Escanear puertos con nmap

Proyecto: Auditoría de Seguridad en máquina “Metasploit2”

Tipo de Test: Pentesting Interno

Fecha de Ejecución: Enero 2026

Elaborado por: Jose Rodriguez

ÍNDICE

INFORME DE PENTESTING..... 1
ÍNDICE.....2
1. Resumen Ejecutivo.....3
Riesgos Críticos (Máxima Severidad).....4
Riesgos Altos.....4
Riesgos Medios.....4
2. Alcance y Metodología.....4
Alcance del Proyecto.....4
Metodología Utilizada.....5
Faces de Ejecucion.....5
Herramientas Empleadas.....6
3. Resumen de Hallazgos.....7
Clasificación por Severidad.....8
● El CVSS es un estándar abierto que proporciona un método para capturar las características esenciales de una vulnerabilidad y producir una puntuación numérica (de 0 a 10) y una representación textual de su gravedad1.....8
4. Vulnerabilidades Identificadas.....9
Resumen Técnico.....10
Evidencias Técnicas.....11
Escaneo.....11
Revision Web.....12
Revision Source.....13
Escaneo en Busca de Objetos Ocultos.....13
Mapeo de Base de Datos.....14
Injection SQL - Bypass de Autenticación.....14
Informacion recavada.....14
Conexion SSH.....15
Recaudación de Información.....16
Transferencia de Archivos para Análisis.....17
Identificación de Hash.....18
Desencriptación de Hash.....18
Movimiento lateral, Escalación de privilegios.....19
Recabación de información.....20
5. Análisis de Riesgos.....21
6. Recomendaciones de Mitigación.....22

1. Resumen Ejecutivo

El análisis de seguridad realizado sobre el sistema objetivo identificó múltiples debilidades o "vulnerabilidades" que podrían permitir a terceros no autorizados comprometer la integridad y disponibilidad de la información. Estas fallas se deben principalmente al uso de versiones de software obsoletas que no han sido actualizadas y a configuraciones de red que exponen servicios críticos a ataques externos.

A continuación, se presenta un resumen de los hallazgos clasificados por su nivel de peligro:

Riesgos Críticos

Se detectó la presencia de "puertas traseras" en el servicio de transferencia de archivos (FTP) y en el sistema de archivos compartidos (Samba). Estos fallos son extremadamente graves, ya que permiten a un atacante tomar el control total del equipo de forma inmediata, actuando como el administrador principal del sistema y pudiendo robar, modificar o borrar cualquier dato.

Riesgos Altos

El sistema utiliza versiones muy antiguas de servicios de comunicación y bases de datos (como SSH y MySQL). Estas versiones tienen errores conocidos que facilitan la ejecución de comandos dañinos o permiten que un atacante engañe al sistema para entrar sin una contraseña válida, lo que pone en riesgo la privacidad de toda la información almacenada.

Riesgos Medios

Se identificaron componentes que permiten ataques de "denegación de servicio", lo que significa que un intruso podría saturar el sistema hasta dejarlo fuera de línea e inaccesible para los usuarios legítimos. Asimismo, el sistema revela información técnica innecesaria sobre sus cuentas y configuración, lo cual sirve como una "hoja de ruta" para que un atacante planifique ataques más sofisticados.

En conclusión, el estado actual del sistema presenta una exposición severa. Es imperativo actualizar todos los programas a sus versiones más recientes y cerrar los accesos innecesarios para evitar el control total del servidor por parte de cibercriminales.

2. Alcance y Metodología

Alcance del Proyecto

- **Objetivos de la Evaluación**
    - Identificar hosts activos
    - Identificar puertos abiertos en la red
    - Servicios operando en esos puertos
    - Identificar vulnerabilidades en la Servicios detectados
    - Evaluar las debilidades de seguridad.

- **Sistemas y Aplicaciones Incluidas**

Componente	**Dirección IP**
Metasploit2	10.0.2.6

Faces de Ejecucion

- Fase 1: Reconocimiento
- Fase 2: Escaneo y Enumeración

Herramientas Empleadas

Nombre	Fase	Proposito
nmap	Reconocimiento Escaneo y Enumeración	Descubrimiento de la red y Mapeo del objetivo. Se usa para identificar hosts activos, determinar qué puertos están abiertos, qué servicios se están ejecutando y la versión del sistema operativo o servicio.

3. Resumen de Hallazgos

El análisis de seguridad del sistema reveló un total de 10 puertos abiertos con múltiples servicios críticos que presentan un estado de seguridad precario debido a la falta de parches y el uso de software en fin de vida (EOL), lo que clasifica el riesgo global del sistema como Crítico.

Se identificó una vulnerabilidad CRÍTICA (CVSS 9.8) en el servicio vsFTPd 2.3.4 (Puerto 21/tcp), la cual contiene un backdoor (CVE-2011-2523) que permite la ejecución remota de comandos (RCE) con privilegios de root de manera inmediata. De igual forma, los servicios de Samba 3.x (Puertos 139/tcp y 445/tcp) presentan vulnerabilidades CRÍTICAS de desbordamiento de memoria y ejecución remota de código (CVE-2017-7494), permitiendo el compromiso total del sistema de archivos.

En cuanto a la infraestructura de acceso y datos, se detectó una vulnerabilidad de severidad ALTA en el servicio OpenSSH 4.7p1 (Puerto 22/tcp), la cual es susceptible a ataques de enumeración de usuarios y posibles fallos de RCE bajo condiciones específicas (CVE-2023-38408). Adicionalmente, el motor de base de datos MySQL 5.0.51a (Puerto 3306/tcp), al ser una versión obsoleta, es vulnerable a la omisión de autenticación (CVE-2012-2122) y ataques de denegación de servicio (DoS), clasificando el riesgo como ALTO (CVSS 7.8).

Finalmente, se identificaron fallos de seguridad de nivel MEDIO en la capa de aplicación web y servicios HTTP. El servidor Apache 2.2.8 (Puerto 80/tcp) y Tomcat/Coyote 1.1 (Puerto 8180/tcp) presentan susceptibilidad a ataques Slowloris DoS (CVE-2007-6750), permitiendo el agotamiento del pool de conexiones del servidor. También se observó la fuga de información mediante el comando VRFY en el servicio SMTP (Puerto 25/tcp), facilitando la recolección de nombres de usuario válidos para ataques de fuerza bruta posteriores. Es imperativo realizar una actualización mayor del sistema operativo o la migración de servicios a versiones con soporte activo.

4. Vulnerabilidades Identificadas

Puerto	Servicio	Versión de Software	Vulnerabilidad	Descripción	Referencia
21/tcp	ftp	vsftpd 2.3.4	vsFTPd version 2.3.4 backdoor	Puerta trasera en vsftpd 2.3.4 que permite ejecución de comandos como root.	https://www.cvedetails.com/cve/CVE-2011-2523/
22/tcp	ssh	OpenSSH 4.7p1	Vulnerabilidades Múltiples (RCE/Enumeración)	Versión antigua propensa a ejecución remota de código y denegación de servicio.	https://www.cvedetails.com/cve/CVE-2023-38408/
25/tcp	smtp	Postfix smtpd	SMTP Open Relay / VRFY	El comando VRFY permite descubrir nombres de cuentas válidas en el sistema.	https://www.cvedetails.com/cve/CVE-1999-0531/
80/tcp	http	Apache httpd 2.2.8	Apache Multiple Vulnerabilities	Servidor vulnerable a Slowloris DoS y otras fallas de ejecución.	https://www.cvedetails.com/cve/CVE-2007-6750/
139/tcp	netbios-ssn	Samba smbd 3.X	Samba Mangle Vulnerability	Vulnerabilidad en el manejo de archivos que puede llevar a DoS o ejecución.	https://www.cvedetails.com/cve/CVE-2010-2063/
445/tcp	microsoft-ds	Samba smbd 3.X	Samba RCE (SambaCry)	Ejecución remota de código mediante la carga de librerías compartidas.	https://www.cvedetails.com/cve/CVE-2017-7494/
3306/tcp	mysql	MySQL 5.0.51a	MySQL Unauthorized Access	Falla en la verificación de contraseñas que permite el acceso sin credenciales válidas.	https://www.cvedetails.com/cve/CVE-2012-2122/
8180/tcp	http	Apache Tomcat 1.1	Slowloris DOS attack	Ataque que agota los recursos del servidor mediante conexiones parciales abiertas.	https://www.cvedetails.com/cve/CVE-2007-6750/

Resumen Técnico

La evaluación técnica se inició mediante un escaneo exhaustivo de los puertos abiertos en el sistema objetivo para definir la superficie de ataque disponible. Una vez identificados los puntos de entrada activos, se procedió a realizar un análisis de seguridad detallado sobre cada uno de los servicios detectados, verificando rigurosamente las versiones de software en ejecución. Esta fase permitió correlacionar los servicios y sus versiones específicas con vulnerabilidades conocidas (CVEs), estableciendo así la base técnica para determinar los riesgos críticos, altos y medios presentes en la infraestructura.

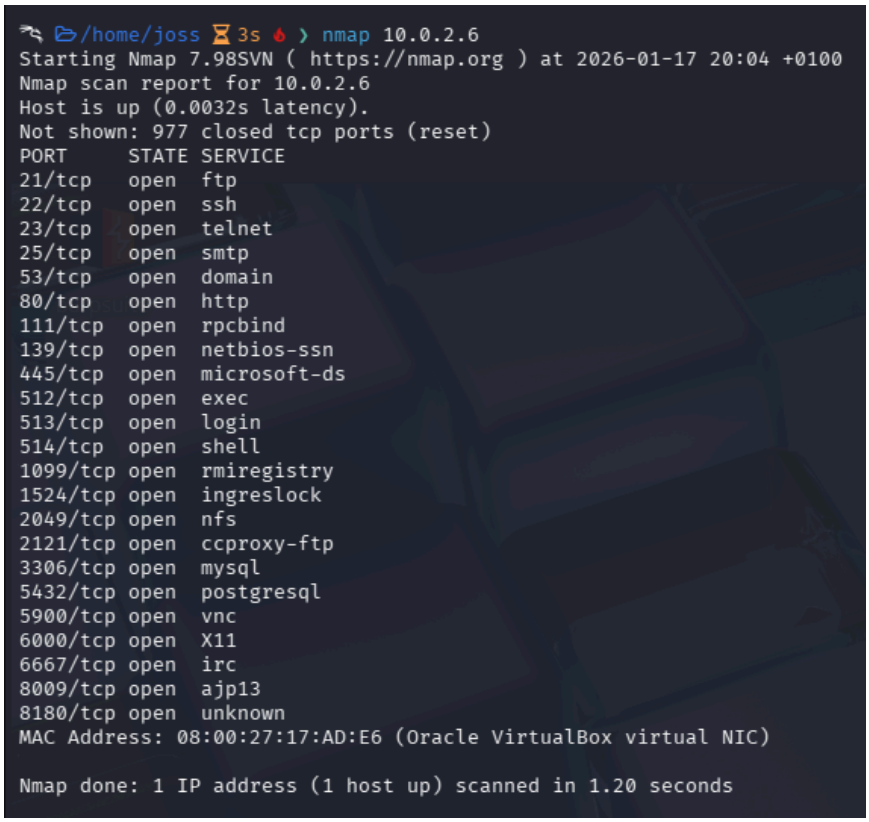
Puntos clave del análisis realizado:

- Identificación de superficie: Determinación de puertos TCP/UDP abiertos.
- Fingerprinting de servicios: Identificación de protocolos (FTP, SSH, HTTP, etc.).
- Análisis de versiones: Verificación de versiones específicas (ej. vsFTDP 2.3.4, Apache 2.2.8) para identificar software obsoleto o vulnerable.

Evidencias Técnicas

Escanear puertos con nmap

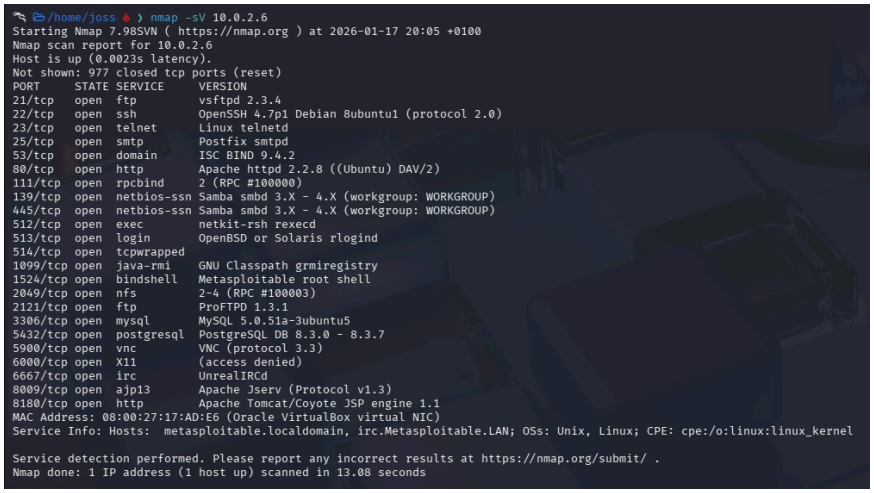
nmap 10.0.2.6



```
/home/joss 3s ❯ nmap 10.0.2.6
Starting Nmap 7.98SVN ( https://nmap.org ) at 2026-01-17 20:04 +0100
Nmap scan report for 10.0.2.6
Host is up (0.0032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:17:AD:E6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.20 seconds
```

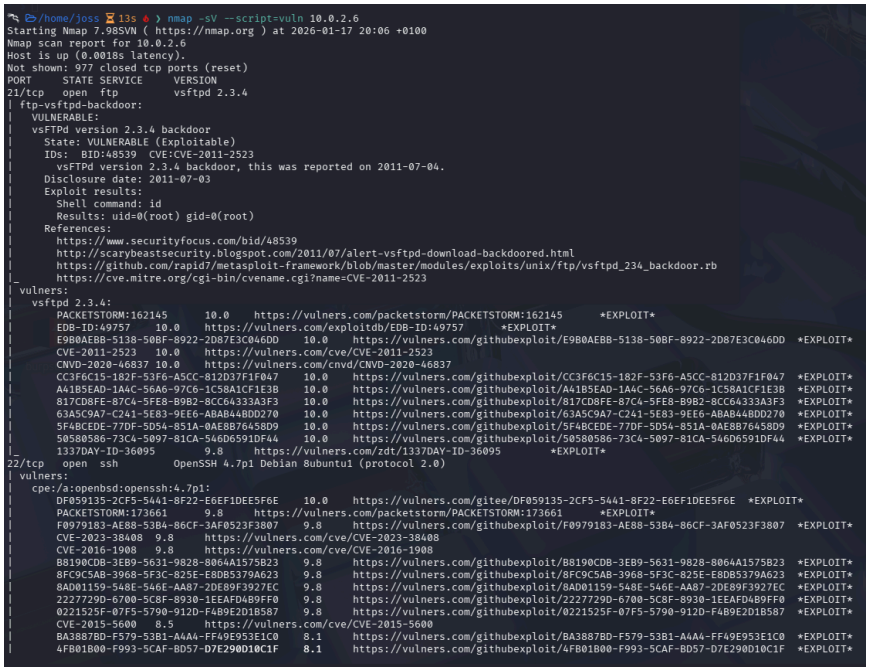
nmap -sV 10.0.2.6



```
/home/joss ❯ nmap -sV 10.0.2.6
Starting Nmap 7.98SVN ( https://nmap.org ) at 2026-01-17 20:05 +0100
Nmap scan report for 10.0.2.6
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:17:AD:E6 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.08 seconds
```

nmap -sV --script=vuln 10.0.2.6



```
/home/joss 13s ❯ nmap -sV --script=vuln 10.0.2.6
Starting Nmap 7.98SVN ( https://nmap.org ) at 2026-01-17 20:06 +0100
Nmap scan report for 10.0.2.6
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| vulners:
|   vsftpd 2.3.4:
|       PACKETSTORM:162145      10.0    https://vulners.com/packetstorm/PACKETSTORM:162145      *EXPLOIT*
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757      *EXPLOIT*
|       E9B0AEBB-5138-50BF-8922-2D87E3C046DD    10.0    https://vulners.com/githubexploit/E9B0AEBB-5138-50BF-8922-2D87E3C046DD  *EXPLOIT*
|       CVE-2011-2523   10.0    https://vulners.com/cve/CVE-2011-2523
|       CNVD-2020-46837 10.0    https://vulners.com/cnvd/CNVD-2020-46837
|       CC3F6C15-182F-53F6-A5CC-812D37F1F047    10.0    https://vulners.com/githubexploit/CC3F6C15-182F-53F6-A5CC-812D37F1F047  *EXPLOIT*
|       A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B    10.0    https://vulners.com/githubexploit/A41B5EAD-1A4C-56A6-97C6-1C58A1CF1E3B  *EXPLOIT*
|       817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3    10.0    https://vulners.com/githubexploit/817CD8FE-87C4-5FE8-B9B2-8CC64333A3F3  *EXPLOIT*
|       63A5C9A7-C241-5E83-9EE6-ABAB44BDD270    10.0    https://vulners.com/githubexploit/63A5C9A7-C241-5E83-9EE6-ABAB44BDD270  *EXPLOIT*
|       5F4BCEDE-77DF-5D54-851A-0AE8B7645BD9    10.0    https://vulners.com/githubexploit/5F4BCEDE-77DF-5D54-851A-0AE8B7645BD9  *EXPLOIT*
|       50580586-73C4-5097-81CA-546D6591DF44    10.0    https://vulners.com/githubexploit/50580586-73C4-5097-81CA-546D6591DF44  *EXPLOIT*
|_      1337DAY-ID-36095        9.8     https://vulners.com/zdt/1337DAY-ID-36095        *EXPLOIT*
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       DF059135-2CF5-5441-8F22-E6EF1DEE5F6E    10.0    https://vulners.com/gitee/DF059135-2CF5-5441-8F22-E6EF1DEE5F6E  *EXPLOIT*
|       PACKETSTORM:173661      9.8     https://vulners.com/packetstorm/PACKETSTORM:173661      *EXPLOIT*
|       F0979183-AE88-53B4-86CF-3AF0523F3807    9.8     https://vulners.com/githubexploit/F0979183-AE88-53B4-86CF-3AF0523F3807  *EXPLOIT*
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
|       CVE-2016-1908   9.8     https://vulners.com/cve/CVE-2016-1908
|       B8190CDB-3EB9-5631-9828-8064A1575B23    9.8     https://vulners.com/githubexploit/B8190CDB-3EB9-5631-9828-8064A1575B23  *EXPLOIT*
|       8FC9C5AB-3968-5F3C-825E-E8DB5379A623    9.8     https://vulners.com/githubexploit/8FC9C5AB-3968-5F3C-825E-E8DB5379A623  *EXPLOIT*
|       8AD01159-548E-546E-AA87-2DE89F3927EC    9.8     https://vulners.com/githubexploit/8AD01159-548E-546E-AA87-2DE89F3927EC  *EXPLOIT*
|       2227729D-6700-5C8F-8930-1EEAFD4B9FF0    9.8     https://vulners.com/githubexploit/2227729D-6700-5C8F-8930-1EEAFD4B9FF0  *EXPLOIT*
|       0221525F-07F5-5790-912D-F4B9E2D1B587    9.8     https://vulners.com/githubexploit/0221525F-07F5-5790-912D-F4B9E2D1B587  *EXPLOIT*
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       BA3887BD-F579-53B1-A4A4-FF49E953E1C0    8.1     https://vulners.com/githubexploit/BA3887BD-F579-53B1-A4A4-FF49E953E1C0  *EXPLOIT*
|       4FB01B00-F993-5CAF-BD57-D7E290D10C1F    8.1     https://vulners.com/githubexploit/4FB01B00-F993-5CAF-BD57-D7E290D10C1F  *EXPLOIT*
```

5. Análisis de Riesgos

El análisis técnico del activo revela que el riesgo global es CRÍTICO, fundamentado en la presencia de múltiples vectores de entrada que permiten desde la ejecución remota de comandos con privilegios máximos hasta el compromiso total de la infraestructura y los datos.

Análisis de Riesgos de las Vulnerabilidades Encontradas:

- Riesgo de Compromiso Total del Sistema (RCE): La vulnerabilidad detectada en vsFTPd 2.3.4 (CRÍTICA, CVE-2011-2523) representa el riesgo más severo, ya que la existencia de un backdoor permite a un atacante obtener un shell con privilegios de root de forma inmediata y sin autenticación. Este nivel de acceso otorga control absoluto sobre el sistema operativo, permitiendo la manipulación de cualquier archivo o proceso.
- Riesgo de Explotación de Servicios de Red: El uso de versiones obsoletas en servicios de archivos compartidos como Samba 3.x (CRÍTICA, CVE-2017-7494) expone al host a la carga de librerías compartidas maliciosas, lo que facilita el movimiento lateral y la persistencia dentro de la red corporativa.
- Riesgo de Acceso no Autorizado a Bases de Datos: La presencia de MySQL 5.0.51a (ALTA, CVE-2012-2122) introduce un riesgo crítico de bypass de autenticación, donde un atacante podría acceder a la base de datos sin una contraseña válida, comprometiendo la confidencialidad y la integridad de los registros almacenados.

Análisis de Debilidades de Seguridad en el Host:

- Debilidad por Componentes Obsoletos y EOL (End-of-Life): Se identificó una superficie de ataque masiva debido al uso de software que ha alcanzado su fin de vida útil, como Apache 2.2.8, OpenSSH 4.7p1 y PHP 5.2.4. Estos componentes carecen de parches para vulnerabilidades modernas, clasificándose bajo el fallo OWASP A06: Componentes Vulnerables y Obsoletos, lo que garantiza que cualquier atacante con exploits públicos pueda comprometer el servicio.
- Debilidad en la Disponibilidad del Servicio (DoS): El host presenta debilidades estructurales ante ataques de denegación de servicio. La vulnerabilidad Slowloris (MEDIA, CVE-2007-6750) detectada en los puertos 80 y 8180 indica que el servidor no gestiona correctamente las conexiones persistentes, permitiendo que un solo atacante agote los recursos de red y deje las aplicaciones web fuera de línea.
- Debilidad por Exposición de Información y Reconocimiento: El sistema revela excesiva información técnica a través de comandos como VRFY en SMTP (Puerto 25) y encabezados HTTP. Estas debilidades de configuración facilitan la fase de reconocimiento, permitiendo a los atacantes enumerar usuarios válidos del sistema y planificar ataques de fuerza bruta o ingeniería social con alta precisión.

6. Recomendaciones de Mitigación

Gestión de Vulnerabilidades Críticas y Remediación de RCE (Prioridad Máxima)

- **Eliminación del Backdoor en FTP: Se debe desinstalar de forma inmediata la versión vsFTPd 2.3.4, ya que contiene un código malicioso (CVE-2011-2523) que otorga acceso de root. Se recomienda actualizar a la versión más reciente del software o reemplazarlo por una alternativa segura como SFTP integrado en una versión actualizada de SSH.**
- **Actualización Crítica de Samba: Es imperativo actualizar el servicio Samba 3.x a una versión parcheada para mitigar vulnerabilidades de ejecución remota de código (CVE-2017-7494). Si el intercambio de archivos mediante SMB no es un requisito operativo, el servicio y sus puertos asociados (139 y 445) deben deshabilitarse.**

Actualización y Endurecimiento (Hardening) de Componentes (Prioridad Alta)

- **Migración de Base de Datos EOL: El motor MySQL 5.0.51a ha alcanzado su fin de ciclo de vida (EOL). Se debe migrar a una versión soportada (ej. MySQL 8.x) para corregir fallos críticos de autenticación (CVE-2012-2122). Adicionalmente, se debe restringir el acceso al puerto 3306 únicamente a localhost o mediante una VPN.**
- **Actualización de OpenSSH: Se requiere actualizar OpenSSH 4.7p1 a la versión más reciente para mitigar la enumeración de usuarios y potenciales vectores de denegación de servicio o RCE. Se recomienda deshabilitar el acceso mediante contraseña y utilizar únicamente autenticación basada en llaves criptográficas (Ed25519).**
- **Actualización del Servidor Web y Entorno PHP: Actualizar el stack web (Apache 2.2.8 y PHP 5.2.4) a versiones modernas. El uso de PHP 5.x expone al sistema a una vasta cantidad de exploits conocidos que no recibirán parches de seguridad.**

Refuerzo de la Configuración y Disponibilidad (Prioridad Media)

- **Mitigación de Denegación de Servicio (DoS): Para neutralizar la vulnerabilidad Slowloris (CVE-2007-6750) detectada en los servicios web (Puertos 80 y 8180), se deben configurar límites de tiempo de espera (timeouts) más agresivos en Apache mediante el módulo mod_reqtimeout y establecer un número máximo de conexiones por dirección IP única.**

Reducción de Superficie de Reconocimiento:

- **SMTP: Deshabilitar el comando VRFY en el servidor de correo para impedir que atacantes externos realicen una enumeración exitosa de usuarios locales.**
- **Banner Grabbing: Configurar las directivas de servidor para ocultar las versiones de software en los encabezados de respuesta (ej. ServerTokens Prod y ServerSignature Off en Apache).**
- **Análisis de las Debilidades de Seguridad en el Host**
- **El host presenta una arquitectura de seguridad deficiente caracterizada por las siguientes debilidades sistémicas:**
- **Obsolescencia Tecnológica Extrema: La debilidad más crítica es la persistencia de software "Legacy" en servicios de cara a la red. Esto indica una falta de gestión de activos y de políticas de actualización, lo que convierte al host en un blanco fácil para scripts automatizados de explotación.**
- **Configuración de Servicios Insegura: Se observa una falta de endurecimiento (Hardening) básico. La exposición de comandos de enumeración (VRFY) y la presencia de servicios vulnerables a DoS sugieren que el sistema se mantiene con configuraciones por defecto, las cuales no están diseñadas para entornos de producción seguros.**
- **Exceso de Servicios Innecesarios: El host mantiene abiertos servicios que amplían la superficie de ataque (IRC, SMTP, FTP, etc.) sin una segmentación aparente. Esta debilidad facilita el movimiento lateral y aumenta las probabilidades de que un compromiso en un servicio menor escale al control total del servidor.**