



# INICIO GRABACIÓN



**SANJOSÉ**  
FUNDACIÓN DE EDUCACIÓN SUPERIOR



## **METODOLOGÍAS DE ANÁLISIS DE VULNERABILIDADES**

El objetivo de este capítulo es implementar una metodología de análisis de vulnerabilidades con la finalidad de tratar de mitigar o bajar los riesgos que se encuentran en determinados sistemas dentro de la organización. Para esto se establecen una serie de pasos para lograr dicho proceso.

# Acuerdo de confidencialidad



Una de las tareas principales que se debe verificar, es la parte del acuerdo de confidencialidad entre ambas partes, donde intervienen la empresa y el analista de seguridad. Es importante realizar un acuerdo de confidencialidad entre las dos partes involucradas en el análisis, debido a que, a lo largo de la búsqueda de vulnerabilidades, se puede obtener alguna información crítica para la organización analizada, por ejemplo, nombres de usuario y contraseñas, algunos agujeros de seguridad, documentos que se encuentran expuestos en la red, etc.

Desde el punto de vista del analizador, el acuerdo de confidencialidad le ofrece un marco legal sobre el cual trabajar, constituyendo un respaldo formal a la labor realizada.

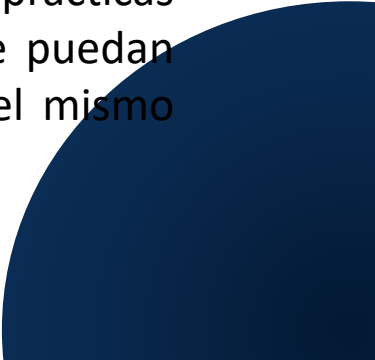
ACUERDO DE CONFIDENCIALIDAD
LUGAR Y FECHA
PARTES QUE INTERVIENEN
A QUE SE DEDICAN
MOTIVO
SERVICIO
CLÁUSULA DE CONFIDENCIALIDAD



# Establecimiento de las reglas del juego



Otro de los puntos que se deben de establecer, son las reglas del juego, esto se refiere a todo antes de comenzar con el análisis de vulnerabilidades, ya que es necesario definir cuáles van hacer las tareas que se van a realizar y cuáles serán los límites, permisos y obligaciones que se van a respetar. Es probable que la organización que sea analizada no esté interesada en que sus servicios se suspenden, probablemente por algún ataque de denegación de servicio que sea exitoso por parte del analista. En caso de que esto suceda el experto deberá ser capaz de determinar las vulnerabilidades, durante el análisis se debe de mantener informada a la menor cantidad de personas, de forma de que la utilización de la red por parte del personal sea normal, con la finalidad de evitar cambios en la forma de trabajo de los usuarios de manera regular, ya que, si los usuarios de la red son informados que se va a realizar un cierto análisis, probablemente, lo que van a hacer es modificar algunas prácticas inseguras que normalmente realizan por miedo precisamente a que puedan ser reprendidos, despedidos y si esto sucede el análisis no tendrá el mismo efecto.

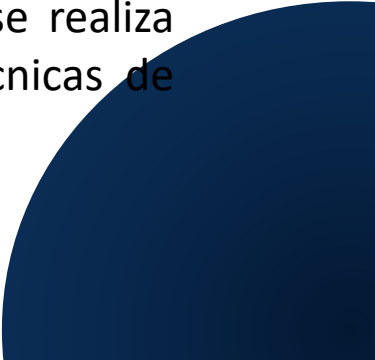




## Recolección de información

Otro de los puntos que se debe de verificar, es la parte de la recolección información, así como anteriormente se ha analizado los test de caja negra y caja blanca, el análisis de vulnerabilidades comienza con la obtención de información del objetivo, si se está seleccionando un test de caja negra, el proceso de análisis será muy similar al proceso seguido por un atacante, si se realiza el proceso de caja blanca, este es el momento para recopilar la mayor cantidad de información de acceso a servicios, información y todo lo que se considere necesario al momento de realizar el análisis. Por ejemplo, si se está realizando un test de caja blanca probablemente lo que hay que obtener son direcciones de servidores, nombres de usuarios, contraseñas, servicios que se llegan a brindar, esquemas de redireccionamiento, topologías de red, niveles de privilegios, etc.

Si se realiza un test de caja negra se puede obtener probablemente alguna dirección, nombres de dominio, correos electrónicos, etc. Cuando se realiza este tipo de análisis para recolectar la información uno de las técnicas de análisis para levantar la información es el llamado OSINT.





- **Requisitos:** En esta fase se establecen todos los requerimientos que se tienen que cumplir, como las condiciones que tienen que cumplirse según los objetivos planteados para resolver el problema.
- **Identificación de las fuentes de información:** En esta fase se especifican a partir de los requisitos establecidos, todas las fuentes necesarias que serán recopiladas, se deben concretar y especificar las fuentes de información que serán relevantes con el objetivo de optimizar el proceso de adquisición.
- **Adquisición:** En esta fase se obtiene la información partiendo de los orígenes indicados.
- **Procesamiento:** Esta fase se basa en dar formato a la información recopilada para que pueda ser analizada.
- **Análisis:** Aquí en esta fase se genera inteligencia a partir de los datos recopilados y procesados.
- **Inteligencia:** Se base en presentar la información recopilada de una manera eficaz, útil y comprensible para que pueda ser correctamente explotada.





# Análisis interior



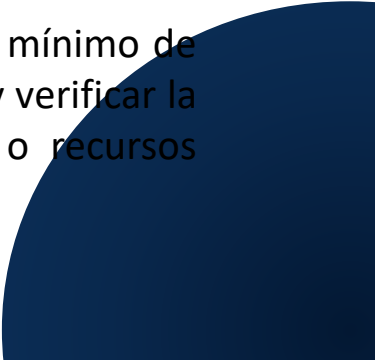
se debe verificar varios tipos de test, un análisis interior trata de mostrar o demostrar hasta dónde se puede llegar con los privilegios de un usuario típico dentro de la organización, para poder realizarlo se requiere que la organización provea una computadora con un nombre de usuario y una clave de acceso normal de un usuario específico.

**La revisión de la privacidad:** aquí simple y sencillamente el analista se centra en cómo se gestiona desde el punto de vista ético y legal el almacenamiento, transmisión y control de la información que todos los usuarios típicos o los empleados utilizan día a día.

**Testeo de aplicaciones de internet:** La parte del análisis de aplicaciones de internet o de aplicaciones web, este estudio se emplea de manera diferente, por ejemplo, se realizan técnicas de análisis de software para encontrar fallas de seguridad en aplicaciones que sean cliente servidor de un sistema desde internet.

**Testeo de sistema de detección de intrusos:** En este tipo de análisis, normalmente se enfoca en la parte del rendimiento de los sistemas de identificación de intrusos, la mayor parte de este análisis normalmente no se puede llevar a cabo de manera adecuada, si no, accediendo a los registros del sistema de identificación de intrusos.

**Testeo de medidas de contingencia:** En este tipo de análisis se debe medir el mínimo de recursos necesarios que se necesitan en el subsistema, para realizar las tareas y verificar la detección de medidas presentes para la detección de intentos de acceso o recursos protegidos.





**Descifrado de contraseñas:** Descifrar las contraseñas es el proceso de validar cuan robusta puede ser una clave, a través del uso de herramientas de recuperación de contraseñas de manera automática, dejando normalmente al descubierto las aplicaciones de algoritmos criptográficos débiles y mal implementados o contraseñas débiles debido a factores humanos ya que las personas no se encuentran preparadas lo suficiente como para poder registrar una buena clave de seguridad.

**Testeo de denegación de servicios:** La denegación de servicio es una situación, donde una circunstancia sea intencional o de manera accidental previene a el sistema de que llegue a funcionar de manera exactamente como se dice lo diseñó.

**Evaluación de políticas de seguridad:** En la evaluación de políticas, la reducción de riesgos en una organización con la utilización de tipos de específicos de tecnologías, por ejemplo Cisco, existen dos funciones a llevar a cabo, lo primero es el análisis de lo escrito contra el estado actual de las conexiones y segundo asegurar que la política esté incluida dentro de las justificaciones del negocio de la organización.





# Análisis exterior



el principal objetivo de este tipo de análisis, es acceder en forma remota a los servidores de la organización y sobre todo obtener privilegios o permisos que no deberían estar disponibles. Este test puede comenzar con técnicas ya sea aplicando ingeniería social para poder obtener alguna información y luego se podría utilizar en algún intento de acceso.

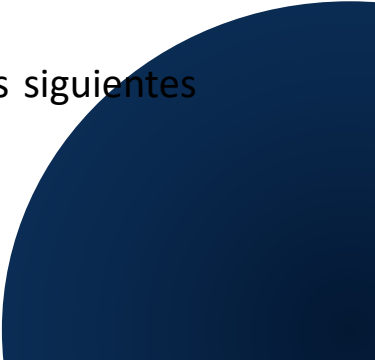
**Revisión de la inteligencia competitiva:** Esta parte se basa en toda la información recolectada a partir de la presencia en internet de la organización.



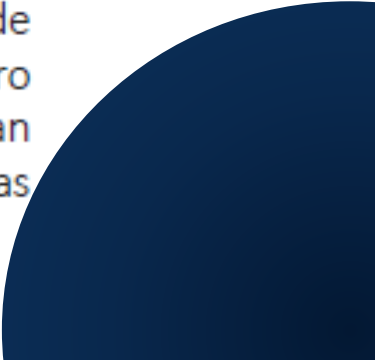
**Revisión de la privacidad:** Esta etapa se basa en un punto de vista legal y ético del almacenamiento, transmisión y control de los datos basados en la privacidad del cliente.




**Análisis de solicitud:** Éste es el método para obtener privilegios de acceso a una organización y sus activos, preguntando sencillamente al personal de entrada usando las comunicaciones como algún teléfono, correo, chat, etc., desde una posición privilegiada o de una forma fraudulenta que tiende a ser simplemente un análisis basado en ingeniería social.

**Análisis de sugerencia dirigida:** Aquí en este método, se intenta lograr que un integrante de la organización ingrese a un sitio o reciba un correo electrónico en este sitio o el correo se podría agregar a herramientas que luego serían utilizadas en el intento de acceso.

Una vez que se recopila esta información se procede a realizar algunas de las siguientes pruebas que se muestran a continuación:




- 
- 
1. **Sondeo de red:** Sirve como Introducción a los sistemas a ser analizados, aquí se analizan nombres de dominio, nombres de servidores, direcciones IP, mapas de red, información del proveedor de internet, propietarios de sistema y servicios.
  2. **Identificación de los servicios de sistemas:** En esta prueba se deben enumerar los servicios de internet activos o sobretodo accesibles, así como, traspasar el firewall con el objetivo de encontrar más máquinas activas, luego es necesario llevar adelante un análisis de la aplicación que escucha, tras dicho servicio. Tras la identificación de los servicios el siguiente paso simplemente es identificar al sistema con el fin de obtener respuestas que pueden dirigir el sistema operativo y su versión, técnicamente realizar un análisis de Fingerprint.
  3. **Búsqueda y verificación de vulnerabilidades:** Esta prueba se basa en la identificación, comprensión y verificación de las vulnerabilidades o debilidades, errores de configuración dentro de un servidor o en una red. La búsqueda de vulnerabilidades se realiza mediante herramientas automáticas para determinar agujeros de seguridad existente y niveles de parcheado de los sistemas, pero se debe tener en cuenta nuevas vulnerabilidades que se publican en sitios donde normalmente todavía no incluyen las herramientas automáticas.
- 

- 
- 
4. **Testeo de aplicaciones de internet:** Aquí se emplean diferentes técnicas de análisis de software para encontrar fallos de seguridad en aplicaciones cliente, como se está realizando un análisis externo, se pueden utilizar en este módulo los test de caja negra.
  5. **Testeo de relaciones de confianza:** La parte de enrutamiento técnicamente está diseñado para asegurar que sólo aquellos que deben ser expresamente permitidos puede ser aceptado en la red.
  6. **Verificación de redes inalámbricas:** Aquí en este caso se menciona la parte del estándar 802.11, que es un método para la verificación del Wireless que normalmente se basa en la parte de la cobertura y el acceso de los Access Point por red ad hoc.
- 



## Documentación e informes

En los puntos anteriores se analizó la parte del análisis interno y externo, ahora se debe realizar un análisis acerca de la parte de la documentación y los informes. Como en la parte de la finalización del análisis de vulnerabilidades se debe presentar un informe, donde se detalle cada uno de los test que se han realizado y los resultados de los mismos. Este informe debe especificar la lista de vulnerabilidades que han sido probadas, las vulnerabilidades detectadas, lista de servicios y dispositivos vulnerables, el riesgo o el nivel de riesgo que involucra cada vulnerabilidad que ha sido encontrada en cada servicio y dispositivo, como tal se debe incluir los resultados de los programas utilizados.





## **HERRAMIENTAS PARA EL ANÁLISIS DE VULNERABILIDADES**

El objetivo es mostrar las herramientas más utilizadas para el análisis de vulnerabilidades en los sistemas, los pasos necesarios para interpretar todos los fallos encontrados y sobre todo las posibles soluciones para dichas falencias.

# análisis de vulnerabilidades



Actualmente existen muchas herramientas para el análisis de fallos e inseguridades en el mercado, una de estas aplicaciones tipo escáner más populares es Nessus, esta solución es un escáner de vulnerabilidades desarrollado por la empresa Tenable Network Security, en la actualidad ofrece distintas soluciones no solo de escaneos de redes para encontrar fallos, sino, aplicaciones más completas como Nessus Security Center

- Cumplimiento de estándares
- Detección de Malware,
- Escáner de vulnerabilidades



# análisis de vulnerabilidades



Acunetix también trabaja con vulnerabilidades que pueden tener un impacto muy grande las cuales están integradas en su escáner, esta herramienta que tiene varias posibilidades de trabajo para su utilización, se instala y se trabaja de manera local o se realiza los escaneo en línea.

De manera muy general en esta herramienta se puede seleccionar a un objetivo y con ello se puede realizar un escaneo para detectar vulnerabilidades, con esto, se puede seleccionar un rango determinado de direcciones IP y comenzar la detección de las posibles fallas dentro de la empresa.



## Audit your website security

Firewalls, SSL, and hardened networks are futile against web application hacking! Hackers are concentrating on web-based applications (shopping carts, forms, login pages, etc.) - accessible 24/7 - and directly connected to your database back-ends with valuable data. Web applications are tailor-made, less tested than off-the-shelf software and likely to have undiscovered vulnerabilities that can be a recipe for disaster. Don't overlook Website security at your organization!

Acunetix is the leading web vulnerability scanner used by serious Fortune 500 companies and widely acclaimed to include the most advanced SQL Injection and XSS black box scanning technology. It automatically crawls your website and performs black box AND grey box hacking techniques which finds dangerous vulnerabilities that can compromise your website and data.

## Choose Scanning Options

Scan Type

Full Scan

Report

Full Scan

Schedule

High Risk Vulnerabilities

Cross-site Scripting Vulnerabilities

SQL Injection Vulnerabilities

Weak Passwords

Crawl Only

Create Scan

Close



# análisis de vulnerabilidades



Languard es un escáner de vulnerabilidades que tiene algunas ventajas sobre otras herramientas, ya que permite escaneos de forma local y en red, para los escaneos se pueden necesitar algunos datos como pueden ser las credenciales de un usuario ya sea estándar, el cual puede ser administrador local o administrador de dominio y a partir de ahí se puede ir realizando los análisis. Entre las múltiples ventajas de esta herramienta se puede mencionar:

- Automatizar la actualización de múltiples SO
- Buscar vulnerabilidades
- Auditar hardware y software
- Realizar informes de cumplimiento



También busca las vulnerabilidades en más de 60000 evaluaciones de vulnerabilidades que se realizan a través de las redes LanGuard, esto incluye entornos virtuales, dispositivos móviles y datos de la red, tanto de infraestructura como CISCO, TRICOM, datos de sistemas operativos como Windows, Linux, Mac, entre otras.



FUNDACIÓN DE EDUCACIÓN SUPERIOR

**SAN JOSÉ**

INSTITUCIÓN TECNOLÓGICA

FIN DE  
GRABACIÓN