CAPÍTULO 2
Conceptos Generales de Seguridad

La mejor forma de predecir el futuro es crearlo.
[Peter Drucker]

En un entorno, donde cada vez mas dispositivos se incorporan a una misma red para el intercambio de información, debemos conocer los riesgo que se generan.

La seguridad significa que el costo para romperla excede al costo del bien de cómputo asegurado, esto es, el tiempo requerido para romper la seguridad, excede el tiempo de vida útil del bien de cómputo, siendo éste último hardware, software o información.

2.1. Principios básicos de seguridad

Se ha observado que los sistemas relacionados o no con la computación tienen debilidades reales, el propósito de la seguridad en cómputo es brindar caminos para prevenir las debilidades que puedan ser explotadas en los sistemas que involucren el uso de hardware, software, transporte e información digital. Actualmente se emplea el término *Seguridad* en muchas actividades de la vida diaria, proteger las casas, pago y compras en Internet, en el automóvil, uso de controles contra desastres y en casos más especiales, hacer uso de seguros que garanticen recuperar el valor de los bienes.

Cuando se hace referencia a la palabra *Seguridad* tiene definiciones como certeza, firmeza, confianza, sin riesgo, dícese de las cosas ciertas, firmes y libres de peligro o riesgo, estado de las cosas bajo protección, confianza, tranquilidad de una persona, procedente de la idea de que no hay ningún peligro que temer.

Cuando se habla a cerca de seguridad en cómputo se hace referencia a todas las medidas para prevenir pérdidas de cualquier clase, significa que se contemplan tres aspectos básicos de cualquier sistema relacionado con el cómputo, confidencialidad, integridad y disponibilidad (figura 2.1).

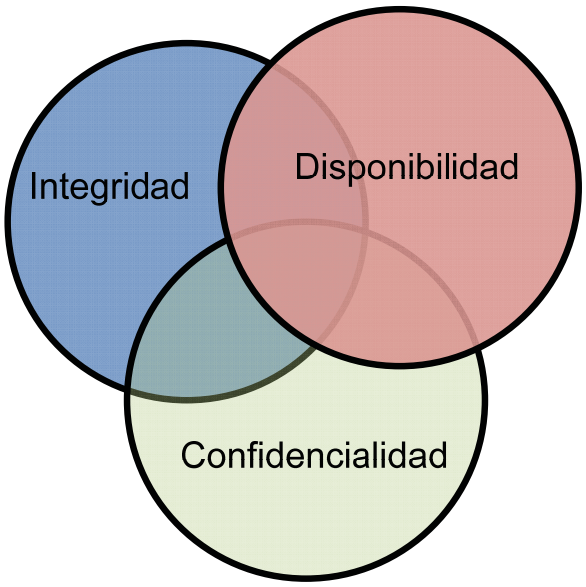

Figura 2. 1 Principios de seguridad.

La seguridad en cómputo intenta asegurar los tres principios, sobre tres activos principales, software, hardware e información, además de la comunicación entre ellos y las debilidades humanas que interactúen con éstos, esto constituye la base de la seguridad en cómputo. Realizar un análisis de la situación actual brinda el panorama para la construcción de un sistema seguro, ayuda a encontrar el balance correcto de los tres factores (integridad, disponibilidad y confidencialidad) para una implementación óptima de seguridad, al definir cuál es el pilar primordial que se desea asegurar sin dejar de pensar en los otros dos.

Como un profesional en la seguridad es importante brindar un balance entre agregar barreras de seguridad para prevenir ataques y permitir que el sistema siga siendo funcional a los usuarios. La seguridad, funcionalidad y facilidad de uso, deben ser contempladas para generar este balance. En general, cuando se incrementa la seguridad, la funcionalidad del sistema y facilidad de uso disminuyen.

1. Integridad

Significa que los activos pueden ser modificados sólo por partes autorizadas o caminos autorizados, en este contexto se incluye escribir, cambiar, modificar estado, borrar y crear.

El término integridad, tiene diferentes significados en distintos contextos, por ejemplo, si se refiere a conservar la integridad de algún elemento, puede significar que el mismo es:

- Idéntico.
- Certero, exacto.
- Sin modificaciones, alteraciones o agregaciones.
- Modificado sólo en formas aceptables.
- Modificado sólo por personas autorizadas.
- Modificado sólo por procesos autorizados.
- Consistente.
- Con sentido.

Integridad puede también significar dos o más de estas propiedades, la integridad está protegida en la mayoría de las ocasiones con controles de acceso que determinan que personas, procesos o entidades tienen acceso a los recursos para lograr escribir, cambiar, modificar, borrar y crear. En los sistemas de cómputo la integridad de los archivos es garantizada empleando algoritmos hash y firma digital.

2. Disponibilidad

Se refiere a que los activos están accesibles para las partes autorizadas en tiempos apropiados, en otras palabras, si una persona o sistema tuvo acceso legítimo a un conjunto de objetos particulares, este acceso no deberá impedirse.

Disponibilidad aplica tanto a datos como a servicios, se dice que un objeto o servicio está disponible si:

- Éste está presente en una forma útil.
- Si tiene capacidad suficiente para prestar el servicio.
- El servicio se completa dentro de un periodo de tiempo aceptable.
- El servicio involucra una filosofía de tolerancia a fallas.
- Tiene concurrencia, que es un acceso simultáneo, administrando tiempos muertos.

En sistemas de cómputo no existe una medida a tomar que garantice la disponibilidad de algún activo al 100%, por las implicaciones en gasto que puede tener esta propiedad de la seguridad, así como las nuevas debilidades que se detectan día a día en los diferentes sistemas en general. En tiempos pasados la seguridad en cómputo fue exitosa enfocándose a la confidencialidad y la integridad, la implementación de disponibilidad es uno de los siguientes grandes cambios.

3. Confidencialidad

Asegura que los activos sean accedidos sólo por partes autorizadas, es importante definir qué se entiende por "acceso", acceso no sólo se refiere a leer, sino también a ver, imprimir o simplemente conocer la existencia de un activo particular. Confidencialidad en algunas ocasiones es también llamada privacidad o secreto.

La confidencialidad es uno de los principios de seguridad que más importancia se le ha dado desde la antigüedad, en el campo militar, diplomático y político se empleaban distintas formas para transportar la información y en caso de caer en manos de un tercero éste no pudiera interpretarla.

Algunas de las maneras que se utilizan para garantizar la confidencialidad son:

- ***Valija Diplomática*** (Mecanismo empleado para enviar información de tal manera que sólo la persona involucrada pueda tener acceso a la información).
- ***Cifrado simétrico*** (Emplean una misma contraseña para ocultar y para recuperar la información).
- ***Cifrado asimétrico*** (Emplea dos contraseñas diferentes, una para ocultar la información y otra para recuperarla).
- ***Mecanismos para ocultar la información de los propietarios.***

2.2. Vulnerabilidades, amenazas, riesgo y control

Cuando se prueba un sistema de cómputo, una de las tareas principales es pensar cómo el sistema podrá tener un mal funcionamiento, de esta manera se busca mejorar el diseño del mismo. Un sistema de cómputo consta de tres componentes que se valoran por separado; hardware, software y datos, cada uno de estos activos tiene un valor propio el cual afecta al sistema de diferente manera, esta estimación es necesario realizarla ya que lleva a determinar la prioridad de atención de los activos. En este proceso intervienen cinco factores: vulnerabilidades, amenazas, riesgo, ataques y control.

Las **vulnerabilidades** son debilidades en el sistema de seguridad, por ejemplo, un procedimiento, diseño, implementación, que pueden ser explotados causando pérdidas o daños, un ejemplo claro es cuando un sistema particular puede tener acceso a datos sin autorización, debido a que éste no verifica la identidad del usuario antes de permitirle el acceso a los datos.

Una **amenaza** a un sistema de cómputo es un conjunto de circunstancias que pueden ser potencialmente causa de pérdidas o daños, para ver la diferencia entre vulnerabilidad y amenaza, se

puede considerar el siguiente ejemplo; un contenedor de agua está limitado por una pared, dicha pared presenta una fisura, el agua al subir de nivel comenzará a ejercer presión en la fisura y causará un daño a la persona que se encuentra fuera al momento que se produzca un desborde de agua, la fisura del muro es una vulnerabilidad que es aprovechada por la fuerza del agua y puede ocasionar lesiones a la persona (figura 2.2).

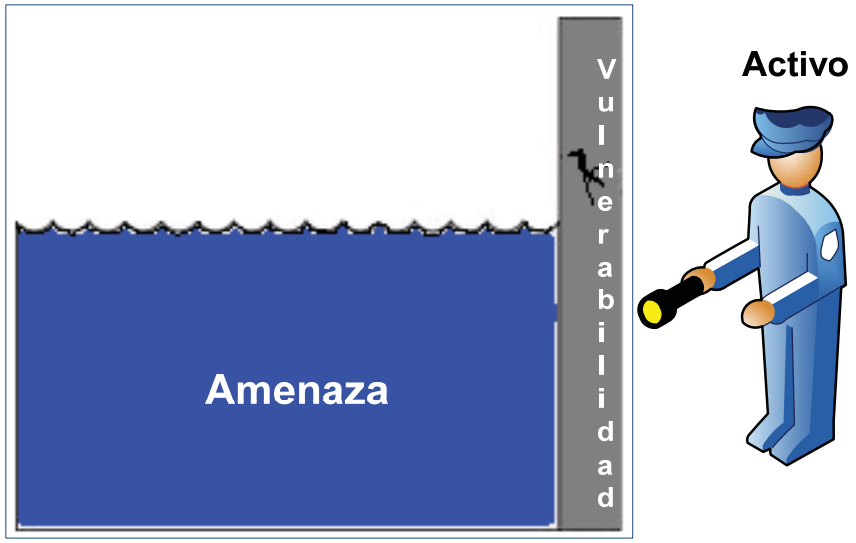

Figura 2. 2 Diagrama amenaza, vulnerabilidad y activo.

Un ***riesgo*** está definido como la probabilidad de que una amenaza explote una vulnerabilidad, además si una amenaza explota una vulnerabilidad se lleva a cabo un ataque, en el caso anterior el riesgo está definido con base en la velocidad de aumento en el nivel de agua.

El ***control o mecanismo*** se define como una medida de protección empleada, un control es un dispositivo, acción, procedimiento o técnica que elimina o reduce una vulnerabilidad, en el caso anterior se podría sellar la fisura con la finalidad de disminuir el riesgo.

Las amenazas presentan cuatro tipos básicos de operación (intercepción, interrupción, modificación y fabricación) enfocados a los tres activos de sistemas de cómputo (figura 2.3).

La ***interrupción*** se refiere a impedir la comunicación entre dos entidades, esto atenta directamente a la disponibilidad.

La ***intercepción*** permite la comunicación entre dos entidades, pero los datos que son trasmitidos pueden ser vistos por un tercero, atenta contra la confidencialidad.

La ***modificación*** involucra a una tercera entidad entre los dos punto principales de una comunicación, permitiéndole modificar la información que se transmiten en ambas direcciones, atenta contra la integridad.

La ***fabricación*****,** es muy similar a la modificación, solo que en ese caso la información transmitida es completamente generada por una tercera entidad, atenta contra la integridad.

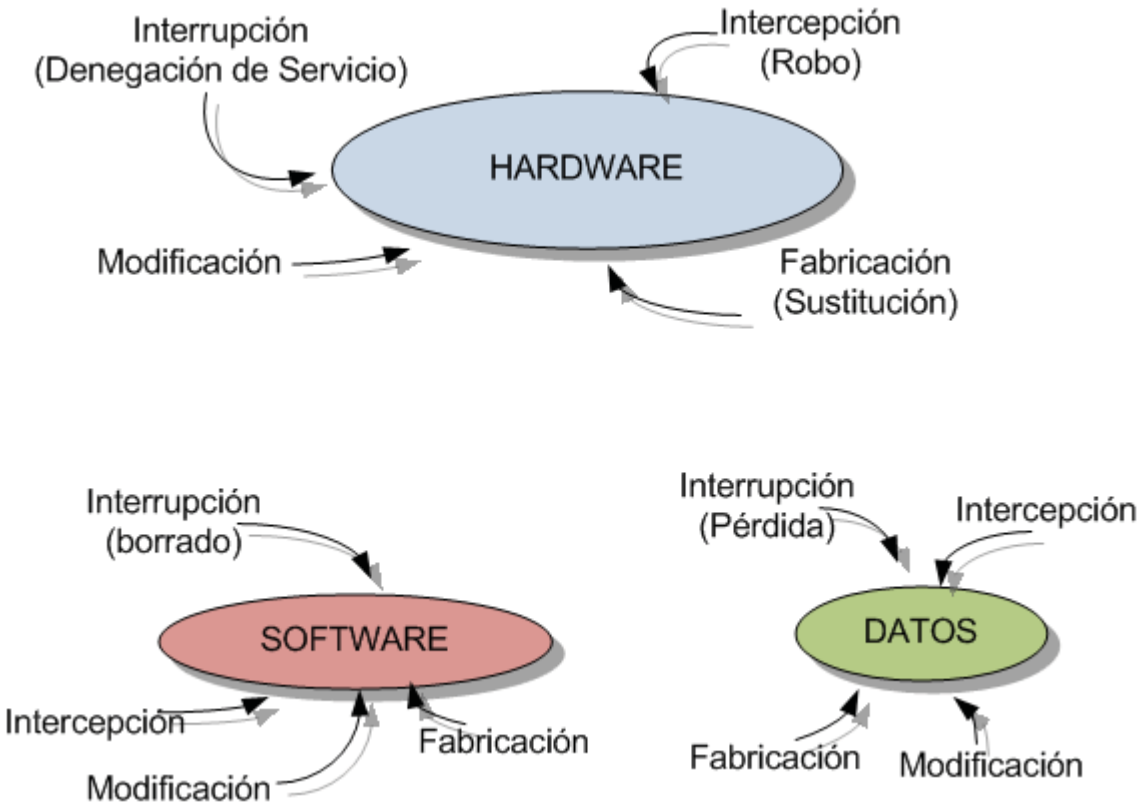

Figura 2. 3 Vulnerabilidades de los sistemas de cómputo.

Las vulnerabilidades de hardware son mayores debido a que están compuestas de objetos físicos los cuales son más fáciles de atacar, al agregar un dispositivo, cambiando el mismo, eliminándolo, interceptando el tráfico de él, inundándolo de tráfico hasta que deje de funcionar, ataques físicos al mismo, mojarlo, corto circuito, quemarlo, congelarlo y robo principalmente, sin embargo, su diseño e implementación puede colocarlo como dispositivo seguro.

Profesionales de la seguridad en cómputo repetidamente encuentran que la más grande amenaza de seguridad son de origen interno, debido a la cantidad de datos a los que tienen acceso para hacer su trabajo los empleados, además de conocer las vulnerabilidades de la institución de una manera más sencilla.[2]

El equipo de cómputo es de uso limitado si no se cuenta con software (Sistemas operativos, controladores, servicios y aplicaciones en general), cualquiera de este software puede ser reemplazado, cambiado, destruido y explotado maliciosamente o accidentalmente al provocar un comportamiento anómalo. Accidentalmente o no, las amenazas explotan las vulnerabilidades de software, En el caso de los datos, éstos pueden ser interpretados en ocasiones por el público en general, ataques a este activo tienen mayor impacto que ataques al software y hardware, ya que en ocasiones los datos se convierten en información que contiene secretos empresariales, cuentas bancarias, bases de datos inmensas con identificaciones personales, registros escolares, historias médicas y muchos más, los cuales si caen en manos equivocadas pueden provocar un daño

[2] Robert Richardson, CSI Computer Crime & Security Survey, 2008, pág. 16-17.

impresionante o al ser utilizada para provocar otros ataques a partir de la obtención, modificación y divulgación de ésta.

2.3. Ataques

Los ataques son la culminación de una amenaza al explotar una vulnerabilidad, estos en general son acciones que atentan contra la disponibilidad, integridad y confidencialidad de algún activo, éstas son las razones primordiales por las cuales actúa la seguridad buscando limitar la acción de éstos o minimizando su alcance, pueden ser realizados de diferentes maneras como robo, ingeniería social, ataque remoto, acceso físico, ataques internos, penetración, entre otros, así como por diferentes tipos de entidades, humanas, lógicas y naturales.

En general los ataques son producidos por diversas entidades físicas y lógicas, dentro de las físicas se encuentran las personas que buscan realizar algún daño, a éstas se les conoce como atacantes o perpetradores en términos generales (Véase apéndice A).

La consecuencia de los ataques depende del tipo de impacto sobre el activo, algunas de las más comunes son:

- Pérdidas económicas.
- Pérdida de imagen pública.
- Responsabilidades legales.
- Daño o pérdida de la vida.
- Incumplimiento de acuerdos de servicio para el público o departamentos de gobierno.
- Violación de acuerdos de confidencialidad.
- Incapacidad para llevar a cabo tareas críticas.
- Modificación o pérdida de datos.

El impacto es una representación del daño o percepción de los daños, una vez que se ha culminado el ataque, en relación con la confidencialidad, integridad y disponibilidad.[3]

Para llevar a cabo un ataque se requiere una planeación previa del mismo, es decir, el atacante debe contar con un esquema en el cual se detalle el objetivo y la metodología a emplear, actualmente las razones por las que un atacante desea concretar un plan de ataque son principalmente obtener ganancias económicas y fraudes.

Los ataques comprometen directamente la integridad, confidencialidad y disponibilidad de un sistema o red, en mayor volumen actualmente son virus, accesos no autorizados a recursos digitales, phishing, pharming, DoS, bots, abuso de redes wireless, ataques a DNS, sniffers.[4]

Muchas de las herramientas utilizadas para ejecutar ataques son herramientas empleadas en el campo de la administración, adicional a esto, hay herramientas de uso dedicado para obtener un

[3] Mike Horton Clinton Mugge, Hacknotes network security, McGraw-Hill, 2003, pág 30.
[4] Robert Richardson, CSI Computer Crime & Security Survey, 2008, pág. 19.

beneficio directo, algunas de estas herramientas son *ping, traceroute, whois, finger, rusers, nslookup, rcpinfo, telnet, dig.*

2.3.1. Fases de un ataque

Para llevar a cabo un ataque se sigue una metodología, ésta consta de cinco pasos y está definida por *Certified Ethical Hacker* – Hacker Ético Certificado, reconocimiento, escaneo, obtención del acceso, manteniendo el acceso y encubrimiento de rastros, esta metodología se contempla sólo para ataques lógicos aunque puede ser adaptada para ataques físicos (figura 2.4).[5]

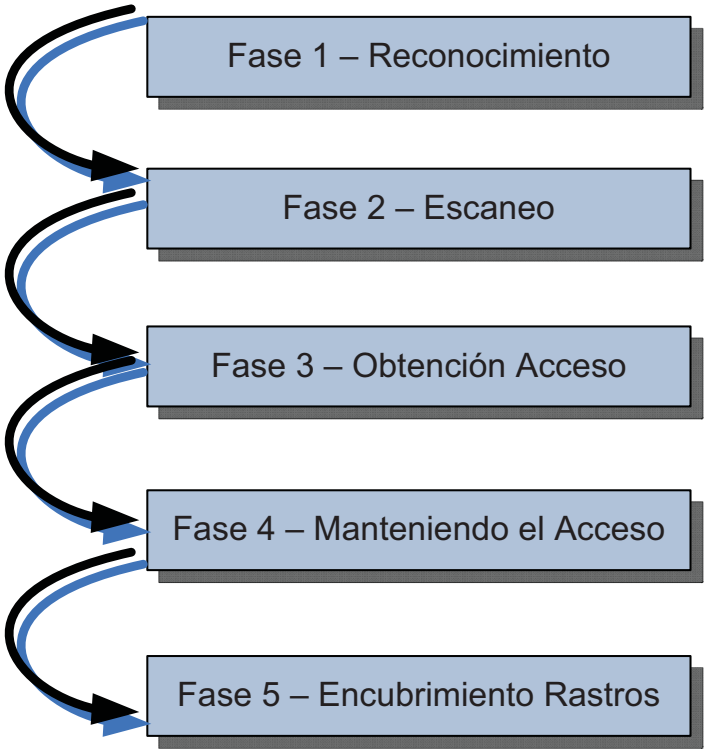

Figura 2. 4 Fases de un ataque.

Los ataques en general tienen dos clasificaciones (figura 2.5), en el caso de la primera se dividen en ataques internos y externos, ésta se refiere al origen donde se lleva a cabo el ataque, es decir, desde el interior de la organización o desde el exterior. En la segunda clasificación intervienen ataques pasivos y activos, los pasivos son ataques que sólo intentan obtener información del sistema sin provocar perturbaciones en él, atentando únicamente en contra de la confidencialidad, a diferencia de los activos que modifican el estado de integridad, disponibilidad y confidencialidad del sistema.

[5] Kimberly Graves, CEH Official Certified Ethical Hacker, Sybex 2007 pág. 31.

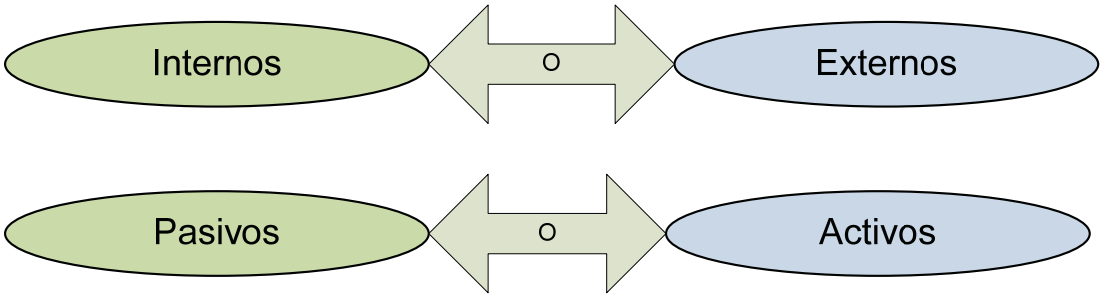

Figura 2. 5 Tipos de ataques.

En la ***fase uno reconocimiento,*** se involucra la obtención de información que se encuentra de manera pública del objetivo, se emplean dos tipos de reconocimiento: pasivo y activo. En el caso de los reconocimientos pasivos, éstos consisten en obtener información sin alterar los principios básicos de la seguridad, como métodos de implementación se utilizan búsquedas en Internet, google y en el sitio de la organización donde muestre información sin autenticarse, como es directorio de ejecutivos, características del software empleado en su sitio, principalmente, también es llamado obtención de información, la ingeniería social y dumpster diving (husmear en la basura para localizar documentos importantes) se consideran métodos de obtención de información pasiva. Observar el tráfico de la red es otra forma de reconocimiento pasivo, ya que no se generan paquetes adicionales que puedan observarse, pero existen otros métodos de detección para estos casos, siendo éste un campo de información muy útil, ya que dentro de la información que se brinda están los rangos de IP, convención de nombre, servidores o redes ocultas.

El reconocimiento activo involucra el descubrimiento de la red sobre hosts individuales, direcciones IP, servicios, versiones de los servicios, sistema operativo, observar el trafico de red, servidores, redes ocultas o intranets, principalmente, este tipo de escaneo genera un riesgo mayor al crear paquetes en la red para obtener información, este tipo de reconocimiento puede darle al atacante indicadores de medidas de seguridad empleadas en el lugar como es el caso de los firewalls.

Dentro de la fase dos*,* ***escaneo,*** se toma la información descubierta durante la fase de reconocimiento y se utiliza ésta para examinar la red. Algunas de las herramientas que se emplean para esta fase pueden incluir escaneo de puertos, mapeo de red y escaneo de vulnerabilidades.

En la fase tres**,** ***obtención del acceso*****,** se lleva a cabo el ataque real, las vulnerabilidades descubiertas durante el reconocimiento y el escaneo, la información encontrada es explotada para obtener acceso, los métodos principales que se emplean en esta fase son el acceso local a una computadora, Internet, acceso fuera de línea, denegación de servicio, robo de sesión, entre otros. [6]

Manteniendo el acceso es la cuarta fase, una vez obteniendo el acceso se busca generar un mecanismo que permita ingresar al sistema para generar ataques futuros, en ocasiones los mismos atacantes protegen al equipo para evitar que otros puedan atacarlo una vez que se tiene acceso a éste, cuando el equipo es comprometido se le conoce como un sistema zombi.

[6] Para información detallada véase el apéndice A.

La última fase, ***encubrimiento de rastros***, es empleada para evitar ser detectado por el personal de seguridad de la institución o del equipo, busca eliminar toda evidencia que se genere al momento de realizar el ataque para anular acciones legales, algunos de los elementos que buscan eliminar o modificar en esta fase son las bitácoras, alarmas en IDS (Intrusion Detection System – sistema detector de intrusos), registros en firewalls, horario de ingreso a un sistema, cuentas de usuario y log de un sistema.

2.3.2. Ataques físicos

La seguridad física es el área más crítica de la seguridad en las tecnologías de la información, si una organización falla en la adecuada implementación de la seguridad física, entonces todos los otros mecanismos de seguridad implementados como firewall, VPN, cifrado, firmas digitales, entre otros, pueden ser evitados. Los ataques por medios físicos abarcan amenazas ocasionadas tanto por el hombre como por la naturaleza (incendios accidentales, tormentas, temblores, condiciones climatológicas e inundaciones), algunos ejemplos de ataques físicos provocados por el hombre contemplan el robo, corte de suministro eléctrico, amenazas ocasionadas involuntariamente, acciones hostiles, robo, fraude o sabotaje.

Es muy importante ser consciente que aunque la organización sea la más segura desde el punto de vista de ataques lógicos, la seguridad será nula si no se ha previsto combatir un daño físico, como lo es un incendio. La seguridad física es uno de los aspectos más olvidados al diseñar un sistema informático, esto puede derivar en que para un atacante sea más fácil perpetrar físicamente que lógicamente, algunos de los ataques físicos más comunes se muestran en la tabla 2.1 donde se relaciona la amenaza con el principio de la seguridad que busca vulnerar.

Tabla 2. 1 Amenazas Físicas.

Amenaza	Atenta contra
Terremoto	Disponibilidad
Fuego	Disponibilidad
Inundación	Disponibilidad
Fallas de alimentación	Disponibilidad
Tornado	Disponibilidad
Temperatura	Disponibilidad
Robo	Confidencialidad, disponibilidad
Modificación	Integridad

Para los ataques físicos realizados por el hombre la medida más empleada para combatirlos es el control de acceso, al implementar controles de acceso por medio de guardias, detectores de metales, utilización de sistemas biométricos y mecanismos de autenticación generales, en el caso de los ataques físicos de carácter natural, éstos no se pueden prever pero sí estudiar su posibilidad de aparición con base en un estudio de las características geográficas donde se encuentre la institución.

Tener controlado el ambiente y acceso físico permite disminuir siniestros, trabajar mejor manteniendo la sensación de seguridad, descartar falsas hipótesis si se producen incidentes, tener los medios para responder frente a un incidente.

Los ataque físicos son provocados de manera intencionada, siniestros, por desconocimientos de los usuarios y desastres naturales, los más comunes son:

- Falta de controles de acceso físico.
- Fallas eléctricas.
- Alteraciones del entorno como temperatura, niveles de humedad o presión.
- Inundaciones, incendios, terremotos.
- Salud física del administrador de los sistemas.

2.3.3. Ataques lógicos

Esta categoría se asigna a todos los ataques que explotan las debilidades de los protocolos empleados y el software en general, los protocolos de comunicación y el software carecen en su mayoría de seguridad o ésta ha sido implementada en forma de parche tiempo después de su creación. Debido a que la creación de protocolos y software nuevo es creación del hombre, tienden a tener errores en sus primeras versiones, algunos ejemplos de las debilidades lógicas más comunes son:

- Fallas en el diseño de las arquitecturas de hardware.
- Fallas de seguridad en los sistemas operativos.
- Fallas de seguridad en las aplicaciones.
- Errores en las configuraciones de los sistemas y dispositivos.
- Los protocolos de comunicación tienen debilidades.
- Los usuarios carecen de información respecto a la seguridad de la información.

Esta lista podría seguir extendiéndose a medida que se evalúen mayor cantidad de elementos de un sistema informático, dentro de los ataques lógicos más comunes se encuentran: spam, virus, gusanos, pharming, phishing, robo de identidad, keyloggers, hombre en el medio, botnet, enumeración.[7]

Un paso importante que debe realizar una organización es el mapeo de cada amenaza contra qué pilar de la seguridad (integridad, confidencialidad y disponibilidad) atenta, algunas de éstas son mostradas en la tabla 2.2.

[7] Amenazas Lógicas - Tipos de Ataques, http://www.segu-info.com.ar/ataques/ataques.htm

Tabla 2. 2 Amenazas Lógicas.

Amenaza	Atenta contra
Denegación de Servicio	Disponibilidad
Código malicioso	Confidencialidad, disponibilidad e integridad
Acceso no autorizado	Confidencialidad
Phishing	Confidencialidad, disponibilidad e integridad
Errores humanos	Confidencialidad, disponibilidad e integridad
Errores de programación	Confidencialidad, disponibilidad e integridad
Errores de transmisión	Integridad, disponibilidad
Ingeniería social	Confidencialidad, disponibilidad e integridad

Las organizaciones no se pueden permitir el lujo de denunciar ataques contra sus sistemas, pues el nivel de confianza de los clientes bajaría enormemente, la mayor parte de éstos no se reportan. Se busca con frecuencia que los administradores tengan cada vez mayor conciencia respecto a la seguridad de sus sistemas, pero esto no es en todos los casos, actualmente existe diferentes fuentes de apoyo para implementar seguridad como nuevas herramientas de seguridad en el mercado, los *advisories* (documentos explicativos) sobre los agujeros de seguridad detectados y la forma de solucionarlos, lanzados por el CERT (Computer Emergency Response Team – Equipo de respuesta a incidentes de cómputo), securityfocus (organización dedicada para facilitar la discusión de temas relacionados con seguridad en cómputo), SANS Institute (organización líder en entrenamiento de seguridad en cómputo) entre otros, todo esto ha dado frutos e incrementado los niveles de seguridad.

La importancia de conocer los ataques que existen y la manera de operar de cada uno de ellos es una de las responsabilidades que recae en los profesionales de la seguridad de la información, por lo que es recomendable que se cuente con un panorama técnico de la manera de operar de los ataques, los ataques lógicos es una clasificación que se da a todos aquellos que se realizan por medios digitales, servidores, computadoras, teléfonos celulares, redes cableadas e inalámbricas. Los principales ataques lógicos se describen a continuación:

1. **Password cracking**[8]

Tomando en cuenta el uso de contraseña como el mecanismo de autenticación más utilizando, es muy común que personas ajenas intenten obtener dicha contraseña utilizando distintas técnicas. Password cracking consiste en romper o encontrar la clave de acceso de un sistema, al cual no se

[8] Para mayor detalle ver apéndice B

tiene autorización para ingresar, generalmente se utilizan técnicas como fuerza bruta, ataque de diccionario, estadísticos, determinado por medio de algoritmos definidos.

2. Malware[9]

Es el término que se le da al software malicioso, el cual tiene como objetivos principales, dañar, alterar o eludir un equipo de cómputo o funciones de red.

Este tipo de software pude ser móvil como aplicaciones applets de Java, controles ActiveX, troyanos, que además pueden propagarse por la red así como cambiar la funcionalidad de programas útiles, en general, cualquier tipo de software diseñado con la finalidad de dañar es considerado como malware.

3. IP Spoofing[10]

Suplantación de IP, es una técnica utilizada por los intrusos para sustituir la dirección IP origen de un paquete, esto se consigue con programas principalmente destinados para ello con la finalidad de reducir la oportunidad de ser detectado pero en realidad se está suplantado a un equipo verdadero, la suplantación de identidad implica una alteración de un paquete a nivel TCP.

En este tipo de ataque entran en juego tres máquinas: un atacante, una víctima, y un sistema suplantado que tiene cierta relación con la víctima; para que el intruso pueda conseguir su objetivo necesita por un lado establecer una comunicación falsa con su objetivo y por otro evitar que el equipo suplantado interfiera con el ataque.

4. Fingerprinting[11]

Se refiere a la obtención de huellas dactilares, es una variante del escaneo que permite de manera rápida y con un alto grado de certeza obtener el tipo de sistema operativo, versión de una aplicación o protocolo que un equipo está utilizando, entre otros, por medio de la información que se brinda al momento de hacer una comunicación entre equipos, esta información específica por lo regular el nombre y versión del servicio como FTP, e-mail, servidores web, esta técnica permite que el atacante encuentre las vulnerabilidades específicas de la versión del sistema operativo o software utilizado permitiéndole ver cuál es el camino más sencillo para obtener acceso al objetivo.

5. DoS[12]

El ataque DoS (Denial of Service - denegación de servicios) se enfoca a negar, alentar o saturar un servicio por varios motivos debido a demasiadas peticiones o envío de paquetes, saturación de red, memoria, procesador y espacio de almacenamiento.

---

[9] Para mayor detalle ver apéndice B

[10] Para mayor detalle ver apéndice B

[11] Para mayor detalle ver apéndice B

[12] Para mayor detalle ver apéndice B

El ataque DoS puede ser causado por inundación de peticiones, es decir, que el servidor atiende demasiadas conexiones simultáneas a tal grado que llega un momento en que no es posible atenderlas o saturar el tráfico en el segmento de red, se puede presentar el mismo caso cuando se transfieren grandes cantidades de archivos al disco duro de un sistema con el objetivo de agotar el espacio del disco duro, ejecutar una aplicación que consuma muchos recursos de su memoria RAM hasta llegar a su límite, una aplicación que consuma el poder de procesamiento de un equipo hasta bloquearlo.

6. Envenenamiento ARP[13]

El protocolo ARP es parte de la pila de protocolos TCP/IP y es el responsable de traducir la dirección hardware del nivel de enlace (MAC) a partir de la dirección IP. El ataque como su nombre lo indica, va dirigido a este protocolo, una máquina cuando intenta establecer una comunicación con otro equipo, envía una petición de la dirección MAC con base en la dirección IP del otro equipo si cuenta con su dirección MAC en la caché (tabla dinámica o estática en un equipo que mapea las direcciones IP con una dirección MAC correspondiente) no pregunta por ésta, en caso contrario, envía un broadcast solicitando la dirección MAC de la IP correspondiente, pero este proceso puede ser intervenido y con esto el tráfico realizado entre dos equipos pasa por un tercer equipo .

El ataque se basa en envenenar la caché *ARP* de los dos nodos cuya comunicación se desea intervenir con información falsa haciéndole creer al host origen que la MAC del destino es la MAC de la máquina atacante. De este modo, el tráfico generado entre ambas máquinas tiene como destino la máquina atacante y desde la cual los paquetes son reenviados al destino real, evitando así la detección del ataque, (figura 2.6).

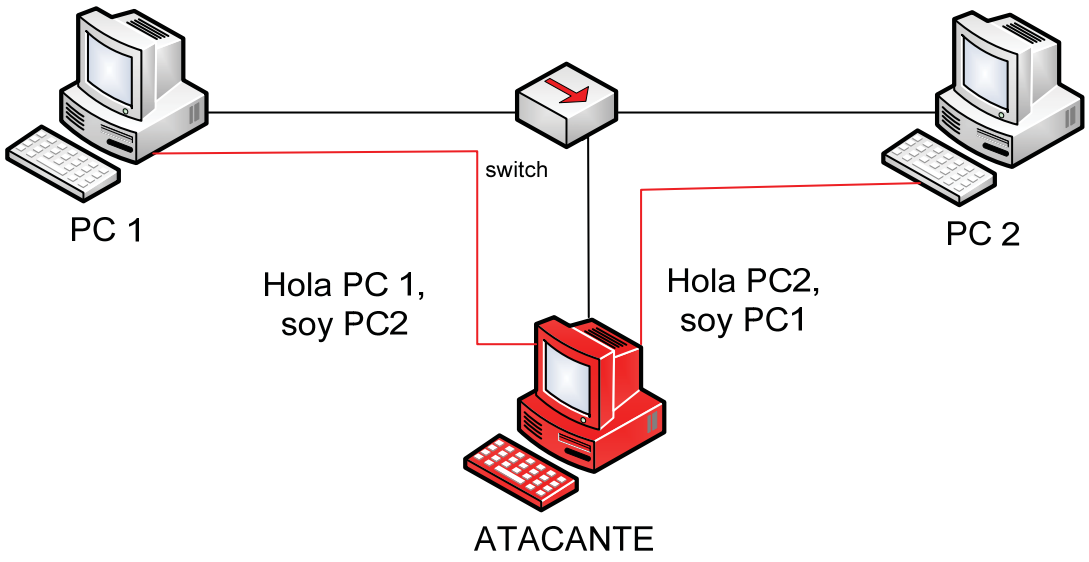

Figura 2. 6 Envenenamiento ARP.

[13] Para mayor detalle ver apéndice B

Pharming

Es la explotación de una vulnerabilidad en el software de los servidores DNS o en los equipos de los propios usuarios, dentro de los archivos que resuelven el protocolo DNS, permite a un atacante redirigir un nombre de dominio (*domain name*) a otra máquina distinta, de esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido accederá en su explorador de Internet a la página web que el atacante haya especificado para ese nombre de dominio.

La manera en que funciona dicha técnica es la siguiente, un intruso crea un sitio web, posteriormente envía un correo con contenido malicioso, el destinatario recibe y abre dicho correo, al ejecutarlo el código malicioso puede modificar los DNS con la finalidad de re direccionar al usuario a un sitio no seguro a través del cual puede obtener información (figura 2.7).

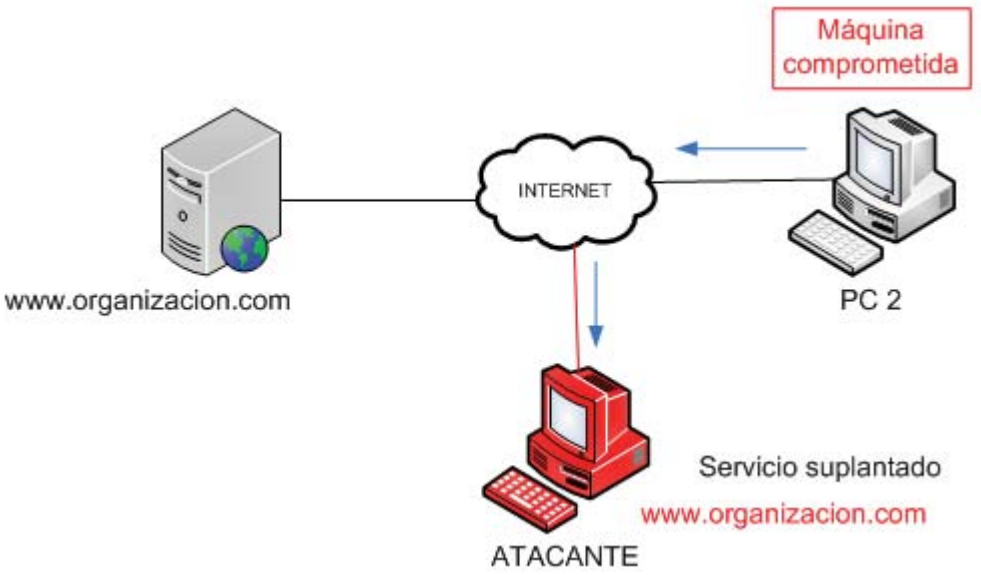

Figura 2. 7 Pharming.

7. Phishing[14]

El phishing es una modalidad de estafa diseñada con la finalidad de robar la identidad, consiste en obtener información de manera ilegal de un usuario, como lo son cuentas bancarias así como cualquier tipo de información que pueda ser de utilidad. Dado que los mensajes y los sitios Web que envían los atacantes parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

La forma de operar es a través de correos electrónicos o ventanas emergentes enviados a la víctima haciéndola creer que provienen de una organización legítima o captando su interés con información que permite engañarla al emplear ingeniería social combinada con la suplantación de identidad,

[14] Para mayor detalle ver apéndice B

haciendo que el usuario crea ingresar al servidor original debido a que accede a paginas idénticas a las que desea visitar (figura 2.8).

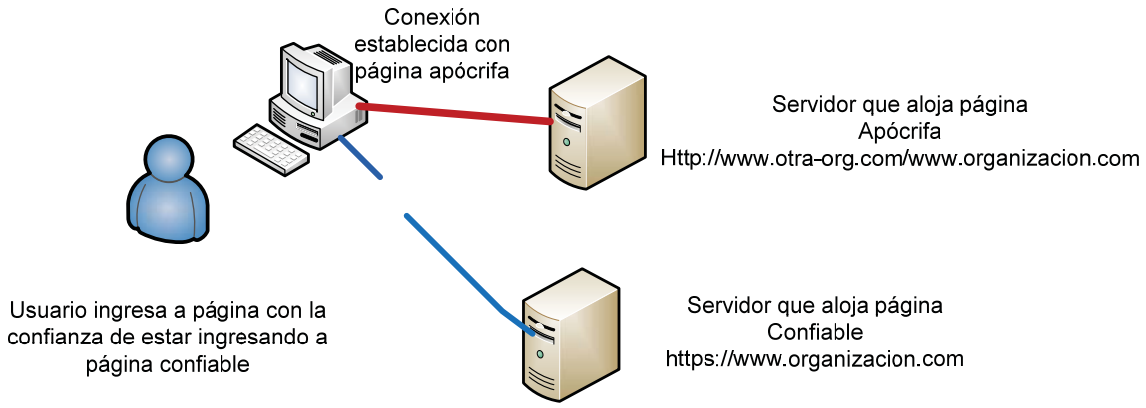

Figura 2. 8 Phishing.

8. Botnet[15]

Equipos comprometidos y controlados por un equipo maestro, son utilizados para aumentar la capacidad de cómputo, así como el poder de los ataques, se han buscado nuevas formas, para lograr reducir el tiempo de ataque y aumentar su efectividad, una botnet es una manera de aumentar el poder de cómputo y con ello la capacidad de realizar un ataque en menos tiempo.

Una botnet puede estar formada por algunos cuantos equipos o por millones de ellos, son difíciles de detectar, usualmente se propagan a través de archivos troyanos, virus, gusanos, incluso con el solo hecho de visitar una página, el usuario podría formar parte de una botnet y no estar enterado. Estas redes son tan famosas a tal grado que son compradas o rentadas por aquellos que deseen obtener algún tipo de beneficio (figura 2.9).

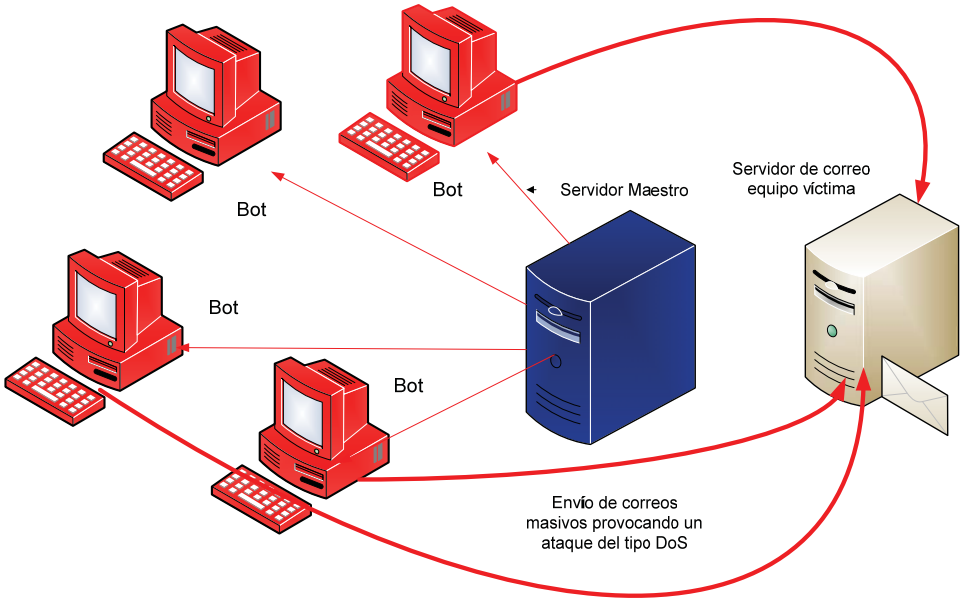

Figura 2. 9 Botnet.

[15] Para mayor detalle ver apéndice B

9. Man in the middle

Man in the middle significa hombre en el medio (MitM) es el término que se utiliza para describir un tipo de ataque, a través de esta técnica el intruso puede modificar a voluntad los mensajes o información que se está transmitiendo a través de la red entre dos entidades, es difícil que los usuarios se percaten de este tipo de ataque. En éste participan tres entidades, los dos usuarios que están intercambiando información y el atacante (figura 2.10).

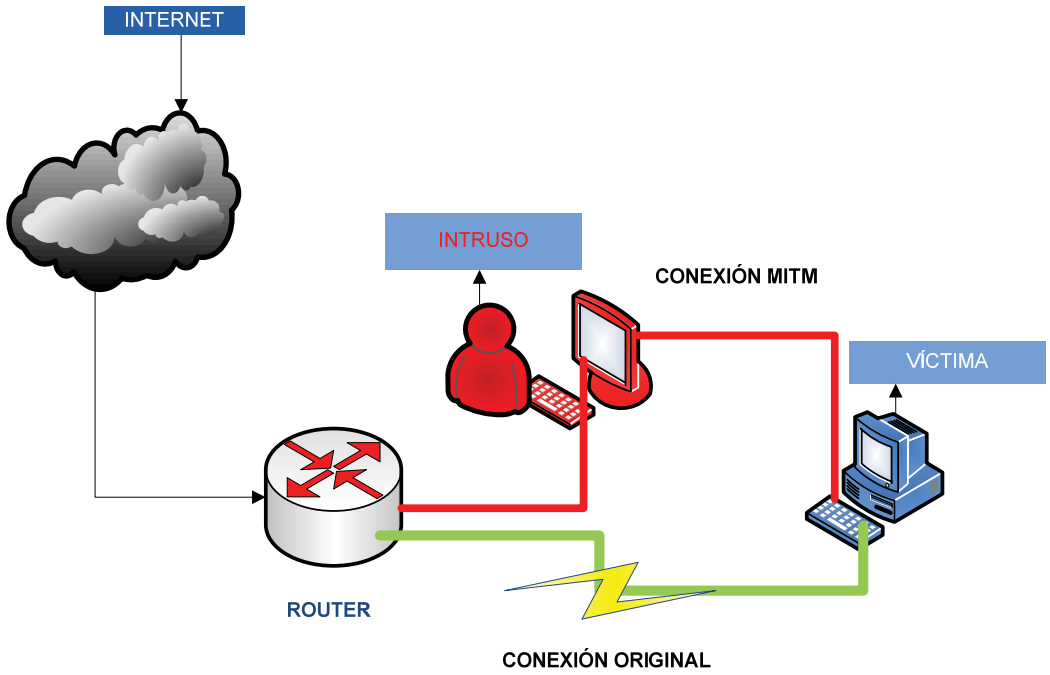

Figura 2. 10 Man in the middle.

Algunos ejemplos de ataques Man in the middle comunes son: ARP spoofing, DNS spoofing, DHCP spoofing. Existen en la red programas y basta información acerca de cómo protegerse de este tipo de ataques, algunos de ellos son: Ettercap, dsniff y fragrouter.

10. SQL injection[16]

SQL (*Structured Query Language - Lenguaje de Consulta Estructurado),* es un estándar de ANSI para las consultas a bases de datos utilizado en manejadores como Oracle, SQL server, Postgres, MySQL, entre muchos otros más, éste lenguaje permite obtener información almacenada en las bases de datos, por ejemplo, obtener la lista de empleados de una institución, nóminas y en general cualquier tipo de información que se encuentre almacenada en una base y pueda ser de utilidad.

Sin embargo, los intrusos le han encontrado otra finalidad, por ejemplo, un usuario malicioso que intente entrar a un sitio en la red donde se necesite autenticar podría enviar una sentencia SQL en el campo del usuario o contraseña e inferir (obtener información confidencial a partir de datos no

[16] Para mayor detalle ver apéndice B

confidenciales) para intentar obtener información o entrar al sistema, por lo que estos ataques están dirigidos a los sitios web que hagan uso de bases de datos.

11. Backdoors[17]

Es una técnica utilizada por los intrusos para garantizar un futuro ingreso a un sistema con mayor facilidad, las puertas traseras se instalan una vez que el equipo ha sido comprometido, dejar una puerta trasera permite al usuario ingresar al equipo de manera más sencilla y sin que sea detectado.

Una de las características de las puertas traseras, es la capacidad que tienen para remover evidencias de su existencia, ya que no queda un registro en las bitácoras del sistema, pero una vez que el intruso hace uso de ella es posible detectarla.

12. Rootkits[18]

Los rootkits son un conjunto de herramientas que pueden ser utilizados para obtener el acceso a un sistema con privilegios de administrador y a los recursos de una computadora así como también esconder la presencia de los procesos que forman el rootkit en la máquina de la víctima.

Este tipo de técnica, es ejecutado después de haber comprometido un equipo por diferentes motivos como son, troyanos, ejecutar archivos adjuntos que vienen en un correo electrónico, conectar dispositivos con configuración de auto ejecución a un equipo, buffer overflow y otros ataques lógicos más que permitan acceso a los sistemas. Cada conjunto de herramientas (rootkits) es diseñado para una plataforma específica, tipo y versión, por ejemplo, los troyanos que oculten procesos al ejecutar comando como ps, netstat, puertos abiertos, puertas traseras (intetd), sniffers así como programas que eliminen bitácoras.

13. Footprinting[19]

Realizar un ataque implica distintas etapas ya mencionadas anteriormente, una de ellas es la recolección de información utilizando técnicas como la obtención del rastro de información a través Internet (footprinting), uno de los propósitos fundamentales de esta técnica es analizar los caminos para poder tener acceso a un equipo o sistema. La información obtenida permite al intruso conocer las vulnerabilidades del sistema y con ello las herramientas a utilizar contra dichas vulnerabilidades.

Dentro del proceso de esta técnica, no sólo consiste en conocer información acerca del sistema, también se incluye información como mapas de la red, localización física del equipo o persona, además de información del personal que ahí labore, la cual le podría ser de utilidad para aplicar ingeniería social.

[17] Para mayor detalle ver apéndice B

[18] Para mayor detalle ver apéndice B

[19] Para mayor detalle ver apéndice B

14. Escaneos[20]

El escaneo forma parte de la recopilación de información, ya que haciendo uso de ésta técnica, el intruso puede obtener mayor información que le facilite el acceso a una red o sistema, durante un escaneo se puede obtener información como la dirección IP, el tipo de servicios, así como aplicaciones instaladas con la finalidad de elegir el exploit adecuado para explotar alguna debilidad que presenten.

15. Enumeración

Después del escaneo, la etapa siguiente es la enumeración la cual consiste en organizar la información recopilada como lo es nombres de usuario, nombres de equipos, redes, puertos abiertos, sistema operativo utilizado, obtener este tipo de información requiere de una constate interacción entre el sistema y el intruso, razón por la cual puede ser identificado.

Uno de los principales objetivos de la enumeración es identificar cuentas de usuarios con suficientes privilegios, ya que el contar con una cuenta que tenga más privilegios permite escalar de manera más rápida a los siguientes niveles.

Muchas de las herramientas utilizadas están diseñadas para analizar redes IP que contienen información del NetBIOS (Network Basic Input/Output System -especificación de interfaz para acceso a servicios de red), nombre del equipo, usuarios conectados, así como la dirección MAC utilizados por los sistemas operativos de Microsoft.

Entre las herramientas que comúnmente son utilizadas se encuentran: DumpSec, SMB auditing, NetBIOS auditing.

2.3.4. Ingeniería social

La ingeniería social ha sido una amenaza para todo tipo de organizaciones desde mucho tiempo atrás, es una de las formas más comunes para tratar de conseguir información sensitiva de la organización, obtener acceso a un sistema o dificultar su disponibilidad, los objetivos en la ingeniería social son las personas situadas en ciertos roles, como administradores de sistemas que permitan utilizar la información que manejan de una manera maliciosa.

La ingeniería social no se considera un ataque lógico directo, pero sí como parte de un ataque lógico ya que es utilizado en combinación con la tecnología en algunos casos, juega un papel muy importante para los intrusos en la planeación de un ataque. Cuando se convierte en un ataque, éste consiste en aprovechar las habilidades de convencimiento y sacar provecho de la vulnerabilidad que el ser humano tiene, *la confianza*, para obtener información relevante que al intruso le podría servir para llevar a cabo algún otro ataque.

[20] Para mayor detalle ver apéndice B

Algunos métodos incluyen realizar una llamada telefónica para obtener datos personales, envío de correos electrónicos a nombre de otros, copias de correos electrónicos, documentos que desecha una institución, entrevistar a empleados de áreas especificas , contacto cara a cara, métodos técnicos como troyanos, backdoors, suplantación de identidad, phishing, pharming entre otros. La ingeniería social trata de obtener información de las personas como cuentas de usuario y contraseñas, secretos industriales, cuentas bancarias, listas de empleados, proveedores, clientes, información del sistema, información de la infraestructura, horarios de empleados, información de investigaciones, información que permita establecer conexiones remotas, en sí cualquier tipo de información que permita al atacante obtener el beneficio que busca.

El problema es tal que dentro del mundo de la seguridad, el ser humano es considerado el eslabón más débil de un esquema de seguridad, una forma de evitar en mayor medida este tipo de ataques, es a través de la educación de los usuarios, proporcionando información acerca de este tipo de ataques y la seguridad en general.

Para salvaguardar efectivamente una organización de la ingeniería social se combinan tres ángulos de defensa: conciencia, procesos/ procedimientos y gente.[21]

Los empleados debe tener *conciencia* del tipo de información que se considera sensitivo, con la finalidad de tener la discreción que se debe en el manejo ésta, solo después de la clasificación de la información se puede informar a los empleados de aquella que se considera sensitiva en cada departamento.

Los *procesos o procedimientos* que se realizan deben salvaguardarse por los responsables de cada área de acción, con la finalidad de que si se llegara a conocer alguno de estos no se pueda atacar, ya que se requiere el dato sensitivo de otro proceso para concretar un ataque.

La *gente* es el punto más débil, la manera de buscar minimizar los ataques de ingeniería social es a través de la educación.

2.4.Controles de seguridad

Generalmente los controles o mecanismos se refieren a medidas de seguridad que buscan reducir la posibilidad de que se presente un ataque, pueden ser clasificadas de las siguientes tres maneras:

a) **Física**, medidas físicas para prevenir el acceso no autorizado a sistemas incluyendo personal de seguridad, luces, circuitos cerrados, candados, alarmas, mecanismos de monitoreo, medidas de seguridad ambiental, tecnologías avanzadas de autenticación, medidas de seguridad para dispositivos de hardware, este punto también es reforzado con la implementación de políticas de seguridad que determinan el procedimiento que deben seguir los usuarios para garantizar la seguridad.

[21] Mike Horton, Hacknotes network security, McGraw-Hill, 2003, cap 8, pág 142,145.

b) ***Técnica*****,** medidas de seguridad técnica como son firewalls, IDS, filtro de contenido, antivirus, actualizaciones de software y sistema operativo, Hardening–endurecimiento de sistemas, medidas de seguridad en software, medidas de seguridad en la comunicación, herramientas de seguridad adicionales que sean implementadas en sistemas remotos, redes y servidores. Muchas de las herramientas empleadas de este tipo son de software y algunas otras de hardware.

c) ***Operacional***, medidas de seguridad operacional, para analizar amenazas y el impacto que se tenga si se presenta un ataque, debe ser un proceso documentado en las políticas de seguridad de la organización, este tipo de herramienta es implementando de manera normativa.

Cualquiera de estas tres clasificaciones puede ser parte de un sistema de seguridad en cómputo, la elección de éstas depende meramente de las necesidades específicas y primordiales de cada organización.

En redes de datos existe una arquitectura de seguridad OSI definida en el ISO (International Standard Organization – Organización internacional para la estandarización) 7498-2, donde se define el servicio de seguridad como la característica que debe tener un sistema, para satisfacer una política de seguridad, a diferencia de un mecanismo de seguridad, ya que éste es un procedimiento concreto utilizado para implementar el servicio de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad (Sólo las entidades autorizadas podrán interpretar la información).
- Autenticación (Verifica la identidad de quien dice ser).
- Integridad (Se hace referencia al concepto integridad).
- Control de acceso (Define el acceso o negación a un recurso).
- No repudio (Se comprueba el origen de los datos).
- Disponibilidad (En todo momento el servicio o recurso estará disponible).

2.5.Análisis de riesgo

La administración de riesgos, es el proceso que permite a los administradores del negocio lograr un balance entre los costos operacionales y económicos, de las medidas de protección del negocio que soporta a la misión de la empresa, es una parte fundamental de la administración de la seguridad.

Entre los beneficios que genera:

- Identifica los puntos más débiles de la infraestructura de TI, que da soporte a los procesos críticos de la organización.
- Guía la selección de medidas de protección de costo adecuado.
- Determina dónde es necesario contar con esquemas de recuperación de desastres y continuidad de negocio.

- Permite realizar políticas de seguridad mejor adaptadas a las necesidades de la organización.
- Es un elemento para la toma de decisiones estratégicas.

  En general los análisis de riesgos que se pueden llevar a cabo son de dos tipos, cualitativos y cuantitativos, la elección de éste depende de cómo se desea llevar a cabo el análisis.

a) *Cuantitativo*

- Enfocado a determinar valores numéricos (generalmente monetarios) para los componentes objeto del análisis, así como al nivel de posibles pérdidas.
- Los resultados son objetivos, basados en métricas generadas igualmente de forma objetiva, éstos se expresan en porcentajes, probabilidades de ocurrencia de amenazas, pesos, etcétera.
- Es sencillo mostrar el costo-beneficio en términos comprensibles para la alta dirección (no técnicos).
- Los cálculos pueden resultar complejos.
- El trabajo previo requiere tiempo y esfuerzos considerables.

b) *Cualitativo*

- No requiere determinar valores numéricos (generalmente monetarios) para los componentes objeto del análisis, así como al nivel de posibles pérdidas.
- No es necesario contar con la frecuencia de ocurrencia de las amenazas.
- Los resultados son subjetivos.
- No hay una base para demostrar el costo-beneficio.
- Los cálculos son sencillos.
- La calidad del análisis depende del equipo conformado.

Los componentes generales de un análisis de riesgo son:

1. ***Enunciar el alcance del análisis***; establece cuál es el activo informático a ser evaluado, Define cuál será el entregable (reporte, estrategia, mecanismo, etcétera.).

2. ***Conformar el equipo que sustentará el proceso de análisis de riesgos***; dueños de las funcionalidades, usuarios a todos los niveles, diseñadores y analistas de sistemas, desarrolladores de sistemas, administradores de BD, auditores, personal de seguridad física, telecomunicaciones, jurídico, administración de operaciones, sistemas operativos, seguridad información.

3. ***Identificar las amenazas***; es recomendable contar con una lista propuesta antes del análisis (tal vez basada en hechos que ya ocurrieron). Fomentar lluvias de ideas considerando lectura ilegal de información, negación de servicio, explotación de deficiencias en plataformas operativas, vandalismo en páginas web, falsificación de identidad, virus, caballos de Troya, gusanos, ingeniería social, se puede priorizar de acuerdo con integridad, confidencialidad y disponibilidad

4. ***Priorizar las amenazas y riesgos***; tabla para dar prioridades a las amenazas (por consenso), y para estimar el impacto a la organización.

5. ***Determinar la prioridad en función del impacto.***

6. ***Estimar el impacto total de la amenaza conforme al riesgo que representa.***

7. ***Identificar medidas de protección.***

8. ***Realizar un análisis costo/beneficio***; en este análisis se debe determinar cuáles son los controles que dan un máximo de protección a un menor costo (puede haber controles que sirvan para mitigar la ocurrencia de varias amenazas).

9. ***Ordenar las medidas de protección por prioridades***; debe ordenarse la selección para elegir el control adecuado.

    a) Cuántas amenazas puede mitigar un control.
    b) El impacto en la productividad al implantar un control.
    c) Controles que pueden desarrollarse en casa.
    d) Estimar un nivel de aceptación de riesgo.

10. ***Reportar el resultado del análisis***; el producto del análisis es un reporte donde se documentan los hallazgos, identificación de los controles, recomendación de controles puede en ocasiones llegar hasta esbozar un plan de implantación de los controles sugeridos, permite crear un histórico que permitirá apoyar las decisiones en análisis futuros.

11. ***Proponer soluciones estratégicas***[22]

Lo más complicado al momento de hacer un análisis de riesgo es determinar el valor de los activos, para esto se pueden utilizar varios métodos como lo son orden superior, política general, legislación, entrevistas con listas de verificación, cuestionarios, consenso (Delphi), valor en libros.

[22] Risk Management Guide for Information technology System, NIST SP800-30