

ÍNDICE:

Caso práctico	2
Diseñar el plan de auditoría.....	2
Organiza las fases de la auditoría	4
Presentación y valoración de vulnerabilidades.	5
Vulnerabilidad 1:	5
Vulnerabilidad 2:	7
Vulnetabilidad 3:	9
Bibliografía:.....	12

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

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 quieras conseguir con la elección de cada tipo de auditoría.

PAUTAS DE SEGURIDAD INFORMÁTICA

Auditoría	Justificación de la Auditoría	Activo(s) y justificación	Enfoque (manual, automática, etc)	Origen (interna o externa)	Información proporcionada (tipo de caja)	Objetivo
Seguridad de Servidores Críticos	Los servidores críticos son esenciales para la continuidad del negocio y su seguridad es prioritaria	3 servidores críticos, estos son fundamentales para la continuidad de la actividad del negocio	Enfoque manual y automático, ya que la combinación de ambas permite un análisis exhaustivo	Externa, una empresa especializada a que de imparcialidad y profesionalidad	Caja negra, no se da información para simular ataques reales	Identificar y mitigar todas las vulnerabilidades que puedan afectar a la continuidad del negocio
Seguridad de Servidores Web	Los servidores web es la puerta de entrada habitual de ciberataques	10 servidores web. Estos activos están expuestos a internet y son susceptibles a ataques	Automática, permite un escaneo rápido de gran cantidad de sistemas	Externa, para poder asegurar un enfoque imparcial y una buena evaluación	Caja gris, se da cierta información para conseguir una evaluación dirigida y controlada	Identificar y subsanar vulnerabilidades de los servidores web y mejorar la seguridad
Seguridad de Servidores de Correo	Los servidores de correo son un activo crítico para la comunicación y es un vector de ataque que hay que tener en cuenta	Los servidores de correo expuestos a internet, estos son activos esenciales para la comunicación interna y externa de la organización	Manual y automática. La combinación permite una revisión exhaustiva y detallada	Externa, para asegurar una revisión exhaustiva y detallada	Caja blanca, se da toda la información necesaria para conseguir una evaluación detallada	Identificar y solucionar posibles vulnerabilidades en los servidores de correo
Seguridad de Acceso VPN	Los accesos VPN permiten crear un canal para la conexión remota con la red interna y deben ser seguros	Accesos VPN. Estos accesos permiten la conexión con la red interna y deben ser seguros	Manual, permiten la revisión en detalle de configuraciones y políticas de seguridad	Externa, asegurando la imparcialidad y efectuada por personal especializado	Caja gris, para conseguir una evaluación dirigida	Identificar vulnerabilidad y errores en las conexiones VPN para mejorar la seguridad
Seguridad de la Red Interna	Hay que considerar la importancia de realizar esta auditoria para tener una visión general de la seguridad interna y poder identificar vulnerabilidades	Toda la red interna. Proporciona una visualización general de la seguridad de la red interna	Manual y automática. Para conseguir una revisión exhaustiva y detallada	Externa, proporciona una evaluación imparcial y especializada	Caja blanca, se proporciona la información necesaria para una evaluación exhaustiva	Identificar y mitigar posibles vulnerabilidades en la red interna

He diferenciado en las auditorias los servidores críticos de los otros de correo, VPN y WEB ya que estos están diferenciados en el enunciado,

pero cualquiera de ellos debería considerarse críticos por la capacidad de que un actor externo y malintencionado pueda aprovecharse de una vulnerabilidad y acceder a ellos.

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.

Auditoría	Duración	Fases					
		Toma de requisitos	Realización de pruebas	Seguimiento de pruebas	Reporting	Cierre de auditoría	Reuniones de seguimiento
Seguridad de Servidores Críticos	2 semanas y 3 días	3 días	Una semana	3 días	1 día	1 día	semanales
Seguridad de Servidores Web	2 semanas y 2 días	2 días	Una semana	2 días	1 día	1 día	semanales
Seguridad de Servidores de Correo	2 semanas y 2 días	2 días	Una semana y 3 días	3 días	1 día	1 día	semanales
Seguridad de acceso VPN	2 semanas	2 días	Una semana	1 día	1 día	1 día	semanales
Seguridad red interna	2 semanas y 3 días	2 días	Una semana	3 días	1 día	1 día	semanales

Se ajustan los tiempos teniendo en cuenta la importancia el trabajo y lo ajustado del tiempo disponible de 3 meses, también se ha ejecutado las auditorias una a una para interferir lo menos posible en la actividad de la empresa.

NOTA: Se debe indicar la temporalización de cada una de las fases de la auditoria.

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.**

Vulnerabilidad 1:

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.

Del texto de esta vulnerabilidad he sacado las siguientes conclusiones:

- **Afecta a:** Servidor.
- Esta vulnerabilidad afecta directamente al servidor de correo, permitiendo a un actor malintencionado tomar el control del servidor de correo, acceder a los mensajes de correo y suplantar la identidad de todos los usuarios, con el riesgo que ello supone. No afecta directamente a los clientes, aunque las consecuencias pueden impactar a los usuarios finales.
- **Valoración:**
- **Base:**
 - ✓ **Vector de ataque (AV):** Red(N)- se puede explotar la vulnerabilidad a través de la red.
 - ✓ **Complejidad del Ataque (AC):** Baja (L) - No se requiere ninguna condición especial para explotar la vulnerabilidad.

- ✓ **Privilegios Requeridos (PR):** Ninguno (N) - No se requieren privilegios para explotar la vulnerabilidad.
- ✓ **Interacción del Usuario (UI):** Ninguna (N) - No se requiere interacción del usuario.
- ✓ **Alcance (S):** No Cambiado (U) - La vulnerabilidad afecta solo al componente vulnerable.
- ✓ **Impacto en la Confidencialidad (C):** Alto (H) - Permite acceso completo a los mensajes de correo.
- ✓ **Impacto en la Integridad (I):** Alto (H) - Permite suplantar la identidad de los usuarios.
- ✓ **Impacto en la Disponibilidad (A):** Alto (H) - Permite tomar el control del servidor.

The screenshot shows a dual-layer interface. On the left, a Moodle-based course page for 'Hacking Ético (24-25)' displays a task titled 'Tarea para HE01'. This task includes three steps: 'Descripción de la tarea.', 'Información de interés.', and 'Evaluación de la tarea.' A blue callout box labeled 'NOTA' points to the task area. On the right, a modal window titled 'Common Vulnerability Scoring System Version 3.1 Calculator' is open over the task details. The calculator interface includes sections for 'Attack Vector (AV)', 'Scope (S)', 'Confidentiality (C)', 'Attack Complexity (AC)', 'Integrity (I)', 'Availability (A)', 'Privileges Required (PR)', and 'User Interaction (UI)'. The 'Base Score' is prominently displayed as 9.8 (Critical). Below the calculator, a 'Vector String' field contains the value 'CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/CH:H/A:H'.

➤ Temporal:

- ✓ **Explotabilidad (E):** Funcional (F) - Existe un exploit público y funcional.
- ✓ **Remediación (RL):** Solución Oficial (O) - Existe un parche propuesto por el fabricante.
- ✓ **Reportado (RC):** Confirmado (C) - La vulnerabilidad ha sido confirmada.

The screenshot shows a dual-pane interface. On the left, the 'Aula Virtual' platform displays a task titled 'Hacking Ético (24-25)' with three main steps: 'Descripción de la tarea.', 'Información de interés.', and 'Evaluación de la tarea.'. A note on the right says 'Para como cumplir'. On the right, a separate window titled 'Common Vulnerability Scoring' shows the following details:

- Privileges Required (PR):** High (H)
- User Interaction (UI):** Required (R)
- Availability (A):** High (H)
- Vector String:** CVSS3.1#AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C
- Temporal Score:** 9.1 (Critical)
- Exploit Code Maturity (E):** Functional (F)
- Remediation Level (RL):** Official Fix (O)
- Report Confidence (RC):** Confirmed (C)

- **CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C**
- **Justificación:** Esta vulnerabilidad permite el acceso al servidor del correo, la lectura de mensajes y la suplantación de identidad, un acceso completo. Lo cual puede tener un gran impacto en la compañía

Vulnerabilidad 2:

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.

Del texto de esta vulnerabilidad he sacado las siguientes conclusiones:

- **Afecta a:** Servidor
- **Justificación:** Esta vulnerabilidad, la cual afecta al servidor web, permite a un atacante ejecutar consultas de tipo SQL con fines maliciosos para acceder a datos almacenados. Aunque se requiere autenticación de usuario, la vulnerabilidad reside en el servidor web y no en el cliente.
- **Valoración:**
- **Base:**
 - ✓ **Vector de ataque (AV):** Red(N)- se puede explotar la vulnerabilidad a través de la red.

- ✓ **Complejidad del Ataque (AC):** Baja (L) - No se requiere ninguna condición especial para explotar la vulnerabilidad.
- ✓ **Privilegios Requeridos (PR):** Bajo (L) - Se requiere autenticación de usuario.
- ✓ **Interacción del Usuario (UI):** Ninguna (N) - No se requiere interacción del usuario.
- ✓ **Alcance (S):** No Cambiado (U) - La vulnerabilidad afecta solo al componente vulnerable.
- ✓ **Impacto en la Confidencialidad (C):** Alto (H) - Permite acceso a datos sensibles de la empresa.
- ✓ **Impacto en la Integridad (I):** Alto (H) - Permite la modificación de datos.
- ✓ **Impacto en la Disponibilidad (A):** Alto (H) - puede afectar en la disponibilidad del sistema.

The screenshot shows a web browser window with two main tabs open:

- CETI_HE-Tarea para HE01**: This tab displays a task assignment for "Hacking Ético (24-25)". It includes sections for "Página Principal", "Mis cursos", and "CIDEAD 2024". Below these are links for "UTO1.- Hacking ético, conceptos y herramientas p..." and "Tarea para HE01". Under "Tarea para HE01", there is a list of steps: "Tarea online HE01.", "1.- Descripción de la tarea.", "2.- Información de interés.", and "3.- Evaluación de la tarea.". A blue callout box labeled "NOTA" points to the first step, stating "Para cumplir con la entrega".
- Common Vulnerability Scoring System Version 3.1 Calculator**: This tab is from first.org/cvss/calculator/3.1#CVSS3.1#AV:N/ACL:PRL:U:N/S:U/C:H/I:H/A:H. It shows the CVSS version 3.1 calculator interface. The "Base Score" is 8.8 (High). The calculator fields are set as follows:
 - Attack Vector (AV)**: Network (N) (highlighted), Adjacent (A), Local (L), Physical (P).
 - Scope (S)**: Unchanged (U) (highlighted), Changed (C).
 - Confidentiality (C)**: None (N) (highlighted), Low (L), High (H).
 - Integrity (I)**: None (N) (highlighted), Low (L), High (H).
 - Availability (A)**: None (N) (highlighted), Low (L), High (H).
 The "User Interaction (UI)" field is set to "None (N) Required (R)". The "Vector String" at the bottom is `CVSS:3.1#AV:N/ACL:PRL:U:N/S:U/C:H/I:H/A:H`.

On the right side of the browser window, there is a sidebar with various notifications and messages.

➤ Temporal:

- ✓ **Explotabilidad (E):** No Disponible (U) - No existe un exploit público.
- ✓ **Remediación (RL):** Solución Temporal (T) - No hay parche disponible, pero se puede mitigar con diferentes acciones.
- ✓ **Reportado (RC):** No Confirmado (U) - La vulnerabilidad no ha sido confirmada aun por el fabricante.

The screenshot shows a dual-pane interface. On the left, the 'Aula Virtual' platform displays a task titled 'Hacking Ético (24-25)' with sub-sections like 'Página Principal', 'Mis cursos', and 'CIDEAD 2024'. A sidebar on the far left contains icons for navigation and course management. On the right, a 'Common Vulnerability Scoring' tool from 'first.org' is open, specifically for calculating CVSS 3.1 scores. The tool shows the following parameters and their settings:

- Privileges Required (PR):** Low (L)
- User Interaction (UI):** None (N)
- Availability (A):** High (H)
- Temporal Score:** 7.1 (High)
- Exploit Code Maturity (E):** Unproven (U)
- Remediation Level (RL):** Temporary Fix (T)
- Report Confidence (RC):** Unknown (U)

The vector string for the score is listed as: CVSS3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:U.

➤ **CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:U**

Justificación: Esta vulnerabilidad permite el acceso al servidor web y da acceso a datos sensibles de la empresa, comprometiendo la disponibilidad, la confidencialidad y la integridad de estos, lo cual puede tener un gran impacto en la compañía.

Vulnabilidad 3:

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.

Del texto de esta vulnerabilidad he sacado las siguientes conclusiones:

- **Afecta a:** Servidor
- **Justificación:** Esta vulnerabilidad afecta al servicio FTP, permitiendo a un atacante ejecutar código con privilegios

del sistema y acceder a una subred de administración. La vulnerabilidad reside en el servidor y no en los clientes ya que no es accesible para los usuarios.

▪ Valoración:

➤ Base:

- ✓ **Vector de ataque (AV):** Red(N) - se puede explotar la vulnerabilidad a través de la red.
- ✓ **Complejidad del Ataque (AC):** Alta (H) - Se requiere una prueba de concepto modificada para explotar la vulnerabilidad.
- ✓ **Privilegios Requeridos (PR):** Ninguno (N) - No se requieren privilegios para explotar la vulnerabilidad.
- ✓ **Interacción del Usuario (UI):** Ninguna (N) - No se requiere interacción del usuario.
- ✓ **Alcance (S):** Cambiado (C) - La vulnerabilidad permite acceder a una red no disponible para usuarios.
- ✓ **Impacto en la Confidencialidad (C):** Alto (H) - Permite el acceso a datos sensibles.
- ✓ **Impacto en la Integridad (I):** Alto (H) - Permite modificar datos.
- ✓ **Impacto en la Disponibilidad (A):** Alto (H) - puede afectar a la disponibilidad del sistema.

The screenshot shows a dual-browser setup. On the left, a window titled 'CETI HE: Tarea para HE01' displays a task assignment for 'Hacking Ético (24-25)' with three steps: '1.- Descripción de la tarea.', '2.- Información de interés.', and '3.- Evaluación de la tarea.' A note on the right says 'Para cumplir con la tarea de correo de la otra expuesta'. On the right, a separate window titled 'Common Vulnerability Scoring System Version 3.1 Calculator' shows the CVSS 3.1 calculator interface. The 'Base Score' is 9.0 (Critical). The configuration is as follows:

Metric Group	Value
Attack Vector (AV)	Network (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	Changed (C)
Attack Complexity (AC)	Physical (P)
Integrity (I)	None (N)
Privileges Required (PR)	Low (L)
Availability (A)	High (H)
User Interaction (UI)	None (N)

The 'Vector String' is displayed as: CVSS3.1/AV:N/AC:H/PR:N/UI:N/S:C/H:H/A:H

➤ Temporal:

- ✓ **Exploitabilidad (E):** Prueba de Concepto (P) - Existe una prueba de concepto modificada.
- ✓ **Remediación (RL):** Solución Oficial (O) - Existe un parche público.

- ✓ **Reportado (RC):** Confirmado (C) - La vulnerabilidad ha sido confirmada.

The screenshot shows a web browser window with two main tabs. The left tab is titled 'CETI_HE: Tarea para HE01' and displays a course interface for 'Hacking Ético (24-25)'. The right tab is titled 'Common Vulnerability Scoring' and shows a detailed breakdown of a vulnerability. Key information from the scoring calculator includes:

- Vector String:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
- Temporal Score:** 8.1 (High)
- Exploit Code Maturity (E):** Proof-of-Concept (P) (highlighted), Functional (F), High (H)
- Remediation Level (RL):** Official Fix (O) (highlighted)
- Report Confidence (RC):** Confirmed (C) (highlighted)

➤ **CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C**

Justificación: Esta vulnerabilidad afecta al servicio FTP y además da acceso a una subred no disponible a los usuarios, lo cual puede comprometer la red interna de la empresa y dar acceso a datos privados.

Cabe destacar que todas estas vulnerabilidades descritas y a las cuales he calculado el CVSS están sujetas a interpretación, ya que nouento con todos los datos y carezco de la experiencia necesaria para poder hacer una valoración ajustada.

Bibliografía:

- Temario de la asignatura.
- Calculadora CVSS. <https://www.first.org/cvss/calculator/3.1>
- Guía de usuario CVSS 3.1. <https://www.first.org/cvss/v3.1/user-guide>