Starting Nmap 7.94SVN (https://nmap.org) at 2024-10-24 07:22 EDT

Nmap scan report for 10.0.2.5
Host is up (0.00010s latency).
Not shown: 999 closed tcp ports (reset)

PORT STATE SERVICE VERSION
80/tcp open http Apache httpd 2.4.62 ((Debian))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-server-header: Apache/2.4.62 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
| /wordpress/: Blog
|_ /wordpress/wp-login.php: WordPress login page.

MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in

No se encontró ningún tipo de vulnerabilidad a la hora de realizar un escaneo.

Apache HTTP Server 2.4.7
Vulnerabilidad de Divulgación de Código Fuente: CVE-2019-02111
Esta vulnerabilidad permite a un atacante ejecutar código arbitrario con privilegios de root

Vulnerabilidad de Autenticación: CVE-2019-02171
Permite a un usuario con credenciales válidas autenticarse usando otro nombre de usuario

OpenSSL 1.0.1f
Vulnerabilidad Heartbleed: CVE-2014-01602
Esta vulnerabilidad permite a un atacante leer memoria de servidores afectados

Vulnerabilidad de Manejo de Certificados: CVE-2023-04643
Puede causar consumo excesivo de recursos

Vulnerabilidad de Verificación de Certificados: CVE-2023-04653
Permite a un atacante afirmar políticas de certificado inválidas

OpenSSH 6.6.1p1
Vulnerabilidad de Inyección de Comandos: CVE-2015-65654
Permite a un atacante ejecutar comandos arbitrarios en el sistema

Vulnerabilidad de Denegación de Servicio: CVE-2015-65664
Puede causar un ataque de denegación de servicio