



Martin.vila@isec-global.com

Isec Information Security Inc.

ETHICAL HACKING

MODULO I - MÉTODOS AVANZADOS DE HACKING Y PROTECCIÓN

DIFERENCIALES I-SEC

- ① **Somos Líderes en SERVICIOS PROFESIONALES en Seguridad de la Información en Latinoamérica.**
- ① **Trayectoria de 15 años desarrollando proyectos de Seguridad de la Información en Argentina y Latinoamérica.**
- ① **Desarrollamos Diagnósticos basados en Normas Internacionales, como la Norma ISO 17799 Seguridad de la Información (ahora 27001), Cobit, ITIL, entre otras.**
- ① **Nuestro Plantel de Profesionales cuenta con las Certificaciones más Prestigiosas.**
- ① **Nuestra Independencia Comercial es Garantía de Éxito**

Nuestros Servicios



Audit & Consulting Services:

- ① Profesionales Certificados
- ① Soluciones concretas, efectivas y sostenibles en el tiempo
- ① Independencia Comercial



I-SEC Legal & Forensic

- ① Asesoramiento Legal
- ① Esclarecimiento de ilícitos Informáticos



Education Center

- ① Seminarios Internacionales
- ① Instructores Certificados
- ① Asesoramiento y Coaching permanente



InfoSecurity

- ① El Mega Evento de Seguridad de la Información
- ① 20 Ediciones realizadas en Latinoamérica



INFORMACIÓN PREVIA AL USUARIO RECONOCIMIENTO PREVIO DERECHOS DE AUTOR

El contenido de los presentes manuales técnicos (o sistema de instrucción o curso según corresponda) ha sido creado y desarrollado por I-SEC INFORMATION SECURITY y se encuentra debidamente protegido por las leyes de Propiedad Intelectual vigentes, incluyendo imágenes, diseños de arte, textos, programa de computación y marca registrada. Queda expresamente prohibida su copia o reproducción total o parcial no autorizada, como así también, la utilización fraudulenta de la idea y concepto plasmado en su contenido.

Ethical Hacking – Módulo I

Métodos Avanzados de Hacking y Protección

- 1. Ethical Hacking y Seguridad de la Información**
 - **Situación Actual**
 - **Estrategias de Defensa**
 - **Mapa de la Seguridad**
 - **Alineación con la Norma ISO 27001**
2. Metodologías de Penetration Testing
3. Hacking
4. Know How
5. Laboratorios Prácticos

Situación Actual:

En los 80 los ataques se realizaban sobre sistemas **individuales o centralizados**, inclusive hasta mediados de la década del 90 se materializaban a través de un **acceso local o por línea telefónica**.

Hoy en día con la llegada de Internet los ataques crecieron exponencialmente por varios factores:

- Acceso global a **costo reducido**
- Las **empresas necesitan exponer** sus servicios e información en la red
- Internet brinda **anonimato** o rastros débiles
- Efectivizar un ataque hoy en día **NO requiere un gran conocimiento** y hay herramientas free para todo tipo de ataque.
- Los ataques alcanzaron una madurez que sobrepasan el alcance de la **legislatura**.
- No existe una **conciencia** en materia de seguridad de la Información.
- Desde el 2006 se observa que se convierte en un **negocio**.



Situación Actual:

Los ataques más vistos durante este último año, la mayoría obtienen beneficios económicos

Keylogging, troyanos, spoofing, Password cracking, Denegación de servicio, arp poison, Exploits, sniffing

XSS, SQL Injection, phishing, ransomware, spam, spyware, snmp walk, gathering, Exploits

War dialing, voip sniffing, vishing, clonaciones.

Dumpster diving, Robo o extravío de notebooks, ingeniería social, destrucción de documentos

War driving, man in the middle, war nibbling, wep cracking, sniffing, exploits

Secuestro de archivos

Código Malicioso en Dispositivos Móviles

Malware 0Day

Ataques a nuevas tecnologías

Redes zombies

Regionalización de la codificación

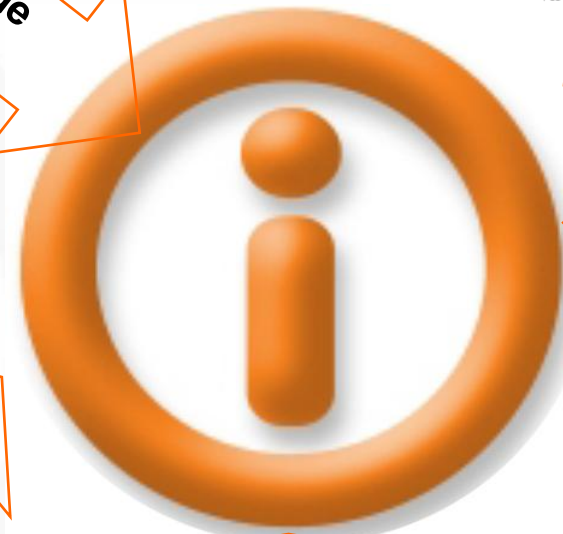
Mutaciones de Phishing & Pharming

- Spear Phishing (envío a un grupo reducido)
- Inyección de código malicioso (keyloggers, troyanos, hijackers)
- Content Injection Phishing (Web reales comprometidos con código malicioso)
- Vishing (Voip Phishing), Drive by pharming

PRINCIPALES RIESGOS

- Violación de e-mails
- War Dialing
- Exploits
- Spamming
- Programas "bomba"
- War Driving, War Walking y War Nibbling
- Denegación de servicio
- Password cracking
- Man in the middle
- Destrucción de equipos
- INGENIERÍA SOCIAL
- Violación de contraseñas
- SQL Injection
- Intercepción de comunicaciones
- Violación de privacidad de los empleados
- Virus & Gusanos
- Mails "anónimos" con información crítica o con agresiones
- extravío de notebooks
- escalamiento de privilegios
- ning
- es informáticos
- Robo de información
- ad de la Información
- rupción de los
- Backups inconsistentes
- so claudes
- RED DIRECCIONAMIENTO DE PUERTOS
- Destrucción de soportes documentales
- l de información clave
- ido a documentos impresos
- icios de log inexistentes o que no son chequeados
- Instalaciones default

Últimos parches no instalados



Estrategias de defensa

Las estrategias de defensa proveen hoy **más beneficios** que costos...

...sin embargo la mayoría de las contramedidas que hoy poseen las redes son **netamente detectivas**

No todas ellas están debidamente **explotadas**

Pocos ven hoy la **utilidad** de desarrollar una metodología de defensa

implementación

Las estrategias de defensa **NO** están debidamente **Maduras** al nivel del **Usuario Tecnología**

Para implementar una red defensiva
¿hay que esperar que la ataquen?

La seguridad depende principalmente del **Factor Humano** y en menor grado del factor Tecnológico.

Solo un muy bajo porcentaje de los ataques son **detectados** por las empresas damnificadas y aun menor, el de los que se **reportan**.

Los controles de seguridad se implementan de manera **reactiva**.

Estrategias de defensa

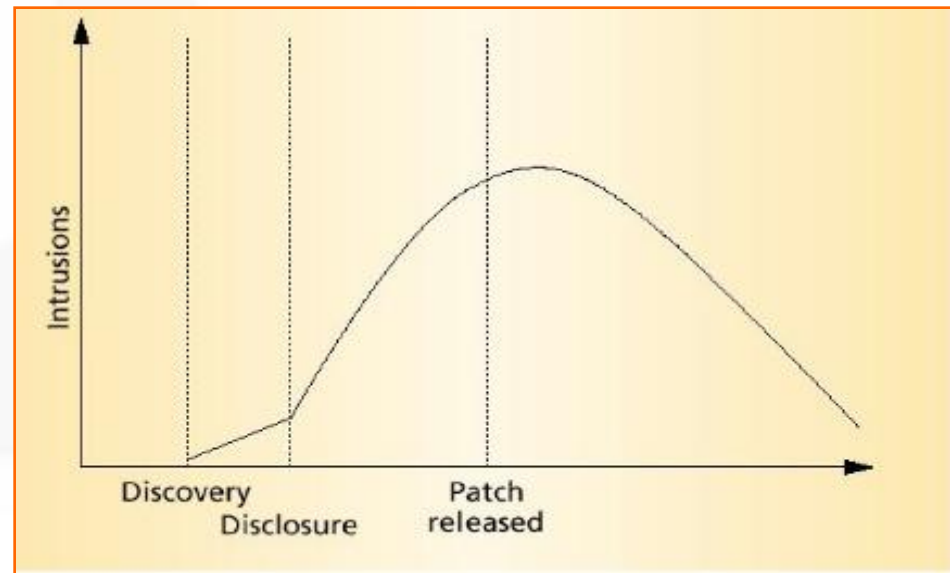
Mitos y Creencias:

- Los parches de seguridad solucionan el problema completamente.
- Los exploits son difíciles de utilizar y se necesitan skills avanzados.
- Si el exploit no está publicado para una vulnerabilidad dada entonces no existen.
- La única forma de remediación es instalar los parches de seguridad.
- Las únicas vulnerabilidades de un sistema son las publicadas.

Los tiempos se acortan: Hoy en día, el tiempo que existe entre el reporte de una vulnerabilidad, la publicación del parche o la generación del código exploit para aprovecharse del mismo, **se esta reduciendo considerablemente.**

Antes se tardaba mucho en generar el exploit

Cada vez es más probable que un atacante **explote** una vulnerabilidad aun no parcheada **antes** que salga la remediación.



Estrategias de defensa

Existen varias soluciones referidas a metodologías o estrategias de defensa

Ej.1: Remediación y Work Around

LSASS Vulnerability CAN-2003-0533

Se produce gracias a un Stack Overflow en LSASRV.dll del Local Security Authority Subsystem Service (LSASS), el cual un atacante con acceso al puerto TCP 139 del sistema afectado, podía fácilmente tomar control remoto del equipo a través de la obtención de una shell

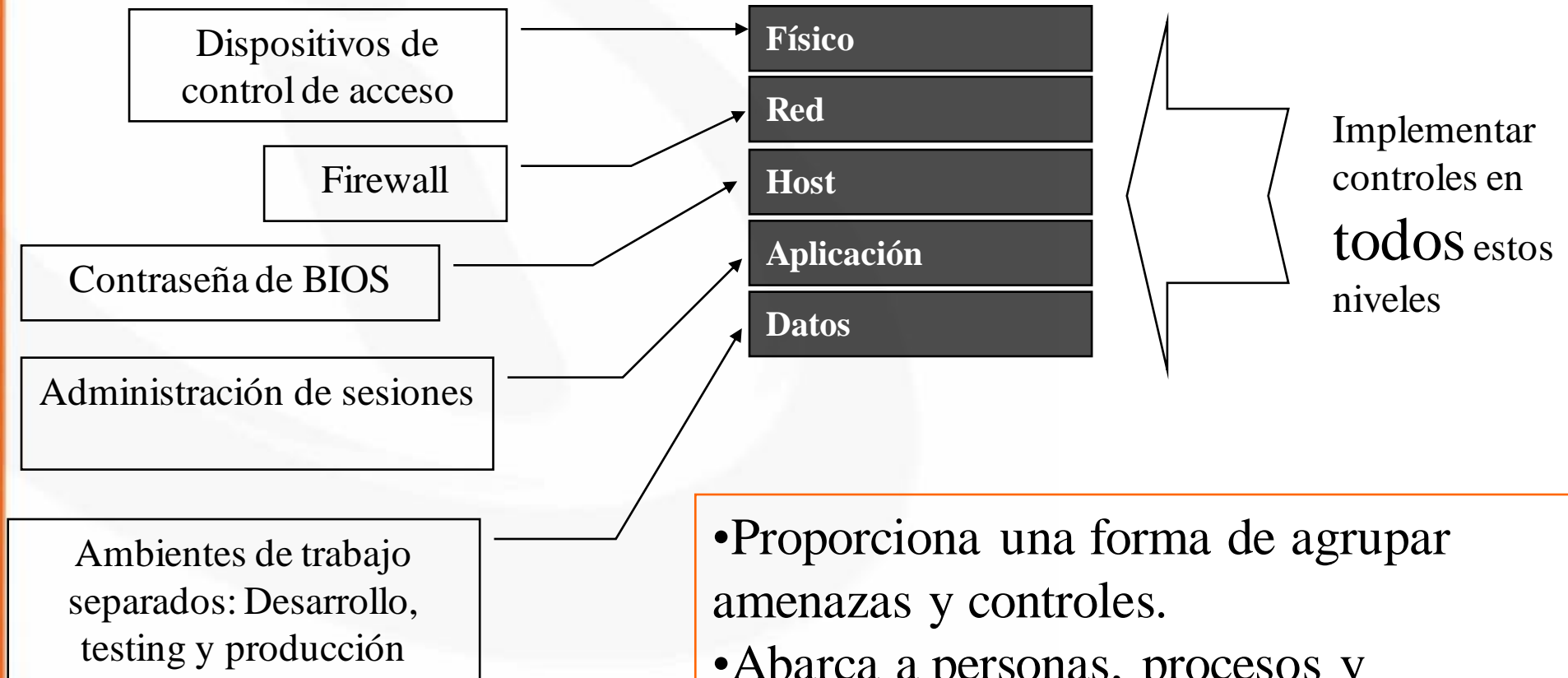
Remediación: Instalar el parche de seguridad previamente testeado en ambiente separado.

Work Around: Esto es fácilmente mitigable, con el solo hecho de seguir las buenas practicas recomendadas, a la hora de configurar las reglas de filtrado de un firewall, es decir filtrando el acceso al puerto TCP 139.

Estrategias de defensa

Existen varias soluciones referidas a metodologías o estrategias de defensa

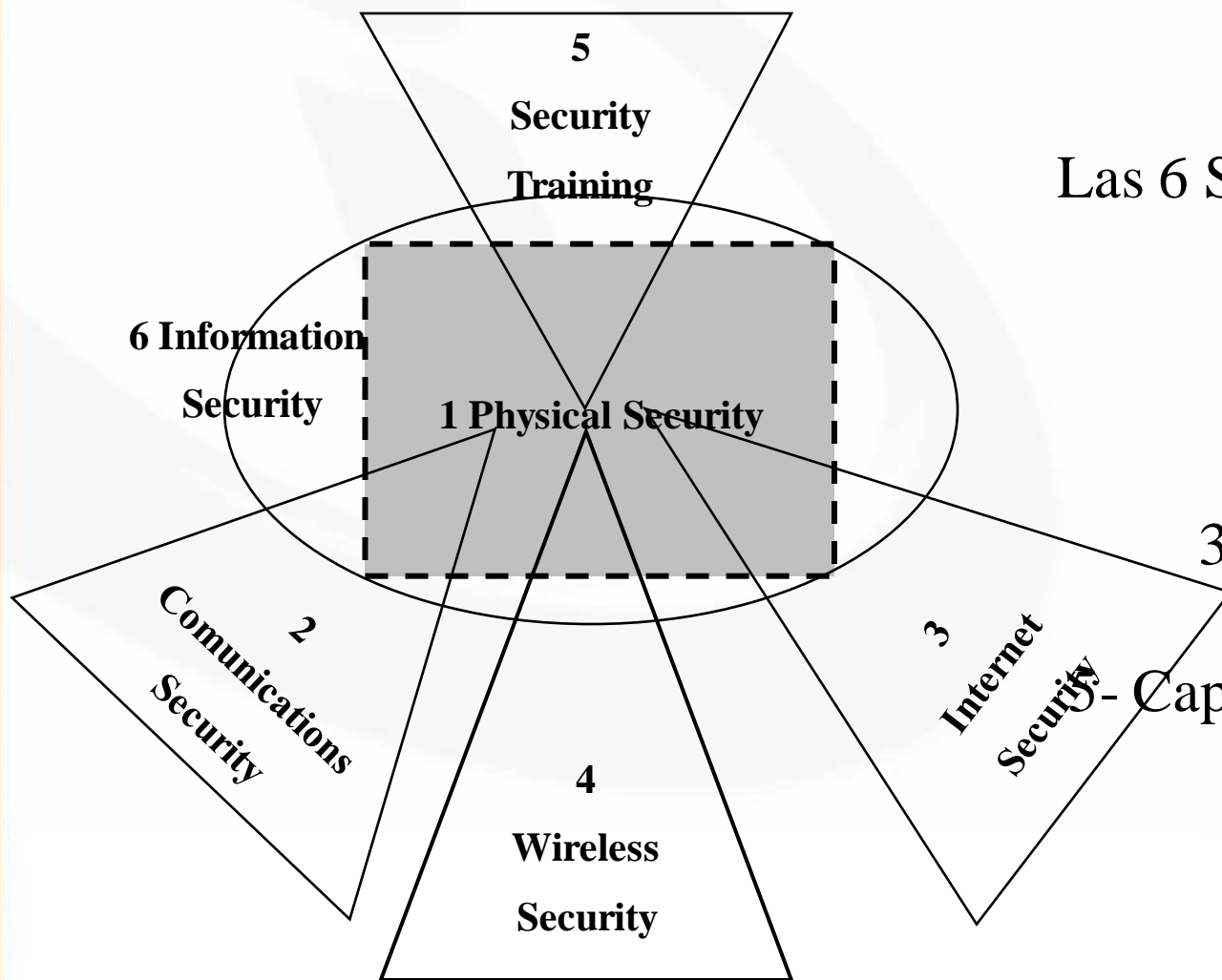
Ej.2: Defensa en Profundidad



- Proporciona una forma de agrupar amenazas y controles.
- Abarca a personas, procesos y tecnología.

Mapa de la Seguridad

Es un imagen de la presencia de seguridad en la Organización.
Fuente OSSTMM, Open Source Security Testing Methodology Manual



¿Qué Testear?

Las 6 Secciones del mapa son

- 1- Seguridad Física
- 2- Seguridad en comunicaciones
- 3- Seguridad en Internet
- 4- Seguridad Wireless
- 5- Capacitación en Seguridad
- 6- Seguridad de la Información

Mapa de la Seguridad

¿Qué Testear?

La seguridad depende principalmente del **Factor Humano** y en menor grado del factor Tecnológico.



CONFIDENTIALITY
INTEGRITY
AVAILABILITY

confidencialidad:

accesible sólo a aquellas personas autorizadas a tener acceso.

integridad:

exactitud y totalidad de la información y los métodos de procesamiento.

disponibilidad:

acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Alineación con Norma ISO 27001 Gestión de Seguridad de la Información, Evaluación e Implementación de medidas de Seguridad en Tecnologías de la Información.

15.2 Revisiones de la política de seguridad y la compatibilidad técnica

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

La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes y las plataformas técnicas y sistemas de información deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad.

15.2.2 Verificación de la compatibilidad técnica

Se debe verificar periódicamente la compatibilidad de los sistemas de información con los estándares de implementación de la seguridad. La verificación de la compatibilidad técnica comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de cumplimiento requiere asistencia técnica especializada. Debe ser realizada manualmente (si es necesario, con el apoyo de adecuadas herramientas de software) por un ingeniero en sistemas experimentado, o por un paquete de software automatizado que genere un informe técnico para su ulterior interpretación por parte de un especialista.

La verificación de compatibilidad también puede comprender pruebas de penetración, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito.

Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas. Se deben tomar recaudos en caso de que una prueba de penetración exitosa pueda comprometer la seguridad del sistema e inadvertidamente permita explotar otras vulnerabilidades,

Las verificaciones de compatibilidad técnica sólo deben ser realizadas por personas competentes y autorizadas o bajo la supervisión de las mismas.

Ethical Hacking – Módulo I

Métodos Avanzados de Hacking y Protección

1. Ethical Hacking y Seguridad de la Información

2. Metodologías de Penetration Testing

- **Enfoque Metodológico**
- **Modelos de Aplicación**
- **Consideraciones del Security Tester**

1. Hacking
2. Know How
3. Laboratorios Prácticos

Enfoque Metodológico

Objetivo: consiste en realizar un **intento de intrusión controlado** a los sistemas de información de la compañía, con el objetivo de **identificar las vulnerabilidades** a las que están expuestas las redes y **definir los planes de acción para mitigar los riesgos.**

Se busca emular a todos los **tipos de intrusos** y **obtener evidencias** concretas del resultado obtenido.



Las pruebas fehacientes de que se ha realizado la intrusión con éxito pueden depender del tipo de ataque realizado, definiéndose en si se permite o NO la realización final del ataque, identificando vulnerabilidades que permitan entre otras cosas:

- **Captura del Trofeo:** obtención de algún tipo de archivo de los servidores o redes
- **Sembrado de pruebas** en los objetivos
- **Otros:** captura de paquetes, limitación del servicio del recurso, etc.

Enfoque Metodológico

Keylogging, troyanos, spoofing, Password cracking, Denegación de servicio, arp poison, Exploits, sniffing

XSS, SQL Injection, pharming, phishing, ransomware, spam, spyware, snmp walk , information gathering, Exploits



Red Física



Web



Telefónica

War dialing, voip sniffing, vishing, clonaciones.



Dumpster diving, Robo o extravío de notebooks, ingeniería social, destrucción de documentos

Físicamente



Transmisiones y Emanaciones



War driving, man in the middle, war nibbling, wep cracking, sniffing, exploits



Enfoque Metodológico

Existen Ambientes más detallados:

Ambientes

White Box (con información del objetivo)

Black Box (sin información del objetivo)

Grey Box (Híbrido)

Blind/Blackbox: El Security Tester, no cuenta con ninguna información del objetivo, pero el cliente tiene conocimientos de que tipo de test se realizaran y cuando.

Double blind/ Blackbox: El Security Tester, no cuenta con ninguna información del objetivo y el cliente no cuenta con información sobre las tareas a realizar por el security tester, como así tampoco sobre el cuando.

Graybox: El security tester, solo conoce información parcial sobre los objetivos, dicha información será seleccionada por el cliente, el cliente tiene conocimientos de que tipo de test se realizaran y cuando

Double Graybox: El security tester, solo conoce información parcial sobre los objetivos, dicha información será seleccionada por el cliente, el cliente conoce las técnicas a utilizar por el security tester, pero no conoce el como y el cuando estas serán utilizadas.

Whitebox: El security tester tiene pleno conocimiento del objetivo, dicha información será entregada por el cliente, antes de iniciado el test, el cliente tiene pleno conocimiento de las tareas a realizar por el security tester y del como y el cuando.

Reversal: El security tester tiene pleno conocimiento del objetivo, dicha información será entregada por el cliente, antes de iniciado el test, el cliente no cuenta con información sobre las tareas a realizar por el security tester, como así tampoco sobre el cuando.

Enfoque Metodológico

PEN TEST EXTERNOS

Se compone de un elevado número de pruebas:

- Ataques de Reconocimiento.
- Detección de conexiones externas.
- Obtención de rangos de direcciones en Internet.
- Detección de protocolos.
- Scanning de puertos TCP, UDP.
- Análisis Dispositivos de comunicaciones
- Análisis de seguridad de conexiones remotas.
- Scanning de vulnerabilidades.
- Ingeniería Social.
- Prueba de ataques de denegación de servicio.
- Ejecución de código Exploit aplicable.
- Information Gathering
- DNS Stuff

PEN TEST INTERNOS

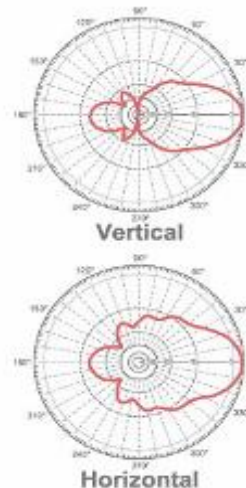
Adicionalmente a las pruebas anteriores se pueden agregar:

- Análisis de protocolos internos.
- Test a nivel de autenticación de usuarios.
- Análisis de la seguridad de los Servidores.
- Nivel de detección de la intrusión de los sistemas.
- Análisis de la seguridad de las estaciones de trabajo.
- Ejecución de código exploits
- Intento de DOS desde la red interna.
- Keylogging
- Lectura de tráfico de red para la obtención de usuario y password, lectura de correos, etc.

Enfoque Metodológico

PEN TEST INTERNOS/EXTERNOS Seguridad inalámbrica: War Driving, War Walking y War Nibbling

- Ataque aplicado a las Wireless Lan
- Búsqueda de Accesos a la red interna, vía Access Points
- Wireless Sniffing
- WEP Cracking
- War Nibbling (tecnologías Bluetooth)
- Rfid attack
- Verificación de Dispositivos Infrarrojos



Especificaciones Electricas

Frecuencia	2400-2500 MHz
Ganancia	14.5 dBi
Angulo de rad. -3dBi	30 Grados (horizontal)
Impedancia	50 Ohm
Potencia Max.	50 Watts
ROE	<1.5:1

Especificaciones Mecanicas

Peso	0.52 Kg.
Longitud	415 mm, Diam. 64mm
Material	UV-Inhibidor
Montaje	3/4" dia. mast.
Polarización	Vertical



Etapas

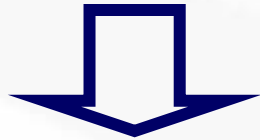
Briefing del Objetivo



Definición de Tareas y
herramientas a utilizar



Trabajo de Campo



Confección del informe
& QA Control de Calidad

Entrevistas Previas

Alcances de la intrusión

Convenios de Confidencialidad

- Trabajo de Campo:
- Reconocimiento Superficial
- Enumeración y Reconocimiento en Profundidad
- *Definición de las Herramientas a Utilizar*
- Ataque Puro
- *Redefinición de pruebas y herramientas a utilizar en base a resultados obtenidos*
- Borrado de rastro y evidencias
- Consolidación
- Reporting: Documentación formal y desarrollo de Informes Finales (Técnico y Ejecutivo)

Con o sin el Acuerdo de No Divulgación, el analista de seguridad esta éticamente obligado a mantener la confidencialidad y garantizar la no divulgación de la información del cliente ni los resultados del análisis.

Modelos de Aplicación



OWASP

The Open Web Application Security Project

Modelos de Aplicación

OSSTM

Open Source Security Test Metodology

www.isecom.org



El OSSTMM es un manual de seguridad, en el que participan abiertamente más de 130 profesionales de todo el mundo, y que cumple con los estándares ISO 27001 y las normas dictadas por organismos internacionales. (Orange Book, ICM3)

El OSSTMM es un conjunto de Reglas y Guidelines para **cómo testear, qué testear y por qué testear los eventos**, para que un test deba ser considerado dentro del OSSTM debe:

OSSTM – Alineación con Estándares Internacionales y Leyes Vigentes

Estados Unidos: USA Government Information Security Reform Act of 2000, section 3534(a)(1)(A);

Alemania: Deutsche Bundesdatenschutzgesetz (BDSG);

España: la Agencia de Protección de Datos Personales (APD y su Ley LOPD);

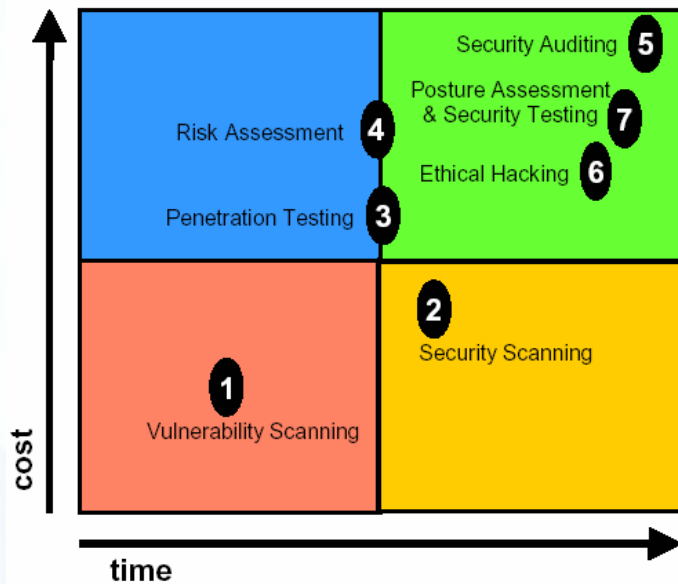
Canadá: Canada Act Respecting the Protection of Personal Information in the Private Sector (1993).

No debe ser abstracto, tangible.

- Ser cuantificable
- Consistente
- Válido en el tiempo mas allá del “Ahora”
- Cumplir con las leyes individuales y locales y el derecho a la privacidad

Modelos de Aplicación

Tipos de Test basados en tiempo y Costo



- 1. Búsqueda de Vulnerabilidades:** comprobaciones automáticas de un sistema.
- 2. Escaneo de la Seguridad:** búsquedas de vulnerabilidades (falsos positivos) y análisis profesional individualizado.
- 3. Penetration Test:** se refiere en general a los proyectos orientados a objetivos en los cuales dicho objetivo es obtener un trofeo, que incluye ganar acceso privilegiado con medios pre-condicionales.
- 4. Evaluación de Riesgo:** se refiere a los análisis de seguridad a través de entrevistas e investigación de nivel medio que incluye la justificación negocios, las justificaciones legales y las justificaciones específicas de la industria.

5. Auditoría de Seguridad: hace referencia a la inspección manual con privilegios administrativos del sistema

6. Hacking Ético: se refiere generalmente a los tests de intrusión en los cuales el objetivo es obtener trofeos en la red dentro del tiempo predeterminado de duración del proyecto.

7. Test de Seguridad y su equivalente militar, Evaluación de Postura, es una evaluación de riesgo con orientación de proyecto de los sistemas y redes, a través de la aplicación de análisis profesional mediante escaneos de seguridad donde la intrusión se usa generalmente para confirmar los falsos positivos y los falsos negativos dentro del tiempo permitido de duración del proyecto.

Modelos de Aplicación

Information System Security
Assessment Framework
www.oisssg.org



Es una metodología integradora de los siguientes conceptos de management y checklist de control:

- Evaluar, las políticas y procesos de seguridad de la información, para reportar el nivel de cumplimiento con los estándares de la industria de TI, leyes y regulaciones locales.
- Identificar los activos dependientes del negocio en la infraestructura de servicios proveída por TI.
- Conducir Penetration test y Vulnerability Assesment, para identificar vulnerabilidades que puedan convertirse en riesgos potenciales

Es un modelo basado en checklist
No tan tecnico ni intrusivo
Referido a demostrar riesgos

Esta metodología se basa y soporta a:
IEC/ISO 27001:2005(BS7799)
Sarbanes Oxley SOX404
CoBIT
SAS70
COSO

Modelos de Aplicación

www.owasp.org



OWASP

The Open Web Application Security Project

Objetivo: principalmente esta metodología esta orientada al desarrollo seguro de aplicaciones Web.

Tools: Adicionalmente al manual, se han desarrollado varias herramientas prácticas para verificación de seguridad y para el entrenamiento:

Webgoat

Webscarab

Define chequeos:

Autenticación – Diferentes tipos de autenticación y sus problemas más comunes.

Autorización – Conceptos de control de accesos.

Administración de Sesiones – Describe la manera adecuada de administrar sesiones.

Auditoría y Logging.

Validación de Datos – Describe estrategias para lidiar con entradas no esperadas por la aplicación.

Inyecciones - SQL, XML, LDAP, code, user agent (includes XSS) y otras.

Privacidad – Aspectos de privacidad relacionados con la aplicación.

Criptografía – Cómo y dónde utilizarla, cuales son los errores mas comunes.

Representación Canonica.

Consideraciones del Security Tester

Las soluciones deben ser **prácticas y realistas**.

Cuándo testear es tan importante como qué testear y porqué testear.

Esperar para hacer el test, esperar para reportar los problemas y esperar para solucionarlos, es un error.

Haga las cosas pequeñas, porque en definitiva, todas son cosas pequeñas.

Testear se refiere a los **detalles**, y muy a menudo los pequeños detalles llevan a las más importantes fallas de seguridad.

El **nivel de riesgo** que se determine debe poder ser **medido y cuantificado** según la realidad del Cliente.

Deberán **conocer las herramientas** que utilizarán durante el test como así también su procedencia, también se requiere que sean probadas en ambientes controlados antes de su utilización.

Si durante el test se descubre una vulnerabilidad de **alto riesgo** ésta deberá ser comunicada de inmediato al cliente junto con la solución a la misma

Ethical Hacking – Módulo I

Métodos Avanzados de Hacking y Protección

1. Ethical Hacking y Seguridad de la Información
2. Metodologías de Penetration Testing

3. Hacking

- **Identificación de Intrusos**
- **Tipos de Atacantes**
- **Tipos y consideraciones de los ataques**

4. Know How
5. Laboratorios Prácticos

Identificación de Intrusos

INTRUSO

“Alguien que quiere acceder a los sistemas con o sin autorización pero con fines que pueden perjudicar a la organización”.

HACKER
CRACKER
PHREAKER
EMPLEADOS
OTROS

El mundo Underground-El Mundo de los Sombreros

White Hat: “ Los chicos buenos” también se llaman “Samurais” a los que trabajan para las fuerzas de seguridad o agencias de inteligencia.

Grey Hat: “Mercenarios” trabajan con el que mas paga carecen de ética.

Black Hat: “ Los chicos malos” crackers, virukers y otros



Tipos de Atacantes

Conociendo al Enemigo: ¿Qué los Motiva?

PROTAGONISTAS DEL
**SIGLO
XX**



SIGLO
XXI



- Curiosidad y desafío
- Entretenimiento
- Creencias políticas
- Deseo de información
- Emoción de obtener privilegios de acceso
- Instalar troyanos y puertas traseras
- Intento de comprometer otros sistemas
- Usarlo como trofeo para obtener “status” en el ambiente



Tipos de Atacantes

Perfil del Atacante

Old School: Lentos, cuidadosos, precisos, invasivos

Profesionales: Rápidos, cuidadosos, precisos, algunas veces invasivos

Scripts Kiddies: Lentos, imprecisos, invasivos

Defacers: Rápidos, precisos, medianamente invasivos

Wannabe: Principiantes en el tema, o llegan a su objetivo o quedan en la categoría de Scripts Kiddies

Enfoque

- Los atacantes tienen tiempo ilimitado
- Se deben proteger todos los sistemas del ataque
- Los atacantes sólo deben encontrar un agujero, mientras nosotros debemos cubrir todos.

Go Back.

TUCSON REGION

Global Web fraud case has 17 local indictments

By Laurie Laine

ARIZONA DAILY STAR

Tucson, Arizona | Published: 11.08.2005

Seventeen Tucson-area residents were indicted on charges of using stolen credit and debit card numbers and other personal information to steal money from ATMs as part of an international computer-based theft ring.

The group used card numbers and other financial information supplied by people in foreign countries to make counterfeit bank or credit cards and then wired back half the stolen money as payment, officials said in announcing the federal indictments.

unsealed M...

LANACION.COM

Política

Centro del lector
Ingresar
Registrarse

Noticias | Deportiva | Entretenimientos | Tecnología | Opinión | Edición Impresa

Últimas noticias | Política | Economía | Inf. General | Externo | Ciencia/Salud | Cultura | Humor

Lunes 20 de marzo de 2006 | Publicado en la ed. Impresa: Política | Lectura: A

Noticias | Política | Nota

Irregularidades en el Estado: tráfico de información confidencial

Habrían robado los datos de 12 millones de personas

La justicia federal busca determinar si la Anses filtró registros a una empresa privada

Herramientas
Imprimir
Enviar
Agregar

Tipos y Consideraciones de los Ataques

¿Donde apuntan los ataques ?

Aprovecharse de errores en las aplicaciones

Validación de entrada de datos
Administración de Sesiones
Administración de Cookies
Variables de usuario
Funcionalidad

Aprovecharse de errores humanos

Ataques de diccionario
Dumpster diving
Ingeniería Social

Aprovecharse de vulnerabilidades en los sistemas

SQL Injection
Unicode
HTR Chunked Encoding
Apache Chunked Encoding
Buffer overflows, overrun
Cross Site Scripting

Tipos y Consideraciones de los Ataques

Clases de Ataques

Passive
Active
Close-in
Insider
Distribution

Clases de Ataques

Pasivo

No altera la funcionalidad, sólo escucha y transmite, o simplemente escucha. Análisis de tráfico, monitoreo de comunicaciones, captura de credenciales de acceso. Divulga información sin intentar romperlas por ejemplo obtiene medidas de protección, usuarios y contraseñas.

Activo

Modificación del flujo de datos transmitido o generando uno falso, intenta romper las medidas de protección. Pueden ser: Interrupción, Intercepción, Modificación, Fabricación, Destrucción.

Ataque de cercanía

Son los ataques relacionados con la aproximación de personas a redes, sistemas o dispositivos con el propósito de modificar, obtener o denegar acceso a la información. Ejemplo Wardriving, Warnibling, intercepción de emanaciones electromagnéticas.

Tipos y Consideraciones de los Ataques

Clases de Ataques

Passive
Active
Close-in
Insider
Distribution

Clases de Ataques

Insider Factor

Son personas que ya tienen acceso a la información y pertenecen a la compañía, generalmente provocan disclosure, robo o daño de la información. Usa esa información de una forma fraudulenta o suele bypassar controles para ingresar a sectores restringidos de los sistemas o para obtener beneficios laborales: “getting the job done”.

Ataques de distribución

Distribution attacks se enfocan en la modificación del software o hardware de un producto o durante el proceso de fabricación o durante la distribución se introduce código malicioso como backdoors, loggers para obtener información o acceder a sistemas cuando los dispositivos o los software sean instalados.

Ethical Hacking – Módulo I

Métodos Avanzados de Hacking y Protección

1. Ethical Hacking y Seguridad de la Información
2. Metodologías de Penetration Testing
3. Hacking

4. Know How

- Ataques
- Information Gathering

5. Laboratorios Prácticos



Ataques

Cuando tratamos con seguridad y gestión de riesgos, muchos piensan con respecto a estos aspectos en términos de probabilidades y predecibilidad. Ellos preguntan: ¿Cuales son las chances de que un incidente, amenaza o ataque pueda ocurrir? ¿Cuán predecible es que este evento ocurra?

Lo que dice el manual

entamente proactivas para identificar ataques
organizaciones depende de defensas que estén fortalecidas
con una base de datos de los ataques conocidos.

Un testeador de intrusión sabe que para contrarrestar las defensas, también debe tener una base de datos actualizada sobre los ataques conocidos. Esto ayuda en la rapidez y la efectividad de cada intento. Una y otra vez, determinados "hacks éticos" serán exitosos, y el testeador apreciará mucho estas joyas de su base de datos de ataques, registrando el índice de éxitos.

Armado de esta información, el testeador de intrusión, intentará abusar de la red de su cliente hasta que uno de sus ataques tenga éxito.

Isec Information Security Inc.

PROFESIONALES EN SEGURIDAD DE LA INFORMACIÓN

ETHICAL HACKING

MÉTODOS AVANZADOS DE HACKING Y PROTECCIÓN

Level 1

1. Objetivo: Familiarizarse con el sistema Operativo y ejecutar los comandos básicos necesarios para los testeos.

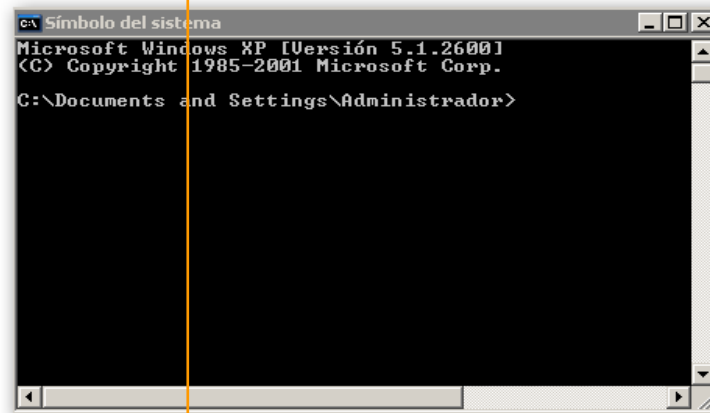
Herramienta: cmd.exe

Analizar e interpretar las salidas de los siguientes comandos.

- > ipconfig
- > ipconfig /all
- > ipconfig /renew
- > ipconfig /flushdns
- > ipconfig /registerdns
- > ipconfig /displaydns

- > ping -t a la ip del compañero
- > ping -t -l 65000 a la ip del compañero

- > arp -a
- > arp -s 157.55.85.212 00-aa-00-62-c6-09, luego > arp -a
- > arp -d *, luego > arp -a



- > net accounts
- > net use \\ipdelcompañero\ipc\$ "" /user:""
- > net view \\ipdelcompañero
- > net use \\ipdelcompañero\ipc\$ /delete

- > netstat -an
- > netstat -r
- > netstat -v

**Hemos llegado,
GRACIAS!!!!!!!**

info@isec-global.com
www.isec-global.com
Office: +54 11 5219-ISEC (4732)

Isec Information Security Inc.

PROFESIONALES EN SEGURIDAD DE LA INFORMACIÓN

ETHICAL HACKING

MÉTODOS AVANZADOS DE HACKING Y PROTECCIÓN