Universidad Autónoma De Chiapas

Facultad de Contaduría y Administración

Campus 1

Ing. En Desarrollo Y Tecnologias De Software

7 "M"

OPT.2 - Análisis de Vulnerabilidades

Sub1 - Introducción al Pentesting

Act. 1.4 Elaborar Infografía referente a tipos de ataque sobre sistemas web y móvil

Alumno:

Marco Antonio Zúñiga Morales - A211121

Docente:

Dr. Luis Gutiérrez Alfaro

Tuxtla Gutiérrez, Chiapas

Martes, 13 de febrero de 2024

INFOGRAFÍA

TIPOS DE ATAQUE SOBRE UN SISTEMA WEB Y MÓVIL

Los ataques informáticos son diversos y avanzan continuamente, apuntando a hardware, software, datos y redes, conforme los atacantes innovan y los sistemas se complejizan.

SISTEMAS WEB

Inyección SQL

Manipulación de bases de datos a través de entradas maliciosas.

XSS (Cross-Site Scripting)

Inyección de scripts maliciosos en páginas web.

CSRF (Cross-Site Request Forgery)

Ejecución de acciones no autorizadas por usuarios autenticados.

SSRF (Server-Side Request Forgery)

Envío de peticiones maliciosas desde el servidor.

Secuestro de sesión

Control no autorizado de sesiones de usuario.

Desbordamiento de buffer

Ejecución de código arbitrario por sobrecarga de datos.

SISTEMAS MÓVILES

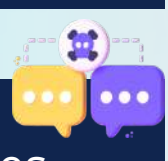
Malware

Aplicaciones maliciosas que roban información o dañan el dispositivo.

Intercepción de SMS/Llamadas

Captura de mensajes o llamadas para obtener información sensible.

MitM (Man-in-the-Middle)



Interceptación de la comunicación entre móviles y servidores.

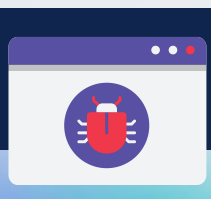
Ataques de canal lateral

Explotación de información del sistema como el uso de batería.

Aplicaciones falsas

Apps maliciosas que imitan a las legítimas.

Vulnerabilidades del SO



Explotación de fallos en el sistema operativo móvil.

TIPOS DE ATAQUES

Ataques de Software

Malware
Virus, gusanos, troyanos y ransomware.

XSS
Inserción de scripts maliciosos en sitios web.

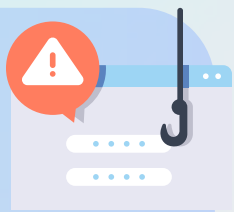
Inyección SQL
Manipulación de bases de datos mediante entradas maliciosas.

Ataques de Red

- **DoS/DDoS:** Sobrecarga de sistemas para denegar servicio.
- **MitM:** Intercepción de comunicaciones.
- **Sniffing:** Captura de datos en tránsito.
- **Spoofing:** Falsificación de identidad para acceso no autorizado.

Ataques de Ingeniería Social

- **Phishing:** Engaño para obtener datos personales.
- Spear Phishing: Phishing dirigido y personalizado.
- **Baiting:** Atracción con promesas falsas.
- **Pretexting:** Creación de escenarios falsos para obtener información.



Ataques a los Datos

Interceptación
Captura de datos en tránsito o almacenados.

Manipulación
Alteración o destrucción de datos para beneficio ilícito.

Ataques Criptográficos

- **Criptoanálisis:** Descifrado sin la clave.
- **Fuerza bruta:** Prueba exhaustiva de combinaciones.

Ataques Físicos

- **Acceso no autorizado:** Robo o daño físico.
- **Tampering:** Modificación física de dispositivos.

ESTRATEGIAS DE MITIGACIÓN

- **Actualización de software:** Mantener sistemas y aplicaciones actualizados.
- **Políticas de seguridad sólidas:** Implementar y seguir políticas de seguridad estrictas.
- **Educación en seguridad:** Formación continua en buenas prácticas de seguridad.
- **Validación de datos:** Prevención de inyecciones SQL y XSS.
- **Políticas de seguridad de contenido:** Protección contra XSS.
- **Uso de HTTPS:** Cifrado de la comunicación para seguridad.
- **Actualizaciones y parches:** Mantenimiento de software y SO al día.
- **Principios de seguridad en desarrollo:** Aplicaciones móviles desarrolladas con seguridad desde el inicio.

CONCLUSIÓN

La seguridad informática es esencial en un mundo digitalmente conectado, requiriendo la implementación de estrategias proactivas de mitigación, actualizaciones regulares y educación continua para proteger contra una amplia gama de ataques informáticos.

REFERENCIA BIBLIOGRÁFICA

Brathwaite, S., & Team, W. (2024, 7 enero). Los 5 ataques a sitios web más comunes y cómo defenderse de ellos. Website Rating. https://www.websiterating.com/es/online-security/most-common-website-attacks-how-to-defend-against-them/

Chkadmin. (2022, 11 mayo). Top 6 Mobile Security Threats and How to Prevent Them. Check Point Software. https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-mobile-security/top-6-mobile-security-threats-and-how-to-prevent-them/#:~:text=Principales%20amenazas%20de%20seguridad%20m%C3%B3vil%20Los%20dispositivos%20m%C3%B3viles,vulnerabilidades%20dentro%20del%20dispositivo%20y%20del%20SO%20m%C3%B3vil.

Esteban, S. (2024, 12 febrero). Inyección SQL: Definición y ejemplos reales. Backtrack Academy. https://backtrackacademy.com/articulo/inyeccion-sql-definicion-y-ejemplos

Las 7 principales amenazas de seguridad móvil: smartphones, tablets y dispositivos con Internet móviles – Lo que depara el futuro. (2023, 13 julio). www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

López, A. (2023, 23 octubre). Estos son todos los ataques a las redes que existen y cómo evitarlos. RedesZone. https://www.redeszone.net/tutoriales/seguridad/listado-completo-ataques-redes-como-evitarlos/

¿Qué es la inyección de SQL? Definición y explicación. (2023, 19 abril). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/sql-injection

¿Qué es un ataque cibernético? | IBM. (s. f.). https://www.ibm.com/mx-es/topics/cyber-attack

Tipos de ataques - Seguridad Web | MDN. (2023, 14 julio). MDN Web Docs. https://developer.mozilla.org/es/docs/Web/Security/Types_of_attacks