Rkhunter Malware Host Profile Report

System: scorpio
OS: Linux Mint 18.3

Date: Mon Jun 24 07:37:32 CDT 2019

```
[ 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
    Checking for prerequisites                              [ OK ]
    /usr/local/bin/rkhunter                                 [ OK ]
    /usr/local/bin/skdet                                    [ OK ]
    /usr/local/bin/lwp-request                              [ Warning ]
    /usr/sbin/adduser                                       [ Warning ]
    /usr/sbin/chroot                                        [ OK ]
    /usr/sbin/cron                                          [ OK ]
    /usr/sbin/groupadd                                      [ Warning ]
    /usr/sbin/groupdel                                      [ Warning ]
    /usr/sbin/groupmod                                      [ Warning ]
    /usr/sbin/grpck                                         [ Warning ]
    /usr/sbin/nologin                                       [ Warning ]
    /usr/sbin/pwck                                          [ Warning ]
    /usr/sbin/rsyslogd                                      [ Warning ]
    /usr/sbin/sshd                                          [ Warning ]
    /usr/sbin/tcpd                                          [ OK ]
    /usr/sbin/useradd                                       [ Warning ]
    /usr/sbin/userdel                                       [ Warning ]
    /usr/sbin/usermod                                       [ Warning ]
    /usr/sbin/vipw                                          [ Warning ]
    /usr/sbin/unhide                                        [ OK ]
    /usr/sbin/unhide-linux                                  [ OK ]
    /usr/sbin/unhide-posix                                  [ OK ]
    /usr/sbin/unhide-tcp                                    [ OK ]
    /usr/bin/awk                                            [ OK ]
    /usr/bin/basename                                       [ OK ]
    /usr/bin/chattr                                         [ OK ]
    /usr/bin/curl                                           [ Warning ]
    /usr/bin/cut                                            [ OK ]
    /usr/bin/diff                                           [ OK ]
    /usr/bin/dirname                                        [ OK ]
    /usr/bin/dpkg                                           [ Warning ]
    /usr/bin/dpkg-query                                     [ Warning ]
    /usr/bin/du                                             [ OK ]
    /usr/bin/elinks                                         [ OK ]
    /usr/bin/env                                            [ OK ]
    /usr/bin/file                                           [ Warning ]
    /usr/bin/find                                           [ OK ]
    /usr/bin/GET                                            [ OK ]
    /usr/bin/groups                                         [ OK ]
    /usr/bin/head                                           [ OK ]
    /usr/bin/id                                             [ OK ]
    /usr/bin/ipcs                                           [ Warning ]
    /usr/bin/killall                                        [ OK ]
    /usr/bin/last                                           [ Warning ]
    /usr/bin/lastlog                                        [ Warning ]
    /usr/bin/ldd                                            [ Warning ]
    /usr/bin/less                                           [ OK ]
    /usr/bin/links                                          [ OK ]
    /usr/bin/locate                                         [ OK ]
    /usr/bin/logger                                         [ Warning ]
    /usr/bin/lsattr                                         [ OK ]
    /usr/bin/lsof                                           [ OK ]
    /usr/bin/lynx                                           [ Warning ]
    /usr/bin/mail                                           [ OK ]
    /usr/bin/md5sum                                         [ OK ]
    /usr/bin/mlocate                                        [ OK ]
    /usr/bin/newgrp                                         [ Warning ]
    /usr/bin/passwd                                         [ Warning ]
    /usr/bin/perl                                           [ Warning ]
    /usr/bin/pgrep                                          [ Warning ]
    /usr/bin/pkill                                          [ Warning ]
    /usr/bin/pstree                                         [ OK ]
    /usr/bin/rpm                                            [ Warning ]
    /usr/bin/runcon                                         [ OK ]
    /usr/bin/sha1sum                                        [ OK ]
```

Rkhunter Malware Host Profile Report

System: scorpio
OS: Linux Mint 18.3

Date: Mon Jun 24 07:37:32 CDT 2019

/usr/bin/sha224sum	[OK]
/usr/bin/sha256sum	[OK]
/usr/bin/sha384sum	[OK]
/usr/bin/sha512sum	[OK]
/usr/bin/size	[Warning]
/usr/bin/sort	[OK]
/usr/bin/ssh	[Warning]
/usr/bin/stat	[OK]
/usr/bin/strace	[OK]
/usr/bin/strings	[Warning]
/usr/bin/sudo	[Warning]
/usr/bin/tail	[OK]
/usr/bin/telnet	[OK]
/usr/bin/test	[OK]
/usr/bin/top	[Warning]
/usr/bin/touch	[OK]
/usr/bin/tr	[OK]
/usr/bin/uniq	[OK]
/usr/bin/users	[OK]
/usr/bin/vmstat	[Warning]
/usr/bin/w	[Warning]
/usr/bin/watch	[Warning]
/usr/bin/wc	[OK]
/usr/bin/wget	[Warning]
/usr/bin/whatis	[OK]
/usr/bin/whereis	[Warning]
/usr/bin/which	[OK]
/usr/bin/who	[OK]
/usr/bin/whoami	[OK]
/usr/bin/numfmt	[OK]
/usr/bin/gawk	[OK]
/usr/bin/lwp-request	[Warning]
/usr/bin/mail.mailutils	[OK]
/usr/bin/x86_64-linux-gnu-size	[Warning]
/usr/bin/x86_64-linux-gnu-strings	[Warning]
/usr/bin/telnet.netkit	[OK]
/usr/bin/w.procps	[Warning]
/sbin/depmod	[Warning]
/sbin/fsck	[Warning]
/sbin/ifconfig	[OK]
/sbin/ifdown	[Warning]
/sbin/ifup	[Warning]
/sbin/init	[Warning]
/sbin/insmod	[Warning]
/sbin/ip	[Warning]
/sbin/lsmod	[Warning]
/sbin/modinfo	[Warning]
/sbin/modprobe	[Warning]
/sbin/rmmod	[Warning]
/sbin/route	[OK]
/sbin/runlevel	[Warning]
/sbin/sulogin	[Warning]
/sbin/sysctl	[Warning]
/bin/bash	[OK]
/bin/cat	[OK]
/bin/chmod	[OK]
/bin/chown	[OK]
/bin/cp	[OK]
/bin/date	[OK]
/bin/df	[OK]
/bin/dmesg	[Warning]
/bin/echo	[OK]
/bin/ed	[OK]
/bin/egrep	[Warning]
/bin/fgrep	[Warning]
/bin/fuser	[OK]
/bin/grep	[OK]
/bin/ip	[Warning]
/bin/kill	[Warning]
/bin/less	[OK]
/bin/login	[Warning]
/bin/ls	[OK]
/bin/lsmod	[Warning]
/bin/mktemp	[OK]
/bin/more	[Warning]
/bin/mount	[Warning]
/bin/mv	[OK]
/bin/netstat	[OK]
/bin/ping	[OK]

Rkhunter Malware Host Profile Report

System: scorpio
OS: Linux Mint 18.3

Date: Mon Jun 24 07:37:32 CDT 2019

```
    /bin/ps                                                 [ Warning ]
    /bin/pwd                                                [ OK ]
    /bin/readlink                                           [ OK ]
    /bin/sed                                                [ OK ]
    /bin/sh                                                 [ OK ]
    /bin/su                                                 [ Warning ]
    /bin/touch                                              [ OK ]
    /bin/uname                                              [ OK ]
    /bin/which                                              [ Warning ]
    /bin/kmod                                               [ Warning ]
    /bin/systemd                                            [ Warning ]
    /bin/systemctl                                          [ Warning ]
    /lib/systemd/systemd                                    [ Warning ]
    /etc/rkhunter.conf                                      [ OK ]

Checking for rootkits...

  Performing check of known rootkit files and directories
    55808 Trojan - Variant A                                [ Not found ]
    ADM Worm                                                [ Not found ]
    AjaKit Rootkit                                          [ Not found ]
    Adore Rootkit                                           [ Not found ]
    aPa Kit                                                 [ Not found ]
    Apache Worm                                             [ Not found ]
    Ambient (ark) Rootkit                                   [ Not found ]
    Balaur Rootkit                                          [ Not found ]
    BeastKit Rootkit                                        [ Not found ]
    beX2 Rootkit                                            [ Not found ]
    BOBKit Rootkit                                          [ Not found ]
    cb Rootkit                                              [ Not found ]
    CiNIK Worm (Slapper.B variant)                          [ Not found ]
    Danny-Boy's Abuse Kit                                   [ Not found ]
    Devil RootKit                                           [ Not found ]
    Diamorphine LKM                                         [ Not found ]
    Dica-Kit Rootkit                                        [ Not found ]
    Dreams Rootkit                                          [ Not found ]
    Duarawkz Rootkit                                        [ Not found ]
    Ebury backdoor                                          [ Not found ]
    Enye LKM                                                [ Not found ]
    Flea Linux Rootkit                                      [ Not found ]
    Fu Rootkit                                              [ Not found ]
    Fuck`it Rootkit                                         [ Not found ]
    GasKit Rootkit                                          [ Not found ]
    Heroin LKM                                              [ Not found ]
    HjC Kit                                                 [ Not found ]
    ignoKit Rootkit                                         [ Not found ]
    IntoXonia-NG Rootkit                                    [ Not found ]
    Irix Rootkit                                            [ Not found ]
    Jynx Rootkit                                            [ Not found ]
    Jynx2 Rootkit                                           [ Not found ]
    KBeast Rootkit                                          [ Not found ]
    Kitko Rootkit                                           [ Not found ]
    Knark Rootkit                                           [ Not found ]
    ld-linuxv.so Rootkit                                    [ Not found ]
    Li0n Worm                                               [ Not found ]
    Lockit / LJK2 Rootkit                                   [ Not found ]
    Mokes backdoor                                          [ Not found ]
    Mood-NT Rootkit                                         [ Not found ]
    MRK Rootkit                                             [ Not found ]
    Ni0 Rootkit                                             [ Not found ]
    Ohhara Rootkit                                          [ Not found ]
    Optic Kit (Tux) Worm                                    [ Not found ]
    Oz Rootkit                                              [ Not found ]
    Phalanx Rootkit                                         [ Not found ]
    Phalanx2 Rootkit                                        [ Not found ]
    Phalanx2 Rootkit (extended tests)                       [ Not found ]
    Portacelo Rootkit                                       [ Not found ]
    R3dstorm Toolkit                                        [ Not found ]
    RH-Sharpe's Rootkit                                     [ Not found ]
    RSHA's Rootkit                                          [ Not found ]
    Scalper Worm                                            [ Not found ]
    Sebek LKM                                               [ Not found ]
    Shutdown Rootkit                                        [ Not found ]
    SHV4 Rootkit                                            [ Not found ]
    SHV5 Rootkit                                            [ Not found ]
    Sin Rootkit                                             [ Not found ]
    Slapper Worm                                            [ Not found ]
    Sneakin Rootkit                                         [ Not found ]
    'Spanish' Rootkit                                       [ Not found ]
```

Rkhunter Malware Host Profile Report

System: scorpio
OS: Linux Mint 18.3

Date: Mon Jun 24 07:37:32 CDT 2019

```
    Suckit Rootkit                                    [ Not found ]
    Superkit Rootkit                                  [ Not found ]
    TBD (Telnet BackDoor)                             [ Not found ]
    TeLeKiT Rootkit                                   [ Not found ]
    T0rn Rootkit                                      [ Not found ]
    trNkit Rootkit                                    [ Not found ]
    Trojanit Kit                                      [ Not found ]
    Tuxtendo Rootkit                                  [ Not found ]
    URK Rootkit                                       [ Not found ]
    Vampire Rootkit                                   [ Not found ]
    VcKit Rootkit                                     [ Not found ]
    Volc Rootkit                                      [ Not found ]
    Xzibit Rootkit                                    [ Not found ]
    zaRwT.KiT Rootkit                                 [ Not found ]
    ZK Rootkit                                        [ Not found ]

  Performing additional rootkit checks
    Suckit Rootkit additional checks                  [ OK ]
    Checking for possible rootkit files and directories  [ None found ]
    Checking for possible rootkit strings             [ None found ]

  Performing malware checks
    Checking running processes for deleted files      [ Warning ]
    Checking running processes for suspicious files   [ None found ]
    Checking for hidden processes                     [ None found ]
    Checking for files with suspicious contents       [ Warning ]
    Checking for login backdoors                      [ None found ]
    Checking for sniffer log files                    [ None found ]
    Checking for suspicious directories               [ None found ]
    Checking for suspicious (large) shared memory segments  [ Warning ]

  Performing Linux specific checks
    Checking loaded kernel modules                    [ OK ]
    Checking kernel module names                      [ OK ]

Checking the network...

  Performing checks on the network ports
    Checking for backdoor ports                       [ None found ]
    Checking for hidden ports                         [ None found ]

  Performing checks on the network interfaces
    Checking for promiscuous interfaces               [ None found ]
    Checking for packet capturing applications        [ Warning ]

Checking the local host...

  Performing system boot checks
    Checking for local host name                      [ Found ]
    Checking for system startup files                 [ Found ]
    Checking system startup files for malware         [ None found ]

  Performing group and account checks
    Checking for passwd file                          [ Found ]
    Checking for root equivalent (UID 0) accounts     [ None found ]
    Checking for passwordless accounts                [ None found ]
    Checking for passwd file changes                  [ None found ]
    Checking for group file changes                   [ None found ]
    Checking root account shell history files         [ OK ]

  Performing system configuration file checks
    Checking for an SSH configuration file            [ Found ]
    Checking if SSH root access is allowed            [ Not allowed ]
    Checking if SSH protocol v1 is allowed            [ Not allowed ]
    Checking for other suspicious configuration settings  [ None found ]
    Checking for a running system logging daemon      [ Found ]
    Checking for a system logging configuration file  [ Found ]
    Checking if syslog remote logging is allowed      [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types           [ Warning ]
    Checking for hidden files and directories         [ Warning ]

Checking application versions...

    Checking version of GnuPG                         [ OK ]
    Checking version of OpenSSL                       [ OK ]
    Checking version of OpenSSH                       [ OK ]
```

Rkhunter Malware Host Profile Report

System: scorpio
OS: Linux Mint 18.3

Date: Mon Jun 24 07:37:32 CDT 2019

```
System checks summary
=====================

File properties checks...
    Files checked: 158
    Suspect files: 74

Rootkit checks...
    Rootkits checked : 505
    Possible rootkits: 6

Applications checks...
    Applications checked: 3
    Suspect applications: 0

The system checks took: 18 minutes and 43 seconds

All results have been written to the log file: /var/log/rkhunter.log

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```