





Puertos encontrados

<i>Puerto</i>	<i>Estado</i>	<i>Servicio</i>	<i>Versión</i>
80/TCP	OPEN	HTTP	Apache httpd 2.4.65

Vulnerabilidades encontradas

<i>ID</i>	<i>CVE</i>	<i>Score</i>	<i>Description</i>
1337DAY-ID-34882	CVE-2020-11984	7.5	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
FD2EE3A5-BAEA-5845-BA35-E6889992214F	CVE-2024-40898	6.1	SSRF in Apache HTTP Server on Windows with mod_rewrite in server/vhost context, allows to potentially leak NTML hashes to a malicious server via SSRF and malicious requests. Users are recommended to upgrade to version 2.4.62 which fixes this issue.
E606D7F4-5FA2-5907-B30E-367D6FFECD89	CVE-2024-40725	7.4	A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue.
EDB-ID:46676	CVE-2019-0211	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
EDB-ID:40909	CVE-2016-8740	7.2	The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.
CDC791CD-A414-5ABE-A897-7CFA3C2D3D29	CVE-2024-38472	8.2	Es un identificador de exploit público del CVE-2024-38472. Este exploit permite ejecución remota de código (RCE) mediante una vulnerabilidad de SSRF (Server-Side Request Forgery), afectando a servicios internos expuestos como Jenkins a través de rutas UNC. El código está escrito en Ruby y actúa como un

			módulo de Metasploit.
A0F268C8-7319-5637-82F7-8DAF72D14629	CVE-2022-26377	8.9	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
1337DAY-ID-35422	CVE-2020-11993	8.6	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
1337DAY-ID-32502	CVE-2019-0211	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
PACKETSTORM:152441	CVE-2019-0211		
1337DAY-ID-26497	CVE-2019-0211		

Conclusiones

Nmap bajo mi opinión me parece buena herramienta para poder gestionar las posibles vulnerabilidades que hay en la máquina, pero siempre hay que asegurarse que sean 100% fiables, ya que hay varias que coloca como **"EXPLOIT"** mientras son por ejemplo una GUID perteneciente a Windows.

Mientras se realice manualmente una revisión de las vulnerabilidades que puedan haber en la máquina, todo estará bien.