

NAME: TEMIDAYO OLUWARANTIMI BLESSING

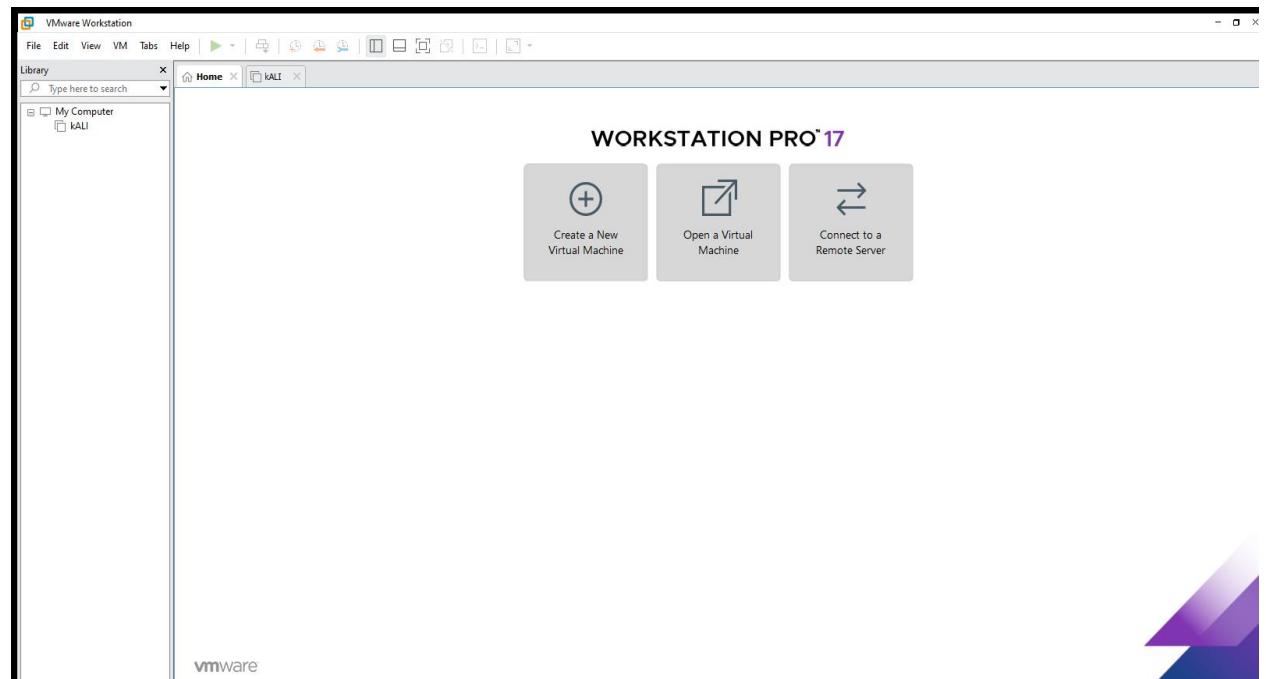
STUDENT ID: IDEAS/24/51291

Lab 1: Investigate Kali Linux Objectives

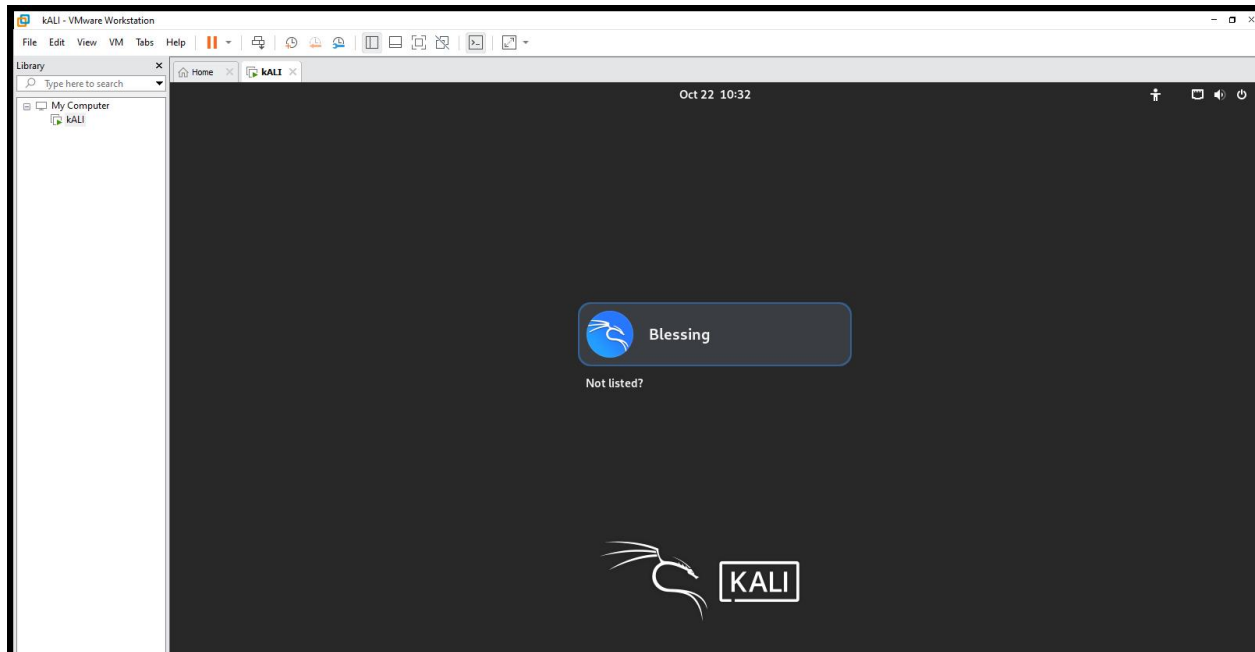
- **Familiarization of Kali Linux GUI**

1. Start Virtual Machine (VM), power on the already installed Kali. The default username is Kali while the default password is Kali. While the Kali from the institute AIVTIC default username and password is aivtic.
2. Explore the desktop to be familiar with its operations.
3. Customize the panel.
4. Access Settings.

PICTURE OF VM
LAYOUT



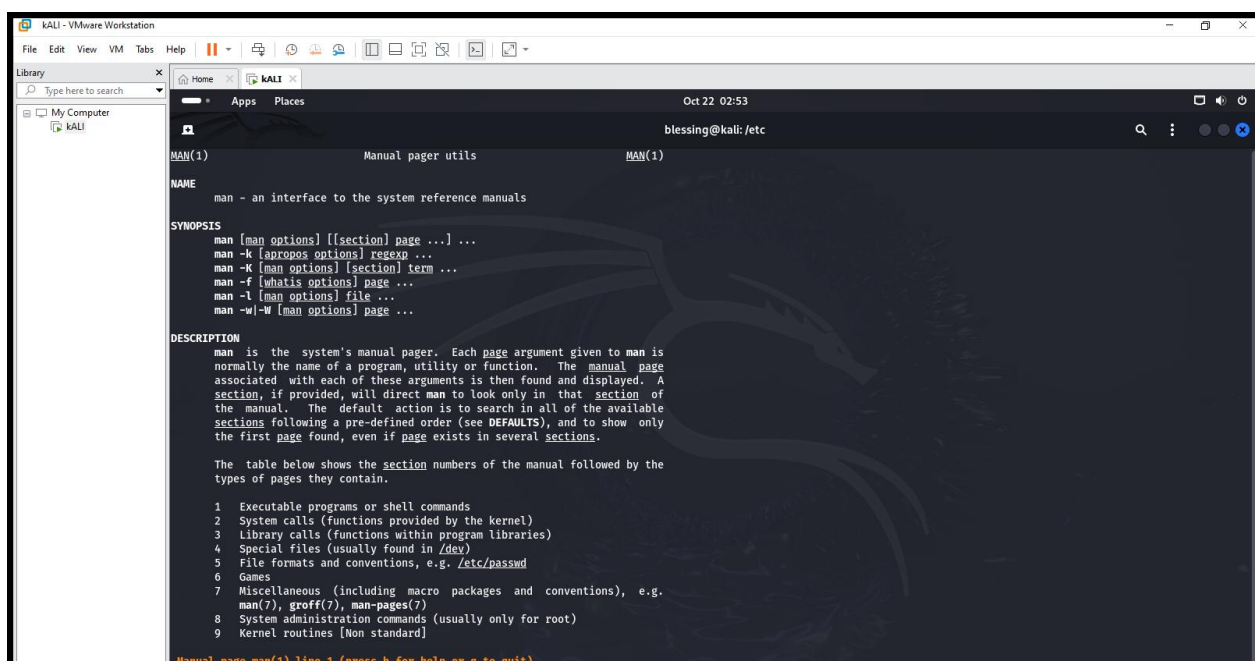
KALI LAYOUT



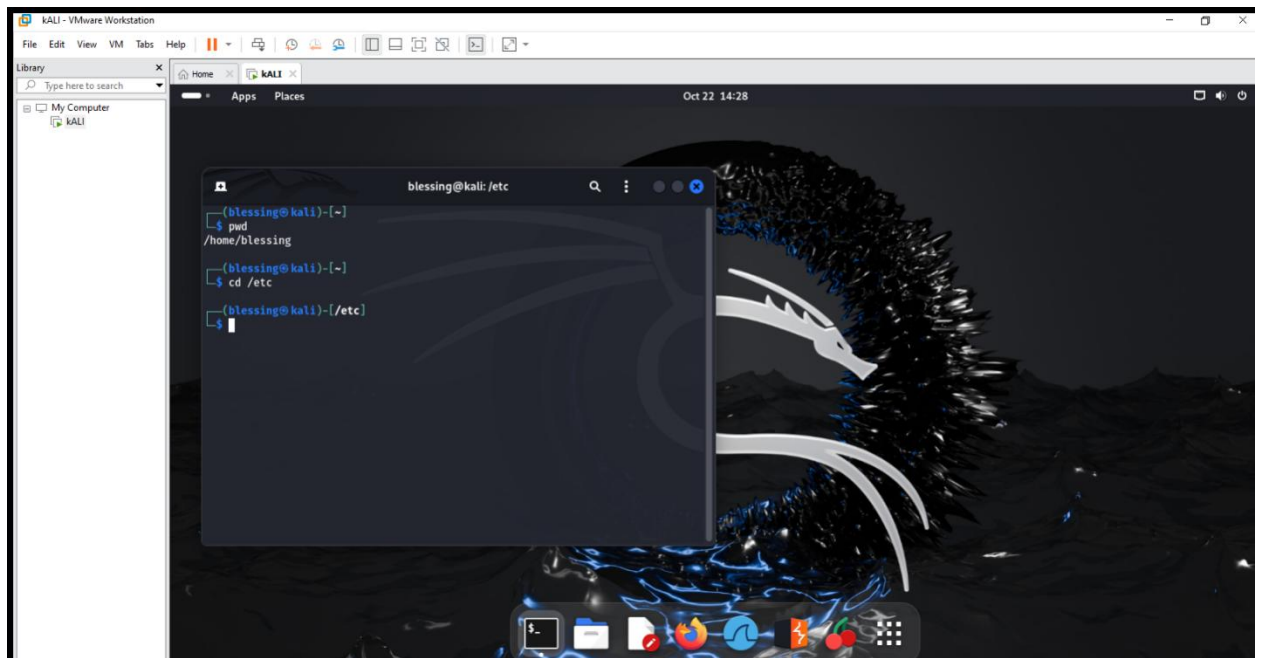
- **Familiarization of Kali Linux Shell**

1. Command Documentation

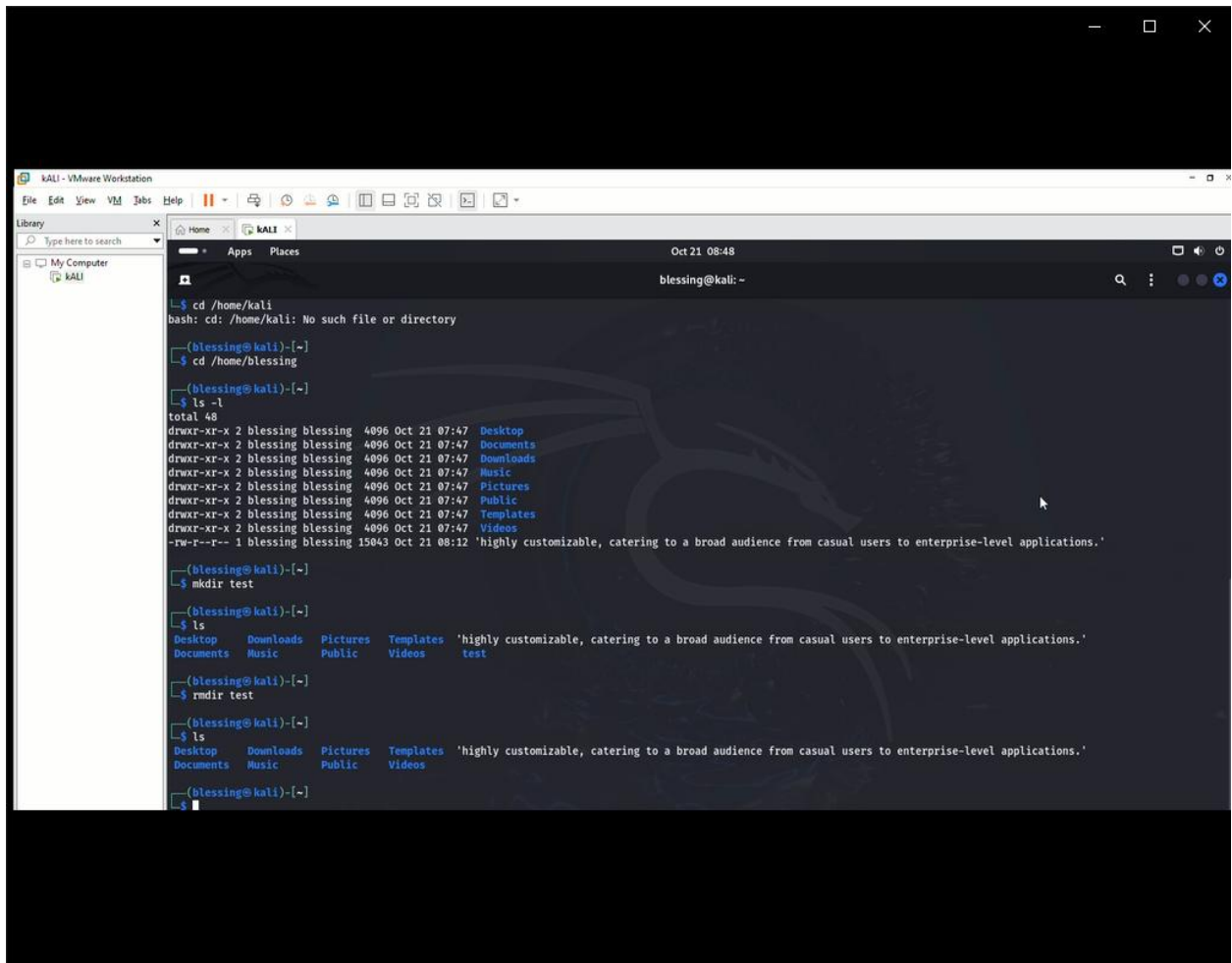
- i. The MAN Page – used to display the user manual of any command that we can run on the terminal.



- ii. Some sections included in a MAN's page includes: Executable programs or shell commands, System calls, Library calls, Special files, File formats and conventions, Games.
- **Create and Change Directory**
 - i. Print the current working directory (PWD) - /home/blessing
 - ii. Navigate to another directory. For example etc – cd /etc



- List files in current directory
- Create new directory
- Confirm new directory creation

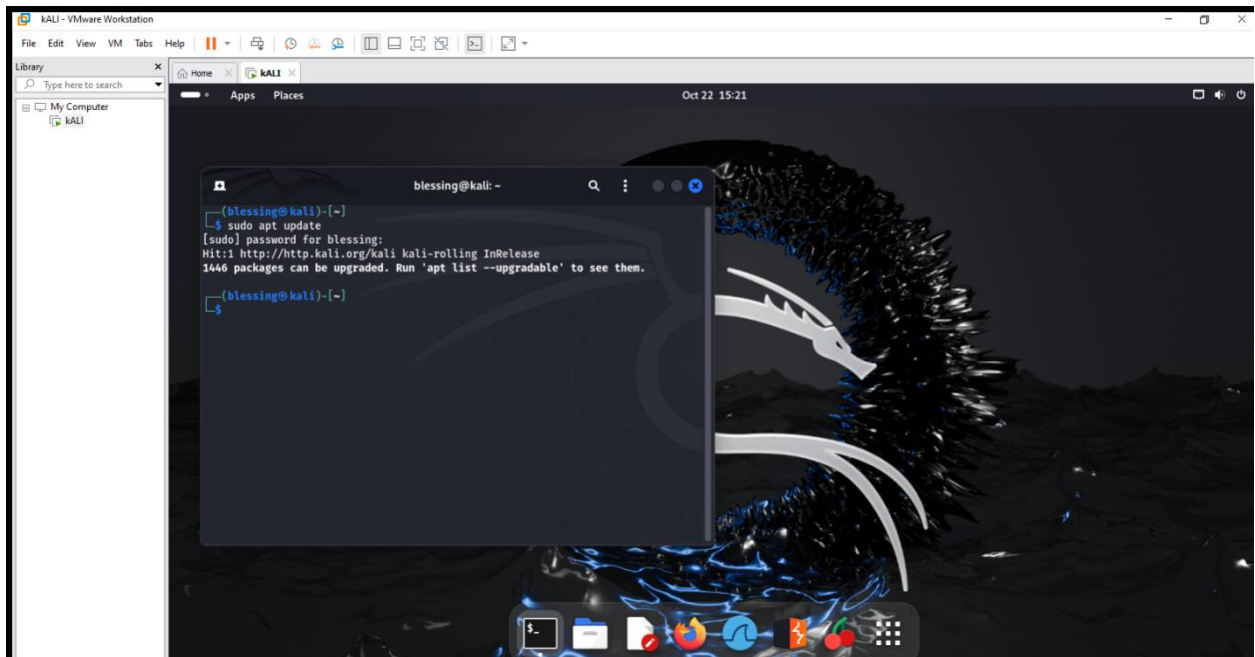


- Remove the directory
- Confirm directory removal

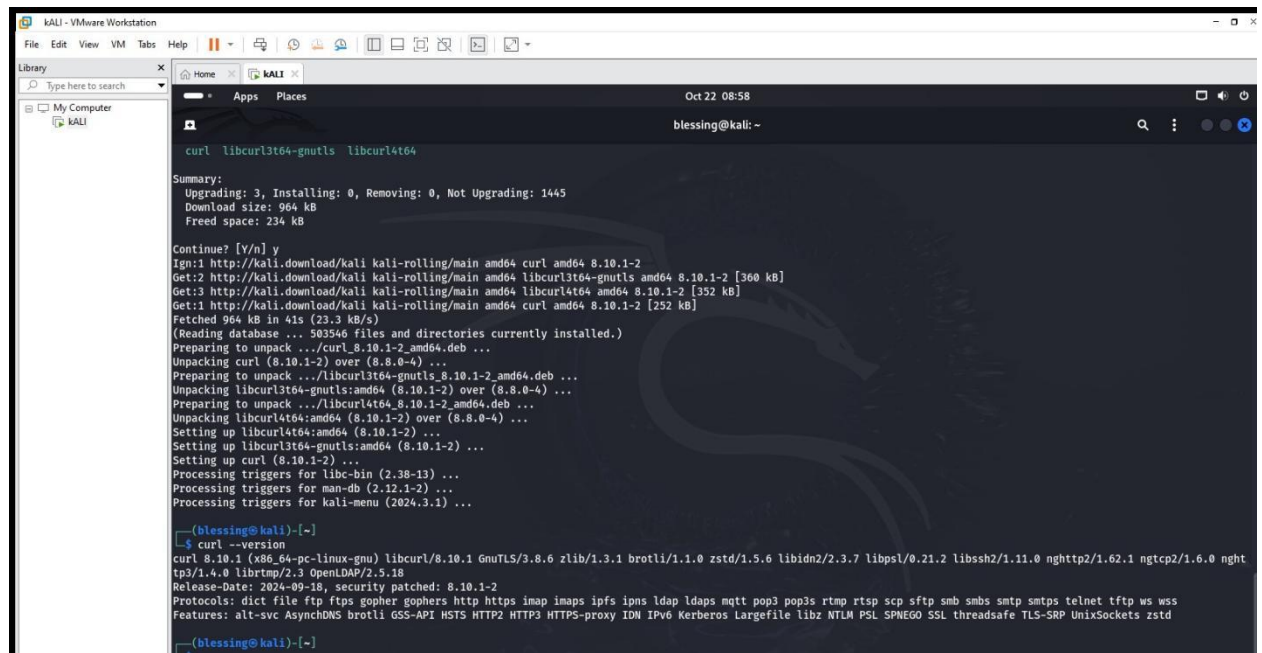
The picture above includes an example of directory removal and its confirmation.

LAB 2: Installing Packages and Applications

- Updating Package List



- Installing Packages
 - i. Curl Installation
 - ii. Confirm the Installation



- Upgrading Packages

- Review upgrade messages

```

blessing@kali: ~
└─$ sudo apt upgrade git
git is already the newest version (1:2.43.0-1+b1).
git set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
└─$ cat /etc/sources.list
cat: /etc/sources.list: No such file or directory
└─$ cat /etc/apt/sources.list
#deb cdrom:[Kali GNU/Linux 2024.3rc2_Kali-last-snapshot_ - Official amd64 BD Bi
nary-1 with firmware 20240818-17:59]/ kali-rolling contrib main non-free non-fre
e-firmware

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
└─$

```

- Removing Packages

```

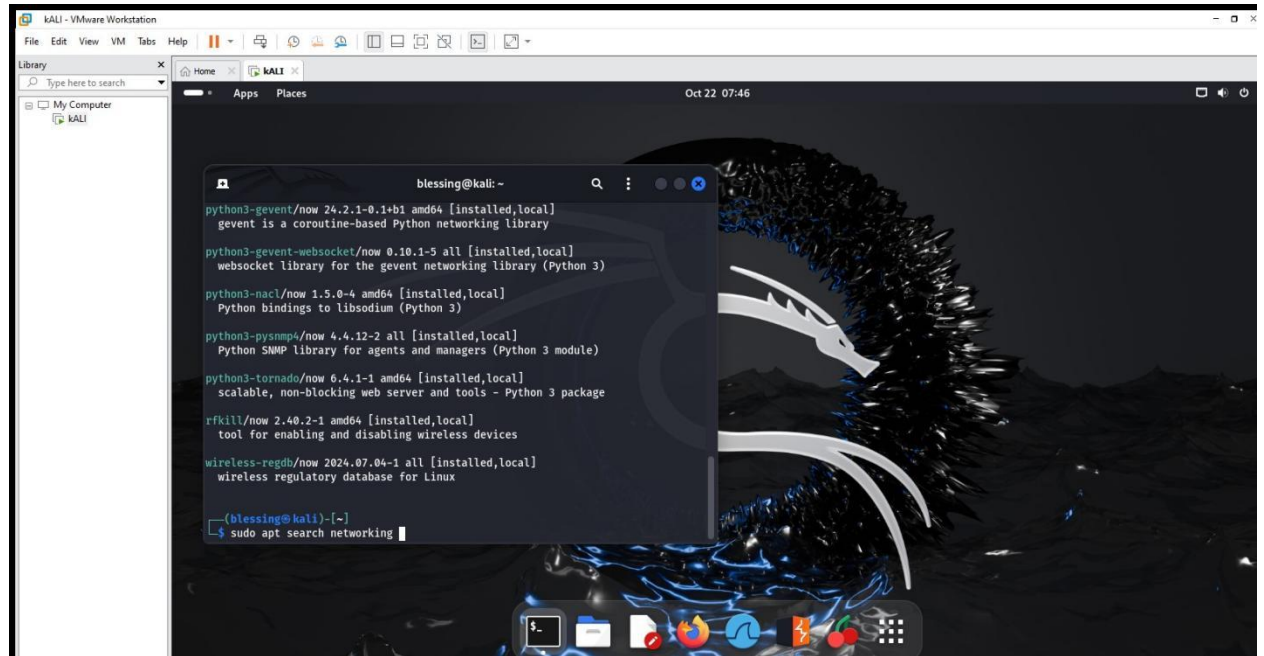
blessing@kali: ~
└─$ sudo apt autoremove
python3-celery
python3-cffi
python3-clic-help
python3-click-didyoumean
python3-click-repl
python3-cmd2
python3-configobj
python3-cpuinfo
python3-cvss
python3-defusedxml
python3-django
python3-elasticsearch
python3-email-validator
python3-ephem
python3-faraday-agent-parameters-types
python3-faraday-plugins
python3-feedparser
python3-filedepot
python3-filteralchemy
python3-flask-celery-helper
python3-flask-classful
python3-flask-lvsession
python3-flask-limiter
python3-flask-login
python3-flask-mail
python3-flask-principal
python3-flask-sqlalchemy
python3-flaskext.wtf
python3-flatbuffers
python3-gevent
python3-validators
python3-venusian
python3-vine
python3-webargs
python3-wsaccel
python3-wtforms
python3-yaswfp
python3-zapv2
python3-zope.deprecation
python3-zope.event
redis-server
redis-tools
rpm
rsh-redone-client
ruby-cms-scanner
ruby-ethon
ruby-get-process-mem
ruby-opt-parse-validator
ruby-progressbar
ruby-typhoeus
ruby-yajl
rwho
rwhod
smtp-user-enum
sparta-scripts
toilet-fonts
unicornscan
uriscan
waipiti
xsltproc
Use 'sudo apt autoremove' to remove them.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1446
└─$ sudo apt remove curl

```

In the diagram, it shows that curl has already been removed previously.

- Searching for Packages

i. Search for Networking Packages

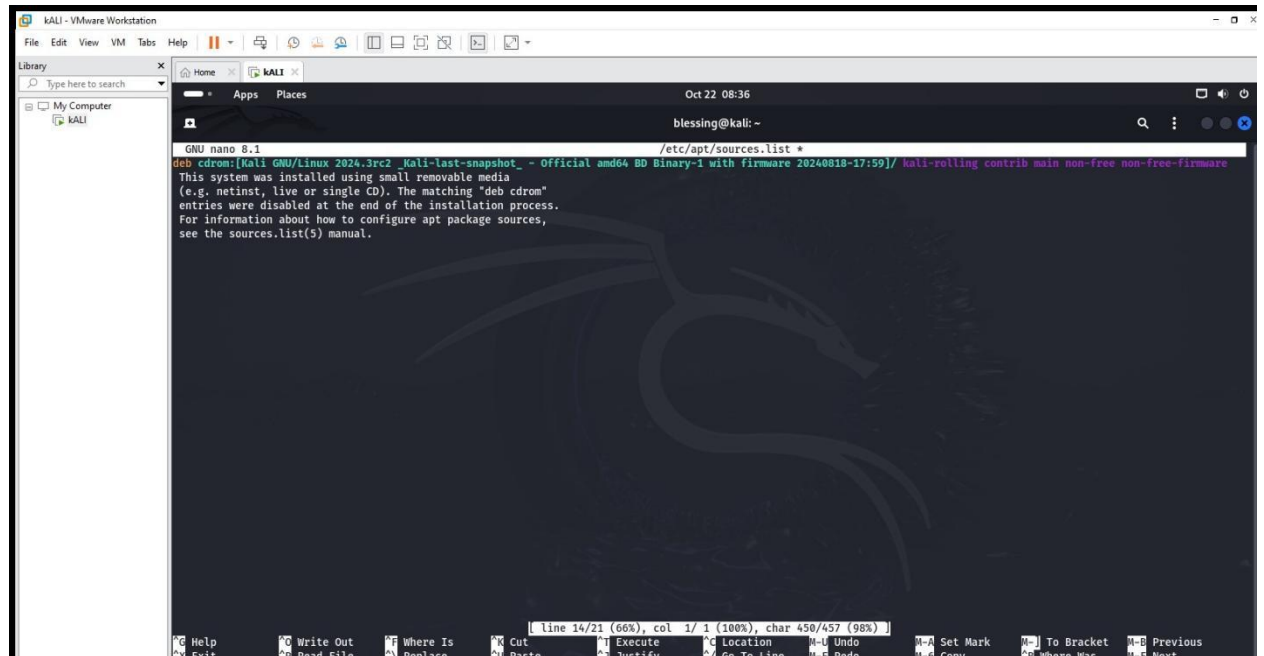


The screenshot shows a Kali Linux terminal window with the command `sudo apt search networking` executed. The output lists several Python networking libraries and tools, including `python3-gevent`, `python3-gevent-websocket`, `python3-nacl`, `python3-pysnmp4`, `python3-tornado`, `rftkill`, and `wireless-regdb`. The terminal window is titled `blissing@kali: ~` and the system clock shows `Oct 22 07:46`.

ii. Review Results

• Managing Repositories

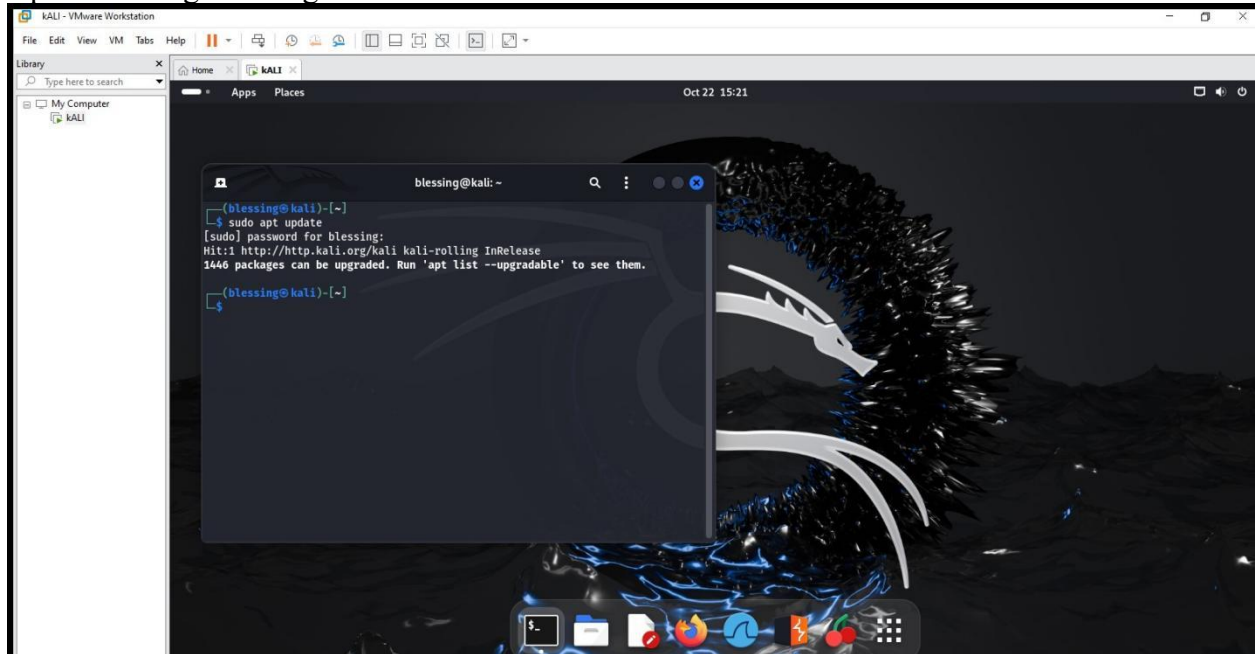
- i. Edit repositories
- ii. Modify repositories entries
- iii. Save and Exit: `Ctrl + o` to save and `ctrl + x` to exit editor



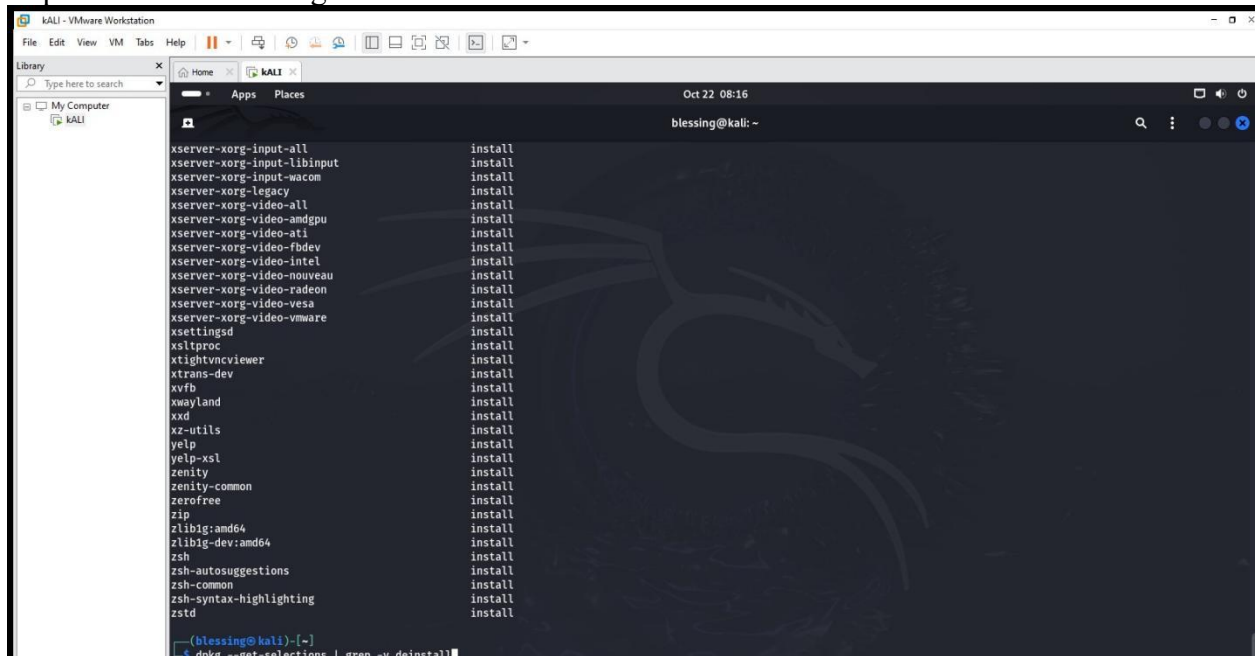
The screenshot shows a nano text editor window editing the `/etc/apt/sources.list` file. The file content includes the Kali Linux repository information and a note about the installation process. The terminal window is titled `blissing@kali: ~` and the system clock shows `Oct 22 08:36`. The nano editor status bar at the bottom indicates `line 14/21 (66%), col 1/1 (100%), char 450/457 (98%)`.

- **Final Review**

- i. **Update Package List Again**



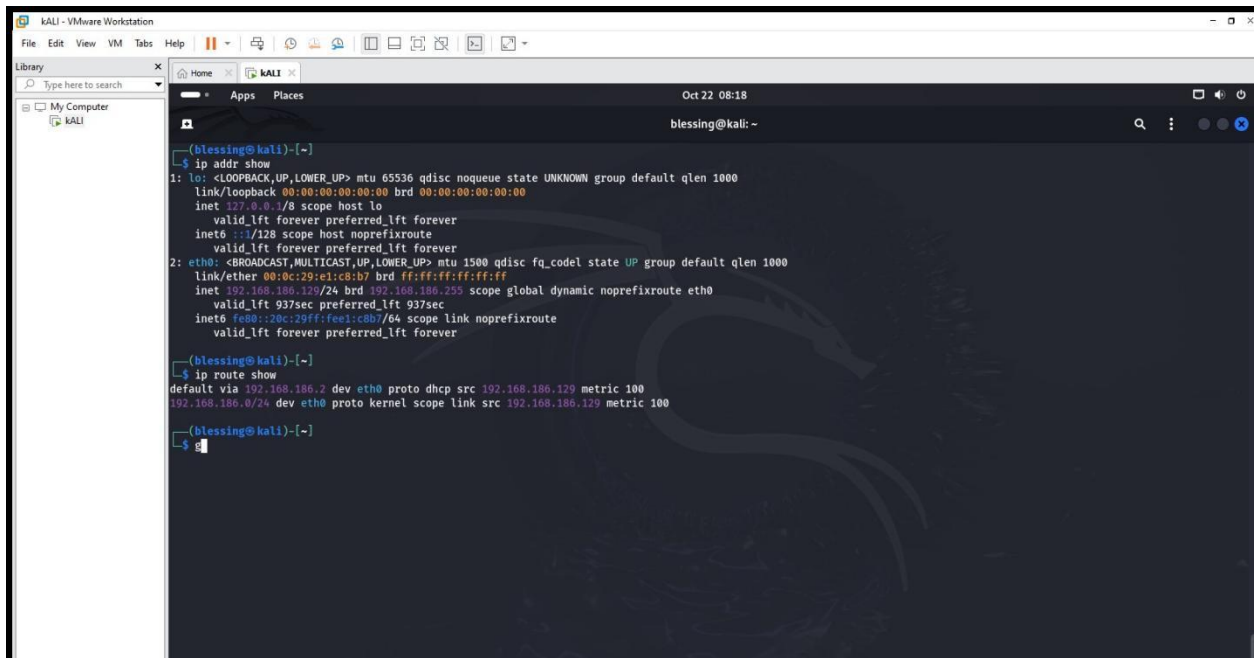
- ii. **Explore Installed Packages**



LAB 3: NETWORKING COMMANDS

- **Displaying Network Configuration**

- i. Check Network Interfaces

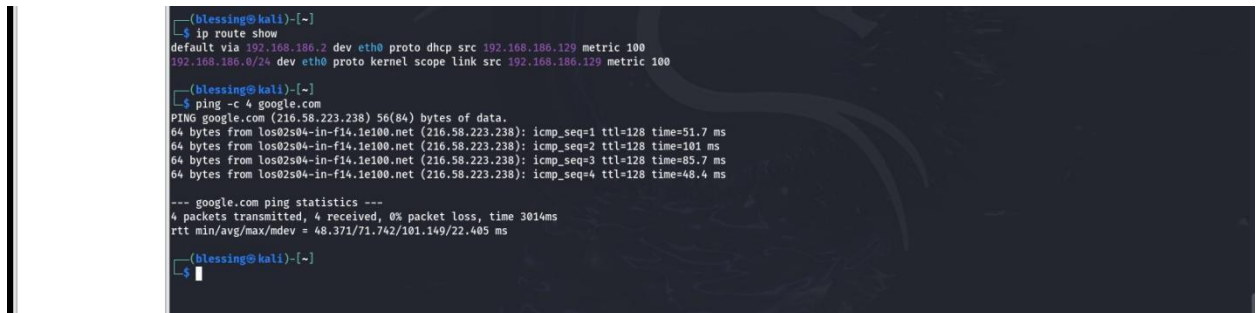


```
(blessing@kali)-[~]
$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e1:c8:b7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.186.129/24 brd 192.168.186.255 scope global dynamic noprefixroute eth0
        valid_lft 937sec preferred_lft 937sec
    inet6 fe80::20c:29ff:fe1:c8b7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(blessing@kali)-[~]
$ ip route show
default via 192.168.186.2 dev eth0 proto dhcp src 192.168.186.129 metric 100
192.168.186.0/24 dev eth0 proto kernel scope link src 192.168.186.129 metric 100

(blessing@kali)-[~]
$
```

- ii. List Routing Table



```
(blessing@kali)-[~]
$ ip route show
default via 192.168.186.2 dev eth0 proto dhcp src 192.168.186.129 metric 100
192.168.186.0/24 dev eth0 proto kernel scope link src 192.168.186.129 metric 100

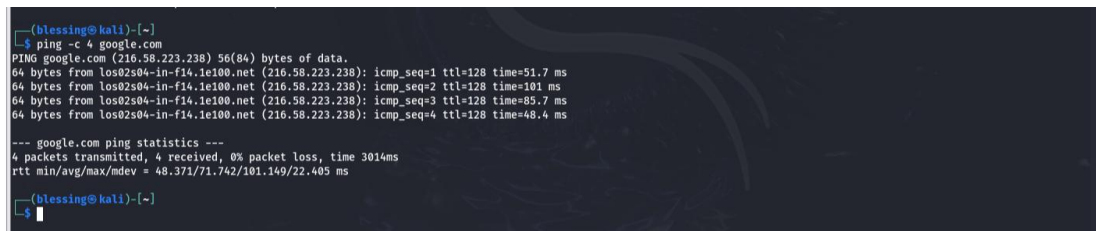
(blessing@kali)-[~]
$ ping -c 4 google.com
PING google.com (216.58.223.238) 56(84) bytes of data:
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=1 ttl=128 time=51.7 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=2 ttl=128 time=101 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=3 ttl=128 time=85.7 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=4 ttl=128 time=48.4 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 48.371/71.742/101.149/22.405 ms

(blessing@kali)-[~]
$
```

- **Testing Network Connectivity**

- i. Ping a Host

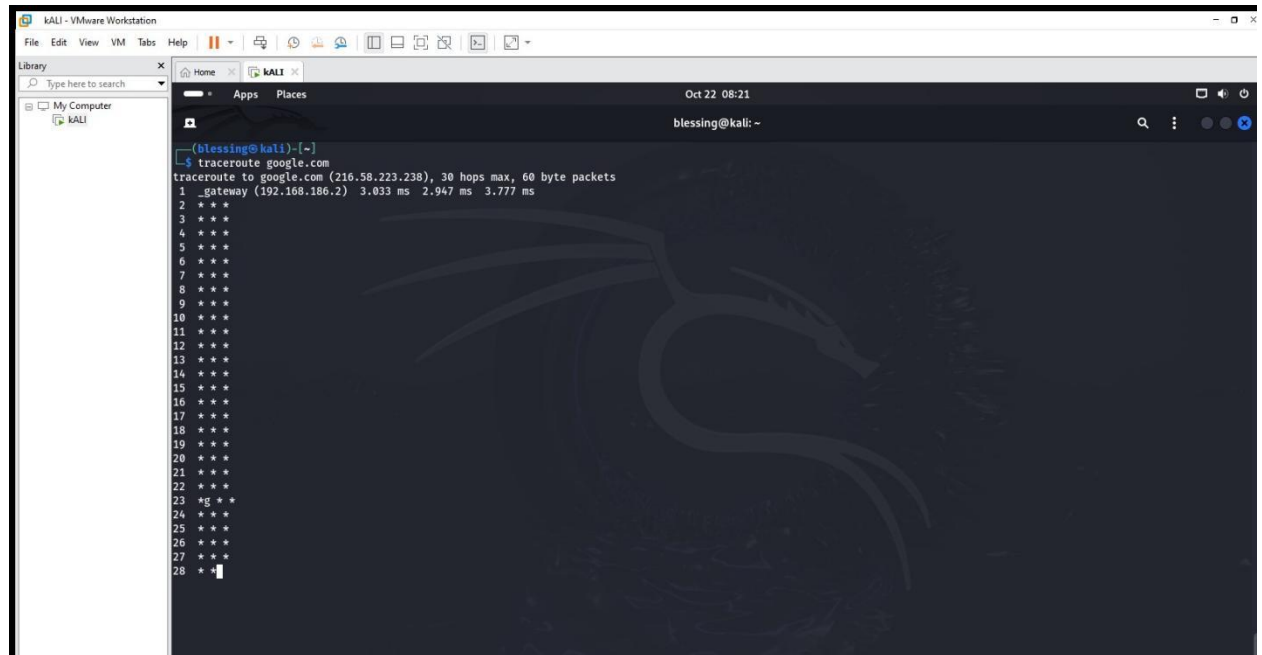


```
(blessing@kali)-[~]
$ ping -c 4 google.com
PING google.com (216.58.223.238) 56(84) bytes of data:
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=1 ttl=128 time=51.7 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=2 ttl=128 time=101 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=3 ttl=128 time=85.7 ms
64 bytes from los02s04-in-f14.1e100.net (216.58.223.238): icmp_seq=4 ttl=128 time=48.4 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 48.371/71.742/101.149/22.405 ms

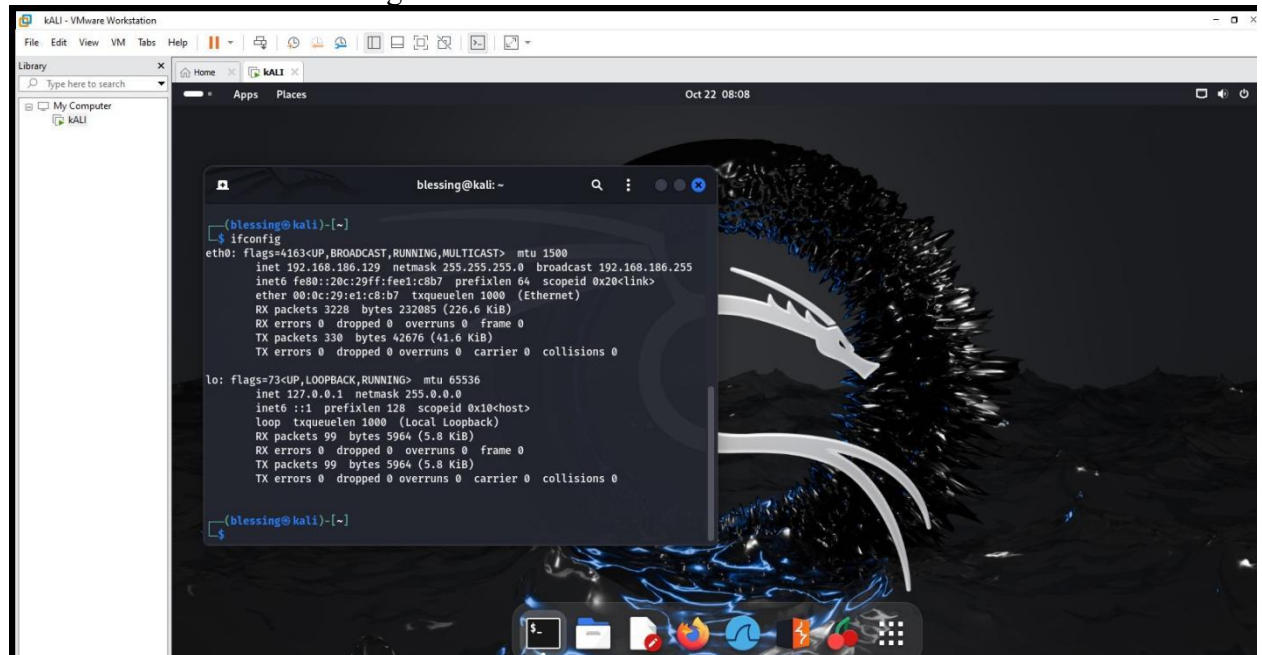
(blessing@kali)-[~]
$
```

ii. Trace Route to a Host



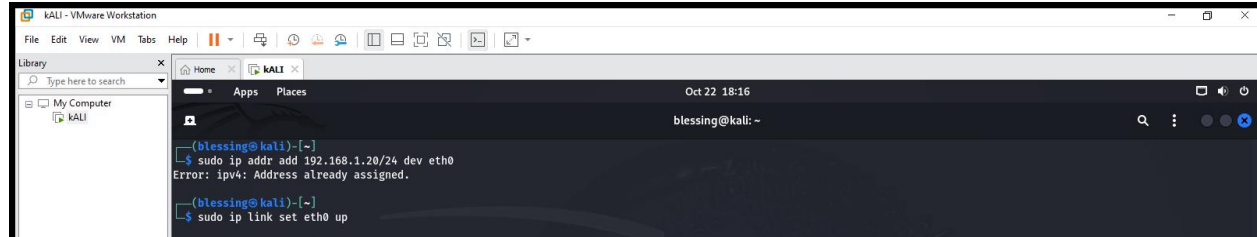
• Configuring Network Interfaces

i. View Current Interface Configuration



ii. Manually Configure an Interface

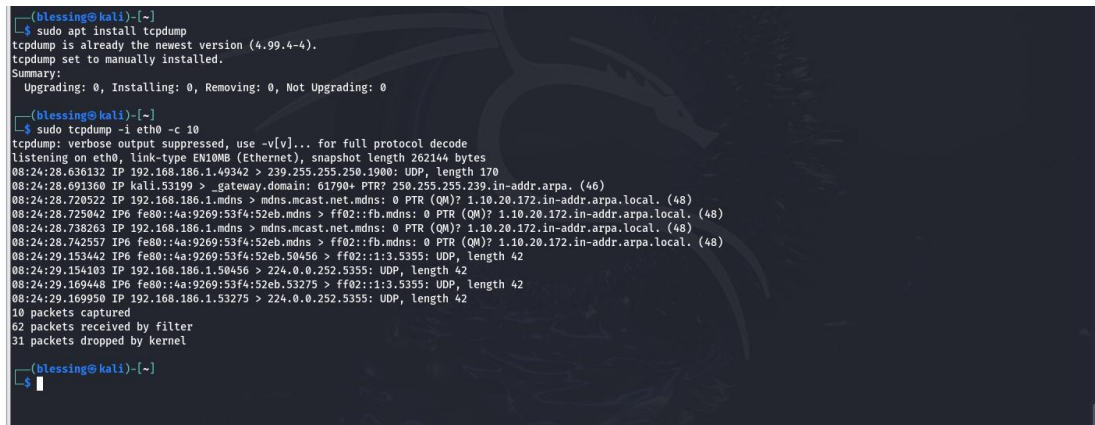
iii. Bring the Interface Up



```
(blessing@kali)-[~]
$ sudo ip addr add 192.168.1.20/24 dev eth0
Error: ipv4: Address already assigned.
(blessing@kali)-[~]
$ sudo ip link set eth0 up
```

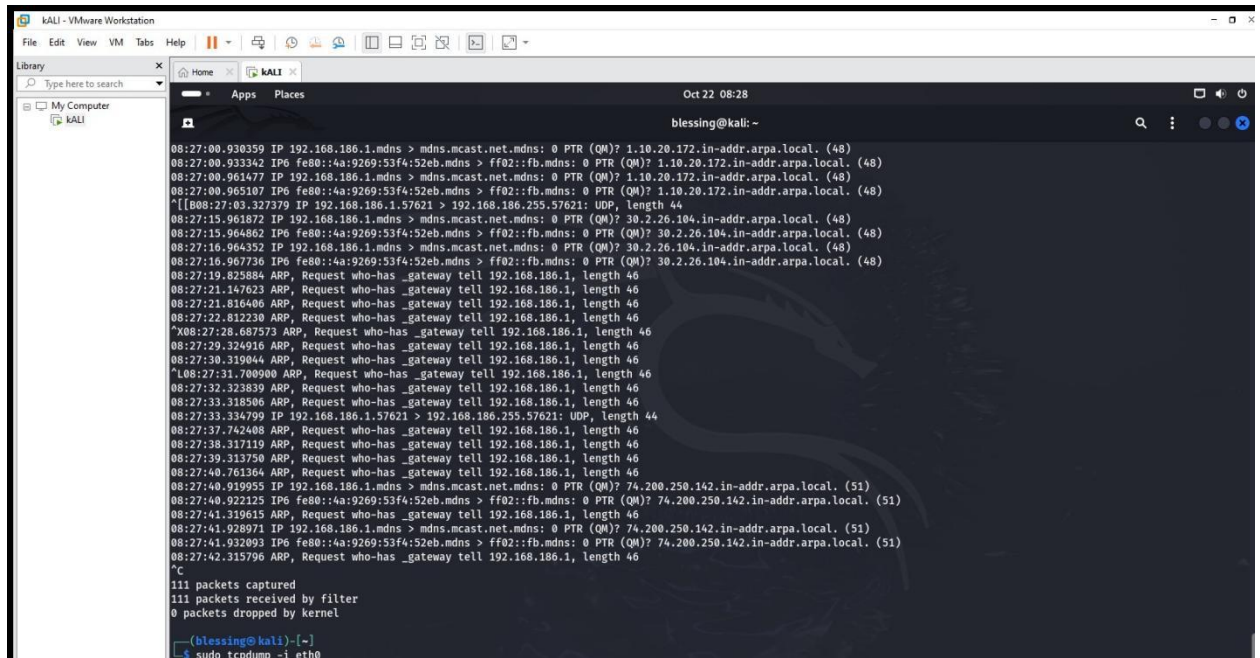
• Monitoring Network Traffic

- i. Install tcpdump
- ii. Capture Network Traffic



```
(blessing@kali)-[~]
$ sudo apt install tcpdump
tcpdump is already the newest version (4.99.4-4).
tcpdump set to manually installed.
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
(blessing@kali)-[~]
$ sudo tcpdump -i eth0 -c 10
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
08:24:28.636132 IP 192.168.1.49342 > 239.255.255.250: UDP, length 170
08:24:28.691368 IP kali.53199 > _gateway.domain: 61790+ PTR? 250.255.255.239.in-addr.arpa. (46)
08:24:28.720522 IP 192.168.180.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:24:28.725042 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:24:28.738263 IP 192.168.180.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:24:28.742557 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:24:29.153442 IP6 fe80::4a:9269:53f4:52eb.50456 > ff02::1:3.5355: UDP, length 42
08:24:29.154103 IP 192.168.186.1.50456 > 224.0.0.252.5355: UDP, length 42
08:24:29.169448 IP6 fe80::4a:9269:53f4:52eb.53275 > ff02::1:3.5355: UDP, length 42
08:24:29.169950 IP 192.168.186.1.53275 > 224.0.0.252.5355: UDP, length 42
10 packets captured
62 packets received by filter
31 packets dropped by kernel
(blessing@kali)-[~]
$
```

iii. Analyze Network Traffic – Use ctrl + c to stop capture



```
Oct 22 08:28
blessing@kali: ~
08:27:00.930359 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:27:00.933342 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:27:00.961477 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
08:27:00.965107 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 1.10.20.172.in-addr.arpa.local. (48)
*[[B08:27:03.327379 IP 192.168.186.1.57621 > 192.168.186.255.57621: UDP, length 44
08:27:15.961872 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 30.2.26.104.in-addr.arpa.local. (48)
08:27:15.964862 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 30.2.26.104.in-addr.arpa.local. (48)
08:27:16.964352 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 30.2.26.104.in-addr.arpa.local. (48)
08:27:16.967736 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 30.2.26.104.in-addr.arpa.local. (48)
08:27:19.825884 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:21.147623 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:21.816406 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:22.812230 ARP, Request who-has_gateway tell 192.168.186.1, length 46
*X08:27:28.687573 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:29.324916 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:30.319044 ARP, Request who-has_gateway tell 192.168.186.1, length 46
*108:27:31.700000 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:32.323839 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:33.318506 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:33.334799 IP 192.168.186.1.57621 > 192.168.186.255.57621: UDP, length 44
08:27:37.742408 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:38.317119 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:39.313750 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:40.761364 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:40.919955 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 74.200.250.142.in-addr.arpa.local. (51)
08:27:40.922125 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 74.200.250.142.in-addr.arpa.local. (51)
08:27:41.319615 ARP, Request who-has_gateway tell 192.168.186.1, length 46
08:27:41.928971 IP 192.168.186.1.mdns > mdns.mcast.net.mdns: 0 PTR (QM)? 74.200.250.142.in-addr.arpa.local. (51)
08:27:41.932093 IP6 fe80::4a:9269:53f4:52eb.mdns > ff02::fb.mdns: 0 PTR (QM)? 74.200.250.142.in-addr.arpa.local. (51)
08:27:42.315796 ARP, Request who-has_gateway tell 192.168.186.1, length 46
"C
111 packets captured
111 packets received by filter
0 packets dropped by kernel
(blessing@kali)-[~]
$ sudo tcpdump -i eth0
```

• Final Review

i. Check Network Status

```
(blessing@kali)-[~]
$ nmcli device status
DEVICE  TYPE      STATE      CONNECTION
eth0    ethernet  connected  Wired connection 1
lo      loopback  connected (externally)  lo

(blessing@kali)-[~]
$ g
```

ii. Check Firewall Status

