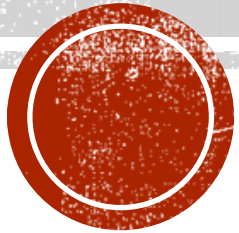
FUNDAMENTOS DE SEGURIDAD DE LA INFORMACIÓN

Unidad I



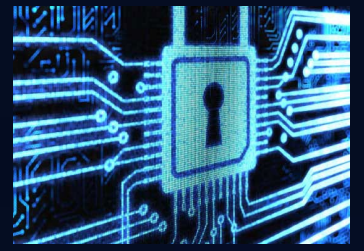
INTRODUCCIÓN

- La seguridad de la información no garantiza la seguridad de su organización, de su información o de sus sistemas de computo. La seguridad de la información no puede por si misma proporcionar la protección para su información. Por decirlo así, la seguridad de la información no es magia negra.
- De muchas maneras, la seguridad de la información es una resolución. Hay que estar resuelto a examinar las amenazas y las vulnerabilidades de su organización y manejarlas apropiadamente.

¿QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN?

- De acuerdo con el diccionario en línea Merriam-Webster
  - "conocimiento obtenido a partir de la investigación, el estudio, inteligencia, noticias, hechos, datos, una señal o carácter; representando datos, algo que justifique el cambio en una construcción que representa la experiencia física o mental u otra construcción.
  - Estar libre de peligro, a salvo; libre de miedo o de la ansiedad
- Uniendo las dos definiciones
  - Medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimiento, hechos, datos o capacidades

HISTORIA DE SEGURIDAD



- Seguridad Física
- Seguridad en las comunicaciones
- Seguridad de las emisiones
- Seguridad Computacional
- Seguridad de Redes
- Seguridad de la información

BREVE HISTORIA

TIPOS DE ATAQUES

- **Ataque** es cualquier acción que explota una vulnerabilidad

- Existen cuatro categorías principales de ataques
  - Acceso
  - Modificación
  - Denegación de servicio
  - Refutación

- Los ataques pueden ocurrir a través de medios técnicos como herramientas especificas diseñadas para ataques o mediante explotación de vulnerabilidades en un sistema de computo o pueden presentarse a través de una ingeniería social.

INGENIERÍA SOCIAL

Es simplemente el uso de medios no técnicos para obtener acceso no autorizado.

Por ejemplo

Haciendo llamadas telefónicas o entrar en una instalación pretendiendo ser un empleado en ella

LOS ATAQUES PUEDEN EJECUTARSE POR DIVERSOS MOTIVOS:

- para obtener acceso al sistema;
- para robar información, como secretos industriales o propiedad intelectual;
- para recopilar información personal acerca de un usuario;
- para obtener información de cuentas bancarias;
- para obtener información acerca de una organización (la compañía del usuario, etc.);
- para afectar el funcionamiento normal de un servicio;
- para utilizar el sistema de un usuario como un "rebote" para un ataque;
- para usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable

ATAQUE DE ACCESO

- Es un intento de obtener información que el atacante no esta autorizado a ver.
  - Se puede presentar en cualquier lugar donde en el que la información este depositada.
  - O se puede presentar durante la transmisión.

- Este ataque esta dirigido contra la confidencialidad de la información

TIPOS DE ATAQUES DE ACCESO

- Fisgoneo

  Consiste en hurgar entre los archivos de información con la esperanza de hallar algo interesante.

- Escuchar furtivamente

  Cuando alguien escucha una conversación de la que no forma parte.

- Intercepción

  Es un ataque activo contra la información. Cuando un atacante intercepta información y la captura antes de que alcance su destino.

Flujo Normal

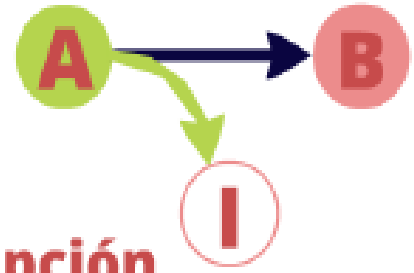
Interrupción

Interrupción

En el caso de una interrupción un activo del sistema se pierde, se hace no disponible o inutilizable. Un ejemplo de ello puede ser la destrucción maliciosa de un dispositivo de hardware o el borrado de un programa o archivo.

Flujo Normal

Intercepción



Intercepción

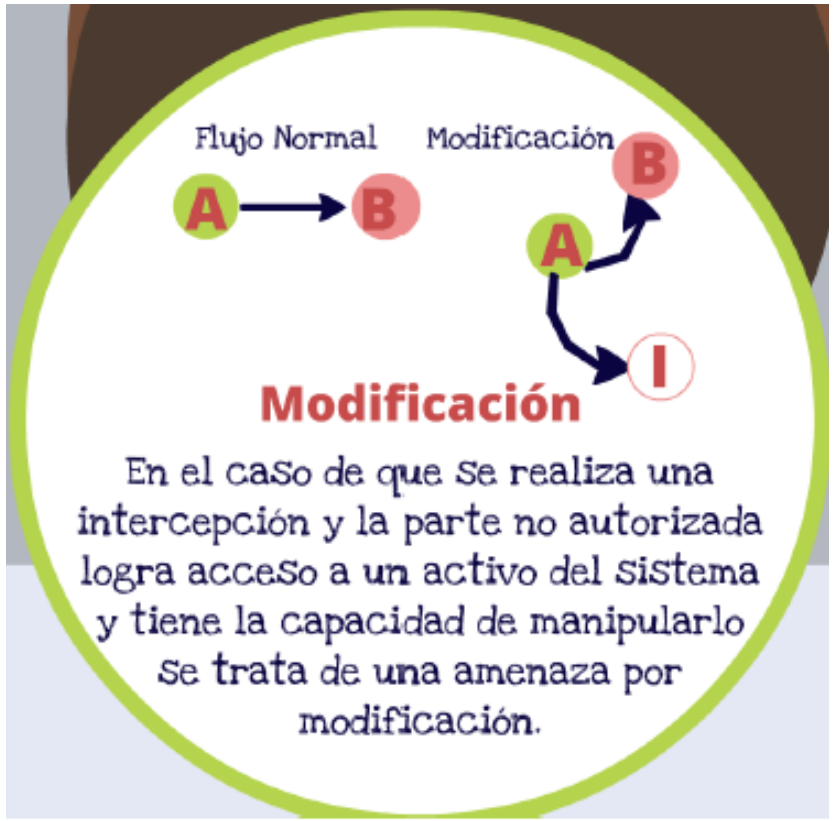
En el caso de una intercepción implica que alguien logre acceso no autorizado a un activo del sistema. Esta parte no autorizada puede ser una persona, programa, dispositivo, etc. Un ejemplo de ella puede ser el copiado de datos, la intervención de un canal de red.

ATAQUES DE MODIFICACIÓN

- Es un intento modificar la información que un atacante no esta autorizado a modificar.
- Este tipo de ataque es en contra de la integridad de la información

TIPOS DE ATAQUES DE MODIFICACIÓN

- Cambios
  - Es cuando se modifica la información
- Inserción
  - Es cuando se agrega información que no existía con anterioridad
- Eliminación
  - Es la remoción de la información existente


Flujo Normal
A
B
Modificación
B
A
I
Modificación
En el caso de que se realiza una intercepción y la parte no autorizada logra acceso a un activo del sistema y tiene la capacidad de manipularlo se trata de una amenaza por modificación.


Flujo Normal
A
B
Fabricación
A
B
I
Fabricación
La parte no autorizada que accede al sistema también puede crear objetos falsos en un sistema. Ejemplo de ello son la inserción de transacciones en un sistema o BD, fabricación de paquetes de datos, etc.

ATAQUES DE DENEGACIÓN DE SERVICIO (DOS, DENIAL OF SERVICE)

- Son ataques que niegan el uso de los recursos a los usuarios legítimos del sistema, de la información o de las capacidades.

Denegación de servicio

Podríamos definir los ataques DOS (Denegation Of Service) como la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También se incluyen en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso.

TIPOS DE ATAQUES DE DENEGACIÓN DE SERVICIO

- Denegación de acceso a la información
  - Provoca que dicha información no este disponible
- Denegación de acceso a las aplicaciones
  - Es un ataque en contra de un sistema de computo que ejecuta la aplicación
- Denegación de acceso a sistemas
  - En este tipo de ataque, el sistema junto con todas las aplicaciones que corren en el mismo y toda la información que se encuentra almacenada en el, dejan de estar disponibles.
- Denegación de acceso a comunicaciones
  - Este tipo de ataque puede abarcar desde cortar un alambre para entorpecer las comunicaciones de radio hasta inundar redes con trafico excesivo.

Existen tres tipos básicos de denegación de servicio:

- Consumo de recursos: El atacante intenta consumir los recursos del servidor hasta agotarlos: ancho de banda, tiempo de cpu, memoria, disco duro...
- Destrucción o alteración de la configuración: Se intenta modificar la información de la máquina. Este tipo de ataques necesitan de técnicas más sofisticadas.
- Destrucción o alteración física de los equipos: Se intenta denegar el servicio destruyendo físicamente el servidor o algunos de sus componentes, cortando el cable de conexión, o el cable de la red eléctrica.

ATAQUES DE REFUTACIÓN

- Es un intento de proporcionar información falsa o de negar que una transacción o evento reales hubieran ocurrido

TIPOS DE ATAQUES DE REFUTACIÓN

- Simulación
  - Es un intento de actuar como, o hacerse pasar, por alguien mas o por algún otro sistema.
- Denegación de un evento
  - Es simplemente negar que la acción se haya realizado como fue registrada

HACKER

- Son aquellos individuos que buscan entrometerse en sistemas de computo o hacer que tales sistemas queden inutilizables.
- Los hackers suelen ser
  - Del sexo masculino
  - Con edades entre los 16 y los 35 años
  - Personas solitarias
  - Inteligentes
  - Técnicamente muy competentes

MOTIVACIÓN DE HACKER

- Retos
  - Presumir sus logros
- Codicia
  - Ganar dinero, bienes, servicios o información
- Propósito malintencionado
  - Es el vandalismo o cometer actos malintencionados

TÉCNICAS DE LOS HACKERS

- Compartición Abierta
- Contraseñas deficientes
- Fallas de programación
- Ingeniería social
- Desbordamiento del búfer
- Denegación de servicio

CÓDIGO MALINTENCIONADO

- Cubre tres diferentes tipos de programas:
  - Virus
    - Son programas que van a cuestas de otros programas ejecutables
  - Programas de caballos de Troya
    - Es un programa completo y autocontenido que está diseñado para realizar algún tipo de acción malintencionada. Oculta su naturaleza maliciosa detrás de la fachada de algo útil o interesante.
  - Gusanos
    - Es un programa que se arrastra de sistema en sistema sin ninguna ayuda de sus victimas. Este se extiende por sus propios medios y también se reproduce por si mismo

Caballos de Troya

Malware que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Puede ser muy peligroso cuando es un programador de la propia empresa quien lo instala en un programa.

Spam

El spam o correo no deseado, si bien no lo podemos considerar como un ataque propiamente dicho, lo cierto es que provoca hoy en día pérdidas muy importantes en empresas y muchos dolores de cabeza.

Virus

Código diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, las macros de aplicaciones y archivos ejecutables.

Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red como ya estamos acostumbrados.

SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

- Confidencialidad
- Integridad
- Disponibilidad
- Responsabilidad

CONFIDENCIALIDAD

- Mantiene el secreto de la información.
- Cuando se utiliza apropiadamente, la confidencialidad permite que solamente los usuarios autorizados tengan acceso a la información.

INTEGRIDAD

- Mantiene la exactitud de la información.
- Cuando se utiliza adecuadamente, la integridad permite que los usuarios tengan la confianza de que la información es correcta y que no ha sido modificada por un individuo no autorizado

DISPONIBILIDAD

- Mantiene la utilidad de la información.
- La disponibilidad permite a los usuarios tener acceso a los sistemas de computo, a la información en los sistemas y a las aplicaciones que realizan operaciones sobre la información

RESPONSABILIDAD

- Suele ser olvidado cuando hablamos de seguridad.
- La razón principal es que el servicio de responsabilidad no protege contra los ataques por si mismo

	Confidencialidad	Integridad	Disponibilidad	Responsabilidad
Acceso	X			X
Modificación		X		X
Denegación del servicio			X	
Rechazo		X		X