Offensive Audit Services

IES “Rafael alberti” | C. Amiel, s/n, 11012 Barriada de la Paz

Investigación, análisis e identificación de los diversos tipos de ataques informáticos

Grupo 3 - CIBER

2023

# Proyecto 2: Offensive Audit Services

Tabla de contenido

[Proyecto 2: Offensive Audit Services 1](#_Toc148788299)

[Introducción 2](#_Toc148788300)

[Clasificación de Tipos de Ataque 3](#_Toc148788301)

[Investigación de Tipos de Ataque 3](#_Toc148788302)

[Tipos de Auditoría Ofensiva 6](#_Toc148788303)

[Descripción de los Servicios 6](#_Toc148788304)

[Investigación de Fases de Ataque 6](#_Toc148788305)

[Investigación de Metodologías de Pentesting 6](#_Toc148788306)

[Tipos de Auditoría Ofensiva 7](#_Toc148788307)

[Descripción de los Servicios 7](#_Toc148788308)

## Introducción

En el mundo actual en la era digital la evolución es frenética y constante. Este hecho supone grandes avances en materia informática, lo que lleva a mejorar las vidas de millones de personas, ofreciendo facilidades y soluciones que en años pasados se antojaban como ‘fantásticas’, y en algunos casos hasta ’futuristas’. La realidad, sin embargo, no está carente de ciertos problemas, y esto se debe principalmente a dos factores, el factor humano, ya sea debido a un descuido o el desconocimiento por parte de un trabajador o particular, o por la maldad inherente a ciertas personas, que les mueve a querer perpetrar acciones ilegales contra empresas y/o particulares, ya sea por motivo de lucro, por motivos políticos o incluso simplemente sólo por el placer de hacerlo; y las múltiples vulnerabilidades y fallos de seguridad en sistemas existentes, que abren una puerta a una infinidad de posibles ataques, lo que conforma el mundo de la ciberseguridad.

Debido a estas dos poderosas razones, hemos podido ver un aumento exponencial de las amenazas cibernéticas, lo que ha llevado a profesionales de la seguridad ofensiva a comprender, clasificar y abordar una amplia variedad de tipos de ataques capaces de poner en peligro la seguridad de las organizaciones. Estos profesionales se dan a la tarea de estudiar estos ataques, analizarlos a profundidad y clasificarlos, para así poder entenderlos en términos de sus características, métodos y objetivos, para poder determinar cuáles son los más críticos desde el punto de vista de una organización.

Además de clasificar estos ataques, también se busca diseñas estrategias de auditoría ofensiva, lo cual es un componente esencial en el ámbito de la ciberseguridad. Las auditorías ofensivas nos permiten identificar debilidades y vulnerabilidades en sistemas, aplicaciones y redes antes que los atacantes las puedan explotar.

## Clasificación de Tipos de Ataque

Como antes hemos explicado, el modus vivendi de los profesionales de la ciberseguridad orbita en torno a la búsqueda y estudio de las vulnerabilidades y fallos de seguridad informáticos, analizando y comprendiendo los diversos tipos de ataques que los sistemas y aplicaciones pueden sufrir, anticipándose a ellos.

Precisamente por ese motivo llevaremos a cabo una investigación y subsiguiente clasificación de la amplia gama de tipos de ataques posibles, así como de los tipos de auditorías ofensivas que ofrecemos, exponiendo una descripción de los susodichos servicios.

### Investigación de Tipos de Ataque

Cuando hablamos de tipos de ataques informáticos, nos viene a la mente una gran cantidad y diversidad de formas, comúnmente maliciosas, de acceder de una forma no autorizada a sistemas e incluso controlarlos, obtener datos confidenciales, e incluso producir daños en los equipos, redes, sistemas y servicios que sufran estos ataques cibernéticos. El mundo de la informática es amplio, así como por extensión lo es el de la ciberseguridad, y es por ello que hemos de comprender la rama de posibles áreas donde estos cibercrímenes son perpetrados.

Por motivos de comprensión y de organización, dividiremos este abanico de ataques entre las diferentes áreas susceptibles de sufrir ataques, que son el software, los servicios de mensajería electrónica, las páginas web, las redes informáticas y el IOT (*Internet of Things*).

#### Servicios de mensajería electrónica

[…]

#### Software

El *software* es un conjunto de programas, aplicaciones y datos que permiten que un equipo informático realice tareas específicas. Es la parte lógica y no física de un sistema que le permite funcionar y llevar a cabo diversas funciones tales como el procesamiento de datos, la gestión del hardware o la ejecución de aplicaciones. Como podremos imaginar, cualquier software no está exento de la posibilidad de sufrir diversos tipos de ciberataques, los cuales clasificaremos y analizaremos, con el fin de comprender mejor cómo funcionan y qué buscan lograr.

Antes de comenzar a clasificar las formas usadas por los atacantes para vulnerar un sistema debemos entender la diferencia entre un *exploit* y un *virus*. Mientras que un exploit es un software malicioso usado para aprovechar las vulnerabilidades de un sistema objetivo, un virus se acopla en un programa legítimo para camuflarse, y al ser ejecutado, el código malicioso entra en escena, copiándose en programas y ficheros del sistema.

|  |  |  |  |
| --- | --- | --- | --- |
| Nombre | Características | Métodos | Objetivo |
| Ataque de Fuerza Bruta | * Un ataque de fuerza bruta es un método utilizado para descubrir contraseñas o claves de cifrado desconocidas * Este tipo de ataque trata de probar todas las combinaciones posibles de caracteres, números y símbolos hasta encontrar la correcta | * A través de un software especializado, los atacantes automatizan este proceso, probando miles de combinaciones por segundo * Es común enfocarse en encontrar contraseñas débiles | * El objetivo principal es el de obtener acceso no autorizado a cuentas, sistemas o datos protegidos por contraseña * Suele ser usado en cuentas online, sistemas protegidos por contraseñas o incluso en el descifrado de datos |
| Ataque de Diccionario | * A diferencia del tipo de ataque anterior, en un ataque de diccionario se utiliza una lista predefinida de palabras y combinaciones de caracteres * Estos ataques suelen ser más eficientes que los de fuerza bruta, ya que se centran en contraseñas comunes y más probables | * Uso de software especializado o scripts en su defecto, que automatizan la prueba de contraseñas en la lista del diccionario * Se puede personalizar el diccionario para adaptarlo al objetivo | * El objetivo principal es adivinar la contraseña de un usuario, cuenta, sistemas o datos protegidos * Tras la obtención de la contraseña, el objetivo suele ser robar información confidencial, acceder a sistemas no autorizados, etc |
| Ataque de Escalada de Privilegios | * Intento por parte del atacante de lograr un nivel de acceso o privilegios en un sistema superior al concedido inicialmente * Esta clase de ataque suelen servirse de vulnerabilidades y fallos en la configuración de seguridad de sistemas para obtener dichos privilegios * El atacante suele buscar cuentas de root o administrador | * No existe un solo método para lograr una escalada de privilegios, dado que esto varía de un sistema operativo a otro * Algunas de las técnicas usadas por atacantes para lograr dichos privilegios incluyen la inyección de código o la suplantación de identidad * Estos ataques pueden suceder en sistemas locales, donde el atacante ya tiene acceso al mismo, o en sistemas remotos, donde se ha comprometido previamente una cuenta con un nivel menor de privilegios | * El objetivo principal de este tipo de ataque es lograr un mayor control sobre un sistema, abriendo la puerta a atacantes a acciones que previamente les serían imposibles, tales como acceder a datos confidenciales, instalar malware o incluso modificar el propio sistema a su antojo |
| Rootkit | * Tipo de software malicioso diseñado para ocultarse en un sistema objetivo y proporcionar a los atacantes acceso no autorizado al mismo * El término “rootkit” viene de “root”, que alude a los mayores privilegios en sistemas UNIX, lo que serían privilegios de administración en Windows * Los rootkits suelen funcionar ocultándose de los usuarios y de los sistemas de seguridad * Pueden llegar a modificar el SO, aumentando su control del mismo y asegurando su persistencia | * Este tipo de malware suele instalarse en los sistemas objetivo de diferentes maneras, ya sea a través del uso de la ingeniería social como el phishing, ocultos en software de otra índole, aparentemente inocuo, etc | * El principal objetivo es el de otorgar a los atacantes acceso al sistema infectado, así como de mantener dicho acceso de forma persistente * El objetivo de los atacantes es robar contraseñas o datos financieros, información confidencial o alterar o destruir el sistema objetivo |
| Troyano | * Malware destinado a camuflarse como un programa legítimo e inocuo, y así otorgar acceso no autorizado a un sistema a los atacantes * Aunque pueda parecer lo mismo que un rootkit, la diferencia radica en la detección de ambos por parte del sistema, ya que el rootkit se enfoca más en ocultar su presencia tanto del usuario como de sus sistemas de seguridad, mientras que el troyano trata de ejecutar acciones maliciosas en el sistema directamente | * Esta clase de software malicioso puede transmitirse en correos de phishing, descarga de software pirata, enlaces malintencionados, la explotación de alguna vulnerabilidad, o incluso documentos o imágenes | * Al igual que un rootkit, los troyanos pueden dar acceso no autorizado a un sistema, y también suelen utilizarse para robar todo tipo de información * Los troyanos suelen usarse para crear puertas traseras (*backdoors*) en los sistemas atacados * También poseen capacidades de espionaje tales como el uso de keyloggers (software que registra las pulsaciones de teclado) o capturar la pantalla |
| Adware | * El adware es un tipo de software diseñado para mostrar anuncios no deseados en el sistema objetivo, y suelen manifestarse como banners, pop-ups, etc | * Comúnmente el adware se instala en un sistema formando parte de un software legítimo | * El objetivo principal del adware es generar ingresos para los anunciantes y desarrolladores del mismo * Algunos tipos de adware pueden llegar a recopilar información del usuario, a fin de poder mostrar publicidad personalizada a estas personas, o directamente vender esta información a otras empresas |
| Spyware | * El spyware es un tipo de software malicioso diseñado para ser capaz de recopilar información de la víctima * Este tipo de malware se oculta, funcionando en segundo plano * Es capaz de rastrear la navegación en Internet, registrar pulsaciones de teclado y robar contraseñas o información sensible | * El spyware se suele instalar de forma encubierta en un sistema objetivo, a través de descargas de programas pirata, phishing o incluso unido a software legítimo * Una vez que se instala funciona de forma sigilosa, en segundo plano | * El objetivo consiste en la recopilación de información del usuario infectado * Estos datos pueden incluir tarjetas de crédito, contraseña, historial de Internet o correos electrónicos |
| Gusano | * Clase de malware que funciona propagándose a través de redes y sistemas informáticos, sin necesidad de intervención humana * La diferencia con otros tipos de virus o malware no necesitan ir adjuntos a archivos o programas, dado que se replican de forma automática | * Los gusanos aprovechan vulnerabilidades para propagarse por redes y sistemas informáticos * Una vez infectado un sistema, el gusano analiza la red en busca de otros objetivos a los que copiarse, y si no los encuentra usará Internet para esa misma tarea | * El objetivo principal y razón de la existencia de un gusano es propagarse a otros sistemas, infectándolos para poder seguir propagándose * Algunos gusanos pueden contener payloads maliciosos |
| Botnets | * El término “botnet” viene de la expresión robot network o red de robots * Esta es una red de sistemas infectados (“bots” o “zombis”) por un atacante | * Los bots que componen una botnet suelen integrarse a esta a través de malware que los infectó previamente * Una vez infectado, el bot se comunica con un servidor de Comando y Control (C&C), controlado por el atacante * Algunas botnet tienen varios C&C | * Ataques DDoS * Distribución de Spam * Robo de Datos a gran escala * Infección de más dispositivos * Cryptojacking o minado de criptomonedas a gran escala |
| Rogueware | * El rogueware es un software malicioso y fraudulento, diseñado para aparentar ser un software legítimo y/o de seguridad, cuando realmente lleva a cabo acciones ilegales * Suelen venderse como programas diseñados para mejorar el rendimiento de un dispositivo, pero realmente realizan acciones maliciosas | * El rogueware suele contraerse a través de descargar software de sitios no oficiales ni confiables, phishing, etc * Una vez instalado, este tipo de software muestra alertas de “supuestos problemas” que requieren de nuestra atención de forma inmediata * Incluso existen casos que poseen una versión “premium”, que no ofrece ningún beneficio real, siendo además de una intrusión informática, una estafa | * El objetivo prioritario del rogueware es el lucro y la estafa a las víctimas a través de la venta de un software falso, que no sólo no los protege, sino que los daña * El rogueware es además capaz de robar información del usuario y su sistema * También posee la capacidad de instalar malware adicional |

#### Web

[…]

#### Redes

[…]

#### Internet of Things (IOT)

[…]

### Tipos de Auditoría Ofensiva

A fin de garantizar la seguridad de los sistemas, redes y dispositivos de los clientes, ofrecemos diversos tipos de auditorías ofensivas, con un enfoque práctico y directo. Este enfoque nos permite llegar a la raíz de los posibles problemas, fallos y/o debilidades en configuraciones de seguridad, localizar contraseñas débiles o encontrar vulnerabilidades críticas que pudieran ser explotadas por cibercriminales.

Antes de comenzar es importante proponer acuerdos, establecer límites y estudiar las regulaciones y normas de su compañía, a fin de delimitar el área que auditar, así como los horarios a los que llevar a cabo la auditoría en cuestión. Otro aspecto a tener en cuenta es discutir el tipo de prueba a llevar a cabo, siendo las opciones a elegir las siguientes:

* **Pruebas de Caja Negra (Black Box Testing).** En las pruebas de caja negra, los analistas de seguridad no conocemos los detalles internos y exactos del funcionamiento de su sistema, dado que el enfoque debe simular un ataque por parte de un elemento externo a la empresa, identificando vulnerabilidades sin acceso al código o a la estructura interna del sistema.
* **Pruebas de Caja Gris (Gray Box Testing).** Las pruebas de caja gris otorgan un conocimiento parcial del sistema al analista de ciberseguridad, ofreciendo detalles sobre el diseño o arquitectura del sistema, pero sin entrar en el código del mismo. Esto permite realizar pruebas con un enfoque mayor en un área concreta.
* **Pruebas de Caja Blanca (White Box Testing).** En las pruebas de caja blanca, a los evaluadores se les da un conocimiento completo del sistema, incluido el acceso al código fuente y la arquitectura interna del mismo. Esto da la posibilidad de llevar a cabo pruebas complejas, profundas y exhaustivas, con el objeto de identificar vulnerabilidades y/o fallos en el código del sistema.

Conociendo esto, se explicarán los tipos de auditorías ofensivas. Estas se dividen entre las diferentes áreas informáticas, y el objetivo de cada tipo es centrar los esfuerzos en un área concreta, para mayor efectividad y profundidad de las pruebas.

Una vez explicado esto, procederemos a revisar las auditorías que se hayan a su disposición:

#### Auditoría de Red

[…]

#### Auditoría de Seguridad en la Nube

[…]

#### Auditoría de Seguridad de Software

Una de las áreas más importantes en el panorama actual de la tecnología y de la información en general es el software, dado el papel fundamental que este desempeña en la operación de las organizaciones.

No es de extrañar que este sea uno de los puntos clave por los que los atacantes suelen encontrar vulnerabilidades y fallos de seguridad y/o de configuración, usándolos para perpetrar sus ataques y acceder de forma no autorizada a los sistemas ajenos. Es por ello que ofrecemos una auditoría exclusiva al ámbito del software, analizando los programas en la red y sistemas de su empresa, ofreciendo un informe detallado de los resultados encontrados, ofreciendo soluciones para fortalecer su seguridad, la de su compañía y de sus empleados.

#### Auditoría de Seguridad de IoT

[…]

### Descripción de los Servicios

Ahora que dispone de una lista de posibles auditorías que puede contratar, podrá ver a continuación una explicación a detalle de cada una de las auditorías anteriormente mencionadas, ofreciéndole una descripción precisa de los servicios ofertados.

#### Auditoría de Seguridad de Software

Nuestra Auditoría de Seguridad Ofensiva orientada al Software está diseñada para simular los ataques de cibercriminales reales, con el objetivo de identificar vulnerabilidades, fallos en configuraciones de seguridad, contraseñas débiles o por defecto en todas las aplicaciones y programas utilizados en su organización. Este estudio le permitirá mantener a salvo sus sistemas y datos confidenciales, mejorando su seguridad.

Comenzando por el entorno donde se llevarán a cabo las pruebas, existe la opción de realizarse de forma interna o externa a su organización, según los intereses que tenga el cliente. Obviamente, ambos enfoques ofrecen resultados distintos, así como enfoques distintos:

* **Auditoría Interna.** Una auditoría interna se realiza teniendo acceso a la red interna de la empresa cliente, llevando a cabo las pruebas de penetración o pentesting desde allí, pudiendo incluir las propias oficinas, su Intranet o una VPN.
* **Auditoría Externa.** Las auditorías externas se llevan a cabo desde fuera de la red de la organización, no teniendo acceso a los sistemas internos o datos de la empresa cliente.

Una vez que hemos elegido si queremos una auditoría externa o interna, también debemos optar entre enfoques diferentes a la hora de realizar las pruebas, dado que estas podrán tener una mayor superficie para realizarlas, o llegar a una mayor profundidad en el sistema de la empresa cliente, obteniendo resultados más concretos en un área. Estos tres enfoques son los siguientes:

* **Análisis de Vulnerabilidades (Vulnerability Assessment).** Los análisis de vulnerabilidades consisten en la identificación y la recopilación de vulnerabilidades, fallos de configuraciones de seguridad, contraseñas débiles o por defecto, y en general fallos en la seguridad general de la empresa que puedan proporcionar un vector de ataque a un posible atacante. Este tipo de pruebas son las que cubren una mayor superficie, pero alcanzan un nivel de penetración menor en los sistemas de la empresa cliente.
* **Test de Penetración (Pentesting).** Los tests de pentesting buscan realizar simulaciones de ataque controladas a la infraestructura, red y sistemas de la empresa cliente, con el fin de lograr resultados más precisos que un análisis superficial. Estas pruebas siempre se realizan siguiendo un código ético y cumpliendo unas normas acordadas con el cliente, tales como vetar ciertas partes de la infraestructura de la red de la empresa, limitar el pentesting a ciertas horas, etc. Normalmente en esta clase de pruebas no es necesario hacer hincapié en el ocultamiento de los sistemas de seguridad de la empresa, y en la discreción, dado que la misión consiste en obtener el mayor número de fallas de seguridad posibles, sin preocuparse del sigilo.
* **Red Teaming.** Las pruebas de Red Team podría decirse que son las más realistas de las tres, dado que alcanzan el mayor nivel de profundidad posible en los sistemas de la empresa, simulando un ataque real por parte de cibercriminales. Este tipo de prueba no posee constricciones de ningún tipo, pudiendo usar técnicas de Ingeniería Social como el Spear-Phishing, así como buscar ocultarse de los sistemas de seguridad de la empresa o explotar vulnerabilidades, tal y como lo haría un atacante real. El objetivo consiste no sólo en analizar las vulnerabilidades y fallos de seguridad de la compañía, sino en evaluar también la capacidad de respuesta de la misma.

Ya elegido el tipo exacto de pruebas que desea para su empresa, pasaremos a explicar el esquema general de la auditoría, desde la realización de las pruebas hasta la presentación del informe con los resultados obtenidos.

Se ha de remarcar que este es un mero esquema general con un enfoque claro en la seguridad del software de la empresa, haciendo hincapié en esta área concreta. Si se elige un enfoque de análisis externo, obviamente se obtendrá una evaluación general de la seguridad de sus programas, pero careciendo de un nivel alto de detalles.

## Investigación de Fases de Ataque

### Investigación de Metodologías de Pentesting

Las pruebas de pentesting son importantes en el ámbito de la seguridad informática, dado que poniendo a prueba los sistemas en los que realizan las pruebas, logran obtener resultados y, por ende, posibles soluciones o mitigaciones a fallos de seguridad y vulnerabilidades.

Teniendo en cuenta las auditorías que ofrecemos, hemos elegido implementar la metodología PTES (*Penetration Testing Execution Standard*), que posee un enfoque en un amplio espectro de áreas. Esta metodología está diseñada para poder ser aplicada tanto en redes y sistemas, aplicaciones web, redes, aplicaciones (software), ingeniería social e incluso seguridad física. Esta elección se hace debido al hecho de no existir una metodología concreta para el ámbito del software, pero sí una que cubre en gran medida, la mayoría de campos relevantes en el campo de la seguridad informática.

### Tipos de Auditoría Ofensiva

[…]

### Descripción de los Servicios

[…]