Escaneo de puertos con nmap

(la tabla esta consultada con ia, para leer todo el texto que me ha dado la terminal después del escaneo de vulnerabilidades)

Puerto	Servicio	Versión	Vulnerabilidad (ejemplo)	Descripción	Referencia
22	SSH	OpenSSH 9.2p1 Debian 2+deb12u7	CVE-2023-38408, CVE-2023-28531, y múltiples identificadores con exploits	El escaneo con el script `vulners` muestra múltiples vulnerabilidades asociadas a la versión detectada de OpenSSH; algunas entradas listadas tienen puntuaciones altas y exploits públicos disponibles — riesgo de explotación remota/privilegios si alguna aplica.	Link
80	HTTP	Apache httpd 2.4.65 ((Debian))	Exposición de `/server-status`; presencia de WordPress (/wordpress/)	`http-enum` encontró `/server-status/` (puede filtrar información interna del servidor) y un WordPress accesible (`/wordpress/` y `/wordpress/wp-login.php`) — posibles fugas de información o vulnerabilidades de CMS si WordPress/no está parcheado.	Link
443	HTTPS	Apache httpd 2.4.65 ((Debian)) sobre TLS	Igual que en puerto 80: `/server-status` y WordPress detectado	Mismas observaciones que en el puerto 80; además, habría que revisar la configuración TLS/SSL (ciphers, versiones) y certificados para riesgos adicionales.	Link