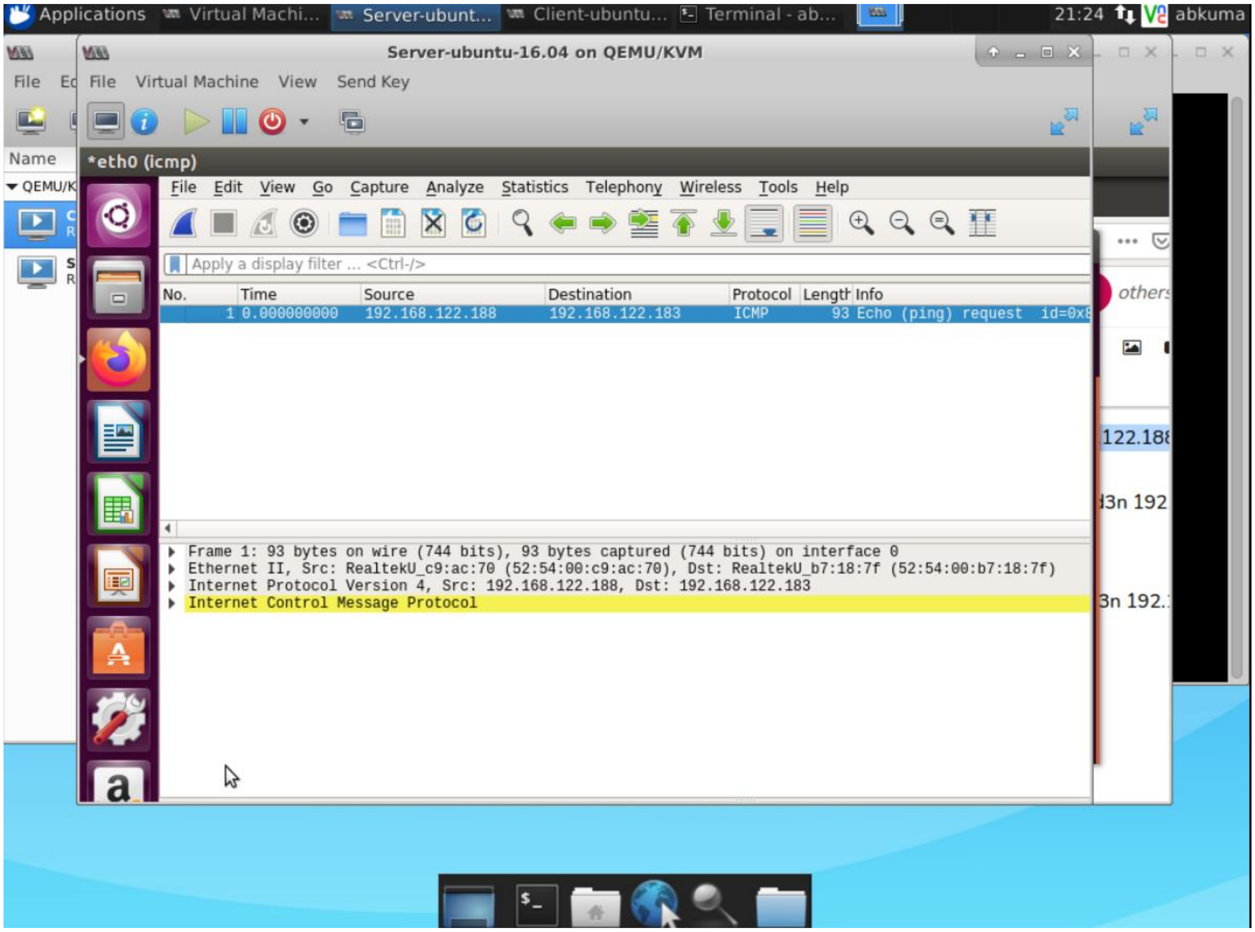
Lab 7 : Rootkit & Integrity check

Abhinav Kumar: abkuma@iu.edu

3.3 Data Capture

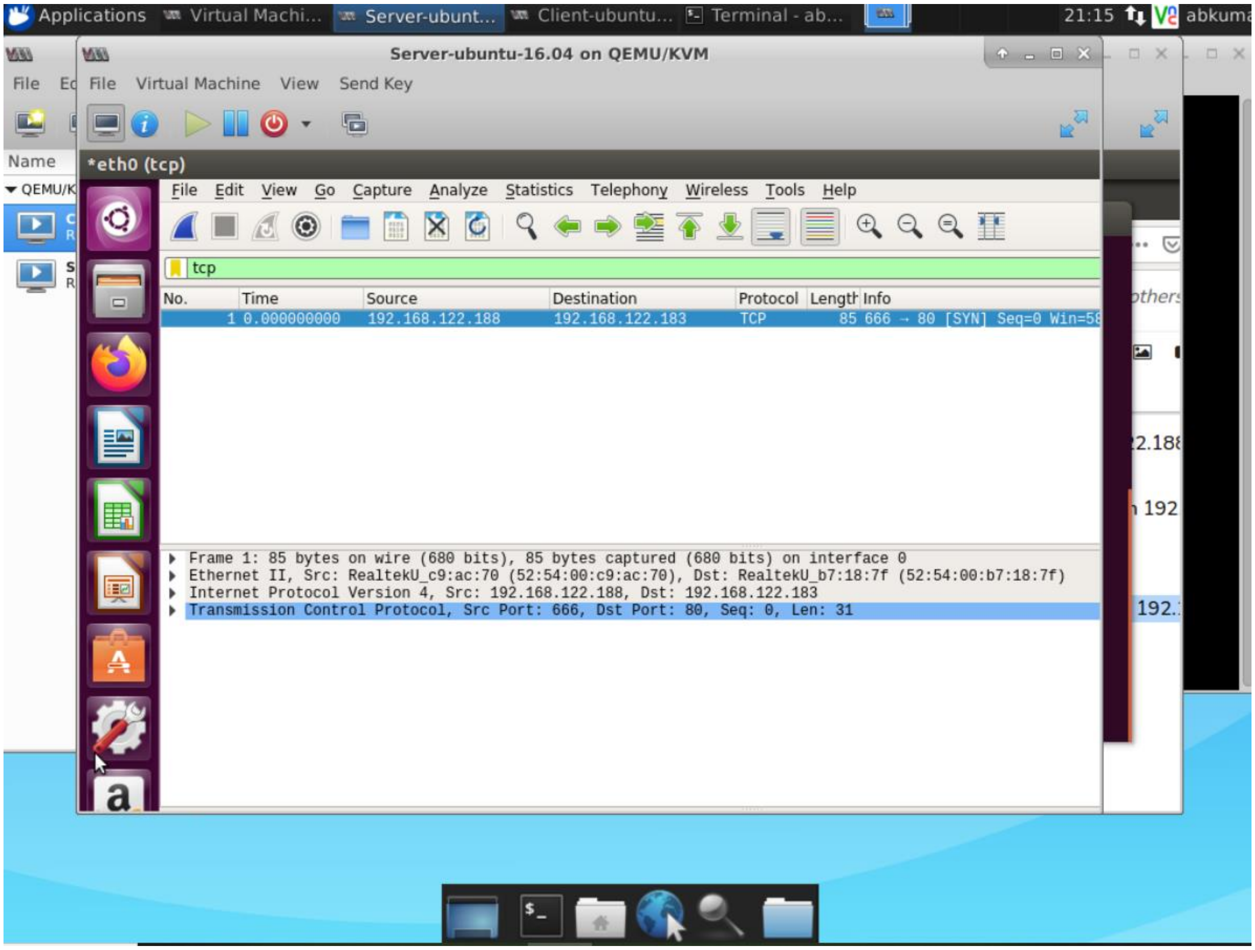
For ICMP



```
No.   Time         Source            Destination       Protocol Length Info
    1 0.000000000  192.168.122.188   192.168.122.183   ICMP         93 Echo (ping) request  id=0x8
```

```
▸ Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
▸ Ethernet II, Src: RealtekU_c9:ac:70 (52:54:00:c9:ac:70), Dst: RealtekU_b7:18:7f (52:54:00:b7:18:7f)
▸ Internet Protocol Version 4, Src: 192.168.122.188, Dst: 192.168.122.183
▸ Internet Control Message Protocol
```

For TCP

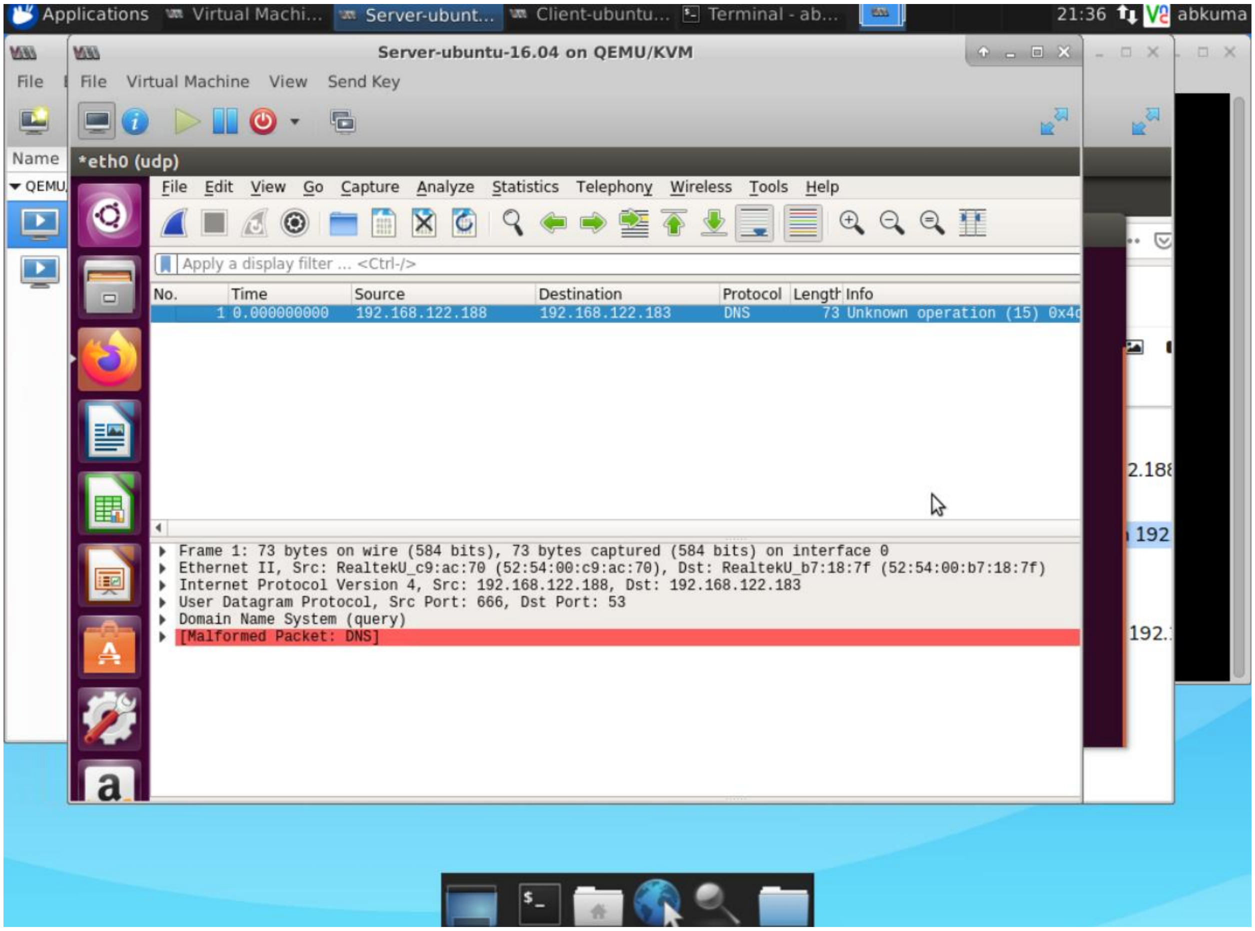


tcp

```
No.      Time          Source            Destination       Protocol Length Info
       1 0.000000000   192.168.122.188   192.168.122.183   TCP          85 666 → 80 [SYN] Seq=0 Win=58
```

```
▸ Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 0
▸ Ethernet II, Src: RealtekU_c9:ac:70 (52:54:00:c9:ac:70), Dst: RealtekU_b7:18:7f (52:54:00:b7:18:7f)
▸ Internet Protocol Version 4, Src: 192.168.122.188, Dst: 192.168.122.183
▸ Transmission Control Protocol, Src Port: 666, Dst Port: 80, Seq: 0, Len: 31
```

For UDP

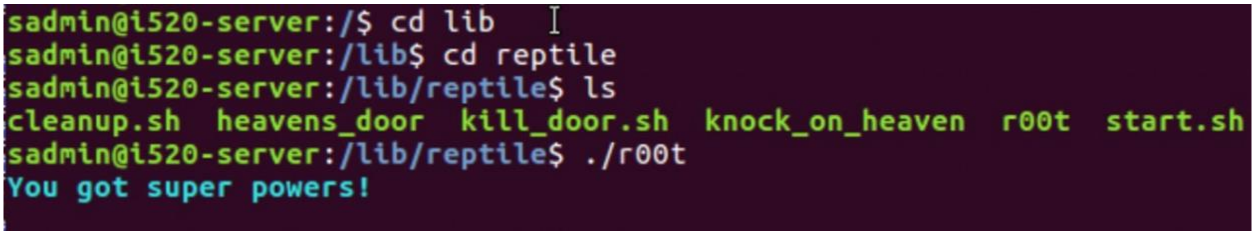


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.122.188	192.168.122.183	DNS	73	Unknown operation (15) 0x4c

```
▸ Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface 0
▸ Ethernet II, Src: RealtekU_c9:ac:70 (52:54:00:c9:ac:70), Dst: RealtekU_b7:18:7f (52:54:00:b7:18:7f)
▸ Internet Protocol Version 4, Src: 192.168.122.188, Dst: 192.168.122.183
▸ User Datagram Protocol, Src Port: 666, Dst Port: 53
▸ Domain Name System (query)
▸ [Malformed Packet: DNS]
```

3.4. Assuming Root Privileges without sudo

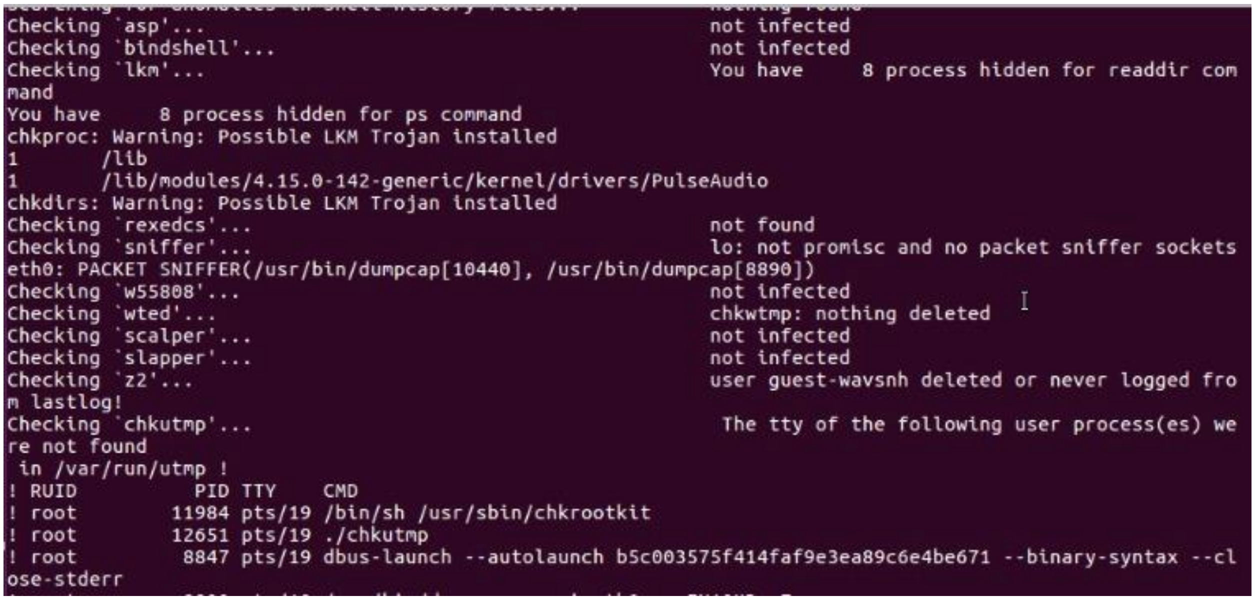
We can see You got super powers!



```
sadmin@i520-server:/$ cd lib
sadmin@i520-server:/lib$ cd reptile
sadmin@i520-server:/lib/reptile$ ls
cleanup.sh  heavens_door  kill_door.sh  knock_on_heaven  r00t  start.sh
sadmin@i520-server:/lib/reptile$ ./r00t
You got super powers!
```

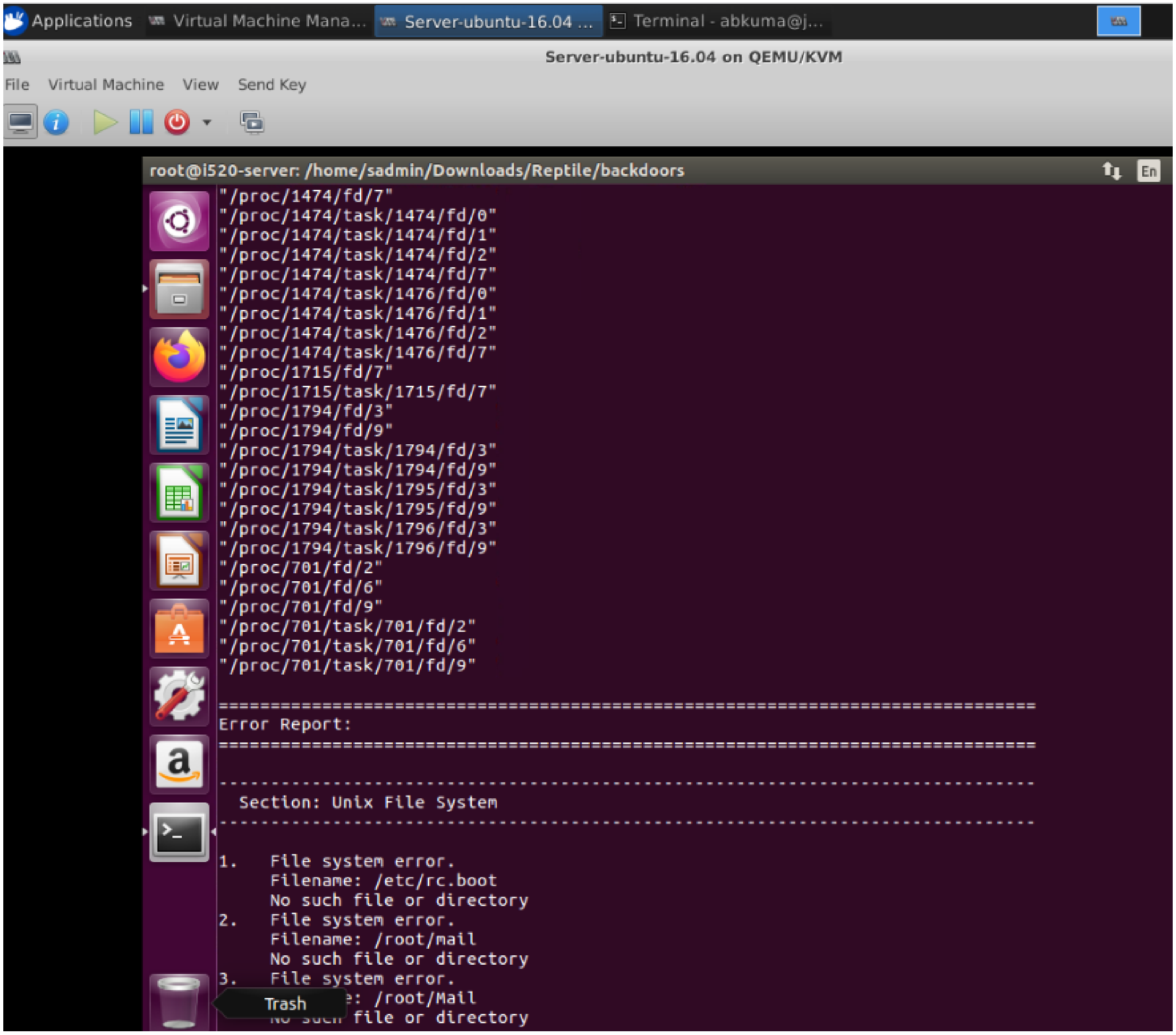
3.5 Rookit Detection

Chkrootkit : Running 'sudo chkrootkit' displays a list of all applications and determines whether any rootkits are present in the processes.



```
Checking `asp'...                                           not infected
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           You have     8 process hidden for readdir com
mand
You have     8 process hidden for ps command
chkproc: Warning: Possible LKM Trojan installed
1       /lib
1       /lib/modules/4.15.0-142-generic/kernel/drivers/PulseAudio
chkdirs: Warning: Possible LKM Trojan installed
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer sockets
eth0: PACKET SNIFFER(/usr/bin/dumpcap[10440], /usr/bin/dumpcap[8890])
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            user guest-wavsnh deleted or never logged fro
m lastlog!
Checking `chkutmp'...                                        The tty of the following user process(es) we
re not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! root        11984 pts/19 /bin/sh /usr/sbin/chkrootkit
! root        12651 pts/19 ./chkutmp
! root         8847 pts/19 dbus-launch --autolaunch b5c003575f414faf9e3ea89c6e4be671 --binary-syntax --cl
ose-stderr
```

Tripwire : Tripwire creates a hash (fingerprint) of all the files on your system and notifies you when one of them changes. It enables you to use a remote host as your "trusted" machine, scanning your target machines for any file changes. If you notice a change, you know something is amiss. Of course, you'll need some form of change control so that ordinary system upgrades don't get detected as an intrusion.



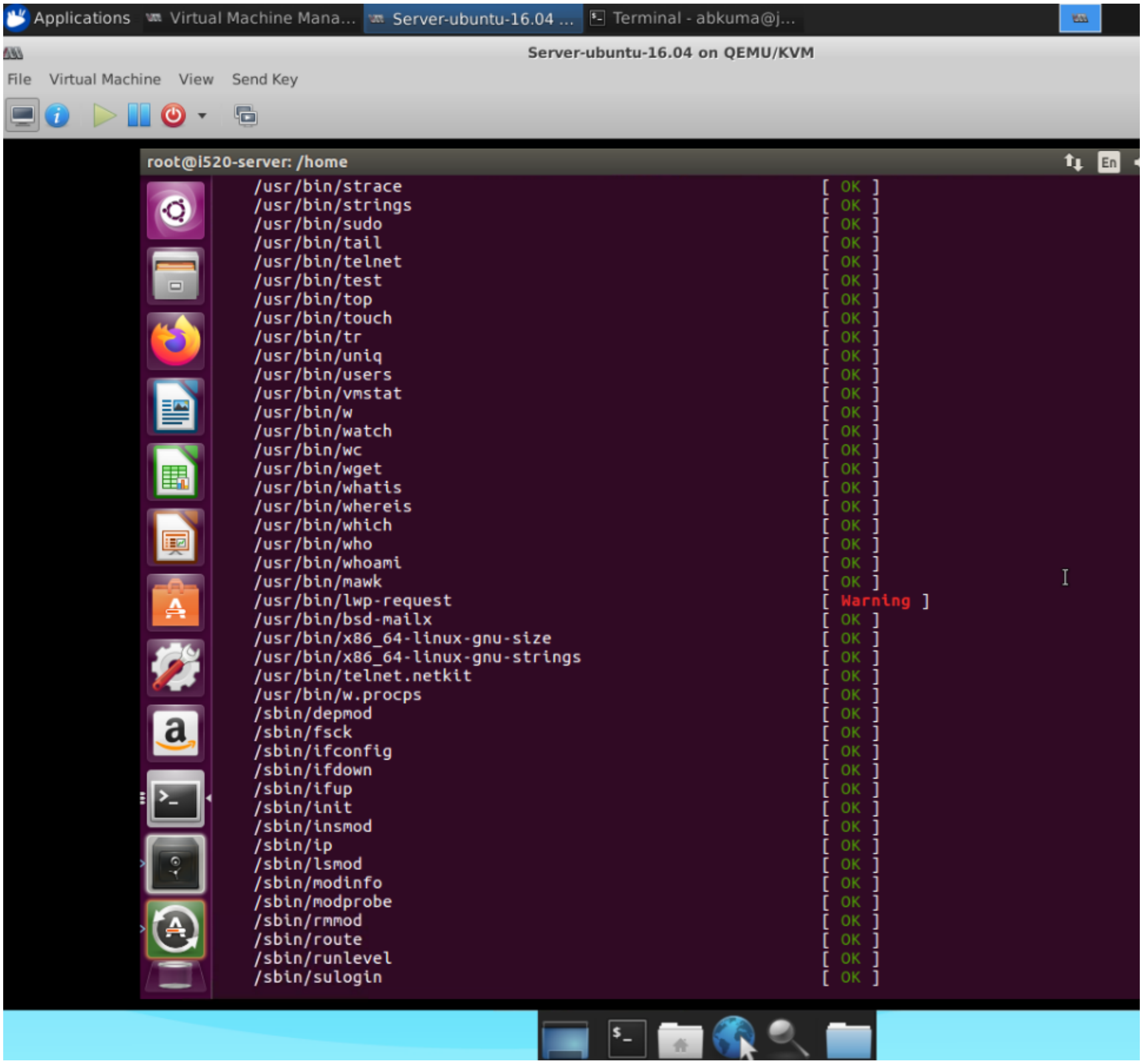
```
"/proc/1474/fd/7"
"/proc/1474/task/1474/fd/0"
"/proc/1474/task/1474/fd/1"
"/proc/1474/task/1474/fd/2"
"/proc/1474/task/1474/fd/7"
"/proc/1474/task/1476/fd/0"
"/proc/1474/task/1476/fd/1"
"/proc/1474/task/1476/fd/2"
"/proc/1474/task/1476/fd/7"
"/proc/1715/fd/7"
"/proc/1715/task/1715/fd/7"
"/proc/1794/fd/3"
"/proc/1794/fd/9"
"/proc/1794/task/1794/fd/3"
"/proc/1794/task/1794/fd/9"
"/proc/1794/task/1795/fd/3"
"/proc/1794/task/1795/fd/9"
"/proc/1794/task/1796/fd/3"
"/proc/1794/task/1796/fd/9"
"/proc/701/fd/2"
"/proc/701/fd/6"
"/proc/701/fd/9"
"/proc/701/task/701/fd/2"
"/proc/701/task/701/fd/6"
"/proc/701/task/701/fd/9"

==============================================================================
Error Report:
==============================================================================

------------------------------------------------------------------------------
  Section: Unix File System
------------------------------------------------------------------------------

1.    File system error.
      Filename: /etc/rc.boot
      No such file or directory
2.    File system error.
      Filename: /root/mail
      No such file or directory
3.    File system error.
      Filename: /root/Mail
      No such file or directory
```

Rkhunter



```
  /usr/bin/strace                                          [ OK ]
  /usr/bin/strings                                         [ OK ]
  /usr/bin/sudo                                            [ OK ]
  /usr/bin/tail                                            [ OK ]
  /usr/bin/telnet                                          [ OK ]
  /usr/bin/test                                            [ OK ]
  /usr/bin/top                                             [ OK ]
  /usr/bin/touch                                           [ OK ]
  /usr/bin/tr                                              [ 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/mawk                                            [ OK ]
  /usr/bin/lwp-request                                     [ Warning ]
  /usr/bin/bsd-mailx                                       [ 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 ]
  /sbin/depmod                                             [ OK ]
  /sbin/fsck                                               [ OK ]
  /sbin/ifconfig                                           [ OK ]
  /sbin/ifdown                                             [ OK ]
  /sbin/ifup                                               [ OK ]
  /sbin/init                                               [ OK ]
  /sbin/insmod                                             [ OK ]
  /sbin/ip                                                 [ OK ]
  /sbin/lsmod                                              [ OK ]
  /sbin/modinfo                                            [ OK ]
  /sbin/modprobe                                           [ OK ]
  /sbin/rmmod                                              [ OK ]
  /sbin/route                                              [ OK ]
  /sbin/runlevel                                           [ OK ]
  /sbin/sulogin                                            [ OK ]
```

4.0

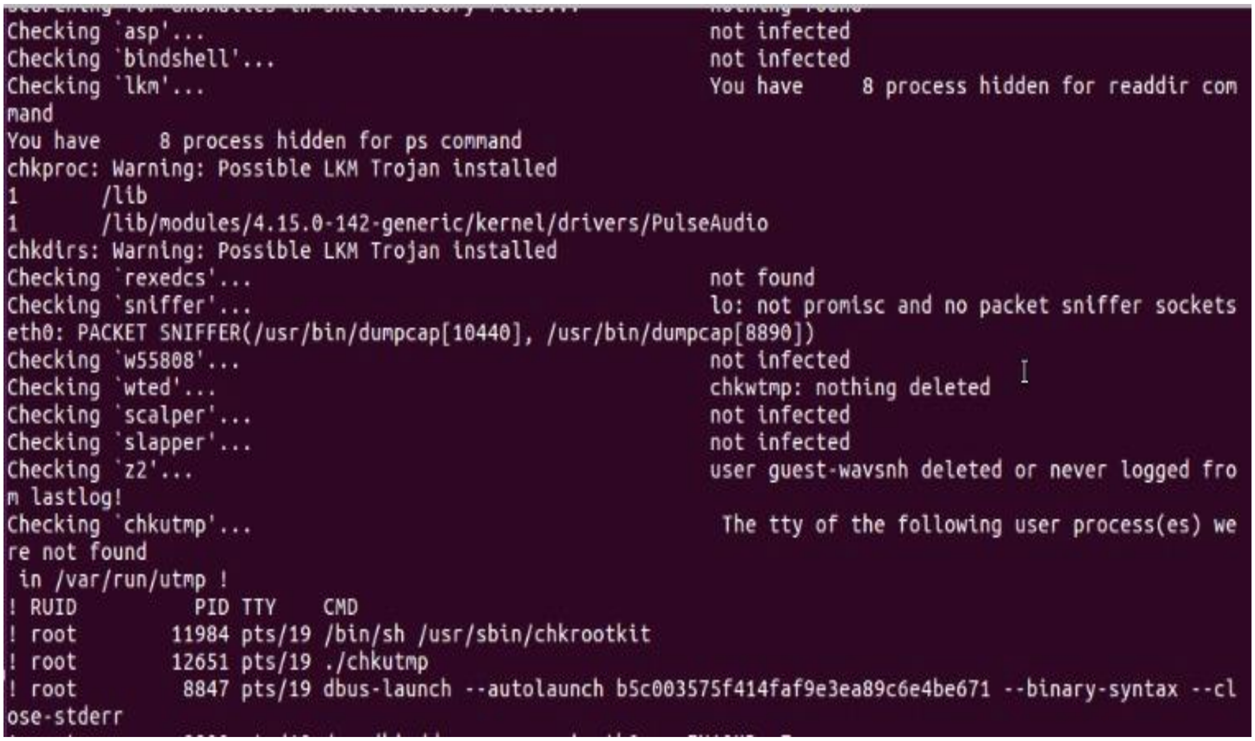
1)How did you determine that the rootkit is installed? Did tripwire find the rootkit? If so, what did tripwire tell you about it? If not, what other tools helped you to find the rootkit? What is the output (screenshot) of the detection?

Rootkit is a type of malware that is present on a computer but is undetectable. Rootkits are usually in a format that is not easy to read. Tripwire was unable to detect the rootkit, as can be shown. It simply informs us about the various procedures.

Tripwire verifies the directories and files with the database established and notifies us if there are any changes. It produces an error report that lists all of the changes and errors that were discovered.

So according to me, rkhunter, chkrootkit and unhide are much better to detect the presence of

rootkit than tripwire since they provide us more detailed information.



```
Checking `asp'...                                           not infected
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           You have     8 process hidden for readdir com
mand
You have     8 process hidden for ps command
chkproc: Warning: Possible LKM Trojan installed
1       /lib
1       /lib/modules/4.15.0-142-generic/kernel/drivers/PulseAudio
chkdirs: Warning: Possible LKM Trojan installed
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer sockets
eth0: PACKET SNIFFER(/usr/bin/dumpcap[10440], /usr/bin/dumpcap[8890])
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            user guest-wavsnh deleted or never logged fro
m lastlog!
Checking `chkutmp'...                                        The tty of the following user process(es) we
re not found
 in /var/run/utmp !
! RUID          PID TTY    CMD
! root        11984 pts/19 /bin/sh /usr/sbin/chkrootkit
! root        12651 pts/19 ./chkutmp
! root         8847 pts/19 dbus-launch --autolaunch b5c003575f414faf9e3ea89c6e4be671 --binary-syntax --cl
ose-stderr
```

<span style="color:red">2)Where is the rootkit installed in the server VM?</span>

It is installed under /lib/reptile directory. We also saw some odd behavior in the unhide folders, indicating that the rootkit is indeed present in the lib folder.

3)If you use none of the above tools (tripwire, chkrootkit, rkhunter, unhide, and unhide.rb), how can you find the rootkit and/or detect its existence?

We can use tools to check the communication on different ports. A monitoring system can be set up to identify unauthorized communication coming to and from system ports and notify the same alerts to check the existence of the rootkit. Few other methods can be used like behavior analysis can be used. Under this a rootkit is activated, the system will begin sending data in the background, slowing it down or causing it to behave in unexpected ways. It's a clear indication that something is wrong with the system which will help to detect the existence of rootkit. One more way is the system memory search . Under which search the system memory of your computer to discover if anything is out of order. Check all access points for signs of invoked processes during the search, and keep track of any imported library calls from Dynamic-Link Libraries. Some of them can be connected or diverted to do other tasks.

4)Can you disable the backdoor of the rootkit without uninstalling the rootkit or removing it?

We can find the process ID and terminate it. We can try looking for the port number it's using, then the process id, and finally the executable that's been allocated to process id. We go there and we can delete the executable or linked file by getting the file.

5)How can you completely disable the rootkit? Do not use the script that the rootkit provides.

1)Manual removal: Under this we manually search for the boot log files for any known rootkit names. Any file which is found can be denied permission for all the users which should render them inactive until complete removal is possible usually after all other appended files have been located and neutralized.

2)Semi-automatic method: Under this we use a scan application to find the rootkit files, and then delete them manually.

3)Automatic Rootkit: Under this several specialist pieces of software that employ various combinations of signature-based analysis; detecting interceptions; data comparison from different sources; integrity checking; registry comparisons, to locate the rootkit and related components and to remove them.

4)Remove Rootkit by Reformat and Install: Under this we will back up our non-exe. files to a remote location. Then we will reformat the drive and reinstall the operating system to kill all rootkits apart from those in the BIOS-level.