Informe de Vulnerabilidades en el Servidor utilizando Nmap

Este informe presenta las vulnerabilidades detectadas durante un escaneo con Nmap a un servidor Linux. Las pruebas se realizaron bajo un entorno controlado, con el objetivo de identificar riesgos y proponer soluciones efectivas para mejorar la seguridad.

Se utilizó la herramienta Nmap para llevar a cabo un escaneo de seguridad en el servidor objetivo. Este escaneo permitió identificar puertos abiertos y servicios en ejecución, sus versiones y posibles vulnerabilidades asociadas.
Los resultados obtenidos destacan debilidades críticas que podrían ser explotadas por atacantes para comprometer la seguridad del sistema.

Detalles del Escaneo

El escaneo se realizó con el comando:

nmap -sV --script=vuln <IP_servidor>

Salida del escaneo

```
└─$ nmap -sV --script=vuln 192.168.0.14
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-19 14:26 EST
Nmap scan report for 192.168.0.14
Host is up (0.00060s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /info.php: Possible information file
|_  /wordpress/wp-login.php: Wordpress login page.
```

Resultado

- Puerto 80 (HTTP): Apache HTTP Server 2.4.62 detectado.
- Directorio /wordpress identificado como un blog WordPress.
- Archivo info.php identificado como posible archivo informativo.
- URL /wordpress/wp-login.php detectada como página de inicio de sesión de WordPress.

Vulnerabilidades Detectadas

Puerto	Servicio	Versión	Descripción	Referencia
80	HTTP	Apache 2.4.62	Vulnerabilidad de encabezado malicioso que permite ataques de desbordamiento de búfer (CVE-2023-25 690). Puede provocar la ejecución remota de código (RCE).	CVE-2023-25 690
80	HTTP	Apache 2.4.62	Vulnerabilidad de denegación de servicio (DoS) al procesar solicitudes específicas con mod_lua habilitado (CVE-2022-22 720).	CVE-2022-22 720
80	HTTP	Apache 2.4.62	Vulnerabilidad de Server-Side Request Forgery (SSRF) que puede filtrar hashes NTLM a través de solicitudes manipuladas en mod_rewrite (CVE-2024-40 898).	CVE-2024-40 898
80	HTTP	Apache 2.4.62	Posible divulgación de código fuente en archivos solicitados indirectamente debido a configuraciones heredadas incorrectas (CVE-2024-40 725).	CVE-2024-40 725
80	WordPress	No especificada	Inyección SQL (SQLi) que permite a atacantes acceder a la base de datos y extraer información confidencial (CVE-2022-21 661).	CVE-2022-21 661

Recomendaciones

- **Actualizar Software:** Mantener Apache y WordPress en sus versiones más recientes.
- **Configurar Seguramente:** Deshabilitar módulos innecesarios y ajustar configuraciones de seguridad en Apache y WordPress.
- **Auditorías Periódicas:** Realizar pruebas de penetración para identificar vulnerabilidades antes de que sean explotadas.
- **Validación de Entradas:** Implementar validaciones estrictas para prevenir ataques como la inyección SQL.

Conclusión

El escaneo con Nmap revela vulnerabilidades significativas en el servidor que ejecuta Apache y WordPress. Estas vulnerabilidades resaltan la importancia de mantener los sistemas actualizados, configurar adecuadamente los servicios y realizar auditorías periódicas para garantizar la seguridad de los datos y servicios proporcionados.