



**Seguridad Informática**  
Junio 2008

**SE**

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Introducción

- Debido a que la tecnología avanza constantemente, la seguridad informática se ve en la misma necesidad de ir en paralelo con este avance.
- Como es de esperarse este crecimiento se dio junto con los delitos cibernéticos los cuales son aplicados a través de numerosas técnicas, que igualmente los intrusos van depurando.
- Esta diversidad de delitos va desde el engaño, soborno, extorsión, ataques realizados con dolo y mala fe que afectan a cualquier institución.
- Estos delitos provocan grandes pérdidas a cualquier empresa o institución,

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Objetivo

- Concienciar a los usuarios de sistemas informáticos, redes, Internet o telecomunicaciones, que existe un gran riesgo en el uso irresponsable de dicha tecnología.
- Recordar siempre que el menor de los riesgos es el tener que volver a instalar el software de la computadora para reestablecerla, de ahí en adelante el daño puede ir en aumento, sin contar el costo de horas hombre perdidas.
- Conocer las técnicas que se utilizan para explotar las vulnerabilidades que afectan las aplicaciones y sistemas operativos, que pueden afectar la información del registro.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Historia 1/2

- "A finales de la década de los 60, el Ministerio de Defensa de los Estados Unidos desarrollo una red experimental de computadores para aplicaciones e investigaciones de tipo militar, a la que se denomino ARPANET(Advanced Research Projects Agency Network). Las principales aplicaciones de la red ARPA permitieron compartir recursos a lo largo de todo el país y desde sus comienzos los usuarios le dieron aplicaciones de intercambio de información".
- A finales de la década de los 70 se creo un comité informal que trabajó en lo que se denomino protocolos TCP/IP (Transmission Control Protocol/Internet Protocol).

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Historia 2/2

- Hacia 1983 se dio el paso definitivo a estos protocolos y la red ARPA fue dividida en dos partes:
- **MILNET (Red Militar)** la primera y la más grande, se destinó para aplicaciones militares.
- La otra parte continuó su aplicación a la investigación, se convirtió en la espina dorsal de lo que es hoy la red de redes de computadores más grandes del mundo, conocida como **INTERNET**.
- A finales de los 80's no se le daba importancia a la seguridad en las redes de computadoras, no obstante, Internet iba creciendo de forma acelerada al sumarse redes considerables a alrededor del mundo.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## Hacker

- Se utiliza el termino Hackers para definir a todas aquellas personas, apasionadas de la informática, que disfrutan intentando acceder a otros ordenadores, burlando la seguridad de los sistemas; cuanto mas difícil y mas complejo sea el acceso, mayor será el reto.
- El fin de los hackers es aprender y divertirse, por lo que es frecuente que una vez conseguido el acceso lo comuniquen a la persona correspondiente, para que los sistemas de seguridad sean mejorados y así tener una meta más difícil.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Cracker 1/3

- Es una persona que rompe la seguridad de los sistemas persiguiendo un objetivo **ilícito**, suelen tener ideales políticos o filosóficos, o bien se mueven por arrogancia, orgullo, egoísmo, ambición.
- Un cracker actúa del mismo modo que un hacker, pero una vez que logra ingresar al sistema no se da por satisfecho, sino que le hace “crac”, es decir, lo quiebra. Sus hazañas típicas son la copia de información confidencial, movimientos de pequeñas sumas de dinero y compras a nombre de otros.
- Están ligados también a la piratería, al permitir que las compañías utilicen demos de ciertas aplicaciones como si tuvieran la licencia de las mismas

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Cracker 2/3

- Quien suministre la información al cracker intentará que la víctima del ataque no sea consciente de que ha ocurrido algo anormal. Para ello, lo mejor es realizar una discreta copia de los datos contenidos en la computadora de la víctima de manera directa o través del módem o las redes de la compañía.
- Por ejemplo, para dar con una clave de acceso, el cracker sabe de ciertas palabras que la gente suele utilizar, por lo que la víctima debe ser consciente de esto y evitar en lo posible caer en convenciones tales como: letras muy cercanas; nombre y apellido; el login, pero con una pequeña alteración;

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Cracker 3/3

- También realiza combinaciones de nombre-apellido o iniciales; nombre del novio(a) del hermano(a), tío(a), hijo(a), madre, padre; calle en donde vive;
- Fecha de nacimiento; combinaciones nombre-fecha;
- Nombre del equipo favorito de fútbol americano (la palabra Dallas se encuentra entre las primeras en las utilerías que los crackers utilizan para quebrar contraseñas), entre otras.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Phreacker

- Personas que intentan usar la tecnología para explorar y/o controlar los sistemas telefónicos.
- Originalmente, este término se refería a los usuarios de las conocidas "blue boxes" (dispositivos electrónicos que permitían realizar llamadas gratuitamente).
- Ahora bien, como en la actualidad las compañías telefónicas utilizan sistemas digitales en lugar de electromecánicos, los phreakers han pasado a utilizar muchas de las técnicas de los hackers.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Ataques

- **Robert Thomas Morris**
- El 3 de noviembre de 1988, equipos como VAX y SUN conectados al Internet se vieron afectados en su rendimiento y posteriormente se paralizaron. Se vieron afectados Bancos, Universidades e instituciones de gobierno, la causa fue un GUSANO, desarrollado por **Morris**, recién graduado en Computer Science en la Universidad de Cornell.
- Se estimó que en 90 minutos, el gusano logró infectar 6.000 equipos alrededor del mundo originando pérdidas entre 100.000 a 10.000.000.



# Seguridad de la Información

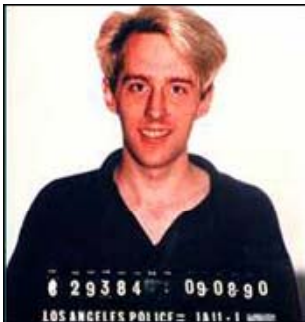


SECRETARÍA  
DE ECONOMÍA

SE

## ■ Phreacker

- **Kevin Poulse** paso a la fama al ganarse un Porsche, claro, de manera ilícita.
- La estación de Radio KII-FM en los Angeles, celebró un aniversario organizando un concurso, el cual consistía en que la llamada número 102 que entrara a la Radio, sería la ganadora del Porsche 944 S2, Kevin había phackeado la central telefónica de "Pacific Bell" de tal forma que aseguro que su llamada fuese la 102.



# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Cracker



- **Kevin David Mitnick**, es quizás el más famoso hackers de los últimos tiempos. descubrió y reveló información de alta seguridad perteneciente al FBI, incluyendo cintas del consulado de Israel, en Los Ángeles.
- Fue capturado en 1995 y liberado en el 2000, después de permanecer casi 5 años en un prisión federal
- Le **costó al estado norteamericano y a empresas privadas, millones de dólares** al ser objeto de hurto de su software, información y alteración de los datos de las mismas. (unas de sus víctimas Motorola, Novell, Nokia y Sun Microsystems, el FBI, el Pentágono y la Universidad de Southern California).

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Cracker



- **Vladimir Levin** graduado en matemáticas de la Universidad Tecnológica de San Petesburgo, Rusia, fue acusado y preso por la Interpol después de meses de investigación por ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, sustraer más de 10 millones de dólares, de cuentas corporativas del Citibank. fue sentenciado a 3 años de prisión y a pagar la suma de US \$ 240,015.
- Los técnicos tuvieron que mejorar sus sistemas de seguridad contra "crackers" y Vladimir Levin ahora se encuentra en libertad

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Gusanos y Caballos de Troya

- Gusano o Worm Son programas que tratan de reproducirse a si mismo, no produciendo efectos destructivos sino el fin de dicho programa es el de colapsar el sistema o ancho de banda, replicándose a si mismo.
- Caballo de Troya o Camaleones Son programas que permanecen en el sistema, no ocasionando acciones destructivas sino todo lo contrario suele capturar datos generalmente password enviándolos a otro sitio, o dejar indefensa a la PC donde se ejecuta,

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

- Joke Program simplemente tienen un payload (imagen o sucesión de estas) y suelen destruir datos.
- Bombas Lógicas o de Tiempo Programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o un estilo técnico (Bombas Lógicas), etc... Si no se produce la condición permanece oculto al usuario.
- Retro Virus Este programa busca cualquier antivirus, localiza un bug (fallo) dentro del antivirus y normalmente lo destruye.
- Virus Son una combinación de gusanos, caballos de troya, joke programs, retros y bombas lógicas. Suelen ser muy **DESTRUCTIVOS**. "La vida de un virus".

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Administración de la Seguridad

- Análisis de amenazas
- Análisis de vulnerabilidades
- Plan integral de seguridad informática
- Políticas
- Estándares
- Procedimientos
- Clasificación de activos informáticos
- Integrar un grupo de responsables de la Seguridad informática
- Auditorias

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ Clasificación de la información

- Pública
  - La que se encuentra al alcance del público.
- Interna
  - La que se distribuye únicamente al personal de la organización o institución
- Confidencia
  - No puede ser divulgada a individuos no autorizados, podría causar un impacto negativo y significativo a la institución o empresa.
  - Ejemplos llaves privadas, información de clientes o de áreas de negocios etc.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

- **Planes de contingencia**
  - Plan de contingencia puede considerar dos escenarios en los que se debe conocer como deberá operar en caso de alguna contingencia
    - Que falle o falte un elemento interno de la organización
      - Dispositivos informático
    - Falle un elemento externo de la empresa
      - Proveedor de mantenimiento.

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

- **La seguridad informática**
  - Esto involucra principalmente tres aspectos
    - Confidencialidad
    - Integridad
    - Disponibilidad

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

- **La seguridad informática**
  - Esto involucra principalmente tres aspectos
    - Confidencialidad
    - Integridad
    - Disponibilidad

# Seguridad de la Información



SECRETARÍA  
DE ECONOMÍA

SE

## ■ La seguridad informática

- Esto involucra principalmente tres aspectos
  - Confidencialidad, proteger la información de ser leída o copiada por personas no autorizadas
  - Integridad, proteger la información de ser borrada o modificada, sin autorización
  - Disponibilidad, que la información este disponible en todo momento.