

Ethical Hacking Seminar

EH001

La permanente exposición al riesgo de robo, extravío, alteración o delitos sobre la información confidencial de las empresas, situando a estas en una posición bastante delicada y crítica, por lo que se hace imperioso conocer las herramientas y metodologías utilizadas por los mismos hackers y posibles atacantes, para poder contrarrestarlas eficazmente.

El seminario de Ethical Hacking brinda un amplio conocimiento y práctica real en equipos de las más actuales herramientas y técnicas de ataque y defensa, permitiéndonos consecuentemente actuar profesionalmente sobre el tema. Tiene un enfoque totalmente práctico, basado en distintos tipos de ataques y sobre diversos entornos.

¿A quién esta dirigido?:

Especialmente a Profesionales de áreas de Sistemas, Consultores de Tecnología, Auditores Internos y Externos de Sistemas, Profesionales, Administradores y Responsables de Seguridad Informática.

Material:

Al finalizar el entrenamiento se entregará un CD con las presentaciones, manuales, las herramientas utilizadas durante el seminario y herramientas adicionales complementarias (52 herramientas).

Certificado:

Se entregarán certificados de asistencia a todos los participantes

Duración:

2 Días (16hs)

Requisitos:

Conocimientos Básicos de Tecnología.

Seminario taller 100% Práctico, un participante por computador

Temario a Desarrollar

• Módulo I:

- Situación Actual
- Tendencias Actuales. Dónde Apuntan los ataques hoy
- Riesgos y Componentes asociados. Nuevos Riesgos
- Datos estadísticos

• Módulo II: Metodologías de Penetration Testing - Ethical Hacking

Conceptos Generales

- Tipos de Test. Detalles y alcances
- Etapas metodológicas
- Metodologías Internacionales camino al Estándar

• Módulo III: Hacking

- Conoce al enemigo. Tipificación de perfiles
- La amenaza Interna
- Anatomía de un ataque

• Módulo IV: Ataques

- Análisis de los ataques más conocidos y sus medidas de seguridad:
- BackDoors
- Rootkits
- Port Scanning
- Wipping Trace
- DOS/DDOS
- Escalamiento de privilegios
- Exploit Code
- Wireless Hacking (802.11 y bluetooth)
- Ingeniería Social
- Spoofing
- Mobile Code.Java Applets, Activex
- Key logging
- Man in the middle

- Password craking
- Proxy attack
- Port redirection
- Sql Injection
- Sniffing
- XSS
- Trojan Horses
- Virus/Worms

.. **Módulo Práctico:**

En el laboratorio se utilizarán las distintas técnicas y herramientas, utilizadas actualmente para realizar un **Test de Penetración** en sus diferentes etapas:

- Information Gathering
- Reconocimiento
- Enumeración Superficial y en Profundidad
- Captura de Tráfico
- Ataque Puro
- Borrado de Rastro y consolidación

Detalle de los laboratorios a desarrollar:

Lab 01 Comandos Básicos TCP/IP

Objetivo: Correr los comandos básicos e interpretar las salidas en la consola

Lab 02 Reconocimiento

Objetivo: Recolectar información de los sistemas objetivos

Lab 03 Sniffing

Objetivo: Utilizar un sniffer y leer el tráfico de red

Lab 04 Port Scanning

Objetivo: Escanear puertos e interpretar las salidas

Lab 05 Hacking Netbios

Objetivo: Realizar un scan al puerto 139 en busco de recursos compartidos en la LAN

Lab 06 Scanning de Vulnerabilidades

Objetivo: Realizar un scaneo de la LAN en busca de vulnerabilidades en los host de la RED

Lab 07 Código Malicioso

Objetivo: Fabricar un archivo malicioso, ocultarlo y ejecutarlo y acceder al sistema remoto

Lab 08 Troyanos

Objetivo: Configuración de un troyano y ejecución del mismo para aprovechar del sistema comprometido

Lab 09 Google Hack

Objetivo: Analizar ejemplos de ingeniería social, archivos confidenciales, archivos de configuración con información crítica mostrados por el instructor

Lab 10 Keylogger

Objetivo: Aprender a manejar y configurar un Keylogger

Lab 11 Malware

Objetivo: Entender el funcionamiento de este tipo de código malicioso

Lab 12 Password Cracking

Objetivo: Crackear las contraseñas

Lab 13 Hacking Automático

Objetivo: Sniffing, Password Cracking, Instalación de Troyano, Acceso al sistema comprometido

Lab 14 Netcat

Objetivo: Aprender a utilizar algunos comandos del netcat

Lab 15 Código Exploit DOS

Objetivo: Denegación de servicio al Servidor

Lab 16 Código Exploit

Objetivo: Realizar un ataque completo - Objetivo principal obtener consola remota

Lab Final Test de Intrusión Controlado

Objetivos: Utilización de Metodología de Penetration Test:

- Reconocimiento
- Enumeración
- Ataque (Plantar Trofeo o Sacar Trofeo)
- Borrado de Rastro
- Consolidación

Herramientas a utilizar:

Se usarán algunas de las siguientes: *Nmap, Netcat, Curl, Whisker, Pwdump2, Pwdump4, Raibowcrack, User2sid, Sid2User, LC5, Ettercap, Shed, Enum, T-smb, Smb, relay, Smbf, dsniff, hping2, Exploits de Microsoft, Exploits de Linux, Exploits de Unix, Framework, Metasploit, Sitedigger, Sam, Spade, SANS/FBI, Verify, Vulnerability, Whois, DNSlookup, Transfer, Zone, Ethereal, Iris, Nessus, Netsumbber, Wep, Crack, Airsnort, Snort, N-Stealth, MailBomber, Brutus, Hydra, Herramientas de Programación Perl, Thoneloc, Cain&Abel, DatabaseScanner, DBS42, Hyena, Sterm15, Cisco, BugScanner, Resource Kit Nt 4.0, Resource Kit de Windows 2000, Resource Kit Windows 2003.*

Recursos: Cada participante contará con un computador conectado a la red, en dónde realizarán sus prácticas.