

CURSO ETHICAL HACKING – NIVEL I

DURACION: 12 HORAS (4 SESIONES)

SUMILLA

El **NIVEL I** es una introducción a los conocimientos de Hacking con temas como: anonimato en la red para empezar a trabajar en el mundo del hacking y ataques básicos a maquinas con acceso físico.

OBJETIVOS

Dar un acercamiento inicial al mundo del Hacking permitiendo a su vez que los asistentes logren comprender lo vulnerable que pueden llegar a ser los sistemas que se utilizan en el día a día.

METODOLOGIA

La capacitación está estructurada para darse en 4 clases distribuidas de la siguiente manera.

Fecha	Duración(hrs)
1er Sábado	3
2do Sábado	3
3er Sábado	3
4to Sábado	3
Total Horas	12

De necesitar tiempo para abarcar los temas, habrá alguna sesión con mayor duración.

Las clases cuentan con 2 profesores, los cuales se encargan de dictar la clase y hacer el seguimiento de los asistentes en la parte práctica.

El curso consta de partes tanto teóricas como prácticas. Se proveerán a los alumnos las herramientas necesarias para hacer las pruebas que se realizan a medida que el profesor realiza la explicación.

La metodología de trabajo se basa en la realización y desarrollo de ejercicios prácticos que permitirán a los participantes avanzar paso a paso y aumentar constantemente el nivel de conocimientos con respecto a los temas impartidos.

Para ello el profesor hará una exposición teórico-practica de cada tema y posteriormente el alumno desarrollara el conjunto de ejercicios propuestos.

CONTENIDO

SESION 1

- Acercamiento a conceptos:
 - DNS
 - PROXY
 - Funcionamiento de Web Browsing
 - Puertos, servicios, NAT
 - Explicación de la ruta: maquina – sw firewall – router
- Técnicas de anonimato
 - Web proxys
 - Funcionamiento
 - Como ganan ellos
 - Cuando usarlos
 - Tips y herramientas
 - Posible comportamiento por parte de una institución al tratar de bloquear direcciones o palabras y como evadir dichas técnicas
 - Home proxys
 - Como montar un servidor Proxy para usarlo de pasarela desde algún otro punto
 - Ventajas y desventajas de este método
 - Recomendaciones para seguridad de la maquina y posibles ataques de los cuales pueden ser víctima estas maquinas
 - Server proxys
 - Listados de proxys
 - Utilización de proxys en forma manual
 - Herramientas gestadoras de proxys
 - Multiple mirroring
 - Técnica avanzada para evadir rastreos
 - Que programas lo manejan y como mantenerlo configurado
 - Fake Mailing
 - Como enviar mails anónimos
 - Suplantación de identidad
 - Acercamiento a algunos fakes que hay en la web
 - Mails privados y mails públicos: Tips
 - Acercamiento a la metodología de seguimiento por parte de entidades policiales cuando hay sucesos delictivos informáticos
 - Que sucede cuando hay un Proxy de por medio
 - Escenario optimo para no ser rastreado

- Anonimato y encubrimiento por terceros
 - Como se usan recursos de otra persona o entidad para lanzar los ataques

SESION 2

- Acercamiento a hackeo de maquinas con acceso físico
 - Acercamiento a hackeo de cabinas
 - Mercado negro de BD de correos en Perú
 - Detalles a tomar en cuenta cuando se usa una maquina de terceros
 - Como romper la seguridad de programas de protección usados en cabina
 - Hackeo de cybercontrol
 - Hackeo de deep freeze
 - Control sobre cookies para sesiones ilícitas de correo
 - Uso de keyloggers

SESION 3

- Como estudiar un programa
 - Pruebas de instalación en maquinas virtuales
 - Método de prueba y uso de keygens para no infectarse
 - Herramienta de seguimiento de registros
 - Caso deepfreeze para simular hackeo de cabina
- Secuestros de páginas web
 - Ataques manuales
 - Ataques tuneados y automatizados
 - Técnicas para disfrazar información
 - Acercamiento a ejemplos de phishing local

SESION 4

- Google Hacking
 - Modificadores
 - Comodines
 - Honeypots
 - Honeynets
 - Herramientas
- Hackeo de sistemas locales WindowsXP
 - Uso de recursos y herramientas
 - Dumpeo de contraseñas
- Ataque complejo para hackeo y espionaje de cabinas