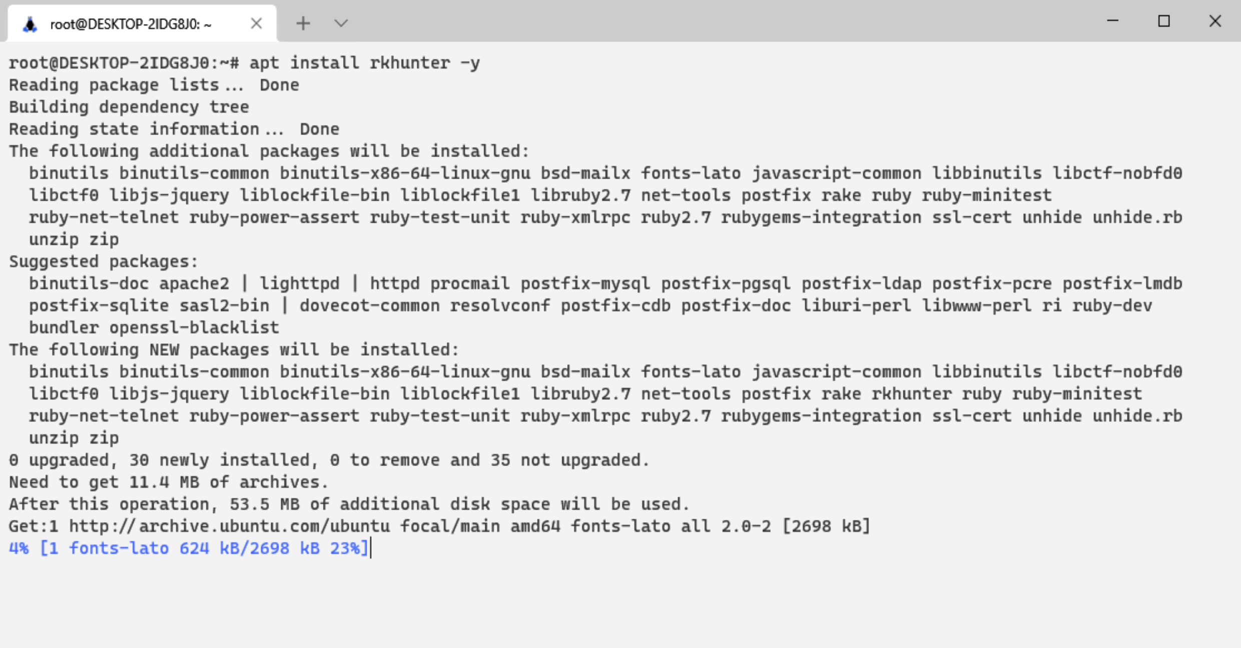
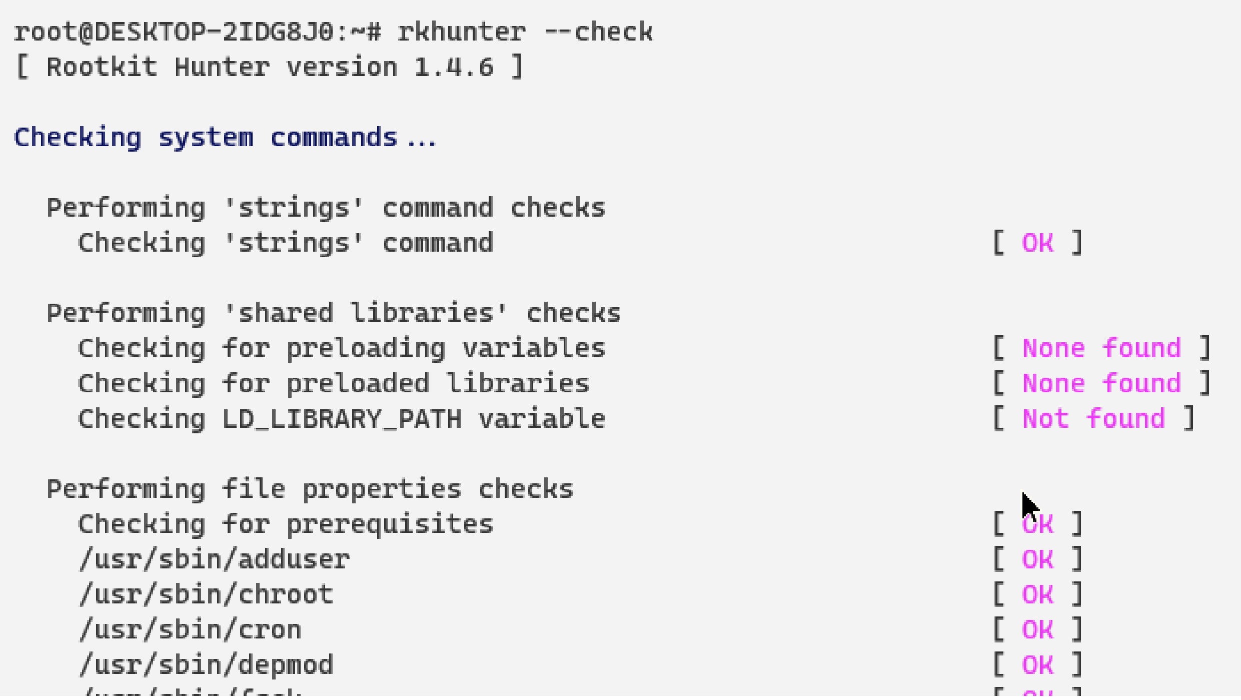
OUTPUT

Install the Rootkit hunter package in Kali Linux for checking Root kit vulnerabilities,

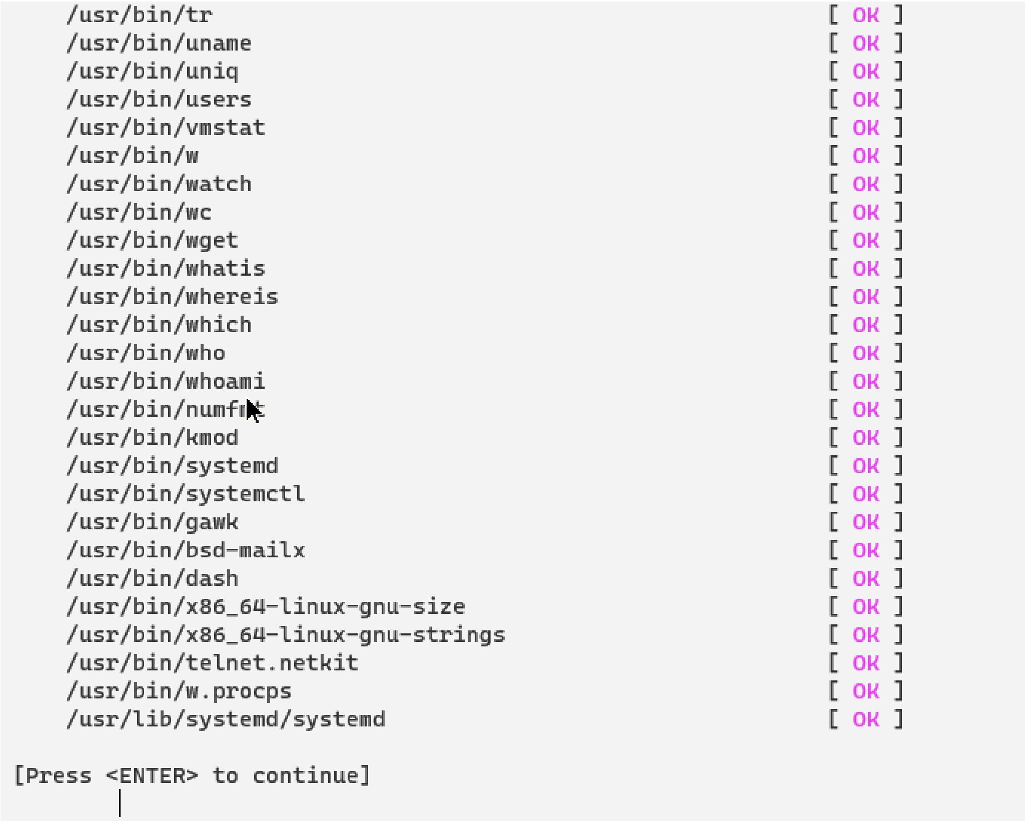


```
root@DESKTOP-2IDG8J0:~# apt install rkhunter -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato javascript-common libbinutils libctf-nobfd0
  libctf0 libjs-jquery liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake ruby ruby-minitest
  ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc ruby2.7 rubygems-integration ssl-cert unhide unhide.rb
  unzip zip
Suggested packages:
  binutils-doc apache2 | lighttpd | httpd procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb
  postfix-sqlite sasl2-bin | dovecot-common resolvconf postfix-cdb postfix-doc liburi-perl libwww-perl ri ruby-dev
  bundler openssl-blacklist
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato javascript-common libbinutils libctf-nobfd0
  libctf0 libjs-jquery liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake rkhunter ruby ruby-minitest
  ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc ruby2.7 rubygems-integration ssl-cert unhide unhide.rb
  unzip zip
0 upgraded, 30 newly installed, 0 to remove and 35 not upgraded.
Need to get 11.4 MB of archives.
After this operation, 53.5 MB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu focal/main amd64 fonts-lato all 2.0-2 [2698 kB]
4% [1 fonts-lato 624 kB/2698 kB 23%]
```

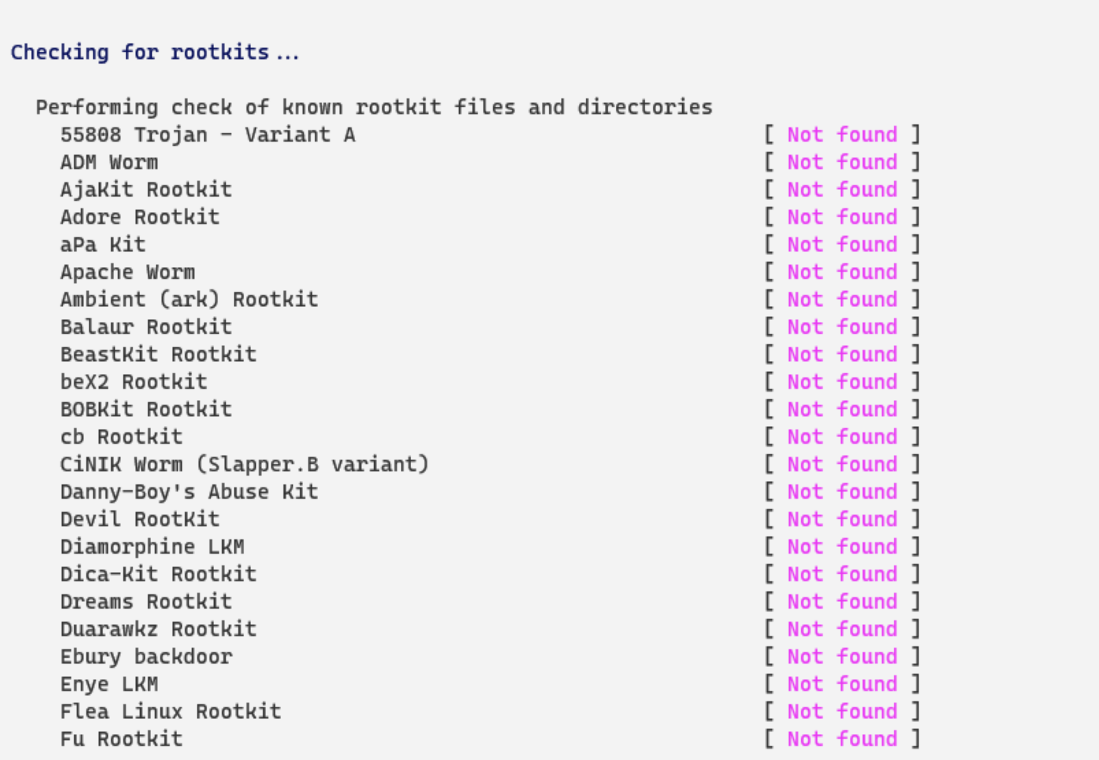
Check for Vulnerabilities by running rkhunter package with –check flag enabled,



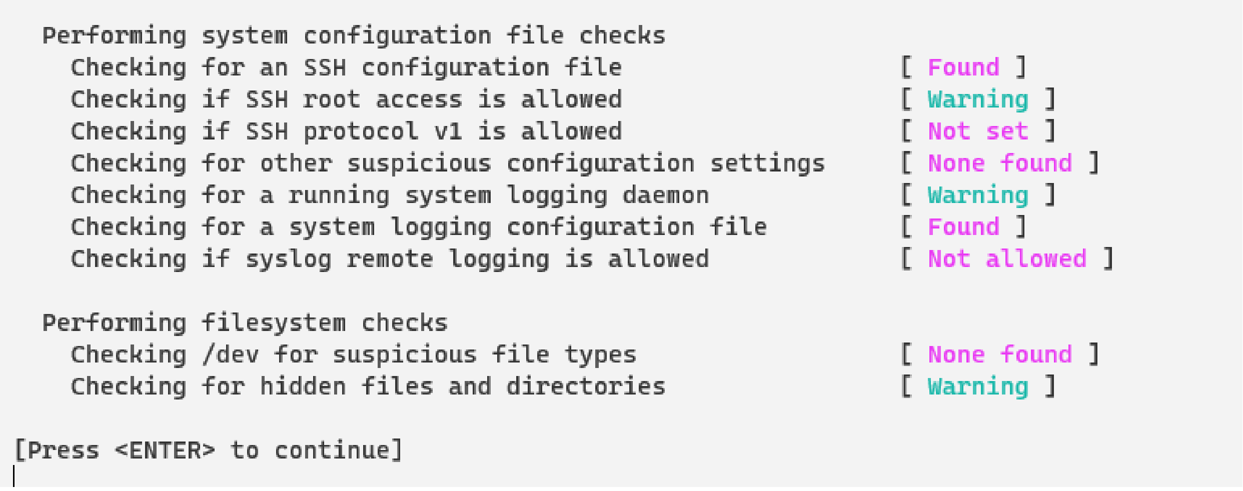
```
root@DESKTOP-2IDG8J0:~# rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

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/sbin/adduser                                    [ OK ]
    /usr/sbin/chroot                                     [ OK ]
    /usr/sbin/cron                                       [ OK ]
    /usr/sbin/depmod                                     [ OK ]
    /usr/sbin/fsck                                       [ OK ]
```



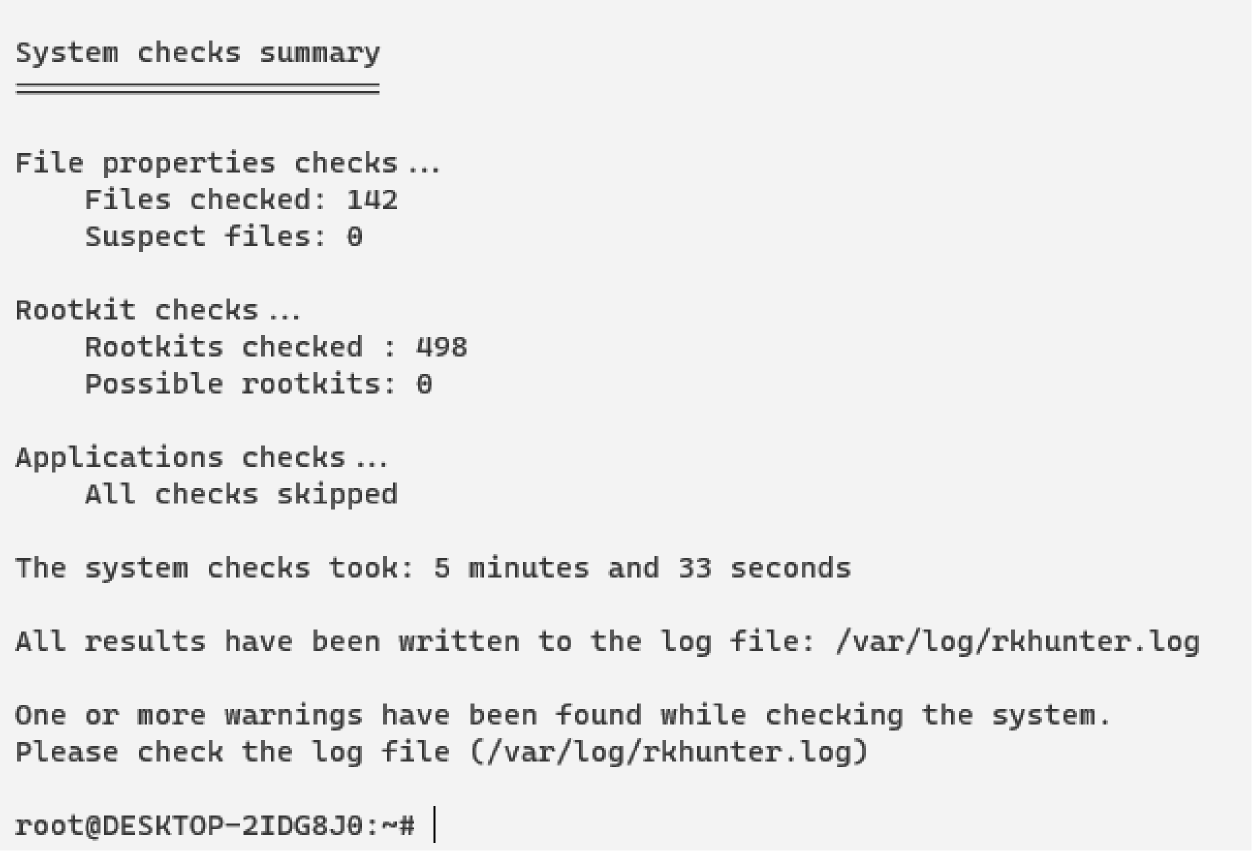
```
    /usr/bin/tr                                           [ OK ]
    /usr/bin/uname                                        [ OK ]
    /usr/bin/uniq                                         [ OK ]
    /usr/bin/users                                        [ OK ]
    /usr/bin/vmstat                                       [ OK ]
    /usr/bin/w                                            [ OK ]
    /usr/bin/watch                                        [ OK ]
    /usr/bin/wc                                           [ OK ]
    /usr/bin/wget                                         [ OK ]
    /usr/bin/whatis                                       [ OK ]
    /usr/bin/whereis                                      [ OK ]
    /usr/bin/which                                        [ OK ]
    /usr/bin/who                                          [ OK ]
    /usr/bin/whoami                                       [ OK ]
    /usr/bin/numfmt                                       [ OK ]
    /usr/bin/kmod                                         [ OK ]
    /usr/bin/systemd                                      [ OK ]
    /usr/bin/systemctl                                    [ OK ]
    /usr/bin/gawk                                         [ OK ]
    /usr/bin/bsd-mailx                                    [ OK ]
    /usr/bin/dash                                         [ OK ]
    /usr/bin/x86_64-linux-gnu-size                        [ OK ]
    /usr/bin/x86_64-linux-gnu-strings                     [ OK ]
    /usr/bin/telnet.netkit                                [ OK ]
    /usr/bin/w.procps                                     [ OK ]
    /usr/lib/systemd/systemd                              [ OK ]

[Press <ENTER> to continue]
```



```
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 ]
```



```
  Performing system configuration file checks
    Checking for an SSH configuration file                [ Found ]
    Checking if SSH root access is allowed                [ Warning ]
    Checking if SSH protocol v1 is allowed                [ Not set ]
    Checking for other suspicious configuration settings  [ None found ]
    Checking for a running system logging daemon          [ Warning ]
    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               [ None found ]
    Checking for hidden files and directories             [ Warning ]

[Press <ENTER> to continue]
```



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

File properties checks...
    Files checked: 142
    Suspect files: 0

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

Applications checks...
    All checks skipped

The system checks took: 5 minutes and 33 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)

root@DESKTOP-2IDG8J0:~#
```