Conceptos de vulnerabilidades

ANÁLISIS DE VULNERABILIDADES

Herramientas de vulnerabilidades

Un escáner de vulnerabilidades es un software que evalúa tu red y sistemas en busca de vulnerabilidades e informa los riesgos asociados con ellos. Además, el escaneo de vulnerabilidades es también uno de los primeros pasos en las pruebas de penetración.

Los escáneres de vulnerabilidades funcionan mediante un mecanismo de tres pasos que converge hacia el objetivo de la organización de identificar las vulnerabilidades y el riesgo que pueden representar.

1. **Detección**
2. **Clasificación**
3. **Remediación**

Herramientas de vulnerabilidades .

- Nmap

Es la abreviatura de Network Mapper. Es una herramienta de línea de comandos Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Permite a los administradores de red encontrar qué dispositivos se ejecutan en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

- Joomscan

Escáner de seguridad Joomscan es una herramienta de auditoría de sitios web para Joomla. Está escrito en Perl y es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, Defectos de RFI, BIA, Defecto XSS, inyección ciega de SQL, protección de directorios y otros.

Herramientas de vulnerabilidades .

- WPScan

Diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web. Con ella, puedes auditar sistemas, verificar su estado y corregir cada fallo que encuentres antes de que lo aproveche un delincuente.

- Nessus Essentials

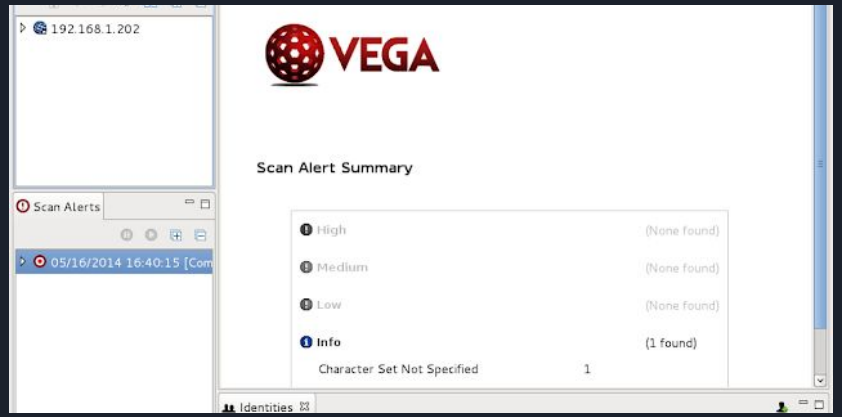
una herramienta de seguridad que busca debilidades en los sistemas informáticos y redes.

Nessus se utiliza para identificar y analizar vulnerabilidades de seguridad en sistemas operativos, aplicaciones y dispositivos de red. Es capaz de escanear todo tipo de dispositivos, desde servidores hasta dispositivos móviles, routers y firewalls.

Herramientas de vulnerabilidades .

- Vega

Vega es un programa dedicado a la seguridad de las páginas web, el cual es un programa que permite saber todas las vulnerabilidades que tiene un sitio web para que después tú mismo puedas corregirlas.



Vega puede ayudarle a encontrar y validar la inyección de SQL, Cross-Site Scripting (XSS), reveló inadvertidamente información sensible, y otras vulnerabilidades.

Inteligencia Misceláneo

- Gobuster

Gobuster es una herramienta de línea de comandos utilizada en pruebas de penetración para realizar ataques de fuerza bruta o enumeración de rutas/directorios en aplicaciones web. Busca nombres de archivos y directorios mediante solicitudes HTTP.

- Dumpster Diving

En su Guía de ciberataques, Incibe y OSI definen el dumpster diving como “el proceso de buscar en nuestra basura para obtener información útil sobre nuestra persona o empresa que luego pueda utilizarse contra nosotros para otro tipo de ataques”.

Buscando en los documentos impresos que tiramos a una papelera o un contenedor, los ciberdelincuentes esperan encontrar números de tarjetas bancarias, contactos o anotaciones con credenciales.

Inteligencia Misceláneo

- La Ingeniería Social

Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.

Inteligencia Activa

- Análisis de dispositivos y puertos con Nmap.

Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

- Parámetros opciones de escaneo de nmap

- Escaneos de ping: Detectan si los objetivos están en línea, pero no escanean los puertos. Se pueden hacer con las opciones -Pn o -PT
- Escaneos de puertos: Detectan los puertos abiertos, cerrados o filtrados en los objetivos. Se pueden hacer con las opciones -sS, -sU, -sT, entre otras.
- Escaneos de servicios: Identifican los servicios y versiones que se ejecutan en los puertos abiertos. Se pueden hacer con las opciones -sV o -A

Inteligencia Activa

- Full TCP scan

Un escaneo abierto completo establece un protocolo de enlace TCP de tres vías antes de realizar cualquier escaneo de puertos en el sistema de destino, con el objetivo de determinar su estado si están abiertos y cerrados.

- Stelth Scan

TCP SYN (Stealth) Scan (-sS). El escaneo SYN es la opción de escaneo predeterminada y más popular para siempre razón. Se puede realizar rápidamente, escaneando miles de puertos por En segundo lugar, en una red rápida no obstaculizada por firewalls intrusivos. Análisis SYN es relativamente discreto y sigiloso, ya que nunca completa TCP Conexiones.

Inteligencia Activa

- Fingerprintig

Footprinting es la primera forma para que los evaluadores de penetración puedan recoger información sobre hardware o red.

Se trata de un procedimiento de exploración con el que podemos conocer a nuestro enemigo. Para que ese procedimiento de penetración sea completo, debemos acumular toda la información posible.

- Zenmap

Zenmap es la GUI oficial de Nmap Security Scanner. Es una multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) Aplicación gratuita y de código abierto que tiene como objetivo hacer que Nmap sea fácil de usar para los principiantes mientras proporciona funciones avanzadas para usuarios experimentados de Nmap.