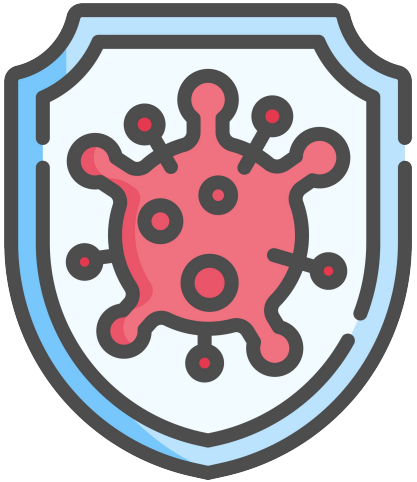
UNIVERSIDAD DE COSTA RICA

CI Centro de Informática



Ciberataques

Seguridad de la información

Temas: II Parte

I Parte

- Ataques a contraseñas
- Ataques por Ingeniería Social
- Medias de protección

II Parte:

- **Ataques a las conexiones**
- **Medidas de protección**

III Parte

- Ataques por malware
- Medidas de protección

Centro de Informática

Expositores:

Ing. Rebeca Esquivel Flores,M.Sc.

Sr. Mario Murillo Chinchilla.

Área de Gestión de Comunicaciones, CI.

Centro de
Informática

Ataques Ciberseguridad

Los ciberdelincuentes se encuentran siempre al acecho de nuevas formas para atacar a los usuarios, aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas.

1. Ataques a las conexiones

Se basan en un conjunto de técnicas:

- Los ataques a las conexiones cableadas e inalámbricas se realizan con diversos software y herramientas para saltar las medidas de seguridad, infectar y tomar control de los dispositivos.
- Se interponen en el intercambio de información entre nosotros y el servicio web, para monitorizar y robar datos personales, bancarios, contraseñas, entre otros.

Redes trampa
Spoofing
Ataques a Cookies
Ataques DDoS
Inyección SQL Escaneo de puertos Man in the middle
Sniffing.

1.Ataques a las conexiones

Redes Trampa

¿Cómo funciona?

- Creación de redes wifi falsas.
- Creación de una red wifi gemela, simulando ser legítima y segura, con un nombre igual o parecida, utilizando software o hardware y configurando los mismos parámetros.

Centro de Informática

Ataques a las conexiones

Redes Trampa

¿Cual es su objetivo?

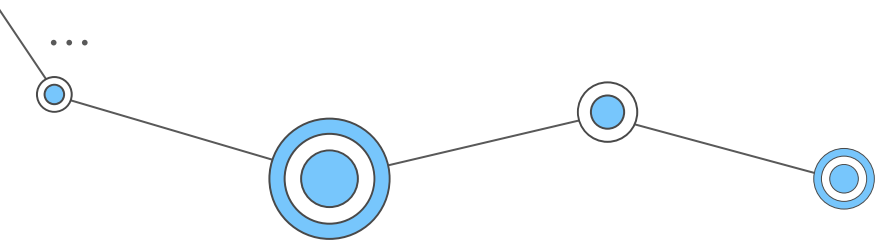
Robar datos cuando accedemos a la cuenta bancaria, redes sociales o correo electrónico.

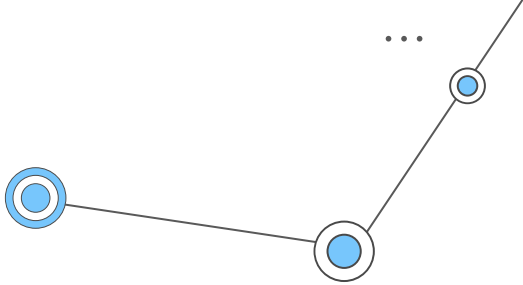
El ciberdelincuente puede tomar control sobre nuestra navegación, accediendo a determinadas páginas web fraudulentas o paǵinas web muy similares a la original, preparadas para el engaño o para la infección por malware.

¿Cómo se propaga/infecta/extiende?

En lugares con una red wifi pública, con gran afluencia de usuarios.

La red falsa pueda pasar desapercibida y engañar al mayor número de víctimas posible.





CI Centro de Informática

Ataques a las conexiones

Redes Trampa

¿Cómo me protejo?

Aprendiendo a identificar las redes wifi falsas:

- Redes abiertas, que además permiten introducir cualquier contraseña.
- Desconecte la función del dispositivo móvil para conectarse automáticamente a redes abiertas.
- En caso de necesidad, se puede recurrir a una VPN.

Ataques a las conexiones

Spoofing

¿Cómo funciona?

Empleo de técnicas de hacking de forma maliciosa para suplantar nuestra identidad, la de una web o una entidad. Se basa en tres partes: el atacante, la víctima y el sistema o entidad virtual que va a ser falsificado.

El objetivo de los atacantes es, disponer de un acceso a nuestros datos mediante esta suplantación. Según el tipo de Spoofing, la suplantación y el engaño se llevarán a cabo de forma distinta.

Como protección, es fundamental que nos mantengamos alerta y sigamos las recomendaciones para una navegación segura.

Hacking: conjunto de técnicas a través de las cuales se accede a un sistema informático, vulnerando las medidas de seguridad establecidas originariamente.

Ataques a las conexiones

IP Spoofing

¿Cómo funciona?

El ciberdelincuente consigue falsificar su dirección IP y hacerla pasar por una dirección distinta.

Consigue saltarse las restricciones del enrutador del servidor o del nuestro y hacernos llegar un paquete con malware.

Centro de Informática

Ataques a las conexiones

IP Spoofing

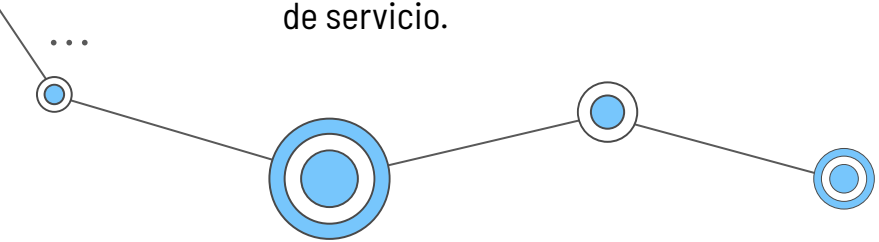
¿Cual es su objetivo?

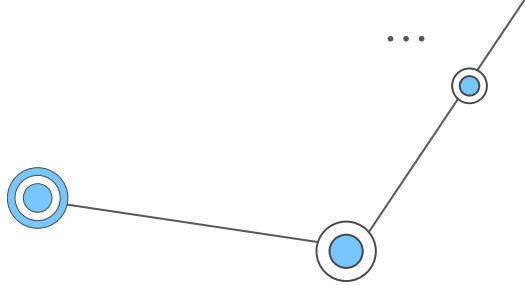
Obtener acceso a redes que sirven para autenticar a los usuarios o que aplican permisos en función de la dirección IP de origen, para saltarse restricciones y robar credenciales.

Utilizarse para ataques DDoS por lo que, podría tomar control de nuestros dispositivos para llevar a cabo un ataque de denegación de servicio.

¿Cómo se propaga/infecta/extiende?

La falsificación de la dirección IP del atacante se consigue mediante software especial desarrollado a propósito para esta función.





Centro de Informática

Ataques a las conexiones

IP Spoofing

¿Cómo me protejo?

Es recomendable llevar a cabo un filtrado de las direcciones IP para controlar las conexiones entrantes.

- Evitar acceder a correos desconocidos
- Tener cuidado al acceder a páginas web (revisar bien el nombre de la URL)
- Averiguar posibles soluciones técnicas aplicables a nuestros dispositivos

Ataques a las conexiones

Web Spoofing

¿Cómo funciona?

Consiste en la suplantación de una página web real por otra falsa. La web falsa es una copia del diseño de la original, llegando incluso a utilizar una URL (ruta) muy similar. El atacante trata de hacernos creer que la web falsa es la original.

Por ejemplo: hacienda.cr.com (falso),

https://www.hacienda.go.cr/ (verdadero)

Centro de Informática

Ataques a las conexiones

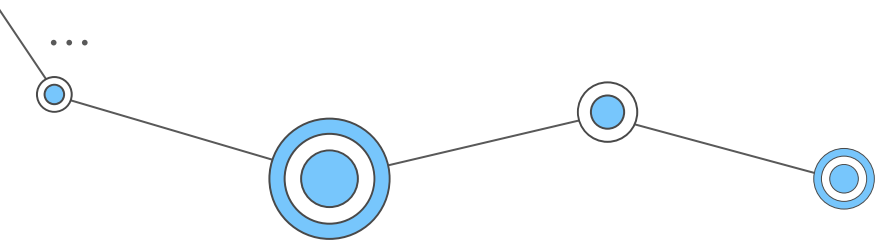
Web Spoofing

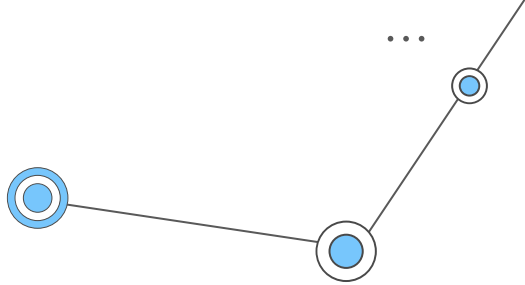
¿Cual es su objetivo?

Falsificar una web para robar las credenciales o los datos que intercambiemos con dicho servicio.

¿Cómo se propaga/infecta/extiende?

El atacante se sirve de otro tipo de ataques, como la ingeniería social o anuncios maliciosos, para que realicemos el acceso al enlace de la página web falsa.





CI Centro de Informática

Ataques a las conexiones

Web Spoofing

¿Cómo me protejo?

Al ser un ataque que llega en forma de enlace, se debe revisar con mucho cuidado la URL (ruta) para identificar diferencias con la original.

Desconfíe de las web **sin https ni certificados digitales** y en caso contrario, compruebe si se trata de la web que dice ser.

Ataques a las conexiones

Email Spoofing

¿Cómo funciona?

Consiste en suplantar la dirección de correo de una persona o entidad de confianza.

También suele ser usado para enviar de forma masiva correos de Spam o cadenas de bulos u otros fraudes.

Centro de Informática

Ataques a las conexiones

Email Spoofing

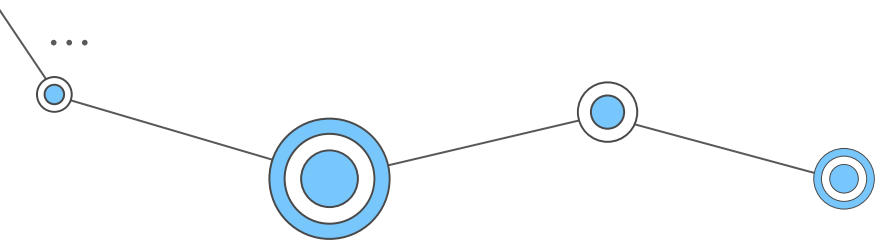
¿Cual es su objetivo?

Conseguir información personal sirviéndose de la confianza que transmite la identidad suplantada o también engañarnos para conseguir que descarguemos malware en el equipo.

¿Cómo se propaga/infecta/extiende?

El atacante ha podido obtener el **email** suplantado a partir de otro tipo de ataques, como la **ingeniería social**.

Además, es muy utilizado en otro tipo de ataques como el phishing o el spam, para aumentar sus probabilidades de éxito.



Ataques a las conexiones

Email Spoofing

¿Cómo me protejo?

Utilizar firma digital o cifrado a la hora de enviar email, nos permitirá autenticar los mensajes y prevenir suplantaciones.

Si la organización con la que nos comunicamos dispone de firma digital, también será más sencillo identificar este tipo de ataques.

Finalmente, analizando el contenido como si se tratara de un phishing bastará para identificar el engaño.

Ataques a las conexiones

DNS Spoofing

¿Cómo funciona?

A través de programas maliciosos específicos y aprovechándose de vulnerabilidades en las medidas de protección, los atacantes consiguen infectar y acceder a nuestro dispositivo.

Cuando tratamos de acceder a una determinada web desde el navegador, este nos llevará a otra web elegida por el atacante. Para ello, los atacantes tienen que suplantar la DNS (Domain Name System); es decir, la tecnología utilizada para conocer la dirección IP del servidor donde está alojado el dominio al que queremos acceder.

Aunque intentemos acceder a la URL (ruta) correcta, el navegador nos redireccionará a la web fraudulenta, ya que el atacante habría modificado la DNS.

Ataques a las conexiones

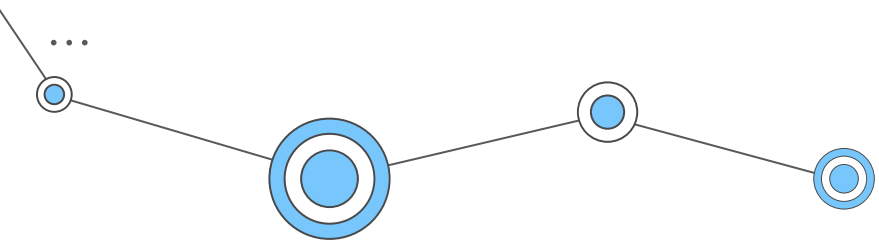
DNS Spoofing

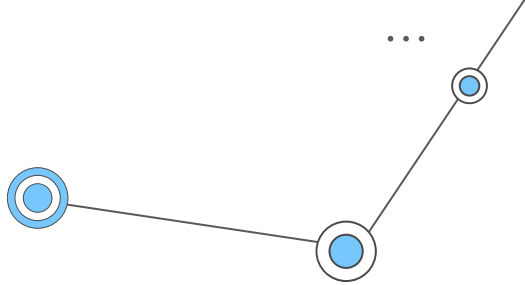
¿Cuál es su objetivo?

Modificar los DNS para re dirigirnos cada vez que intentemos acceder a una página web fraudulenta preparada por el atacante.

¿Cómo se propaga/infecta/extiende?

Sirviéndose de la escasez de medidas de seguridad en nuestro dispositivo, así como de malware especializado, el atacante consigue acceder a la configuración del enrutador para modificar los DNS.





Ataques a las conexiones

DNS Spoofing

¿Cómo me protejo?

La mejor forma de prevenir este ataque es blindar la seguridad del enrutador, restringiendo las conexiones remotas, cambiando las contraseñas por defecto, además de seguir las pautas para identificar web fraudulentas.

Ataques a las conexiones

Ataques a Cookies

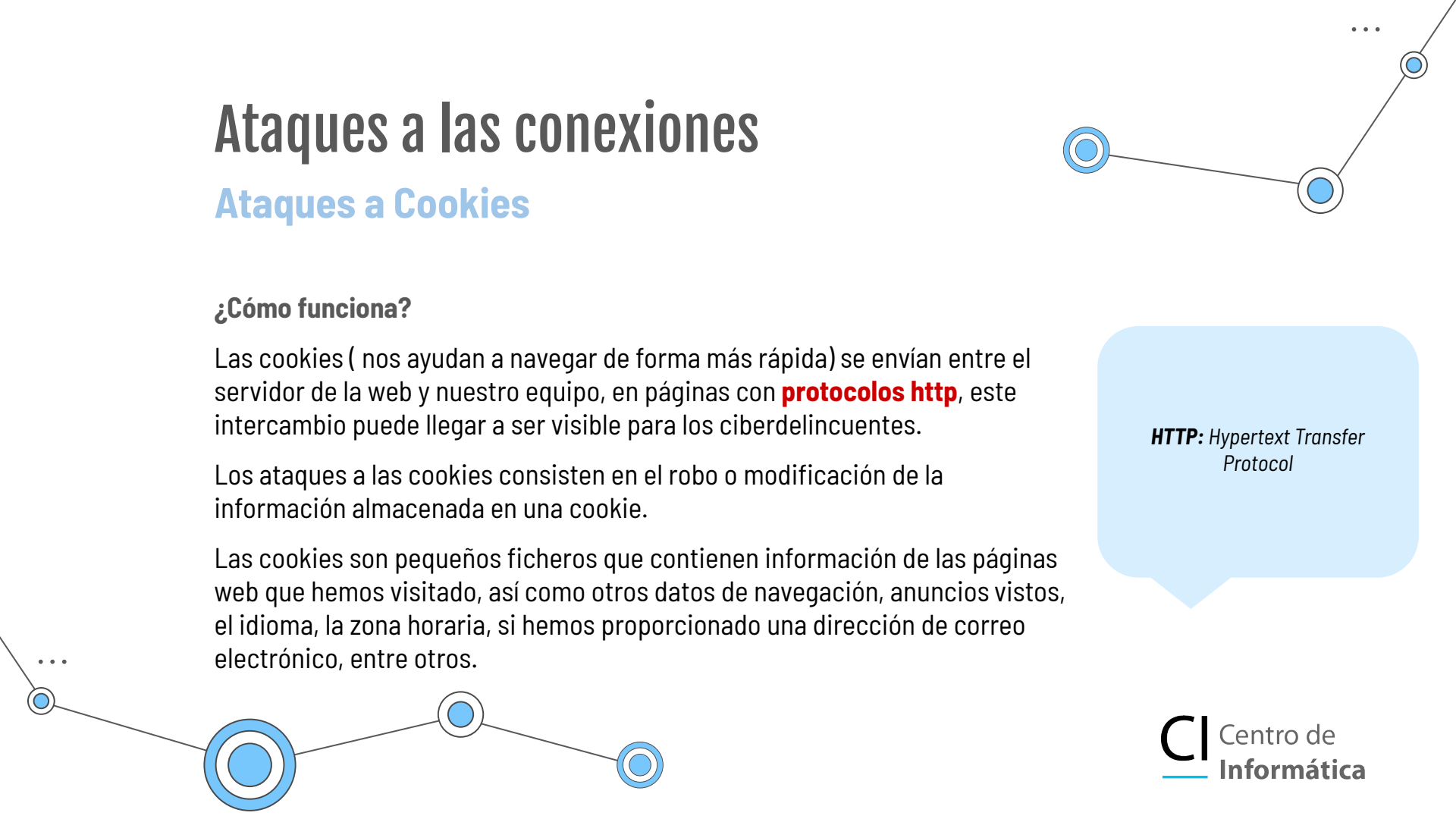
¿Cómo funciona?

Las cookies (nos ayudan a navegar de forma más rápida) se envían entre el servidor de la web y nuestro equipo, en páginas con **protocolos http**, este intercambio puede llegar a ser visible para los ciberdelincuentes.

Los ataques a las cookies consisten en el robo o modificación de la información almacenada en una cookie.

Las cookies son pequeños ficheros que contienen información de las páginas web que hemos visitado, así como otros datos de navegación, anuncios vistos, el idioma, la zona horaria, si hemos proporcionado una dirección de correo electrónico, entre otros.

HTTP: *Hypertext Transfer Protocol*



Centro de Informática

Ataques a las conexiones

Ataques a Cookies

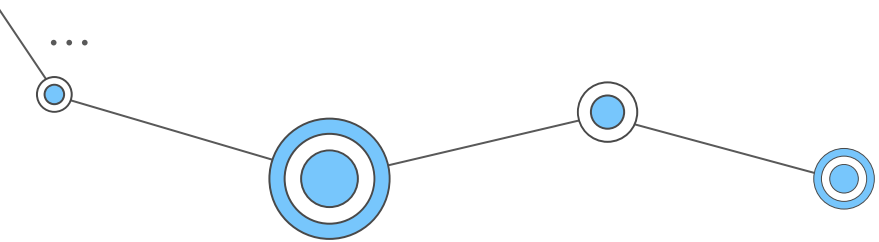
¿Cual es su objetivo?

Este tipo de ataques tienen como objetivo:

- El robo de identidad y credenciales.
- Obtener información personal sin nuestra autorización.
- Modificar datos.

¿Cómo se propaga/infecta/extiende?

Los atacantes se sirven de diferentes técnicas y malware, así como de la falta de protocolos de cifrado que protegen la información intercambiada entre nosotros y el servidor web (http).



Ataques a las conexiones

Ataques a Cookies

Existen dos tipos de ataques a las cookies:

- **Robo de cookies:** Aprovechando la falta de seguridad en el **protocolo http**, los atacantes son capaces de recibir una cookie perteneciente a un intercambio entre nosotros y el servidor. El atacante puede llegar a identificarse como la víctima en la web o acceder a datos sensibles.
- **Envenenamiento de cookies:** Sirviéndose de la misma vulnerabilidad, el atacante puede llegar a modificar el valor recogido en la cookie. Por ejemplo, para modificar el precio que hemos pagado por un artículo en una tienda online.

Ataques a las conexiones

Ataques a Cookies

¿Cómo me protejo?

Con una correcta configuración de las cookies desde nuestro navegador favorito, es recomendable seguir estas pautas:

- Mantener actualizado el navegador, complementos y plugins instalados. Descargarlos desde sitios oficiales.
- Eliminar cada cierto tiempo los datos de navegación, como las cookies, el historial y el caché.
- Revisar detenidamente las notificaciones o mensajes que aparecen al acceder a una web antes de aceptarlos.
- A la hora de intercambiar información sensible, datos confidenciales o muy personales, es mejor utilizar el modo incógnito.
- No guardar las contraseñas dentro del navegador y utilizar gestores de contraseñas en su lugar.

CI Centro de Informática

Ataques a las conexiones

Ataque DDoS

¿Cómo funciona?:

DDoS son las siglas en inglés de “Ataque Distribuido Denegación de Servicio” y consiste en atacar un servidor web al mismo tiempo desde muchos equipos diferentes, para que deje de funcionar al no poder soportar tantas peticiones.

Centro de Informática

Ataques a las conexiones

Ataque DDoS

¿Cual es su objetivo?

Provocar la caída de la web. Dependiendo del servicio y del tiempo que permanezca caído, las consecuencias pueden ser mayores.

Los afectados por un ataque DDOS son principalmente los servicios web. Las consecuencias son una pérdida de reputación, suspensión del servicio, pérdidas económicas, consecuencias de una brecha en su seguridad y robo de datos.

En el caso de los usuarios, no pueden acceder al servicio caído debido al ataque.

Si nuestros equipos han sido infectados, también podemos ser cómplices del ataque sin saberlo y formar parte de un grupo de PC infectados y controlados por un atacante de forma remota. (Botnet)

Ataques a las conexiones

Ataque DDoS

¿Cómo se propaga/infecta/extiende?

El ataque como tal no se propaga, sino que el ciberdelincuente o los ciberdelincuentes lanzan un ataque desde diversos dispositivos infectados.

La propagación se lleva a cabo a partir de otro tipo de ataques con los que infectan dispositivos e ir aumentando la potencia del ataque.

Ataques a las conexiones

Ataque DDoS

¿Cómo me protejo?

- **Actualizaciones:** Las actualizaciones de seguridad nos protegerán de posibles vulnerabilidades en el software.
- **Conexión sólida:** Un buen ancho de banda nos ayudará a reducir los efectos de un ataque DDOS y a reponernos antes.
- **Reducir la superficie afectada:** Una solución muy útil es limitar la infraestructura de nuestro servicio web que pueda ser atacada, por ejemplo, redirigiendo el tráfico directo de Internet.
- **Monitorización continua:** Existen herramientas para analizar la actividad del sitio web y detectar posibles ataques DDOS antes de que se conviertan en un problema. El firewall puede ayudarnos a detectar posibles intrusos o una actividad fuera de lo normal.
- **Proveedor fiable:** Elegir un proveedor que nos ofrezca garantías, como un servicio de prevención o una infraestructura sólida para aguantar un intento de ataque.

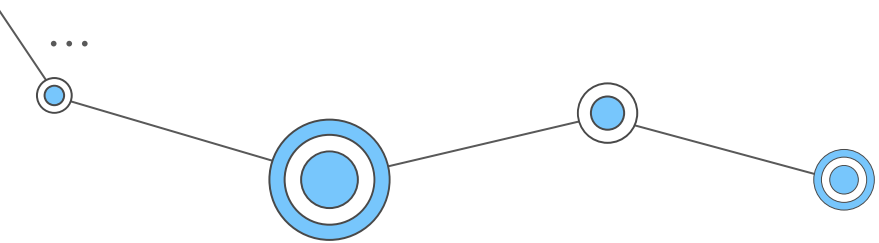
Ataques a las conexiones

Inyección SQL

¿Cómo funciona?

La inyección de SQL es una vulnerabilidad de seguridad web que permite a un atacante interferir con las consultas que una aplicación realiza a su base de datos.

***SQL** es un lenguaje de programación utilizado para interactuar con bases de datos.*



Centro de Informática

Ataques a las conexiones

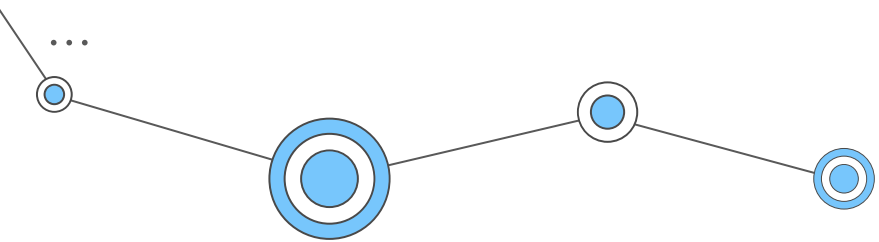
Inyección SQL

¿Cual es su objetivo?

Tener acceso a los datos sensibles recogidos en la base de datos del servicio o aplicación web para robarlos o destruirlos.

¿Cómo se propaga/infecta/extiende?

Los atacantes inyectan líneas de código SQL malicioso en la base de datos de las aplicaciones web. Para ello, se sirven de cualquier canal de entrada para enviar comandos maliciosos como elementos input, cadenas de consulta, cookies y archivos.



Ataques a las conexiones

Inyección SQL

¿Cómo me protejo?

Como usuarios, no podemos hacer mucho para prevenir este tipo de ataques, pues depende de la seguridad implementada por el servicio web.

En el caso de los desarrolladores web, es fundamental que sigan las recomendaciones basadas en el diseño seguro y desarrollo de código seguro, que priorice la privacidad de las comunicaciones y la protección de nuestros datos.

Ataques a las conexiones

Escaneo de puertos

¿Cómo funciona?

El ataque de escaneo de puertos (port scan), es el proceso en el que se analizan automáticamente los puertos de una máquina conectada a la red, con la finalidad de identificar cuáles están abiertos, cerrados o cuentan con algún protocolo de seguridad.

Centro de Informática

Ataques a las conexiones

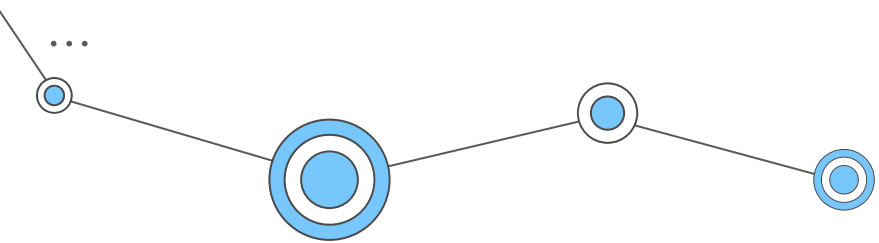
Escaneo de puertos

¿Cual es su objetivo?

En este tipo de ataques, el objetivo suele ser el robo de nuestra información como credenciales o datos bancarios, pero también ofrecen una entrada para controlar dispositivos conectados a una red.

¿Cómo se propaga/infecta/extiende?

Los ciberdelincuentes se sirven de varios programas con los cuales se pueden escanear los puertos de un enrutador.



Ataques a las conexiones

Escaneo de puertos

¿Cómo me protejo?

Como medida de protección, el enrutador tiene el papel protagonista a la hora de proteger los sistemas de la mayoría de los ataques a las conexiones.

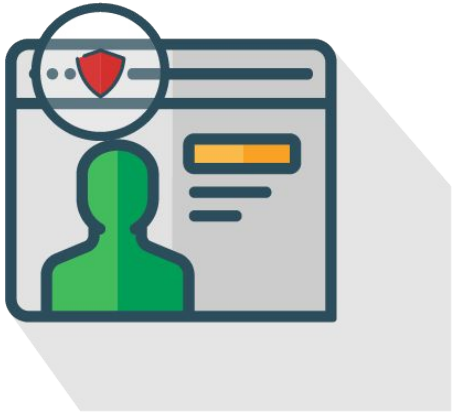
Es fundamental configurarlo correctamente, controlar las conexiones entrantes y los dispositivos conectados por medio de un filtrado MAC, mantener el firewall activado y controlar los puertos que tenemos abiertos. Y, como cualquier dispositivo, mantenerlo actualizado para protegerlo de posibles brechas de seguridad.

Ataques a las conexiones

Man in the middle

¿Cómo funciona?

Este tipo de ataque requiere que el atacante se sitúe entre nosotros y el servidor con el que nos estamos comunicando.



Centro de Informática

Ataques a las conexiones

Man in the middle

¿Cual es su objetivo?

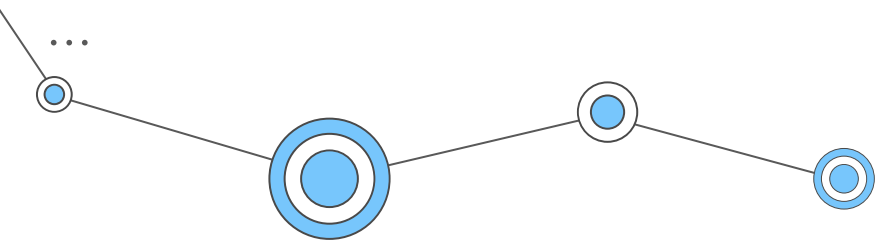
Interceptar, leer o manipular los datos intercambiados, como mensajes, credenciales, transferencias económicas, entre otros.

Generalmente, el atacante monitoriza nuestra actividad online y registra la información que más le interese.

¿Cómo se propaga/infecta/extiende?

Suelen ser habituales en redes públicas o en redes wifi falsas localizadas en sitios públicos como centros comerciales, aeropuertos u hoteles.

El atacante consigue monitorizar la actividad online dentro de la red infectada.



Ataques a las conexiones

Man in the middle

¿Cómo me protejo?

La primera norma es no conectarse a redes públicas. Además, es recomendable mantener nuestro dispositivo y software instalado actualizado a su última versión, utilizar aplicaciones de cifrado, disponer de contraseñas robustas y si es posible, añadir una capa extra de seguridad con la verificación en dos pasos.

Aplicar buenas prácticas de navegación segura, como acceder solo a **web con https y certificado digital** y conectarse a redes wifi por medio de una VPN si es necesaria la conexión a Internet.

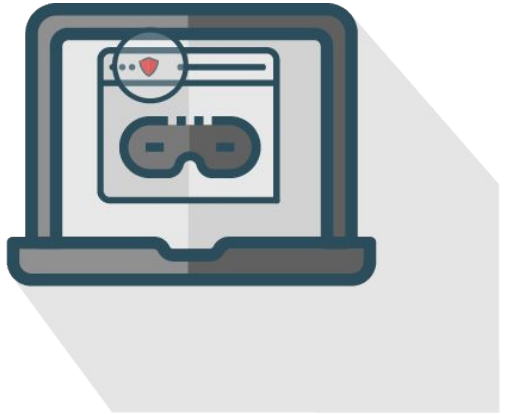
Ataques a las conexiones

Sniffing

¿Cómo funciona?

Se trata de una técnica utilizada para escuchar todo lo que ocurre dentro de una red.

Los atacantes utilizan herramientas de hacking, conocidas como sniffers, de forma malintencionada para monitorizar el tráfico de una red.



Centro de Informática

Ataques a las conexiones

Sniffing

¿Cual es su objetivo?

Mediante el uso de diferentes herramientas, los atacantes buscan capturar, interpretar y robar paquetes de datos lanzados por la red, para analizarlos y hacerse con nuestros datos.

¿Cómo se propaga/infecta/extiende?

Los sniffers no son virus y, por ello, no pueden reproducirse por sí mismos y deben ser controlados por terceras personas.

Pueden ser instalados como cualquier otro programa con o sin nuestro consentimiento.

Ataques a las conexiones

Sniffing

¿Cómo me protejo?

Existen herramientas de protección antimalware que pueden detectar y eliminar los sniffers instalados en un equipo. Sin embargo, dado que no son considerados como malware, no siempre son detectados y deben ser eliminados de forma manual.

Para evitarlo, se deben seguir todas las pautas para prevenir la descarga de software malicioso cuando navegamos por la red, como no descargar adjuntos sospechosos, no navegar por web fraudulentas y evitar conectar dispositivos USB desconocidos, entre otros.

Ataques a las conexiones

Aplicaciones Básicas

NMAP

THE HARVESTER

WIRESHARK

OWASP-ZAP

UNIVERSIDAD DE COSTA RICA

CI Centro de Informática

¡Muchas gracias!

Contactos:

Rebeca Esquivel, rebeca.esquivelflores@ucr.ac.cr

Mario Murillo, mario.murillo@ucr.ac.cr

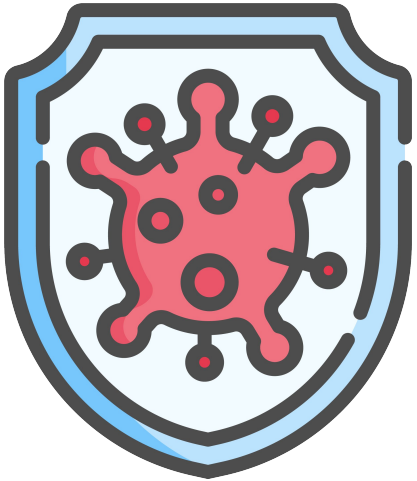
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Referencia: Guía de Ciberataques

INCIBE (Instituto Nacional de Ciberseguridad España 2020)

UNIVERSIDAD DE COSTA RICA

CI Centro de Informática



Unidad de Riesgo y Seguridad
Centro de Informática
Universidad de Costa Rica

Seguridad de la información