Testbed basado en WWTP sobre GNS3 para desarrollo de pruebas de seguridad

Ander Gómez Iglesias

2023

Resumen

El objetivo de este documento es diseñar un *testbed* o banco de pruebas para un proyecto de una planta de tratamiento de aguas residuales o *Waster Water Treatment Plant (WWTP)*. Para ello se parte del proyecto ICSsVirtualForCiberSec, el cual virtualiza el despliegue de sistema de control industrial de una WWTP y realiza varios ataques mediante el protocolo Modbus.

1. Introducción

Debido a los avances de las últimas décadas en la industria inteligente, cada vez es más frecuente el uso de servicios como Cloud o IoT en los sistemas de control industrial (SCI) con el fin de cumplir los objetivos de la Industria 4.0. Esta conectividad tan alta a la que se exponen estos dispositivos tiene como resultado un incremento de los riesgos de ciberseguridad.

En los últimos años se han dado varios casos de ciberataques dirigidos a sistemas de control industriales, como TRITON [6], el famoso Stuxnet [5], o sin ir más lejos el reciente PIPEDREAM [3] del grupo CHERNOVITE. Cabe destacar este último, ya que se trata de una colección de exploits y herramientas diseñada para atacar dispositivos de múltiples fabricantes. El volumen y la gravedad de los ataques es cada vez mayor, y con ello el riesgo de catástrofe de las infraestructuras.

Para solventar estos problemas se emplean sistemas de detección y prevención de intrusos. Sin embargo, para poder investigar estos sistemas de detección de intrusiones es necesario contar con un entorno seguro y controlado, ya que de lo contrario se podría producir un fallo crítico y desencadenar una catástrofe. Por este motivo, los SCI operacionales no son idóneos para la investigación, y surge la necesidad de disponer de un banco de pruebas o testbed capaz de simular un SCI real.

2. Estado del Arte

En este apartado se van a analizar varios documentos relativos al diseño de un testbed para sistemas de control industriales.

2.1. Trabajos Previos

Alireza D. et al. presentaron el pasado 2022 ICSSIM [2] , un framework que permite desarrollar testbeds personalizados virtuales para sistemas de control industriales, en los que se pueden investigar y analizar varios tipos de amenazas y ciberataques.

El objetivo de ICSSIM es producir testbeds de SCIs extensibles, versátiles, reproducibles, de bajo coste y comprensivos, además de ser lo más realistas posibles. Para ello se emplea la tecnología de contenedores de Docker y simulación de software y hardware *in the loop* [1]

El diseño del framework sigue en líneas generales la Purdue Enterprise Reference Architecture o PERA [7], es decir, divide las tareas en diferentes fases.Gracias a este framework se reduce el tiempo de creación de testbed, testeo de ciberataques y logging. ICCSIM cuenta con múltiples scripts de ataques para facilitar la investigación, además de un ejemplo para demostrar sus funcionalidades.

Israel Barbosa et al. [1] realizan una propuesta de un testbed orientado a plantas de energía nucleares para poder investigar diferentes ataques de ciberseguridad. La propuesta simula una red que

[1] https://mathworks.com/help/simscape/ug/what-is-hardware-in-the-loop-simulation.html

implementa el protocolo Modbus/TCP, e implementa varios elementos de control industrial utilizando componentes de software de código abierto.

La propuesta nace de la dificultad de suspender la operación de la planta nuclear para la realización de pruebas de ciberseguridad, debido al alto riesgo que conlleva manipular material radiactivo de forma segura. Se consiguen realizar simulaciones realistas tanto de los procesos físicos controlados como de las redes de comunicación que se emplean en la central nuclear, combinando software y hardware de bajo coste y por tanto consiguiendo una propuesta asequible y al alcance de la mayoría de investigadores.

Conrad Ekisa et al. [4] propone un testbed comprensivo de código abierto para SCIs con el fin de demostrar las principales debilidades de ciberseguridad dentro den un SCI, así como las estrategias para remediarlas.

El proyecto busca identificar y desarrollar una colección de herramientas de código abierto que consigan emular de la manera más fiel posible los principales componentes de un entorno de control industrial. Estos componentes incluyen controladores lógico programables o PLC, interfaces máquina-humano o HMI, un *data historian*, esto es, una base de datos que almacena datos en forma de valores serie-temporales provenientes de varias fuentes de una planta de procesos, una *workstation* para la configuración de los PLCs y por último los componentes que controlan estos PLCs.

Además de eso, se busca desarrollar casos de estudio específicos con fines didácticos, dando la oportunidad a los aprendices de reproducir y entender las consecuencias de un ciberataque orientado a SCIs, así como las contramedidas necesarias para remediarlo. De esta forma se desarrollan las capacidades de detección, prevención y análisis de ciberataques , facilitando las principales tácticas, tecnicas y procedimientos (TTPs) empleadas. Esto es fundamental, ya que la barrera técnica es uno de los principales inconvenientes para los menos experimentados a la hora de crear entornos de análisis de ciberseguridad en SCIs.

Teniendo en cuenta todos lo mencionado anteriormente, se establece como objetivo del proyecto la simulación realista de una planta de tratamiento de aguas residuales mediante el uso de software y de una forma confiable, reproducible, escalable y entendible.

3. Tabla Enumerativa/Comparativa de tecnologías y Herramientas

En esta sección se muestras las principales herramientas y tecnologías empleadas en el proyecto, así como una breve descripción de cada una.

Tecnologías	
ICS	Solución para monitorizar y controlar procesos industriales en los que se reciben datos de sensores remotos que controlan las variables del proceso.
SCADA	Concepto que se emplea para realizar software de ICS. Facilita la retroalimentación en tiempo real y controla el proceso automáticamente.
PLC	Controlador Lógico Programable. Computadora empleada en la automatización de varios procesos industriales, p.e. líneas de montaje. Diseñados para tener múltiples I/O, mayor rango de temperatura, resistencia a vibraciones, impactos y ruido eléctrico.
Modbus	Protocolo de comunicación basado en arquitetura maestro/esclavo o cliente/servidor. Se ha establecido como un estándar en al industria, debido a su fácil implementación y el hecho de ser gratuito y de código abierto.
ModTester	Framework unificado de pentesting para el protocolo Modbus. Recopila diferentes herramientas para explotar vulnerabilidades, creando así un accesible toolkit con multitud de herraminetas para el protocolo Modbus.

Herramientas	
GNS3	Popular simulador gráfico de red que permite combinar dispositivos tanto reales como virtuales.
ScadaLTS	Solución que permite construir tu propio sistema SCADA. Multiplataforma, basada en web y de código abierto.
OpenPLC	PLC de código abierto basado en software y de fácil uso.
MySQL	Sistema de gestión de bases de datos relacionales de código abierto muy popular.
Simulink	Entorno de programación visual que funciona sobre Matlab. Se ejecuta sobre una imagen de matlab en un contenedor de Docker
Docker Compose	Herramienta que permite desplegar y orquestar múltiples contenedores de Docker. Se emplea un único archivo de configuración YAML para configurar todos los servicios de la aplicación.

Referencias

[1] Israel Barbosa de Brito and Rafael T. de Sousa. Development of an open-source testbed based on the modbus protocol for cybersecurity analysis of nuclear power plants. *Applied Sciences (Switzerland)*, 12, 8 2022.

[2] Alireza Dehlaghi-Ghadim, Ali Balador, Mahshid Helali Moghadam, Hans Hansson, and Mauro Conti. Icssim-a framework for building industrial control systems security simulation testbeds. 10 2022.

[3] Inc. Dragos. Pipedream: Chernovite's emerging malware targeting industrial control systems. 2022.

[4] Conrad Ekisa, Diarmuid O. Briain, and Yvonne Kavanagh. An open-source testbed to visualise ics cybersecurity weaknesses and remediation strategies - a research agenda proposal. Institute of Electrical and Electronics Engineers Inc., 6 2021.

[5] Ralph Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 9:49–51, 5 2011.

[6] Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems understanding the malware, its communications and its ot payload. 2018.

[7] T J Williams. The purdue enterprise reference architecture:. *Purdue Laboratory Jor Applied Industrial Control, Purdue University, West LaJayette, IN 47907, USA*, 1993.