Universidad Autónoma De Chiapas.

Actividad. 2.1 Herramientas pasivas.

Estudiante: José Gilberto Guzmán Gutiérrez.

LIDTS. 7ºM.

A200119.

Catedrático: DR. Luis Gutiérrez Alfaro.

Tuxtla Gutiérrez Chiapas. 31 de agosto del 2023.

Responde las siguientes preguntas.

1. Explica que es network security o seguridad en la red.

   Es el campo de la ciberseguridad centrado en **proteger las redes informáticas de las ciber amenazas**. La seguridad de la red tiene tres objetivos principales: impedir el acceso no autorizado a los recursos de la red; detectar y detener los ciberataques y las violaciones de seguridad en curso; y garantizar que los usuarios autorizados tengan acceso seguro a los recursos de red que necesitan, cuando los necesitan.

2. Explicar los tipos de ataques, vulnerabilidades y amenazas.

   - Ataque de malware: Se refiere a **virus de software malicioso, incluidos gusanos, software espía, ransomware, adware y troyanos**. Irrumpe en una red a través de una vulnerabilidad. Cuando el usuario hace clic en un enlace peligroso, descarga un archivo adjunto de correo electrónico o cuando se utiliza un pendrive infectado.
   - Ataque de suplantación de identidad: Es un tipo de ataque de ingeniería social en el que **un atacante se hace pasar por un contacto confiable y envía correos electrónicos falsos a la víctima**. Sin darse cuenta de esto, la víctima abre el correo y hace clic en el enlace malicioso o abre el archivo adjunto del correo. Al hacerlo, los atacantes obtienen acceso a información confidencial y a las credenciales de la cuenta. También pueden instalar malware mediante un ataque de phishing.
   - Ataque de contraseña: Es una forma de ataque en la que **un hacker descifra su contraseña con varios programas y herramientas para descifrar contraseñas** como Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. Existen diferentes tipos de ataques de contraseña, como ataques de fuerza bruta, ataques de diccionario y ataques de registradores de teclas.
   - Ataque del hombre en el medio: Un ataque de hombre en el medio (MITM) también se conoce como ataque de escucha ilegal. En este ataque, un atacante **se interpone en una comunicación de dos partes, es decir, el atacante secuestra la sesión entre un cliente y un host**. Al hacerlo, los piratas informáticos roban y manipulan datos.
   - Ataque de inyección SQL**: Se transmite inyectando un código malicioso en el cuadro de búsqueda de un sitio web vulnerable**, lo que hace que el servidor revele información crucial. Esto da como resultado que el atacante pueda ver, editar y eliminar tablas en las bases de datos. Los atacantes también pueden obtener derechos administrativos a través de esto.
   - Ataque de denegación de servicio: Aquí, los atacantes **atacan sistemas, servidores o redes y los inundan con tráfico para agotar sus recursos y ancho de banda**. Cuando esto sucede, atender las solicitudes entrantes se vuelve abrumador para los servidores, lo que hace que el sitio web que aloja se

cierre o se ralentice. Esto deja desatendidas las solicitudes de servicio legítimas. También se conoce como ataque DDoS (denegación de servicio distribuido) cuando los atacantes utilizan varios sistemas comprometidos para lanzar este ataque.

- Amenaza interna: Como sugiere el nombre, una amenaza interna no involucra a un tercero sino a una persona interna. En cuyo caso; **podría ser un individuo dentro de la organización que sepa todo sobre la organización**. Las amenazas internas tienen el potencial de causar daños tremendos.
- Criptojacking: **Se produce cuando los atacantes acceden a la computadora de otra persona para extraer criptomonedas**. El acceso se obtiene infectando un sitio web o manipulando a la víctima para que haga clic en un enlace malicioso. También utilizan anuncios online con código JavaScript para ello. Las víctimas no son conscientes de esto ya que el código de minería Crypto funciona en segundo plano; un retraso en la ejecución es la única señal que podrían presenciar.
- Explotación de día cero: **Ocurre después del anuncio de una vulnerabilidad de red**; En la mayoría de los casos no existe solución para la vulnerabilidad. Por lo tanto, el proveedor notifica la vulnerabilidad para que los usuarios estén al tanto; sin embargo, esta noticia también llega a los atacantes.
- Ataque al abrevadero: La víctima aquí es un grupo particular de una organización, región, etc. En tal ataque, **el atacante apunta a sitios web que el grupo objetivo utiliza con frecuencia**. Los sitios web se identifican ya sea monitoreando de cerca al grupo o adivinando. Después de esto, los atacantes infectan estos sitios web con malware, que infecta los sistemas de las víctimas. El malware en tal ataque apunta a la información personal del usuario. En este caso, también es posible que el hacker acceda remotamente al ordenador infectado.

3. Explica los conceptos básicos como confidencialidad, integridad, disponibilidad y autenticación.

   Confidencialidad, integridad, disponibilidad, autenticidad y no repudio (a menudo abreviado como "CIA" o "CIAAN") son las cinco propiedades de seguridad principales que se utilizan para garantizar la seguridad y confiabilidad de los sistemas de información.

   - Confidencialidad: Es importante para proteger la información confidencial contra la divulgación a partes no autorizadas. Esto **incluye la protección de datos en reposo, en tránsito y en uso**. Las técnicas comunes utilizadas para mantener la confidencialidad incluyen cifrado, controles de acceso y enmascaramiento de datos.
   - Integridad: Es importante para garantizar que la información no haya sido manipulada o modificada de forma no autorizada. Esto **incluye proteger los datos contra modificaciones, eliminaciones o adiciones no autorizadas**.

Las técnicas comunes utilizadas para mantener la integridad incluyen firmas digitales, códigos de autenticación de mensajes y hash de datos.

- Disponibilidad: Es importante para garantizar que la información y los sistemas sean accesibles para los usuarios autorizados cuando los necesiten. Esto **incluye proteger contra ataques de denegación de servicio y garantizar que los sistemas tengan alta disponibilidad y puedan resistir fallas**. Las técnicas comunes utilizadas para mantener la disponibilidad incluyen equilibrio de carga, redundancia y planificación de recuperación ante desastres.
- Autenticidad: La autenticidad es importante para garantizar que la información y la comunicación provengan de una fuente confiable. Esto **incluye protección contra suplantación de identidad, suplantación de identidad y otros tipos de fraude de identidad**. Las técnicas comunes utilizadas para establecer la autenticidad incluyen la autenticación, los certificados digitales y la identificación biométrica.
- No repudio: Es importante para garantizar que una parte no pueda negar haber enviado o recibido un mensaje o transacción. Esto **incluye protección contra la manipulación de mensajes y ataques de repetición**. Las técnicas comunes utilizadas para establecer el no repudio incluyen firmas digitales, códigos de autenticación de mensajes y marcas de tiempo.

4. Política de seguridad.

Es un documento **que establece por escrito cómo una empresa planea proteger sus activos físicos y de tecnología de la información (TI) que se actualizan y cambian continuamente** a medida que cambian las tecnologías, las vulnerabilidades y los requisitos de seguridad.

La política de seguridad de una empresa puede incluir una política de uso aceptable. Estos describen cómo la empresa planea educar a sus empleados sobre la protección de los activos de la empresa. También incluyen una explicación de cómo se llevarán a cabo y aplicarán las medidas de seguridad, y un procedimiento para evaluar la efectividad de la política para garantizar que se realicen las correcciones necesarias.

5. Presenta las características de una política de seguridad.

Las políticas exitosas de seguridad de la información establecen qué se debe hacer y por qué se debe hacer, pero no cómo hacerlo. Una buena política tiene las siguientes siete características:

- Aprobada: La política cuenta con el apoyo de la gerencia.
- Relevante: la política es aplicable a la organización.
- Realista: La política tiene sentido.
- Alcanzable: la política se puede implementar con éxito.
- Adaptable: la política puede adaptarse al cambio.
- Aplicable: la política es legal.

- Inclusivo: El alcance de la política incluye a todas las partes relevantes.

6. Por qué se requiere atención especial la seguridad web.

   La seguridad web **es crucial debido a la naturaleza pública de Internet y la creciente dependencia de las aplicaciones y servicios en línea**. Las vulnerabilidades en los sistemas web pueden exponer información sensible y permitir que los atacantes obtengan acceso no autorizado.

7. Por qué preocuparse sobre la seguridad web.

   - **Protección de datos personales y financieros.**
   - **Prevención de robos de identidad.**
   - **Evitar interrupciones en servicios en línea.**
   - **Mantener la reputación de la empresa u organización.**

8. Que son las vulnerabilidades en servicio DNS a través de herramientas web.

   - Túnel DNS: **Implica codificar los datos de otros programas o protocolos dentro de consultas y respuestas de DNS**. Por lo general, presenta cargas útiles de datos que pueden apoderarse de un servidor DNS y permitir a los atacantes administrar el servidor remoto y las aplicaciones. A menudo depende de la conectividad de red externa de un sistema comprometido, lo que proporciona una vía de acceso a un servidor DNS interno con acceso a la red. También requiere controlar un servidor y un dominio, que funciona como un servidor autorizado que lleva a cabo programas ejecutables de carga útil de datos, así como túneles del lado del servidor.
   - Amplificación de DNS: Realizan denegación de servicio distribuido (DDoS) en un servidor objetivo. Esto **implica explotar servidores DNS abiertos que están disponibles públicamente para abrumar a un objetivo con tráfico de respuesta DNS**. Normalmente, un ataque comienza cuando el actor de la amenaza envía una solicitud de búsqueda de DNS al servidor DNS abierto, falsificando la dirección de origen para convertirla en la dirección de destino. Una vez que el servidor DNS devuelve la respuesta del registro DNS, se pasa al nuevo objetivo, que está controlado por el atacante.
   - Ataque de inundación de DNS: **Implican el uso del protocolo DNS para llevar a cabo una inundación del protocolo de datagramas de usuario (UDP)**. Los actores de amenazas implementan paquetes de solicitud de DNS válidos (pero falsificados) a una velocidad de paquetes extremadamente alta y luego crean un grupo masivo de direcciones IP de origen. Dado que las solicitudes parecen válidas, los servidores DNS del objetivo comienzan a responder a todas las solicitudes. A continuación, el servidor DNS puede verse abrumado por la enorme cantidad de solicitudes. Un ataque DNS requiere una gran cantidad de recursos de red, lo que agota la infraestructura DNS objetivo hasta que se

desconecta. Como resultado, el acceso a Internet del objetivo también disminuye.

- Suplantación de DNS: **Implica el uso de registros DNS alterados para redirigir el tráfico en línea a un sitio fraudulento que se hace pasar por el destino previsto**. Una vez que los usuarios llegan al destino fraudulento, se les solicita que inicien sesión en su cuenta. Una vez que ingresan la información, esencialmente le dan al actor de amenazas la oportunidad de robar las credenciales de acceso, así como cualquier información confidencial ingresada en el formulario de inicio de sesión fraudulento. Además, estos sitios web maliciosos se utilizan a menudo para instalar virus o gusanos en las computadoras de los usuarios finales, proporcionando al actor de la amenaza acceso a largo plazo a la máquina y a cualquier dato que almacene.
- Ataque NXDOMAIN: **Intenta saturar el servidor DNS utilizando un gran volumen de solicitudes de registros no válidos o inexistentes**. Estos ataques suelen ser manejados por un servidor proxy DNS que utiliza la mayoría (o todos) de sus recursos para consultar el servidor DNS autorizado. Esto hace que tanto el servidor DNS autorizado como el servidor proxy DNS consuman todo su tiempo manejando solicitudes incorrectas. Como resultado, el tiempo de respuesta a solicitudes legítimas se ralentiza hasta que finalmente se detiene por completo.

9. Que son las búsquedas vulnerabilidades a través de google.

   El Google hacking o Dorking no es más que **un modo de buscar cosas un poco más especializada**, por el nombre "Google Hacking" se puede dar la impresión de que solo se usa en google, pero eso no es correcto. El dorking no es más que una búsqueda avanzada en donde hacemos uso de operadores que funcionan como un filtro para dirigir la búsqueda directamente a donde nosotros queremos, también usamos símbolos para buscar palabras o frases exactas. Esto nos servirá para buscar en casi cualquier motor de búsqueda que encontremos en internet.

10. Que es la herramienta maltego.

Es una herramienta integral para **el análisis gráfico de enlaces que ofrece minería de datos y recopilación de información en tiempo real**, así como la representación de esta información en un gráfico basado en nodos, haciendo fácilmente identificables patrones y conexiones de múltiples órdenes entre dicha información. También ofrece la posibilidad de conectar fácilmente datos y funcionalidades de diversas fuentes mediante Transforms. A través de Transform Hub, puede conectar datos de más de 80 socios de datos, una variedad de fuentes públicas (OSINT), así como sus propios datos.

11. Que son las amenazas en seguridad de la información.

Son eventos o circunstancias que pueden causar daño a los sistemas y datos. Estas amenazas incluyen ataques cibernéticos, malware, phishing, espionaje, robo de datos, sabotaje y más. La gestión de amenazas busca identificar, evaluar y mitigar estos riesgos para mantener la seguridad de la información.

Bibliografías.

1. What is network security? (s/f). Ibm.com. Recuperado el 31 de agosto de 2023, de https://www.ibm.com/topics/network-security
2. Shruti, M. (2020, noviembre 30). Types of cyber attacks you should be aware of in 2023. Simplilearn.com; Simplilearn. https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
3. Kolbach, A. (1674211008000). Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation. Linkedin.com. https://www.linkedin.com/pulse/confidentiality-integrity-availability-authenticity-albert-kolbach/
4. Lutkevich, B. (2021, septiembre 17). What is a Security Policy? - Definition from Search. Security; TechTarget. https://www.techtarget.com/searchsecurity/definition/security-policy
5. Rowe, B. (1499354066000). Characteristics of a successful information security policy. Linkedin.com. https://www.linkedin.com/pulse/characteristics-successful-information-security-policy-branden-rowe/
6. Ann, J. (2017, octubre 23). Why Web Security is Important –. IPage Blog; iPage. https://ipage.com/blog/why-web-security-is-important/
7. (S/f). Strategynewmedia.com. Recuperado el 1 de septiembre de 2023, de https://strategynewmedia.com/why-web-security-is-important/
8. Dizdar, A. (2022, mayo 29). 5 DNS attack types and how to prevent them. Bright Security. https://brightsec.com/blog/dns-attack/
9. Google Hacking - Dorking - wiki de elhacker.net. (s/f). Elhacker.net. Recuperado el 1 de septiembre de 2023, de https://wiki.elhacker.net/bugs-y-exploits/nivel-web/google-dorking
   Raggi, N. (s/f). Google hacking: averigua cuanta información sobre ti o tu empresa aparece en los resultados. Welivesecurity.com. Recuperado el 1 de septiembre de 2023, de https://www.welivesecurity.com/la-es/2021/07/29/google-hacking-averigua-que-informacion-sobre-ti-o-empresa-aparece-resultados/
10. What is maltego? (s/f). Maltego Support. Recuperado el 1 de septiembre de 2023, de https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-
11. Follow, R. (2018, junio 19). Threats to information security. GeeksforGeeks. https://www.geeksforgeeks.org/threats-to-information-security/