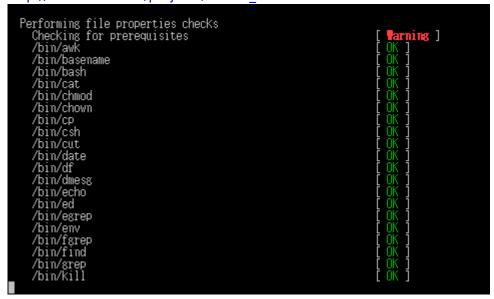
# **Security and System Auditing Tools**

#### 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/

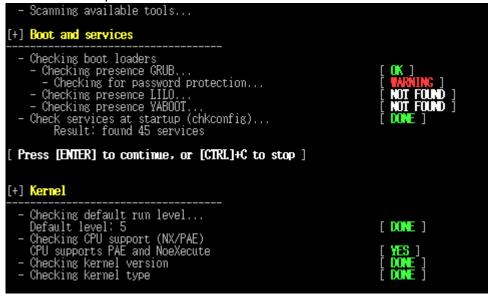
```
Searching for rootedoor... mothing found
Searching for ENYELKM rootkit default files... mothing found
Searching for common ssh-scanners default files... mothing found
Searching for anomalies in shell history files... mothing found
Checking `asp'... mot infected
Checking `bindshell'... mot infected
Checking `lkm'... chkproc: mothing detected
Checking `rexedcs'... mot found
Checking `rexedcs'... mot found
Checking `rexedcs'... mot found
Checking `rexedcs'... mot found
Checking `rexedcs'... mot promisc and mo PF_PACKET sockets
cscotun0: mot promisc and no PF_PACKET sockets
Checking `wf5808'... mot infected
Checking `wf5808'... mot infected
Checking `scalper'... mot infected
Checking `scalper'... mot infected
Checking `slapper'... mot infected
Checking `slapper'... mot infected
Checking `slapper'... mot infected
Checking `chkutmp'... The tty of the following user process(es) were mot 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-s5vedQ/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 <a href="https://cisofy.com/lynis/">https://cisofy.com/lynis/</a> for a full description and documentation.



#### 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/

From:

https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/security:audit

Last update: 2018/05/01 09:50

