Lab03 Firewalls

Prepared By Dr. Wooi Ping Cheah

Reference: COMP3052.SEC.LAB.03.Firewalls.Port.Scanning by Mike Pound

Cloning Kali-Linux Virtual Machine

- You have had a Kali-Linux virtual machine (called Kali-Linux-2020.3-amd64 COMP3006) installed on your pc/laptop. This virtual machine will be used as a Client in this lab session.

- Now, you need to make a clone of the Kali-Linux virtual machine. The newly created clone (called Kali-server) will be used as a Server in this lab session.

- You can create a clone of the Kali-Linux virtual machine by following the steps described in the following videoclip: https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=84d40490-bbf2-4c1d-a100-afc2007c7ef7&start=0

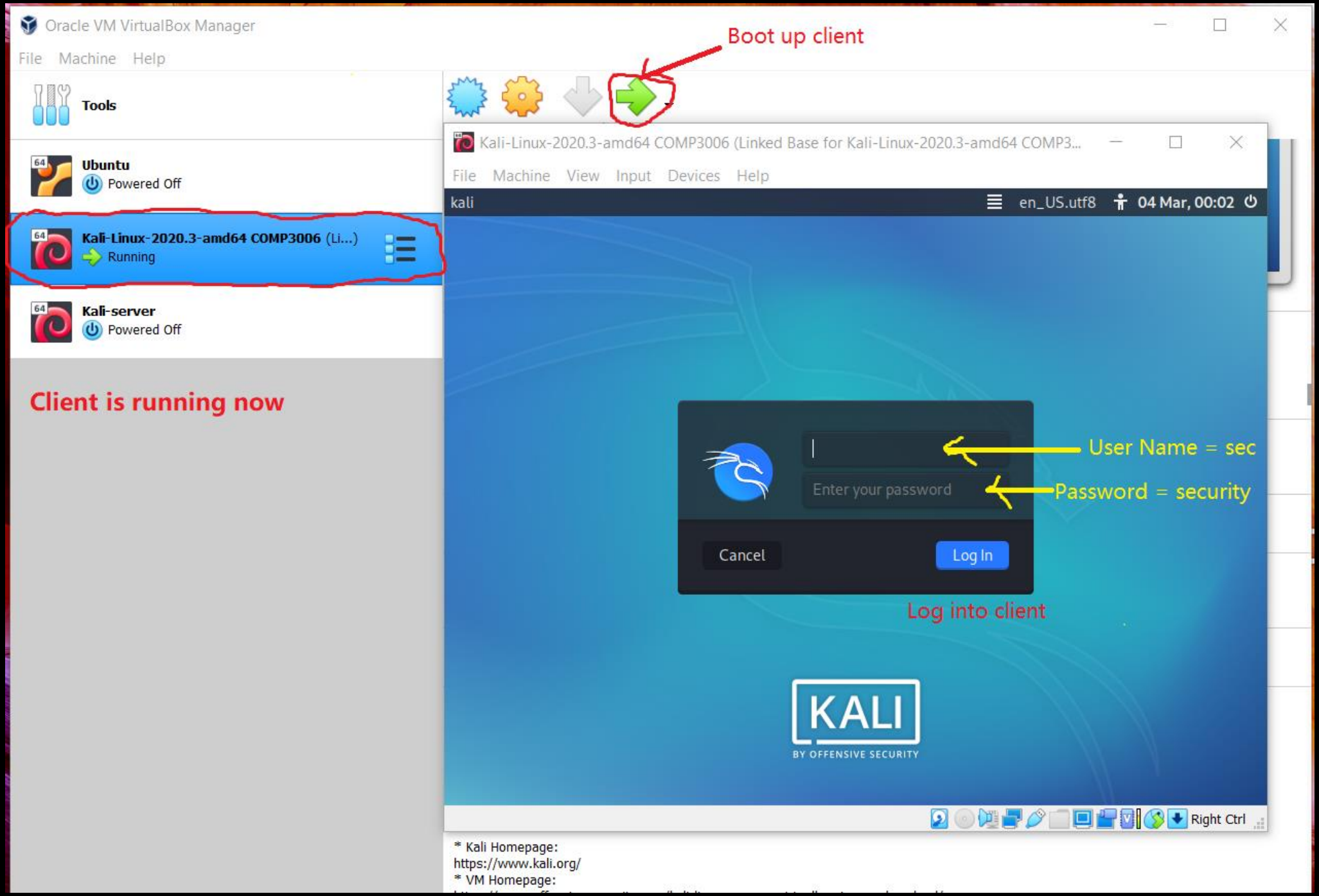
Configuring Client and Server

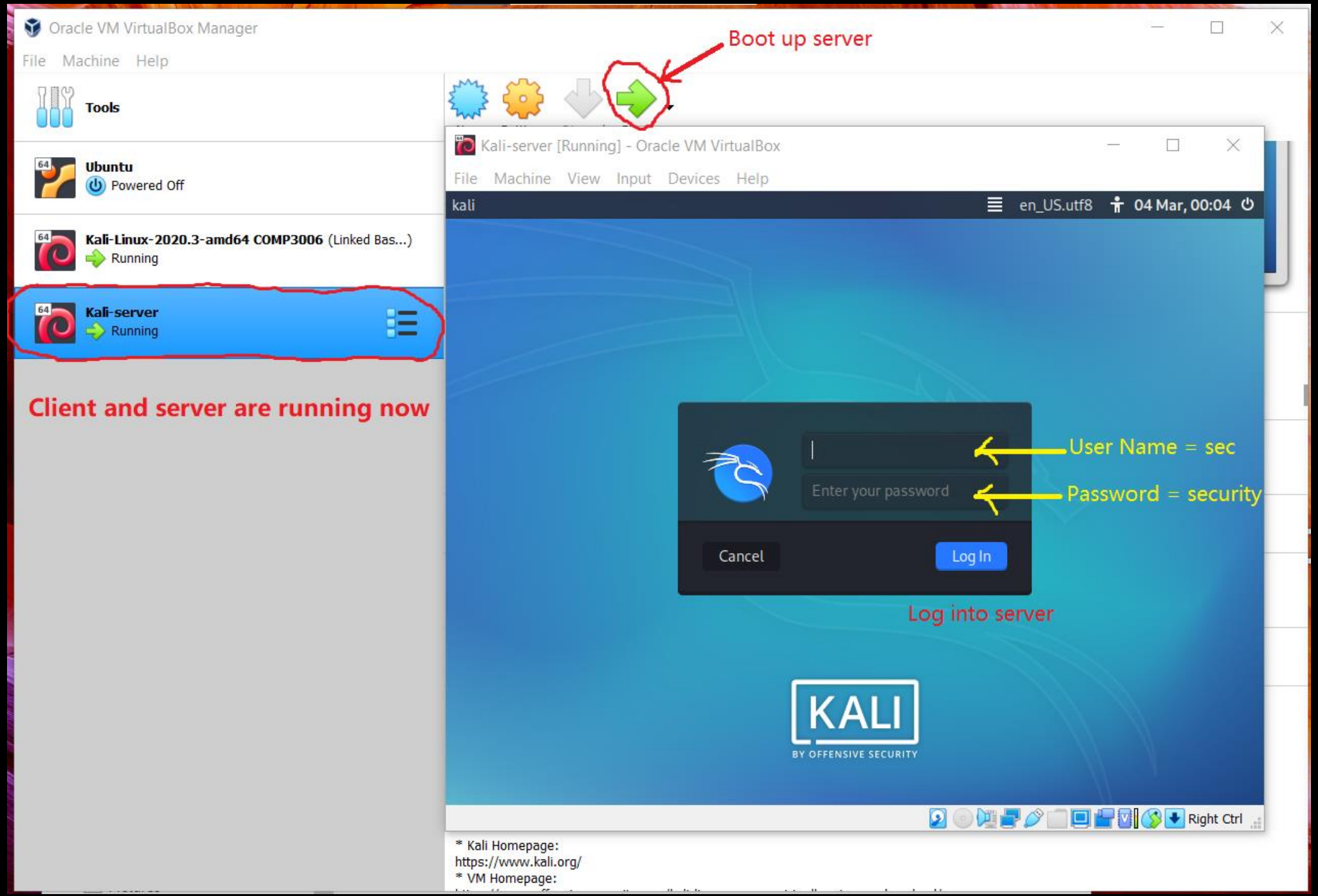
- You need to configure the client and the newly created clone (the server) by following the steps described in one the following videoclips, depending on whether you are using Oracle VM VirtualBox Version 6 or Version 7:
  V6 - https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=19d691b1-c30f-4d7c-8993-afc2007de859&start=0
  V7 - https://video.nottingham.edu.cn/Panopto/Pages/Viewer.aspx?id=2b83a6a0-e8d8-45d5-b06f-afc2007f3344&start=0

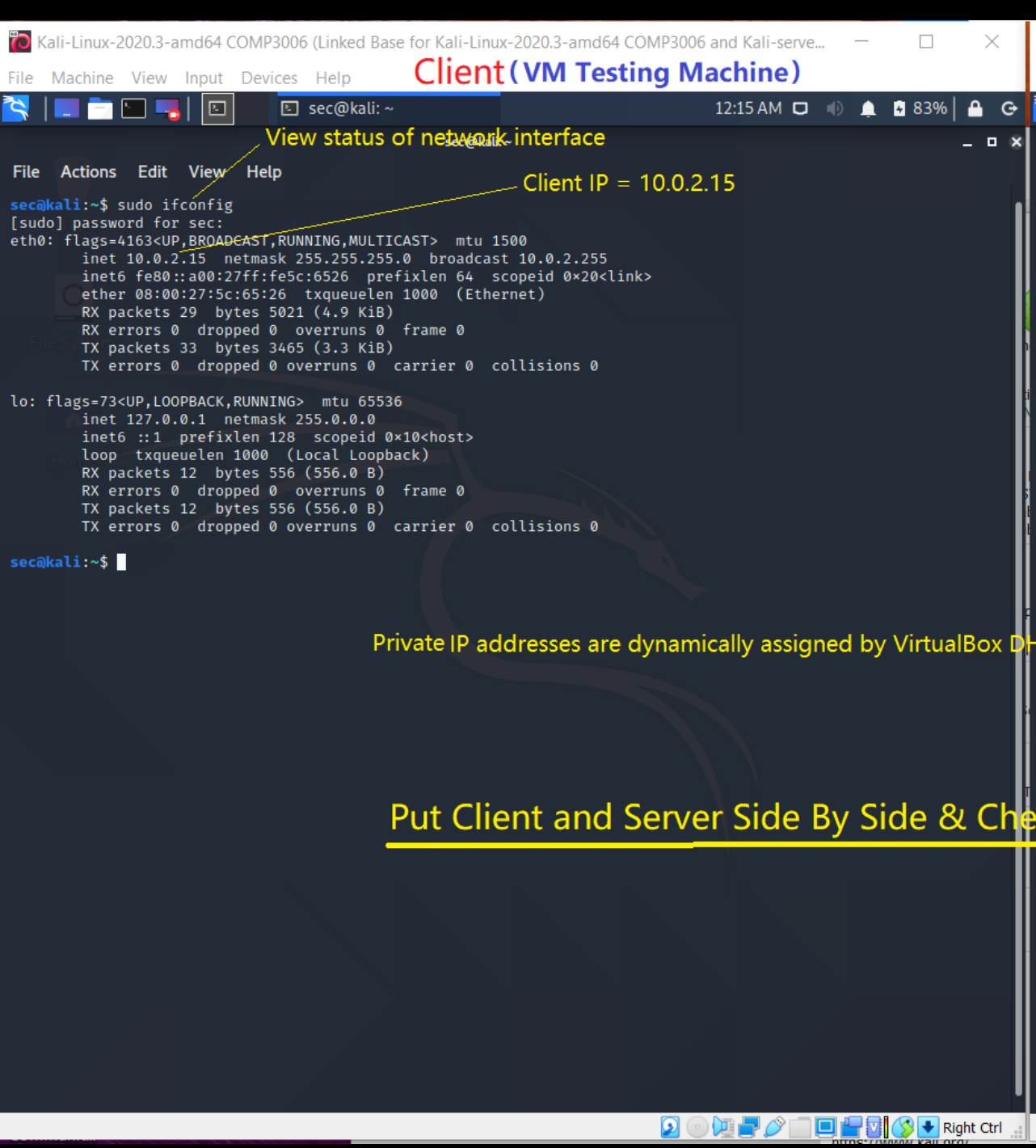
- Remember to √ the "Enable Network Adapter" for both the client and the server.
- Remember to select "NAT Network" (not "NAT") for both the client and the server.
- Remember to click the button for generating a new MAC address for the Kali-server. Otherwise, there will be a conflict because both the client and the server have the same MAC address.

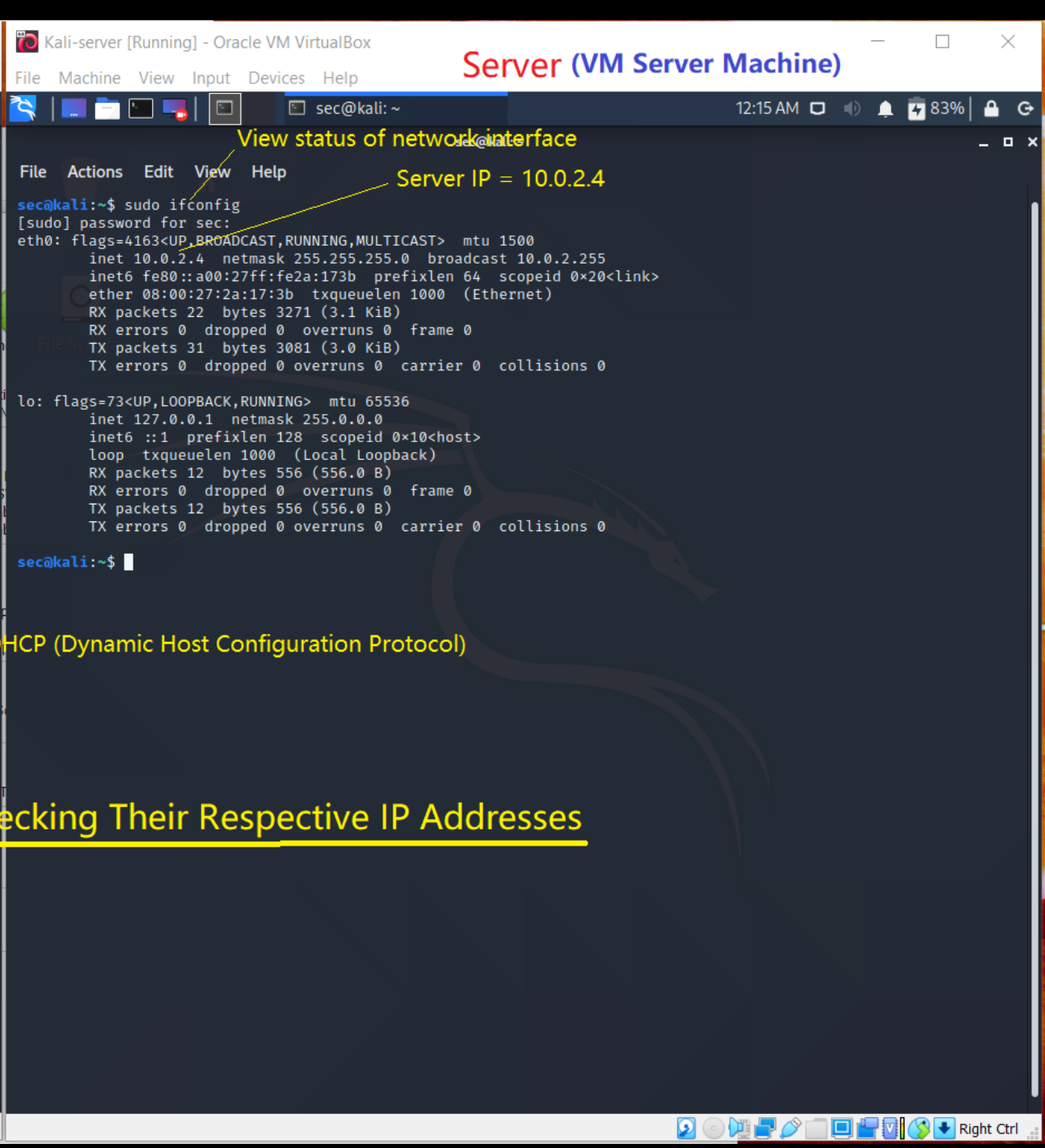
Ready to Start

- You can now start this lab session working on the network communication between the client (Kali-Linux-2020.3-amd64 COMP3006) and the server (Kali-server), focusing on the network security aspect.


Oracle VM VirtualBox Manager
File Machine Help
Boot up client
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3-amd64 COMP3006 (Li...)
Running
Kali-server
Powered Off
Client is running now
Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3...
File Machine View Input Devices Help
kali
en_US.utf8
04 Mar, 00:02
User Name = sec
Enter your password
Password = security
Cancel
Log In
Log into client
KALI
BY OFFENSIVE SECURITY
Right Ctrl
* Kali Homepage:
https://www.kali.org/
* VM Homepage:


Oracle VM VirtualBox Manager
File Machine Help
Boot up server
Tools
Ubuntu
Powered Off
Kali-Linux-2020.3-amd64 COMP3006 (Linked Bas...)
Running
Kali-server
Running
Client and server are running now
Kali-server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali
en_US.utf8
04 Mar, 00:04
Enter your password
User Name = sec
Password = security
Cancel
Log In
Log into server
KALI
BY OFFENSIVE SECURITY
Right Ctrl
* Kali Homepage:
https://www.kali.org/
* VM Homepage:





Private IP addresses are dynamically assigned by VirtualBox DHCP (Dynamic Host Configuration Protocol)

Put Client and Server Side By Side & Checking Their Respective IP Addresses

ICMP (Internet Control Message Protocol) Echo Request Using Ping Command

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

sec@kali: ~ 12:20 AM 83%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 29  bytes 5021 (4.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 3465 (3.3 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 1000  (Local Loopback)
        RX packets 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ sudo ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
From 10.0.2.15 icmp_seq=1 Destination Host Unreachable
From 10.0.2.15 icmp_seq=2 Destination Host Unreachable
From 10.0.2.15 icmp_seq=3 Destination Host Unreachable
From 10.0.2.15 icmp_seq=4 Destination Host Unreachable
From 10.0.2.15 icmp_seq=5 Destination Host Unreachable
From 10.0.2.15 icmp_seq=6 Destination Host Unreachable
From 10.0.2.15 icmp_seq=7 Destination Host Unreachable
From 10.0.2.15 icmp_seq=8 Destination Host Unreachable
From 10.0.2.15 icmp_seq=9 Destination Host Unreachable
From 10.0.2.15 icmp_seq=10 Destination Host Unreachable
From 10.0.2.15 icmp_seq=11 Destination Host Unreachable
From 10.0.2.15 icmp_seq=12 Destination Host Unreachable
From 10.0.2.15 icmp_seq=13 Destination Host Unreachable
From 10.0.2.15 icmp_seq=14 Destination Host Unreachable
From 10.0.2.15 icmp_seq=15 Destination Host Unreachable
^C
--- 10.0.2.6 ping statistics ---
17 packets transmitted, 0 received, +15 errors, 100% packet loss, time 16369ms
pipe 4
sec@kali:~$
```

Ping wrong (unavailable) IP address

Unreachable

Break the execution using CTRL C

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ 12:20 AM 83%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe2a:173b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2a:17:3b  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 3271 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3081 (3.0 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ sudo ping 10.0.2.14
PING 10.0.2.14 (10.0.2.14) 56(84) bytes of data.
From 10.0.2.4 icmp_seq=1 Destination Host Unreachable
From 10.0.2.4 icmp_seq=2 Destination Host Unreachable
From 10.0.2.4 icmp_seq=3 Destination Host Unreachable
From 10.0.2.4 icmp_seq=4 Destination Host Unreachable
From 10.0.2.4 icmp_seq=5 Destination Host Unreachable
From 10.0.2.4 icmp_seq=6 Destination Host Unreachable
From 10.0.2.4 icmp_seq=7 Destination Host Unreachable
From 10.0.2.4 icmp_seq=8 Destination Host Unreachable
From 10.0.2.4 icmp_seq=9 Destination Host Unreachable
From 10.0.2.4 icmp_seq=10 Destination Host Unreachable
From 10.0.2.4 icmp_seq=11 Destination Host Unreachable
From 10.0.2.4 icmp_seq=12 Destination Host Unreachable
From 10.0.2.4 icmp_seq=13 Destination Host Unreachable
From 10.0.2.4 icmp_seq=14 Destination Host Unreachable
From 10.0.2.4 icmp_seq=15 Destination Host Unreachable
^C
--- 10.0.2.14 ping statistics ---
16 packets transmitted, 0 received, +15 errors, 100% packet loss, time 15446ms
pipe 4
sec@kali:~$
```

Ping wrong (unavailable) IP address

Unreachable

Break the execution using CTRL C

Right Ctrl

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

sec@kali: ~ 12:25 AM 83%

sec@kali: ~

File Actions Edit View Help

```
        RX packets 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ sudo ping 10.0.2.6
PING 10.0.2.6 (10.0.2.6) 56(84) bytes of data.
From 10.0.2.15 icmp_seq=1 Destination Host Unreachable
From 10.0.2.15 icmp_seq=2 Destination Host Unreachable
From 10.0.2.15 icmp_seq=3 Destination Host Unreachable
From 10.0.2.15 icmp_seq=4 Destination Host Unreachable
From 10.0.2.15 icmp_seq=5 Destination Host Unreachable
From 10.0.2.15 icmp_seq=6 Destination Host Unreachable
From 10.0.2.15 icmp_seq=7 Destination Host Unreachable
From 10.0.2.15 icmp_seq=8 Destination Host Unreachable
From 10.0.2.15 icmp_seq=9 Destination Host Unreachable
From 10.0.2.15 icmp_seq=10 Destination Host Unreachable
From 10.0.2.15 icmp_seq=11 Destination Host Unreachable
From 10.0.2.15 icmp_seq=12 Destination Host Unreachable
From 10.0.2.15 icmp_seq=13 Destination Host Unreachable
From 10.0.2.15 icmp_seq=14 Destination Host Unreachable
From 10.0.2.15 icmp_seq=15 Destination Host Unreachable
^C
--- 10.0.2.6 ping statistics ---
17 packets transmitted, 0 received, +15 errors, 100% packet loss, time 16369ms
pipe 4
sec@kali:~$ sudo ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.686 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.456 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.552 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.481 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.436 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.478 ms
64 bytes from 10.0.2.4: icmp_seq=7 ttl=64 time=0.471 ms
64 bytes from 10.0.2.4: icmp_seq=8 ttl=64 time=0.448 ms
64 bytes from 10.0.2.4: icmp_seq=9 ttl=64 time=0.476 ms
64 bytes from 10.0.2.4: icmp_seq=10 ttl=64 time=0.570 ms
64 bytes from 10.0.2.4: icmp_seq=11 ttl=64 time=0.501 ms
64 bytes from 10.0.2.4: icmp_seq=12 ttl=64 time=0.484 ms
64 bytes from 10.0.2.4: icmp_seq=13 ttl=64 time=0.433 ms
64 bytes from 10.0.2.4: icmp_seq=14 ttl=64 time=0.490 ms
64 bytes from 10.0.2.4: icmp_seq=15 ttl=64 time=0.465 ms
64 bytes from 10.0.2.4: icmp_seq=16 ttl=64 time=0.454 ms
^C
--- 10.0.2.4 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15345ms
rtt min/avg/max/mdev = 0.433/0.492/0.686/0.061 ms
sec@kali:~$
sec@kali:~$
```

Ping IP of server

ICMP reply (echo) from server

CTRL C to break

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ 12:25 AM 83%

sec@kali: ~

File Actions Edit View Help

```
From 10.0.2.4 icmp_seq=3 Destination Host Unreachable
From 10.0.2.4 icmp_seq=4 Destination Host Unreachable
From 10.0.2.4 icmp_seq=5 Destination Host Unreachable
From 10.0.2.4 icmp_seq=6 Destination Host Unreachable
From 10.0.2.4 icmp_seq=7 Destination Host Unreachable
From 10.0.2.4 icmp_seq=8 Destination Host Unreachable
From 10.0.2.4 icmp_seq=9 Destination Host Unreachable
From 10.0.2.4 icmp_seq=10 Destination Host Unreachable
From 10.0.2.4 icmp_seq=11 Destination Host Unreachable
From 10.0.2.4 icmp_seq=12 Destination Host Unreachable
From 10.0.2.4 icmp_seq=13 Destination Host Unreachable
From 10.0.2.4 icmp_seq=14 Destination Host Unreachable
From 10.0.2.4 icmp_seq=15 Destination Host Unreachable
^C
--- 10.0.2.14 ping statistics ---
16 packets transmitted, 0 received, +15 errors, 100% packet loss, time 15446ms
pipe 4
sec@kali:~$ sudo ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.429 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.467 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.438 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.464 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.406 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.431 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.424 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.461 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.402 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=0.422 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.586 ms
64 bytes from 10.0.2.15: icmp_seq=12 ttl=64 time=0.465 ms
64 bytes from 10.0.2.15: icmp_seq=13 ttl=64 time=0.527 ms
64 bytes from 10.0.2.15: icmp_seq=14 ttl=64 time=0.478 ms
64 bytes from 10.0.2.15: icmp_seq=15 ttl=64 time=0.493 ms
64 bytes from 10.0.2.15: icmp_seq=16 ttl=64 time=0.476 ms
64 bytes from 10.0.2.15: icmp_seq=17 ttl=64 time=0.482 ms
64 bytes from 10.0.2.15: icmp_seq=18 ttl=64 time=0.448 ms
64 bytes from 10.0.2.15: icmp_seq=19 ttl=64 time=0.433 ms
64 bytes from 10.0.2.15: icmp_seq=20 ttl=64 time=0.415 ms
C64 bytes from 10.0.2.15: icmp_seq=21 ttl=64 time=0.412 ms
64 bytes from 10.0.2.15: icmp_seq=22 ttl=64 time=0.505 ms
64 bytes from 10.0.2.15: icmp_seq=23 ttl=64 time=0.554 ms
64 bytes from 10.0.2.15: icmp_seq=24 ttl=64 time=0.552 ms
64 bytes from 10.0.2.15: icmp_seq=25 ttl=64 time=0.520 ms
^C
--- 10.0.2.15 ping statistics ---
25 packets transmitted, 25 received, 0% packet loss, time 24564ms
rtt min/avg/max/mdev = 0.402/0.467/0.586/0.049 ms
sec@kali:~$
sec@kali:~$
```

Ping IP of client

ICMP reply (echo) from client

CTRL C to break

Right Ctrl

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

VM Testing Machine (use for testing the server machine)

sec@kali: ~ 12:00 AM 85%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 3661 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2697 (2.6 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$
```

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VM Server Machine (providing services, such as ssh and http, to the client machine)

sec@kali: ~ 12:00 AM 85%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe2a:173b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:2a:17:3b  txqueuelen 1000  (Ethernet)
        RX packets 5  bytes 990 (990.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 2313 (2.2 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 14  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 710 (710.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: man:sshd(8)
             man:sshd_config(5)
sec@kali:~$
sec@kali:~$ sudo service ssh start
sec@kali:~$
sec@kali:~$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; vendor preset: disabled)
     Active: active (running) since Sun 2023-03-05 23:58:21 EST; 20s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 1319 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 1320 (sshd)
      Tasks: 1 (limit: 2308)
     Memory: 2.3M
     CGroup: /system.slice/ssh.service
             └─1320 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Mar 05 23:58:21 kali systemd[1]: Starting OpenBSD Secure Shell server...
Mar 05 23:58:21 kali sshd[1320]: Server listening on 0.0.0.0 port 22.
Mar 05 23:58:21 kali sshd[1320]: Server listening on :: port 22.
Mar 05 23:58:21 kali systemd[1]: Started OpenBSD Secure Shell server.
sec@kali:~$
```

Check and Start ssh Service

Check the status of the ssh (remote login) service

ssh service is curently inactive (or dead)

Start the ssh service

ssh service is currently active (running)

Right Ctrl

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

VM Testing Machine

sec@kali: ~ 12:14 AM 85%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 3661 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2697 (2.6 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$
```

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

VM Server Machine

sec@kali: ~ 12:14 AM 85%

sec@kali: ~

File Actions Edit View Help

Check and Start the http Service

```
sec@kali:~$
sec@kali:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: inactive (dead)
       Docs: https://httpd.apache.org/docs/2.4/

Mar 06 00:06:27 kali systemd[1]: Starting The Apache HTTP Server ...
Mar 06 00:06:28 kali apachectl[1387]: AH00558: apache2: Could not reliably determine the server's fully qualifie>
Mar 06 00:06:28 kali systemd[1]: Started The Apache HTTP Server.
Mar 06 00:12:20 kali systemd[1]: Stopping The Apache HTTP Server ...
Mar 06 00:12:20 kali apachectl[1484]: AH00558: apache2: Could not reliably determine the server's fully qualifie>
Mar 06 00:12:20 kali systemd[1]: apache2.service: Succeeded.
Mar 06 00:12:20 kali systemd[1]: Stopped The Apache HTTP Server.

sec@kali:~$
sec@kali:~$ sudo service apache2 start
sec@kali:~$
sec@kali:~$ sudo service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
     Active: active (running) since Mon 2023-03-06 00:13:54 EST; 11s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 1506 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 1510 (apache2)
      Tasks: 6 (limit: 2308)
     Memory: 12.1M
     CGroup: /system.slice/apache2.service
             ├─1510 /usr/sbin/apache2 -k start
             ├─1511 /usr/sbin/apache2 -k start
             ├─1512 /usr/sbin/apache2 -k start
             ├─1513 /usr/sbin/apache2 -k start
             ├─1514 /usr/sbin/apache2 -k start
             └─1515 /usr/sbin/apache2 -k start

Mar 06 00:13:54 kali systemd[1]: Starting The Apache HTTP Server ...
Mar 06 00:13:54 kali apachectl[1509]: AH00558: apache2: Could not reliably determine the server's fully qualifie>
Mar 06 00:13:54 kali systemd[1]: Started The Apache HTTP Server.

sec@kali:~$
sec@kali:~$
```

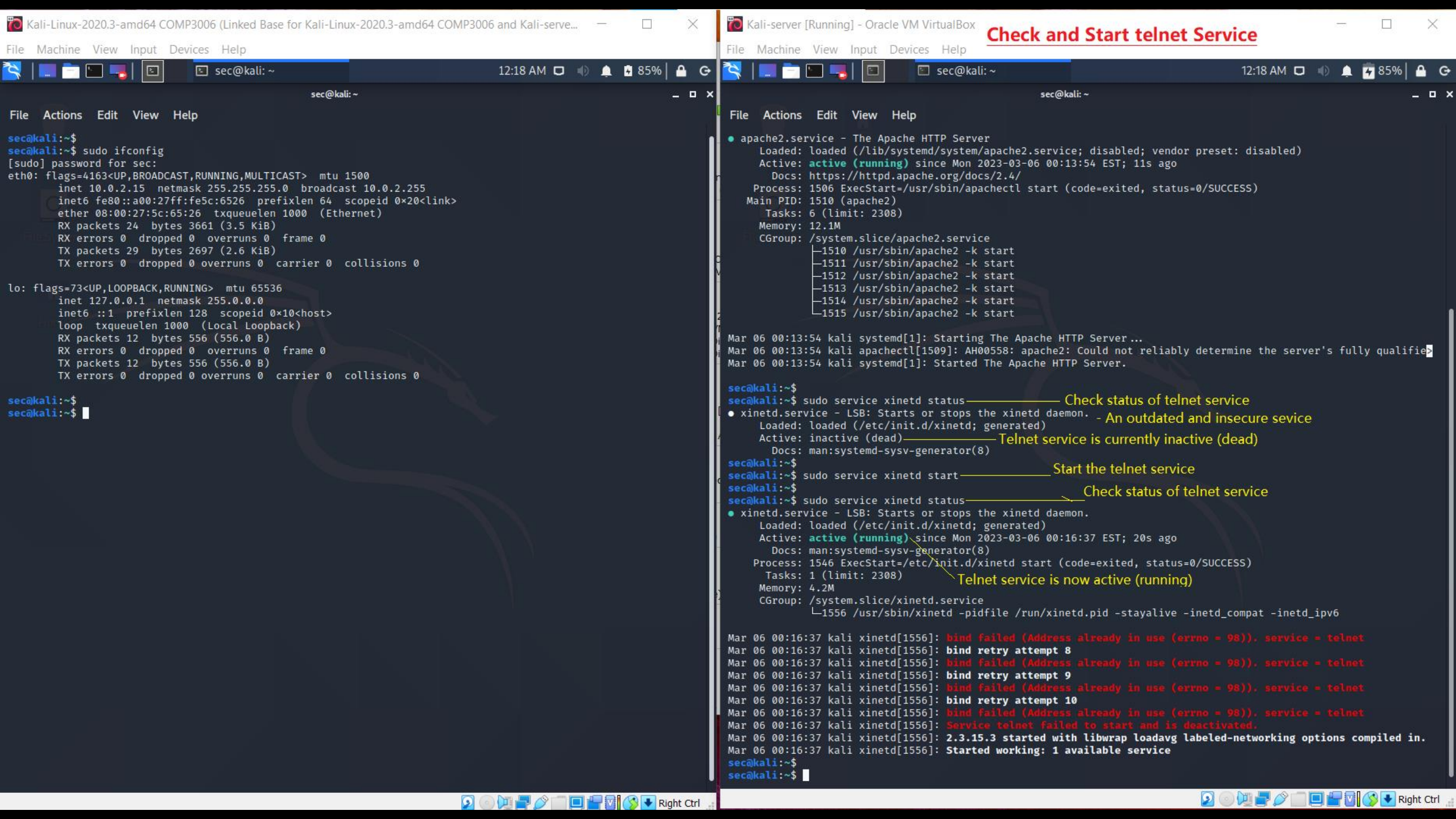
Check the status of the http service

The http service is currently inactive (dead)

Start the http service

http service is currently active (running)

Right Ctrl


Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...
File Machine View Input Devices Help
sec@kali: ~
12:18 AM
85%
sec@kali: ~
File Actions Edit View Help
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:5c:65:26 txqueuelen 1000 (Ethernet)
RX packets 24 bytes 3661 (3.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 29 bytes 2697 (2.6 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 12 bytes 556 (556.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12 bytes 556 (556.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sec@kali:~$
sec@kali:~$
Right Ctrl
Kali-server [Running] - Oracle VM VirtualBox
Check and Start telnet Service
File Machine View Input Devices Help
sec@kali: ~
12:18 AM
85%
sec@kali: ~
File Actions Edit View Help
● apache2.service - The Apache HTTP Server
Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
Active: active (running) since Mon 2023-03-06 00:13:54 EST; 11s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 1506 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 1510 (apache2)
Tasks: 6 (limit: 2308)
Memory: 12.1M
CGroup: /system.slice/apache2.service
├─1510 /usr/sbin/apache2 -k start
├─1511 /usr/sbin/apache2 -k start
├─1512 /usr/sbin/apache2 -k start
├─1513 /usr/sbin/apache2 -k start
├─1514 /usr/sbin/apache2 -k start
└─1515 /usr/sbin/apache2 -k start
Mar 06 00:13:54 kali systemd[1]: Starting The Apache HTTP Server ...
Mar 06 00:13:54 kali apachectl[1509]: AH00558: apache2: Could not reliably determine the server's fully qualifie
Mar 06 00:13:54 kali systemd[1]: Started The Apache HTTP Server.
sec@kali:~$
sec@kali:~$ sudo service xinetd status
Check status of telnet service
● xinetd.service - LSB: Starts or stops the xinetd daemon.
- An outdated and insecure sevice
Loaded: loaded (/etc/init.d/xinetd; generated)
Active: inactive (dead)
Telnet service is currently inactive (dead)
Docs: man:systemd-sysv-generator(8)
sec@kali:~$
sec@kali:~$ sudo service xinetd start
Start the telnet service
sec@kali:~$
sec@kali:~$ sudo service xinetd status
Check status of telnet service
● xinetd.service - LSB: Starts or stops the xinetd daemon.
Loaded: loaded (/etc/init.d/xinetd; generated)
Active: active (running) since Mon 2023-03-06 00:16:37 EST; 20s ago
Docs: man:systemd-sysv-generator(8)
Process: 1546 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
Tasks: 1 (limit: 2308)
Memory: 4.2M
CGroup: /system.slice/xinetd.service
└─1556 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
Telnet service is now active (running)
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 8
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 9
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 10
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: Service telnet failed to start and is deactivated.
Mar 06 00:16:37 kali xinetd[1556]: 2.3.15.3 started with libwrap loadavg labeled-networking options compiled in.
Mar 06 00:16:37 kali xinetd[1556]: Started working: 1 available service
sec@kali:~$
sec@kali:~$
Right Ctrl

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

sec@kali: ~ 12:20 AM 85%

sec@kali: ~

File Actions Edit View Help

```
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 3661 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2697 (2.6 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$
```

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Check and Start sql Service

sec@kali: ~ 12:20 AM 85%

sec@kali: ~

File Actions Edit View Help

```
     Docs: man:systemd-sysv-generator(8)
  Process: 1546 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
    Tasks: 1 (limit: 2308)
   Memory: 4.2M
   CGroup: /system.slice/xinetd.service
           └─1556 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6

Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 8
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 9
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 10
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: Service telnet failed to start and is deactivated.
Mar 06 00:16:37 kali xinetd[1556]: 2.3.15.3 started with libwrap loadavg labeled-networking options compiled in.
Mar 06 00:16:37 kali xinetd[1556]: Started working: 1 available service
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: inactive (dead)
       Docs: man:systemd-sysv-generator(8)
sec@kali:~$
sec@kali:~$ sudo service mysql start
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: active (running) since Mon 2023-03-06 00:19:36 EST; 16s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 1588 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
      Tasks: 33 (limit: 2308)
     Memory: 102.5M
     CGroup: /system.slice/mysql.service
             ├─1615 /bin/sh /usr/bin/mysqld_safe
             ├─1732 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-
             └─1733 logger -t mysqld -p daemon error

Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] InnoDB: Buffer pool(s) load completed at 230306
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Server socket created on IP: '::'.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Reading of all Master_info entries succeeded
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Added new Master_info '' to hash table
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] /usr/sbin/mysqld: ready for connections.
Mar 06 00:19:35 kali mysqld[1733]: Version: '10.3.23-MariaDB-1'  socket: '/var/run/mysqld/mysqld.sock'  port: 33
Mar 06 00:19:36 kali mysql[1588]: Starting MariaDB database server: mysqld ..
Mar 06 00:19:36 kali systemd[1]: Started LSB: Start and stop the mysql database server daemon.
Mar 06 00:19:36 kali /etc/mysql/debian-start[1810]: Triggering myisam-recover for all MyISAM tables and aria-rec

sec@kali:~$
sec@kali:~$
```

Check the status of the sql service

The current status of sql service is inactive (dead)

Start the sql service

Check the status of the sql service again

The current status of the sql service is active (running)

Right Ctrl

IP and Port Scanning Using Nmap - Detect IPs

Subnet Calculator
https://mxtoolbox.com/SubnetCalculator.aspx

```
sec@kali:~$
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
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:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 3661 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2697 (2.6 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$ sudo nmap -sn 10.0.2.1/27
[sudo] password for sec:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-06 01:49 EST
Nmap scan report for 10.0.2.1
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
MAC Address: 08:00:27:EB:A9:B1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00037s latency).
MAC Address: 08:00:27:2A:17:3B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 32 IP addresses (5 hosts up) scanned in 0.67 seconds
sec@kali:~$
```

nmap command is for IP and port scanning

-sn option instructs nmap not to perform detailed scans of ports, just to return their IP addresses

This represents a range of IP addresses from 10.0.2.0 to 10.0.2.31 (a subnet of 32 IP addresses in total).

This is a CIDR notation in representing IP subnets.

4 virtual network interface cards (NICs) were detected. Each of them has an IP address.

2 of them were created using VirtualBox.

Kali-server
Kali-Linux-2020.3-amd64
COMP3006

This is the client VM itself

```
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: inactive (dead)
       Docs: man:systemd-sysv-generator(8)
sec@kali:~$
sec@kali:~$ sudo service mysql start
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: active (running) since Mon 2023-03-06 00:19:36 EST; 16s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 1588 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
      Tasks: 33 (limit: 2308)
     Memory: 102.5M
     CGroup: /system.slice/mysql.service
             ├─1615 /bin/sh /usr/bin/mysqld_safe
             ├─1732 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-
             └─1733 logger -t mysqld -p daemon error

Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] InnoDB: Buffer pool(s) load completed at 230306
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Server socket created on IP: '::'.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Reading of all Master_info entries succeeded
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Added new Master_info '' to hash table
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] /usr/sbin/mysqld: ready for connections.
Mar 06 00:19:35 kali mysqld[1733]: Version: '10.3.23-MariaDB-1'  socket: '/var/run/mysqld/mysqld.sock'  port: 33
Mar 06 00:19:36 kali mysql[1588]: Starting MariaDB database server: mysqld ..
Mar 06 00:19:36 kali systemd[1]: Started LSB: Start and stop the mysql database server daemon.
Mar 06 00:19:36 kali /etc/mysql/debian-start[1810]: Triggering myisam-recover for all MyISAM tables and aria-rec

sec@kali:~$
sec@kali:~$
```

IP and Port Scanning Using Nmap - Detect Ports

Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...

File Machine View Input Devices Help

sec@kali: ~ 01:54 AM 85%

sec@kali: ~

File Actions Edit View Help

```
        inet6 fe80::a00:27ff:fe5c:6526  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:5c:65:26  txqueuelen 1000  (Ethernet)
        RX packets 24  bytes 3661 (3.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 29  bytes 2697 (2.6 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 12  bytes 556 (556.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 556 (556.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$
sec@kali:~$ sudo nmap -sn 10.0.2.1/27
[sudo] password for sec:
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-06 01:49 EST
Nmap scan report for 10.0.2.1
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
MAC Address: 08:00:27:EB:A9:B1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00037s latency).
MAC Address: 08:00:27:2A:17:3B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 32 IP addresses (5 hosts up) scanned in 0.67 seconds
sec@kali:~$
sec@kali:~$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2023-03-06 01:53 EST
Nmap scan report for 10.0.2.4
Host is up (0.00015s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.3p1 Debian 1 (protocol 2.0)
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.43 ((Debian))
3306/tcp open  mysql   MySQL 5.5.5-10.3.23-MariaDB-1
MAC Address: 08:00:27:2A:17:3B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
sec@kali:~$
```

-sV option instructs nmap to perform a detailed port scan

Now the hacker can target at the server (IP address = 10.0.2.4)

4 open ports were detected.
They can be the targets for the hackers.

Right Ctrl

Kali-server [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

sec@kali: ~ 01:54 AM 85%

sec@kali: ~

File Actions Edit View Help

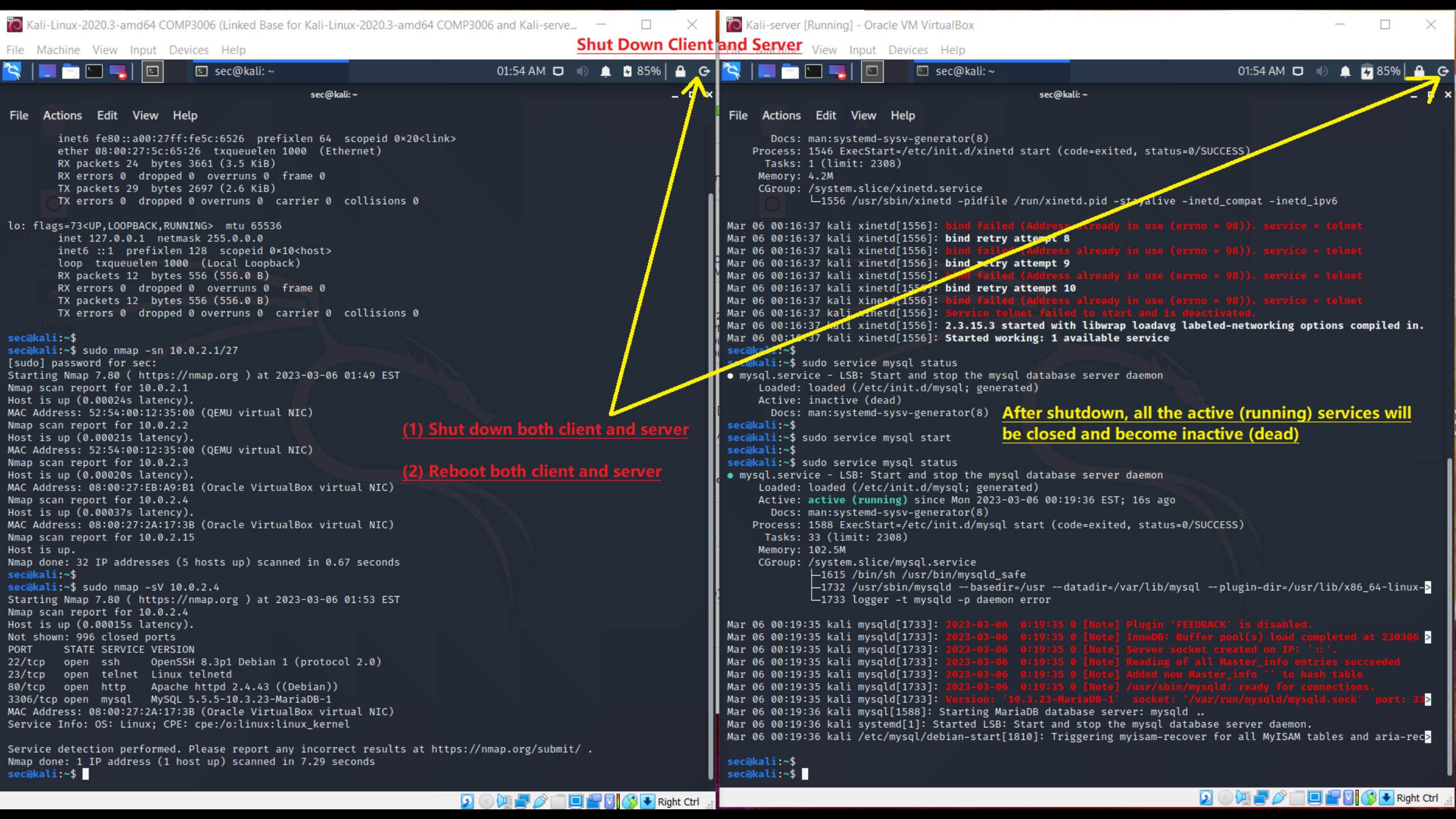
```
       Docs: man:systemd-sysv-generator(8)
    Process: 1546 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
      Tasks: 1 (limit: 2308)
     Memory: 4.2M
     CGroup: /system.slice/xinetd.service
             └─1556 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6

Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 8
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 9
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 10
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: Service telnet failed to start and is deactivated.
Mar 06 00:16:37 kali xinetd[1556]: 2.3.15.3 started with libwrap loadavg labeled-networking options compiled in.
Mar 06 00:16:37 kali xinetd[1556]: Started working: 1 available service
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: inactive (dead)
       Docs: man:systemd-sysv-generator(8)
sec@kali:~$
sec@kali:~$ sudo service mysql start
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
     Loaded: loaded (/etc/init.d/mysql; generated)
     Active: active (running) since Mon 2023-03-06 00:19:36 EST; 16s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 1588 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
      Tasks: 33 (limit: 2308)
     Memory: 102.5M
     CGroup: /system.slice/mysql.service
             ├─1615 /bin/sh /usr/bin/mysqld_safe
             ├─1732 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-
             └─1733 logger -t mysqld -p daemon error

Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] InnoDB: Buffer pool(s) load completed at 230306
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Server socket created on IP: '::'.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Reading of all Master_info entries succeeded
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] Added new Master_info '' to hash table
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06  0:19:35 0 [Note] /usr/sbin/mysqld: ready for connections.
Mar 06 00:19:35 kali mysqld[1733]: Version: '10.3.23-MariaDB-1'  socket: '/var/run/mysqld/mysqld.sock'  port: 33
Mar 06 00:19:36 kali mysql[1588]: Starting MariaDB database server: mysqld ..
Mar 06 00:19:36 kali systemd[1]: Started LSB: Start and stop the mysql database server daemon.
Mar 06 00:19:36 kali /etc/mysql/debian-start[1810]: Triggering myisam-recover for all MyISAM tables and aria-rec

sec@kali:~$
sec@kali:~$
```

Right Ctrl


Kali-Linux-2020.3-amd64 COMP3006 (Linked Base for Kali-Linux-2020.3-amd64 COMP3006 and Kali-serve...
File Machine View Input Devices Help
Shut Down Client and Server
sec@kali: ~
01:54 AM
85%
sec@kali: ~
File Actions Edit View Help
inet6 fe80::a00:27ff:fe5c:6526 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:5c:65:26 txqueuelen 1000 (Ethernet)
RX packets 24 bytes 3661 (3.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 29 bytes 2697 (2.6 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 12 bytes 556 (556.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12 bytes 556 (556.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sec@kali:~$
sec@kali:~$ sudo nmap -sn 10.0.2.1/27
[sudo] password for sec:
Starting Nmap 7.80 (https://nmap.org) at 2023-03-06 01:49 EST
Nmap scan report for 10.0.2.1
Host is up (0.00024s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
MAC Address: 08:00:27:EB:A9:B1 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.4
Host is up (0.00037s latency).
MAC Address: 08:00:27:2A:17:3B (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 32 IP addresses (5 hosts up) scanned in 0.67 seconds
sec@kali:~$
sec@kali:~$ sudo nmap -sV 10.0.2.4
Starting Nmap 7.80 (https://nmap.org) at 2023-03-06 01:53 EST
Nmap scan report for 10.0.2.4
Host is up (0.00015s latency).
Not shown: 996 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.3p1 Debian 1 (protocol 2.0)
23/tcp open telnet Linux telnetd
80/tcp open http Apache httpd 2.4.43 ((Debian))
3306/tcp open mysql MySQL 5.5.5-10.3.23-MariaDB-1
MAC Address: 08:00:27:2A:17:3B (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.29 seconds
sec@kali:~$
(1) Shut down both client and server
(2) Reboot both client and server
Right Ctrl
Kali-server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
01:54 AM
85%
sec@kali: ~
File Actions Edit View Help
Docs: man:systemd-sysv-generator(8)
Process: 1546 ExecStart=/etc/init.d/xinetd start (code=exited, status=0/SUCCESS)
Tasks: 1 (limit: 2308)
Memory: 4.2M
CGroup: /system.slice/xinetd.service
└1556 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 8
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 9
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: bind retry attempt 10
Mar 06 00:16:37 kali xinetd[1556]: bind failed (Address already in use (errno = 98)). service = telnet
Mar 06 00:16:37 kali xinetd[1556]: Service telnet failed to start and is deactivated.
Mar 06 00:16:37 kali xinetd[1556]: 2.3.15.3 started with libwrap loadavg labeled-networking options compiled in.
Mar 06 00:16:37 kali xinetd[1556]: Started working: 1 available service
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
Loaded: loaded (/etc/init.d/mysql; generated)
Active: inactive (dead)
Docs: man:systemd-sysv-generator(8)
sec@kali:~$
sec@kali:~$ sudo service mysql start
sec@kali:~$
sec@kali:~$ sudo service mysql status
● mysql.service - LSB: Start and stop the mysql database server daemon
Loaded: loaded (/etc/init.d/mysql; generated)
Active: active (running) since Mon 2023-03-06 00:19:36 EST; 16s ago
Docs: man:systemd-sysv-generator(8)
Process: 1588 ExecStart=/etc/init.d/mysql start (code=exited, status=0/SUCCESS)
Tasks: 33 (limit: 2308)
Memory: 102.5M
CGroup: /system.slice/mysql.service
├1615 /bin/sh /usr/bin/mysqld_safe
├1732 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86_64-linux-
└1733 logger -t mysqld -p daemon error
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] Plugin 'FEEDBACK' is disabled.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] InnoDB: Buffer pool(s) load completed at 230306
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] Server socket created on IP: '::'.
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] Reading of all Master_info entries succeeded
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] Added new Master_info '' to hash table
Mar 06 00:19:35 kali mysqld[1733]: 2023-03-06 0:19:35 0 [Note] /usr/sbin/mysqld: ready for connections.
Mar 06 00:19:35 kali mysqld[1733]: Version: '10.3.23-MariaDB-1' socket: '/var/run/mysqld/mysqld.sock' port: 33
Mar 06 00:19:36 kali mysql[1588]: Starting MariaDB database server: mysqld ..
Mar 06 00:19:36 kali systemd[1]: Started LSB: Start and stop the mysql database server daemon.
Mar 06 00:19:36 kali /etc/mysql/debian-start[1810]: Triggering myisam-recover for all MyISAM tables and aria-rec
sec@kali:~$
sec@kali:~$
After shutdown, all the active (running) services will be closed and become inactive (dead)
Right Ctrl