BIRSA | CONSULTORIA TECNOLOGICA

# ANALISIS DE VULNERABILIDADES

# CONTENIDO


1. Definición ataque informático
2. Importancia de la seguridad informática
3. Posibles ataques
4. Ataques registrados en 2018
5. ¿Cómo detectar un ataque?
6. Solución completa: Pruebas de penetración

# ATAQUE INFORMATICO

## DEFINICION

El estándar de seguridad ISO / IEC 27000 (públicado en mayo de 2009) describe un ataque a una red informática o de información como un "intento de destruir, exponer, alterar, inhabilitar, robar, obtener acceso no autorizado o hacer uso no autorizado de cualquier cosa que tenga valor para la organización".

(IBM, Noviembre 2020)

# IMPORTANCIA DE LA SEGURIDAD INFORMATICA

La seguridad informática es un punto clave para prevenir el robo de información tanto personal como de la empresa.

Para evitar esta serie de riesgos, o posibles riesgos, es importante entender que la seguridad informática no se reduce a actualizaciones de apps o programas, si no que más bien abarca diferentes medidas de seguridad.

# POSIBLES ATAQUES

## VIRUS

Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático.

## TROYANOS

Malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda al atacante un acceso remoto al equipo infectado.

## RANSOMWARE

Software malicioso que infecta un equipo y muestra mensajes exigiendo que se pague una tarifa para que el sistema vuelva a funcionar.

# ATAQUES

## REGISTRADOS EN 2018

### ESTADOS UNIDOS

Los datos de 11.9 millones de pacientes de un hospital (incluidas tarjetas de crédito y cuentas bancarias) estuvieron ocho meses expuestos por el error de seguridad.

### LONDRES

Una empresa suspendió sus servicios en 30 países tras descubrir agujeros en sus sistemas.

### ESPAÑA

Un ataque de ransomware obligó a una cadena empresarial a llevar a cabo la suspensión de la programación local.

### MADRID

Un hospital de la región permaneció varios días con los equipos de cómputo y las pantallas de salas de espera inutilizables debido a un ransomware en su red.

LOS DATOS DE APROXIMADAMENTE

# 50 MILLONES DE USUARIOS

## ESTUVIERON EXPUESTOS DEBIDO A UNA VULNERABILIDAD EN LA PLATAFORMA GOOGLE+

El 8 de octubre de 2018 Google anunció el cierre temporal de Google+ para agosto de 2019. Sin embargo, el 10 de diciembre de 2018 Google decidió adelantar el cierre de la plataforma a abril de 2019 tras el descubrimiento de un nuevo bug que afectó a más de 50 millones de usuarios y que puso en riesgo la información de perfil de sus cuentas durante varios días.

# ¿Como detectar un ataque?

PARA DETECTAR UN ATAQUE ES NECESARIO REALIZAR UNA SERIE DE ANÁLISIS EN LA RED INFORMÁTICA MEDIANTE DISTINTAS HERRAMIENTAS DE APOYO PARA COMPLEMENTAR EL PROCESO.

# EN BIRSA CONSULTORIA TECNOLOGICA

## NOS PONEMOS A SU DISPOSICION,

BRINDANDO UNA SOLUCIÓN COMPLETA PARA LLEVAR A CABO UN ANÁLISIS DE VULNERABILIDADES EN LA RED, CON LA FINALIDAD DE IDENTIFICAR SOFTWARE MALISIOSO Y/O INTRUSOS.

# SOLUCION COMPLETA

## PRUEBAS DE PENETRACIÓN

Realizar un escaneo de la red para detectar el flujo de datos que se transmiten en la misma y, con ello, identificar las vulnerabilidades que se presentan dentro de la red. Posteriormente, se realizan pruebas de penetración para “brincar” la seguridad y determinar qué tan segura es la red.

**Actividades a realizar**

1. Escaneo de red
2. Detección de vulnerabilidades
3. Pruebas de penetración

# Contacto

614 255 49 50

Calle Ramírez Calderón #1407 Col. San Felipe,
Chihuahua, Chih.

www.birsamexico.com

info@birsamexico.com

ESCANÉAME