Unidad 5. Administración de incidentes

DESARROLLO Y GESTIÓN DE SEGURIDAD DE REDES

5.1 Preparación para un ataque

Un ataque es un evento exitoso o no, que atenta sobre el buen funcionamiento del sistema.

En el flujo normal de la información no debe existir ningún tipo de obstáculos para que la información llegue al destinatario.

Amenazas o ataques

Las cuatro categorías generales de amenazas o ataques son las siguientes:

Interrupción

1. Intercepción
2. Modificación
3. Suplantación o fabricación

Ataques pasivos
Ataques activos.

Amenazas o ataques

INTERRUPCIÓN

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.

Ejemplos de estos ataques: destrucción de un elemento de hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de archivos.

Flujo con interrupción

Amenazas o ataques

INTERCEPCIÓN Y MODIFICACIÓN

Se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema. Este es un ataque en contra de la confidencialidad.

Ejemplos de este tipo de ataque: acceso a una base de datos, entrada a través de la red en un sistema informático ajeno, etc.

Amenazas o ataques

INTERCEPCIÓN

Amenazas o ataques

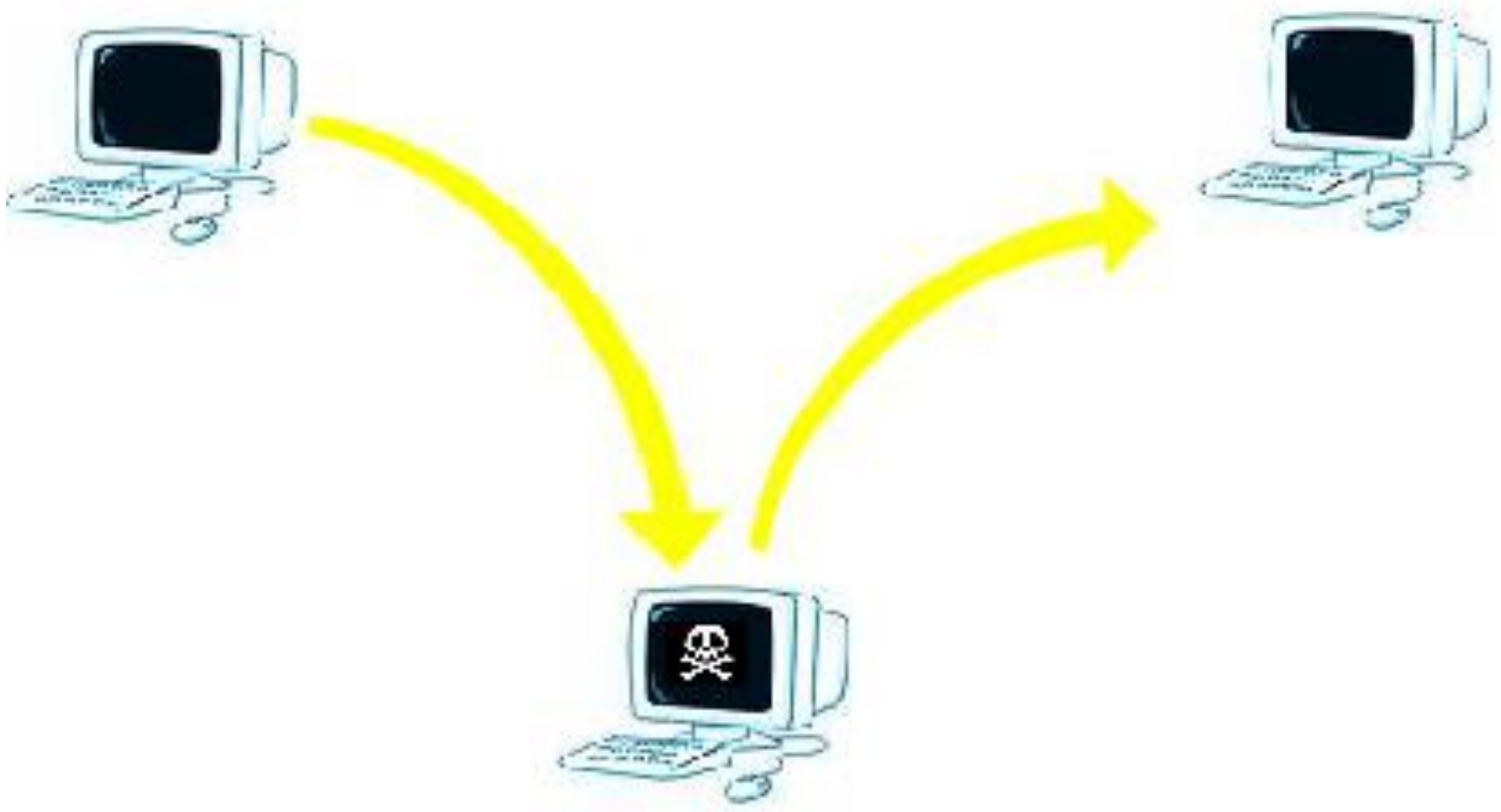
INTERCEPCIÓN Y MODIFICACIÓN

Intercepción se produce cuando un programa, proceso o persona accede a una parte del sistema para la cual no tiene autorización. Es el incidente de seguridad más difícil de detectar, ya que generalmente no produce una alteración en el sistema. Este es un ataque en contra de la confidencialidad.

Ejemplos de este tipo de ataque: acceso a una base de datos, entrada a través de la red en un sistema informático ajeno, etc.

Amenazas o ataques

MODIFICACIÓN



Amenazas o ataques

SUPLANTACIÓN O FABRICACIÓN

Una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

Ejemplos de este tipo de ataques: virus informáticos, caballos de Troya, transacciones electrónicas falsas, introducción de datos en una base, etc.

Amenazas o ataques

SUPLANTACIÓN O FABRICACIÓN

Ataques Pasivos

Los ataques pasivos reciben su nombre debido a que el atacante (o perpetrador u oponente o persona que se entromete) no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida.

Cualquier ataque pasivo tiene los siguientes objetivos principales:

- Intercepción de datos: consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje.
- Análisis de tráfico: consiste en la observación de todo tráfico que pasa por la red.

Ataques Pasivos

Con los ataques pasivos se obtiene información que puede consistir en:

- Obtención del origen y destinatario de la comunicación, con ello se determina la localización y la identidad de los anfitriones (emisor, receptor).
- Control de volumen de tráfico intercambiado entre las entidades monitoreadas, de esta forma se obtienen todos los datos necesarios para percatarse de la actividad o inactividad inusuales.
- Control de las horas habituales del intercambio de datos entre las entidades de la comunicación, con ello se extraen los datos acerca de los periodos de actividad.

Ataques Activos

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido –modificación de la corriente de datos- o la creación de un falso flujo de datos –creación de una corriente falsa-.

Los ataque activos pueden clasificarse de la siguiente manera:

- Enmascaramiento o suplantación de identidad: el intruso se hace pasar por una entidad diferente.
- Replica o reactuación: uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que realiza una retransmisión subsecuente.
- Modificación de mensajes: una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados, esto provoca que se produzca un efecto no autorizado.

5.2 Manejo de ataques y vulnerabilidades

Un ataque en un sistema de cómputo contempla tres etapas principales:

1. Preparación: el método de ataque se plantea u otras preparaciones se realizan.
2. Activación: el ataque se activa o dispara
3. Ejecución: la misión se lleva a cabo mediante la desviación de los controles de acceso, violación de secretos o integridad, denegación de servicio, robo de servicios, o simplemente dar a conocer el ataque.

Preparación y planteamiento

Algunas formas de efectuar esta primera etapa son:

Recolección de la información: los individuos que poseen ciertos derechos sobre la información o flujos de información secreta, simplemente recolectan la del sistema que están autorizados a monitorear, sin embargo, las personas externas deben ingeniárselas para obtenerlas, esto pude lograrse a través de engaños, basándose principalmente en convencer a la gente de haga lo que en realidad no debería.

Preparación y planteamiento

Caballo de Troya: un usuario coloca un programa dentro de su dominio de protección, cuando el programa se ejecuta, obtiene los privilegios de dicho usuario, de esta manera se convierte en un cómplice inconsciente ya que envía y concede información a los perpetradores de sus archivos (de forma no aparente).

Propagación programada: se refiere al código malicioso que se introduce en un equipo de cómputo ya que puede multiplicar su ámbito y daño.

Preparación y planteamiento

Puerta trasera: el software contiene mecanismos escondidos que permiten a los diseñadores (o quienes sepan el secreto) desviar los controles.

Enmascaramiento o engaño: significa que se pretende ser alguien más, de tal manera que se puede obtener los derechos de acceso de una persona. El enmascaramiento envuelve un ataque en los controles de autenticación, por lo que el sistema puede enmascarse como otro sistema para engañar al usuario y descubrir información.

Preparación y planteamiento

Exploración: consiste en el enviar una secuencia de información cambiante a una computadora para encontrar valores que muestren respuestas positivas, como son las contraseñas, números telefónicos, etc.

Mal uso de la autoridad: si el atacante penetra de manera legítima al sistema, la preparación es mucho más fácil ya que está haciendo mal uso de la autoridad que posee dentro de la organización.

Activación

En esta segunda etapa, la activación puede realizarse de las siguientes manera:

Si el ámbito de preparación asume el control de una interrupción de un sistema operativo, el código de ataque es invocado cuando la interrupción se lleva a cabo, si no es así, el perpetrador puede invocar directamente un programa que lleve a cabo la misión.

Activación

Un ataque más sofisticado impone un retardo entre la preparación y la activación, el retardo puede provocar que el ataque sea más destructivo, hablando específicamente de los virus.

Una bomba de tiempo se encuentra arreglada para estallar a una hora y día determinados

Ejecución

La ejecución del ataque está sustentado en la misión que se tenga y en esta tercera etapa las misiones pueden ser:

- Mal uso activo
- Mal uso pasivo
- Mal uso activo

Afecta la integridad de la información o disponibilidad de los servicios. Los archivos pueden ser destruidos o sutilmente alterados.

5.3 Técnicas forenses

El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Recoge pruebas con extremo cuidado, respetando la cadena de custodia de dichas evidencias.

5.3 Técnicas forenses

Dichas técnicas incluyen reconstruir el bien informático, examinar datos residuales, autenticar datos y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

La informática forense es una disciplina relativamente joven que empezó a practicarse en los años 80 con el análisis directo de los medios digitales.

5.3 Técnicas forenses

OBJETIVOS

La Informática forense permite la solución de conflictos tecnológicos relacionados con seguridad informática y protección de datos.

Gracias a ella, las empresas obtienen una respuesta a problemas de privacidad, competencia desleal, fraude, robo de información confidencial y/o espionaje industrial surgidos a través de uso indebido de las tecnologías de la información.

5.3 Técnicas forenses

Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

5.3 Técnicas forenses

Mediante sus procedimientos se identifican, aseguran, extraen, analizan y presentan pruebas generadas y guardadas electrónicamente para que puedan ser aceptadas en un proceso legal.

5.3 Técnicas forenses

El análisis forense informático es una prueba clave en numerosas ocasiones, como por ejemplo:

- Revelación de secretos, espionaje industrial y confidencialidad
- Delitos económicos, societarios o contra el mercado o los consumidores
- Delitos contra la propiedad intelectual e industrial
- Vulneración de la intimidad
- Sabotaje
- Uso indebido de equipos
- Amenazas, calumnias e injurias.

5.3 Técnicas forenses

- Cumplimiento de obligaciones y contratos
- Delitos contra la Propiedad Intelectual, en caso de Software Pirata o documentos con el debido registro de derechos de Autor.
- Robo de Propiedad Intelectual y Espionaje industrial (que aunque no se crea, sí existe en nuestro país).
- Blanqueo de Dinero, vía transferencia de fondos por Internet.
- Acoso Sexual (vía e-mail); Chantaje o amenazas (vía e-mail).
- Acceso no autorizado a propiedad intelectual.
- Corrupción.
- Destrucción de Información Confidencial.
- Fraude (en apuestas, compras, etc. Vía e-mail).
- Pornografía en todas sus formas, inclusive en la más devastadora: Pornografía infantil.

5.3 Técnicas forenses

PROCESOS TÉCNICOS DE LA INFORMÁTICA FORENSE

Para obtener pruebas, los investigadores examinaban la "vida interior" de los ordenadores con ayuda de las herramientas de administración del sistema (Sysadmin).

No obstante, esa forma de proceder podía ocasionar la modificación de los datos, lo que a su vez podía dar lugar a alegaciones de falsificación de las pruebas.

5.3 Técnicas forenses

Ello condujo a la adopción de otro enfoque, el análisis forense, que se compone de tres pasos:

1. Identificación y preservación de los datos con el fin de crear un duplicado forense, es decir, una copia exacta de los datos de un soporte digital, sin modificar los datos originales.

5.3 Técnicas forenses

2. Análisis de los datos así protegidos por medio de un software especial y de métodos para la recopilación de pruebas. Medidas típicas son, por ejemplo, la búsqueda de contraseñas, la recuperación de archivos borrados, la obtención de información del registro de Windows (base de datos de registro), etc.
3. Elaboración de un informe por escrito sobre las evidencias descubiertas en el análisis y en el que se incluyan también las conclusiones extraídas del estudio de los datos y de la reconstrucción de los hechos o incidentes.

Actividad de Tarea

Realiza un RESUMEN con las Herramientas para la seguridad informática [software de seguridad] que se encuentran en la actualidad y la cuantificación del valor de la seguridad.

Se entregará en una presentación de PPT por correo electrónico, mañana martes, 9 de febrero antes de las 9:00am

Bibliografía

Seguridad Informática
http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/MetodoAtaque.php

Informática Forense
http://www.gitsinformatica.com/forense.html