

**Jueves 4 y Viernes 5 de Diciembre**

## Técnicas de prevención y ejecución de hacking (módulo II)

¿Imagina un cuerpo policíaco que no conozca las técnicas de los delincuentes que tratan de combatir? ¿Cómo saber cuándo atacarán? ¿Cómo combatirlos si no se sabe cómo piensan? Algo similar sucede en la Seguridad de la Información. El objetivo principal de este curso es revisar los "modos operandis" de los delincuentes informáticos con un objetivo claro: Saber cómo prevenir los ataques y a última instancia minimizar su impacto.

En este curso realizaremos una revisión de las técnicas de Hacking utilizando ingeniería social, intrusión en sitios web, el robo y utilización fraudulenta de credenciales y contraseñas, secuestro de información, construcción de exploits y trojanos, técnicas de evasión de los sistemas de seguridad, Linux hacking y violación de la seguridad inalámbrica.

### Objetivo principal

Conocer las mejores técnicas y herramientas que utilizan los Hackers a través de más de 15 prácticas en entornos operativos diversos (Windows, Linux, Redes Inalámbricas) el estudiante tendrá una visión general de las técnicas utilizadas por los hackers así como de los medios principales de protección contra las actividades criminales.

### Orientado a

Gerentes, Supervisores y Administradores de sistemas que deseen ampliar sus conocimientos de seguridad. Auditores/consultores, webmasters, desarrolladores que necesiten profundizar en técnicas de Hacking.

## Contenido del curso

### ✚ Técnicas de Ingeniería Social

- Tipos, Objetivos y Prevención básica de la Ingeniería Social como arma de hacking
- Fases de la Ingeniería Social
- Medidas para evitar ser víctima de la Ingeniería Social
- Ataques de Phishing
  - \* ¿En qué consiste el Phishing?
  - \* ¿Cuales son las formas más comunes?
  - \* Ejemplos Escalofriantes y Cotidianos
- Técnicas de Oscurecimiento de la URL
  - \* Codificación de URL
- Mapeo de Imágenes
- Envenenamiento de DNS

### ✚ Ataques a sitio Web

- ¿Cómo son comprometidos los servidores?
- Ataques sobre Internet Information Services
- Vulnerabilidades de WebDav
- Vulnerabilidades de RPC DCOM
- Troyanos para ASP
- Ataques sobre Apache Web Server
- Mod-Security Apache
- Acceso y Destrucción de Bitácoras (logs)
- Medidas para evitar ataques sobre Servidores Web

### ✚ Robo de Contraseñas

- Tipos y Vías de Autenticación
- Certificados Digitales
- Biometría
- Acceso a claves en Cache
- Destrucción del Cache
- Rompimiento de Claves
- Robo de Contraseñas del MSN
- Robo de Contraseña de Archivos Protegidos
- Medidas para proteger Contraseñas

### ✚ Escribiendo exploits

- Prerrequisitos para escribir exploits
- Tipos de Exploits
- Métodos de ataques
- Shell Code
- Buffer Overflow
- Programas Lanzaderas de Exploits
- Los Exploits más famosos y exitosos

### ✚ Evasión de Los Sistemas de Seguridad

- Detección de Intrusos
- Tipos de IDS
- Técnicas para la Evasión del Control de los IDS
- Firewall: ¿Cómo funciona?
- Técnicas para evadir los controles por firewalls
- HoneyPot: tipos, acciones
- Herramientas para detectar la presencia de honey pots.

### ✚ Hackeando Linux

- ¿Linux es más seguro?
- Explotación de las vulnerabilidades en Linux
- Robo de Contraseñas en Linux
- Firewalls en Linux
- Rootkits
- Herramientas de control de la seguridad en Linux
- Medidas para asegurar Linux

### ✚ Hackeando Redes Inalámbricas

- Conceptos fundamentales de seguridad en Redes Inalámbricas
- Normas Wireless
- Rompimiento de claves inalámbricas
- Fortalezas WEP, WPA, WPA2
- Metodología para atacar redes inalámbricas
- Herramientas para wireless hacking
- Ataques de hombre en el medio en redes inalámbricas
- Ataques a Servicios de telefonía celular
- Auditoria de servicios wireless
- Medidas para asegurar redes wireless

Inversión Bs.F. 3.700,00 + I.V.A.

Jueves 5 y Viernes 6 de Diciembre  
8:00am – 12:00m y 2:00pm-5:00pm TOTAL 16 horas

## Resumen curricular del instructor

Ingeniero en Computación con Maestría en Computación.

Especialista de Seguridad informática Nivel Instructor Senior.

Miembro Activo de IEEE ( Institute of Electrical and Electronics Engineers)

Miembro ISSA (Information Systems Security Association)

Con quince (15 años de experiencia en el área de Tecnología y seis (6) años en seguridad de la información el instructor de SNSecurity posee sólidos conocimientos y experiencia en las siguientes áreas:

- Seguridad: Diseño e implantación de políticas de seguridad, Firewalls, Criptografía de Clave Pública y Privada, Autenticación, Detección de
- Enrutamiento: Enrutamiento Estático y Dinámico, OSPF, RIP, BGP, Sistemas Autónomos, Listas de Acceso, políticas de acceso, NAT, PAD, QoS.
- Administración de Sistemas Operativos: UNIX (Solaris), LINUX (RedHat, Slackware), Windows NT y 2000.

En el área de docencia su trayectoria en estos últimos seis (6) años se ha venido desempeñado como:

- Profesor en los Cursos de entrenamiento para el personal de Petróleo de Venezuela (PDVSA), materia dictada Criptografía y Seguridad de Redes. 1995-2002
- Coordinador y Expositor del Taller de Seguridad de Redes, Workshop for Latin America and Caribbean, INET, Escuela Latinoamericana de Redes 2001.
- Coordinador y Expositor de la I Escuela Venezolana de Seguridad de Cómputo
- Profesor del Diplomado de Diseño de Redes Empresariales. Universidad Tecnológica Equinoccial, Quito, Ecuador. 2002
- Coordinador y Expositor del Taller de Seguridad de Redes, Workshop for Latin America and Caribbean, INET, Escuela Latinoamericana de Redes 2002 Santo Domingo República Dominicana.
- Instructor de la Academia Cisco Fundación Escuela Latinoamericana de Redes 2003.
- Miembro de la Comisión Latinoamericana de desarrollo de políticas regionales para asignación de Recursos de Internet (LACNIC)
- Coordinador y Expositor del Taller de Seguridad de Redes, Workshop for America Latina and Caribbean, INET, Escuela Latinoamericana de Redes 2003.
- Coordinador y Expositor del Taller de Seguridad de Redes, Workshop for America Latina and Caribbean, INET, Escuela Latinoamericana de Redes 2005.
- Coordinador y Expositor del Taller de Seguridad de Redes, Workshop for Latin America and Caribbean, INET, Escuela Latinoamericana de Redes 2006. Quito, Ecuador 2006

## Instructores Certificados

**SNSecurity** disponen de formadores con alta calificación certificada en las tecnologías, herramientas y normativas de seguridad necesarias para garantizar la calidad de los contenidos.

[http://www.snsecurity.com/index.php?option=com\\_content&task=category&sectionid=10&id=92&Itemid=124](http://www.snsecurity.com/index.php?option=com_content&task=category&sectionid=10&id=92&Itemid=124)



Los cursos presenciales de **SNSecurity** son 100% prácticos, cada participante contará con:

- ✚ Material práctico y de apoyo en un CD
- ✚ Instructores Certificados
- ✚ Laboratorios Reales
- ✚ Certificado entregado al final del curso



### Próximos cursos para el mes de Julio y Agosto

- ✚ **Curso:** Análisis Forense. Curso teórico/práctico  
**Fecha:** 9 y 10 Octubre  
**Costo:** 2.700,00 + IVA
- ✚ **Curso:** Aspectos Legales para la Seg. Información  
**Fecha:** 13 y 14 de Noviembre  
**Costo:** 1.700,00 + IVA
- ✚ **Curso:** Administraciones Planes Continuidad del Negocio  
**Fecha:** 27 y 28 Noviembre  
**Costo:** 2.000,00 + IVA

**Diana Sanoja**

**Formación Especializada Seguridad Información**

**Contáctenos +58-212-881-2913/886-9470**

**formacion@snsecurity.com**