Paso 4 - Bloquea el exploit y previene la escalacion

Fecha: 8 de enero de 2026 (America/New_York)

Objetivo

Contener el servicio comprometido, bloquear el vector de entrada (FTP) y aplicar medidas rapidas para reducir riesgo de escalacion de privilegios, dejando evidencia verificable para el entregable del proyecto.

Acciones ejecutadas

• Se creo un directorio de evidencia (IR) con marca de tiempo.

• Se detuvo el servicio FTP (vsftpd) con systemctl stop.

• Se verifico que vsftpd quedo inactivo y que el puerto 21 dejo de estar en escucha (ss -tulpn).

• Se recolecto evidencia de configuracion de vsftpd (anonymous_enable, write_enable, ssl_enable y chroot).

• Se recopilaron listas de control (/etc/ftpusers) y logs del servicio con journalctl.

• Se ejecutaron verificaciones para prevencion de escalacion (montaje de /tmp; listado SUID/SGID; busqueda de NOPASSWD).

• Se guardaron archivos de evidencia en una carpeta local.

Evidencia clave (extractos)

1) Detencion del servicio comprometido

```
systemctl is-active vsftpd
inactive

systemctl status vsftpd --no-pager
Active: inactive (dead) since Thu 2026-01-08 17:59:52 EST; ...
```

2) Verificacion de puertos en escucha (sin *:21)

```
sudo ss -tulpn
tcp LISTEN 0 128 0.0.0.0:22        0.0.0.0:*    users:(("sshd",pid=584,fd=3))
tcp LISTEN 0 20  127.0.0.1:25       0.0.0.0:*    users:(("exim4",pid=1056,fd=4))
tcp LISTEN 0 128 127.0.0.1:631      0.0.0.0:*    users:(("cupsd",pid=551,fd=7))
... (sin entrada para *:21)
```

3) Hallazgos de configuracion vsftpd (riesgo)

```
sudo grep -nE "anonymous_enable|local_enable|write_enable|...|ssl_enable" /etc/vsftpd.conf
25:anonymous_enable=YES
28:local_enable=YES
31:write_enable=YES
151:ssl_enable=NO
```

4) Listas de control de usuarios FTP

```
/etc/ftpusers (usuarios sin acceso FTP)
root
daemon
bin
sys
...
nobody
```

Observaciones

• La contencion es efectiva: vsftpd quedo detenido y el puerto 21 ya no esta expuesto.

• La configuracion encontrada en /etc/vsftpd.conf es insegura (anonymous_enable=YES, write_enable=YES, ssl_enable=NO).

• Adicionalmente, la opcion chroot_local_user aparece comentada (no aplicada), lo que puede aumentar el impacto si el servicio se reactivara sin endurecimiento.

Recomendaciones de mitigacion

• Evitar que el servicio se reactive solo: sudo systemctl disable --now vsftpd (opcional: sudo systemctl mask vsftpd).

• Aplicar regla de firewall para negar 21/tcp (UFW/iptables/nftables) y conservar evidencia del ruleset.

• Endurecer vsftpd.conf antes de reactivar: anonymous_enable=NO, write_enable=NO, chroot_local_user=YES; habilitar TLS si aplica al laboratorio.

• Mantener controles anti-escalacion: /tmp con noexec/nosuid/nodev; revisar SUID/SGID inusuales; eliminar NOPASSWD no autorizado en sudoers.

Ruta de evidencia generada

Evidencia guardada en: **/home/debian/paso4_fix_2026-01-08_175952**

Nota: La evidencia de firewall puede estar en archivos como 04_ufw_status.txt o 05_iptables_rules.txt dentro de esa carpeta.