



Autor: Estrella Hernández Candelario

Tutor: Juan Manuel Escaño González

Ciberseguridad en Sistemas de Control Industrial

Trabajo Fin de Grado

Ingeniería de Telecomunicación

Dpto. Ingeniería de Sistemas y Automática

Escuela Técnica Superior de Ingeniería

Universidad de Sevilla

Sevilla, 2023

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*

*A mis maestros*

Agradecimientos

Los estilos adoptados por nuestra Escuela y utilizada en este texto es una versión y adaptación a Word® del la versión LATEX que el Prof. Payán realizó para un libro que desde hace tiempo viene escribiendo para su asignatura. Por ello, la Escuela le está agradecida. Por otro lado, la adaptación se hizo sobre un formato que el Prof. Aguilera arregló, basándose en su tesis doctoral. Su aportación ha sido muy relevante para que este formato vea la luz. Esta adaptación la llevamos a cabo el alumno Silvio Fernández, becario del Centro de Cálculo, y yo mismo, sobre un trabajo preliminar del alumno Julián José Pérez Arias.

A esta hoja de estilos se le incluyó unos nuevos diseños de portada. El diseño gráfico de las portadas para proyectos fin de grado, carrera y máster, está basado en el que el Prof. Fernando García García, de la Facultad de Bellas Artes de nuestra Universidad, hiciera para los libros, o tesis, de la sección de publicación de nuestra Escuela. Nuestra Escuela le agradece que pusiera su arte y su trabajo a nuestra disposición.

*Estrella Hernández Candelario*

*Sevilla, 2023*

Resumen

En nuestra Escuela se producen un número considerable de documentos, tantos docentes como investigadores. Nuestros alumnos también contribuyen a esta producción a través de sus trabajos de fin de grado, máster y tesis. El objetivo de este material es facilitar la edición de todos estos documentos y a la vez fomentar nuestra imagen corporativa, facilitando la visibilidad y el reconocimiento de nuestro Centro.

Por otro lado, los alumnos muestras casi siempre un desconocimiento absoluto de los programas informáticos de edición de texto. Esto es, de los elementos de un texto y de las herramientas para editarlos.

El objetivo de este documento es doble. Por un lado, establecer un formato uniforme, mediante la adaptación de este fichero en formato electrónico, y por otro iniciar al usuario en las herramientas de edición de Microsoft Word.

Abstract

In our school there are a considerable number of documents, many teachers and researchers. Our students also contribute to this production through its degree-master's theses. This material's aim is easier to edit these documents while promoting our corporate image, providing visibility and recognition of our Center.

... -translation by google-

Índice

Agradecimientos 8

Resumen 9

Abstract 10

Índice 11

Índice de Tablas 12

Índice de Figuras 13

Introducción 11

1 Línea Temporal de Ciberataques Industriales 13

2 Retos y Factores Críticos de la Ciberseguridad Industrial 15

3 Tecnologías de la Operación 16

3.1 Sistema de Control Industrial 16

3.2 Protocolos de comunicación industriales 18

3.2.1 Modicon Communication Bus 18

3.2.2 Distributed Network Protocol 23

3.2.3 OLE for Process Control (OPC) 26

4 Estudio de Ciberataques y Amenazas 26

4.1 Ciclo de vida de un ciberataque 26

4.2 Vectores de ataques y Vulnerabilidades 28

5 Medidas de Seguridad 29

5.1 Standards y Buenas Prácticas 29

5.1.1 ISO/IEC 27000 30

5.1.2 NIST SP 800-82 31

5.1.3 NERC CIP 31

5.1.4 IEC-62443 32

5.2 Securización de zonas 33

5.3 Auditorias y Pentesting 35

5.4 Sistemas de detección y prevención: IDS, IPS y SIEM 36

6 Pentesting en Sistemas de Control Industrial 38

6.1 Configuración del entorno de pruebas 38

6.2 Implementación del ataque 39

6.2.1 Fase 1. Reconocimiento 39

6.2.2 Fase 2. Escaneo 42

6.2.3 Fase 3. Análisis y Sniffing del Tráfico de Red 44

6.2.4 Fase 4. Man In the Middle 46

6.2.5 Fase 5. Inyección de Datos Falsos 49

6.2.6 Análisis y Validación de Resultados 49

7 Conclusiones y líneas futuras 50

Referencias 50

Anexo I: Configuración Cliente y Servidor Modbus 53

Anexo II: Despliegue contenedor Docker 54

Anexo III: Sniffer con Scapy 56

# **Índice de Tablas**

Tabla 2–1. Tipos de transmisión y frecuencia central 8

Tabla 3–1 Tipos de transmisión y frecuencia central 15

# **Índice de Figuras**

**No se encuentran elementos de tabla de ilustraciones.**

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].

Diagrama

Descripción generada automáticamente

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 da una descripción de la estructura de un sistema 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**: con esta práctica se pretende simular un ataque de inyección de datos falsos sobre una configuración cliente-servidor Modbus. La realización de ataques controlados y en simulación permite la detección de vulnerabilidades en el sistema sin necesidad de alterar la producción, aspecto crucial para los sistemas de control industrial e infraestructuras críticas.

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>

# 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]](#footnote-2)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]](#footnote-3) 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]](#footnote-4) 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 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]](#footnote-5)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) o *Incontroller* (Mandiant). 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 [11].

Escala de tiempo

Descripción generada automáticamente

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

# 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 productivos 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 a las 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 riesgos de 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 [12].

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 [13].[13]

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.

# 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.

## 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]](#footnote-6). Para realizar la conexión de sensores y actuadores con el PLC normalmente se utilizan buses de campo como Modbus, Profibus, EtherNet/IP, Interbus, etc. [14]

Diagrama

Descripción generada automáticamente

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]](#footnote-7), radio, vía MQTT[[7]](#footnote-8) o OPC UA [[8]](#footnote-9)[15].
* **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 [16]. 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.

Diagrama

Descripción generada automáticamente

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 [16].

* **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.

## 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. Esta comunicación fluida y el intercambio de datos son cruciales para la supervisión y regulación precisa y eficiente de los procesos de producción. Es esencial que las señales fluyan sin obstáculos de un dispositivo a otro a través de estas redes para garantizar el funcionamiento óptimo del sistema. 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.

### 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.

Logotipo

Descripción generada automáticamente con confianza baja

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 [17].

* 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: [18]

* 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.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figura 6. Modelo cliente servidor Modbus [17]

El protocolo Modbus TCP se define como un sistema de mensajería de aplicación situado en el séptimo nivel del modelo OSI[[9]](#footnote-10). 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 recibidos correctamente y en el orden correcto.

Interfaz de usuario gráfica

Descripción generada automáticamente

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.

Diagrama

Descripción generada automáticamente

Figura 7. Handshake Modbus TCP [19]

* **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 [18] 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.

Diagrama

Descripción generada automáticamente

Figura 8. Cierre conexión Modbus TCP [20]

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) [18].

Imagen que contiene Diagrama

Descripción generada automáticamente

Figura 9. Trama Modbus TCP [17]

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.

Imagen que contiene Aplicación

Descripción generada automáticamente

Figura 10. Rango de códigos de función Modbus [17]

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

Tabla

Descripción generada automáticamente

Figura 11. Códigos de función Modbus más utilizados [17]

* 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 7 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.

#### Vulnerabilidades del protocolo Modbus

Este protocolo carece de importantes características de seguridad lo que lo hace vulnerable ante ataques cibernéticos. Las implementaciones serie de Modbus hacen uso de RS232 o RS485, ambos protocolos de pertenecientes a la capa física. No corresponde a esta capa la implantación de medidas de seguridad puesto que son funcionalidades que se desarrollan en las capas superiores. Estas capas superiores son, según la implementación utilizada, el nivel de enlace, HDLC y Ethernet. A continuación, se muestran algunas de las vulnerabilidades más reportadas de este protocolo a nivel de capa de aplicación: [21]

* El protocolo Modbus carece de autenticación. Para iniciar una sesión Modbus basta con una dirección, un código de función y datos asociados válidos. Para proporcionar un mensaje válido basta con realizar un análisis del tráfico de red o de la configuración del dispositivo.
* El protocolo carece de un sistema de verificación de la integridad de una trama para dispositivos pares. Esto facilita a los hackers la alteración de las tramas.
* No se utilizan técnicas de encriptación para mantener la confidencialidad de las tramas, las tramas Modbus se transfieren en texto plano. Realizando un ataque *Man In The Middle* es posible capturar los paquetes y acceder a la información de la trama, además de obtener información relevante sobre la configuración y el uso del dispositivo.
* La trama no contiene una marca de tiempo, por lo que los dispositivos pares no tienen información sobre si la respuesta es reciente o antigua. Mediante la manipulación de las tramas se puede alterar el funcionamiento por la falta de coincidencia de los valores de campo en tiempo real.

Estas vulnerabilidades convierten a Modbus un blanco para atacar los sistemas de control industrial. Los ataques más reportados son *Man In The Middle (MITM)* en forma de *False Command Injection (FCI)*, *False Access Injection (FAI)*, *False Response Injection* (FRI) y ataques *Deny of Service (DoS).*

### 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.

Un dibujo de un perro

Descripción generada automáticamente con confianza media

Figura 12. 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 [22].

Diagrama

Descripción generada automáticamente

Figura 13. Pila protocolos DNP3 [22]

**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.

Tabla

Descripción generada automáticamente

Figura 14. 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 [23]. 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.

### OLE for Process Control (OPC)

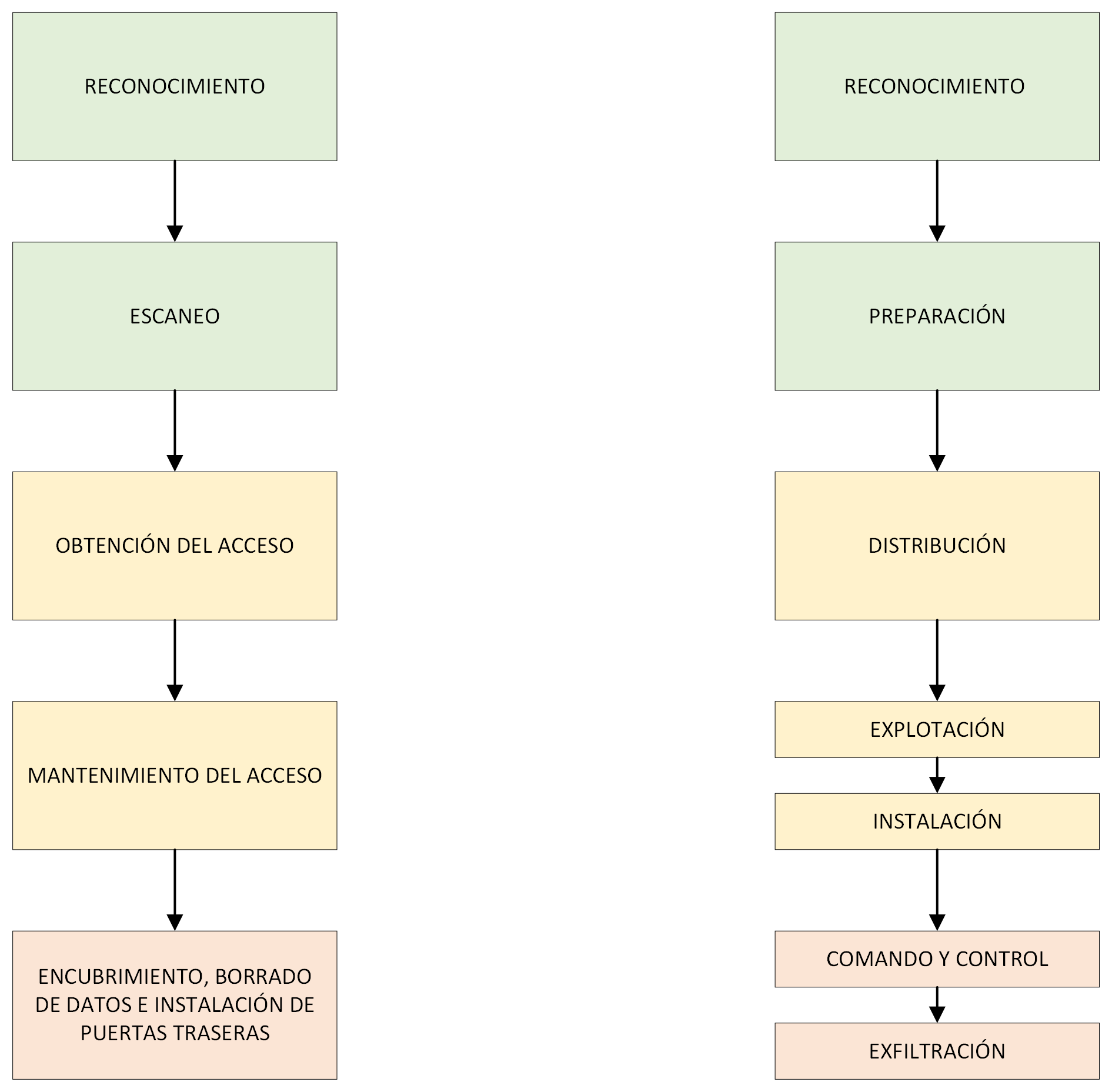
# Estudio de Ciberataques y Amenazas

En este capítulo, se explora la ciberseguridad desde la perspectiva del atacante, desentrañando las fases que atraviesa para realizar con 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.

## 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, y la “Cyber Kill Chain”, desarrollada por Lockheed Martin, una empresa de seguridad y defensa.

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.



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 ICS y el análisis de la susceptibilidad a ataques del proceso y el modelo operativo. [24]

1. 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.

1. 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.

1. 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]](#footnote-11) 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.

1. 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 informáticos. Para lograrlo, pueden utilizar rootkits [[11]](#footnote-12)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.

## Vectores de ataques y Vulnerabilidades

A continuación, se detallan algunos de los puntos críticos y vulnerabilidades identificados en sistemas de control industrial, destacando los vectores de ataques más comunes. Un vector de ataque se define como una vía o método específico que los atacantes emplean para comprometer un sistema o proceso [25]. En este contexto, es común hacer referencia a los sistemas, dispositivos o activos críticos susceptibles de ser atacados como “target” u “objetivo” [26]

* **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 el objetivo de hacerlo inaccesible para 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 [27]. 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.

Gráfico, Gráfico circular

Descripción generada automáticamente

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 un ataque potencial. 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.

# Medidas de Seguridad

## Standards 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. 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 [28].

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 actualmente está siendo revisada y reestructurada para su potencial aceptación por parte de 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.

### 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 [29].

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 la gestión de la seguridad de la información que es aplicable a cualquier tipo de organización, incluidas las organizaciones industriales.
* ISO/IEC 27002: proporciona una colección de controles y buenas prácticas que pueden ser implementadas por 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.

Texto, Carta

Descripción generada automáticamente

### 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 sistemas de control distribuidos, ambos ampliamente utilizados 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 [30].
* 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 [30].

Diagrama, Escala de tiempo

Descripción generada automáticamente

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 [30].

### 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 específicamente para los sistemas de transmisión de energía de las empresas de servicios públicos [31]. 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 [32]. A continuación, se ofrece una breve descripción de cada estándar en la tabla adjunta, mientras que la lista completa se puede consultar en el siguiente enlace de referencia [33].

|  |  |
| --- | --- |
| 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 |

### 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 [34]. 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 [35].

Diagrama

Descripción generada automáticamente

#### 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 [28].

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, el cual establece métricas de conformidad que son sumamente útiles para evaluar el cumplimiento de prácticas de seguridad en estos sistemas.

#### 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 [28].

#### 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.

#### 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 [28].

En conclusión, 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.

## 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 [36].

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 dividir la red en segmentos más pequeños y aislados entre sí, con el fin de mejorar el flujo de tráfico y evitar que una vulnerabilidad se propague a toda la red.

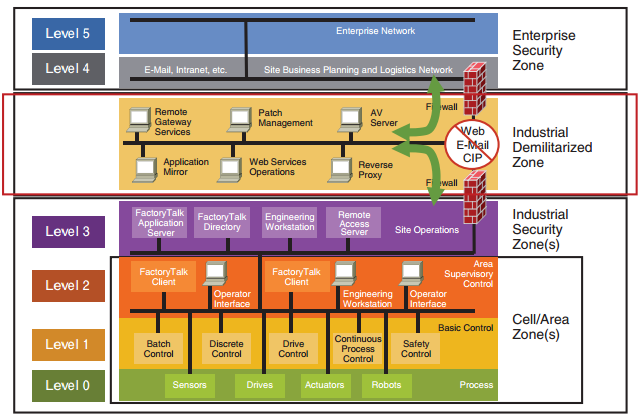
La segmentación de redes ofrece ventajas en seguridad y cumple con los requisitos del estándar ISA/IEC 62443. Una de estas ventajas es un mayor control sobre el acceso a los recursos. Al limitar el acceso solo a los usuarios o dispositivos que realmente necesitan interactuar con una determinada parte 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 3.5.1 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 [37]

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 [38]:



* **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).

En resumen, 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.

## Auditorias 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 [39].

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 [40].

Estas prácticas son complementarias y su aplicación conjunta proporciona una defensa robusta ante las amenazas e incidentes de seguridad.

## 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 [21].

En la siguiente figura 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 [41].

Diagrama

Descripción generada automáticamente

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 [21].

Diagrama

Descripción generada automáticamente

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 [40].

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 [42].

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

En resumen, 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.

# 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.

## Configuración del entorno de pruebas

Para llevar a cabo el proceso mencionado, se desarrolló una configuración de red industrial elemental que emplea el protocolo de comunicación Modbus, detallado en el capítulo 3.2.1. Este protocolo se usa mucho en el sector, por lo que las vulnerabilidades identificadas podrían afectar a la mayoría de los sistemas de control industrial. Por consiguiente, este estudio resulta útil para detectar dichas vulnerabilidades y diseñar las medidas de protección necesarias para resguardar los activos.

Para crear el entorno de pruebas, se simula un servidor Modbus responsable de administrar los datos y responder a las solicitudes de los clientes Modbus, así como un cliente encargado de iniciar las solicitudes al servidor Modbus para leer o escribir datos.

A causa de las limitaciones en las prestaciones de memoria RAM del equipo utilizado para llevar a cabo las prácticas de pentesting, se ha optado por una configuración basada en contenedores Docker.

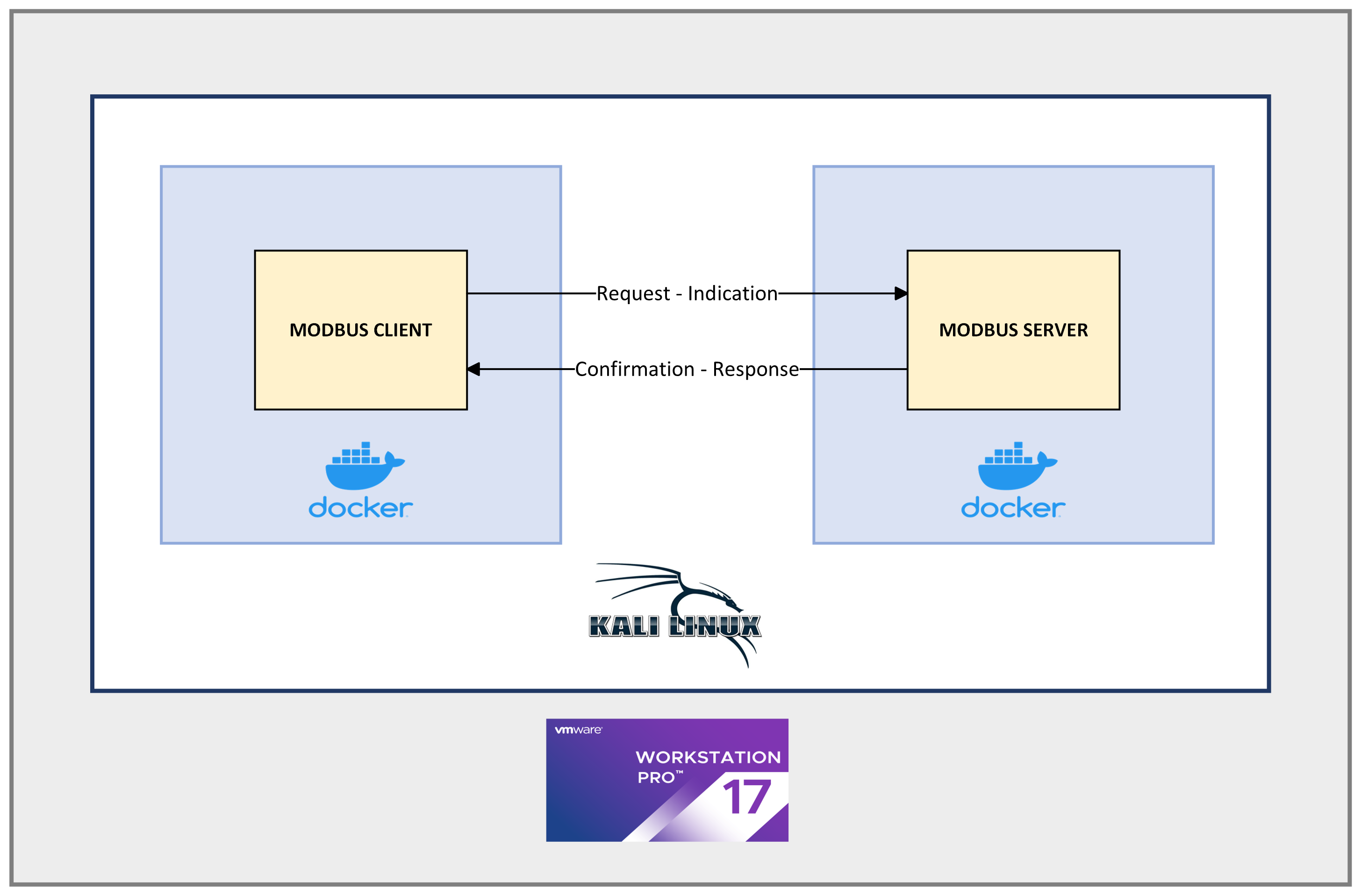
Los contenedores representan una forma versátil de virtualización del sistema operativo. Un solo contenedor puede ejecutar desde microservicios hasta aplicaciones completas, albergando todos los elementos necesarios como ejecutables, código binario y archivos de configuración. A diferencia de la virtualización tradicional, los contenedores son más ligeros y portátiles al no contener imágenes completas del sistema operativo [43].

A continuación, se muestra la arquitectura implementada:

* En primer lugar, se ha instalado Kali Linux[[12]](#footnote-13), una distribución de Linux especializada en *pentesting,* auditorías de seguridad y análisis forense digital. Está basada en Debian y proporciona una amplia gama de herramientas de seguridad, análisis de redes y datos.

Este software se ha aloja en la aplicación de virtualización VM Workstation 17 PRO, que permite la instalación y ejecución de varios sistemas operativos simultáneamente en un único dispositivo físico.

* Dentro de la máquina virtual Kali Linux, se ha desplegado un contenedor Docker[[13]](#footnote-14) que aloja el software necesario para simular un servidor Modbus y replicar una red haciendo uso de este protocolo. Para más información sobre Docker y el despliegue del servidor, consultar el siguiente anexo:
* De esta misma forma, se ha desplegado un cliente Modbus en otro servidor Docker conectado a la misma red del servidor Modbus.
* Para emular la interacción cliente-servidor en una red Modbus, se han desarrollado dos scripts usando el lenguaje de programación Python. Estos scripts hacen uso de la biblioteca *pymodbus* y se basan en los ejemplos proporcionados en la documentación de dicha librería [44]. *pymodbus* es una herramienta en Python diseñada para simplificar la implementación y la interoperabilidad de dispositivos que utilizan el protocolo Modbus en entornos de automatización industrial y sistemas de control. Esta biblioteca permite crear tanto clientes como servidores Modbus, facilitando así la comunicación eficaz y fiable entre dispositivos dentro de una red Modbus. Los pasos seguidos para el diseño de cliente y servidor, junto con los scripts utilizados se encuentran en el siguiente anexo:



## Implementación del ataque

Este estudio de pentesting se ha enfocado en la fase posterior a la explotación, donde se simula un escenario donde el atacante ya ha conseguido acceso al objetivo. Este enfoque permite identificar y mitigar las vulnerabilidades que podrían permitir al atacante mantener el acceso no autorizado y realizar acciones maliciosas dentro del sistema comprometido.

A pesar de partir del acceso a la red por parte del atacante, se describen algunas técnicas y herramientas utilizadas por los atacantes en las fases previas a la explotación.

### Fase 1. 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.

Esta fase consiste en explorar diversas fuentes, desde sitios web públicos relacionados con el objetivo hasta perfiles de redes sociales de la empresa, así como documentación técnica proveniente de fabricantes de los dispositivos utilizados en el sector.

En la industria, la falta de concienciación en ciberseguridad lleva a muchas veces a mantener las contraseñas por defecto de los dispositivos de campo, lo que supone dejarlo expuesto a ataques de diccionario, utilizando listas como las siguientes. En GitHub, se pueden encontrar varios repositorios que contienen registros de contraseñas por defecto organizadas por fabricante y producto.

* + - [ICS Master](https://github.com/w3h/icsmaster/)
    - [SCADAPASS](https://github.com/scadastrangelove/SCADAPASS)

A continuación, se detallan algunas de las herramientas más reconocidas y empleadas en esta fase para recopilar información de la red de manera pasiva.

* **Google Dorks:** es una técnica de búsqueda avanzada que utiliza consultas específicas en el motor de búsqueda de Google que permite encontrar información sensible y vulnerabilidades en sitios web. Algunos ejemplos de 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.

En este ejemplo 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.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

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.

Interfaz de usuario gráfica

Descripción generada automáticamente

Si se logra obtener acceso a uno de estos sistemas mediante credenciales predeterminadas, como las proporcionadas anteriormente, 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.

* **Shodan:** es un motor de búsqueda especializado que explora y recopila información sobre dispositivos conectados a Internet [45].

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.

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

Interfaz de usuario gráfica

Descripción generada automáticamente

La cantidad de dispositivos indexados al buscar en el puerto 502, asignado al protocolo Modbus, es extensa.

Imagen que contiene Gráfico

Descripción generada automáticamente

En el siguiente repositorio podemos encontrar listas con directivas útiles para obtener información valiosa sobre los dispositivos de campo:

* + - [ICS IoT Shodan Dorks](https://github.com/AustrianEnergyCERT/ICS_IoT_Shodan_Dorks)

En resumen, estas técnicas y herramientas en la fase de reconocimiento proporcionan una base sólida para comprender la infraestructura y encontrar posibles vectores de ataque en el entorno de sistemas de control industrial, abriendo la puerta al conocimiento de los sistemas necesario para las siguientes fases del proceso.

### Fase 2. Escaneo

Introducción

#### 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 [45].

En la documentación oficial de Nmap 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): listado de sistemas sin enviar paquetes. Nmap realiza una resolución inversa DNS mediante la cual obtiene los nombres de los equipos. Esta opción es una forma de obtener información valiosa sin “hacer ruido” al no enviar ningún paquete al objetivo.
* *-PU* [lista de puertos] (Ping UDP): esta opción 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. Estos son algunos scripts útiles para escaneos en sistemas industriales:

**modbus-discover.nse**:

Escanea dispositivos Modbus y direcciones IP y puertos utilizados

<https://github.com/nmap/nmap/blob/master/scripts/modbus-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 valiosa 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 proporciona un ataque más agresivo.

Texto

Descripción generada automáticamente

El análisis de la red revela una serie de hallazgos significativos sobre el host 172.17.0.2, correspondiente al servidor Modbus. En primer lugar, se confirma que el host está activo y responde a las solicitudes de ping, lo que indica su disponibilidad y conectividad en la red. Sin embargo, al escanear los 1000 puertos TCP en el host, se observa que todos están en un estado "ignorado". Esta situación sugiere posibles configuraciones de firewall o la falta de respuesta de los servicios en el host, lo que podría dificultar el acceso a ciertos servicios o funcionalidades.

Además, se identifica la dirección MAC del host, lo que resulta útil para identificar el fabricante del dispositivo. Herramientas como “Mac Lookup” permiten obtener información detallada sobre el fabricante a partir de la dirección MAC extraída. En este caso, se observa que la dirección MAC pertenece a un contenedor Docker, lo que proporciona información valiosa para un posible atacante. 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.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

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. Este dato es importante para comprender la topología de la red y la proximidad física entre los dispositivos

Ejecutando este script para las direcciones IP de los dos equipos objetivo de estudio se ha recopilado la siguiente información, potencialmente útil para fases posteriores del análisis de penetración:

|  |  |  |
| --- | --- | --- |
| Equipo | IP | MAC |
| Cliente | 172.17.0.3 | 02:42:AC:11:00:03 |
| Servidor | 172.17.0.2 | 02:42:AC:11:00:02 |

#### Wireshark

Wireshark es el analizador de protocolos más popular del mercado, permite capturar y visualizar el tráfico de una red en tiempo real e inspeccionar paquetes y detalles de la conexión. Esto la convierte en una herramienta fundamental para el análisis de comunicaciones industriales, identificación de vulnerabilidades y pruebas de penetración.

### Fase 3. Análisis y Sniffing del Tráfico de Red

Desde este apartado, el análisis se centra en el escenario diseñado para llevar a cabo un ataque simulado de inyección de datos falsos en la comunicación entre el cliente y el servidor Modbus. Este proceso sigue una serie de etapas planificadas. Primero, en este capítulo, el atacante hará un exhaustivo análisis del tráfico de red entre cliente y servidor. Este análisis pretende recopilar la mayor cantidad posible de información sobre el comportamiento de la comunicación, que luego se utilizará en fases posteriores del ataque.

En la segunda fase, el atacante se situará en medio de la comunicación cliente-servidor, e interceptará todos los paquetes enviados entre ambos extremos. Este tipo de ataque, conocido como ataque Man In The Middle (MITM), le permitirá al atacante monitorear y manipular el flujo de información entre los dispositivos, estableciendo así el control en la comunicación.

Por último, el atacante empleará la información recopilada previamente y su conocimiento sobre el protocolo Modbus para introducir datos ilegítimos en una de las tramas de comunicación. Estos datos falsos alterarán la integridad de la comunicación entre los dispositivos objetivo, generando potenciales repercusiones en la integridad y seguridad del sistema.

Durante esta primera fase, el atacante busca interceptar el tráfico intercambiado por los objetivos del ataque, cliente y servidor Modbus. Su objetivo primordial es obtener una visión detallada de cómo se comunican estas entidades y analizar el intercambio de tramas. Una vez que el atacante ha logrado infiltrarse en el entorno operativo (recordemos que asumimos esta premisa en el contexto de nuestro estudio), comienza a utilizar herramientas de análisis de tráfico como Wireshark o Scapy. Estas herramientas le permiten examinar minuciosamente las tramas que se intercambian entre el cliente y el servidor, proporcionándole una comprensión profunda de la dinámica de la comunicación y revelando posibles puntos vulnerables que podrían ser explotados.

Scapy es una poderosa biblioteca interactiva de manipulación de paquetes escrita en Python. Puede codificar y decodificar paquetes de muchos protocolos, enviarlos por la red, capturarlos y encontrar solicitudes y respuestas [43].[46]

Se ha diseñado un script (*Sniffing.py*) utilizando la herramienta Scapy, para capturar todos los mensajes dirigidos al puerto 502, puerto predeterminado para las comunicaciones Modbus. Cada mensaje capturado se almacena en una base de datos, como se muestra en la siguiente figura. Estos mensajes serán posteriormente analizados y utilizados en las siguientes fases del estudio de penetración.

El script mencionado, junto con una descripción detallada de la metodología utilizada para la captura de tráfico y el diseño de la base de datos utilizada para el almacenamiento de mensajes, está disponible para su consulta en el Anexo X.

Imagen que contiene Diagrama

Descripción generada automáticamente

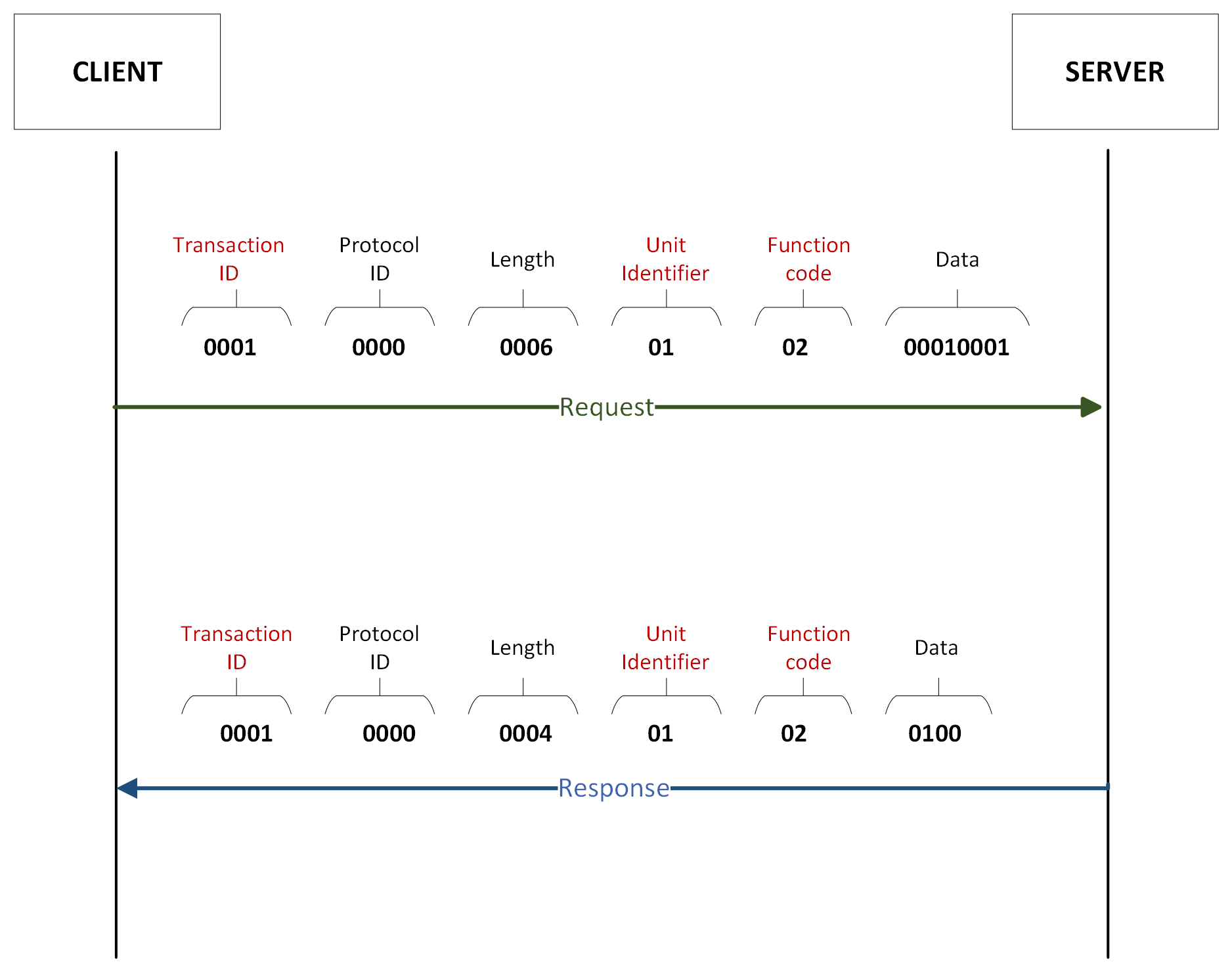
Después de ejecutar el script durante un período de tiempo prolongado que permita capturar exhaustivamente todos los mensajes disponibles en la red, las tramas se registrarán en la base de datos, separando los parámetros de cada una según se muestra en la siguiente figura. Esta figura ilustra las tramas almacenadas durante esta fase al ejecutar el script mencionado anteriormente.

Un conjunto de letras negras en un fondo blanco

Descripción generada automáticamente con confianza media

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 hacerse pasar por los dispositivos en la próxima fase.



En resumen, durante esta fase, el atacante intercepta el tráfico de red para capturar las tramas intercambiadas entre el cliente y el servidor. El objetivo principal es identificar qué respuesta se corresponde con cada petición, lo que permite al atacante suplantar a los dispositivos en pasos posteriores sin perturbar la comunicación normal entre ellos.

### Fase 4. Man In the Middle

Durante este estudio, el atacante tiene como objetivo ejecutar un ataque de "Man in the Middle" (MITM). El proceso general de un ataque Man in the Middle es el siguiente:

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.

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.

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.

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 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 responde con su dirección MAC. Este dispositivo almacena esta información temporalmente en la tabla caché ARP.

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.

Imagen que contiene Aplicación

Descripción generada automáticamente

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, como Linux, Mac OS y Windows [47].

La herramienta Ettercap se 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 *docker0,* ya que en la arquitectura construida el cliente y el servidor se encuentran desplegados en contenedores Docker en la red denominada *docker0.*

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

Captura de pantalla de un celular

Descripción generada automáticamente

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”*.

Captura de pantalla de un celular

Descripción generada automáticamente

Captura de pantalla de un celular

Descripción generada automáticamente

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 sin reenviar las tramas interceptadas al servidor, 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 ha interrumpido, el cliente envía constantemente peticiones para iniciar la comunicación con el dispositivo esclavo, pero no recibe respuesta alguna.

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

Consultas a la base de datos para obtener el mensaje correspondiente a la petición

Diagrama

Descripción generada automáticamente

Consultas a la base de datos para obtener el mensaje correspondiente a la respuesta

Diagrama

Descripción generada automáticamente

### Fase 5. Inyección de Datos Falsos

Introducción

### Análisis y Validación de Resultados

# Conclusiones y líneas futuras

# 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] “Analysis of the Threat to Electric Grid Operations”.

[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] “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

[12] “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

[13] “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

[14] “Practical Industrial Cybersecurity.”

[15] “Qué es una RTU | Becolve digital.” Accessed: Oct. 30, 2023. [Online]. Available: https://becolve.com/blog/que-es-una-rtu/

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

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

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

[19] 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.

[20] “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/

[21] “incibe\_protocolos\_seguridad\_red\_sci”.

[22] 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.

[23] “Overview of DNP3 Security Version 6.”

[24] 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

[25] “¿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

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

[27] “The legacy of ‘insecure by design’ and its implications for certifications and risk management”.

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

[29] “ISO - ISO/IEC 27000 family — Information security management.” Accessed: Mar. 17, 2024. [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family

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

[31] “RELIABILITY | RESILIENCE | SECURITY CIP Definitions Modifications to CIP Standards,” 2016.

[32] “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

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

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

[35] “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/

[36] “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

[37] “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

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

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

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

[41] “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

[42] “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

[43] “¿Qué son los contenedores? - Docker | NetApp.” Accessed: Feb. 17, 2024. [Online]. Available: https://www.netapp.com/es/devops-solutions/what-are-containers/

[44] “Get Docker | Docker Docs.” Accessed: Feb. 17, 2024. [Online]. Available: https://docs.docker.com/get-docker/

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

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

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

[48] “Welcome to PyModbus’s documentation! — PyModbus 3.7.0dev documentation.” Accessed: Mar. 05, 2024. [Online]. Available: https://pymodbus.readthedocs.io/en/latest/

[49] “¿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

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

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

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

Anexo I: Configuración Cliente y Servidor Modbus

En este estudio se ha hecho uso de simulaciones para estudiar las vulnerabilidades y realizar pruebas de penetración sobre el protocolo Modbus. Generalmente, una comunicación Modbus consta de un cliente encargado de realizar peticiones y un servidor que las responde (para más información sobre el protocolo, consultar el capítulo x). Estos dispositivos se han implementado mediante simulación utilizando la librería *Pymodbus*. Esta librería es una implementación completa del protocolo Modbus en Python que ofrece funcionalidades tanto para interactuar con dispositivos reales como para simular su funcionamiento [48].

En este anexo se describe en primer lugar los pasos a seguir para la instalación de la librería. Posteriormente, se describen los scripts utilizados para la implementación de nuestra arquitectura particular.

**Instalación librería *pymodbus***

Para instalar la librería *pymodbus* en Python se puede utilizar “pip”, el sistema de gestión de paquetes estándar de Python, como se indica en la documentación referenciada anteriormente [48]. Para ello, se debe abrir la terminal y ejecutar el siguiente comando:

pip install pymodbus

Una vez ejecutado el comando se descargará e instalará la librería y estaría lista para importarla en los scripts de Python.

**Configuración Cliente/Servidor Modbus**

Los scripts utilizados para la simulación tanto de cliente como servidor se han llevado a cabo adaptando a las necesidades del proyecto los ejemplos proporcionados en la documentación de *pymodbus*. Estos ejemplos se pueden descargar en el siguiente repositorio: [pymodbus/examples at dev · pymodbus-dev/pymodbus (github.com)](https://github.com/pymodbus-dev/pymodbus/tree/dev/examples). A continuación, se detallan los scripts utilizados para la configuración de cada uno y las modificaciones realizadas:

* Cliente:
* Servidor:

Anexo II: Despliegue contenedor Docker

En esta guía se muestran los pasos seguidos para el despliegue del servidor Modbus en un contenedor Docker.

**1. Instalación Docker**

* Actualización de paquetes del sistema

sudo apt update

* Instalar Docker

sudo apt install docker.io

* Inicio del servicio

sudo systemctl start docker

* Habilitar inicio automático de Docker

sudo systemctl enable docker

**2. Crear dockerfile**

Un dockerfile contiene una serie de instrucciones utilizadas por Docker para construir una imagen. Estas imágenes son la base para crear contenedores Docker que contengan todos los archivos y bibliotecas necesarios para ejecutarse. Parra construir el script dockerfile se utilizarán las siguientes instrucciones:

* + FROM: inicio en un dockerfile, se define la imagen base que se utilizará para construir la nueva imagen. En este caso se utiliza la imagen de la versión 3.9 de Python puesto que el código del servidor Modbus está escrito en este lenguaje.
  + WORKDIR: establece el directorio de trabajo en el que se ejecutaran todas las instrucciones.
  + COPY: copian los ficheros especificados del sistema local al contenedor. Es importante añadir un fichero (requirements.txt) que contenga las dependencias de Python necesarias para ejecutar la aplicación dentro del contenedor.
  + RUN: ejecuta comandos en el contenedor cuando se construye la imagen. Se utiliza para instalación de paquetes y configuración del entorno.
  + CMD: comando por defecto que se ejecutará al iniciar el contenedor.

**3. Construcción de la imagen**

* Ejecutar el siguiente comando para que se construya la imagen. Es importante estar situados en el directorio en el que se encuentra el archivo dockerfile.

sudo docker build -t modbus-server .

* Ejecutar el contenedor ejecutándolo en segundo plano (-*d*) y mapeando el puerto 502 del sistema al puerto 502 del contenedor (*-p puerto\_host:puerto-contenedor*).

sudo docker run -d -p 502:502 --name modbus-container modbus-server

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

**4. Comandos útiles para utilizar el contenedor.**

* Verificar contenedores en ejecución. La opción -a permite visualizar todos los contenedores, incluidos aquellos que están detenidos.

sudo docker ps

* Detener contenedor.

sudo docker stop modbus-container

* Eliminar contenedor.

sudo docker rm modbus-container

* Mostrar los registros generados por un contenedor que está en ejecución.

sudo docker logs modbus-container

Anexo III: Sniffer con Scapy

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 [49]. [↑](#footnote-ref-2)
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. [↑](#footnote-ref-3)
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. [↑](#footnote-ref-4)
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 [50]. [↑](#footnote-ref-5)
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) [51] [↑](#footnote-ref-6)
6. GPRS (General Packet Radio Service) es un estándar de comunicación inalámbrica que permite la transmisión eficiente de datos a través de redes móviles. [↑](#footnote-ref-7)
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). [↑](#footnote-ref-8)
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. [↑](#footnote-ref-9)
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 [52]. [↑](#footnote-ref-10)
10. Un troyano, también conocido como caballo de Troya, es un tipo de archivo informático malicioso que simula ser legítimo e inofensivo. [↑](#footnote-ref-11)
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. [↑](#footnote-ref-12)
12. <https://www.kali.org/> [↑](#footnote-ref-13)
13. <https://www.docker.com/> [↑](#footnote-ref-14)