Universidad Autónoma de Chiapas
Facultad de contaduría y administración C-I

Carrera:
Lic. En ing en desarrollo y tecnologías de software.

Materia:
Análisis de vulnerabilidades.

Catedrático:
Mtro. Luis Gutiérrez Alfaro.

Nombre del alumno:
González Aguilar Eduardo - A211154

Semestre: 7. **Grupo:** M.

Nombre de la actividad:
Herramientas pasivas.

Enlace GitHub:
AguilarEduardo/AnalisisDeVulnerabilidades (github.com)

Fecha de entrega:
24/02/2024.

Seguridad en la red: La seguridad en redes, también conocida como network security, se refiere a las medidas y prácticas diseñadas para proteger la integridad, confidencialidad y disponibilidad de los datos y recursos en una red de computadoras. Esto implica la implementación de políticas, procedimientos y herramientas para prevenir y detectar ataques cibernéticos, así como para responder adecuadamente en caso de que ocurran.

Tipos de ataques, vulnerabilidades y amenazas:

Ataques: Incluyen malware, ataques de denegación de servicio (DDoS), phishing, ingeniería social, entre otros.

Vulnerabilidades: Son debilidades en sistemas, aplicaciones o infraestructuras que pueden ser explotadas por atacantes para comprometer la seguridad.

Amenazas: Son posibles eventos o situaciones que pueden causar daño a la seguridad de la red, como hackers, virus, errores humanos, desastres naturales, entre otros.

Conceptos básicos:

Confidencialidad: Garantiza que la información solo sea accesible para aquellos autorizados a verla.

Integridad: Asegura que la información no sea alterada o modificada por personas no autorizadas.

Disponibilidad: Asegura que la información y los recursos estén disponibles cuando se necesiten.

Autenticación: Verifica la identidad de usuarios y sistemas para garantizar que solo los usuarios autorizados accedan a los recursos.

Política de Seguridad:

Una política de seguridad es un conjunto de reglas, procedimientos y directrices que definen cómo se deben proteger los activos de información de una organización y cómo responder a incidentes de seguridad. Establece las normas y responsabilidades para garantizar la seguridad de la red y los datos.

Características de una Política de Seguridad:

- Claridad y coherencia en las reglas y directrices.
- Participación y compromiso de la alta dirección.
- Actualización periódica para adaptarse a nuevas amenazas y tecnologías.
- Educación y concienciación de los empleados.
- Procedimientos claros de respuesta a incidentes.

Importancia de la Seguridad Web:

La seguridad web es crucial debido a la creciente dependencia de las organizaciones en la tecnología web para operar. La información confidencial y los servicios críticos están expuestos a diversas amenazas, como ataques de hackers, malware y vulnerabilidades en aplicaciones web.

Vulnerabilidades en Servicio DNS y Búsquedas de Vulnerabilidades:

Las vulnerabilidades en el servicio DNS pueden permitir a los atacantes manipular las consultas de DNS, redirigir tráfico de red y realizar ataques de envenenamiento de caché. Las búsquedas de vulnerabilidades a través de Google pueden revelar información sensible, como contraseñas, credenciales de acceso y datos confidenciales expuestos públicamente en sitios web y servidores mal configurados.

Herramienta Maltego:

Maltego es una herramienta de inteligencia de código abierto utilizada para recopilar y analizar información de diversas fuentes en línea para investigaciones de seguridad cibernética, análisis de amenazas y gestión de incidentes.

Amenazas en Seguridad de la Información:

Las amenazas en seguridad de la información incluyen ataques cibernéticos, robo de datos, malware, phishing, ingeniería social, errores humanos, desastres naturales y fallas de hardware o software que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.

Conclusión.

La seguridad en redes y en la web es fundamental en la era digital para proteger la información y los activos críticos de organizaciones y usuarios. La implementación de políticas de seguridad robustas, la educación continua de los empleados y el uso de herramientas y tecnologías de seguridad adecuadas son esenciales para mitigar riesgos y responder efectivamente a las amenazas emergentes en el ciberespacio.

Fuentes de informacion.

¿Qué es la seguridad de red? | *IBM*. (s. f.). https://www.ibm.com/mx-es/topics/network-security#:~:text=En%20un%20nivel%20b%C3%A1sico%2C%20la%20seguridad%20de%20red,y%20sistemas%20que%20est%C3%A1n%20conectados%20a%20la%20red.

Qué es la seguridad de la información | *Cloudflare*. (n.d.). Cloudflare. https://www.cloudflare.com/es-es/learning/security/what-is-information-security/