Guía de Pentesting Básico

V1.0 Jul 2014

Ing. Aarón Mizrachi
CISA | ITILv3F

Introducción al Pentesting

Definición:

Es un **tipo de auditoría externa** basada en ataques, **orientada a ganar acceso en los sistemas de información**, y realizada **con la finalidad de buscar fallas de seguridad**.

Las técnicas y procedimientos utilizados serán similares a los de un hacker, sin embargo, tendrán autorización, y serán ejecutadas de forma ética.

Cuál es el valor real de una prueba de penetración

- **Probar** que **las medidas de seguridad** hayan sido diseñadas e implementadas de forma correcta.
- **Identificar vulnerabilidades** que **no** puedan ser **detectadas por análisis de vulnerabilidad**
- **Identificar el riesgo real de una vulnerabilidad**. Por ejemplo, varias vulnerabilidades de riesgo bajo pueden alinearse para, en su conjunto ser una vulnerabilidad de alto riesgo.
- **Demostrar que el peligro es real.** Muchas veces la seguridad es subestimada en la toma de decisión estratégica y operacional de una compañía. La única forma de lograr un cambio de actitud es mediante la demostración de un ataque inocuo (mismo efecto que una vacuna).
- **Es llevada a cabo por** hackers éticos **profesionales con amplia experiencia** en el área.

Cumplimiento

- La **legislación** en varios paises obliga a ciertas empresas (ej. Bancos), a realizar dichas pruebas anualmente.
- Según el **CSC 20-1** (Critical Security Controls for Effective Cyber Defense v5), se recomienda realizar pruebas de penetración internas y externas regularmente. Los CSC son una guía base de requerimientos mínimos para mantener nuestra organización segura.
- Se deben realizar pruebas de penetración regularmente para cumplir con **ISO-27002** (punto ISO-27002:2005 15.2.2)

Cuales son los componentes del sistema de información a ser probados?

Un sistema de información no solo esta compuesto por servidores. Un sistema de información comprende toda la galaxia de elementos que giran en torno a la información:

- Servidores
- Backups
- Administradores
- Usuarios
- Redes
- Estaciones de trabajo
- Señales Radioeléctricas
- Seguridad Física
- Entorno en general

Todos los elementos del sistema de información deben ser probados.

Que no hace una pentest

- **Conseguir todas las vulnerabilidades**
  - En caso de ser un ataque de caja negra, los sistemas que no logren ser comprometidos pueden tener vulnerabilidades ocultas que solo son visibles desde una posición administrativa.
  - Al ser un test rápido, la probabilidad de ocurrencia de falsos negativos y falsos positivos se incrementa.
- **Atacar todas las vulnerabilidades**
  - Hay vulnerabilidades que técnicamente no pueden ser atacadas en un periodo de tiempo acotado.
  - Hay vulnerabilidades que no son técnicamente explotables a menos que ocurran eventos específicos (ej. Ocurrencia de una configuración específica, ocurrencia en tiempo, etc)
  - Pueden existir varias rutas de ataque, el atacante puede elegir utilizar solo una y documentar el resto de las vulnerabilidades.
- **Corregir las vulnerabilidades**
  - El pentester no debe solucionar las vulnerabilidades, ya que se presenta un conflicto de interés. Solo debe limitarse a realizar recomendaciones para solucionarlas, y en caso de ser necesario, se realizará una nueva auditoría para verificar que hayan sido corregidas.

Que no debe hacer un pentester.

- Salirse del alcance de la prueba.
- Actuar de forma no-ética.
- Dejar de reportar algún hallazgo encontrado.
- No cumplir con las leyes locales, regionales y nacionales.

Tipos de Prueba

Tipos de Prueba

- **Caja Negra:** El atacante no recibe ningún tipo de información previa del sistema.
- **Caja Gris:** El atacante recibe información parcial, como por ejemplo, usuarios sin privilegios, dimensionamiento de la plataforma.
- **Caja Blanca:** El atacante recibe información previa de los sistemas. Como por ejemplo, claves de usuario de administrador. Es propicio para realizar análisis de vulnerabilidad (no recomendado para pentest)

Tipos de Prueba

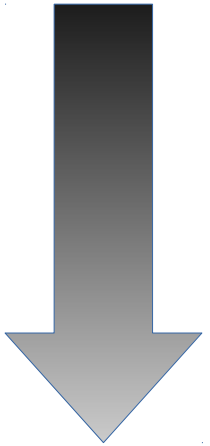
- **Abierta:** Tanto el atacante como el atacado saben plenamente de la prueba y estan en constante comunicación.
- **Ciego:** El atacado tiene conocimiento de la realización del ataque, sin embargo, el atacante no tiene información previa, ni esta en comunicación formal con el atacado (excepto para reportar ataques que afecten la disponibilidad).
- **Doble Ciego:** El atacado no tiene información sobre el atacante, y el atacante tampoco tiene información sobre el atacado. (Caso ideal, ya que además de probar los sistemas en si, prueba la respuesta y monitoreo de los administradores)

Prueba Escalonada

Lo ideal es realizar la prueba de forma escalonada desde caja negra hacia caja gris.

Ejemplo:

1. Primero sin ningún tipo de acceso
2. Con acceso a las instalaciones
3. Con acceso a un punto de la red no privilegiado
4. Con acceso a un punto de red y un usuario sin privilegios
5. Con acceso a un punto de red privilegiado

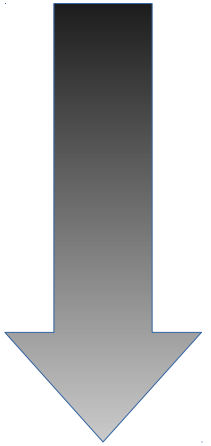


Prueba Escalonada

La prueba de red escalonada permitirá probar ataques desde distintos perfiles.

Ejemplo.

1. Un atacante externo
2. Un visitante
3. Un visitante con acceso a red
4. Un empleado sin privilegios
5. Un empleado con ciertos privilegios



Prueba Escalonada

- En caso de que el atacante consiga escalar privilegios, se demuestra un mayor grado de compromiso con los sistemas.

Tipos de pruebas genéricas

- **Interna**: Realizada dentro de la organización. Busca probar el perímetro interno de la organización.
- **Externa**: Realizada desde fuera de la organización. Busca probar el perimetro expuesto a internet.
- **WiFi:** Busca probar la seguridad en señales radioeléctricas.

Análisis de Vulnerabilidad

- Un análisis de vulnerabilidad busca reportar las fallas conocidas sin explotarlas.
- **Caja Blanca (ideal):**
  - Con acceso directo y claves de administrador, se puede validar los parches de seguridad y revisar el código fuente de las aplicaciones, así como que las políticas de seguridad sean las correctas.
- **Caja Negra (no ideal):**
  - Sin accesos, la única información sobre vulnerabilidades serán las que se puedan determinar mediante técnicas de prueba y “adivinación”.

Ataque en grupos

- A veces, debido a la complejidad de la prueba, los pentesters (igual que los hackers en el mundo real), se congregan en grupos. Dichos grupos pueden dividirse tareas de acuerdo a su experticia.
  - Por ejemplo: Dentro del grupo pueden haber expertos en sistemas operativos específicos, lenguajes de programación específicos, ataques específicos... etc.

Metodologías

Metodologías

- **OWASP**: Nos provee de un marco abierto para realizar pruebas de intrusión a sitios web.
- **PTES**: Penetration Testing Execution Standard, provee una guía/marco detallada para la ejecución de una prueba de penetración (recomendado).
- **OSSTMM**: Open Source Security Testing Methodology Manual. Metodología realizada por la comunidad para estandarizar las pruebas de seguridad. Este modelo es genérico para cualquier prueba de seguridad (no solo pentest).
- **ISSAF**: Information System Security Assessment Framework. Guía extensiva, esta enfocada en pentesting y en el aspecto de negocio de seguridad de la información.
- **NIST 800-115**: Provee de procesos repetibles para la conducción de evaluaciones de seguridad, incluyendo metodología para pentesting.

Fases de una prueba de penetración (Caja Gris/Negra)

Etapa de Planificación

Fase A-1: Dimensionamiento
Se define con el cliente el alcance y objetivos de la prueba

Fase A-2: Planificación de la etapa de análisis
Se planifica horario y ejecución de la prueba basado en las métricas y requerimientos

Documentación

Fases de una prueba de penetración (Caja Gris/Negra)

Etapa de Análisis

Fase B-1: Reconocimiento
Se basa en conseguir toda la información disponible de forma pasiva.

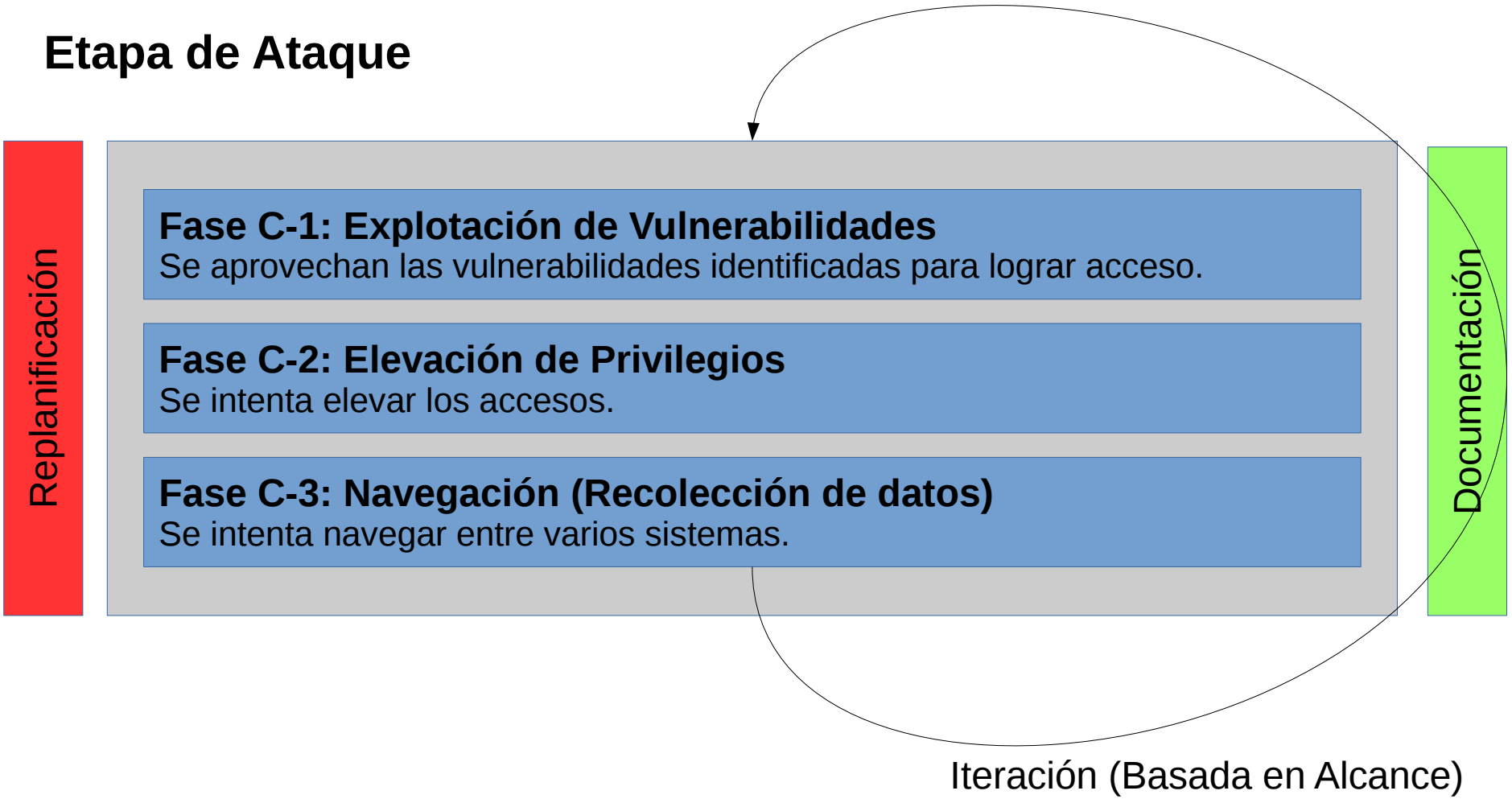
Fase B-2: Escaneo
Busca identificar los servicios que estan corriendo en la red.

Fase B-3: Enumeración (Análisis de Vulnerabilidad – Caja Negra)
Busca identificar las vulnerabilidades presentes en los sistemas.

Fase B-4: Planificación de la etapa de ataque
Se planifica la ejecución del ataque, y en caso de ser necesario redimensionamos la prueba

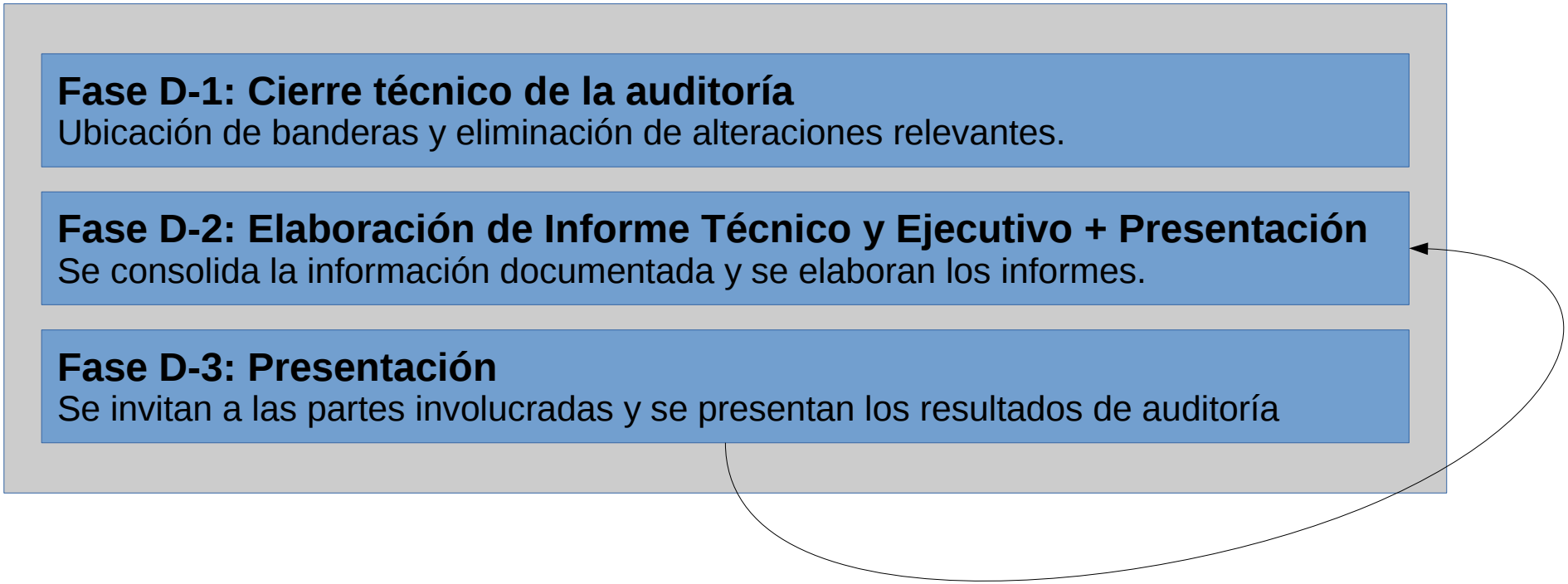
Documentación

Fases de una prueba de penetración (Caja Gris/Negra)



Fases de una prueba de penetración (Caja Gris/Negra)

Etapa de Finalización



Reportes

Elaboración de un informe técnico

El informe técnico esta **compuesto por los hallazgos encontrados** durante la prueba. Este **contiene**:

- Descripción detallada de la **metodología** utilizada.
- **Reporte detallado** y estructurado de cada uno **de las vulnerabilidades** conseguidas en los elementos analizados (hosts, websites, páginas, etc).
  - Detalle de las vulnerabilidad
  - Severidad y Riesgo de la vulnerabilidad
  - Alcance de la vulnerabilidad
  - Referencias
  - Sugerencias para su reparación y/o mitigación
- **Detalles de la intrusión**
  - Vulnerabilidades utilizadas
  - Procedimientos ejecutados (en detalle)
  - Capturas de pantalla / Pruebas de la intrusión
- **Consolidado técnico** (Estadísticas, sugerencias, plan de mitigación de riesgos, etc)
- **Consideraciones adicionales**, recomendaciones y conclusiones.

Elaboración de un informe ejecutivo

El informe ejecutivo contiene información de alto nivel gerencial útil para la toma de decisiones. Este **contiene**:

- Descripción de la **metodología** utilizada.
- Descripción de la **actividad** realizada
- **Detalles** de la ejecución (fecha, personal, autorizador, etc)
- Consolidado de los **hallazgos** encontrados
  - **Estadística** de vulnerabilidades encontradas por segmento (red, zona, etc)
  - **Principales amenazas** (a alto nivel: por categoría)
  - **Nivel de la amenaza** global (bajo, medio, alto, crítico)
- **A quien esta dirigido** este documento.

Elaboración de una presentación

La presentación contiene tanto los hallazgos a nivel gerencial, como un avance técnico de los elementos mas relevantes. Este podría contener:

- Descripción de la **metodología** utilizada.
- Descripción de la **actividad** realizada
- Consolidado de los **hallazgos** encontrados
  - **Estadística** de vulnerabilidades encontradas por segmento (red, zona, etc)
  - **Principales amenazas** (a alto nivel: por categoría)
  - **Nivel de la amenaza** global (bajo, medio, alto, crítico)
- **Vulnerabilidades principales** encontradas
- **Pruebas de ingreso** que sean significativas.

Consideraciones en la ejecución de la prueba

Que documentos debe tener un pentester para poder iniciar una prueba?

- Un pentester debe tener un documento donde se le apruebe a realizar dicha prueba. El documento debe estar firmado por un responsable dentro de la empresa con suficiente atribuciones para firmar dicho documento.
- El atacante debe conservar consigo una copia fiel de dicho documento durante toda la ejecución de la prueba. Y el original debe conservarlo por siempre.
- Un documento donde se defina el alcance de la prueba.

Disponibilidad de los sistemas

- Al realizar una prueba de penetración se debe determinar que tipos de ataque debe realizar el atacante. Uno de ellos es la denegación de servicio.
- En caso de que el cliente no desee pruebas de denegación de servicio, o estas estén acotadas en un horario restringido (para evitar una caida perjudicial del sistema), ello debe ser acordado antes de iniciar la prueba.

Prueba Offline en Replicas

- Para mantener la disponibilidad y la sorpresa en el ataque, un atacante puede elegir reconstruir el ambiente del atacado en maquinas virtuales.
- Dichas máquinas virtuales le mostrarán al atacante los errores comunes que un administrador puede cometer configurando el servidor, dando un mejor entendimiento.
- Adicionalmente permitirá probar ataques sin afectar la disponibilidad del sistema real, y en caso de considerarse listo, el atacante podrá ejecutar el ataque en los servidores reales.

Licitación

Que departamento debe contratar una prueba de penetración?

- Las empresas grandes comenzaron teniendo un grupo pequeño de seguridad de la información dentro de IT, luego evolucionaron a gerencia y luego a dirección de seguridad de la información.
- El motivo de esto es evitar conflictos de interés entre IT y Auditoría.
- El departamento adecuado sería el de seguridad de la información. El modelo en el cual trabaja una prueba de penetración, es el de auditoría externa.
- En caso de no existir un departamento de seguridad de la información, la prueba puede ser contratada por el director de IT, siempre y cuando entienda que debe garantizarse a toda costa la independencia de la auditoría.

Pentesting Automatizado vs Pentesting Manual

- **El pentesting automatizado** se realiza a través de herramientas que permiten facilitar la labor del pentester. Por ejemplo, Core Security provee una solución de explotación de vulnerabilidades automatizada.
- **El pentesting manual** se realiza probando y construyendo directamente las vulnerabilidades. Existen muchas vulnerabilidades que no pueden ser conseguidas con herramientas autómatas, ya que estas no entienden muy bien el alcance y/o el riesgo que es adaptado a una organización específica.
- **La mejor estrategia** es cubrir lo que pueda ser automatizado mediante herramientas, y complementar con chequeos manuales.

Ejemplos de vulnerabilidades no detectadas por herramientas autómatas

- Ejemplos sencillos de vulnerabilidades no detectadas por herramientas autómatas puede ser:
  - Una aplicación de negocio donde la clave sea un número de 4 dígitos que sea vulnerable a fuerza bruta, y que la prueba de la clave requiera de alguna codificación especial (ej. Clave enviada en base64).
  - Una vulnerabilidad donde la salida ocurra por una vía alterna (ej. Email)
  - Aplicaciones hecha en casa donde un procedimiento vulnerable se ejecute en un horario específico.

Comercialización del pentest

- Existen 3 tipos de pruebas:
  - **Scan de vulnerabilidades simple:** No es una prueba de penetración, pero ayuda a la organización a detectar fallas. Si es una empresa pequeña, quizá solo necesite esto.
  - **Pentest Automatizado:** Lo venden comunmente como pentest, sin embargo, las herramientas automatizadas no garantizan el resultado
  - **Pentest realizado por un experto:** Este tipo de prueba puede combinar ataques automatizados con ataques avanzados.

Que tipo de pentest debo contratar?

- Debe seleccionar a su pentester de acuerdo a sus requerimientos.
- Debe realizar una autoevaluación. Realice la siguiente pregunta:
  - Es importante su información?
  - Altera a su negocio que su información sea robada y entregada a la competencia?
  - Altera a su negocio que su información sea alterada? (ej. Agregar saldo, ventas ficticias, contabilidad, etc)
  - Altera a su negocio que sus sistemas informáticos sufran una caida?

Que tipo de pentest debo contratar?

Mientras mas se sienta identificado con las preguntas de la lamina anterior, usted deberá buscar un auditor de mayor experiencia y conocimiento.

En caso de que su apetito de riesgo sea alto y la información que maneje no sea crítica, quizá usted esté buscando solo un análisis de vulnerabilidades automatizado.

Cada cuanto debo realizar un pentest?

- La respuesta genérica es: frecuentemente.
- La respuesta detallada es, depende de los siguientes factores:
  - Ha instalado nuevo software o actualizado software viejo?.
  - Ha desincorporado software?
  - Ha creado nuevos usuarios?
- Adicionalmente, día a día se descubren nuevas vulnerabilidades, por lo tanto, se recomienda que al menos cada 6 meses para organizaciones de mediano a mayor tamaño.

Quienes pueden estar interesados en una prueba de penetración?

Todo aquel que tenga una infraestructura de TI y valore la información allí contenida

Perfil del Auditor

Certificaciones de Seguridad y Auditoría de Sistemas Compatibles con pentesting

- **CISA**: Certificación ISACA. Califica a la persona como auditor certificado. Conoce de cinco módulos: Auditoría, Seguridad, gobierno de TI, soporte y mantenimiento.
- **CISM**: Certificación de ISACA. Manager de Seguridad de la Información
- **CISSP**: Certificación de ISC2, cualifica los conocimientos en seguridad de la información y manejo gerencial de la misma.
- **ISO27001/27002:** Certificación para la aplicación de normas de seguridad.
- **Security+**: Conoce teoría de seguridad de la información

Certificaciones de Seguridad y Auditoría de Sistemas Compatibles con pentesting

- **CEH/ECSA**: Certificaciones de EC-Council orientadas al Ethical Hacking. Actualmente van por la versión 8. Califica a la persona en la teoría y la ejecución de herramientas.
- **LPT**: Ultimo nivel de certificación de EC-Council para ethical hacking.
- **GPEN:** Certificación de GIAC de pentesting. Parecida a CEH, Califica a la persona en la teoría, mas que en la ejecución de herramientas.
- **OSCP/OSCE**: Certificaciones de Offensive-Security (creadores de Backtrack/Kali). Califica a la persona en cuanto a sus habilidades para lograr ingresar en sistemas.

Son suficientes y/o necesarias las certificaciones?

El pentester debería...

- **Participar en ejercicios CTF (Capture The Flag):** Son competencias en las cuales participan hackers. El objetivo es lograr conseguir una bandera
- **Tener amplio conocimiento de otras áreas útiles**: virtualización, redes, sistemas operativos, bases de datos, programación, gestion de IT, etc.
- **Ir constantemente a conferencias y seminarios**: Estar al día es importante para lograr la diferencia.
- **Dictar cursos asociados al tema**: Los cursos requieren casi obligatoriamente que el pentester este al día y se mantenga estudiando. Además, reafirma su dominio sobre el tema.

Son suficientes y/o necesarias las certificaciones?

El pentester debería...

- **Realizar investigación y desarrollo**: La investigación profundiza el conocimiento y las habilidades del pentester. Alguien que esta constantemente investigando, logrará mejores resultados en menor tiempo.
- **Contribuir con la comunidad**: Reportar fallas y vulnerabilidades en los sistemas demuestra su valor ético.
- **Estar en contacto con otros hackers**: El acercamiento a la comunidad permitirá conocer de primera mano las tendencias. Incluso antes que en las publicaciones.
- **Lograr Indepencia**: La independencia garantiza que un auditor no este parcializado a la hora de escribir un reporte. Punto clave para cualquier auditor (CISA)

Notas finales

Este documento no pretende reemplazar ninguna metodología específica de pentesting.

Esta diseñado como una guía básica para orientar al lector sobre el funcionamiento del mundo del pentest.