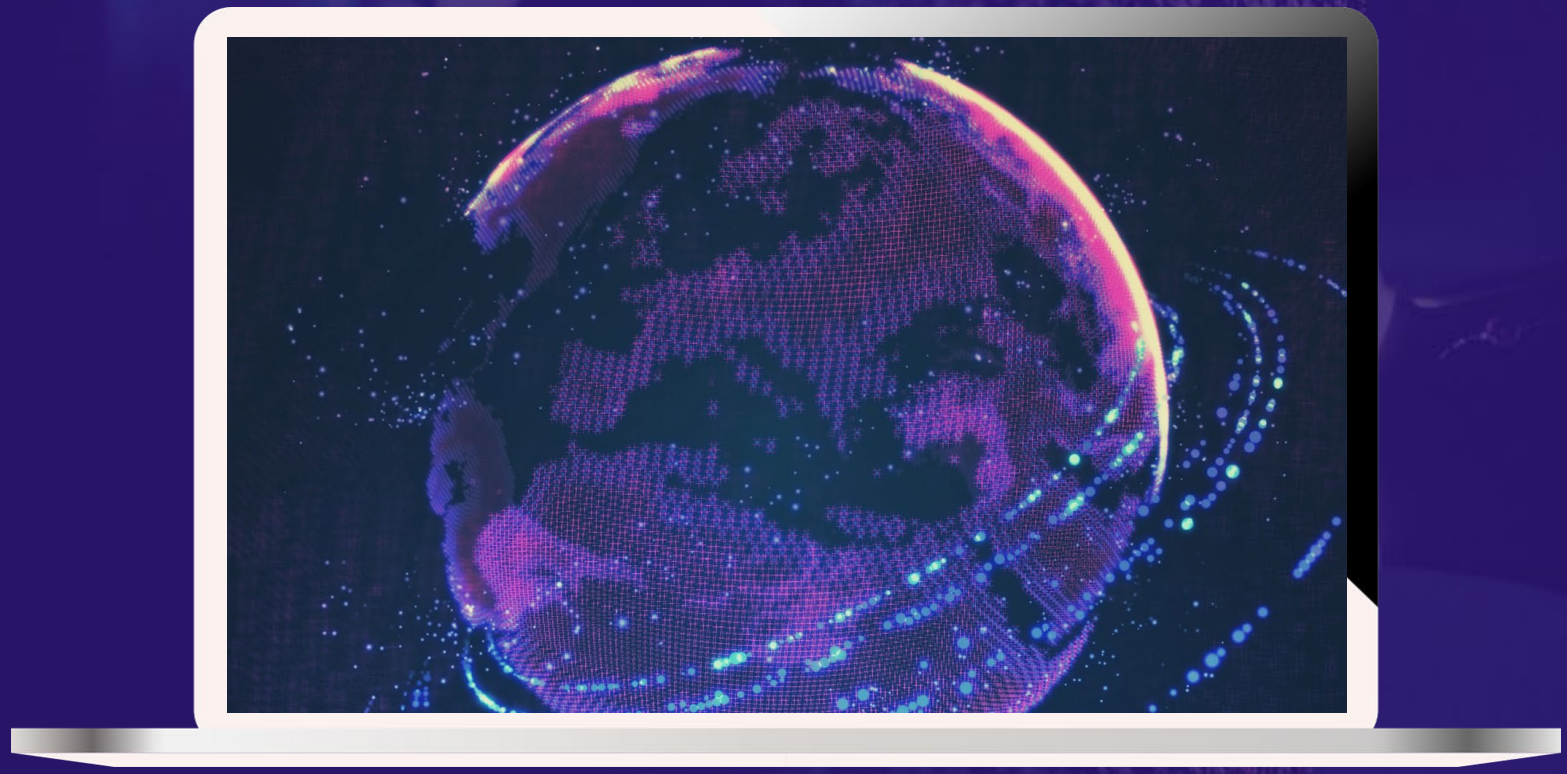
Beneficios de realizar Pentesting

KARINA ASTUDILLO B., MSC

CEO – CONSULTING SYSTEMS

@KASTUDILLOB

Contenido



¿Qué es Hacking?

El hacking informático recurre a la manipulación de la conducta normal de un equipo y de los sistemas que tiene conectados . Esto se hace generalmente mediante scripts o programas que manipulan los datos que pasan a través de una conexión de red, con el fin de acceder a la información del sistema .

Las técnicas del hacking incluyen el uso de exploits, virus, gusanos, troyanos, ransomware, secuestros del navegador de internet, rootkits y ataques de denegación de servicio, entre otros.

¿Qué es un hacker?

Un hacker es un experto en ciberseguridad que cuenta con los conocimientos y habilidades para explotar vulnerabilidades informáticas en sistemas y redes.

CRACKER

Este término fue creado por la comunidad Hacker para referirse a aquellos que usan sus conocimientos con fines poco éticos.

En general se tiene la idea de que un hacker es un pirata informático que se infiltra en sistemas informáticos sin autorización, ilegalmente, para robar, modificar o destruir información. Esta visión, es errónea. De esa definición se desprende el concepto de cracker.

Categorías Principales

- Whitehackers, whitehats o hackers éticos
- Blackhackers, blackhats o crackers
- Greyhat hackers

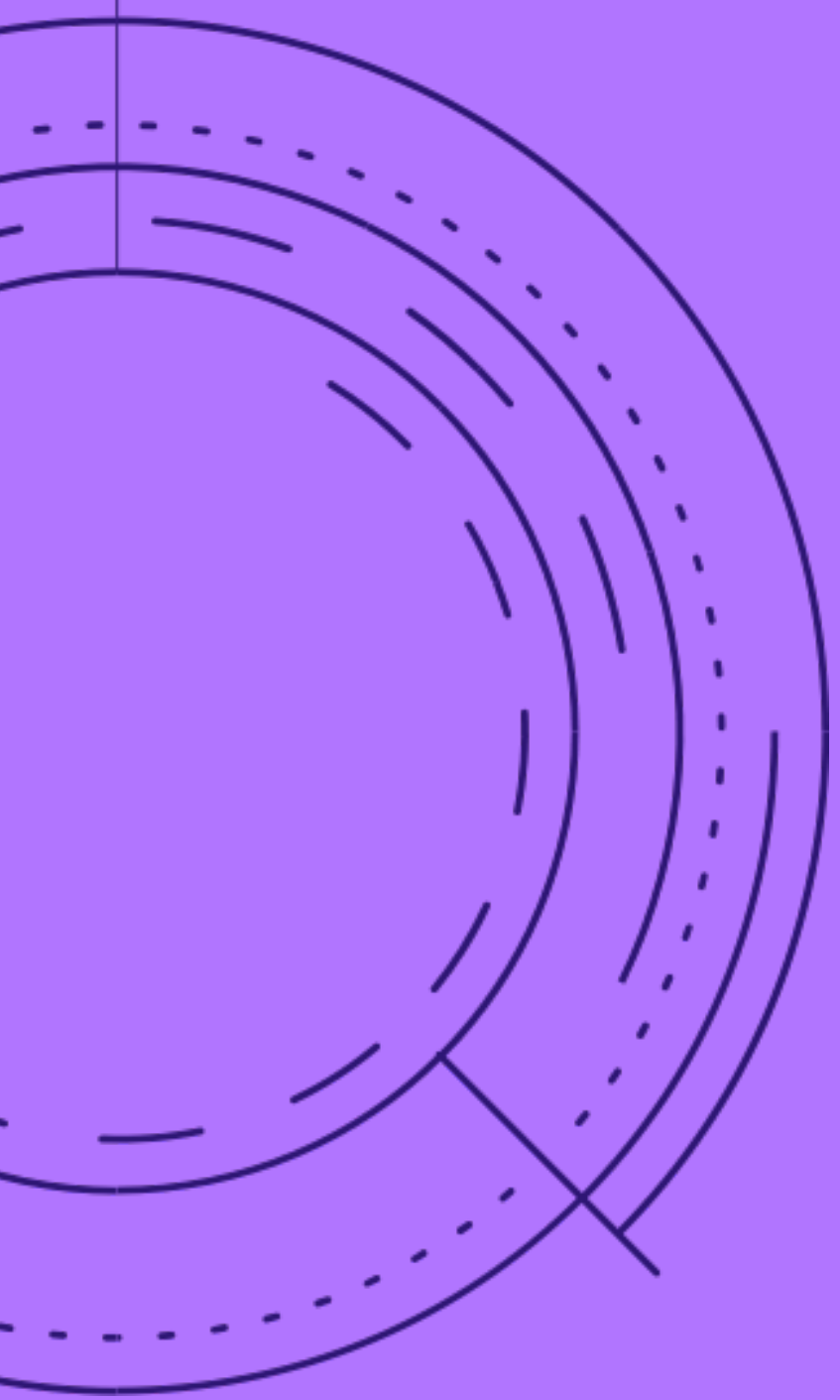
Categorías

Whitehackers , whitehats o hackers éticos. Son profesionales dedicados a la búsqueda y solución de vulnerabilidades en sistemas empresariales, gubernamentales y particulares. Estas personas suelen trabajar para las empresas de informática.

Dentro de este grupo podemos englobar a los llamados:

Bluehat hackers (“sombreros azules”) Generalmente son consultores o profesionales externos de seguridad dedicados a betatesting o comprobación de un software o hardware antes de su lanzamiento oficial y salida al mercado, para intentar exponer las vulnerabilidades existentes.

Red Hat hackers (“sombreros rojos”) Se refiere a hackers que hacen uso de sistemas Linux y herramientas opensource principalmente y que al igual que un whitehat buscan detener las acciones de los blackhats . Empero, sus técnicas suelen ser muy distintas. En lugar de dejar que las autoridades se hagan cargo, un redhat podría lanzar un ataque agresivo hacia los sistemas de un blackhat con el objetivo de destruir sus recursos o inhabilitarlos.



- **Blackhackers , blackhats o crackers**

Son personas dedicadas a utilizar (de forma profesional o amateur) sus conocimientos para actividades delictivas y sacar un provecho económico: En muchos casos están relacionados con la delincuencia organizada.

- **Greyhat hackers**

“sombreros grises”. En esta categoría encajan aquellas personas de doble moral que trabajan indistintamente tanto para firmas de seguridad como para organizaciones criminales.

ÉTICA HACKER

Ética Hacker

La ética hacker es un conjunto de principios morales y filosóficos surgidos, y aplicados a las comunidades virtuales de hackers.
La expresión se suele atribuir al periodista Steven Levy en su ensayo seminal Hackers: Heroes of the Computer Revolution, publicado en 1984, donde describe y enuncia con detalle los principios morales que surgieron a finales de los años cincuenta en el Instituto Tecnológico de Massachusetts (MIT) y, en general, en la cultura de los aficionados a la informática de los años sesenta y setenta.
Los principios clave pueden resumirse en el acceso libre a la información y en que la informática puede mejorar la calidad de vida de las personas

La ética hacker es una ética de tipo axiológico, es decir, una ética basada en una determinada serie de valores.

Himanen rescata algunos valores fundamentales:

- Pasión
- Libertad
- Conciencia social
- Verdad
- Honestidad
- Anticorrupción
- Lucha contra la alienación de las personas
- Igualdad social

Valores fundamentales

- Libre acceso a la información (conocimiento libre)
- Valor social (reconocimiento entre semejantes)
- Accesibilidad
- Actividad
- Preocupación responsable
- Curiosidad
- Creatividad
- Interés

Ventajas Del Haking Ético

- Combatir contra el terrorismo y las brechas de seguridad nacional: Hay muchas organizaciones terroristas en el mundo que usan la tecnología computacional tratando de crear caos y perjuicios a los gobiernos y organizaciones, un hacking ético minucioso puede anticiparse a estos ataques y prevenir muchos daños.

- Tener un sistema computacional que evite que personas maliciosas obtengan acceso a información restringida: Como los hackers éticos tienen las mismas herramientas y conocimientos que los hackers criminales, pueden desarrollar medidas preventivas que impidan el acceso a información sensible por parte de cualquier intruso.

- Tener implementadas las medidas preventivas adecuadas para evitar brechas de seguridad: La seguridad de la información no se trata sólo de sistemas computacionales seguros, sino que también es necesario implantar normas y crear conciencia en los trabajadores de la organización sobre la importancia de la seguridad de los datos cruciales.

Desventajas Del Haking Ético

Como en todo tipo de actividades que tienen un lado oscuro, habrá personas deshonestas que representan un inconveniente.

Un grayhat podría hacerse pasar por hacker ético y usar el conocimiento adquirido del sistema para realizar actividades de hacking criminal.

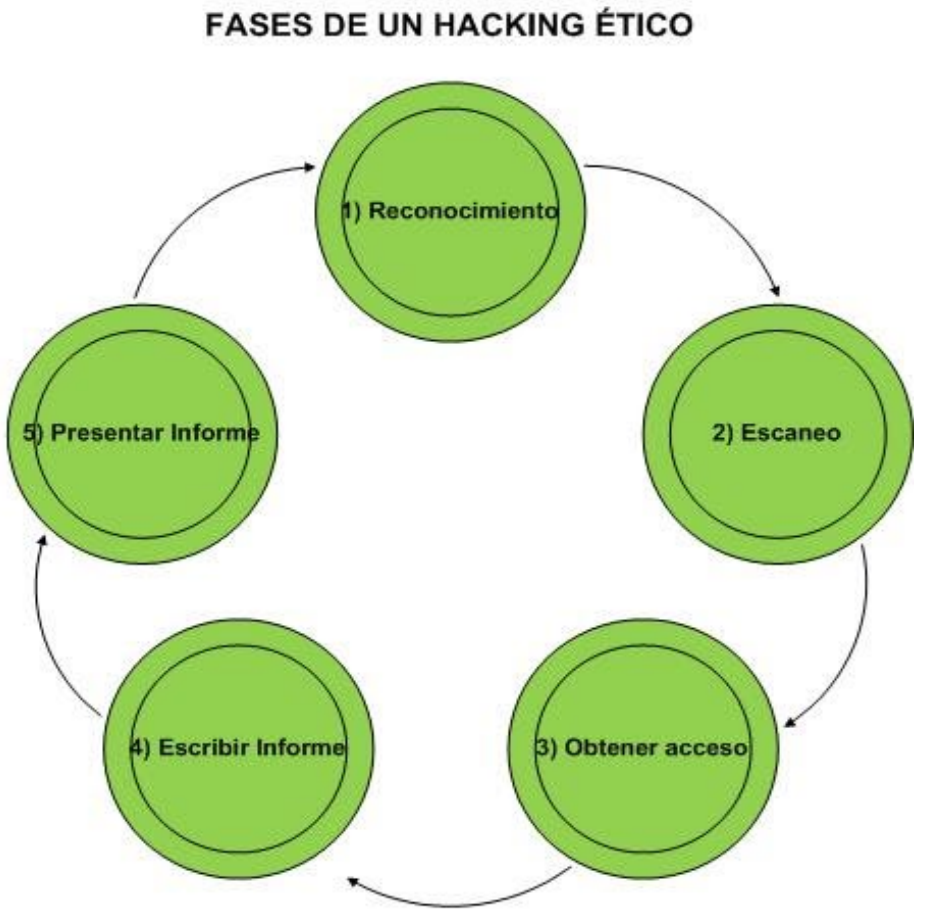
Permitir que sean visibles datos sensibles de la compañía.

La posibilidad de que el supuesto hacker ético envíe y/o inserte código malicioso, virus u otro tipo de cosas destructivas y dañinas en el sistema computacional.

Ruptura de seguridad masiva.

Fases del hacking

Fuente: EC-Council
Elaboración: la autora



Fuente: EC-Council y la experiencia
Elaboración: la autora

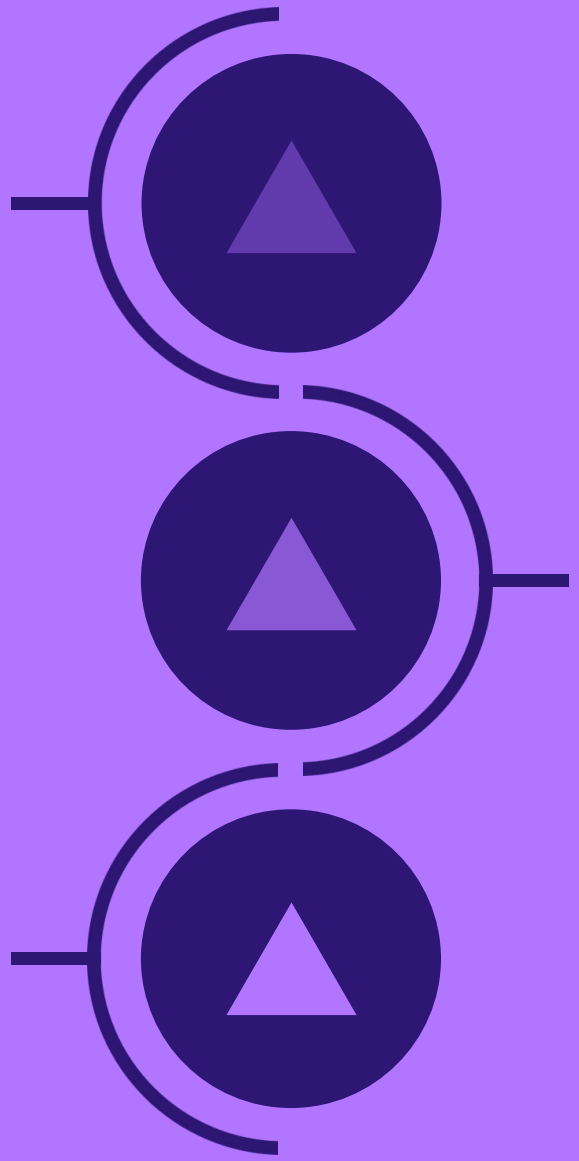
Fuente: Astudillo K., (2018). Hacking Ético 101, 3ra Edición. Editorial RA

Reconocimiento

En esta fase el hacker indaga información general acerca de sus objetivos que le será útil en las siguientes fases. Ej: averiguar el dominio DNS, los rangos de direcciones IP asignados, etc.

Obtener Accceso

Durante esta fase el hacker analizará las vulnerabilidades encontradas durante la fase previa y seleccionará aquellas a explotar para tratar de ganar acceso a los sistemas del objetivo.



Escaneo

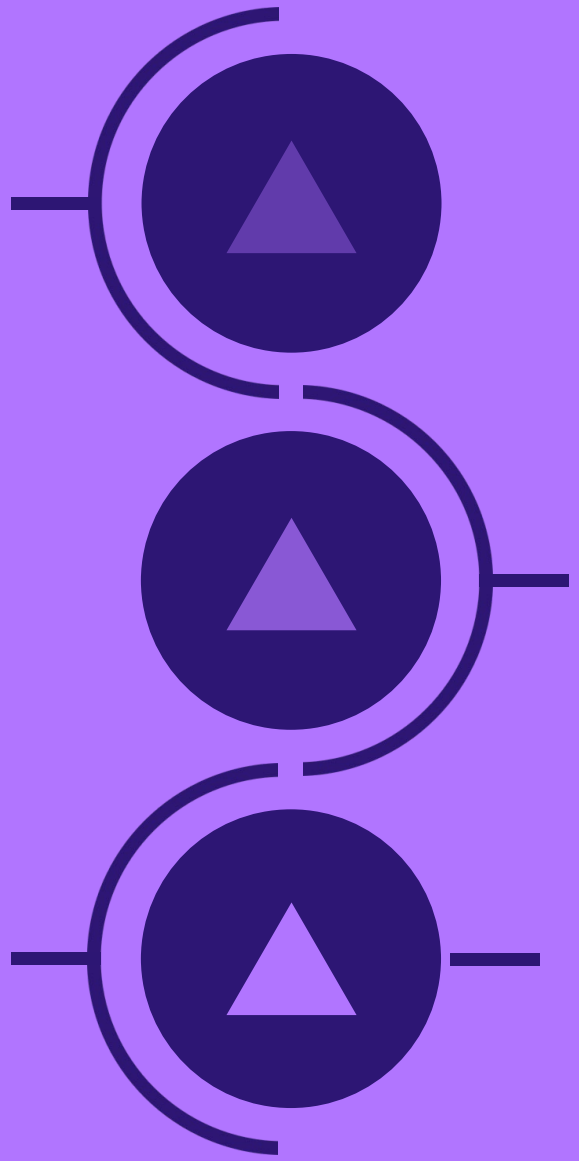
Aquí el hacker profundiza en la obtención de información del objetivo, basándose en la fase previa. Ej: barridos de ping, escaneo de puertos, análisis de vulnerabilidades. Etc.

Mantener Acceso

Aquí el hacker puede hacer uso de backdoors, rootkits u otro tipo de malware para poder volver a conectarse a los hosts previamente hackeados sin necesidad de volver a explotar la vulnerabilidad que le permitió el acceso en primer lugar.

Escritura del informe

Esta es una fase propia de un pentesting en la cual el hacker ético elabora un informe de auditoría el cual contiene un resumen ejecutivo con los hallazgos y recomendaciones de remediación.

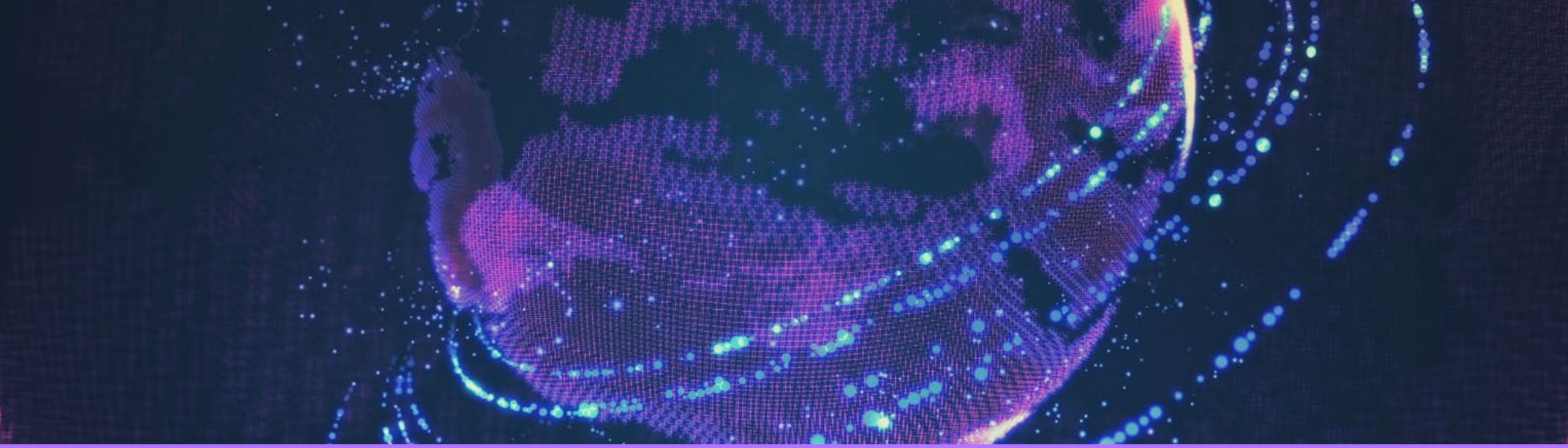


Borrar Huellas

Un cracker tratará de eliminar evidencias que lo incriminen en esta fase a través del borrado de logs, eliminación de cuentas creadas previamente, etc.

Presentación del informe

En esta fase el pentester expone sus hallazgos y recomendaciones de remediación a la alta gerencia y al blue team de la organización cliente.

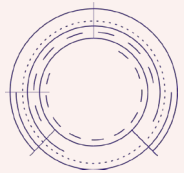


Pruebas de Intrusión
(Pentesting)

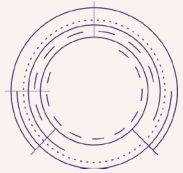
¿Qué es un Pentester o Hacker Ético?

Los Ethical Hackers son expertos que realizan una serie de medidas para determinar la vulnerabilidad de un sistema.

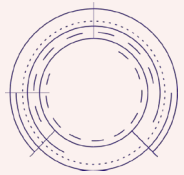
A esta práctica normalmente se le conoce como Pen - test (penetration test) o test de intrusión.



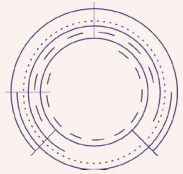
Profesional de seguridad informática



Efectúa pruebas de intrusión



Halla huecos de seguridad



Realiza recomendaciones de remediación

¿Por qué se necesitan Pentesters?

La cantidad de ciberataques ha aumentado considerablemente en los últimos años.

Existen miles de herramientas de hacking disponibles en Internet listas para ser descargadas y usadas.

Cada vez las herramientas de hacking se vuelven más y más sofisticadas.

El impacto de una fuga de datos puede ser muy grave para una organización.

Una intrusión que se hace pública impacta negativamente la imagen de la empresa afectada y puede costarle la pérdida no sólo de dinero sino también de clientes.

Pen- Test (Penetration Test)

Las pruebas de intrusión permiten

a) Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.

b) Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.

c) Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

Pen-test (penetration test)

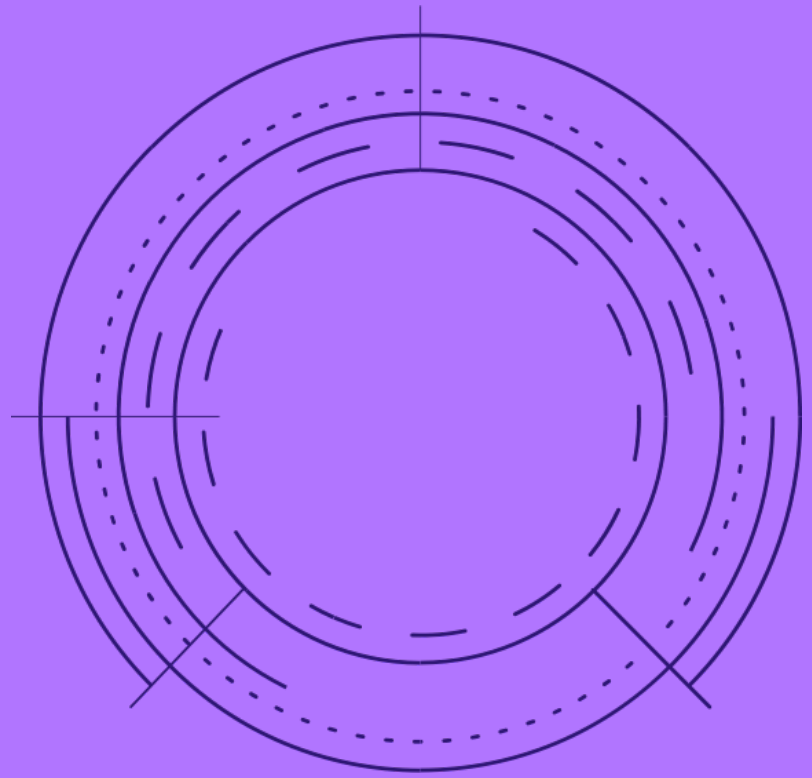
Para ejecutar un pen - test se sigue una serie de pautas, usadas también por los atacantes (recopilación de información, descripción de la red, exploración de los sistemas, extracción de información, acceso no autorizado a información sensible o crítica, auditoría de las aplicaciones web...), pero con la diferencia de haber sido consensuadas previamente con los responsables del sistema objetivo.

La labor de los pentesters siempre está ligada a las necesidades y preocupaciones que pueda tener una entidad. Por ello, cada prueba de intrusión será diferente y su éxito dependerá de las habilidades y experiencias que tengan el o los profesionales involucrados.

Pentesters

•Existen tres tipos de pentestings, los cuales están relacionados con la cantidad de información que se posea sobre la entidad a auditar y la manera en que se vayan a realizar las pruebas de intrusión .

- Caja blanca (White box)
- Caja gris (Grey box)
- Caja negra (Black box)



CAJA BLANCA (WHITE BOX)

Es el más completo, debido a que parte de un análisis integral. Con este se evalúa toda la infraestructura de la red. El pentester tiene conocimiento sobre todos los aspectos de seguridad de la entidad (medidas, estructura de la red, contraseñas, etcétera).

CAJA GRIS (GREY BOX)

Es el más recomendado por los especialistas. A diferencia del anterior, el pentester no posee la información específica para realizar el test de penetración, por eso, requiere de tiempo y recursos para identificar la información necesaria acerca de las posibles vulnerabilidades existentes

Caja negra (Black box)

En este caso no hay información sobre la entidad y se actúa de forma similar a un ciberdelincuente para tratar de reconocer fallos en la estructura de la red.

Para realizar una prueba de penetración de forma profesional, se requieren también conocimientos de programación, metodologías y documentación. No obstante, esos aprendizajes se adquieren una vez que se conocen y se saben utilizar muchas herramientas que son parte del proceso de penetration testing.

A continuación, se describirán algunas herramientas básicas.

Nombre de la herramienta	Plataforma	Tipo
Nmap	Mac OS, Linux, OpenBSD, Solaris, Windows	Escáner de puertos
Nessus	Mac OS, Linux, Windows	Analizador de vulnerabilidades
Metasploit	Mac OS, Linux, Windows	Framework de pentesting
Aircrack-Ng	Multiplataforma	Suite para hacking inalámbrico

Herramientas Básicas de Pentesting

Existen cientos de herramientas de hacking disponibles en Internet.
Estas son apenas unas cuantas que se destacan por su popularidad.

Servicios opcionales

Wardialing

Es un tipo de auditoría enfocada en determinar la seguridad de servidores de comunicaciones que se conectan a un pool de módems para proveer acceso telefónico remoto.

Wardriving

También llamado WiFi hacking, el wardriving persigue detectar vulnerabilidades que podrían estar presentes en las redes inalámbricas del cliente.

Ingeniería Social

La ingeniería social ataca al eslabón más débil de la cadena de seguridad: las personas. Existen distintos tipos de ingeniería social, pero de forma general se clasifican en: basada en humanos y basada en computador.

Simulación de Equipo Robado

En este tipo de pruebas el auditor simula el robo de un dispositivo móvil de un ejecutivo importante de la empresa, para tratar de hallar vulnerabilidades que permitan exfiltrar información.

CONSULTING

SYSTEMS

https://www.consulting-systems.tech

info@consulting-systems.tech