Abertay University

Installing the pen testing network on a home machine.

Note 1: -

Note that Information contained in this document is for educational purposes.

.

Contents

.

1 INTRODUCTION

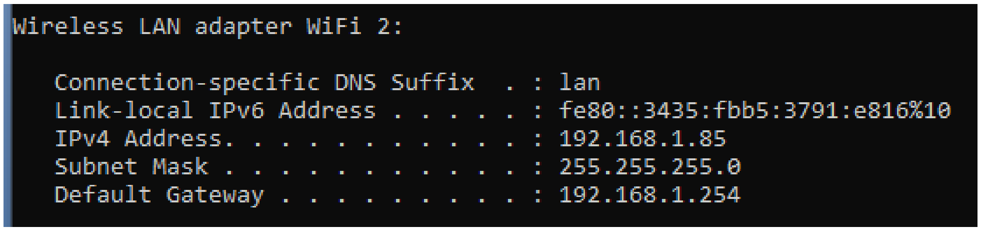
ADVICE– Get VMWARE Workstation and Server1 working first. Once they are working then the others are generally easy.

1.1 CHECK THAT YOUR INTERNET CONNECTION DOES NOT CONFLICT.

Initially, you should check that your home Internet connection is not in the **192.168.10.x** range. Note that this is unusual.

- From your main Windows desktop, run a command prompt (**cmd**).
- Type **ipconfig**

Look for your Internet connection. In the case below, it is in the **192.168.1.x** range so there will be no conflicts.



```
Wireless LAN adapter WiFi 2:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::3435:fbb5:3791:e816%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.85
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.254
```

If your Internet connection is in the **192.168.10.x** range then you have the options of (1) Disabling your Internet card when you are working on the pen testing material or (2) Re-configuring your home network.

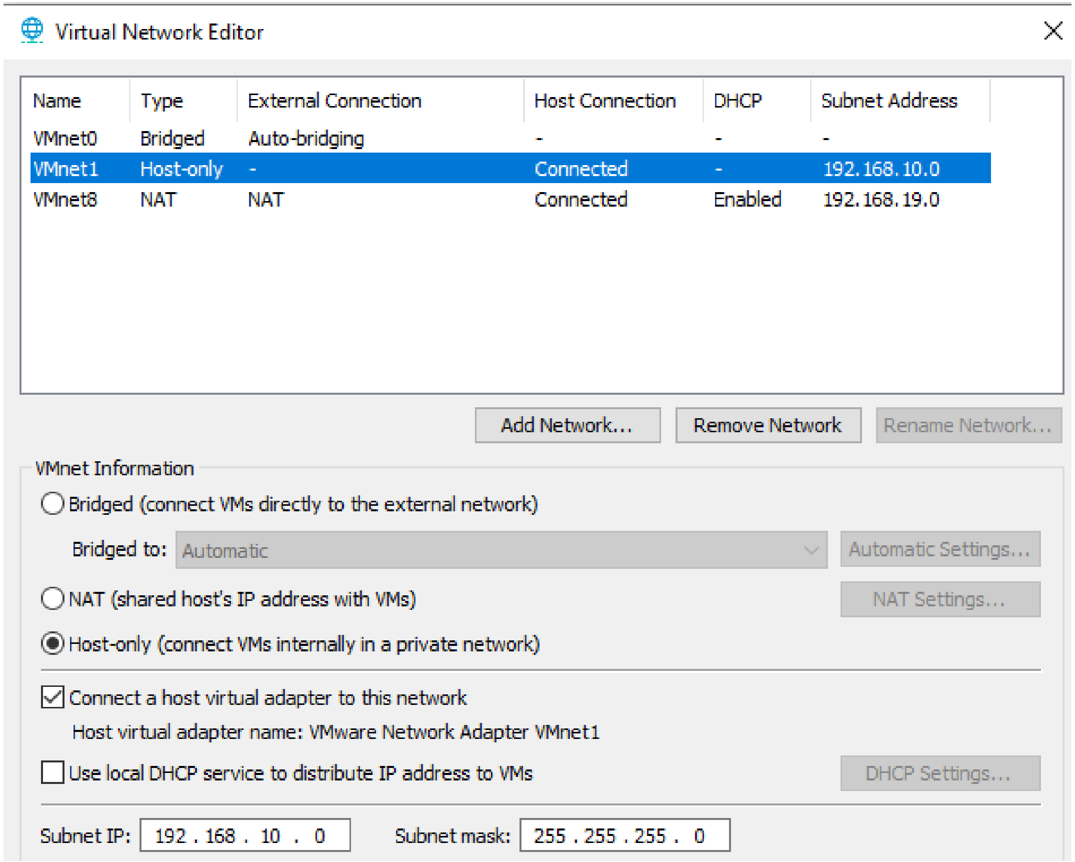
Under Windows, you can disable your Network card from Network Status, Change Adapter Options then right-click on the card and choose Disable. It can be re-enabled in the same way.

1.2 Install VMWARE Workstation

- **Download and Install VMWARE Workstation 16**. The serial number is held in the file **"VMWARE license.txt"**. Please keep this secret – you would normally get your own license but the technician who deals with VMWARE is off work long term so we are having trouble accessing the system.

1.3 Configure VMWARE Workstation

- **Run VMWARE Workstation** and select **Edit** then **Virtual Network Editor**. Make sure that **VMNET1** has been set correctly (see screenshot below).



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	-	192.168.10.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.19.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

○ NAT (shared host's IP address with VMs)

● Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

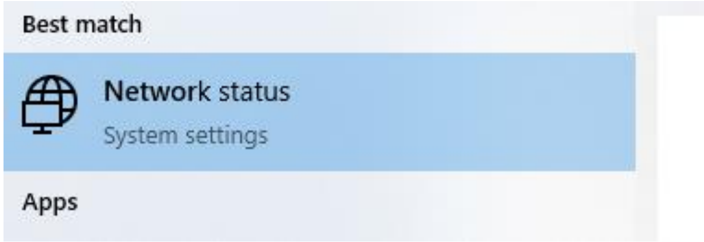
□ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 10 . 0 Subnet mask: 255 . 255 . 255 . 0

1.4 Configure VMNET1 in Windows

Under Windows, we must set the IP address of **VMNET1 to 192.168.10.254**.

- Search for **Network Status**

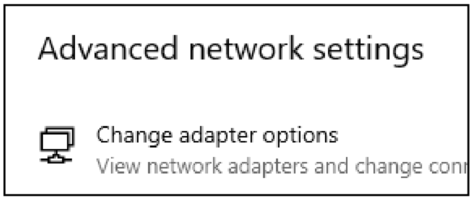


Best match

Network status
System settings

Apps

- From **Advanced Network Settings**, select **Change Adapter options**.

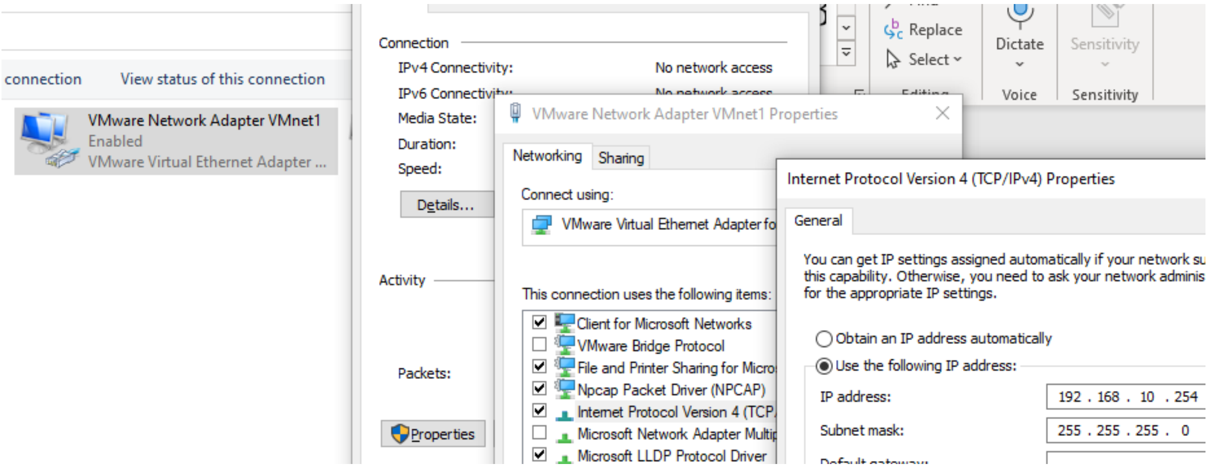


Advanced network settings

Change adapter options
View network adapters and change con

- **Right click on VMNET1** and select **Properties**

- Then select Internet Protocol Version 4 and Sset the IP address to **192.168.10.254** and the Subnet mask to **255.255.255.0. No gateway or DNS is required**.



VMware Network Adapter VMnet1
Enabled
VMware Virtual Ethernet Adapter ...

Connection
IPv4 Connectivity: No network access
IPv6 Connectivity: No network access
Media State:
Duration:
Speed:

Activity

Packets:

VMware Network Adapter VMnet1 Properties

Connect using:
VMware Virtual Ethernet Adapter fo

This connection uses the following items:
☑ Client for Microsoft Networks
☐ VMware Bridge Protocol
☑ File and Printer Sharing for Micro
☑ Npcap Packet Driver (NPCAP)
☑ Internet Protocol Version 4 (TCP
☐ Microsoft Network Adapter Multip
☑ Microsoft LLDP Protocol Driver

Internet Protocol Version 4 (TCP/IPv4) Properties

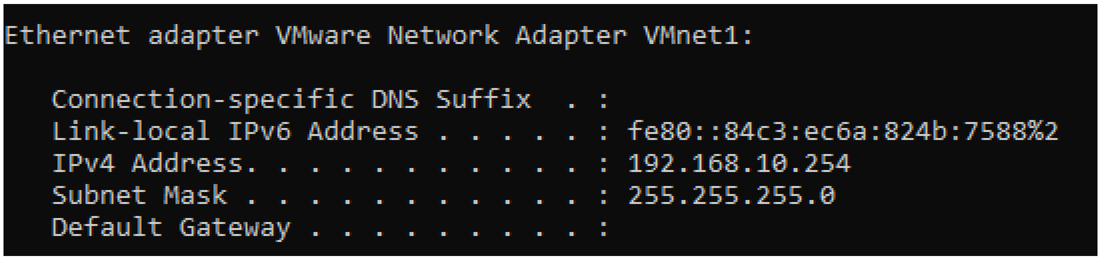
You can get IP settings assigned automatically if your network su
this capability. Otherwise, you need to ask your network adminis
for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 10 . 254
Subnet mask: 255 . 255 . 255 . 0
Default gateway:

- From your main Windows desktop, run a command prompt (**cmd**).

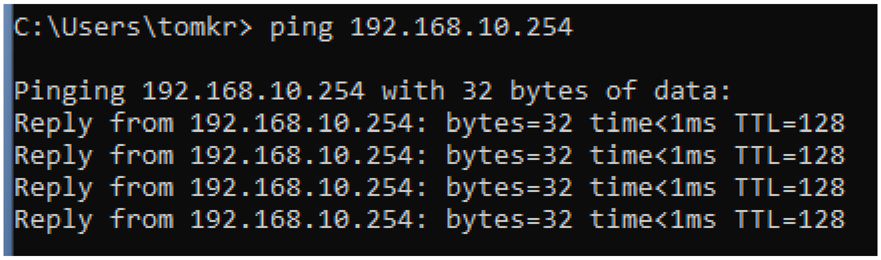
- Type **ipconfig**

As shown below, you should be able to see that vmnet1 is set to **192.168.10.254**



```
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::84c3:ec6a:824b:7588%2
   IPv4 Address. . . . . . . . . . . : 192.168.10.254
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

To make sure that it is working properly, type **ping 192.168.10.254**



```
C:\Users\tomkr> ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
Reply from 192.168.10.254: bytes=32 time<1ms TTL=128
```

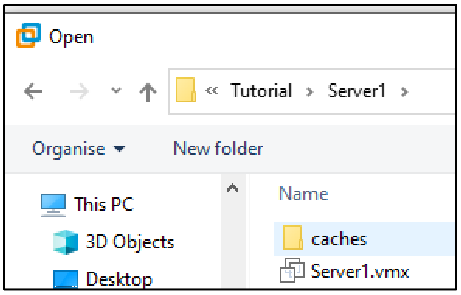
If you do **not** receive a ping response then something is wrong. It may be a Firewall issue? But this must be investigated before continuing.

1.5 Under VMWARE workstation, install Server1

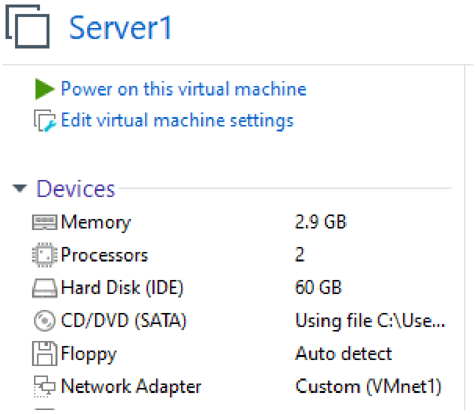
- Download the virtual machine named **Server1 and unzip to a folder e.g. C:\VMs\Server1.**

For the three VMs, a recommended folder structure is C:\VMs\Tutorial\Server1, C:\VMs\Tutorial\Server2 and C:\VMs\Tutorial\Client1

- **Under VMWARE Workstation**, Select **Open** then **browse to find the .VMX file of the Server 1 virtual machine.** The VMX file is the configuration file.



- In VMWARE, select Edit Virtual machine settings and make sure that the **Network Adapter** is **VMnet1** (see screenshot below).



Server1

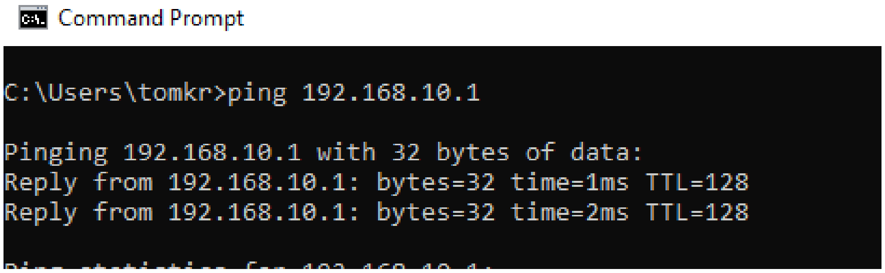
Devices

Memory	2.9 GB
Processors	2
Hard Disk (IDE)	60 GB
CD/DVD (SATA)	Using file C:\Use...
Floppy	Auto detect
Network Adapter	Custom (VMnet1)

- **Power on the Virtual machine until it's FULLY booted** (select "I moved it" if asked).

  Note: Server1 is the machine we are about to pen test so we do not get username and password to log in to it!

- From your main Windows desktop, run a command prompt (**cmd**) you should be able to successfully **ping 192.168.10.1**



```
C:\Users\tomkr>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=128
Reply from 192.168.10.1: bytes=32 time=2ms TTL=128
```

If you do **not** receive a ping response then something is wrong. It may be a Firewall issue? But this must be investigated before continuing.

1.6 UNDER VMWARE WORKSTATION, INSTALL SERVER2

- Download the virtual machine named **Server2 and unzip to a folder e.g. C:\VMs\Server2**

- **Power on the Virtual machine until it's FULLY booted** (select "I moved it" if asked).

- As before, try to ping the machine (**192.168.10.2** in this case). If you do **not** receive a ping response then something is wrong.

1.7 Under VMWARE workstation, install Client1

- Download the virtual machine named **Client1 and unzip to a folder e.g. C:\VMs\Client1**

- **Power on the Virtual machine until it's FULLY booted** (select "I moved it" if asked).

- As before, try to ping the machine (**192.168.10.10** in this case). If you do **not** receive a ping response then something is wrong.

1.8 Under VMWARE workstation, install Kali Linux

- Download the virtual machine named **Client1 and unzip to a folder e.g. C:\VMs\Client1**

- **Power on the Virtual machine until it's FULLY booted** (select "I moved it" if asked).

- As before, from Windows, try to ping the machine (**192.168.10.25**). If you do **not** receive a ping response then again, something is wrong.

- Log in to Kali linux (username and password are kali/kali).

- Run a terminal.

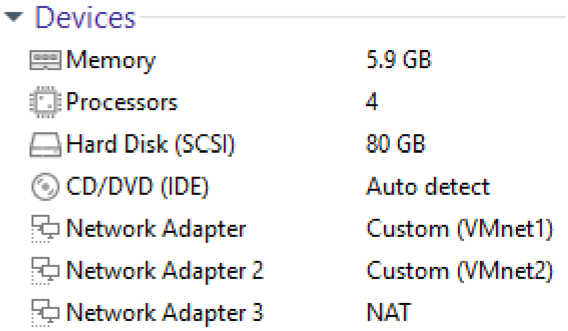
- You should be able to ping the Windows machine i.e. ping 192.168.10.254 and also ping any other machine **THAT IS ON** i.e. 192.168.10.1, 192.168.10.2 and 192.168.10.10.

If any of the pings fail then make sure that the machines are actually on!

2 KALI LINUX TECHNICAL DETAILS

If you examine the Kali Linux virtual machine settings then you should see that there are three network adapters.

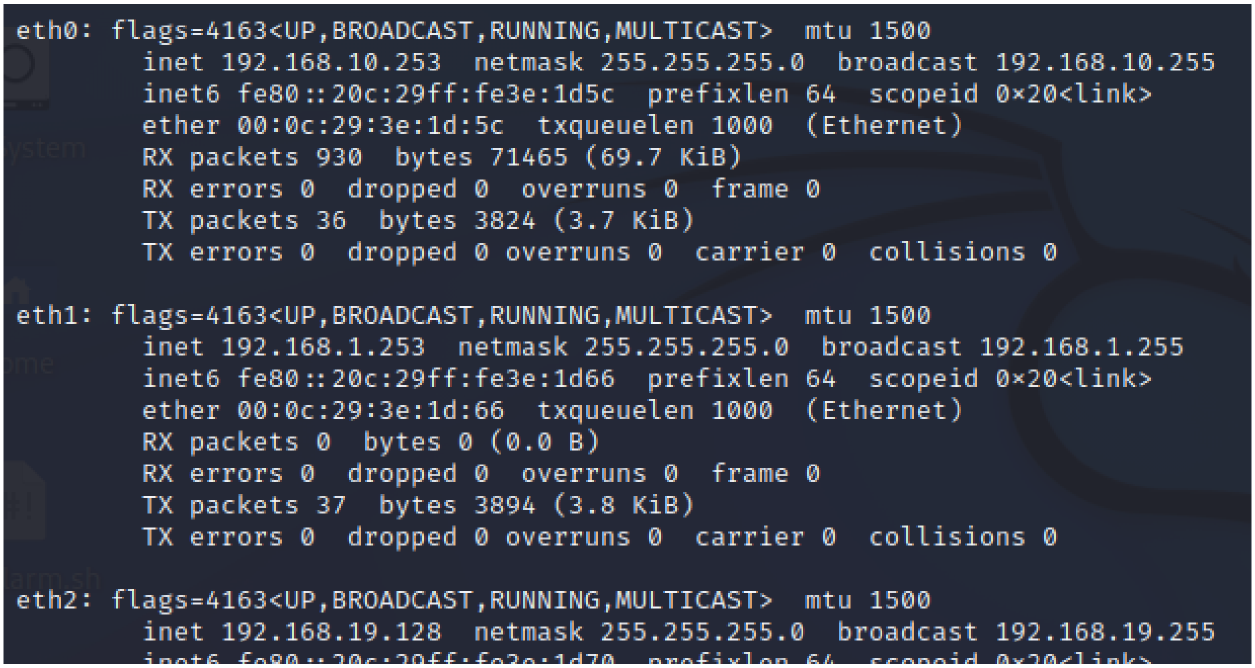
The first (VMnet1) is used for infrastructure pen testing (192.168.10.x network), the second (VMnet2) is used for web app pen testing classes (192.168.1.x network) and the third (nat) is used to give internet access to the Kali linux machines.



Devices

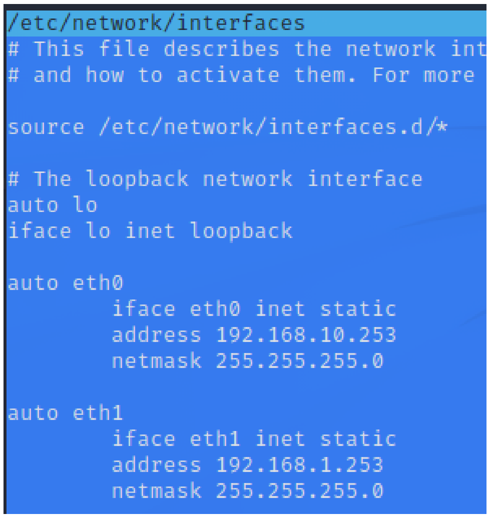
Memory	5.9 GB
Processors	4
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Custom (VMnet1)
Network Adapter 2	Custom (VMnet2)
Network Adapter 3	NAT

If you issue the **ifconfig** command from Kali, you will see the IP addresses. Eth2 is a DHCP given address i.e. it s not fixed.



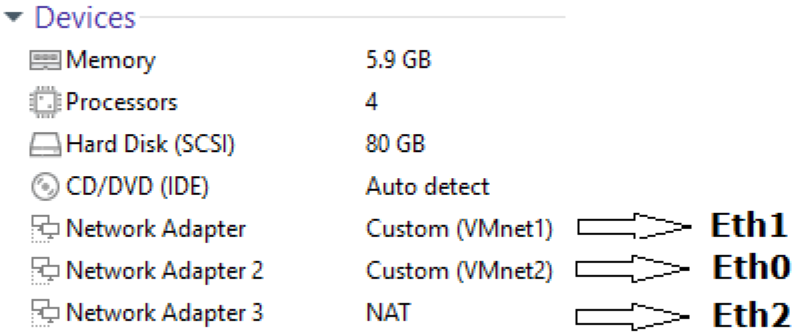
```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.253  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::20c:29ff:fe3e:1d5c  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3e:1d:5c  txqueuelen 1000  (Ethernet)
        RX packets 930  bytes 71465 (69.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 36  bytes 3824 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.253  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe3e:1d66  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3e:1d:66  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3894 (3.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.19.128  netmask 255.255.255.0  broadcast 192.168.19.255
        inet6 fe80::20c:29ff:fe3e:1d70  prefixlen 64  scopeid 0x20<link>
```

These are specified in the following file: -



```
/etc/network/interfaces
# This file describes the network int
# and how to activate them. For more

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
        iface eth0 inet static
        address 192.168.10.253
        netmask 255.255.255.0

auto eth1
        iface eth1 inet static
        address 192.168.1.253
        netmask 255.255.255.0
```

Note: - One strange Kali issue to be aware of is that the eth ports are swapped around. You would think that eth0 would be the first card but often it isn't. The diagram below shows what can often happen.



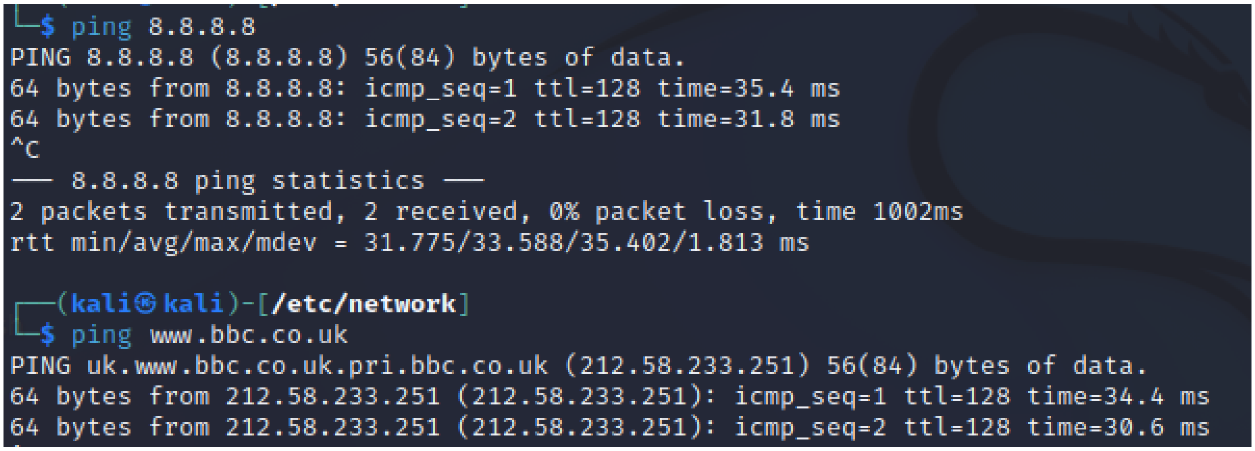
Devices

Memory	5.9 GB	
Processors	4	
Hard Disk (SCSI)	80 GB	
CD/DVD (IDE)	Auto detect	
Network Adapter	Custom (VMnet1)	⇨ Eth1
Network Adapter 2	Custom (VMnet2)	⇨ Eth0
Network Adapter 3	NAT	⇨ Eth2

2.1 Internet connection issues

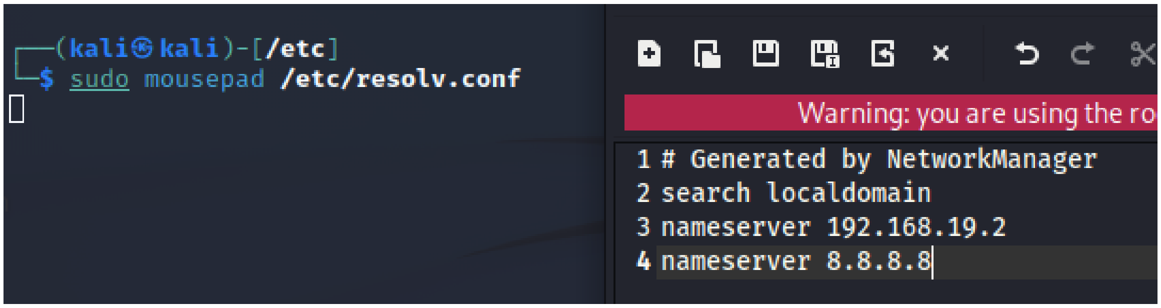
The following should show that your Internet connection is working okay.

Firstly can I see the outside world? 8.8.8.8 is a Google DNS server. Secondly is the DNS working? i.e. can it resolve the name (www.bbc.co.uk) to it's IP?



```
└─$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=35.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=31.8 ms
^C
── 8.8.8.8 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 31.775/33.588/35.402/1.813 ms

┌──(kali㉿kali)-[/etc/network]
└─$ ping www.bbc.co.uk
PING uk.www.bbc.co.uk.pri.bbc.co.uk (212.58.233.251) 56(84) bytes of data.
64 bytes from 212.58.233.251 (212.58.233.251): icmp_seq=1 ttl=128 time=34.4 ms
64 bytes from 212.58.233.251 (212.58.233.251): icmp_seq=2 ttl=128 time=30.6 ms
```

If you have any DNS issues then the file **/etc/resolve.conf** can be edited to include a DNS server see below: -



```
┌──(kali㉿kali)-[/etc]
└─$ sudo mousepad /etc/resolv.conf
```

Warning: you are using the ro

```
# Generated by NetworkManager
search localdomain
nameserver 192.168.19.2
nameserver 8.8.8.8
```

2.2 Updating Kali

From time to time, updating Kali sounds like a good idea. Be aware that an update or upgrade etc can break things.