4 DEFINICIÓN DE UN MARCO DE AUDITORÍA

4.1 INTRODUCCIÓN

Un marco de auditoría es una definición de alto nivel de una serie de objetivos a cumplir y un listado de tareas con detalles más o menos técnicos de que se busca y cómo se debe buscar en cada una las pruebas a realizar.

Este marco de auditoría se ha dividido en las siguientes fases:

- Estudio de la documentación
- Captura de información
- Análisis
- Documentación

Las dos primeras fases definen **qué** tipo de datos se deben obtener para realizar el estudio, la primera se refiere a documentación y buenas prácticas que se realizan en la empresa, en la segunda fase se especifican que información técnica es necesario obtener y que herramientas se pueden utilizar.

La tercera fase define **cómo** deberían hacerse las cosas y sobretodo como no se deberían hacerse algunas de las más importante y de las que anteriormente hemos obtenido/capturado información.

La cuarta fase **resume los hallazgos** encontrados en la fase anterior, esta fase es puramente de documentación. Se enumeran y describen brevemente los documentos que deberían componer un informe de auditoría y se dan ejemplos de cómo deberían ser.

Este marco de auditoría se ha pensado de manera que las fases 1ª, 2ª y 3ª las puedan realizar tres equipos independientes, en el caso de la 4ª fase es recomendable que lo realice el mismo equipo que hizo la fase de análisis aunque perfectamente podría ser un cuarto equipo de personas.

Hay que tener en cuenta que un marco de auditoría es una herramienta para organizar y facilitar el trabajo al auditor que lo va a utilizar y no un libro donde se explique que es cada tipo de prueba, herramienta o mecanismo de defensa. Por tanto se recomienda que la persona que utilice este marco de auditoría tenga experiencia en la realización de auditorías técnicas, análisis de riesgos y/o uso de herramientas de seguridad.

Se observará que este marco de auditoría va de menos técnico a más, la razón de esto es que si podemos averiguar información del estado de los sistemas sin tener que realizar ninguna prueba mucho mejor ya que disminuimos el riesgo de bloquear un sistema en una prueba técnica, además de tener que invertir menos tiempo.

(Doggan, 2005)

Finalmente comentar que esta es una primera versión del marco de auditoría y por tanto es incompleto, pese haber sido probado en una empresa y refinado posteriormente, no es sino con el uso continuado en distintos entornos y la revisión por otras personas que cualquier marco de trabajo madura hasta convertirse en el estándar de-facto.

4.2 ESTUDIO DE DOCUMENTACIÓN

4.2.1 ACTIVOS Y ESQUEMA DE RED

1) ¿Existe un listado de activos?

La empresa debería tener identificados y clasificados todos los activos que intervienen en los sistemas de control industrial como PLC, ordenadores, switches, routers, motores, válvulas, buses industriales, buses informáticos, etc.

De cada activo se debería saber:

- Breve descripción
- Localización física

- Dirección MAC
- Dirección IP
- Marca y modelo
- Fecha de instalación
- Historial de reparaciones
- Historial de actualizaciones de firmware/software
- Técnico/Departamento/Empresa Responsable
- Otra información relevante

2) ¿Existe un listado de activos críticos?

De todos los activos se debería identificar los que son especialmente críticos, explicar las razones de su criticidad e identificar que operaciones requiere para su mantenimiento.

3) Esquemas de red

La empresa debería tener mapas de red detallados y exhaustivos de todas las plantas y sistemas industriales. En estos mapas se debería ver el tipo de dispositivo, a que switch está conectado, su dirección IP, marca, modelo y/o sistema operativo.

4.2.2 GESTIÓN DE INCIDENCIAS

1) ¿Cómo reportan las incidencias los usuarios de la red?

Deben existir varios métodos para reportar incidentes para que en caso de desastre siempre esté al menos un método disponible. Algunos métodos recomendados son:

- Formulario
- Email
- Teléfono directamente al Centro de Gestión de Incidentes

Los usuarios deberían conocer la existencia de todos estos métodos para reportar los incidentes y saber que incidentes deben reportar.

2) **¿Existe algún procedimiento de gestión de incidencias?**

Debería estar definido un proceso de gestión de incidencias donde se detallaran los distintos puntos:

- Proceso de recepción de incidencias
- Priorización de la resolución: en función de que se prioriza la atención de unas incidencias sobre otras
- Mecanismos de resolución y herramientas: cómo se decide quién es responsable de solucionar la incidencia, cómo la debe resolver, que herramientas tiene a su disposición, forma de cerrar los casos, etc.
- Post-incidente: tareas que se realizan cuando se resuelve un incidente para prevenir que vuelva a ocurrir.

3) **¿Se realizan resúmenes de los incidentes?**

Se debería resumir de forma mensual, trimestral y anual los incidentes gestionados para obtener estadísticas que ayuden en la gestión de la seguridad de la empresa.

4) **¿Se revisan los resúmenes para ver qué tipo de incidentes ocurren más a menudo y analizar las causas?**

Debería haber un comité encargado de revisar los indicadores obtenidos y tomar acciones concretas para reducir los incidentes más recurrentes.

5) **¿Se guardan las evidencias de incidentes durante un periodo de al menos un año?**

Se recomienda retener las evidencias de incidentes (logs) durante un año o en su defecto el máximo que marque la ley. Los informes y estadísticas de los incidentes se recomienda guardarlos durante un periodo de cinco años como mínimo.

4.2.3 PLANES DE CONTINGENCIA

4.2.3.1 COPIAS DE SEGURIDAD

1) **¿Se realizan copias de seguridad? ¿De qué activos?**

Se deberían realizar copias de respaldo de la mayoría de sistemas críticos de la empresa, incluyendo el firmware y programas que corren en los PLC.

2) **¿Con que frecuencia se realizan copias de seguridad?**

Una planificación recomendada de las copias de seguridad es la que sigue:

- Completa anual
- Completa mensual
- Completa semanal
- Incremental o diferencial diaria sobre la copia semanal

Se recomienda realizar las copias durante el periodo de menor uso de la red local para evitar interferencias con el resto de usuarios.

3) **¿Cómo se gestiona los medios físicos (discos, cintas, DVD, etc.) en los que se realiza las copias?**

Se recomienda trasladar los medios donde se hayan realizados las copia p.ej. cintas, DVD, discos, etc.) a otro lugar separado del sistema del que se guardan los datos para que en caso de desastre (fuego, inundación, terremoto) se puedan asegurar los datos.

4) **¿Cada cuanto tiempo se verifica si las copias se han realizado correctamente? ¿Cómo?**

Se recomienda mínimo una vez al mes verificar que se pueden recuperar de forma correcta los datos y deseablemente esta recuperación se podrá realizar en poco tiempo.

4.2.3.2 RECUPERACIÓN DE DESASTRES

1) **¿Existe un plan de recuperación ante desastres?**

Debería existir un plan de recuperación ante desastres donde se especificara como mínimo como restablecer los sistemas críticos para mantener las operaciones vitales del negocio en funcionamiento o recuperarlas lo más rápido posible.

Algunos elementos a tener en cuenta:

- Debería haber un segundo Centro de Procesamiento de Datos
- Componentes de repuesto de las piezas que más frecuentemente se estropean
- Datos de contactos de los técnicos, empresa instaladora, fabricante, etc.
- Procedimiento detallado de puesta en marcha de cada sistema

2) ¿Los sistemas críticos están en alta disponibilidad?

Idealmente los sistemas críticos estarán en una configuración de alta disponibilidad en caso de fallo del sistema principal entrará en funcionamiento un segundo sistema. La puesta en marcha del segundo sistema puede ser automática o manual en función del tiempo que puede estar un servicio/sistema parado.

3) ¿Existen protecciones contra fallos del suministro eléctrico?

Se deberían contemplar proteger a los sistemas informáticos e industriales con las siguientes medidas de protección eléctrica:

- Protección contra subidas de tensión y otras irregularidades
- Garantizar el suministro eléctrico en caso de caída del proveedor principal
- Utilizar Sistemas de Alimentación Ininterrumpida (SAI) para garantizar un apagado controlado de los sistemas informáticos en caso de fallo del suministro eléctrico

4) ¿Está documentado el plan de recuperación de desastres?

Debería existir una documentación general de cómo reaccionar ante diversos tipos de desastres.

4.2.4 GESTIÓN DE LA SEGURIDAD

1) ¿Existe un responsable de seguridad?

Debería haber una persona que fuera el máximo responsable en cuestiones de seguridad, que coordinara todos los esfuerzos del resto del personal y que tuviera poder dentro del esquema organizacional de la empresa para permitirle tomar decisiones a nivel mando.

4.2.5 POLÍTICAS DE SEGURIDAD

1) ¿Cómo se clasifica la información?

Se debería clasificar la información, tanto en papel como digital, en varios niveles según la criticidad de la información. Una posible clasificación es: Público, Interno y Confidencial.

4.2.5.1 CONTROL DE ACCESO

1) ¿Cómo se controlan los accesos físicos a las fábricas, lugares de trabajo y activos críticos de la empresa?

Se debería controlar el acceso a los activos críticos de la empresa mediante la combinación de algunos de los siguientes métodos:

- Cámaras de seguridad
- Guardas que vigilan los puntos de entrada
- Armarios con llave
- Cajas fuerte
- Salas dedicadas para el equipo sensible
- Puertas de seguridad

2) ¿Cómo se registran los accesos?

Cada vez que una persona entra y sale de las instalaciones de la empresa se debería registrar en una hoja de registro, como mínimo:

- Nombre
- Empresa
- Hora entrada
- Hora de salida
- Persona responsable

En el caso de acceder a zonas sensibles el visitante siempre estará acompañado de una persona de la empresa y será su responsabilidad velar por que cumpla la política de la empresa.

3) ¿Están documentados los puntos de acceso a cada oficina/fábrica?

Deberían estar documentado todos los puntos de entrada y salida de cada una de las instalaciones de la empresa.

4.2.5.2 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1) ¿Existen procedimientos de test antes de poner un sistema crítico en funcionamiento?

Antes de poner en funcionamiento un sistema crítico o después de una actualización de software o hardware es importante realizar pruebas para verificar que el sistema se comporta de la manera prevista.

2) ¿Se encuentran solo los puertos y servicios necesarios habilitados?

En todos los ordenadores de la empresa pero especialmente los servidores, PLC y otros elementos sensibles del proceso de manufactura, se deberían deshabilitar todos los servicios innecesarios o implementarse un dispositivo firewall para permitir el acceso solo a los sistemas que lo requieran.

3) ¿Existe un plan de actualizaciones de seguridad?

Debería existir un calendario de actualizaciones de seguridad definido en función de la criticidad de las máquinas, exposición a ataques y de los periodos de mantenimiento asignados a cada cadena de producción. Estas actualizaciones incluye el sistema operativo de máquinas cliente y servidores, aplicaciones y firmware de PLC y maquinaria industrial.

En caso de no poder instalar una actualización se deberá justificar y registrar la causa, en caso de incompatibilidad con software de terceros se deberá pedir a la empresa desarrolladora que actualice su producto para hacerlo compatible con las actualizaciones de seguridad del fabricante del sistema operativo.

4) ¿Prevención de software malicioso?

Deberán usarse sistemas para prevenir código malicioso en las redes de la empresa y especialmente en las industriales mediante el uso de antivirus, antispyware y otras tecnologías relacionadas.

Los sistemas que no pueden ejecutar software antivirus deberán estar protegidos de otras redes mediante filtrado antivirus en un dispositivo de red, p.ej. un firewall.

5) ¿Gestión de cuentas de usuario?

El departamento de Recursos Humanos (RRHH) deberá informar al departamento de administración de sistemas cuando un empleado deja la empresa para que se pueda dar de baja del sistema. Es recomendable que el aviso se haga con cierto tiempo antes sobre todo si la persona que deja la empresa lo hace de forma no amistosa y además tiene acceso a información/recursos valiosos.

6) Contraseñas por defecto

Ningún sistema se debería dejar con las contraseñas que vienen en la configuración por defecto.

Las claves del servicio SNMP se deberían cambiar y en ningún caso serán "public", "private" ni tampoco una palabra relacionada con la empresa o que aparezca en un diccionario.

7) ¿Gestión de contraseñas?

Se debería comprobar que las contraseñas de todos los sistemas cumplen con las características marcadas por la empresa.

Los sistemas industriales y paneles táctiles de administración deberían tener una contraseña fácil de recordar pero distinta para cada administrador o técnico

8) ¿Se monitorizan los eventos de seguridad?

En la medida de lo posible se debería monitorizar los eventos de seguridad producidos por los sistemas más críticos y que participan directamente en los procesos de fabricación o de control.

9) ¿Existen sistemas de detección de intrusos? ¿Hay algún sensor en las redes industriales? ¿Están las firmas de ataques contra sistemas industriales instaladas?

Deberían existir sistemas de detección de intrusos en los segmentos de redes industriales y a ser posible con patrones especializados en detección de ataques contra este tipo de redes. Esto es especialmente importante si la red industrial no se puede segmentar físicamente o lógicamente con firewalls del resto de redes de oficina.

10) ¿Qué se hace con el material informático una vez no se usa?

El material informático que pueda contener datos sensibles se debería borrar de forma segura o en su defecto se debería destruir antes de ser desechado.

11) ¿Se hacen auditorías de los sistemas conectados al perímetro de la red al menos una vez al año?

Los sistemas que están en el perímetro de la red deberían ser auditados como mínimo una vez al año, algunos de estos sistemas son:

- Servidores en la DMZ
- Puntos de acceso WIFI
- Terminadores VPN
- Servidores que aceptan conexiones VPN
- Firewall
- Servidor de correo

12) ¿Se revisa y mantiene la documentación anualmente?

Se debería mantener toda la documentación referente a seguridad de los sistemas industriales actualizada y revisarla como mínimo una vez al año.

4.2.5.3 CONTROL DE CAMBIOS

1) **¿Se realiza control de cambios sobre el software instalado?**

Se debería realizar un control de cambios en el software instalado en cada máquina y especialmente en los servidores directamente relacionados con los PLC.

2) **¿Se realiza control de cambios sobre el firmware instalado en dispositivos industriales?**

Se debería realizar un control de cambios en el software y firmware instalado en cada PLC.

4.2.5.4 CONCIENCIACIÓN Y FORMACIÓN

1) **¿Existe definido un plan de concienciación sobre seguridad de la información en la empresa? ¿Se realiza este plan de concienciación pensando en operadores y administradores de los sistemas industriales?**

Es recomendable crear un plan de concienciación del personal en temas de seguridad de la información y así hacer que todos los empleados participen de forma directa en el objetivo de conseguir una empresa más segura.

2) **¿Existe un plan de formación sobre seguridad de la información para operadores y administradores del sistema industrial?**

Los operadores y administradores de los sistemas deberían recibir formación especializada en seguridad de la información y en los riesgos que afectan a los dispositivos industriales.

3) **¿Se realiza algún tipo de asesoría de riesgo del personal antes de ser contratado?**

En sistemas de alto riesgo (centrales nucleares, sistemas militares, etc.) es recomendable realizar una comprobación de antecedentes y del perfil psicológico del personal antes de contratarlo.

4.3 CAPTURA DE INFORMACIÓN

4.3.1 DISEÑO DE LA RED

Objetivo

Determinar los activos informáticos e industriales y su topología de la red para verificar que los listados de activos y mapas de red suministrados por la empresa son correctos y están actualizados.

Metodología activa

Verificar los nodos de la red y su topología mediante escaneos con alguna de las siguientes herramientas: Ping, Cheops-NG, Nmap -sP

Determinar si existen redes inalámbricas bluetooth, WIFI, UHF, etc. mediante: Netstumbler

Metodología pasiva

Algunas alternativas disponibles:

- Capturar tráfico de la red durante un periodo de tiempo y determinar que nodos están activos para cada segmento de red. Herramientas: Wireshark , Snort.
- Otra opción es buscar en las tablas CAM de cada switch de la red.
- Buscar en las tablas de routing.
- Seguir el cableado de red en la búsqueda de nodos no documentados.

4.3.2 PROTOCOLOS DE RED

Objetivo

Estudiar los protocolos usados en la red y descubrir si existen vulnerabilidades en los protocolos.

Metodología activa

Probar distintas combinaciones de peticiones de protocolos industriales contra los dispositivos que los utilizan para ver el comportamiento ante tales peticiones. Este proceso puede ser muy lento por lo que se recomienda automatizarlo o en caso de haber poco tiempo en el proyecto no realizar esta parte de la auditoría.

Herramientas: fuzzers, OPC Security Tester.

Metodología pasiva

Solo se podrá determinar que protocolos se utilizan pero no se podrán realizar ataques contra los sistemas.

Herramientas: Wireshark

4.3.3 PUERTOS Y SERVICIOS

Objetivo

Determinar qué puertos están abiertos en cada nodo de la red, ver el servicio y la versión que está escuchando y que sistema operativo los ejecuta.

Metodología activa

Utilizar escáneres de puertos y de servicios para obtener información de los sistemas remotos.

Herramientas:

- Nmap
    - –sS –sV –s0: detección de puertos TCP, servicios y sistema operativo
    - –sS –sV –sR –s0: detección de puertos TCP, servicios y sistema operativo
    - –sU –sV –sR –s0: detección de puertos UDP, servicios, servicios RPC y sistema operativo
- Otras: amap, xprobe

Hay que tener en cuenta que el escaneo RPC frecuentemente tiene efectos secundarios negativos en algunos sistemas, algunas de las otras opciones y escaneos también pueden tenerlos aunque se suele dar con menos frecuencia.

Metodología pasiva

Capturar tráfico de la red durante un buen periodo de tiempo para determinar los puertos, inspeccionando el tráfico capturado con herramientas especializadas, como p0f, se puede llegar a saber los servicios y el sistema operativo de cada sistema conectado a la red.

Una alternativa es diseñar reglas para el detector de intrusos Snort para que detecte las versiones de los servicios de cada sistema que nos interese de la red.

Otra alternativa es ejecutar en cada máquina el comando "Netstat" para obtener los puertos y servicios que se escuchan y obtener mediante el registro de Windows o buscando en la configuración de cada servicio/programa la versión, así como la del sistema operativo.

Finalmente también es posible utilizar la metodología activa contra un sistema offline, de backup o virtualizado.

Herramientas:

- Captura de datos: Wireshark
- Análisis de la información: p0f, Wireshark, búsqueda de cadenas para determinar las versiones de los servicios.
- Snort: detección de los servicios mediante firmas especialmente diseñadas.
- Puertos por máquina: netstat -an (no resuelve direcciones IP ni puertos) solo interesa los que están en modo LISTEN. En algunos sistemas operativos también se puede obtener la versión del servicio que escucha.

4.3.4 VULNERABILIDADES

Objetivo

Determinar las vulnerabilidades existentes en los servicios descubiertos en el paso anterior.

Metodología activa

Escanear los sistemas con una herramienta especializada, primero se deberá escanear con una herramienta de uso general como Nessus para luego buscar información en los servicios que más nos interese con otras herramientas más específicas.

Herramientas:

- Escáner de vulnerabilidades: Nessus
- Escáner de vulnerabilidades en servidores y aplicaciones web: Nikto
- Servidores OPC: OPC Security Scanner
- Servidores/Clientes SCADA: ¿?
- PLC: ¿?

Metodología pasiva

Búscar en bases de datos de vulnerabilidades los servicios y versiones para determinar posibles vulnerabilidades.

También es posible utilizar la metodología activa contra un sistema offline, de backup o virtualizado.

Herramientas: Bases de datos de vulnerabilidades (ALTAIR-UPC, Mitre CVE, IBM-ISS X-Force, Secunia, etc).

4.3.5 VERIFICAR CONTRASEÑAS

Objetivo

Comprobar que los servicios que requieren autenticación son mínimamente resistentes y en caso de estar basados en contraseñas estas no son una palabra de diccionario o demasiado corta como para ser explotada en poco tiempo.

Metodología activa

Realizar ataques masivos contra los sistemas de autenticación de los sistemas poco críticos mediante múltiples peticiones activas, claves SNMP, acceso a routers, etc.

Herramientas: THC-Hydra, Brutus

Metodología pasiva

Obtener los ficheros de contraseñas y tratar de atacarlos en otro ordenador no conectado a la red.

Capturar hashes de contraseñas de la red y tratar de atacarlos offline.

Herramientas: John The Ripper, Cain & Abel

4.4 ANÁLISIS

4.4.1 INTRODUCCIÓN

Una vez en la fase anterior se han obtenido los datos del estado de las políticas, redes y sistemas se deberá hacer un análisis más o menos técnico y centrado en las vulnerabilidades sobre los dispositivos industriales.

En las siguientes secciones los puntos que más nos interesa auditar.

(Paul W. Oman, 2006)

4.4.2 PUNTOS DE ACCESO A LA RED INDUSTRIAL

Todo acceso físico o lógico a la red industrial deberá estar controlado.

En el caso de accesos lógicos la red industrial idealmente debería estar desconectada de redes inalámbricas, servidores no directamente relacionados con el proceso industrial, ordenadores

cliente, conexiones directas a Internet y otras redes que pudieran atacar a dispositivos tan sensibles como los industriales.

4.4.2.1 REDES PRIVADAS VIRTUALES (VPN)

Verificar que no existen túneles VPN o conexiones desde terceras empresas hasta las redes industriales ya que fácilmente si los sistemas de origen están comprometidos por un atacante o virus este va a pasar dentro de la red industrial.

4.4.2.2 ACCESO INALÁMBRICO

Verificar que no existen redes inalámbricas directamente relacionadas con los sistemas industriales.

En caso contrario:

- Verificar que el dispositivo utilizado no tiene vulnerabilidades en la base de datos especializada WirelessVE (http://www.wirelessve.org)
- Existe un firewall entre la red inalámbrica y el resto de la red para limitar los servicios que pueden transmitir por este medio.
- WIFI:
    - SSID está oculto
    - Se filtra a los clientes según dirección MAC
    - Se utiliza un mecanismo de cifrado y autenticación seguro[8]

[8] Preferiblemente WPA o WPA2 con certificados, en el caso de no poder usarlos la contraseña de acceso o "passfrase" debe ser suficientemente larga y no estar en un diccionario, ya que existen herramientas que pueden atacarla de una forma rápida probando del orden de 18.000 claves por segundo mediante tablas rainbow.(COWPATTY, 2006)

(wirelessdefence, 2006)

- Otras redes: En el caso de utilizar otro tipo de comunicación inalámbrica como UHF, GSM, Packet Radio, etc. Se debería verificar que los datos se cifran antes de ser transmitidos.

4.4.2.3 MODEMS

En el caso de usar módems para transmitir información desde subestaciones hasta un sistema SCADA se debería comprobar que:

- Los datos se cifran antes de ser transmitidos
- Existe algún mecanismo de autenticación que previene que un tercero pueda entrar en la red SCADA mediante una simple llamada telefónica con MODEM.

4.4.3 COMUNICACIÓN DE DATOS DENTRO DE LA RED INDUSTRIAL

Se recomienda que todo el tráfico sensible entre sistemas de la red industrial sea cifrado, esto es especialmente importante si los datos se envían hacia otras redes del sistema MES pero que no son industriales sino de servidores, p.ej. hacia el sistema ERP o servidores de trazabilidad.

4.5 ENTREGABLES

4.5.1 CONTRATO Y ACUERDO

Antes de empezar cualquier actividad de auditoría la empresa auditada debe firmar un documento por el que entienden los riesgos que conlleva realizar auditorías y eximen de cualquier culpa al auditor en caso de que hubiera algún incidente.

Además es posible que la empresa haga firmar al auditor un contrato conforme ha leído, entiende y acepta la política de seguridad de la empresa.

4.5.2 INFORME EJECUTIVO

Es un documento que utilizando lenguaje de alto nivel explica que pruebas se han realizado, los hallazgos y los siguientes pasos a realizar. No debe extenderse más de dos o tres páginas.

4.5.3 INFORME

Explicación de la metodología utilizada, en caso de que no se audite alguno de los apartados enumerados en las secciones 4.2 y 4.3 se debe justificar la razón.

Para cada tipo de vulnerabilidad encontrada se debe explicar en qué sentido afecta al negocio y como mitigar o reducir el riesgo que representa para el sistema pero de forma general. Siempre se adjuntarán los resultados de las herramientas de auditoría utilizadas en un soporte digital adjunto.

4.5.4 MAPA DE RED

Es un diagrama donde se sitúan los elementos más importantes de la infraestructura del sistema analizado con especial énfasis en los del sistema MES, de forma que un rápido vistazo uno se pueda hacer la idea del estado actual de la arquitectura de red.

Ejemplo:

ALMACÉN

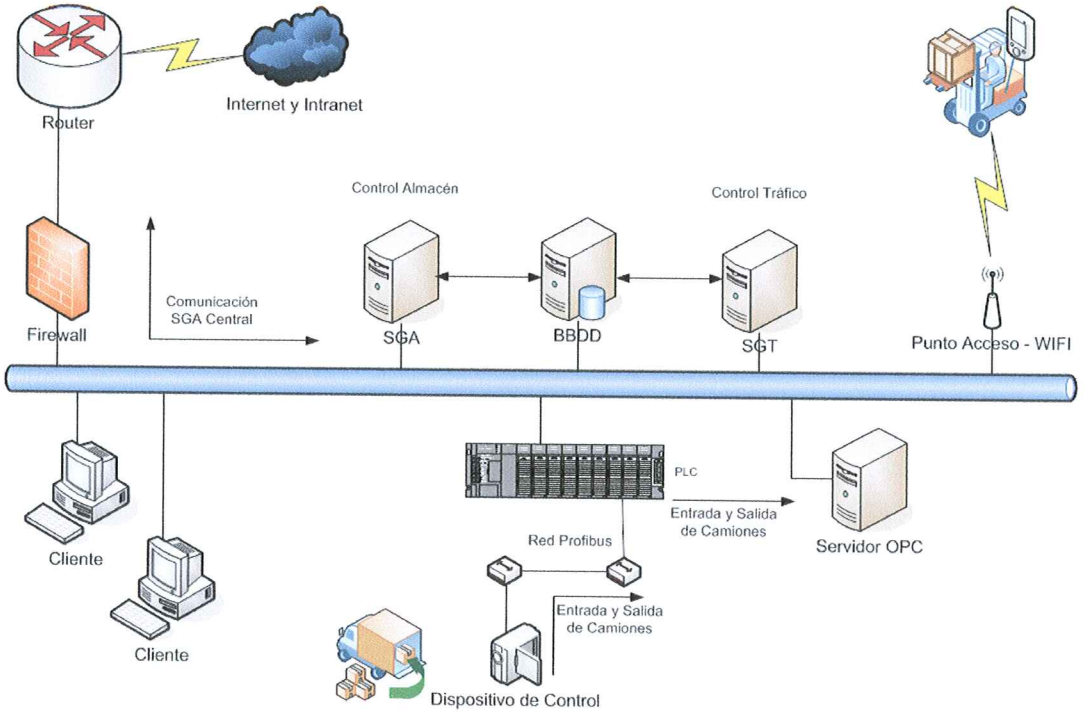

Ilustración 9. Esquema simplificado de la red de un almacén

4.5.5 LISTADO DE PUERTOS Y SERVICIOS POR MÁQUINA

Es un simple listado en una hoja de cálculo de los puertos y servicios encontrados en cada máquina, debería permitir ordenar los resultados por puerto, servicio y máquina.

Ejemplo:

Máquina	IP	Puerto	Tipo	Servicio	Información adicional	
PLC	x	139	TCP	netbios-ssn		
OPC	a	445	TCP	microsoft-ds		
BBDD	b	139	TCP	netbios-ssn		
BBDD	c	445	TCP	microsoft-ds		

4.5.6 LISTADO DE VULNERABILIDADES/CONTRASEÑA DÉBILES POR MÁQUINA

Es un simple listado en una hoja de cálculo de los puertos, vulnerabilidades y contraseñas débiles encontradas en cada máquina, debería permitir ordenar los resultados por puerto, vulnerabilidad y máquina.

Ejemplo:

Lugar	Máquina	IP	Puerto	Tipo	Servicio	Vulnerabilid	Exploit	Usuario/P	Riesgo	Salvaguarda
Oficinas	PLC	xxx	7	UDP	Echo	Servicio inne	N/A	-	1	Desactivar se
Oficinas	PLC	xxx	9	UDP	Discard	Servicio inne	N/A	-	1	Desactivar se
Oficinas	PLC	xxx	13	UDP	daytime	Servicio inne	N/A	-	1	Desactivar se
Oficinas	ERP	xxx	20	TCP	FTP	Tráfico no cif	N/A	-	1	Usar SFTP
Oficinas	ERP	xxx	21	TCP	FTP	Tráfico no cif	N/A	-	1	Usar SFTP
Oficinas	ERP	xxx	23	TCP	Telnet	Tráfico no cif	N/A	-	1	Usar SSH

4.5.7 ANÁLISIS DE LAS VULNERABILIDADES MÁS IMPORTANTES Y RECOMENDACIONES PARA MITIGAR/REDUCIR EL RIESGO

Para cada una de las vulnerabilidades más importantes (según la cantidad y la severidad pueden ser un número entre cinco y diez) se describe, se valora el riesgo que introduce al sistema, sistemas afectados y salvaguardas a aplicar.

Ejemplo del análisis de una vulnerabilidad:

Redes WIFI

ID: 1

Descripción: las redes WIFI de la empresa no están convenientemente protegidas ya que o no usan mecanismos de cifrado y autenticación o son débiles.

Riesgo asociado: 5

Sistemas afectados: todos los puntos de acceso en la fábrica de envasados.

Salvaguardas: aplicar mecanismos de cifrado y autenticación seguros, mínimo WPA con clave compartida (preshared-key) aunque sería recomendable WPA2 con protocolo AES y un servidor de autenticación RADIUS contra el que tuviera que autenticar cada máquina/usuario. Otros mecanismos que se recomienda activar son el filtrado por direcciones MAC, ocultación del SSID y disminuir la potencia de los puntos de acceso para reducir la cobertura.

4.5.8 PLAN DE ACTUACIÓN

Es una recomendación del auditor de que salvaguardas se deberían aplicar primero para mejorar la seguridad del sistema y especialmente de las vulnerabilidades que más riesgo introducen al sistema. Para cada recomendación se debe describir brevemente cuál es el trabajo a realizar, materiales necesarios y su dificultad.

Ejemplo:

Paso	Descripción	Operaciones	Material	Dificultad
1	Implantar Firewalls	Determinar reglas Escoger producto Implantar firewall	- - Firewall	Media Media Media
2	Implantar Detector de Intrusos	Determinar zonas de la red de interés Implantar IDS	TAP Máquina dedicada	Alta
3	Actualizaciones de seguridad	Actualizar Servidores Linux	-	Baja
5	Otras menos prioritarias	Concienciación/Formación Securización servidores Cifrado de la información crítica	-	-

	Test de intrusión	
	Implantación	sistemas
	detección intrusos	

4.6 CHECKLIST

En este apartado están enumeradas las pruebas a realizar por el auditor:

1) Estudio de documentación
   a) Activos y esquema de red
      i) ¿Existe un listado de activos?
      ii) ¿Existe un listado de activos críticos?
      iii) Esquemas de red
   b) Gestión de incidencias
      i) ¿Cómo reportan las incidencias los usuarios de la red?
      ii) ¿Existe algún procedimiento de gestión de incidencias?
      iii) ¿Se realizan resúmenes de los incidentes?
      iv) ¿Se revisan los resúmenes para ver qué tipo de incidentes ocurren más a menudo y analizar las causas?
      v) ¿Se guardan las evidencias de incidentes durante un periodo de al menos un año?
   c) Planes de contingencia
      i) Copias de seguridad
         (1) ¿Se realizan copias de seguridad? ¿De qué activos?
         (2) ¿Con que frecuencia se realizan copias de seguridad?
         (3) ¿Cómo se gestiona los medios físicos (discos, cintas, DVD, etc.) en los que se realiza las copias?
         (4) ¿Cada cuanto tiempo se verifica si las copias se han realizado correctamente? ¿Cómo?
      ii) Recuperación de desastres
         (1) ¿Existe un plan de recuperación ante desastres?

(2) ¿Los sistemas críticos están en alta disponibilidad?

(3) ¿Existen protecciones contra fallos del suministro eléctrico?

(4) ¿Está documentado el plan de recuperación de desastres?

d) Gestión de la seguridad

i) ¿Existe un responsable de seguridad?

e) Políticas de seguridad

i) ¿Cómo se clasifica la información?

ii) Control de acceso

iii) ¿Cómo se controlan los accesos físicos a las fábricas, lugares de trabajo y activos críticos de la empresa?

iv) ¿Cómo se registran los accesos?

v) ¿Están documentados los puntos de acceso a cada oficina/fábrica?

f) Gestión de la seguridad de la información

i) ¿Existen procedimientos de test antes de poner un sistema crítico en funcionamiento?

ii) ¿Se encuentran solo los puertos y servicios necesarios habilitados?

iii) ¿Existe un plan de actualizaciones de seguridad?

iv) ¿Prevención de software malicioso?

v) ¿Gestión de cuentas de usuario?

vi) Contraseñas por defecto

vii) ¿Gestión de contraseñas?

viii) ¿Se monitorizan los eventos de seguridad?

ix) ¿Existen sistemas de detección de intrusos? ¿Hay algún sensor en las redes industriales? ¿Están las firmas de ataques contra sistemas industriales instaladas?

x) ¿Qué se hace con el material informático una vez no se usa?

xi) ¿Se hacen auditorías de los sistemas conectados al perímetro de la red al menos una vez al año?

xii) ¿Se revisa y mantiene la documentación anualmente?

g) Control de cambios

i) ¿Se realiza control de cambios sobre el software instalado?

ii) ¿Se realiza control de cambios sobre el firmware instalado en dispositivos industriales?

iii) Concienciación y Formación

iv) ¿Existe definido un plan de concienciación sobre seguridad de la información en la empresa? ¿Se realiza este plan de concienciación pensando en operadores y administradores de los sistemas industriales?

v) ¿Existe un plan de formación sobre seguridad de la información para operadores y administradores del sistema industrial?

vi) ¿Se realiza algún tipo de asesoría de riesgo del personal antes de ser contratado?

2) captura de información

a) Diseño de la red

b) Protocolos de Red

c) Puertos y Servicios

d) Vulnerabilidades

e) Verificar contraseñas

5 APLICACIÓN DEL MARCO DE AUDITORÍA EN ENTORNO DE LABORATORIO

5.1 INTRODUCCIÓN

Tras haber desarrollado la metodología es el momento de probarla antes de ponerla en práctica en un entorno de producción para verificar que las pruebas técnicas recomendadas no son dañinas para los sistemas de información.

En el capitulo anterior se han dividido las técnicas de auditoría en dos grupos activas y pasivas en función de si inyectan paquetes en la red para obtener la información necesaria. Ahora solo se van a probar las técnicas de tipo activo para verificar si realmente son dañinas contra los sistemas de información y los de control industrial.

Con este fin se han realizado una batería de pruebas con las opciones más comunes del escáner de puertos Nmap y del escáner de vulnerabilidades Nessus[9].

Con este fin se ha utilizado el laboratorio de ESAII de la asignatura SIA, formado por los siguientes elementos:

- Router con NAT para la salida a Internet y comunicación con otras redes.
- Servidor proxy para controlar que sistemas externos pueden comunicar con el laboratorio y viceversa.
- Servidor de BBDD MySQL para almacenamiento de datos de aplicaciones.
- PC para la programación del PLC.
- PLC de la marca WAGO
- Conector Ethernet a RS-232 para conectar un lector de código de barras y una pantalla para presentar los códigos de barras.
    - En el puerto 1001 TCP está el lector de códigos de barras
    - En el puerto 1002 TCP está la pantalla que recibe los caracteres por una simple conexión serie
- Switch que conecta todos los elementos de la red local.

Durante todas las pruebas contra el PLC Wago se ejecutó el programa de simulación Arena y se verificó que los resultados de la simulación no varían. Para el dispositivo Lantronix se verificó que el lector de códigos de barras seguía funcionando. En todos se verificó que tras las pruebas la comunicación de red y los servicios (Web, FTP, Telnet, etc.) seguían funcionando.

---

[9] Las pruebas se realizaron desde la dirección IP 192.168.1.159

Los resultados de todas estas pruebas se encuentran en \Documentación\LabUPC\Auditoria\

5.2 MAPA DE RED

Ya existía un mapa de red pero se ha hecho otro para representar de forma simplificada los elementos a estudiar.

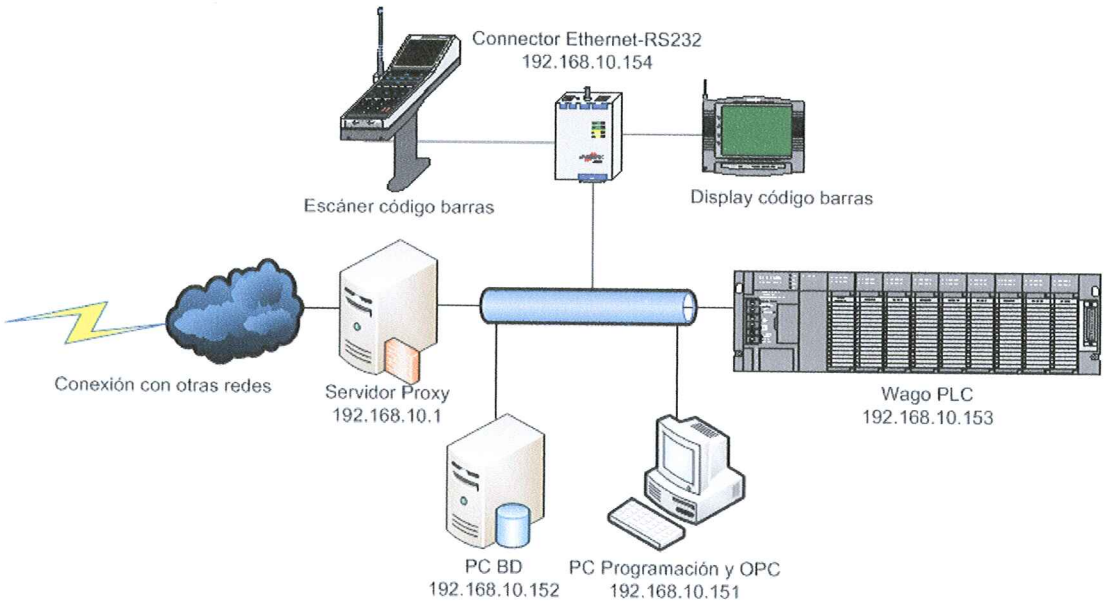

Ilustración 10. Mapa de la red laboratorio ESAII-SIA

5.3 ESCANEO DE LA RED

Se ha realizado un escaneo de la red para verificar que el mapa de red es exacto y no existen otras redes.

El escaneo se realizó con Nmap (Nmap –sP) y se descubrieron otras máquinas en la red:

- 192.168.10.104
- 192.168.10.107
- Y el rango de direcciones IP 192.168.10.201-210

Estas máquinas no se han incluido en el mapa ya que según el administrador de la red pertenecen a otros laboratorios y clases del departamento de ESAII. En un entorno real estos sistemas deberían estar segregados del resto mediante un router o firewall que impidiera el acceso a los dispositivos críticos como son el PLC y servidor BBDD y OPC. Como el entorno en el que se está trabajando es un laboratorio donde el PLC no trabaja con sistemas reales y los datos del servidor BBDD y OPC son simulados no es necesaria la segregación ya que lo que impera es la facilidad de uso para los alumnos.

5.4 ESCANEO DE PUERTOS

5.4.1 INTRODUCCIÓN

Se escanearon los sistemas más significativos del laboratorio para descubrir que puertos tienen abiertos y probar su resistencia contra este tipo de pruebas.

Las máquinas analizadas son:

- Servidor OPC
- Servidor BBDD
- PLC Wago
- Convertidor Lantronix

Las pruebas realizadas contra estos sistemas son:

- -sS: escaneo de puertos TCP mediante envío de paquetes con flag SYN
- -sV: detección de servicios en cada puerto
- -sR: detección de servicios RPC en cada puerto
- -sO: detección del sistema operativo
- -sU: escaneo de puertos UDP
- -T5: máxima velocidad de escaneo
- Combinación -sS y -sV

- Combinación -sS, -sV y -sO
- Combinación -sS, -sV, -sR y -sO

5.4.2 RESULTADOS

De los puertos y servicios reconocidos en estas pruebas se realizó un fichero Excel para facilidad a la hora de ver la información. El fichero se puede encontrar en \Documentación\LabUPC\Auditoria\puertosServicios

A destacar que los servidores BBDD y OPC tienen muy pocos puertos abiertos lo que indica que posiblemente usen algún firewall.

Una de las sorpresas se encontró al ver que los servicios Web y FTP del PLC Wago se bloquean al realizar un escaneo UDP sin que se ilumine ninguno de sus LED, y sin que la simulación de I/O de la planta se vea interrumpida funcionando.

5.5 ESCANEO DE VULNERABILIDADES

5.5.1 INTRODUCCIÓN

Para realizar las pruebas de escaneo de vulnerabilidades se utilizó la herramienta Nessus.

Las máquinas analizadas son:

- Servidor OPC
- Servidor BBDD
- PLC Wago
- Convertidor Lantronix

Las pruebas realizadas contra estos sistemas son:

- Escaneo con todos los plugins activados excepto denegación de servicio
- Escaneo con solo los plugins de denegación de servicio activados

En esta ocasión se desestimó hacer las pruebas de denegación de servicio contra los servidores de BBDD y OPC ya que existe una vulnerabilidad en ambos que permite la ejecución de código remota.

5.5.2 RESULTADOS

Servidores OPC y BBDD

Los servidores OPC como BBDD están basados en Microsoft Windows XP y tienen una vulnerabilidad en el servicio de compartición de ficheros (puerto 445 TCP) que podría permitir a un atacante remoto ejecutar código (CVE-2006-1314, CVE-2006-1315). Esto ilustra que aunque estos servidores se han actualizado al menos una vez en el año 2006 es necesario realizar actualizaciones periódicas, lo que en ciertos entornos puede ser complicado.

En estos servidores no se han realizado más pruebas ya que no son relevantes para el estudio.

Lantronix

Las pruebas realizadas con el software de análisis de vulnerabilidades detectaron varias vulnerabilidades:

Vulnerabilidad	Descripción	Riesgo
Servidor TFTP	El servidor TFTP permite conectar y obtener la configuración del sistema	3
Servidor TFTP vulnerable a ciertos paquetes UDP	Es possible bloquear el servidor TFTP remoto mediante paquetes UDP especialmente largos (CVE-2002-0813, CVE-2003-0380)	2
SNMP con clave por defecto	La clave de lectura del servidor SNMP es "public" lo que permite obtener información remotamente	2

Se ha visto que existen algunas vulnerabilidades no obstante se ha inspeccionado manualmente otros puertos para ver si se detectan otras vulnerabilidades:

Vulnerabilidad	Descripción	Riesgo
Servidor Telnet sin contraseña	Se ha descubierto un servidor Telnet en el puerto 9999 sin contraseña cambiar la configuración del sistema. Como se demuestra en el cuadro de texto más abajo.	5
Servidor Web sin contraseña	Se ha descubierto un servidor Web sin contraseña que permite ver la configuración y cambiar algunos parámetros. Como se demuestra en la Ilustración 11	4
El contenido de la pantalla cambia	Al escanear el puerto 1002 cambia el contenido de la pantalla con texto enviado por el escáner (Ilustración 12). En este escenario no tiene mayor importancia no obstante si hubiera otro dispositivo mecánico hubiera sido posible que este se moviera de forma no predecible.	4

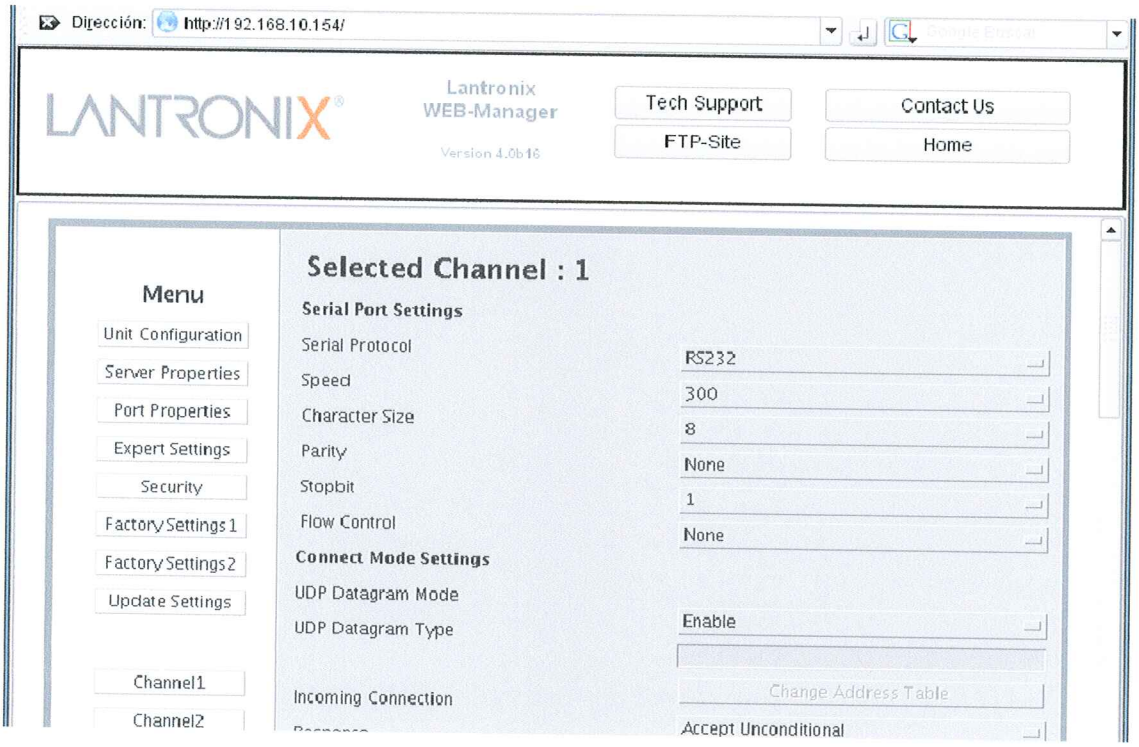

Ilustración 11. Servidor Web permite modificar configuración de Lantronix

Ilustración 12. Cambio del texto de la pantalla de código de barras por texto de los mensajes enviados por el escáner

```
cdoce@linux-home:~> telnet 192.168.10.154 9999
Trying 192.168.10.154...
Connected to 192.168.10.154.
Escape character is '^]'.

Serial Number 6318510  MAC address 00204A63484E
Software version 05.2 (030722) U200
```

PLC Wago

Las pruebas realizadas con el software de análisis de vulnerabilidades detectaron varias vulnerabilidades:

Vulnerabilidad	Descripción	Riesgo
Tráfico UDP	Es posible bloquear la pila IP mediante un ataque "Nestea" (CVE-1999-0257) que causa una Denegación de Servicio. En la unidad de comunicación del PLC cuatro de los LEDs se iluminan de color rojo y parpadean (ver Ilustración 13) lo que significa un fatal error y necesita un reset.	4