

Seguridad en la Red Informática Mundial

Semana 1 clases 1 y 2

Mtra. María Noemí Araíza Ramírez



Nombre de la materia: Seguridad en la Red Informática de la Maestría en Dirección e Ingeniería de Sitios Web, tiene un valor de 6 créditos.

Se impartirán un total de 16 sesiones de 120 minutos, esto son 2 horas a la semana siendo un total de 32 horas en el semestre

Tema 1. Metodologías de desarrollo de aplicaciones web seguras

- Introducción
- Metodología Microsoft
- OSSTMM
- OWASP

Objetivos

- Conocer los motivos para Desarrollar Seguro
- Conocer las Metodologías más extendidas
- Conocer cómo aplicar una metodología
- Referencias externas

Tema 2. Top 10 de vulnerabilidades según OWASP

- Introducción
- Riesgos de seguridad en aplicaciones
- Los 10 riesgos más serios

Objetivos

- Qué es OWASP Top10
- Qué objetivos y motivaciones tiene
- Qué son los Riesgos de Seguridad de Aplicaciones
- Conocer cómo me afectan
- Conocer los 10 Riesgos más importantes

Vamos a tener 16 semanas de curso mas una de examen
serán de la siguiente forma: Semanas de la 1 a la 5

	CONTENIDO TEÓRICO	ACTIVIDADES (10 puntos)
Semana 1	Semana de introducción a la asignatura	
Semana 2	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras 1.1. Introducción	
Semana 3	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.2. Metodología Microsoft	Foro: ¿Qué otras vulnerabilidades conoces en entornos Web que no se mencionen en el top 10? (1,3 puntos)
Semana 4	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.2. Metodología Microsoft	
Semana 5	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.3. OSSTMM	

Semanas 6 a la 9

Semana 6	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.3. OSSTMM	
Semana 7	Semana de repaso	
Semana 8	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.4. OWASP	Actividad: Investigación de otras metodologías de desarrollo de aplicaciones Web seguras (1,3 puntos)
Semana 9	Tema 1. Metodologías de desarrollo de aplicaciones Web seguras (continuación) 1.4. OWASP	

Semanas 10 a la 13

Semana 10	Tema 2. Top 10 de vulnerabilidades según OWASP 2.1. Introducción	
Semana 11	Tema 2. Top 10 de vulnerabilidades según OWASP (continuación) 2.1. Introducción	Actividad: Práctica guiada con WebGoat (3,4 puntos)
Semana 12	Tema 2. Top 10 de vulnerabilidades según OWASP (continuación) 2.2. Riesgos de seguridad en aplicaciones	
Semana 13	Tema 2. Top 10 de vulnerabilidades según OWASP (continuación) 2.2. Riesgos de seguridad en aplicaciones	

Semanas 14 a la 17

Semana 14	Tema 2. Top 10 de vulnerabilidades según OWASP (continuación) 2.3. Los riesgos más serios	Actividad: Actividad: Análisis de vulnerabilidades con herramientas Proxy HTTP (4 puntos)
Semana 15	Tema 2. Top 10 de vulnerabilidades según OWASP (continuación) 2.3. Los riesgos más serios	
Semana 16	Semana de repaso	
Semana 17	Examen final	

Actividades

Foro:

¿Qué otras vulnerabilidades conoces en entornos Web que no se mencionen en el top 10?

Valor: 1,3 puntos

Fecha límite de entrega: 7 de junio a las 23:55

Actividades

Actividad 1:

Investigación de otras metodologías de desarrollo de aplicaciones web seguras

Valor: 1,3 puntos

Fecha limite de entrega: 5 de julio a las 23:55

Actividades

Actividad 2:

Practica guiada con WebGoat

Valor: 1,3 puntos

Fecha limite de entrega: 26 de julio a las 23:55

Actividad 3:

Análisis de vulnerabilidades con herramientas proxy HTTP

Valor: 1,3 puntos

Fecha limite de entrega: 16 de agosto a las 23:55

Bibliografía a tomar en cuenta

Seguridad informática para la empresa. Álvarez, Gonzalo. Mc Graw Hill. 2009

Resumen

La informática ha pasado a formar parte de la actividad cotidiana de empresas y particulares. Los ordenadores almacenan información, la procesan y la transmiten a través de redes, abriendo nuevas posibilidades de ocio y de negocio. Cuanto mayor es el valor de la información gestionada, más importante es asegurarla. La mayoría de usuarios particulares y de empresas poseen la percepción de que la seguridad de la información es una tarea difícil de aplicar, que exige gran cantidad de dinero y de tiempo. En realidad, con muy poco esfuerzo se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad de particulares y de pequeñas y medianas empresas. Haciendo uso de herramientas que vienen suministradas con el propio sistema operativo o que son en su mayoría gratuitas, en este libro aprenderá como mantener la seguridad informática en su empresa.

Bibliografía a tomar en cuenta

Seguridad informática. Escrivá, Gema. Mc Millán Iberia. 2013

Resumen

Los temas que ofrece son Seguridad de la información y seguridad informática, Conceptos básicos relacionados con la seguridad informática, Principios básicos de la seguridad informática, Políticas de seguridad y Planes de contingencia

Los objetivos del libro son conocer las diferencias entre seguridad de la información y seguridad informática, Aprender los conceptos básicos relacionados con el mundo de la seguridad informática, Describir cuáles son los principios básicos de seguridad y Aprender en qué consisten los planes de contingencia

Objetivos

- Conocer los motivos para Desarrollar Seguro
- Conocer las Metodologías más extendidas
- Conocer cómo aplicar una metodología

Introducción

El mantra de todo buen ingeniero de seguridad es: "La seguridad no es un producto, sino un proceso." implica algo mas que la implantación de criptografía robusta en un sistema: se trata de diseñar el sistema entero de manera que todas las medidas de seguridad, incluyendo la criptografía, trabajen conjuntamente.

Bruce Schneier

Podemos decir que la informática se ha extendido ya a todas las actividades profesionales y humanas.

“Las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y de electricidad.

Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad”.

El ambiente de cómputo se ha vuelto muy complejo, si consideramos que están involucrados los equipos, tipos de redes, switches, ruteadores, puntos de acceso, sistemas operativos, sitios Web, aplicaciones, puertos, servicios, teléfonos inteligentes; todos ellos interconectados y operando por millones y millones de líneas de código.

Mientras más complejo, más vulnerable.

¿Qué es seguridad?

Seguridad (del latín securitas) hace referencia a la ausencia de riesgo, a la plena confianza que se tiene en algo o alguien, pero también se puede definir dependiendo del área o campo a la que se haga referencia en la seguridad.

En general, podríamos decir que la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano".

¿Qué son seguridad de la información y seguridad informática?

Uno de los activos que se considera muy importante para una empresa, es la información que esta maneja.

La información es el conjunto de datos que definen a una empresa.

En ese sentido veremos dos perspectivas, una la seguridad de la información y la seguridad informática.

¿Qué es seguridad de la información?

La vamos a definir como el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información:

- Integridad: asegurando que la información y sus métodos de proceso son exactos y completos.
- Confidencialidad: hacer constar que sólo pueden acceder a la información y modificarla los usuarios autorizados.
- Disponibilidad: dejando que la información pueda estar disponible cuando los usuarios la requieran.

En resumen este concepto engloba las medidas de seguridad que van a afectar a la información no importando el tipo de esta, soporte en el que se almacene, forma en que se transmita, etc.

¿Qué es seguridad informática?

Es una rama de la seguridad de la información que intenta proteger la información que utiliza una infraestructura informática y de telecomunicaciones para ser almacenada o transmitida.

En función de lo que se quiere proteger:

- Seguridad física: que se asocia a la protección física del sistema ante amenazas como inundaciones, incendios, robos, etc.
- Seguridad lógica: mecanismos que protegen la parte lógica de un sistema informático (datos, aplicaciones y sistemas operativos). Uno de los medios más utilizados es la criptografía.

En función del momento en que tiene lugar la protección:

- Seguridad activa: se encarga de prevenir, detectar y evitar cualquier incidente en los sistemas informáticos antes de que se produzca (medidas preventivas).
Por ejemplo, utilización de contraseñas.
- Seguridad pasiva: comprende todas aquellas técnicas o procedimientos necesarios para minimizar las consecuencias de un incidente de seguridad (medidas correctoras).
Por ejemplo, las copias de seguridad.

Conceptos básicos en materia de seguridad

Activos, vulnerabilidades, amenazas, ataques, riesgos, etc.

Activo

Es el recurso del sistema (informático o no) que involucra a los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc. que una organización necesita para lograr sus objetivos, como el proteger debidamente aquello que se enfrente a un eventual suceso o percance intencionado o no.

En la informática se consideran activos principales de una empresa:

- Información: datos almacenados en cualquier tipo de soporte.
Por ejemplo, documentos, libros, patentes, correspondencia, manuales de usuario, etc.
- Software: programas o aplicaciones que utiliza la organización para su buen funcionamiento.
Por ejemplo: las aplicaciones comerciales, los sistemas operativos, etc.
- Físicos: la infraestructura tecnológica empleada para almacenar, procesar, gestionar o transmitir toda la información para el buen funcionamiento de la organización.
Por ejemplo: servidores, computadoras de escritorio, etc.
- Personal de la organización que utilice la estructura tecnológica y de comunicación para el manejo de la información.

Vulnerabilidad

Se refiere a la debilidad “agujeros de seguridad” de un activo que pueda afectar de alguna manera el correcto funcionamiento del sistema informático.

Hablamos de fallos en la implementación de las aplicaciones o en la configuración del sistema operativo, etc.

Como ejemplo tenemos el no utilizar algún tipo de protección frente a fallos eléctricos o no contar con mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos.

Amenaza

Es cualquier entidad o circunstancia que atenta contra el buen funcionamiento de un sistema informático. Sin embargo hay amenazas que afectan a los sistemas de forma involuntaria, como un desastre natural.

Se tienen dos tipos de amenazas, las pasivas y las activas.

- Pasivas, conocidas como “escuchas”. Su objetivo es obtener información relativa a una comunicación.
Por ejemplo, los equipos informáticos portátiles que utilizan programas especializados para monitorizar el tráfico de una red WiFi.
- Activas, que intentan realizar algún cambio no autorizado en el estado del sistema, son más peligrosas que las anteriores.
Como ejemplos se encuentran la inserción de mensajes ilegítimos, la usurpación de identidad, etc.

MAGERIT es la metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica.

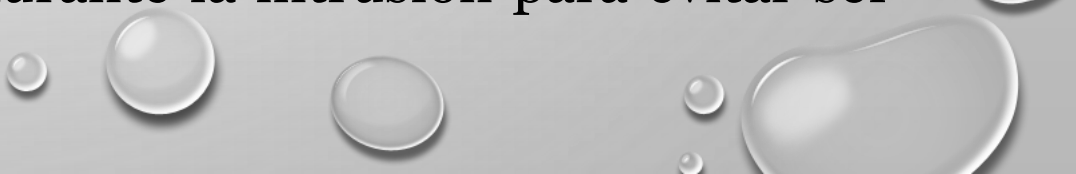
Grupos de amenazas	Ejemplos
Desastres naturales	Fuego, daños por agua, desastres naturales.
Desastres industriales	Fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
Errores y fallos no intencionados	Errores de usuarios, errores de configuración, etc.
Ataques deliberados	Manipulación de la configuración, suplantación de la identidad del usuario, Difusión de software dañino, etc.

Ataque

Es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Son acciones intencionadas o fortuitas que pueden llegar a poner en riesgo un sistema.

Como ejemplos de ataques tenemos la utilización de programas para conseguir acceso al servidor de forma ilegítima o la realización de ataques de denegación de servicio para colapsar el servidor.

Un ataque informático pasa por las siguientes fases:

- Reconocimiento. Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.
 - Exploración. Se intenta conseguir información sobre el sistema a atacar, como por ejemplo, direcciones IP, nombres de host, datos de autenticación, etc.
 - Obtención de acceso. A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.
 - Mantener el acceso. Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.
 - Borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado.
- 

Riesgo

Según la UNE-71504:2008, un riesgo “es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización”.

El Centro Criptológico Nacional define el riesgo como “la probabilidad de que una amenaza se materialice aprovechando una vulnerabilidad y causando daño (impacto) en un proceso o sistema”.

El riesgo es, una medida de la probabilidad de que se materialice una amenaza.

Por ejemplo, si la instalación eléctrica del edificio es antigua, existirá un riesgo elevado de sufrir una interrupción del servicio en caso de producirse una subida de tensión.

Álvarez, Marañón, Gonzalo, and García, Pedro Pablo Pérez. Seguridad informática para empresas y particulares, McGraw-Hill España, 2004. ProQuest Ebook Central,
<http://ebookcentral.proquest.com/lib/univunirsp/detail.action?docID=3195263>.

Escrivá, Gascó, Gema, et al. Seguridad informática, Macmillan Iberia, S.A., 2013. ProQuest Ebook Central,
<http://ebookcentral.proquest.com/lib/univunirsp/detail.action?docID=3217398>.