|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CÓDIGO CERTIFICADO:** | | | FC9-09/2020/4730CPP | | | | **CODIGO INTERNO CAM:** | | FC/20/6704 | |
| **ACCION:** | 6 | | | **GRUPO** | | 100 | | | | |
| **NOMBRE CERTIFICADO:** | | | | IFCT0109- SEGURIDAD INFORMÁTICA | | | | | | |
| **MÓDULO:** | | MF0487\_3 AUDITORIA DE SEGURIDAD INFORMÁTICA | | | | | | | | |
| **CENTRO DE FORMACIÓN/ENTIDAD:** | | | | | Core Networks, SL | | | **CENSO:** | | 27.593 |

PRUEBA PRÁCTICA

|  |  |  |
| --- | --- | --- |
| Nombre y apellidos: DIEGO ARMANDO SIMBAÑA | | Calificación |
| NIF 02562559Z | Fecha: 25/06/2021 |
| Firma: | |

**EXAMEN PRÁCTICO**

1. Denominación de la prueba práctica

Auditar redes de comunicación y sistemas informáticos

1. Objetivos específicos a los que responde la practica (capacidades)

Objetivos específicos a los que responde la practica (capacidades)

Analizar y seleccionar las herramientas de auditoría y detección de vulnerabilidades del sistema informático implantando aquellas que se adecúen a las especificaciones de seguridad informática.

Aplicar procedimientos relativos al cumplimiento de la normativa legal vigente.

Planificar y aplicar medidas de seguridad para garantizar la integridad del sistema informático y de los puntos de entrada y salida de la red departamental.

1. Definición de la práctica:

* Descripción:
* La prueba consistirá en realizar un supuesto en el que se usen las herramientas de auditoría y detección de vulnerabilidades de un sistema informático, aplicar procedimientos relativos al cumplimiento de la normativa legal vigente y planificar y aplicar medidas de seguridad para garantizar la integridad de un sistema informático y la red en la que se encuentra.
* Medios para su realización:Un ordenador personal y software necesario para la realización de la práctica
* Instrucciones:
* Parte 1: Herramientas de auditoría y detección de vulnerabilidades
* Parte 2: Procedimientos de la normativa legal vigente
* Parte 3: Medidas de seguridad para garantizar la integridad
* Duración:4 horas

1. Evaluación de la práctica (Lista de verificación u Hoja de evaluación)

* Resultados que hay que demostrar (criterios de evaluación). Se refieren a las actividades de la práctica a evaluar.
* Explicar las diferencias entre vulnerabilidades y amenazas.
* Enunciar las características de los principales tipos de vulnerabilidades y programas maliciosos existentes, describiendo sus particularidades.
* Describir el funcionamiento de una herramienta de análisis de vulnerabilidades, indicando las principales técnicas empleadas y la fiabilidad de las mismas.
* Seleccionar la herramienta de auditoría de seguridad más adecuada en función del servidor o red y los requisitos de seguridad.
* Explicar la normativa legal vigente (autonómica, nacional, europea e internacional) aplicable a datos de carácter personal.
* Exponer los trámites legales que deben cumplir los ficheros con datos de carácter personal, teniendo en cuenta la calidad de los mismos.
* Describir los niveles de seguridad establecidos en la normativa legal vigente asociándolos a los requisitos exigidos.
* Identificar las fases del análisis de riesgos, describiendo el objetivo de cada una de ellas.
* Describir los términos asociados al análisis de riesgos (amenaza, vulnerabilidad, impacto y contramedidas), estableciendo la relación existente entre ellos.
* Describir las técnicas de análisis de redes, explicando los criterios de selección.
* Describir las topologías de cortafuegos de red comunes, indicando sus funcionalidades principales
* La importancia de cada actividad con respecto al total.
* No prima ninguna actividad con respecto a las demás, ya que si no se hacen las actividades, según el orden del ejercicio no se podrá avanzar para la realización de la siguiente parte.
* Indicadores de logro. Son los indicadores con los que se evalúa la práctica (autonomía, resultados, proceso, tiempo, seguridad, limpieza…).
* Comprobación de resultados
* Escalas de desempeño. Son las escalas de puntuación de cada indicador.
* Herramientas de auditoría y detección de vulnerabilidades (3,5 puntos)
* Procedimientos de la normativa legal vigente (3 puntos)
* Medidas de seguridad para garantizar la integridad (3,5 puntos)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Resultados parciales a comprobar** | **Indicadores de logro** | **Escalas** | | | | | **Puntuación máxima** | | **Puntuación obtenida** |
| Herramientas de auditoría y detección de vulnerabilidades | Uso de las herramientas de auditoría y detección de vulnerabilidades | No lo realiza de forma correcta | | 0 | | 3.5 | |  | |
| Sí lo realiza de forma correcta | | 3.5 | |
| Procedimientos de la normativa legal vigente | Aplica los procedimientos de la normativa legal vigente | No lo realiza de forma correcta | | 0 | | 3 | |  | |
| Sí lo realiza de forma correcta | | 3 | |
| Medidas de seguridad para garantizar la integridad | Configura las medidas de seguridad para garantizar la integridad | No lo realiza de forma correcta | | 0 | | 3.5 | |  | |
| Sí lo realiza de forma correcta | | 3.5 | |
| **Valor mínimo exigible: 5** | | | **Valor máximo / Valor obtenido** | | **10** | |  | |  |

**EXAMEN PRÁCTICO**

Una PYME dispone de un servidor donde centraliza parte de los servicios de la empresa:

* Se dispone de un programa de gestión de nóminas
* Programa de stock de productos que se comunica con el stock de los proveedores

Los servicios que van a realizar en la empresa, requieren de la automatización de ficheros de datos de clientes, proveedores e información sobre nóminas de los empleados

Sobre este supuesto se van a realizar 3 tareas:

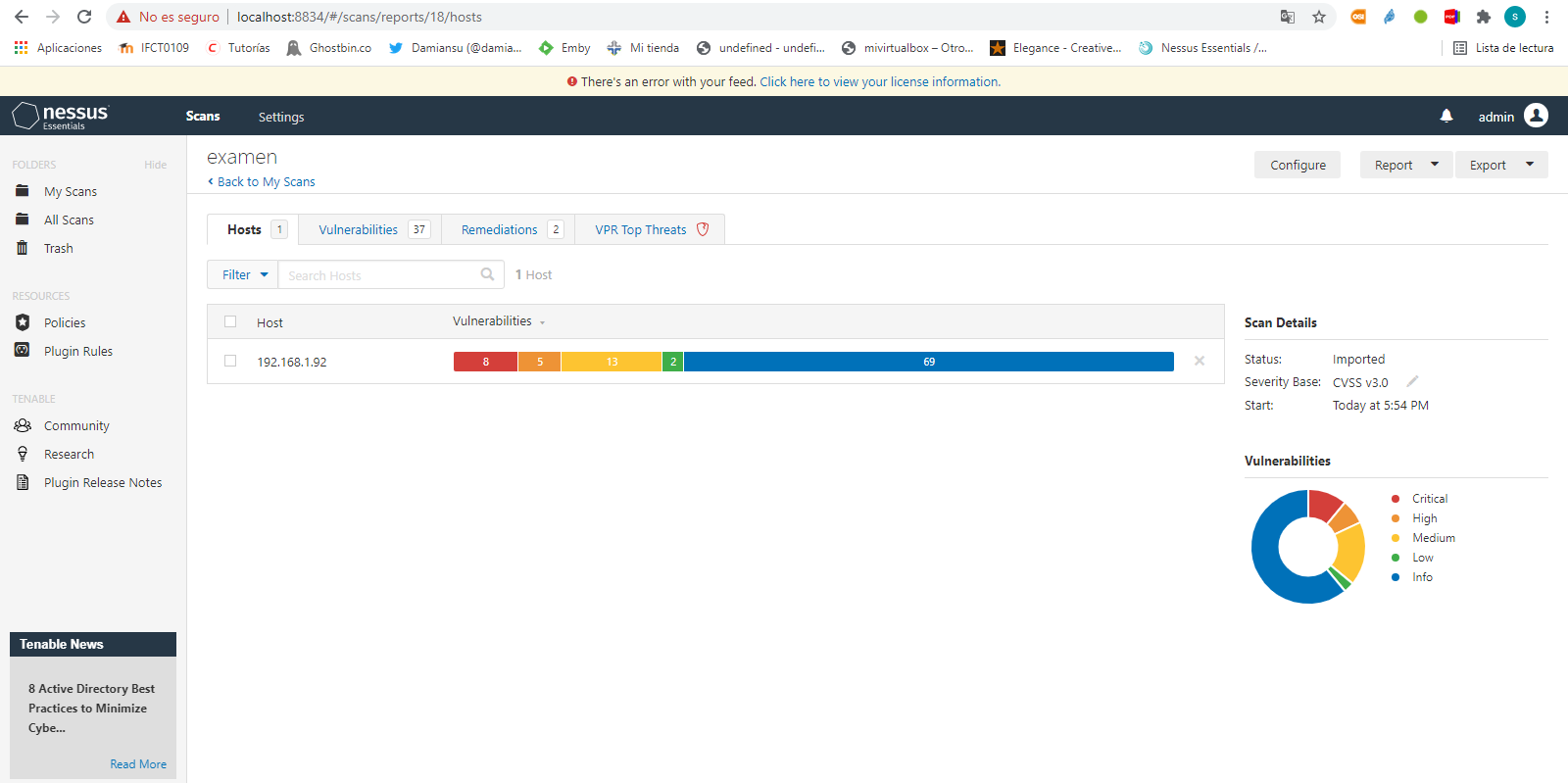
1. Auditoría y detección de vulnerabilidades
2. Procedimientos de la normativa legal vigente
3. Medidas de seguridad para garantizar la integridad

**Herramientas de auditoría y detección de vulnerabilidades**

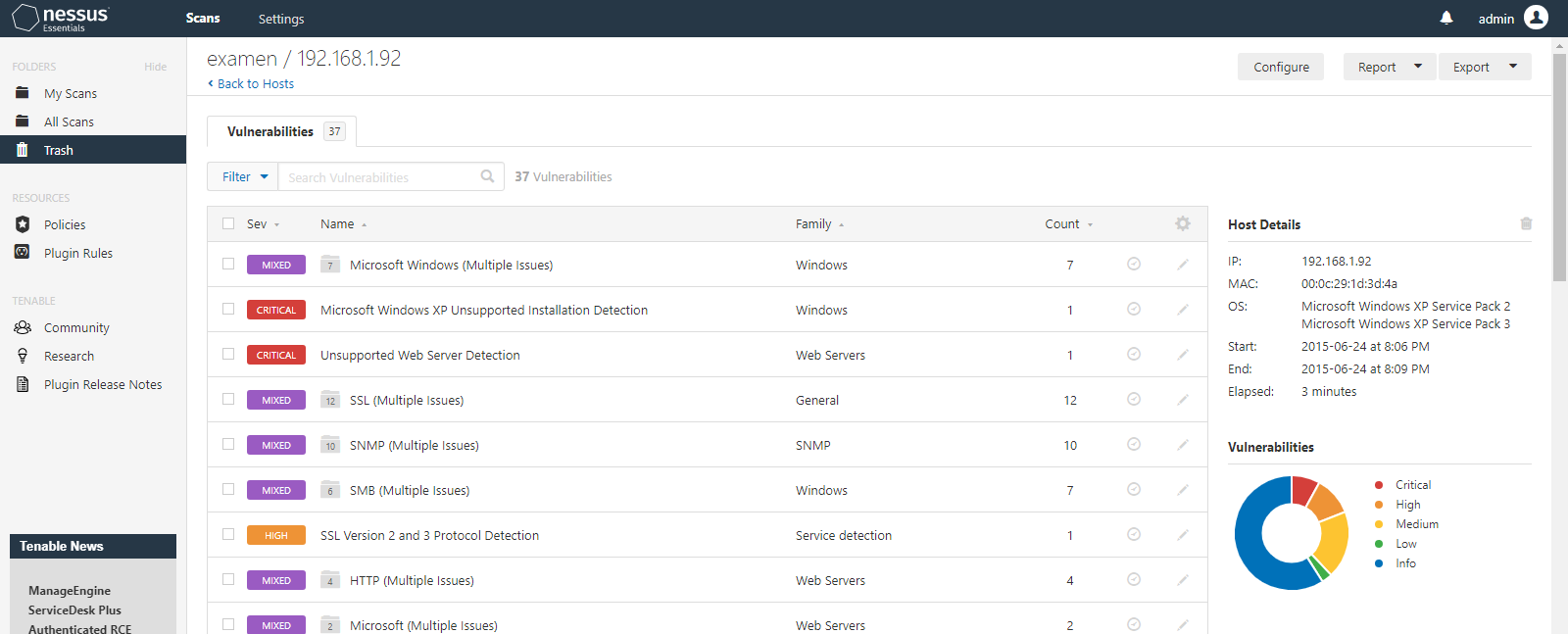
1. El responsable de la empresa nos pide consejo para poder establecer la seguridad necesaria que debería de tener el servidor. Para ello, realiza un resumen sobre la posible fortificación del servidor, incluyendo medidas de salvaguarda software y hardware y el porqué de esas medidas.

- Fortificar el servidor con usuarios autenticados y con permisos dependiendo del que tenga cada usuario, instalar un firewall físico para toda la red local, configurar e instalar solo los servicios que se vayan a utilizar o necesitar, copias de seguridad, actualizaciones regulares de los sistemas operativos, control de acceso al servidor y equipos clientes, buenas prácticas de usabilidad de aplicaciones y de la información, instalación de programas originales, antivirus , malwares, realización de auditorias de seguridad periódica, escáner de vulnerabilidades, etc.

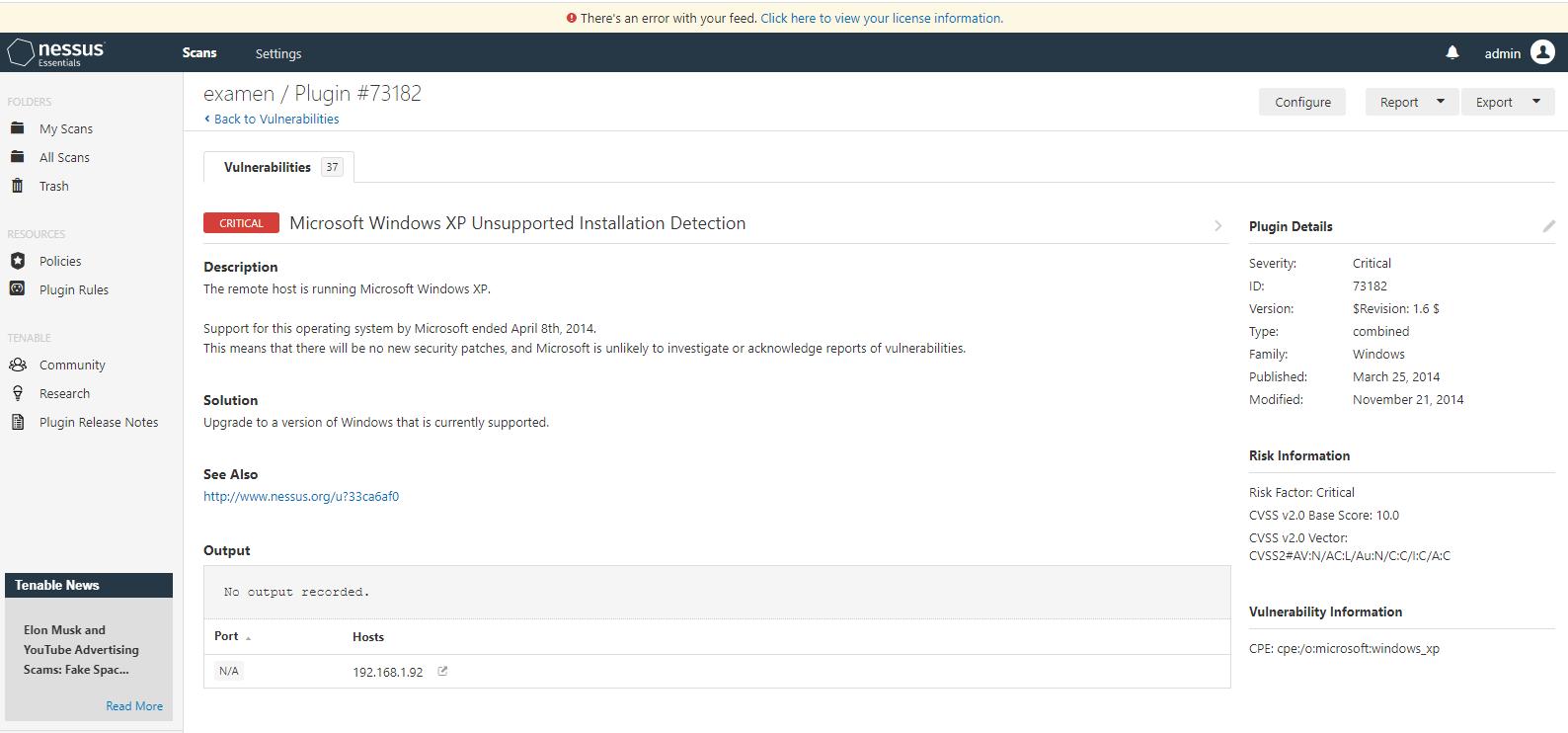
1. Tenemos acceso al servidor. Realiza un escáner de vulnerabilidades sobre el equipo.

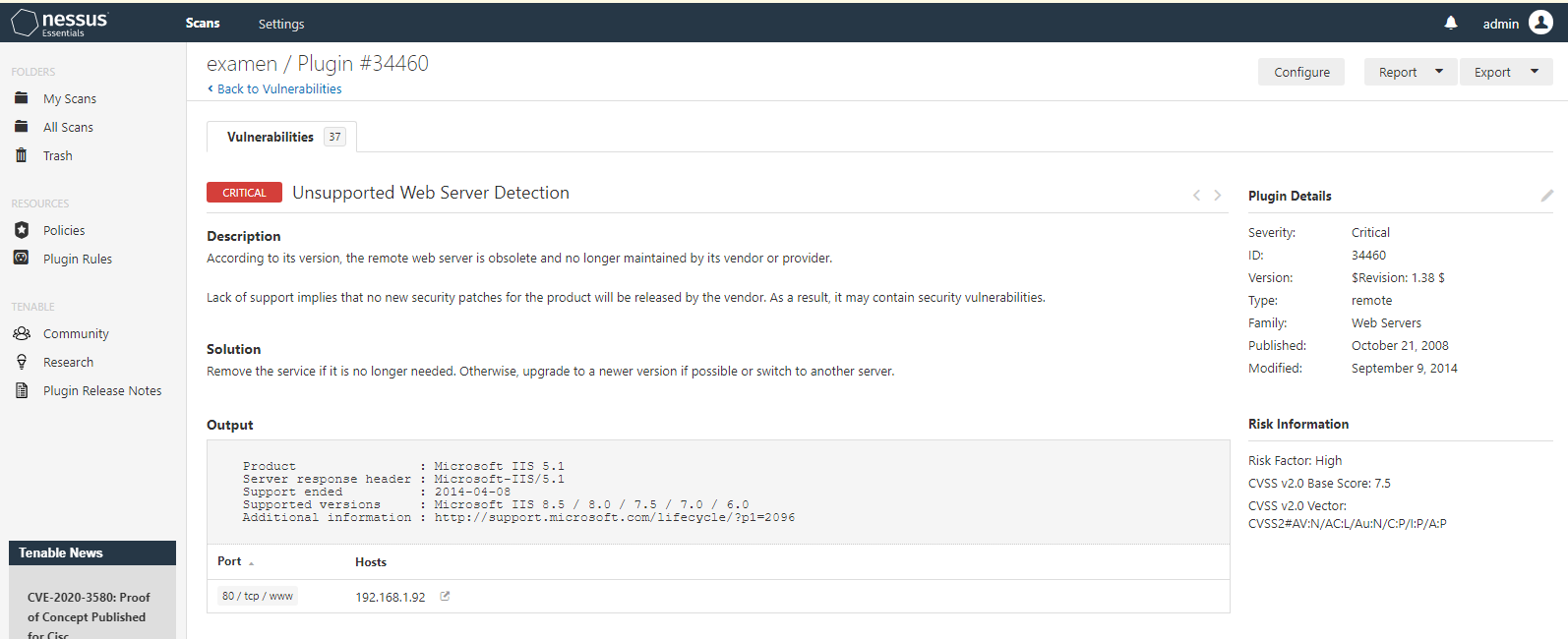
Se realiza un escáner de vulnerabilidades con la herramienta Nessus.

1. Identifica las vulnerabilidades más importantes y comenta las soluciones que propone la herramientas de análisis de vulnerabilidades.



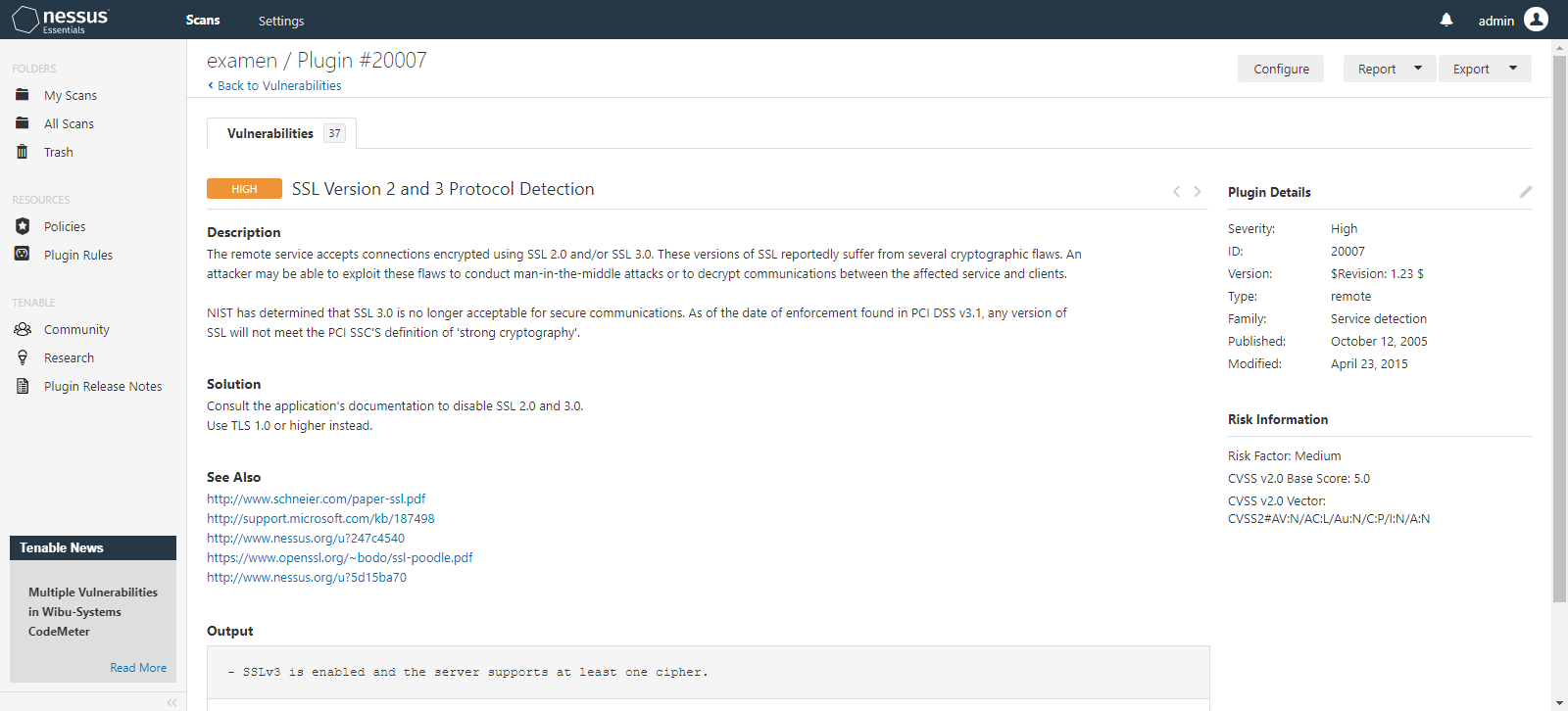
Las vulnerabilidades mas importantes que nos encontramos son las criticas.

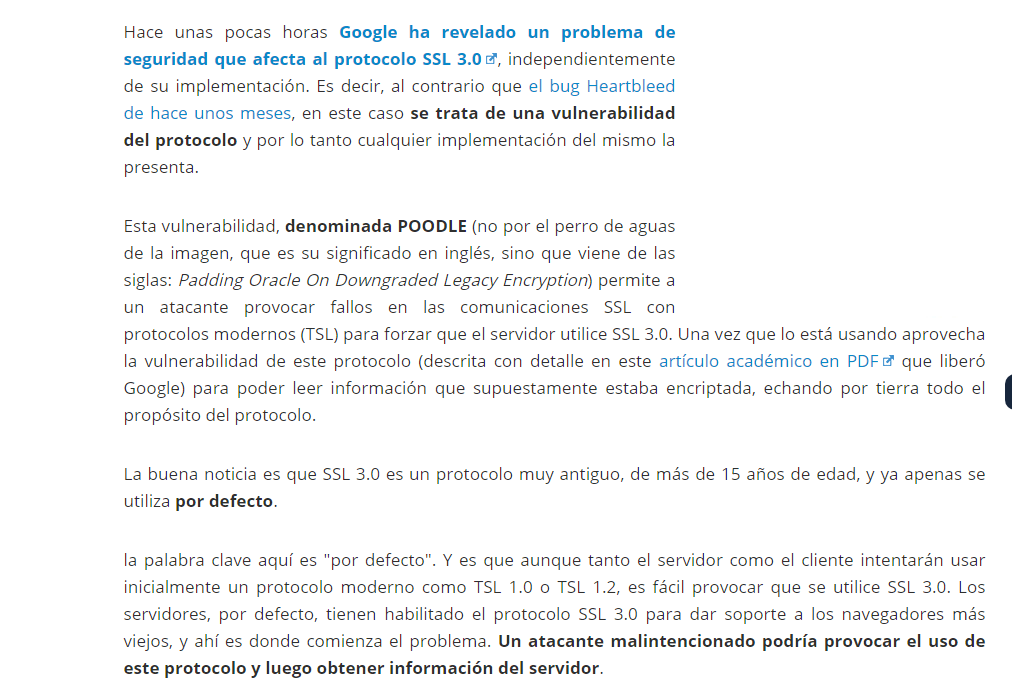
Un error muy crítico del escáner de vulnerabilidades que nos presentan es la presencia de un Windows XP, el cual ya no tiene soporte por parte del fabricante luego nos podemos encontrar con vulnerabilidades que no han sido parchadas o corregidas. Por tanto, lo recomendado sería actualizar el sistema operativo a uno mas actual y con soporte.



Error critico con un servidor web que tampoco tiene soporte. La solución es eliminar este servicio o actualizar a una nueva versión.

1. Realizar una comprobación de alguna vulnerabilidad que se ha detectado, para poder mostrarla al responsable de la empresa.





https://www.campusmvp.es/recursos/post/Como-solucionar-la-vulnerabilidad-de-SSL-30-POODLE-en-Internet-Information-Server-(IIS).aspx

1. Redactar el informe de auditoría, reflejando las irregularidades detectadas, y las sugerencias para su regularización en el caso de ese equipo.

(No sugerencias generalizadas como en el apartado 1, algo específico)

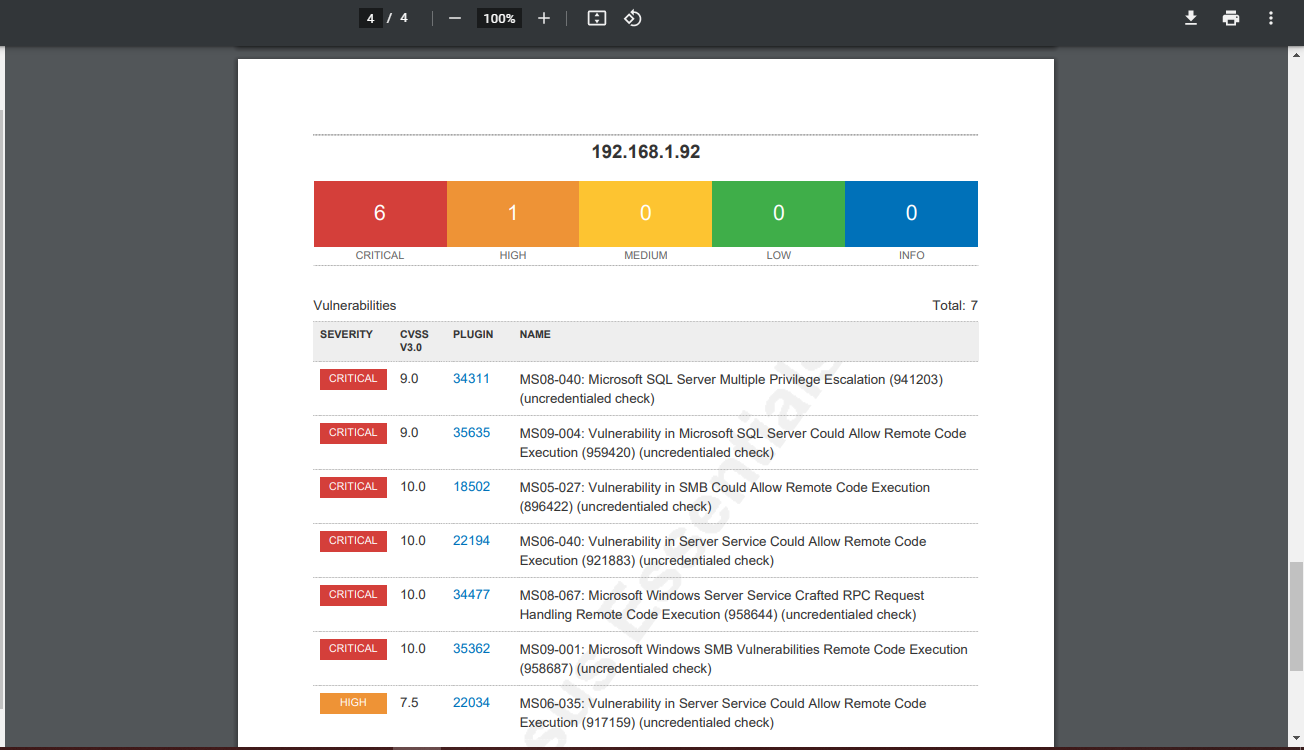
- Actualización del sistema operativo cliente.

- Desinstalar servicios que no se estén utilizando.

- Actualización del sistema operativo servidor con periodicidad (parches de seguridad).

- Utilización del TSL.

- Utilización de SMB mediante autenticación del servidor.



Informe generado automáticamente a través de Nessus.

**Procedimientos de la normativa legal vigente**

La estructura de los ficheros que utiliza la empresa son las siguientes:

* Datos\_clientes.csv

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NOMBRE | APELLIDOS | DNI | DOMICLIO | CUENTA\_BANCARIA | FOTO | … |

* Datos\_proveedores.csv

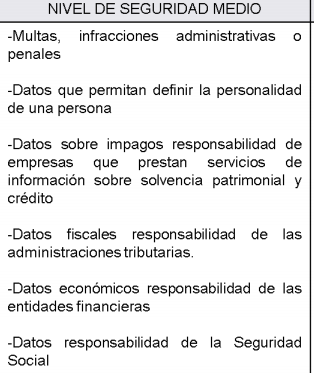
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NOMBRE | APELLIDOS | CIF | RAZÓN\_SOCIAL | CUENTA\_BANCARIA | INFRACCIONES\_ADMINISTRATIVAS | … |

* Empleados.csv

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| NOMBRE | APELLIDOS | CIF | RAZÓN\_SOCIAL | CUENTA\_BANCARIA | MOTIVO\_DE\_BAJA | … |

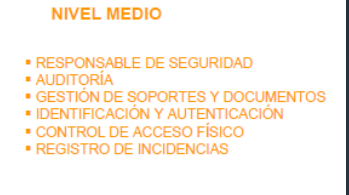
1. ¿Qué nivel de seguridad debería tener cada uno de los ficheros y por qué?

* Datos\_clientes.csv: este fichero al tener datos muy relevantes de los usuarios debería tener un nivel de seguridad medio. Ya que:
* Datos\_proveedores.csv: también debería tener un nivel medio
* Empleados.csv: nivel medio.



1. ¿Qué medidas de seguridad implementarías partiendo del supuesto que es un sistema automatizado y el nivel de seguridad de todos los ficheros?

Se debería implementar esto:



1. El responsable del fichero te dice que todos los ficheros tienen un nivel de seguridad MEDIO. Si crees que no es correcto, que infracciones se les podría atribuir.

Sanciones Graves: multa de 40.001 € a 300.000 €

Se pueden considerar como graves:

Tratar datos de menores de edad sin recabar su consentimiento, cuando tenga edad para ello, o de sus padres o tutores.

No acreditar esfuerzos razonables para verificar la validez del consentimiento del menor o de sus padres o tutores.

No atender de forma reiterada u obstaculizar la solicitud de los derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad de los datos en los tratamientos en los que no se requiere la identificación del afectado.

No adoptar las medidas técnicas y organizativas apropiadas para aplicar la protección de datos desde el diseño.

No adoptar las medidas técnicas y organizativas que garanticen el tratamiento de los datos personales necesarios para cada uno de los fines específicos del tratamiento.

No adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos.

Brechas de seguridad ocurridas por no haber adoptado las medidas adecuadas de seguridad.

No designar un representante del responsable o encargado del tratamiento no establecido en territorio de la UE, de acuerdo al artículo 27 del RGPD.

No atender las solicitudes de las agencias de protección de datos.

Contratar un encargado del tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas necesarias, de acuerdo al Capítulo IV del RGPD.

Encargar el tratamiento de datos a un tercero sin el debido contrato.

Contratación por parte del encargado del tratamiento de otros encargados sin contar con la autorización del responsable.

Infracción de lo dispuesto en el artículo 28.10 del RGPD respeto a la determinación de los fines y los medios de tratamiento por parte del encargado.

No disponer del registro de actividades.

No cooperar con la AEPD u otras autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de la LOPDGDD.

El tratamiento de datos personales sin cumplir con lo recogido en el artículo 28 de la LOPDGDD.

Incumplir el deber de informar de las violaciones de seguridad por parte del encargado del tratamiento al responsable.

No informar de las violaciones de seguridad a la AEPD, según el artículo 33 del RGPD.

No informar al afectado de una violación de seguridad de datos personales.

Llevar a cabo el tratamiento de datos sin realizar una evaluación de impacto cuando esta es exigible.

Tratar datos personales sin haber realizado consulta previa a la AEPD cuando esta sea obligatoria.

No designar a un delegado de protección de datos cuando sea obligatorio.

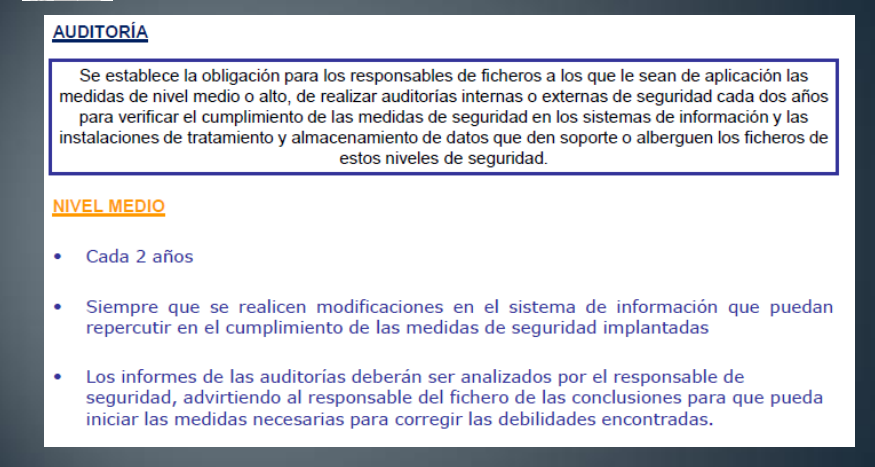
No permitir que el delegado de protección de datos pueda cumplir con sus funciones.

Utilizar sellos o certificaciones en materia de protección de datos que no hayan sido otorgados por una entidad de certificación acreditada o estén expirados.

Incumplimientos de los organismos de certificación recogidos en el artículo 73, letras z, aa, ab y ac de la LOPDGDD.

La multa de estas infracciones se encuentra entre 40.001 € y 300.000 €.

1. Elaborar el informe correspondiente a los ficheros de carácter personal, indicando las definiciones encontradas y las correcciones pertinentes.



**Medidas de seguridad para garantizar la integridad**

Realizar un análisis de riesgo usando la tabla ACIDA sobre **uno** de los siguientes activos u otro que consideres:

* Aplicación
* Nóminas de los empleados
* Stock del almacén
* Stock de los proveedores
* …

