

Capítulo 6. Amenazas a la Seguridad Informática

PATRICIA MEDINA MGP.

Clasificación de los intrusos en las redes

Hackers

- ▶ Son intrusos que se dedican a estas tareas como pasatiempo y como reto técnico: entran en los sistemas informáticos para demostrar y poner a prueba su inteligencia y conocimientos de los entresijos de internet, pero no pretenden provocar daños en estos sistemas.
- ▶ El perfil típico es el de una persona joven , con amplios conocimientos de informática y de internet son expertos en (lenguajes de programación, arquitectura de ordenadores, servicios y protocolos de comunicaciones, sistemas operativos)



Crackers

- Son individuos con interés en atacar un sistema informático para obtener beneficios de forma ilegal o simplemente para provocar algún daño a la organización propietaria del sistema, motivados por intereses económicos, políticos, religiosos.



Sniffers

- ▶ Son individuos que se dedican a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como internet



Phreakers

- ▶ Son intrusos especializados en sabotear las redes telefónicas para poder realizar llamadas gratuitas.
- ▶ Los Phreakers desarrollaron las famosas “Cajas azules” que podían emitir distintos tonos en las frecuencias utilizadas por las operadoras para la señalización interna de sus redes, cuando de estas todavía eran analógicas.



Spammers

- ▶ Son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.
- ▶ Además, muchos de estos mensajes de correo no solicitados pueden contener código dañino (virus informáticos) o forman parte de intentos de estafa realizados a través de internet.



Piratas informáticos

- ▶ Los piratas informáticos son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.



Creadores de virus y programas dañinos

- ▶ Se trata de expertos informáticos que pretenden demostrar sus conocimientos construyendo virus y otros programas dañinos , que distribuyen hoy en día a través de internet para conseguir una propagación exponencial y alcanzar así una mayor notoriedad.
- ▶ En estos últimos años han refinado sus técnicas para desarrollar virus con una clara actividad delictiva , ya que los utilizan para obtener datos sensibles de sus victimas.



Lamers (Script-kiddies, Click – kiddies)

- ▶ Son aquellas personas que han obtenido determinados programas o herramientas para realizar ataques informáticos y que los utilizan sin tener conocimientos técnicos de como funcionan.



Amenazas del personal interno

- ▶ También debemos tener en cuenta el papel desempeñado por algunos empleados en muchos de los ataques e incidentes de seguridad informática , ya sea de forma voluntaria o involuntaria. Así, podríamos considerar el papel de los empleados que actúan como fisgones en la red informática de su organización, los usuarios incautos o despistados , o los empleados descontentos o desleales que pretenden causar algún daño a la organización.



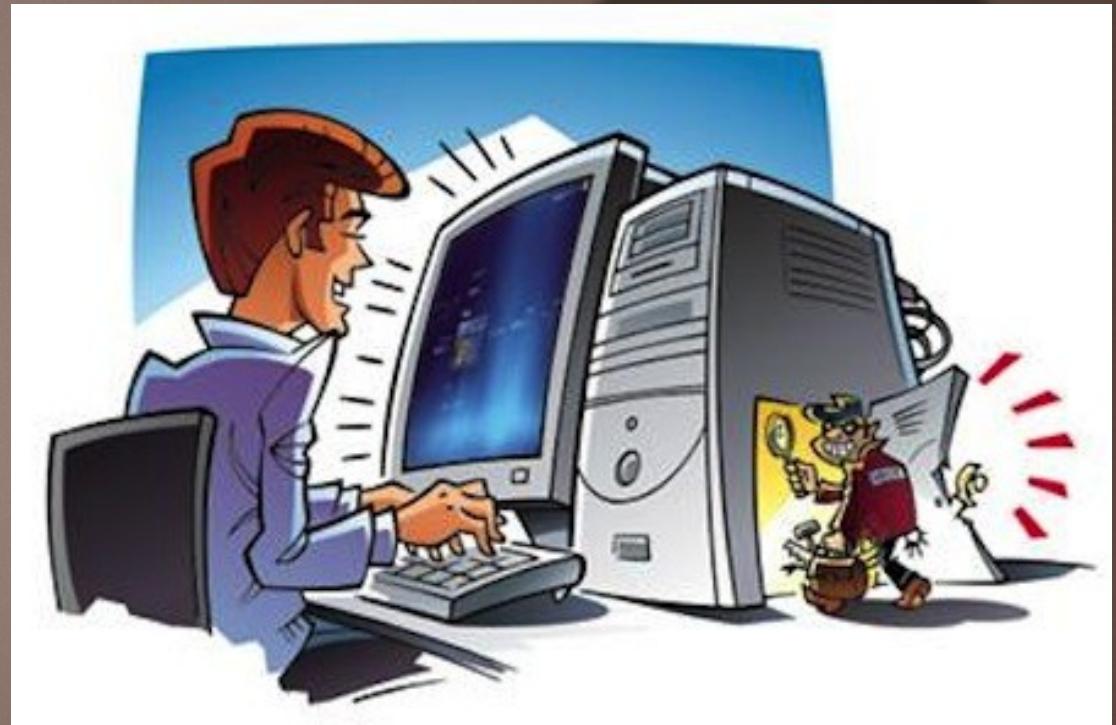
Ex-Empleados

- ▶ Los ex empleados pueden actuar contra su antigua empresa u organización por despecho o venganza , accediendo en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización.
- ▶ También pueden provocar la activación de “bombas lógicas” para causar determinados daños en el sistema informático como venganza tras un despido.



Intrusos remunerados

- ▶ Los intrusos remunerados son expertos informáticos contratados por un tercero para la sustracción de información confidencial, llevar a cabo sabotajes informáticos contra una determinada organización



Algunos hackers, crackers y phreakers

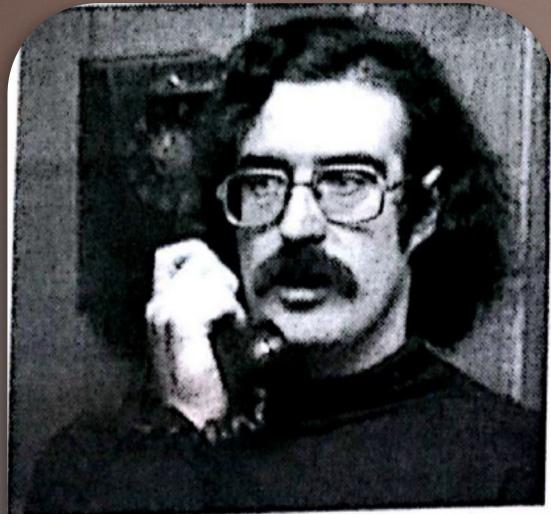


Figura 6.1. John Draper

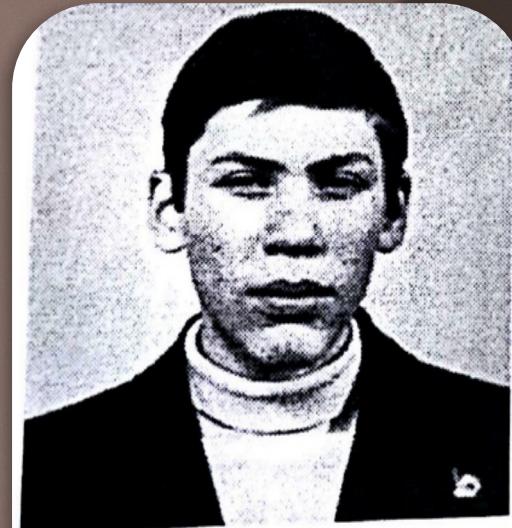


Figura 6.2. Vladimir Levin

Algunos hackers, crackers y phreakers

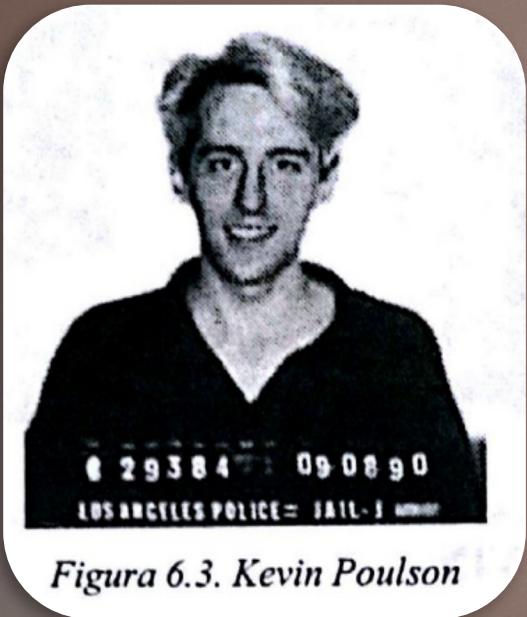


Figura 6.3. Kevin Poulsen



Figura 6.4. Kevin Mitnick

Motivaciones de los atacantes

Consideraciones económicas

- Llevar a cabo operaciones fraudulentas, robo de información confidencial que posteriormente es vendida a terceros, extorciones.

Diversión

- Algunos usuarios de internet realizan estos ataques como una forma de pasar el rato delante de su ordenador

Ideología

- Ataques realizados contra determinadas organizaciones , empresas y websites gubernamentales con un contenido claramente político.

Autorrealización

Búsqueda de reconocimiento social

- Y de cierto estatus dentro de una comunidad de usuarios

Fases de un ataque informático

Descubrimiento y exploración del sistema informático

Búsqueda de vulnerabilidades en el sistema

Explotación de las vulnerabilidades detectadas

- Se suelen utilizar herramientas específicamente construidas para tal fin conocidas como exploits

Corrupción o compromiso del sistema

- Modificación de programas y ficheros del sistema para dejar instaladas determinadas puertas traseras o troyanos

Eliminación de las pruebas que puedan revelar el ataque y el compromiso del sistema

- Eliminación o modificación de los registros de actividad del equipo, modificación de los programas que se encargan de monitorizar la actividad del sistema.

Triangulo de la intrusión

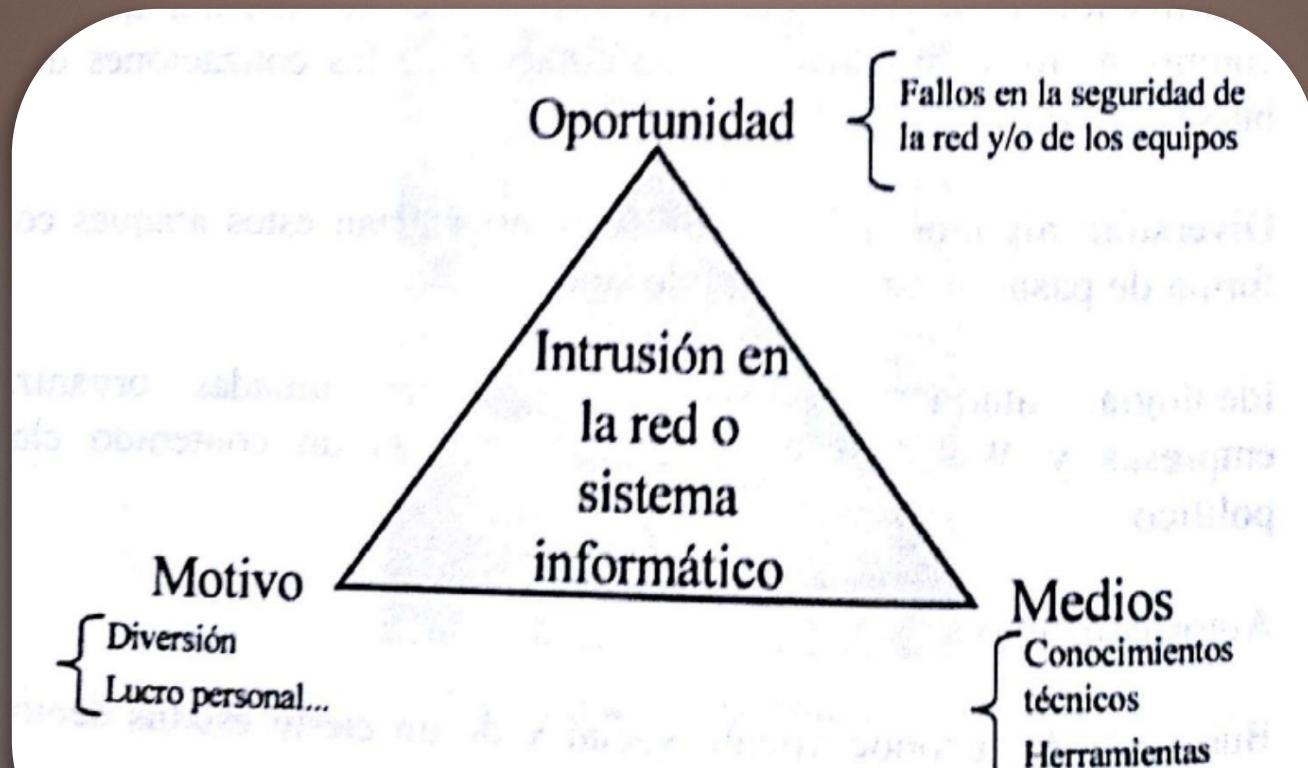


Figura 6.5. El "Triángulo de la Intrusión"

Medios y herramientas en la actualidad para llevar a cabo sus ataques

Escáneres de puertos

- Que permiten detectar los servicios instalados en un determinado sistema informático

Sniffers

- Dispositivos que capturan los paquetes de datos que circulan por una red

Exploits

- Herramientas que buscan y explotan vulnerabilidades conocidas

Backdoors Kits

- Programas que permiten abrir y explotar “puertas traseras” en los sistemas

Rootkits

- Programas utilizados por los atacantes para ocultar “puertas traseras” en los propios ficheros ejecutables y servicios del sistema.

Medios y herramientas en la actualidad para llevar a cabo sus ataques

Auto-rooters

- Herramientas capaces de automatizar totalmente un ataque

Password-crackers

- Aplicaciones que permiten averiguar las contraseñas de los usuarios del sistema comprometido

Generadores de virus y otros programas malignos

Herramientas que facilitan la ocultación y la suplantación de direcciones IP

- Dificultando de este modo la identificación del atacante

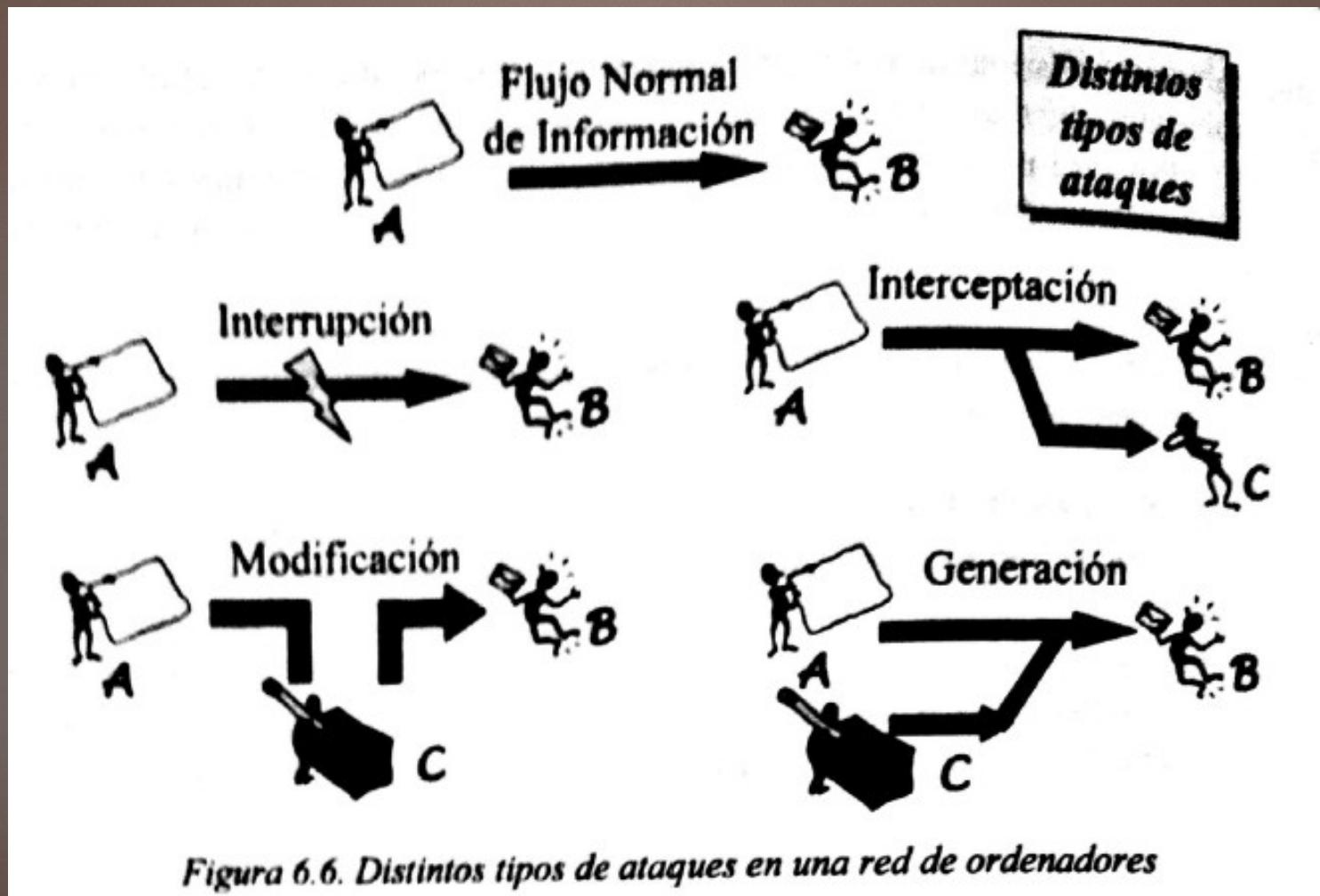
Herramientas de cifrado y protocolos criptográficos

- Cada vez es mas frecuente que el atacante utilice protocolos criptográficos en sus conexiones con los sistemas y maquinas que ha conseguido comprometer , dificultando de este modo su detección y estudio

ATAQUE ACTIVOS: QUE PRODUCEN CAMBIOS EN LA INFORMACIÓN Y EN LA SITUACIÓN DE LOS RECURSOS DEL SISTEMA .

ATAQUE PASIVOS: SE LIMITAN A REGISTRAR EL USO DE LOS RECURSOS Y ACCEDER A LA INFORMACIÓN GUARDADA O TRANSMITIDA POR EL SISTEMA.

Tipos de ataques contra redes y sistemas informáticos



1. Actividades de reconocimiento de sistemas

- ▶ Persiguen obtener información previa sobre las organizaciones y sus redes y sistemas informáticos, realizando para ello un escaneo de puertos para determinar que servicios se encuentran activos o bien un reconocimiento de versiones de sistemas operativos y aplicaciones



Huellas Identificativas

- ▶ Para la identificación de versiones de sistemas operativos y aplicaciones instaladas es necesario obtener lo que se conoce como huellas identificativas del sistema, que son cadenas de texto que identifican el tipo de servicio y su versión y que se incluyen en las respuestas a las peticiones realizadas por los equipos clientes del servicio en cuestión.
- ▶ **Fingerprinting:**
- ▶ Es el conjunto de técnicas y habilidades que permiten extraer toda la información posible sobre un sistema, Los atacantes utilizaran esta información para tratar de explorar las vulnerabilidades potenciales del sistema en cuestión.

Técnicas de escaneo

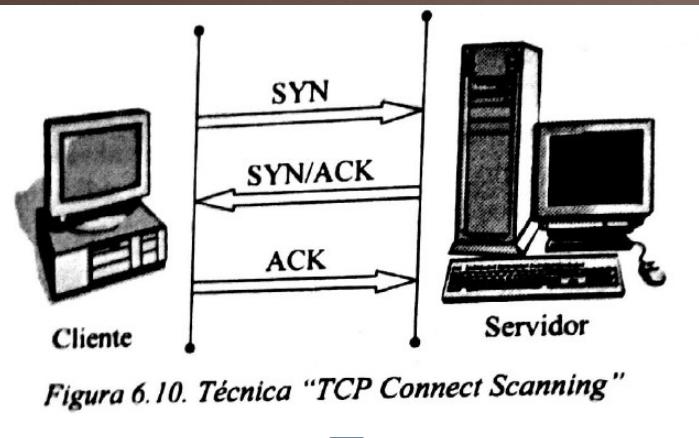


Figura 6.10. Técnica "TCP Connect Scanning"

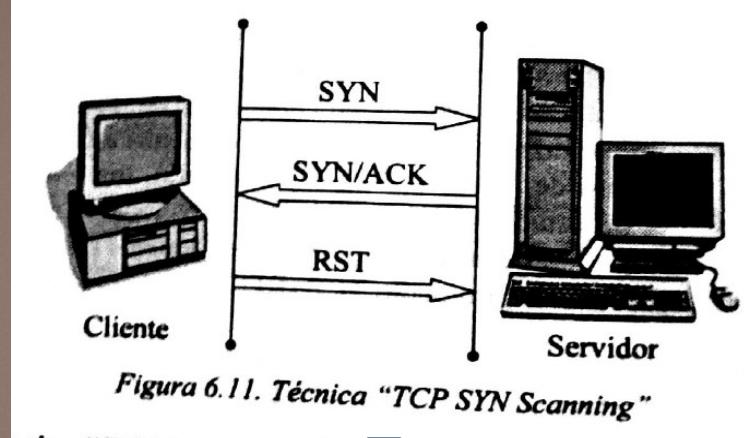


Figura 6.11. Técnica "TCP SYN Scanning"

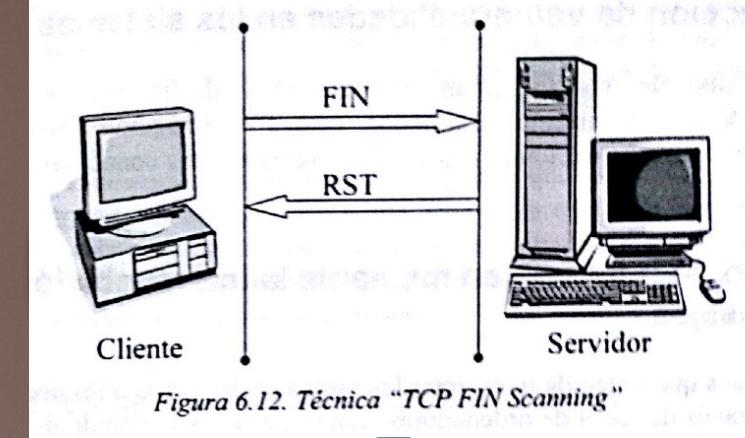


Figura 6.12. Técnica "TCP FIN Scanning"

Es la mas sencilla , ya que consiste en el envío de un paquete de intento de conexión al puerto del servicio que se pretende investigar, para comprobar si el sistema responde aceptando la conexión o denegándola.

Se intenta abrir la conexión con un determinado puerto para a continuación, en cuanto se confirma que el puerto esta abierto, enviar un paquete RST que solicita terminar la conexión. Esta técnica de escaneo no es registrada por algunos servidores.

(Escaneo oculto de puertos) ha sido propuesta como una técnica de escaneo que trata de evitar ser registrada por los cortafuegos y servidores de una organización.

Otras técnicas de escaneo

TCP Null Scanning

- En esta técnica se envía un paquete TCP con todos los flags a cero en su cabecera

TCP ACK Scanning

- Técnica que permite determinar si un cortafuegos actúa simplemente como filtro de paquetes o mantiene el estado de las sesiones.

TCP Fragmentation Scanning

- Técnica de escaneo que recurre a la fragmentación de paquetes TCP

TCP Window Scanning

- Permite reconocer determinados puertos abiertos a través del tamaño de ventana de los paquetes TCP

TPC RPC Scanning

- En los sistemas Unix esta técnica permite obtener información sobre puertos abiertos en los que se ejecutan servicios de llamada a procedimientos remotos RPC

UDP ICMP Port Unreachable Scanning

- Técnica que emplea paquetes UDP para tratar de localizar algunos puertos abiertos

2. Detección de vulnerabilidades en los sistemas

- ▶ Este tipo de ataques tratan de detectar y documentación las posibles vulnerabilidades de un sistema informático, para a continuación desarrollar alguna herramienta que permita explotarlas (herramientas conocidas popularmente como “exploits”)



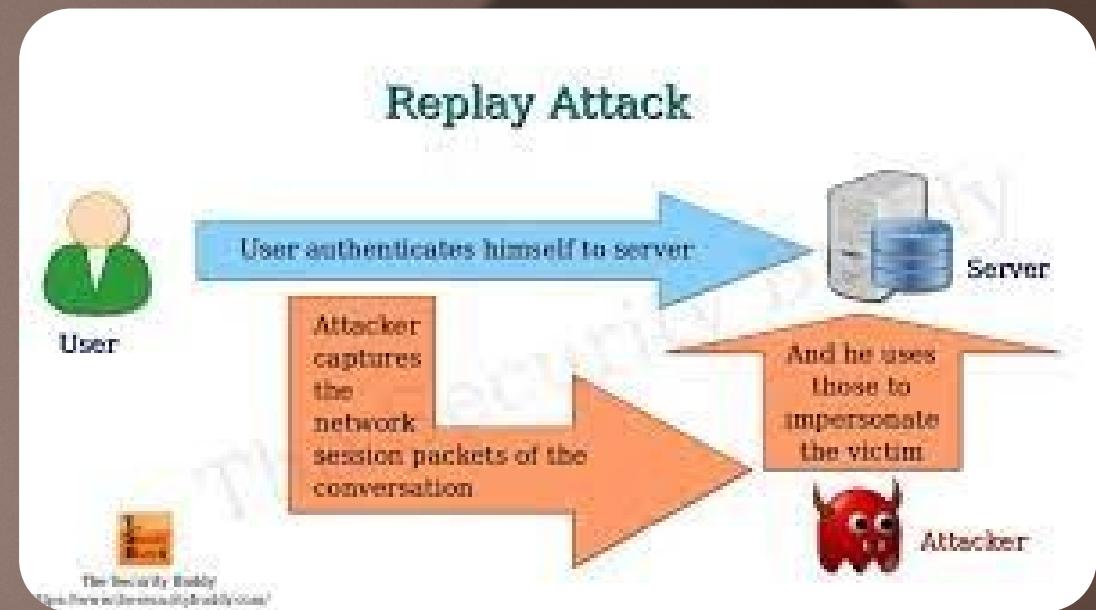
3. Robo de información mediante la interceptación de mensajes

- ▶ Ataques que tratan de interceptar los mensajes de correo o los documentos que se envían a través de redes de ordenadores como internet, vulnerando de este modo la confidencialidad del sistema informático y la privacidad de sus usuarios.



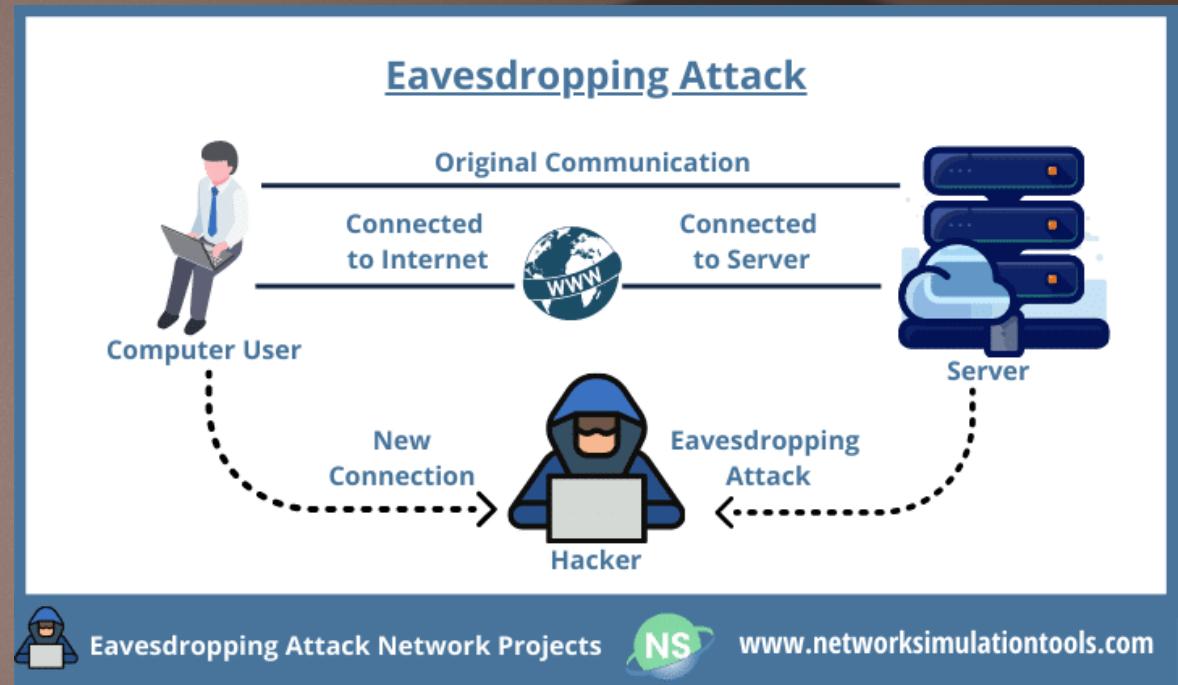
4. Modificación del contenido y secuencia de los mensajes transmitidos

- ▶ En estos ataques los intrusos tratan de reenviar mensajes y documentos que ya habían sido previamente transmitidos en el sistema informático, tras haberlos modificado de forma maliciosa (por ejemplo, para generar una nueva transferencia bancaria contra la cuenta de la víctima del ataque) también se conocen como ataques de repetición.



5. Análisis del tráfico

- ▶ Estos ataques persiguen observar los datos y el tipo de tráfico transmitido a través de redes informáticas, utilizando para ello herramientas como los “sniffers”. Así se conoce como “eavesdropping” a la interceptación del tráfico que circula por una red de forma pasiva, sin modificar su contenido. Una organización podría protegerse frente a los “sniffers” recurriendo a la utilización de redes conmutadas y de redes locales virtuales (VLAN)



6. Ataques de suplantación de la identidad

IP SPOOFING

- Mediante la cual un atacante consigue modificar la cabecera de los paquetes enviados a un determinado sistema informático para simular que proceden de un equipo distinto al que verdaderamente los ha originado.

DNS SPOOFING

- Pretenden provocar un direccionamiento erróneo en los equipos afectados, debido a una traducción errónea de los nombres de dominio a direcciones IP, facilitando la redirección de los usuarios de los sistemas afectados hacia páginas web falsas

Cambios en el registro de nombres de dominio de internic

- Utiliza un sistema de autenticación de usuarios registrados con un bajo nivel de seguridad. Este proceso de autenticación es necesario para poder solicitar cambios ante InterNIC o ante alguna de las empresas registradoras de nombres de dominio.

SMTP SPOOFING

- Para tratar de engañar al destinatario o causar un daño en la reputación del supuesto remitente es otra técnica frecuente de ataque basado en la suplantación de la identidad de un usuario.

Captura de cuentas de usuario y contraseñas

- También es posible suplantar la identidad de los usuarios mediante herramientas que permitan capturar sus contraseñas, como los programas de software espía o los dispositivos hardware especializados que permitan registrar todas las pulsaciones en el teclado de un ordenador.

7. Modificaciones del trafico y de las tablas de enrutamiento

- ▶ Los ataques de modificación del trafico y de las tablas de enrutamiento persiguen desviar los paquetes de datos de su ruta original a través de internet, para conseguir, por ejemplo, que atraviesen otras redes o equipos intermedios antes de llegar a su destino legitimo, para facilitar de este modo las actividades de interceptación de datos.
- ▶ La utilización del encaminamiento fuente en los paquetes IP permite que un atacante pueda especificar una determinada ruta prefijada, que podría ser empleada como ruta de retorno, saltándose todas las reglas de enrutamiento definidas en la red.

8. Conexión no autorizada a equipos y servidores

- Violación de sistemas de control de acceso
- Explotación de agujeros de seguridad “Exploits”
- Utilización de “puertas traseras” (Backdoors)
- Utilización de “rootkits” programas similares a los troyanos.
- “Wardialing” conexión a un sistema informático de forma remota a través de un modem

9. Consecuencias de las conexiones no autorizadas a los sistemas informáticos

- ▶ Acceso a información confidencial guardada en un servidor. Los atacantes incluso podrían tener acceso a datos y ficheros que habían sido borrados del sistema.
- ▶ Utilización inadecuada de determinados servicios por parte de usuarios no autorizados, suponiendo una violación de los permisos establecidos en el sistema.
- ▶ Transmisión de mensajes mediante un servidor de correo por parte de usuarios ajenos a la organización. Esto podría facilitar el reenvío masivo de mensajes de spam a través de un servidor SMTP configurado de forma inadecuada.
- ▶ Utilización de la capacidad de procesamiento de los equipos para otros fines, como, por ejemplo, para tratar de romper las claves criptográficas de otros sistemas.

9. Consecuencias de las conexiones no autorizadas a los sistemas informáticos

- ▶ Creación de nuevas cuentas de usuario con privilegios administrativos, que faciliten posteriores accesos al sistema comprometido.
- ▶ Consumo del ancho de banda de la red de la organización para otros fines.
- ▶ Almacenamiento de contenidos ilegales en los equipos: muchos atacantes aprovechan los equipos comprometidos de una organización para guardar y distribuir copias piratas de software, canciones o videos, pornografía infantil..
- ▶ Modificación o destrucción de archivos y documentos guardados en un servidor.
- ▶ Website vandalism: modificación del contenido y de la apariencia de unas determinadas páginas web pertenecientes a la organización.

10. Introducción en el sistema de “malware” código malicioso.

1. Virus informáticos, troyanos y gusanos

2. Ataques de “Cross-site Scripting” XSS

- Obtención de cookies e identificadores de usuarios, que permiten capturar sesiones y suplantar la identidad de los afectados.
- Modificación de contenidos para engañar al visitante víctima del ataque. (robar datos sensibles, como contraseñas, datos bancarios)

3. Ataques de inyección de código SQL

11. Ataques contra los sistemas criptográficos

Los “Ataques de fuerza bruta”

- Tratan de explorar todo el espacio posible de claves para romper un sistema criptográfico.

Los “ataques de diccionario”

- Trabajan con una lista de posibles contraseñas. (códigos postales, fechas del calendario etc..)

Los ataques contra el diseño del algoritmo

Los ataques contra los dispositivos hardware

- o las aplicaciones software que lo implementan

Las distintas técnicas de criptoanálisis

- Criptoanálisis lineal, diferencial, técnicas de análisis estadístico de frecuencias

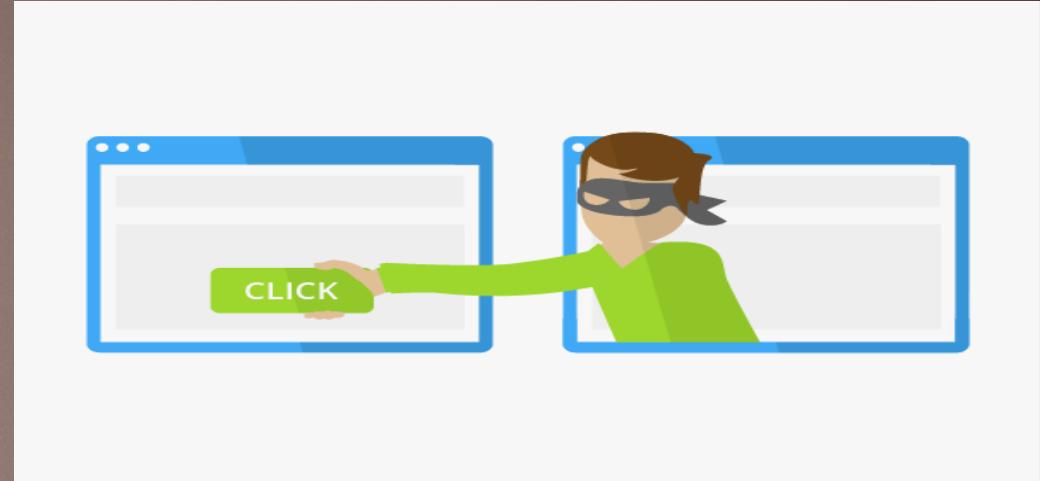
12. Fraudes, engaños y extorsiones

► El “pharming” es una variante del “phishing” en la que los atacantes utilizan un virus que conecta a las víctimas desde su ordenador a páginas falsas en lugar de a las legítimas correspondientes a sus propias entidades financieras, para sustraer sus datos (números de cuenta y claves de acceso). El “pharming” y el “phishing” también pueden ser empleados para robar y utilizar de forma fraudulenta números de tarjeta de crédito.



12. Fraudes, engaños y extorsiones

- ▶ El “clickjacking” es una estrategia que pretende engañar al usuario para que este haga clic en un enlace o botón que en apariencia es inofensivo, cuando en realidad lo hace sobre otro enlace controlado por terceros.
- ▶ “Ransom-ware” software malicioso cuyo fin es el lucro de su creador por medio de rescates.



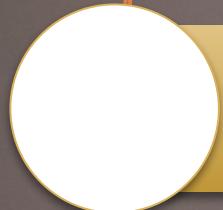
13. Denegación del servicio (Ataques DoS-Denial of Service)



Ejecutar algunas actividades que produzcan un elevado consumo de los recursos de las maquinas afectadas. (procesador,memoria y disco duro provocando una caída en su rendimiento.



Provocar el colapso de redes de ordenadores mediante la generación de grandes cantidades de trafico generalmente desde múltiples equipos.

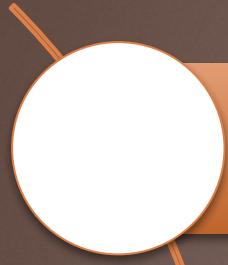


Trasmisión de paquetes de datos malformados o que incumplan las reglas de un protocolo, para provocar la caída de un equipo que no se encuentre preparado para recibir este tipo de trafico malintencionado.



Sabotajes mediante routers “maliciosos”, que se encarguen de proporcionar información falsa sobre tablas de enrutamiento que impidan el acceso a ciertas maquinas de la red.

13. Denegación del servicio (Ataques DoS- Denial of Service)



Activación de programas “bacteria”, cuyo objetivo es replicarse dentro de un sistema informático, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado



Envío masivo de miles de mensajes de correo electrónico provocando la sobrecarga del servidor de correo y de las redes afectadas.



“Ataque reflector”, que persigue generar un intercambio ininterrumpido de tráfico entre dos o más equipos para disminuir su rendimiento o incluso conseguir su completo bloqueo dentro de una red informática.



Incumplimiento de las reglas de un protocolo. Suelen utilizar(UDP, ICMP, TCP) sin llegar a establecer una conexión completa con el equipo atacado.

El incumplimiento de las reglas de un protocolo, tipos de ataques:

“El ping de la muerte”

“Land Attack”

**“Supernuke” o
“Winnuke”**

“Teardrop”

“Syn Flood”

Tipos de ataques de Denegación de servicio (DoS)

“Connection Flood”

“Net Flood”

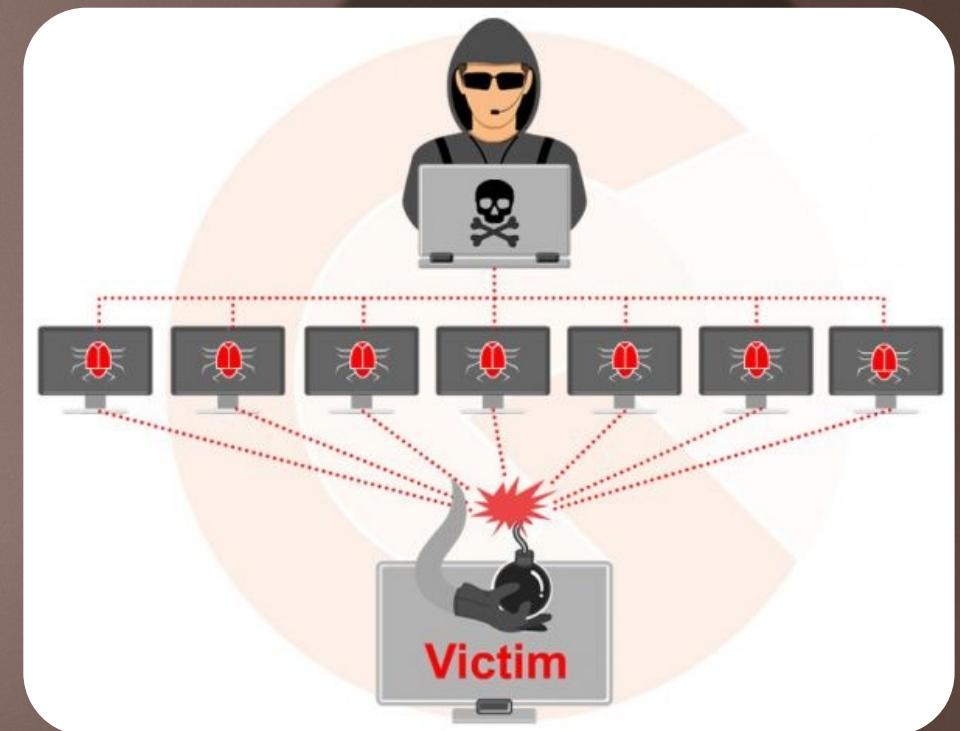
“Smurf”

“Bomba UDP”

“Snork UDP”

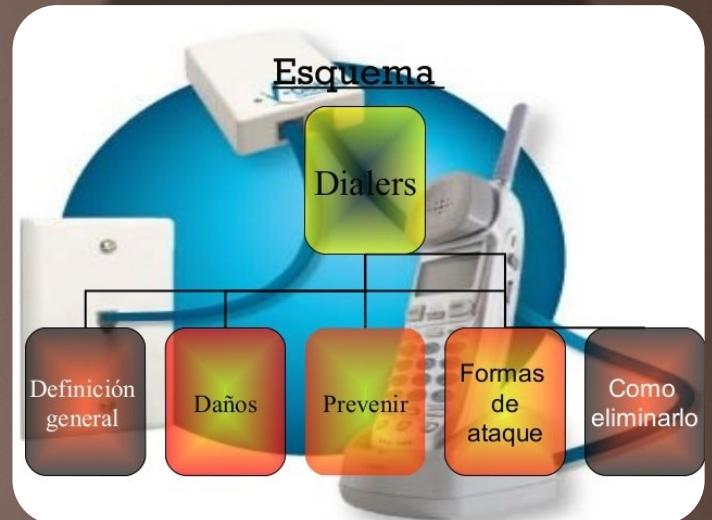
14. Ataques de Denegación de servicio Distribuidos (DDoS)

- ▶ Los ataques de denegación de servicio distribuidos (DDoS) se llevan a cabo mediante equipos “zombis”. Los equipos “zombis” son equipos infectados por virus o troyanos, sin que sus propietarios lo hayan advertido, que abren puertas traseras y facilitan su control remoto por parte de usuarios remotos.
- ▶ Estos usuarios maliciosos suelen organizar ataques coordinados en los que pueden intervenir centenares o incluso miles de estos equipos, sin que sus propietarios y usuarios legítimos lleguen a ser conscientes del problema, para tratar de colapsar las redes y los servidores objeto del ataque.



15. Marcadores telefónicos (“dialers”)

- ▶ Los “dialers” o “marcadores telefónicos” son pequeños programas que se encargan de marcar números telefónicos que dan acceso a algún tipo de servicio, con una tarifa telefónica muy superior a la normal.
- ▶ Estos virus son capaces de crear un nuevo acceso telefónico a redes en el ordenador infectado que se configura como el predeterminado para la conexión a Internet, o bien pueden modificar el acceso telefónico a redes que el usuario utiliza habitualmente para sus conexiones a Internet, cada vez que sea ejecutado, el numero marcado no sea el correspondiente al proveedor de servicios de internet del usuario, sino un numero de tarifa especial, ocasionando un grave problema económico a la víctima, quien detectara la situación anormal al recibir sus próximas facturas del servicio telefónico.



PARA COMBATIR DE FORMA MAS EFICAZ LAS DISTINTAS AMENAZAS QUE AFECTAN A LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS, SE HAN CREADO VARIOS *ORGANISMOS ESPECIALIZADOS* CUYA MISIÓN ES ALERTAR A LOS GOBIERNOS, EMPRESAS Y CIUDADANOS EN GENERAL PARA PODER CONTENER Y MINIMIZAR LOS DAÑOS OCASIONADOS POR LOS ATAQUES INFORMÁTICOS.

1. CERT/CC (Computer Emergency Response Team/Coordination Center)

- ▶ El CERT, el equipo de respuesta a emergencias informáticas, es el primer y mas conocido centro de respuesta, creado en diciembre de 1988 por la agencia DARPA de Estados Unidos para gestionar los incidentes de seguridad relacionados con Internet.
- ▶ Se encuentra en el instituto de ingeniería del software de la Universidad Carnegie Mellon. La dirección en internet es <http://www.cert.org>



2. CERT INTECO



- ▶ El Centro de respuesta a incidentes de seguridad fue creado en 2006 en España dentro del Instituto Nacional de tecnologías de la información (INTECO) su dirección en internet es <http://cert.inteco.es/>

3. Agencia Europea de seguridad de las redes y de la información

- ▶ Agencia Europea creada por decisión del consejo y del Parlamento (EC 460/2004) con la finalidad de alcanzar un alto nivel de seguridad en las redes y en el tratamiento de la información dentro de la Unión Europea. Esta agencia comenzó oficialmente sus actividades en septiembre de 2005, tras fijar su sede institucional en la Isla de Creta.
- ▶ Su dirección en internet es <http://www.enisa.europa.eu/>



4. CSRC (Computer Security Resource Center)

- ▶ El CSRC, “Centro de recursos de seguridad informática”, es un centro dependiente del NIST. Su dirección en internet es <http://csrc.nist.gov/>



5. US-CERT

- ▶ El US-CERT es un centro de respuesta a incidentes de seguridad informática que depende del National Cyber Security Division (NCSD) en el Departamento de Seguridad Interior



6. FIRST (Forum of Incident Response and Security Teams)

- ▶ Foro constituido en 1990 con el objetivo de facilitar el intercambio de información sobre incidentes de seguridad entre los distintos miembros que lo integran (Centros de respuesta a incidentes de distintos países y organizaciones) así como la detección, prevención y recuperación de estos incidentes de seguridad.
- ▶ Su dirección en internet es <http://www.first.org/>



7. Otros centros de seguridad y respuesta a incidentes

- ▶ Otros países también han puesto en marcha sus respectivos centros de respuesta a incidentes de seguridad como el AusCERT (<http://www.auscert.org.au>) de Australia o el DFN-CERT (<http://www.cert.dfn.de>) de Alemania.
- ▶ Es España también podemos destacar los servicios del IRIS-CERT, centro de respuesta a incidentes de seguridad de la red IRIS, que da soporte a los centros de investigación y Universidades del país a través de la dirección de Internet <http://www.rediris.es/cert/>
- ▶ El centro de alerta temprana sobre virus y seguridad informática fue creado en julio de 2001 por el ministerio de ciencia y Tecnología español para ofrecer información, alertas y distintos recursos sobre seguridad informática a ciudadanos y empresas, <http://www.alerta-antivirus.es>
- ▶ En la actualidad se encuentra integrado dentro del INTECO, en la dirección <http://www.inteco.es/Seguridad>

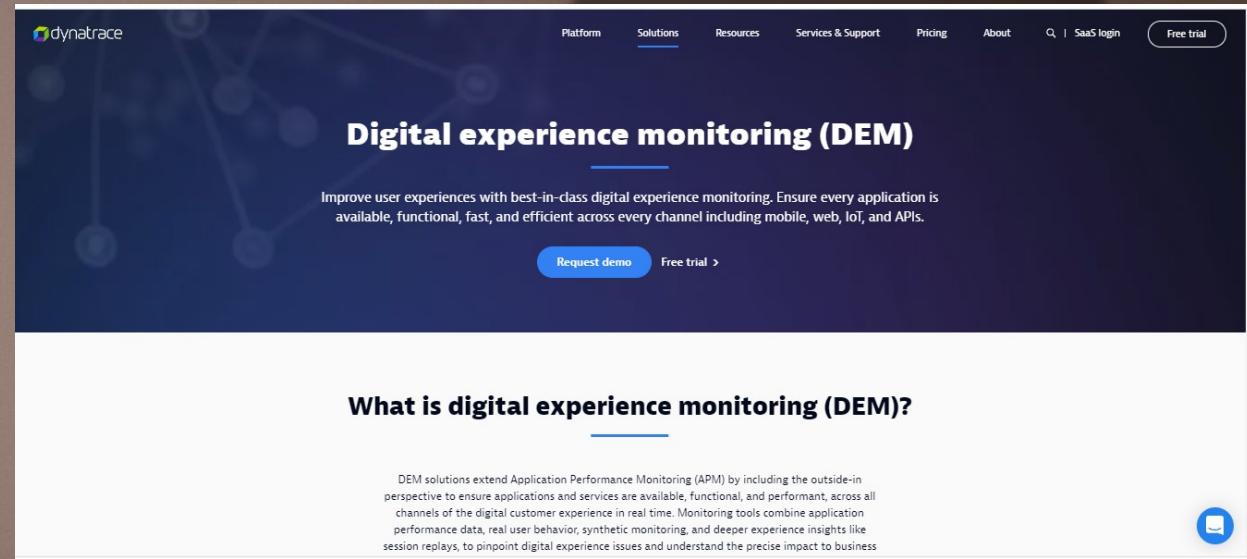
8. Bases de datos de ataques e incidentes de seguridad

- ▶ También existen distintos organismos que se encargan de capturar y agrupar los registros de incidencias (logs) y ataques sufridos por distintas organizaciones en una base de datos Dshield sistema de detección de intrusiones distribuido es una de las bases de datos sobre incidentes de seguridad informática mas conocida. <http://www.dshield.org/>

The screenshot shows the SANS Internet Storm Center website. The top navigation bar includes a 'Threat Level: GREEN', a 'Handler on Duty: Xavier Mertens', and links for 'Log In or Sign Up for Free!' and 'Integrate our data into your projects'. The main content area features a sidebar with links to 'Contact Us', 'Diary', 'Podcasts', 'Jobs', 'Tools', 'Data', and 'Forums', along with 'Questions?' and 'Feedback?' links. The main content area displays a diary entry titled 'Apache is Actively Scan for CVE-2021-41773 & CVE-2021-42013' published on 2021-10-16. The entry discusses an Apache 2.4.49 directory traversal vulnerability and includes links to a contact form, reporting bugs, and Slack. It also mentions a honeypot capturing various types of scans. The sidebar on the right shows a list of recent diary entries.

8. Bases de datos de ataques e incidentes de seguridad

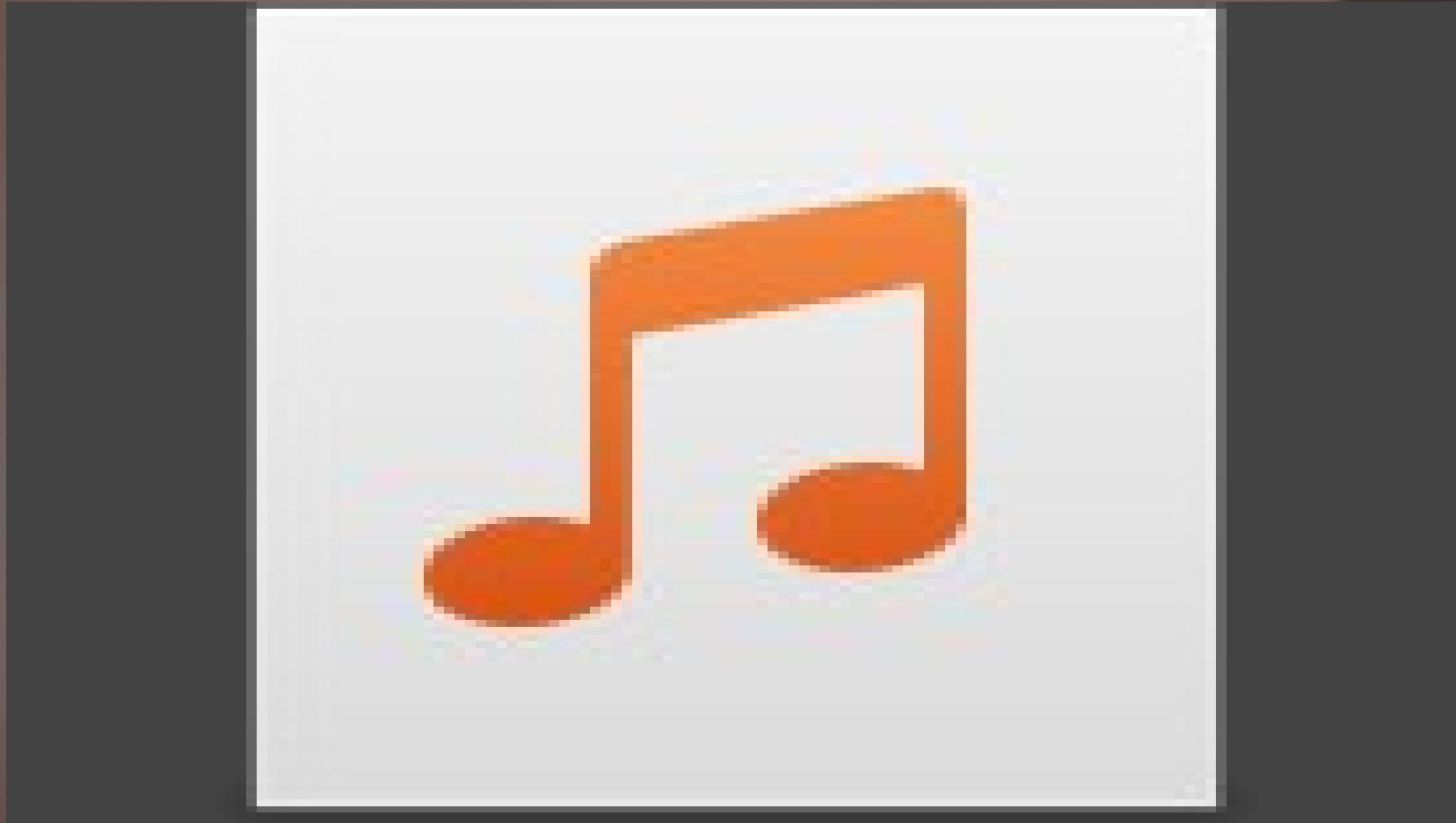
- ▶ Otra completa base de datos con referencias sobre incidentes de seguridad se encuentra disponible en Security Focus (<http://www.securityfocus.com/>)
- ▶ Asimismo podemos encontrar algunos servicios que se encargan de evaluar el estado del tráfico en internet, como Internet Health Monitoring (www.internetpulse.net) que contribuye a la detección y control de los ataques de Denegación de servicio (DoS)



Videos de Respuesta a incidentes



Videos de Respuesta a incidentes





Gracias