Fase 2 - Detección y Corrección de una Vulnerabilidad

1. Introducción

En esta fase del proyecto, se detectó y explotó una vulnerabilidad en la máquina Debian comprometida. El objetivo principal fue identificar configuraciones inseguras o servicios vulnerables, explotarlos de forma controlada y aplicar medidas correctivas para devolver el sistema a un estado seguro.

---

2. Vulnerabilidad Detectada

Se detectó una configuración insegura en el servicio **SSH** que permitía:

- Inicio de sesión con el usuario `root` (configuración `PermitRootLogin yes`).
- Autenticación por contraseña en lugar de claves públicas (configuración `PasswordAuthentication yes`).
- Uso de credenciales débiles para el usuario `debian`.

Estas configuraciones facilitaron un ataque de fuerza bruta exitoso que permitió obtener acceso al sistema con privilegios elevados. Además, se detectaron configuraciones adicionales en los logs y archivos que indicaban posibles manipulaciones realizadas por el atacante.

En paralelo, se identificaron riesgos adicionales en el sistema, como archivos y directorios sospechosos relacionados con servicios secundarios, como `ruby` y `LibreOffice`, que podrían representar puntos de compromiso secundarios en el sistema.

3. Proceso de explotación

3.1. Enumeración inicial

Se realizó un escaneo completo con Nmap para identificar los servicios abiertos y sus configuraciones:

```
sudo nmap -sV -A -p- 192.168.1.137
```

Resultados clave:

- Puertos detectados:
  - 21/tcp: FTP (estado: filtered).
  - 22/tcp: SSH (estado: open).
  - 80/tcp: HTTP (estado: filtered).
- Versión de SSH: **OpenSSH 9.2p1 Debian 2+deb12u4**.

Se observó que aunque el puerto **SSH (22)** estaba abierto, los puertos 21 (FTP) y 80 (HTTP) permanecían filtrados, lo que limitó la posibilidad de exploración adicional en esos servicios. Sin embargo, la versión del servicio SSH detectada indicó que podría existir una configuración insegura o credenciales débiles en uso.

3.2. Exploración del servicio SSH

Al confirmar que el puerto 22 estaba accesible, se intentó un ataque de fuerza bruta para detectar credenciales débiles utilizando la herramienta **`hydra`**.

Comando utilizado:

```
hydra -l debian -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.137
```

Resultados:

- El ataque identificó una combinación de usuario y contraseña válida:
  - Usuario: **`debian`**
  - Contraseña: **`123456`**

3.3. Acceso al sistema y escalación de privilegios

Con las credenciales obtenidas, se estableció una conexión SSH al sistema:

```
ssh debian@192.168.1.137
```

Escalación a superusuario (`root`): El usuario **`debian`** tenía configurado acceso total mediante **`sudo`** sin restricciones, lo que permitió ejecutar el siguiente comando:

```
sudo su
```

Resultado: Acceso exitoso como `root`, obteniendo el control completo del sistema.

3.4. Análisis detallado del sistema

Una vez dentro, se realizó un análisis exhaustivo de archivos, configuraciones y logs relevantes:

- **Configuración de SSH:** El archivo `/etc/ssh/sshd_config` mostró configuraciones inseguras que facilitaban el acceso:
  - **PermitRootLogin yes**
  - **PasswordAuthentication yes**
  - **AllowUsers debian**

- **Archivos sensibles:** Se inspeccionaron los archivos `/etc/shadow` y `/etc/passwd` para identificar usuarios del sistema y configuraciones adicionales:
  - **cat /etc/shadow**
  - **cat /etc/passwd**

Se detectaron contraseñas cifradas y usuarios asociados a servicios que utilizaban shells restringidos (`/usr/sbin/nologin`).

- **Directorios de logs:** En el directorio `/var/log` se observó:
  - **Ausencia de archivos clave: `auth.log`** y **`syslog`**, lo que indicaba una posible manipulación por parte del atacante para ocultar actividad.
  - **Presencia de archivos relevantes: `chkrootkit-daily.log`** y **`lastlog`**. El archivo **`lastlog`** contenía referencias corruptas a la IP de la máquina atacante.

3.5. Resultados de `chkrootkit`

El archivo `/var/log/chkrootkit/chkrootkit-daily.log` reveló:

- **Archivos sospechosos:**
  - Directorios relacionados con `ruby` y `LibreOffice` que requerían eliminación manual.
- **Advertencia de packet sniffer:**
  - Aunque la interfaz `enp0s3` no estaba en modo promiscuo, se identificó un posible sniffer en la red.

Estos hallazgos confirmaron que la máquina había sido manipulada y requería medidas correctivas inmediatas.

---

4. Medidas aplicadas para corregir la vulnerabilidad

4.1. Configuración segura de SSH

- Se modificó el archivo `/etc/ssh/sshd_config` para deshabilitar configuraciones inseguras:
  - **PermitRootLogin no**
  - **PasswordAuthentication no**
- Reinicio del servicio:
  - **systemctl restart ssh**

4.2. Eliminación de archivos sospechosos

- Se eliminaron los archivos detectados como sospechosos por `chkrootkit`:
  - **rm -rf /usr/lib/ruby/gems/3.1.0/gems/typeprof-0.21.2/vscode**
  - **rm -rf /usr/lib/ruby/vendor_ruby/rubygems/ssl_certs/.document**
  - **rm -rf /usr/lib/ruby/vendor_ruby/rubygems/tsort/.document**
  - **rm -rf /usr/lib/ruby/vendor_ruby/rubygems/optparse/.document**
  - **rm -rf /usr/lib/libreoffice/share/.registry**

4.3. Eliminación de archivos sospechosos

- Se bloquearon puertos innecesarios y se permitió solo el acceso a SSH:
  - **iptables -A INPUT -p tcp --dport 22 -j ACCEPT**
  - **iptables -A INPUT -p tcp --dport 80 -j DROP**
  - **iptables -A INPUT -p tcp --dport 21 -j DROP**
  - **iptables -A INPUT -p tcp --dport 3306 -j DROP**

4.4. Eliminación de archivos sospechosos

- Se actualizaron los paquetes del sistema:
    - **apt update && apt upgrade -y**

4.5. Eliminación de archivos sospechosos

- Se asignaron nuevas contraseñas seguras a los usuarios **`debian`** y **`root`**:
    - **echo "debian:RootForce23" | chpasswd**
    - **echo "root:RootForce23" | chpasswd**

---

5. Conclusión

La vulnerabilidad en SSH fue explotada con éxito para obtener acceso al sistema. Las medidas correctivas implementadas incluyen:

- Configuración segura del servicio SSH.
- Eliminación de archivos sospechosos.
- Bloqueo de puertos innecesarios.
- Actualización del sistema y refuerzo de contraseñas.

Estas acciones devolvieron el sistema a un estado seguro y funcional, mitigando el riesgo de futuras explotaciones.