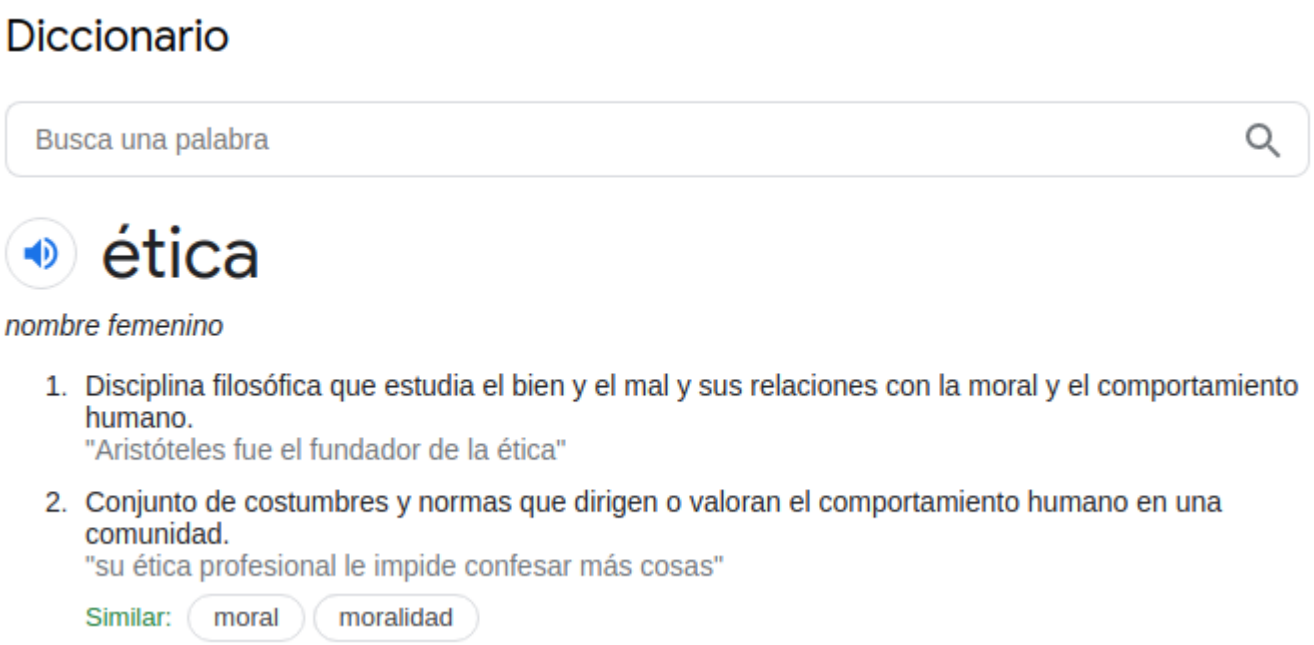
6669 Criptografía y Seguridad Informática

Penetration Test

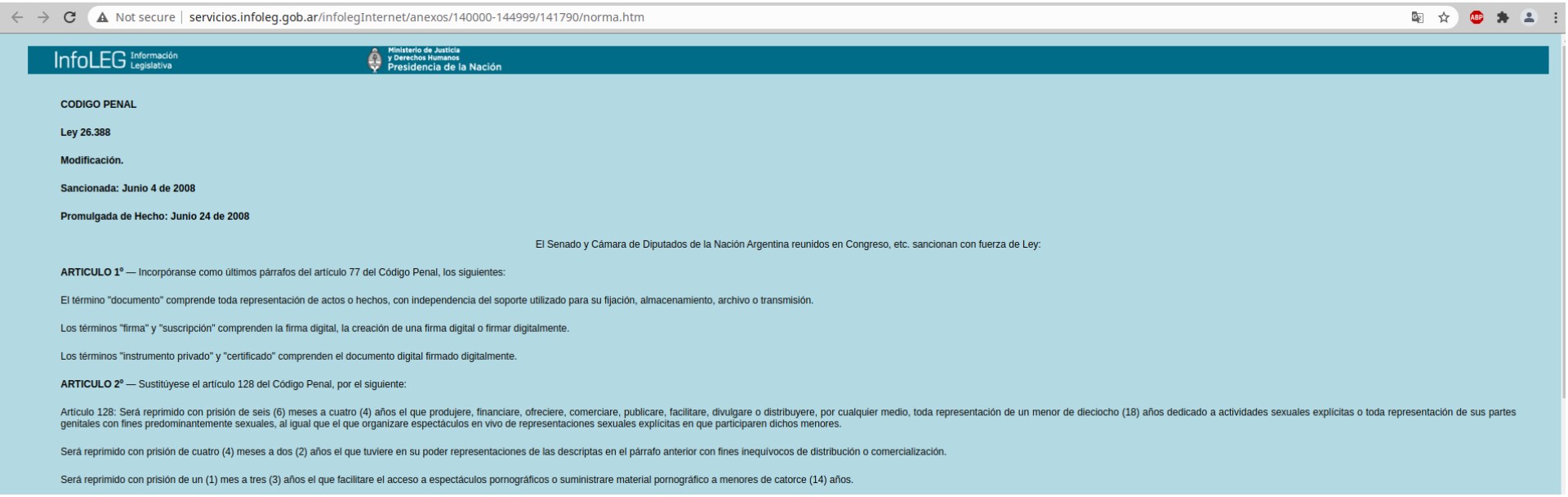
Penetration Test

- ✔ Introducción
- ✔ Amenazas
- ✔ Distintos tipos de atacantes
- ✔ Hackers, Cracker y distintos Sombreros
- ✔ Distintos tipos de Pentests
- ✔ Análisis de Vulnerabilidades vs Penetration Test

Ética Profesional



Ley de Delitos Informáticos (Ley 26.388)



Not secure | servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

InfoLEG Información Legislativa

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

CODIGO PENAL

Ley 26.388

Modificación.

Sancionada: Junio 4 de 2008

Promulgada de Hecho: Junio 24 de 2008

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

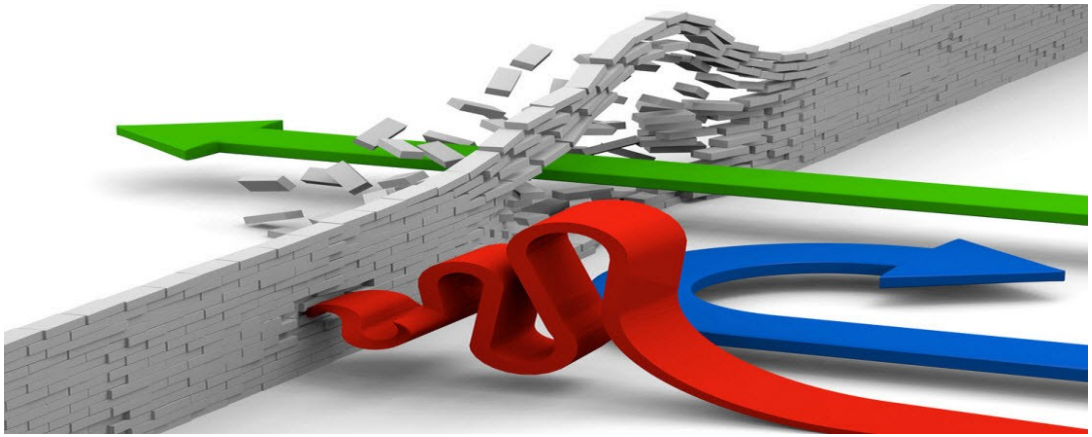
Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Tipos penales en la Convención de Budapest

- ✔Acceso Ilícito
- ✔Interceptación ilícita
- ✔Interferencia en los datos
- ✔Interferencia en el sistema
- ✔Abuso de dispositivos
- ✔Falsificación informática
- ✔Fraude informática
- ✔Delitos relacionados con material de abuso sexual infantil
- ✔Delitos relacionados con la propiedad intelectual

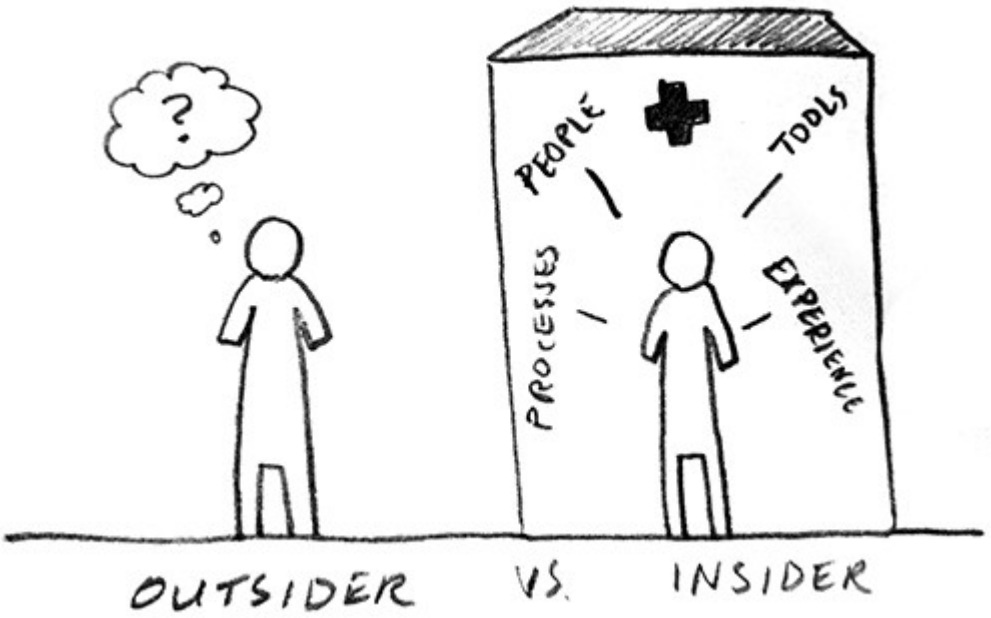
Introducción

La finalidad que tiene un Penetration Test es identificar de forma temprana vulnerabilidades que podrían ser aprovechadas por un atacante.



Amenazas

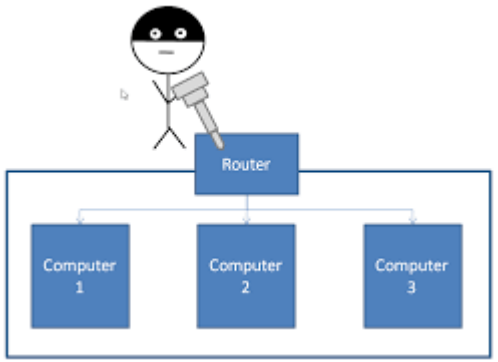
Existen distintos tipos de amenazas que pueden tener interés en atacar nuestros sistemas. Entre ella podemos tener amenazas externo y/o internas.



Amenazas Externas

Entre las Amenazas Externas encontramos:

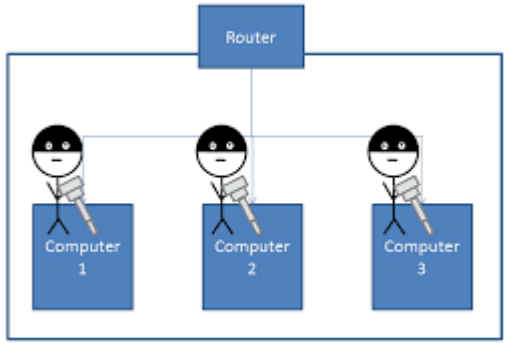
- Crimen Organizado
- Terrorismo
- Gobiernos
- Competidores
- Hacktivistas
- Otro tipo de atacantes



Amenazas Internas

Entre las Amenazas Internas encontramos:

- Empleados Despistados
- Empleados Descontentos
- Administradores Despistados
- Administradores Descontentos
- Clientes
- Proveedores



Distintos Niveles de Atacantes

Los atacantes pueden tener distintos niveles de conocimiento sobre cómo atacar los sistemas informáticos.

Entre ellos encontramos los siguientes:

- Script kiddies
- Nivel Intermedio
- Nivel Elevado
- Investigadores de Seguridad
- Atacantes de Elite

Hackers, Cracker y distintos Sombreros

Hackers, Cracker y distintos Sombreros

Not secure | dle.rae.es/?id=JxlUKkm

hacker

Adapt. del ingl. *to hack*.

1. m. y f. *Inform.* **pirata informático.**

2. m. y f. *Inform.* Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

Hackers, Cracker y distintos Sombreros

cracker

Voz ingl.

1. m. y f. *Inform.* **pirata informático.**

Hackers, Cracker y distintos Sombreros

Con respecto a los sombreros, podemos identificar los siguientes:

- Black Hat: Atacante malicioso quien, apartir de sus conocimientos, trata de romper la seguridad de los sistemas
- White Hat: Experto en Ciberseguridad que intenta mejorar la seguridad de los sistemas, encontrando vulnerabilidades y corrigiendo las mismas.
- Grey Hat: Experto en Ciberseguridad que trabaja en ambos lados.

Distintos tipos de Penetest

Al igual que con los sombreros, los tipos de Pentest se clasifican por colores pero en este caso son Cajas.

- Black Box: La finalidad que tiene este tipo de análisis es pararse como lo haría un atacante externo. Sin diponer de conocimientos sobre las tecnologías existentes e ir aprendiendo sobre la infraestructuras, reconociendo vulnerabilidades y explotándolas.
- Grey Box: En este caso, se plantea un escenario de un usuario con pocos privilegios y la finalidad es tratar de conseguir escalar en privilegios.
- White Box: El último escenario es identificar vulnerabilidades desde adentro, suponiendo que pudiesen existir backdoors, tanto del lado del código como de la configuración de la infraestructura.

Penetest – Black Box

El pentester dispondrá únicamente de la/s URL/s o la/s IP/s que deba analizar.

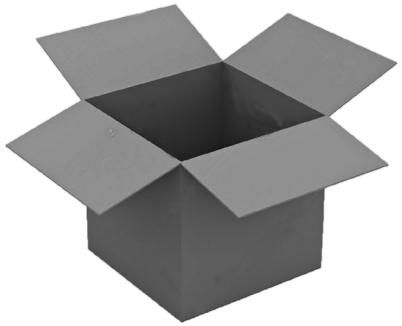
Irá descubriendo la infraestructura a medida que se vayan escaneando los objetivos.

Una vez descubiertas los servicios, se irán descubriendo vulnerabilidades y a partir de allí se irán explotando las mismas con el fin de cumplir con el objetivo del proyecto.

Penetest – Grey Box

Simulando ser un usuario disconforme de la organización se tratará de identificar vulnerabilidades.

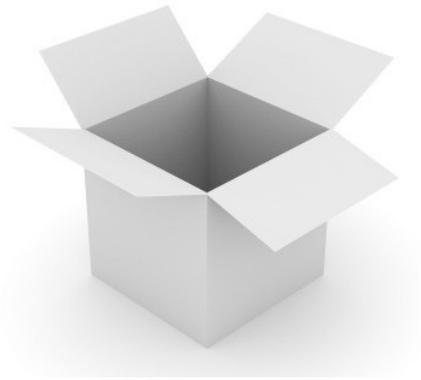
A partir de dichas vulnerabilidades se intentará escalar en privilegios con el fin de tomar control sobre la infraestructura.



Penetest – White Box

En este tipo de análisis se plantea el acceder a la información no solo desde el exterior del entorno del sistema objetivo sino que también se analizará tanto desde el código fuente del mismo como la configuración de la infraestructura que soporta el mismo.

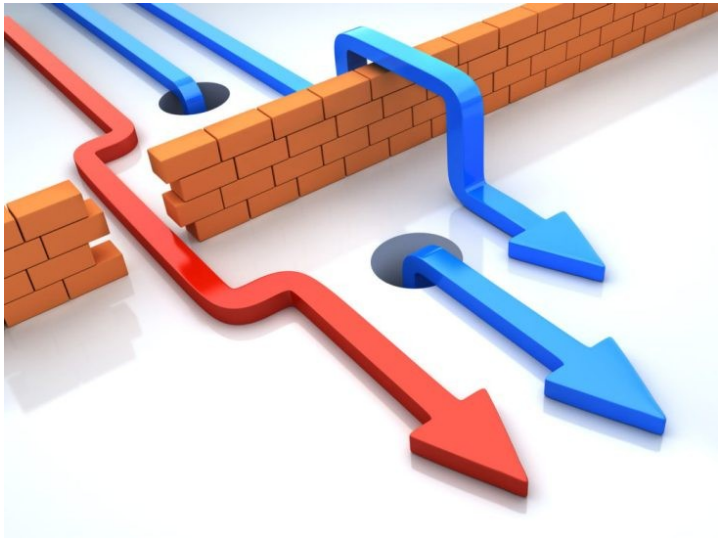
De este modo se podrá testear la aplicación en mayor profundidad recolectando mayor cantidad de vulnerabilidades en el entorno.



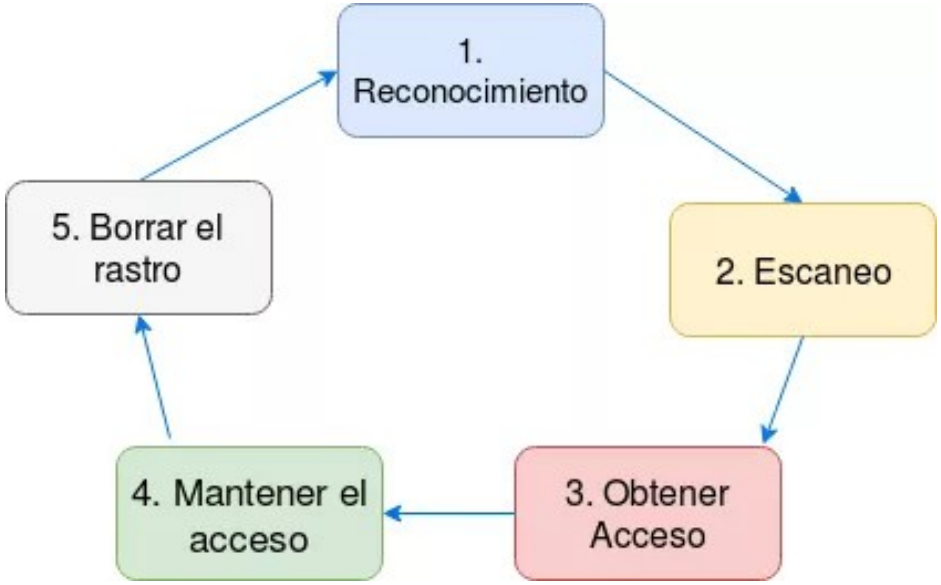
Análisis de Vulnerabilidades vs Penetration Test

Dentro de un Análisis de Vulnerabilidades o VA se analizarán los servicios disponibles y se identificarán todas las vulnerabilidades posibles.

Este tipo de análisis permite identificar el abanico de vulnerabilidades que podrían ser aprovechados por un atacante real.



Fases estándares de un Pentest



Fases reales de un Pentest

- ✔ Acuerdo de Confidencialidad
- ✔ Reconocimiento
- ✔ Enumeración
- ✔ Explotación
- ✔ Post Explotación
- ✔ Informes

Acuerdo de Confidencialidad

Un NDA, acuerdo de confidencialidad, acuerdo de no divulgación, también referidos como contratos o convenios de confidencialidad, es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.

El NDA se firma habitualmente cuando dos empresas o individuos acuerdan alguna relación comercial y necesitan entender los procesos usados en la otra compañía con el propósito de evaluar el interés de dicha relación.

Reconocimiento

En esta Fase se reconocerá el campo de trabajo sobre el cual se encuentra inmerso el objetivo.

Entre algunas de las técnicas utilizadas dentro de esta fase se encuentran las siguientes:

- Buscadores Web
  - Google Hacking
  - Shodan
- Base de datos Whois
- Consultas DNS
- Ingeniería Social
  - Redes Sociales
  - Dumpster Diving
- Información dentro de los correos electrónicos

Enumeración

A la fase de Enumeración también se la conoce como un reconocimiento activo, en esta fase empezaremos a utilizar herramientas que analizarán nuestro objetivo profundamente.

Dependerá de la labor a realizar, ya que, tenemos herramientas para analizar infraestructura, aplicaciones Web, escaneadores de vulnerabilidades, clonadores de sitios web, técnicas para acceder a información de un usuario por medio de correos electrónicos, entre otros.

Explotación

A partir de las vulnerabilidades descubiertas en la fase anterior, tendremos que dedicarle un tiempo a la investigación de las herramientas y técnicas para explotar las mismas.

Una vez encontrado y/o desarrollado el exploit correspondiente, procederemos a explotar las vulnerabilidades.

Algunos repositorios:

- www.packetstormsecurity.org
- www.exploit-db.com
- Metasploit

Explotación - Payload

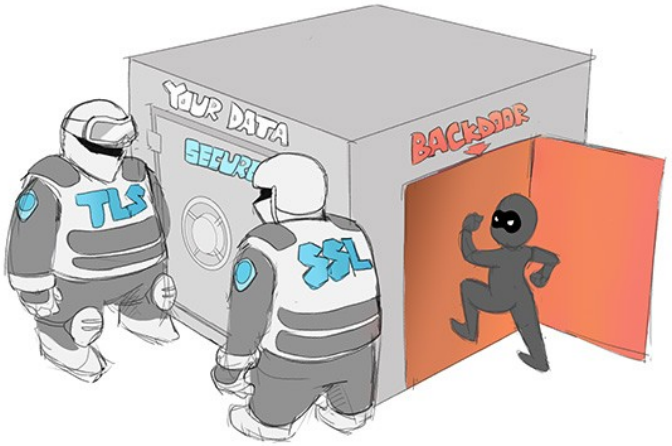
Se conoce como Payload a la carga maliciosa. El mismo, comunmente va junto con el exploit. El exploit es el encargado de explotar la vulnerabilidad y el payload será la porción de código que nos permitá realizar la acción posterior.

Por ejemplo, ejecutar una shell que nos permita tomar control del equipo vulnerado.

Post Explotación

Una vez que conseguimos explotar la vulnerabilidad, el siguiente paso será lograr mantener persistencia. Para ellos podemos migrar de proceso, dejar un backdoor, un troyano o un rootkit.

Lo más usual es utilizar un Backdoor, el cual nos permitirá mantener el acceso contra la máquina víctima por medio de un método alternativo.



Post Explotación

La fase de Borrar Rastros, tiene como finalidad establecer cómo dentro de una organización pueden responder ante un incidente, cómo pueden trabajar aplicando Informática Forense si los registros fueron borrados o modificados.

Informe

Como última fase tenemos la Generación del Informe.

El mismo debe tener el contenido adecuado para su destinatarios. Qué quiere decir esto? Tiene que ver con el lenguaje que utilizaremos en cada reporte.

Suelen realizarse 2 (dos) informes finales:

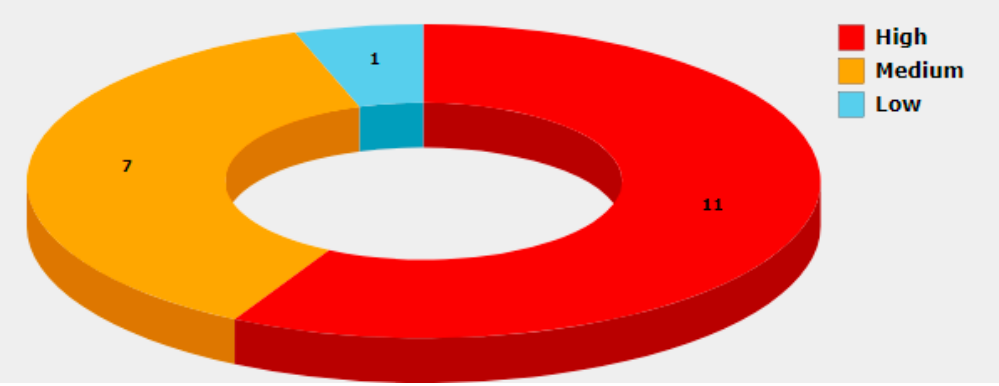
- Ejecutivo
- Técnico

Informe Ejecutivo

En el Informe Ejecutivo debe especificarse las tareas realizadas y una conclusión con respecto a los resultados obtenidos a partir del análisis realizado

Debe ser claro y conciso, tratando de utilizar palabras no técnicas para que pueda ser comprendido por gente del Negocio.

Algo que no debe faltar en este informe es el estado de situación del objetivo analizado y gráficos que simplifiquen su entendimiento.



Informe Ejecutivo

- Carátula
- Índice
- Objetivo
- Alcance
- Línea de Tiempo
- Explicación del Ataque
- Resumen Ejecutivo
- Conclusión

Informe Técnico

Por último tenemos el Informe Técnico, este último tendrá todo el contenido incluído en el Informe Gerencial sumando todo lo necesario como para que el área técnica de la Organización comprenda las acciones realizadas durante el proceso.

Deberá indicar las herramientas utilizadas, todas las vulnerabilidades identificadas, los hosts donde fueron ubicadas, cuales fueron explotadas, CVEs asociados a cada vulnerabilidad junto con su respectiva criticidadevidencias.

Tendrá que disponer de recomendaciones de mejora con el fin de mitigar todas las vulnerabilidades descubiertas.

Informe Técnico

A los ejes del Informe Ejecutivo deben adicionarse al Informe Técnico los siguientes:

- Herramientas utilizadas
- Detalle de vulnerabilidades
  - Nombre de Vulnerabilidad
  - Criticidad
  - Descripción
  - Impacto
  - Recomendación
  - Referencias
  - Activo
  - Evidencia