




# Reporte

|   |   |
|---|---|
|  Propietario |  Ayala Arroyo Raúl |
|  Etiquetas   |   |

## Informe de Pruebas de Penetración para Metasploitable v1

### 1. Objetivo y Alcance

El objetivo de esta prueba es identificar y explotar vulnerabilidades en la máquina virtual Metasploitable v1, evaluando la seguridad de sus servicios y analizando posibles brechas explotables.

### 2. Herramientas y Técnicas Utilizadas

- **Nessus:** Escaneo de vulnerabilidades para obtener una lista inicial de servicios y vulnerabilidades potenciales.
- **Nmap:** Herramienta de escaneo de red utilizada para verificar puertos específicos y las versiones de servicios activos.
- **Metasploit:** Framework de explotación utilizado para explotar vulnerabilidades conocidas en servicios y versiones específicos.

### 3. Resultados de Vulnerabilidades Explotadas

A través de los escaneos de Nessus y Nmap, se confirmaron múltiples vulnerabilidades en los servicios clave de la máquina Metasploitable v1.

### 4. Descripción: Listado y Descripción de Cada Vulnerabilidad Encontrada

| Servicio | Puerto | Versión Identificada | Descripción de Vulnerabilidad  |
|----------|--------|----------------------|--|
| FTP      | 21     | vsftpd 2.3.4         | Vulnerabilidad en esta versión que permite una puerta trasera, explotable para obtener acceso no autorizado. |

|             |      |                              |  |
|-------------|------|------------------------------|--|
| <b>DNS</b>  | 53   | ISC BIND 9.4.2               | Vulnerabilidad en la versión de BIND que permite obtener información de versión y posibles explotaciones específicas.    |
| <b>HTTP</b> | 80   | Apache httpd 2.2.8 (Ubuntu)  | Exposición del tipo y versión del servidor web que podría permitir ataques dirigidos a esa versión específica de Apache. |
| <b>HTTP</b> | 8180 | Apache Tomcat/Coyote JSP 1.1 | Exposición del tipo y versión de Tomcat, que podría explotarse mediante ataques contra esta versión del servidor JSP.    |

## 5. Impacto: Evaluación del Impacto de Cada Vulnerabilidad

- **FTP (vsftpd 2.3.4):** La versión de vsftpd 2.3.4 es conocida por su puerta trasera, que permite a los atacantes obtener acceso remoto sin autenticación.
- **DNS (ISC BIND 9.4.2):** La exposición de la versión permite que los atacantes investiguen posibles vulnerabilidades específicas, comprometiendo el servidor DNS y su disponibilidad.
- **HTTP (Apache 2.2.8):** Con la versión de Apache expuesta, los atacantes pueden intentar explotar vulnerabilidades conocidas que podrían dar acceso o permitir ataques de denegación de servicio.
- **HTTP (Apache Tomcat 1.1):** La versión expuesta de Tomcat/Coyote puede ser blanco de ataques para explotar vulnerabilidades de autenticación o ejecución remota de código en aplicaciones JSP.

## 6. Comandos y Herramientas Utilizadas para la Explotación

- **Nmap:** `nmap -sV -p 21,53,80,8180 192.168.100.16` para verificar puertos y versiones específicas de servicios activos.
- **Metasploit Framework:**
  - Exploits utilizados para vsftpd 2.3.4 ( `exploit/unix/ftp/vsftpd_234_backdoor` ) para aprovechar la puerta trasera.

- Modulo para Tomcat ( [exploit/multi/http/tomcat\\_mgr\\_upload](#) ) para subir un archivo y obtener acceso mediante la consola de administración.

## 7. Mitigación

- **FTP (vsftpd 2.3.4):** Actualizar vsftpd a una versión sin puerta trasera, o cambiar a un servidor FTP más seguro.
- **DNS (ISC BIND 9.4.2):** Configurar BIND para ocultar su versión y aplicar las últimas actualizaciones de seguridad.
- **HTTP (Apache 2.2.8):** Actualizar Apache y configurar para no mostrar información de versión o tipo de servidor.
- **HTTP (Apache Tomcat 1.1):** Reforzar el acceso a la consola de Tomcat mediante autenticación más robusta y actualización a una versión segura.