# Informe de Seguridad Generado por Molly AI

## Sesión: Escaneo_IP_190_119_84_12

Fecha de Generación: 2025-07-24 21:24:00

# Resumen de Escaneo de Red - Sesión: Escaneo_IP_190_119_84_12

**Tipo de Escaneo:** Network Scan

**Objetivo:** 190.119.84.12

**Fecha de Inicio:** 2025-07-24T21:22:35.691332

**Estado:** completed

**Fecha de Finalización:** 2025-07-24T21:24:00.218764

**Resumen:** ¡Hola! El escaneo de red en 190.119.84.12 ha finalizado. He analizado los resultados y aquí te presento un resumen de los hallazgos:

Se detectó un único host activo en la dirección IP 190.119.84.12, ejecutando varios servicios. A continuación, te detallo los servicios encontrados, las vulnerabilidades detectadas y las recomendaciones para mitigar los riesgos:

**1. SSH (Puerto 22 y 2222): OpenSSH 8.9p1 Ubuntu 3ubuntu0.13**

* **Vulnerabilidades:** Se detectaron varias vulnerabilidades, incluyendo CVE-2007-2768, CVE-2008-3844, CVE-2023-28531, CVE-2023-38408 y CVE-2023-48795. Estas vulnerabilidades podrían permitir a atacantes obtener información de usuario, ejecutar código remotamente, o incluso comprometer la integridad de la conexión SSH. (Puedes preguntarme sobre cualquier CVE en particular, por ejemplo: "¿Qué es CVE-2023-38408?")

* **Mitigación:** Actualiza inmediatamente a OpenSSH 9.6 o una versión superior con soporte activo. Implementa la autenticación por claves públicas en lugar de contraseñas. Revisa y refuerza la configuración de tu firewall.

**2. HTTP (Puerto 80): OpenResty web app server**

* **Vulnerabilidades:** No se han detectado vulnerabilidades específicas con la información proporcionada.

* **Mitigación:** Asegúrate de usar la última versión de OpenResty. Configura HTTPS (SSL/TLS) con un certificado válido para encriptar el tráfico. Revisa y aplica las mejores prácticas de seguridad para servidores web, incluyendo la protección contra ataques comunes como inyección SQL y XSS.

**3. HTTPS (Puerto 443): openresty**

* **Vulnerabilidades:** No se han detectado vulnerabilidades específicas con la información proporcionada.

* **Mitigación:** Similar al servicio HTTP, asegúrate de tener un certificado SSL/TLS válido, una configuración segura para OpenResty, y protecciones contra ataques comunes a servidores web.

**4. MySQL (Puerto 3306): MySQL 8.0.42-0ubuntu0.22.04.1**

* **Vulnerabilidades:** Se detectaron CVE-2009-2942 y CVE-2017-12419.

* **Mitigación:** Aunque la versión es relativamente reciente, actualiza a la última versión de MySQL para parchear las vulnerabilidades conocidas. Implementa prácticas de seguridad como contraseñas fuertes, control de acceso estricto, y auditoría de la base de datos.

**5. PostgreSQL (Puerto 5432): PostgreSQL 9.6.0 o superior**

* **Vulnerabilidades:** Se detectaron varias vulnerabilidades en versiones anteriores de PostgreSQL (CVE-2009-2943, CVE-2010-3781, CVE-2017-7548, CVE-2018-1053, CVE-2018-1058). La versión exacta no se conoce, pero dado que 9.6 ya no cuenta con soporte, es altamente probable que existan vulnerabilidades.

* **Mitigación:** Actualiza inmediatamente a una versión de PostgreSQL con soporte a largo plazo (LTS). Configura la base de datos con contraseñas fuertes, control de acceso estricto y un firewall adecuado.

**6. HTTP (Puerto 8000): Jetty**

* **Vulnerabilidades:** No se han detectado vulnerabilidades específicas sin conocer la versión de Jetty.

* **Mitigación:** Actualiza a la última versión de Jetty e implementa buenas prácticas de seguridad para servidores web, incluyendo HTTPS.

En resumen, la actualización de tu software a las últimas versiones disponibles es crucial para mejorar tu postura de seguridad. No dudes en preguntarme cualquier duda sobre los CVEs encontrados o sobre otras cuestiones de seguridad.

# Hosts Descubiertos y Servicios Abiertos

## Host: 190.119.84.12 (190.119.84.12)

**SO:** None

**Servicios Abiertos:**

- Puerto: 22/tcp (ssh vOpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)) Estado: open
- Puerto: 80/tcp (http vOpenResty web app server) Estado: open
- Puerto: 443/tcp (ssl v/https openresty) Estado: open
- Puerto: 2222/tcp (ssh vOpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)) Estado: open
- Puerto: 3306/tcp (mysql vMySQL 8.0.42-0ubuntu0.22.04.1) Estado: open
- Puerto: 5432/tcp (postgresql vPostgreSQL DB 9.6.0 or later) Estado: open
- Puerto: 8000/tcp (http vJetty) Estado: open