

# Escaneo de puertos con nmap

Puerto	Servicio	Versión	Vulnerabilidad	Descripción	Referencia
80/tcp	HTTP	Apache httpd 2.4.65	CVE-2025-54090	Fallo relacionado con RewriteCond expr; revisar parches y confirmar si 2.4.65 incluye la corrección.	<a href="https://cvedetails.com/cve/CVE-2025-54090/">https://cvedetails.com/cve/CVE-2025-54090/</a>
80/tcp	HTTP (wordpress en /wordpress/)	Wordpress (detectado)	Wordpress expuesto / login público.	`/wordpress/` y `/wordpress/wp-login.php` detectados. Riesgo según plugins/themes; revisar versiones.	<a href="https://wordpress.org/support/article/hardening-wordpress/">https://wordpress.org/support/article/hardening-wordpress/</a>
80/tcp	Web app (endpoints con parámetros )	(no aplica / variable)	Posible SQL injection (detección automatizada)	Nmap `http-sql-injection` listó múltiples URLs candidatas; es una alerta que requiere verificación manual.	<a href="https://owasp.org/www-community/attacks/SQL_Injection">https://owasp.org/www-community/attacks/SQL_Injection</a>
80/443	HTTP / HTTPS	Apache httpd 2.4.65 (debian)	Slowloris DoS — Likely vulnerable (CVE-2007-6750)	`http-slowloris-check` reportó: "VULNERABLE: Slowloris DOS attack". Riesgo de denegación de servicio; mitigación.	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750</a>
80/tcp	HTTP	Apache httpd (≤ 2.4.63 afect.)	CVE-2024-43394	SSRF por rutas UNC en mod_rewrite que afecta versiones ≤2.4.63; verificar si aplicable.	<a href="https://knowledge.broadcom.com/external/article/407938/">https://knowledge.broadcom.com/external/article/407938/</a>
80/tcp	HTTP	Apache httpd (≤ 2.4.63 afect.)	CVE-2024-47252	Insuficiente escapado en mod_ssl/logs en versiones ≤2.4.63; revisar parches y logs.	<a href="https://knowledge.broadcom.com/external/article/407938/">https://knowledge.broadcom.com/external/article/407938/</a>