

Lab 1 – Testing Kali Linux

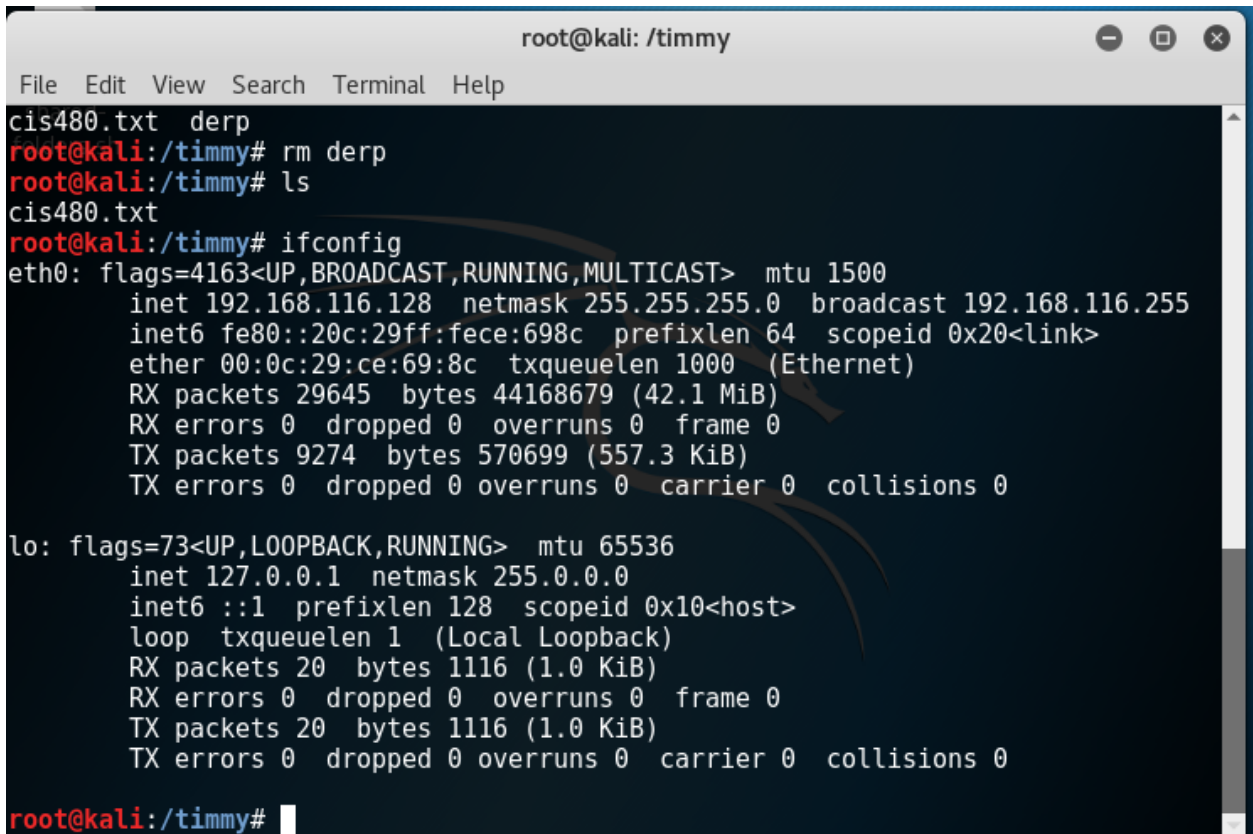
- This is an individual assignment, and worth 20 points.
- The due date and time is 4:00 Thur, September 7 (Sec 01) / 7:00 Thur, September 7 (Sec 76).
- You need to provide your answers to the “Lab1-Outcome.docx.” Change the file name following the naming convention suggested below.
- Naming convention is as follows: homework, hypen, last name, first initial, and extension (e.g., Lab1-Outcome-ImG.docx). If you do not follow the convention, I will deduct 1.
- Make screenshots small so that you can save space.

Tasks

- (Task 1) For this task, you should read the file “Basic Linux Commands for Linux Terminal Beginners (pcsteps.com).pdf” on posted the Blackboard.
 - Open a terminal.
 - On root, create a directory with your first name.
 - Within the directory you created, create an empty file named “cis480.txt”.
 - Using “echo” command, add the text “test1” to the text file.
 - Using “echo” command, append the text “test2” to the text file.
 - Using “cat” command, display the content in the “cis480.txt”.
 - Using “grep” command, search for “test1”.
 - On root, using “tar” command, compress everything in your directory.
 - Delete the compressed file.
- Show the commands you executed and outcomes in one or two screenshots.
- (Task 1) Take screenshots of the outcome.

```
root@kali: /timmy
File Edit View Search Terminal Help
root@kali:~# mkdir /timmy
root@kali:~# touch /timmy/cis480.txt
root@kali:~# echo test1 >> /timmy/cis480.txt
root@kali:~# echo test2 >> /timmy/cis480.txt
root@kali:~# cat /timmy/cis480.txt
test1
test2
root@kali:~# grep test1 /timmy/cis480.txt
test1
root@kali:~# tar -cf /timmy/derp /timmy/cis480.txt
tar: Removing leading '/' from member names
root@kali:~# cd /timmy
root@kali:/timmy# tar -cf derp cis480.txt
root@kali:/timmy# ls
cis480.txt  derp
root@kali:/timmy# rm derp
root@kali:/timmy# ls
cis480.txt
root@kali:/timmy#
```

- (Task 2) Let's try **ifconfig** command. The Windows equivalent is ipconfig. The commands you can use are:
 - ifconfig --help (for help)
 - ifconfig (to get the IP address of your system)
- Run a **ifconfig** command to display the IP address, netmask, broadcast associated with the Kali. Take a screenshot of the outcome.
 - (Task 2) Take a screenshot of the outcome.



```
root@kali: /timmy
File Edit View Search Terminal Help
cis480.txt derp
root@kali:/timmy# rm derp
root@kali:/timmy# ls
cis480.txt
root@kali:/timmy# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.116.128 netmask 255.255.255.0 broadcast 192.168.116.255
    inet6 fe80::20c:29ff:fece:698c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:ce:69:8c txqueuelen 1000 (Ethernet)
    RX packets 29645 bytes 44168679 (42.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9274 bytes 570699 (557.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:/timmy#
```

(Task 3) Let's next try **netstat** to display the ports that are open in your system. The state of each port can be listening, waiting, or connected. **netstat** by default does not tell which service is leading a port to be open.

- Run a **netstat** command to display the listening server sockets. Take a screenshot of the outcome. If the screen displays too many entries, you can resize the screen after zooming in/out (View > Zoom In/Out).

(Task 3) Take a screenshot of the outcome.

```
root@kali: /timmy# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags   Type       State           I-Node  Path
unix  2      [ ]     DGRAM      0
unix  2      [ ]     DGRAM      0
unix  3      [ ]     DGRAM      0
unix  2      [ ]     DGRAM      0
unix  2      [ ]     DGRAM      0
unix 15      [ ]     DGRAM      0
unix  7      [ ]     DGRAM      0
unix  3      [ ]     STREAM    CONNECTED      15303
unix  3      [ ]     STREAM    CONNECTED      19530
unix  3      [ ]     STREAM    CONNECTED      16819 /run/user/131/bus
unix  3      [ ]     STREAM    CONNECTED      18412 /run/systemd/journal/stdout
unix  3      [ ]     STREAM    CONNECTED      14843 /run/user/131/bus
unix  3      [ ]     STREAM    CONNECTED      18474
unix  3      [ ]     STREAM    CONNECTED      18310 /run/user/0/bus
unix  3      [ ]     STREAM    CONNECTED      15301
unix  3      [ ]     STREAM    CONNECTED      15266
unix  3      [ ]     STREAM    CONNECTED      20504
unix  2      [ ]     DGRAM      0
unix  2      [ ]     DGRAM      0
unix  3      [ ]     STREAM    CONNECTED      16290
unix  3      [ ]     STREAM    CONNECTED      18413 /run/systemd/journal/stdout
```

- (Task 4) Next, let's try **tracert** (tracert in Windows) to trace the route to the destination by sending ICMP Echo Request messages.
 - tracert (for options)
 - tracert www.louisville.edu
- Run a **tracert** command to trace the route to www.louisvilleky.gov. Take a screenshot of the outcome.
 - (Task 4) Take a screenshot of the outcome.

```
C:\Users\tim.mahan>tracert www.louisvilleky.gov

Tracing route to www.louisvilleky.gov [50.19.81.233]
over a maximum of 30 hops:

  1      *          *          77 ms  10.200.255.254
  2      2 ms      2 ms      2 ms  jsr-wlan-v705-1.louisville.edu [136.165.223.126]
  3      7 ms      2 ms      2 ms  eks-gig-v309.bb.louisville.edu [136.165.254.93]
  4     10 ms      3 ms      2 ms  mitc-gig-v307.bb.louisville.edu [136.165.254.138]
  5     32 ms      4 ms      2 ms  rtr-blk-v903.kec.net [199.120.154.41]
  6      3 ms      3 ms      3 ms  rtr-ky-ron-i2-blk.kec.net [199.120.154.82]
  7      3 ms      2 ms      2 ms  128.163.164.170
  8      7 ms      7 ms      7 ms  et-7-0-0.4079.sdn-sw.cinc.net.internet2.edu [162.252.70.88]
  9      8 ms      7 ms     10 ms  et-7-0-0.4079.sdn-sw.indi.net.internet2.edu [162.252.70.87]
 10     13 ms     13 ms     13 ms  et-3-1-0.4079.rtsw.chic.net.internet2.edu [162.252.70.78]
 11     32 ms     29 ms     32 ms  et-0-1-0.4079.sdn-sw.ashb.net.internet2.edu [162.252.70.60]
 12     27 ms     27 ms     31 ms  et-10-0-0.4079.rtr.ashb.net.internet2.edu [162.252.70.75]
 13     28 ms     27 ms     31 ms  64.57.30.39
 14      *          *          *      Request timed out.
 15      *          *          *      Request timed out.
 16    2466 ms    2319 ms    2147 ms  54.239.110.175
 17     30 ms     31 ms     28 ms  54.239.111.31
 18     51 ms     52 ms     69 ms  52.93.24.8
 19     28 ms     28 ms     28 ms  52.93.24.5
 20      *          *          *      Request timed out.
 21      *          *          *      Request timed out.
 22      *          *          *      Request timed out.
 23      *          *          *      Request timed out.
 24      *          *          *      Request timed out.
 25     89 ms     29 ms     29 ms  ec2-50-19-81-233.compute-1.amazonaws.com [50.19.81.233]

Trace complete.
```

- (Task 5) Let's try **ping** to test the connection to a host.
Run a **ping** command to test the connection to www.louisvilleky.gov. Send the ECHO REQUEST message five times only. For this, you have to use count option (-c). Take a screenshot of the outcome.

(Task 5) Take a screenshot of the outcome.

```

root@kali: /timmy
File Edit View Search Terminal Help
unix 3 [ ] STREAM CONNECTED 17850 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 19711 /var/run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 18119 /var/run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 17637 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 18379 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 20715 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 19837 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 17242 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 9048 /run/systemd/journal/stdout
root@kali:/timmy# ping www.louisvilleky.gov -c 5
PING www.louisvilleky.gov (50.19.81.233) 56(84) bytes of data.
64 bytes from ec2-50-19-81-233.compute-1.amazonaws.com (50.19.81.233): icmp_seq=1 ttl=128 time=28.2 ms
64 bytes from ec2-50-19-81-233.compute-1.amazonaws.com (50.19.81.233): icmp_seq=2 ttl=128 time=30.3 ms
64 bytes from ec2-50-19-81-233.compute-1.amazonaws.com (50.19.81.233): icmp_seq=3 ttl=128 time=30.3 ms
64 bytes from ec2-50-19-81-233.compute-1.amazonaws.com (50.19.81.233): icmp_seq=4 ttl=128 time=29.2 ms
64 bytes from ec2-50-19-81-233.compute-1.amazonaws.com (50.19.81.233): icmp_seq=5 ttl=128 time=30.3 ms

--- www.louisvilleky.gov ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 28.296/29.737/30.394/0.840 ms
root@kali:/timmy#

```