

Dominio 6: GESTION DE OPERACIONES Y COMUNICACIONES

Procesos de:

- Planificación y aprobación de sistemas
- Protección contra software malicioso
- Mantenimiento back up
- Administración de la red
- Administración y seguridad de los medios de almacenamiento
- Acuerdos de intercambio de información y software

Dominio 7

Sistema de Control de Accesos

Dominio 7: SISTEMA DE CONTROL DE ACCESOS

Requerimientos de negocio para el control de accesos

- Coherencia entre las políticas de control de acceso y de clasificación de información de los diferentes sistemas y redes

Administración de accesos de usuarios

- Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información.

Dominio 7: SISTEMA DE CONTROL DE ACCESOS

- Administración de accesos de usuarios
- Administración de privilegios
- Responsabilidades del usuario
- Control de acceso a la red
- Camino forzado
- Autenticación de usuarios para conexiones externas
- Monitoreo del acceso y uso de los sistemas

Dominio 8

Desarrollo y Mantenimiento de Sistemas

Dominio 8: DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Requerimientos de seguridad de los sistemas.

Asegurar que la seguridad es incorporada a los sistemas de información.

- Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

Dominio 8: DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Seguridad en los sistemas de aplicación

Se deben diseñar en los sistemas de aplicación, **incluyendo las aplicaciones realizadas por el usuario**, controles apropiados y pistas de auditoría o registros de actividad, incluyendo:

- la validación de datos de entrada,
- procesamiento interno, y
- salidas.

Dominio 9

Plan de Continuidad del Negocio

Dominio 9: PLAN DE CONTINUIDAD DEL NEGOCIO

Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres.

- Se debe implementar un proceso de administración de la continuidad de los negocios
- Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio.

Dominio 10

Cumplimiento

Dominio 10 : CUMPLIMIENTO

- Impedir infracciones y violaciones de las leyes del derecho civil y penal; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad.
- Garantizar la conformidad de los sistemas con las políticas y estándares de seguridad de la organización.
- Maximizar la efectividad y minimizar las interferencias de los procesos de auditoría de sistemas.

Dominio 10 : CUMPLIMIENTO

Recolección de evidencia

La evidencia presentada debe cumplir con las pautas establecidas en la ley pertinente o en las normas específicas del tribunal en el cual se desarrollará el caso:

- validez de la evidencia: si puede o no utilizarse la misma en el tribunal;
- peso de la evidencia: la calidad y totalidad de la misma;

Dominio 10 : CUMPLIMIENTO

- adecuada evidencia de que los controles han funcionado en forma correcta y consistente durante todo el período en que la evidencia a recuperar fue almacenada y procesada por el sistema.

Para lograr la validez de la evidencia, las organizaciones deben garantizar que sus sistemas de información cumplan con los estándares o códigos de práctica relativos a la producción de evidencia válida.

Dominio 10 : CUMPLIMIENTO

Revisiones de la política de seguridad y la compatibilidad técnica

Garantizar la compatibilidad de los sistemas con las políticas y estándares (normas) de seguridad de la organización.

Dominio 10 : CUMPLIMIENTO

Auditoria de sistemas

Optimizar la eficacia del proceso de auditoria de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoria en el transcurso de las auditorias de sistemas.

Laboratorio

Simulación de “Hacking” en vivo

Ethical Hacking

- Etapas de un Ethical Hacking – Pen Test
- Demo de Utilización de Herramientas de Hacking
- Conclusiones finales

Ethical Hacking

El enfoque de trabajo para esta práctica incluye las siguientes actividades:

- Reconocimiento inicial de las redes y recursos
- Definición de pruebas y herramientas a utilizar
- Ejecución de las actividades
- Redefinición de pruebas y herramientas a utilizar en base a resultados obtenidos
- Obtención de resultados y evidencias probatorias
- Limpieza de evidencias
- Documentación formal y desarrollo de Informes Finales

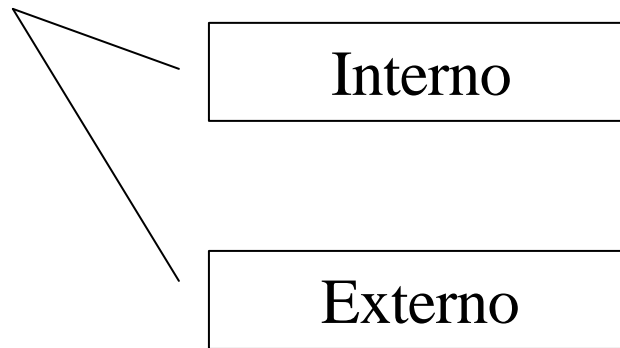
Ethical Hacking

- Técnicas mediante la cual se intenta acceder a un **objetivo** con el fin de cumplir una premisa anteriormente fijada.
- El **objetivo** es generalmente obtener accesos, cuentas con permisos, archivos, o tomar control del hardware para su posterior utilización.
- REGLA : implícitamente el Ethical Hacking no debe dañar el objetivo ni debe utilizar la información obtenida para ningún otro fin que el antes descripto.

Ethical Hacking

- También conocido como :
 - Penetration Test
 - Test de vulnerabilidad

- Puede ser



Ethical Hacking EXTERNO

- Se compone de un elevado número de pruebas, entre las que se pueden nombrar:
 - Pruebas de passwords.
 - Detección de conexiones externas.
 - Obtención de rangos de direcciones en Internet.
 - Detección de protocolos.
 - Scanning de puertos TCP, UDP e ICMP.
 - Intentos de acceso vía Internet.
 - Intentos de acceso vía accesos remotos o módems.
 - Análisis de la seguridad de las conexiones con proveedores o entidades externas a la Organización.
 - Pruebas de vulnerabilidades.
 - Prueba de ataques de denegación de servicio.

Ethical Hacking INTERNO

- Se compone de numerosas pruebas, entre las que podemos citar:
 - Análisis de protocolos internos.
 - Test a nivel de autenticación de usuarios.
 - Test de los Servers principales Windows NT, UNIX, Linux y Novell.
 - Análisis de la seguridad de la red interna.
 - Nivel de detección de la intrusión de los sistemas.
 - Análisis de la seguridad de las estaciones de trabajo.
 - Seguridad de la red.

Algunos aspectos a tener en cuenta

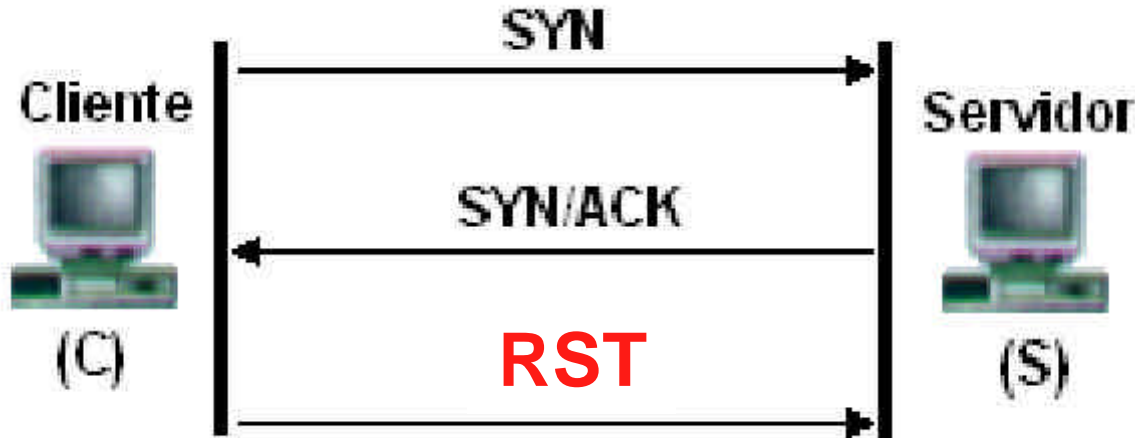
- Debemos pensar como un intruso y respetar esos pasos.
- Empezamos...
 - Buscar puertas.... (puertos habilitados)
 - Localizar vulnerabilidades
 - Aprovechar vulnerabilidades
 - Borrar los rastros.... Los visitaran muy pronto...
 - Como analista de seguridad, documentar e informar.

Algunos ejemplos de ataques y herramientas

- **Ataques de Monitorización – Scanning**
 - TCP Connect Scanning
 - Escaneo de puertos básicos de puertos TCP
 - Rápido escaneo de puertos
 - Usaremos **Nmap, Superscan, LanGuard....**
 - **Ejemplo :**
 - **Nmap –sT ip**
 - **Languard, búsquedas por rangos**
 - **Superscan, el buscador de principiantes...**

Algunos ejemplos de ataques y herramientas

- Ataques de Monitorización – Scanning
 - TCP SYN Scanning



Muy difícil de detectar, por que puede ocultarse el IP

Ejemplo : nmap -sS ip

Algunos ejemplos de ataques y herramientas

- **Ataques de Monitorización**

- Eavesdropping – Packet Sniffing

- Pasiva interceptación del tráfico de red.
- Consiste en colocar la placa de red en modo promiscuo (**desactiva filtro de verificación de direcciones**), todos los paquetes de la red llegan a esta máquina.
- Los IDS detectan las placas de red que están con el bit alterado, por estar en modo promiscuo.
- **Ejemplo :**
 - **Ethereal**
 - **Snort**
 - **Analyzer**

Algunos ejemplos de ataques y herramientas

- **Ataques de Monitorización**

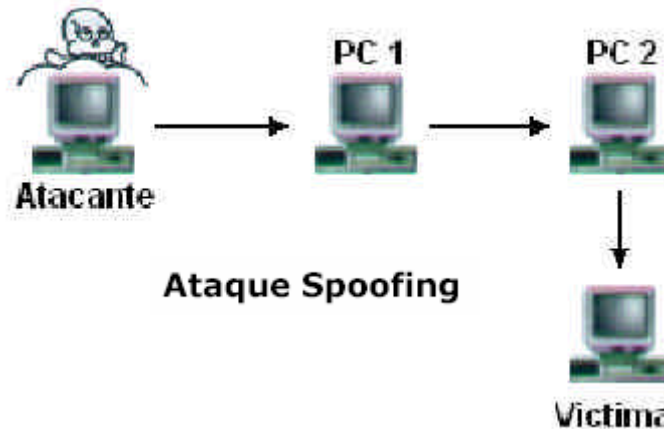
- Snooping – Downloading

- Igual que el Sniffing : obtener información sin modificarla.
- Captura información y saca copias que son almacenadas en la máquina del sniffer.
- **Ejemplo :**
 - LC4 – Abrir un archivo SAM._
 - Ethereal



Algunos ejemplos de ataques y herramientas

- **Ataques de autenticación – Spoofing**
 - IP Spoofing
 - “La máquina se hace pasar por otra”



Kevin Mitnick

- **Ejemplo** : Conexiones compartidas de Internet de un S.O.

Algunos ejemplos de ataques y herramientas

- Ataques de autenticación
 - BackDoors
 - Código en un programa que permite saltar la autenticación.
 - Algunos funcionan como agentes
 - Más conocidos : BackOrefice (BackDoor) y Netbus (Patch.exe).
 - **Ejemplo :**
 - Netbus. DEMO

Algunos ejemplos de ataques y herramientas

- Ataques de autenticación
 - Exploits
 - Programas o código malicioso para explorar agujeros de seguridad, errores en diseño de plataforma o de administración.
 - Los más comunes : WEB y CORREO.
 - **Ejemplo:**
 - Unicode de IIS. [DEMO](#)
 - Info: <http://packetstorm.widexs.nl/papers.html>
 - Software de detección : N-Stealth.

<http://www.mivictima.com.ar/scripts/..%c0%af../winnt/system32/cmd.exe?/c+>

Algunos ejemplos de ataques y herramientas

- Ataques de autenticación
 - Obtención de Password
 - Uso de diccionarios de “Fuerza Bruta”
 - Ejemplo :
 - LC4, Brutus, ShadowScan

Cantidad de claves generadas según el número de caracteres empleado

Cantidad de Caracteres	26–Letras minúsculas	36–Letras y dígitos	52–Mayúsculas y minúsculas	96–Todos los caracteres
6	51 minutos	6 horas	2,3 días	3 meses
7	22,3 horas	9 días	4 meses	24 años
8	24 días	10,5 meses	17 años	2.288 años
9	21 meses	32,6 años	890 años	219.601 años
10	45 años	1.160 años	45.840 años	21.081.705 años

Algunos ejemplos de ataques y herramientas

- **Denial of Service (DoS)**
 - Bloquear los servicios de la víctima.
 - Servicios Web, Correo, VPN, etc...
 - Variedades....
 - JAMMING o Flooding
 - Desactivar o saturar recursos del sistema.
 - Uso excesivo de memoria, red, disco, etc.
 - Uso de disco (SPAM o Mail Bomber sobre un SMTP)
 - Ping de la muerte (NT Sp4 BLUE SCREEN, TCP Overflow)
 - **Ejemplo** : Usar herramientas para denegacion de servicio.
 - » Panther2 – [Panther2](#)

Algunos ejemplos de ataques y herramientas

- **Denial of Service (DoS)**
 - OOB, Supernuke o Winnuke
 - Ataque clásico al puerto 137, 128 y 139 de Windows.
 - OOB = Out Of band
 - OOB envía paquetes manipulados al puerto 139, UDP y con el BIT URGENTE (URG) habilitado (1).
 - **Ejemplo:**
 - Desde los Windows 98 acceder a <http://www.jtan.com/resources/winnuke.html> y a <http://onlinescanner.com/>
 - Winnuke

Algunos ejemplos de ataques y herramientas

- **Denial of Service (DoS)**
 - Teardrop I y II, Newtear, Bonk y Boink
 - Similar al SuperNuke, afecta a los fragmentos de paquetes. Esto es aprovechado cuando el S.O. No arma correctamente los fragmentos que se superponen.
 - Consume recursos hasta colapsar el SO.
 - NT 4.0 muy susceptible.
 - Son implementaciones más conocidas como Newtear, Bonk y Boink

Programa Anual de Seguridad de la Información y Auditoría de Sistemas

NORMA ISO 17799 – COBIT Audit Guidelines

Duración: 8 meses

Buenos Aires, desde el 2 de mayo 2003

A quién está dirigido

Principalmente está dirigido a:

Estudiantes y Profesionales de Sistemas, Ingeniería, Administración, Contadores, y/o similares, Profesionales y Consultores de TI, Auditores de Sistemas.

Examen y certificado final (opcional) al cierre del año.

**Enfoque de Teoría según Normas Internacionales y
Casos Prácticos de implementación.**

Laboratorios técnicos directamente en los equipos.

**Los CV de los mejores promedios serán presentados a
las principales compañías de Argentina (con
autorización).**

Las vacantes son limitadas.

Duración

4 hs semanales, todos los viernes de 9 a 13 hs, del viernes 2 de mayo al 12 de diciembre de 2003

Costo

Total de la Inscripción: \$200 mensuales por 8 meses. Bonificación especial del 20% para Alumnos, docentes y egresados de CAECE.

Lugar:

**Universidad CAECE, Buenos Aires, Argentina.
Tte. Gral. J. D. Perón 2933. Capital Federal**

A confirmar horario fuera del laboral.

Dirección del Programa e Instructor

Martín Diego Vila Toscano

Business Director I –Sec Information Security (2003)

Instructores Responsables

Natalia Scaliter

Lider HP Consulting - IT Security Hewlett-Packard Argentina

Enrique Dutra

Socio Gerente de Punto Net Soluciones (2002-2003)

Donald R. Glass, CISSP, CISA, MSCE, CNE

Manager de Enterprise Risk Management (Florida – USA, 2003)

Contenido del Programa de Especialización

Implementación de un Programa de Seguridad en la Compañía

- Ø Evaluación de Riesgos
- Ø Roles en la Compañía
- Ø Clasificación de la Información
- Ø Concientización de usuarios
- Ø Sistema de control y sanciones
- Ø Principales Casos de Fraudes y Ataques Informáticos

Contenido del Programa de Especialización

Definición de las Políticas y Normas

- Ø Aceptación de la Dirección
- Ø Desarrollo del Manual de Políticas
- Ø Diseño de los estándares técnicos de seguridad

Contenido del Programa de Especialización

Seguridad en el área de Sistemas

- Ø Desarrollo de procedimientos internos
- Ø Controles en los procesos de desarrollo y operaciones del área
- Ø Plan de Continuidad del Procesamiento

Contenido del Programa de Especialización

Seguridad en las redes de información

- Ø **Análisis de las principales vulnerabilidades de las redes**
- Ø **Sistemas operativos de red**
- Ø **Equipos de Comunicación**
- Ø **Servicios de Correo**
- Ø **Bases de Datos**
- Ø **Estaciones de trabajo**
- Ø **Sistemas Aplicativos.**
- Ø **Aplicaciones eBusiness.**

Contenido del Programa de Especialización

Seguridad Avanzada

- Ø Encriptación
- Ø Firmas Digitales
- Ø Firewalls
- Ø IDS
- Ø Wireless
- Ø Biometría y otras tecnologías

Contenido del Programa de Especialización

Hacking

- Ø Técnicas más comunes de hacking
- Ø Metodología de Penetration Testing

Contenido del Programa de Especialización

Herramientas de seguridad

- Ø administración centralizada
- Ø encriptación
- Ø detección de intrusos
- Ø monitoreo
- Ø auditoria
- Ø antivirus

Contenido del Programa de Especialización

Normativa Internacional y Leyes en Argentina

- Ø **Riesgos y Delitos Informáticos**
- Ø **Informática forense**
- Ø **Protección de Datos Personales – “Habeas Data”**
- Ø **Firma Digital**
- Ø **Propiedad intelectual / Software Legal**
- Ø **Delito Informático**
- Ø **Regulación de las Comunicaciones Comerciales Publicitarias por Correo Electrónico – “Antispam”**
- Ø **Normativa del Banco Central de la República Argentina**

Contenido del Programa de Especialización

Auditoría de Sistemas

- Ø Principales características de una Auditoría de Sistemas
- Ø Informes del Auditor
- Ø Definición de un Programa Integral de Auditoría de Sistemas

Contenido del Programa de Especialización

Talleres y Laboratorios prácticos

- Ø **Desarrollos de políticas de seguridad**
- Ø **Pruebas de hacking**
- Ø **Casos prácticos de implementación**
- Ø **Diseño de un Programa Detallado de Seguridad de la Información**

Información y registración

Vía web

<http://www.caece.edu.ar/Cursos/continua/61.asp>

Vía email

difusion@caece.edu.ar

Eroisen@caece.edu.ar

Vía telefónica

(54-11) 5217 7888 Int 318 AT: DIFUSION

(54-11) 5217 7888 Int 312 AT: Lic. Elida Roisen

Contactos Técnicos

martin.vila@i-sec.com.ar

enrique.dutra@i-sec.com.ar

natalia_scaliter@hp.com

Cierre de la Conferencia



**Facilidad en el USO vs mejor PROTECCION
de la Información**

Cierre de la Conferencia

TODO el Personal es
RESPONSABLES de **PROTEGER**
la **INFORMACIÓN** de la
COMPAÑÍA

