SANS

THE MOST TRUSTED NAME IN HANDS-ON INFORMATION & SOFTWARE SECURITY TRAINING & PROFESSIONAL CERTIFICATION

Community SANS Madrid

12–17 de MARZO 2012

SEC542: Web App Penetration Testing & Ethical Hacking

Tests de intrusión en aplicaciones web y hacking ético

FORMACIÓN IMPARTIDA EN CASTELLANO, CON MATERIAL EN INGLÉS, EN LAS OFICINAS DE VASS MADRID

"SANS permite formarse en técnicas y herramientas del mundo real que son útiles para la auditoría desde Internet"

– CALEB McCARY, THE BOEING COMPANY

VASS

Community SANS

SEC542:
Web App Penetration Testing & Ethical Hacking

12—17 DE MARZO, 2012 => 6-DAY COURSE • 6 CPE CREDITS PER DAY • LAPTOP REQUIRED

Sobre el curso

Este curso de nivel intermedio/avanzado enseña el arte de analizar y explotar aplicaciones web, con el objetivo de poder encontrar vulnerabilidades en las aplicaciones web de una organización antes de que lo haga un posible atacante. Mediante ejercicios prácticos y una meticulosa formación de manos de un instructor experimentado, se detalla una metodologìa para la realización de pruebas de intrusión de aplicaciones web dividida en cuatro fases: reconocimiento, mapeado, descubrimiento y explotación de vulnerabilidades.
Por ejemplo, se realizarán ataques de inyección SQL, profundizando en cómo los atacantes extraen datos sensibles, se utilizarán ataques de Cross-Site Scripting para controlar a clientes objetivo, y se explorarán muchas otras vulnerabilidades típicas de aplicaciones web en detalle, empezando por técnicas de descubrimiento efectivas a través de un proceso de análisis estructurado. A lo largo del curso se aprenderán todos los detalles asociados a cada ataque y su contexto, de forma que podrán ser aplicarlos de manera intuitiva en cualquier entorno y aplicación web. Al finalizar se dispondrá de los conocimientos para evaluar la seguridad de las aplicaciones web y descubrir las vulnerabilidades más comunes y críticas existentes en entornos web hoy en día.

***El curso será impartido en español, con el material en inglés**

DÍA 1: LA WEB DESDE EL PUNTO DE VISTA DEL ATACANTE

Visión general de la web desde la perspectiva del auditor de seguridad. Explorando los diferentes protocolos, servidores y clientes. Análisis de las distintas arquitecturas web. Descubriendo la gestión de sesiones web. Descripción de los diferentes tipos de vulnerabilidades web. Análisis del alcance, proceso, detalles y distintos tipos de pruebas de intrusión en aplicaciones web.

DÍA 2: RECONOCIMIENTO Y MAPEADO

Descubriendo la infraestructura de la aplicación web. Identificación de las redes, equipos y sistemas operativos. Configuración de SSL y sus debilidades. Explorando hosts virtuales y su impacto en la evaluación. Aprendizaje de métodos para identificar balanceadores de carga. Descubrimiento de la configuración del software empleado. Explorando fuentes de información pùblicas. “Google hacking”. Herramientas de recolección de la estructura y enlaces web (spiders). Programación de scripts para la automatización de peticiones web. Diagramas de flujo de la aplicación. Análisis de relaciones dentro de una aplicación. El lenguaje JavaScript desde el punto de vista del atacante.

DÍA 3: DESCUBRIMIENTO DE VULNERABILIDADES EN EL SERVIDOR

Aprendizaje de métodos para descubrir vulnerabilidades. Fugas de información. Técnicas de recopilación de usuarios. Inyección de comandos de SO. Inyección SQL e inyección SQL ciega. Explorando técnicas de ataque para distintas bases de datos. “Cross-Site Scriptingî. Falsificación de peticiones mediante “Cross-Site Request Forgery”. Análisis de sesiones web. Técnicas y herramientas de “fuzzing”. Discusión sobre los diferentes tipos de interfaces de las aplicaciones web.

DÍA 4: DESCUBRIMIENTO DE VULNERABILIDADES EN LOS CLIENTES

Aprendizaje de métodos para analizar código cliente: Flash, Java, etc. Explorando applets y objetos maliciosos. Descubriendo vulnerabilidades en aplicaciones web a través de sus componentes cliente. Atacando WebServices y aplicaciones web basadas en web 2.0 y AJAX, y como afectan éstos a las pruebas de intrusión. Los lenguajes Python y PHP desde el punto de vista del atacante. Ampliando habilidades para extender las herramientas que utilizamos.

DÍA 5: EXPLOTANDO VULNERABILIDADES

Aprovechando las vulnerabilidades descubiertas en fases previas. Explorando métodos para convertir los navegadores web en “zombies”. Utilización de “zombies” para escanear puertos y atacar redes internas. Explorando “frameworks” de ataque: AttackAPI, BeEF, o XSS-Proxy. Sacando provecho de los ataques para obtener acceso al sistema. Cómo expandir los ataques a través de la aplicación web. Entendiendo los métodos para interactuar con un servidor a través de inyección SQL. Robo de “cookies” y secuestro de sesiones. Ejecución de comandos de SO a través de vulnerabilidades en aplicaciones web. Ejemplo práctico de un escenario de ataque.

DÍA 6: “CAPTURE THE FLAG” (CTF)

El ùltimo día de clase, los asistentes tendrán acceso a una red real y podrán completar una prueba de intrusión en su totalidad. El objetivo de esta competición de tipo “captura la bandera” (CtF) es que los asistentes exploren las técnicas, herramientas y metodología aprendidos durante los cinco días previos del curso. Será posible aplicar las ideas y métodos estudiados contra diferentes aplicaciones web objetivo. Al finalizar el ejercicio, los participantes presentarán los resultados y la metodología que han utilizado para completar la prueba. Durante el reto se dispondrá de la máquina virtual basada en Samurai WTF, empleada durante todo el curso, así como para el análisis y realización de pruebas de intrusión reales.

Lugar de impartición de la formación

VASS Consultoría de Sistemas
Avda. Doctor Severo Ochoa, 25 - 1ª Planta.
28100 Alcobendas (Madrid)
http://www.vass.es

Certificación oficial SANS GIAC Web Application Penetration Tester (GWAPT)
http://www.giac.org

Biografía del instructor

RAÚL SILES
– SANS INSTRUCTOR –

Raúl Siles es fundador y analista de seguridad de Taddong. Sus más de 10 años de experiencia ofreciendo servicios y soluciones avanzadas de seguridad incluyen diseño y revisión de arquitecturas de seguridad, pruebas de intrusión, investigación de incidentes, análisis forense, evaluaciones de seguridad e investigación de seguridad en nuevas tecnologías, como aplicaciones web, wireless, honeynets, virtualización, dispositivos móviles y VoIP. Raúl es uno de los pocos profesionales que han obtenido la certificación GIAC Security Expert (GSE). Es autor e instructor de cursos del SANS, ponente habitual en conferencias de seguridad, autor de libros y artículos de seguridad, y contribuye a proyectos de investigación y open-source. Le encantan los retos de seguridad, y es miembro de organizaciones internacionales, como el Honeynet Project o el Internet Storm Center (ISC). Raúl tiene una Ingeniería Superior Informática por la UPM (España) y un master de postgrado en seguridad y comercio electrónico. Más información en http://www.raulsiles.com.

Información de registro

DETALLES DEL REGISTRO: http://www.sans.org/info/89409
COSTE: SEC542: WEB APP PENETRATION TESTING & ETHICAL HACKING
Si efectúa el pago antes del 1 de Febrero: **2.750€** ||| Si efectúa el pago antes del 15 de Febrero (incluido): **2.950€**
Si efectúa el pago después del 15 de Febrero: **3.250€**
CONTACTO SANS: Barbara Basalgète, SANS EMEA Director: +33 6 71 48 24 01 | bbasalgete@sans.org
CONTACTO VASS: Marlene Sánchez: +34 91 662 34 04 | marlene.sanchez@vass.es
Rafael Ausejo Prieto: rafael.ausejo@vass.es

Información sobre el programa "Community SANS EMEA"

La modalidad de enseñanza "Community SANS" en EMEA (Europa, Oriente Medio y África) ofrece los cursos más populares de SANS en tu comunidad e idioma local. Se emplea para ello un formato de clase reducido, con no más de 25 estudiantes. Los instructores son seleccionados minuciosamente de entre los mejores candidatos del programa "local mentor" o son expertos de seguridad cualificados que han superado un proceso riguroso de selección denominado "el tribunal de la muerte". El material del curso se imparte en días consecutivos, siendo los contenidos exactamente los mismos que se imparten en las conferencias SANS de mayor tamaño. Además del excelente material asociado al curso, no sólo podrás aplicar las habilidades y conocimientos adquiridos en clase tan pronto vuelvas a la oficina, sino que también podrás seguir en contacto con los colegas de tu comunidad que conociste durante el curso, con los que compartes inquietudes e intereses.

– EXCEPCIONALMENTE, ESTE CURSO SERÁ IMPARTIDO POR EL INSTRUCTOR OFICIAL DEL MISMO EN EMEA, Y MIEMBRO DE TU COMUNIDAD LOCAL –

SANS y VASS Consultoría de Sistemas, empresa que opera en el mercado español de Seguridad de la Información, han firmado un acuerdo de colaboración para la introducción en España de los cursos SEC542.

Acerca de SANS

SANS es la mayor y más reconocida fuente de información acerca de formación en seguridad y certificación en el mundo. SANS también desarrolla, mantiene, y provee –sin coste alguno- una gran colección de documentos relacionados a la seguridad de información, y opera el sistema de alerta temprana Internet Storm Center. El SANS Institute (System Administration, Network and Security) fue establecido en 1989 como una organización de colaboración de educación e investigación y desarrollo. A día de hoy, el programa incluye a más de 165.000 profesionales de la seguridad en todo el mundo. Profesionales, desde auditores y administradores de redes hasta gerentes de sistemas de información comparten sus experiencias y buscan soluciones conjuntas para los distintos retos a los que se enfrentan. El espíritu detrás de SANS es la cooperación entre los miles de profesionales de la seguridad a lo largo de todas las organizaciones globales, corporaciones, universidades, etc. para el beneficio de toda la comunidad. **http://www.sans.org**

Sobre VASS

VASS, Valor Añadido en Soluciones y Servicios, es una empresa 100% privada, particular e independiente, integradora de productos y servicios con un alto nivel de especialización e innovación. Desde 1999, la estrategia de VASS ha sido seleccionar aquellas áreas de negocio de valor estratégico (CRM, eBusiness, BI, Microsoft, ERP, Innovación, Explotación de Sistemas y Seguridad de la Información) apostando en cada una por las tecnologías que consideramos líderes. Sobre estas tecnologías construimos equipos de alta especialización y dotamos al mercado de un modelo de éxito que consiste en la combinación de una empresa ágil, cercana y flexible pero con un profundo conocimiento y dominio de la tecnología.
http://www.vass.es