Reporte de Escaneo Nmap con Detección de Vulnerabilidades

Información general

- IP objetivo: **192.168.1.8**
- Host activo con baja latencia (0.0016s - 0.0025s)
- MAC Address: 08:00:27:D1:65:C7 (Oracle VirtualBox virtual NIC)
- Nmap versión: 7.95

Puertos y servicios detectados (`-sV`)

Puerto	Estado	Servicio	Versión
80/tcp	abierto	HTTP	Apache httpd 2.4.62 (Debian)

Resultados del escaneo con scripts de vulnerabilidades (`--script=vuln`)

- **broadcast-avahi-dos (CVE-2011-1002):**
  - Detectó hosts multicast (224.0.0.251)
  - Resultado: **No vulnerable** (hosts activos pero no afectados)
- **http-stored-xss:**
  - No se encontraron vulnerabilidades de Cross Site Scripting almacenado
- **http-csrf:**
  - No se encontraron vulnerabilidades de Cross-Site Request Forgery
- **http-dombased-xss:**
  - No se encontraron vulnerabilidades de XSS basadas en DOM
- **http-server-header:**
  - Servidor web reporta encabezado: `Apache/2.4.62 (Debian)`
- **http-enum:**
  - Se detectó la ruta `/wordpress/` indicando un blog Wordpress
  - También detectada la página de login: `/wordpress/wp-login.php`

Análisis y recomendaciones

- El servidor corre Apache 2.4.62, que debe mantenerse actualizado para mitigar vulnerabilidades conocidas.
- No se detectaron vulnerabilidades XSS ni CSRF con los scripts estándar de Nmap.
- La presencia de Wordpress indica que se debe revisar la versión y plugins instalados, ya que Wordpress es un vector común de ataques si no se mantiene actualizado.
- Revisar configuraciones de seguridad y acceso para `/wordpress/wp-login.php` para evitar ataques de fuerza bruta o explotación.
- Mantener monitoreo y realizar escaneos periódicos para detectar nuevas vulnerabilidades.