# Qué es la seguridad informática

En los tiempos actuales la seguridad informática ha tomado un papel privilegiado en el área informática, ya que la mayoría de la personas saben los riegos que corren al estar expuestas a la gran red de redes es decir el Internet.

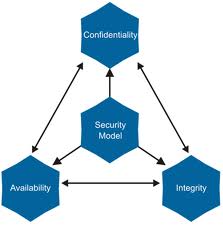
La mayoría de organizaciones están cambiando las formas de realizar sus negocios, y esto se debe en gran medida al avance tecnológico que ha hecho posible el desarrollo de un software cada vez más complejo que facilite la interconexión entre los distintos sitios de trabajo. Pero a pesar de que esto significa una mejora, también ha hecho posible que toda la información de una determinada empresa se encuentre en la red, entonces aquí viene la gran interrogante ¿Como la empresa asegura sus sistemas, sus redes y sobretodo su información confidencial, y aún más importante como sabe la empresa que la tecnología adquirida es segura?

La información es demasiado importante para dejarla en un segundo plano y por tanto hay que protegerla, conociendo como se perpetúa un ataque desde el punto de vista de un hacker y de esta manera tomar medidas para contrarrestarlo.

**El objetivo que persigue la seguridad informática, es identificar ciertas vulnerabilidades de un sistema y establecer contramedidas que imposibiliten que distintas amenazas exploten dichas vulnerabilidades.**

Pero hay que tener en cuenta la seguridad informática es dinámica, esto quiere decir que los sistemas son actualizados constantemente por la aparición de nuevas vulnerabilidades que atentan a la seguridad de la información

Las características que la seguridad informática debe garantizar son:



* Confidencialidad: La confidencialidad es la protección de los datos transmitidos de ataques pasivos. Con respecto a la liberación del contenido del mensaje, varios niveles de protección pueden ser identificados. El servicio más amplio protege todos los datos de usuario transmitidos entre dos usuarios durante un período de tiempo. Por ejemplo, si un circuito virtual se establece entre dos sistemas, esta amplia protección impediría la liberación de los datos de usuario transmitidos por el circuito virtual. Formas más estrechas de este servicio también se pueden definir, incluida la protección de un solo mensaje o incluso campos específicos dentro de un mensaje. Estos refinamientos son menos útiles que el enfoque amplio e incluso pueden ser más complejo y costoso de implementar.
* Integridad: Al igual que con la confidencialidad, la integridad se puede aplicar a un flujo de mensajes, un mensaje solo, o campos seleccionados dentro de un mensaje. Una vez más, el enfoque más útil y directo es la protección total del flujo.

Un servicio de integridad orientado a la conexión, que se ocupa de un flujo de mensajes, asegura que los mensajes son recibidos como enviados, sin duplicación, inserción, modificación, reorganización, o las repeticiones. La destrucción de los datos también está cubierta por este servicio. Por otro lado, un servicio de integridad sin conexión, en la que se ocupa de mensajes individuales sólo sin tener en cuenta cualquier contexto más amplio, generalmente proporciona protección contra la única modificación mensaje. Kent señala que un servicio híbrido se puede ofrecer para aplicaciones que requieren algún tipo de protección contra la reproducción y reordenamiento pero que no requieren la secuenciación estricta.

Podemos hacer una distinción entre el servicio con y sin recuperación. Debido a que el servicio de integridad se refiere a ataques activos, estamos preocupados con la detección en lugar de la prevención. Si se detecta una violación de la integridad, a continuación, el servicio puede simplemente informar de esta violación, y alguna otra porción de software de la intervención humana se requiere para recuperarse de la violación. La incorporación de mecanismos de recuperación automatizados es, en general, la alternativa más atractiva.

* Disponibilidad: Una variedad de ataques puede resultar en la pérdida o reducción de la disponibilidad. Algunos de estos ataques son susceptibles a las contramedidas automatizadas, tales como la autenticación y el cifrado, mientras que otros requieren algún tipo de acción física para prevenir o recuperarse de la pérdida de la disponibilidad de los elementos de un sistema distribuido.

# Terminología Básica

## Ataque

## Vulnerabilidad

## Hacker

## Evaluacion de un objetivo

## Exploit

## Zero-Day

## Vector de ataque

## Pentesting

“Una metodología de prueba en la que los evaluadores, por lo general trabajan bajo restricciones específicas, intentando evadir o derrotar a los elementos de seguridad de un sistema de información.” [NIST 800-53].

Pero además de una metodología son necesarias ciertas técnicas que nos permitan realizar una evaluación de las debilidades de un sistema informático, siendo este sistema informático no solo los servidores o sistemas de información, sino también a las aplicaciones web, la seguridad física de una empresa y todo lo que pueda ser vulnerado.

# Pentesting

## Objetivo del Pentesting

Los intrusos siempre van a aprovechar las vulnerabilidades de un sistema para poder ingresar de forma no autorizada, pero estas vulnerabilidades a menudo no solo se deben a la falta de actualización del sistema, sino que también se debe a descuidos y malas configuraciones por parte del administrador de la red o por los usuarios de la misma.

Los objetivos que persigue el Pentesting son:

* Evaluar un sistema o proyecto
* Conocer la situación real de la organización
* Medir y obtener una calificación objetiva del nivel de seguridad
* Mejora continua de la seguridad
* Cumplir con regulaciones y auditorias

## Tipos y alcances del Pentesting

Los proyectos de un servicio de pentesting pueden clasificarse en:

* Externo: En el cual se somete a los sistemas a pruebas de seguridad informática que simulan la realización de un ataque por parte de un atacante que se encuentra fuera del red interna
* Interno: En el cual se somete a los sistemas a pruebas de seguridad informática que simulan la presencia de un atacante que se encuentra en la red interna, es decir dentro de la organización o empresa.

Las pruebas de pentesting en general se realizan sobre:

* Sistemas (\*) informáticos
* Redes y configuración de un sistema
* Aplicaciones web
* Redes wireless

Como se mencionó anteriormente existen una serie de metodologías en el Pentesting, y son las siguientes:

* Black box (caja negra)
* Gray box (caja gris)
* White box (caja blanca)

### Black Box

Un test de penetración de caja negra es aquel en donde se simula el ataque de un hacker malicioso y en el cual el auditor o pentester solo tendrá los recursos que un hacker malicioso tendría, como es la información pública o la obtenida por medio de distintos métodos que se explicarán en la fase de footprinting.

#### Ventajas:

1. Estimación real de las amenazas
2. Obtención de resultados a través de información pública
3. El esfuerzo del cliente es mínimo

#### Desventajas:

1. Dificultad de recolectar la información
2. Pueden pasar desapercibidas ciertas vulnerabilidades.
3. Las recomendaciones para los fallos de seguridad en muchos casos con generales.

### White box

Para llevar a cabo un test de caja blanca los pentester deben tener información detallada de toda la infraestructura de la empresa (archivos de configuración, documentación, diagramas, etc.) este tipo de ataque es más exhaustivo porque no solo se revisan vulnerabilidades inmediatas sino también configuraciones potencialmente peligrosas.

#### Ventajas:

1. Extremadamente minucioso.
2. Las recomendaciones para reparar fallos son muy precisas.
3. Detección de amenazas inmediatas, así como defectos de configuración y construcción.

#### Desventajas:

1. Requiere muchos recursos tanto del auditor como del cliente
2. Se requiere revisar el código fuente de las aplicaciones
3. Auditoria de red.

### Gray box

Los test de caja gris se realizan como una combinación de los test de caja negra y los test de caja blanca, en el cual los pentester simulan ataques de hackers maliciosos pero con información detallada del sistema que se está auditando.

#### Ventajas:

1. Más rentable.
2. Estimación realista de las amenazas.

#### Desventajas:

1. No simula un ataque real como en el test de caja negra.

# Clases de hackers

## Hacker de sombrero Blanco

Este tipo de hackers son personas, que de manera altruista o no, dedica su tiempo a la búsqueda de vulnerabilidades en un sistema para posteriormente reportarlas al administrador del mismo y colaborar con él en su consecuente reparación.

Sus objetivos no son para nada maliciosos, al contrario normalmente realiza su trabajo bajo un consentimiento del propietario del sistema.

## Hacker de sombrero Negro (Black Hat)

El black hat es lo que se llamaría cracker, y sus fines además de lucrativos la mayoría de la veces, totalmente destructivos, generalmente son personas con extraordinarios conocimientos sobre computación.

Jamás notificara de algún error encontrado y los utilizara en su conveniencia generalmente para echar abajo servidores importantes, borrar información privada, etc.

## Hacker de sombrero gris (Grey Hat)

Este tipo de hacker es una mezcla de los dos anteriores (White hat y black hat), aunque de la mayoría de la veces se acerca más a las metodologías utilizadas por un white hat.

Este tipo de personaje se encuentra en un dividido entre las dos fronteras, pero debido a su actitud y ética le permite decidir con certeza qué comportamientos son los más adecuados a la situación que enfrentan, por este motivo se lo puede categorizar con un hacker ético.

Además existen otros términos como lamer, script kiddie, newbie, wannabie. Los matices cambian dependiendo de la orientación que posean hacia el bien o hacia el mal, pero todos tienen en común el bajo nivel de conocimientos de las técnicas de hacking.

# Fases en los test de penetración



## Etapa de reconocimiento

Es esta etapa el pentester tiene la tarea de recopilar la mayor cantidad de información relacionada con el objetivo, y para ello utiliza técnicas como footprinting o ingeniería social.

La información que trata de conseguir el pentester suele ser la siguiente:

* Nombres de usuarios y cuentas de correo electrónico
* Direcciones IP de servicios de terceros
* Rangos de direcciones IP asignadas
* Dirección física de la empresa
* Proveedores y clientes
* Software y Hardware
* Números telefónicos

Esta etapa suele realizarse de manera pasiva y por lo que normalmente se requiere de mucho software, ya que la información se la puede conseguir utilizando ingeniería social y en muchos casos en redes sociales.

Pero también puede utilizarse un reconociendo activo, el cual involucra una interacción con el objetivo es decir el personal de la empresa

## Etapa de escaneo

Esta etapa es de pre-ataque en donde se escanea la red del objetivo pero ya con información de la fase previa. Se suele tener con objetivo la identificación de direcciones ips, dominios, hardware y software en la red pero de una manera más profunda ya que ya que se requiere identificar la MAC address del objetivo, información de los usuarios, Host/Dominios, routers, servicios, sistema operativo y se suele utilizar diferentes herramientas como son Nmap, Enum, PSTools, User2SID, etc.

A través de identificar toda esta información se puede detectar vulnerabilidades y puntos posibles de entrada.

En esta etapa se suele utilizar tanto un reconocimiento activo como pasivo.

## Etapa de obtener acceso

Esta etapa se refiere al punto donde el atacante obtiene acceso al sistema operativo de un computador en la red del objetivo.

También en esta etapa se puede descartar falsos positivos obtenidos en la fase previa.

Generalmente para obtener acceso a través de algún punto débil de la red del objetivo se utiliza exploits, frameworks de penetración, password cracking, denegación de servicio, sesión hijacking. Los frameworks más utilizados son:

* Metasploit
* Core Impact
* Canvas
* SaintExploit

Después de obtener el acceso el atacante puede escalar privilegios para obtener un completo control del sistema.

## Etapa de mantener acceso

En esta etapa el atacante intenta retener los privilegios obtenidos en la fase previa.

A menudo el atacante blinda el sistema contra otros posibles hackers, protegiendo sus puertas traseras, rootkis y troyanos.