

REPORTE DE VULNERABILIDAD

Fecha: 19 de febrero de 2025

Autor: Marcos Maldonado Eremia.

Objetivo: Evaluar la seguridad de la máquina con IP [192.168.1.10](#) mediante un escaneo con Nmap para identificar puertos abiertos, servicios activos y posibles vulnerabilidades.

1. Instalación y Uso de Nmap

Para realizar el escaneo, primero nos aseguramos de que Nmap esté instalado en la máquina Kali Linux:

```
“sudo apt-get install nmap”
```

Una vez instalado, ejecutamos los siguientes comandos para el análisis:

2. Escaneo de Puertos y Servicios

Se ejecutó un escaneo básico a la IP objetivo:

```
“nmap 192.168.1.10”
```

Resultado: Se identificó que el host está activo y tiene servicios corriendo.

Para identificar los servicios y versiones, ejecutamos:

```
“nmap -sV 192.168.1.10”
```

Resultados obtenidos:

- **Puerto 80/tcp abierto**
- **Servicio: Apache HTTPD 2.4.62 (Debian)**
- **Dirección MAC: 08:00:27:D1:65:C7 (VirtualBox NIC)**

3. Escaneo de Vulnerabilidades

Se realizó un escaneo con scripts de detección de vulnerabilidades:

```
“nmap -sV --script=vuln 192.168.1.10”
```

Resultados:

- Se detectaron versiones de WordPress antiguas en varias rutas:
 - WordPress 2.2, 2.5, 2.6, 2.7
 - WordPress principal en versión 6.7.1
- No se encontraron vulnerabilidades CSRF o XSS conocidas en la versión de Apache detectada.

Captura de pantalla del escaneo:

```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
root@kali)-[/home/kali]
# nmap -sV 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 14:14 EST
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0020s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:D1:65:C7 (PCS Systemtechnik/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 13.18 seconds

root@kali)-[/home/kali]
# nmap -sV --script=vuln 192.168.1.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 14:15 EST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|   Hosts are all up (not vulnerable).
Nmap scan report for 192.168.1.10 (192.168.1.10)
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-server-header: Apache/2.4.62 (Debian)
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-enum:
|   /wordpress/: Blog
|   /wp-login.php: Possible admin folder
|   /readme.html: Wordpress version: 2
|   /: Wordpress version: 6.7.1
|   /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.
|   /wordpress/wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|   /readme.html: Interesting, a readme.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
|_ http-wordpress-users:
|   Username found: thefogcold4geeks-com
|_ 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 detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.41 seconds

root@kali)-[/home/kali]
#
```

4. Búsqueda de Vulnerabilidades

Para los servicios detectados, se realizó una búsqueda en bases de datos públicas:

- **Apache 2.4.62:**
 - Se recomienda revisar en la NVD: <https://nvd.nist.gov/>
 - También en CVE Details: <https://www.cvedetails.com/>
 - **WordPress versiones antiguas (2.2 - 2.7):**
 - Históricamente, estas versiones han sido vulnerables a ataques de ejecución remota de código y XSS.
 - Se recomienda verificar en la Exploit Database: <https://www.exploit-db.com/>
-

5. Conclusiones y Recomendaciones

- **Actualizar Apache HTTPD** a la última versión estable.
 - **Actualizar WordPress** a la versión más reciente para mitigar vulnerabilidades conocidas.
 - **Habilitar un firewall** para restringir el acceso a puertos no utilizados.
 - **Revisar los permisos de acceso** en las páginas de administración de WordPress.
 - **Monitorear registros de acceso** para detectar posibles intentos de explotación.
-