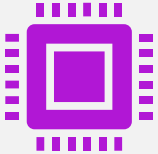
Capítulo 2: Ataques, conceptos y técnicas

Los profesionales de la ciberseguridad analizan qué ocurrió después de un ciberataque.

Capítulo 2: Ataques, conceptos y técnicas



Explica las vulnerabilidades de software y hardware de seguridad y las distintas categorías de las vulnerabilidades de seguridad.

Analiza los diferentes tipos de software malicioso (conocido como malware) y los síntomas de malware. Cubre las diferentes maneras en que los atacantes pueden infiltrarse en un sistema, así como los ataques de denegación de servicio.

Ataques, conceptos y técnicas

La mayoría de los ciberataques modernos se consideran ataques combinados.

Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo.

Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque.

Búsqueda de vulnerabilidades en la seguridad

- Las vulnerabilidades de seguridad son cualquier tipo de defecto en software o hardware.
- Después de obtener conocimientos sobre una vulnerabilidad, los usuarios malintencionados intentan explotarla.
- Un *ataque* es el término que se utiliza para describir un programa escrito para aprovecharse de una vulnerabilidad conocida.

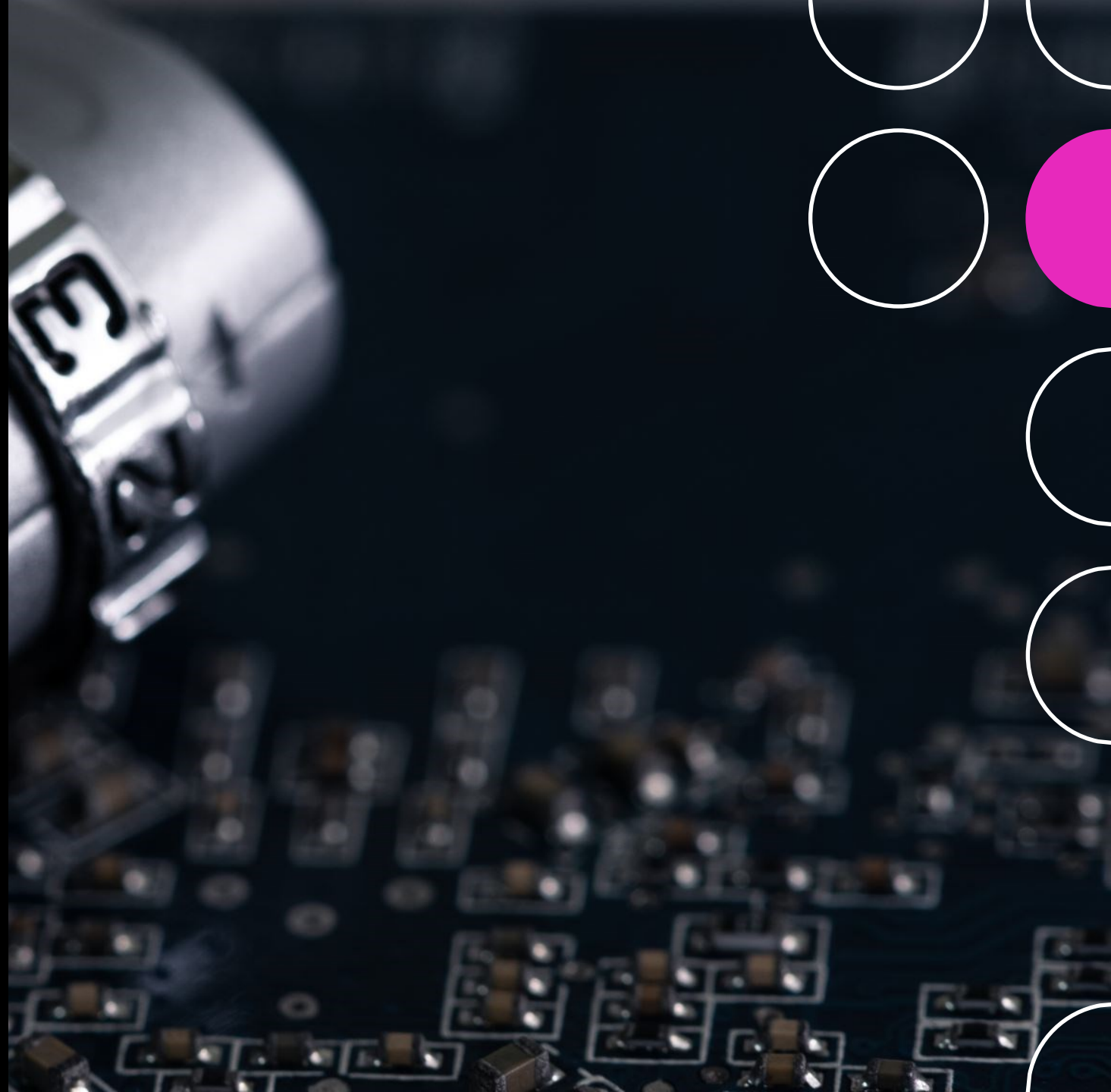
Búsqueda de vulnerabilidades en la seguridad

El acto de aprovecharse de una vulnerabilidad se conoce como ataque.

El objetivo del ataque es acceder a un sistema, los datos que aloja o recursos específicos.

Vulnerabilidades de software

Las vulnerabilidades de software generalmente se introducen por errores en el sistema operativo o el código de aplicación;



Vulnerabilidades de software

a pesar de todos los esfuerzos realizados por las empresas para encontrar y corregir las vulnerabilidades, es común que surjan nuevas vulnerabilidades. Microsoft, Apple y otros productores de sistemas operativos lanzan parches y actualizaciones casi todos los días.

Las actualizaciones de las aplicaciones también son comunes. Las aplicaciones como navegadores web, aplicaciones móviles y servidores web son actualizadas con frecuencia por las empresas y las organizaciones responsables de estas.

SYNful Knock

En 2015, una vulnerabilidad importante, llamada SYNful Knock, se descubrió en Cisco IOS.

Esta vulnerabilidad permitió a los atacantes obtener el control de los routers de nivel empresarial, como los antiguos routers 1841, 2811 y 3825 de Cisco.

Los atacantes pudieron así monitorear todas las comunicaciones de red y tuvieron la capacidad de infectar otros dispositivos de la red.

Esta vulnerabilidad se introdujo en el sistema cuando una versión alterada de IOS se instaló en los routers.

Para evitar esto, verifique siempre la integridad de la imagen de IOS descargada y limite el acceso físico al equipo solo al personal autorizado.

El objetivo de las actualizaciones de software

- El objetivo de las actualizaciones de software es mantenerse actualizado y evitar el aprovechamiento de vulnerabilidades.
- Si bien algunas empresas tienen equipos de prueba de penetración dedicados a la búsqueda y la corrección de vulnerabilidades de software antes de que puedan ser aprovechadas, hay investigadores de seguridad independientes que también se especializan en la búsqueda de vulnerabilidades de software.
- El Proyecto Zero de Google es un excelente ejemplo de esta práctica.
- Después de descubrir varias vulnerabilidades en los diversos programas de software utilizados por los usuarios finales, Google formó un equipo dedicado a encontrar vulnerabilidades de software.
- La investigación de seguridad de Google puede encontrarse aquí.

Vulnerabilidades de hardware

- Las vulnerabilidades de hardware se presentan a menudo mediante defectos de diseño del hardware.
- La memoria RAM, por ejemplo, consiste básicamente en condensadores instalados muy cerca unos de otros.
- Se descubrió que, debido a la cercanía, los cambios constantes aplicados a uno de estos condensadores podían influir en los condensadores vecinos.
- Por este fallo de diseño, se generó una vulnerabilidad llamada Rowhammer.
- Mediante la reescritura repetida de memoria en las mismas direcciones, el ataque Rowhammer permite que se recuperen los datos de las celdas de memoria de direcciones cercanas, incluso si las celdas están protegidas.

Vulnerabilidades de hardware

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

La memoria RAM, por ejemplo, consiste básicamente en condensadores instalados muy cerca unos de otros.

Se descubrió que, debido a la cercanía, los cambios constantes aplicados a uno de estos condensadores podían influir en los condensadores vecinos.

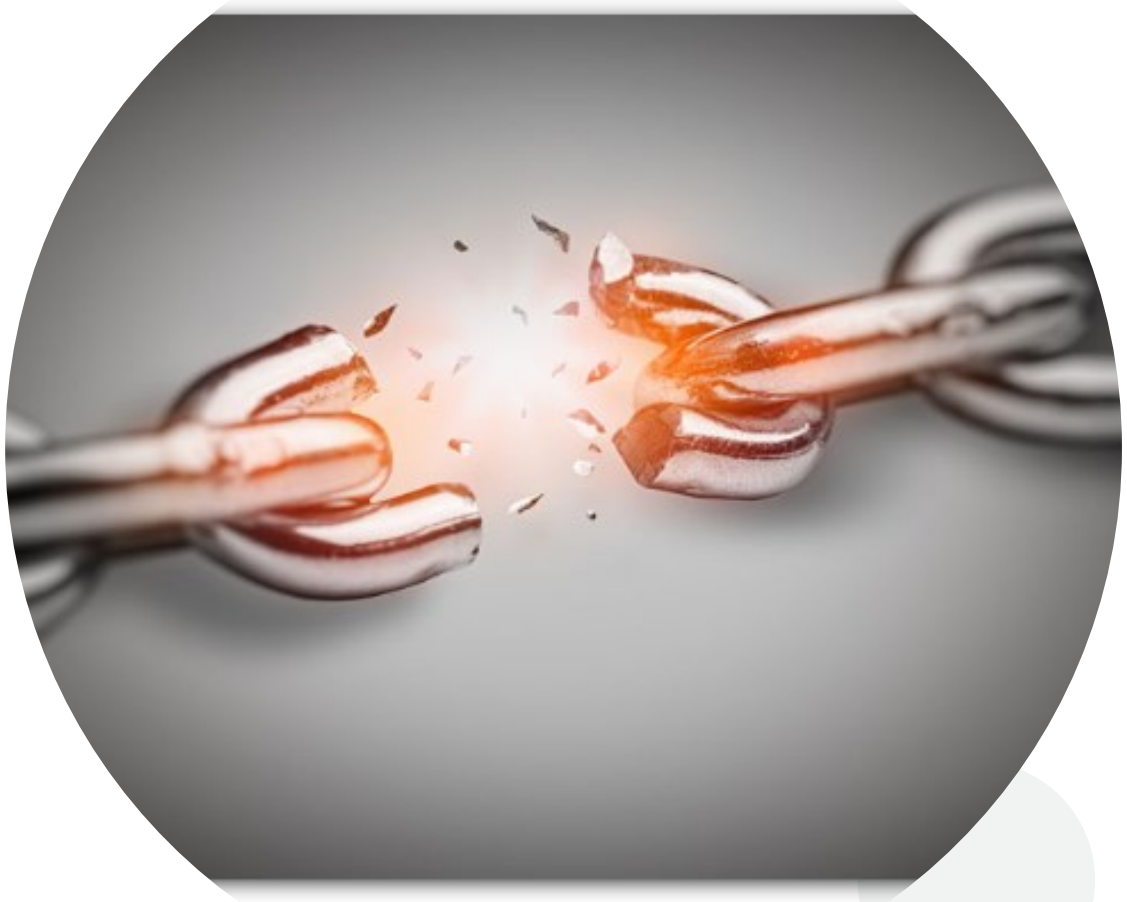
Por este fallo de diseño, se generó una vulnerabilidad llamada **Rowhammer.**

Mediante la reescritura repetida de memoria en las mismas direcciones,

el ataque Rowhammer permite que se recuperen los datos de las celdas de memoria de direcciones cercanas, incluso si las celdas están protegidas.

Ataques altamente dirigidos

- Las vulnerabilidades de hardware son específicas de los modelos de dispositivos y generalmente no se ven atacadas por intentos comprometedores aleatorios.
- Si bien las vulnerabilidades de hardware son más comunes en **ataques altamente dirigidos,** la protección contra malware tradicional y la seguridad física son suficientes para proteger al usuario común.



Clasificación de las vulnerabilidades de seguridad

Clasificación de las vulnerabilidades de seguridad

Desbordamiento del 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.

Clasificación de las vulnerabilidades de seguridad

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.

Clasificación de las vulnerabilidades de seguridad

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.**

Clasificación de las vulnerabilidades de seguridad

Debilidades en las prácticas de seguridad:

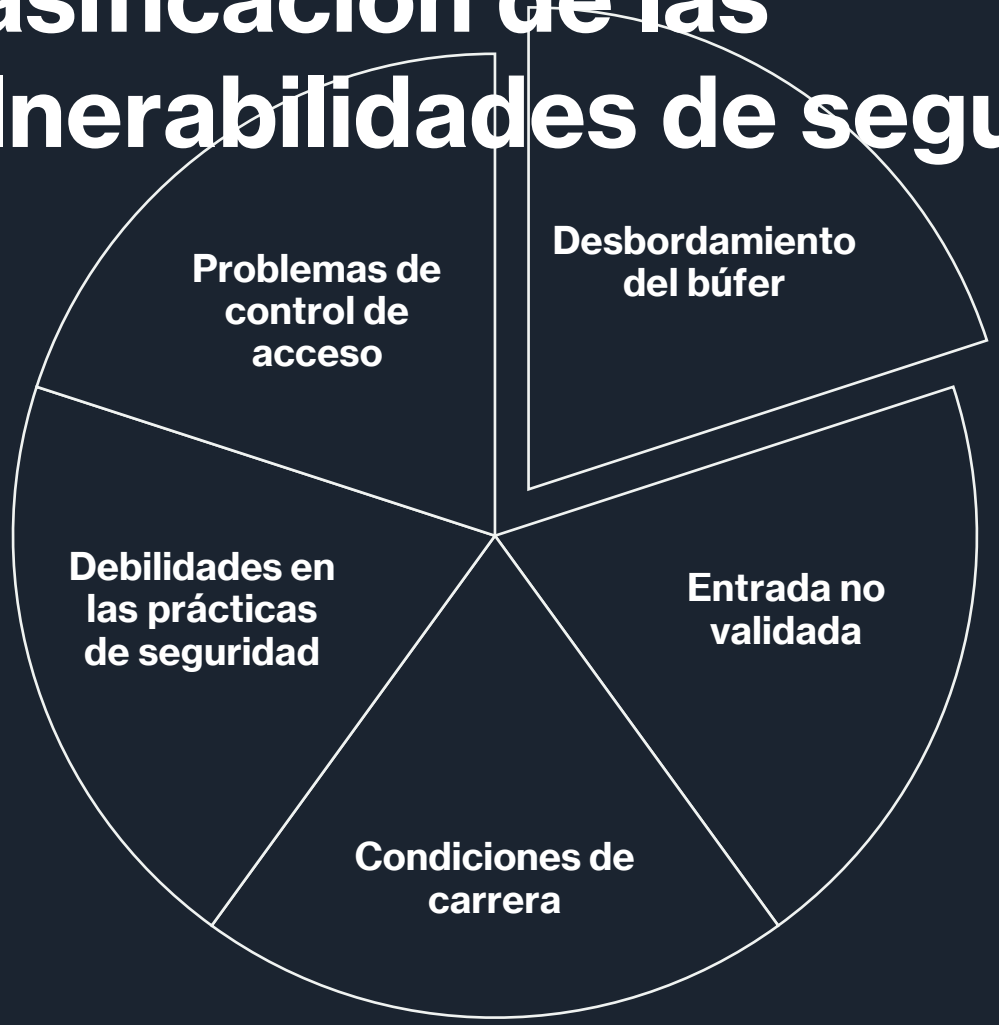
- Los sistemas y los datos confidenciales pueden protegerse con técnicas tales como autenticación, autorización y encriptación.
- Los desarrolladores no deben intentar crear sus propios algoritmos de seguridad porque es probable que introduzcan vulnerabilidades.
- Se recomienda encarecidamente que los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

Clasificación de las vulnerabilidades de seguridad

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.

Clasificación de las vulnerabilidades de seguridad



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

- Malware, acrónimo para el inglés “Malicious Software” (Software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema. A continuación, se encuentran algunos tipos comunes de malware:

- **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. En el intento por superar las medidas de seguridad, el spyware a menudo modifica las configuraciones de seguridad. El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

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

- **Bot:** de la palabra robot, un bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea. Si bien la mayoría de los bots son inofensivos, un uso cada vez más frecuente de bots maliciosos es el de los botnets. Varias computadoras pueden infectarse con bots programados para esperar silenciosamente los comandos provistos por el atacante.

- **Ransomware:** este malware está diseñado para mantener captivo un sistema de computación o los datos que contiene hasta que se realice un pago. El ransomware trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario. Algunas otras versiones de ransomware pueden aprovechar vulnerabilidades específicas del sistema para bloquearlo. El ransomware se esparce por un archivo descargado o alguna vulnerabilidad de software.

- **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. Estas ventanas muestran mensajes falsificados que indican que el sistema está en riesgo o necesita la ejecución de un programa específico para volver al funcionamiento normal. En realidad, no se evaluó ni detectó ningún problema y, si el usuario acepta y autoriza la ejecución del programa mencionado, el sistema se infecta con malware.

- **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 detectarlos. A menudo, una computadora infectada por un rootkit debe limpiarse y reinstalarse.

- **Virus:** un 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. Los virus pueden ser inofensivos y simplemente mostrar una imagen o pueden ser destructivos, como los que modifican o borran datos. Los virus también pueden programarse para mutar a fin de evitar la detección. La mayoría de los virus ahora se esparcen por unidades USB, discos ópticos, recursos de red compartidos o correo electrónico.

- **Troyano:** un 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. A menudo, los troyanos se encuentran en archivos de imagen, archivos de audio o juegos. Un troyano se diferencia de un virus en que se adjunta a archivos no ejecutables.

- **Gusanos:** 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 por la red. Los gusanos comparten patrones similares. Todos tienen una vulnerabilidad de activación, una manera de propagarse y contienen una carga útil.

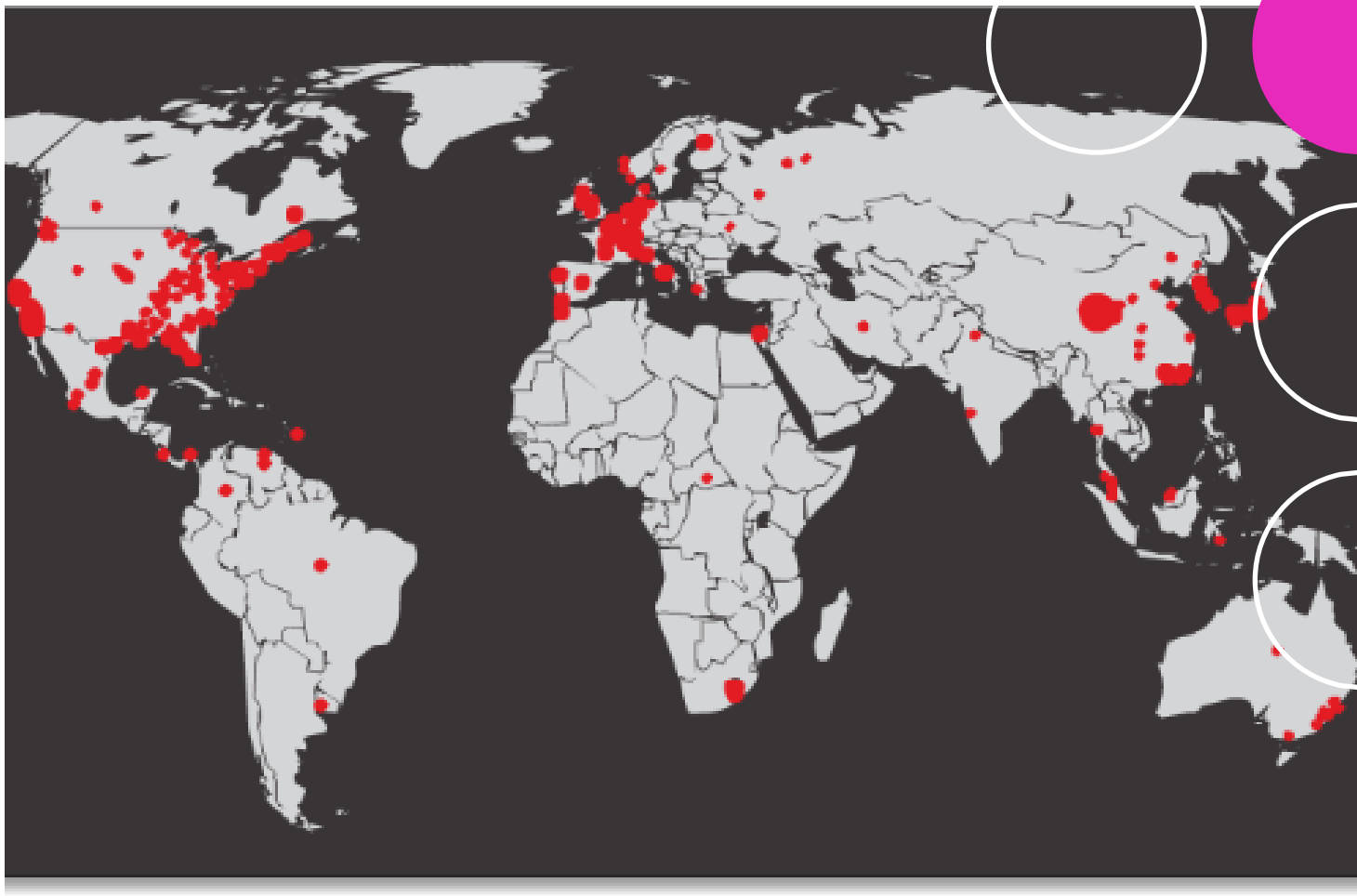
- Los gusanos son responsables de algunos de los ataques más devastadores en Internet. Como se muestra en la Figura 1, en 2001 el gusano Código Rojo infectó 658 servidores. En el plazo de 19 horas, el gusano infectó más de 300 000 servidores, como se muestra en la Figura 2.

- **Hombre en el medio (MitM):** el 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. Los ataques MitM se usan ampliamente para robar información financiera. Existen muchas técnicas y malware para proporcionar capacidades de MitM a los atacantes.

- **Hombre en el móvil (MitMo):** una variación del hombre en el medio, el MitMo es un tipo de atague 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.

Tipos de malware

- Malware, acrónimo para el inglés “Malicious Software” (Software malicioso), es cualquier código que pueda utilizarse para robar datos, evitar los controles de acceso, ocasionar daños o comprometer un sistema.



Tipos de malware

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.

En el intento por superar las medidas de seguridad, el spyware a menudo modifica las configuraciones de seguridad.

El spyware con frecuencia se agrupa con el software legítimo o con caballos troyanos.

Adware:

El software de publicidad está diseñado para brindar anuncios automáticamente.

El adware a veces se instala con algunas versiones de software.

Algunos adware están diseñados para brindar solamente anuncios, pero también es común que el adware incluya spyware.

Bot:

De la palabra robot, un bot es un malware diseñado para realizar acciones automáticamente, generalmente en línea.

Si bien la mayoría de los bots son inofensivos, un uso cada vez más frecuente de bots maliciosos es el de los botnets.

Varias computadoras pueden infectarse con bots programados para esperar silenciosamente los comandos provistos por el atacante.

Tipos de malware

Ransomware:

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

El ransomware trabaja generalmente encriptando los datos de la computadora con una clave desconocida para el usuario.

Algunas otras versiones de ransomware pueden aprovechar vulnerabilidades específicas del sistema para bloquearlo.

El ransomware se esparce por un archivo descargado o alguna vulnerabilidad de software.

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.

Estas ventanas muestran **mensajes falsificados** que indican que el sistema está en riesgo o necesita la ejecución de un programa específico para volver al funcionamiento normal.

En realidad, **no se evaluó ni detectó ningún problema** y, si el usuario acepta y autoriza la ejecución del programa mencionado, el sistema se infecta con malware.

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 detectarlos.

A menudo, una computadora infectada por un rootkit debe limpiarse y reinstalarse.

Tipos de malware

Virus:

Un 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.

Los virus pueden ser inofensivos y simplemente mostrar una imagen o pueden ser destructivos, como los que modifican o borran datos.

Los virus también pueden programarse para mutar a fin de evitar la detección.

La mayoría de los virus ahora se esparcen por unidades USB, discos ópticos, recursos de red compartidos o correo electrónico.

Troyano:

Un 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.

A menudo, los troyanos se encuentran en archivos de imagen, archivos de audio o juegos.

Un troyano se diferencia de un virus en que se adjunta a archivos no ejecutables.

Gusanos:

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 por la red.

Los gusanos comparten patrones similares.

Todos tienen una vulnerabilidad de activación, una manera de propagarse y contienen una carga útil.

En el plazo de 19 horas, el gusano rojo infectó más de 300 000 servidores

Tipos de malware

Hombre en el medio (MitM):

El 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.

Los ataques MitM se usan ampliamente para robar información financiera.

Existen muchas técnicas y malware para proporcionar capacidades de MitM a los atacantes.

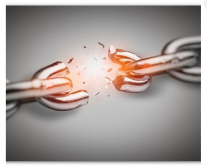
Hombre en el móvil (MitMo):

Una 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

- Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes 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.

Síntomas de malware

- Independientemente del tipo de malware con el que se ha infectado un sistema, estos son síntomas frecuentes de malware:

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.

Los ingenieros sociales con frecuencia dependen de la disposición de las personas para ayudar, pero también se aprovechan de sus vulnerabilidades.

Por ejemplo, un atacante puede llamar a un empleado autorizado con un problema urgente que requiere acceso inmediato a la red.

El atacante puede atraer la vanidad o la codicia del empleado o invocar la autoridad mediante técnicas de nombres.

Estos son algunos tipos de ataques de ingeniería social:

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.

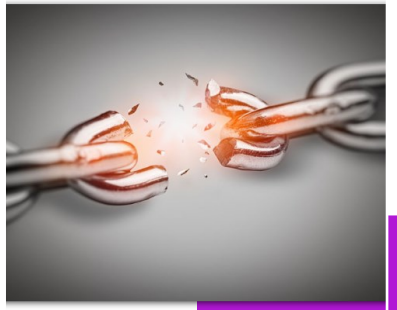
Seguimiento: esto es cuando un atacante persigue rápidamente a una persona autorizada a un lugar seguro.

Algo por algo (quid pro quo): esto es cuando un atacante solicita información personal de una parte a cambio de algo, por ejemplo, un obsequio.

Decodificación de contraseñas Wi-Fi

- La decodificación de contraseñas Wi-Fi es el proceso de detección de la contraseña utilizada para proteger la red inalámbrica. Estas son algunas técnicas utilizadas en la decodificación de contraseñas:

Algunas técnicas utilizadas en la decodificación de contraseñas:



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.
- Este es un archivo de texto que contiene una lista de palabras tomadas del diccionario.
- Un programa luego prueba cada palabra y las combinaciones comunes.
- Debido a que los ataques por fuerza bruta llevan tiempo, las contraseñas complejas llevan mucho más tiempo para descifrar.
- Algunas herramientas para forzar las contraseñas incluyen Ophcrack, L0phtCrack, THC Hydra, RainbowCrack y Medusa.

Algunas técnicas utilizadas en la decodificación de contraseñas:

Ingeniería social:

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

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.
- El objetivo de este mensaje es engañar al destinatario para que instale malware en su dispositivo o comparta información personal o financiera.
- Un ejemplo de suplantación de identidad es un correo electrónico falsificado similar al enviado por una tienda de conveniencia que solicita al usuario que haga clic en un enlace para reclamar un premio.
- El enlace puede ir a un sitio falso que solicita información personal o puede instalar un virus.

Suplantación de identidad

- La 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.

Amenazas persistentes avanzadas

- 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 (DoS) son un tipo de ataque a la red. Un ataque DoS da como resultado cierto tipo de interrupción del servicio de red a los usuarios, los dispositivos o las aplicaciones. Existen dos tipos principales de ataques DoS:

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

- **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 zombie 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.

DDoS

- **Los 7 mayores ataques DDoS de la historia de internet**
  - Gusano Morris
  - Ataque DDoS que tumbó Yahoo!, Amazon, eBay y muchos otros portales
  - Code Red, el gusano que provocó un DDoS a La Casa Blanca
  - SQL Slammer, el ataque que aumentó un 25% el tráfico de Internet
  - Ataque DDoS contra Spamhaus
  - DynDNS, el ataque masivo que tumbó medio Internet
  - Ataque contra Github

Envenenamiento SEO

- Los motores de búsqueda, como Google, funcionan clasificando páginas y presentando resultados relevantes conforme a las consultas de búsqueda de los usuarios.
- Según la importancia del contenido del sitio web, puede aparecer más arriba o más abajo en la lista de resultados de la búsqueda.
- La optimización de motores de búsqueda (SEO, por sus siglas en inglés) es un conjunto de técnicas utilizadas para mejorar la clasificación de un sitio web por un motor de búsqueda. Aunque muchas empresas legítimas se especializan en la optimización de sitios web para mejorar su posición, un usuario malintencionado puede utilizar la SEO para hacer que un sitio web malicioso aparezca más arriba en los resultados de la búsqueda. Esta técnica se denomina envenenamiento SEO.
- El objetivo más común del envenenamiento SEO es aumentar el tráfico a sitios maliciosos que puedan alojar malware o ejercer la ingeniería social.
- Para forzar un sitio malicioso para que califique más alto en los resultados de la búsqueda, los atacantes se aprovechan de los términos de búsqueda populares.

¿Qué es un ataque combinado?

- Los ataques combinados son ataques que usan diversas técnicas para comprometer un objetivo.
  - Mediante el uso de varias técnicas de ataque simultáneas, los atacantes tienen malware que combina gusanos, troyanos, spyware, registradores de pulsaciones, spam y esquemas de suplantación de identidad.
  - Esta tendencia de ataques combinados revela malware más complejo y pone los datos de los usuarios en gran riesgo.

¿Qué es un ataque combinado?

- Los tipos más comunes de ataque combinado utilizan mensajes de correo electrónico no deseado, mensajes instantáneos o sitios web legítimos para distribuir enlaces donde se descarga malware o spyware secretamente en la computadora.
- Otro ataque combinado común utiliza DDoS combinado con correos electrónicos de suplantación de identidad (phishing).
  - Primero, el ataque DDoS se utiliza para suspender un sitio web popular de un banco y enviar correos electrónicos a sus clientes disculpándose por la inconveniencia.
  - El correo electrónico además redirecciona a los usuarios a un sitio de emergencia falso donde la información real de inicio de sesión puede ser robada.

¿Qué es un ataque combinado?

- Muchos de los gusanos más perjudiciales de las computadoras, como Nimbda, CodeRed, BugBear, Klez y Slammer, se categorizan mejor como ataques combinados, como se muestra a continuación:
  - Algunas variantes de Nimbda utilizan archivos adjuntos de correo electrónico, descargas de archivos de un servidor web comprometido y uso compartido de archivos de Microsoft (intercambios anónimos) como métodos de propagación.
  - Otras variantes de Nimbda pueden modificar las cuentas de invitado del sistema para proporcionar al atacante o código malicioso los privilegios administrativos.
  - Los gusanos recientes Conficker y ZeuS/LICAT también son ataques combinados.
  - Conficker utiliza todos los métodos de distribución tradicionales.

¿Qué es la reducción del impacto?

- Si bien la mayoría de las empresas exitosas de hoy en día son conscientes de los problemas de seguridad comunes y ponen gran esfuerzo en su prevención, no hay ningún conjunto de prácticas de seguridad 100 % eficiente.
  - Dado que es probable que ocurra una BRECHA DE seguridad si el premio es grande, las empresas y organizaciones también deben estar preparadas para contener el daño.
- Es importante comprender que el impacto de la BRECHA de seguridad no solo está relacionado con el aspecto técnico, los datos robados, las bases de datos dañadas o los daños a la propiedad intelectual;
  - los daños también se extienden a la reputación de la empresa. Responder ante una infracción de datos es un proceso muy dinámico.

¿Qué es la reducción del impacto?

A continuación, hay algunas medidas importantes que una empresa debe adoptar cuando identifica una violación de seguridad, según muchos expertos en seguridad:

- Comunicar el problema.
    - Informar internamente a los empleados del problema y llamarlos a la acción. Informar externamente a los clientes a través de comunicación directa y anuncios oficiales. La comunicación genera transparencia, que es crucial para este tipo de situación.
- Ser sincero y responsable en caso de que la empresa tenga la culpa.
- Proporcionar detalles.
    - Explicar por qué ocurrió la situación y qué se vio afectado. También se espera que la empresa se haga cargo de los costos de los servicios de protección contra el robo de identidad para los clientes afectados.

¿Qué es la reducción del impacto?

- A continuación, hay algunas medidas importantes que una empresa debe adoptar cuando identifica una violación de seguridad, según muchos expertos en seguridad:
- Comprender qué causó y facilitó la violación de seguridad.
    - De ser necesario, contrate expertos en informática forense para investigar y conocer los detalles.
- Aplicar lo aprendido de la investigación de informática forense para garantizar que no se produzcan violaciones de seguridad similares en el futuro.
- Asegurarse de que todos los sistemas estén limpios, que no se hayan instalado puertas traseras y que no haya nada más comprometido.
    - Los atacantes con frecuencia probarán dejar una puerta trasera para facilitar las infracciones futuras. Asegúrese de que esto no suceda.
- Capacitar a los empleados, los partners y los clientes acerca de cómo prevenir las violaciones futuras.

Resumen

- Este capítulo cubre las maneras en que los profesionales de la ciberseguridad analizan qué ocurrió después de un ciberataque. Explica las vulnerabilidades de seguridad en software y hardware y las distintas categorías de las vulnerabilidades de seguridad.
- Explica los diferentes tipos de software malicioso (conocido como malware) y los síntomas de malware. Parte del malware analizado incluyó virus, gusanos, troyanos, spyware, adware y otros.

Resumen

- Se cubrieron las diferentes maneras en que los atacantes pueden infiltrarse en un sistema, entre ellas, la ingeniería social, la decodificación de contraseñas Wi-Fi, la suplantación de identidad y el aprovechamiento de vulnerabilidades. También se explicaron distintos tipos de ataques de denegación de servicio.
- Los ataques combinados usan varias técnicas para infiltrarse en un sistema y atacarlo. Muchos de los gusanos más perjudiciales para las computadoras, como Nimbda, CodeRed, BugBear, Klez y Slammer, se categorizan mejor como ataques combinados. Cuando un ataque no puede evitarse, es el trabajo del profesional de ciberseguridad reducir el impacto de dicho ataque.