Servicios y Seguridad, un enfoque basado en estrategias de ataque y defensa

Marcela Castro-León[1], Francesc Boixader[1], Manel Taboada[1], Dolores Rexachs[2], Emilio Luque[2]
[1]Escola Universitària d'Informàtica Tomàs Cerdà.
Sant Cugat del Vallès, Barcelona, España
{marcela.castro, francesc.boixader,manel.taboada}@eug.es
[2]Universidad Autónoma de Barcelona.
Barcelona, España
{dolores.rexachs, emilio.luque}@uab.es

Resumen. En este artículo se presenta el enfoque metodológico de la asignatura Servicios y Seguridad del Grado de Informática y Servicios, título oficial de la Universidad Autónoma de Barcelona que se imparte en la Escuela Universitaria de Informática Tomás Cerdá. Proponemos un enfoque basado en estrategias de ataque y defensa utilizadas en sistemas informáticos. Los modelos de estrategia constituyen el hilo conductor que permite relacionar cómo contribuyen el resto de temas, como criptografía, estándares de seguridad, metodologías de modelado de amenazas y de evaluación de riesgos en la configuración de un sistema de servicios web seguro. La parte práctica incluye sesiones de laboratorio y el desarrollo de un trabajo de *hacking*. En el laboratorio los alumnos aprenden a configurar la seguridad de un servidor de aplicaciones web, a generar certificados de servidor y de clientes, y a incluir opciones de seguridad en aplicaciones y en servicios web. Realizando el trabajo práctico los alumnos aprenden a defender mejor al sistema a través del conocimiento de las técnicas y herramientas que utilizan los atacantes para descubrir y explotar las vulnerabilidades de las infraestructuras y aplicaciones.

Palabras Clave: Servicios web, Seguridad de servicios, Estándares de seguridad de servicios web, WS-Security, XML-Security, *Threat-Modeling*.

Abstract. This article describes the methodological approach of the subject Services and Security of the Bachelor's Degree in Information Technology and Services (*Universitat Autonoma de Barcelona)*, which is taught at the Tomas Cerda Computer Science School. We propose an approach based on attack and defense strategies which are used in computer systems. Strategy models are the thread that relates how the rest of the topics as cryptography, security standards, threat modeling and risk assessment methodologies contribute in setting up a secure web service based system. The practical part includes laboratory sessions and development of a work of hacking. In the laboratory students learn to set up a web server application, to generate server and client's certificates, and to include security options into applications and web services. By doing the practical work students learn how to defend the system in a better way through the knowledge of the techniques and tools used by *hackers* to discover and exploit vulnerabilities of infrastructure and applications.

Keywords: web services, web-service security, web-service security standards, WS-Security, XML-Security, *Threat-Modeling*.

1 Introducción

El Grado de Informática y Servicios [1] título oficial de la Universidad Autónoma de Barcelona que se imparte en la Escuela Universitaria de Informática Tomás Cerdá, surge al detectar en el tejido económico de este país una demanda de profesionales en las empresas de servicios, y su propósito es acercar la informática a dicho sector.

El perfil objetivo de este grado se ajusta al de un ingeniero informático. Este profesional debe ser capaz de evaluar, diseñar e implementar los sistemas de información en los que la tecnología juega un papel clave, con el objeto de gestionar la información utilizada por las empresas en todas sus áreas de negocio.

La seguridad informática es hoy una de las competencias más requeridas de un ingeniero de servicios. Las empresas están muy interesadas en fortalecer sus sistemas a la luz de sus vulnerabilidades y de los ataques cibernéticos que se conocen día a día. La tendencia actual de utilizar plataformas de *Cloud Computing* hace que los responsables de las aplicaciones deban revisar la seguridad de las arquitecturas utilizadas para valorar si éstas están o no preparadas para asumir los riesgos de seguridad que conlleva el movimiento a la nube.

Dichas competencias se pretenden trabajar a través de la asignatura de Servicios y Seguridad que incluye el Plan de Estudios del Grado en Informática y Servicio. El temario para dicha asignatura puede ser extenso y diverso. A los temas de seguridad tradicional relacionados con tener un entorno web y una red segura, se tienen que añadir cómo se deberían programar o configurar los servicios web para intercambiar mensajes que cumplan con los objetivos de seguridad de identificación, autenticación, confiabilidad, integridad, privacidad y no repudio. Esto implica integrar una gran variedad de conceptos partiendo desde la seguridad en las redes, configuración de la infraestructura, sistemas de criptografía, vulnerabilidades de software, estándares de seguridad en servicios, etc.

Las estrategias de ataque y defensa utilizadas actualmente [2] constituyen el hilo conductor del temario de esta asignatura. Pueden ser de ataque o de defensa, y se clasifican de acuerdo a lo indicado en la **Tabla 1** - Tipos de estrategias de ataque y defensa. Son modelos abstractos de funcionamiento que abarcan todas las alternativas utilizadas. Son independientes de las metodologías y herramientas de seguridad actuales y pueden utilizarse en un futuro para relacionar tecnologías emergentes.

Tabla 1 - Tipos de estrategias de ataque y defensa

Estrategias	Criterio	Tipos
Ataque	Según la trayectoria desde origen al destino	Directo; Progresivo; Masivos; Dirección Errónea
Defensa	Según el nivel de intromisión del atacante.	Decepción; Frustración; Resistencia; Reconocimiento y Recuperación

El temario se desarrolla en referencia a dichas estrategias, y constituyen su marco conceptual. De esta manera, se pretende lograr una mejor cohesión y comprensión de la extensa variedad de conceptos a tratar. Así al inicio de la asignatura se explica cómo funcionan los modelos como mecanismos generales. El alumno está preparado

para comprenderlas sin conocimientos previos específicos. El resto de los temas se relacionan con sus correspondientes modelos de defensa y ataque.

A través del enfoque basado en estrategias el alumno aprende a diferenciar y a valorar el uso de las técnicas de seguridad conociendo qué aporta cada una en el cuadro global de la seguridad del sistema y de la información de la empresa.

La asignatura tiene dos tipos de actividades prácticas. Por un lado, los alumnos realizan una serie de problemas de laboratorio, en los cuales configuran la seguridad de un entorno web utilizando los diferentes estándares que se ven en la teoría. Por otro lado, desarrollan un trabajo práctico en el cual utilizan técnicas de *hacking* para detectar vulnerabilidades de sitios webs. Este trabajo les permite a los alumnos conocer cuáles son los puntos débiles de un sistema que se convierten en amenazas de mayor riesgo de ocurrencia debido a que ya existen técnicas y herramientas de uso libre en internet que las detectan y explotan. Así entonces, estos casos tienen una mayor prioridad en ser solventados lo antes posible en un sistema real.

Este artículo presenta en la Sección 2, el diseño de la asignatura. En la Sección 3, se expone la metodología y en la 4 se presentan los resultados obtenidos. En la Sección 5 se comentan otros enfoques de centros donde se estudia Seguridad orientada a servicios y por último, en la Sección 6, se presentan las conclusiones.

2 La asignatura de Servicios y Seguridad

2.1 Contexto

Seguridad y Servicios es una asignatura optativa de 6 ECTS de cuarto año del grado en Informática y Servicios en la Escuela Universitaria de Informática Tomás Cerdá. Es obligatoria para obtener la mención de "Gestión de Servicios".

La asignatura pretende que se comprendan los aspectos a tener en cuenta para disponer de un sistema de servicios seguro. Se revisan los elementos de seguridad de identificación y autentificación, autorización, integridad, confidencialidad y privacidad, desarrollando las principales recomendaciones y técnicas actuales. Se basa en las soluciones estándares indicadas por las instituciones más relevantes en este ámbito como el *National Institute of Standards and Technology* (NIST) [3], *World Wide Web Consortium* (W3C) [5], *Advanced Open Standard for the Information Society* (OASIS) [6]. El alumno trabaja los principales conceptos de seguridad de servicios web fundamentales para gestionar, diseñar y desarrollar sistemas orientados a servicios, que por su naturaleza abierta a la red, están expuestos a amenazas y a vulnerabilidades, y requieren tener un nivel de seguridad adecuado. Se enseña la metodología para elaborar un modelo de amenazas *Threat Modeling* [4,5] para detectar, documentar vulnerabilidades y realizar una evaluación de riesgos.

2.2 Competencias

Del conjunto de competencias asociadas al grado de Informática y Servicios, la asignatura Servicios y Seguridad cubre las siguientes competencias específicas:

1. Evaluar sistemas hardware/software en función de un criterio de calidad determinado.
2. Determinar las soluciones tecnológicas adecuadas para la seguridad informática.
3. Analizar, identificar y definir los requisitos que se han de tener en cuenta para elaborar un plan de seguridad.
4. Aplicar las diferentes normativas sobre seguridad, protección de datos, etc., en todas aquellas situaciones que lo precisen.

En relación a las competencias transversales asociadas al grado, en la asignatura se trabajan la de gestionar (planificar) el tiempo y los recursos disponibles, y el desarrollo de estrategias de aprendizaje autónomo.

2.3 Objetivos y Temario

A continuación se describen los objetivos de aprendizaje de la asignatura, a partir de los cuales se desarrollan las competencias, se evalúan los resultados de aprendizaje y se elabora el temario.

Tabla 2 Objetivos por bloque temático

Bloque	Objetivos
Objetivos de la seguridad	Conocer los objetivos de la seguridad. Dimensiones. Tipos de ataques por cada capa de red OSI.
Estrategias de seguridad	Aprender los modelos de estrategia de ataque y de defensa que se utilizan actualmente para comprometer los sistemas informáticos.
Criptografía simétrica y asimétrica. Malware. Estándares de seguridad.	Reconocer los tipos de *malware*, su potencial de daño progresivo y masivo y técnicas de detección y de evitar sus daños cada vez en forma más proactiva. Conocer los algoritmos de flujo y bloque actuales de la Criptografía Simétrica. Ventajas y limitaciones. Criptografía e Infraestructura de clave pública. Protocolos y estándares. Ventajas y limitaciones. Aprender los principales estándares de seguridad de servicios web: SSL/TLS, XML-Security, WS-Security, etc. Modelos de funcionamiento. Herramientas que implementan estándares.
Metodologías de gestión de riesgos	Aprender metodologías de gestión de riesgos. Identificar vulnerabilidades y valorar amenazas. Realizar un modelo de arquitectura de seguridad.

El temario se desarrolla a partir de los objetivos de cada uno de los bloques indicados en la **Tabla 2** Objetivos por bloque temático en forma secuencial. Este programa está diseñado para ser desarrollado en un semestre de 6 ECTS, que corresponden a 150 horas de trabajo del alumno. La mitad son destinadas a trabajo autónomo. El trabajo dirigido y supervisado, 64 horas, se lleva a cabo en un total de 32 sesiones de 2 horas/sesión, que se realizan a lo largo de 16 semanas.

2.4 Enfoque basado en estrategias de ataque y defensa

Con el propósito de realizar una formación conceptual y comprender las técnicas de seguridad, utilizamos un enfoque basado en estrategias de defensa y ataque [2]. De este modo el alumno aprende a diferenciar y a valorar el uso de las técnicas de seguridad conociendo qué aporta cada una en el cuadro global de la seguridad del sistema. Los sistemas de defensa suelen aplicar en forma sistemática los controles disponibles en cada una de las capas, dejando así activos supervisados más de una vez mientras que otros no tienen control. Una visión estratégica global facilita que se apliquen controles en forma metódica para conocer qué aspectos están cubiertos y cuáles no, logrando un sistema más fuerte y posiblemente con menores costes de control.

Si bien los ataques se pueden producir en diferentes niveles y con múltiples técnicas y pudiendo ser internos o externos a la organización, siguen uno de los siguientes modelos representados en la Figura 1 - Estrategias de ataque.

a) Directo: El atacante atenta contra su objetivo sin utilizar servidores intermedios excepto los normales de encaminamiento. Son ejemplos de este tipo de ataque el correo no deseado, el envenenamiento de caché del DNS, o el encaminamiento con reglas de filtrado (*blackholing*).

b) Progresivo: El atacante usa una serie de servidores intermedios entre el punto de lanzamiento y su objetivo. Varios ataques siguen esta estrategia ya sea contratando servidores intermedios en el mercado negro o por el compromiso manual o automático de uno de éstos utilizando técnicas de *malware*.

c) Masivo: el atacante compromete un grupo de servidores y utiliza todos ellos para actuar contra el servidor objetivo. Este modelo se utiliza para ataques del tipo *Distributed Denial of Service* (*DDOS*) o para captura de tráfico del servidor de destino.

d) Dirección errónea: Se distrae a las técnicas de defensa. Puede ser un ataque enmascarado utilizando direcciones falsas o bien que se pretenda un ataque a otros servidores para distraer a la defensa. De esta manera los atacantes tienen más posibilidades de que el verdadero ataque no se detecte.

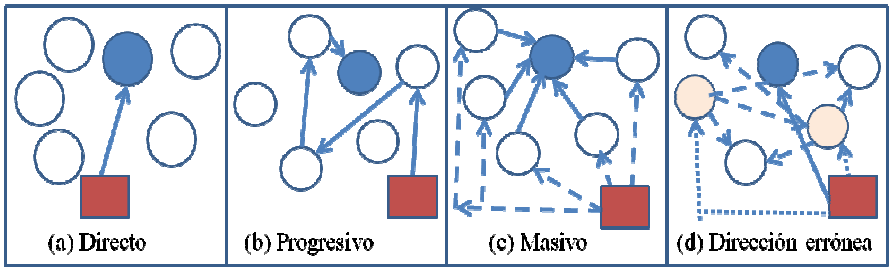

Figura 1 - Estrategias de ataque – Cuadro Rojo: Origen – Círculo Azul: Destino.

Las estrategias de defensa se aplican en diferentes capas de la red en forma de controles, de modo que si uno falla, pueda funcionar otro. Se basan en el arte de la guerra y se clasifican según sea el nivel de intromisión del atacante. En primer lugar se intenta evitar una incidencia inicial obstaculizando la identificación de los activos

valiosos. Luego, se trata de dificultar que el ataque avance y finalmente se intenta reconocer al adversario y recuperar el sistema. Están representadas en la Figura 2.

a) Decepción: Se trata que el atacante actúe contra un activo que no interese a la empresa, que no sea productivo para el ataque, que no sea un servidor crítico que tenga información confidencial. Puede utilizarse la técnica de *honeypot* utilizando máquinas virtuales con información falsa para confundir al atacante o un *tarpit* que responda a consultas de red con información incorrecta o incompleta.

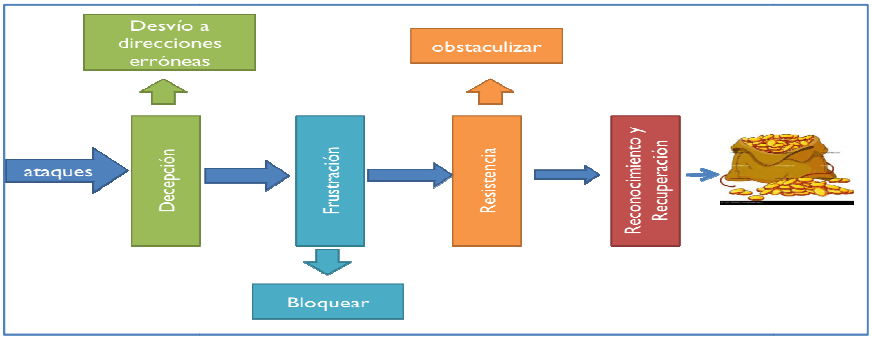

Figura 2 - Estrategias de defensa

b) Frustración: estas técnicas tienen como objetivo denegar el acceso inicial de un ataque. Se impide el ingreso a cualquier medio que pueda utilizarse. Por ejemplo, las listas de control de acceso en los enrutadores o los firewalls.

c) Resistencia: estas técnicas pretenden que un ataque no pueda progresar después de haber entrado al sistema. Limita la propagación de actividad en el ordenador o en la red. Requiere de una actuación más activa de los controles de seguridad, y mayor esfuerzo que las anteriores, aunque muchos de los métodos de la frustración pueden utilizarse, como control de puertos. Son ejemplos de técnicas de resistencia la encriptación o la segmentación de la red en zonas seguras.

d) Reconocimiento y recuperación: La idea es identificar al ataque lo antes posible y recuperar el servicio atacado. En primer lugar se ha de identificar el ataque y diagnosticarlo en términos de propósito, medios o impacto. Se pueden aplicar técnicas de comparación de patrones de tráfico o de detección de cambios de configuración. Luego, se han de recuperar los ordenadores y redes afectadas a un estado seguro. Se recomienda que la estrategia de recuperación esté relacionada con el diagnóstico, para asegurar que se guarden los datos necesarios para investigar el ataque y para minimizar los recursos perdidos durante el ataque.

3 Metodología docente

3.1 Actividades de aprendizaje

Los contenidos son trabajados en sesiones teóricas y sesiones de perfil práctico. Las sesiones teóricas buscan una participación activa del estudiante, y siguen el

temario presentado en la sección anterior. Los conceptos son expuestos en clases magistrales utilizando presentaciones que incluyen las referencias bibliográficas para que el alumno pueda profundizar más a través del trabajo autónomo. También se plantea a los alumnos la realización de actividades (algunas individuales, otras mediante trabajo cooperativo) como responder a preguntas, relacionar temas, lectura y debate de artículos de investigación, a través de las cuales el alumno reflexiona y asimila el tema tratado.

La Tabla 3 – Metodologías por bloque temático y su estrategia relacionada muestra la relación de las diferentes actividades que se realizan para conseguir los objetivos propuestos.

Tabla 3 – Metodologías por bloque temático y su estrategia relacionada

Bloque temático	Metodología	Estrategias relacionadas
Objetivos de la seguridad	Clases teórico/prácticas basadas en la guía de seguridad de servidores web de NIST [3].	-
Estrategias de seguridad	Clases teórico/prácticas de Modelos de estrategias de ataque y defensas basado en [2].	-
Criptografía simétrica y asimétrica.	Clases teórico/prácticas basadas en el material audiovisual publicado por el proyecto IntyPedia [6] y por el libro [7].	Defensa: frustración y resistencia
Malware.	Lectura de artículo [8] y debate grupal para tipos de *malware* e innovaciones en técnicas de detección.	Ataque
Estándares de seguridad.	Clases teórico/prácticas [4] - Lectura de artículos [9] [10] [11] [12] y debate grupal para profundizar sobre técnicas de ataques y defensa utilizadas actualmente.	Ataque/Defensa
Metodologías de gestión de riesgos	Clases teórico/practicas basadas en [4] y [5].	Defensa

En las sesiones prácticas, se plantean dos tipos de actividades: las sesiones de laboratorio, que se incluyen dentro de las actividades dirigidas, y el desarrollo de un trabajo práctico, una actividad supervisada que el alumno lleva a cabo de forma autónoma.

Sesiones de laboratorio

Se asignan cinco clases (10 horas) para realizar una serie de ejercicios de laboratorio en los cuales el alumno configura la seguridad de un servidor de aplicaciones web mediante el uso de SSL, generación y uso de certificados de servidor y de clientes y programación de aplicaciones y servicios web basada en java.

Para esta actividad es conveniente utilizar una plataforma consolidada que minimice las incidencias por errores, y que esté adoptada por un gran número de usuarios para que el alumno aprenda una herramienta usada en el ámbito profesional. Se utiliza una plataforma basada en *Netbeans*, *Glassfish* y servicios web *SOAP* y

ReST en Java. La configuración de servicios web en diferentes escenarios de seguridad, haciendo uso de certificados de clave pública en cliente y/o servidor se utiliza el documento publicado por *Oracle* [13].

Trabajo Práctico

Durante parte del tiempo asignado al aprendizaje autónomo los alumnos desarrollan un trabajo práctico (estimado en 25 horas) basado en técnicas de *hacking*, El propósito es que aprendan a proteger mejor los sistemas a través de conocer las técnicas que los atacantes utilizan para descubrir y atacar las vulnerabilidades de los sistemas web. Sabiendo qué herramientas están disponibles en internet en forma abierta, el profesional informático puede valorar y explicar mejor los riesgos de compromiso de servicio y de información si no se toman las medidas adecuadas. Como referencia para el desarrollo de este trabajo, utilizamos el libro de Web Hacking [14] entre otros recursos web de uso público que explican cómo utilizar paso a paso herramientas de detección de vulnerabilidades y como perpetuar ataques a distintos niveles: a servidores DNS, al protocolo HTTP, ataques del tipo *Cross-Site Scripting*, inyección SQL a base de datos, etc. Debido a que utilizar técnicas de *hacking* es un delito y por tanto no pueden realizarse sobre un sitio web sin tener autorización, proveemos a los alumnos de sitios web que pueden utilizarse para encontrar vulnerabilidades, de acuerdo con los administradores de dichos recursos.

3.2 Actividades de evaluación

Las actividades de evaluación de la asignatura consisten en:
a) Dos exámenes: que suponen un 40% de la nota final (20% cada prueba). El primero se realiza antes de la semana 8 (mitad del semestre), con el objetivo de que los alumnos estudien los conceptos básicos y así poder valorar la comprensión hasta ese momento. Al final del semestre, se realiza un examen de toda la asignatura. A través de estos exámenes se evalúan los resultados de aprendizaje relativos a las cuatro competencias de la asignatura.
b) Trabajo práctico: que supone el 30% de la nota de la asignatura, y a través del cual se evalúan los resultados de aprendizaje de las competencias 1 a 3.
c) Actividades prácticas en clases teóricas y laboratorio: que suponen el 30% de la nota de la asignatura, y a través de las cuales se evalúan los resultados asociados a las competencias 2 a 4.

4 Resultados Obtenidos

La presente propuesta se ha utilizado en el primer semestre del último curso académico 2014/2015. Al final del semestre, se realizó una encuesta, para saber la valoración del enfoque basado en estrategia por parte de los alumnos, en la que se preguntó ¿Cómo valoras el enfoque basado en estrategias de ataque y defensa? En una respuesta de 1 a 5, (5 es la máxima valoración), se obtuvo una media de 4.5, es decir, un 90%. En la encuesta participaron todos los alumnos. Sin embargo, los alumnos han indicado que se necesitaban más clases prácticas para llevar a cabo el trabajo de

hacking o bien con objetivos más concretos o actividades más acotadas. Sugirieron eliminar algunos temas o que ocuparan menos tiempo como por ejemplo el *malware*. Los trabajos prácticos presentados denotan que los alumnos han indagado mucho sobre herramientas de *hacking*, dando evidencias de que les motiva descubrir vulnerabilidades en sitios en servicio.

5 Servicios y Seguridad en otros centros educativos

La seguridad orientada a servicios web se estudia en otros centros nacionales. Presentamos aquí las principales similitudes y diferencias detectadas a partir de la información pública en internet. Cabe destacar que en todos los casos corresponden a asignaturas de 6 créditos y que la principal diferencia detectada es que no disponen de un enfoque basado en estrategias.

La Universidad de Valladolid en el grado de Ingeniería Informática de Servicios y Aplicaciones, imparte "Seguridad Informática" como asignatura obligatoria del 3er. curso[15]. Los contenidos son similares, incluso plantean prácticas de *hacking* para saber cómo defenderse. Sin embargo, no incluyen metodologías de gestión de riesgos.

En la Universidad de Sevilla se dicta "Seguridad en Sistemas Informáticos y en Internet" en el Grado en Ingeniería de Computadores [16], asignatura optativa de 4º curso. Si bien trata sobre protocolos de internet, en el bloque temático no se indica que se profundice en estándares de seguridad para servicios web.

En la Universidad de Zaragoza, en el Grado en Ingeniería de Tecnologías y Servicios de Telecomunicación, la asignatura de "Seguridad en redes y servicios" [17], es obligatoria del 3er. curso. Tiene un bloque temático similar, excepto que no se indica si el plan de seguridad se realiza con técnicas de *Threat Modeling*.

La Universidad Politécnica de Madrid, imparte "Seguridad en Redes y Servicios" en el Grado de Ingeniería Telemática, como obligatoria de 6 créditos en el 3er.curso [18]. En su temario dispone de un bloque que cubre la Legislación española sobre seguridad de la información y recomendaciones y auditorías. En nuestro grado, estos temas se ven en asignaturas como "Sociedad y legislación informática" y "Auditoría y Calidad de Servicios".

6 Conclusiones

Se ha presentado la metodología de la asignatura Seguridad y Servicios que se dicta como optativa en el cuarto curso del Grado de Informática y Servicios de la Escuela Universitaria de Informática Tomás Cerdá. La propuesta se basa en incluir un enfoque basado en estrategias de ataques y de defensa que facilite la comprensión de los temas estableciendo una relación entre estos y el correspondiente modelo en que se enmarca dicho tema. Ha tenido una buena aceptación por parte de los alumnos y hemos detectado que se han mostrado más motivados durante las clases. Siguiendo los comentarios de los alumnos, en el próximo curso, reestructuraremos el trabajo de *hacking* dando objetivos más concretos y mayor soporte.

Referencias

1. Boixader F, Guardiola J, Albert M, Ribas J. El Grado en Informática y Servicios. Una respuesta a la nueva demanda del contexto social. In: JENUI 2010. "XVI Jornadas de Enseñanza Universitaria de la Informática." Universidade de Santiago de Compostela. Escola Técnica Superior d'Enxeñaría; 2010:130–135..
2. Timothy J. Shimeall and Jonathan M. Spring. Introduction to Information Security: A Strategic-Based Approach. In: Elsevier; 2013:382..
3. Scarfone ASTWK. Guide to Secure Web Services Recommendations of the National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf.
4. Bertino E, Martino L, Paci F, Squicciarini A, Elisa Bertino, Lorenzo Martino, Federica Paci AS. Security for Web Services and Service-Oriented Architectures. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010. doi:10.1007/978-3-540-87742-4.
5. Suvda Myagmar, Adam J. Lee WY. Threat Modeling as a Basis for Security Requirements. In: Symposium on requirements engineering for information security (SREIS).Vol 2005.; :1–8.
6. Intypedia.: http://www.intypedia.com/.
7. Chwan-Hwa (John) Wu; J. David Irwin. Introduction to Computer Networks and Cybersecurity - CRC Press Book. (Press C, ed.).; 2013:1336..
8. Damshenas M, Ali Dehghantanha RM. A SURVEY ON MALWARE PROPAGATION, ANALYSIS, AND DETECTION. Int J Cyber-Security Digit Forensics. 2013;2(4):10–29..
9. Jensen M, Gruschka N, Herkenhöner R. A survey of attacks on web services. In: Computer Science - Research and Development.Vol 24.; 2009:185–197..
10. Chapman IM, Leblanc SP, Partington A. Taxonomy of cyber attacks and simulation of their effects. In: MMS '11 Proceedings of the 2011 Military Modeling & Simulation Symposium. Society for Computer Simulation International; 2011:73–80.
11. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl. 2011;34(1):1–11.
12. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci. 2014;80(5):973–993..
13. The WSIT Tutorial. http://docs.oracle.com/cd/E17802_01/webservices/webservices/reference/tutorials/wsit/doc/.
14. Berta S. Web Hacking. (Manuales USERS - Creative Andina Corp, ed.). RedUsers Usershop; 2013:320.
15. Universidad de Valladolid - Ingeniería Informática de Servicios y Aplicaciones. http://www.uva.es/opencms/consultas/planesestudios/guia?menu=3&codigo_plan=413&codigo_asignatura=40823&grupo=1&ano_academico=1314.
16. Universidad de Sevilla- Ingeniería de Computadores. http://www.us.es/estudios/grados/plan_204/asignatura_2040035#contenidos.
17. Universidad de Zaragoza - Ingeniería de Tecnologías y Servicios de Telecomunicación. http://titulaciones.unizar.es/asignaturas/30353/contexto14.html.
18. Universidad Politécnica de Madrid - Ingeniería Telemática.: https://www.euitt.upm.es/estudios/grado/telematica/fichas-de-asignaturas?codasig=53&curso_academico=2014&semestre=6&titulacion=59TL.