Tarea 4 Seguridad Informática Básica – Gpo. 2 Fecha de entrega: 19 /10/ 23

Equipo 4 || Integrantes:

Castelan Ramos Carlos 317042711
Martínez González Héctor Eduardo 316322122
Martínez Sánchez Berenice Vianney 317581223
Pineda González Rodrigo 317224397
Vega Alvarez Marcos 420054432

9.5

Liste 30 ataques informáticos existentes e indique de qué trata cada uno.
Por ejemplo. Spam: es cualquier forma de comunicación no solicitada que se envía de forma masiva.

1. **Phishing:** Intento de obtener información confidencial (contraseñas, datos bancarios) haciéndose pasar por una entidad de confianza.

2. **Malware:** Software malicioso que puede dañar o acceder ilegalmente a sistemas informáticos.

3. **Virus:** Programa informático que se replica y propaga, causando daño en los sistemas infectados.

4. **Keylogger:** Herramienta que registra las pulsaciones de teclado, utilizada para robar contraseñas y datos sensibles.

5. **Ransomware:** Malware que cifra los archivos de la víctima y exige un rescate para desbloquearlos.

6. **Spyware:** Software que recopila información del usuario sin su consentimiento y la envía a terceros.

7. **Adware:** Su principal función es la de mostrar anuncios de forma masiva. El objetivo es recaudar información y transmitirla para estudiar el comportamiento del usuario y dirigir mejor el tipo de publicidad.

8. **Doxing:** Este concepto se refiere a la práctica de realizar investigaciones en línea y divulgar información personal de un individuo o entidad con la intención de amenazar, intimidar o humillar.

9. **Ataque LOKI:** El ataque LOKI se emplea con el propósito de enviar datos de manera encubierta, aprovechando el flujo de tráfico normal en una red, sin que el usuario pueda detectarlo.

10. **Man in the Middle:** El ataque implica la intercepción clandestina de la comunicación entre dos sistemas para robar datos o información valiosa de forma ilícita.

11. **Ataque DoS:** Un ataque de denegación de servicio (DoS) ocurre cuando un intruso impide que un usuario se autentique o acceda normalmente a un sistema o sitio web, lo que puede representar una amenaza común en entornos empresariales.

12. **Whaling:** Dirigido a altos ejecutivos, como CEOs y CFOs, con el propósito de robar información confidencial a la que solo ellos tienen acceso. Se asemeja al phishing en su enfoque persuasivo, pero el atacante se hace pasar por un alto cargo, ya sea dentro de la misma empresa o de otra.

13. **Inyección SQL:** Es un peligroso tipo de ataque informático que implica la inserción de código malicioso a través de vulnerabilidades en páginas web. Esto permite a los hackers acceder a la información de las empresas en línea y robar datos o manipular la información alojada en sus sitios web.

14. **Password attack:** Buscan obtener las credenciales de un usuario legítimo para acceder al sistema. Utilizan métodos como el ataque de fuerza bruta, ataques de diccionario y "shoulder surfing" (observar a alguien mientras ingresa sus credenciales).

15. **Trust exploitation:** Se basan en el uso de un host en el que el sistema confía para lanzar un ataque. Es una suplantación, en el que el atacante envía información falsa con la dirección IP o MAC de un host confiable, engañando al sistema de confianza.

16. **Packet sniffing:** Implica el uso de herramientas de captura de paquetes para analizar el tráfico de red. La tarjeta de red del atacante se configura en modo promiscuo, lo que le permite interceptar y examinar los paquetes de datos que circulan en la red para obtener información valiosa sobre el sistema.

17. **Dumpster diving:** El atacante revisa la basura de las organizaciones en busca de documentos que contienen información que podría ayudarle a comprender el sistema y descubrir posibles puntos de vulnerabilidad.

18. **Ping of death:** Se envía un ping defectuoso que no cumple con las normas del protocolo IP, lo que provoca un desbordamiento de memoria en el host de destino, causando un fallo del sistema y deshabilitando los servicios alojados en él. Es un ataque que explota vulnerabilidades en el manejo de paquetes de red.

19. **Spoofing de DNS (DNS Spoofing)**: Este implica la manipulación de los servidores DNS para redirigir el tráfico de Internet a sitios web falsos. Los atacantes pueden utilizar esto para engañar a los usuarios y robar sus datos confidenciales.

20. **Ataque de Fuerza Bruta en Cifrado (Brute-Force Encryption):** En este ataque, los atacantes intentan descifrar contraseñas o claves de cifrado probando todas las combinaciones posibles. Es un método intensivo en recursos y a menudo se utiliza en el robo de contraseñas.

21. **Suplantación de Identidad por Correo Electrónico (Email Spoofing):** Los atacantes envían correos electrónicos falsificados que parecen provenir de una fuente legítima. Esto se utiliza comúnmente para engañar a las personas y obtener acceso no autorizado a cuentas o información confidencial.

22. **Ataque de Fuzzing:** Es una técnica en la que los atacantes envían datos aleatorios o manipulados a una aplicación o sistema para encontrar vulnerabilidades o errores de software que puedan ser explotados.

23. **Ataque de Suplantación de Protocolo (Protocol Spoofing):** En este tipo de ataque, los atacantes envían paquetes de datos que simulan el comportamiento de un protocolo de red legítimo para comprometer la integridad de la comunicación.

24. **Ataque de Envenenamiento de ARP (ARP Poisoning):** Los atacantes falsifican las tablas de resolución de direcciones ARP en una red local para redirigir el tráfico a través de ellos mismos. Esto les permite interceptar y modificar los datos en tránsito.

25. **Ataque de Secuestro de Sesión (Session Hijacking):** Este ataque implica la interceptación de sesiones de usuario activas en aplicaciones web o servicios en línea para obtener acceso no autorizado a cuentas y datos.

26. **Ataque de Enrutador Comprometido (Compromised Router Attack):** Los atacantes toman el control de enrutadores de red para interceptar y manipular el tráfico que fluye a través de ellos, lo que les permite llevar a cabo actividades maliciosas, como el espionaje.

27. **Ataque de Relleno de Token (Token Padding Attack):** En este ataque, los atacantes manipulan tokens de autenticación o cifrado al agregar datos maliciosos para evitar la detección y alterar el comportamiento de aplicaciones.

28. **Ataque de Secuestro de Subdominio (Subdomain Takeover):** Este ataque aprovecha subdominios no utilizados o mal configurados de un sitio web para redirigir el tráfico o alojar contenido malicioso en esos subdominios.

29. **Ataque de Elevación de Privilegios (Privilege Escalation):** Los atacantes buscan debilidades en sistemas o aplicaciones para aumentar sus privilegios y obtener un mayor control sobre el sistema, lo que les permite realizar acciones que normalmente no estarían autorizados.

30. **Ataque de Enmascaramiento de URL (URL Masking):** En este ataque, los atacantes ocultan la verdadera URL de un sitio web malicioso detrás de una URL aparentemente legítima para engañar a las víctimas y redirigirlas a sitios maliciosos.

Referencias.

Colocar en orden alfabético

- Seguridad, U. (2019, 7 julio). *20 ejemplos de ataques informáticos que puede sufrir una empresa*. Blog de Seguridad para Empresas. https://uss.com.ar/corporativo/ejemplos-de-ataques-informaticos-empresa/
- Plata, J. M. (2022). Tipos de ataques informáticos. *CNIPJ*. https://cnipj.es/tipos-ataques-informaticos/
- School, T. (2023). Tipos de ataques informáticos: ¿cuáles son y cómo operan? *Tokyo School*. https://www.tokioschool.com/noticias/tipos-ataques-informaticos/
- Universidad Autónoma de Ciudad Juárez. (2023). *Seguridad informática.* https://www.uacj.mx/CGTI/CDTE/JPM/Documents/IIT/infseguridad/U2-5.html
- Equipo editorial de IONOS. (2020). DNS spoofing: así funciona y así puedes protegerte. *IONOS Digital Guide*. https://www.ionos.mx/digitalguide/servidores/seguridad/dns-spoofing/
- Jiménez, J. (2023, 15 octubre). Suplantación de ARP: qué es y cómo afecta a nuestra red. *RedesZone*. https://www.redeszone.net/tutoriales/redes-cable/ataques-arp-spoofing-evitar/
- KeepCoding, R. (2023, 25 septiembre). ¿Qué es fuzzing? | KeepCoding Bootcamps. *KeepCoding Bootcamps*. https://keepcoding.io/blog/que-es-fuzzing-ciberseguridad/
- Khoyotte, & Khoyotte. (2023). ¿Alguna vez te has preguntado cómo de seguras son tus contraseñas? Un read more. *Seguridad en la informática*. https://seguridadenlainformatica.com/ataque-de-fuerza-bruta-en-ciberseguridad/
- Medina, E. (2018). Cómo comprobar si tu router ha sido afectado por un malware o un ataque. *MuyComputer*. https://www.muycomputer.com/2015/09/15/comprobar-router-afectado-malware-ataque/
- *¿Qué es DNS spoofing? – Ataques, prevención y más | ProofPoint ES*. (2023, 10 octubre). Proofpoint. https://www.proofpoint.com/es/threat-reference/dns-spoofing

- *¿Qué es el secuestro de sesión (session hijacking) y cómo prevenirlo? - Blog | GlobalSign*. (2021, 3 septiembre). GlobalSign. https://www.globalsign.com/es/blog/session-hijacking-and-how-to-prevent-it
- *Qué es email spoofing: suplantación de identidad en correos electrónicos*. (2021, 23 marzo). https://www.welivesecurity.com/la-es/2021/03/23/que-es-email-spoofing-suplantacion-identidad-correos-electronicos/
- *¿Qué es un ataque de fuerza bruta?* (2023, 18 agosto). www.kaspersky.es. https://www.kaspersky.es/resource-center/definitions/brute-force-attack
- Security, P. (2023, 18 julio). *Qué es el spoofing y cómo prevenir un ataque*. Panda Security Mediacenter. https://www.pandasecurity.com/es/mediacenter/consejos/que-es-el-spoofing/
- Seifreed. (2013). Dirb, fuzz en servidores webs. *DragonJAR - Servicios de Seguridad Informática*. https://www.dragonjar.org/dirb-fuzz-en-servidores-webs.xhtml