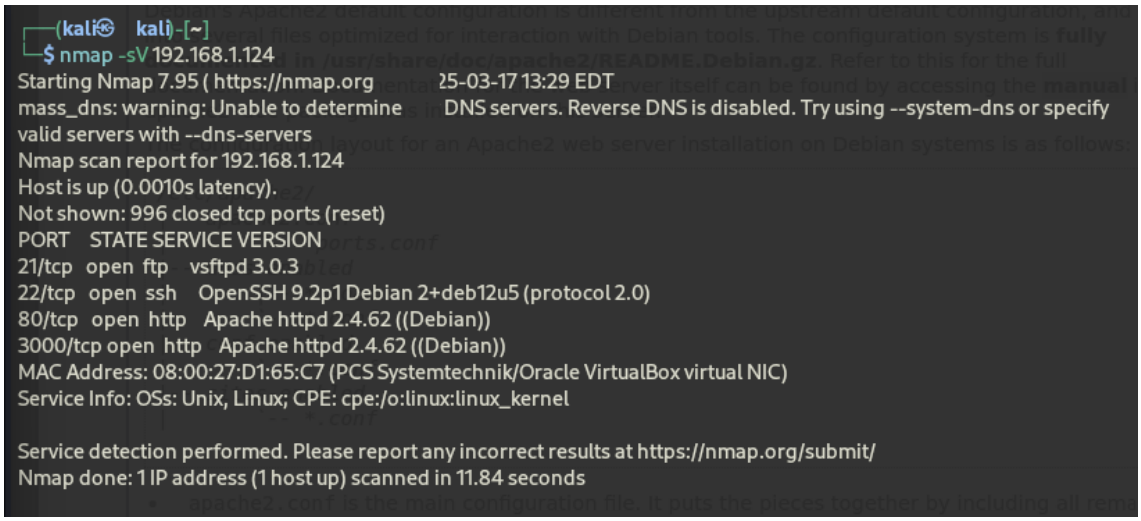
Vulnerabilitys report – Debian device

En esta práctica utilizaremos la herramienta Nmap, la cual se usa para la exploración de red y auditoría de seguridad. El propósito será escanear la red, en concreto una máquina Debian en específico que tiene ejecutándose un servicio web con Apache2, mysqli, MariaDB y Wordpress.

La configuración de red en este caso es de Adaptador Puente, de modo que tiene acceso a Internet y mi ordenador anfitrión puede conectarse a dicho servicio web.
Realizaremos el escaneo con Nmap a través de la máquina virtual Kali.
El siguiente comando mostrará los hosts activos y los puertos abiertos junto al servicio y versión que están ejecutando en una red o en un dispositivo, mediante los argumentos –sV acompañados de la dirección IP de la máquina Debian.

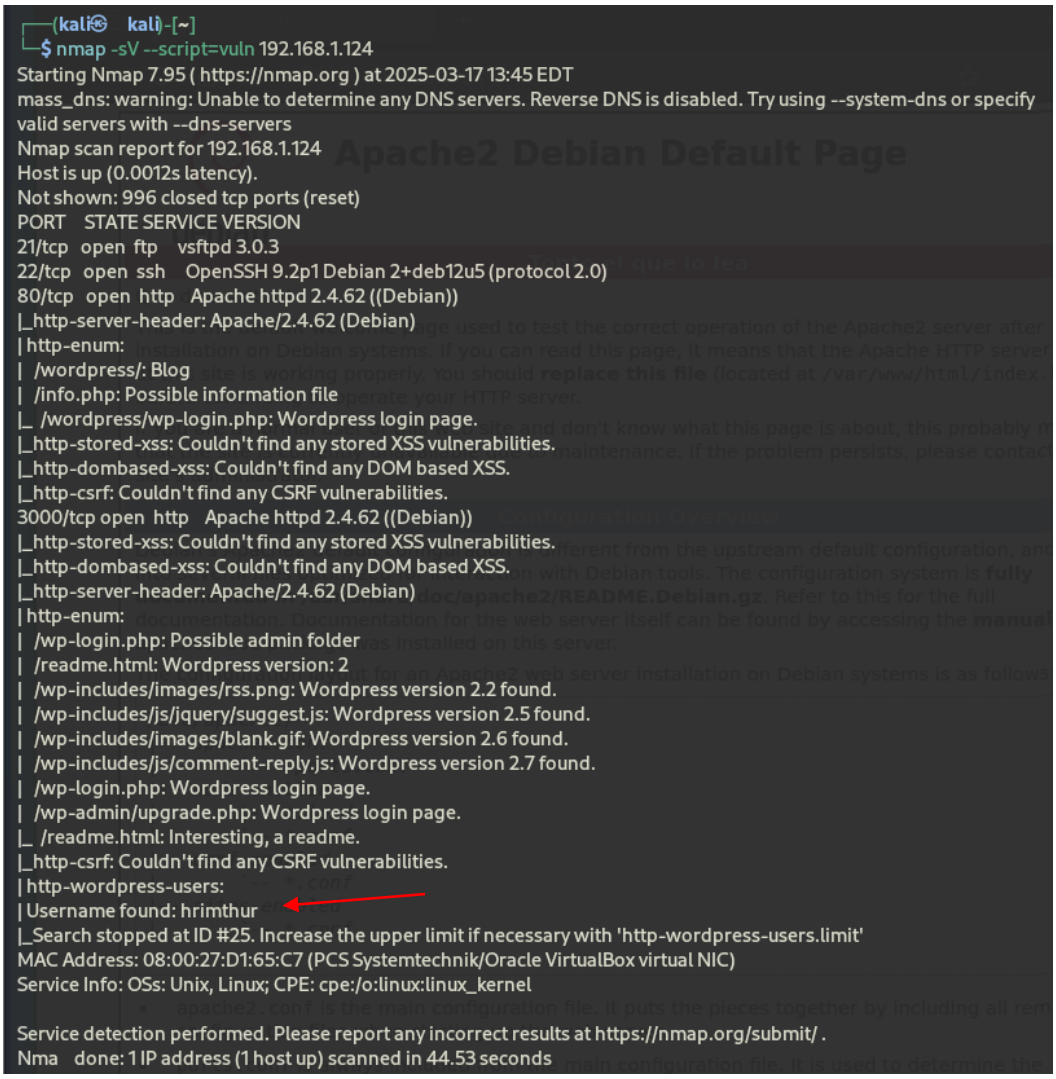
nmap –sV 192.168.1.124



Podemos apreciar en qué puertos se están corriendo los servicios, en este caso ftp, ssh y http, este último mediante dos puertos distintos. Junto a sus versiones.

A continuación, vamos a ejecutar un comando un poco más exhaustivo para que nos brinde mayor información. Nmap cuenta con scripts preestablecidos, uno de ellos tiene el propósito de listar las posibles vulnerabilidades de las versiones.

nmap –script=vuln 192.168.1.124



Podemos observar como aparte de las vulnerabilidades de las versiones que se están ejecutando, ha encontrado posibles vulnerabilidades en la página web Wordpress, incluso nos ha facilitado un nombre de usuario que ha detectado, hrimthur.

Tabla de vulnerabilidades

Puerto	Servicio	Versión	Descripción	Referencia	Nivel de Riesgo
21	ftp	Vsftpd 3.0.3	Permite a los atacantes provocar una denegación de servicio debido a un número limitado de conexiones permitidas.	Link a CVE	**Alto**

Puerto	Servicio	Versión	Descripción	Referencia	Nivel de Riesgo
22	Ssh	OpenSSH 9.2p	No se han encontrado vulnerabilidades de esta versión, la más reciente que presentaba problemas era la versión 9.0p1		**Ninguno**
80	http	Apache httpd 2.4.62	Permite filtrar hashes NTML a un servidor malicioso mediante SSRF y solicitudes maliciosas.	Link a CVE	**Alto**
3000	http	Apache httpd 2.4.62	En ciertas circunstancias donde se solicitan archivos indirectamente, provocan la divulgación del código fuente de contenido local.	Link a CVE	**Medio**

Aquí dejo todo el ouput del comando ejecutado por si lo quieres examinar más detenidamente.

nmap –script=vuln 192.168.1.124

Starting Nmap 7.95 (https://nmap.org) at 2025-03-17 13:45 EDT

mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers

Nmap scan report for 192.168.1.124

Host is up (0.0012s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)

80/tcp open http Apache httpd 2.4.62 ((Debian))

|_http-server-header: Apache/2.4.62 (Debian)

| http-enum:

| /wordpress/: Blog

| /info.php: Possible information file

|_ /wordpress/wp-login.php: Wordpress login page.

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

3000/tcp open http Apache httpd 2.4.62 ((Debian))

|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

|_http-dombased-xss: Couldn't find any DOM based XSS.

|_http-server-header: Apache/2.4.62 (Debian)

| http-enum:

| /wp-login.php: Possible admin folder

| /readme.html: Wordpress version: 2

| /wp-includes/images/rss.png: Wordpress version 2.2 found.

| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.

| /wp-includes/images/blank.gif: Wordpress version 2.6 found.

| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.

| /wp-login.php: Wordpress login page.

| /wp-admin/upgrade.php: Wordpress login page.

|_ /readme.html: Interesting, a readme.

|_http-csrf: Couldn't find any CSRF vulnerabilities.

| http-wordpress-users:

| Username found: hrimthur

|_Search stopped at ID #25. Increase the upper limit if necessary with 'http-wordpress-users.limit'

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

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 44.53 seconds