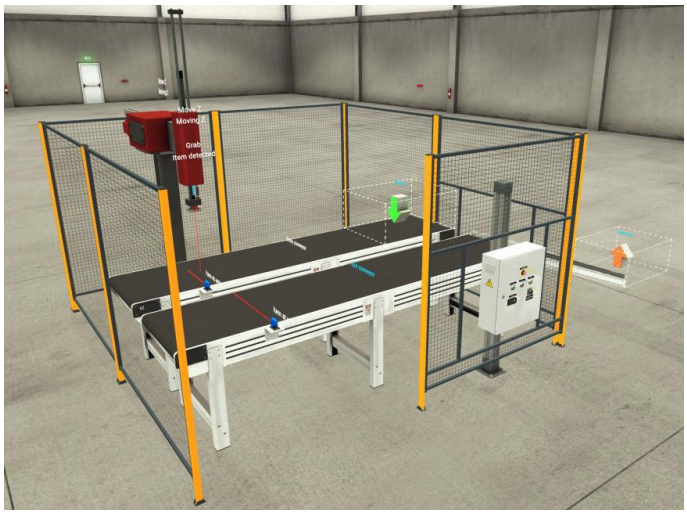


Figura 66. Escena "Pick and Place" Factory IO

Para conectar la escena con el PLC, se accede a la sección "Drivers" (File -> Drivers) para configurar el protocolo de comunicación deseado. En el desplegable de la izquierda se puede seleccionar el protocolo deseado para realizar la conexión con el PLC, en este caso se selecciona “Modbus TCP/IP Client”.

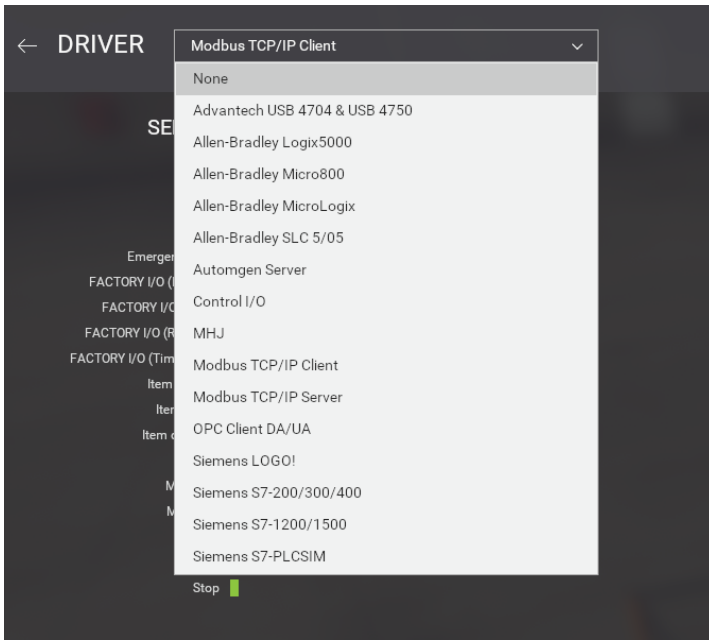


Figura 67. Factory IO - Opciones protocolos de comunicación

A continuación, se describe la configuración necesaria para establecer la conexión con el PLC, se puede consultar la Figura 68 para referencia:

- Se debe hacer clic en "Configuration".
- En el campo "Host", se introduce la dirección del controlador al que se desea conectar. En este caso, la dirección asignada al PLC es "192.245.103.100".
- Se establece el puerto de comunicación. Se utiliza el puerto por defecto en Modbus, que es el puerto "502".
- Para la configuración de las entradas y salidas, se utilizan las bobinas. Por lo tanto, se configura el campo "Read Digital" con el valor "Coils" y el campo "Read Register" con el valor "Holding Registers".
- Por último, se configura el número de entradas y salidas del PLC de acuerdo con lo programado en el programa implementado en el PLC. Como se especifica en el anexo X, las entradas están configuradas desde la marca 0 hasta la 10, y las salidas desde la 11 hasta la 17. Por eso, hay que introducir los valores como se muestra en la siguiente figura.

Luego, se asigna cada sensor y actuador a su entrada y salida respectivas. Para esta asignación, es crucial considerar la configuración establecida en la programación del PLC, garantizando una conexión correcta de los sensores y actuadores. En Factory IO, simplemente se arrastra el sensor a la entrada correspondiente para conectarlo, y se sigue el mismo procedimiento para los actuadores. Una vez completada la conexión de todos los dispositivos de manera adecuada, se hace clic en *"Connect"* para establecer la conexión de la planta con el autómata. En la Figura 69 se muestra la asignación de sensores y actuadores.

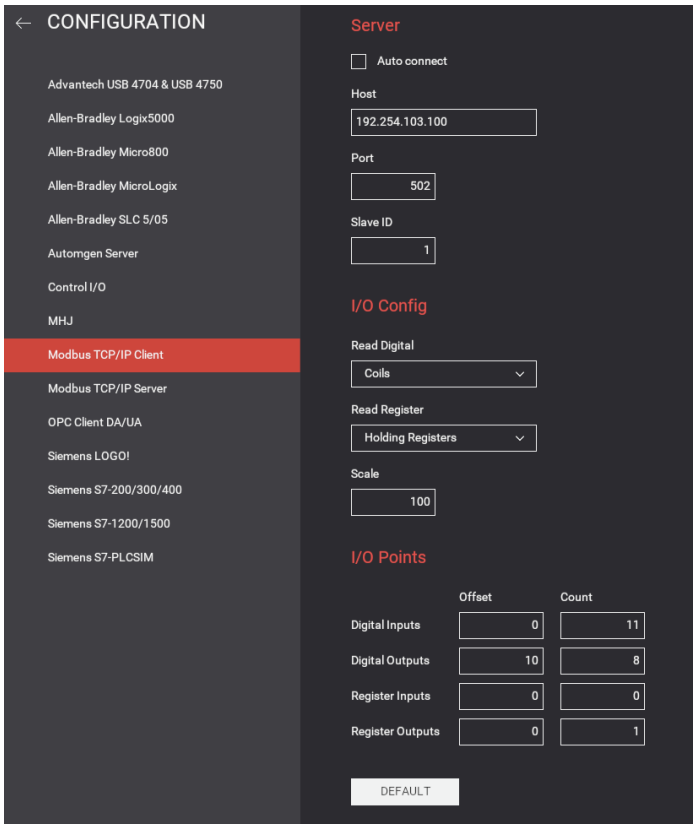


Figura 68. Factory IO. Configuración cliente Modbus

Figura 69. Factory IO. Conexión sensores y actuadores

Para poner en marcha la planta, es imprescindible hacer clic en "Play" para activar el modo de funcionamiento. Es importante tener en cuenta que el PLC también debe estar iniciado para que funcione correctamente. En el panel de control, podemos supervisar y controlar las funciones de arranque, parada y emergencia. Estos botones operarán según la configuración establecida en la lógica del PLC. En este caso, para iniciar el proceso de arranque, es necesario presionar el botón "Start".

Figura 70. Factory IO. Puesta en marcha

Anexo II: Programación y Configuración PLC Schneider M221

EcoStruxure Machine Expert – Basic es un software del fabricante Schneider que permite configurar, programar y poner en marcha algunos dispositivos de este fabricante. Es un software intuitivo y práctico que permite la programación en varios lenguajes como Ladder, ST, LB, FI, etc.

Con esta guía se pretende describir la configuración y programación del PLC Schneider M221 para conectar con la planta virtualizada y llevar a cabo el control de esta.

El proceso de configuración comienza seleccionando el dispositivo adecuado. Para esto, es necesario acceder a los ajustes y configurar el modelo de PLC deseado, tal y como se muestra en la imagen.

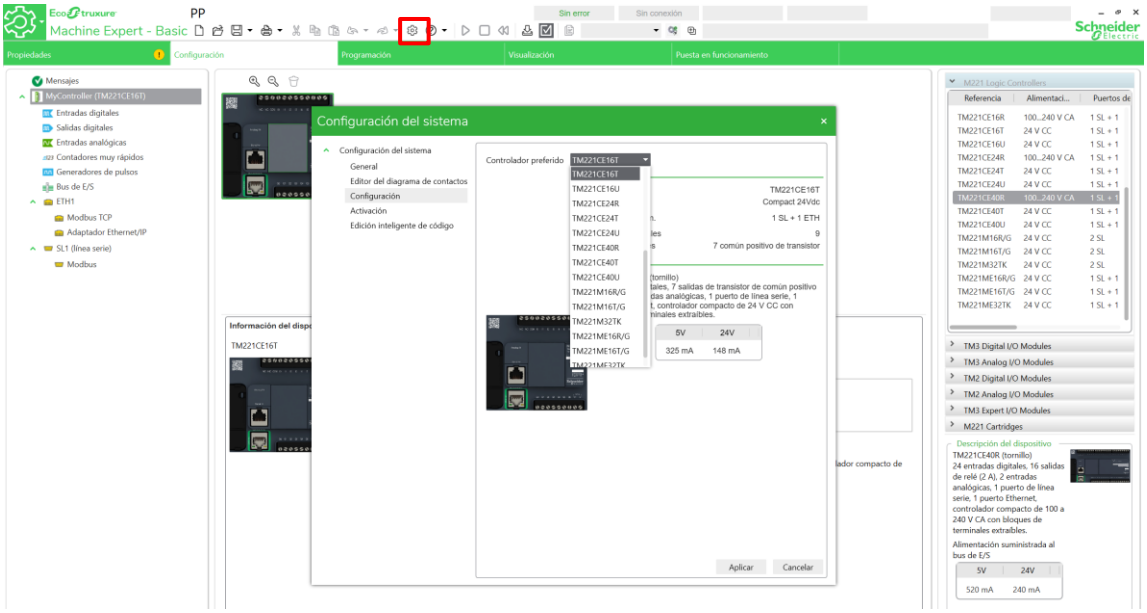


Figura 71. EcoStruxure Machine Expert Basic - Configuración controlador

Después, se asigna una dirección IP estática al PLC. Para ello, se accede a la sección "ETH1" ubicada en el menú izquierdo de la ventana "Configuración". En esta sección, se elige la opción "Dirección IP fija" y se ingresa la dirección IP deseada, en este caso, 192.254.103.100, junto con la máscara de red correspondiente. Además, es importante habilitar todos los parámetros de seguridad para asegurar una conexión exitosa. Para más detalles se puede consultar la Figura 72 como referencia.

Para establecer la comunicación, se conecta el controlador al PC mediante USB y se carga la configuración. Tras completar este paso, la dirección IP estática se asigna al PLC. Posteriormente, se puede desconectar el cable USB y conectar únicamente el controlador a través del puerto Ethernet. Para ello en la ventana “Puesta en funcionamiento” se selecciona la IP correspondiente y se hace click en “Iniciar sesion”, en este momento sera posible cargar la programación desde el PC al controlador e inciarlo.

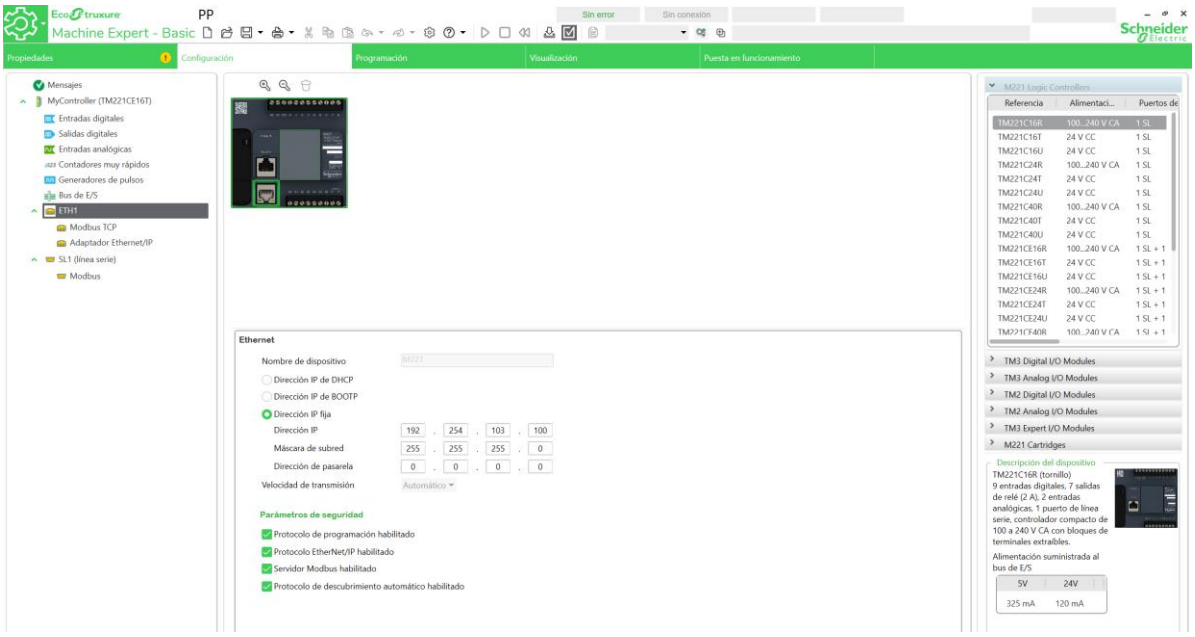


Figura 72. EcoStruxure Machine Expert Basic - Configuración IP PLC

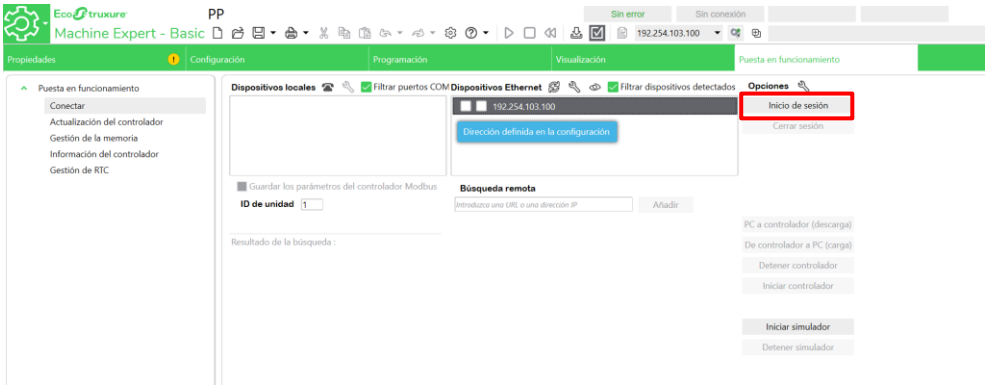


Figura 73. EcoStruxure Machine Expert Basic - Puesta en funcionamiento controlador

Este software también ofrece un entorno de programación en varios lenguajes. En este caso se ha decidido utilizar el lenguaje Ladder, por su frecuente uso en sistemas automatizados. Para ello en la ventana "Programacion" se han creado dos tareas complementarias "RUN MÁQUINA" y "SECUENCIA", como se muestra en la siguiente figura.

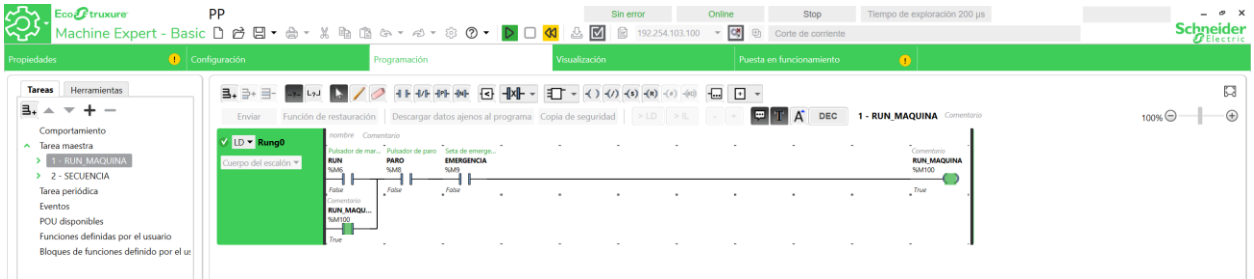


Figura 74. EcoStruxure Machine Expert Basic - Programación controlador

La tarea "RUN MÁQUINA" supervisa el panel de control de la fábrica, iniciando el funcionamiento si se presiona el botón "Run" y deteniéndolo ante un "Stop" o una situación de "Emergencia". Activar esta tarea

implica el inicio de la tarea "SECUENCIA", que ejecutará la lógica del programa. El archivo del proyecto completo se encuentra disponible en el repositorio de Github del proyecto, en la carpeta Schneider Project.

Anexo III: Configuración Kali Linux

Kali Linux[19] es una distribución de Linux especializada en seguridad informática y pruebas de penetración. Está diseñada para proporcionar una plataforma robusta y versátil para investigadores de seguridad, profesionales de la ciberseguridad y entusiastas de la informática. Incluye una amplia gama de herramientas de hacking ético, forense digital y análisis de vulnerabilidades, lo que la convierte en una opción popular para realizar pruebas de seguridad en redes, sistemas y aplicaciones.

En este escenario se ha descargado una imagen de este sistema operativo para poder desplegar una virtualización del sistema en el mismo PC donde se aloja el software de la fábrica configurada. El distribuidor Kali Linux proporciona varias opciones de software gratuito para desplegar en maquina virtuales con softwares de virtualización, como VMWare o Virtualbox. En el siguiente enlace se ha descargado el software correspondiente para VMWare: Get Kali | Kali Linux

En este caso, debido a la familiaridad y las funcionalidades específicas que ofrece, se ha seleccionado VMWare Workstation 17 Pro[20] para llevar a cabo la virtualización. Este software, líder en virtualización, permite crear y administrar máquinas virtuales en entornos de escritorio. Ofrece características avanzadas como la compatibilidad con sistemas operativos múltiples y la ejecución de múltiples máquinas virtuales simultáneamente.

Para abrir la máquina virtual se hace click en "Open a Virtual Machine" y en el explorador de archivo se selecciona el archivo descargado anteriormente. Este archivo se ha subido en el repositorio correspondiente de este proyecto, permitiendo abrir la máquina atacante con las configuraciones aplicadas a lo largo del proyecto y contiene los ficheros creados para las pruebas realizadas. En la siguiente imagen se puede ver el estado de la aplicación tras abrir la máquina virtual y se muestran las características configuradas para esta máquina como la memoria RAM asignada o el tipo de conexión a red.

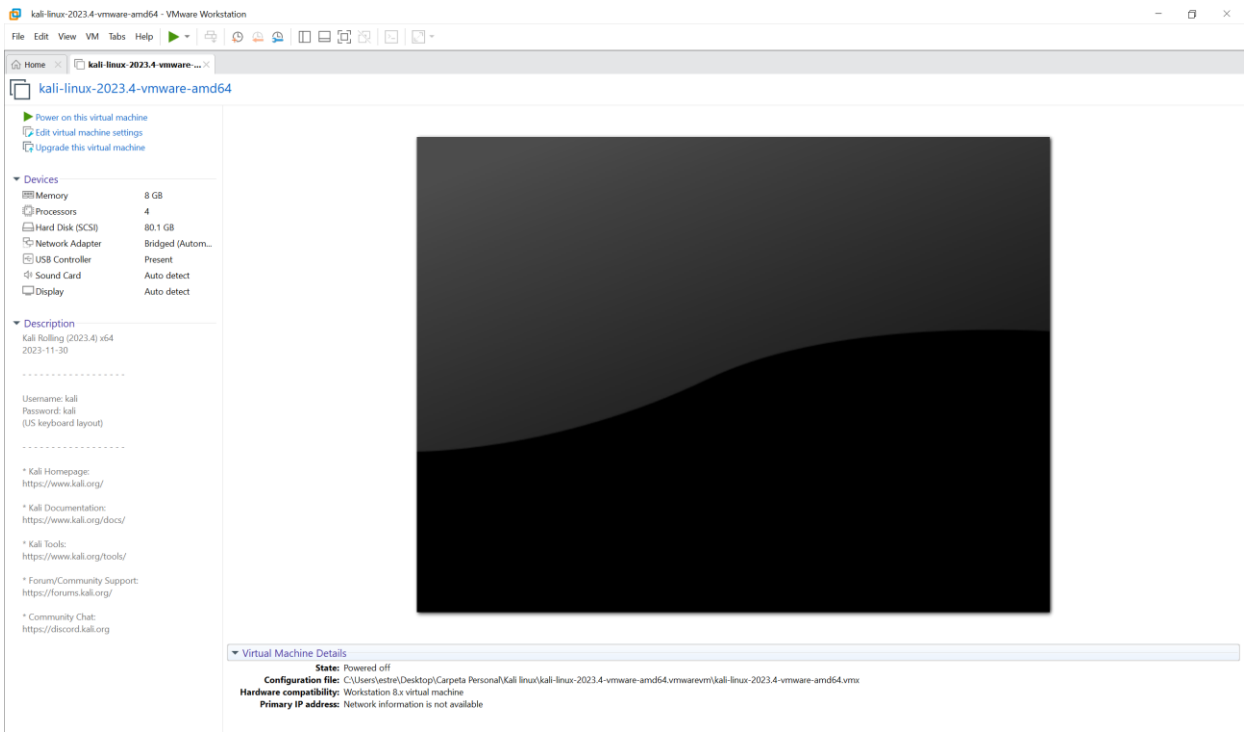


Figura 75. VMWare Workstation 17 PRO. Máquina Kali Linux

[19] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution
[20] VMware Desktop Hypervisors for Windows, Linux, and Mac

Para conectar esta máquina a la red de control en la que se encuentra la fábrica y el PLC es importante configurar correctamente las interfaces de red de la máquina. Para ello, se ha configurado del adaptador en modo *"bridge"* lo que permite conectar la máquina virtual con el host como si estuviera conectado físicamente, por tanto, permite la conexión con otros dispositivos conectados físicamente a la misma red en el host.

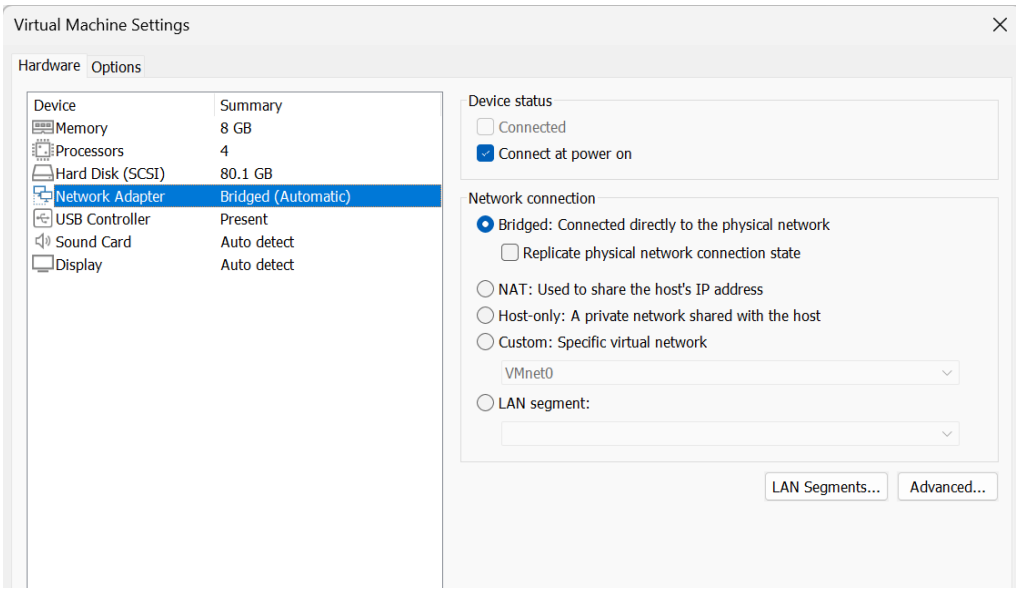


Figura 76. VMWare Workstation 17 PRO - Configuración de red máquina Kali Linux

Luego, es necesario configurar los ajustes de red para que la conexión bridge se realice con el adaptador de red al que se ha conectado el PLC, ya que un PC puede tener varios adaptadores de red. Para ello, el primer paso consiste en consultar los adaptadores de red para consultar la red del controlador, esto se realiza ejecutando en la consola del host el comando *"ipconfig"*. El siguiente paso, ajustar la configuración para conectar con el adaptador determinado. Para esto se navega en VMWare a *"Virtual Network Editor"* y se selecciona el adaptar al que queremos conectar en modo *"bridge"* como se muestra en la siguiente figura.

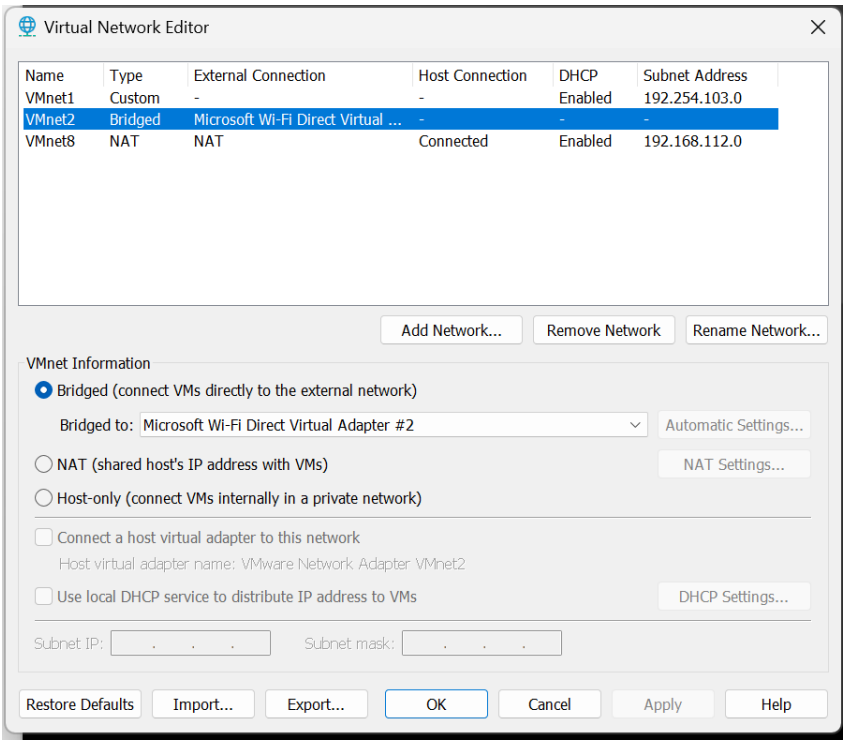


Figura 77. VMWware Workstation 17 PRO - Configuración adaptadores de red

Finalmente, se pulsa en "Power on this virtual machine" para lanzar el sistema Kali Linux y se introducen las

credenciales de usuario.

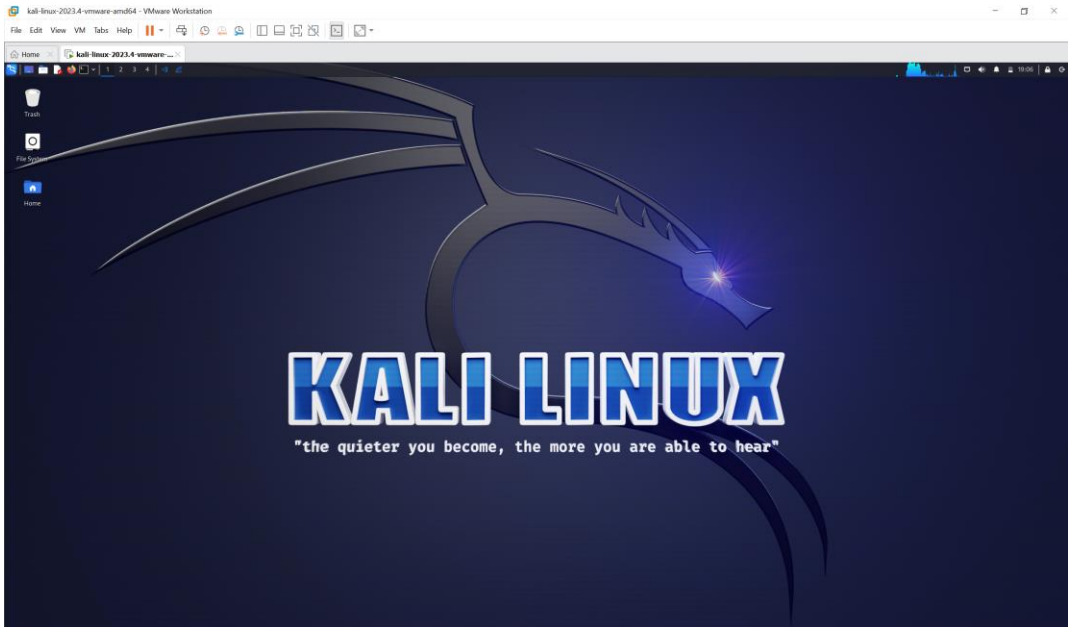


Figura 78. Kali Linux. Interfaz Sistema Operativo

Como se ha introducido, este sistema tiene preinstaladas las herramientas más conocidas para pruebas de penetración y auditorias de seguridad por lo que los softwares utilizados en este proyecto (Metasploit, Wireshark, Nmap, etc.) están disponibles en el sistema.

Todos los scripts elaborados durante el proyecto se han creado en el entorno de desarrollo integrado (IDE) Visual Studio Code. Esta herramienta posibilita la escritura, ejecución y depuración del código, ofreciendo una interfaz sencilla y personalizable que facilita la conexión directa con repositorios y la realización de operaciones de sincronización de manera simple.