SEGURIDAD REDES

MTIE Oliver Manuel García Mauricio


Seguridad de la red

Riesgos de intrusiones en la red

Robo de información

Pérdida y manipulación de datos

Robo de identidad

Interrupción del servicio

Robo de información

Ingreso no autorizado a una computadora para obtener información confidencial. La información puede utilizarse o venderse con diferentes fines. Ejemplo: robar información patentada de una organización, como información de investigación y desarrollo.

Ya sean redes conectadas por cable o inalámbricas, las redes de computadoras son cada vez más fundamentales para las actividades cotidianas. Tanto las personas como las organizaciones dependen de sus computadores y de las redes para funciones como correo electrónico, contabilidad, organización y administración de archivos. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes.

Los intrusos pueden obtener acceso a la red a través de vulnerabilidades del software, ataques al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona. Por lo general, a los intrusos que obtienen acceso mediante la modificación del

Robo de información

Pérdida y manipulación de datos

Robo de identidad

Interrupción del servicio

Interrupción del servicio

Se impide que los usuarios legítimos puedan acceder a servicios que deberían poder utilizar. Ejemplos: ataques de denegación de servicios (DoS) a servidores, dispositivos de red o enlaces de comunicaciones de red.

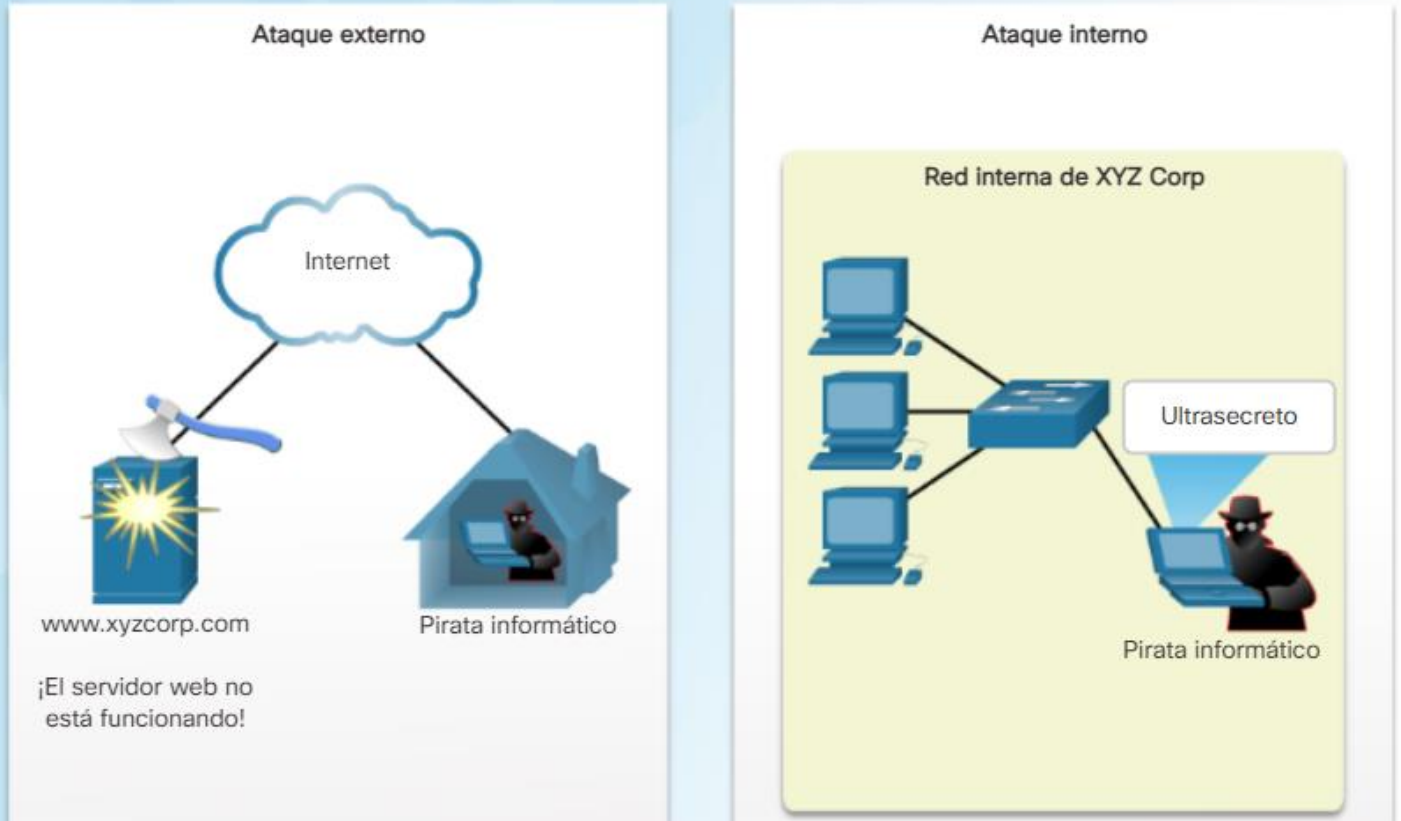
al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que el pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Robo de identidad
- Pérdida y manipulación de datos
- Interrupción del servicio

Haga clic en cada signo más (+) de la figura para obtener más información.

Externo versus interno



¿De dónde vienen?

Las amenazas de seguridad causadas por intrusos en la red pueden originarse tanto en forma interna como externa.

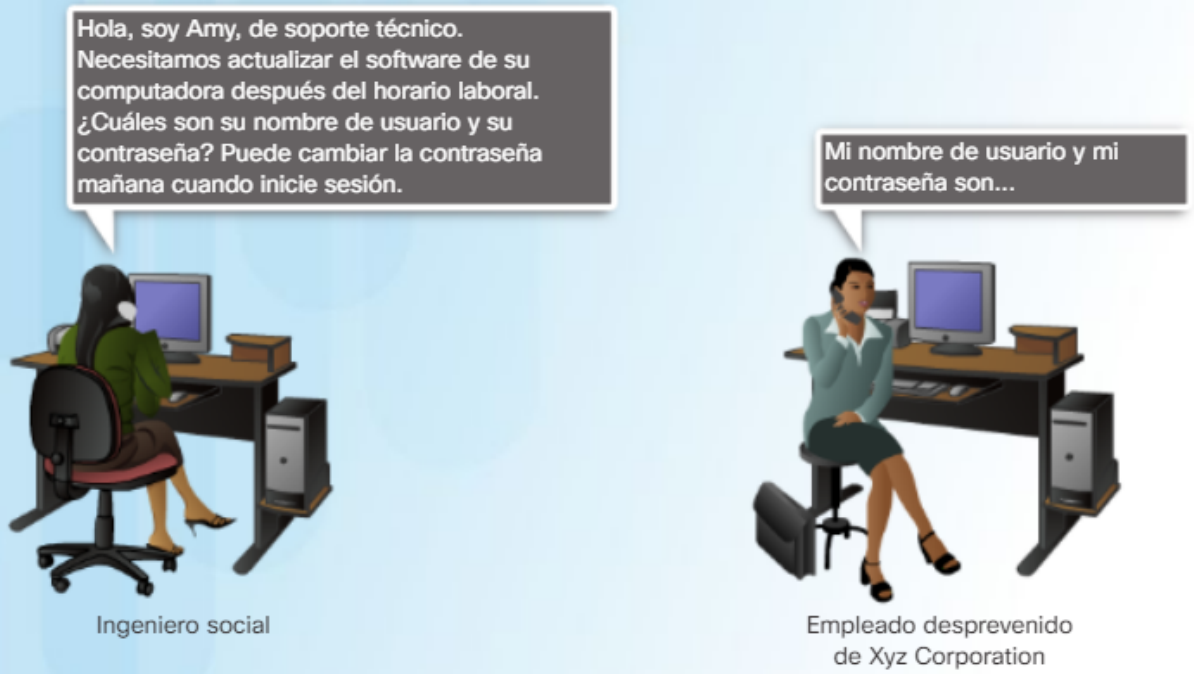
Amenazas externas

Las amenazas externas provienen de personas que trabajan fuera de una organización. Estas personas no tienen autorización para acceder al sistema o a la red de la computadora. Los atacantes externos logran ingresar a la red principalmente desde Internet, enlaces inalámbricos o servidores de acceso telefónico.

Amenazas internas

Las amenazas internas se producen cuando alguien tiene acceso autorizado a la red a través de la cuenta de un usuario o si tiene acceso

Descripción general de la ingeniería social



¿Quiere mi contraseña?

Para un intruso, una de las formas más fáciles de obtener acceso, ya sea interno o externo, es el aprovechamiento de las conductas humanas. Uno de los métodos más comunes de aprovechamiento de las debilidades humanas se denomina ingeniería social.

Ingeniería social

Ingeniería social es un término que hace referencia a la capacidad de algo o alguien para influenciar la conducta de un grupo de personas. En el contexto de seguridad de computadoras y red, ingeniería social se refiere a un conjunto de técnicas que se usan para engañar a los usuarios internos para que realicen acciones específicas o divulguen información confidencial.

A través de estas técnicas, el atacante se

Phishing

Aprovecharse de la confianza del usuario

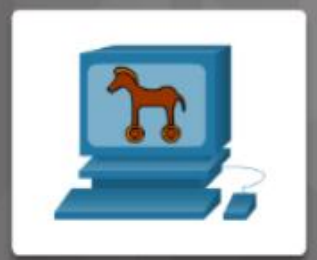
Tres de los métodos más comunes que usan los hackers para obtener información directamente de los usuarios autorizados reciben nombres poco comunes: pretexting, phishing y vishing.

Pretexting

Pretexting es una forma de ingeniería social en la que se utiliza una situación inventada (la evasiva) para que una víctima divulgue información o lleve a cabo una acción. Generalmente, el contacto con el objetivo se establece telefónicamente. Para que el pretexting sea efectivo el atacante deberá establecer la legitimidad con la víctima o el objetivo deseado. Esto requiere, por lo general, que el atacante cuente con conocimientos o investigaciones previas. Por ejemplo: si el atacante conoce el número de seguro social del objetivo, puede utilizar esta información para

Virus

Gusanos



Caballos de Troya

Cuando el software es el problema

La ingeniería social es una amenaza de seguridad común que se basa en la debilidad humana para obtener los resultados deseados.

Además de la ingeniería social, existen otros tipos de ataques que explotan las vulnerabilidades de los software de computadoras. Algunos ejemplos de técnicas de ataque son: virus, gusanos y caballos de Troya. Todos estos son tipos de software maliciosos que se introducen en un host. Pueden dañar un sistema, destruir datos y también denegar el acceso a redes, sistemas o servicios. También pueden enviar datos y detalles personales de usuarios de PC desprevenidos a delincuentes. En muchos casos, pueden replicarse y propagarse a otros hosts conectados a la red. Imagine lo difícil que sería reconstruir archivos guardados, como archivos de juegos, archivos de claves de

Reproducir

Programas maliciosos

Virus

Un virus es un programa que se propaga modificando otros programas o archivos. Un virus no puede iniciarse por sí mismo, sino que debe ser activado. Una vez activado, un virus no puede hacer más que replicarse y propagarse. A pesar de ser simple, hasta este tipo de virus es peligroso, ya que puede utilizar rápidamente toda la memoria disponible e interrumpir completamente el sistema. Un virus más peligroso puede estar programado para borrar o dañar archivos específicos antes de propagarse. Los virus pueden transmitirse por correo electrónico, archivos descargados, mensajes instantáneos, CD o dispositivos USB.

Gusanos

Un gusano es similar a un virus pero, a diferencia de éste, no necesita adjuntarse a un programa existente. Un gusano utiliza la red

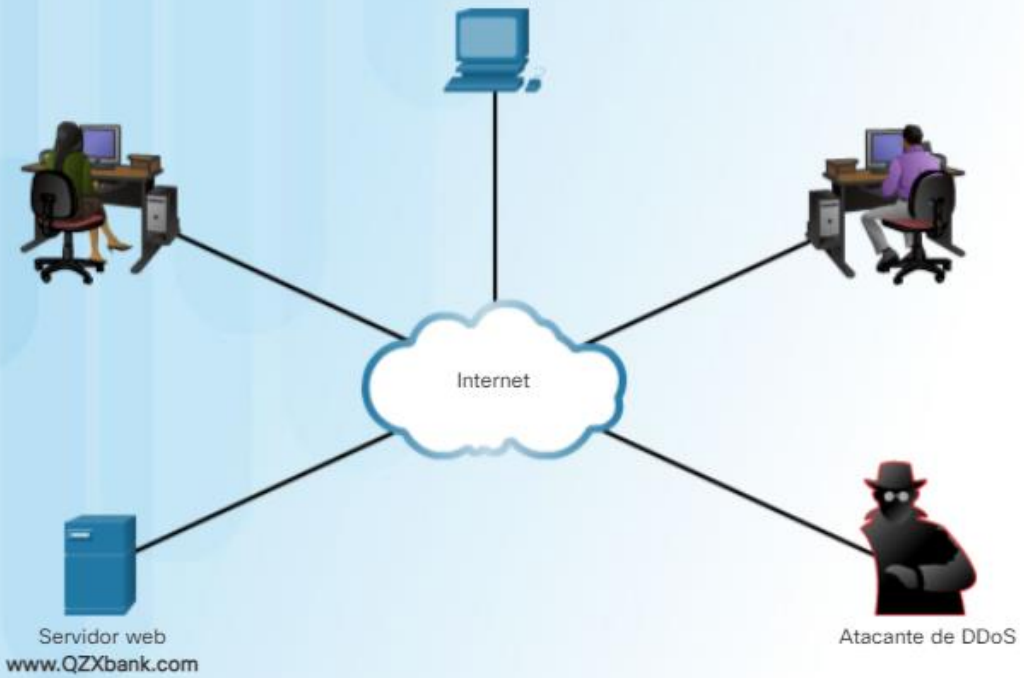
Reproducir

Gusanos

Un gusano es similar a un virus pero, a diferencia de éste, no necesita adjuntarse a un programa existente. Un gusano utiliza la red para enviar copias de sí mismo a cualquier host conectado. Un gusano puede ejecutarse independientemente y propagarse rápidamente. No requieren necesariamente activación o intervención humana. Los gusanos que se propagan por sí mismos por la red pueden tener un impacto mucho mayor que un simple virus y pueden infectar rápidamente grandes partes de Internet.

Caballos de Troya

Un troyano es un programa escrito para que parezca un programa legítimo, cuando en realidad es una herramienta de ataque. No puede replicarse. Un caballo de Troya se basa en su apariencia legítima para engañar a una víctima a fin de que inicie el programa. Puede ser relativamente inofensivo o contener códigos que pueden dañar el contenido del disco duro



Ser víctima de saturación por paquetes

Los ataques de DoS que provienen de una única dirección IP pueden interrumpir el funcionamiento de un sitio web durante un período de tiempo hasta que se logra aislar el ataque y tomar medidas de defensa. Los tipos de ataques más sofisticados pueden desconectar servicios web durante mucho más tiempo.

Denegación de servicio distribuida (DDoS, Distributed Denial of Service)

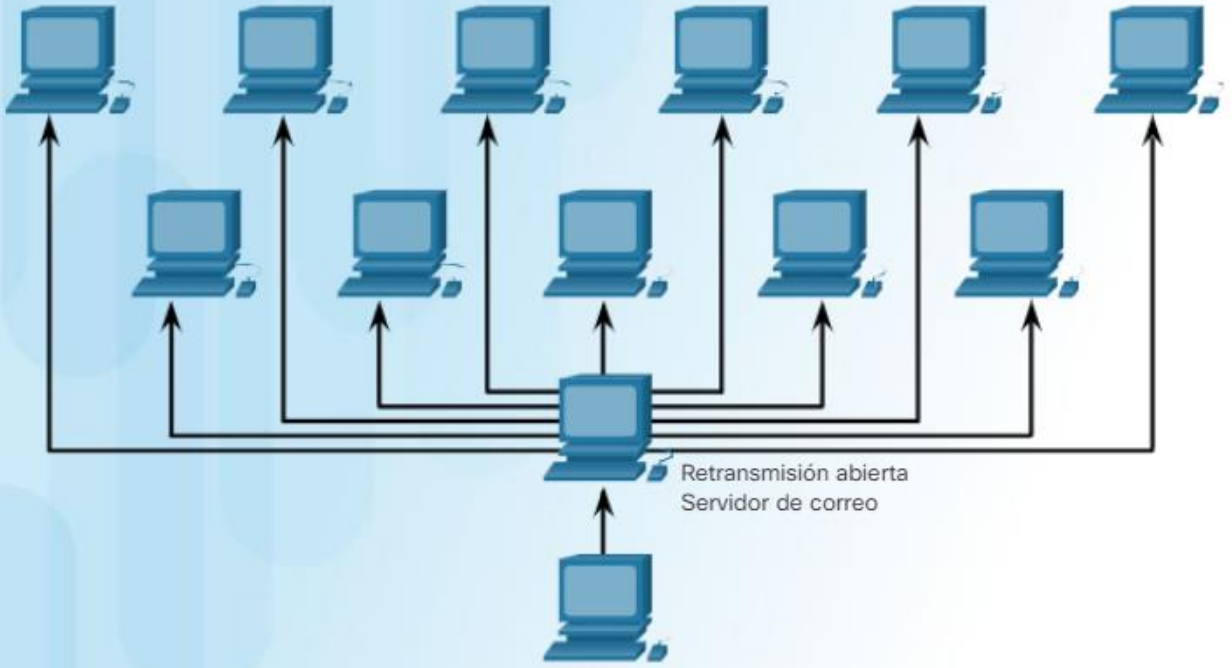
La DDoS es una forma de ataque DoS más sofisticada y potencialmente más perjudicial. Está diseñada para saturar y sobrecargar los enlaces de red con datos inútiles. Los ataques DDoS operan en una escala mucho mayor que los ataques DoS. Generalmente, cientos o miles de puntos de ataque intentan saturar un objetivo al mismo tiempo. Los puntos de ataque

Adware

El adware es una forma de spyware utilizada para recopilar información acerca de un usuario, de acuerdo con los sitios Web que éste visita. A continuación, esta información se utiliza para publicidad orientada a un usuario en particular. Generalmente, el usuario instala el adware a cambio de un producto "gratuito". Cuando un usuario abre una ventana del navegador, el adware puede iniciar nuevas instancias del navegador que intentan publicitar productos o servicios de acuerdo con las prácticas de navegación del usuario. Las ventanas no deseadas del explorador pueden abrirse repetidamente y pueden dificultar mucho la navegación por Internet, en especial en las conexiones de Internet más lentas. El adware puede ser muy difícil de desinstalar.

Elementos emergentes y ventanas pop-under

Los elementos emergentes y las ventanas pop-under son ventanas de publicidad adicionales que aparecen cuando se visita un sitio Web. A



Botnets y zombis

Otro de los molestos productos derivados de nuestra confianza cada vez mayor en las comunicaciones electrónicas es el tráfico de correo electrónico no deseado. En algunas ocasiones, los comerciantes no desean perder tiempo con el marketing orientado. Desean enviar sus publicidades por correo electrónico a tantos usuarios finales como sea posible, con la esperanza de que alguien se interese en su producto o servicio. Este enfoque de marketing de amplia distribución en Internet se conoce como correo no deseado. Una de las principales formas en las que el spam puede enviarse es mediante el uso de un botnet o bot.

"Bot" deriva de la palabra "robot", que describe el funcionamiento del dispositivo cuando queda infectado. El software tipo bot malicioso infecta un host, generalmente por medio de un correo electrónico o de un enlace a una página web, cuando descarga e instala una función de