# Pruebas de seguridad

| | |
|---|---|
| Estado | Done |
| Fecha Inicio | @6 de octubre de 2023 |
| № ID | CAL-12 |
| Fecha última edición | @26 de octubre de 2023 17:01 |

## Objetivos

- Identificar posibles vulnerabilidades en la aplicación o sitio web.
- Asegurarnos de que todas las actualizaciones de seguridad y parches estén aplicados en el servidor y en la aplicación.

Podemos realizar un análisis de seguridad utilizando herramientas como OWASP ZAP o Nessus e identificar posibles vulnerabilidades en la página http://impetu.com.co/ construida en Odoo.

OWASP ZAP es una herramienta de código abierto específicamente diseñada para pruebas de seguridad de aplicaciones web.

Nessus por otra parte es una herramienta más completa, conocida por su amplia base de datos de vulnerabilidades y su capacidad para realizar escaneos automatizados y programados, adicionalmente puede utilizarse en una variedad de escenarios, no solo en aplicaciones web.

La tarea de mapear vulnerabilidades consiste en identificar y analizar las vulnerabilidades en los sistemas de la red objetivo, como pretendemos realizar un escaneo más amplio de sistemas y redes instalaremos Nessus siguiendo estos pasos:

1. Descargar e instalar la herramienta de Nessus, seleccionando el instalador de 64 bits.

   https://www.tenable.com/downloads/nessus?_gl=1*18xyt4e*_ga*OTY2OTY0MjQ4LjE2OTY5NDMwNzI.*_ga_HSJ1XWV6ND*MTY5Njk0MzE3MC4xLjEuMTY5Njk0MzM0

   Verificamos que el archivo se encuentre en la carpeta de Descargas, abrimos la terminal y ejecutamos los comandos:

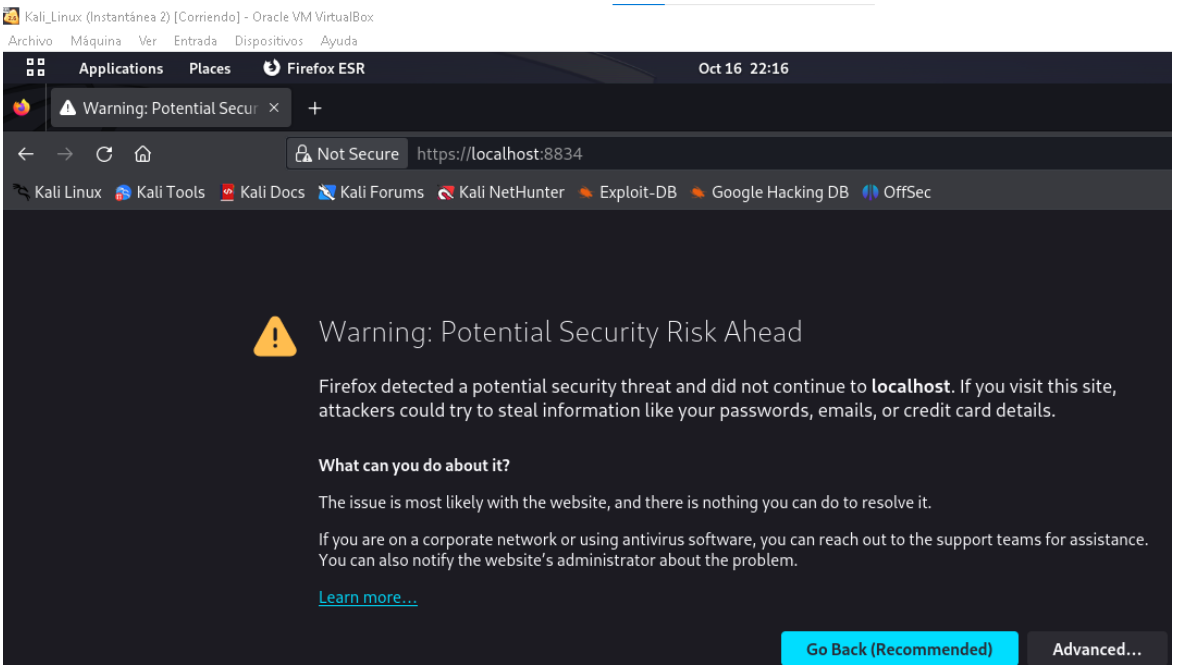
   ```
   cd Dercargas
   #Listamos el contenido
   ls
   #Instalamos Nessus
   sudo dpkg -i Nessus-10.6.1-ubuntu1404_amd64.deb
   #Ingresamos la contraseña y esperamos que finalice el proceso
   ```

2. Abrir la herramienta y configúrala para realizar un escaneo de seguridad en la URL de la página http://impetu.com.co/.

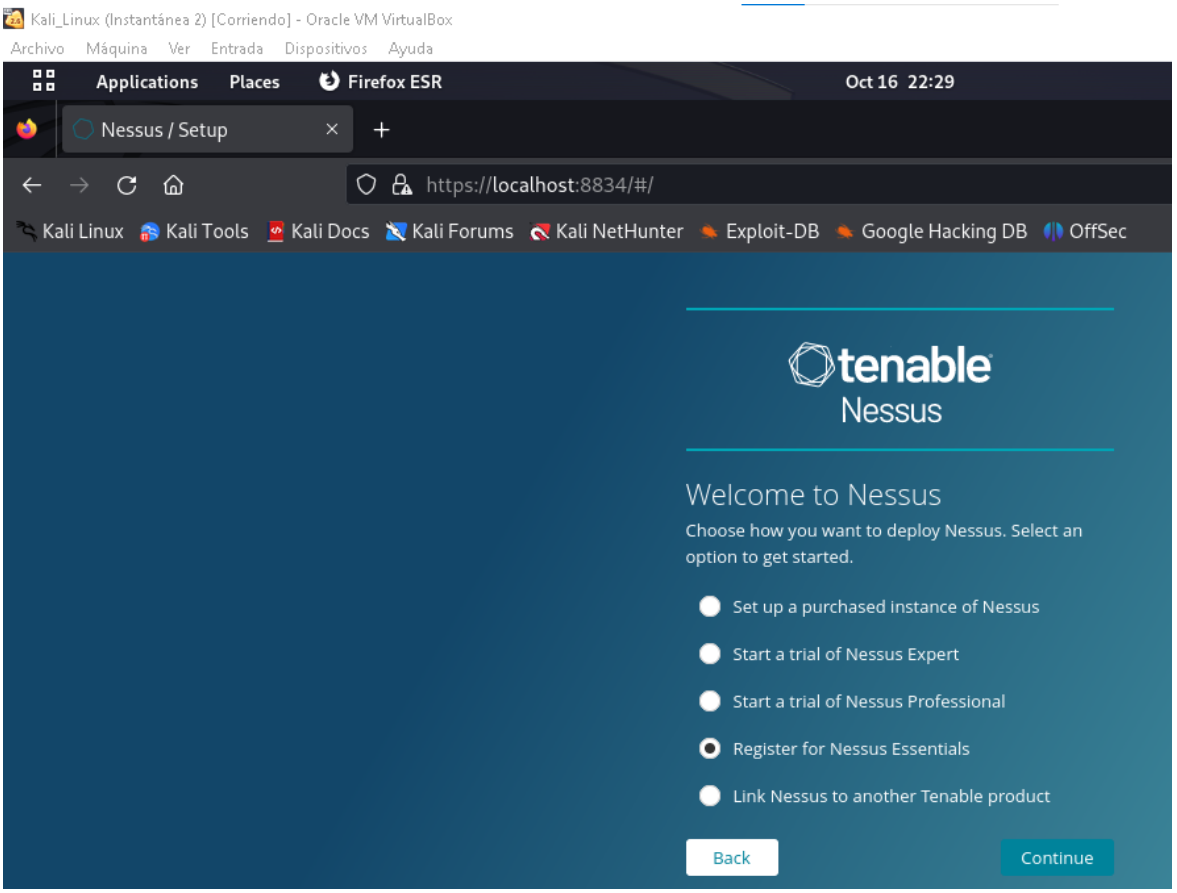
→ Para usar la herramienta (Nessus Esentials) es necesario registrarnos en el sitio https://es-la.tenable.com/products/nessus/nessus-essentials con nuestro email para generar un código de activación del programa

```
#Iniciamos el servicio
sudo /bin/systemctl start nessusd.service
```

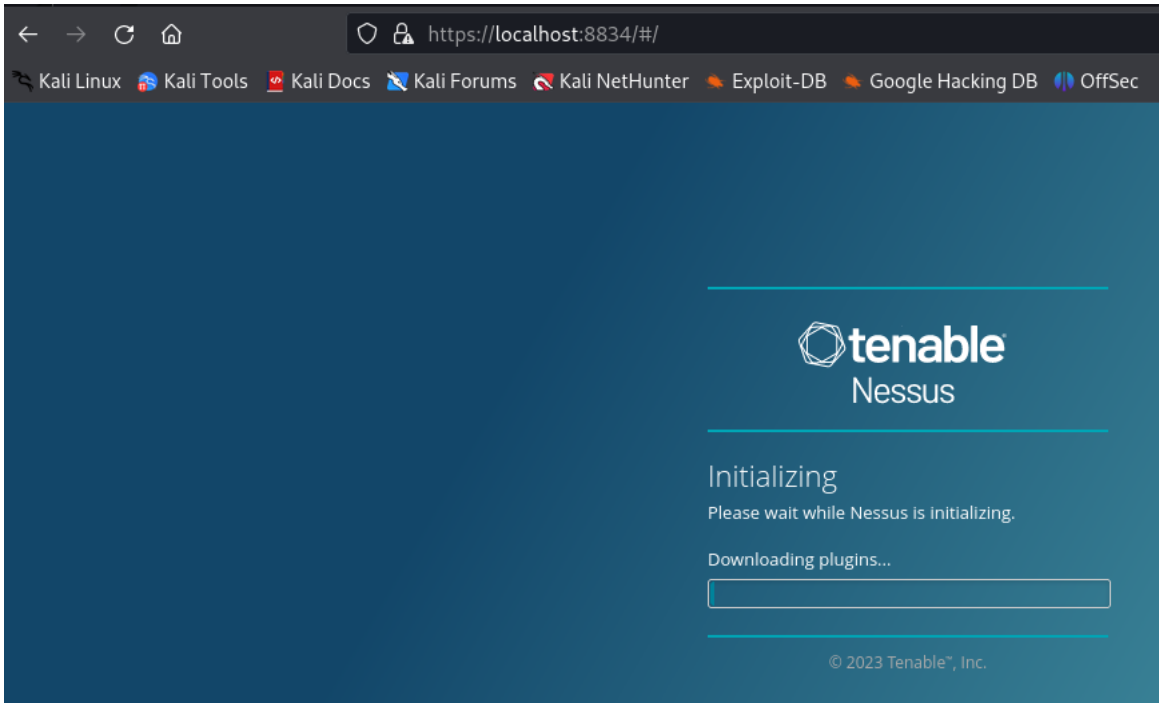
→ Con el servicio iniciado , abrimos un navegador e ingresamos a Nessus: **https://localhost:8834, clic** en "Advanced" y luego en "Accept the Risk and Continue" para ir a Nessus**:**



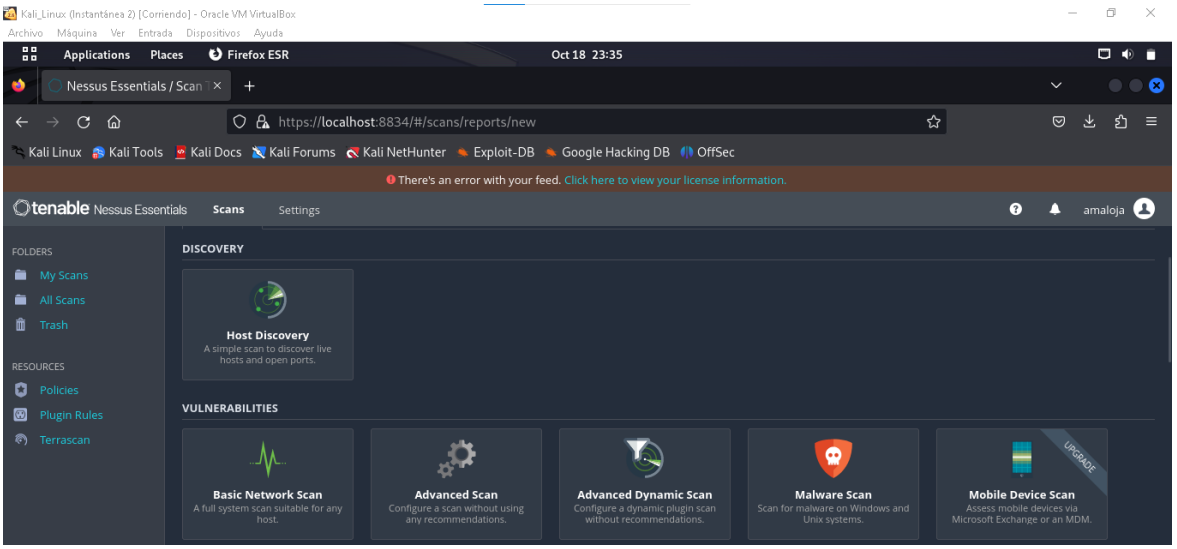

→ Seleccionamos **"Nessus Essentials"**



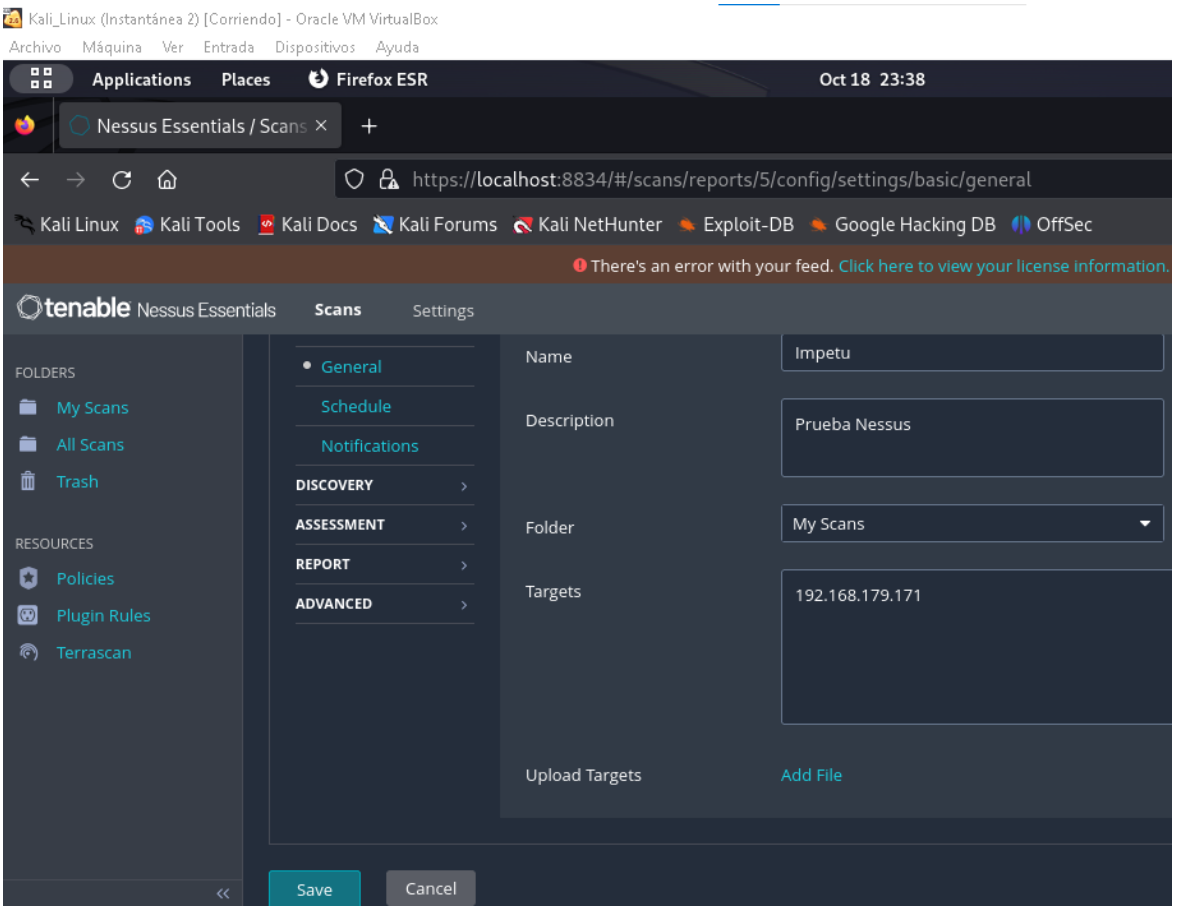

→ En este punto es necesario ingresar el código de activación y crear un usuario para usar el programa, posterior a ello se lleva a cabo el proceso de compilación de los componentes:




→ Damos clic en **"New Scan"** y seleccionamos el tipo de escaneo a usar, como vemos las opciones son variadas:




→ Damos clic en **"Basic Network Scan"** para un escaneo básico e ingresamos los detalles del escaneo con la IP objetivo

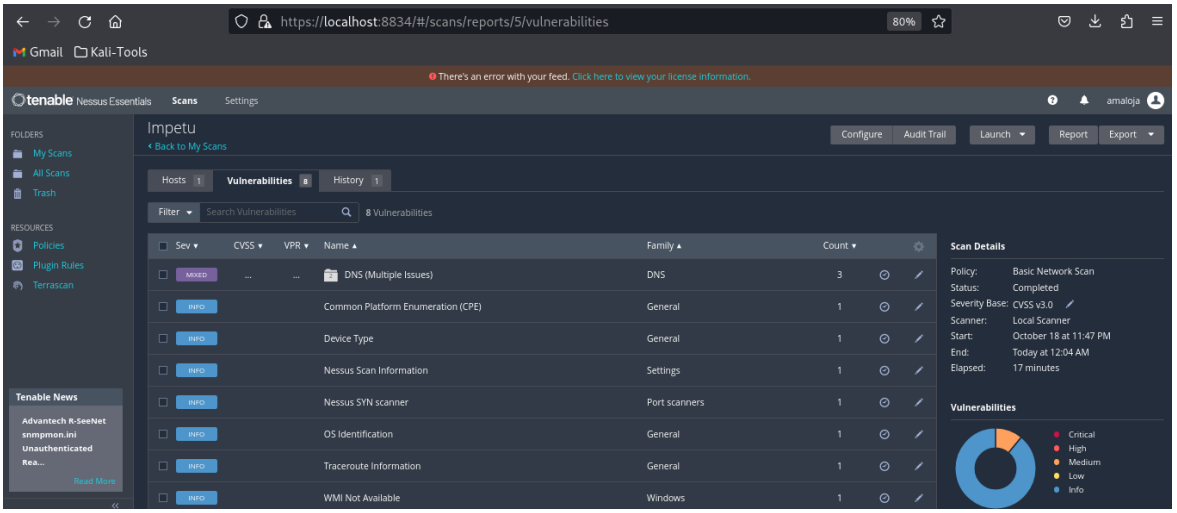



→ Damos clic en **"Save"** para guardar este proyecto

3. Iniciar el escaneo de seguridad para que la herramienta analice la página en busca de posibles vulnerabilidades.

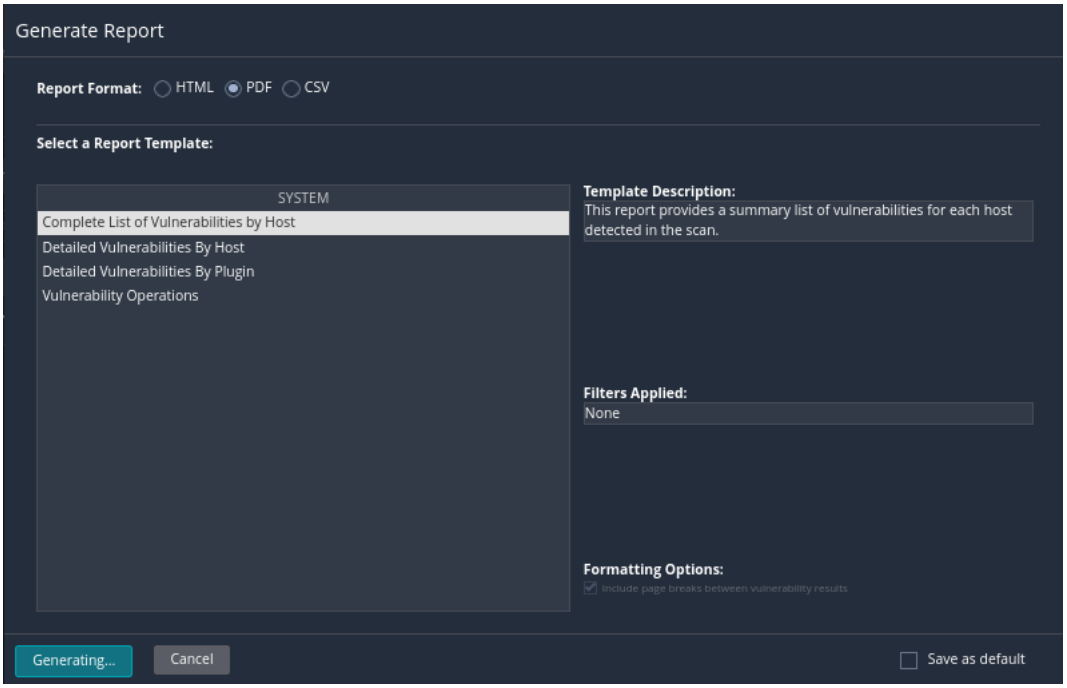
   → Damos clic en el icono **"Launch"** para iniciar el escaneo en el equipo de destino

   → Esperamos que el escaneo sea realizado, al finalizar pulsamos sobre el objetivo para ver las vulnerabilidades encontradas



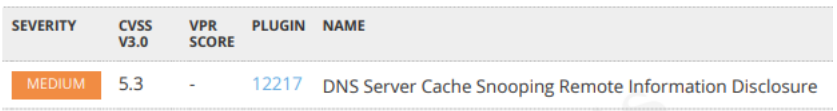

4. Una vez finalizado el escaneo, revisar los resultados proporcionados por la herramienta, los podemos obtener dando clic a **Report.** Esto incluirá una lista de posibles vulnerabilidades encontradas en la página.

   Cada una estará dividida por colores en base a su nivel de riesgo indicando la cantidad y al lado podemos ver una representación de estas, damos clic sobre alguna sección para ver más específicamente las vulnerabilidades detectadas:




5. Analizamos cada vulnerabilidad identificada y tomamos las medidas necesarias para solucionarlas. Esto puede implicar aplicar actualizaciones de seguridad y parches en el servidor y en la aplicación Odoo.

Impetu_Nessus.pdf



La respuesta que se obtuvo del escaneo Nessus indica que se ha encontrado una vulnerabilidad en el servidor DNS de la dirección IP del dominio impetu.com.co, veamos lo que significa esta respuesta:

1. **Severity (Severidad):** El nivel de severidad de la vulnerabilidad es "medio", lo que sugiere que la vulnerabilidad no es extremadamente crítica, pero aún es importante abordarla.
2. **CVSS (Sistema de puntuación de vulnerabilidad común):** La puntuación CVSS es 5,3. CVSS es un sistema de puntuación estandarizado que se utiliza para evaluar la gravedad de las vulnerabilidades. Una puntuación de 5.3 se encuentra en el rango medio de severidad.
3. **Plugin 12217:** El número de plugin, en este caso, es 12217, lo que corresponde a una entrada específica en la base de datos de vulnerabilidades de Nessus. Cada número de complemento se relaciona con un tipo particular de vulnerabilidad o prueba.
4. **Nombre (Name):** El nombre de la vulnerabilidad es "Divulgación remota de información de snooping de caché del servidor DNS". Esto significa que la vulnerabilidad se refiere a la capacidad de un atacante para realizar "DNS Server Cache Snooping", lo que puede llevar a la divulgación de información remota.

- **DNS Server Cache Snooping (Espionaje de la caché del servidor DNS):** DNS Server Cache Snooping es una técnica que permite a un atacante consultar la caché de un servidor DNS para obtener información confidencial sobre los registros DNS almacenados en el servidor. Esto puede incluir información sobre los nombres de dominio, las direcciones IP y otros detalles sensibles.
- **Remote Information Disclosure (Divulgación remota de información):** Esto significa que un atacante, de manera remota, podría acceder a la información confidencial que se encuentra en el servidor DNS al aprovechar esta vulnerabilidad. La divulgación de esta información puede ser perjudicial y se considera una amenaza para la seguridad.

En resumen, la vulnerabilidad encontrada (DNS Server Cache Snooping) podría permitir a un atacante obtener información confidencial almacenada en el servidor DNS, y su severidad se califica como "media" con una puntuación CVSS de 5.3. Para abordar esta vulnerabilidad, es importante tomar medidas para corregirla y asegurarse de que el servidor DNS esté configurado de manera segura.