Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Hacking Ético

UD01. Pautas de seguridad informática.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

		Pag
1.	Caso práctico	2
2.	Apartado 1: Diseñar el plan de auditoría	2
3.	Apartado 2: Organiza las fases de la auditoría	3
4.	Apartado 3: Presentación y valoración de vulnerabilidades	5
5.	Bibliografía	11

1.- Descripción de la tarea.

Caso práctico

Una vez han completado la creación del nuevo departamento de "Seguridad Ofensiva" y Juan, junto con su equipo han finalizado las sesiones de formación. Teresa les reúne para asignarles su primer cometido.

Teresa les comenta que el primer cometido del equipo es diseñar un plan de auditoría para este primer trimestre. Dado que es la primera vez que se enfrentan a un reto de estas características ha acordado con la dirección que este primer trimestre les realizará la auditoría una empresa externa. Además, el presupuesto asignado para este trimestre sólo permite que se realicen un máximo de 5 auditorías.

El equipo de Juan tiene que diseñar el tipo de auditorías que se realizará teniendo en cuenta las siguientes premisas:

- ✓ Disponen de un total de 20 activos expuestos a internet entre servidores web, servidores de correo, acceso VPN.
- ✓ De estos 20 activos, 3 de ellos se consideran críticos para el negocio.
- ✓ Además, también les interesa realizar una primera revisión de la red interna.

¿Qué te pedimos que hagas?

- ✓ **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 incluidos en cada auditoría.
    - Indicar en cada caso el tipo de auditoría dependiendo del enfoque, origen e información proporcionada y justifica cada caso.
    - Indica el objetivo que quieres conseguir con la elección de cada tipo de auditoría.

Tras analizar el enunciado, observar el acotamiento de tiempos y presupuesto, creo que aunque sea la primera vez que van a realizarse auditorías, podemos aprovechar al máximo el hecho de que esta primera vez se encargue a una empresa externa, aprovechar su experiencia y así evitar comenzar con auditorías automáticas, buscando volumen de vulnerabilidades y visión general de nuestros sistemas.

Por ello, planteo ir de las capas externas hacia adentro, y las auditorías serían las siguientes:

Test de Intrusión Físico: Comenzamos midiendo las capacidades de contención y detención de accesos no autorizados en las sedes y oficinas a auditar, fijándonos sobre el **hardware** y la **red local**. Se intentará acceder sin previo aviso, dejando conectado un dispositivo no autorizado en la red con el propósito de conectarse de manera remota y realizar la intrusión.

Auditoría con pruebas de Caja Negra: Obtenidos los informes del test anterior, ponemos el foco sobre los distintos **dispositivos, equipos, servidores, y red local,** sin conocimiento sobre aplicación e infraestructura, buscando vulnerabilidades dentro de los límites marcados, para superar la seguridad de los sistemas y ganar accesos a estos.

Auditoría con pruebas de Caja Gris: Disponiendo de información parcial de aplicaciones y sistema interno, realizamos una simulación como atacante (que a estas alturas ya tendría conocimientos sobre el sistema), sobre los **equipos, servidores**, topología de **red**, e incluso parte del **software**, para evaluar la capacidad de respuesta de los distintos usuarios.

Creo que por la extensión, debería de incorporar al menos una reunión de seguimiento, según los datos que se vayan obteniendo, y analizar si hay que modificar algo en ellas.

Auditoría con pruebas de Caja Blanca: Con todo lo anterior, pasamos a los elementos críticos, centrando esta parte en **red interna y aplicaciones**. Necesitamos para estas pruebas credenciales autorizadas y recursos utilizados para encontrar posibles vulnerabilidades de las aplicaciones con autenticación. Para ello se revisarán todas las configuraciones, políticas, servicios… buscando puntos críticos.

Ejercicio de Red Team: Simulamos un ataque por parte de un ciberdelincuente sobre toda la infraestructura y **todos los activos** anteriores. Para ello, deberán definirse objetivos a cumplir y líneas rojas que no deben ser sobrepasadas. Se informará a un grupo reducido de la organización de la realización de las pruebas, con la finalidad de medir la capacidad de respuesta ante un ataque real, con escenarios específicos para la empresa.

- ✓ **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.

Al plantearse un calendario de tres meses, he considerado que uno de ellos tendría 30 días.

	MES 1	MES 2	MES 3
1	**Test de Intrusión Física** **Pre-engagement:** Al tratarse de la primera auditoría le asignaremos dos jornadas para la toma de requisitos, con los aspectos organizativos y procedimentales.		
2			**Reunión de Cierre de la Auditoría:** Presentación de resultados, previos y necesarios para la siguiente etapa.
3	**Realización de pruebas:** Dispondremos, acorde a lo planteado en el primer		**Auditoría de Caja Blanca** **Pre-engagement**

	apartado, de un periodo de 10 días.		
4			**Realización de pruebas:** Dispondremos, acorde a lo planteado en el primer apartado, de un periodo de 10 días.
5			
6			
7			
8			
9			
10			
11			
12			
13	**Reporting:** Dedicación de dos jornadas para la elaboración de informes.		
14		**Seguimiento de las pruebas.** Reunión de mitad de ciclo	
15	**Reunión de Cierre de la Auditoría:** Presentación de resultados, previos y necesarios para la siguiente etapa.	**Realización de pruebas:** Dispondremos, tras la reunión de seguimiento, de un periodo de 15 días.	**Reporting:** Dedicación de dos jornadas para la elaboración de informes.
16	**Auditoría Caja Negra** **Pre-engagement:** Las siguientes auditorías, cuentan con un día para analizar los aspectos organizativos y procedimentales, en base a lo que se reciba desde la etapa anterior.		
17	**Realización de pruebas:** Dispondremos, acorde a lo planteado en el primer apartado, de un periodo de 10 días.		**Reunión de Cierre de la Auditoría:** Presentación de resultados, previos y necesarios para la siguiente etapa.
18			**Ejercicio de Red Team**

			Pre-engagement
19			**Realización de pruebas:** Dispondremos, acorde a lo planteado en el primer apartado, de un periodo de 10 días.
20			
21			
22			
23			
24			
25			
26			
27	**Reporting:** Dedicación de dos jornadas para la elaboración de informes		
28			**Reporting:** Dedicación de dos jornadas para la elaboración de informes.
29	**Reunión de Cierre de la Auditoría:** Presentación de resultados, previos y necesarios para la siguiente etapa.		
30	**Auditoría Caja Gris** **Pre-engagement**	**Reporting:** Al ser una fase de pruebas de mayor duración, le dedicamos tres jornadas para la elaboración de informes.	**Reunión de Cierre de la Auditoría:** Presentación de resultados.
31	**Realización de pruebas:** Dispondremos, acorde a lo planteado en el primer apartado, de una duración de 15 días iniciales.		

✓ **Apartado 3: Presentación y valoración de vulnerabilidades.**

En este caso nos ponemos en el lado de los auditores y tenemos que analizar 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 electrónico 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.
  - 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.
  - 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.

Listamos las **métricas base** para poder analizar de forma individualizada cada vulnerabilidad. Estas son:
Vector de ataque (AV). Complejidad del ataque (AC). Privilegios requeridos (PR). Interacción del usuario (UI). Scope/Alcance(S). Confidencialidad (C). Integridad (I). Disponibilidad(A).

Listamos las **métricas temporales**:
Madurez del código de explotación (E). Nivel de remediación (RL). Confianza del informe (RC)

Vulnerabilidad en el sistema de correo.

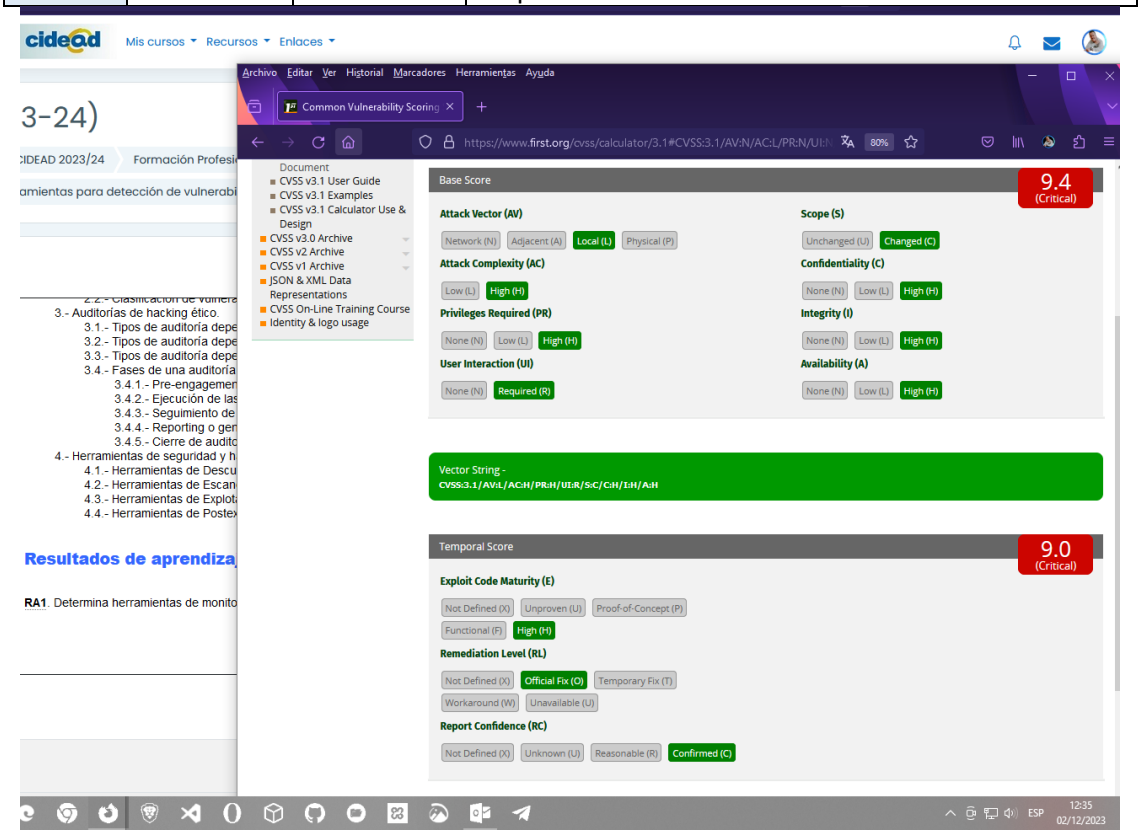
Métricas base.

Métrica	Valor	Abreviatura	Descripción.
AV	Red	N	La vulnerabilidad se puede explotar desde cualquier lugar, incluso desde redes externas y de Internet.
AC	Baja	L	No hay condiciones especiales en el acceso al equipo o no se requiere ninguna interacción con el usuario.
PR	Ninguno	N	No se requieren privilegios para explotar la vulnerabilidad.

UI	Ninguna	N	No se requiere ninguna interacción del usuario para explotar la vulnerabilidad.
S	Sin cambio	U	Una vulnerabilidad en un componente vulnerable no afecta a ningún componente que esté en un ámbito de seguridad diferente al del componente vulnerable (sin desplazamiento horizontal).
C	Alto	H	Hay un alto impacto en la confidencialidad, por el acceso a todos los correos.
I	Alto	H	Hay un alto impacto en la integridad por suplantación.
A	Bajo	L	Hay un impacto bajo en la disponibilidad. No tiene por qué influenciar o interrumpir el servicio.

Métricas temporales.

Métrica	Valor	Abreviatura	Descripción
E	Alto	H	Se ha publicado un código de explotación de alta calidad que es consistente y fiable en el éxito de la explotación. Este exploit es ampliamente conocido y es autónomo o no es necesario un exploit (lanzamiento manual). Es accesible desde exploit-db y como parche del fabricante.
RL	Oficial	O	Se ha publicado una solución completa y permanente por el autor o el proveedor del componente vulnerable. Esta puede ser mediante un parche o una actualización .
RC	confirmado	C	Se ha confirmado la existencia de la vulnerabilidad mediante el reconocimiento del autor o el proveedor del componente vulnerable, o mediante la publicación de pruebas o análisis detallados

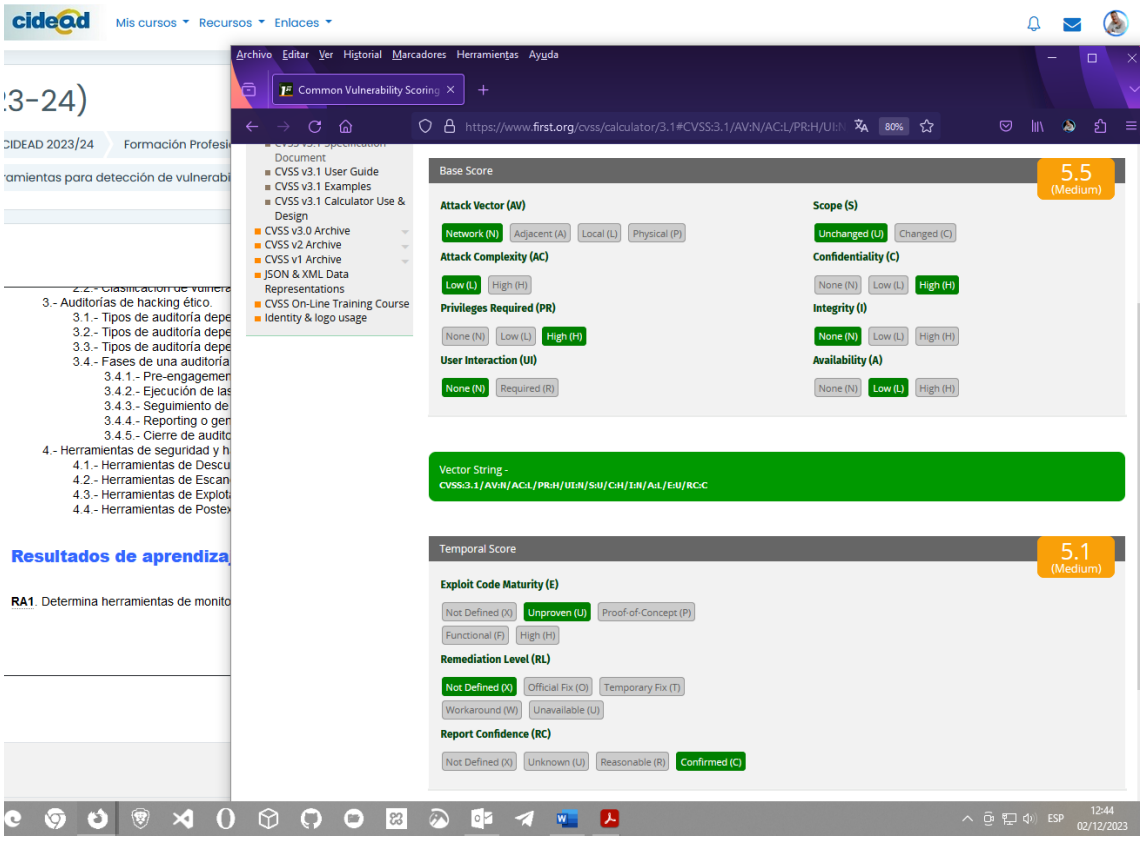


Vulnerabilidad de inyección SQL.

Métrica	Valor	Abreviatura	Descripción.
AV	Red	N	La vulnerabilidad se puede explotar desde cualquier lugar, incluso desde redes externas y de Internet.
AC	Baja	L	No hay condiciones especiales en el acceso al equipo o no se requiere ninguna interacción con el usuario.
PR	Altos	H	Se requieren privilegios que proporcionan un control significativo o total sobre el componente vulnerable (requiere credenciales de acceso).
UI	Ninguna	N	No se requiere ninguna interacción del usuario para explotar la vulnerabilidad.
S	Sin cambio	U	Una vulnerabilidad en un componente vulnerable no afecta a ningún componente que esté en un ámbito de seguridad diferente al del componente vulnerable (sin desplazamiento horizontal).
C	Alto	H	Hay un alto impacto en la confidencialidad, por el acceso a la base de datos.
I	Ninguna	N	No hay impacto en la integridad, pues solo son consultas y se ha descubierto en auditoría.
A	Bajo	L	Hay un impacto bajo en la disponibilidad. No tiene por qué influenciar o interrumpir el servicio, por haberse descubierto en auditoría.

Métricas temporales.

Métrica	Valor	Abreviatura	Descripción
E	No probado	U	No hay exploit disponible, o este exploit es teórico. No es una vulnerabilidad conocida, localizada por el auditor.
RL	No definido	X	No se dispone de información sobre el nivel de remediación. Tiene el mismo efecto que elegir “no disponible” (U).
RC	confirmado	C	Se ha confirmado la existencia de la vulnerabilidad mediante el reconocimiento del autor o el proveedor del componente vulnerable, o mediante la publicación de pruebas o análisis detallados.

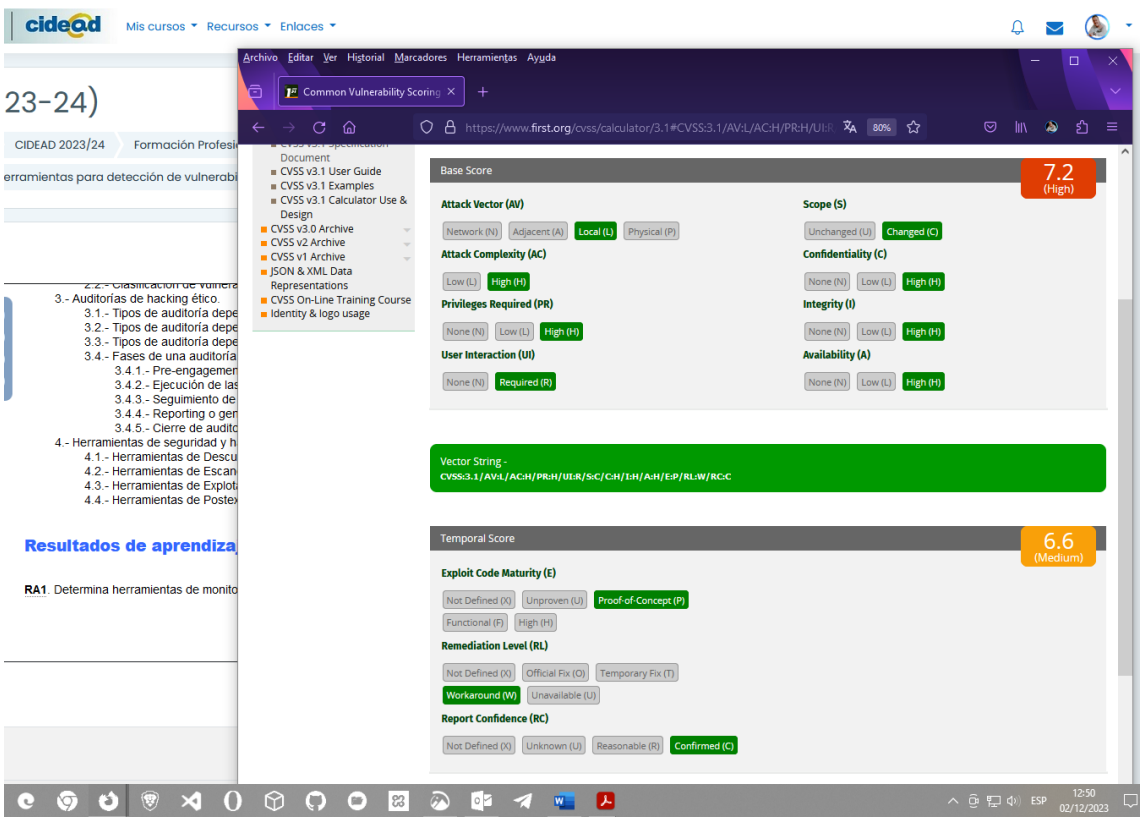


Vulnerabilidad de ejecución remota de código.

Métrica	Valor	Abreviatura	Descripción.
AV	Local	L	La vulnerabilidad requiere acceso local al sistema (acceso FTP) o a un servicio oculto.
AC	Alta	H	Se requiere una condición difícil o improbable (era desconocida), o se requiere alguna interacción con el usuario. Se deben estudiar las condiciones del equipo y su entorno para el éxito del ataque.
PR	Altos	H	Se requieren privilegios que proporcionan un control significativo o total sobre el componente vulnerable (requiere de credenciales).
UI	Requerida	R	Se requiere alguna interacción del usuario para explotar la vulnerabilidad (hay una prueba de concepto modificada).
S	Cambiado	C	Una vulnerabilidad en un componente vulnerable afecta a un componente que está en un ámbito de seguridad diferente al del componente vulnerable (accede a FTP y a la subred).
C	Alto	H	Hay un alto impacto en la confidencialidad, por el acceso a los ficheros.
I	Alto	H	Hay un alto impacto en la integridad por poder hacer cambios en los ficheros del FTP.
A	Alto	H	Hay un impacto alto en la disponibilidad, pues servicio y ficheros pueden verse afectados.

Métricas temporales.

Métrica	Valor	Abreviatura	Descripción
E	Prueba de concepto	P	Se ha publicado un código de prueba de concepto o una demostración. Esta técnica o código no es funcional en muchas ocasiones y se necesitan modificaciones por parte de un atacante experimentado.
RL	Provisional	W	Existe una solución provisional no oficial, como un parche creado por usuario para mitigar la vulnerabilidad.
RC	confirmado	C	Se ha confirmado la existencia de la vulnerabilidad mediante el reconocimiento del autor o el proveedor del componente vulnerable, o mediante la publicación de pruebas o análisis detallados



Webgrafía.

Temario plataforma CIDEAD UT01.- Hacking ético, conceptos y herramientas para detección de vulnerabilidades

Documentación CVSS 3.1: https://www.first.org/cvss/v3.1/specification-document

Calculadora CVSS: https://www.first.org/cvss/calculator/3.1