universidad de león

Escuela de Ingenierías

Industrial, Informática y Aeroespacial

GRADO EN INGENIERÍA INFORMÁTICA

Trabajo de Fin de Grado

ANÁLISIS DE CIBERSEGURIDAD EN SUSESTACIONES CON EL ESTANDAR IEC 61850

CYBERSECURITY ANALYSIS IN SUBSTATIONS WITH IEC 61850 STANDARD

Autor: Marcos González Maestre
Tutor: Isaías García Rodríguez

(Julio, 2022)

UNIVERSIDAD DE LEÓN
Escuela de Ingenierías Industrial, Informática y Aeroespacial

GRADO EN INGENIERÍA INFORMÁTICA
Trabajo de Fin de Grado

ALUMNO: Marcos González Maestre

TUTOR: Isaías García Rodríguez

TÍTULO: Análisis de ciberseguridad en subestaciones con el estándar IEC 61850

TITLE: Cybersecurity analysis in substation with IEC 6150 STANDARD

CONVOCATORIA: Mes, Año

RESUMEN:

El resumen reflejará las ideas principales de cada una de las partes del trabajo, pudiendo incluir un avance de los resultados obtenidos. Constará de un único párrafo y se recomienda una longitud no superior a 300 palabras. En cualquier caso, no deberá superar una página de longitud.

ABSTRACT:

Palabras clave: Lorem, ipsum, dolor, sit, amet.

Firma del alumno:	**VºBº Tutor/es:**

Índice

Índice de Ilustraciones

1 Introducción

1.1 INTRODUCCIÓN

En la actualidad, vivimos en un mundo globalizado y en constante cambio y evolución. Por la parte de ingeniería informática que nos involucra, es muy importante estar alerta y en constante evolución y aprendizaje para seguir el ritmo evolutivo de nuestro planeta. Ya lo pudimos ver, como durante la pandemia del COVID, todas las empresas tuvieron que adoptar medidas para el teletrabajo, que sin la colaboración de ingenieros y de instituciones informáticas hubiera sido todo mucho más complicado.

Adentrándonos en el ámbito informático, veremos qué pasa lo mismo en la rama de la ciberseguridad informática. Cada día que pasa, sale algo nuevo, algún nuevo gusano que puede comprometer el sistema de una empresa, posibles ataques a infraestructuras criticas de todo tipo (como por ejemplo en el ámbito nuclear), nuevos protocolos y estándares, los cuales se empiezan a aplicar e distintas situaciones o nuevas plataformas y aplicaciones usadas en este ámbito.

Durante la realización de este trabajo, estamos viendo como de importante es la ciberseguridad en el ámbito de infraestructuras críticas relacionadas con la energía. Sabiendo que cualquier falla de seguridad en una central nuclear por ejemplo puede desencadenar en una catástrofe humanitaria grandísima. O cualquier fallo o brecha en una subestación eléctrica, puede dejar sin electricidad a una gran parte de ciudadanos de un país incluido empresas situadas en esa zona. Y todo ello, desemboca en una única situación, caos en la población y pérdidas dinerarias irreparables para las empresas.

1.2 JUSTIFICACIÓN DEL PROYECTO

1.3 OBJETIVOS DEL PROYECTO

1.4 ESTRUCTURA DEL PROYECTO

1.5 METODOLOGÍA

Para poder tener los conocimientos necesarios y la base adecuada para la correcta realización del proyecto, fue necesario un periodo de tiempo de aprendizaje que consistió en la lectura y comprensión del estándar IEC 61850, lo cual englobaba la lectura de todos los capítulos del estándar y unas preguntas y ejercicios realizada por el tutor. Una vez conseguido estos conocimientos, IED SCOUT fue la plataforma usada para ver una simulación de comunicación entre un suscriptor y un publicador que emulaba el manejo de un IED real. Una vez entendido y visto cómo funciona la comunicación entre suscriptor y publicador, pasamos a usar la herramienta NOZOMI.

2 Planificación y gestión del proyecto

2.1 ALCANCE DEL PROYECTO

2.2 PLANIFICACIÓN

3 Estado del arte

3.1 ESTO ES UNA PRUEBA

4 Tecnologías usadas

4.1 VMWARE WORKSTATION PRO

VMWARE es una herramienta de virtualización que sirve para emular un elemento al que no estamos teniendo acceso. Es decir, físicamente no tenemos acceso directo a ese recurso, ya que solo lo estamos emulando. Esta herramienta ha sido usada para la implantación y configuración de la herramienta que más abajo explicaré, Nozomi.

Ilustración 1.. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia)

Seguimps escribiendo

4.2 NOZOMI NETWORKS

Nozomi es una compañía de software relacionado con el tratamiento de los datos y la ciberseguridad. Se definen así mismo como *"la mejor opción en soluciones de seguridad y visibilidad de la tecnología operativa y del internet de las cosas. Acelera la transformación digital protegiendo la infraestructura crítica así como a las organizaciones industriales y gubernamentales de las ciber-amenazas"*. Disponen de una serie de productos, entre los que se encuentran los siguientes:

a. Nozomi Vantage
b. Nozomi Guardian
c. Nozomu Central Management Console
d. Nozomi Cyber Threat Intelligence
e. Nozomi OT y IoT Asset Intelligence

4.3 WIRESHARK

La herramienta Wireshark es una de las herramientas más antiguas, conocidas y usadas en el ámbito de redes y ciberseguridad. Wireshark se puede definir como un analizador de protocolos de código abierto cuyo principal objetivo es analizar el tráfico en la red. Está disponible tanto para plataformas Windows como para Linux. Wireshark posee una amplia gama de filtros de búsqueda de tramas para los más de 1000 protocolos soportados actualmente.

Originalmente Wireshark nació del proyecto de la herramienta llamada Ethereal, la cual haya personas que les suene el nombre y posiblemente la hayan usado. Ethereal se empezó a desarrollar en 1997 y la cual se dejó de implementar en el año 2006. A partir de ahí paso a llamarse como la conocemos hoy en día, Wireshark.

Ilustración 2. Logo de la herramienta Wireshark (Fuente: https://www.wireshark.org)

4.3.1 PARA QUE SE USA WIRESHARK

La idea básica de esta herramienta es que el usuario pueda ver con detalle el tráfico de paquetes que se está generando en una determinada red. Se tiene que tener en cuenta que hasta en redes domésticas en las que un solo host está conectado, habrá movimiento de paquetes. En este tipo de redes pequeñas, se podrá ver con facilidad todos los tipos de paquetes y para qué sirven cada uno.

Si por el contrario, la red a la que se conecta el host, es una red mucho más extensa (esto quiere decir que hay un número alto de host conectados en la misma red, ejemplo: oficina de una empresa con 25 trabajadores conectados en la misma red), habrá mucho más paquetes y será más difícil captar los paquetes que interesen. Por lo que se tendrán que usar lo que se denomina como filtros. Esta herramienta posee infinidad de filtros para detectar los paquetes que contengan la característica indicada en ese filtro. Por ejemplo si se quiere ver únicamente los paquetes que contengas una IP de origen o de destino usaremos este filtro: ip.src_host==192.1.168.1.128 || ip.dst==192.168.1.128, donde 192.168.1.128 sería la IP del host que queremos que aparezcan sus paquetes.

Adentrándose más en las características principales de Wireshark, se puede llegar a ver paquetes perdidos, actividad maliciosa en la red mediante la captura de paquetes http, así como problemas de latencia o problemas de conexiones. En apartados superiores, veremos varias implementaciones y usos de esta herramienta.

En resumen, con Wireshark podremos ver y analizar todos los paquetes de nuestra red como si estuviéramos en un laboratorio con un microscopio analizando todo lo que pasa en una determinada red.

4.4 IED SCOUT

IED Scout es una herramienta que nos permite la automatización de protección de subestaciones que disponen del estándar IEC 61850. También nos permite ver la comunicación entre un suscriptor y un publicador.

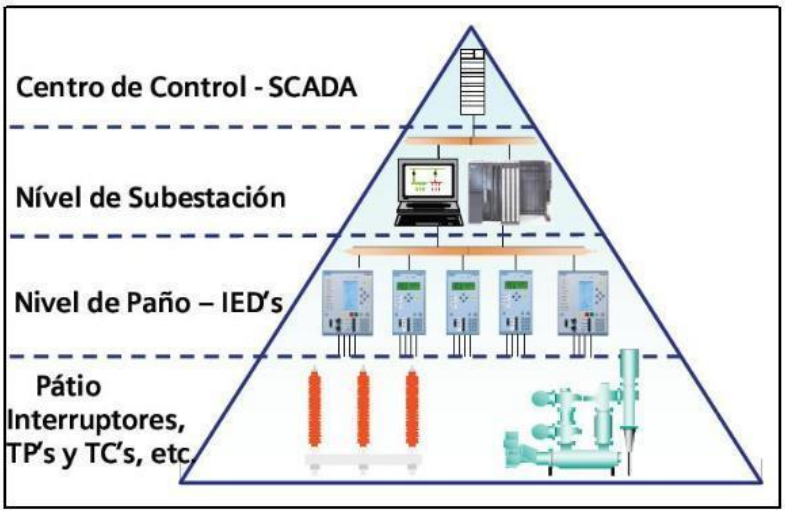
4.5 ADVANCED IP SCANNER

Escáner de la red fiable y gratuito para analizar LAN. El programa escanea todos los dispositivos de red, le da acceso a las carpetas compartidas y a los servidores FTP, le proporciona control

remoto de las computadoras (mediante RDP y Ranedmin) e incluso puede apagar las computadoras de manera remota. Es fácil de usar y se ejecuta como una edición portable. Debe ser la primera opción para cada administrador de red.

4.6 IEDs

Tenemos varios tipos de IEDS. Que son los siguientes:



https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM

5 Núcleo del trabajo

5.1 CIBERSEGURIDAD EN LA ACTUALIDAD

5.2 ESTANDAR IEC 61850

5.2.1 INTRODUCCION AL IEC 61850. ¿QUÉ ES?

IEC 61850 es un estándar relacionado con

5.2.2 ORÍGENES DEL ESTANDAR IEC 61850

5.2.3 ESTRUCTURA DEL IEC 61850

5.2.4 MODELOS DE COMUNICACIÓN