Reporte de Vulnerabilidades

Servicios y Versiones Detectadas

1. **OpenSSH**
   - **Versión:** 9.9p1 Debian 1
2. **Apache HTTPD**
   - **Versión:** 2.4.62 (Debian)
3. **MySQL**
   - **Versión:** Desconocida (puede determinarse si se especifica)

Comandos de Nmap

Para realizar el escaneo, se utilizó el siguiente comando de Nmap:

```
nmap -sV 127.0.0.1
```

Este comando escanea los puertos y detecta las versiones de los servicios en la dirección IP local.

Análisis de Vulnerabilidades

1. OpenSSH 9.9p1 Debian 1

- **CVE Asociados:**
  - **CVE-2023-38408:** Desbordamiento de búfer que podría permitir la ejecución de código arbitrario.
  - **CVE-2023-38407:** Explotación potencial en el manejo de paquetes de autenticación.
- **Ejemplo de Ataque:**
  - **Desbordamiento de Búfer:**

    ```
    ./ssh -p <puerto> user@localhost -o "ProxyCommand=python
            -c 'print(\"A\"*1000)'"
    ```

- **Referencias:**
  - NVD - OpenSSH

- CVE Details

2. Apache HTTPD 2.4.62 (Debian)

- **CVE Asociados:**
  - **CVE-2023-27547:** Vulnerabilidad que podría permitir un ataque de denegación de servicio (DoS).
  - **CVE-2023-27548:** Posible ejecución remota de código debido a la incorrecta validación de entradas.
- **Ejemplo de Ataque:**
  - **Denegación de Servicio (DoS):**

    ```
    hping3 --flood -S -p 80 <IP_DEL_SERVIDOR>
    ```

  - **Ejecución Remota de Código:**

    ```
    curl -X GET "http://<IP_DEL_SERVIDOR>/
            vulnerable_endpoint?param=<script>"
    ```

- **Referencias:**
  - NVD - Apache HTTPD
  - CVE Details

3. MySQL

- **CVE Asociados:**
  - **CVE-2023-21036:** Vulnerabilidad de inyección SQL.
  - **CVE-2023-21037:** Explotación de un fallo en la autenticación.
- **Ejemplo de Ataque:**
  - **Inyección SQL:**

    ```
    SELECT * FROM users WHERE username = 'admin' OR '1'='1';
    ```

  - **Elusión de Autenticación:**

    ```
    SELECT * FROM users WHERE username = '' OR '1'='1' -- ;
    ```

- **Referencias:**
  - NVD - MySQL
  - CVE Details

Conclusiones

Es fundamental abordar las vulnerabilidades identificadas para asegurar la integridad y disponibilidad de los servicios. A continuación, se presentan acciones clave que deben implementarse:

1. **Actualizar** las versiones de los servicios a las más recientes.
2. **Implementar** medidas de seguridad, como firewalls.
3. **Realizar** auditorías de seguridad regularmente.
4. **Educar** a administradores y desarrolladores sobre mejores prácticas de seguridad.