Reporte de Vulnerabilidades

Servicios y Versiones Detectadas

- Apache HTTPD
  Versión: 2.4.62 (Debian)

Comandos de Nmap

Para realizar el escaneo, utilizamos el siguiente comando de Nmap:

`nmap -sV --script=vuln 192.168.1.10`

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

Análisis de Vulnerabilidades

1. **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 80 192.168.1.10`
  - Ejecución Remota de Código:
    `curl -X GET "[http://192.168.1.10/vulnerable](http://192.168.1.10/vulnerable)\_endpoint?param=\<script\>"`
- **Referencias:**
  - NVD - Apache HTTPD
  - CVE Details

1. **WordPress Detectado**

- Ruta detectada: /wordpress/
- Acceso de login: /wordpress/wp-login.php

Descripción:

Se identificó la presencia del CMS WordPress, accesible desde la red. Esta plataforma, aunque sencilla y flexible, es también objetivo frecuente de ataques, especialmente si no está actualizada o si se utilizan plugins vulnerables.

- **CVE Asociados:**
  - CVE-2023-2745: Escalada de privilegios que permite a usuarios con permisos bajos ejecutar acciones administrativas.

    - CVE-2023-23488: Vulnerabilidad de tipo XSS persistente que puede ser utilizada para ejecutar scripts maliciosos en el navegador de otros usuarios.
- **Plugins vulnerables:**
  WordPress es altamente dependiente de plugins. Muchos ataques aprovechan fallos conocidos en plugins populares como "Contact Form 7", "Elementor", etc.
- **Ejemplo de Ataque:**
    - Fuerza bruta en login:
      `hydra -l admin -P rockyou.txt http://\<IP\>/wordpress/wp-login.php -V`
    - Inyección SQL vía parámetro vulnerable:
      `id=1' OR '1'='1`

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.