Lo mas importante del capítulo “como atacan las redes SCADA” es comprender que aunque una red se encuentre aislada, no garantiza que este libre de ataques en su seguridad, algo importante a resaltar es que aunque la industria tome las medidas necesarias para asegurar su seguridad en redes SCADA una mala capacitación a los usuarios puede generar problemas al ser el humano el que interactúa de manera directa o indirecta con dispositivos de la red, es recomendable tomar medidas de seguridad como bloquear puertos USB o cualquier método de comunicación de los equipos que se encuentren dentro de la red SCADA.

Tipos de ICS y componentes ….

Componentes de ICS y protocolos…

Arquitectura Purdue, lo mas importante a destacar de esta arquitectura es su estructura y separación de componentes en capas y niveles y que estos lleven un orden y proceso de comunicación lógico y estricto, al separar los componentes pertenecientes a la red corporativa de los componentes de la red industrial se garantiza la correcta comunicación y seguridad de cada uno de los niveles. Si se pretende el acceso o comunicación de la zona Enterprise a la zona Cell es estrictamente obligatorio pasar por la zona de manufactura mediante protocolos. Resulta mala practica tener doble tarjeta de red en un equipo para tener acceso a la red corporativa y a la red industrial esto rompe con la filosofía y estructura de la arquitectura Purdue.

Amenazas de sw componentes y personas, el ojo humano e incluso los HMI están sujetos a vulnerabilidades ya que el ojo humano no puede identificar cambios mínimos o imperceptibles de comportamiento de componentes y el HMI no identifica o alerta de manera eficiente estos cambios o anomalías, es por ello la importancia de la implementación de tecnologías como Machine Learning o inteligencia Artificial, que sean estas tecnologías las encargadas de analizar el comportamiento de componentes y poder emitir una alerta o notificación de acuerdo a eventos o situaciones pasadas o a situaciones no programadas como el apagado repentino de un ventilador, o el aumento no justificado de una válvula, etc.

Stuxnet demuestra que la industria y su arquitectura de red industrial se encuentra vulnerable, el proyecto Stuxnet fue realizado y ejecutado de manera exitosa cumplió su objetivo principal que en primera instancia era comprobar si existía una fábrica de tratamiento de uranio clandestina y una vez comprobada dicha información, atacar la red industrial y colapsar los componentes acelerando y desacelerando las maquinas repetidamente. Sin embargo, el anonimato no fue su fuerte al ser descubierto su ataque por parte de los fabricantes de antivirus mas reconocidos a nivel mundial. Como enseñanza demuestra que se debe estar al tanto de este tipo de ataques ya que las industrias si es mas no están al ojo de las organizaciones políticas, pero incluso su propia competencia puede hacer uso de este tipo de ataques.

Casos de estudio: Las redes industriales no están exceptas a los ataques, así mismo sus protocolos de comunicación no son 100% seguros y se encuentran vulnerables a los ataques, hay que dar la importancia necesaria tanto o mas como a las redes corporativas.

Técnicas de ataque

Spear Phishing:

Es un ataque a especie de engaño, al simular ser otra persona o entidad, puede diseñar correos electrónicos bastante creíbles basados en tus gustos o contactos, es importante filtrar los permisos a la información en redes sociales que no sea publica toda tu información, asegurarse de que el remitente que te envía el correo sea de tus contactos o que el dominio pertenezca a la empresa que te contacta, se puede utilizar sitios que comprueban si un link es peligroso que sin duda nos ayudara a mantenernos más seguros.

Recomendaciones tras un ataque de tipo spear phishing:

Como primer paso se debe revisar el remitente y hacer un match con el contenido del email, por ejemplo, si el contenido del correo electrónico sugiere la actualización de contraseña de una cuenta de Amazon, el dominio del remitente debería ser amazon.com de no ser así podría ser muy seguramente un spear phishing. La siguiente recomendación es acceder directamente a la dirección de la cual solicitan nuestros datos, por ejemplo, si recibimos un correo sobre una nueva solicitud de amistad en una red social, deberíamos acceder directamente a la red social e iniciar sesión para aceptar dicha solicitud desde la propia aplicación. Por último, nunca se debe hacer clic directamente en los enlaces de los correos electrónicos aun así creamos o estemos seguros de que son reales.

Watherhole attack:

Es un ataque APT o ataques avanzados persistentes consisten que mediante un navegador web solicitar al usuario actualice o instale un software en específico obviamente haciéndolo creer como una actualización real, uno de los mas atacados con este método es el software flash de adobe por lo cual se recomienda no utilizar dicho software en nuestro navegador de preferencia o a su vez deshabilitarlo.

Ataques HID:

Es un ataque mediante el uso de dispositivos de interfaz con humano como USB, CD, y cualquier otro tipo de dispositivo que interactue con el usuario, el proceso es el siguiente, mediante un USB extraviado el cual puede ser real o simular un dispositivo de entrada como el teclado comprometer el computador. Que se debe hacer, como primer paso nunca se debe conectar un dispositivo que lo encontramos y no conocemos su procedencia, si lo conectamos no abrir ninguno de los archivos o programas que incluye ya que este puede ser el accionar que comprometer a nuestro equipo ya que estos están diseñados para evadir los antivirus.

Ataques BEC:

Compromiso de email corporativo, este ataque consiste en infiltrarse en la organización mediante los métodos anteriores y una vez dentro investigar la red para analizar el giro de negocio, proveedores, pagos, información sensible por ultimo paso suplantar la identidad de altos mandos enviando ordenes de transferencias de dinero o información mediante correo electrónico, se debe seguir las recomendaciones planteadas en los métodos anteriores para detectar emails fraudulentos y para saber como actuar ante estas situaciones.

Modulo 3 gestion de riesgos SCADA:

Software: es importante la utilización de software especializado para la gestión de riesgos de redes SCADA ente los disponibles tenemos GRASSMARLIN el cual nos permite analizar todos y cada uno de los componentes de la red, ver quien se comunica con quien bajo que protocolos lo hace, obtener informes del inventario de la red.

Frameworks de seguridad, estrategias y políticas: los frameworks de seguridad o marcos de trabajo deben ser tomados como un modelo, se debe adaptar a la institución y en realidad lo que importa es en saber utilizar las herramientas o buenas practicas de acuerdo a la necesidad u objetivos que se quiera cubrir, la metodología recomendada es: plan, do, check, act (planificar, hacer, verificar, actuar)

NISTIR: framework para el sector eléctrico, sin embargo, este puede ser adaptado a otro tipo de industria, el proceso a seguir es el siguiente: identificar las amenazas, las vulnerabilidades y las consecuencias de acuerdo con ello se puede tener una mejor apreciación del riesgo.

IEC 62443: hace énfasis en la importancia de los procesos, la tecnología y las personas, es una serie de documentos. Se debe separa en zonas de acuerdo con el tipo de componentes y entre zona y zona se debe configurar un firewall o un diodo de datos en donde se establecen las reglas para determinar quien se comunica con quien y bajo que protocolo.

NIST 800-82: es una adaptación de NIST 800-53 orientado a las redes industriales, se alinea mucho a la arquitectura Purdue.

Vulnerabilidades e impactos: existen dos métodos para realizar el análisis de vulnerabilidades el uno es el escaneo activo, el cual consiste en cruzar o validar la información del inventario emitido.

Gestión de riesgos:

Es la posibilidad de que la amenaza determinada explote las vulnerabilidades de un activo

Es un proceso continuo de identificación, valoración y respuesta las acciones que se pueden tomar frente a los riesgos son: mitigar, transferir, evitar y aceptar. Para la clasificación del riesgo se puede utilizar la metodología DREAD. Es de buena practica diseñar un mapa de calor para el análisis del riesgo de la empresa es cual esta conformado por la probabilidad de ocurrencia frente al impacto generado. El riesgo esta determinado por las amenazas, vulnerabilidades y las consecuencias.

Metodología de assessment de seguridad:

Es recomendable el uso del software CSET, este es un software gratuito muy intuitivo y funccional el cual nos permitirá realizar un assessment de seguridad siguiendo el siguiente proceso: selección de estándares, en esta etapa se debe seleccionar con que estándares o frameworks se realizara la evaluación. Determinar los SAL, estos deben estar determinados de acuerdo a la realidad de la empresa imaginando el peor escenario posible. Creación de diagrama, el software posee una herramienta para la creación del diagrama de red de la industria. Contestar las preguntas, estas preguntas van estar determinadas de acuerdo al estándar y framework seleccionado previamente. Análisis de resultados, el sw emite resultados gráficos y reportes los cuales pueden ser descargados, analizados, realizar una comparación con evaluaciones anteriores.

Estrategias para el estudio de la seguridad:

Se debe identificar que tipo de logs se maneja en la red industrial sobre los incidentes o impactos potenciales. Se debe seguir el siguiente proceso:

Definir los objetivos general y específicos.

Incorporar los beneficios de la ejecución del plan estratégico de seguridad.

Describir las consecuencias que se pueden dar en caso de no cumplir con el plan estratégico que se esta diseñando.

Describir los esfuerzos actuales, describir la realidad de la industria.

Con toda la información reunida, se debe definir el alcance en ello se define los roles y responsabilidades.

Modulo 4 controles de seguridad de SCADA, concienciación de usuarios

Identificación, autenticación y autorización: quien, que y como esta accediendo el usuario a la red industrial. El enfoque consiste en establecer permisos adecuados, imponer controles de acceso y monitorear la actividad del usuario.

La autenticación basada en riesgo permite determinar si el usuario que intenta acceder a la red a pesar de utilizar el mismo usuario y contraseña pero la dirección IP es otra, las cookies han cambiado y otro tipo de indicadores, dado esto nos indica un nivel de riesgo alto con el cual podemos establecer un umbral y gestionar este tipo de acceso.

Seguridad lógica: recomendaciones a tomar en cuenta:

Eliminar programas o funciones no necesarios.

Listas blancas a nivel de red, configurar el firewall para aceptar solo cierto tipo de conexiones.

Whitelinsting en la configuración del software.

El correlacionador de eventos SIEM, es capaz de detectar y almacenar todo tipo de eventos, el SIEM necesita monitoreo y alerta frente a las anomalías, esta el SOC quien afina o dice como afinar, las alertas debe pasa un triaje adecuado, el CSIRT puede comunicarse con otros CSIRT y saber como resolver una incidencia.

El SIEM no es el techo o limite sobre el control de incidencias, lo siguiente es la implementación de un orquestador de incidencias y respuesta automática esto puede hacerse gracias a las tecnologías y protocolos de comunicación como STIX el cual utiliza archivos en formato JSON de las incidencias notificadas por la comunidad, este es un estándar que mediante el servidor taxi que maneja STIX se puede alimentar una bdd de incidencias, teniendo esto lo siguiente es configurar e implantar CACAO un protocolo o estándar de playbooks, procedimientos repetibles, y mediante un protocolo M2M tomar acciones inmediatas de acuerdo al playbook mediante OpenC2.

Seguridad física:

La seguridad física es tan importante como la lógica ya que si descuidamos esta es el primer acceso no autorizado que se pueda hacer a la organización, se debe dar mucha importancia a las cerraduras, implementar doble autenticación en puertas de acceso. La política de escritorio limpio sugiere, no dejar contraseñas a la vista, si se abandona la estación de trabajo bloquear la maquina, no dejar documentos con tarjetas de acceso, si alguien esta observando nuestro trabajo se debe parar y pedir que la persona se retire, no descuidar llaves o métodos de acceso, destruir la información confidencial antes de desecharla.

Resumen buenas practicas de seguridad.

Se debe considerar un mapa de calor, el SAT en CSET la evaluación de seguridad industrial.

Hacer concienciación de usuarios, recordar que es el primer acceso o victima en un ataque cibernético, capacitar a los operarios de IT y OT y cada uno de los miembros de la organización.

Hacer monitoreo de actividades sospechosas, se puede implementar tecnologías de machine learning e inteligencia artificial.

Descubrir vulnerabilidades.}

Tener sensores SCADA en el endpoint, manejar listas blancas y monitoreo de cambios.

Monitoreo de protocolos propietarios y estándares SCADA, también monitorizar protocolos IT por ejemplo p2p.

Visualización de la red, realizar una visualización independiente de la red, evitando un ataca man in the middle.

Usar inteligencia artificial para descubrir anomalías.

Monitoreo continuo en un SOC y CSIRT OT no de IT.