Índice

1. Introducción

En esta fase del proyecto se ha llevado a cabo un análisis exhaustivo del servidor Debian comprometido, con el fin de identificar la posible puerta de entrada del atacante, detectar configuraciones inseguras y aplicar medidas correctivas que impidan la escalación de privilegios y mejoren la seguridad del sistema. Las acciones abarcan el análisis de logs, escaneo de malware, auditoría de servicios activos y configuraciones de archivos sensibles.

2. Análisis de Logs del Sistema

2.1 Revisión del servicio SSH

Se utilizaron los registros del servicio SSH para detectar accesos sospechosos:

```
sudo journalctl -u ssh --since "2024-10-08" --until "2024-10-08 19:00:00"
```

2.2 Eventos sospechosos detectados

- Se detectaron reinicios frecuentes del servicio `ssh.service` el día 08 de octubre.
- A las 17:40:59 se registró un inicio de sesión exitoso como **root** desde la dirección IP `192.168.0.134`:

```
Accepted password for root from 192.168.0.134 port 45623 ssh2
```

Este evento evidencia una intrusión directa al sistema mediante credenciales de superusuario. El acceso directo como root sin restricciones representa una vulnerabilidad crítica.

3. Escaneo del Sistema con Rootkit Hunter (rkhunter)

3.1 Objetivo del escaneo

El propósito del escaneo fue detectar presencia de malware, rootkits o modificaciones sospechosas en binarios del sistema.

3.2 Resultados generales

- No se encontraron rootkits conocidos ni puertas traseras.
- Sin embargo, se emitieron advertencias menores que requieren atención.

3.3 Advertencias relevantes

- **Archivo sospechoso:** `/usr/bin/lwp-request`.
  - Herramienta legítima, pero potencialmente utilizada para conexiones externas maliciosas.
  - Se verificó su origen mediante: `dpkg -S /usr/bin/lwp-request`.
- **Segmentos de memoria compartida:**
  - Advertencia por tamaño anómalo.
  - Se revisaron los segmentos con `ipcs -m`, sin hallazgos maliciosos.
- **Configuración SSH insegura:**
  - Se detectó la directiva `PermitRootLogin yes` en `/etc/ssh/sshd_config`, lo que permitía acceso directo como root.

4. Análisis de Servicios Vulnerables

4.1 Servicio SSH

- Se detectó configuración insegura permitiendo autenticación como root.
- Esta configuración fue corregida mediante:

```
PermitRootLogin no
sudo systemctl restart ssh
```

4.2 Servicio FTP (vsftpd)

- Se identificaron los siguientes parámetros inseguros en `/etc/vsftpd.conf`:
  - `anonymous_enable=YES`
  - `write_enable=YES`
  - `ssl_enable=NO`

Estos valores permiten:

- Acceso anónimo sin autenticación.
- Subida de archivos sin control (potencial malware).
- Transmisión de credenciales sin cifrado (susceptible a sniffing).

Medidas recomendadas:

- Desactivar acceso anónimo y habilitar SSL:

```
anonymous_enable=NO
ssl_enable=YES
```

- Reiniciar el servicio:

```
sudo systemctl restart vsftpd
```

- En caso de no necesitar FTP, deshabilitar:

```
sudo systemctl disable --now vsftpd
```

4.3 Archivo wp-config.php de WordPress

El archivo contiene información crítica como:

- Usuario: `wordpressuser`
- Contraseña: `123456`
- Claves de seguridad sin configurar.
- Constante `ABSPATH` mal definida como `_DIR_`.
- Permisos extremadamente inseguros:

```
-rwxrwxrwx 1 www-data www-data 3017 Sep 30 12:02 wp-config.php
```

Medidas correctivas aplicadas:

```
sudo chmod 640 wp-config.php
sudo chown www-data:www-data wp-config.php
```

- Se recomendó cambiar la contraseña de base de datos.
- Se corrigió la constante:

```
define('ABSPATH', __DIR__ . '/');
```

4.4 Configuración de Apache e Indexación Web

- El directorio raíz de Apache permitía la visualización de archivos al acceder vía navegador (`Index of /`).
- En `apache2.conf` se detectó:

```
Options Indexes FollowSymLinks
```

Medida aplicada:

```
Options -Indexes FollowSymLinks
```

- Se reinició Apache:

```
sudo systemctl restart apache2
```

5. Medidas Correctivas Aplicadas

- Bloqueo de acceso root por SSH.
- Reconfiguración o desactivación de FTP inseguro.
- Corrección de permisos y configuración en `wp-config.php`.
- Desactivación de indexación en Apache.
- Revisión y validación de binarios mediante rkhunter.

6. Conclusiones y Recomendaciones Finales

- El sistema presentaba varias configuraciones inseguras, las cuales fueron corregidas exitosamente.
- Se recomienda:
    - Implementar políticas de contraseñas robustas.
    - Cifrado de servicios críticos (FTP, bases de datos).
    - Auditorías periódicas con herramientas como `rkhunter`, `lynis`, `clamav`.
    - Monitoreo de logs automático.
    - Mínimo uso de usuarios con privilegios root.

Con estas acciones se fortalece la postura de seguridad del servidor y se evita la recurrencia de ataques similares.