TAREA 01

HACKING ÉTICO, CONCEPTOS Y HERRAMIENTAS PARA DETECCIÓN DE VULNERABILIDADES

HACKING ÉTICO

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

PAUTAS DE SEGURIDAD INFORMÁTICA
Diseñar un plan de auditoría para este primer trimestre, el presupuesto asignado sólo permite que se realicen un máximo de 5 auditorías.
El equipo tiene que diseñar el tipo de auditorías que se realizará teniendo en cuenta las siguientes premisas:

Disponen de 20 activos expuestos a internet (servidores web, servidores de correo, acceso VPN)
De estos 20 activos, 3 de ellos se consideran críticos para el negocio
Les interesa realizar una primera revisión de la red interna.

Apartado 1: Diseñar el plan de auditoría
Teniendo en cuenta las premisas y restricciones indicadas por teresa diseñar el plan de auditoría.
Como mínimo has de plantear y explicar las siguientes cuestiones y razonar correctamente tu elección:
Indicar que tipo de auditorías realizarías y sobre los activos, necesitas elaborar tu respuesta con las siguientes premisas:

- **Justificar la elección de cada auditoría elegida.**
- **Justificar los activos incluídos en cada auditoría.**
- **Indicar en cada caso el tipo de auditoría dependiendo del enfoque, orígen e información proporcionada y justifica cada caso**
- **Indica el objetivo que quieres conseguir con la elección de cada tipo de auditoría.**

Para la realización de este apartado puedes usar la siguiente tabla como referencia:

Auditoría	Justificación Auditoría	Activo(s) y justificación	Enfoque (manual, automática, etc)	Origen (interna o externa)	Información proporcionada (tipo de caja)	Objetivo
Externa	Evaluar vulnerabilidades externas	Web, correo, VPN	Automático y manual	Externa	Caja negra	Detectar brechas críticas en activos expuestos en Internet
Interna	Identificar riesgos internos con acceso básico	Red interna	Automático y manual	Interna	Caja gris	Detectar configuraciones débiles y accesos no autorizados a la red
Servidores críticos	Asegurar configuración segura de servidores	Web, correo, VPN	Manual	Interna	Caja blanca	Corregir configuraciones incorrectas o contraseñas débiles
VPN	Proteger accesos remotos a la red (VPN)	VPN	Automático y manual	Interna	Caja blanca	Revisar cifrado y configuración VPN, evitar accesos no autorizados
Políticas seguridad	Revisión políticas de seguridad	Roles/permisos y políticas	Manuales	Interna	Caja blanca	Asegurar que las configuraciones/políticas estén bien implementadas

Comenzando con un análisis a grandes rasgos de este caso, la empresa cuenta con 20 activos (web, correo y VPN), 3 de ellos críticos. Debido a los activos y el presupuesto para 5 auditorías, esta empresa tendrá un tamaño pequeño o mediano en la que habrá implantadas medidas o utilizado recursos de seguridad básicas/limitadas, lo que significa que pueda haber amenazas tanto internas como externas.
En las auditorías tendremos el objetivo de detectar y minimizar las vulnerabilidades existentes, priorizando los activos más críticos.

1- Auditoría Externa:
Esta primera auditoría nos servirá para identificar las vulnerabilidades más peligrosas que un atacante, desde fuera, pueda encontrar sin tener información sobre la empresa. Los activos elegidos como objetivo serán los 3 recursos esenciales ya que son los elementos más importantes y con más riesgo para el funcionamiento de la empresa y una posible brecha podría causar un grave impacto.
Nos centraremos en los activos críticos porque al ser esenciales para el negocio cualquier vulnerabilidad podría causar un serio problema (servidor web, correo y VPN).
Al ser una empresa con un nivel de seguridad bajo, empezaremos con un enfoque automático para hacernos una idea e identificar el mayor número de posibles vulnerabilidades de lo que está en la red (utilizando herramientas como nmap o nessus/openvas). Una vez hayamos identificado las debilidades haremos pruebas más concretas de manera manual para explotarlas.
El origen será externo, ajeno a la infraestructura de la empresa para descubrir las vulnerabilidades en los activos que la compañía tiene expuestos en internet, intentando robar información.
Todas las pruebas las llevaremos a cabo sin tener ningún tipo de información sobre la infraestructura a auditar (caja negra) para simular un ataque real desde el exterior.
Como resumen, simulamos un ataque con el objetivo de encontrar las vulnerabilidades que podrían ser explotadas por un atacante externo sobre los activos críticos.

2- Auditoría Interna:
En caso de que un atacante consiguiera el acceso a la red, vamos a evaluar los riesgos internos que podría explotar. Para ello debemos identificar configuraciones débiles, accesos no autorizados y reconocer posibles movimientos que el atacante pudiese hacer dentro de la red para acceder a otros recursos.
Los activos seleccionados serán la red interna y los dispositivos conectados a ella, ya que una brecha en dichos puntos podría facilitar un mayor impacto.
Esta vez también recurriremos a pruebas automáticas para hacer un escaneo de la red utilizando herramientas como wireshark o arp y después de forma manual buscaremos configuraciones y reglas de acceso vulnerables.
El origen del ataque será interno, desde dentro de la red, por lo que por lo que deberemos tener acceso a la red, tendrá un enfoque de caja gris en la que la empresa nos deberá facilitar un acceso básico (no tendremos credenciales con privilegios).
El objetivo será detectar las vulnerabilidades internas en las configuraciones que pueda encontrar un atacante con acceso básico sobre la red para fortalecer la seguridad interna.

3- Auditoría a los servidores críticos:
Debemos garantizar que los activos más importantes de la empresa estén configurados de la forma más segura posible, una mala configuración da lugar a una vulnerabilidad. Un servidor con una mala configuración o débil puede comprometer las operaciones y las contraseñas.
Los activos elegidos son los tres servidores críticos (Servidor web, correo y VPN) ya que es fundamental que funcionen y estén protegidos para evitar ataques.
Para detectar vulnerabilidades que requieren un estudio minucioso utilizaremos pruebas manuales para la revisión de las contraseñas para acceder a los recursos, los servicios que están más expuestos y si sus versiones están actualizadas.
La auditoría será de origen interno porque necesitamos estar dentro de la red y los recursos y utilizaremos un enfoque de caja blanca teniendo un perfil administrador para hacer la evaluación lo más completa posible.
En esta auditoría debemos estudiar y corregir configuraciones incorrectas en los servidores, así como contraseñas sencillas o recursos desactualizados haciendo un análisis en profundidad con un enfoque de caja blanca.

4- Auditoría de VPN:
A continuación evaluaremos la seguridad de la conexión VPN al ser un acceso a la red interna, una vulnerabilidad podría permitir el acceso a los atacantes comprometiendo la información. Es importante proteger este servicio ante accesos no permitidos, por ello revisaremos la configuración y protegeremos dichas comunicaciones.
El activo elegido será el servidor VPN, como sirve para conectar usuarios externos con la red interna, significa que es un punto de entrada crítico y debemos centrarnos en ello.
Haremos un enfoque combinando pruebas automáticas con manuales para identificar qué cifrados pueden ser débiles y hacer pruebas comprobando que las configuraciones sean fuertes ante ataques.
Esta auditoría se enfocaría en hacer pruebas desde dentro y desde fuera, así que tendría tanto origen externo, para comprobar accesos no autorizados, como internos, para comprobar que las configuraciones estén bien hechas y que los usuarios no accedan donde no deben.
Necesitaríamos saber algo de información básica para saber qué configuraciones utilizan y para trabajar en base a ellas, por tanto sería de tipo caja gris.
Como objetivo analizaremos la seguridad de las conexiones mediante VPN, evaluando el cifrado para prevenir accesos no deseados.

5- Auditoría a las políticas de seguridad
Esta última auditoría servirá para examinar las políticas de seguridad del negocio, no basta solo proteger los activos críticos sin defender los procesos internos. Que las políticas estén correctamente actualizadas y aplicadas de forma que cumplan los estándares, ayuda a gestionar los riesgos, minimizándolos para no tener debilidades en los sistemas.
Vamos a analizar los roles/permisos, las políticas, las configuraciones sobre el firewall y los servidores, ya que nos permitirán controlar y evitar las vulnerabilidades.
Esta vez el enfoque será utilizando pruebas manuales revisando que todas las políticas implantadas de la empresa cumplan los estándares establecidos globalmente.
Lo llevaremos a cabo de forma interna, desde dentro de la infraestructura, teniendo todo el acceso y la información sobre los activos objetivo, caja blanca.
Tendremos como objetivo identificar los puntos débiles en los activos elegidos y asegurar que estén actualizadas, que sean efectivas, y que estén correctamente implementadas.

Todas estas auditorías realizadas nos han ayudado a hacer un análisis acerca de las vulnerabilidades de la empresa. Comenzando por las debilidades externas de los activos críticos, siguiendo por los riesgos de movimientos laterales en la estructura interna. Posteriormente la configuración de los servidores y los accesos a la red vía VPN. Finalmente evaluando las políticas y su correcta implementación. Todo ello nos ayudará a tener una visión desde múltiples perspectivas de la seguridad de la empresa para reforzarla en todos los aspectos.

Apartado 2: Organiza las fases de la auditoría
Una vez has planteado las auditorías que realizarías, es necesario que indiques para cada una de ellas un calendario (o timeline) en el que se refleje los hitos de cada una de las fases con estimaciones de tiempo:

Utiliza un calendario o línea temporal para indicar cuándo se realizaría cada fase y el tiempo estimado.

- **Indica los objetivos a cumplir en cada fase.**
- **Justifica para cada auditoría si se contemplan reuniones de seguimiento o no, en caso afirmativo cada cuánto tiempo.**

Para la realización de este apartado puedes usar la siguiente tabla como referencia:

Auditoría	Duración	Fases				
		Toma de requisitos	**Realización de pruebas**	**Seguimiento de pruebas**	**Reporting**	**Cierre de auditoría**
Externa	1 semana	Reunión inicial y recopilar información (2 días)	Pruebas sobre los activos: automáticas y manuales (3 días)	Analizar vulnerabilidades encontradas (1 días)	Elaborar informe (1 días)	Reunión cierre, entrega informe (1 días)
Interna	1 semana	Facilitar información acceso red (1 días)	Escanear red, revisión configuración (2 días)	encontrar y corregir posibles errores (2 días)	Elaborar informe (1 días)	Reunión cierre, entrega informe (1 días)
Servidores críticos	2 semana	Acceso servidores (2 días)	Revisión configuraciones (5 días)	Identificar y reparar configuraciones vulnerables (3 días)	Elaborar informe (2 días)	Reunión cierre, entrega informe (2 días)
VPN	1 semana	Revisar configuración VPN (2 días)	Evaluar protocolos y accesos (2 días)	identificar posibles brechas (2 días)	Elaborar informe (1 días)	Reunión cierre, entrega informe (1 días)
Políticas Seguridad	2 semana	Revisar políticas y estándares globales (2 días)	Evaluación políticas (5 días)	Comprobar correcto implementado (2 días)	Elaborar informe (1 días)	Reunión cierre, entrega informe (2 días)

Este plan de auditorías durará de forma estimada alrededor de 2 meses, suponiendo que es una empresa pequeña con una estructura sencilla y que el departamento, al haber hecho trabajo de formación, han sabido facilitarles la información necesaria sobre la organización.

1- Auditoría Externa:
Con una duración de 1 semana, tiene el objetivo de identificar las vulnerabilidades que presenten los recursos que están expuestos, de manera que un atacante externo pudiese acceder. No sería necesario hacer seguimiento, porque es un análisis rápido al utilizar herramientas automáticas, no se necesita información sobre la empresa y no se está constantemente haciendo pruebas de penetración, ya que puede producirse un error en el servicio que ofrecen.

2- Auditoría Interna:

También tendrá una duración de 1 semana, en la que tendremos como finalidad identificar configuraciones débiles que permiten acceder a otros recursos una vez dentro de la red , sería aconsejable una reunión de seguimiento en mitad de la prueba para: comentar lo encontrado y poder guiar las pruebas a lo que sea más importante para el cliente.

3- Auditoría a los servidores críticos:
Esta auditoría se alargará durante 2 semanas, revisaremos las configuraciones de los servidores, actualizando las últimas versiones e implementado parches seguros, debido a que es tarea manual nos llevará más tiempo y necesitaremos información acerca de los servidores. Sí se requerirá seguimiento una reunión a mitad del proceso, para revisar el proceso y ajustar pruebas.

4- Auditoría de VPN:
Tenemos como objetivo evaluar la seguridad de la conexión VPN y detectar brechas de conexión con las credenciales de los usuarios. Como el análisis que vamos a realizar es sobre un mismo punto de acceso, durará 1 semana y no hará falta seguimiento de las pruebas.

5- Auditoría a las políticas de seguridad
La última auditoría durará 2 semanas, revisaremos que las políticas se adecuen a los estándares globales y detectar debilidades para proponer soluciones, con pruebas manuales de la correcta implementación de las políticas. En este caso será beneficioso hacer una reunión de seguimiento a mitad del proceso, para verificar avances y ajustar el enfoque.

Apartado 3: Presentación y valoración de vulnerabilidades.

En este caso nos ponemos en el lado de los auditores y tenemos que analizar las siguientes vulnerabilidades que se han localizado durante las pruebas. Para cada una de ellas hay que completar la siguiente descripción.

- **Valoración de la vulnerabilidad especificando los grupos de métricas base y temporal. Además, indica el vector CVSS resultante, realizar capturas de pantalla de los valores indicados.**
- **Es muy importante justificar vuestra elección en los puntos del formulario CVSS.**
- **Justificar si es una vulnerabilidad que afecta al servidor o a los clientes.**

Las vulnerabilidades localizadas son las siguientes.

➔ Una vulnerabilidad en el **sistema de correo** de la compañía que permite tomar el control del servidor y acceder a los mensajes de correo de cualquier usuario, también puedes enviar correos electrónicos suplantando la identidad de los usuarios. El servidor de correo se encuentra expuesto en internet. La vulnerabilidad presenta tanto un exploit público accesible desde exploit-db como un parche propuesto por el fabricante.

Según la valoración CVSS, esta vulnerabilidad se podría considerar crítica, por la facilidad para explotarla, poniendo en riesgo la información privada de la empresa. El vector de ataque sería externo, desde el propio internet y tendría poca complejidad, su impacto sería alto ya que pone en riesgo la confidencialidad e integridad de los datos. Vector CVSS temporal: sería menor que la valoración base por la existencia de un parche disponible.
CVSS: 9.8 (crítica)
La vulnerabilidad sería crítica porque afecta directamente al servidor comprometiendo sus funciones y afectando a los usuarios por la exposición de los datos, tiene un impacto grave para la privacidad de la empresa

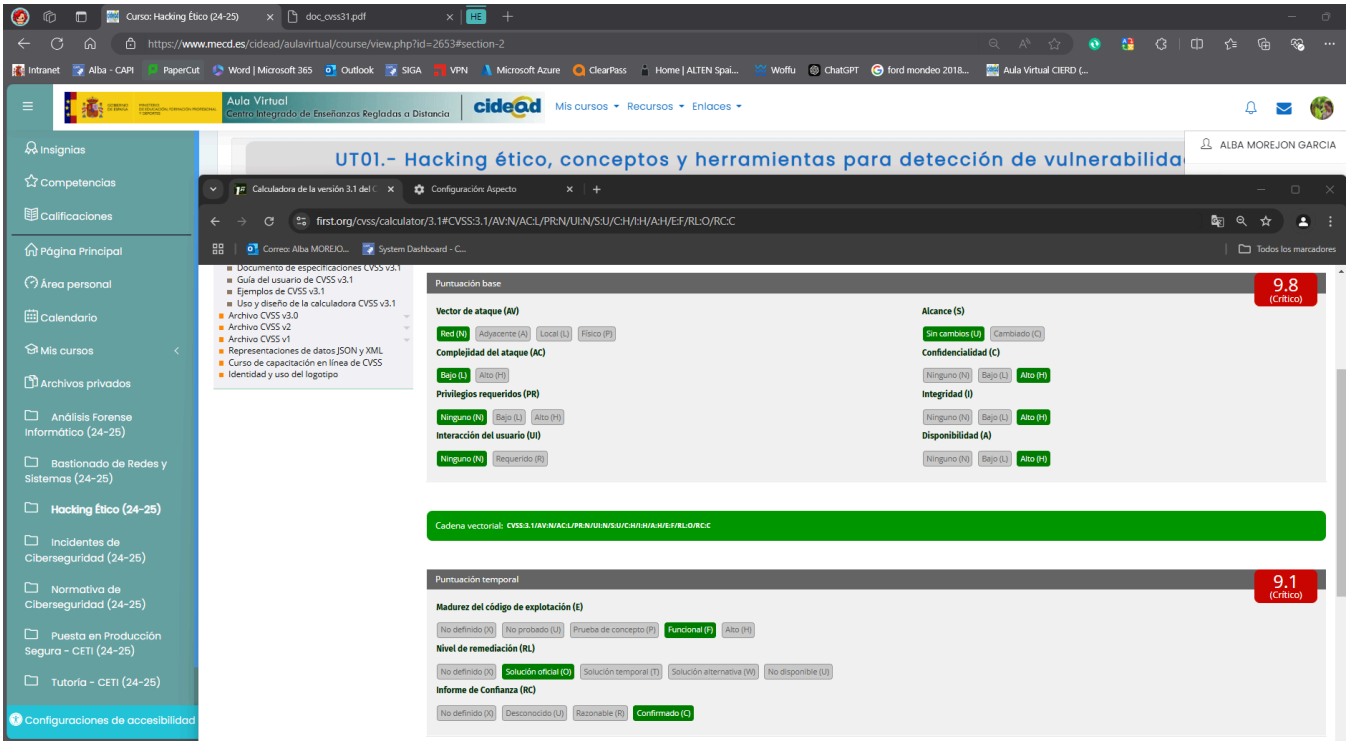
➔ Una vulnerabilidad de **inyección SQL** en la que se pueden consultar datos de otras Bases de Datos como la Base de Datos de Contabilidad. El servidor web está expuesto en internet, pero se requiere de un usuario para el acceso a la funcionalidad vulnerable. No es una vulnerabilidad conocida, el auditor la localizó en tiempo de auditoría.

Según la valoración CVSS, esta vulnerabilidad se podría considerar de severidad alta, un atacante podría acceder y visualizar datos confidenciales de la empresa, sin embargo el impacto no sería grave. El vector de ataque en remoto, el atacante accedería al servidor desde el propio internet con credenciales, pero eso tiene poca complejidad. Vector CVSS temporal: sería más difícil de explotar porque no existe un exploit público y se necesita la intervención de un auditor, pero no dejaría de ser una vulnerabilidad.
CVSS: 7.5 (alta)
La vulnerabilidad afecta directamente al servidor web y al almacén de datos, el atacante podría acceder a información privada de la empresa aunque los clientes no se verían afectados directamente.

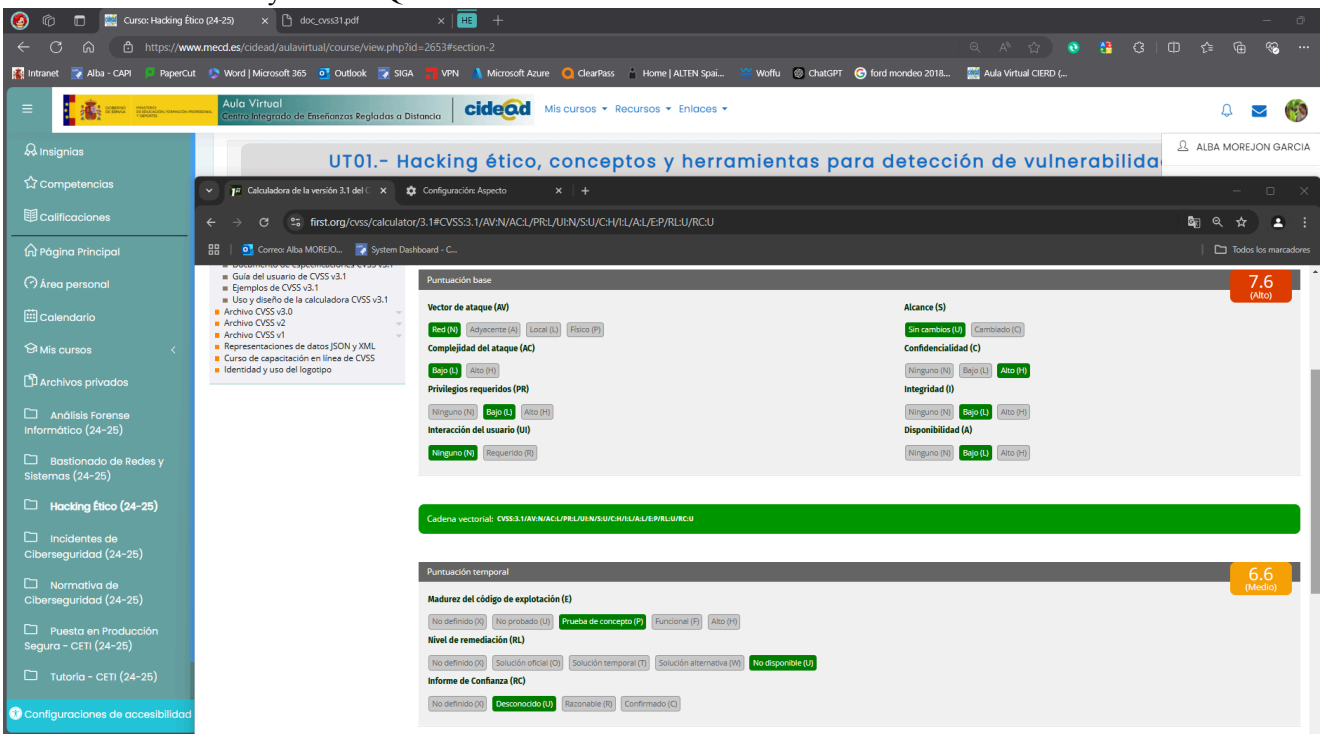
- ➔ Una vulnerabilidad de ejecución remota de código en un **servidor FTP** en la red interna de la organización. El servicio FTP se estaba ejecutando con privilegios del sistema (puede realizar cualquier acción en el sistema). Además, el acceso al servidor permite acceder a una subred de administración que no se encuentra accesible desde la red LAN de usuarios. Existe un parche público para corregir la vulnerabilidad. No hay exploit público, pero sí una prueba de concepto que el auditor ha tenido que modificar para poder explotar de manera correcta la vulnerabilidad.

Según la valoración CVSS, esta vulnerabilidad se podría considerar de crítica, por el impacto en la seguridad y capacidad de propagarse, requiere cierto conocimiento para explotarla. Un atacante podría modificar código con privilegios en el propio sistema, el vector de ataque es interno ya que accedería desde la red interna del negocio, su impacto sería alto porque podría modificar y acceder a cualquier parámetro dentro de la infraestructura. Vector CVSS temporal: no existe exploit público, existe un parche, como previamente mencionado esto no hace imposible el ataque, solo lo complica.
CVSS: 9.0 (crítica)
La vulnerabilidad afecta directamente al servidor FTP, se necesitaría estar dentro de la red interna que se debe acceder con credenciales pero una vez dentro podría comprometer la seguridad de toda la red, a los usuarios no estarían implicados directamente.

Capturas:
1. Vulnerabilidad en el sistema de correo



2. Vulnerabilidad de inyección SQL



3. Vulnerabilidad de ejecución remota de código en un servidor FTP