


David Murillo Santiago  
24 Nov 2024  
IS4543  
Professor Mireles

### Setting Up Lab Environment

I began by configuring the virtual network settings in VMware Workstation Pro to establish an isolated and controlled environment for the virtual machines. I created a custom network (VMnet10) with the subnet 172.16.100.0/24 and disabled DHCP to enforce static IP assignments. For the MS2 virtual machine, I set up two network adapters: the first connected to a "Host-Only" network with the IP address 192.168.189.128/24, and the second assigned to the custom VMnet10 network with the IP address 172.16.100.50/24. I verified that the MAC addresses for the interfaces matched the settings in VMware Workstation Pro and updated the MS2 network configuration files accordingly. On the Kali virtual machine, I ensured its network interface was properly configured with the IP address 192.168.189.129/24 within the same subnet as MS2's first network adapter. For the Windows XP virtual machine, I assigned a static IP address of 172.16.100.100/24, aligning it with the VMnet10 subnet and MS2's second network adapter.



```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ip a | grep 192  
    inet 192.168.189.129/24 brd 192.168.189.255  
eth0  
  
(kali@kali)-[~]  
$
```

**Kali IP 192.168.189.129**

```
msfadmin@metasploitable:~$ ip a | grep -E "192:172"  
    inet 192.168.189.128/24 brd 192.168.189.255 scope global eth0  
    inet 172.16.100.50/24 brd 172.16.100.255 scope global eth1  
msfadmin@metasploitable:~$
```

**MS2 IP 192.168.189.128 & 172.16.100.50**

```
C:\ Command Prompt

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 4:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.100.100
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 172.16.100.1

C:\Documents and Settings\Administrator>
```

XP IP 172.16.100.100

Next, to prove connectivity between the devices, I pinged them from each machine.

```
nlp212-MurilloSantiago_Kali

Power on this virtual machine
Edit virtual machine settings

Devices
Memory 7.8 GB
Processors 4
Hard Disk (SCSI) 80.1 GB
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect

Description
Kali Rolling (2024.3) x64
2024-08-18

Username: kali
Password: kali
(US keyboard layout)

* Kali Homepage:
https://www.kali.org/

* Kali Documentation:
https://www.kali.org/docs/

* Kali Tools:
https://www.kali.org/tools/

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ ping -c4 192.168.189.128
PING 192.168.189.128 (192.168.189.128) 56(84) bytes of data.
64 bytes from 192.168.189.128: icmp_seq=1 ttl=64 time=4.60 ms
64 bytes from 192.168.189.128: icmp_seq=2 ttl=64 time=0.653 ms
64 bytes from 192.168.189.128: icmp_seq=3 ttl=64 time=0.367 ms
64 bytes from 192.168.189.128: icmp_seq=4 ttl=64 time=0.528 ms

— 192.168.189.128 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3050ms
rtt min/avg/max/mdev = 0.367/1.535/4.595/1.769 ms
```

I successfully pinged the MS2 VM from Kali

```
msfadmin@metasploitable:~$ ping -c4 192.168.189.129
PING 192.168.189.129 (192.168.189.129) 56(84) bytes of data.
64 bytes from 192.168.189.129: icmp_seq=1 ttl=64 time=0.359 ms
64 bytes from 192.168.189.129: icmp_seq=2 ttl=64 time=0.331 ms
64 bytes from 192.168.189.129: icmp_seq=3 ttl=64 time=0.502 ms
64 bytes from 192.168.189.129: icmp_seq=4 ttl=64 time=0.458 ms

--- 192.168.189.129 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.331/0.412/0.502/0.072 ms
msfadmin@metasploitable:~$
```

I successfully pinged the Kali VM from the MS2 device.

```
msfadmin@metasploitable:~$ ping -c4 172.16.100.100
PING 172.16.100.100 (172.16.100.100) 56(84) bytes of data.
64 bytes from 172.16.100.100: icmp_seq=1 ttl=128 time=8.00 ms
64 bytes from 172.16.100.100: icmp_seq=2 ttl=128 time=0.367 ms
64 bytes from 172.16.100.100: icmp_seq=3 ttl=128 time=0.304 ms
64 bytes from 172.16.100.100: icmp_seq=4 ttl=128 time=0.354 ms

--- 172.16.100.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.304/2.257/8.005/3.318 ms
msfadmin@metasploitable:~$ _
```

I was also able to ping the XP box from the same MS2 device.

C:\ Command Prompt

```
C:\Documents and Settings\Administrator>ping -n 4 172.16.100.50
Pinging 172.16.100.50 with 32 bytes of data:
Reply from 172.16.100.50: bytes=32 time<1ms TTL=64
Reply from 172.16.100.50: bytes=32 time<1ms TTL=64
Reply from 172.16.100.50: bytes=32 time<1ms TTL=64
Reply from 172.16.100.50: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.100.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

I was able to ping the MS2 device from the XP box as well.