PRACTICAL 9

AIM: Analyzing malware that uses rootkits to hide its presence on a system.

Description:

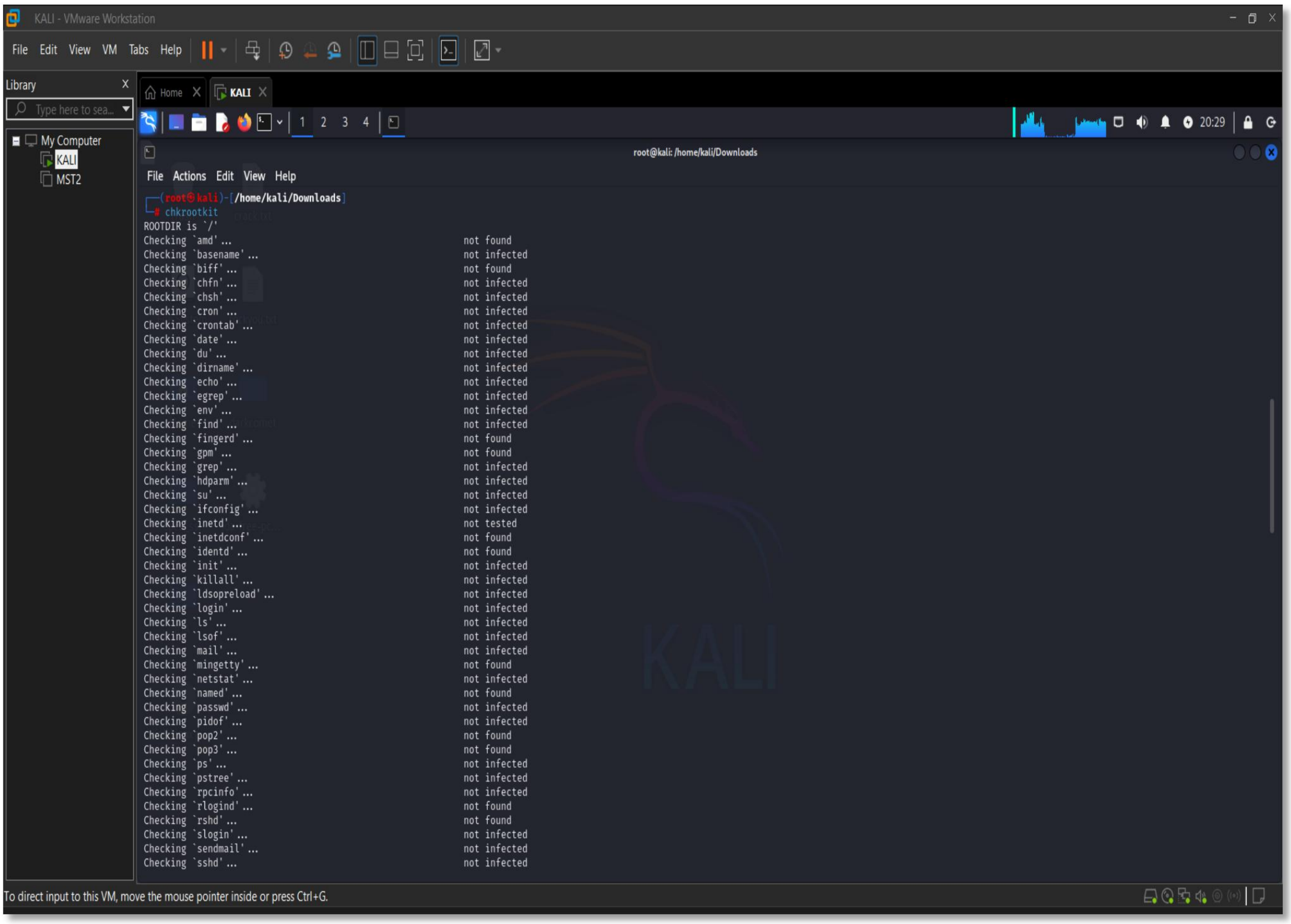
A rootkit is a type of stealthy malware that Operates with root/admin-level privileges Hides files, processes, registry keys, and network connections Often hooks or modifies kernel/system calls Can be user-mode or kernel-mode

Rootkits are dangerous because they persist across reboots, evade detection, and enable backdoors, data exfiltration, and command execution.

Step 1: Use Anti-Rootkit Scanners.

chkrootkit:

Checks for known rootkits
Detects anomalies in system binaries (e.g., ifconfig, ls, ps)

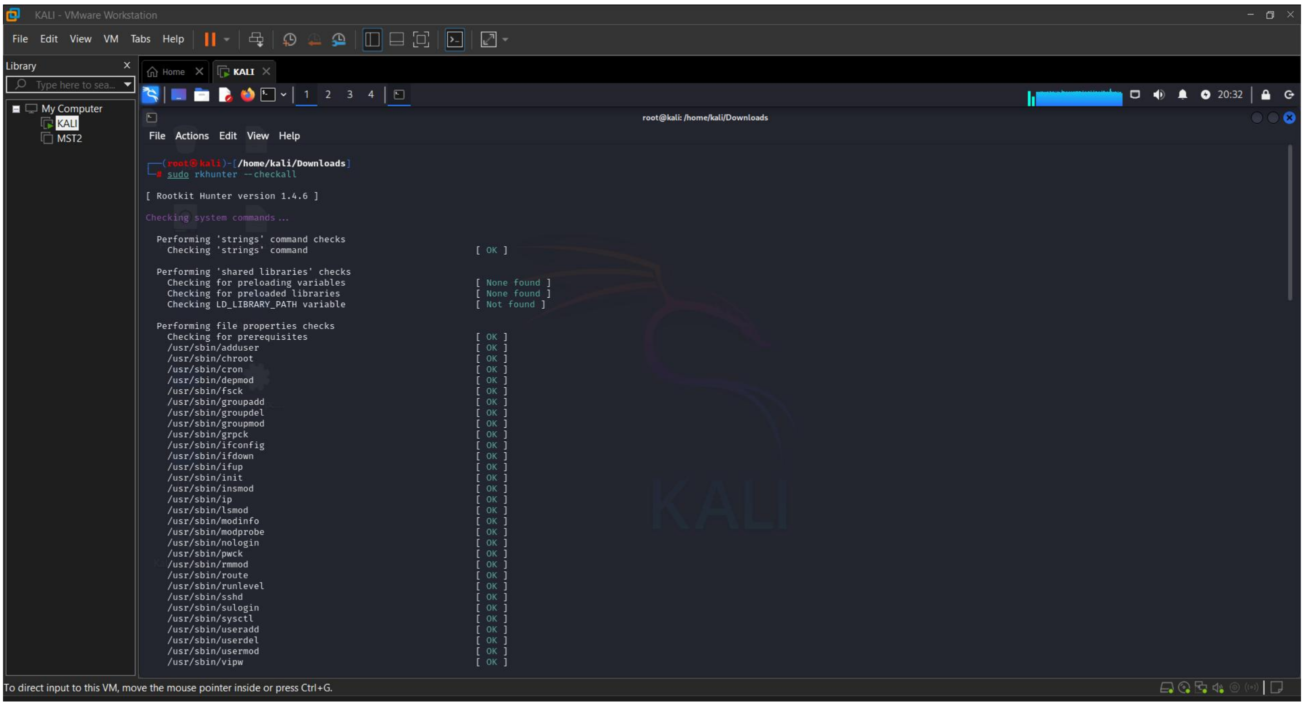


KALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
KALI
MST2
Home
KALI
1 2 3 4
20:29
root@kali: /home/kali/Downloads
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# chkrootkit
ROOTDIR is `/'
Checking `amd' ...                                          not found
Checking `basename' ...                                     not infected
Checking `biff' ...                                         not found
Checking `chfn' ...                                         not infected
Checking `chsh' ...                                         not infected
Checking `cron' ...                                         not infected
Checking `crontab' ...                                      not infected
Checking `date' ...                                         not infected
Checking `du' ...                                           not infected
Checking `dirname' ...                                      not infected
Checking `echo' ...                                         not infected
Checking `egrep' ...                                        not infected
Checking `env' ...                                          not infected
Checking `find' ...                                         not infected
Checking `fingerd' ...                                      not found
Checking `gpm' ...                                          not found
Checking `grep' ...                                         not infected
Checking `hdparm' ...                                       not infected
Checking `su' ...                                           not infected
Checking `ifconfig' ...                                     not infected
Checking `inetd' ...                                        not tested
Checking `inetdconf' ...                                    not found
Checking `identd' ...                                       not found
Checking `init' ...                                         not infected
Checking `killall' ...                                      not infected
Checking `ldsopreload' ...                                  not infected
Checking `login' ...                                        not infected
Checking `ls' ...                                           not infected
Checking `lsof' ...                                         not infected
Checking `mail' ...                                         not infected
Checking `mingetty' ...                                     not found
Checking `netstat' ...                                      not infected
Checking `named' ...                                        not found
Checking `passwd' ...                                       not infected
Checking `pidof' ...                                        not infected
Checking `pop2' ...                                         not found
Checking `pop3' ...                                         not found
Checking `ps' ...                                           not infected
Checking `pstree' ...                                       not infected
Checking `rpcinfo' ...                                      not infected
Checking `rlogind' ...                                      not found
Checking `rshd' ...                                         not found
Checking `slogin' ...                                       not infected
Checking `sendmail' ...                                     not infected
Checking `sshd' ...                                         not infected
```

Step 2: Use rkhunter (Rootkit Hunter):

rkhunter --checkall

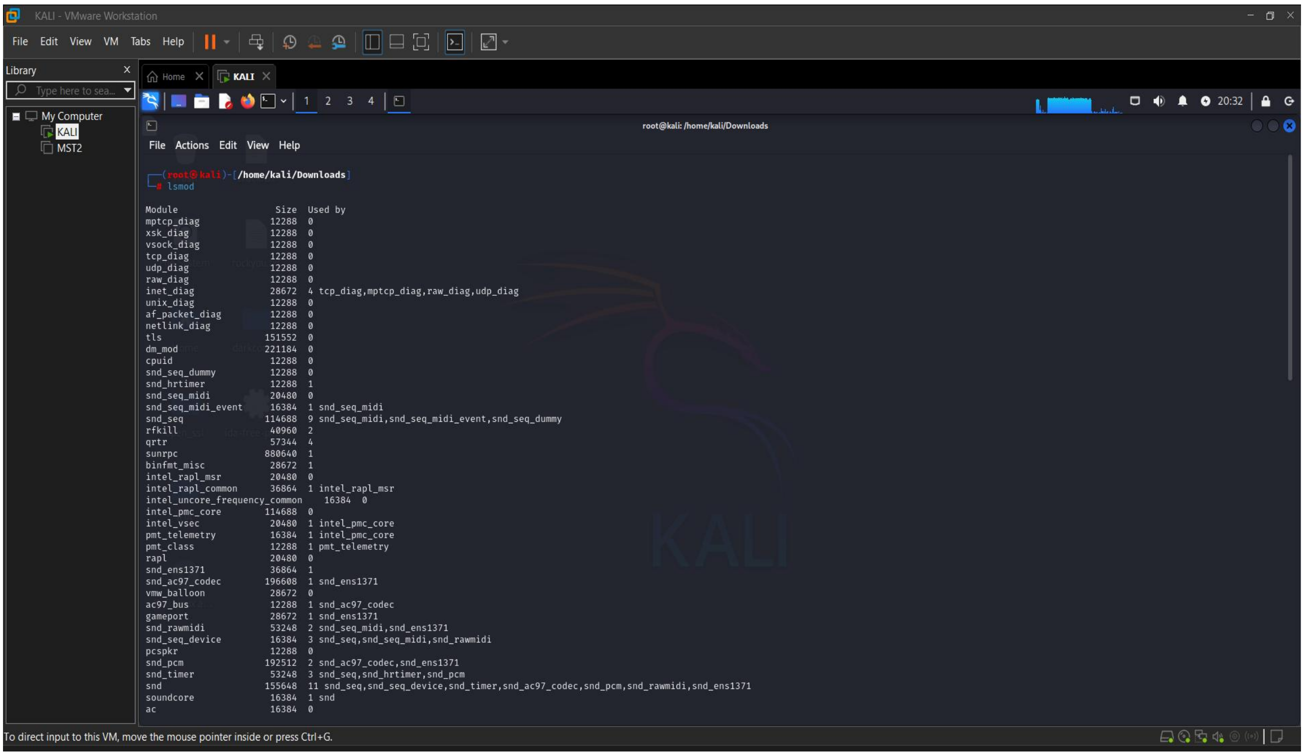

KALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
KALI
MST2
Home
KALI
1 2 3 4
20:32
root@kali: /home/kali/Downloads
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo rkhunter --checkall

[ 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/sbin/groupadd                                   [ OK ]
    /usr/sbin/groupdel                                   [ OK ]
    /usr/sbin/groupmod                                   [ OK ]
    /usr/sbin/grpck                                      [ OK ]
    /usr/sbin/ifconfig                                   [ OK ]
    /usr/sbin/ifdown                                     [ OK ]
    /usr/sbin/ifup                                       [ OK ]
    /usr/sbin/init                                       [ OK ]
    /usr/sbin/insmod                                     [ OK ]
    /usr/sbin/ip                                         [ OK ]
    /usr/sbin/lsmod                                      [ OK ]
    /usr/sbin/modinfo                                    [ OK ]
    /usr/sbin/modprobe                                   [ OK ]
    /usr/sbin/nologin                                    [ OK ]
    /usr/sbin/pwck                                       [ OK ]
    /usr/sbin/rmmod                                      [ OK ]
    /usr/sbin/route                                      [ OK ]
    /usr/sbin/runlevel                                   [ OK ]
    /usr/sbin/sshd                                       [ OK ]
    /usr/sbin/sulogin                                    [ OK ]
    /usr/sbin/sysctl                                     [ OK ]
    /usr/sbin/useradd                                    [ OK ]
    /usr/sbin/userdel                                    [ OK ]
    /usr/sbin/usermod                                    [ OK ]
    /usr/sbin/vipw                                       [ OK ]
```

Step 3: Analyze Kernel Modules

Rootkits often insert malicious kernel modules.

List loaded modules: lsmod


KALI - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to sea...
My Computer
KALI
MST2
Home
KALI
1 2 3 4
20:32
root@kali: /home/kali/Downloads
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# lsmod

Module                  Size  Used by
mptcp_diag             12288  0
xsk_diag               12288  0
vsock_diag             12288  0
tcp_diag               12288  0
udp_diag               12288  0
raw_diag               12288  0
inet_diag              28672  4 tcp_diag,mptcp_diag,raw_diag,udp_diag
unix_diag              12288  0
af_packet_diag         12288  0
netlink_diag           12288  0
tls                   151552  0
dm_mod                221184  0
cpuid                  12288  0
snd_seq_dummy          12288  0
snd_hrtimer            12288  1
snd_seq_midi           20480  0
snd_seq_midi_event     16384  1 snd_seq_midi
snd_seq               114688  9 snd_seq_midi,snd_seq_midi_event,snd_seq_dummy
rfkill                 40960  2
qrtr                   57344  4
sunrpc                880640  1
binfmt_misc            28672  1
intel_rapl_msr         20480  0
intel_rapl_common      36864  1 intel_rapl_msr
intel_uncore_frequency_common    16384  0
intel_pmc_core        114688  0
intel_vsec             20480  1 intel_pmc_core
pmt_telemetry          16384  1 intel_pmc_core
pmt_class              12288  1 pmt_telemetry
rapl                   20480  0
snd_ens1371            36864  1
snd_ac97_codec        196608  1 snd_ens1371
vmw_balloon            28672  0
ac97_bus               12288  1 snd_ac97_codec
gameport               28672  1 snd_ens1371
snd_rawmidi            53248  2 snd_seq_midi,snd_ens1371
snd_seq_device         16384  3 snd_seq,snd_seq_midi,snd_rawmidi
pcspkr                 12288  0
snd_pcm               192512  2 snd_ac97_codec,snd_ens1371
snd_timer              53248  3 snd_seq,snd_hrtimer,snd_pcm
snd                   155648  11 snd_seq,snd_seq_device,snd_timer,snd_ac97_codec,snd_pcm,snd_rawmidi,snd_ens1371
soundcore              16384  1 snd
ac                     16384  0
```

Conclusion:

Analyzing malware that uses rootkits requires advanced techniques, because rootkits are designed to hide their presence by manipulating system internals. On Kali Linux, tools like chkrootkit, rkhunter, and file integrity checkers like AIDE help you uncover these hidden threats. Always compare suspected systems to known-good baselines, and perform memory and disk analysis to detect signs of manipulation. Rootkit detection is an essential part of deep forensic investigations and system hardening.