Introducción a las vulnerabilidades

PID_00255333

Guillermo Navarro Arribas

Universitat Oberta de Catalunya

Índice

Introducción

Hoy en día nadie duda de la importancia que tiene la seguridad informática en nuestras vidas. Vivimos, cada vez más, rodeados de dispositivos informáticos que nos facilitan el día a día. Reservar entradas o realizar la compra por Internet, un coche con un alto grado de automatización y capacidad de comunicación, un teléfono móvil en el que hablar parece una función secundaria, la digitalización de prácticamente todos los datos relacionados con nosotros (desde la Administración pública, las empresas, o nuestros datos personales, como agenda, correo electrónico, documentos, etc.), son cosas con las que nos hemos acostumbrado a vivir. De la misma manera, también hemos empezado a percibir la importancia de la seguridad informática. Hoy en día son frecuentes las noticias en la prensa no especializada sobre incidentes de seguridad en el mundo digital, como robo de tarjetas de crédito, suplantación de identidad, robo de datos confidenciales, o incluso ataques dirigidos sobre infraestructuras críticas.

Esta asignatura introduce la problemática de la seguridad informática y lo hace describiendo y estudiando una parte concreta de ella: las vulnerabilidades que presentan los sistemas de información. La existencia de una vulnerabilidad en un sistema de información es lo que posibilita que dicho sistema pueda ser atacado. Por ello, al hacer un repaso de las vulnerabilidades estamos dando una introducción al problema de la seguridad informática por su base. Dicho de otra manera, veremos el porqué de la seguridad informática.

Este módulo introduce los conceptos básicos sobre los que se va a desarrollar la asignatura. Veremos qué es una vulnerabilidad, por qué son importantes, cómo se clasifican y cómo se gestionan.

Objetivos

Los objetivos que el estudiante debe haber conseguido después de estudiar los contenidos de este módulo son los siguientes:

1. Entender el concepto de vulnerabilidad de seguridad y su contexto.
2. Conocer cómo se identifican y catalogan las vulnerabilidades.
3. Saber cómo se gestionan las vulnerabilidades, y la existencia de equipos especializados.

1. Nociones básicas

Una **vulnerabilidad** de seguridad se puede ver como el punto de partida de todo el proceso que implica la seguridad en general. Por ejemplo, un ataque informático sobre un servidor web generalmente parte de una vulnerabilidad en alguno de los sistemas que implementan o dan soporte al servidor: errores en la implementación del mismo servidor o sistema operativo, fallos en el diseño de protocolos de comunicación, errores propiciados por la inexperiencia del personal encargado de utilizar o administrar el servidor, etc. La dificultad de prever estos errores y, por tanto, los posibles ataques que se deriven lleva a la implantación de medidas preventivas y reactivas, como el uso de cortafuegos, sistemas de detección de anomalías o intrusiones, realización de auditorías de seguridad, planes de contingencia, o educación a usuarios y administradores.

Definir lo que es una vulnerabilidad no es sencillo y para ello es necesario dotar de contexto a dicha definición. En este sentido, nos centraremos en vulnerabilidades de seguridad en sistemas de información.

Consideramos los sistemas de información (SI) de manera muy general como cualquier sistema destinado a recoger, almacenar, procesar y/o distribuir conjuntos de información. Aunque generalmente se asocia el concepto de sistema de información al mundo empresarial, adoptamos el sentido más amplio de SI abarcando su uso tanto personal como dentro de una organización. En general, al hablar de SI nos referiremos a un sistema informático, aunque no todos los SI son informáticos. Es importante resaltar que el estudio de la seguridad de los SI y sus vulnerabilidades abarca no solo a los SI propiamente, sino también el estudio de todas las entidades y los fenómenos que puede afectar directa o indirectamente a los SI. Esta es una visión muy amplia de SI que puede comprender entre otros: ordenadores de uso personal, teléfonos móviles, servidores de correo electrónico, servidores web, sistemas de almacenamiento de datos, sistemas de comunicación de información, redes telemáticas, a los usuarios de dichos sistemas, etc.

Ved también

Veremos algún ejemplo de vulnerabilidades de los sistemas de información no informáticos en el módulo "Ingeniería social".

La seguridad en los SI comienza a partir de la existencia de vulnerabilidades relativas a estos sistemas. Una vulnerabilidad no tendría sentido si luego no pudiese ser explotada por un ataque con el objetivo de violar la seguridad del sistema. Es muy común asociar el concepto de vulnerabilidad a *error*, aunque esta equivalencia conviene matizarla adecuadamente. En esta línea, adoptamos la siguiente definición de vulnerabilidad.

Una **vulnerabilidad de seguridad** es un fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema.

A continuación detallamos algunos de los conceptos relacionados.

Lectura complementaria

Las definiciones básicas de este apartado están basadas en:
R. Shirey *Internet Security Glossary*, RFC 2828, IETF. Disponible en línea en: http://www.ietf.org/rfc/rfc2828.txt

Una **política de seguridad** es el conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema con el propósito de proteger sus recursos críticos y sensibles. En otros términos, es la declaración de lo que está permitido y lo que no está permitido hacer.

La política de seguridad es la base de la seguridad de un sistema. En ella se detallan los servicios de seguridad del sistema, se determina quién y/o qué se puede o no hacer con los recursos del sistema, y generalmente se especifica cómo se implementan dichos servicios. La implementación concreta de una política de seguridad se lleva a cabo mediante **mecanismos de seguridad**. La política no tiene por qué ser una declaración formal, a veces se trata de simples directrices sobre la seguridad del sistema en lenguaje informal.

Por lo general, hablamos de incidente de seguridad para referirnos a cualquier hecho que supone una violación de la seguridad del sistema. En el caso de que el incidente sea intencionado, nos referimos a él como ataque.

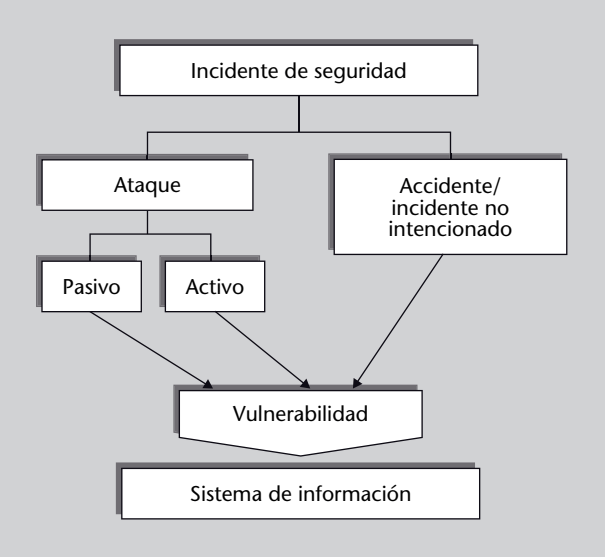
Un **ataque** es una agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema.

Un ataque puede ser activo o pasivo. Un **ataque activo** intenta alterar el sistema, sus recursos u operaciones. Un **ataque pasivo** intenta aprender o utilizar información del sistema pero no afecta al propio sistema, ni a su funcionamiento. En la figura 1 se muestran los conceptos vistos hasta ahora.

Otro aspecto importante que trataremos en este módulo es el de riesgo y amenaza. Toda vulnerabilidad implica una amenaza al sistema y, por tanto, entraña un riesgo.

Una **amenaza** es una violación de la seguridad en potencia, que existe a partir de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún daño en el sistema.

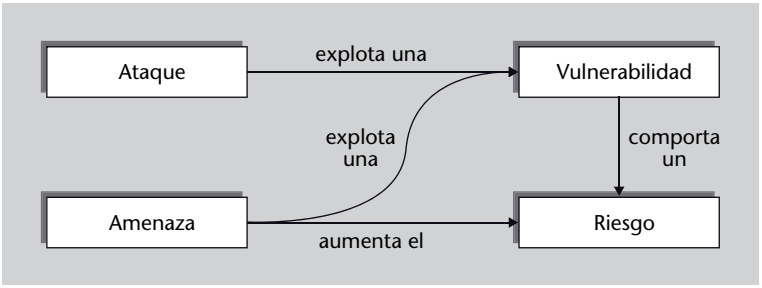
Figura 1. Relación entre conceptos de seguridad



Es importante distinguir entre **ataque** y **amenaza**. Un ataque es una acción intencionada realizada directa o indirectamente por un atacante al que se le atribuye cierta capacidad de acción inteligente. Por el contrario, una amenaza es la posibilidad de que ocurra una violación de la política de seguridad. Esta violación puede ser provocada por un ataque o por incidentes no deliberados causados de manera fortuita, como desastres naturales.

Una parte importante en la seguridad informática es evaluar el riesgo asociado a un servicio o sistema. Este riesgo suele ser directamente proporcional a la existencia de vulnerabilidades y amenazas. Aunque hay que tener en cuenta que no siempre a mayor número de vulnerabilidades mayor es el riesgo asociado a un sistema. El riesgo vendrá determinado también por la criticidad o gravedad de la vulnerabilidad. En la figura 2 se muestran los principales conceptos vistos hasta ahora.

Figura 2. Relación entre conceptos de seguridad

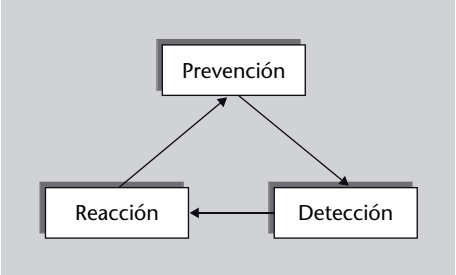


El **riesgo** es una expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad particular con resultados especialmente perjudiciales.

Una vez evaluado el riesgo, considerando las posibles amenazas al sistema, el trabajo de los expertos en seguridad consiste en desarrollar contramedidas

con el objetivo de mitigar dicho riesgo. Es importante tener en cuenta que, dada la actual complejidad de los sistemas informáticos, resulta prácticamente imposible disponer de un sistema libre de vulnerabilidades y amenazas. En esta línea, el proceso de seguridad se suele percibir como un ciclo, donde se aplican medidas de prevención, detección y reacción (podéis ver la figura 3).

Figura 3. Ciclo de la seguridad

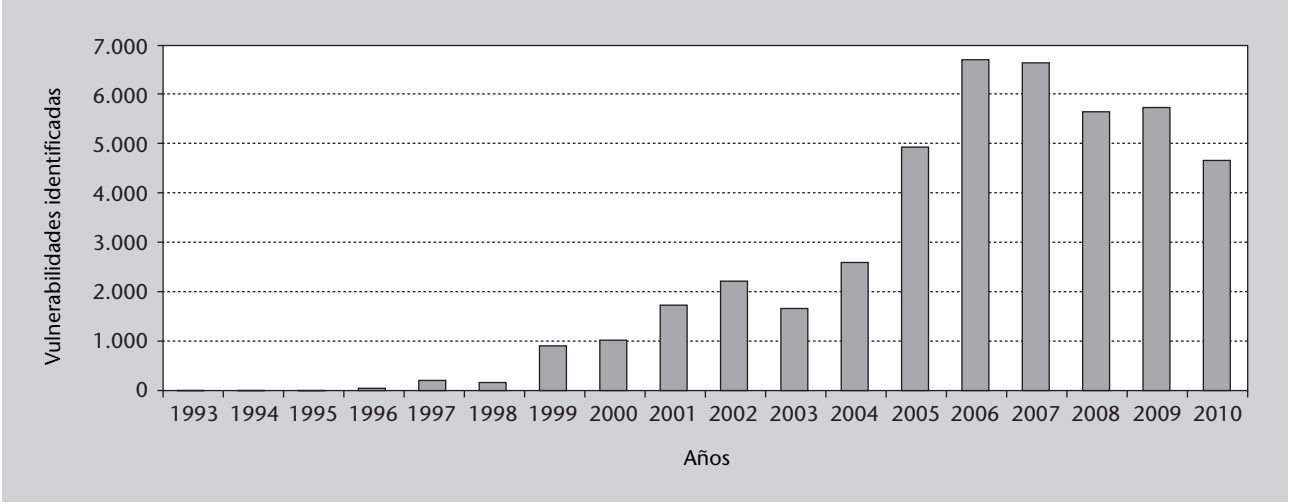


En esta asignatura nos centramos en el origen de la seguridad informática al contemplar la problemática desde el punto de vista de las vulnerabilidades. Muchas veces será necesario ver los posibles ataques que pueden explotar cierta vulnerabilidad para entender dicha vulnerabilidad. En este sentido, nos centramos en procesos de prevención, al intentar prever posibles ataques o amenazas al sistema. Rara vez se detallarán medidas de detección, como la detección de intrusos, o reacción, como respuesta en tiempo real a ataques, puesto que estos mecanismos se analizarán en otras asignaturas.

1.1. Ejemplos de vulnerabilidades

La proliferación de sistemas informáticos y especialmente de Internet ha hecho crecer drásticamente el número de vulnerabilidades. Estimar el número de vulnerabilidades existentes es difícil, pero existen datos de, por ejemplo, el número de vulnerabilidades diferentes catalogadas, como las mostradas en la figura 4. Notad que no se muestra el número de vulnerabilidades, sino el de vulnerabilidades diferentes identificadas. El hecho de que una vulnerabilidad en concreto tenga mayor o menor presencia no se muestra en este gráfico.

Figura 4. Número de vulnerabilidades diferentes por año



Fuente: National Vulnerability Database, http://nvd.nist.gov.

Los siguientes son algunos ejemplos de vulnerabilidades:

- **Sony PSN** (*PlayStation Network*): un ataque en mayo del 2011 a la red de usuarios PSN de Sony acabó con el posible robo de información personal de sus cerca de 70 millones de usuarios, que incluía información de tarjetas de crédito. En dicho ataque se explotó una vulnerabilidad conocida (no se ha revelado a qué sistemas afectan).

- **Stuxnet**: gusano que infecta sistemas industriales y especialmente sistemas SCADA (*Supervisory Control And Data Acquisition*) de Siemens para la configuración y el control de procesos industriales. Fue descubierto en julio del 2010 y una particularidad de este gusano es que sus objetivos parecían ser muy concretos: centros de enriquecimiento de uranio de Irán. El gusano explota un total de 4 vulnerabilidades del sistema operativo Windows de Microsoft (2 de ellas eran conocidas, y 2 eran vulnerabilidades de *zero-day*).

- **Ataque de Mitnick**: en 1994 se produjo uno de los ataques informáticos más publicitados y documentados, mediante el cual un *hacker* llamado Kevin Mitnick consiguió acceder a los ordenadores de Tsutomu Shimomura, situados en la Universidad de California, para robar el código fuente de un teléfono móvil. Mitnick explotó vulnerabilidades en el protocolo TCP de denegación de servicio y de secuestro de sesión.

Lectura complementaria

Podéis encontrar más información sobre el caso Mitnick-Shimomura en los libros:

T. Shimomura; J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It*. Hyperion Books.

J. Littman (1997). *The Fugitive Game: Online with Kevin Mitnick*. Little, Brown and Company publishers.

J. Goodell (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And the Man Who Hunted Him Down*. Dell publishers.

Lectura complementaria

Podéis encontrar más información sobre Stuxnet en:
N. Falliere; L. Murchu; E. Chien (2011). W32.Stuxnet Dossier. Symantec Security Response, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Ved también

El tipo de vulnerabilidades que explota Stuxnet se estudian en el módulo "Vulnerabilidades de bajo nivel y software malicioso".

Ved también

En el módulo "Vulnerabilidades en redes" se estudian el tipo de vulnerabilidades que explotó Kevin Mitnick.

Existen maneras de poder identificar y clasificar vulnerabilidades, que se pueden hacer públicas para que todo el mundo pueda aplicar medidas preventivas. Muchos problemas de seguridad vienen por no tener los sistemas informáticos actualizados con los últimos parches de seguridad que evitan vulnerabilidades conocidas. Aun así, siempre hemos de asumir que existen vulnerabilidades no conocidas y que pueden dar lugar a incidentes de seguridad. Estas vulnerabilidades no conocidas, de las que es muy difícil protegerse, se denominan vulnerabilidades de día-cero o en inglés *zero-day vulnerabilities*.

Ved también

En el apartado 2 de este módulo presentaremos una clasificación de las vulnerabilidades.

Así mismo, también vemos que muchos ataques informáticos explotan más de una vulnerabilidad. Esto es especialmente latente en ataques que realizan varias acciones diferentes. Un ejemplo claro donde se explotan varias vulnerabilidades son las *botnets*.

Ved también

Las *botnets* se estudian en el módulo "Botnets".

2. Gestión de vulnerabilidades

Un proceso muy importante dentro de la seguridad informática hoy en día es la gestión de vulnerabilidades. Dentro de la seguridad preventiva, uno de los puntos clave es encontrar vulnerabilidades en sistemas existentes que puedan suponer una amenaza ante ataques potenciales. A tal efecto se destinan muchos recursos a diferentes niveles, desde los propios fabricantes de hardware y software, hasta entidades gubernamentales o asociaciones altruistas.

Los equipos encargados de la gestión de vulnerabilidades e incidentes de seguridad suelen recibir el nombre de CERT (*Computer Emergency Response Team*) o CSIRT (*Computer Security Incident Response Team*). La principal tarea de estos equipos es la gestión de incidencias de seguridad. En la práctica, sirven como medio para la difusión de vulnerabilidades de seguridad a usuarios (particulares u organizaciones), que suelen ser reportadas por los propios usuarios.

El primer centro de coordinación CERT fue creado en 1988, por DARPA (*Defense Advanced Research Projects Agency*), en el Instituto de Ingeniería del Software (*Software Engineering Institute*, SEI) de la Carnegie Mellon University en Estado Unidos, y actualmente continúa siendo una referencia internacional. La necesidad de crear este centro fue impulsada por el gran impacto que tuvo el gusano Morris. La aparición de Internet hacía posible la rápida distribución de código malicioso, dando lugar a la aparición de virus, gusanos*, etc. Como respuesta a esta problemática se crearon estos equipos CERT, que rápidamente se han extendido por todo el mundo. Actualmente, el CERT original de la Carnegie Mellon University se conoce como CERT/CC (CERT Coordination Center), ya que actúa como coordinador y da soporte a equipos CERT (o CSIRT) de nivel nacional (generalmente gubernamentales) en todo el mundo. En la tabla 1 se muestran algunos de los principales CERT en territorio español incluyendo su URL, año de creación y ámbito de aplicación.

*En inglés, *worm*

Morris Worm

El gusano Morris fue uno de los primeros virus que se distribuyeron por Internet. Fue creado por Robert Morris, un estudiante de la Cornell University, y distribuido desde el MIT (*Massachusetts Institute of Technology*) en 1988. Se propagaba explotando distintas vulnerabilidades del sistema operativo UNIX. Aunque no existen datos fiables, se estimó que llegó a infectar aproximadamente a un 10 % de las máquinas que en aquella época estaban conectadas a Internet.

La proliferación de equipos CERT por el mundo ha hecho necesario establecer cierta coordinación entre ellos. Aparte de CERT/CC, existen centros de coordinación de equipos CERT a escala internacional, como FIRST (*Forum of Incident Response and Security Teams*), TF-CSIRT (*Computer Security Incident Response Teams Task Force*) en el ámbito europeo, o CSIRT.es (Equipos de Seguridad y Atención a Incidentes) en el español.

Los equipos CERT disponen de bases de datos y canales de distribución (como listas de correo) para distribuir información relativa a vulnerabilidades. Su

Tabla 1. Principales equipos CERT en territorio español

esCERT UPC	Universidad Politécnica de Cataluña	
	http://escert.upc.edu/	1994
	Universidades y pymes catalanas	
IRIS-CERT	RedIris (Red.es, Ministerio de Industria, Turismo y Comercio)	
	http://www.rediris.es/cert/	1997
	Universidades	
S21sec CERT	Grupo S21sec Gestión SA.	
	https://cert.s21sec.com/	2000
	Clientes y ciudadanos	
CCN-CERT	Centro Criptográfico Nacional (Centro Nacional de Inteligencia, Ministerio de Defensa)	
	https://www.ccn-cert.cni.es/	2006
	Administración pública (general, autonómica y local)	
INTECO CERT	Instituto Nacional de Tecnologías de la Comunicación (Ministerio de Industria, Turismo y Comercio)	
	http://cert.inteco.es/	2007
	Pymes y ciudadanos	
CSIRT-CV	Centre Seguretat TIC de la Comunitat Valenciana	
	http://www.csirtcv.gva.es/	2007
	Ciudadanos, pymes y Administración pública de la Comunidad Valenciana	
CESICAT	Centre de Seguretat de la Informació de Catalunya (Generalitat de Catalunya)	
	http://www.cesicat.cat/	2010
	Ciudadanos, pymes, universidades/centros de investigación y Administración pública en Cataluña	

principal tarea es recoger información sobre vulnerabilidades, clasificarlas y publicar su existencia, así como posibles medidas para mitigarlas. La información la suelen suministrar fabricantes, organizaciones o usuarios directamente a un CERT que luego suele distribuir información a otros equipos CERT con los que esté coordinado. Así mismo, la distribución puede ser directa y abierta al público, restringida a organizaciones concretas, o a suscriptores. Como recogen y distribuyen información, los CERT depende mucho del tipo de CERT y su ámbito de aplicación. En general, se considera una buena práctica difundir información de vulnerabilidades de modo abierto y gratuito a toda la comunidad de usuarios de Internet con el objetivo de mejorar la seguridad general de la Red. Por ello, la mayor de los CERT importantes distribuyen esta información libremente.

Ejemplo de publicación de vulnerabilidad

En la tabla 2 podemos ver una vulnerabilidad real reportada por CCN-CERT sobre la aplicación Powerpoint de Microsoft. La publicación de dicha vulnerabilidad incluye información que puede ser de utilidad a usuarios u organizaciones. Este es un formato típico usado por la mayoría de los CERT. Para que una vulnerabilidad sea admitida en una BD de un CERT, generalmente pasa por un proceso de verificación. Este proceso es complejo e importante, ya que entre otras cosas se encarga de clasificar y etiquetar de manera única la vulnerabilidad. Esta identificación única (en el caso de la tabla 2 es CVE-2011-1269, y CVE-2011-1270) permite evitar duplicados y coordinar acciones entre diferentes CERT. En el subapartado 2.2 veremos cómo se etiquetan dichas vulnerabilidades.

Tabla 2

Múltiples vulnerabilidades en Microsoft PowerPoint	
Clasificación de la vulnerabilidad	
Riesgo	Medio
Nivel de confianza	Oficial
Impacto	Obtener acceso
Dificultad	Experto
Requerimientos del atacante	Acceso remoto sin cuenta a un servicio estándar
Información sobre el sistema	
Plataforma afectada	Microsoft
Software afectado	Microsoft Office 2003 SP3
	Microsoft Office XP SP3
	Microsoft Office 2007 SP2
	Microsoft Office 2004 para MacOS
	Microsoft Office 2008 para MacOS
	Open XML File Format Converter para MacOS
Descripción	
Se han descubierto múltiples vulnerabilidades en Microsoft PowerPoint en Windows y MacOS. Las vulnerabilidades son descritas a continuación: - CVE-2011-1269: Se ha descubierto una vulnerabilidad en "PowerPoint". La vulnerabilidad reside en un error en el modo como trata los archivos. Un atacante remoto podría obtener acceso o ejecutar código arbitrario mediante un archivo "PowerPoint" especialmente manipulado. - CVE-2011-1270: Se ha descubierto una vulnerabilidad en "PowerPoint". La vulnerabilidad reside en un error en el modo como trata los archivos. Un atacante remoto podría obtener acceso o ejecutar código arbitrario mediante un archivo "PowerPoint" especialmente manipulado. El boletín MS11-036 sustituye al MS11-022	
Solución	
Actualización de software Microsoft (MS11-036) Ver tabla de actualizaciones en: http://www.microsoft.com/technet/security/Bulletin/MS11-036.mspx	
Identificadores estándar	
CVE	CVE-2011-1269
	CVE-2011-1270
BID	NULL
Recursos adicionales	
Microsoft Security Bulletin (MS11-036): http://www.microsoft.com/technet/security/Bulletin/MS11-036.mspx	
Histórico de versiones	
Version	Fecha
1.0	2011-05-11

Fuente: CCN-CERT

2.1. Sobre la libre publicación de vulnerabilidades

A la hora de decidir si se hace o no pública una vulnerabilidad, se plantea un dilema que suele acarrear una polémica importante. Por una parte, están los partidarios de publicar libremente una vulnerabilidad una vez es conocida; de esta manera, todo el mundo puede conocer su existencia y aplicar las medidas preventivas adecuadas. Por otra parte, hay gente que piensa que hacer pública información relativa a vulnerabilidades equivale a dar armas al enemigo, ya que muchas veces son vulnerabilidades conocidas (no corregidas) las que se utilizan en ataques informáticos.

En el campo de la seguridad informática, por lo general, se considera como buena práctica el ofrecer la mayor claridad posible sobre problemas y mecanismos de seguridad, y no basar la seguridad de un sistema en la ocultación de información. Es decir, un atacante lo primero que hace al querer atacar un sistema concreto es recoger información sobre ese sistema: sistema operativo, software que utiliza, etc., y luego busca vulnerabilidades que puedan ser explotadas en dicho sistema. El intentar ocultar información sobre el sistema para impedir que el atacante pueda buscar vulnerabilidades en él es algo común. Sin embargo, esta es una práctica de dudosa eficacia y puede llegar a dar una falsa sensación de seguridad. Por ello, muchos expertos abogan por asumir que el posible atacante dispone de esa información y, por tanto, no es necesario ocultarla. Esta idea toma su inicio en el principio de Kerckhoff (1835-1903) sobre los criptosistemas.

Principio de Kerckhoff

Los criptosistemas "no deben ser necesariamente secretos, y deben poder caer en manos del enemigo sin que ello conlleve inconveniente alguno".

A. Kerckhoffs (1883). La cryptographie militaire. *Journal des sciences militaires* (vol. IX, pág. 5-83, enero, pág. 161-191, febrero).

Esta idea de que el método o sistema no debe ser secreto se extiende hoy en día por la mayoría de los sistema de información, y muchos expertos abogan por la libre publicación de vulnerabilidades.

Siguiendo estos principios, la mayoría de los CERT adoptan un compromiso en la publicación de vulnerabilidades. En general, abogan por la libre publicación. Sin embargo, suelen informar a los fabricantes días previos a la aparición de la vulnerabilidad en su web para que estos puedan desarrollar medidas preventivas o parches de seguridad.

Vulnerabilidades publicadas por el CERT/CC

CERT/CC actualmente hace pública cualquier vulnerabilidad que le sea reportada en 45 días, independientemente de la existencia de parches o soluciones por parte de los fabricantes. Durante esos 45 días, CERT/CC notifica al fabricante del producto dónde se ha encontrado la vulnerabilidad. La independencia de estos equipos CERT posibilita que puedan evitar presiones por parte de fabricantes en la publicación de vulnerabilidades de sus productos.

2.2. Etiquetado e identificación de vulnerabilidades

Para poder identificar vulnerabilidades, existen identificadores únicos que impiden que se publiquen duplicados y facilitan la posibilidad de hacer referencia a vulnerabilidades concretas. El sistema de identificación más importante a escala internacional es el CVE (*Common Vulnerabilities and Exposures*). CVE se presenta como un estándar de nombres de vulnerabilidades de seguridad informática de uso gratuito y público. Se autodefine como un diccionario de vulnerabilidades (no como una base de datos), donde cualquiera puede buscar el nombre (identificador) que recibe una vulnerabilidad concreta.

Para etiquetar una vulnerabilidad en el CVE, se sigue el procedimiento siguiente:

1) Se descubre una vulnerabilidad.

2) Se le asigna un identificador CVE con el estado *candidato*. Esta asignación la hace un *CVE Candidate Numbering Authority* (CNA), que son los principales fabricantes de software y hardware, así como organizaciones y empresas del sector, autorizados por CVE.

3) La vulnerabilidad se publica en la página web de CVE y se propone al consejo editor de CVE su aprobación.

4) El consejo editor decide mediante votación si acepta la vulnerabilidad, con lo que pasa a estado *entry* y se añade a la lista de CVE, o si por el contrario se desestima.

La importancia de CVE viene dada por su gran adopción a escala internacional. La mayoría de los equipos CERT, fabricantes de software y hardware, desarrolladores de sistemas operativos y organizaciones, así como productos destinados a la seguridad informática utilizan los identificadores CVE.

Gestión del CVE

Actualmente, CVE está gestionado por *The Mitre Corporation*, empresa estadounidense que actúa como líder del consejo editor. Cabe destacar también que CVE está actualmente esponsorizado por el *U.S. Department of Homeland Security*.

El consejo editor de CVE debe decidir entre otras cosas qué se considera como vulnerabilidad. Para ello, utiliza una definición propia.

Según CVE, una vulnerabilidad es un estado de un sistema informático (o conjunto de sistemas) que cumple alguno de los siguientes casos:

- Permite a un atacante ejecutar comandos como otro usuario.
- Permite a un atacante acceder a datos violando las restricciones de control de acceso específicas para dichos datos.
- Permite a un atacante suplantar a otra entidad.
- Permite a un atacante llevar a cabo una denegación de servicio.

Como se puede ver, la definición de vulnerabilidad de CVE es bastante más restrictiva y específica que la definición genérica que hemos adoptado en el apartado 1. Esto es así para poder restringir un poco la aplicabilidad de CVE, ya que de otra manera resultaría muy difícil poder dar cabida a todas la vulnerabilidades. Hay que tener en cuenta también que CVE nace y se gestiona bajo la esponsorización de agencias de inteligencia y defensa cuya principal preocupación es la defensa ante atacantes (de aquí la insistencia en el atacante en la definición).

BugTraq

Aparte de CVE, existen otros esquemas de identificación de vulnerabilidades. Cabe destacar BID (BugTraq ID), que es un identificador asignado por la lista BugTraq. BugTraq es una lista de correo electrónico sobre seguridad informática creada en 1993. Su objetivo (entre otros) era facilitar la difusión de vulnerabilidades libremente (sin necesidad de solicitar permiso al fabricante). Aunque fue muy popular, ha ido perdiendo importancia especialmente después de que fue adquirida por la empresa SecurityFocus, que a su vez fue absorbida por Symantec.

2.3. Bases de datos de vulnerabilidades

Aunque como se ha comentado anteriormente la mayoría de los equipos CERT ofrecen bases de datos de vulnerabilidades, existen alguna bases de datos a las que los CERT suelen a hacer referencia. Entre ellas, destacamos:

- **The Open Source Vulnerability Database (OSVD)**. Base de datos de código abierto creada de modo independiente, que está gestionada por la organización sin ánimo de lucro *Open Security Foundation*.

OSVD: http://osvdb.org/

- **National Vulnerability Database (NVD)**. Base de datos perteneciente al gobierno de Estado Unidos de acceso público.

NVD: http://nvd.nist.gov/

- **SecurityFocus Vulnerability Database**. Base de datos mantenida por la empresa Symantec. Esta empresa también dispone de la lista de distribución *BugTraq*, que llegó a ser el principal canal de difusión de vulnerabilidades en los años noventa.

SecurityFocus Vulnerability Database: http://www.securityfocus.com/bid

- **Exploit DB**. Base de datos de vulnerabilidades que tiene la particularidad de que, además de publicar las vulnerabilidades, publica los *exploits* correspondientes (de ahí su nombre). Estos son programas o *scripts* que permiten explotar dicha vulnerabilidad, es decir, programas que permiten realizar un ataque que se aproveche de la vulnerabilidad. Aunque sirven como prueba de concepto y para testear sistemas, su potencial uso malicioso es el motivo por el que el resto de las bases de datos y CERT no publican *exploits*.

Exploit DB: http://www.exploit-db.com/

Aparte de estas bases de datos genéricas, todos los fabricantes de aplicaciones, sistemas operativos (incluyendo las organizaciones que distribuyen sistemas operativos de código libre), o hardware, suelen tener bases de datos donde encuentran clasificadas vulnerabilidades relacionadas con sus productos, sistemas o servicios.

2.4. Evaluación de vulnerabilidades

En el ejemplo de la tabla 2 se puede observar que a la vulnerabilidad se le atribuye un nivel de riesgo, dificultad o impacto. El hecho de poder dar este nivel de riesgo es importante, ya que permite evaluar qué vulnerabilidades son potencialmente más peligrosas y, por tanto, más urgentes. Esto también se tiene en cuenta a la hora de hacer una estimación del riesgo del sistema. De todos modos, es difícil establecer una métrica común para evaluar la criticidad de vulnerabilidades.

En esta línea, el sistema de evaluación más extendido se conoce como CVSS (*Common Vulnerability Scoring System*). CVSS es un intento de estandarizar un métrica común para evaluar vulnerabilidades. La idea es obtener un número (o

conjunto de números) que nos den una idea del peligro potencial que supone una vulnerabilidad.

CVSS distingue entre tres métricas básicas:

- **Métrica base**, aspectos de la vulnerabilidad constantes en el tiempo y entorno descritos en la tabla 3. Estas métricas proporcionan un valor entre 0 y 10 que determina la gravedad de la vulnerabilidad. Esta se etiqueta como *low* (valor en [0,0,3,9]), *medium* (valor en [4,0,6,9]) o *high* (valor en [7,0,10,0]). La métrica base también se expresa como vector:

```
AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C].
```

Tabla 3. Métrica base de CVSS

Vector de acceso (AV)	Cómo se explota la vulnerabilidad. Puede ser localmente (L), desde una red adyacente (A) o desde cualquier red (N).
Complejidad de acceso (AC)	Complejidad que requiere el atacante una vez ha accedido al sistema. Esta puede ser alta (H), media (M) o baja (L).
Autenticación (Au)	Número de veces que el atacante debe autenticarse contra un sistema. Pueden ser múltiples (M), una (S) o ninguna (N).
Impacto de confidencialidad (C), integridad (I) y disponibilidad (A)	Tres indicadores sobre el impacto que puede tener la vulnerabilidad en la confidencialidad, integridad y disponibilidad del sistema. Para cada uno los valores puede ser: ninguno (N), parcial (P) o completo (C).

Ejemplo

La vulnerabilidad CVE-2002-0392 de la tabla 4 tiene un vector base:

```
AV:N/AC:L/Au:N/C:N/I:N/A:C
```

Es decir, vector de acceso: *network*, desde cualquier red (AV:N); complejidad de acceso: baja (AC:L); autenticación: ninguna (Au:N); confidencialidad: ninguno (C:N); integridad: ninguno (I:N), y disponibilidad: completo (A:C). Este vector ya nos da mucha información de la vulnerabilidad. Esta es una vulnerabilidad que se puede explotar desde cualquier red, que tiene impacto sobre la disponibilidad (posiblemente mediante un ataque de denegación de servicio), es fácil de explotar y sin necesidad de autenticarse.

Tabla 4. Métrica base de CVSS

Vulnerabilidad		Scores CVSS		
		Base	Temporal	Entorno
CVE-2002-0392	Apache Chunked-Encoding Memory Corruption Vulnerability	**7,8**	6,4	0,0-9,2
CVE-2003-0818	Microsoft Windows ASN.1 Library Integer Handling Vulnerability	**10,0**	8,3	0,0-9,0
CVE-2003-0062	Buffer Overflow in NOD32 Antivirus	**6,2**	4,9	0,0-7,5

Cálculo de CVSS

Existen aplicaciones que facilitan el cálculo del *score* CVSS, como las siguientes:

- NIST CVSSv2 Calculator (http://nvd.nist.gov cvss.cfm)
- IPA, Japan (http://jvnrss .ise.chuo-u.ac.jp/jtg/cvss /en/CVSSv2.html)

- **Métrica temporal**, métricas que pueden cambiar en el tiempo. Comprenden la explotabilidad (existencia de *exploits* y su grado de disponibilidad), nivel de curación o *remediation level* (existencia de soluciones y si son definitivas o temporales) y la confianza del anuncio (hasta qué nivel se ha confirmado la existencia de la vulnerabilidad). La métrica temporal se combina con la base para dar un valor entre 0 y 10.

- **Métricas del entorno**, métricas relativas al entorno del sistema informático propiamente dicho, que incluye el riesgo que puede suponer a una

organización o a personas individuales. Aquí se contempla el *daño colateral potencial*, que mide el daño que puede ocasionar a terceros la explotación de dicha vulnerabilidad (daño a personas, a bienes físicos, a la productividad o a los beneficios). También se incluye la distribución de objetivos o *target distribution*, que mide la proporción de sistemas vulnerables en el entorno. Estas métricas dan un valor entre 0 y 10, que generalmente se expresa como intervalo mínimo-máximo.

A partir de todas estas métricas, CVSS proporciona un valor numérico o *score* general sobre la vulnerabilidad. En la tabla 4 vemos algún ejemplo de *scores* CVSS para 3 vulnerabilidades concretas. El *score* que se suele utilizar más es el de métricas base; en este caso nos da unos valores que clasificarían las dos primeras vulnerabilidades con un nivel de criticidad alto (*high*) y la última con un nivel medio (*medium*).

3. Clasificación de vulnerabilidades

Existen varias clasificaciones de vulnerabilidades y ninguna de ellas prevalece sobre el resto. El hecho de adoptar una clasificación u otra viene muchas veces condicionado por el propósito de dicha clasificación. En nuestro caso, y con el objetivo de proporcionar una visión global de la seguridad informática, hemos adoptado una clasificación que se basa en el tipo de sistema al que afecta la vulnerabilidad. De esta manera, distinguimos entre:

- **Vulnerabilidades de bajo nivel y software malicioso**. A aquí entran vulnerabilidades que afectan al sistema operativo y aplicaciones a bajo nivel propiciadas generalmente por errores en la programación, como *buffer overflows* o *race conditions*. También se incluye en este tipo de vulnerabilidades el estudio de software malicioso, como virus o gusanos que explotan este tipo de vulnerabilidades.

- **Vulnerabilidades de red**. Son vulnerabilidades que afectan a software y componentes de red o interconexión de redes. Estas vulnerabilidades pueden ir desde redes locales a Internet. Principalmente, se observan vulnerabilidades en los diferentes protocolos de red, así como vulnerabilidades derivadas del análisis de tráfico.

- **Vulnerabilidades en aplicaciones web**. La importancia de Internet y las aplicaciones web, desde el comercio electrónico, las redes sociales, o lo que actualmente se denomina como *cloud computing*, provoca que dichas aplicaciones merezcan un apartado propio. Estas son vulnerabilidades propias de aplicaciones pensadas para ser ofrecidas mediante una interfaz web y a las que generalmente tienen acceso un gran número de usuarios. En general, se consideran vulnerabilidad de más alto nivel que las del primer apartado, e incluyen *cros-site scripting*, inyección de código, etc.

- **Vulnerabilidades de ingeniería social**. Este apartado concentra las vulnerabilidades asociadas a los usuarios de los sistemas informáticos. Tienen más relación con el aspecto psicológico de dichos usuarios que con problemas puramente técnicos. Ejemplos típicos son el *spam*, *phising*, etc.

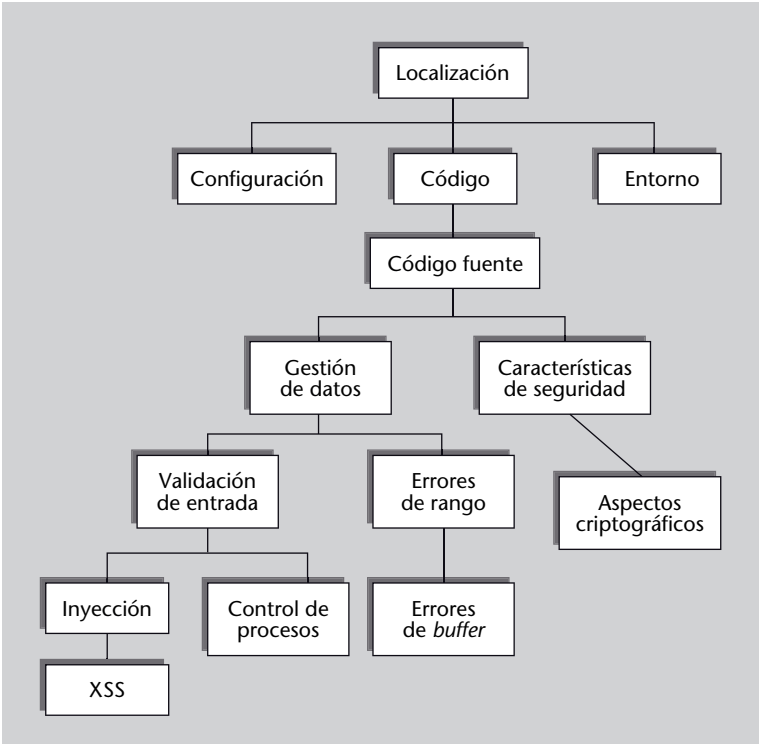
Otra posible clasificación de las vulnerabilidades se basa en la idenificación del servicio al cual afectan. De este modo, si tomamos la clasificación que tradicionalmente se aplica a los servicios de seguridad (confidencialidad, integridad y disponibilidad), tenemos vulnerabilidades que comportan:

- Pérdida de integridad.
- Pérdida de confidencialidad.
- Pérdida de disponibilidad.

En este caso, la clasificación va orientada a identificar qué pueden permitir hacer estas vulnerabilidades a un posible atacante. Por ejemplo, una vulnerabilidad que permita una denegación de servicio es manifiestamente una vulnerabilidad de disponibilidad, así como vulnerabilidades que permitan espiar comunicaciones lo son de confidencialidad. Este es uno de los criterios que expresa directamente la métrica base de CVSS vista en el subapartado 2.4.

Siguiendo la clasificación anterior basada en servicios, encontramos una posible extensión. El CWE (*Common Weakness Enumeration Specification*) proporciona una enumeración jerárquica de tipos de vulnerabilidades orientadas a software. La clasificación de CWE es muy detallada y permite fijar numerosos niveles de abstracción (según se va bajando por la jerarquía), como ejemplo mostramos una pequeña parte de dicha clasificación relativa a la localización de la vulnerabilidad en la figura 5.

Figura 5. Estructura parcial de CWE



En general, existen muchas maneras de clasificar vulnerabilidades; por ejemplo, cualquiera de los criterios y métricas que hemos comentado en el subapartado 2.4 pueden servir para clasificar vulnerabilidades.

Resumen

En este módulo hemos introducido el concepto de vulnerabilidad en lo que a sistema de información se refiere. Como hemos podido ver, las vulnerabilidades son de vital importancia en cualquier proceso de seguridad, puesto que una vulnerabilidad se puede ver como primer escalón del proceso de seguridad. Dicha importancia ha quedado de relieve con la enumeración de algunos ejemplos célebres de ataques que explotaban vulnerabilidades concretas.

La propia definición de vulnerabilidad nos ha llevado a definir conceptos muy relacionados, como los ataques y las amenazas. Aunque pueden parecer lo mismo, su distinción se hace necesaria para una comprensión correcta de cada concepto y su relación con el riesgo que cada uno de ellos implica.

Posteriormente, hemos analizado cómo se realiza la gestión de las vulnerabilidades, que, para una mejor efectividad, precisa la coordinación de distintos centros a escala mundial. Hemos identificado los centros más relevantes internacionales y nacionales haciendo hincapié en los mecanismos de identificación, clasificación y evaluación de vulnerabilidades en función de su criticidad.

Por último, hemos dado algunas posibles clasificaciones que permiten agrupar las vulnerabilidades a partir de sus caracerísticas. A partir de las clasificaciones descritas se fundamentarán cada uno de los módulos de la asignatura.

Actividades

1. Buscad por Internet algún ataque informático reciente del que hayáis tenido noticia. En ese ataque identificad la vulnerabilidad o vulnerabilidades explotadas y clasificadlas según lo que se ha visto en el apartado 3.

2. Buscad la vulnerabilidad CVE-1999-0508 en varias bases de datos de vulnerabilidades. Explicad brevemente en qué consiste dicha vulnerabilidad y comentad la evaluación de la vulnerabilidad utilizando CVSS que dan las bases de datos, su posible impacto, clasificación y solución.

3. Buscad una vulnerabilidad reciente en alguna base de datos de vulnerabilidades y describid aproximadamente cómo obtendríais los valores CVSS a partir de las características de la vulnerabilidad. Finalmente, utilizad alguna de las calculadoras CVSS, por ejemplo http://nvd.nist.gov/cvss.cfm?calculator&version=2, para obtener los valores CVSS.

Glosario

amenaza *f* Violación de la seguridad en potencia, que existe en función de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún daño en el sistema.

ataque *m* Agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema.

CERT (*computer emergency response team*) *m* Equipo de respuestas a emergencias informáticas. Una de sus principales tareas consiste en la gestión de vulnerabilidades.

CSIRT (*computer security incident response team*) *f* Equipo de respuesta a incidentes de seguridad informática. Una de sus principales tareas consiste en la gestión de vulnerabilidades.

CVE (*common vulnerabilities and exposures*) *f* Estándar publico para la identificación de vulnerabilidades. Asocia un identificador único a cada vulnerabilidad diferente.

CVSS (*common vulnerability scoring system*) *f* Marco común para la evaluación de la criticidad de vulnerabilidades.

exploit *m* Programa o *script* que permite explotar una o varias vulnerabilidades, es decir, programa que permite realizar un ataque aprovechando la vulnerabilidad.

política de seguridad *f* Conjunto de reglas y prácticas que definen y regulan los servicios de seguridad de una organización o sistema con el propósito de proteger sus recursos críticos y sensibles. En otras palabras, es la declaración de lo que está permitido y lo que no está permitido hacer.

riesgo *m* Expectativa de pérdida expresada como la probabilidad de que una amenaza particular explote una vulnerabilidad concreta con resultados especialmente perjudiciales.

rootkit *m* Programa que permite el acceso privilegiado a un ordenador y consigue ocultar su presencia al administrador. Suele hacer uso de varias vulnerabilidades para instalarse y conseguir su propósito.

vulnerabilidad de día-cero (*zero-day vulnerability*) *f* Vulnerabilidad de cuya existencia, en el momento de ser explotada, no se tiene conocimiento previo.

vulnerabilidad de seguridad *f* Fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema.

Bibliografía

Bishop, M. (2002). *Computer Security: Art and Science*. Boston: Addison Wesley

Mell, P.; Scarfone, K.; Romanosky, S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0* [artículo en línea]
<http://www.first.org/cvss/cvss-guide.html>

Shirey, R. (2000). *Internet Security Glossary*. RFC 2828, IETF