WHITE HAT ACADEMY

"Para detener al enemigo, tienes que conocer sus métodos"

TACTICAL EXPLOITS LAB

¿Estás listo para enfrentar a los atacantes?

Por primera vez en MÉXICO, el curso

TACTICAL EXPLOITS LAB

En la mente de un Hacker

Los cursos tradicionales de seguridad se enfocan en la revisión exhaustiva y superficial de una gran cantidad de herramientas, sin explotar su potencial táctico y sin entender los conceptos fundamentales. Por lo tanto, no se domina a nivel de hands-on una Metodología exitosa de penetración.

Este Curso está enfocado en el estudio de una Metodología de desarrollo de exploits del tipo Buffer Overflow. Se cubren las diferentes fases del proceso, desde el descubrimiento de una vulnerabilidad de día cero hasta la codificación exitosa de un código que explote la vulnerabilidad en cuestión. Es la forma en la que trabajan los hackers reales, por eso es importante entender sus métodos. Utilizamos como Framework de ataque a BackTrack, que es la distribución más reconocida mundialmente de pentest.

Este conocimiento permitirá a los administradores de sistemas y redes la adopción de una estrategia exitosa de defensa a profundidad en sus organizaciones.

Informes: (55)56815921 **capacitacion@whitehatconsultores.com**

WHITEHAT ACADEMY

Conoce la ultima version del prestigiado curso estrella de WHITEHAT ACADEMY: TACTICAL EXPLOITS LAB
impartido con gran éxito a las empresas más importantes a nivel nacional, donde se muestra el poder de la Seguridad Tactica, con laboratorios sobre sitios REALES, analizando las técnicas mas modernas de ataque y contradefensa en seguridad de sistemas y redes.

Incluye gran numero de horas dedicadas a laboratorios hands-on, totalmente rediseñados, y con los mejores kits de ataque actualizados y efectivos, incluyendo lo mejor de los congresos black hat a nivel internacional, así como casos reales de hacking en México.

Módulo 1. Hackeo Ético

El participante entenderá los conceptos y códigos de conducta requeridos para usar la metodología de penetración avanzada y su compromiso con la legalidad en el uso de la misma.

Módulo 2. BackTrack

BackTrack es el Framework de penetración más avanzado y más utilizado en todo el mundo, tanto por los hackers como por los profesionales de la seguridad.
En esta sección se revisarán los fundamentos de esta poderosa distribución de Linux.

Módulo 3. Básicos de scripting para el profesional de Seguridad

Lenguajes Perl y Python, que son necesarios para investigar vulnerabilidades de seguridad. Se efectuarán ejercicios básicos y su aplicación a la seguridad.

Módulo 4. Básicos de Assembler para win32

En esta sección se dará una introducción al lenguaje ensamblador (assembler) para el procesador Intel y Windows. La revisión está enfocada a tópicos relevantes a la seguridad, como:

* Registros más importantes
* Stack y Heap
* Registro eip
* Assembler y compilers
* shellcodes

Módulo 5. Debuggeando aplicaciones en Windows

En esta sección se aprenderá a utilizar el debugger (OllyDbg, Immunity Debugger) y algunas otras herramientas para analizar el estado del stack, la memoria del sistema y los registros más importantes del procesador en el contexto de la seguridad de los sistemas y entender cómo funciona la magia del buffer overflow.

Informes: (55)56815921 **capacitacion@whitehatconsultores.com**

Taller de debuggeo de aplicaciones

Módulo 6. Fuzzing

Un fuzzer es un programa que intenta descubrir vulnerabilidades de seguridad mediante el envío de entradas aleatorias a los programas. En estas condiciones, si el programa contiene una vulnerabilidad, el programa puede lanzar una excepción, interrumpir la aplicación o enviar un mensaje de falla. Es el primer paso en la secuencia de descubrimiento de una vulnerabilidad y su posterior explotación. En este módulo se aplicarán algunas herramientas de fuzzing para descubrir aplicaciones vulnerables.

Taller de desarrollo de fuzzers.

Módulo 7. El poder de MetaSploit

En este módulo se aprenderá a dominar el framework de open source más avanzado para creación, investigación y utilización de Exploits. Se mostrará su aportación en el proceso de desarrollo de un exploit.

Módulo 8. Ciclo de desarrollo de un Exploit desde cero

En este módulo se revisará mediante ejemplos el ciclo completo de desarrollo de un Exploit, desde el descubrimiento de la vulnerabilidad del tipo Buffer Overflow en una aplicación hasta la creación exitosa de un código que la explote.

* Fuzzing
* Debugging el aplicativo
* Stack/Heap Buffer Overflow Básico en win32
* Creación de Exploits usando MetaSploit
* Uso de payloads
* Uso de NOPS
* Uso de opcodes and "jump to register"
* Filtraje de caracteres
* Codificación de shellcodes
* Técnicas especiales adicioales

Módulo 9. Trabajando con exploits públicos

En esta sección se aprenderá a utilizar y modificar algunos exploits disponibles en sitio públicos como exploit-db a efecto de hacerlos operables, portables a otras plataformas o cambiar el efecto final sobre el sistema atacado mediante la manipulación del payload.

CERTIFICACIONES DE LOS INSTRUCTORES

Todos nuestros cursos son impartidos por un equipo completo de especialistas en los diversos tópicos tratados y con diversas certificaciones de la industria a nivel internacional, así como practicantes de las mejore metodologias y mejores practicas de seguridad, con gran experiencia probada en casos reales de ciber crimen e incidentes informáticos.

Fechas y Horarios de los Cursos: solicitar informes

REQUISITOS

Laptop Windows XP+, con al menos 1 GB RAM y al menos 8GB espacio en HD.
Conocimientos de intermedios de Linux.
Conocimientos de Networking y Protocolos.

Comprometerse a usar la información en forma ética y legal, sólo para actividades de defensa empresarial o personal.

INVERSION

Solicitar informes

Como parte del Curso, te entregaremos una Carpeta conteniendo toda la información analizada, así como un Diploma Oficial de Asistencia. Asimismo, no solamente te llevarás las herramientas utilizadas, sino todo una máquina virtual del Framework de ataque, totalmente operativo.

Informes: (55)56815921 capacitacion@whitehatconsultores.com