ANÁLISIS DE UN CIBERATAQUE

BUSQUEDA DE VULNERABILIDADES DE SEGURIDAD

Las VULNERABILIDADES sin cualquier tipo de defecto en el software y hardware

Un ATAQUE. Es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida

VULNERABILIDAD DE SOFTWARE

Las vulnerabilidades de software generalmente se introducen por errores en el sistema operativo o el código de aplicación; a pesar de todos los esfuerzos realizados por las empresas para encontrar y corregir las vulnerabilidades, es común que surjan nuevas vulnerabilidades.

El objetivo de las actualizaciones de software es mantenerse actualizado y evitar el aprovechamiento de vulnerabilidades.

Existen investigadores dedicados a analizar estás estructuras de software, un ejemplo es el proyecto Zero-Day de Google

https://code.google.com/p/google-security-research/issues/list?can=1

VULNERABILIDAD DE HARDWARE

Las vulnerabilidades de hardware se presentan a menudo mediante defectos de diseño del hardware.

Las vulnerabilidades de hardware son específicas de los modelos de dispositivos y generalmente no se ven atacadas por intentos comprometedores aleatorios, aunque son losas dirigidos, pero la seguridad física que tienen es suficiente para el usuario común

CLASIFICACIÓN DE LAS VULNERABILIDADES DE SEGURIDAD

Desbordamiento de búfer:

esta vulnerabilidad ocurre cuando los datos se escriben más allá de los límites de un búfer. Los búferes son áreas de memoria asignadas a una aplicación. Al cambiar los datos más allá de los límites de un búfer, la aplicación accede a la memoria asignada a otros procesos. Esto puede llevar a un bloqueo del sistema, comprometer los datos u ocasionar el escalamiento de los privilegios.

Entrada no validada:

Los programas suelen trabajar con la entrada de datos. Estos datos que entran al programa pueden tener contenido malicioso diseñado para que el programa se comporte de manera no deseada. Considere un programa que recibe una imagen para procesar. Un usuario malintencionado podría crear un archivo de imagen con dimensiones de imagen no válidas. Las dimensiones creadas maliciosamente podrían forzar al programa a asignar búferes de tamaños incorrectos e imprevistos.

Condiciones de carrera:

****esta vulnerabilidad sucede cuando el resultado de un evento depende de resultados ordenados o temporizados. Una condición de carrera se convierte en una fuente de vulnerabilidad cuando los eventos ordenados o temporizados requeridos no se producen en el orden correcto o el tiempo adecuado.

Debilidades en las prácticas de seguridad:

Los sistemas y los datos confidenciales pueden protegerse con técnicas tales como autenticación, autorización y encriptación. Los desarrolladores no deben intentar crear sus propios algoritmos de seguridad porque es probable que introduzcan vulnerabilidades. Se recomienda encarecidamente que los desarrolladores utilicen las bibliotecas de seguridad ya creadas, aprobadas y verificadas.

Problemas de control de acceso:

El control de acceso es el proceso de controlar quién hace qué y va desde la administración del acceso físico a los equipos hasta determinar quién tiene acceso a un recurso, por ejemplo, un archivo, y qué pueden hacer con este, como leerlo o modificarlo. Muchas vulnerabilidades de seguridad se generan por el uso incorrecto de los controles de acceso. Casi todos los controles de acceso y las prácticas de seguridad pueden superarse si el atacante tiene acceso físico a los equipos objetivo. Por ejemplo, no importa que haya configurado los permisos de un archivo, el sistema operativo no puede evitar que alguien eluda el sistema operativo y lea los datos directamente del disco. Para proteger los equipos y los datos contenidos, el acceso físico debe restringirse y deben usarse técnicas de encriptación para proteger los datos contra robo o daño.

TIPOS DE MALWARE

El malware o MALICIOUA SOFTWARE. Es cualquier código que pueda utilizarse para robar daros, evitar controles de acceso, ocasionar daños o comprometer un sistema

Spyware:

este malware está diseñado para rastrear y espiar al usuario. El spyware a menudo incluye rastreadores de actividades, recopilación de pulsaciones de teclas y captura de datos

Adware

Software de publicidad está diseñado para brindar anuncios automáticamente. El adware a veces se instala con algunas versiones de software. Algunos adwares están diseñados para brindar solamente anuncios, pero también es común que el adware incluya spyware

Bot

Un Bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea

Rasomware

este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago.

Scareware

Este tipo de malware está diseñado para persuadir al usuario de realizar acciones específicas en función del temor. El scareware falsifica ventanas emergentes que se asemejan a las ventanas de diálogo del sistema operativo.

Rootkit

este malware está diseñado para modificar el sistema operativo a fin de crear una puerta trasera. Los atacantes luego utilizan la puerta trasera para acceder a la computadora de forma remota. La mayoría de los rootkits aprovecha las vulnerabilidades de software para realizar el escalamiento de privilegios y modificar los archivos del sistema. También es común que los rootkits modifiquen las herramientas forenses de supervisión del sistema, por lo que es muy difícil detectarlo

Virus

Virus es un código ejecutable malintencionado que se adjunta a otros archivos ejecutables, generalmente programas legítimos. La mayoría de los virus requiere la activación del usuario final y puede activarse en una fecha o un momento específico.

Troyano

Es malware que ejecuta operaciones maliciosas bajo la apariencia de una operación deseada. Este código malicioso ataca los privilegios de usuario que lo ejecutan.

Gusano

Los “Gusanos” son códigos maliciosos que se replican mediante la explotación independiente de las vulnerabilidades en las redes. Los gusanos, por lo general, ralentizan las redes. Mientras que un virus requiere la ejecución de un programa del host, los gusanos pueden ejecutarse por sí mismos. A excepción de la infección inicial, ya no requieren la participación del usuario. Una vez infectado el host, el gusano puede propagarse rápidamente

Hombre en el medio MitM

MitM permite que el atacante tome el control de un dispositivo sin el conocimiento del usuario. Con ese nivel de acceso, el atacante puede interceptar y capturar información sobre el usuario antes de retransmitirla a su destino. y sacan información financiera

Hombre en el móvil

Variación del hombre en el medio, el MitMo es un tipo de ataque utilizado para tomar el control de un dispositivo móvil. Cuando está infectado, puede ordenarse al dispositivo móvil que exfiltre información confidencial del usuario y la envíe a los atacantes. ZeuS, un ejemplo de ataque con capacidades de MitMo, permite que los atacantes capturen silenciosamente SMS de verificación de 2 pasos enviados a los usuarios.

Síntomas de malware

- Aumento del uso de la CPU
- Disminución de la velocidad de la computadora
- La computadora se congela o falla con frecuencia
- Hay una disminución en la velocidad de navegación web
- Existen problemas inexplicables con las conexiones de red
- Se modifican los archivos
- Se eliminan archivos
- Hay una presencia de archivos
- Programas e iconos de escritorio desconocidos
- Se ejecutan procesos desconocidos
- Los programas se cierran o reconfiguran solos
- Se envían correos electrónicos sin el conocimiento o el consentimiento del usuario.

Ingeniería social

La ingeniería social es un ataque de acceso que intenta manipular a las personas para que realicen acciones o divulguen información confidencial

Pretexto:

Esto es cuando un atacante llama a una persona y miente en el intento de obtener acceso a datos privilegiados. Un ejemplo implica a un atacante que pretende necesitar datos personales o financieros para confirmar la identidad del objetivo.

Seguimiento

Es cuando un atacante persigue rápidamente a una persona autorizada a un lugar seguro.

Algo por algo

Es cuando un atacante solicita información personal de una parte a cambio de algo, por ejemplo, un obsequio

Decodificación de contraseñas de WIFI

Es el proceso de detección de la contraseña de Wi-Fi

Ingeniería social:

El atacante manipula a una persona que conoce la contraseña para que se la proporcione.

Ataques por fuerza bruta:

El atacante prueba diversas contraseñas posibles en el intento de adivinar la contraseña. Si la contraseña es un número de 4 dígitos, por ejemplo, el atacante deberá probar cada una de las 10 000 combinaciones. Los ataques por fuerza bruta normalmente involucran un archivo de lista de palabras.

Monitoreo de la red:

Mediante la escucha y la captura de paquetes enviados por la red, un atacante puede descubrir la contraseña, si la contraseña se envía sin cifrar (en texto plano). Si la contraseña está cifrada, el atacante aún puede revelarla mediante una herramienta de decodificación de contraseñas.

Suplantación de identidad

La suplantación de identidad es cuando una persona maliciosa envía un correo electrónico fraudulento disfrazado como fuente legítima y confiable.

Suplantación de identidad focalizada es un ataque de suplantación de identidad altamente dirigido. Si bien la suplantación de identidad y la suplantación de identidad focalizada usan correos electrónicos para llegar a las víctimas, los correos electrónicos de la suplantación de identidad (phishing) focalizada se personalizan para cada persona específica. El atacante investiga los intereses del objetivo antes de enviarle el correo electrónico. Por ejemplo, el atacante descubre que al objetivo le interesan los automóviles y que está interesado en la compra de un modelo específico. El atacante se une al mismo foro de debate sobre automóviles donde el objetivo es miembro, publica una oferta de venta del automóvil y envía un correo electrónico al objetivo. El correo electrónico contiene un enlace a imágenes del automóvil. Cuando el objetivo hace clic en el enlace, el malware se instala en la computadora del objetivo.

Aprovechamiento de vulnerabilidades

- El aprovechamiento de vulnerabilidades es otro método común de infiltración. Los atacantes analizan las computadoras para obtener información. A continuación, encontrará un método común de aprovechamiento de vulnerabilidades: Paso 1. Recopilación de información sobre el sistema de destino. Esto se puede hacer de muchas formas diferentes, como con un escáner de puerto o a través de la ingeniería social. El objetivo es aprender tanto como sea posible acerca de la computadora de destino. Paso 2. Parte de la información pertinente aprendida en el Paso 1 puede ser el sistema operativo, su versión y una lista de los servicios que ejecuta. Paso 3. Una vez que conoce el sistema operativo y la versión del objetivo, el atacante busca cualquier vulnerabilidad conocida específica para dicha versión del SO u otros servicios del sistema operativo. Paso 4. Cuando encuentra una vulnerabilidad, el atacante busca usar un ataque desarrollado anteriormente. Si no se ha desarrollado ningún ataque, el atacante puede considerar desarrollar uno. Una forma de lograr la infiltración es a través de amenazas persistentes avanzadas (APT). Estas consisten en una operación cautelosa y avanzada de varias fases a largo plazo contra un objetivo específico. Debido a la complejidad y el nivel de habilidad requeridos, las APT generalmente están bien financiadas. Las APT apuntan a las organizaciones o las naciones por motivos políticos o comerciales. Generalmente relacionadas con el espionaje con base en la red, el propósito de las APT es implementar malware personalizado en uno o varios sistemas de destino y pasar desapercibidas. Con múltiples fases de operación y varios tipos personalizados de malware que afecten a distintos dispositivos y realizan funciones específicas, un atacante

individual generalmente carece del conjunto de habilidades, recursos o la perseverancia necesarios para llevar a cabo una APT.

DoS

Los ataques de denegación de servicio. Son un tipo de ataque a la red que da como resultado cierto tipo de interrupción entre los servicios de red, dispositivos y aplicaciones

Cantidad abrumadora de tráfico:

Esto ocurre cuando se envía una gran cantidad de datos a una red, a un host o a una aplicación a una velocidad que no pueden administrar. Esto ocasiona una disminución de la velocidad de transmisión o respuesta o una falla en un dispositivo o servicio.

Paquetes maliciosos formateados:

Esto sucede cuando se envía un paquete malicioso formateado a un host o una aplicación y el receptor no puede manejarlo. Por ejemplo, un atacante envía paquetes que contienen errores que las aplicaciones no pueden identificar o reenvía paquetes incorrectamente formateados. Esto hace que el dispositivo receptor se ejecute muy lentamente o se detenga. Los ataques de DoS se consideran un riesgo importante porque pueden interrumpir fácilmente la comunicación y causar una pérdida significativa de tiempo y dinero. Estos ataques son relativamente simples de llevar a cabo, incluso por un atacante inexperto.

DDoS

Un ataque DoS distribuido (DDoS) es similar a un ataque DoS, pero proviene de múltiples fuentes coordinadas. Por ejemplo, un ataque DDoS podría darse de la siguiente manera: Un atacante crea una red de hosts infectados, denominada botnet. Los hosts infectados se denominan zombies. Los zombies son controlados por sistemas manipuladores. Las computadoras zombi constantemente analizan e infectan más hosts, lo que genera más zombies. Cuando está listo, el hacker proporciona instrucciones a los sistemas manipuladores para que los botnet de zombies lleven a cabo un ataque DDoS.

Envenenamiento de SEO

La optimización de motores de búsqueda

Es un conjunto de técnicas utilizadas para clasificar mejor una página web y darle mejor posicionamiento, el problema radica en dónde un software malicioso aparezca más arriba en los resultados de búsqueda lo que se denomina envenenamiento de SEO