:::::::: Informe de vulnerabilidades detectadas con Nmap ::::::::

Autor: Samuel-G3
Fecha: 01/06/2025
TÃ-tulo del proyecto: Escaneo de puertos y detecciÃ³n de vulnerabilidades en una mÃ¡quina Debian

1. Objetivo

El objetivo de esta prÃ¡ctica es analizar una mÃ¡quina Debian (objetivo) desde una mÃ¡quina Kali Linux (atacante) utilizando la herramienta Nmap. Se busca identificar servicios activos, puertos abiertos y posibles vulnerabilidades que podrÃ-an comprometer la seguridad del sistema.
2. Entorno de trabajo

- MÃ¡quina atacante: Kali Linux
- MÃ¡quina objetivo: Debian
- DirecciÃ³n IP objetivo: 10.0.2.4
- Herramienta utilizada: Nmap 7.95

3. Escaneos realizados
3.1 Escaneo bÃ¡sico de puertos

Comando utilizado:

```
nmap 10.0.2.4
```

Resultado:

- Puerto 21/tcp â\200\224 servicio ftp â\200\224 abierto
- Puerto 80/tcp â\200\224 servicio http â\200\224 abierto

3.2 DetecciÃ³n de versiones de servicios

Comando utilizado:

```
nmap -sV 10.0.2.4
```

Resultado:

- Servicio FTP: vsftpd 3.0.3
- Servicio HTTP: Apache httpd 2.4.62 (Debian)

3.3 Escaneo de vulnerabilidades

Comando utilizado:

```
nmap -sV --script=vuln 10.0.2.4
```

4. Vulnerabilidades detectadas
Servicio: vsftpd 3.0.3 (puerto 21/tcp)

- CVE-2021-30047
  - Puntaje CVSS: 7.5
  - DescripciÃ³n: vulnerabilidad que permite ejecuciÃ³n remota de cÃ³digo.
  - Fuente: https://vulners.com/cve/CVE-2021-30047
- CVE-2021-3618
  - Puntaje CVSS: 7.4

DescripciÃ³n: vulnerabilidad de denegaciÃ³n de servicio (DoS).

Fuente: https://vulners.com/cve/CVE-2021-3618

Servicio: Apache httpd 2.4.62 (puerto 80/tcp)

No se detectaron vulnerabilidades crÃ-ticas durante el escaneo.

Se encontraron los siguientes directorios y archivos relevantes:

/wordpress/

/info.php

/wp-login.php

5. Recomendaciones

Actualizar el servicio vsftpd a una versiÃ³n que no sea vulnerable a las CVE reportadas.

Eliminar o restringir el acceso al archivo info.php, ya que puede exponer informaciÃ³n sensible del servidor.

Aplicar medidas de protecciÃ³n adicionales en el entorno de WordPress, como autenticaciÃ³n multifactor y limitaciÃ³n de intentos de inicio de sesiÃ³n.

Revisar la configuraciÃ³n del servidor Apache para aplicar buenas prÃ¡cticas de seguridad y ocultar informaciÃ³n del servidor en los encabezados HTTP.

6. ConclusiÃ³n

El escaneo realizado ha demostrado que la mÃ¡quina objetivo expone servicios que presentan vulnerabilidades conocidas. La explotaciÃ³n de estas vulnerabilidades podrÃ-a comprometer la integridad y la disponibilidad del sistema. Se recomienda aplicar las actualizaciones necesarias y reforzar la configuraciÃ³n de seguridad para mitigar estos riesgos.