Vulnerability Report

1. Puerto y Servicio

Puerto	Servicio	Versión
80/tcp	HTTP	Apache 2.4.62 (Debian)
22/tcp	SSH	Cerrado

2. Vulnerabilidades Detectadas

Ruta/Archivo	Versión Detectada	Descripción
`/`	6.8.1	Versión actual del CMS WordPress.
`/readme.html`	2.2	Archivo revelador de versión obsoleta.
`/wp-includes/images/rss.png`	2.2	Imagen de versión antigua.
`/wp-includes/js/jquery/suggest.js`	2.5	Script JavaScript antiguo.
`/wp-includes/images/blank.gif`	2.6	Imagen común en WordPress 2.6.
`/wp-includes/js/comment-reply.js`	2.7	Script típico de esa versión.
`/wp-admin/upgrade.php`	2.7	Script para actualización de WordPress.
`/wp-login.php`	-	Página de login de administrador.
`/readme.html`	-	Archivo informativo accesible públicamente.

3. Usuario Detectado

Usuario de WordPress encontrado: `**julitenti**`

4. Observaciones del sistema

- Dirección IP objetivo: 192.168.1.10
- MAC Address: 08:00:27:D5:43:FB
- Fabricante: Oracle VirtualBox
- Host: Debian corriendo Apache y WordPress
- Puerto 22 (SSH) está cerrado
- Puerto 80 (HTTP) está abierto

---

5. Herramientas utilizadas

- **Kali Linux**: Máquina atacante
- **Nmap 7.95**: Para escaneo de red y vulnerabilidades
- **Script**: nmap -p 80 -sV --script=vuln 192.168.1.10

---

6. Recomendaciones

- Eliminar archivos antiguos (readme.html, etc.)
- Actualizar y endurecer la instalación de WordPress
- Cambiar rutas por defecto (como /wp-login.php)
- Cerrar puertos innecesarios y restringir acceso SSH si no se usa
- Usar firewall como ufw correctamente configurado

7. Conclusión

Durante este ejercicio de análisis de red se descubrió un servidor HTTP Apache corriendo WordPress con archivos expuestos de versiones antiguas. También se logró enumerar el nombre de usuario de WordPress. Aunque no se detectaron vulnerabilidades de tipo XSS o CSRF, la exposición de versiones antiguas y archivos administrativos representa un riesgo de seguridad. Se recomienda aplicar parches, eliminar archivos innecesarios y seguir prácticas de hardening.