APUNTES 01

HACKING ÉTICO, CONCEPTOS Y HERRAMIENTAS PARA DETECCIÓN DE VULNERABILIDADES

HACKING ÉTICO

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

En esta unidad de trabajo aprenderás los conceptos generales del ámbito de la especialización en "hacking ético", terminología y tipos de actividades llevadas a cabo. Continuando con los conceptos básicos se realizará un breve resumen del tipo de herramientas utilizadas en esta disciplina. Continuaremos explicando los principios en los que se sustenta la seguridad de la información, y detallaremos el concepto de vulnerabilidad, tipos de vulnerabilidades y la valoración de la criticidad de las mismas basándonos en el estándar CVSS. También se mostrarán los distintos tipos de auditoría realizadas desde el enfoque de "hacking ético", se detallarán todas las fases involucradas en este tipo de auditorías mostrando las necesidades particulares de cada una de ellas. Para finalizar, se detallará el proceso de documentación de las vulnerabilidades y la presentación de resultados.

1.- CONCEPTOS GENERALES EN HACKING ÉTICO

Hacking ético: disciplina que se encarga de comprobar el nivel de madurez en materia de seguridad de un determinado activo o sistema informático. Para ello se realizan una serie de pruebas de seguridad (también conocidas como pruebas de intrusión o auditorías de hacking ético). En este tipo de pruebas se utilizan técnicas comúnmente ejecutadas por atacantes externos para comprometer la seguridad de un determinado sistema. El propósito de estas pruebas consiste en detectar las vulnerabilidades presentes en un determinado sistema o aplicación, antes de que sean descubiertas por un ciberdelincuente. La finalidad principal consiste en solventar las vulnerabilidades localizadas para evitar que un atacante pudiera aprovecharlas para comprometer el sistema afectado.

1.1.- DIFERENCIAS ENTRE ACTORES/ACTIVIDADES ÉTICAS O CRIMINALES

Muchos medios de comunicación (prensa, radio o televisión) tienden a confundir términos entre personas y/o actividades que se encuentran en el lado criminal o en el lado ético.

Diferentes actores

- Hacker, se refiere a cualquier experto de las tecnologías de comunicación e información que utiliza sus conocimientos técnicos para encontrar y resolver un problema concreto relacionado con la seguridad de la información. Esta categoría suele estar formada por técnicos e ingenieros informáticos con conocimientos específicos en seguridad. Están habituados a detectar errores o fallos de seguridad en sistemas informáticos, aplicativos, dispositivos o infraestructuras tecnológicas. Dado que se rigen por un concepto "ético" los fallos descubiertos son comunicados a los desarrolladores del software/producto o publican los hallazgos encontrados en portales específicos para que la información se encuentre a disposición de todo el mundo.
- Ciberdelincuente o Cibercriminal, al igual que un hacker ético, por lo general, un cibercriminal también suele disponer de amplios conocimientos técnicos en materia de seguridad en tecnologías de la información, lo cual le permite identificar fallos de seguridad en distintos sistemas informáticos, aplicativos, dispositivos o infraestructuras tecnológicas. Sin embargo, al contrario que sucede con los hackers éticos, este tipo de actores, intentan lucrarse mediante la realización de actividades utilizando para ello los fallos de seguridad localizados.
- Hacktivista, cualquier hacker ético que utilice sus destrezas técnicas en el ámbito de la seguridad de la información con fines sociales, ecológicos, humanitarios o que tenga repercusión en la defensa de los derechos humanos.

Actividades Relacionadas

- Auditorías de hacking ético / Test de intrusión, es el tipo de actividad que realiza un hacker ético con la finalidad de descubrir fallos en un sistema informático. Se cuenta con el permiso del propietario del sistema informático a auditar y se reportan los fallos de seguridad localizado para que puedan ser solucionados y no sean aprovechados por un ciberdelincuente para perpetrar un ataque informático.
- Incidente de seguridad / Ataque informático, actividad realizada por uno o varios ciberdelincuentes en la que se consigue obtener un beneficio económico de la explotación de una determinada vulnerabilidad. Casos comunes son el uso del ransomware para secuestrar equipos y pedir un rescate a la víctima. Obtención de información privada para coacción o chantaje o, incluso, daño económico o reputacional.
- Hacktivismo, tipo de actividades de hacking ético ejecutadas por un activista que tienen un componente social, ecológico, humanitario, etc. A continuación se enumeran varias actividades que son consideradas partes de hacktivismo.

Libre compartición de información: Como la propia WikiPedia, en la cual se genera y comparte contenido de dominio público para garantizar que todo el mundo tenga derecho a adquirir nuevos conocimientos.

Liberación de información clasificada: Caso Wikileaks o las filtraciones de los papeles de pandora con el pretexto de que la información liberada ha de estar en disposición de toda la sociedad.

Paralización de actividades económicas: Se han dado casos en los que los hacktivistas movilizaban a un gran número de personas con el fin de acceder repetidamente a páginas de comercio electrónico para colapsar su acceso y paralizar las ventas.

Tipos de redes disponibles en internet

- ClearNet, se refiere a todo el contenido que se encuentra disponible de manera pública en internet, o en su defecto el contenido al que se accede con algún usuario en la plataforma. En resúmen, es la parte de internet accesible por todos.
- DeepWeb, se refiere a todo el contenido privado que no se encuentra a disposición del público en general, pero que a través de la ClearNet es posible acceder a ciertos datos contenidos en ella. POr poner un ejemplo, la Base de Datos de una tienda online se encuentra alojada en la DeepWeb, sin embargo accedes a cierta información a través de la ClearNet como los productos disponibles, precios y comentarios.
- DarkWeb, redes privadas utilizadas por los ciberdelincuentes para ofrecer sus servicios, vender información previamente robada, vulnerabilidades no reportadas a los fabricantes, etc. También existen zonas en la DarkWeb destinada a la venta de sustancias prohibidas o material no autorizado. El acceso a este tipo de redes se realiza mediante clientes de acceso a la red Tor. Es una red que no es para nada confiable dado que también se producen numerosos engaños. También es utilizada por los cibercriminales a modo de red puente para intentar encubrir el origen real de las pruebas.

1.2.- SEGURIDAD DE LA INFORMACIÓN VS SEGURIDAD INFORMÁTICA

En ocasiones se tiende a confundir estos dos conceptos estando el concepto de "Seguridad de la información" más enfocado a la parte estratégica y la "Seguridad informática" más orientado a la parte operacional.

- Seguridad de la información: conjunto de medidas establecidas por las distintas organizaciones, ya sean estas públicas o privadas, con el fin de proteger la información garantizando su confidencialidad, integridad y disponibilidad.
- Seguridad informática: área de la rama tecnológica/informática orientada a la protección de las infraestructuras, ya sean éstas hardware o software, y de la información que contiene, procesa o transmite.

1.3.- PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

Existen tres principios fundamentales que debe respetar la seguridad/gestión de la información:

- Confidencialidad: La confidencialidad requiere que la información sea accesible de forma única a las personas que se encuentran autorizadas. Es necesario proteger la información mediante sistemas de autorización y control. La confidencialidad hace referencia a la necesidad de ocultar o mantener en secreto determinada información o recursos.
- Integridad: La integridad, requiere que la información se mantenga inalterada ante incidentes o accesos malintencionados. Sólo se podrá modificar la información en caso de que el mecanismo de autorización lo permita. El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.
- Disponibilidad: La disponibilidad requiere que el sistema informático se mantenga accesible sin sufrir ninguna degradación o interrupción en el servicio. Es necesario que se ofrezcan los recursos que requieran los usuarios cuando se necesiten. El objetivo es necesario prevenir interrupciones no autorizadas de los recursos informáticos.

2.- CONCEPTO DE RIESGO Y VULNERABILIDAD

Riesgo, relacionado con seguridad de la información, entendemos riesgo como la pérdida potencial, daño o destrucción de un determinado activo (Sistema de información) como resultado de la explotación de una vulnerabilidad al materializarse las consecuencias de una amenaza.

- Activo: Objeto o recurso de valor (tangible o intangible) empleado en una empresa u organización. Cuya pérdida o daño constituiría un riesgo para la organización.
- Amenaza: Evento que puede causar un incidente de seguridad en una empresa u organización produciendo pérdidas o daños potenciales en sus activos.
- Vulnerabilidad: Debilidad que puede ser explotada con la materialización de una o varias amenazas a un activo. INCIBE (Todos los derechos reservados)

2.1.- VALORACIÓN DE VULNERABILIDADES

Hay que tener en cuenta que no todas las vulnerabilidades presentan la misma criticidad o impacto en la organización.

Por ejemplo, no tiene el mismo impacto una vulnerabilidad de “degradación del servicio” que permita ralentizar el sistema afectado, impacto en la disponibilidad, que una vulnerabilidad de “ejecución remota de comandos” con la que pueda tener un control total sobre el activo de manera remota. En este último caso la vulnerabilidad impacta directamente en la confidencialidad, integridad e incluso disponibilidad de la información.

Common Vulnerability and Score System

CVSS (Common Vulnerability Scoring System), estándar abierto para poder evaluar correctamente la criticidad de una determinada vulnerabilidad, y que esta evaluación sea coherente con el impacto que tendría la vulnerabilidad de ser explotada en la organización. Este sistema, ideado y mantenido por la organización FIRST (global Forum of Incident Response and Security Teams) otorga una puntuación a cada vulnerabilidad identificada dependiendo de unas métricas específicas y así poder estimar el impacto de la misma.

Actualmente, el estándar se encuentra en su versión 3.1 y está formado por tres grupos de métricas que nos permiten obtener el nivel global de la puntuación

- Métrica Base, representa las características intrínsecas de la vulnerabilidad a evaluar. Por ejemplo, tiene en cuenta que posición en la red ha de tener el atacante para poder aprovecharse de la vulnerabilidad, necesidades de disponer de algún tipo de acceso previo al sistema, o indicar los pilares de la seguridad de la información se ven afectados en caso de explotar con éxito la vulnerabilidad, etc.
- Métrica temporal, representa las características de la vulnerabilidad que pueden cambiar a lo largo del tiempo. Por ejemplo, una vulnerabilidad sobre la que exista un parche o solución oficial no será tan crítica como una vulnerabilidad de la que no existe una solución oficial. De manera similar, en caso de existir un exploit/herramienta pública que nos permita abusar de esta vulnerabilidad la criticidad será

mucho mayor que si no hubiera ningún tipo de herramienta que permita abusar de la vulnerabilidad de manera sencilla.

- Métrica de entorno, representa las características de la vulnerabilidad propias del entorno en que ha sido encontrada. Permite ajustar y dar más peso a la confidencialidad, a la integridad, etc. De esta manera se adecúa la criticidad de la vulnerabilidad al entorno específico en el que ha sido descubierta.

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

Existen varias calculadoras CVSS que se pueden utilizar para realizar el cálculo de la criticidad de una vulnerabilidad obtendremos dos resultados principales:

- Valor: Puntuación 0-10 de la criticidad de la vulnerabilidad evaluada.
- Vector CVSS: Recoge en un único vector los valores que hemos indicado en cada métrica para calcular la criticidad de la vulnerabilidad.

2.2.- CLASIFICACIÓN DE VULNERABILIDADES

Dependiendo del acceso al componente vulnerable, el primer grupo de vulnerabilidades se puede catalogar según el tipo de acceso requerido para acceder al componente vulnerable

- Vulnerabilidad remota, en este caso es posible acceder al componente vulnerable de manera remota, normalmente porque el componente vulnerable se encuentra expuesto directamente en internet.
- Vulnerabilidad local, de manera totalmente opuesta, en este caso para acceder al componente vulnerable es necesario disponer de un acceso local al activo vulnerable. Este primer acceso local se puede conseguir mediante distintas vías:

- El atacante tiene acceso al activo vulnerable.
- El atacante ha comprometido previamente el activo vulnerable y tiene acceso de manera remota.

Dependiendo a quién va dirigida, dependiendo quien se vea afectado tras materializar la vulnerabilidad podremos realizar la siguiente agrupación

- Vulnerabilidades que afectan al cliente, en este caso concreto la materialización de la vulnerabilidad tiene un impacto directo sobre el cliente del aplicativo.
- Vulnerabilidades de servidor, en este otro caso la materialización de la vulnerabilidad afecta de manera directa al componente o servicio afectado.

Dependiendo de su tiempo de vida, dependiendo del tiempo de vida de una vulnerabilidad podemos englobar las vulnerabilidades en 3 tipos de categorías diferentes:

- Vulnerabilidades Zero day Este tipo de vulnerabilidades no se conocen de manera pública, tan siquiera por la organización responsable del diseño del producto afectado, sin embargo, la vulnerabilidad es descubierta y, normalmente, explotada por ciberdelincuentes para atacar sistemas. También puede referirse a la vulnerabilidad no conocida que encuentra un investigador de seguridad y la reporta a la compañía u organización responsable del producto. Aunque tengan constancia de la vulnerabilidad, hasta que no se publica la vulnerabilidad y se genera un parche o actualización para solventarla ésta es considerada una vulnerabilidad de tipo “0-Day”
- Vulnerabilidades One day Este tipo de vulnerabilidades ocurren cuando el producto afectado publica un parche para una vulnerabilidad que no se conocía. Al ser publicada se comparan las versiones anteriores con la versión publicada, se localiza el fallo en las versiones anteriores y se genera la vulnerabilidad para las versiones anteriores que presentan el fallo. Normalmente la prueba de concepto que explota la vulnerabilidad no está accesible de manera pública.
- Vulnerabilidades públicas Este tipo de vulnerabilidades explotan un fallo conocido en versiones antiguas del sistema o el software y cuyo código, para explotar la vulnerabilidad, se encuentra disponible de manera pública. De esta manera cualquiera puede acceder al código y utilizarlo para atacar los sistemas vulnerables.

3.- AUDITORÍAS DE HACKING ÉTICO

Existen distintos tipos de auditoría de hacking ético. Estas se pueden clasificar en base a una serie de premisas, por ejemplo, basándonos en la complejidad de la auditoría, basándonos en el origen de las pruebas, o según su enfoque. Además, estas categorías se pueden combinar entre sí. La única premisa a tener en cuenta es que sólamente podremos escoger un tipo de clasificación de cada grupo de categorías.

Por ejemplo, una auditoría puede catalogarse como “Test de intrusión externo con un enfoque de caja negra”. Por el contrario la siguiente catalogación “Auditoría Manual de la aplicación de venta online con un enfoque de caja negra y caja blanca” no sería correcto debido a que se indican dos categorías distintas del mismo bloque de clasificación. A continuación se detalla los distintos bloques de catalogación de auditorías.

3.1.- TIPOS DE AUDITORÍA DEPENDIENDO DEL ENFOQUE

Este tipo de clasificación se realiza atendiendo al tipo de enfoque que se quiera dar a la auditoría. Por ejemplo, ¿La auditoría a realizar estará orientada a cubrir una gran cantidad de activos de la compañía sin importar localizar vulnerabilidades mucho menos complejas? o, por el contrario, ¿Me interesa más tratar de simular un ataque real sobre la compañía?. Tipos de auditorías existentes dependiendo del enfoque que se le quiera dar:

Auditoría con pruebas automáticas

- Este tipo de pruebas se realizan únicamente empleando herramientas especializadas que, sin apenas iteración del auditor, identifican vulnerabilidades en los sistemas remotos.
- Normalmente indican posibles vulnerabilidades basándose en la versión del servicio o aplicativo que se encuentra prestando servicio en un determinado puerto.
- Debido a la forma en la que se detectan las vulnerabilidades, se producen muchos falsos positivos. Por ello, el auditor ha de verificar la veracidad de las vulnerabilidades.
- Una auditoría que haga uso de pruebas automáticas tiene por objetivo identificar el mayor número de posibles vulnerabilidades en los activos auditados consumiendo un menor menor tiempo de auditoría.
- Normalmente se realizan como primera opción en empresas que presentan un nivel de madurez en seguridad bastante bajo, para hacerte una primera idea de los activos disponibles y sus vulnerabilidades potenciales. También se puede realizar este tipo de auditorías de manera recurrente para verificar rápidamente cambios en los activos.

Auditoría con pruebas manuales

- Las pruebas se realizan por un auditor de manera manual, apoyándose en herramientas específicas dependiendo de la técnica utilizada.
- También pueden hacer uso de aplicaciones automáticas, para realizar una cobertura rápida de posibles vulnerabilidades que tendrá que verificar manualmente.
- Tienen como objetivo detectar vulnerabilidades que requieran de un estudio más minucioso y en las que son necesarias adaptar las pruebas a realizar.

Test de intrusión

- Las pruebas se realizan por un auditor de manera manual apoyándose en herramientas específicas. También se contempla el uso de sistemas secundarios para ciertos tipos de pruebas.
- Tratan de comprometer el sistema remoto a través de una vulnerabilidad identificada.
- Tienen como objetivo comprobar el grado real de amenaza que podría producirse al aprovecharse de las vulnerabilidades localizadas durante la auditoría y verificar el impacto específico que tendrían sobre la compañía.

Test de intrusión físico

- Las pruebas se realizan intentando acceder a las instalaciones de la compañía sin previo aviso.
- La finalidad de las pruebas consiste en medir las capacidades de contención y detención de un acceso no autorizado en las distintas sedes u oficinas del cliente auditado.
- En ocasiones, como parte de la auditoría, también se deja conectado un dispositivo no autorizado en la red con el propósito de conectarse a la red de manera remota y desde ahí realizar la intrusión.

Ejercicio de Red Team

- Las pruebas que se realizan tratan de simular ataques e intrusiones complejas por parte de un ciberdelincuente.
- No se proporciona ningún tipo de información de partida y el auditor ha de realizar una fase de reconocimiento previo al igual que lo haría un atacante.
- Únicamente se informa a un grupo muy reducido de la organización de la realización de las pruebas. No se informa a los equipos de seguridad de la realización del mismo con la finalidad de medir su capacidad de respuesta ante un ataque real.
- Se diseñan escenarios de ataque específicos a realizar en función del grado de madurez de la organización auditada.
- Se definen varios objetivos a cumplir y se establecen ciertas restricciones o líneas rojas que no han de ser sobrepasadas.

3.2.- TIPOS DE AUDITORÍA DEPENDIENDO DEL ORIGEN

Este tipo de clasificación se realiza atendiendo al punto en el que se encuentre posicionado el auditor para realizar las pruebas de auditoría.

Auditoría con pruebas externas

- Las pruebas se realizan de manera totalmente externas a la infraestructura del cliente (desde internet). Dicho de otro modo “Desde fuera”.
- Tienen por objetivo descubrir vulnerabilidades que se pudieran encontrar en el perímetro externo de la compañía. Es decir, en los activos que la compañía tiene expuestos en internet.
- Se parte de el supuesto en que el ciberdelincuente quiere realizar alguna de las siguientes acciones:

- Robo de información/espionaje industrial.
- Causar un impacto económico.
- Realizar fraude contra los usuarios.

Auditoría con pruebas internas

- Las pruebas se realizan desde la infraestructura interna del cliente. Dicho de otro modo, "Desde Dentro".
- Tienen por objetivo descubrir vulnerabilidades que un atacante podría localizar si se encontrase dentro de la compañía.
- Se parte de los siguientes supuestos:

- Empleado descontento.
- Equipo de empleado comprometido.
- Dispositivos no autorizados conectados en la red (por ejemplo, tras una intrusión física).

3.3.- TIPOS DE AUDITORÍA DEPENDIENDO DE LA INFORMACIÓN PROPORCIONADA

Este tipo de clasificación se realiza atendiendo a la información proporcionada al auditor para realizar las pruebas de auditoría.

Auditoría con pruebas de caja negra

- Las pruebas se realizan sin ningún tipo de conocimiento sobre la aplicación o infraestructura a auditar.
- No se dispone de tecnologías utilizadas, frameworks o lenguajes de programación utilizados, diagramas de red o de flujo, etc.
- En este tipo de pruebas si se contempla que puedes partir de uno, varios usuarios iniciales o, que por el contrario, no dispongas de ningún usuario al iniciar las pruebas.

Auditoría con pruebas de caja blanca

- Las pruebas se realizan con toda la información necesaria relativa a la aplicación o sistema, infraestructura, diagramas de red o de flujo, etc.
- En ciertas ocasiones también se dispone del código fuente del aplicativo a auditar para poder localizar vulnerabilidades en código.
- Posibilidad de realizar consultas a los responsables del servicio o aplicativo a fin de ampliar el conocimiento necesario para auditar el sistema o aplicativo lo más concretamente posible.
- Normalmente se parte, al menos, con un usuario inicial que nos permita acceso al aplicativo o infraestructura. Aunque también nos pueden proporcionar usuarios con distintos privilegios o roles.

Auditoría con pruebas de caja gris

- Las pruebas se realizan con información parcial de la aplicación o sistema interno. Por ejemplo, te pueden indicar las tecnologías utilizadas, diagramas de red, pero no disponer del código fuente del aplicativo.
- En ocasiones también se crean reglas de excepción en el firewall para realizar la auditoría para evitar que al realizar las pruebas exista algún mecanismo de defensa, ajeno al activo a auditar, que no permita realizar las pruebas de manera correcta.

3.4. FASES DE UNA AUDITORÍA

El proceso de auditoría comprende una serie de fases definidas con los hitos a cumplir antes, durante y después de las pruebas. Dependiendo de la duración de las mismas, o incluso si se realizan en un período cíclico, existen fases que pueden estar presentes.

- Pre-engagement o toma de requisitos: Se reúnen las partes implicadas y se acuerdan ciertos aspectos organizativos y procedimentales.
- Realización de las pruebas: Esta es la fase de realización de las pruebas, varía dependiendo en enfoque acordado, tiene una duración finita.
- Seguimiento de las pruebas: Ei la duración de las pruebas se estima que va a ser demasiado extensa en el tiempo se agendan reuniones de seguimiento.
- Reporting o documentación: Es la fase de generación de informes. En estos informes se describen todas las vulnerabilidades localizadas y catalogadas en base a su riesgo. También se realiza un "informe ejecutivo” en el que se detalla a alto nivel el nivel de madurez en materia de seguridad de los activos auditados.
- Cierre de auditoría: Se entregan los informes al cliente y se agenda una reunión de cierre con el cliente en la que se presentan los resultados.

3.4.1.- PRE-ENGAGEMENT O TOMA DE REQUISITOS

La fase de Pre-engament o toma de requisitos engloba todas las labores organizativas y procedimentales previas a la realización de las pruebas de seguridad así como establecer los

requerimientos, y obligaciones de ambas partes. Se divide en dos tipos de labores que detallaremos.a continuación.

Labores organizativas
Se refieren a las acciones a tener en cuenta antes de iniciar la auditoría y a recopilar toda la información necesaria para la correcta ejecución de las pruebas. A continuación mostramos los puntos indispensables:

- Delimitar el alcance de la auditoría

Se ha de limitar el alcance de las pruebas para acotar los activos a auditar con la finalidad de calcular el tiempo necesario de auditoría y/o priorizar sistemas críticos. A continuación se muestran ejemplos de alcance de las distintas auditorías:
- Auditar determinados sistemas o aplicación/aplicaciones específicas. Nos tienen que proporcionar la IP o el nombre de host para identificar los activos específicos a auditar.
- Auditar todo un dominio o un rango de direcciones IP.
- Auditar todos los activos dado un nombre de organización (Enfoque de Red Team).

- Entorno y enfoque de las pruebas (producción, preproducción)

Se ha de tener claro el tipo de pruebas que se realizarán durante la auditoría (automáticas, manuales, test de intrusión, ejercicio de Red Team, etc.).
También se especificarán el origen de las pruebas, si se va optar por realizar la auditoría desde un enfoque interno o totalmente externo a la organización. En este último caso se procederá a indicar al cliente la dirección IP de origen de las pruebas del auditor.
Además, se ha de especificar el entorno en el que realizar las pruebas, en condiciones normales las pruebas se realizan en producción. Sin embargo, dependiendo de la criticidad de la aplicación es posible que tengamos que realizar las pruebas en algún otro entorno secundario para no interferir en la aplicación que se encuentra prestando servicio.
- Producción: Entorno en el que presta servicio la aplicación
- Preproducción/Integración: Es un entorno secundario no accesible al usuario. Suele ser una réplica del entorno de producción en el que se prueban nuevas funcionalidades antes de pasarlas a producción.
- Desarrollo: Entorno en el que se van probando los nuevos desarrollos de la aplicación previa a su paso a preproducción/integración. Suele ser un entorno bastante inestable debido a que crean nuevas funcionalidades, o modifican las existentes, continuamente. Es decir, “No hay una foto fija”.

- Necesidad de usuarios

Se ha de determinar si se necesitan usuarios para realizar las pruebas o si las pruebas se inician sin disponer de ningún usuario. Por otro lado, en ciertas ocasiones, también puede ser preferible disponer de varios usuarios con distintos roles (o distintos niveles de privilegios) que me permitan realizar pruebas de autorización o lógica de negocio que de otro modo no podría realizar (Por ejemplo, acceder a operativas de un usuario más privilegiado).

- Personas de contacto

Se han de designar las personas de contacto por parte de la entidad auditada y del personal que realiza la auditoría a fin de coordinar, en el menor tiempo posible, cualquier duda, incidencia o problemática que pudiera surgir durante la realización de las pruebas.

Labores procedimentales
Recopila todos los procedimientos específicos que deberemos seguir a la hora de realizar las pruebas o comunicarnos con el cliente durante las pruebas. A continuación mostramos los puntos indispensables:

- Permisos y autorizaciones

Dependiendo de la criticidad de la auditoría, o el tipo de ejercicio es posible que haya que rellenar unos documentos acreditativos en los cuales el cliente autoriza a los auditores a realizar la auditoría sobre el alcance establecido.
Este tipo de autorizaciones son de especial importancia cuando las pruebas a realizar incluyen las siguientes características:
- Se realiza un test de intrusión físico.
- Se realiza un ejercicio de RedTeam.
- El activo a auditar es crítico para el negocio.
- El activo a auditar se encuentra en un ISP que presenta una política restrictiva ante este tipo de pruebas.

Acceso al activo
Se acuerda el tipo de acceso que se necesita para poder tener visibilidad del equipo a auditar. Dependiendo de si el activo a auditar se encuentra accesible de manera pública en internet, o por el contrario el sistema a auditar se encuentra en alguna DMZ protegida y sea necesario habilitar un acceso específico para poder acceder a los activos de la auditoría.
En otras ocasiones, los activos a auditar se encuentran en el entorno de preproducción o desarrollo en la red interna de la compañía, siendo necesario algún acceso especial como el uso de una VPN.

Limitaciones horarias
Otro de los puntos a tener en cuenta es que debido a la naturaleza de la aplicación sea necesario establecer una franja horaria en la que realizar ciertas pruebas específicas, o incluso toda la auditoría. Este hecho dependerá en mayor medida de las preferencias del cliente. Por ejemplo, ciertas aplicaciones críticas y con gran carga de trabajo puede ser preferible auditarlas fuera del horario laboral por si hubiera algún problema se pudiera solucionar antes del horario laboral.

Limitaciones de funcionalidad
De la misma manera, también es posible que existan ciertas funcionalidades o servicios que queden excluidos del alcance de la auditoría.
Por ejemplo, en caso de realizar una auditoría en un cliente bancario, es posible que no se encuentren permitidas la realización de transferencias bancarias con una cuenta legítima de un usuario del banco auditado y tengan que utilizarse cuentas específicas para tales pruebas.

Pruebas no permitidas
Debido a la naturaleza “destructiva” de cierto tipo de pruebas es posible que no se permita realizar pruebas sobre este tipo de operativa a no ser que se indique lo contrario.
Un ejemplo claro de este caso son las pruebas de Denegación/Degradación de Servicio.

Comunicación de incidencias graves
Hay que tener en cuenta si el cliente precisa que se le comuniquen las incidencias de criticidad grave previo a la entrega del informe. Mostrar retroalimentación
Esta casuística es muy común en aplicaciones o sistemas catalogadas de alto riesgo. De esta manera el equipo resolutor puede comenzar a buscar una solución a la vulnerabilidad encontrada lo antes posible.

Aviso de inicio de pruebas

En algunas organizaciones que presentan un alto nivel de madurez en materia de “seguridad informática”, es posible que se requiera avisar por correo electrónico al inicio y a la finalización de las pruebas de manera diaria. Además, se ha de indicar la dirección IP de origen de las pruebas.
Este procedimiento es habitual para que los equipos que se encarguen de la monitorización de incidencias de seguridad puedan verificar que se trata de una prueba controlada y no de un ataque real.

3.4.2.- EJECUCIÓN DE LAS PRUEBAS

Para poder tener una estructura a la hora de realizar un análisis de infraestructura, éste se divide en distintas fases que nos ayudan a mantener un orden de pruebas. Los resultados obtenidos en cada fase retroalimentan la siguiente y aunque hay algunas metodologías que incluyen fases adicionales, todas tienen en común las fases del siguiente gráfico. Cada una de estas fases.
Fase de reconocimiento, En esta fase se recopila información acerca de los activos a auditar, se hace un análisis de la infraestructura a auditar, servicios activos, versiones de sistema operativo y software que presentan los activos.
Fase de escaneo, en esta fase se detectan vulnerabilidades que puedan existir en los sistemas y servicios obtenidos en la fase de reconocimiento.
Fase de explotación, en esta fase se materializa la explotación de las vulnerabilidades obtenidas en la fase de escaneo. El objetivo es lograr un mayor nivel de acceso o de privilegios en los activos.
Fase de postexplotación, en esta última fase partimos de un acceso en el sistema remoto a través de una vulnerabilidad previamente explotada. Se realizan técnicas para poder aumentar el nivel de privilegios en este sistema, acceder a otros activos internos, ejecutar técnicas que nos brinden un acceso secundario sin tener que volver a explotar la vulnerabilidad, etc. Como cabe suponer, en caso de no haber obtenido resultados en la fase de explotación, esta fase no podría desarrollarse.

3.4.3.- SEGUIMIENTO DE LAS PRUEBAS

Si se estima que la duración de las pruebas puede extenderse demasiado en el tiempo, por ejemplo varios meses, se realizan reuniones de seguimiento entre los auditores y el personal de la compañía auditada. Por regla general, estas reuniones de seguimiento presentan las siguientes características:

- Las reuniones de seguimiento se realizarán cada 1-2 semanas.
- Se comunicarán al cliente los hallazgos localizados desde la reunión anterior. Se comentarán posibles desviaciones en el itinerario de la auditoría o problemas que pudieran haber surgido desde la reunión anterior.
- Se decidirá en qué activos o secciones incrementar el esfuerzo en las próximas semanas.
- Se confirmará el itinerario y siguientes pasos en la auditoría/pruebas.

3.4.4.- REPORTING O GENERACIÓN DE INFORMES

Es la fase de documentación y generación de informes. En estos informes se describen todas las vulnerabilidades localizadas y catalogadas en base a su riesgo. También se realiza un "informe ejecutivo” en el que se detalla a alto nivel el nivel de madurez en materia de seguridad de los activos auditados.
El informe de Auditoría es el entregable real que se presenta al cliente, es decir, el resultado del trabajo realizado. Tiene como misión los siguientes objetivos:

- Informar a las capas superiores de los vulnerabilidades localizadas y el riesgo particular que pueden generar sobre el activo.
- Informar al personal técnico de las vulnerabilidades localizadas, mostrar cómo reproducirlas y aportar una recomendación para solucionar o mitigar la vulnerabilidad.

Dependiendo del tipo de audiencia al que vaya dirigido el informe (Técnicos o la Dirección) se realizarán informes que se enfoquen más en los problemas técnicos y cómo solventarlos o en el riesgo y posible impacto en el negocio que tiene cada vulnerabilidad en caso de ser explotada. Tipos de Informe:

Informe ejecutivo
Aunque también puede generarse como un informe separado, normalmente en el informe de resultados auditoría se recoge tanto el informe ejecutivo como el informe técnico para que personal de ambos roles puedan interpretarlo. Sin embargo, un empleado con un rol de gestión se apoyará en el resumen ejecutivo para interpretar los riesgos de cada vulnerabilidad y la criticidad de la misma (Basada en el estándar CVSS).
El informe ejecutivo recoge las siguientes secciones:

- Metodología utilizada durante las pruebas.
- Alcance y objeto de la Auditoría.
- Consideraciones y limitaciones.
- Criticidad de las vulnerabilidades descubiertas.
- Resumen de vulnerabilidades.
- Resumen de recomendaciones.

Informe técnico
El informe técnico se encuentra dirigido al personal técnico de la organización dado que se detalla la problemática específica de la vulnerabilidad, razones por las que se produce, detalles para reproducir o explotar la vulnerabilidad y una aproximación a la resolución de las mismas.
Por cada vulnerabilidad localizada detallan los siguientes datos:

- Título de la vulnerabilidad.
- Vector CVSS.
- Valoración CVSS.
- Riesgo.
- Descripción.
- Detalle de la vulnerabilidad.
- Riesgo en caso de ser explotada.
- Recomendación de solución.

Presentación de resultados
Más que un informe es una presentación ejecutiva para explicar las vulnerabilidades y sus riesgos asociados.
Se utiliza durante la presentación de resultados en la fase del cierre de auditoría para estructurar todas las vulnerabilidades localizadas y sus recomendaciones asociadas. Presentación de resultados

3.4.5.- CIERRE DE AUDITORÍA

Se entregan los informes al cliente y se agenda una reunión de cierre con el cliente en la que se presentan resultados y se resuelven dudas.
Por regla general, estas reuniones de seguimiento se caracterizan por las siguientes cuestiones:

- Se realizan una vez han finalizado todos los trabajos de auditoría y se ha entregado el informe de resultados al cliente para que tenga conocimiento de los hallazgos previo a la reunión de cierre.
- Suelen estar involucrados varios departamentos del cliente auditado (Desarrollo, Departamento de Sistemas, Departamento de Seguridad informática (CISO) e, incluso, parte de la alta dirección).
- Se presentan los resultados a alto nivel y se entra en detalle en vulnerabilidades de gravedad más crítica o en cualquiera que el cliente tenga dudas o desee aclarar alguna cuestión.
- Además, se presentan recomendaciones para solventar cada una de las vulnerabilidades localizadas durante la auditoría, aunque el cliente es quién decide la mejor solución ya que tiene todo el conocimiento necesario de cómo está estructurada su infraestructura.

- Se acuerda el posible seguimiento de la resolución de las vulnerabilidades localizadas durante la auditoría para verificar si la solución implementada corrige de manera efectiva la vulnerabilidad.

4.- HERRAMIENTAS DE SEGURIDAD Y HACKING ÉTICO

Por si esto no fuera suficiente, la comunidad open source aporta a este ecosistema la gran mayoría de las herramientas utilizadas. Esto quiere decir que muchas de las herramientas que se utilizan activamente hoy en día puede que queden desactualizadas o en desuso en un futuro. Sin embargo, aparecerán nuevas herramientas destinadas a suplir las carencias que pudieran tener las anteriores.

4.1.- HERRAMIENTAS DE DESCUBRIMIENTO Y RECONOCIMIENTO

La fase de reconocimiento es la primera de todas las fases de una auditoría de sistemas o infraestructura. En ella se trata de obtener la máxima cantidad de información posible de los activos que conforman el alcance de la auditoría.

Reconocimiento pasivo

Es el proceso de recolección de información del objetivo que se está auditando a través de fuentes de información de dominio público. En ningún momento se establece comunicación con el objetivo. En su lugar, esta información es obtenida a través de motores de búsqueda (Google, Bing, etc.), whois, página web de la organización, etc. Algunas herramientas utilizadas durante el reconocimiento pasivo:

- Redes Sociales

Actividades:

- Obtener datos de contacto y personales
- Averiguar intereses personales
- Averiguar tecnologías utilizadas en la compañía

Herramientas:

- twitterscrapper: Recopila información de un determinado perfil en twitter.
- ultimate facebook scrapper: Recopila información de un perfil en Facebook.
- scrapedin crawler: Recopila información de un determinado perfil en LinkedIn.

- Aplicaciones colaborativas

Actividades:

- Se puede obtener las tecnologías utilizadas en la organización. Redes Sociales Aplicaciones colaborativas
- Se puede llegar a obtener porciones de código de aplicativos desarrollados por el cliente objeto de la auditoría.
- Se pueden llegar a extraer credenciales de usuario o APIKeys.

Herramientas:

- pastehunter: Realiza búsquedas en pastebin buscando información sensible o fragmentos de código
- githubscrapper: Herramienta para buscar información sensible en GitHub, encuentra credenciales, APIKeys, ficheros de configuración, etc.

- Buscadores

Actividades:

- Se pueden realizar búsquedas muy concretas haciendo uso de operadores de búsqueda.
- Existen recopilaciones de búsquedas tipo para localizar rápidamente sistemas vulnerables, dispositivos expuestos, etc.

Herramientas:

- Google: Es el buscador más utilizado. Dispone de numerosos operadores de búsqueda.
- Bing: Buscador de Microsoft. Permite realizar búsquedas basadas en direcciones IP.
- Shodan: Indexa tecnología y servicios. Permite realizar búsquedas por servicios y versiones concretas.

- Censys: Buscador parecido a Shodan. Permite realizar activos que compartan los mismos datos en el certificado.

- Registros whois

Actividades:

- Se pueden obtener a quién pertenece una dirección IP pública y sus datos de contacto.
- Se puede localizar los rangos de direccionamiento IP pertenecientes a una determinada compañía.

Herramientas:

- comando whois: Herramienta de consola versiones para vario S.O.
- whois.domaintools.com: Servicios web que nos facilitan la realización de consultas whois a través de este portal en internet

- Email harvesting

Actividades:

- Búsqueda de direcciones de correo electrónico del personal perteneciente a la compañía auditada.

Herramientas:

- theHarvester: Herramienta que recopila información sobre direcciones de correo electrónico asociadas a un determinado dominio.

Reconocimiento activo

Es el proceso de recolección de información del objetivo que se está auditando a través del uso de técnicas o herramientas que se comunican con el activo a auditar.
Estas pruebas pueden ser detectadas por el objetivo dado que es necesaria una interacción directa contra el mismo. Por ejemplo, realizar un descubrimiento de puertos, un crawling, etc.
A continuación se muestran algunas herramientas utilizadas durante el reconocimiento activo:

- Enumeración DNS

Actividades:

- Averiguar la dirección IP asignada a un host (y en algunas ocasiones el host asociado a una determinada dirección IP).
- Obtener los principales servidores asociados a un dominio (NS, MX y SOA).
- Si se encuentra mal configurada la transferencia de zona se pueden volcar todos los registros del dominio.

Herramientas:

- dig y nslookup: herramientas de consola que nos permite realizar consultas DNS de manera manual.
- dnsrecon: automatiza todas las consultas que deberíamos realizar mediante dig o nslookup. Además, Nos proporciona la información de manera estructurada.
- dnsenum: Similar a dnsrecon pero aporta la ventaja de realizar descubrimientos de host y/o subdominios mediante técnicas de fuerza bruta.

- Enumeración SMTP

Actividades:

- Enumerar cuentas de usuario en un determinado dominio.

Herramientas:

- smpt-user-enum: Script que automatiza la enumeración de cuentas de usuario a través del protocolo SMTP y mediante los comandos (RCPT, EXPN y VRFY).

- Enumeración SNMP

Actividades:

- Obtener información de la configuración de dispositivos.
- Modificar la configuración de los dispositivos. Utiliza claves por defecto "public" y "private" para acceder a la información o gestionar los dispositivos respectivamente.

Herramientas:

- onesixtyone: utiliza técnicas de fuerza bruta para averiguar los community strings que nos permiten acceder a los roles public y private.
- snmpwalk: En caso de disponer (o averiguar) las community string de acceso se puede acceder a la configuración de un dispositivo.

- Enumeración SMB

Actividades:

- Permite obtener información de la configuración de una red Microsoft Windows:
  - Políticas de contraseñas
  - Usuarios
  - Grupos
  - Equipos
  - ID de usuario y host

Herramientas:

- nbtscan y enum4linux: Herramientas que establecen una sesión con el sistema remoto y recupera la información disponible.
- Scripts nmap: nmap es una herramienta de análisis de red que proporciona capacidades de enumeración gracias a diversos scripts.

4.2.- HERRAMIENTAS DE ESCANEO Y MONITORIZACIÓN

La fase de escaneo se realiza después de realizar la fase de reconocimiento. En ella tratamos de obtener más información sobre el propósito de los activos incluidos en el alcance de las pruebas.
Se averigua los distintos componentes de la infraestructura, el rol que desempeña cada activo, el número de servicios y versiones de los mismos que se encuentran prestando servicio en cada activo. Además, también se realiza un análisis de las posibles vulnerabilidades existentes en el sistema tomando como referencia las versiones de los servicios que el activo sustenta así como la versión del Sistema Operativo. De esta manera podremos localizar si los activos auditados presentan algún tipo de vulnerabilidad publica.
Tipos de escaneo y una serie de herramientas para poder realizarlos.

Escaneo de red

Trata de obtener mayor información sobre la red objetivo, direccionamiento IP y la arquitectura utilizada para sustentar la infraestructura.

- Wireshark / tcpdump

Wireshark y tcpdump son dos motores de análisis de los datos transmitidos en una comunicación que circula por la red. Aunque no son herramientas que realicen labores de escaneo, se utilizan para poder capturar y analizar los paquetes que enviamos o recibimos a través de nuestra interfaz de red.

- arpscan / net discover

Ambas herramientas permite el descubrimiento de equipos remotos monitorizando los mensajes broadcast de tipo ARP Discovery que llegan a nuestro interfaz de red.

- nmap como escáner de red

La herramienta nmap puede ser utilizada en los tres tipos de categorías de escaneo (Escaneo de red, escaneo de servicios y escaneo de vulnerabilidades). En el caso de realizar un escaneo de red hay que saber previamente el rango de red a escanear (Dato que puede obtenerse mediante el uso de las dos herramientas anteriores)

Escaneo de servicios

Orientada a obtener información sobre los servicios específicos, versiones y tecnología de los mismos presentes en cada activo de la infraestructura.

- nc / netcat

Herramienta de red que permite establecer comunicación con los puertos TCP/UDP, asociar una shell a un puerto en concreto y poner un puerto UDP/TCP a la escucha. Además, el operador -z permite utilizar nc como escáner de puertos

- nmap como escáner de servicios

En cuanto al escaneo de servicios nmap puede localizar puertos abiertos en equipos remotos y utilizar varias técnicas para evadir los sistemas de protección de red en el protocolo TCP.
Estás técnicas de evasión se basan en el funcionamiento del establecimiento de la comunicación en el protocolo TCP

- Zenmap

Proporciona las mismas capacidades que la herramienta nmap pero incorpora la particularidad de poder representar los resultados mediante una interfaz gráfica de una manera más visual. También incluye ciertos tipos de escaneos preconfigurados a falta de introducir el objetivo

Escaneo de vulnerabilidades

Una vez completado los escaneos de red y de servicios, se comprueba si existe alguna vulnerabilidad conocida para cada protocolo y versión del software utilizado.

- nmap como escáner de vulnerabilidades

Es posible utilizar nmap como escáner de vulnerabilidades haciendo uso de los scripts de detección de vulnerabilidades.

- Scripts específicos: Scripts de nmap que buscan ciertas vulnerabilidades de las versiones de algunos servicios. Todos estos scripts se engloban bajo la categoría “vuln” podemos indicar que ejecuten los scripts de este tipo.

- Proyecto vulscan: Utiliza nmap para realizar una búsqueda de posibles vulnerabilidades basándonos en la versión de los servicios localizados en el sistema remoto. Se apoya en un script nse y una base de datos de vulnerabilidades locales para detectar los servicios vulnerables

- nessus

Nessus es la aplicación de escaneo de vulnerabilidades más conocida y utilizada. Realiza los tres tipos de escaneos (escaneo de red, escaneo de servicios/versiones y escaneo de vulnerabilidades) de una manera totalmente desatendida.

- OpenVas

Es un scanner de vulnerabilidades de seguridad parecido a Nessus, también realiza los tres tipos de escaneo de manera desatendida. Aunque tiene una versión de pago, los plugins que detectan las vulnerabilidades no se encuentran tan actualizados como los de nessus.

4.3.- HERRAMIENTAS DE EXPLOTACIÓN

Tras la identificación de vulnerabilidades en los servicios identificados en las fases anteriores, el siguiente paso es poder explotar las vulnerabilidades que hubieran sido descubiertas.
El objetivo de esta frase es mostrar el riesgo real de la vulnerabilidad, en base a la confidencialidad integridad y disponibilidad de la información. Para ello necesitamos hacer uso de ciertas herramientas de explotación dependiendo del vector de ataque. Se enumeran algunas con sus principales características.

Explotación de vectores específicos
Aunque el vector más común de ataque consiste en la explotación de una vulnerabilidad, no es el único vector que nos puede dar acceso a un equipo remoto. A continuación, realizamos una enumeración de los más importantes

- Ejecución de un programa malintencionado

También conocido como malware consiste en generar un payload o shellcode en un formato ejecutable o camuflado dentro de un programa legítimo. Este programa se puede distribuir de distintas maneras a las víctimas, pero siempre está condicionado a un factor de ingeniería social para que la víctima ejecute el malware.
Por ejemplo, esconder el payload en una macro de Excel y enviar un correo masivo a los empleados de una compañía para que crean que en el Excel está la relación de subidas salariales.
Herramientas:
- msfvenom: herramienta para generar y ofuscar malware para distintas plataformas.
- shellter: Herramienta utilizada para camuflar Malware en aplicativos legítimos.
- goPhish: Framework dedicado al envío de correos Phishing.

- Credenciales por defecto o poco robustas

Vector de acceso muy común debido a que cierto software y dispositivos de red se despliegan con una contraseña por defecto establecida por el fabricante. Si esta contraseña no se modifica, puede ser utilizada por un atacante para ingresar en el sistema.
Herramientas:
- Patator: Herramienta para realizar ataques de fuerza bruta con alto grado de configuración. Permite establecer las condiciones necesarias evaluar la respuesta emitida por el equipo remoto y considerar si las credenciales introducidas son correctas.
- Medusa: Herramienta que realiza fuerza bruta de Login en distintos protocolos. Permite paralelismo de conexiones.
- Hydra: Herramienta que realiza fuerza bruta de Login en distintos protocolos. Se recomienda para realizar fuerza bruta de las community strings de SNMP.

Proxies de interceptación
Son herramientas que nos permiten monitorizar las comunicaciones de red e incluso modificar la información enviada por el protocolo. Normalmente este tipo de herramientas se utilizan en comunicaciones a nivel HTTP/HTTPS.

- BurpProxy

Proxy de interceptación HTTP/HTTPS dispone de una versión community (gratuíta) y una versión de pago que incluye numerosas características. Permite monitorizar y modificar el tráfico HTTP/HTTPS, dispone de plugins para ampliar las capacidades del framework e incluso dispone de una funcionalidad de escáner automático.

- ZapProxy

Proxy de interceptación HTTP/HTTPS es una herramienta opensource desarrollado por la fundación OWASP. Permite monitorizar y modificar el tráfico HTTP/HTTPS, dispone de plugins para ampliar las capacidades del framework e incluso dispone de una funcionalidad de escáner automático.

- Echo Mirage

Proxy de interceptación para Sistemas Operativos Microsoft windows que permite monitorizar y modificar los paquetes de red de cualquier protocolo. Está muy limitado en el sentido que no se puede modificar el tamaño del paquete de datos a enviar.

Exploits públicos o Pruebas de Concepto (PoC)
Son herramientas específicas para aprovecharse de una vulnerabilidad en concreto, se suelen desarrollar con fines educativos y suelen disponer de licencia opnesource

- exploit-db

Base de datos online de búsqueda de vulnerabilidades y exploits. disponible en la dirección URL

- Github como repositorio de pruebas de concepto

Utilizado como repositorio de código fuente, también podemos localizar pruebas de concepto de vulnerabilidades, e incluso exploits totalmente funcionales.

- searchsploit

Herramienta disponible en Kali Linux, Base de Datos local con todos los exploits públicos de exploit-db.

Frameworks de explotación
Son herramientas tipo suite que incluyen un gran número de exploits de vulnerabilidades conocidas así como otras características de explotación y postexplotación como puedan ser módulos auxiliares de escaneo, shells avanzadas, servidores tipo Command and Control, etc.

- Metasploit

Esta herramienta es una suite completa de Explotación y Postexplotación y contiene una gran cantidad de exploits y módulos auxiliares para su consulta y uso. Dispone de versiones open source y comercial

- CobaltStrike

En este caso Cobaltstrike es un servidor Comand and Control totalmente configurable, además posee bastantes módulos de postexplotación y un shellcode propio llamado "beacon". En este caso es una herramienta comercial.

4.4.- HERRAMIENTAS DE POSTEXPLOTACIÓN
La fase de Postexplotación está separada por una delgada línea de la fase de explotación. Y es que las dos fases son prácticamente idénticas, la única diferencia es que en la fase de Postexplotación ya partimos de un primer sistema comprometido y nuestro objetivo será utilizar los mismos vectores de ataque para conseguir elevar privilegios en el equipo comprometido o intentar explotar otro equipo al alcance desde el equipo comprometido. Utilizar el equipo para “pivotar” a red interna, etc.
De esta manera, gran parte de las aplicaciones utilizadas durante la fase de explotación también serán utilizadas en esta fase de Postexplotación.

Sellcodes
Una shellcode es un tipo de payload que normalmente inicia una Shell de comandos en un equipo que se ha podido comprometer a través de una vulnerabilidad o exploit, pudiendo controlar de manera remota la máquina comprometida.

- msfvenom

La herramienta msfvenom es un framework incluido en la suite Metasploit que se utiliza para generar los payloads y/o shellcodes. Se puede utilizar la herramienta para generar estos payloads por separado y en numerosos formatos de salida.

- Meterpreter

Meterpreter es un payload avanzado de tipo Shellcode disponible en Metasploit. Es extensible de manera dinámica mediante la inyección de librerías dlls, pudiendo cargar módulos en el equipo comprometido de manera dinámica. Además, se ejecuta msfvenom Meterpreter enteramente en memoria sin dejar traza en disco. Puede inyectarse en distintos procesos siempre que dispongamos de privilegios elevados para modificar el contexto del proceso.

- Beacon

Beacon es el payload avanzado de Cobalt. Es totalmente configurable y permite la modificación de shellcodes a través del “Artifact-Kit”. También permite modificar los protocolos de comunicación que utiliza para tratar de pasar desapercibido mediante tráfico legítimo.
Al igual que meterpreter, puede inyectarse en otros procesos y ejecutarse enteramente en memoria. Por otro lado, permite la carga dinámica de módulos.

Elevación de privilegios
Es el proceso que describe la acción de conseguir un nivel de permisos más elevados en un sistema, existen numerosas técnicas y herramientas para poder realizar este tipo de acciones. A continuación se presentan algunas de las más utilizadas:

- PrivescCheck

Esta herramienta es capaz de enumerar los problemas más comunes de configuración de Windows que se pueden aprovechar para la escalada de privilegios locales. También recopila diversa información que puede ser útil para la explotación y/o post-explotación.
El propósito de esta herramienta es ayudar a los consultores de seguridad a identificar posibles debilidades en las máquinas con Windows durante los Test de intrusión. Genera muchas trazas en el equipo remoto.

- WinPEAS

Al igual que PrivescCheck realiza una búsqueda de patrones claros en la configuración, o en la falta de actualizaciones del sistema, que permitan a un usuario realizar una elevación de privilegios local en un sistema Microsoft Windows.
Como particularidad, para cada técnica de elevación de privilegios presenta un enlace a la información necesaria para aprovecharse de ella.

- LinPEAS

Al contrario que WinPEAS realiza una búsqueda de patrones claros en la configuración, o en la falta de actualizaciones del sistema, que permitan a un usuario realizar una elevación de privilegios local en sistemas basados en LINUX.
De manera similar a su homólogo, para cada técnica de elevación de privilegios presenta un enlace a la información necesaria para aprovecharse de ella.

Extracción de información
Es el proceso que se realiza para tratar de extraer información confidencial o sensible del sistema, por ejemplo, credenciales o hashes.

- Mimikatz

Herramienta utilizada para extraer información sensible de la memoria RAM de Windows, se pueden extraer hashes, credenciales en claro, tokens, etc.
También permite ejecutar técnicas avanzadas para utilizar las credenciales y hashes capturadas, como son el uso de técnicas de tipo "Pass the Hash" y la generación de "Golden Tickets".

- Keyloggers

Las herramientas de tipo keylogger se ejecutan en una máquina comprometida para capturar todas las pulsaciones de teclado. De esta manera se puede llegar a recopilar credenciales que el usuario del equipo haya podido introducir para acceder a un determinado sistema o aplicativo

Autoevaluación I

Cómo describirías a un hacker.

a) Aquella persona con conocimientos de seguridad informática que cuándo descubre una vulnerabilidad la vende en la darknet.
b) Aquella persona que dispone de conocimientos normativos en materia de seguridad y ayuda a las empresas a cumplir determinados estándares normativos en materia de seguridad
c) Un hacker es una persona técnica con grandes conocimientos de seguridad que orienta su trabajo en entender cómo se comportan los sistemas/aplicativos y trata de localizar vulnerabilidades para comunicarlas a la comunidad o al propietario del componente afectado
d) Un hacker es una persona técnica con grandes conocimientos de seguridad que orienta su trabajo en entender cómo se comportan los sistemas/aplicativos y trata de localizar vulnerabilidades con fines sociales, ecológicos, humanitarios o que tenga repercusión en la defensa de los derechos humanos.

Autoevaluación II

Indica cuáles de las siguientes afirmaciones son verdaderas o falsas.

1- La confidencialidad garantiza que la información no puede ser modificada
a) Verdadero
b) Falso

2- La confidencialidad garantiza que la información no puede ser accesible por un usuario que no debería tener privilegios de acceso.
a) Verdadero
b) Falso

3- La integridad garantiza que los datos siempre se encuentren disponibles
a) Verdadero
b) Falso

4- La integridad garantiza que los datos no han sido modificados sin permiso
a) Verdadero
b) Falso

5- Un ataque de denegación de servicio impacta directamente sobre la disponibilidad de un sistema
a) Verdadero
b) Falso

Autoevaluación III

Una vulnerabilidad Zero day
a) Es una vulnerabilidad existente en la que el fabricante tiene conocimiento de ella y está trabajando en el parche.
b) Es una vulnerabilidad de la que el fabricante no es consciente y está siendo explotada de manera ilegítima por ciberdelincuentes o atacantes externos
c) Puedes encontrar el código necesario para explotar vulnerabilidades de tipo Zero day en páginas reconocidas y avaladas en el sector informático.

Autoevaluación IV

Indica si los siguientes razonamientos son verdaderos o falsos

1- Las auditorías de tipo automático generan muchos falsos positivos.
a) Verdadero
b) Falso

2- En las auditorías manuales no se pueden utilizar herramientas automáticas.
a) Verdadero
b) Falso

3- En los test de intrusión únicamente se confirman vulnerabilidades.
a) Verdadero
b) Falso

4- En los test de intrusión físico también se contempla conectar dispositivos no autorizados en la red
   a) Verdadero
   b) Falso
5- En los ejercicios de Red Team vale todo
   a) Verdadero
   b) Falso

Autoevaluación V
Indica la afirmación correcta
   a) En las pruebas de caja negra nunca se proporcionan usuarios de acceso al activo a auditar.
   b) En las pruebas de caja blanca te pueden proporcionar el código fuente del aplicativo a auditar.
   c) En las pruebas de caja gris disponemos de toda la información relativa al aplicativo a auditar.

Autoevaluación VI
Selecciona todas las afirmaciones correctas.
   a) Durante la toma de requisitos no se establecen limitaciones horarias
   b) Durante la toma de requisitos se establecen personas de contacto en ambas partes
   c) Como parte de las labores organizativas se especifica los activos a auditar
   d) Durante la toma de requisitos se especifica si existe alguna funcionalidad que no se deba probar, o se deba probar en otro horario

Autoevaluación VII
Indica, según corresponda, si las afirmaciones son Verdaderas o Falsas
1- Los roles dedicados a la gestión se apoyan en el informe ejecutivo para interpretar los riesgos de la vulnerabilidad
   a) Verdadero
   b) Falso
2- La criticidad de las vulnerabilidades se realiza según el criterio del auditor.
   a) Verdadero
   b) Falso
3- En el informe técnico se detallan todos los pasos necesarios que muestran la vulnerabilidad.
   a) Verdadero
   b) Falso

Autoevaluación VIII
Indica si la opción es verdadera o falsa en cada caso.
1- dnsrecon es una herramienta de enumeración pasiva
   a) Verdadero
   b) Falso
2- Realizar una búsqueda de información en pastebin se considera una técnica de reconocimiento pasivo
   a) Verdadero
   b) Falso
3- El uso de buscadores nos puede proporcionar mucha información sobre los activos incluidos en el alcance.
   a) Verdadero
   b) Falso

Autoevaluación IX
Indica si las siguientes afirmaciones son Verdaderas o Falsas
1- La herramienta nmap puede utilizarse para realizar un escaneo de vulnerabilidades
   a) Verdadero

b) Falso

2- arpscan enumera aplicativos de la red sin necesidad de interactuar con el objetivo.

a) Verdadero
b) Falso

3- Con la herramienta nc no se puede realizar un escaneo de servicios

a) Verdadero
b) Falso

Autoevaluación X

Marca todas las herramientas que se utilicen para realizar técnicas de fuerza bruta de credenciales

a) Patator
b) Wireshark
c) Shellter
d) Hydra Mostrar retroalimentación

Autoevaluación XI

Indica cuál de las siguientes herramientas se utiliza para extraer información de hashes de credenciales en la memoria de un equipo comprometido

a) Mimikatz
b) Keyloggers
c) LinPEAS

TEST I

1- Los sistemas de tipo Keylogger extraen información almacenada en la memoria RAM de un sistema operativo Microsoft Windows ¿Verdadero o falso?

a) Verdadero
b) Falso

2- ¿Cuál de las siguientes herramientas se utilizan en un reconocimiento pasivo?

a) dig
b) snmpwalk
c) nmap
d) shodan

3- Durante la presentación de resultados únicamente se presentan los resultados de la auditoría, pero no se resuelven dudas ni se dan recomendaciones para solventar las vulnerabilidades. ¿Verdadero o Falso?:

a) Verdadero
b) Falso

4- ¿Qué tipo de información podemos recopilar en las redes sociales?:

a) Averiguar tecnologías utilizadas en la compañía.
b) Direccionamiento IP y servicios expuestos en el perímetro de la empresa.
c) Averiguar credenciales de usuarios.
d) Activos pertenecientes a las empresas.

5- Indica cuál de las siguientes herramientas no es un proxy de interceptación:

a) Echo Mirage
b) ZAP
c) Burp
d) Shellter

6-¿Qué es una vulnerabilidad de tipo 0-Day?:

a) Una vulnerabilidad que no es pública.
b) Una vulnerabilidad que no existe.
c) Una vulnerabilidad que no tiene ningún tipo de impacto ni riesgo.
d) Una vulnerabilidad publica.

7- En que portal podemos buscar exploits específicos para una versión de software en concreto:
   a) LinkedIn
   b) Shodan
   c) Censys
   d) Exploit-db

8- ¿Que es la DarkWeb?:
   a) Contenido que se encuentra disponible de manera pública en internet.
   b) Contenido utilizado por los ciberdelincuentes pero que se encuentra disponible de manera pública en internet.
   c) Redes privadas utilizadas por los ciberdelincuentes para ofrecer sus servicios, vender información previamente robada, vulnerabilidades no reportadas a los fabricantes.
   d) Todo el contenido privado que no se encuentra a disposición del público en general.

9- Indica cuál de las siguientes opciones es una afirmación correcta para la Fase de Explotación:
   a) Se detectan vulnerabilidades que puedan existir en los sistemas y servicios
   b) Se utilizan técnicas para poder aumentar el nivel de privilegios en este sistema.
   c) Se recopila información acerca de los activos a auditar.
   d) El objetivo es lograr un primer acceso o de privilegios en los activos.

10- Para poder inspeccionar los datos transmitidos y recibidos por una interfaz de red, a bajo nivel, que herramienta de las siguientes hay que utilizar:
   a) arpscan
   b) netdiscover
   c) wireshark
   d) nmap

Solución
Autoevaluación I: c)
Autoevaluación II: 1 b), 2 a), 3 b), 4 a), 5 a)
Autoevaluación III: b)
Autoevaluación IV: 1 a), 2 b), 3 b), 4 a), 5 b)
Autoevaluación V: b)
Autoevaluación VI: b) c) d)
Autoevaluación VII: 1 a), 2 b) 3 a)
Autoevaluación VIII: 1 b), 2 a), 3 a)
Autoevaluación IX: 1 a), 2 a), 3 b)
Autoevaluación X: a) d)
Autoevaluación XI: a)
TEST I: 1 b), 2 d), 3 b), 4 a), 5 d), 6 a), 7 d), 8 c), 9 b), 10 c)

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)	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.**

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.