Programa del Curso:

Seguridad en el Desarrollo Web

Curso de seguridad informática especialmente pensado para los profesionales del mundo del desarrollo web. Expertos en seguridad nos guiarán a través de asuntos críticos que cualquier desarrollador o diseñador debe conocer para desenvolverse en la profesión. No nos quedamos simplemente en el conocimiento teórico, ahondaremos en la práctica para que los estudiantes puedan aplicar el conocimiento en su día a día.

Bloque 1- Introducción a la Seguridad Informática

Jueves 22 de Enero - Cibercrimen - Gabriel Lazo

Repaso del mundo del cibercrimen, una industria que mueve millones de dólares en fraudes, robos, estafas y extorsiones. Conoceremos los métodos que utilizan para hacerse con la información y control de equipos.

Bloque 2- Seguridad en clientes y servidores

Viernes 23 de Enero - Servidores Apache y DoS ¿Ataques o mala configuración? - David Hernández (Dabo)

Los ataques de Denegación de Servicio (DoS), siguen siendo uno de los quebraderos de cabeza más importantes en materia de seguridad con ejemplos recientes como Sony y su PlayStation Network o Microsoft y Xbox Live. En ocasiones, debido a configuraciones ineficaces, incluso con pocas peticiones/recursos es posible tumbar un servidor con recursos a nivel de Red, CPU o RAM. En esta sesión repasaremos varias opciones esenciales de Apache para evitar picos de tráfico alto puntuales o DoS a pequeña escala que deriven en una denegación de servicio, así como todos los problemas consecuencia de los “cuellos de botella”. Además ayudaremos a que las aplicaciones web se ejecuten más rápido. También se implementarán varias herramientas útiles para paliar los ataques.

***Lunes 26 de Enero* - Servidores GLAMP, ataques y defensas básicas - David Hernández (Dabo)**

Uno de los grandes problemas de un sistema GLAMP (GNU/Linux, Apache, PHP y MYSQL) según se instala, es el grado de exposición frente a múltiples vectores de ataque y revelación de información debido a configuraciones por defecto que deben ser necesariamente modificadas. En esta sesión aprenderemos a poner en marcha medidas de seguridad para proteger al sistema de ataques de fuerza bruta, se implementará un Firewall por Software, sistemas de detección y prevención de intrusos (IDS / IPS), control de archivos de registro (logs), además de repasar cuestiones de seguridad en SSH, Apache, PHP, etc. todo ello de un modo práctico, desde el punto de vista del posible atacante y de quien protege el Servidor. Realizaremos ataques y corregiremos esas posibles brechas de seguridad en tiempo real.

Martes 27 de Enero - Seguridad en Servidores- Rafael Bucio

Seguimos conociendo amenazas comunes que puede sufrir un servidor conectado a Internet. Aprenderemos a monitorizar los servidores y a protegerlos frente a este tipo de ataques maliciosos evitando que se conviertan en un blanco fácil para cualquier tipo de atacante.

Miércoles 28 de Enero - Client Side Web Vulnerabilites - Camilo Galdos

La seguridad de un sitio web no depende solo de los servidores y sistemas operativos, sino también del desarrollo. Conoceremos las vulnerabilidades comunes "client-side" en aplicaciones web y las claves para proteger el desarrollo del lado del cliente (Javascript, HTML5, actionscript, entre otros).

Jueves 29 de Enero - Python para Pentesters - Camilo Galdos

Aprenderemos a hacer fingerprint (primera etapa de un pentesting: buscar subdominios e información de la página) y vulnerability assesment (búsqueda de vulnerabilidades a nivel de la página web). Todo usando python como lenguaje de programación.

Viernes 30 de Enero - Python para Pentesters II- Camilo Galdos

Continuamos en una segunda sesión dedicada a Python para Pentesters y exploiting o explotación de las vulnerabilidades encontradas.

Bloque 3- Pruebas específicas de seguridad

Lunes 2 de Febrero- PHP seguro - Florencio Cano

En esta sesión romperemos todos los mitos de la seguridad de PHP, explicaremos cuales son los principales errores o detalles por los que se dice PHP es un lenguaje inseguro y daremos las claves para mantener un estándar de calidad al momento de desarrollar una aplicación web.

Martes 3 - Pruebas de Penetración contra Aplicaciones Web - Alonso Caballero

Explicaremos las fases del proceso de pruebas de penetración contra aplicaciones web de forma que podamos mitigar sus efectos. Conoceremos la perspectiva mental del atacante. Las partes de una Prueba de Penetración y la definición de su alcance. El reconocimiento y mapeo del proceso con los que obtener los fundamentos necesarios para controlar la aplicación. El descubrimiento de debilidades dentro de las aplicaciones y el mapeo de los vectores de ataque a utilizar contra la aplicación y el lanzamiento de ataques planificados.

Miércoles 4 de Febrero- José Moruno - HoneyPots

Aprenderemos lo que es un HoneyPot y cómo podemos sacar ventaja a esta herramienta de seguridad. Además examinaremos la información que nos arroja en general y cómo podemos interpretarla para nuestro beneficio.

Jueves 5 de Febrero - Santiago Rodriguez - Firewall para aplicaciones web

En esta sesión aprenderemos a instalar y configurar el popular firewall open source de aplicaciones web modSecurity. Lo usaremos para asegurar el acceso a una web hecha en WordPress. A lo largo de la ponencia se demostrarán diversos ejemplos de ataques reales y cómo podemos defendernos de ellos por medio del firewall de aplicaciones web.

Más información en EscuelaIT

Se pueden consultar las dinámicas y ponentes de este curso de seguridad para el desarrollo web desde la propia página de EscuelaIT:

http://escuela.it/cursos/seguridad-en-el-desarrollo-web/

Para resolver cualquier tipo de duda se puede contactar con nosotros en cursos@desarrolloweb.com