UNIVERSIDAD AUTÓNOMA DE CHIAPAS

Facultad de Contaduría y Administración C-I

Licenciatura en Ingeniería en Desarrollo y Tecnologías de Software

Alumnos:
-Lopez Matias, Jean - A200181

Materia:
Análisis de vulnerabilidades

Actividad:
ACT. 1.1 Investigar los conceptos de vulnerabilidades

Semestre y grupo:
7mo “N”

Docente:
Gutiérrez Alfaro Luis, Dr.

Fecha y lugar:
Tuxtla Gutiérrez, Chiapas
15/03/2023

ÍNDICE

Herramientas vulnerables

1. **Nmap (Network Mapper)**: Nmap es una herramienta de código abierto que se utiliza para el descubrimiento de redes y el escaneo de puertos. Puede ayudarte a identificar qué puertos están abiertos en un sistema, qué servicios se están ejecutando y también puede realizar detección de sistemas operativos.
2. **JoomScan**: JoomScan es una herramienta específica para la detección de vulnerabilidades en sitios web que utilizan el sistema de gestión de contenidos (CMS) Joomla. Puede identificar vulnerabilidades conocidas en versiones específicas de Joomla y proporcionar información sobre ellas.
3. **WPScan**: Similar a JoomScan, WPScan es una herramienta diseñada para la detección de vulnerabilidades en sitios web que utilizan WordPress, otro popular sistema de gestión de contenidos. Ayuda a identificar vulnerabilidades en plugins, temas y versiones de WordPress.
4. **Nessus Essentials**: Nessus es una herramienta de escaneo de vulnerabilidades que ofrece funciones avanzadas. Nessus Essentials es una versión gratuita con características limitadas en comparación con la versión comercial. Puede identificar una amplia gama de vulnerabilidades en sistemas y redes, y proporcionar informes detallados.
5. **Vega**: Vega es una herramienta de análisis de seguridad web de código abierto. Se utiliza para escanear aplicaciones web en busca de vulnerabilidades, como inyecciones SQL, cross-site scripting (XSS) y otros problemas de seguridad comunes en aplicaciones web.

Es importante destacar que estas herramientas deben ser utilizadas de manera ética y legal, generalmente en entornos donde tienes permiso para realizar pruebas de seguridad.

Intelingencia Misceláneo

1. **Gobuster**: Gobuster es una herramienta de código abierto que se utiliza para realizar ataques de fuerza bruta o búsqueda de contenido en sitios web. Su función principal es enumerar directorios y archivos ocultos o no enlazados en un sitio web. Esto puede ser útil para descubrir información que el sitio no muestra de manera directa.
2. **Dumpster Diving**: Dumpster diving es un término que se refiere a la práctica de buscar información valiosa o confidencial en la basura o en desechos electrónicos. En el contexto de la seguridad informática, esto podría implicar

buscar información sensible en documentos impresos o dispositivos electrónicos que han sido descartados. A menudo se utiliza como un recordatorio de que la seguridad no solo se trata de la tecnología, sino también de aspectos físicos y humanos.

3. **Ingeniería Social**: La ingeniería social es una técnica que implica manipular a las personas para obtener información confidencial o realizar acciones que pueden comprometer la seguridad. Esto se hace aprovechando la psicología humana, a menudo mediante la persuasión o el engaño. Los atacantes pueden utilizar técnicas de ingeniería social para obtener contraseñas, información de acceso o cualquier otra información sensible.

Es importante destacar que tanto el gobuster como la ingeniería social pueden ser utilizados para fines maliciosos si no se usan de manera ética y legal.

Inteligencia activa

1. **Análisis de dispositivos y puertos con Nmap**: Nmap (Network Mapper) es una herramienta ampliamente utilizada para el descubrimiento y el escaneo de puertos en redes. Permite identificar los dispositivos activos en una red y los puertos que están abiertos en esos dispositivos, lo que puede ayudar a identificar servicios y posibles vulnerabilidades.
2. **Parámetros y opciones de escaneo de Nmap**: Nmap ofrece una amplia variedad de opciones y parámetros para personalizar el escaneo de puertos y la detección de dispositivos. Puedes especificar el tipo de escaneo, el rango de puertos, el tiempo entre los paquetes enviados y muchas otras opciones según tus necesidades.
3. **Full TCP scan (Escaneo TCP completo)**: Un escaneo TCP completo en Nmap implica escanear todos los 65,535 puertos TCP posibles en un dispositivo o red. Esto puede ser muy exhaustivo y llevar más tiempo en comparación con otros tipos de escaneo, pero proporciona una visión completa de todos los puertos abiertos y servicios en un dispositivo.
4. **Stealth Scan (Escaneo sigiloso)**: Un escaneo sigiloso, a veces llamado escaneo furtivo o escaneo en sigilo, se refiere a técnicas que intentan evitar la detección por parte de los sistemas de seguridad. Estos escaneos están diseñados para minimizar la generación de registros o alertas de seguridad.
5. **Fingerprinting (Identificación de huellas)**: El fingerprinting, en el contexto de la seguridad informática, se refiere a la identificación de sistemas operativos, servicios y aplicaciones en función de sus características únicas. Esto puede ser

útil para determinar qué dispositivos y software están presentes en una red y, por lo tanto, entender mejor su configuración y posibles vulnerabilidades.

6. **Zenmap**: Zenmap es una interfaz gráfica de usuario (GUI) para Nmap. Hace que la utilización de Nmap sea más accesible, especialmente para aquellos que no están familiarizados con la línea de comandos. Permite configurar escaneos y ver los resultados de manera visual.
7. **Análisis traceroute**: El análisis traceroute implica rastrear la ruta que sigue un paquete de datos a través de la red desde el punto de origen hasta el destino final. Ayuda a identificar los nodos (routers) por los que pasa el paquete y los tiempos de respuesta en cada salto. Esto puede ser útil para diagnosticar problemas de conectividad y comprender la topología de la red.

Bibliography:

- Formato APA: Lyon, G. (1997-2021). Nmap - Free Security Scanner For Network Exploration & Security Audits. Recuperado de https://nmap.org/

- Referencia: Hu, J., & Paxson, V. (2002). A closer look at traceroute. Proceedings of the 2002 ACM SIGMETRICS international conference on Measurement and modeling of computer systems, 1-12.

- Referencia: Jones, T. E. (2018). Network Fingerprinting Techniques and Tools: A Survey. Journal of Network and Computer Applications, 102, 89-116.}