Informe de Escaneo de Rootkits y Malware

Servidor: Debian (VM) • Fecha: 8 de enero de 2026

Objetivo: detectar indicadores de **rootkits** y **malware** en el servidor, generando evidencia reproducible (logs, hashes y empaquetado).

Herramientas utilizadas

• RKHunter (verificación de rootkits y configuraciones sospechosas).

• chkrootkit (detección rápida de rootkits conocidos).

• ClamAV (escaneo anti-malware con firmas actualizadas).

Resumen de resultados

Herramienta	Evidencia / resultado principal
ClamAV	Known viruses: 3,627,218 • Scanned files: 12,759 • Infected files: 0
chkrootkit	No se encontraron entradas "INFECTED" (comprobado con grep).
RKHunter	Warnings relacionados a lwp-request (script), shared memory, y PermitRootLogin; el resumen indica 1 archivo sospechoso y 6 posibles rootkits (requiere revisar el detalle en /var/log/rkhunter.log).

Evidencia detallada

ClamAV - actualización de firmas

Se confirmo la presencia de las bases de firmas (main/daily/bytecode) en **/var/lib/clamav**:

```
-rw-r--r--  1 clamav clamav 276K Jan  8 17:18 bytecode.cvd
-rw-r--r--  1 clamav clamav  23M Jan  8 16:52 daily.cvd
-rw-r--r--  1 clamav clamav  85M Jan  8 17:18 main.cvd
```

ClamAV - comando de escaneo y resultado

Se ejecuto un escaneo recursivo sobre rutas tipicas del servidor, excluyendo /proc, /sys y /dev para evitar pseudo-sistemas de archivos.

```
sudo clamscan -r /etc /home /var/www /srv /opt \
  --infected \
  --exclude-dir='^/proc' --exclude-dir='^/sys' --exclude-dir='^/dev' \
  --log="$LOG"
sudo chown debian:debian "$LOG"
tail -n 80 "$LOG"
```

Resumen (SCAN SUMMARY) del log:

```
Known viruses: 3627218
Engine version: 1.0.9
Scanned directories: 1083
Scanned files: 12759
Infected files: 0
Data scanned: 633.93 MB
Data read: 454.80 MB (ratio 1.39:1)
Time: 122.039 sec (2 m 2 s)
Start Date: 2026:01:08 17:19:48
End Date:   2026:01:08 17:21:50
```

Log generado: **/home/debian/clamav_scan_2026-01-08_171948.log**

Integridad y empaquetado de evidencia

Se empaquetaron los logs en un archivo comprimido y se calculo el hash SHA-256 del log de ClamAV:

```
Archivo: evidencia_malware_rootkit_2026-01-08.tar.gz (tamano aproximado: 2.3K)
SHA-256 (log ClamAV): fc934b8b39bf6b15e258d58cfd81e016610a732276ee68817c821be93b5462ab
```

RKHunter - hallazgos y validacion recomendada

RKHunter reporto los siguientes warnings en el log de ejecucion:

```
Warning: The command '/usr/bin/lwp-request' has been replaced by a script: /usr/bin/lwp-
  request: Perl script text executable
Warning: The following suspicious (large) shared memory segments have been found:
SSH configuration option 'PermitRootLogin': yes
```

Adicionalmente, en el resumen del log se observa:

```
Files checked: 144
Suspect files: 1
Rootkits checked: 497
Possible rootkits: 6
```

Interpretacion (sin asumir compromiso)

• **lwp-request**: suele ser un falso positivo en Debian (script Perl legitimo). Validar con: *dpkg -S*, *file*, *sha256sum* y *debsums -s*.

• **Shared memory segments**: se observaron segmentos grandes con owner **debian**, permisos **600** y estado **dest** (marcados para eliminacion). Aun asi, se recomienda atribuirlos a procesos con *ipcs -m -p* y *ps -fp <PID>*.

```
(extracto de ipcs -m / ipcs -m -p)
- Propietario: debian
- Permisos: 600
- Status: dest (marcados para eliminarse cuando no estén adjuntos)
- Segmentos grandes observados: 32 MB (33554432 bytes)
```

• **SSH PermitRootLogin: yes**: es una configuracion insegura (hardening). Recomendado: establecer **PermitRootLogin no** en /etc/ssh/sshd_config y reiniciar el servicio SSH; luego re-ejecutar RKHunter.

chkrootkit - resultado

Salida revisada con grep: - No se encontraron entradas "INFECTED". - La mayoría de verificaciones reportan "not infected".

Archivos de evidencia generados

• Log ClamAV: **/home/debian/clamav_scan_2026-01-08_171948.log**

• Log RKHunter: **~/rkhunter_scan_2026-01-08.log** (segun ejecucion del laboratorio)

• Log chkrootkit: **~/chkrootkit_scan_2026-01-08.log** (segun ejecucion del laboratorio)

• Paquete de evidencia: **evidencia_malware_rootkit_2026-01-08.tar.gz**

• Hashes: **~/hashes_evidencia_2026-01-08.txt**

Conclusion

Con firmas actualizadas y un escaneo completo de directorios criticos, ClamAV no detecto malware (Infected files: 0). chkrootkit no reporto indicadores "INFECTED". RKHunter mostro warnings principalmente asociados a configuracion (PermitRootLogin) y elementos a validar (lwp-request y memoria compartida). Se recomienda aplicar hardening de SSH y realizar la verificacion de integridad/atribucion indicada, y luego repetir RKHunter para cerrar la evidencia.