# Informe del Escaneo 1

Aquí está el informe de seguridad basado en los resultados del escaneo:

Estado general de seguridad:

El servidor parece estar razonablemente seguro. Se encontraron algunos puertos abiertos, lo que es normal para un servidor web en funcionamiento. Sin embargo, es importante estar atento a posibles vulnerabilidades y mantener el software actualizado.

Vulnerabilidades encontradas:

- El servidor FTP (ProFTPD) debe actualizarse a la última versión disponible para corregir posibles vulnerabilidades conocidas.
- Se recomienda habilitar la autenticación SPF y DKIM para los servidores SMTP (Postfix) para mejorar la seguridad del correo electrónico.
- El servidor MySQL expone una versión antigua (5.5.5-10.5.8-MariaDB-1:10.5.8+maria~buster) que puede tener vulnerabilidades conocidas. Se recomienda actualizar a la última versión.

Usuarios detectados:

No se encontraron usuarios específicos en el escaneo, pero se

identificaron varios servicios que pueden requerir autenticación, como FTP, SMTP, POP3 e IMAP.

Plugins o temas problemáticos:

No se aplicó, ya que no se trata de un sitio web WordPress.

Recomendaciones básicas:

- Mantenga todos los software del servidor actualizados a las últimas versiones para corregir posibles vulnerabilidades.
- Restrinja el acceso a los puertos y servicios que no sean necesarios para el funcionamiento del servidor.
- Utilice contraseñas seguras y únicas para cada cuenta de usuario y habilite la autenticación de dos factores siempre que sea posible.
- Considere la implementación de un firewall para agregar una capa adicional de seguridad.
- Realice escaneos de seguridad regulares para identificar y corregir posibles vulnerabilidades emergentes.