Las amenazas del sistema y de la red implican el abuso de los servicios y de las conexiones de red, estas amenazas crean una situación en la que se usan inapropiadamente los recursos del Sistema Operativo y los archivos del usuario

Siguiente diapositiva

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Un ejemplo de este malware es el gusano Morris, nombrado así por su creador Robert Morris un estudiante de 23 años, fue el primer ejemplar de malware autorreplicable que afectó a Internet, en 1988, aproximadamente 6000 de los 60 000 servidores conectados a la red fueron infectados por este gusano informático.

El programa intentaba averiguar las contraseñas de otras computadoras usando una rutina de búsqueda que iba cambiando los nombres de usuarios conocidos, una lista de las contraseñas más comunes y también búsqueda al azar. Descubrieron que no todas las computadoras eran afectadas, sino que solo se propagó en las computadoras VAX (son famosas por ser la primer computadora comercial de arquitectura de 32 bits) y las fabricadas por Sun Microsystems, que empleaban Unix.

Se trataba de un programa de 99 líneas de código en C que, aprovechándose de una debilidad en un agente de transporte de correo llamado Sendmail, se replicaba de una máquina a otra. Se estableció que la infección no fue realizada por un virus, sino por un programa gusano, diseñado para reproducirse a sí mismo indefinidamente y no para eliminar datos.

No fue programado con intención de causar daño, pero a causa de un (error de software) o lo que conocemos como bug en su código, los efectos fueron catastróficos para la época porque produjó fallos en cientos de computadoras en universidades, corporaciones y laboratorios de gobierno en todo el mundo antes de que fuera rastreado y eliminado. El ataque fue llamado «Gusano de Internet».  Erradicarlo costó mucho dinero y esto suceso dio origen al CERT un equipo de respuesta a emergencias en computadoras.

Siguiente diapositiva

El escaneo de puertos no es un ataque sino más bien es el proceso en el que se analiza automáticamente los puertos de una máquina conectada a la red con la finalidad de verificar cuáles puertos están abiertos, cerrados o si cuenta con algún protocolo de seguridad, . Dicho escaneo puede tener fines legítimos, sin embargo también es usado para tratar de comunicarse con algún servicio a través de los puertos y este intruso podría aprovechar algún error de alguno de los servicios (por ejemplo errores de desbordamiento de bufer que permiten la creación de una shell de comandos privilegiado, con lo que podrían instalar caballos de Troya).

Existen herramientas de código abierto para la exploración de red así como para auditoria de seguridad que proporciona información acerca de que servicios se están ejecutando (incluyendo los nombres y versiones de las aplicaciones), también información sobre el SO host y acerca de las defensas del mismo (es decir, información sobre el firewall), también pueden llegar a contar con una base de datos de errores y de los modos de aprovecharlos en un ataque.

Los escaneos de puertos son detectables, es por ello que suelen realizarse desde los denominados sistemas zombi que son maquinas independientes que dan un servicio normal a su propietario, pero al mismo tiempo son usadas (de forma desapercibida por el propietario) para retransmisión de correo basura o denegación de servicio. Al hacer esto, resulta difícil determinar el origen del ataque y la persona que lo inicia.

Siguiente diapositiva

Un ataque de denegación de servicio tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una computadora, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red.

Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas originarias en inglés) y la denegación de servicio distribuido o DDoS. La diferencia entre ambos es el número de ordenadores o IP´s que realizan el ataque.

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

En el caso de los ataques DDoS, se hacen peticiones o conexiones usando un gran número de computadoras o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio el cual es el objeto del ataque. Un ataque DDoS es más difícil de detectar, porque el número de peticiones proviene desde distintas IP´s y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Las computadoras que realizan el ataque DDoS son reclutadas mediante la infección de un malware, convirtiéndose así en bots o zombis, capaces de ser controlados de forma remota por un ciberdelincuente. Un conjunto de bots, es decir, de ordenadores infectados por el mismo malware, forman una botnet o también conocida como red zombi. Obviamente, esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina.

Siguiente diapositiva

* *Malware*: el término se refiere de forma genérica a cualquier software malicioso que tiene por objetivo infiltrarse en un sistema para dañarlo. Comúnmente se asocian como tipos de malware a los virus, gusanos y troyanos.
* Virus: es un código que infecta los archivos del sistema mediante un programa maligno, pero para ello necesita que el usuario lo ejecute directamente. Una vez activo, se disemina por todo el sistema a donde el equipo o cuenta de usuario tenga acceso, desde dispositivos de hardware hasta unidades virtuales o ubicaciones remotas en una red.
* Gusanos: es un programa que, una vez infectado el equipo, realiza copias de sí mismo y las difunde por la red. A diferencia del virus, no necesita la intervención del usuario, ya que pueden transmitirse utilizando las redes o el correo electrónico. Son difíciles de detectar, pues su objetivo es difundirse e infectar a otros equipos, y no afectan inicialmente el funcionamiento normal del sistema. Su uso principal es el de la creación de redes zombis (*botnets*), utilizadas para ejecutar acciones de forma remota como ataque de denegación de servicio (*DoS*) a otro sistema.
* Troyanos: similares a los virus, sin embargo, mientras que este último es destructivo por sí mismo, el troyano lo que busca es abrir una puerta trasera (*backdoor*) para favorecer la entrada de otros programas maliciosos. Su misión es precisamente pasar desapercibido e ingresar a los sistemas sin que sea detectado como una amenaza potencial. No se propagan a sí mismos y suelen estar integrados en archivos ejecutables aparentemente inofensivos.
* *Spyware*: es un programa espía, cuyo objetivo es recopilar información de un equipo y transmitirlo a una entidad externa sin el consentimiento del propietario. Su trabajo suele ser silencioso, sin dar muestras de su funcionamiento, llegando incluso a instalar otros programas sin que se perciban. Las consecuencias de su infección incluyen, además, pérdida considerable del rendimiento del sistema y dificultad para conectarse a Internet.
* *AdWare*: su función principal es la de mostrar publicidad. Aunque su intención no es la de dañar equipos, es considerado por algunos una clase de *spyware*, ya que puede llegar a recopilar y transmitir datos para estudiar el comportamiento de los usuarios y orientar mejor el tipo de publicidad.
* *Ransomware*: Este es uno de los más sofisticados y modernos ataques, ya que lo que hace es secuestrar datos (encriptándolos) y pedir un rescate por ellos. Normalmente, se solicita una transferencia en dinero electrónico (*bitcoins*), para evitar el rastreo y localización. Este tipo de ciberataque va en aumento y es uno de los más temidos en la actualidad.
* Escaneo de Puertos: técnica empleada para auditar dispositivos y redes con el fin de conocer que puertos están abiertos o cerrados, los servicios que son ofrecidos, así como comprobar la existencia de algún corta fuegos (*firewall*), la arquitectura de la red, o el sistema operativo, entre otros aspectos. Su empleo permite al atacante realizar un análisis preliminar del sistema y sus vulnerabilidades, con miras a algún otro tipo de ataque, pues cada puerto abierto en un dispositivo, es una potencial puerta de entrada al mismo.
* *Phishing*: no es un software, se trata más bien de diversas técnicas de suplantación de identidad para obtener datos privados de las víctimas, como contraseñas o datos bancarios. Los medios más utilizados son el correo electrónico, mensajería o llamadas telefónicas, y se hacen pasar por alguna entidad u organización conocida, solicitando datos confidenciales, para posteriormente utilizarse por terceros en beneneficio propio.
* *Botnets* (Redes de robots): Son computadoras o dispositivos conectados a la red (teléfonos inteligentes, tabletas, etc.) infectados y controlados remotamente, que se comportan como robots (*bots*) o “zombis”, quedando incorporados a redes distribuidas, las cuales envían de forma masiva mensajes de correo “*spam*” o código malicioso, con el objetivo de atacar otros sistemas o dejarlos fuera de servicio.
* Denegación de Servicios: tiene como objetivo inhabilitar el uso de un sistema o computadora, con el fin de bloquear el servicio para el que está destinado. Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, comienzan a ralentizarse o incluso bloquearse y desconectarse de la red. Existen dos técnicas para este ataque: la denegación de servicio o DoS (*Denial of Service*) y la denegación de servicio distribuido o DDoS (*Distributed Denial of Service*); la diferencia entre ambos es el número de ordenadores que realizan el ataque. En el primero, las peticiones masivas al servicio se realizan desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que no tiene capacidad de respuesta y comienza a rechazar peticiones (denegar el servicio); en el segundo, las peticiones o conexiones se realizan empleando un gran número de computadoras o direcciones IP, todas al mismo tiempo y hacia el mismo servicio objeto del ataque, de forma general, las computadoras que lo realizan se encuentran infestadas, formando parte de una *botnet*, y comportándose como zombis.
* Ataque *MITM* (*Man In The Middle*): conocido como “hombre en el medio”, ocurre cuando una comunicación entre dos sistemas es interceptada por una entidad externa simulando una falsa identidad. En este sentido, el atacante tiene control total de la información que se intercambia, pudiendo manipularla a voluntad, sin que el emisor y el receptor lo perciban rápidamente. Es común que se realice empleando redes WIFI públicas y abiertas, y es muy peligroso ya que se puede obtener información sensible de las víctimas, y es difícil identificarlo si no se poseen unos mínimos conocimientos sobre el tema.

Siguiente diapositiva

criptografía

la criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet.

El termino de criptografía no surge con las ciencias computacionales, sino es un termino muy antiguo que fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

Siguiente diapositiva

Texto

Descripción generada automáticamente con confianza media