Seguridad Informática

Introducción

Seguridad es "Salvaguardar propiedades y personas contra el robo, fuego inundación contrarrestar huelgas y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio"

Henry Fayol

Conceptos Clave

- Protector: poseedor del valor
- Agresor: aspirante a poseedor
- Valor: elemento a proteger

Tipos de agresores

- Internos: piensa que el interés de la organización está por encima de sus interés por lo tanto actúa para sobre poner su interés personal.

- Externos: actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, informacion, etc).

Objetivo de la Seguridad Informática

"Será mantener la Integridad, Disponibilidad, Privacidad (aspectos fundamentales), Control y Autenticidad de la información manejada por computadora"

ALDEGANI

"Downsizing"

Las computadoras pasaron de ser grandes máquinas que ocupaban mucho espacio a ser pequeños elementos perfectamente manejables.

La característica más importante que se perdió fue la seguridad.

Amenazas para la seguridad

Amenaza es como cualquier elemento que comprometa al sistema.

Se pueden analizar las amenazas en tres momentos

1. La prevención (antes)
2. La detección (durante)
3. La recuperación (después)

Relación Operatividad - Seguridad

Relación Operatividad - Seguridad

La Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad de un sistema informático, su operatividad desciende y viceversa

$$Operatividad = \frac{1}{Seguridad}$$

Seguridad Física

Consiste en "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"

Antonio Villalón -Seguridad en Unix y Redes

Tipos de desastres

- Desastres naturales
- Amenazas ocasionadas por el hombre
- Disturbios, sabotajes internos y externos deliberados

Desastres Naturales

- Incendios
- Inundaciones
- Condiciones Climatológicas
  - Terremotos

Amenazas hechas por el hombre

- Alejar señales de radar
- Instalaciones eléctricas hecha por especialista
- Picos eléctricos
- Cableado
  - Interferencia
  - Corte del cable
  - Daños en el cable

Recomendaciones / Estándares

- Cableado de alto nivel de Seguridad (por presión)
- Pisos de placas extraíbles
- Sistema de aire acondicionado
- Estructura física reforzada

Acciones Hostiles

- Robo: robar tiempo de máquina o información importante.
- Fraude: las computadoras han sido instrumento para dichos fines.
- Sabotaje: daño que se hace intencionalmente (imanes).

Control de Accesos

- Control de personas
  - Algo que posee
  - Algo que sabe
  - Algo que es
  - Algo que puede hacer
- Control de vehículos

Mecanismos de seguridad

- Guardias
- Utilización de Detector de metales
- Sistemas Biométricos
  - Huella digital
  - Verificación de voz
  - Verificación automática de firmas (VAF)

- Seguridad con animales
- Protección electrónica
  - Barreras infrarrojas y micro-ondas
- Detector Ultrasónico
- Detectores pasivos sin alimentación
- Sonorización y dispositivos luminosos
- Circuitos cerrados de televisión

Seguridad Lógica

“Todo lo que no
está permitido debe estar prohibido”

- Restringir el acceso a los programas y archivos, que no son de utilidad para el usuario o que representan un riesgo al ser modificados.

- Asegurar que la información correcta se esté empleando en el procedimiento correcto.

- La información enviada y recibida debe ser íntegra y privada; solo a quien fue enviada debe ser capaz de leer la información y debe llegar tal como se envió.

- Se debe contemplar un plan de contingencia para la transmisión de información.

Controles de Acceso

Las formas más comunes de autenticación son:

- Contraseña, número de identificación, PIN, entre otros.

- Llaves físicas o tarjetas magnéticas.

- Llaves biométricas como: huellas digitales, la voz o la retina.

Tipos de acceso según el rol del usuario:

- Lectura; el usuario solo puede observar la información, pero puede compartirla
- Escritura; puede modificar o eliminar la información como lo desee.
- Creación; cuando se tiene este tipo de acceso es posible crear elementos, campos, archivos o recursos nuevos

Dependiendo de la funcionalidad de la organización pueden existir más estándares

Niveles de Seguridad Informática

- Nivel D: no cumplen ninguna especificación de seguridad.

- Nivel C1: Protección Discrecional: los usuarios deben identificarse y autenticar su identidad.

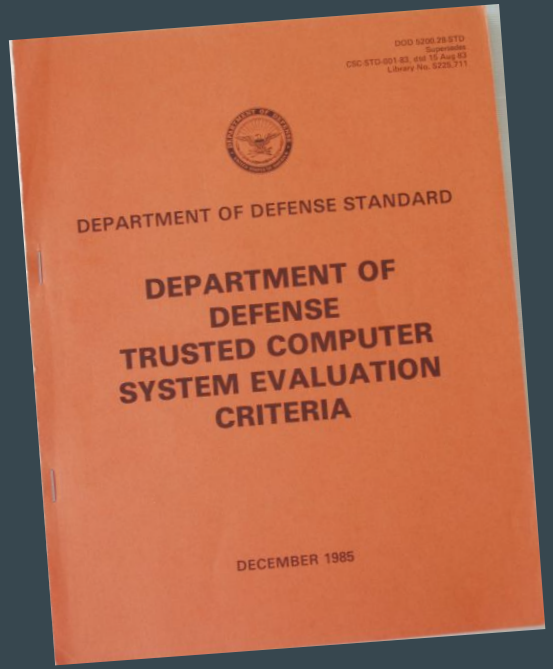
- Nivel C2: Protección de Acceso Controlado: el nivel de acceso es más riguroso. Y algunos usuarios tienen la autorización para realizar tareas de administración.

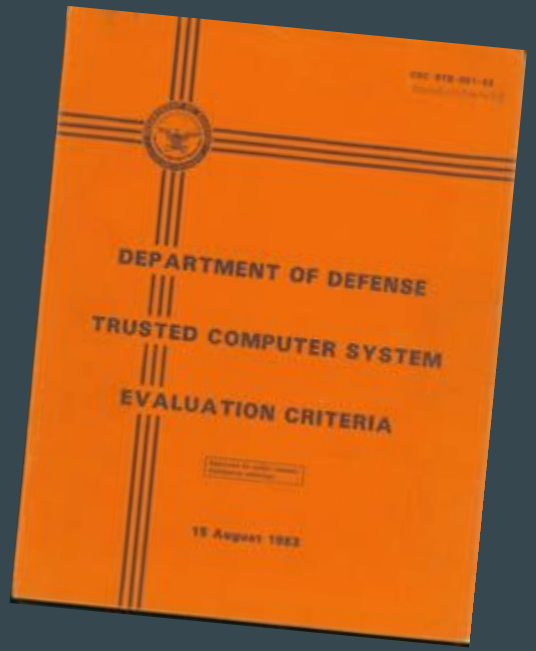
- Nivel B1: Seguridad Etiquetada: crea un nivel de seguridad jerárquico y categórico.

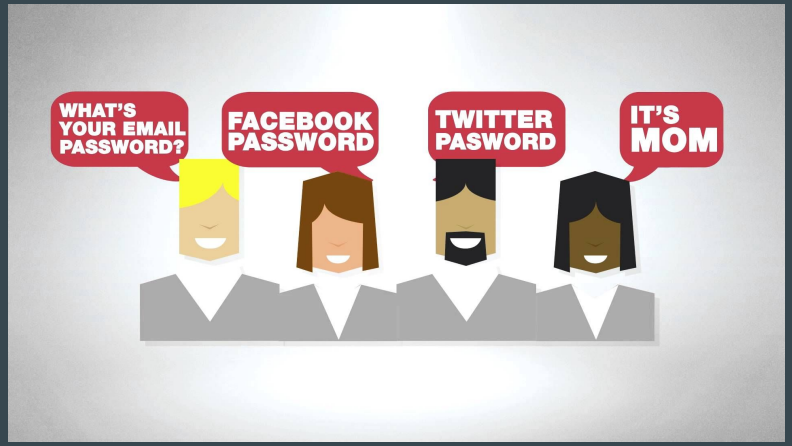
- Nivel B2: Protección Estructurada: se manejan archivos que son accedidos por distintos usuarios. El sistema es capaz de alterar a los usuarios si sus condiciones de accesibilidad.

- Nivel B3: Dominios de Seguridad:Todas las estructuras de seguridad deben ser lo suficientemente pequeñas para poder analizarlas y refuerza los dominios con la instalación de hardware.

- Nivel A: Protección Verificada: debe tener todos los componentes de los niveles inferiores. Y emplea métodos formales.







Ingenieria Social

Técnicas Pasivas

- Observación; es necesario fomentar la memoria visual y la improvisación, pues se debe obtener la mayor cantidad de información en el menor tiempo posible.

- Lenguaje corporal: PNL (Programacion Neurolinguistica)

- En caso de que el objetivo sea un lugar físico, es necesario conocer todas las medidas de seguridad; horarios del personal, cámaras, salidas, entre otros.

- Si el objetivo es una persona, antes de abordarla se debe analizar toda la información disponible del individuo por métodos no intrusivos.

Técnicas no presenciales

- Vía telefónica, el ingeniero social realiza una llamada a su objetivo haciéndose pasar por un técnico de soporte o un asistente de una organización a la cual el objetivo está afiliado.

- Web, los métodos más comunes son los correos electrónicos. Se obtiene información por medio de phishing o infectando el equipo del objetivo.

- Trashing, este método no es el más elegante, pero es bastante sencillo. Se basa en buscar información en basura, o cualquier tipo de almacenamiento.

Prevenciones

- Capacitar al personal.
- No aceptar correos anónimos o conectar dispositivos externos a un equipo de la empresa.
- Se recomienda exigir siempre una explicación del porque requiere cierta información nuestro interlocutor

- Es necesario reconocer que el punto más débil de un sistema informático es el ser humano y su fácil manipulación.

Amenazas Humanas

Existen varios personajes que pueden ser potenciales atacantes del sistema. Se mueven en una delgada e indefinida barrera que separa lo legal de lo ilegal. El término más conocido por el cual son llamados es “hacker”.

La actitud del Hacker

El modo más efectivo de transformarse en un Hacker es imitar la mentalidad de los maestros, no solo intelectualmente, sino además emocionalmente.

El hackerismo es lo que los antropólogos denominan “cultura de la donación”, teniendo esto en cuenta existen cinco clases de cosas que un hacker puede hacer para ser denominado de esta manera.

1. Escribir programas que los demás consideren divertidos y/o útiles, además de donar los programas para que sean utilizados.

2. Ayuda a probar y depurar software libre.

3. Recolecta y filtra información útil e interesante, y construye páginas web o documentos para ponerlos a disposición de los demás.

4. Ayuda a mantener en funcionamiento la infraestructura. La cultura hacker funciona gracias al trabajo voluntario.

5. Hacer algo por la cultura hacker.

Definición de Hacker

Un Hacker es alguien que siempre está en continua búsqueda de información, vive para aprender y todo es un reto para él. El concepto de hacker es generalmente confundido erróneamente por el amarillismo de la prensa, la mitología y la mitomanía de algunas personas.

Un hacker es pirata.

Un hacker es el que entra en los sistemas ajenos y se dedica a destruir la información almacenada en ellos.

Habilidades básicas de un Hacker

El conjunto de habilidades cambia lentamente a lo largo del tiempo a medida que la tecnología crea nuevas tecnologías y descarta otras por obsoletas. Existen dos principales habilidades en un hacker:

1. Aprender a programar.
2. Se considera muy importante aprender Unix

La Ética del Hacker

La comunidad/cultura hacker ha desarrollado un código de ética o serie de principios que son tomados como un acuerdo implícito.

A su vez se desarrollaron unos lineamientos en los cuales se deben de basar al momento de actuar en los sistemas atacados.

Código de Ética

I. El acceso a las computadoras debe ser ilimitado y total.

II. El acceso a la información debe ser libre y gratuito.

III. Desconfíen de la autoridad, promuevan la descentralización.

IV. Los hackers deben ser juzgados por su habilidad, no por criterios absurdos como títulos, edad, raza o posición social.

V. Se puede crear arte y belleza en una computadora.

VI. Las computadoras pueden cambiar tu vida para mejor.

Lineamientos de Ataque

I. Nunca destroces nada intencionadamente en la PC que estés hackeando.

II. Modifica solo los ficheros que hagan falta para evitar tu detección y asegurar tu acceso futuro al sistema.

III. Nunca dejes tus datos reales, tu nombre o tu teléfono en ningún sistema, por muy seguro que creas que es.

IV. Ten cuidado a quien le pasas información. A ser posible no pases nada a nadie que no conozcas su voz, número de teléfono y nombre real.

V. Nunca dejes tus datos personales en un BBS (Bulletin Board System), si no conoces al SysOp (system operator), déjale un mensaje con la lista de gente que pueda responder por tí.

VI. Nunca hackees en computadoras del gobierno. El gobierno puede permitirse gastar fondos en buscarte, mientras que las universidades y las empresas particulares no.

VII. No uses Blue Box a menos que no tengas un PAD local o número gratuito al que conectarte, si se abusa de la Blue Box, puedes ser cazado.

VIII. No des mucha información del sistema que estas hackeando. Di sencillamente "estoy trabajando en ..." pero no digas a quien pertenece, ni el número de teléfono, dirección, etc.

IX. No te preocupes en preguntar, nadie te contestara. Piensa que, por responderte a una pregunta, pueden cazarte a ti, al que te contesta o a ambos.

X. Punto final. Hasta que no estés realmente hackeando, no sabrás que es...

Otros Habitantes del Ciberespacio

Crackers (Black Hat): son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza.

Phreakers: El Phreaking, es la actividad por medio de la cual algunas personas con ciertos conocimientos y herramientas de hardware y software, pueden engañar a las compañías telefónicas para que éstas no cobren las llamadas que se hacen.

Gurús: Son considerados los maestros y los encargados de “formar” a los futuros hackers. Generalmente no están activos, pero son identificados y reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.

Lamers / Script-Kidders: Son aficionados. Prueban todos los programas que llegan a sus manos. Generalmente son los responsables de soltar virus y bombas lógicas en la red sólo con el fin de molestar.

CopyHackers: Literalmente son falsificadores sin escrúpulos que comercializan todo lo copiado (robado).

Bucaneros: Son comerciantes sucios que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers.

Newbie: Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.

Samurai: Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.

Piratas Informáticos: Este personaje (generalmente confundido con el hacker) es el realmente peligroso desde el punto de vista del Copyright, ya que copia soportes audiovisuales (discos compactos, cassettes, DVD, etc.) y los vende ilegalmente.

Otras Actividades

1. **El Carding**, es el uso (o generación) ilegítimo de las tarjetas de crédito (o sus números), pertenecientes a otras personas con el fin de obtener los bienes realizando fraude con ellas.

2. **El Trashing**, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

VLADIMIR LEVIN

KEVIN MITNICK “EL CÓNDOR”

MURPHY IAN “CAPTAIN ZAP”

Amenazas Lógicas

Identificación de las amenazas

Para poder identificar el tipo de amenaza al cual nos enfrentamos es necesario poder conocer los diferentes tipos de ataques, el tipo de acceso, la forma con la que el ataque se llevó a cabo y el objetivo de los o el atacante, estos ataques podrían llegar a producir las siguientes consecuencias:

Identificación de las amenazas

- Data Corruption.
- Denial of Service.
- Leakage.

El ser capaces de poder identificar el ataque es el primer paso para encontrar una solución viable ante el problema.

Tipos de Ataques

- Ingenieria Social
- Ataques de Monitorización
- Ataques De Autentificación
- Ataques DDoS
- Errores de Diseño, implementación y Operación

Ingenieria Social

Este es un tipo de ataque que utiliza la manipulación de las personas para convencerlas de que ejecuten acciones o actos que normalmente no se realizan para sobrepasar la seguridad del sistema.

Ataques de Monitorización

Este tipo de ataques se realiza mediante la observación de la víctima y sus sistemas con el objetivo de obtener información.

- Shoulder Surfing
- Señuelos
- Scanning

Ataques De Autentificación

Este tipo de ataque tiene como objetivo engañar al sistem de la víctima para ingresar al mismo.

- IP Splicing
- IP Spoofing

Ataques DDoS

Estos tipos de ataque consiste en saturar los servidores con mensajes similares para hacer que estos se caigan y a diferencia de sus predecesores estos no provienen solamente de una IP si no de varias.

Cómo “Prevenir” Estos Ataques

Virus Informaticos

Este es un pequeño programa, invisible para el usuario he indetectable por el sistema operativo, su actuar es específico y subrepticio.

Tipos de Propagación

Tipos de Virus

- Archivos ejecutables
- Virus en el sector de Arranque
- Macrovirus
- Gusanos
- Caballos de Troya

Programas antivirus

Protección

Primeros conceptos

Es necesario conocer las vulnerabilidades y ataques a las que un sistema puede estar expuesto para poseer las herramientas necesarias para protegerlo de dichas vulnerabilidades y ataques. Mientras que la seguridad física es un poco obvia, por otra parte hay algunas que no tanto, algunas son tan peligrosas que dan una falsa seguridad.

Vulnerar para proteger

Las personas ajenas al sistema utilizan muchas técnicas para romper la seguridad en un sistema. En términos simples, buscan los puntos débiles del sistema para poder colarse entre ellas, es decir, en este punto no tiene nada que ver lo que hacen los administradores o los testers, ellos se han especializado en técnicas avanzadas para estas tareas.

Administración de la seguridad

Las tareas de administración de seguridad pueden ser divididas en tres grandes grupos:
Autenticación: establece las entidades que pueden o no tener acceso al universo de recursos de cómputo que cierto medio puede ofrecer.
Autorización: se refiere a separar las distintas áreas a las que el usuario tiene acceso dentro del sistema de cómputo.
Auditoría: es la continua vigilancia de los servicios en producción. En esta rama se encuentran el mantener las estadísticas de acceso, estadísticas de uso y políticas de acceso a recursos.

Políticas como primer paso

En la mayoría de los casos, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad agradable, puesto que reflejan su gran voluntad de “hacer algo” que permita detener un posible ataque antes de que este suceda (proactividad). A continuación vamos a citar algunos de los métodos de protección más usados comúnmente.

Penetration Test

“El Penetration Test es un conjunto de metodologías y técnicas, para realizar la evaluación integral de las debilidades de los sistemas informáticos. Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos.”

Penetration Test Externo

El objetivo del mismo es acceder en forma remota a los equipos de la organización y posicionarse como administrador del sistema. Se realizan desde afuera del Firewall y consiste en penetrar la zona desmilitarizada para luego acceder a la red interna. Se compone de un elevado número de pruebas.

Penetration Test Interno

Este tipo de testeo trata de demostrar cual es el nivel de seguridad interno. Se deberá establecer qué puede hacer un Insider y hasta dónde será capaz de penetrar en el sistema siendo un usuario con privilegios bajos. Este Test también se compone de numerosas pruebas.