**Reporte de Vulnerabilidades - Escaneo Nmap**

**Información General**

* **Fecha del escaneo:** 04 de febrero de 2025
* **Dirección IP del objetivo:** 10.0.2.15
* **Sistema Operativo detectado:** Unix

**Número total de puertos detectados:**

* + 968 puertos filtrados (sin respuesta)
  + 30 puertos cerrados (reset)
  + 2 puertos abiertos

**Texto

Descripción generada automáticamente**

**Puertos Abiertos y Servicios Detectados**

**1. Puerto 21/tcp (FTP)**

* **Servicio:** vsftpd 3.0.3
* **Vulnerabilidades Detectadas:**
  + **CVE-2021-30047** (Severidad: 7.5)
    - Referencia: CVE-2021-30047
  + **CVE-2021-3618** (Severidad: 7.4)
    - Referencia: CVE-2021-3618

**2. Puerto 80/tcp (HTTP)**

* **Servicio:** Apache httpd 2.4.62 (Debian)
* **Encabezado del Servidor:** Apache/2.4.62 (Debian)
* **Vulnerabilidades Analizadas:**
  + **DOM-based XSS:** No se encontraron vulnerabilidades
  + **CSRF:** No se encontraron vulnerabilidades
  + **Stored XSS:** No se encontraron vulnerabilidades
* **Recursos Detectados:**
  + **WordPress detectado** en el directorio raíz /wordpress/
  + **Página de inicio de sesión de WordPress:** /wordpress/wp-login.php

**Texto

Descripción generada automáticamente**

**Conclusiones y Recomendaciones**

1. **Actualizar vsftpd a la última versión disponible** para mitigar las vulnerabilidades CVE-2021-30047 y CVE-2021-3618.
2. **Revisar la configuración de seguridad de Apache** para evitar posibles ataques aún no identificados en esta versión.
3. **Verificar la seguridad del sitio WordPress**, asegurando que esté actualizado y protegido contra ataques comunes como fuerza bruta y explotación de plugins vulnerables.
4. **Realizar pruebas adicionales** para detectar posibles vulnerabilidades que no fueron identificadas en este escaneo inicial.