Resumen de Mitigacion y Hardening

Debian VM - Acciones ejecutadas para mitigar el ataque, evitar escalacion y prevenir recurrencia

1. Objetivo

Revertir los cambios del atacante y reducir la superficie de ataque del sistema mediante: cierre de puertos innecesarios, eliminacion de servicios no requeridos, endurecimiento de SSH y mejora del firewall.

2. Medidas tomadas (mitigacion y anti-escalacion)

- Cierre de servicios innecesarios y eliminacion de componentes asociados (p. ej., mDNS/Avahi, CUPS, Exim4; y verificacion de que FTP ya no quedara expuesto).
- Firewall UFW activado con politica por defecto: denegar trafico entrante y permitir saliente; el unico acceso permitido es SSH.
- Proteccion anti-fuerza bruta en SSH mediante rate-limit: regla UFW "22/tcp LIMIT IN".
- Endurecimiento de SSH: bloqueo de login remoto de root, deshabilitar autenticacion por contrasena, deshabilitar X11Forwarding y mantener autenticacion por llave publica.
- Verificaciones post-cambio con comandos de auditoria: ss (puertos), ufw (reglas) y sshd -T (parametros efectivos).

3. Estado final verificado (evidencia tecnica)

Los siguientes puntos reflejan el estado final observado tras aplicar las medidas:

Control	Estado final	Comando de verificacion
Puertos expuestos	Solo 22/tcp (sshd) escuchando (IPv4 e IPv6).	`sudo ss -tulpn`
Firewall (UFW)	Activo; deny incoming / allow outgoing; **22/tcp LIMIT IN**.	`sudo ufw status verbose`
SSH (acceso)	• PermitRootLogin: **no** • PasswordAuthentication: **no** • PubkeyAuthentication: **yes** • X11Forwarding: **no** • PermitEmptyPasswords: **no**	`sudo sshd -T | egrep 'permitrootlogin|passwordauthentication|x11forwarding|pubkeyauthentication|permitemptypasswords'`

Nota: si aparece udp/546 asociado a NetworkManager (DHCPv6 cliente), no representa un servicio servidor expuesto; la exposicion relevante queda determinada por sockets en LISTEN (por ejemplo, 22/tcp).

4. Recomendaciones para prevenir futuros ataques

- **Lista blanca de acceso por SSH:** mantener PasswordAuthentication no y aplicar allowlist con **AllowUsers debian** o **AllowGroups sshusers** para limitar explicitamente quienes pueden autenticarse.
- **Minimo de servicios:** mantener deshabilitados y/o purgados servicios no requeridos. Revisar periodicamente puertos con **ss -tulpn**.
- **Actualizaciones:** ejecutar parches de seguridad regularmente (apt update / full-upgrade) y remover paquetes no usados (autoremove --purge).
- **Proteccion anti-bruteforce:** mantener UFW con rate-limit en 22/tcp. Considerar fail2ban para bloquear IPs con intentos repetidos.
- **Auditoria de persistencia:** revisar cronjobs, unidades systemd (.service/.timer) y llaves SSH (authorized_keys) tras cualquier evento.
- **Backups/snapshots:** mantener snapshots de la VM antes de cambios mayores y respaldos de /etc y del sitio web (si aplica).

5. Checklist rapido de verificacion (para anexar como evidencia)

```
sudo ss -tulpn

sudo ufw status verbose

sudo sshd -T | egrep 'permitrootlogin|passwordauthentication|x11forwarding|pubkeyauthe
ntication|permitemptypasswords'

awk -F: '$3>=1000 && $1!="nobody"{print $1 " UID=" $3}' /etc/passwd
```