

Update #18 - RKHunter Daily Scan with Email Alerting and Log Cleanup

Date: June 3, 2025

Category: Security / Monitoring

Backlink: [Update #17 – Installing Root Kit Detection on Virtual Private Server](#)

Overview

This update enhances our RKHunter setup by:

- Automating daily scans
 - Emailing warnings only (using `msmtp`)
 - Saving results to timestamped log files
 - Cleaning up old logs monthly
-

Script Location

```
/usr/local/bin/rkhunter.sh
```

Script Contents

```
#!/bin/bash
```

```
# === CONFIG ===
EMAIL="natenetworks.alerts@gmail.com"
LOGFILE="/var/log/rkhunter-manual-$(date +%F).log"
WARNING_LOG="/tmp/rkhunter-warnings.log"

# === RUN RKHUNTER TASKS ===
{
    echo "=== RKHUNTER SCAN STARTED: $(date) ==="
    sudo rkhunter --update
    sudo rkhunter --propupd
    sudo rkhunter -c -sk
    echo "=== RKHUNTER SCAN FINISHED: $(date) ==="
} | tee -a "$LOGFILE"

# === EXTRACT WARNINGS ONLY ===
grep 'Warning:' /var/log/rkhunter.log > "$WARNING_LOG"

# === EMAIL IF WARNINGS EXIST ===
if [ -s "$WARNING_LOG" ]; then
{
    echo "To: $EMAIL"
    echo "Subject: ⚠ RKHunter Warning Report - $(hostname) - $(date +%F)"
    echo "Content-Type: text/plain"
    echo
    echo "RKHunter has reported warnings on $(hostname) at $(date):"
    echo
    cat "$WARNING_LOG"
} | msmtput -t
fi

# === CLEANUP ===
rm -f "$WARNING_LOG"
```

Scheduled Daily Cron Job

Added via root crontab:

```
sudo crontab -e
```

```
30 3 * * * /usr/local/bin/rkhunter.sh
```

Monthly Log Cleanup

Old logs older than 30 days are purged automatically:

```
@monthly find /var/log/ -name "rkhunter-manual-*.log" -mtime +30 -delete
```

Email Setup

- Outgoing email uses `msmtp`
 - Alerts are only sent if `grep 'Warning:'` finds any issues
-

Status

- Email tested ☐
 - Logs cleanly date-stamped ☐
 - Monthly cleanup cron job added ☐
 - Script ownership and permissions secured ☐
-

Revision #2

Created 3 June 2025 22:19:51 by Nate Nash

Updated 7 June 2025 00:14:24 by Nate Nash