Vulnerability Report

Máquina para scanear:
VM: Kali

Máquina Objetivo:
VM: Debian
IP: 10.10.50.82

Puertos y servicios:

PORT: 80/tcp
SERVICE: http
VERSION: Apache httpd 2.4.65

Vulnerabilidades:

Puerto	Servicio	Version	Vulnerabilidad	Descripción	Referencia
80	HTTP	Apache httpd 2.4.65 (Debian)	CVE-2025-58098 8.3	Vulnerabilidad que permite la ejecución de comandos vía mod_cgid y SSI	https://nvd.nist.gov/vuln/detail/CVE-2025-58098
			CVE-2025-59775 7.5	Permite la fuga de hashes NTLM mediante configuraciones específicas de manejo de barras en URLs.	https://nvd.nist.gov/vuln/detail/CVE-2025-59775
			CVE-2025-55753 7.5	Un desbordamiento de enteros en fallos de renovación ACME provoca que los reintentos se ejecuten sin demora, saturando el sistema	https://nvd.nist.gov/vuln/detail/CVE-2025-55753
			CNVD-2025-30837 7.5	Vulnerability Apache Server versiones 2.4.30 a 2.4.66 permite al atacante activar intentos de renovación sin demora.	https://vulners.com/cnvd/CNVD-2025-30837
			CNVD-2025-30836 7.5	Apache HTTP Server sufre una vulnerabilidad de falsificación de solicitudes entre sitios que puede revelar hashes NTLM.	https://vulners.com/cnvd/CNVD-2025-30836
			CVE-2025-65082 6.5	Fallo en la neutralización de caracteres permite que variables de entorno configuradas sobrescriban valores críticos del servidor en programas CGI.	https://nvd.nist.gov/vuln/detail/CVE-2025-65082

			CNVD-2025-30833 6.5	La omisión de seguridad de Apache HTTP Server permite la sobreescritura de variables CGI a través del manejo de secuencias de escape en las versiones 2.4.0–2.4.65.	https://vulners.com/cnvd/CNVD-2025-30833
			CVE-2025-66200 5.4	Fallo en mod_userdir y suexec permite que usuarios con permisos FileInfo ejecuten scripts CGI bajo identidades (UID) incorrectas mediante RequestHeader	https://nvd.nist.gov/vuln/detail/CVE-2025-66200
			CNVD-2025-30835 5.4	La falla de ejecución de código Apache HTTP Server en 2.4.7 a 2.4.65 permite que un script CGI se ejecute como un usuario inesperado.	https://vulners.com/cnvd/CNVD-2025-30835