Capitulo 5. Vulnerabilidades de los sistemas informáticos

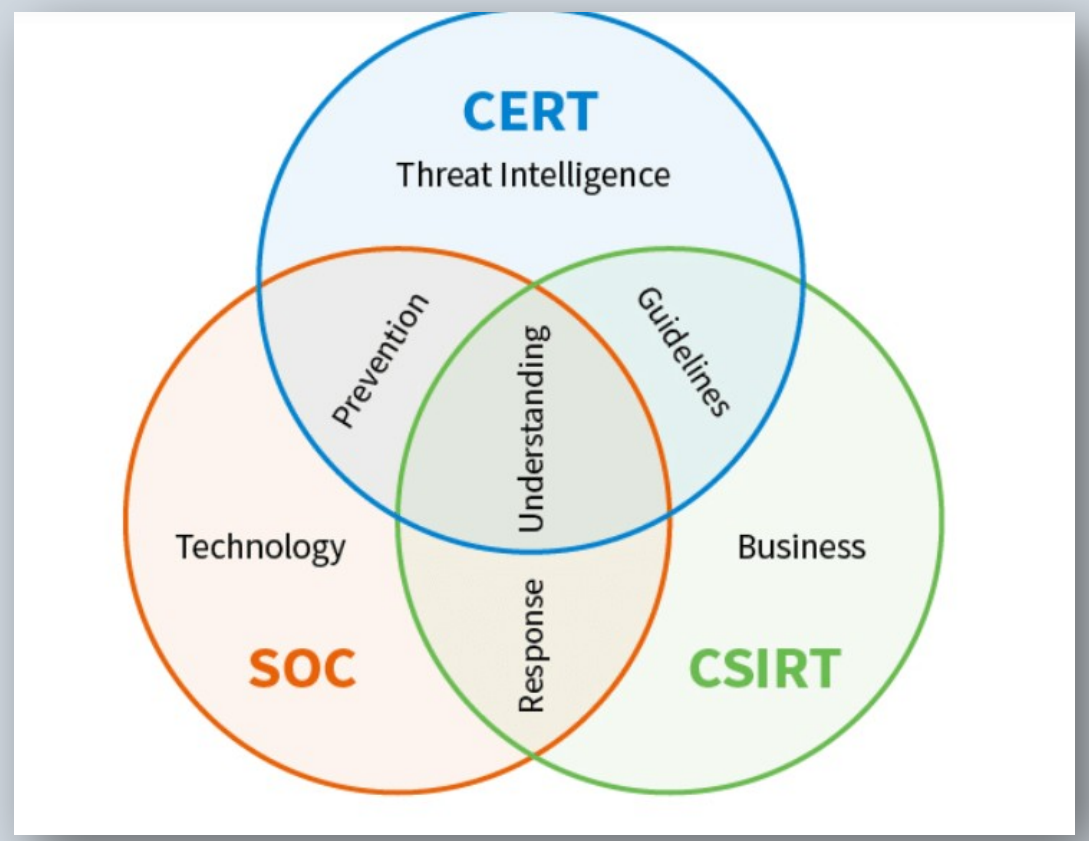
PATRICIA MEDINA
MGP.

Incidentes de seguridad en las redes

- Hasta finales de 1988 muy poca gente se tomaba en serio el tema de la seguridad en redes de ordenadores. el 22 de noviembre de 1988 Robert Morris protagonizo el primer gran incidente de la seguridad informática, uno de sus programas se convirtió en el famoso worm o gusano de internet.
- Miles de ordenadores conectados a la red se vieron inutilizados durante días y las perdidas se estimaron en millones de dólares.

Cert (Equipo de respuesta a emergencias informáticas)

- Es un grupo constituido en su mayor parte por voluntarios cualificados de la comunidad informática, cuyo objetivo principal era facilitar una respuesta rápida a los problemas de seguridad que afectaran a redes de ordenadores conectados a internet.



Causas de las vulnerabilidades de los sistemas informáticos

1. Debilidad en el diseño de los protocolos utilizados en las redes
2. Errores de programación
3. Configuración inadecuada de los sistemas informáticos
4. Políticas de seguridad deficientes e inexistentes

Otras causas de vulnerabilidades

- Ejecución de mas servicios de los necesarios en los equipos, con cuentas de usuario que tienen privilegios excesivos para su función.
- Mantenimiento inadecuado de los sistemas: no se instalan y revisan los parches suministrados por el fabricante.
- Algunas aplicaciones informáticas presentan problemas de usabilidad de cara al usuario poco experimentado, que no es consciente de las opciones relacionadas con la seguridad.
- Modems, con una configuración insegura que facilitan el acceso no autorizado de usuarios externos, mediante técnicas conocida como war dialing
- Routers que utilizan los protocolos de enrutamiento poco seguros que no garantizan la integridad y autenticidad de los mensajes de control mediante los que se intercambian información sobre las rutas. Se recomienda utilizar protocolos de enrutamiento mas avanzados como OSPF o BGP.
- Contar con excesivas relaciones de confianza entre redes y servidores, que facilitan el acceso a servidores sin requerir de autenticación. (Dominios de confianza de Windows, archivos .rhosts y host.equiv y los comandos R que facilitan la confianza transitiva entre varios servidores.

4. Políticas de seguridad deficientes e inexistentes

Situaciones que provocan vulnerabilidades en los sistemas informáticos

- Política de contraseñas poco robusta
- Deficiente control de los intentos de acceso al sistema
- Escaso rigor en el control de acceso a los recursos
- Procedimientos inadecuados para la gestión de soportes informáticos o el control de equipos portátiles.
- Escaso control de las copias generadas en papel con información sensible.

Situaciones que provocan vulnerabilidades en los sistemas informáticos

- Falta de control de los tratamientos realizados por terceros
- Deficiente o inexistente limitación del acceso físico a los equipos mas sensibles , dispositivos de red y cableado
- Instalación de programas poco fiables por parte de los usuarios
- Despreocupación por la instalación de parches y de nuevas versiones de software en servidores y otros equipos críticos
- Escasa protección de equipos portátiles que los usuarios pueden sacar de la red de la organización y que podrían resultar vulnerables frente a virus , troyanos u otros códigos dañinos

Situaciones que provocan vulnerabilidades en los sistemas informáticos

- **Registros de los servidores y de los dispositivos de red sin activar o activados**
- **Información sensible que se guarda sin cifrar en el sistema**
- Despreocupación por el adecuado almacenamiento de las copias de seguridad
- Transmisión de ficheros y mensajes de correo sin cifrar ni autenticar

Causas de las vulnerabilidades de los sistemas informáticos

5. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática
6. Disponibilidad de herramientas que facilitan los ataques
7. Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías
8. Existencias de puertas traseras en los sistemas informáticos
9. Descuido de los fabricantes

5. Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática

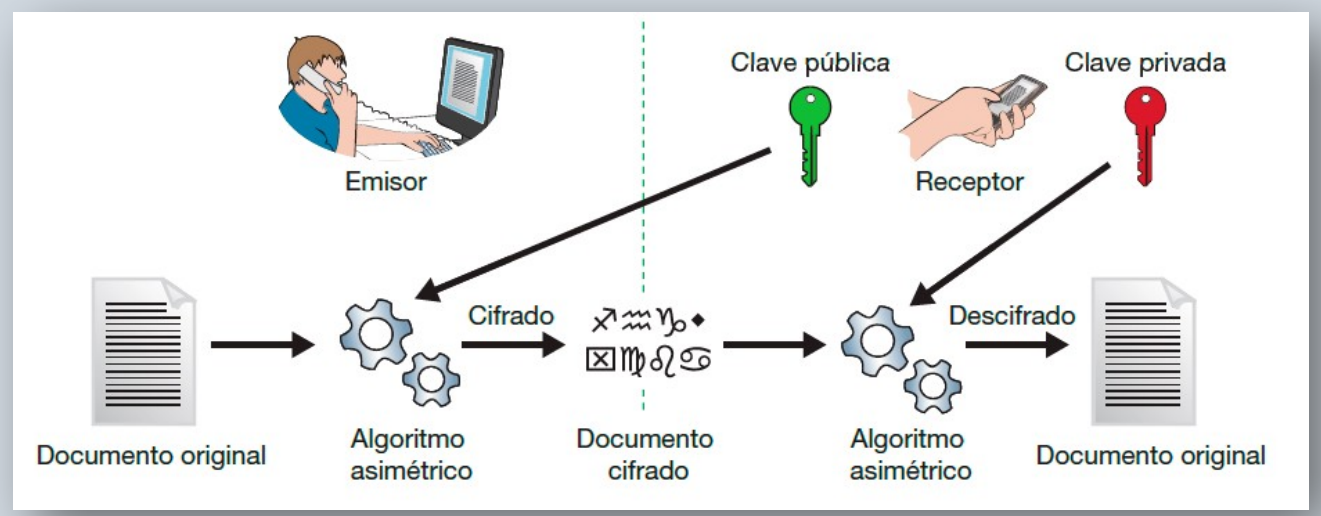
- Un principio básico a tener en cuenta desde el punto de vista de la seguridad informática es que todas las soluciones tecnológicas implantadas por la organización pueden resultar inútiles ante el desconocimiento, falta de información, desinterés o animo de causar daño de algún empleado desleal.
- La mayoría de los problemas relacionados con la seguridad suelen tener su origen en el factor humano.

6. Disponibilidad de herramientas que facilitan los ataques

- En internet se pueden localizar todo tipo de programas gratuitos, fáciles de utilizar gracias a sus interfaces graficas, con detallada documentación sobre su instalación y manejo, que permiten explotar agujeros de seguridad o llevar a cabo ataques mas sofisticados contra redes y sistemas informáticos.

7. Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías

- Los productos y algoritmos criptográficos se consideran tecnología susceptible de doble uso (civil y militar).
- La situación se agravado a raíz de los atentados del 11 de septiembre del 2001, ya que se ha comprobado que los grupos terroristas y el crimen organizado utilizan sistemas criptográficos para tratar de proteger sus comunicaciones.



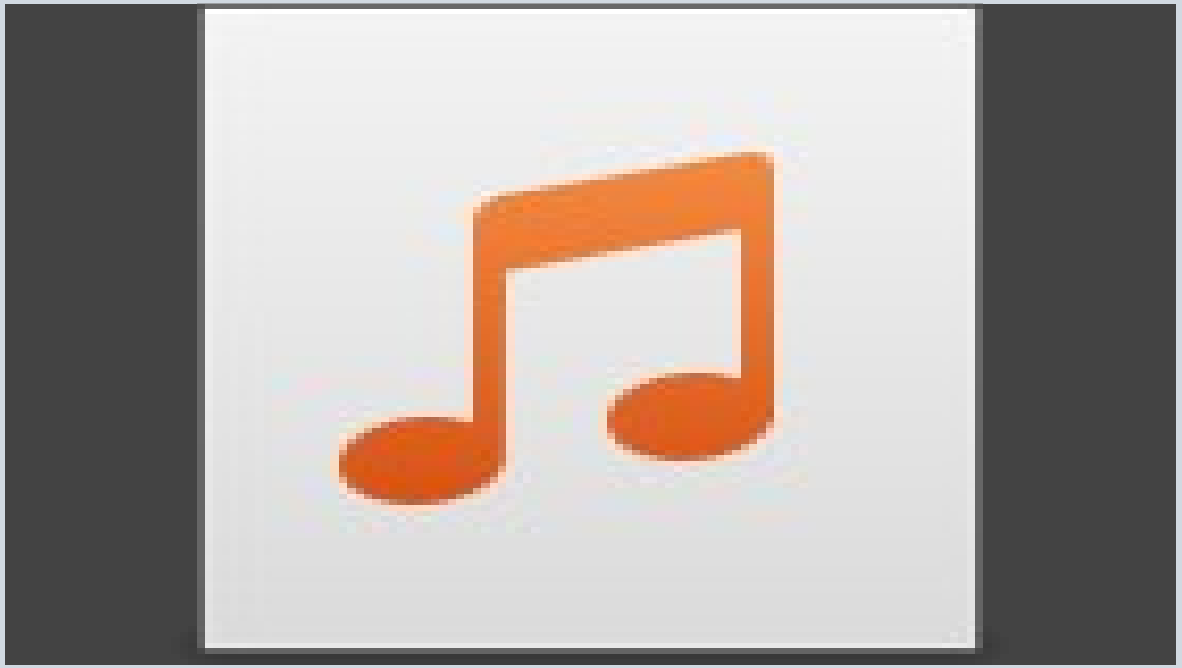
8. Existencias de puertas traseras en los sistemas informáticos

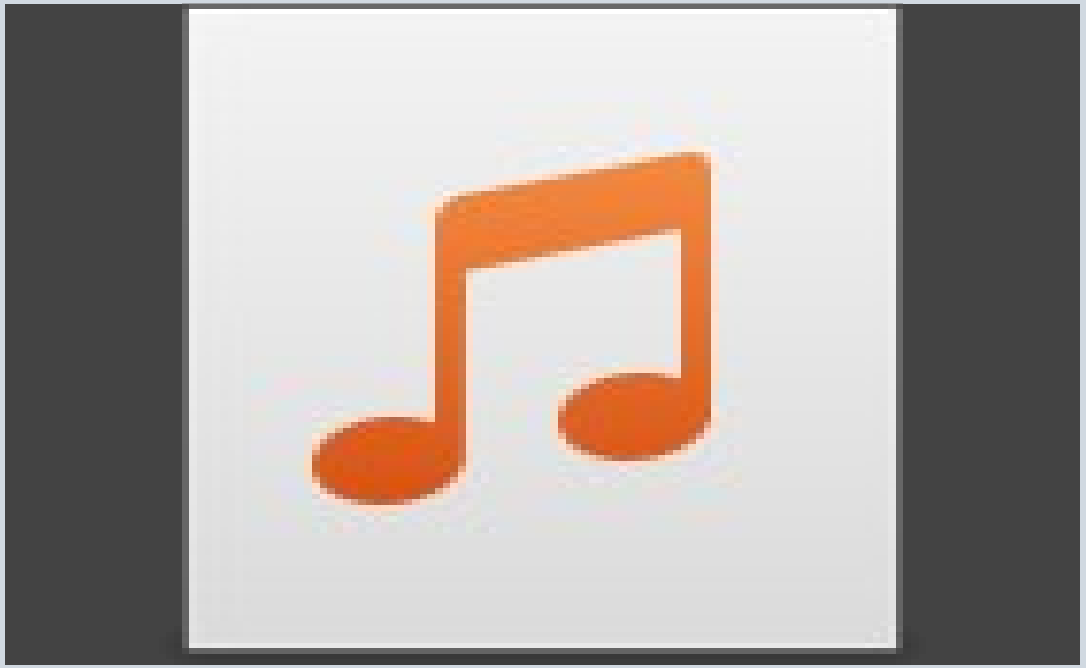
- La puertas traseras (backdoors), constituyen una vía de acceso no autorizado a un sistema informático, saltándose las medidas de protección previstas e implantadas por sus administradores.
- Estas puertas traseras puede tener su origen en una serie de servicios que se utilizan durante las fases de desarrollo de un sistema informático y que por error o descuido se mantienen en la versión final distribuida a los clientes.

9. Descuido de los fabricantes

- En algunos casos los propios fabricantes han contribuido a la propagación de virus y programas dañinos, al incluir su código en los discos duros de sus equipos o en los CD-ROM con los distintos programas y herramientas del sistema.

Videos de causas de vulnerabilidades:





Tipos de Vulnerabilidades

DESCRIPCIÓN DE LOS TIPOS DE VULNERABILIDADES MAS FRECUENTES, QUE PUEDEN AFECTAR TANTO A LOS EQUIPOS COMO A LAS APLICACIONES INFORMÁTICAS.

1. Vulnerabilidades que afectan a los equipos

1. Routers y cable-modems
2. Cámaras web y servidores de video
3. Vulnerabilidades en otros equipos conectados a una red: Impresoras, escáneres, faxes..
4. Teléfonos móviles
5. Agendas Electrónicas

2. Vulnerabilidades que afectan a programas y aplicaciones informáticas

1. Sistemas operativos, servidores y bases de datos
2. Navegadores
3. Aplicaciones Ofimáticas como Word o Excel
4. Otras utilidades y aplicaciones Informáticas

Responsabilidades de los fabricantes de software

EN LOS ÚLTIMOS AÑOS SE HAN DESATADO LAS CRITICAS CONTRA LOS FABRICANTES DE SOFTWARE Y DE EQUIPOS INFORMÁTICOS, A RAÍZ DE LAS CONTINUAS VULNERABILIDADES DESCUBIERTAS EN SUS PRODUCTOS Y A LAS CONSECUENCIAS CADA VEZ MAS GRAVES QUE ESTÁN PROVOCAN A SUS USUARIOS.

Ejemplo de responsabilidades de los fabricantes de software

- En octubre del 2003 se presentaba una demanda colectiva en el Estado de California contra Microsoft , basada en la reclamación de que su software dominante en el mercado era vulnerable a virus capaces de provocar “fallos masivos y en cascada” en las redes de ordenadores.
- Esta demanda alegaba una competencia injusta y la violación de dos leyes de derechos del consumidor de California, una de las cuales tiene el propósito de proteger la privacidad de la información personal en las bases de datos de los ordenadores.

Herramientas para la evaluación de vulnerabilidades

Herramientas para la evaluación de vulnerabilidades

1. Análisis y evaluación de vulnerabilidades
2. Ejecución de tests de penetración en el sistema

1. Análisis y evaluación de vulnerabilidades

- Una organización puede utilizar herramientas para la evaluación de vulnerabilidades, que permiten conocer la situación real de un sistema y mejorar su seguridad, verificando que los mecanismos de seguridad funcionan correctamente.
- Con la información obtenida de estas herramientas es posible justificar la implantación de nuevas medidas de seguridad y la obtención de mas recursos económicos, así como priorizar las medidas a implantar en función de las vulnerabilidades detectadas , seleccionando aquellas que resulten mas adecuadas teniendo en cuenta la relación costo/beneficio.

Revisión de equipos y servidores se deberían analizar y evaluarlos siguientes aspectos:

- Parches del sistema operativo
- Seguridad del sistema de ficheros
- Cuentas de usuarios
- Servicios y aplicaciones instaladas
- Protocolos y servicios de red
- Control de accesos a los recursos
- Registro y auditoria de eventos

Aspectos para garantizar el éxito de las pruebas realizadas en el sistema:

- Definición del alcance y objetivos de las pruebas a realizar
- Conocimiento y experiencia del equipo que analiza las vulnerabilidades y realiza las pruebas de intrusión en el sistema
- Nivel de automatización de las pruebas realizadas contando con el apoyo de las herramientas y metodologías adecuadas
- Actualización periódica de la base de datos de vulnerabilidades a analizar
- Controlar y limitar los posibles riesgos que se deriven de las pruebas, disminución del rendimiento de los equipos , denegación del servicio, exposición de información sensible.
- Realización de las pruebas de forma periódica o en momentos puntuales
- Registrar las puntuaciones y resultados obtenidos en las distintas pruebas realizadas

Documentación con los resultados de las pruebas

Resumen ejecutivo dirigido a personal no técnico

- Con una breve descripción de los trabajos realizados y las principales conclusiones y recomendaciones de

Informe técnico detallado

- Que describa el sistema objeto de estudio y los recursos analizados, todas las pruebas realizadas, las vulnerabilidades que han sido detectadas y las medidas propuestas para remediarlas y mejorar la seguridad del sistema.

Estándares para asegurar la calidad de los trabajos realizados y su evaluación por parte de terceros:

OSSTMM
Es un manual con una serie de secciones compuestas por módulos

OWASP
Para evaluar la seguridad de las aplicaciones web, así como la guía de pruebas de seguridad de red

CVE
Vulnerabilidades exposiciones comunes

2. Ejecución de tests de penetración en el sistema

- Dentro de la evaluación de la seguridad de un sistema informático los “Tests de penetración” representan una valiosa herramienta metodológica

Etapas del tests de penetración .

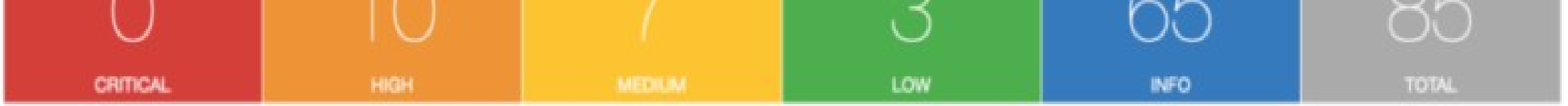
- Reconocimiento del sistema para averiguar que tipo de información podría obtener un atacante o usuario malicioso
- Escaneo propiamente dicho, consistente en la detección y verificación de vulnerabilidades en servidores estándar y en aplicaciones desarrolladas por la propia organización.
- Penetración: intento de explotación de las vulnerabilidades detectadas.
- Generación de informes, con el análisis de los resultados y la presentación de las conclusiones sobre la seguridad del sistema informático.
- Limpieza del sistema, para restaurar la situación inicial (si su seguridad ha sido comprometida por la explotación de alguna de las vulnerabilidades detectadas.

TESTS DE PENETRACIÓN EXTERNOS:

- Se realizan desde el exterior de la red de la organización, para tratar de forzar la entrada en algunos de sus servidores o comprometer su seguridad, mediante pruebas como el escaneo de puertos y la detección de los protocolos utilizados. El análisis del trafico cursado, del rango de direcciones utilizado y de los servicios ofrecidos a través de la red, pruebas de usuarios y de la política de contraseñas.

TESTS DE PENETRACIÓN INTERNOS:

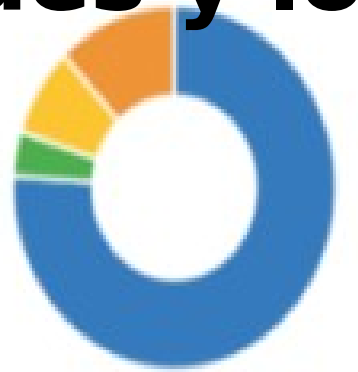
- Se llevan a cabo desde el interior de la red de la organización, mediante pruebas como el análisis de los protocolos utilizados y de los servicios ofrecidos. La autenticación de usuarios y la revisión de la política de contraseñas, la verificación de la seguridad lógica .



Ejemplos permiten llevar a cabo la evaluación de vulnerabilidades y los tests de penetración

Nessus

Una de las mas utilizadas es una herramienta construida en código abierto para sistemas UNIX y Windows que emplea el escáner de puertos NMAP para descubrir los servicios del sistema objeto de estudio.



WHISKE

FOUNDST

SATAN

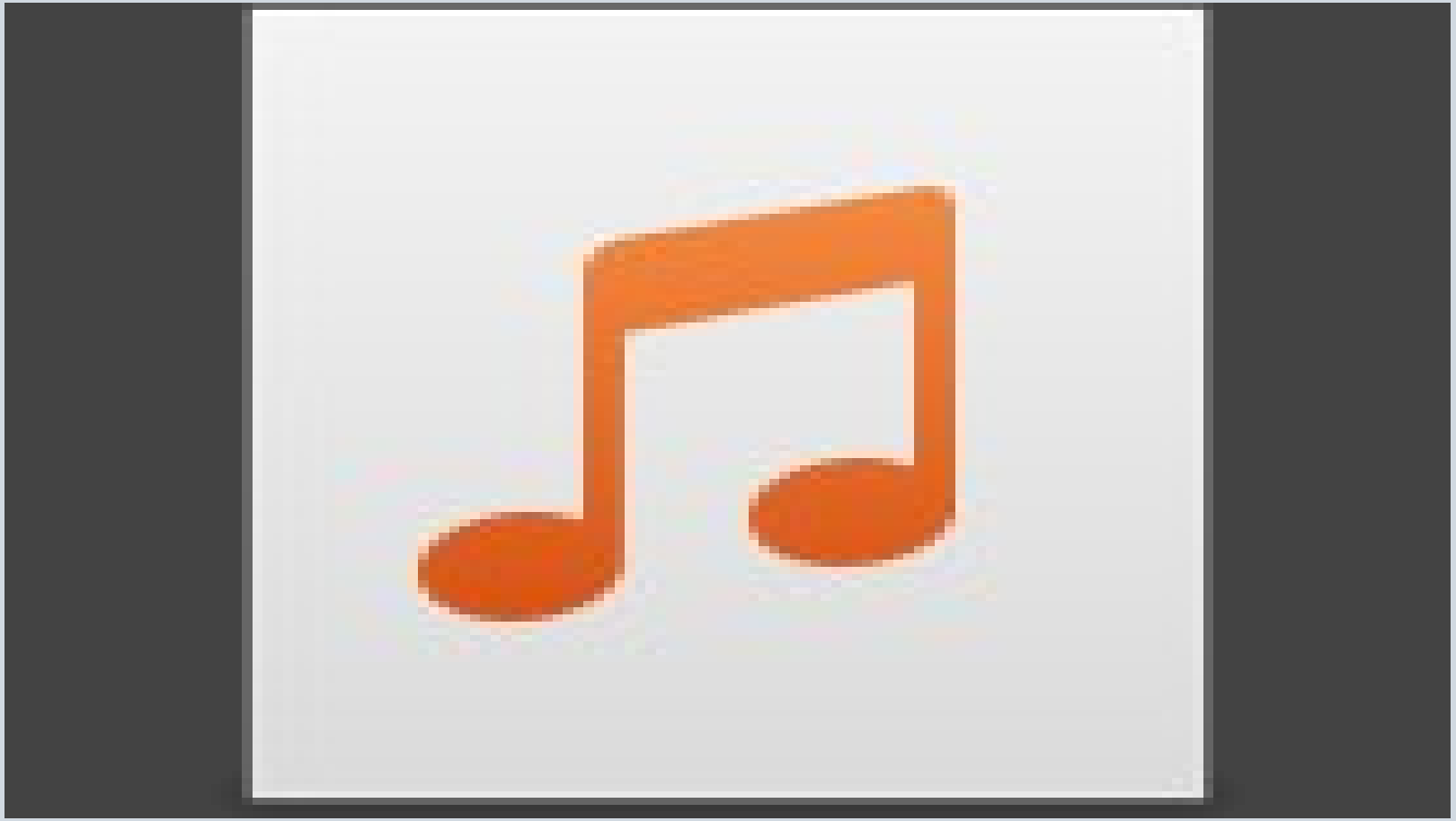
SPIKE

RETINA

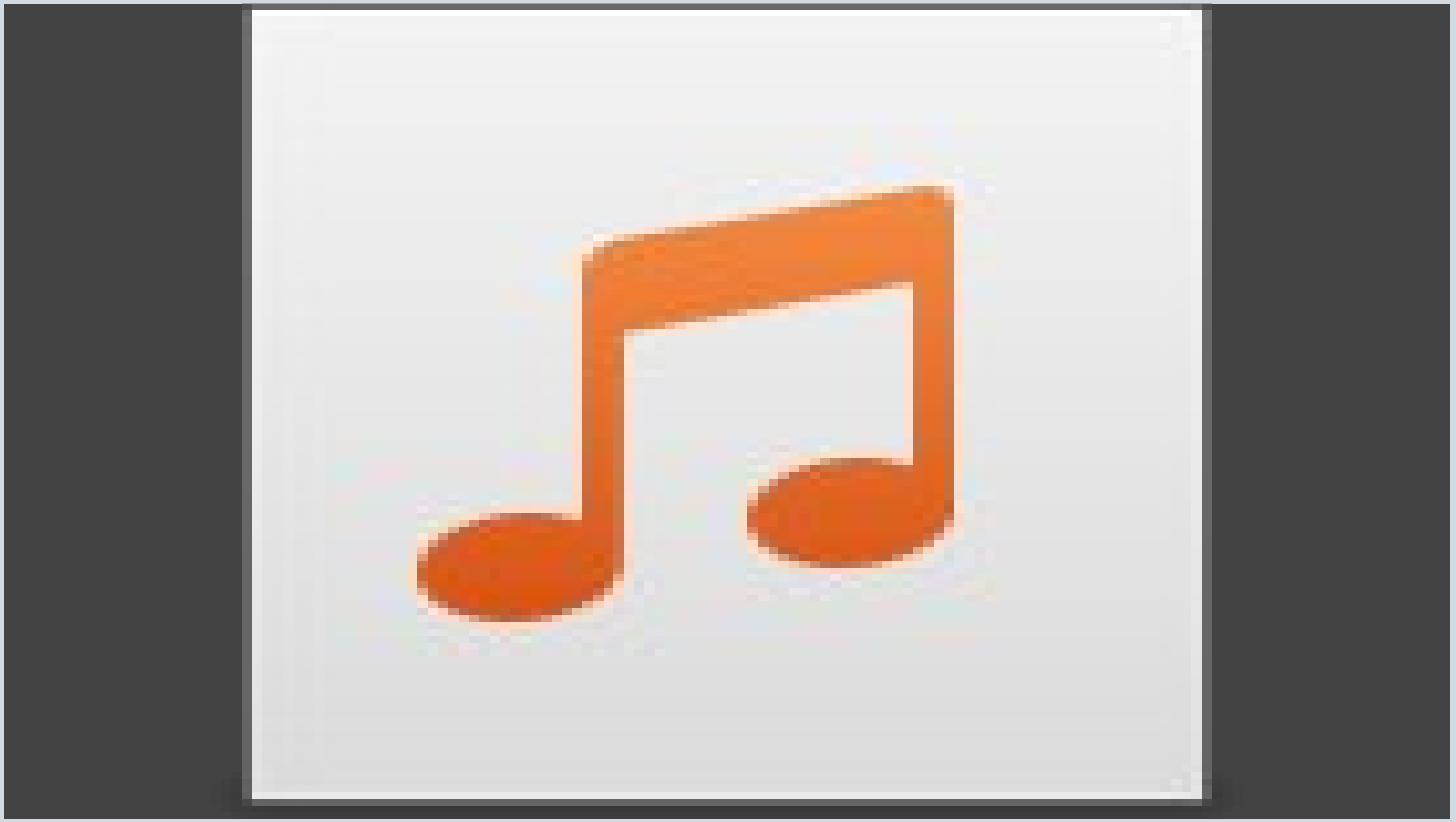
ISS

Nessus®

Video uso de Nessus



Practica Escaneo de vulnerabilidades con la herramienta Nessus y Kali Linux



Como instalar Nessus para Windows 10.