

Tecnológico Nacional de México

Instituto Tecnológico de Reynosa



Equipo conformado por:

Bermudez Dominguez Juan Carlos 19580585  
Castillo Jr Gregorio 19580589

Flores Acosta Sheila Lizeth 19580595

Morales Calixto Daniel Alexander 19580867

Gongora Raga Perla Elizabeth 19580603

Perez Romero Julio Alberto 19580633

Administración de servidores

# Índice

[Índice 1](#_Toc132904340)

[3.1 Conceptos básicos 2](#_Toc132904341)

[3.2 Tipos de ataques 3](#_Toc132904342)

[3.3 Creación del plan, procedimientos y políticas de seguridad 4](#_Toc132904343)

[3.4 Evaluación de riesgos 5](#_Toc132904344)

[3.4.1 Activos a proteger 6](#_Toc132904345)

[3.4.2 Amenazas contra las que se tiene que proteger 7](#_Toc132904346)

[3.4.3 Protección legal 8](#_Toc132904347)

[Bibliografía 9](#_Toc132904348)

# 3.1 Conceptos básicos

# 3.2 Tipos de ataques

Tipos de ataques:

* Ataque de denegación de servicio (DoS)
* Ataque de denegación de servicio distribuido (DDoS)
* Ataque de fuerza bruta
* Ataque de inyección SQL
* Ataque de exploit
* Ataque de phishing
* Ataque de malware
* Ataque de ransomware
* Ataque de hombre en el medio

*Ataque de denegacion de servicio (DoS)*

Un ataque de denegación de servicio (DoS) es un tipo de ataque informático que tiene como objetivo abrumar un servidor o red con tráfico malicioso o solicitudes falsas, lo que provoca una caída del servicio para los usuarios legítimos. El objetivo de este ataque es dejar inoperable un sitio web o servicio en línea, impidiendo que los usuarios legítimos puedan acceder a él.

Los atacantes pueden realizar un ataque DoS de diferentes maneras. Algunos ejemplos incluyen:

Ataque de inundación de tráfico: Este tipo de ataque implica enviar una gran cantidad de tráfico a un servidor, sobrecargando el ancho de banda y haciendo que el servidor deje de responder.

Ataque de amplificación de tráfico: Este tipo de ataque implica aprovechar la vulnerabilidad de un protocolo de red para enviar paquetes de datos falsificados a un servidor, que responde a ellos enviando paquetes a una dirección IP de destino elegida por el atacante.

Ataque de solicitud falsificada: Este tipo de ataque implica enviar solicitudes falsas al servidor, haciéndole creer que está siendo utilizado por usuarios legítimos y agotando los recursos del servidor.

Los ataques DoS pueden ser realizados por un solo atacante o por un grupo de atacantes que coordinan sus esfuerzos. Los motivos detrás de los ataques DoS pueden variar, desde la extorsión hasta la venganza o simplemente por diversión.

Los ataques DoS pueden ser devastadores para las empresas y organizaciones que dependen de sus sitios web y servicios en línea para funcionar correctamente. Para protegerse contra los ataques DoS, es importante tener en cuenta las mejores prácticas de seguridad, como la implementación de firewalls y la gestión del tráfico de red para detectar y bloquear el tráfico malicioso.

*Ataque de denegación de servicio distribuido (DDoS)*

Un ataque de denegación de servicio distribuido (DDoS) es una variante del ataque de denegación de servicio (DoS), en la que un atacante utiliza múltiples dispositivos conectados a Internet para inundar el servidor objetivo con tráfico malicioso o solicitudes falsas.

En un ataque DDoS, los dispositivos utilizados para enviar el tráfico malicioso o las solicitudes falsas son a menudo dispositivos comprometidos o infectados con malware, como computadoras personales, servidores web, enrutadores y otros dispositivos de Internet de las cosas (IoT).

Los atacantes pueden controlar estos dispositivos de forma remota a través de una red botnet, que es una red de dispositivos infectados y controlados por el atacante. Estos dispositivos pueden ser utilizados para enviar tráfico malicioso al servidor objetivo, sobrecargando sus recursos y provocando una caída del servicio.

Una vez que el ataque comienza, puede ser muy difícil detenerlo, ya que el tráfico malicioso proviene de múltiples fuentes, lo que dificulta la identificación del atacante y la mitigación del ataque.

Los ataques DDoS pueden ser motivados por una variedad de razones, desde la extorsión hasta la venganza o simplemente por diversión. Los ataques DDoS pueden ser especialmente devastadores para las empresas y organizaciones que dependen de sus sitios web y servicios en línea para funcionar correctamente.

Para protegerse contra los ataques DDoS, es importante tener en cuenta las mejores prácticas de seguridad, como la implementación de firewalls, sistemas de detección de intrusiones y gestión del tráfico de red para detectar y bloquear el tráfico malicioso. También es importante mantener los dispositivos conectados a Internet actualizados y protegidos contra malware para evitar que sean utilizados como parte de una botnet.

*Ataque de fuerza bruta*

Un ataque de fuerza bruta es un tipo de ataque informático que implica intentar adivinar una contraseña o clave de cifrado mediante la fuerza bruta, es decir, probando todas las combinaciones posibles hasta que se encuentra la correcta.

En un ataque de fuerza bruta, un atacante intenta acceder a un sistema o servicio protegido por una contraseña o clave de cifrado mediante la prueba de diferentes combinaciones de caracteres, desde palabras comunes hasta números y símbolos.

Los ataques de fuerza bruta pueden ser automatizados con herramientas especiales que prueban todas las combinaciones posibles a alta velocidad. Si la contraseña es lo suficientemente débil o corta, el atacante puede tener éxito en adivinarla en un tiempo relativamente corto.

Los ataques de fuerza bruta pueden ser especialmente efectivos contra contraseñas débiles, como "1234" o "contraseña", que son fáciles de adivinar. También pueden ser efectivos contra contraseñas más fuertes si se utilizan técnicas de diccionario que prueban combinaciones de palabras comunes o variaciones de ellas.

Para protegerse contra los ataques de fuerza bruta, es importante utilizar contraseñas fuertes y complejas que contengan una combinación de letras mayúsculas y minúsculas, números y símbolos. También es importante evitar el uso de contraseñas comunes o fáciles de adivinar, como nombres propios, fechas de nacimiento o palabras simples. Además, se pueden utilizar herramientas de seguridad como bloqueos de cuentas después de un número determinado de intentos fallidos de inicio de sesión, la implementación de medidas de autenticación de dos factores y el cifrado de datos sensibles.

*Ataque de inyección SQL*

Un ataque de inyección SQL es un tipo de ataque informático en el que un atacante utiliza una vulnerabilidad en una aplicación web para manipular una base de datos a través de la entrada de datos del usuario.

En un ataque de inyección SQL, el atacante inserta código malicioso en los campos de entrada de una aplicación web, como un formulario de inicio de sesión o un campo de búsqueda. Este código malicioso se utiliza para engañar al servidor de la aplicación para que ejecute comandos SQL no autorizados.

Si el ataque es exitoso, el atacante puede obtener acceso no autorizado a la base de datos, modificar o eliminar datos, o incluso tomar el control del servidor.

Los ataques de inyección SQL pueden ser especialmente peligrosos porque pueden explotar vulnerabilidades en aplicaciones web legítimas y ampliamente utilizadas, como WordPress, Drupal y Joomla.

Para protegerse contra los ataques de inyección SQL, es importante utilizar las mejores prácticas de seguridad de aplicaciones web, como validar y filtrar los datos de entrada del usuario, utilizar consultas parametrizadas y evitar el uso de comandos SQL dinámicos. También es importante mantener las aplicaciones web actualizadas y parcheadas para evitar vulnerabilidades conocidas.

Ataque de exploit

Un ataque de exploit es un tipo de ataque informático en el que un atacante aprovecha una vulnerabilidad en un sistema operativo, una aplicación o un software para tomar el control del sistema o para ejecutar código malicioso.

Los exploits pueden aprovechar vulnerabilidades conocidas o recién descubiertas en el sistema o en la aplicación para ejecutar código arbitrario. Los atacantes pueden utilizar exploits para instalar software malicioso en el sistema de la víctima, robar datos confidenciales, obtener acceso no autorizado a un sistema, o incluso para causar daños físicos en un sistema conectado a Internet de las cosas (IoT).

Los exploits pueden ser específicos de un sistema operativo, una aplicación o un software, o pueden ser ataques de día cero que aprovechan vulnerabilidades desconocidas y sin parchear.

Para protegerse contra los ataques de exploit, es importante mantener todos los sistemas, aplicaciones y software actualizados y parcheados para evitar vulnerabilidades conocidas. También es importante implementar medidas de seguridad como firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para detectar y bloquear posibles ataques de exploit.

Ataque de phishing

Un ataque de phishing es un tipo de ataque informático en el que un atacante intenta engañar a una víctima para que revele información confidencial, como contraseñas, números de tarjetas de crédito, información bancaria o datos personales, a través de técnicas de ingeniería social.

Los ataques de phishing generalmente se realizan por correo electrónico, pero también pueden ser por mensajes de texto, redes sociales, mensajería instantánea o incluso por teléfono. Los atacantes a menudo utilizan tácticas de urgencia o miedo para convencer a la víctima de que revele información confidencial, como afirmar que su cuenta ha sido hackeada o que hay un problema con una transacción.

Los correos electrónicos de phishing suelen ser diseñados para parecer legítimos y engañar a la víctima para que haga clic en un enlace o descargue un archivo adjunto que contiene malware. Una vez que la víctima hace clic en el enlace o descarga el archivo, se puede instalar software malicioso en su dispositivo o se puede dirigir a la víctima a una página web falsa diseñada para parecerse a una página web legítima, como un sitio bancario o de compras en línea, para que revele información confidencial.

Para protegerse contra los ataques de phishing, es importante estar atento a los correos electrónicos o mensajes sospechosos, verificar la autenticidad de la fuente del correo electrónico o mensaje, no hacer clic en enlaces sospechosos, no descargar archivos adjuntos de remitentes desconocidos, y no revele información confidencial en respuesta a correos electrónicos, mensajes o llamadas no solicitadas. También es importante utilizar software de seguridad actualizado y tener medidas de seguridad como autenticación de dos factores y contraseñas fuertes.

*Ataque de malware*

Un ataque de malware es un tipo de ataque informático en el que un atacante utiliza software malicioso, o malware, para tomar el control de un sistema, robar datos confidenciales, o causar daño a un sistema o red.

El malware puede tomar muchas formas, incluyendo virus, gusanos, troyanos, ransomware, adware, spyware y bots. Una vez que el malware infecta un sistema, puede propagarse a otros sistemas en la red o incluso a sistemas externos conectados a la red.

Los atacantes pueden utilizar el malware para espiar a las víctimas, robar información confidencial como contraseñas, números de tarjetas de crédito y otra información personal, tomar el control de sistemas, cifrar archivos y exigir rescate, o incluso para causar daño físico en sistemas conectados a IoT.

Los ataques de malware pueden ocurrir a través de descargas maliciosas, correos electrónicos de phishing, sitios web comprometidos, dispositivos USB infectados y otras técnicas de ingeniería social.

Para protegerse contra los ataques de malware, es importante utilizar software de seguridad actualizado, mantener sistemas y software actualizados y parcheados para evitar vulnerabilidades conocidas, evitar descargas y correos electrónicos sospechosos, no hacer clic en enlaces o archivos adjuntos sospechosos, y tener medidas de seguridad como firewalls, sistemas de detección de intrusiones y sistemas de prevención de intrusiones para detectar y bloquear posibles ataques de malware.

Ataque de ransomware

Un ataque de ransomware es un tipo de ataque informático en el que un atacante utiliza software malicioso para cifrar archivos o sistemas informáticos y luego extorsionar a la víctima para que pague un rescate a cambio de la clave de descifrado.

Los ataques de ransomware pueden ser muy dañinos y pueden afectar a individuos, empresas y organizaciones de todo tipo. Una vez que el malware cifra los archivos o sistemas, la víctima puede perder acceso a datos importantes o incluso a sistemas enteros, lo que puede provocar interrupciones graves en la operación de negocios y organizaciones.

Los ataques de ransomware generalmente se propagan a través de correos electrónicos de phishing o sitios web comprometidos. Los atacantes utilizan técnicas de ingeniería social para hacer que las víctimas hagan clic en enlaces o descarguen archivos que contienen el malware de ransomware.

Una vez que el ransomware infecta el sistema de la víctima, se cifran los archivos importantes, y el atacante muestra un mensaje de rescate en la pantalla, exigiendo un pago en criptomonedas a cambio de la clave de descifrado. Si la víctima no paga el rescate, los atacantes pueden borrar permanentemente los archivos cifrados.

Para protegerse contra los ataques de ransomware, es importante mantener los sistemas y el software actualizados, tener copias de seguridad de los datos importantes, evitar descargas y correos electrónicos sospechosos, tener medidas de seguridad como firewalls y sistemas de detección de intrusiones, y educar a los usuarios sobre las prácticas seguras de navegación en línea.

*Ataque de hombre en el medio*

Un ataque de hombre en el medio (MITM, por sus siglas en inglés) es un tipo de ataque informático en el que un atacante intercepta y manipula la comunicación entre dos partes que están intentando comunicarse. El atacante se sitúa en el medio de la comunicación y hace que ambas partes crean que están hablando directamente entre sí, cuando en realidad están hablando con el atacante.

El objetivo del ataque de MITM es permitir que el atacante obtenga información confidencial, como contraseñas, información de inicio de sesión, detalles de transacciones financieras o cualquier otro tipo de información que se intercambie entre las dos partes.

Los ataques de MITM pueden ocurrir en cualquier tipo de comunicación, incluyendo comunicaciones de red, correos electrónicos, mensajes instantáneos y llamadas telefónicas. Para llevar a cabo el ataque, el atacante puede utilizar una variedad de técnicas, como el secuestro de sesión, la falsificación de direcciones MAC y la suplantación de identidad.

Para protegerse contra los ataques de MITM, es importante utilizar conexiones seguras como HTTPS o SSL/TLS, utilizar una red privada virtual (VPN) para proteger las comunicaciones en línea, verificar la autenticidad de los sitios web y de los correos electrónicos, utilizar contraseñas fuertes y no compartirlas, y tener precaución al conectarse a redes públicas y abiertas. También es importante mantener el software actualizado y utilizar software de seguridad confiable.

# 3.3 Creación del plan, procedimientos y políticas de seguridad

# 3.4 Evaluación de riesgos

## 3.4.1 Activos a proteger

## 3.4.2 Amenazas contra las que se tiene que proteger

## 3.4.3 Protección legal

# Bibliografía