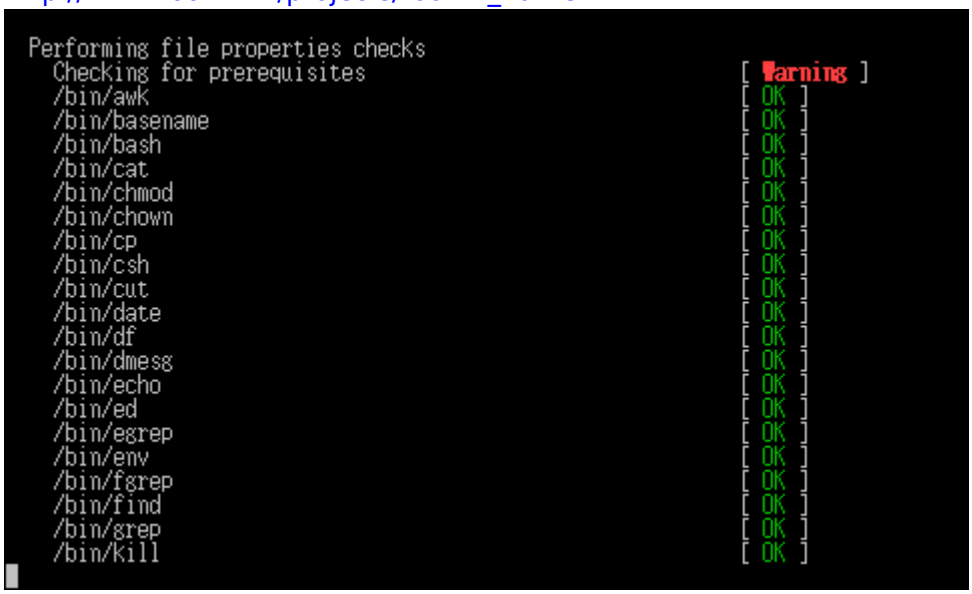
Security and System Auditing Tools

rkhunter

Rootkit Hunter (RKH) is an easy-to-use tool which checks computers running UNIX (clones) for the presence of rootkits and other unwanted tools.
http://www.rootkit.nl/projects/rootkit_hunter.html



chkrootkit

chkrootkit is a tool to locally check for signs of a rootkit. It contains:

- chkrootkit: shell script that checks system binaries for rootkit modification.
- ifpromisc: checks if the network interface is in promiscuous mode.
- chklastlog: checks for lastlog deletions.
- chkwtmp: checks for wtmp deletions.
- chkproc: checks for signs of LKM trojans.
- chkdirs: checks for signs of LKM trojans.
- strings: quick and dirty strings replacement.
- chkutmp: checks for utmp deletions.

http://www.chkrootkit.org/

```
Searching for rootedoor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... virbr0: not promisc and no PF_PACKET sockets
ppp0: not promisc and no PF_PACKET sockets
cscotun0: not promisc and no PF_PACKET sockets
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'...  The tty of the following user process(es) were not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! root         2492 tty1   /usr/bin/Xorg :0 -nr -verbose -auth /var/run/gdm/auth
-for-gdm-s5ved0/database -nolisten tcp vt1
chkutmp: nothing deleted
[root@r309-2 ~]#
```

lynis

Lynis is a security and system auditing tool. It scans a system on the most interesting parts useful for audits, like:

- Security enhancements
- Logging and auditing options
- Banner identification
- Software availability

Lynis is released as a GPL licensed project and free for everyone to use. See https://cisofy.com/lynis/ for a full description and documentation.

```
  - Scanning available tools...

[+] Boot and services
------------------------------------
  - Checking boot loaders
    - Checking presence GRUB...                             [ OK ]
      - Checking for password protection...                 [ WARNING ]
    - Checking presence LILO...                             [ NOT FOUND ]
    - Checking presence YABOOT...                           [ NOT FOUND ]
  - Check services at startup (chkconfig)...                [ DONE ]
       Result: found 45 services

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Kernel
------------------------------------
  - Checking default run level...
    Default level: 5                                        [ DONE ]
  - Checking CPU support (NX/PAE)
    CPU supports PAE and NoeXecute                          [ YES ]
  - Checking kernel version                                 [ DONE ]
  - Checking kernel type                                    [ DONE ]
```

sectool

sectool is a security tool that can be used both as a security audit and intrusion detection system. It consists of set of tests, library and command line interface tool. Tests are sorted into groups and

security levels. Admins can run certain tests, groups or whole security levels. The library and the tools are implemented in python and tests are language independent.
https://fedorahosted.org/sectool/

sectool-gui

sectool-gui provides a GTK-based graphical user interface to sectool.
https://fedorahosted.org/sectool/

rats

RATS scans through code, finding potentially dangerous function calls. The goal of this tool is not to definitively find bugs (yet). The current goal is to provide a reasonable starting point for performing manual security audits.
The initial vulnerability database is taken directly from things that could be easily found when starting with the forthcoming book, “Building Secure Software” by Viega and McGraw.
http://www.fortify.com/security-resources/rats.jsp

tiger

TIGER, or the “tiger” scripts, is a set of Bourne shell scripts, C programs and data files which are used to perform a security audit of UNIX systems. It is designed to hopefully be easy to use, easy to understand and easy to enhance.
http://www.nongnu.org/tiger/