WHITEHAT ACADEMY

"Conoce al enemigo, prepárate para el ataque"

¿Le confiarías una transacción bancaria a la RED segura de tu organización?
¿Estás listo para enfrentar a los atacantes?
¿Cansado de intentar aprender seguridad por medio de slides de power point o por coleccionar una gran cantidad de herramientas?
¿Quieres aprender las modernas tácticas de hackeo EN VIVO?

Por primera vez en México, el curso

MASTER TACTICAL HACKING

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 la a nivel de hands-on una Metodología exitosa de penetración.

Conoce la última versión del curso de WHITEHATACADEMY:
MASTER TACTICAL HACKING impartido con gran éxito a las empresas más importantes a nivel nacional, donde se muestra el poder de la Seguridad Táctica, con laboratorios sobre sitios reales, analizando las nuevas técnicas de ataque y contra defensa en seguridad de sistemas y redes.
Incluye gran número de horas dedicadas a laboratorios hands-on totalmente rediseñados y con los mejores kits de ataque y efectivos, así también, incluye lo mejor de las conferencias Hacker a nivel internacional así como casos reales en México.

Este Curso está enfocado a la explotación táctica de los sistemas, así como la revisión de los conceptos fundamentales.
Se analizará una exitosa metodología de pentest avanzada, con foco en laboratorios REALES, que garantizan un dominio práctico de las técnicas reales de ataque. Utilizamos como Framework de ataque a BackTrack, que es la distribución de pentest más reconocida mundialmente.

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

INSTRUCTORES CERTIFICADOS EN EL ARTE DE LA SEGURIDAD OFENSIVA

Informes: (55) 5681 5921 capacitacion@whitehatconsultores.com

WHITEHAT ACADEMY

"Conoce al enemigo, prepárate para el ataque"

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. Metodología de Tactical Hacking

Se revisará la Metodología de Master Tactical Hacking desde el punto de vista de un atacante.

Módulo 3. 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 4. Open Source Intelligence

Se revisarán los métodos tácticos más exitosos a la hora de investigar y obtener información pública de la víctima. Incluye el uso de las mejores herramientas minería de datos públicos.

- Técnicas de minería de datos públicos
- Uso de DNS
- Uso de Google
- Uso de maltego
- Laboratorios hands-on

Módulo 5. Uso de netcat

Netcat es la navaja suiza que debe estar presente en todo toolkit de seguridad. Aquí se enseñará su uso, desde usos básicos hasta usos avanzados.

- Conexión a puertos TCP/UDP
- Escuchando en puertos TCP/UDP
- Transferencia de archivos
- Shells remotos con netcat
- Otros usos de netcat
- Laboratorios hands-on

Módulo 6. Escanners de puertos

Dentro de la secuencia de ataque, la fase de escaneo es parte esencial de toda metodología de ataque. Un buen reconocimiento de los puertos y servicios expuestos en los sistemas es requisito indispensable para la creación de un plan de ataque exitoso.

- nmap
- Laboratorios hands-on

Módulo 7. Ataque a la Capa 2 y sniffers avanzados

La seguridad de la capa 2 de las redes Ethernet es un tema frecuentemente ignorado por los especialistas en redes, lo que hace de estos ataques los más peligrosos y omnipresentes en todas las redes LAN. En esta sección se revisarán las amenazas más comunes, como arp spoofing en redes switcheadas, secuestros de sesión sobre diversos protocolos, así como el terrible ataque de hombre en el medio y se demostrará porqué no se deben confiar transacciones electrónicas a la mayoría de las redes actuales.

- Arp spoofing (arp poissoning)
- Sniffeando redes switcheadas
- Secuestros de sesión sobre Telnet, ftp
- Ataques de Man-In-The-Middle sobre la red interna
- Ataque MiTM-SSH y MiTM- SSL
- Uso avanzado de ettercap
- Ataques a protocolos de voz: VoIP y IPTel
- Laboratorios hands-on

Informes: (55) 5681 5921 capacitacion@whitehatconsultores.com

WHITEHAT ACADEMY

"Conoce al enemigo, prepárate para el ataque"

Módulo 8. Técnicas avanzadas de crackeo de passwords

Las técnicas de captura y crackeo de passwords han avanzado a ritmos espectaculares en los últimos años, de tal manera que en un gran porcentaje de intentos, es posible capturar y comprometer las credenciales de administrador o de root en los sistemas atacados. Esta sección ofrece al profesional una actualización en dichas técnicas avanzadas que es necesario conocer a efecto de implantar contramedidas que mitiguen su efecto.

- sniffers
- pwdump
- Cain
- John the Ripper
- Rainbow Tables
- Laboratorios hands-on

Módulo 9. Ataques de fuerza Bruta a protocolos

Los ataques de fuerza bruta a protocolos son hoy en día una de las vías más exitosas en el camino de comprometer a un sistema para el atacante decidido. El profesional de la seguridad debe dominar dichas tácticas a efecto de implantar contramedidas, así como para implantar procesos de auditoría interna sobre los sistemas a defender.

- Ataque a servidores SNMP
- Ataque a servidores Telnet, FTP
- Ataque a servidores POP3, IMAP
- Ataque a servidores CISCO telnet
- Ataque a servidores SSH
- Ataque a servidores web-Basic Auth
- Laboratorios hands-on

Módulo 10. Ataque a sitios web

Los ataques a sitios web constituyen el vector número 1 de intrusión y compromiso a los sistemas públicos de Internet y debido a la visibilidad de los mismos, su efecto puede ser devastador, pues no solamente se pueden comprometer los activos, sistemas y procesos de negocio de la organización sino peor aún, un ataque exitoso puede afectar a la reputación y marca de la organización. Y resultan más espectaculares por el hecho de que dichos ataques se efectúan a través de firewalls y equipos de filtraje perimetrales.

- Google hacking
- Unicode attack
- Traversal directory
- Cross Site Scripting (XSS)
- SQL Injection
- Local/Remote File Inclusions
- Laboratorios hands-on

Informes: (55) 5681 5921 capacitacion@whitehatconsultores.com

WHITEHAT ACADEMY

"Conoce al enemigo, prepárate para el ataque"

Módulo 11. El poder de MetaSploit

El proyecto de Open Source MetaSploit Project provee al Profesional de la Seguridad de un potente framework de desarrollo y ejecución de código de exploits contra sistemas vulnerables y ha sido considerado como el mejor de su tipo. Incluye no solamente la posibilidad de ejecutar código de ataque de calidad, sino también un ambiente completo de desarrollo e investigación para los profesionales de hackeo ético. En su base de conocimientos se incluyen algunos de los exploits más sofisticados de la industria y es una herramienta de clase mundial que todo profesional serio de la seguridad debe dominar.

MetaSploit Framework
- Uso de Metasploit
- MSFCLI
- MSFCONSOLE
- MSFWEB
- Uso de payloads:

Meterpreter
PassiveX
VNC payload
Impurity
- Laboratorios hands-on

Otros frameworks de pentest comerciales

Requisitos

Conocimientos de Networking y Protocolos. Conocimientos de intermedios de Linux. Recomendamos el Curso Tactical Linux & BackTrack.

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

MASTER TACTICAL HACKING está dirigido a los responsables de áreas como Sistemas, Telecomunicaciones, Redes, Desarrollo de aplicaciones, personal de Soporte Técnico, administradores de Base de datos, administradores de la seguridad, así como a Consultores de Seguridad.

Como parte del Curso, te entregaremos una Carpeta conteniendo toda la información analizada en el mismo, así como un Certificado Oficial de Asistencia. No solamente te llevarás las herramientas utilizadas, sino toda una máquina virtual del Framework de ataque.

Cupo limitado a 10 personas máximo.

Costo por persona: Solicitar informes

Informes: (55) 5681 5921 capacitacion@whitehatconsultores.com