

Security of corporate systems L1

Lab 1

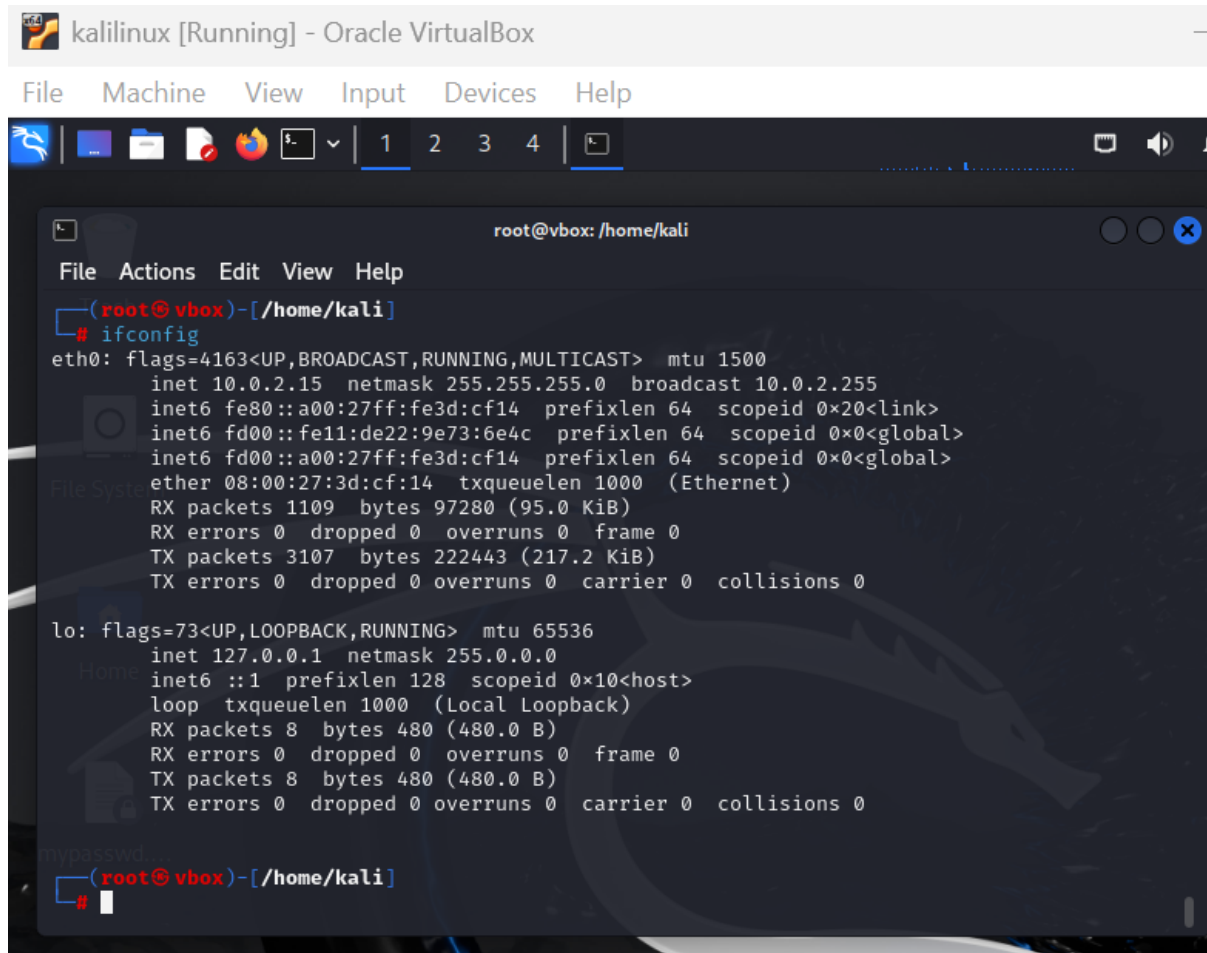
Aghamir Ahmadow

ID:49729

# 1.Check Kali ip address

This command **ifconfig**

shows the IP address of the Kali machine. **inet 10.0.2.15**



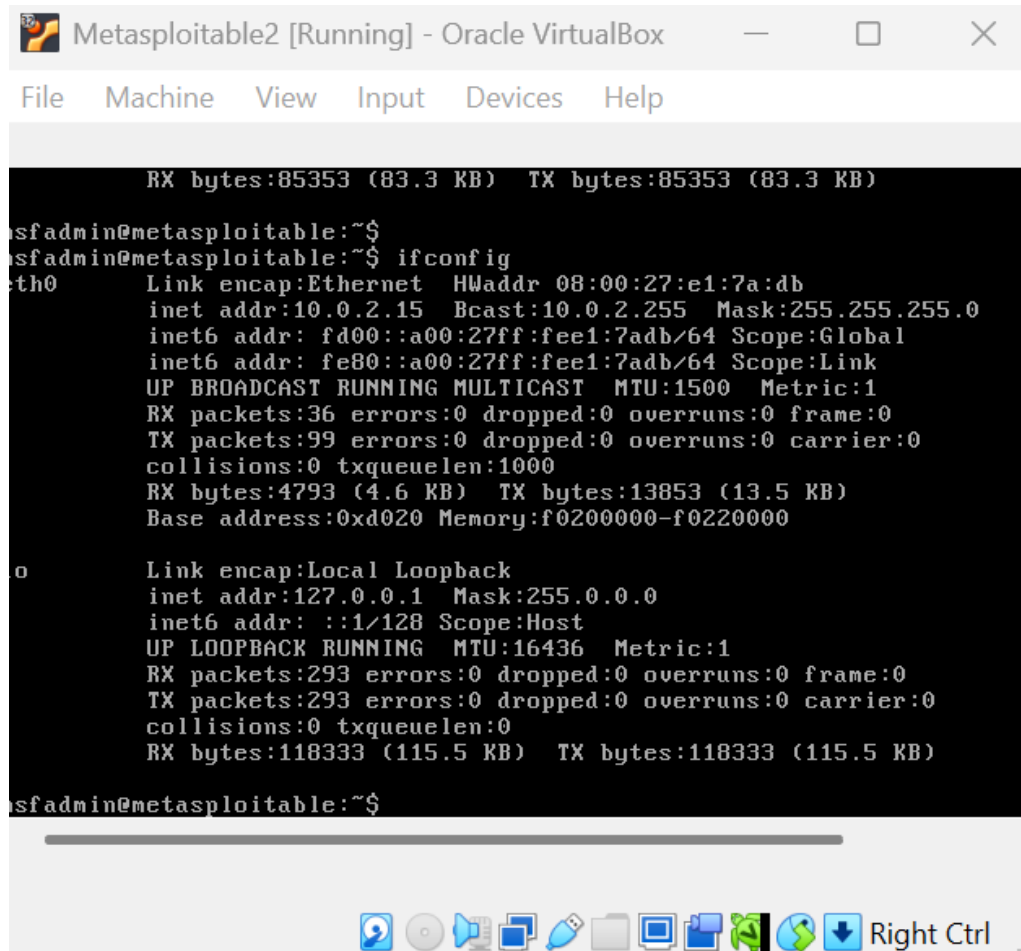
```
kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@vbox: /home/kali
File Actions Edit View Help
(root@vbox)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe3d:cf14 prefixlen 64 scopeid 0x20<link>
    inet6 fd00::fe11:de22:9e73:6e4c prefixlen 64 scopeid 0x0<global>
    inet6 fd00::a00:27ff:fe3d:cf14 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:3d:cf:14 txqueuelen 1000 (Ethernet)
    RX packets 1109 bytes 97280 (95.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3107 bytes 222443 (217.2 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 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

mypasswd
(root@vbox)-[/home/kali]
#
```

## 2. Metasploitable 2 ip address

This command **ifconfig** also shows the IP address on **Metasploitable 2**



```
Metasploitable2 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

RX bytes:85353 (83.3 KB) TX bytes:85353 (83.3 KB)

sfadmin@metasploitable:~$
sfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e1:7a:db
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fd00::a00:27ff:fee1:7adb/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee1:7adb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4793 (4.6 KB)  TX bytes:13853 (13.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000

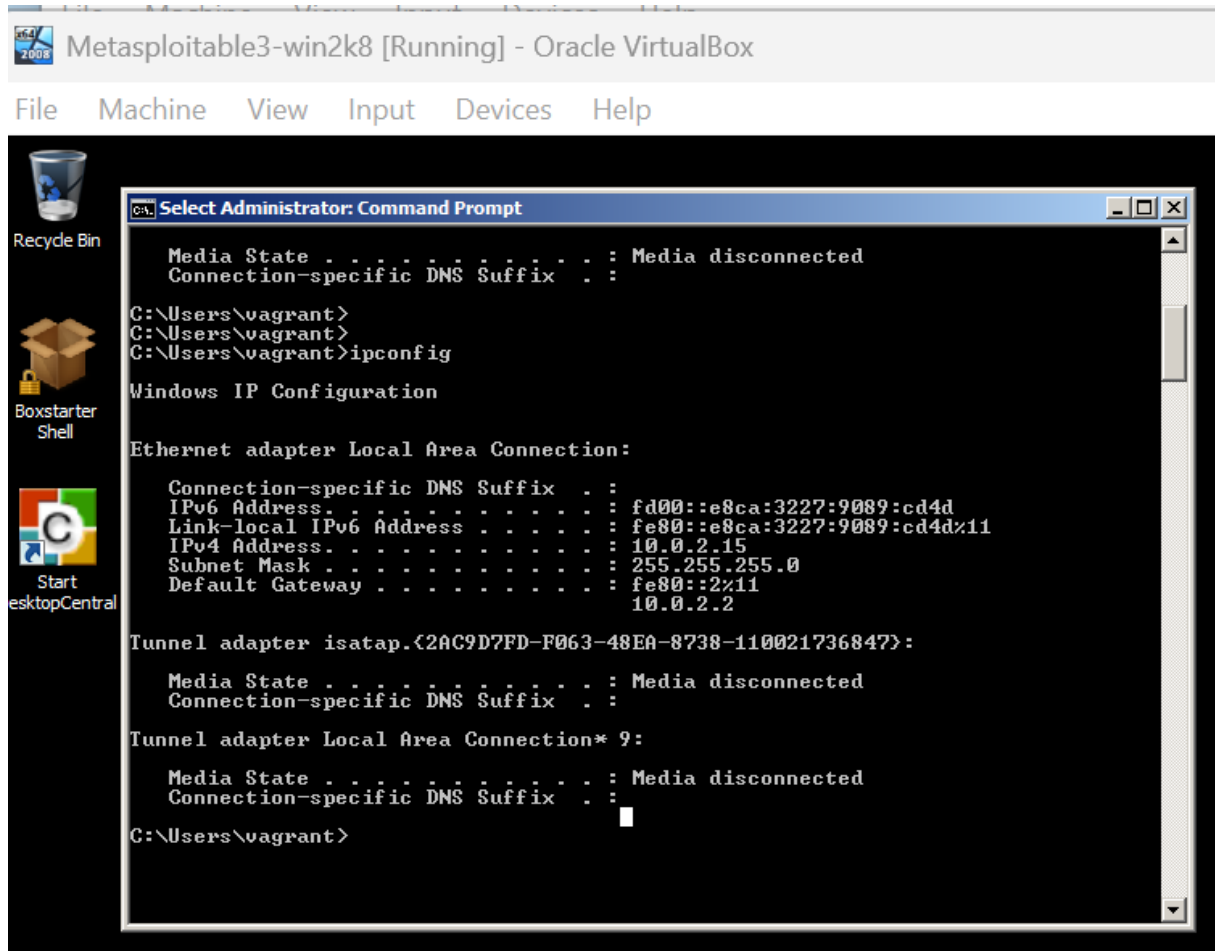
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:293 errors:0 dropped:0 overruns:0 frame:0
          TX packets:293 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:118333 (115.5 KB)  TX bytes:118333 (115.5 KB)

sfadmin@metasploitable:~$
```

The screenshot shows a Windows taskbar at the bottom with various icons including a globe, a CD, a speaker, a folder, a USB drive, a monitor, a document, a green robot, a green circle, and a blue download arrow. The text "Right Ctrl" is visible next to the download icon.

# 3. Metasploitable 3 Ip address

This command **ipconfig** also shows the IP address on **Metasploitable 3**



The screenshot shows a Windows XP desktop environment. At the top, a taskbar displays the title 'Metasploitable3-win2k8 [Running] - Oracle VirtualBox'. Below the taskbar is a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The desktop background is black, and several icons are visible on the left: 'Recycle Bin', 'Boxstarter Shell', and 'Start esktopCentral'. A 'Command Prompt' window is open, displaying the output of the 'ipconfig' command. The output shows the configuration for three network adapters: Ethernet adapter Local Area Connection, Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}, and Tunnel adapter Local Area Connection\* 9. The Ethernet adapter is the primary network interface, showing an IPv4 address of 10.0.2.15 and a subnet mask of 255.255.255.0.

```
C:\Users\vagrant> ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . .             : fd00::e8ca:3227:9089:cd4d
    Link-local IPv6 Address . . . . . : fe80::e8ca:3227:9089:cd4d%11
    IPv4 Address. . . . .              : 10.0.2.15
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : fe80::2%11
                                         10.0.2.2

Tunnel adapter isatap.{2AC9D7FD-F063-48EA-8738-110021736847}:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

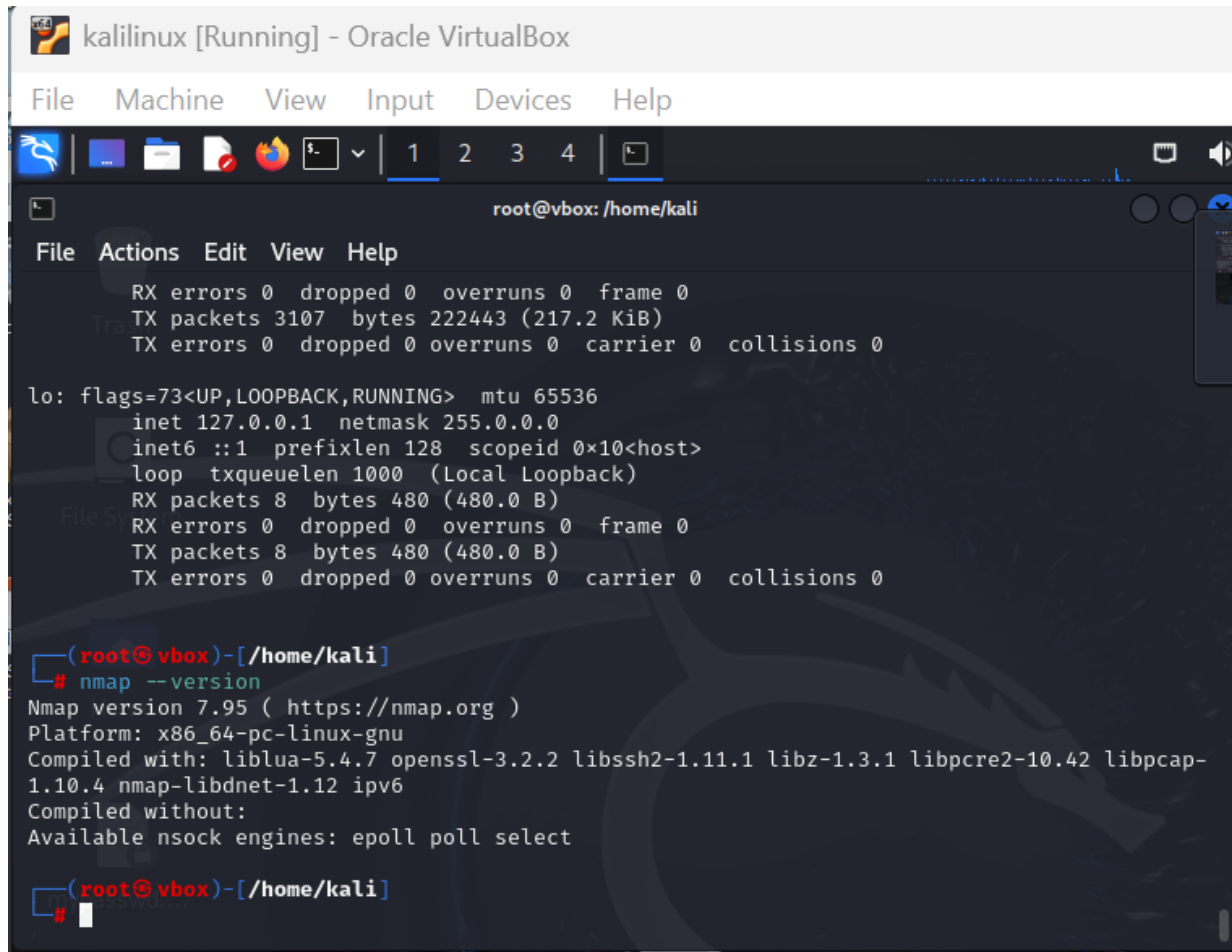
Tunnel adapter Local Area Connection* 9:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\vagrant>
```

# 4.Your Nmap version

i used the command for getting the version: **nmap --version**



```
kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/kali
File Actions Edit View Help
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3107 bytes 222443 (217.2 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 0<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

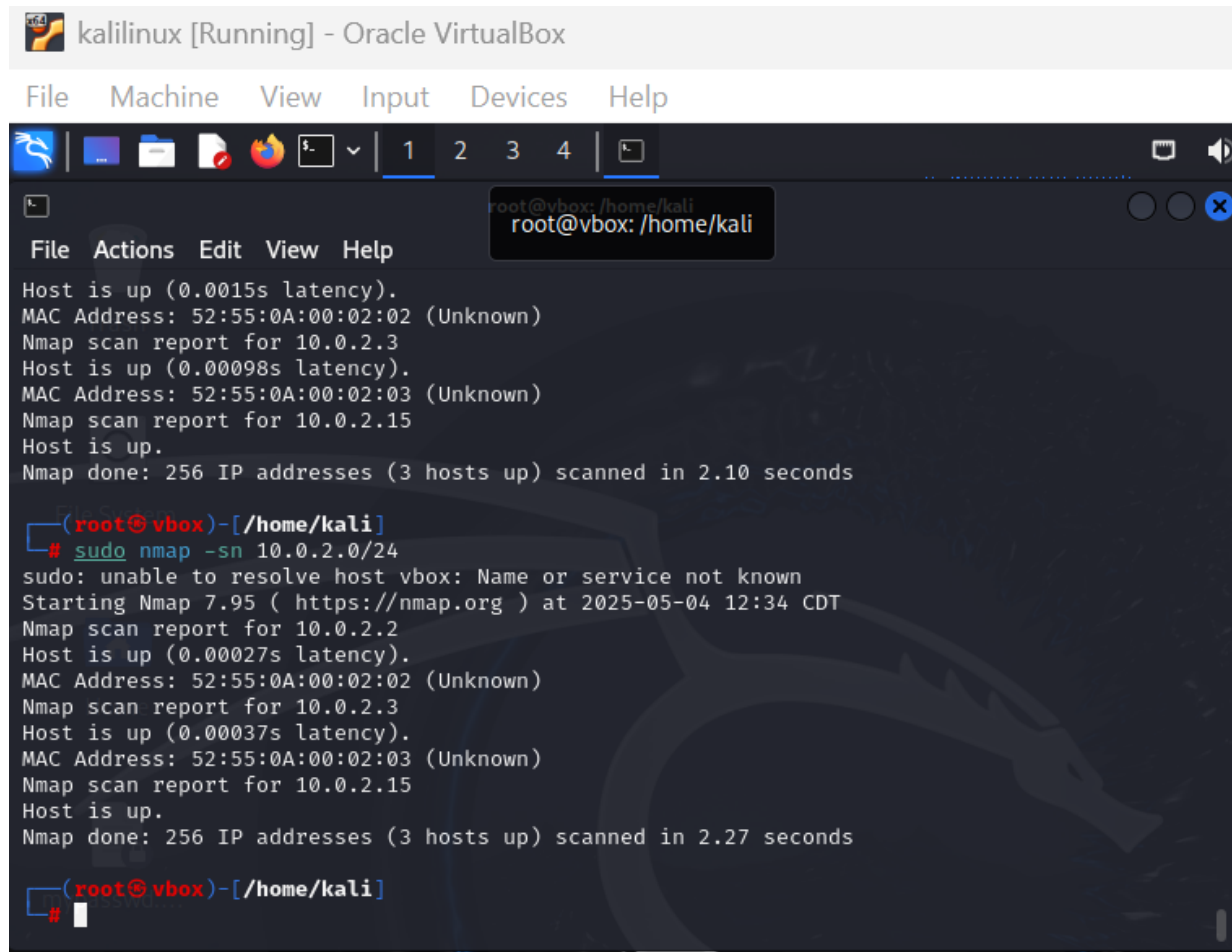
(root@vbox)-[/home/kali]
# nmap --version
Nmap version 7.95 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.7 openssl-3.2.2 libssh2-1.11.1 libz-1.3.1 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

(root@vbox)-[/home/kali]
#
```

# 5. Which hosts are up on your network

I used `sudo nmap -sn 10.0.2.0/24` command and get the hosts:

**10.0.2.2 10.0.2.3 10.0.2.15**



The screenshot shows a terminal window titled "kalilinux [Running] - Oracle VirtualBox". The terminal output displays the results of an nmap scan for the network 10.0.2.0/24. The scan identifies three hosts as up: 10.0.2.2, 10.0.2.3, and 10.0.2.15. The terminal also shows the command used to run the scan and the resulting output, including the nmap version and the time taken to complete the scan.

```
kalilinux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox: /home/kali
root@vbox: /home/kali
File Actions Edit View Help
Host is up (0.0015s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00098s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.10 seconds

(root@vbox)-[/home/kali]
# sudo nmap -sn 10.0.2.0/24
sudo: unable to resolve host vbox: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-04 12:34 CDT
Nmap scan report for 10.0.2.2
Host is up (0.00027s latency).
MAC Address: 52:55:0A:00:02:02 (Unknown)
Nmap scan report for 10.0.2.3
Host is up (0.00037s latency).
MAC Address: 52:55:0A:00:02:03 (Unknown)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.27 seconds

(root@vbox)-[/home/kali]
#
```