rkhunter (Rootkit Hunter)

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0226 - Seguretat informàtica (RA3) / 0378 - Seguretat i alta disponibilitat (RA1)

Sistema operatiu: Ubuntu Server 26.04 LTS

1. Què és rkhunter?

rkhunter (*Rootkit Hunter*) és una eina de codi obert especialitzada a detectar **rootkits**, portes del darrere (*backdoors*) i exploits locals en sistemes tipus Unix. A diferència d'un antivirus com ClamAV, que escaneja fitxers buscant signatures de programari maliciós conegut, rkhunter se centra a detectar **indicis que el sistema ja ha estat compromès**:

- Binaris del sistema modificats (comparant hash/propietats amb una línia base)
- Mòduls de kernel ocults o sospitosos
- Ports típicament associats a backdoors coneguts oberts
- Fitxers i directoris típics de rootkits coneguts
- Canvis sospitosos en comptes d'usuari, permisos i variables d'entorn (`LD_LIBRARY_PATH`, preload)
- Eines del sistema (`strings`, `ls`, `ps`...) que poden haver estat substituïdes per versions troianitzades

1.1. rkhunter vs. ClamAV --- complementarietat

	ClamAV	rkhunter
Què detecta	Malware/virus amb signatura coneguda dins de fitxers	Indicis de compromís del sistema (rootkits, backdoors)
Mecanisme	Escaneig de contingut de fitxers	Comprovació d'integritat + base de dades de signatures de rootkits
Moment típic d'ús	Preventiu (analitzar fitxers rebuts/pujats)	Detectiu (comprovar si el sistema ja ha estat vulnerat)
Freqüència recomanada	Escaneigs puntuals o en accés (on-access)	Comprovacions periòdiques (diàries, via cron)

2. Instal·lació a Ubuntu Server 26.04

Actualitza la llista de paquets

```
sudo apt update
```

Instal·la

```
sudo apt install rkhunter curl
```

NOTA

`curl` és necessari perquè rkhunter l'utilitza per descarregar actualitzacions de les bases de dades de signatures des dels servidors mirall.

3. Configuració bàsica

3.1. Activa el cron diari i les notificacions per correu

```
sudo nano /etc/default/rkhunter
```

```
# Si es posa a "yes", s'executarà una comprovació diària automàtica
 ↪  via cron
CRON_DAILY_RUN="yes"

# Adreça on rebre l'informe
REPORT_EMAIL="root"
```

3.2. Ajusta el fitxer principal de configuració

```
sudo nano /etc/rkhunter.conf
```

Tres paràmetres clau a revisar (les línies concretes poden variar lleugerament segons la versió del paquet):

```
# Permet actualitzar automàticament la llista de miralls de descàrrega
UPDATE_MIRRORS=1

# Mode d'ús dels miralls (0 = fer servir tots per ordre fins que un
 ↪  respongui)
MIRRORS_MODE=0

# Deixar en blanc si no es vol comprovació d'actualitzacions web
 ↪  addicional
WEB_CMD=""
```

CONSELL

`WEB_CMD=""` és un ajust habitual en entorns de laboratori sense accés complet a Internet o darrere d'un proxy, ja que evita que rkhunter intenti llançar una ordre addicional de comprovació web que podria fallar o alentir l'execució.

4. Actualitza la base de dades i crea la línia base

Actualitzar les bases de dades de signatures (rootkits coneguts, ports de backdoors…)

```
sudo rkhunter --update
```

Crear/actualitzar la "línia base" de propietats de fitxers del sistema (hash, permisos…) amb la qual es compararan futures execucions

```
sudo rkhunter --propupd
```

IMPORTANT

`--propupd` s'ha d'executar just després d'una instal·lació neta i verificada del sistema (sense indicis de compromís). Aquesta és la "fotografia de referència": si més endavant `rkhunter --check` detecta que un binari ha canviat respecte a aquesta línia base, ho marcarà com a advertència. Cal tornar a executar `--propupd` conscientment cada vegada que s'apliquin actualitzacions legítimes del sistema (`apt upgrade`), o rkhunter marcarà com a "sospitosos" binaris que en realitat només s'han actualitzat de forma normal.

5. Executa una comprovació manual

```
# --sk: no esperar que l'usuari premi Enter entre seccions (útil en
 ↪  scripts/cron)
# --rwo: mostrar només els resultats amb advertència (Warnings Only)
sudo rkhunter --check --sk
```

Sortida (resumida) esperada:

```
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...
  Performing 'strings' command checks
    Checking 'strings' command                              [ OK ]
  Performing 'shared libraries' checks
    Checking for preloading variables                  [ None found ]
    Checking for preloaded libraries                   [ None found ]
    Checking LD_LIBRARY_PATH variable                   [ Not found ]
  Performing file properties checks
    /usr/sbin/adduser                                       [ OK ]
    ...

System checks summary
=====================
File properties checks...
    Files checked: 183
    Suspect files: 0
```

```
Rootkit checks...
    Rootkits checked : 498
    Possible rootkits: 0

The system checks took: 1 minute and 57 seconds
All results have been written to the log file: /var/log/rkhunter.log
```

El registre complet (amb tots els detalls, no només els avisos) sempre es desa a:

```
sudo less /var/log/rkhunter.log
```

6. Automatització amb cron i notificació per correu

Amb `CRON_DAILY_RUN="yes"` ja configurat (apartat 3.1), Ubuntu executarà automàticament una comprovació diària mitjançant l'script que instal·la el mateix paquet (`/etc/cron.daily/rkhunter`), i n'enviarà el resultat a `REPORT_EMAIL`.

Si es vol un control més fi (per exemple, una comprovació més freqüent que la diària, o enviar-la a una adreça diferent per a la pràctica), es pot definir una tasca pròpia:

```
sudo crontab -e
```

```
# Comprovació de rkhunter cada dia a les 04:30, amb sortida només
 ↪  d'advertències
30 4 * * * /usr/bin/rkhunter --check --sk --rwo --cronjob |
 ↪  /usr/bin/mail -s "Informe rkhunter $(hostname)" root@localhost
```

- `--cronjob`: mode pensat per a execució no interactiva (equivalent a `--sk` més ajustos addicionals de sortida).
- El resultat es canalitza cap a `mail`. Totes dues eines segueixen el mateix patró de "detecció automàtica + notificació".

7. Interpretar els resultats

Resultat	Significat	Acció recomanada
`[ OK ]`	Comprovació superada, sense indicis	Cap acció
`[ Warning ]`	Possible indici de compromís o desviació respecte a la línia base	Investigar manualment el fitxer/procés/port indicat al log
`Suspect files > 0`	Fitxers de sistema amb propietats diferents de la línia base	Comparar amb un sistema net, revisar si prové d'una actualització legítima o d'un compromís real
`Possible rootkits > 0`	Coincidència amb signatura de rootkit conegut	Aïllar la màquina de la xarxa i investigar-la abans de continuar-hi treballant

AVÍS

Un `Warning` **no implica automàticament** que el sistema estigui compromès: sovint és un fals positiu provocat per actualitzacions legítimes o per la mateixa configuració del laboratori (per exemple, eines de xarxa poc habituals com `nmap` instal·lades expressament per als exercicis d'aquest mateix mòdul). Cal sempre investigar el detall al log abans de treure conclusions.

Referències

- Server World --- RKHunter a Ubuntu 26.04 (instal·lació, configuració i ús): https://www.server-world.info/en/note?os=Ubuntu_26.04&p=rkhunter
- Documentació de rkhunter (SourceForge): https://sourceforge.net/projects/rkhunter/

Versions d'aquest document

- HTML - rkhunter.html
- PDF - rkhunter.pdf
- ODT - rkhunter.odt
- MD - rkhunter.md