CURSO AVANZADO DE SEGURIDAD Y METODOS DE HACKING EN SISTEMAS INFORMÁTICOS. NIVEL 2

OBJETIVO DEL CURSO: El curso pretende llevar a los alumnos una ampliación de conocimientos en el campo de las técnicas de intrusión y hacking a sistemas, así como en la metodología del correcto endurecimiento (hardening) y análisis de la seguridad de sistemas Windows/Linux.

Se trabajará sobre el modulo dedicado a inyecciones de código SQL convencionales: su compresión, detección, explotación y prevención en aplicaciones. Aprenderán sobre ataques más sofisticados mediante inyección Blind SQL: su comprensión, detección, explotación y prevención. Los asistentes conocerán y practicaran métodos y técnicas utilizadas para la ruptura de seguridad en el punto final, técnicas de accesos a bases de datos de distintos motores BBDD con el fin de acceder a datos sensibles de una empresa o información confidencial de usuarios.

Modulo 1: Ampliación de conocimientos en metodología de la intrusión a sistemas (ataques a usuarios finales y anonimato)

Dispositivos Maliciosos

- Problemas de seguridad en el punto final.
- Selección y finalidad de cada una de las herramientas a integrar en el dispositivo.
- Procedimiento en la generación de dispositivos USB malignos indetectables.
- Dificultades en su configuración.
- Construcción del USB.
- Ventajas e inconvenientes en su funcionamiento.

Técnicas de Anonimato con TOR

- El proyecto Onion Router.
- Servidores Tor.
- Detección del uso de Proxies.
- Configuración de Tor en sistemas Windows.
- Configuración de Tor en sistemas Linux.
- Los ficheros de configuración y su uso.
- Generando cadenas tor modificadas por el usuario.
- Tor no es tan anónimo, detección del uso de Tor.

Modulo 2: Auditoria de los sistemas y herramientas de diagnostico y verificación de actividades.

Endurecimientos y búsqueda de evidencias en de sistemas Windows/Linux

- Seguridad, herramientas y técnicas recomendadas en sistemas Windows.
- Seguridad, herramientas y técnicas recomendadas en sistemas Linux.
- Herramientas para búsqueda de evidencias en servidores y ordenadores afectados.
- Realización de ejercicios prácticos con las herramientas analizadas.

Modulo 3: Vulnerabilidades e inyección de código SQL

Aprendiendo sobre el problema (inyecciones SQL).

- Introducción a TSQL
- Aprendiendo SQL orientado a la inyección de código.
- Entendiendo porque la aplicación es vulnerable a la inyección de código.
- Localización y análisis de la fisura.
- Explotación del bug.
- Inyecciones de código básicas.
- Analizando y comprendiendo inyecciones avanzadas.
- Recomendaciones a seguir para minimizar riesgos.

Prácticas de inyección SQL

- Herramientas de auditoría y detección de vulnerabilidades de inyección de código
- Uso de herramientas e interpretación de resultados.
- Herramientas para la realización de ataques (SQL Ninja a fondo).
- Trabajos sobre una aplicación Web dinámica vulnerable.
- Inyecciones de código manuales sobre la aplicación y su base de datos.

Técnicas de Blind SQL

- Profundizando en el problema.
- Aprendiendo como funcionan los ataques ciegos SQL.
- Entendiendo porque la aplicación es vulnerable a la técnica.
- Metodología paso a paso de cómo se realizan las inyecciones.
- Utilización de proxies para realizar inyecciones.
- Trabajos sobre una aplicación Web dinámica vulnerable.

- Realización paso a paso de inyecciones blind sql sobre distintos motores de bases de datos.

Características de los módulos:

Herramientas y materiales que se utilizaran durante los módulos del curso.

- Herramientas on line
- Herramientas para la generación de dispositivos.
- Herramientas de auditoría de inyecciones SQL.
- Herramientas para la generación de ataques SQL

Documentación:

El curso incluye documentación digital sobre los módulos del curso así como CD Rom para cada alumno como complemento a su formación con herramientas utilizadas a lo largo del curso.

Profesores titulares del curso:

Antonio Ramos Varón.

Jacinto Grijalva González.

Ruben Martínez Sánchez