UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN

RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

ARTÍCULOS PROFESIONALES DE ALTO NIVEL

TEMA:

EVALUACIÓN DE LA SEGURIDAD DE LOS SISTEMAS DE COMUNICACIÓN EN LA INDUSTRIA 4.0

AUTOR:

ALEX DARIO AIMACAÑA JAMI

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2025

Autor:

Alex Dario Aimacaña Jami
Ingeniero Electrónico.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
aaimacana@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

DEDICATORIA

Este trabajo lo dedico, primeramente, a Dios, porque su bondad me ha permitido llegar hasta este momento. Su inmenso amor me ha sostenido, brindándome la salud, la fuerza y perseverancia para alcanzar otro logro importante a mi vida.

Además, dedico este trabajo a mis padres quienes me han apoyado en mi educación con valores y principios. El apoyo inquebrantable para mi formación académica, enviándome a instituciones educativas donde la calidad de enseñanza ha sido de gran impacto acompañado de valores y principios cristianos.

También se lo dedico a toda mi familia y a mi hermana Carolina en particular. Que esto sea una inspiración para todos aquellos que sueñan, pues los sueños pueden hacerse realidad si los deseas lo suficiente y nunca te rindes. Espero que mis primos puedan usar este ejemplo para sentirse seguros de que no hay obstáculos insuperables cuando el objetivo está enfocado y el deseo de alcanzarlo es fuerte.

Gracias Dios por darme los mejores padres y por permitir que, a través de su esfuerzo y dedicación, me hayan apoyado en todo. Este logro es por ellos y para ellos, ya que has permitido abrir el camino para cambiar las futuras generaciones de mi familia. Siempre confiando en Ti, porque sé que seguirás abriendo caminos que conllevan grandes cosas, acompañados de bendiciones y crecimiento continuo. Gracias por cumplir los anhelos inimaginables de nuestro corazón y si Tú lo permites seguiremos alcanzando grandes metas, pues todo es posible porque Tú estás con nosotros.

Que así sea en el nombre de Jesús, Amén.

AGRADECIMIENTO

Agradezco primero a Dios por su manera de mostrarme su amor en permitir terminar esta etapa que ha sido un proceso de mucha enseñanza.

En segundo, a mis buenos y amados padres Luis Humberto Aimacaña y Aurora Jami Jami por el apoyo constante, los ánimos brindados asi como los valores impartidos desde mi infancia, en especial el de la perseverancia, hoy sin duda alguna este logro es por ellos y para ellos.

A mi hermana Carito, que también ha sido mi fuente de inspiración. Verte estudiar por las noches, persiguiendo tu segunda cerrera con dedicación y perseverancia, sin duda alguna gracias por enseñarme que, aunque se disponga de un tiempo bastante limitado, se puede alcanzar lo que se propone con mucha disciplina, perseverancia y pasión.

A mis amigos Anthony Sánchez y Ruben Toasa; un agradecimiento especial por brindarme de su apoyo incondicional y su compañía a lo largo de este proyecto. Su respaldo me deja una huella en el corazón especialmente en los momentos algo desafiantes del trabajo que sin duda su motivación ha sido la fortaleza para seguir adelante.

Al Ing. Juan Carlos Domínguez que fue el tutor de este trabajo, por el compromiso, la confianza y la guía necesaria desde los primeros pasos hasta la finalización de este trabajo, y por compartirme el conocimiento que sin duda alguna ha sido fundamental en mi formación profesional.

Gracias a todos por los aportes y las buenas vibras transmitidas a lo largo de toda mi vida.

Tabla de Contenido

Resumen 8
Abstract 9
1. Introducción 10
2. Determinación del Problema 12
2.1. Antecedente 13
2.2. Pregunta de la investigación 14
3. Marco teórico referencial 14
3.1. Protocolos de comunicación utilizados en la industria 4.0 15
3.2. Clasificación de Protocolos de comunicación 15
3.3. Dispositivo 4.0 19
3.4. Raspberry Pi 19
3.5. PLC (Controlador Lógico Programable): 20
3.6. Sensores PIR (Sensores de Infrarrojo Pasivo) 20
3.7. Interruptores de Límite 21
3.8. Sensor Óptico 21
3.9. Sensor Piak 22
3.10. Módulo ESP32 22
3.11. Dispositivos IoT y su Relación con los Protocolos 23
3.12. Desafíos en la Comunicación de la Industria 4.0 24
3.13. Interoperabilidad 24
3.14. Latencia 25
3.15. Escalabilidad 25
3.16. Características de Seguridad de los Protocolos 25
3.17. Amenazas y Vulnerabilidades en la Industria 4.0 28
3.18. Estudios Previos 30
4. Materiales y metodología 32
4.1. Materiales para el entorno de prueba 33
4.2. Preparación de ambiente 33
4.2.1. Instalación de Virtual Box 33
4.2.2. Instalación de Kali 37
4.2.3. Preparación para Instalar Kali Linux en VirtualBox 38
4.2.4. Instalar Kali Linux en VirtualBox 43

4.2.5. Instalación de Raspbian 47
4.3. Simulación del servidor o Rasberry de Prueba 49
4.3.1. Objetivo de la Simulación 49
4.4. Pruebas de Penetración 52
4.4.1. Nmap 52
4.4.2. Metasploit 53
4.4.3. Análisis de Red Wireshark 54
5. Resultados y discusión 56
5.1. Resistencia a ataques comunes 56
5.1.1. Ataques de fuerza bruta y diccionario contra los mecanismos de autenticación: 56
5.1.2. Ataques de interceptación y modificación de tráfico: 57
5.2. Informe sobre Ataques de Denegación de Servicio (DoS) 58
5.3. Propuestas de Mejora y Recomendaciones para Fortalecer la Seguridad de los Sistemas de Comunicación en la Industria 4.0 59
5.3.1. Adopción de Protocolos de Seguridad Avanzados 59
5.3.2. Capacitación Continua del Personal 59
5.3.3. Evaluaciones de Seguridad Regulares 59
5.3.4. Desarrollo de un Plan de Respuesta a Incidentes 60
5.3.5. Monitoreo y Detección de Amenazas 60
5.3.6. Colaboración con Expertos en Ciberseguridad 60
5.3.7. Actualización Regular de Software y Sistemas 61
6. Conclusiones 62
7. Referencias 64

Evaluación de la seguridad de los sistemas de comunicación en la industria 4.0

Autor(es):

ALEX DARIO AIMACAÑA JAMI

Resumen

La investigación se centra en evaluar la seguridad de los sistemas de comunicación en la Industria 4.0 ante la creciente amenaza de ciberataques, debido al aumento de la interconectividad de los dispositivos y la digitalización de los procesos industriales. Dado que la comunicación es una parte vital de cómo funcionan estas infraestructuras, los protocolos de comunicación inseguros pueden comprometer la confidencialidad, integridad y disponibilidad de la información. Para abordar este problema, empleamos un método conjunto, que incluye; Una revisión exhaustiva de la literatura (protocolos de comunicación, ciberseguridad), Pruebas de penetración en entornos virtualizados. Se estudiaron esquemas de autenticación/cifrado y se evaluó el rendimiento de varios protocolos para proteger los datos. Se muestra que, aunque varios protocolos como MQTT u OPC UA pueden aportar beneficios en cuanto a la interoperabilidad del usuario, no son tan fuertes en otros aspectos. Muchas de las pruebas de penetración demostraron que los sistemas no están adecuadamente protegidos; por lo tanto, se necesitan medidas de seguridad sólidas junto con controles de seguridad continuos. Se ofrece una potencial capacitación para el personal y un protocolo para la acción responsable en un incidente. Este trabajo es parte de un esfuerzo que contribuye a un mecanismo mundial que puede mejorar la seguridad de los sistemas de comunicación digital, y las organizaciones en Ecuador podrían beneficiarse plenamente del proceso de digitalización sin comprometer su seguridad.

Palabras clave:

Ciberseguridad, Industria 4.0, Protocolos de Comunicación, Pruebas de Penetración

Abstract

The investigation focuses on evaluating the security of communication systems in Industry 4.0 in the face of the growing threat of cyberattacks, due to the increase in the interconnectivity of devices and the digitalization of industrial processes. Given that communication is a vital part of how these infrastructures work, insecure communication protocols can compromise the confidentiality, integrity and availability of information. To address this problem, we employ a joint method, which includes; An exhaustive review of literature (communication protocols, cyber security), Penetration tests in virtualized environments. Authentication/encryption schemes were studied and the performance of various protocols to protect data was evaluated. It is demonstrated that, even though several protocols such as MQTT or OPC UA can provide benefits in terms of user interoperability, they are not as strong in other aspects. Many penetration tests demonstrated that systems are not adequately protected; Therefore, solid security measures are needed along with continuous security controls. It offers potential training for personnel and a protocol for responsible action in an incident. This work is part of an effort that contributes to a global mechanism that can improve the security of digital communication systems, and organizations in Ecuador can fully benefit from the digitalization process without compromising their security.

Keywords: Cybersecurity, Industry 4.0, Communication Protocols, Penetration Tests.

1. Introducción

La Industria 4.0 describe la transformación de la industria manufacturera tal como la conocemos, con tecnologías como IoT, IA y computación en la nube. El nuevo paradigma de la fábrica inteligente intenta hacer que todo el proceso de producción sea aún más eficiente. Dicho logro tiene un impacto en la comunicación entre dispositivos o máquinas y entre estos y las personas, y nos capacita para tomar decisiones en tiempo real. Nos hace productivos y nos brinda flexibilidad y agilidad, que están transformando la manera en que las empresas fabrican, refinan y entregan sus productos. Sin embargo, la magnitud de esta interconexión conlleva serios desafíos, especialmente en el ámbito de la ciberseguridad (González-Hernández & Macías, 2021)

A medida que las infraestructuras industriales se digitalizan y se vuelven cada vez más interdependientes, la necesidad de seguridad en los sistemas de comunicación crece. Además, con estas diversas redes y nuevas tecnologías convergiendo en la era del Internet de las Cosas (IoT), la creciente complejidad de los sistemas ciberfísicos está llevando a un entorno susceptible a varios tipos de ataques cibernéticos. Ataques como el ransomware industrial y el espionaje corporativo pueden comprometer la integridad de los datos y también son críticos para la continuidad de las operaciones y la seguridad de los empleados (Automatica e instrumentacion, 2024)

Por lo tanto, en tales circunstancias, se vuelve imperativo evaluar la seguridad de los sistemas de comunicación en la Industria 4.0. Los modelos de seguridad tradicionales podrían no ser capaces de abordar estos desafíos específicos que enfrentan entornos tan altamente digitalizados. Por esta razón, necesitamos definir métodos atípicos para descubrir, controlar y reducir el riesgo de la interconexión de dispositivos y sistemas. Nos centramos en evaluar la seguridad de los sistemas de comunicación de la Industria 4.0, que pueden conducir a vulnerabilidades y sugerir

mejoras para la confidencialidad, integridad y disponibilidad de la información compartida.

La inspección de los protocolos de comunicación y las pruebas de penetración, junto con el análisis de los métodos de autenticación y encriptación, generarán un nivel global para reforzar la seguridad en esta nueva planta industrial. La importancia de este estudio es contribuir a crear un entorno industrial más resistente y seguro, donde las empresas puedan aprovechar los beneficios

2. Determinación del Problema

La industria 4.0, desde una perspectiva global, es el nuevo movimiento de gestión de sistemas de producción e industriales a través de la digitalización y la interconexión. Pero este avance no se ha logrado sin la inquietante escalada de amenazas cibernéticas. En las organizaciones actuales, las amenazas ambientales, como, por ejemplo, las amenazas a infraestructuras críticas, causarán pérdida económica, interrupción de operaciones y pérdida de reputación. El creciente desarrollo de los ciberdelincuentes, junto con la falta de mecanismos de seguridad estándar para evitar nuevas vulnerabilidades, se considera hoy en día una amenaza para la sostenibilidad de la industria a escala mundial

Esto implica que la penetración de las tecnologías de la Industria 4.0 en América Latina sigue siendo limitada, y puede haber pocas prácticas de ciberseguridad establecidas. Siendo una región de avance tecnológico, el área no tiene formación de personal en el campo de la seguridad informática. Los equipos y sistemas industriales están interconectados, dejándolos expuestos a ataques, y no tienen una cultura de seguridad confiable, lo que representa una amenaza para la integridad de los datos y el correcto funcionamiento de las operaciones. Tal habilitación es bastante importante para que las empresas experimenten los beneficios de la era digital mientras mantienen la seguridad de las estructuras de comunicación. [4]

En Ecuador, este problema se agrava más porque existen tipos de sistemas de bloqueo y procesos de inmunización que se pueden aplicar, salvo algunas políticas de ciberseguridad para la Industria 4.0.

En el caso de Ecuador, al igual que en la mayoría de otros países, las organizaciones, especialmente las pequeñas y medianas empresas (PYMES), no tienen los recursos financieros o intelectuales para implementar medidas de seguridad efectivas. Dichos canales de comunicación no son seguros porque en algunos de ellos se utilizan protocolos que no incluyen seguridad. Dado que esta desafortunada

situación también se ajusta perfectamente a la economía local y a la confianza en los negocios, tienes todos los parámetros equivocados para continuar dañando, lo que significa que las buenas intenciones, la perseverancia e incluso la calma no pueden resolver. Por lo tanto, esto requiere un estudio completo de los sistemas de comunicación en el entorno ecuatoriano, junto con sus debilidades y la propuesta de posibles soluciones que se puedan utilizar para mitigar los mismos (Alvarez Vásquez & Arroyo Morocho, 2021).

2.1. Antecedente

La cuarta revolución industrial es un nuevo desarrollo que se realiza consistentemente basado en la actividad física y la gestión industrial. Está impulsada por la convergencia de tecnologías disruptivas, incluyendo IoT, datificación, IA y la computación en la nube. Como resultado de estos avances, las empresas han aprendido a automatizar y, en algunos casos, cómo interactúan los dispositivos, máquinas y personas entre sí y trabajan.

Pero esta unión ha creado nuevos desafíos, particularmente en el ámbito de la ciberseguridad. Los estudios indican que la superficie de ataque del cibercrimen se ha ampliado junto a la digitalización de los sistemas de fabricación y el aumento de la conectividad a través de las redes industriales. (González-Hernández & Macías, 2021) indican que hay una escasez de profesionales con las habilidades de ciberseguridad requeridas en el sector industrial, lo que expone a las organizaciones a nuevas amenazas.

Además, la Asociación Internacional de Ciberseguridad ha informado que el número de incidentes de seguridad dirigidos al sector industrial ha aumentado a un ritmo alarmante, por lo que existe una necesidad imperiosa de establecer un enfoque integrado para evaluar y mejorar la seguridad de los sistemas de comunicación (oas.org, 2024). Los informes de investigación recientes sobre los ataques a los Sistemas Ciberfísicos (CPS) (por ejemplo, ver Yagnyasenee) indican que son altamente vulnerables a ciberataques, cuya implementación puede causar que las

empresas sufran enormes pérdidas monetarias, así como impactos negativos en el desarrollo debido a la publicidad desfavorable.

El despliegue de la Industria 4.0 en América Latina aún está emergiendo. (Gupta, 2018)sugiere que aún hay muchas organizaciones sin una estrategia operativa en ciberseguridad. La formación en temas de seguridad informática está en particular ausente, donde, como lo señala un informe de la Universidad Politécnica Salesiana, esto agrava el problema (Acosta Gallo, 2024).

La situación es aún peor en Ecuador debido a la ausencia de infraestructura de ciberseguridad y la falta de legislación en ciberseguridad relacionada con los conceptos de la Industria 4.0. Especialmente las pequeñas y medianas empresas (pymes) no tienen la capacidad ni el conocimiento necesario para implementar soluciones seguras. Como resultado, se hará evidente la necesidad de evaluar y garantizar la seguridad de los sistemas de comunicación en el contexto de la Industria 4.0. Esta investigación busca ofrecer una contribución en cuanto al establecimiento de un marco de seguridad que permita a las organizaciones ecuatorianas aprovechar al máximo los beneficios que ofrece la digitalización sin poner en riesgo sus sistemas e información.

2.2. Pregunta de la investigación

¿Evaluar la seguridad de los sistemas de comunicación en la Industria 4.0 en Ecuador permitirá identificar vulnerabilidades y mejorar la protección de los datos en las empresas?

3. Marco teórico referencial

La base teórica es casi inevitable en los estudios de investigación porque es lo que dirige el análisis en la dirección correcta. Integra esas teorías, hasta el punto en que hacen posible situar la investigación en un panorama más amplio del conocimiento, y las integra con otras conceptualizaciones y con otros trabajos que se derivan de

esas conceptualizaciones. Esto se construye mediante una revisión sistemática de la literatura, resultando en 2-3 conceptos clave y comprendiéndose las teorías como relevantes para el estudio.

3.1. Protocolos de comunicación utilizados en la industria 4.0

Esta parte de la investigación presenta un estado del arte sobre los desafíos de la Industria 4.0 en relación con la ciberseguridad. Se identificará el IIOT, lo que ayudará al lector a entender la infraestructura de la industria para ser muy útil, familiarizarse con el IIOT en el dominio industrial y asegurarse de profundizar en la complejidad del dominio industrial.

Una vez que se analicen los problemas y se pueda identificar la infraestructura necesaria para apoyar los procesos más importantes de la Industria 4.0, el próximo gran problema es decidir las principales vulnerabilidades y riesgos que implican estas brechas de seguridad. La comunicación y encriptación del IIOT se analizarán en detalle entonces. Esto construirá un adecuado trasfondo teórico y una amplia información sobre el funcionamiento de la Industria 4.0, los desafíos a enfrentar, y los mecanismos, protocolos y técnicas de encriptación seleccionados para la infraestructura de la industria de cuarta generación.

3.2. Clasificación de Protocolos de comunicación

3.2.1. Protocolos de Capa de Aplicación

3.2.1.1. MQTT:

Significa Transporte de Telemetría de Encolado de Mensajes. Sigue un modelo de publicación/suscripción con dos tipos de entidades: el intermediario y los clientes. El intermediario es un servidor que recibe mensajes de los clientes y los envía a otros clientes que se suscribieron al "tema" en el que estaban interesados en

mensajes entrantes, y los clientes que se conectan al intermediario se suscriben al tema de interés y publican mensajes hacia ellos que el intermediario reenvía a todos los clientes suscritos a ese tema. El protocolo MQTT, liviano y flexible, admite una amplia gama de casos de uso de IoT con TCP/IP, UDP/IP o TLS, lo que hace que las conexiones sean eficientes y de alto rendimiento (Gallardo, 2020).

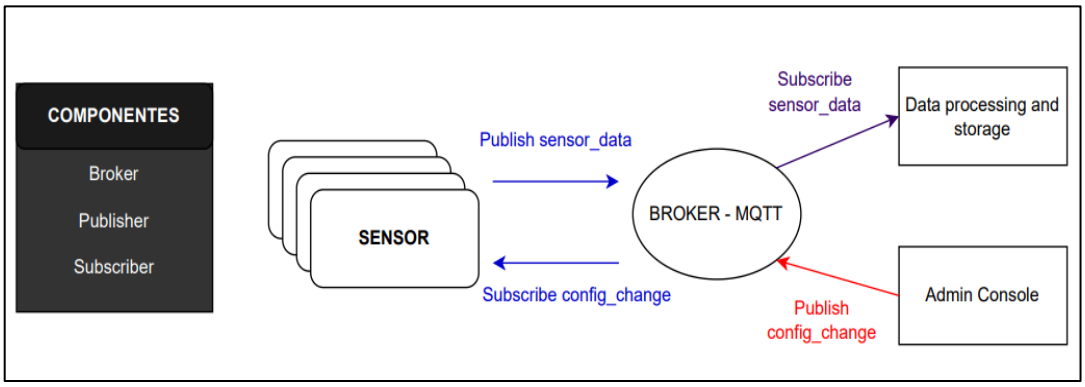


Figura 1. Modelo MQTT. Elaborado por: Alex Aimacaña.

3.2.1.2. HTTP:

Un protocolo para la World Wide Web en la capa de la aplicación. Es un protocolo de transferencia orientado a transacciones cliente-servidor en el que la secuencia petición-respuesta juega su papel en la creación de una conexión. Se intercambian mensajes individuales entre clientes y servidores. El cliente, o más bien el agente de usuario (UA), es cualquier agente que representa al usuario, como un navegador web. Pero, en cambio, el servidor web es el que recibe solicitudes de los clientes y les envía los datos solicitados. A nivel abstracto, un servidor es una sola entidad. Sin embargo, puede estar compuesto por múltiples componentes. La arquitectura web también incluye dispositivos intermediarios, llamados proxies, que manejan mensajes HTTP (Gallardo, 2020).

3.2.1.3. CoAP:

Un protocolo de capa de aplicación para usar con nodos restringidos y redes restringidas en el Internet de las Cosas. CoAP también es un modelo de intercambio de mensajes asincrónico y utiliza transporte basado en UDP a diferencia de HTTP, lo que lo hace más simple y ligero que este último. Algunas de estas características

de CoAP incluyen su interoperabilidad con HTTP en forma de pasarelas, soporte para los mismos métodos REST que los de HTTP, inclusión de seguridad mediante DTLS y la capacidad para el descubrimiento y exploración de recursos en servidores. Estas propiedades hacen del CoAP una mercancía HTTP para entornos con dispositivos de recursos limitados y compatibilidad con la Web existente (Ganazhapa Malla, 2024).

3.2.1.4. OPC UA:

Es un protocolo de interoperabilidad del sistema de automatización industrial. A diferencia de las versiones anteriores, presenta una arquitectura independiente de plataformas específicas, por lo que es compatible con una amplia gama de aplicaciones y dispositivos. Gracias a este estándar, es posible una comunicación segura y eficiente entre máquinas y varios sistemas. Las tecnologías y protocolos se vuelven interoperables. OPC UA ofrece características como modelado de información, seguridad integrada y la capacidad de crecer desde aplicaciones pequeñas hasta sistemas distribuidos. Su arquitectura basada en servicios es uno de los mejores enfoques que lo hace adecuado para ser utilizado en la Industria 4.0 y el IoT, centrado en la conectividad y cooperación en el ámbito industrial. (Hermann Mirko, 2024).

3.2.2. Protocolos de Capa de Transporte:

3.2.2.1. TCP:

TCP (Protocolo de Control de Transmisión) es un protocolo de la capa de transporte en el modelo TCP/IP, que es responsable de facilitar una transferencia de datos confiable entre una aplicación en varios dispositivos de la red. Lo hace abriendo una conexión antes de comenzar a enviar datos.

Esto no es un error en el protocolo que lleva acuses de recibo y retransmisiones para garantizar una entrega fiel. También soporta el control de flujo para evitar ser desbordado, y el control de congestión para evitar la congestión de la red. TCP divide los datos en segmentos más pequeños y también los organiza en orden. El

circuito de control puede estar en un navegador web, correo electrónico, transferencia de archivos, etc., y requiere una entrega estrictamente correcta. (CAICEDO PAREDES, 2022).

3.2.2.2. UDP:

En el modelo TCP/IP, ¿qué protocolo de la capa de transporte ofrece servicios de datagramas sin conexión?, Es más rápido que el TCP, pero no es fiable y no garantiza la llegada de paquetes. Es un protocolo inseguro que acelera la comunicación. No tiene disposiciones para la confirmación de llegada de datos y puede perder algo de información.

Finalmente, no está relacionado y no regula el ritmo de envío, lo que puede llevar a la pérdida de datos por congestión de la red. UDP transmite datos en bloques conocidos como datagramas y es más eficiente que la versión TCP debido a la falta de confirmaciones. Cada uno de ellos debe saber en qué puertos las dos aplicaciones escucharán nuevas conexiones. Por esta razón, es especialmente adecuado para aplicaciones donde la velocidad es más importante, como la transmisión de video, los juegos en línea y VoIP, que priorizan la entrega rápida, incluso si se pierde parte de los datos (González de Lena Alonso, 2022).

3.2.3. Protocolos de Capa de Red:

3.2.3.1. IP:

Esto se debe a que el modelo OSI describe cómo los datos pueden ser transmitidos de un dispositivo a otro en diferentes redes en la Capa de Red, específicamente cuando se habla bajo la definición del Protocolo de Internet (IP). Cada dispositivo conectado a Internet (router, computadora, teléfono, etc.) debe tener su dirección única en la red; este protocolo, en su forma básica, se designa como IPv4 con direcciones de 32 bits (alrededor de 4.3 mil millones de direcciones, aproximadamente cada persona en la Tierra obtiene una dirección única) e IPv6 que utiliza direcciones de 128 bits para compensar la escasez de direcciones. IP es un protocolo sin conexión y no garantiza la entrega o el orden de los paquetes y

permite la fragmentación de datos. Además, tiene una correlación con otros protocolos como el ICMP que maneja los mensajes de error y el ARP que traduce la dirección IP en direcciones MAC (Cano, 2024).

3.2.3.2. IPv6:

Es la última versión del protocolo que se utiliza para identificar dispositivos en Internet debido al hecho de que nos estamos quedando sin espacio bajo el antiguo esquema de direcciones IP (IPv4). También utiliza direcciones de 128 bits, lo que se traduce en un número potencialmente ilimitado de direcciones únicas, por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 ofrece una calidad mucho mejor, como el enrutamiento, y permite configuraciones de computadoras más fáciles en redes locales, en comparación con IPv4. También tiene características de seguridad integradas y soporte de QoS. La demanda de conectividad ha estado aumentando, y para el crecimiento de Internet y las aplicaciones que dependen de ella en todo el mundo, la dirección de red para usar al transmitir esos datos (Cano, 2024).

3.3. Dispositivo 4.0

Los dispositivos IIoT más populares en la Industria 4.0 son equipos inteligentes que ayudan en el proceso de adquisición de datos en el campo industrial. Es posible verificar la producción de la eficiencia del producto de los sistemas y recopilar información. A continuación, se describen los dispositivos principales en la Industria 4.0.

3.4. Raspberry Pi

Una máquina esencial para cada operación de la Industria 4.0. La conexión a Internet ofrece la posibilidad de integrar varias aplicaciones y sistemas que ofrecen recopilación y análisis de datos en tiempo real. También vale la pena mencionar que la Raspberry Pi es una placa extremadamente flexible que también puede ser utilizada para otras aplicaciones, como la automatización de tareas y el control de procesos. Entre otras características, se puede programar con lenguajes amigables

para niños (como Scratch y Python), pero también es un regalo genial para el desarrollador amante de la tecnología en tu vida. Con un tamaño reducido y un bajo costo, es una opción atractiva para las empresas que desean bajar la barrera para la innovación sin tener que invertir mucho dinero por adelantado. En resumen, la Raspberry Pi no solo permite la posibilidad de conectarse, sino que también impulsa el desarrollo de soluciones industriales personalizadas (Acosta Gallo, 2024).

3.5. PLC (Controlador Lógico Programable):

Los utilizamos principalmente para dirigir maquinaria y el sistema operativo en producción. Estos son controladores completamente programables diseñados para adaptarse a una amplia gama de aplicaciones con AOT específico para la industria. Los PLC son capaces de tener múltiples sensores y actuadores conectados a sus entradas/salidas digitales o analógicas, permitiendo que máquinas complejas se controlen con gran precisión. También son bastante resistentes, lo que los hace funcionar bien en condiciones adversas y, por lo tanto, son inmunes a condiciones extremas; en otras palabras, pueden soportar golpes y eso los hace ideales para entornos industriales rigurosos. Conducen a una mayor productividad y al mismo tiempo, reducen los errores humanos y mejoran la seguridad en el lugar de trabajo (Acosta Gallo, 2024).

3.6. Sensores PIR (Sensores de Infrarrojo Pasivo)

El sensor PIR es un sensor único, ya que es el único tipo de sensor capaz de detectar la radiación infrarroja de un humano o un animal. Se utilizan para seguridad (indicando una entrada no autorizada) o para encender una luz. El control de iluminación del espacio en aplicaciones industriales basado en sensores PIR para optimizar la gestión de partes y el ahorro de recursos se puede usar para la supervisión en áreas que involucran el consumo de recursos de iluminación, como salas de trabajo. Funcionan al detectar cambios en la radiación infrarroja, por lo que

pueden detectar a una persona o un animal. No sólo son fáciles de instalar, sino que también se incorporan a su sistema en muy poco tiempo. En conclusión, la tecnología de sensores PIR es la herramienta necesaria que puede ayudarnos a mejorar la seguridad y el control industrial (Acosta Gallo, 2024).

3.7. Interruptores de Límite

Los interruptores portátiles, también conocidos como "sensores de fin de recorrido", son desplegables para controlar la ubicación del objeto y detectar el estado del objeto en una aplicación industrial. Se usan principalmente para indicar cuando un objeto ha llegado a una posición predeterminada de modo que un obstáculo pueda ser detenido o desviado. Eso es importante para proteger la maquinaria y al operador. Los interruptores de límite se encuentran comúnmente en una variedad de contextos, desde cintas transportadoras y robots industriales hasta equipos de estudio. Pueden diseñarse para acomodar diferentes tipos de control: botones, palancas o sensores ópticos. Estos sensores son indispensables para la automatización y el control de procesos en la industria debido a su capacidad de proporcionar retroalimentación sobre la posición de los objetos (Acosta Gallo, 2024).

3.8. Sensor Óptico

El sensor de diámetro puede interrumpir los haces de luz para detectar la presencia de objetos. Los sensores ópticos se utilizan en entornos industriales para medir una variedad de variables como la velocidad y la posición de varios elementos en movimiento. Funcionan emitiendo luz, que puede ser reflejada o absorbida por un objeto que pasa. Como resultado, los sistemas automatizados son capaces de tomar decisiones relevantes en tiempo real, lo que lleva a una mayor eficiencia de los procesos. Los sensores ópticos son independientes del sistema y pueden utilizarse en aplicaciones de clasificación de productos e inspección de calidad. Además, pueden operar en las peores condiciones, por lo que son perfectos para fábricas y

plantas de producción. En resumen, los sensores ópticos juegan un papel vital en la automatización y optimización de los procesos industriales (Acosta Gallo, 2024).

3.9. Sensor Piak

Esta es una herramienta industrial ampliamente utilizada que muchas fuentes en todo el mundo usan para la recopilación de datos infrarrojos. La característica que la hace ideal para la mayoría de las empresas es que mantiene a las compañías en control de los materiales procesados. El sensor Sharp es flexible y puede usarse para varias aplicaciones de automatización de procesos para medir y detectar objetos. Logra esto enviando luz infrarroja y viendo cómo esa luz se refleja en los objetos cercanos. Esto proporciona la capacidad de monitorear los niveles de producción, la identidad y la condición del material en bruto en tiempo real. En la industria, se puede girar y usar fácilmente porque se puede conectar fácilmente a los sistemas de control. (Acosta Gallo, 2024).

3.10.Módulo ESP32

Este microcontrolador es uno de los más usados en la industria. Su capacidad para ser programado para realizar diversas funciones lo convierte en un favorito para proyectos de automatización de tareas y control. Una de las características más asombrosas del ESP32 es su capacidad de comunicación que incluye diferentes tipos de Bluetooth y WiFi ayudándonos a conectarnos con diferentes tipos de dispositivos o sistemas. Esto permite que las redes de sensores y actuadores sean monitoreadas y controladas a distancia. El dispositivo es altamente eficiente en energía y compacto, lo que es adecuado para aplicaciones integradas. Para concluir, el módulo ESP32 ha permitido a las empresas innovar en el área de la Industria 4.0 y sirve como una poderosa herramienta para hacerlo (Acosta Gallo, 2024).

3.11. Dispositivos IoT y su Relación con los Protocolos

En el Internet de las Cosas, hay muchos dispositivos IoT disponibles para enlazar e interactuar con sistemas. Hay diferentes tipos de dispositivos más comunes:

3.11.1. Sensores:

- Sensores de temperatura: Se utilizan para el control y monitoreo de temperatura en aplicaciones industriales.
- Sensores de presión: Empleados para detectar la presión en dispositivos mecánicos y sistemas de fluidos.
- Sensores de humedad: Estos se utilizan para monitorear los niveles de humedad en unidades de manufactura que tienen productos alimenticios y farmacéuticos.

3.11.2. Actuadores:

- Válvulas eléctricas: Controlan el flujo de líquidos o gases en sistemas automatizados.
- Motores eléctricos: Utilizados para mover componentes de maquinaria y equipos automatizados.
- Cilindros neumáticos: Proporcionan movimiento lineal en aplicaciones de automatización.

3.11.3. Controladores:

- Controladores Lógicos Programables (PLC): Dispositivos que automatizan procesos industriales mediante la programación de secuencias de operaciones.
- Microcontroladores: Utilizados en sistemas embebidos para controlar dispositivos y recoger datos de sensores.

- Gateways IoT: Actúan como intermediarios entre dispositivos IoT y la nube, facilitando la transmisión de datos.

3.12. Desafíos en la Comunicación de la Industria 4.0

La siguiente parte de la investigación indica referencias relacionadas con las dificultades de la Industria 4.0 en el ámbito de la ciberseguridad. En este contexto, se inspeccionan dispositivos para comprender en profundidad la infraestructura de la industria y familiarizarse con el campo industrial en el que se aplica el IIoT. De hecho, después de una revisión exhaustiva de desafíos como la interoperabilidad, la latencia y la escalabilidad, además de investigar la infraestructura que sostiene los procesos críticos de la Industria 4.0, abordaremos posteriormente las vulnerabilidades más observadas y los riesgos asociados con las brechas existentes. Después de las discusiones sobre IIoT, la siguiente sección se centrará en los protocolos de encriptación y las técnicas en entornos IIoT para construir una base teórica que establezca un conocimiento detallado sobre cómo funciona la Industria 4.0, dónde están los impedimentos por resolver y qué dispositivos, protocolos y técnicas de encriptación se seleccionan en una infraestructura industrial de cuarta generación (Becerra, 2020).

3.13. Interoperabilidad

Proporciona una coordinación fluida para varios sistemas y aplicaciones. En el contexto de la Industria 4.0, significa que los dispositivos IIoT de diferentes empresas o construidos utilizando diferentes tecnologías pueden trabajar juntos para intercambiar datos. Esta interfaz en las empresas industriales permite, así, que diversos y múltiples sistemas, tecnologías y plataformas se conviertan en parte de un entorno integrado y, por lo tanto, funcionen efectivamente juntos con los procesos ideales empleados. (Barbara, 2024).

3.14. Latencia

La latencia es el período de tiempo entre el inicio de la transmisión de datos y la llegada de esos datos al destino previsto. Esto es esencial para la Industria 4.0, donde se pueden tener que tomar decisiones a la velocidad de los datos en tiempo real. La latencia es crítica en casos como el control de procesos y el monitoreo de maquinaria, donde las largas latencias provocan ineficiencias operativas y problemas de seguridad (Delgado Batista, 2024).

3.15. Escalabilidad

La escalabilidad es la capacidad de un sistema, red o proceso para manejar una cantidad creciente de trabajo, o su potencial para acomodar el crecimiento. En términos de Industria 4.0, esto indica que la estructura debe tener la capacidad de adaptarse a un mayor número de dispositivos conectados y también una mayor cantidad de datos personalizados. La escalabilidad permite a una empresa crecer sus operaciones y adoptar nuevas tecnologías con la garantía de que se necesita poco o ningún rediseño en la arquitectura o el hardware utilizado en la arquitectura, permitiendo así un crecimiento sostenible (Delgado Batista, 2024).

3.16. Características de Seguridad de los Protocolos

En la era de la Industria 4.0, los protocolos de comunicación juegan un papel crucial en la transmisión de datos en los sistemas de IoT, y la seguridad de estos protocolos también es un aspecto clave en la lucha contra el cibercrimen. A medida que los dispositivos se interconectan, también lo hace la necesidad de preservar la privacidad de la información. Estas capacidades aseguran que solo los usuarios autorizados puedan ver los datos, que no sean manipulados durante su tránsito y que los usuarios y máquinas puedan ser identificados.

Sin embargo, las interceptaciones y los ataques de denegación de servicio, por ejemplo, amenazan la seguridad. Manejar estos riesgos de una manera bien organizada es clave para preservar la integridad y accesibilidad del servicio. Esto implica que, en un mundo industrial cada vez más digitalizado, es importante implementar un conocimiento profundo sobre las medidas de seguridad y las posibles vulnerabilidades de estos sistemas para proteger tales sistemas (Cán Chicol, , 2022).

3.16.1. Confidencialidad:

Sólo las personas autorizadas pueden tener acceso a la información. Esto se realiza utilizando métodos de encriptación como AES o TLS para cifrar los datos a medida que viajan, evitando así la interceptación de la información. El deber principal de la confidencialidad es asegurar que la información confidencial se mantenga confidencial y que solo el usuario o dispositivo legítimo pueda hacer uso de ella. El principio de seguridad funciona principalmente en la comunicación, cuando ese único fragmento de información solo puede ser accedido por la persona autorizada. Para encriptar, se utilizan algoritmos como AES con claves de 128, 192 o 256 bits para proteger los datos. Además, TLS es un protocolo de seguridad que asegura la comunicación entre un servidor web y un navegador web, encriptando los datos durante la transferencia (Cán Chicol, , 2022).

3.16.2. Integridad:

Protocolos de Comunicación: Es la garantía de que ningún mensaje ha sido alterado en tránsito, es decir, que lo que el destinatario recibe es exactamente lo que se envió. Esto se realiza mediante el uso de funciones hash como SHA-256, que te proporcionará un hash único para tu porción de datos que cambiará cuando tu porción cambie. Este tipo de técnicas son importantes para fomentar la confianza en las comunicaciones, prevenir la manipulación no autorizada de la información y garantizar su integridad en contextos sensibles (Cán Chicol, , 2022).

3.16.3. Autenticación:

Es un paso importante que permite a los usuarios y dispositivos autenticarse mutuamente. Dicha validación se lleva a cabo utilizando certificados digitales emitidos por una autoridad de certificación, los cuales demuestran que los usuarios y dispositivos son entidades auténticas. También se implementan algunos métodos de autenticación basados en tokens que producen códigos especiales por sesión y hacen que el sistema sea más seguro. Yo también utilizo 2FA (autenticación de dos factores), donde se proporciona una segunda forma de identificación y se solicita una segunda forma de confirmación al usuario. (Cornejo Velázquez, 2024).

3.16.4. No Repudio:

Confirma que un firmante no puede repudiar la firma y el mensaje. Todo está registrado, incluso lo básico, y se puede acceder a los registros, lo que ayuda a que funcione de esta manera o de aquella. Estas herramientas son útiles para documentar comunicaciones desafiadas para que podamos mantenernos más responsables dentro de nuestros círculos digitales de comunicación (Cán Chicol, , 2022).

3.16.5. Disponibilidad:

Es el mantenimiento de los servicios y datos disponibles en todo momento. Redundancia mediante múltiples copias en varios casos, cuando se debe lograr redundancia, es necesario duplicar recursos y sistemas críticos para que no se produzcan fallos. Además, se implementan procedimientos de recuperación ante desastres para asegurar una recuperación rápida del sistema y la restauración de la información en caso de un desastre. Estos son métodos que no se pueden omitir, si se desea que los clientes experimenten un servicio ininterrumpido y puedan acceder a cualquier dato y recurso en todo momento (Cornejo Velázquez, 2024).

3.17. Amenazas y Vulnerabilidades en la Industria 4.0

3.17.1. Ataques de Intercepción:

Estos comprenden, por ejemplo, ataques exitosos contra los datos transmitidos entre dispositivos, de modo que en el peor de los casos incluso se pierde la confidencialidad de la información y la integridad de los datos transmitidos. Una de las formas más comunes de ataques son los llamados ataques de "hombre en el medio" (MitM), en los cuales el atacante se coloca entre el emisor y el receptor, interceptando (y posiblemente modificando) datos que se están enviando. Uno de los riesgos de estos perpetradores incluye la divulgación de información y comunicaciones confidenciales. (Álvarez Roldán, 2020).

3.17.2. Inyección de Código:

Algunos tipos de inyección de código, como cuando un atacante contamina las entradas de un programa para alterar la forma en que se ejecuta, se pueden prevenir. Los hackers maliciosos pueden aprovecharse de la falta de validación y/o sanitización de las entradas del usuario antes de ser incluidas en el código, inyectando código que el sistema ejecuta y descifra. Esto puede ocurrir en cualquier nivel; las consultas a bases de datos y los scripts del lado del servidor, así como del lado del cliente, pueden ser responsables, al igual que el código que has escrito. El impacto potencial de la inyección de código es bastante drástico, que va desde el acceso sin restricciones a datos privados hasta la escalada de privilegios o la usurpación total de la máquina por parte del atacante. Por ello, los equipos de desarrollo de software deben asegurarse de que no solo incorporen una buena validación de entradas, sino también una buena sanitización de entradas.

3.17.3. Fugas de Datos:

Es cuando un dato sensible se expone inadvertidamente como resultado de un error de configuración de seguridad en un sistema. Ocurre cuando la información sensible

o confidencial se comparte accidentalmente de manera no autorizada. Permite a actores malintencionados obtener información sensible, como datos personales o información crítica para el negocio de los usuarios.

Esto puede ser el resultado de una configuración incorrecta, un control de acceso inadecuado, medidas de seguridad que no funcionan correctamente o simplemente un mal diseño de seguridad. La exposición de dichos datos puede presentar un riesgo significativo para la vida privada de la persona involucrada, así como para la reputación y la estabilidad financiera de la institución responsable. Por lo tanto, necesitamos desarrollar marcos de procesos seguros exitosos para prevenir tales incidentes (Arredon Amaro, 2016).

3.17.4. Denegación de Servicio (DoS):

La denegación de servicio impide que los usuarios legítimos utilicen un servicio. Los ataques DoS y DDoS son ataques de fuente única o múltiple contra el servidor o sistema para agotar sus recursos y dejarlo no operativo. Uno de estos ataques es el DDoS, que puede forzar a un servidor a detenerse debido a demasiadas visitas externas; de lo contrario, no responderá a las solicitudes, negando así incluso a los propios usuarios legítimos de la alianza el acceso. Estos ataques pueden causar serias implicaciones financieras y reputacionales (pérdida de ingresos, daño a la reputación de la organización), lo que enfatiza la necesidad de aplicar sistemas de defensa adecuados (Garofalo, 2024)..

3.17.5. Vulnerabilidades en Protocolos:

Las fallas de protocolo ocurren a nivel de diseño y/o implementación de algunos protocolos de comunicación particulares, debido a las debilidades intrínsecas en el diseño de un protocolo adecuado y/o vulnerabilidades que se explotan para lanzar un ataque. Estar expuesto a estas cosas sin medidas de protección es inseguro.

Por ejemplo, si tienes protocolos (como MQTT, CoAP) utilizados en muchos despliegues de Internet de las cosas (IoT) que no tienen una autenticación sólida y

una confidencialidad de datos fuerte, hay una alta probabilidad de exposición a ataques. El espionaje no requiere tales defensas y permite al atacante ver o modificar cualquier cosa que se transmita, destruyendo la integridad de los datos. Como consecuencia, si no se siguen buenas prácticas de seguridad durante el desarrollo y la configuración de los protocolos, el abuso de esas vulnerabilidades es posible. (Garofalo, 2024).

Falta de Actualizaciones:

Lo mismo podría decirse sobre el cuidado y mantenimiento del firmware y software en el dispositivo, lo cual podría permitir que sea comprometido. Esta situación ocurre cuando el producto no cubre todos los agujeros de seguridad de un sistema. De hecho, los dispositivos desprotegidos y sin parches pueden ser objetivos muy fáciles para los cibercriminales que podrían usarlos para acceder a redes o robar información sensible. Un mantenimiento deficiente no solo puede dejar el sistema abierto a ataques, sino que también plantea problemas de integridad y seguridad de la información. Por lo tanto, establecer políticas de actualización y mantenimiento se presenta como una de las formas fundamentales para garantizar la seguridad de dispositivos y sistemas.

3.18. Estudios Previos

A continuación, citas de artículos y estudios que analizan la efectividad y seguridad de los protocolos en la industria 4.0.

Se muestran en la siguiente Tabla 1:

Número	Autor(es)	Título	Año	Fuente	Tipo de Documento	Análisis
1	Albuja Loachamin, Luisa Fernanda; Alvear Loor, Jessica Geovanna; Sarango Romero, Cerónica Janeth	Technological Inequalities in Education in Ecuador: Addressing the Educational Gap	*2023*	(Albuja Loachamin, Alvear Loor, & Sarango Romero, 2023)	Tesis	Analiza las desigualdades tecnológicas en la educación ecuatoriana, proporcionando contexto sobre la necesidad de capacitación en ciberseguridad.
2	Álvarez Vásquez, Oswaldo Wilfrido;	Análisis de la Industria 4.0 como factor diferenciador	2021	(Alvarez Vásquez & Arroyo		Examina cómo la Industria 4.0 impacta el sector industrial en

	Arroyo Morocho, Flavio Roberto	del Sector Industrial del Ecuador		Morocho, 2021)	Ecuador, relevante para entender el contexto de la ciberseguridad en este ámbito.
3	Arredon Amaro, Gustavo Cristian	Diseño de un modelo de gestión para la prevención de fugas de información en disposición móviles de empresas mexicanas	2016	(Arredon Amaro, 2016)	Proporciona un marco para la gestión de la seguridad en dispositivos móviles, útil para establecer prácticas en la Industria 4.0.
4	BASANTES SUÑIGA, ANGELO JESUS	ANÁLISIS COMPARATIVO SOBRE LA PLATAFORMA DE DESARROLLO NOCODE GLIDEAPP Y LA PLATAFORMA LOW-CODE OUTSYSTEMS EN LA CREACIÓN DE APLICACIONES WEB.	2022	(BASANTES SUÑIGA, 2022)	Ofrece una comparación entre plataformas de desarrollo, relevante para la implementación de soluciones seguras en la Industria 4.0.
5	Becerra, L	Tecnologías de la información y las Comunicaciones en la era de la cuarta revolución industrial: Tendencias Tecnológicas y desafíos en la educación en Ingeniería	2020	(Becerra, 2020)	Discute las tendencias tecnológicas y desafíos en educación, ayudando a entender la formación necesaria en ciberseguridad.
6	Bravo Vera, Henry Fabricio	El desarrollo Low/No-code y el futuro de los desarrolladores de software	2022	(Bravo Vera , 2022)	Aborda el impacto del desarrollo low/no-code en la industria, relevante para la seguridad en aplicaciones industriales.
7	Brosnan, Andrew	EXPLORING THE NATURE OF RISK IN DIGITAL TRANSFORMATION: A PROBLEMATISATION PERSPECTIVE OF LOW-CODE/ NO-CODE PLATFORM RISK	2024	(Brosnan, 2024)	Analiza los riesgos asociados a plataformas low-code/no-code, importante para la evaluación de seguridad en la Industria 4.0.
8	CAICEDO PAREDES, JEFFERSON JESÚS	ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DEL PROTOCOLO DE RED DE CAPA DE TRANSPORTE DNS-OVER-QUIC (DOQ) EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO	2022	(CAICEDO PAREDES, 2022)	Evalúa un protocolo de red, proporcionando información técnica relevante para la seguridad en sistemas de comunicación.
9	Cano, Jan Lopera	Diseño y creación de una suite de protocolos de capa de red orientado a videojuegos	2024	(Cano, 2024)	Ofrece insights sobre protocolos de red, útiles para entender la seguridad en la comunicación industrial.
10	Carmona Vásquez, Juan David; Monsalve Giraldo, Edwin Andrés	Plataforma de ciberseguridad para el aprendizaje y entrenamiento de hacking ético para estudiantes universitarios	2024	(Carmona Vásquez & Monsalve Giraldo, 2024)	Presenta una plataforma de ciberseguridad que puede servir como modelo para la capacitación en la industria.

Tabla 1. Estudios Previos de análisis de efectividad y seguridad. Elaborado por Alex Aimacaña

4. Materiales y metodología

Se realizó una revisión de literatura sobre las diferentes vulnerabilidades del IIoT (Internet de las Cosas Industrial) y su solución contraria, los protocolos y técnicas más relevantes utilizados en cifrado, y luego se analizó la estructura para una industria con IIoT. Esto ayudó a destilar los desafíos y oportunidades existentes en la seguridad de datos dentro de este paradigma.

Luego, se analizaron varios protocolos en cuanto a su viabilidad y sus capacidades de seguridad y protección de la información. Se construyeron entornos de prueba competitivos con el Raspberry Pi como el núcleo de nuestro sistema de lectura de sensores para este propósito.

El énfasis en esta evaluación está en la confidencialidad, integridad y disponibilidad de los datos de las organizaciones de interés mientras están en transmisión. El objetivo principal de este trabajo es validar la eficiencia de nuestros protocolos seleccionados en este contexto y diseñar protocolos más robustos para entornos industriales.

Con el fin de realizar pruebas de penetración y descubrir posibles ataques a los sistemas de comunicación, se construyeron escenarios de ataque dentro de las plataformas de prueba. Mediante software específico, los protocolos seleccionados fueron evaluados frente a diferentes patrones de comportamiento de ataque, tales como los basados en inyecciones y ataques de denegación de servicio, para investigar debilidades y futuras mejoras.

En segundo lugar, se evaluaron la idoneidad y las capacidades de seguridad de varios protocolos de comunicación. Se hizo hincapié en los métodos de autenticación (auth) y cifrado utilizados en cada protocolo. Se realizó un análisis comparativo y pruebas de rendimiento de estos mecanismos para evaluar su fortaleza en el mantenimiento de la seguridad de los datos transmitidos en términos de confidencialidad e integridad.

4.1. Materiales para el entorno de prueba

La investigación se llevó a cabo inicialmente en la selección del material necesario para implementar el entorno de prueba, lo que permitió las verificaciones adecuadas de cada protocolo. A continuación, encontrarás las cosas que necesitarás para esto:

- ISO RASPBIAN
- ISO Kali Linux
- Software VirtualBox
- Computadora

Después de probar los materiales para el entorno de prueba, se desarrolló el diseño de múltiples topologías de red. Para estas configuraciones, se analizó la eficiencia de cada una de las arquitecturas en el contexto de la seguridad de la información, como se explica a continuación.

4.2. Preparación de ambiente

4.2.1. Instalación de Virtual Box

Primero, se dirigió a la página oficial de Oracle VM VirtualBox en Academic Software. Una vez allí, damos clic en el botón 'Descargar Oracle VM VirtualBox' y se inicia la descarga del instalador en el computador.

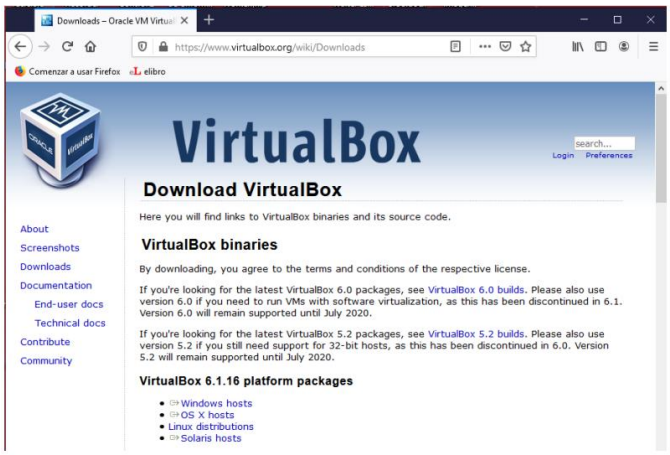


Figura 2. Página Oficial Virtual Box. Elaborado por: Alex Aimacaña

Después de que se complete la descarga. Ubicamos el archivo que tiene la extensión .exe. y damos doble clic en este archivo para abrirlo. Cuando se inicie el instalador, se muestra una ventana de bienvenida al proceso de instalación. Se da clic en el botón 'Next' para avanzar y comenzar a configurar el software en tu máquina.

Figura 3. Instalación Virtual Box. Elaborado por: Alex Aimacaña

Aquí presentamos una lista de componentes que podemos agregar a la instalación. Nos gustaría usar la configuración predeterminada y hacer clic en 'Siguiente'.

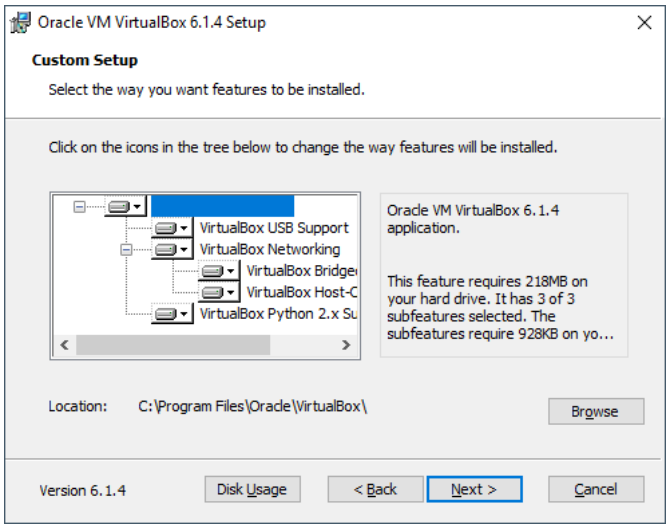


Figura 4. Instalación Virtual Box. Elaborado por: Alex Aimacaña

A continuación, damos check en los recuadros que son accesos directos lo cual facilitarán abrir el programa posteriormente, simplemente damos clic en 'Next' para proceder al siguiente paso.

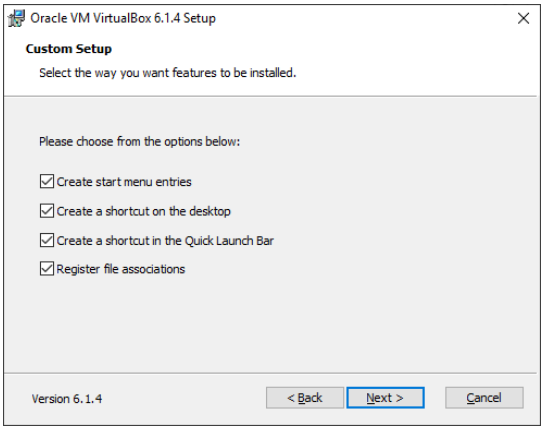


Figura 5. Instalación Virtual Box. Elaborado por: Alex Aimacaña

En esta etapa, se mostrará una alerta en la ventana, y luego se le solicitará si desea continuar con la instalación; simplemente haga clic en "Sí".

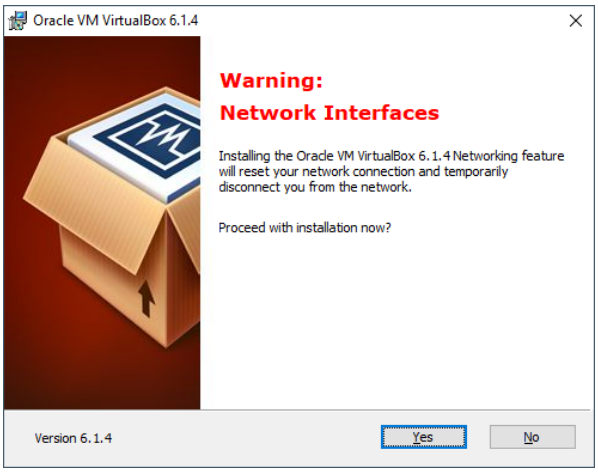


Figura 6. Instalación Virtual Box. Elaborado por: Alex Aimacaña

Ahora podemos comenzar el proceso de instalación del software. Luego, habrá un botón de "Instalar" en el que puede hacer clic para comenzar. Esto almacenará el instalador en su computadora, junto con todos los archivos que necesita para funcionar correctamente. Esto puede tardar unos minutos dependiendo de la rapidez de su computadora, así que tenga paciencia mientras VirtualBox se instala.

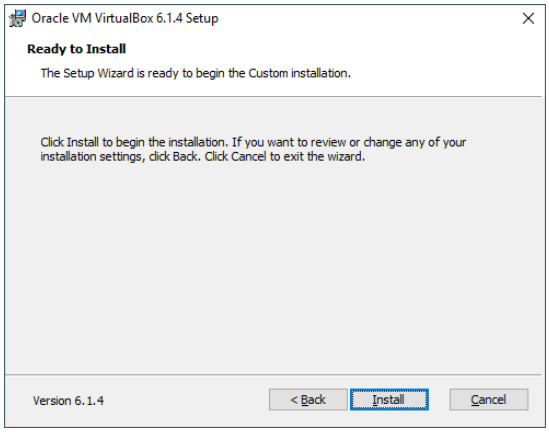


Figura 7. Instalación Virtual Box. Elaborado por: Alex Aimacaña

Se le solicitará nuevamente y haga clic en "Instalar" para instalar el paquete. Ahora VirtualBox está listo para instalarse en su máquina. Monitoree el progreso de la instalación en la barra, y cuando haya terminado, estará listo para su uso.

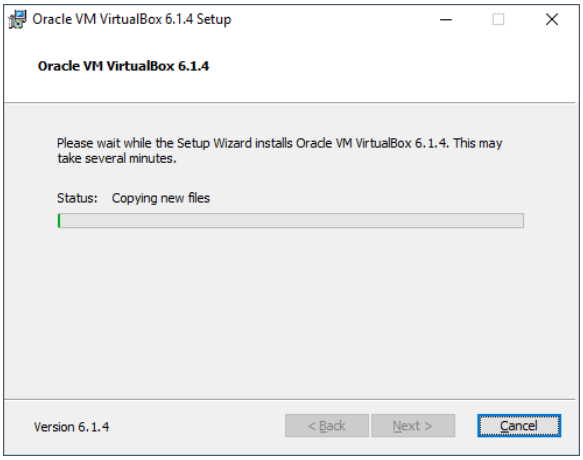


Figura 8. Instalación Virtual Box. Elaborado por: Alex Aimacaña

Una vez instalado, tendrá una opción para ejecutar el programa. Finalmente.

Figura 9. Instalación Virtual Box. Elaborado por: Alex Aimacaña

Interfaz de inicio de Oracle VM VirtualBox

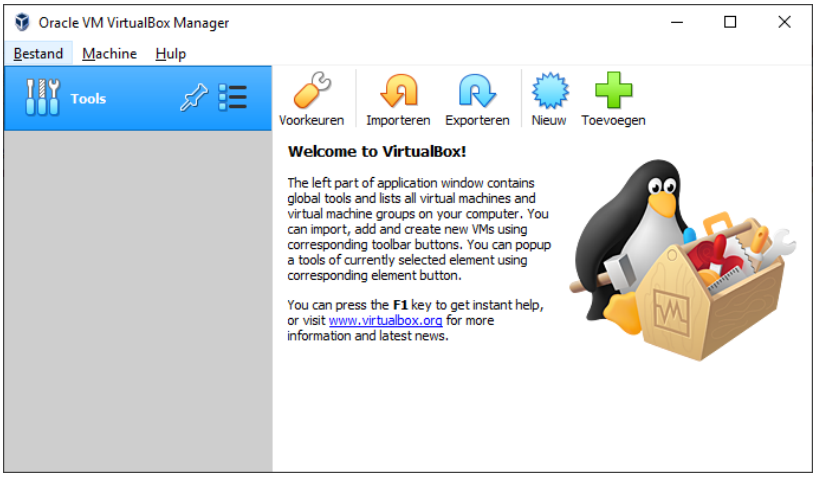


Figura 10. Instalación Virtual Box. Elaborado por: Alex Aimacaña

4.2.2. Instalación de Kali

Hay un sistema operativo tan lleno de herramientas de hacking como los demás, pero que se destaca del resto: Kali Linux, originado por la empresa Offensive Security Ltd. Es una distribución de GNU/Linux basada en Debian diseñada para realizar análisis forense, escribió Hakim Ha en su blog hoy. Como producto, Kali tiene más de 500 programas para auditoría de sistemas y hacking, incluyendo herramientas para hacking ético o no ético.

4.2.3. Preparación para Instalar Kali Linux en VirtualBox

Crear una máquina virtual en VirtualBox antes de instalar Kali Linux. Esto proceso previo es arrancando una imagen ISO del sistema operativo y configurando el hardware virtual, como la RAM, el número de núcleos de CPU y los discos duros virtuales. Todas estas cosas son importantes para aprovechar al máximo y tener una experiencia agradable. A continuación, se numeran los pasos para el entorno para la instalación de Kali Linux.

Paso 1: Descarga de la Imagen ISO de Kali Linux

Para la instalación de Kali Linux, lo primero es descargar los archivos ISO. Kali Linux ofrece imágenes ISO o de instalación para varias arquitecturas (32 bits, 64 bits, ARM64, ARMHF) con múltiples opciones de gestores de ventanas, según el escritorio que prefieras.

Para una guía paso a paso sobre la instalación, se debe consultar la guía de instalación en el sitio oficial de Kali Linux. Desde allí se selecciona la arquitectura de la máquina anfitriona y se da clic en el botón de descarga en la parte inferior izquierda de la tarjeta de instalación. Después de descargar el archivo ISO, se procede a crear la máquina virtual.

Figura 11. Instalación kali Linux. Elaborado por: Alex Aimacaña

Paso 2: Crear una Instancia de VirtualBox de Kali Linux

Una vez descargado la imagen ISO, se procede a crear la nueva máquina virtual dentro de VirtualBox que tendrá Kali Linux. Se inicia el Administrador de VirtualBox y luego haz clic en "Nuevo" para comenzar la configuración. Luego, se asigna un nombra a la máquina virtual y se procede a buscar el archivo ISO descargado.

A continuación, se asigna la memoria RAM y núcleos de CPU. Para asegurar el mejor rendimiento, en este caso, 2 GB de RAM y al menos 1 CPU. Una vez configurados los recursos, se selecciona la máquina y se genera un disco duro virtual. Finalmente, se ha creado una nueva máquina virtual y está en la lista del Administrador de VirtualBox.

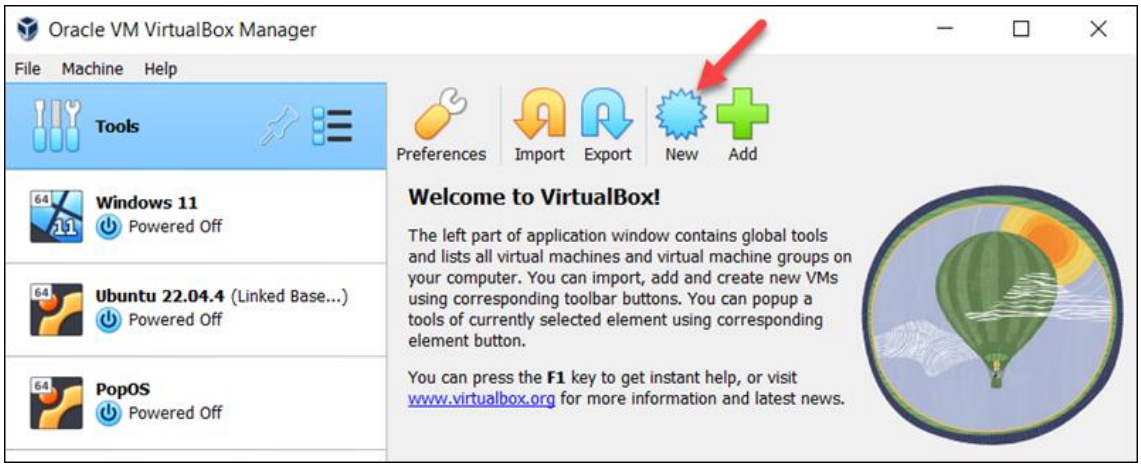


Figura 12. Instalación Kali Linux. Elaborado por: Alex Aimacaña

Se específica para la máquina virtual y suministre la ruta a la imagen ISO. Se da clic en siguiente.

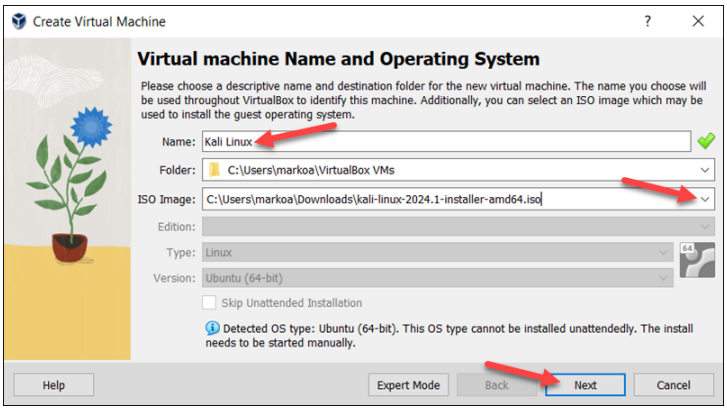


Figura 13. Instalación Kali Linux. Elaborado por: Alex Aimacaña

Selección de la memoria y los cpu’s virtuales

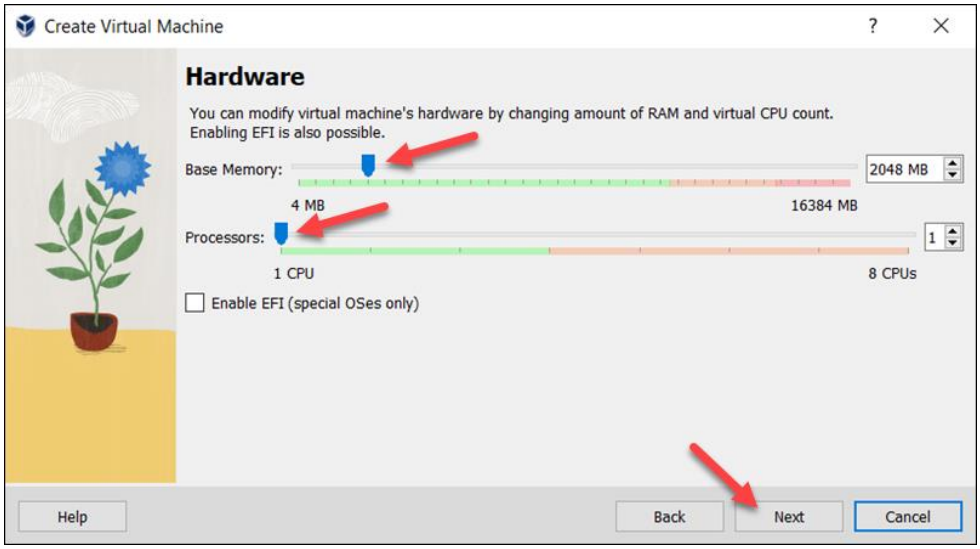


Figura 14. Instalación kali Linux. Elaborado por: Alex Aimacaña

Creación de los discos necesarios para operar el sistema operativo este dependiendo de la cantidad de archivos que se valla a utilizar

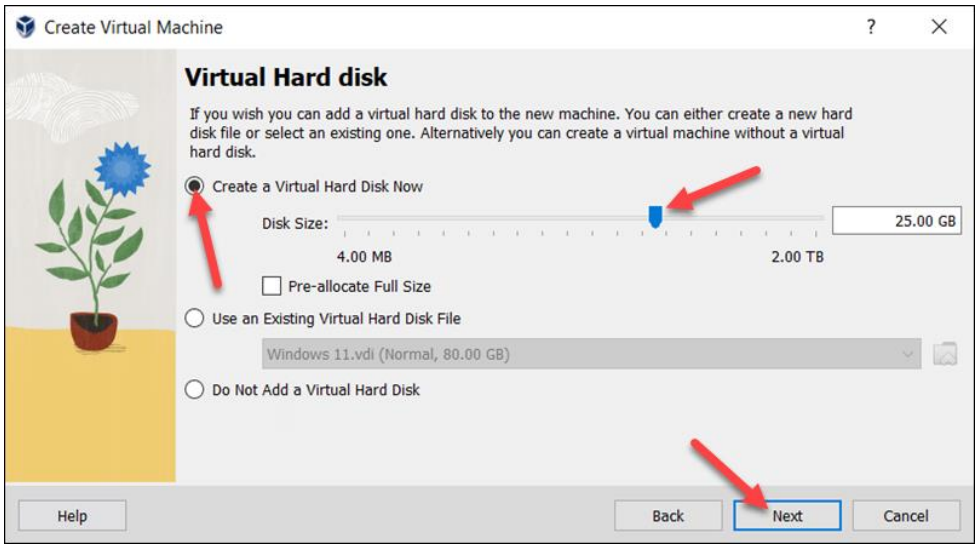


Figura 15. Instalación kali Linux. Elaborado por: Alex Aimacaña

Se revisa la instalación en el informe final de instalación de la máquina virtual en la página de resumen. Se selecciona finalizar para crear la máquina virtual.

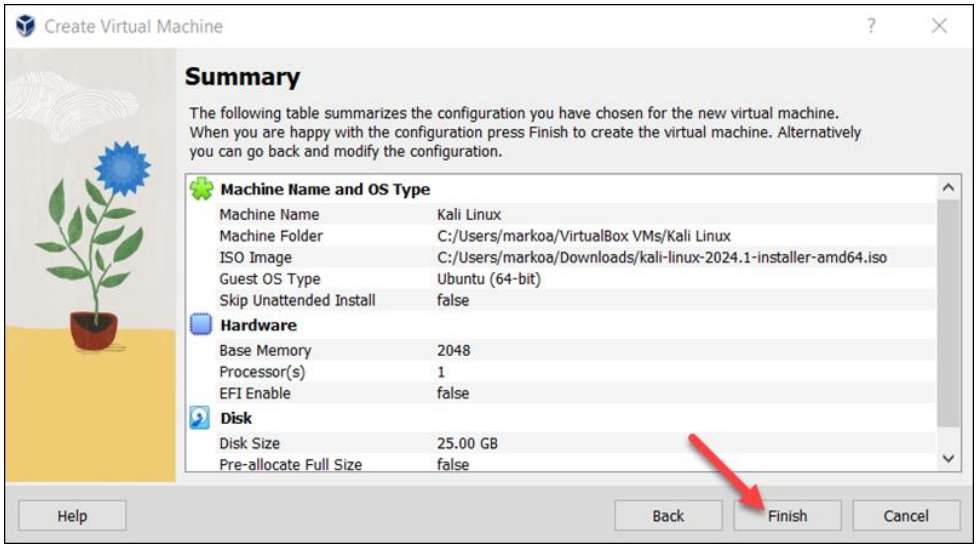


Figura 16. Instalación kali Linux. Elaborado por: Alex Aimacaña

Paso 3: Configurar los Ajustes de la Máquina Virtual e Iniciar

Se elige la máquina virtual Kali Linux y se da clic en el botón Configuración. En la sección general, de dirige a la pestaña en Avanzado y en la opción Bidireccional para "Portapapeles Compartido" y "Arrastrar y Soltar."

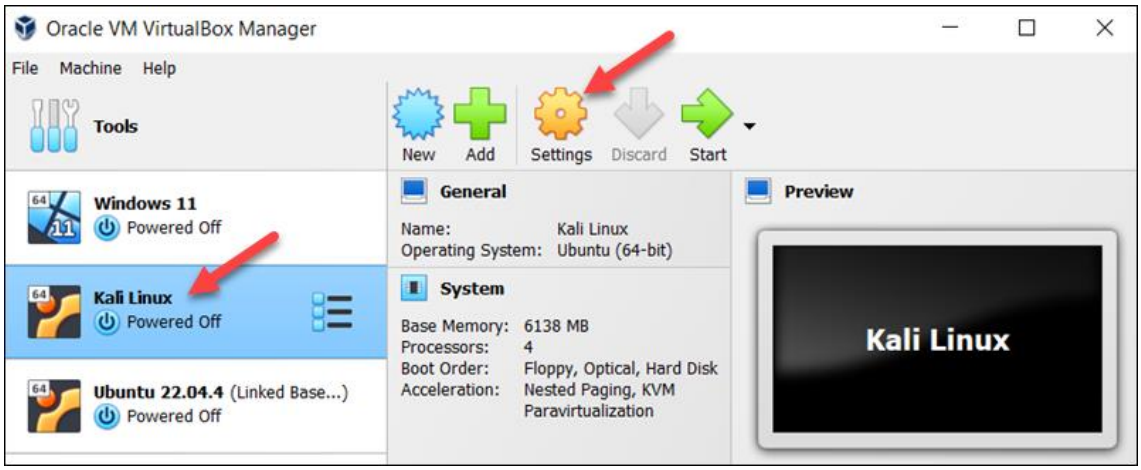


Figura 17. Instalación kali Linux. Elaborado por: Alex Aimacaña

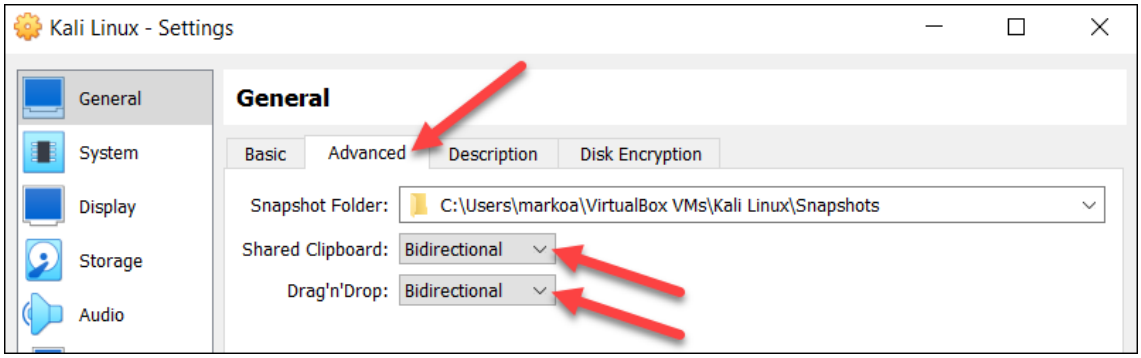


Figura 18. Instalación kali Linux. Elaborado por: Alex Aimacaña

Este proceso permite mover archivos entre las máquinas host e invitada. Luego, clic en Red en la barra lateral y, en el campo "Conectado a", selecciona "Adaptador Puente" para acceder a la red. Luego clic en OK para guardar la configuración y luego en Iniciar el proceso de instalación de Kali Linux.

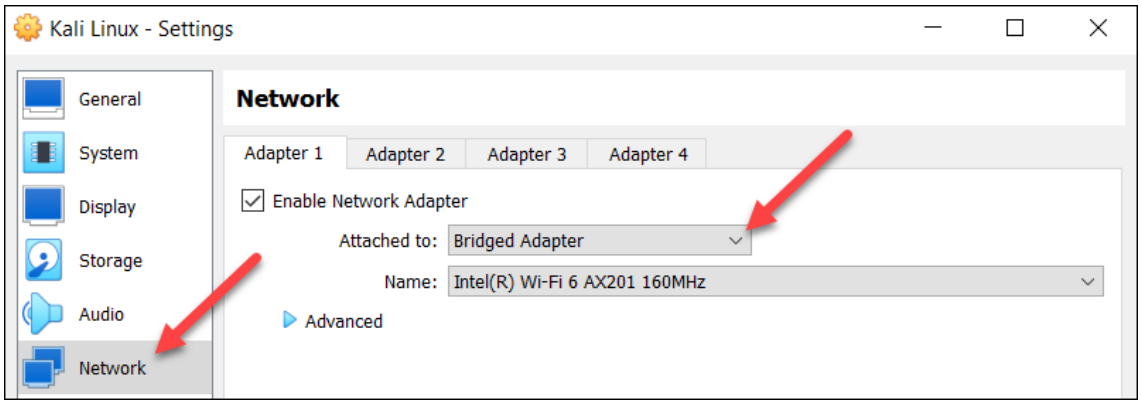


Figura 19. Instalación kali Linux. Elaborado por: Alex Aimacaña

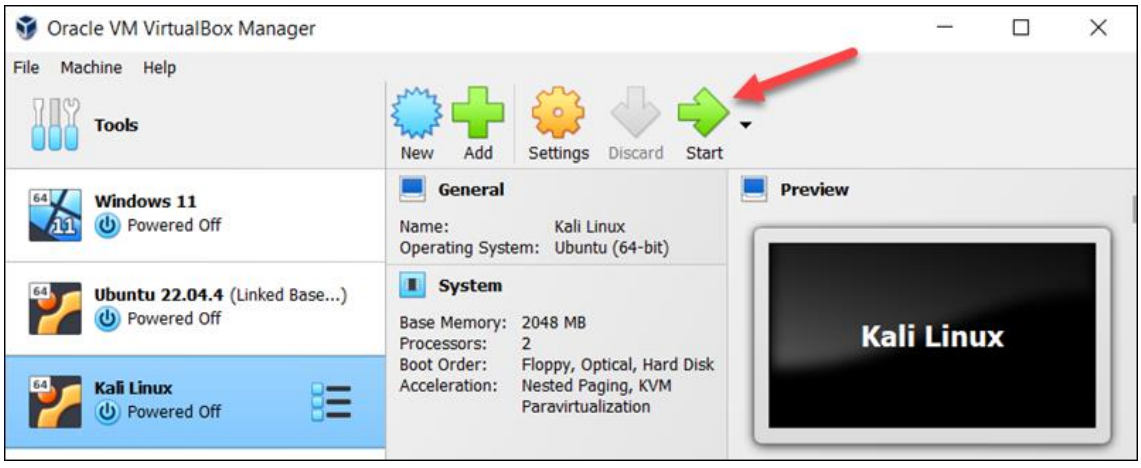


Figura 20. Instalación kali Linux. Elaborado por: Alex Aimacaña

4.2.4. Instalar Kali Linux en VirtualBox

Cuando la máquina virtual se activa, se muestra el menú de instalación de Kali Linux. Desde aquí, se elige en instalación gráfica o la instalación visual, que se percibe como más fácil y amigable. Selecciona el idioma predeterminado del sistema, además del idioma disponible durante la instalación.

Luego, procede a elegir tu país para establecer la configuración regional en el sistema. La disposición del teclado estará disponible, para habilitar la escritura.

Figura 21. Instalación kali Linux. Elaborado por: Alex Aimacaña

Paso 1: Realizar la Configuración Inicial

Para encender la VM y proceder con la instalación de Kali Linux. Se elige la máquina virtual Kali Linux y se da clic en el botón "Configuración". En la sección general, se dirige a la pestaña "Avanzado" y selecciona la opción "Bidireccional" para "Portapapeles Compartido" y "Arrastrar y Soltar".

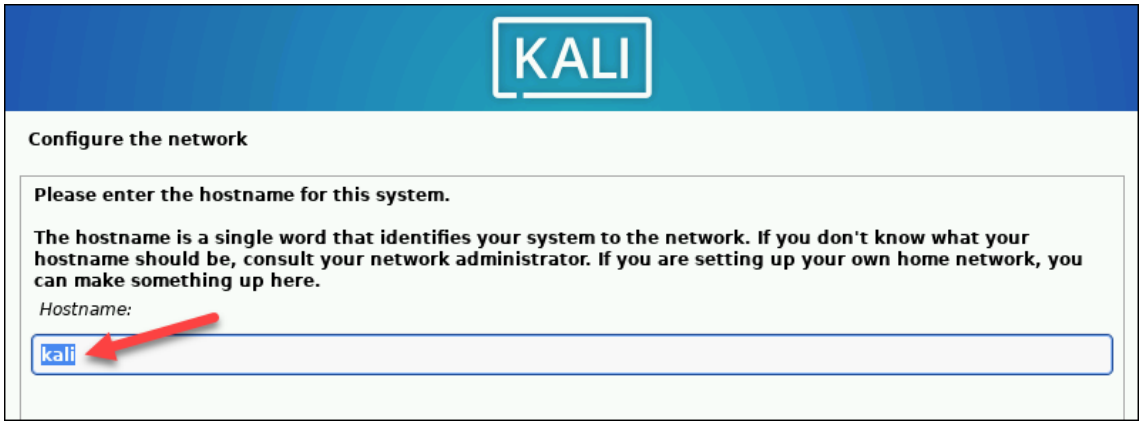


Figura 22. Instalación kali Linux. Elaborado por: Alex Aimacaña

Figura 23. Instalación kali Linux. Elaborado por: Alex Aimacaña

Se asegura en utilizar una contraseña segura para la cuenta. Y por último, se elige la zona horaria correcta de la lista para que el sistema pueda acceder a los registros de tiempo y eventos.

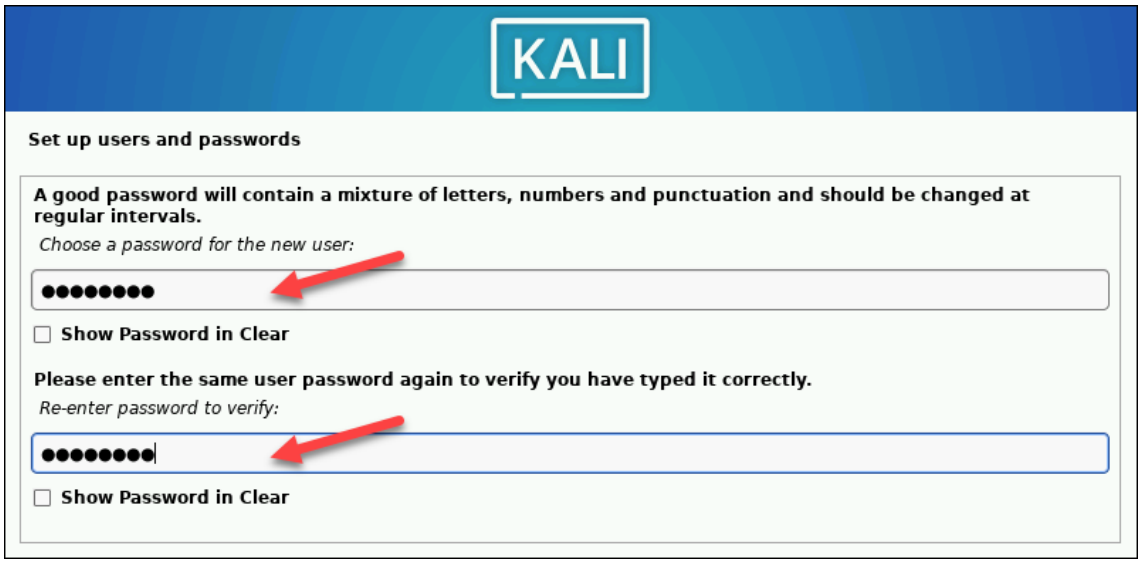


Figura 24. Instalación kali Linux. Elaborado por: Alex Aimacaña

Paso 2: Crear Particiones del Disco Duro

Posteriormente, con la instalación se creará una partición de arranque en el disco duro virtual. En este caso en la opción predeterminada: "Guiado: usar todo el disco".

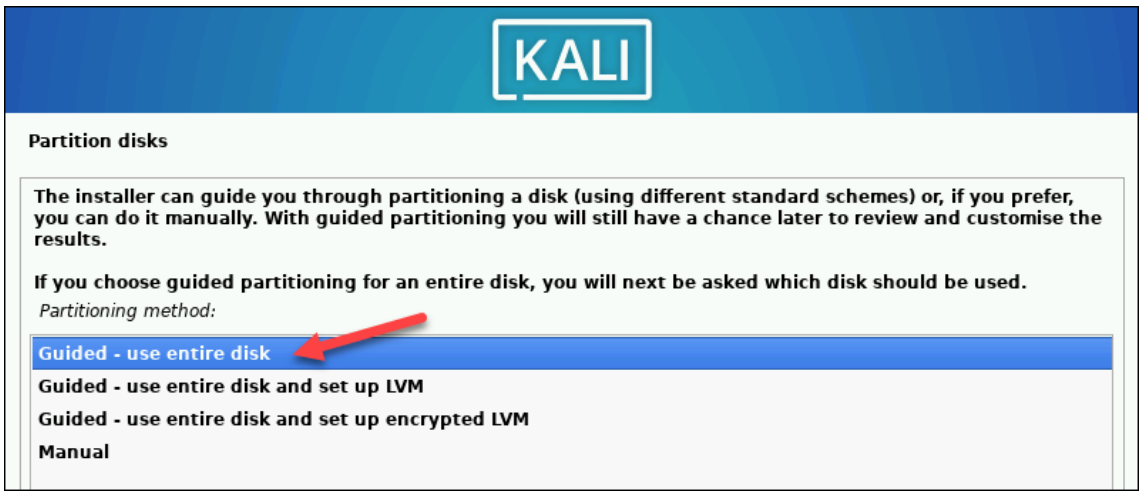


Figura 25. Instalación kali Linux. Elaborado por: Alex Aimacaña

A continuación, se elige el disco en el que se crea la partición, que es el único disco disponible al momento de configurar de la MV. Luego, se selecciona un esquema de particiones el predeterminado es “Todos los archivos en una partición", que estará bien para la mayoría de los usuarios. El asistente se muestra la vista general de las particiones que han sido configuradas, asegurándonos que la configuración esté seleccionada en “Terminar el particionado y escribir cambios en el disco”. Se confirma dando clic en “Sí” en la pantalla siguiente y el asistente comenzará a instalar Kali Linux en tu máquina virtual.

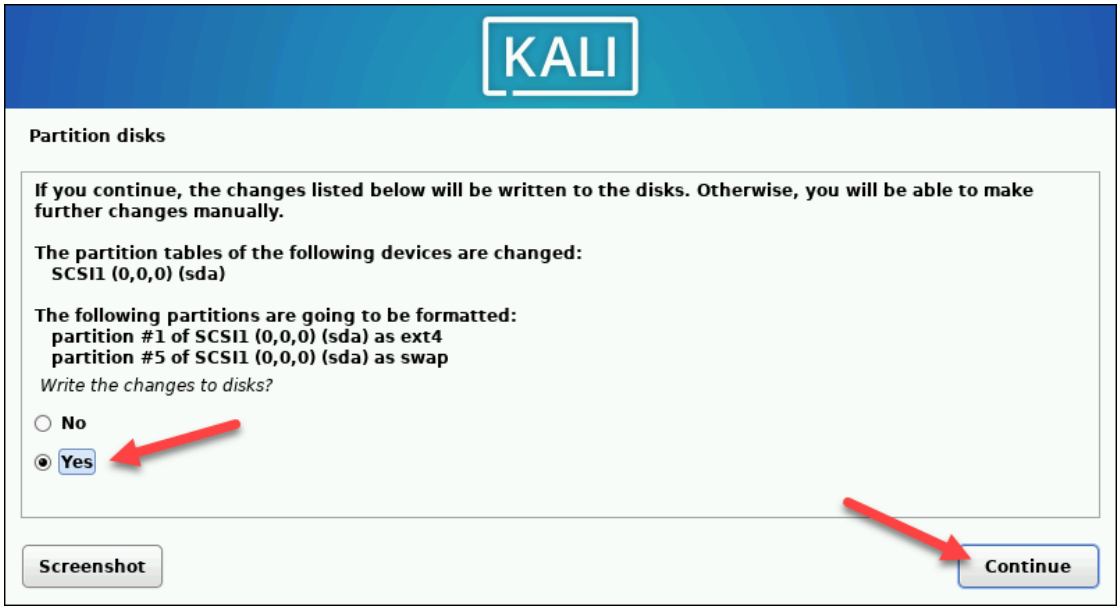


Figura 26. Instalación kali Linux. Elaborado por: Alex Aimacaña

Paso 3: Personaliza la Instalación de Kali Linux

Una vez que el núcleo del sistema instalado, Kali Linux permite ajustar cómo deseas que sea el entorno ejecutando lo siguiente. En este punto, permite seleccionar qué componentes adicionales se desea instalar. En este caso se está utilizando un proxy HTTP, y estará listo el sistema para arrancar.

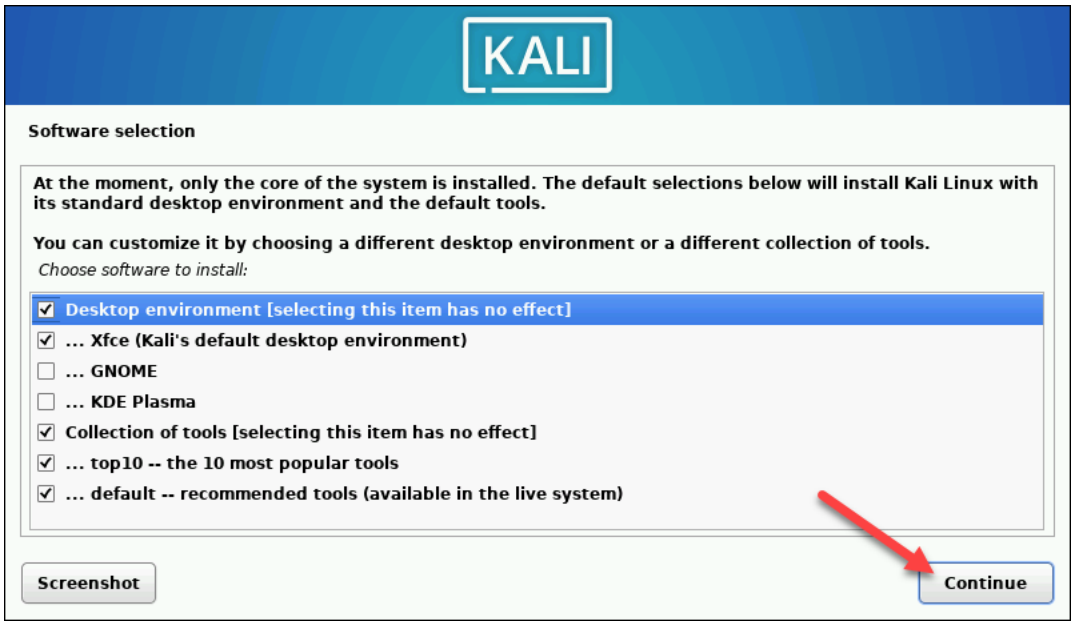


Figura 27. Instalación kali Linux. Elaborado por: Alex Aimacaña

Luego, se da clic en “Continuar” para reiniciar tu MV—cuando arranque, se muestra la pantalla de inicio de sesión de Kali:

4.2.5. Instalación de Raspbian

Descargar Software:

Raspbian Stretch: Descarga la imagen ISO desde el enlace correspondiente.

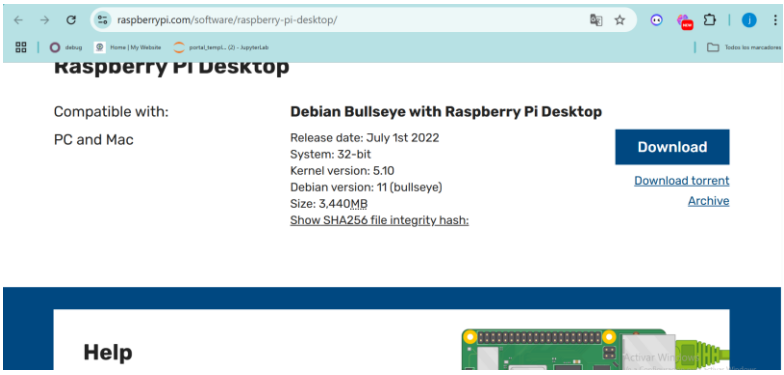


Figura 28. Instalación Raspbian Stretch. Elaborado por: Alex Aimacaña

Crear una Máquina Virtual:

Se abre el Open VirtualBox, luego elige “Máquina -> Nueva” para comenzar a crear una nueva máquina virtual. Se selecciona el “Modo Experto” para acceder a más opciones de configuración. Se asigna un nombre, elige tipo “Linux” y versión “Debian 32 bits”. Asigna un mínimo de 512 MB de RAM y selecciona “Crear un disco duro virtual ahora”.

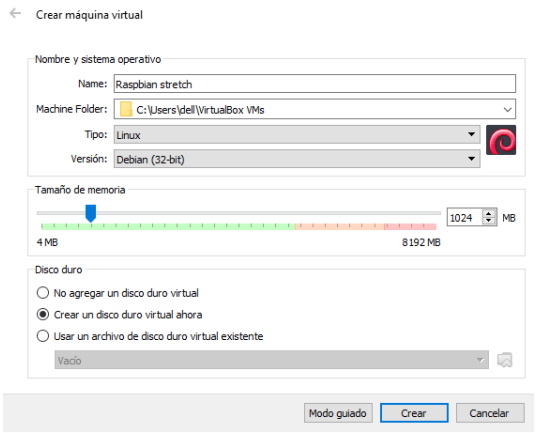


Figura 29. Instalación Raspbian Stretch. Elaborado por: Alex Aimacaña

Configurar la Máquina Virtual:

Para hacerlo, se especifica el tamaño del disco duro virtual (tamaño recomendado es 10-15 GB). Se navega a “Configuración” y modifica los ajustes en la pestaña “Avanzado” para activar el portapapeles bidireccional. Carga la imagen ISO de Raspbian (para instalarla) en “Almacenamiento”.

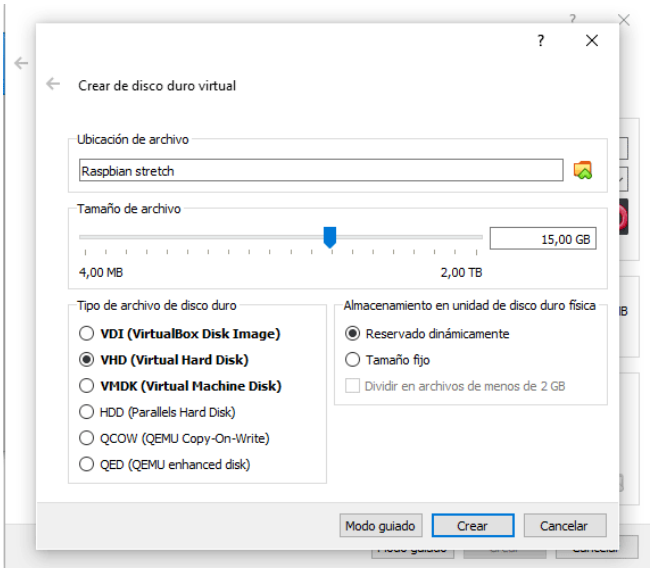


Figura 30. Instalación Raspbian Stretch. Elaborado por: Alex Aimacaña

Configuración de Red:

- En el apartado de “Red”, selecciona “Adaptador puente” para que la máquina virtual obtenga una dirección IP de tu router.
- Instalación de Raspbian:
- Se Inicia la máquina virtual y selecciona “Graphical Install”.
- Se elige el idioma y se selecciona “Guided – use entire disk” para usar todo el disco duro.
- Configura las particiones como prefieras y confirma los cambios.

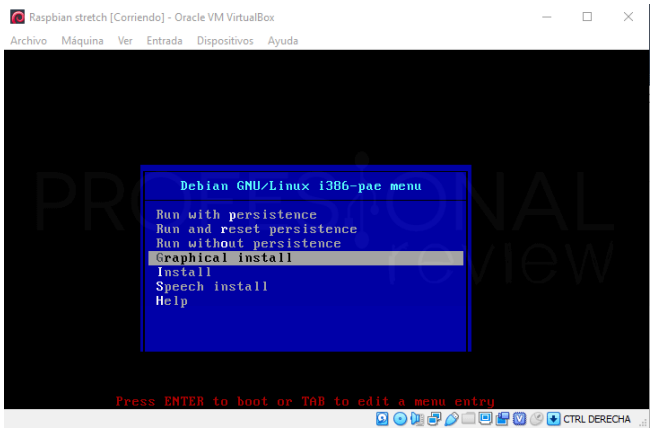


Figura 31. Instalación Raspbian Stretch. Elaborado por: Alex Aimacaña

Finalización:

Una vez que se complete la instalación, se reinicia la máquina virtual y se sigue el asistente para configurar el idioma y conexión a Internet.

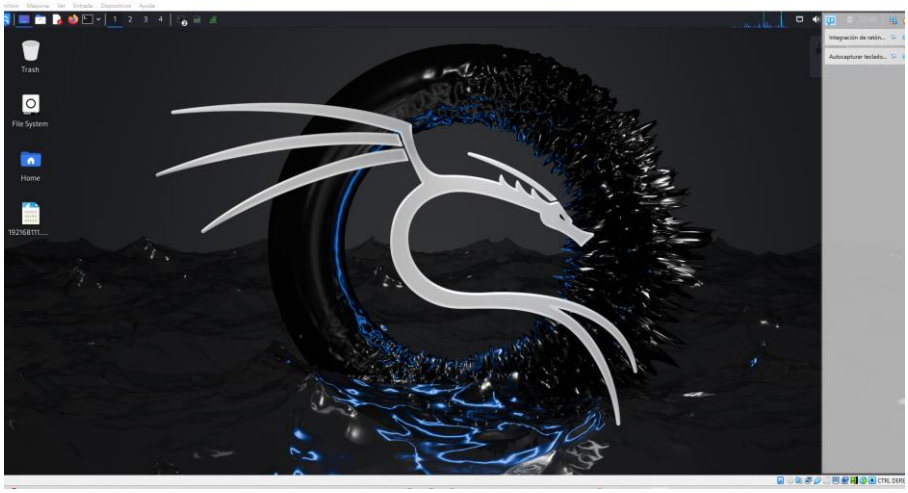


Figura 32. Interfax Raspbian Stretch. Elaborado por: Alex Aimacaña

4.3. Simulación del servidor o Rasberry de Prueba

4.3.1. Objetivo de la Simulación

El propósito de la simulación es controlar una cierta cantidad de producto a través de un ERP (Odoo). Esto se puede lograr mediante registros en otro módulo, que es

un módulo personalizado llamado contador, donde se guarda la información contable.

```python
import xmlrpc.client
import random
import time
from datetime import datetime

# Configuración de la conexión
url = 'https://xxx-testing.odoo.com'  # URL del servidor Odoo
db = 'xxx-iot-testing-produccion-18948545'  # nombre de la base de datos
username = 'IOT001'  # nombre de usuario
password = 'xxxxxx'  # contraseña

# Conectar al servidor Odoo
common = xmlrpc.client.ServerProxy(f'{url}/xmlrpc/2/common')
uid = common.authenticate(db, username, password, {})

if uid:
    print(f'Conexión exitosa. UID: {uid}')
else:
    print('Error de autenticación.')
    exit()

# Conectar a los modelos
models = xmlrpc.client.ServerProxy(f'{url}/xmlrpc/2/object')

while True:
    # Preparar los datos para insertar en product.counter
    product_data = {
        'product_id': 1,  # ID del producto estático
        'timestamp': datetime.now().strftime('%Y-%m-%d %H:%M:%S'),  # Timestamp actual
        'quantity': random.randint(1, 2)  # Cantidad aleatoria entre 1 y 100
    }
    # Crear el registro en product.counter
    try:
        counter_id = models.execute_kw(db, uid, password, 'product.counter', 'create', [product_data])
        print(f'Registro creado con ID: {counter_id}')
    except xmlrpc.client.Fault as e:
        print(f'Error al crear el registro: {e}')

    # Esperar un tiempo aleatorio entre 1 y 10 segundos
    wait_time = random.randint(1, 2)
    print(f'Esperando {wait_time} segundos antes de crear el siguiente registro...')
    time.sleep(wait_time)

    # Esperar un tiempo fijo de 10 segundos antes de la próxima iteración
    time.sleep(5)
```

Figura 33. Código Python Elaborado por: Alex Aimacaña

El siguiente código simula una entrada de producto en Odoo a través de XML-RPC. Primero, se conecta al servidor de Odoo y autoriza al usuario, utilizando ciertas credenciales. Si la autenticación es correcta, el script entra en un bucle interminable en el que produce datos aleatorios para un cierto producto. En cada pasada, generamos un ítem en el modelo product.counter con el ID de producto fijo y la marca de tiempo actual, con un valor de cantidad aleatorio de 1 a 2. Se incluye manejo básico de errores para la inserción de datos. También agrega pausas aleatorias de 1 a 2 segundos con una

espera estática de 5 segundos hasta el siguiente conteo. Este es un escenario contable de imitación en un ambiente de producción, en el cual se puede probar la integración con ERP.

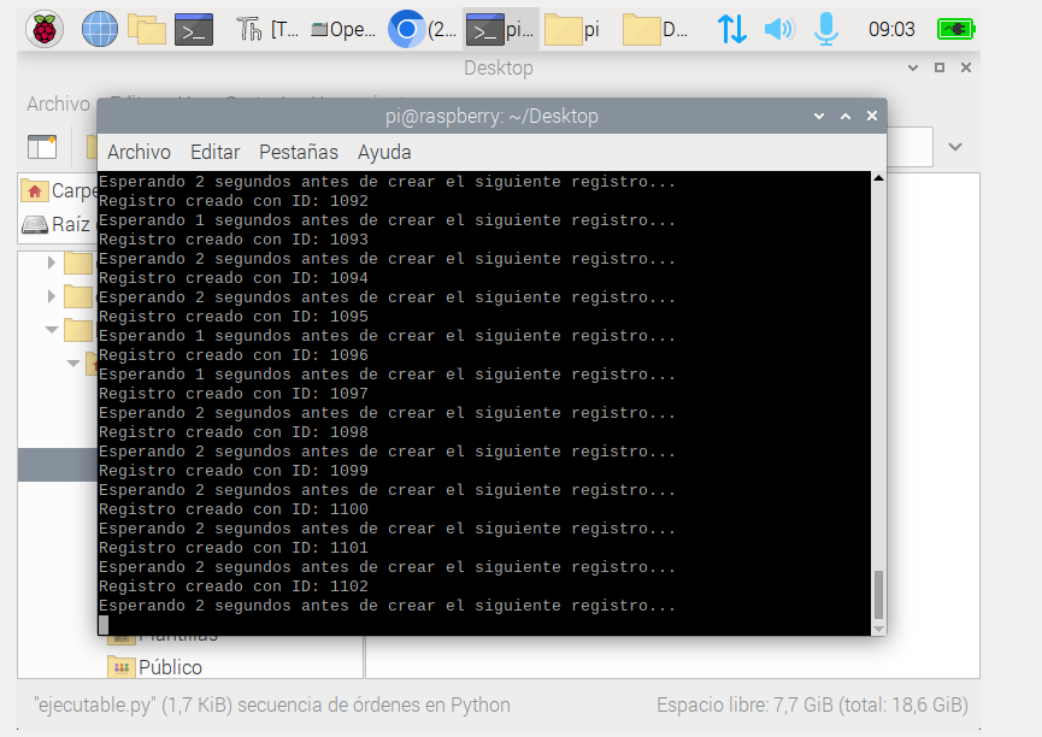


Figura 34. Raspbian Script Ejecutable. Elaborado por: Alex Aimacaña

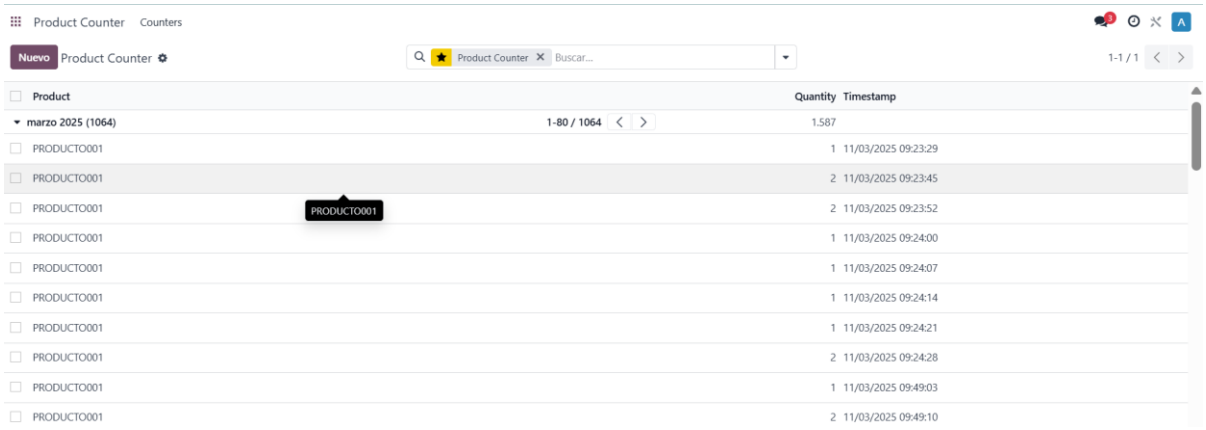


Figura 35. Raspbian Odoo recepción de datos. Elaborado por: Alex Aimacaña

4.4. Pruebas de Penetración

4.4.1. Nmap

Se realizo un escaneo de puertos en la máquina Raspbian desde Kali Linux para identificar los puertos abiertos y los servicios que están corriendo.

```
nmap -sS -sV -O <IP_RASPIAN>
```

-sS: Realiza un escaneo SYN.

-sV: Detecta versiones de servicios.

-O: Detecta el sistema operativo.

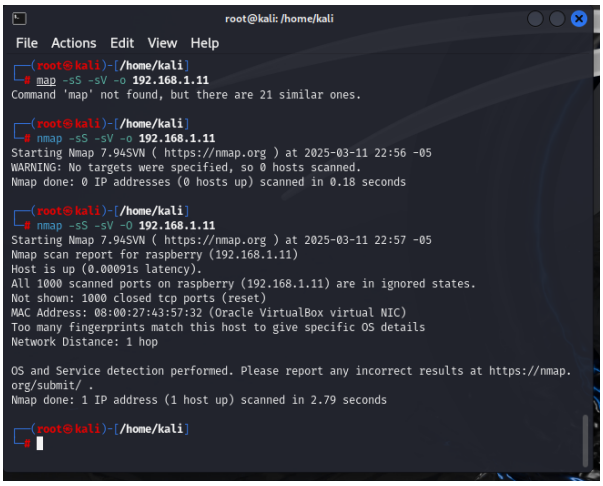


Figura 36. Ejecución comando nmap. Elaborado por: Alex Aimacaña

De acuerdo, al análisis de penetración de nmap se explica con más detalle la información extraída de la imagen:

Ejecución de Nmap:

- Se inició la ejecución de Nmap (Network Mapper) versión 7.945WW en la fecha 2025-03-11 a las 22:57
- El escaneo se realizó en el host raspberry con la dirección IP 190.108.1.11.
- Nmap escaneó todos los 1000 puertos del host raspberry, y encontró que todos los puertos estaban en estado 'Sphered'.

- Se encontraron 1000 puertos TCP cerrados (con estado 'reset').
- La dirección MAC del host es 08:00:27:43:57:32, que corresponde a una máquina virtual de Oracle VirtualBox.
- Nmap no pudo determinar detalles específicos del sistema operativo debido a la gran cantidad de fingerprints que coinciden con el host.
- El escaneo de Nmap se completó en 2.79 segundos.

4.4.2. METASPLOIT

4.4.2.1. MÓDULO AUXILIARY DE METASPLOIT

Se ejecuto el módulo `auxiliary/scanner/http/http_version` de Metasploit. Este módulo se utilizó para escanear el servidor web de un host y obtener información sobre la versión del servidor web.

Opciones del Módulo:

- Proxies: No se ha establecido ningún proxy.
- RHOSTS: La dirección IP del host objetivo es 192.168.1.11.
- RPORT: El puerto objetivo es el 80 (puerto HTTP estándar).
- SSL: El valor de SSL está establecido en `false`, lo que significa que no se utilizará SSL/TLS para las conexiones salientes.
- THREADS: Se ha establecido un valor de 1 para el número de hilos concurrentes (máximo uno por host).
- VHOST: No se ha establecido un nombre de host virtual HTTP.

Resultados del Escaneo:

- Se ha escaneado 1 host (100% completo).
- La ejecución del módulo auxiliar se ha completado.

4.4.3. Análisis de Red Wireshark

4.4.3.1. Captura de tráfico de red

La Figura muestra una captura de tráfico de red realizada con la herramienta Wireshark. La captura se está realizando en la interfaz "etho" una interfaz de red Ethernet.

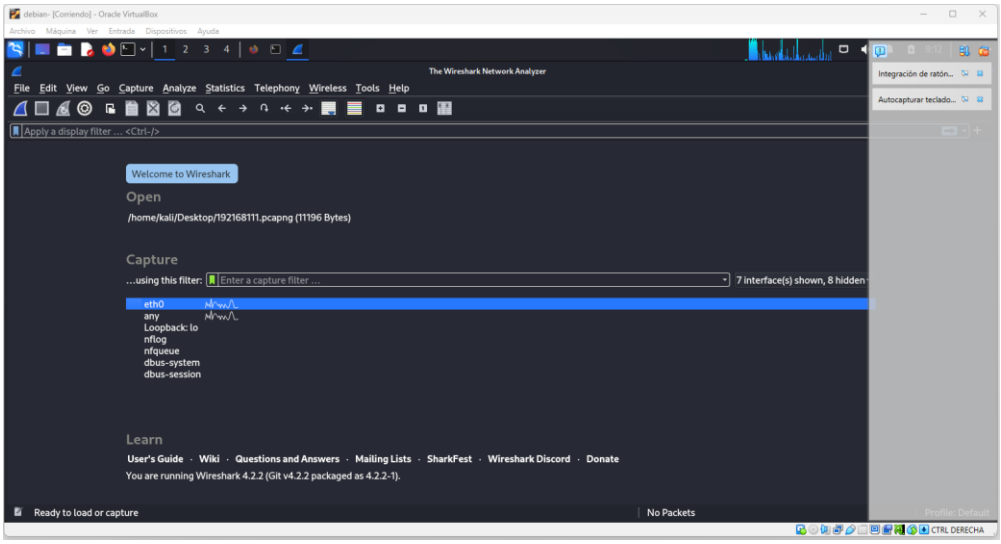


Figura 37. Captura de Trafico de re. Elaborado por: Alex Aimacaña

4.4.3.2. Direcciones IP y protocolo:

Direcciones IP y Protocolo: La IP de origen es 192.168.1.11 y la IP de destino es 239.255.255.250 (que es una dirección IP de multidifusión). Usamos SSDP (Protocolo de Descubrimiento de Servicios), que se utiliza para la publicidad de servicios en la red doméstica.

Paquetes capturados: Se reciben cuatro paquetes SSDP "M-SEARCH"; estos son búsquedas de servicios en la red. Estos paquetes tienen un tamaño de 210 bytes y se envían a la dirección de multidifusión de 239.255.255.250 en el puerto UDP.

4.4.3.3. Paquetes capturados:

Se muestran 4 paquetes SSDP de tipo "M-SEARCH", que son solicitudes de búsqueda de servicios en la red. Estos paquetes tienen una longitud de 210 bytes y se envían a la dirección de multidifusión `239.255.255.250` en el puerto UDP 1900.

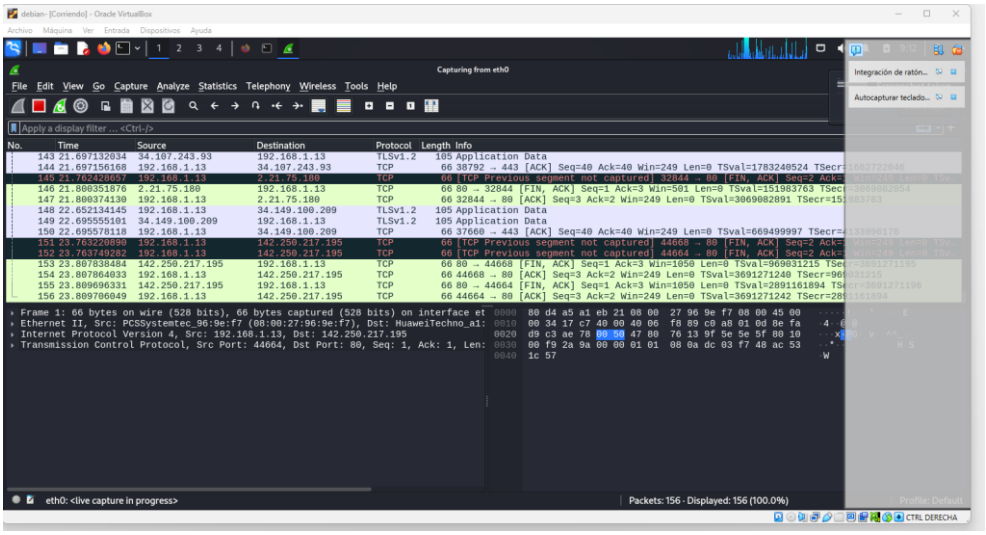


Figura 38. Captura de Trafico de red. Elaborado por: Alex Aimacaña

4.4.3.4. Información de la trama Ethernet:

El origen y destino de la trama Ethernet son `PCSSystemtec_43:57:32` e `IPV4mcast_7f:ff`, respectivamente. Esto muestra que el tráfico ha sido interceptado de una comunicación de red local. Esta captura de Wireshark es como un escaneo de red generado por un dispositivo IP 192.168.1.11 usando el protocolo SSDP para encontrar otros servicios dentro de su red local. Este tipo de acceso se puede encontrar en redes pequeñas con instalaciones de descubrimiento de servicios.

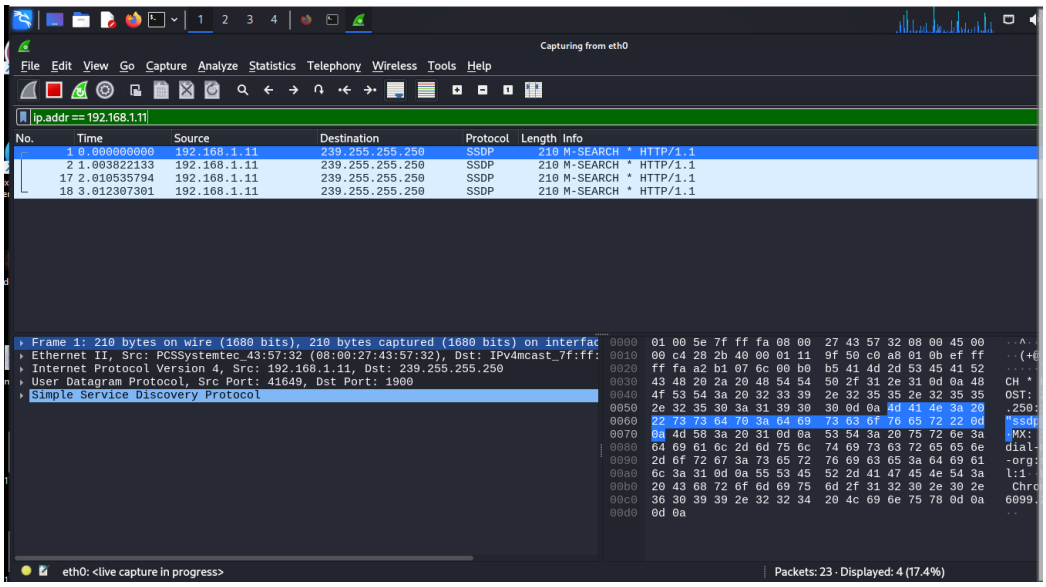


Figura 39. Captura de Trafico de red. Elaborado por: Alex Aimacaña

5. Resultados y discusión

Resultados y Discusión En esta sección examinada, enfatizamos la importancia de un análisis efectivo de los resultados, por un lado, y por otro, constatamos claramente la necesidad de considerar la efectividad de los mecanismos de seguridad desde todos los posibles puntos de vista, tales como: protección contra ataques, protección de datos y las limitaciones de rendimiento. En segundo lugar, hay un enfoque en analizar fortalezas, debilidades y vulnerabilidades para que se puedan hacer recomendaciones más sólidas para aumentar el nivel de seguridad del sistema de comunicación en el sentido de la Industria 4.0:

5.1. Resistencia a ataques comunes

La fase de prueba del protocolo de comunicación seleccionado en la fase anterior incluyó múltiples pruebas de penetración en las pilas de comunicación para probar su resistencia a los ataques más típicos en el espacio de la Industria 4.0.

5.1.1. Ataques de fuerza bruta y diccionario contra los mecanismos de autenticación:

Los modelos de adversarios se modelaron con ataques de fuerza bruta y diccionario sobre el mecanismo de autenticación de los protocolos probados. Descubrieron que la autenticación basada en contraseñas es segura contra ataques en los que la penetración del sistema no es suficiente. En contraste, los protocolos que utilizan autenticación basada en certificados digitales o tokens de seguridad son mucho más resistentes a dichos ataques, elevando considerablemente el nivel en términos de

acceso no autorizado.

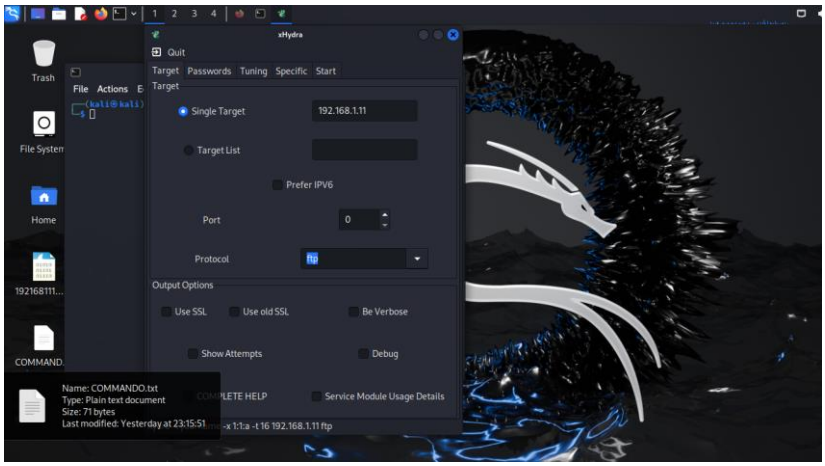


Figura 40. Captura de Trafico de red. Elaborado por: Alex Aimacaña

5.1.2. Ataques de interceptación y modificación de tráfico:

Captura de tráfico; este tráfico se observó cuando los dispositivos en el entorno de prueba estaban comunicándose. El análisis también se proporcionó en herramientas como Wireshark. Los hallazgos indicaron que los protocolos en tiempo real que no operaban con encriptación de extremo a extremo eran susceptibles de interceptación, y el tráfico podía ser falsificado para filtrar información e integridad. El contrapunto es que los protocolos que dependían en gran medida de una fuerte encriptación, como TLS y DTLS, eran realmente buenos para proteger los datos en tránsito de ser manipulados por atacantes.

5.1.3. Ataques de denegación de servicio (DoS):

Se realizaron pruebas exhaustivas para probar diferentes protocolos contra ataques a nivel de aplicación y de red. Estos son ataques maliciosos que impiden el funcionamiento normal de un servicio y pueden llevar a diversos niveles de degradación del rendimiento o incluso a la detención total del servicio.

Los resultados de tales pruebas mostraron que algunos de los protocolos son extremadamente sensibles a estos ataques. La disminución del rendimiento bajo una prueba de sobrecarga fue dramática, lo que indica que es necesaria una mejora en la seguridad de estos sistemas.

Tales vulnerabilidades son críticas en el desarrollo de contramedidas para evitar que estos incidentes se repitan.

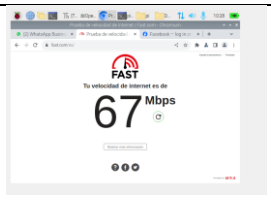
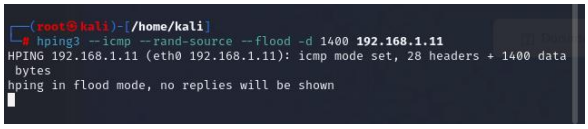
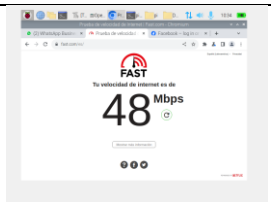
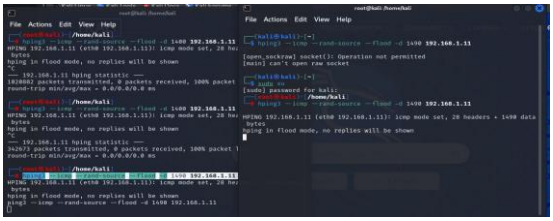
N°	Imagen	Velocidad de Conexión	Ataque
1		67 Mbps	No
2		2.4 Mbps	Si 
3		48 Mbps	No
4		2.0 Mbps	Si 

Tabla 2. Ataques de denegación de servicio (DoS). Elaborado por: Alex Aimacaña

5.2. Informe sobre Ataques de Denegación de Servicio (DoS)

Los resultados de la prueba se muestran en la tabla de resultados con estadísticas de conexión. Se mantuvieron varias tasas de conexión en diversos momentos, dependiendo de la existencia o no de ataques. En escenarios sin ataque, los anchos de banda de conexión estaban en su máximo, mostrando que los protocolos estaban operando correctamente. Sin embargo, en situaciones en las que sí ocurrieron ataques, hubo una reducción significativa en la velocidad de conexión.

Por ejemplo, una conexión que se había comprobado que era de 67 Mbps cayó a unos míseros 2.4 Mbps en medio de un ataque.

Estos datos resaltan la necesidad de que los sistemas estén protegidos contra ataques DDoS y la importancia de las protecciones para la integridad y disponibilidad del sistema.

5.3. Propuestas de Mejora y Recomendaciones para Fortalecer la Seguridad de los Sistemas de Comunicación en la Industria 4.0

5.3.1. Adopción de Protocolos de Seguridad Avanzados

Aunque los protocolos de red de IETF no son inmunes a los ataques de intermediarios, sería una muy mala idea diseñar sistemas de iluminación con algo menos que las mejores prácticas de seguridad. Estos protocolos asegurarán la confidencialidad y la integridad de los mensajes intercambiados, por lo que sería difícil para un atacante interceptar y cambiar los valores que se reciben.

5.3.2. Capacitación Continua del Personal

Todos los empleados, especialmente aquellos que tienen interacción directa con los sistemas de comunicación, deben recibir cursos de capacitación regular sobre ciberseguridad. Asegurar una buena educación en seguridad y mantener la conciencia sobre posibles amenazas ayudará a construir un entorno consciente de la seguridad dentro de la compañía.

5.3.3. Evaluaciones de Seguridad Regulares

Las revisiones de seguridad y las pruebas de penetración regulares también son aconsejables para identificar y corregir debilidades en los sistemas de

comunicación. Estas evaluaciones deben ser un elemento en un proceso continuo de mejora de la calidad, uno que ayude a una organización a evolucionar en respuesta a nuevas amenazas y tecnologías emergentes.

5.3.4. Desarrollo de un Plan de Respuesta a Incidentes

Es importante tener un plan de respuesta a incidentes que delinee los pasos que se tomarán en caso de una violación de seguridad. Eso significa definir roles y responsabilidades, tanto dentro como fuera de la empresa. Un buen plan ayudará a las organizaciones y empresas a responder adecuadamente y a mitigar el impacto de un incidente.

5.3.5. Monitoreo y Detección de Amenazas

Implementar la Supervisión Continúa Hervida por IA: introduce la inteligencia artificial y el aprendizaje automático para rastrear actividades inusuales en la red. Las herramientas para ayudar en la detección de amenazas de esta manera pueden usarse para monitorear en tiempo real las amenazas y, por lo tanto, responder rápidamente a un posible evento.

5.3.6. Colaboración con Expertos en Ciberseguridad

También te recomendamos consultar (y apoyarte en) expertos en ciberseguridad y asesores externos para evaluar tu configuración específica y hacer recomendaciones similares que aborden tu infraestructura particular. Las perspectivas externas pueden ayudar a integrar mejores enfoques y desarrollarlos.

5.3.7. Actualización Regular de Software y Sistemas

Debes asegurarte de que tus sistemas y aplicaciones estén al día con las últimas actualizaciones para ayudar a prevenir la explotación de vulnerabilidades conocidas. Desarrolla una metodología para instalar regularmente parches y actualizaciones de seguridad para ayudar a proteger contra vulnerabilidades de amenazas existentes en todos los dispositivos. La adopción de las propuestas no solo llevará a un sistema de comunicación más seguro para la Industria 4.0, sino que también ayudará a crear un espacio más seguro y fuerte para combatir el ciberterrorismo.

6. Conclusiones

1. El estudio de protocolos de comunicación para la Industria 4.0 ha revelado diferentes protocolos con distintas propiedades de seguridad. Se ha observado que, si bien protocolos como MQTT y OPC UA pueden ofrecer fuertes argumentos hacia la interoperabilidad y la eficiencia, también están asociados con amenazas inherentes si la seguridad no se aplica adecuadamente. Esto resalta la importancia de la evaluación y desarrollo continuo de protocolos para asegurar que se mantengan seguros en un entorno industrial cada vez más diverso.
2. Las pruebas de penetración han sido clave para revelar fallas de seguridad evidentes en los modelos de comunicación de la Industria 4.0. La realidad es que, con la ayuda de ejercicios de ataque, muchos sistemas no cuentan con las defensas mínimas de seguridad necesarias para prevenir un ataque. Estos resultados subrayan el valor de las evaluaciones continuas de riesgos de seguridad para ayudar a las organizaciones a anticipar amenazas y mejorar sus sistemas antes de que ocurran eventos de seguridad.
3. La evaluación de los mecanismos de autenticación y cifrado ha demostrado que, si bien existen tecnologías robustas que pueden proteger la integridad y confidencialidad de los datos, su implementación no siempre es adecuada. Protocolos que utilizan autenticación multifactor y cifrado avanzado han mostrado una mayor resistencia a ataques, mientras que aquellos que dependen de métodos más simples son vulnerables a compromisos. Esto resalta la necesidad de adoptar enfoques más rigurosos en la implementación de medidas de seguridad para proteger la información crítica en la Industria 4.0.
4. Las recomendaciones propuestas para fortalecer la seguridad de los sistemas de comunicación en la Industria 4.0 incluyen la adopción de estándares de seguridad más estrictos y la implementación de protocolos de seguridad más avanzados. Además, se sugiere la capacitación continua del personal en ciberseguridad y la creación de una cultura organizacional que priorice la

seguridad. Estas acciones no solo ayudarán a mitigar los riesgos asociados con las vulnerabilidades actuales, sino que también prepararán a las organizaciones para enfrentar futuros desafíos en un entorno industrial cada vez más digitalizado y conectado.

7. Referencias

Aristizabal Alzate, S., Moreno González, N., Patiño Santisteban, N., Ruano Cadena, M., & Cárdenas Ramos, A. (2023). *Integración del proceso de manufactura del CP Factory con procesos tácticos y operativos de la red de valor a través de un BPMS.* Bogota: Pontificia Universidad Javeriana.

Acosta Gallo, E. D. (2024). *SEGURIDAD EN EL INTERNET DE LAS COSAS INDUSTRIAL IOT EN LA INDUSTRIA 4.0.* Cuenca: Univerdidad Politecnica Salesiana.

Albuja Loachamin, L. F., Alvear Loor, J. G., & Sarango Romero, V. J. (2023). *Technological Inequalities in Education in Ecuador: Addressing the Educational Gap.* ESPE Universidad de las Fuerzas Armadas. Manabi: ESPE Universidad de las Fuerzas Armadas. Obtenido de https://doi.org/10.55813/gaea/ccri/v4/n2/239

Álvarez Roldán, M. (2020). *Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos.* Bogota: nstituto Tecnológico Metropolitano.

Alvarez Vásquez , O., & Arroyo Morocho, F. (2021). *Análisis de la Industria 4.0 como factor diferenciador del Sector Industrial del Ecuador.* Quito: Universidad Central del Ecuador.

Arredon Amaro, G. (2016). *Diseño de un modelo de gestion para la prevencion de fugas de información en dispocición moviles de empresas Mexicanas.* Ciudad de Mexico: Fugas de Datos: Las fugas de datos se refieren a la divulgación no intencionada de información sensible, que puede ocurrir debido a configuraciones inadecuadas o vulnerabilidades en la seguridad de un sistema. Estas situaciones permiten que individuos no.

Automatica e instrumentacion. (05 de 12 de 2024). Obtenido de https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/5020905/amenazas-ciberneticas-industria-reto-ciberseguridad-ot-1-parte

Barbara. (06 de 12 de 2024). *Barbara*. Obtenido de https://www.barbara.tech/es/blog/interoperability-in-industry-why-is-it-essential-to-digitalize-the-sector

BASANTES SUÑIGA, A. (2022). *ANÁLISIS COMPARATIVO SOBRE LA PLATAFORMA DE DESARROLLO NOCODE GLIDEAPP Y LA PLATAFORMA LOW-CODE OUTSYSTEMS EN LA CREACIÓN DE APLICACIONES WEB.* BABAHOYO: UNIVERSIDAD TÉCNICA DE BABAHOYO.

Becerra, L. (2020). *Tecnologías de la información y las Comunicaciones en la era de la cuarta revolución industrial: Tendencias Tecnológicas y desafíos en la educación en Ingeniería.* Pereira: Universidad Católica de Pereira.

Bravo Vera , H. (2022). *El desarrollo Low/No-code y el futuro de losdesarrolladores de software.* Guayaquil: Universidad Laica Eloy Alfaro de Manabí.

Brosnan, A. (2024). *EXPLORING THE NATURE OF RISK IN DIGITAL TRANSFORMATION: A PROBLEMATISATION PERSPECTIVE OF LOW-CODE/ NO-CODE PLATFORM RISK.* Cork: University College Cork.

CAICEDO PAREDES, J. (2022). *ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DEL PROTOCOLO DE RED DE CAPA DE TRANSPORTE DNS-OVER-QUIC (DOQ) EN*

LA UNIVERSIDAD TÉCNICA DE BABAHOYO. Babahoyo: UNIVERSIDAD TÉCNICA DE BABAHOYO.

Cán Chicol, , M. (2022). *Guía de alternativas para un sistema de control y seguridad en usuarios aplicando internet de las cosas (IOT).* Guatemala: Universidad de San Carlos de Guatemala.

Cano, J. (2024). *Diseño y creación de una suite de protocolos de capa de red orientado a videojuegos.* Cataluña, : Tecno Campus.

Cantillo, F. (2021). *DISEÑO Y USO PEDAGÓGICO DE UNA PAGINA WEB EN WIX PARA EL FORTALECIMIENTO DE LAS HABILIDADES DE LECTURA CRÍTICA A LOS ESTUDIANTES DEL GRADO SÉPTIMO I DE LA INSTITUCIÓN EDUCATIVA EL CARMEN.* Cartagena: Universidad de Cartagena.

Carmona Vásquez, J., & Monsalve Giraldo, E. (2024). *Plataforma de ciberseguridad para el aprendizaje y entrenamiento de hacking ético para estudiantes universitarios.* Medellin: Escuela de Ingeniería de Antioquia .

Carvajal Rojas, J. (2017). *La Cuarta Revolución Industrial o Industria 4.0 y su Impacto en la Educación Superior en Ingeniería en Latinoamérica y el Caribe.* Boca Raton: LACCEI International Multi-Conference for Engineering.

Casas, S. (2021). *El Portal de Integración deI PaaS Propuesta de comparación aplicando el proceso analítico jerárquico.* Patagonia Austral: Universidad Nacional de la Patagonia Austral.

Cornejo Velázquez, E. (2024). *La Ciberseguridad en la Adopción de la Industria 4.0.* Pachuca de Soto: UNIVERSIDAD AUTÓNOMA DEL ESTADO DEHIDALGO.

Cortez Torrez, J. (2018). *El marco teórico referencial y los enfoques de investigación.* La Paz: Universidad Mayor de San Andrés.

Delgado Batista, C. (2024). *INDUSTRIA 4.0 EN LA ERA DEL 5G: OPORTUNIDADES Y DESAFÍOS EN LA AUTOMATIZACIÓN DEL HOGAR MEDIANTE EL INTERNET DE LAS COSAS.* Panamá: Centro Regional Universitario de Los Santos.

Deza Villacorta, A. (2024). *Plataforma web Low-code para realizar el seguimiento y la gestión financiera de TI.* Lima: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Flores, A. (2015). *Buscando la excelencia educativa: Gestión de procesos académicos y administrativos en Instituciones Públicas de Educación mediante BPM.* Valencia: Universidad Internacional de Valencia.

Gallardo, V. (2020). *Explotación de los recursos de una casa inteligente en plataformas en la nube mediante tecnologia loT.* Madrid: UNIVERSIDAD pOLITECNICA DE mADRID.

Ganazhapa Malla, Á. (2024). *Dispositivo IoT e-tool utilizando protocolo CoAP para el monitoreo de las condiciones de salud laboral.* Manabi: Universidad Laica Eloy Alfaro de Manabí.

González de Lena Alonso, M. (2022). *Implementación de protocolos RUDP en el desarrollo de videojuegos multijugador.* Madrid: Universidad Rey Juan Carlos.

González-Hernández, I., & Macías, R. (2021). *Competencias del ingeniero industrial en la Industria 4.0.* Quintana Roo: Universidad de Quintana Roo. Obtenido de https://www.ibm.com/es-es/topics/industry-4-0

Gupta, Y. S. (2018). *A Survey on Security Issues in Cyber-Physical Systems.* Assam: National Institute of Technology Silchar.

Hermann Mirko, K. (2024). *Diseño de un sistema Telemetría empleando el protocolo OPC UA para una planta de almacenamiento de agua potable.* Lima: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Hervas, C. (2024). *Transformando la Educación: tecnología, innovación y sociedad en la Era Digital.* Sevilla: Universidad de Sevilla.

Hervás, D. R. (2021). *Tecnologías Low-Code y No-Code: Un caso práctico para estudiar su potencial y limitaciones.* Valencia: Universidad Politecnica de Valencia.

Informe: Gobiernos de América Latina y el Caribe demuestran compromiso inquebrantable para fortalecer sus capacidades en ciberseguridad. (2024). Fundacion de las Naciones Unidad.

Lucas Garcia, J. (2021). *PROGRAMAÇÃO NO-CODE NO ENSINO SUPERIOR: POSSIBILIDADES DE AVALIAÇÃO E APRENDIZAGEM ATIVAS.* Lisboa: Centro Universitário UNA.

Maria De Los Angeles, R. (2024). *Diseño de un sistema Telemetría empleando el protocolo OPC UA para una planta de almacenamiento de agua potable.* Lima: UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS.

Mendoza Armijos, H. (2023). *Libro de Memorias II ACongreso internacional de investigación los Andes Innova 2023.* Quito: Congreso Internacional los Andes Innova.

oas.org. (07 de 12 de 2024). *Reportes sobre incidentes de seguridad en la industria.* (oas.org) Obtenido de https://www.oas.org/ext/es/seguridad/prog-ciber

Ojeda Muñoz, V. (2024). *Caso de Estudio Comparativo de Plataformas Low-Code.* Santa Cruz: UNPA.

Pangol Lascano, A. (2022). *Industria 4.0, implicaciones, certezas y dudas en el mundo laboral.* Habana: Universidad de Ciencias Informáticas (UCI)Universidad de Ciencias Informáticas (UCI).

Parra Arévalo, J. (01 de 11 de 2024). *Análisis del desarrollo de software en no desarrolladores.* Bogota: FundaciónUniversitariaSanMateo. Recuperado el 01 de 11 de 2024

Rivas Mera, S., & Cevallos Sarango, J. (2024). *Impacto de la aplicación del enfoque de desarrollo de software Low Code en la sociedad Ecuatoriana.* Santo Domingo: Universidad de las Fuerzas Armadas.

Salazar, M. T. (2023). *Low Code para optimizar el tiempo de desarrollo de software.* Santo Domingo: Universidad de las Fuerzas Armadas ESPE.

Tamayo Ibáñez, J. (2023). *Low-code como alternativa a la digitalización de empresas. Desarrollo de un caso práctico con Appian.* Barcelona: d'Enginyeria Industrial de Barcelona.

TUITICE GAROFALO, C. (2024). *PROTOTIPO DE IPS DESARROLLADO EN PYTHON O C++ PARA DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO EN INFRAESTRUCTURA LORAWAN USANDO MÁQUINAS DE ESTADOS FINITOS.* DMQ: ESCUELA POLITÉCNICA NACIONAL.

TUITICE GAROFALO, C. (2024). *PROTOTIPO DE IPS DESARROLLADO EN PYTHON O C++ PARA DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO EN INFRAESTRUCTURA LORAWAN USANDO MÁQUINAS DE ESTADOS FINITOS.* DMQ: ESCUELA POLITÉCNICA NACIONAL.