Table of Contents

How to Set Up Metasploitable 2 1
1. Download Necessary Software 1
2. Install Virtualization Software 1
3. Download Metasploitable 2 1
4. Import Metasploitable 2 into Virtualization Software 2
5. Configure Network Settings 3
6. Start Metasploitable 2 5
7. Login to Metasploitable 2 5
8. Check the IP Address of Metasploitable 2 5
8. Verify Network Connectivity 6

How to Set Up Metasploitable 2

1. Download Necessary Software

Before setting up Metasploitable 2, ensure you have the following software installed on your computer:

- **Virtualization Software**: You can use VirtualBox or VMware Workstation/Player.
  - VirtualBox
  - VMware Workstation Player
- **Metasploitable 2 VM**: Download the Metasploitable 2 virtual machine.
  - Metasploitable 2 Download(https://sourceforge.net/projects/metasploitable/)

2. Install Virtualization Software

For VirtualBox:

1. Download the installer from the VirtualBox website.
2. Run the installer and follow the on-screen instructions to complete the installation.

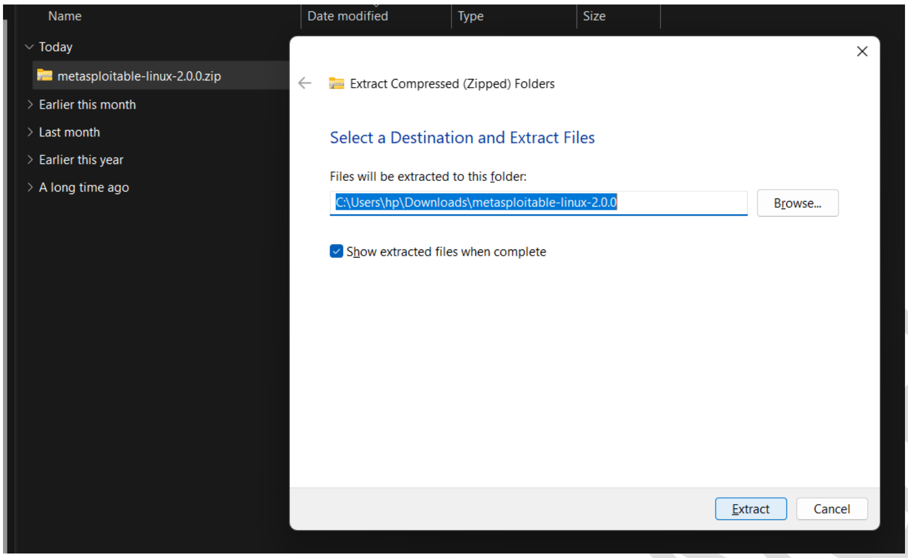
For VMware Workstation Player:

1. Download the installer from the VMware website.
2. Run the installer and follow the on-screen instructions to complete the installation

3. Download Metasploitable 2

1. Visit the Source Forge link provided below. (https://sourceforge.net/projects/metasploitable/files/Metasploitable2/).

2. Click on the `Download` button to get the Metasploitable 2 VM file.
3. Extract the downloaded `.zip` file to a desired location on your computer.



Select a Destination and Extract Files

Files will be extracted to this folder:

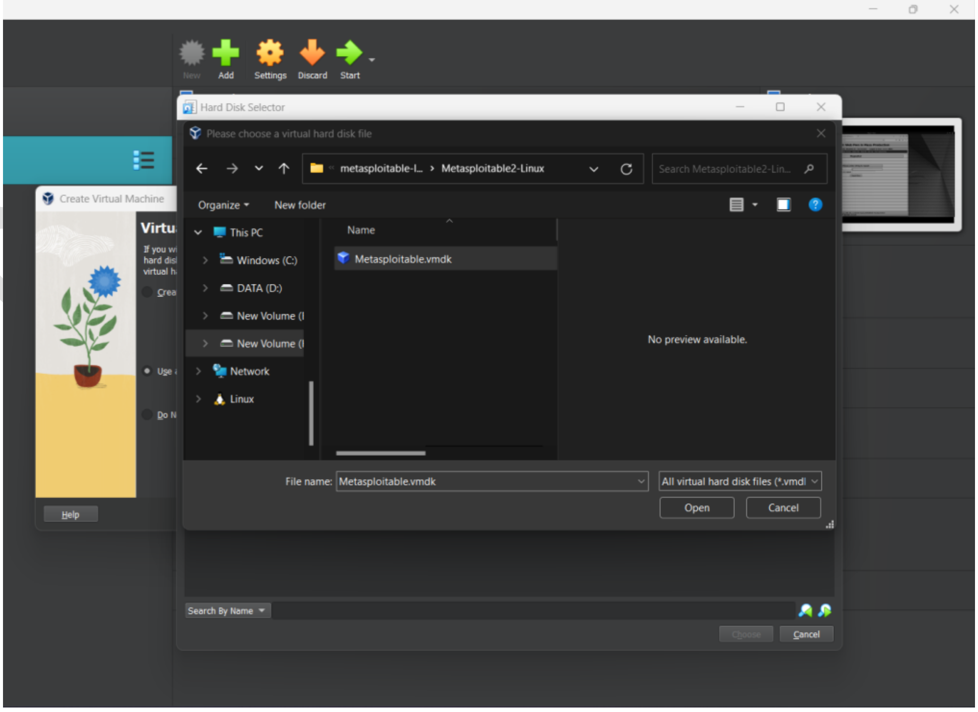
C:\Users\hp\Downloads\metasploitable-linux-2.0.0

☑ Show extracted files when complete

4. Import Metasploitable 2 into Virtualization Software

For VirtualBox:

1. Open VirtualBox.
2. Click on `File` > `Import Appliance`.
3. Click `Choose` and navigate to the folder where you extracted Metasploitable 2.
4. Select the `.vmdk` file and click `Open`.
5. Click `Next`, then click `Import`.



Please choose a virtual hard disk file

metasploitable-l... > Metasploitable2-Linux

Search Metasploitable2-Lin...

Metasploitable.vmdk

No preview available.

File name: Metasploitable.vmdk

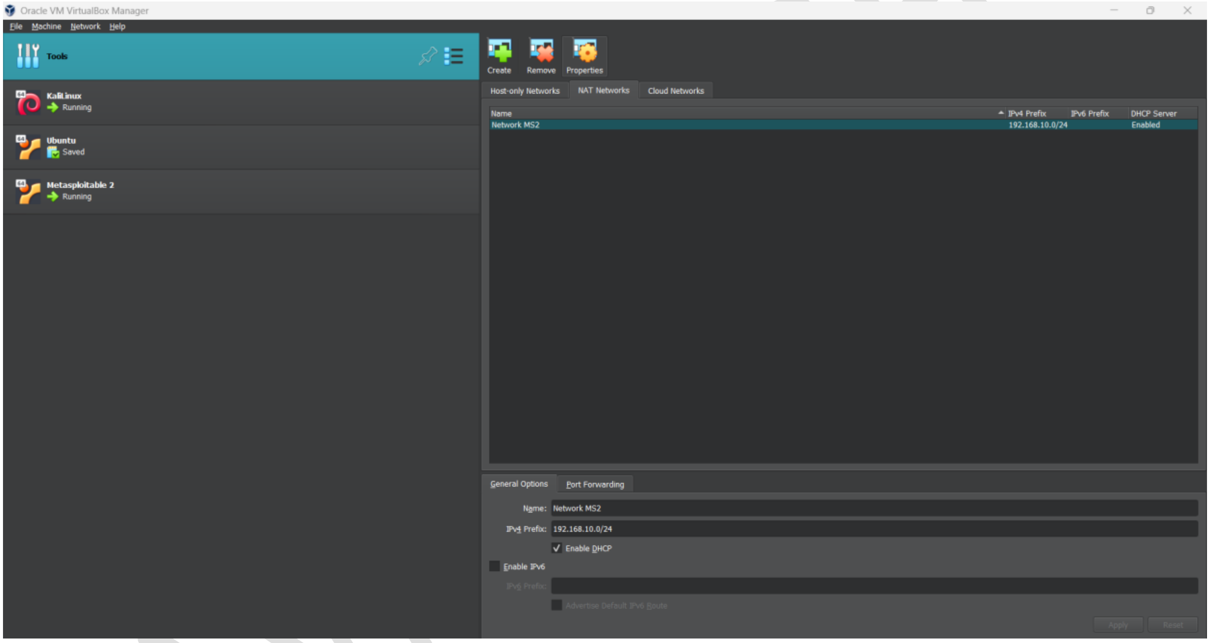
All virtual hard disk files (*.vmdl

5. Configure Network Settings

To interact with Metasploitable 2, you may want to configure its network settings to use Host-only Adapter or NAT. This allows your host machine to communicate with the VM.

For VirtualBox:

1. Select the Metasploitable 2 VM in the VirtualBox Manager.
2. Click on `Settings`.
3. Go to `Network` > `Adapter 1`.
4. Choose `Attached to: Host-only Adapter` or `NAT`.
5. Change the IP address and name needed



Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
Network MS2	192.168.10.0/24		Enabled

Name: Network MS2

IPv4 Prefix: 192.168.10.0/24

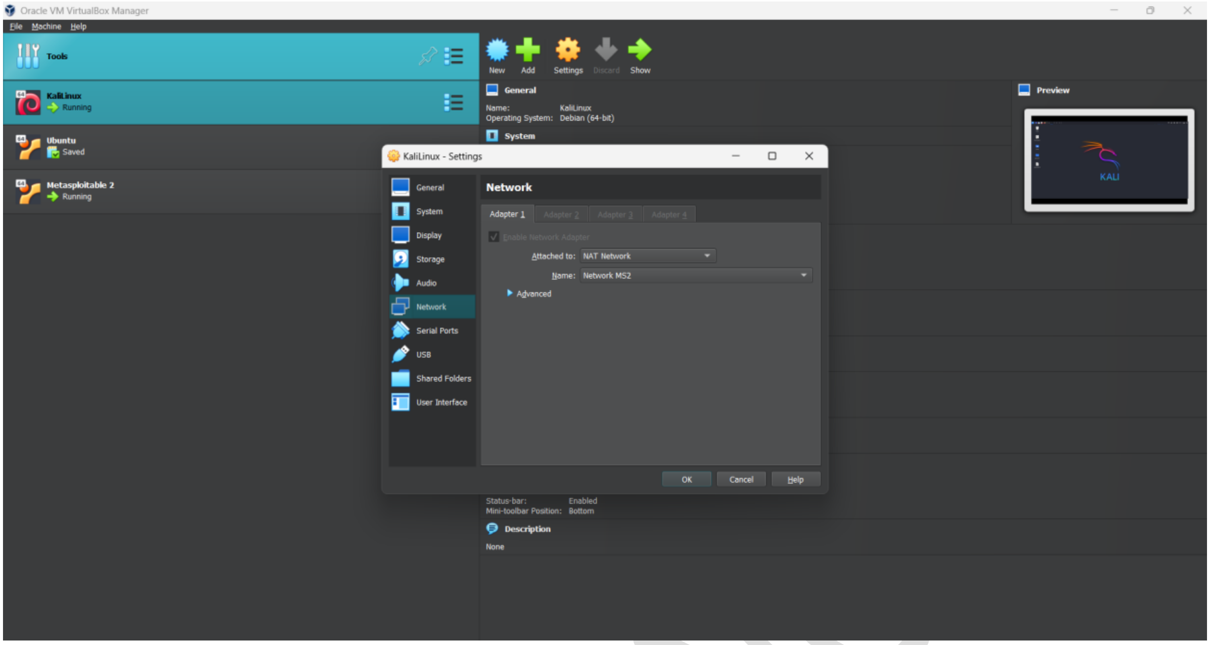
☑ Enable DHCP

□ Enable IPv6

IPv6 Prefix:

□ Advertise Default IPv6 Route

6. Click on `Kali Linux go to Settings and then network` Choose `Attached to: NAT.`



Oracle VM VirtualBox Manager

KaliLinux - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: NAT Network

Name: Network MS2

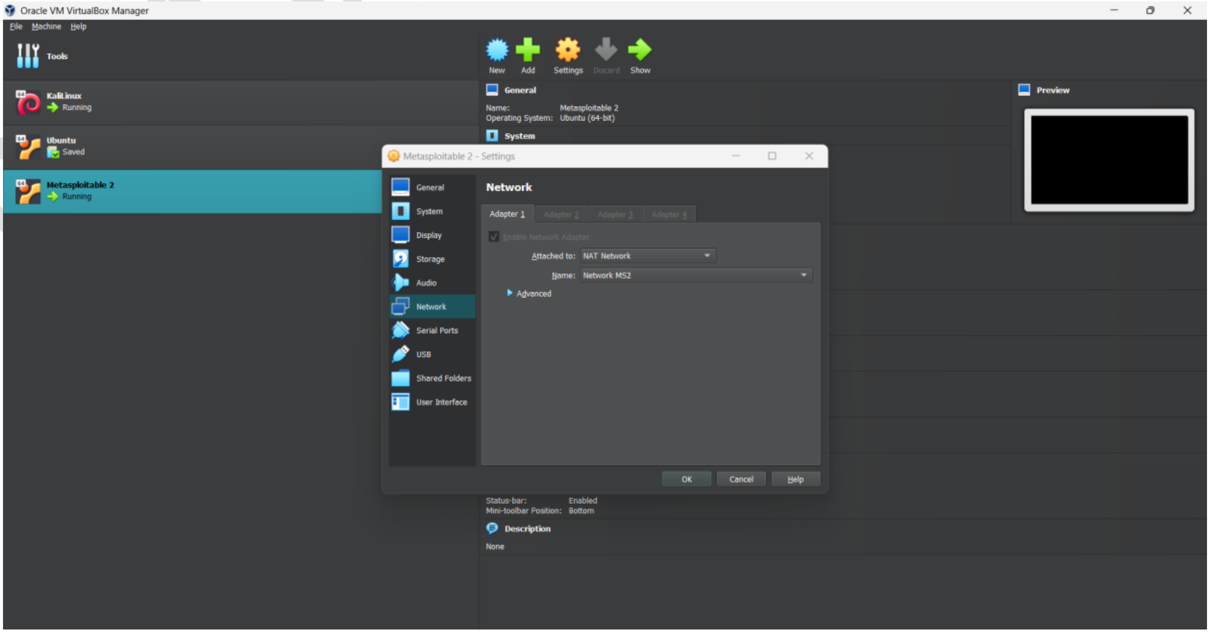
Name: KaliLinux
Operating System: Debian (64-bit)

Status-bar: Enabled
Mini-toolbar Position: Bottom

Description

None

7. Click on `Metasploitable 2 go to Settings and then network` Choose `Attached to: NAT.`



Oracle VM VirtualBox Manager

Metasploitable 2 - Settings

Network

Adapter 1

☑ Enable Network Adapter

Attached to: NAT Network

Name: Network MS2

Name: Metasploitable 2
Operating System: Ubuntu (64-bit)

Status-bar: Enabled
Mini-toolbar Position: Bottom

Description

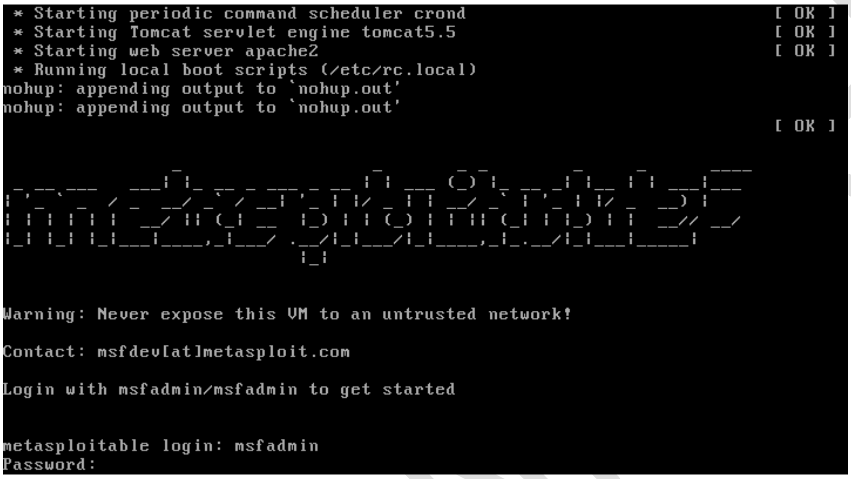
None

6. Start Metasploitable 2

1. Select the Metasploitable 2 VM in your virtualization software.
2. Click on `Start` or `Play virtual machine`.

7. Login to Metasploitable 2

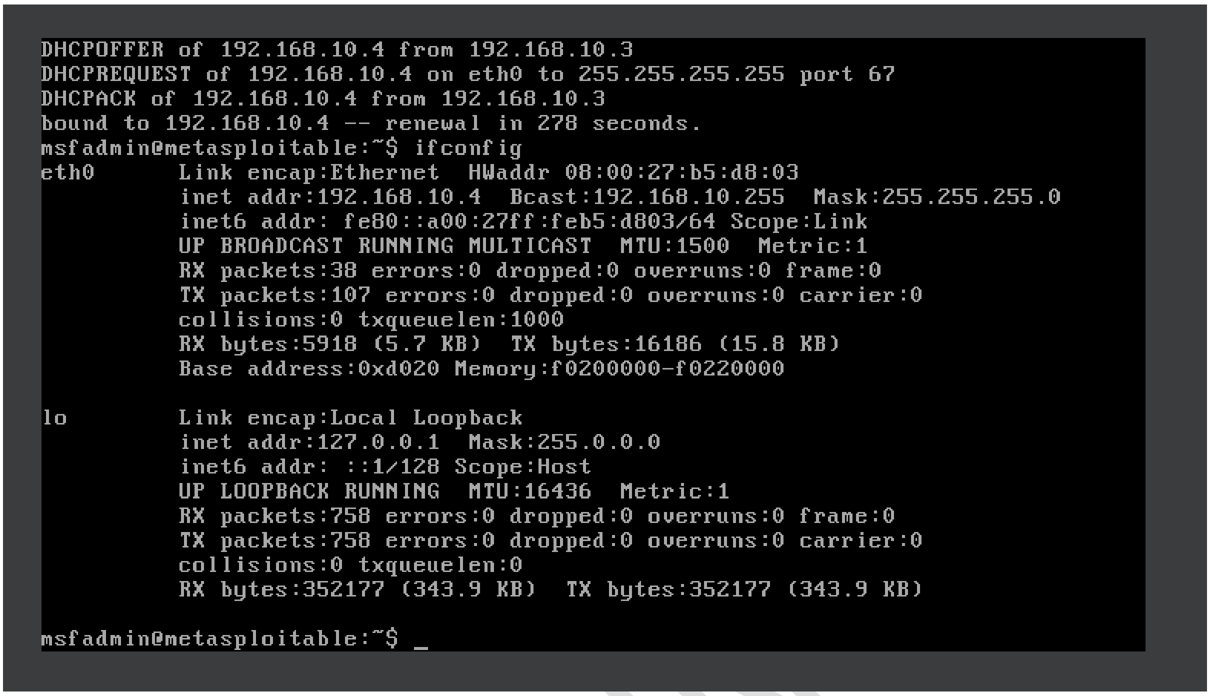
1. Once the VM boots up, you will be prompted to log in.
2. Use the following credentials:
    - **Username**: `msfadmin`
    - **Password**: `msfadmin`



```
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

                _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
```

8. Check the IP Address of Metasploitable 2

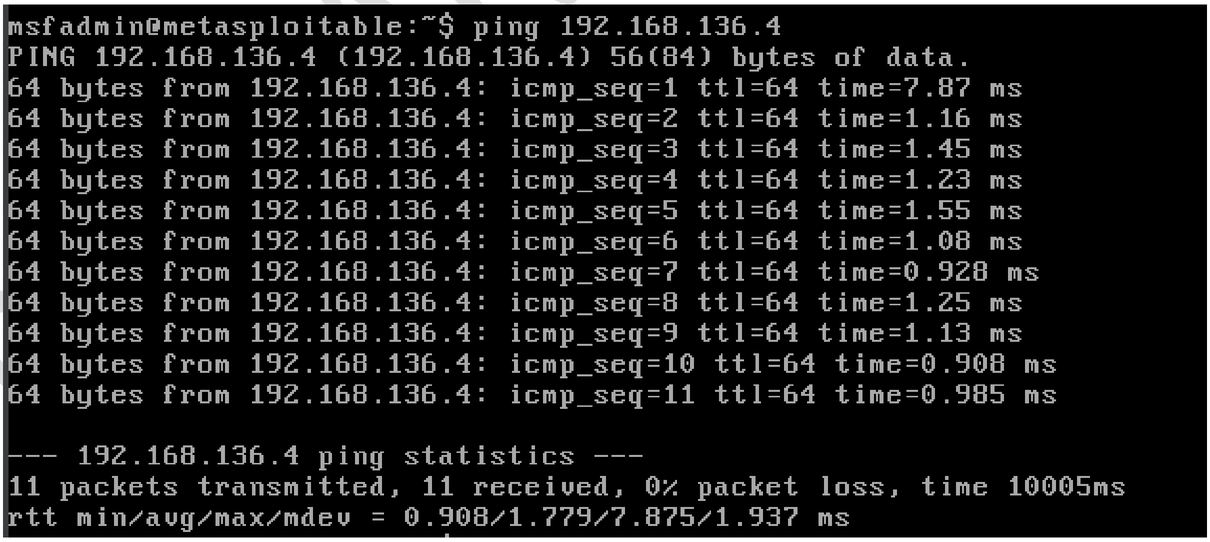
1. Login into Metasploitable 2
2. Use the `dhclient` and then `ifconfig` command on Metasploitable 2 to find its IP address.



```
DHCPOFFER of 192.168.10.4 from 192.168.10.3
DHCPREQUEST of 192.168.10.4 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.10.4 from 192.168.10.3
bound to 192.168.10.4 -- renewal in 278 seconds.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b5:d8:03
          inet addr:192.168.10.4  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb5:d803/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5918 (5.7 KB)  TX bytes:16186 (15.8 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:758 errors:0 dropped:0 overruns:0 frame:0
          TX packets:758 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:352177 (343.9 KB)  TX bytes:352177 (343.9 KB)

msfadmin@metasploitable:~$ _
```

8. Verify Network Connectivity

1. Open a terminal on your host machine.
2. Ping the IP address to ensure connectivity:



```
msfadmin@metasploitable:~$ ping 192.168.136.4
PING 192.168.136.4 (192.168.136.4) 56(84) bytes of data.
64 bytes from 192.168.136.4: icmp_seq=1 ttl=64 time=7.87 ms
64 bytes from 192.168.136.4: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.136.4: icmp_seq=3 ttl=64 time=1.45 ms
64 bytes from 192.168.136.4: icmp_seq=4 ttl=64 time=1.23 ms
64 bytes from 192.168.136.4: icmp_seq=5 ttl=64 time=1.55 ms
64 bytes from 192.168.136.4: icmp_seq=6 ttl=64 time=1.08 ms
64 bytes from 192.168.136.4: icmp_seq=7 ttl=64 time=0.928 ms
64 bytes from 192.168.136.4: icmp_seq=8 ttl=64 time=1.25 ms
64 bytes from 192.168.136.4: icmp_seq=9 ttl=64 time=1.13 ms
64 bytes from 192.168.136.4: icmp_seq=10 ttl=64 time=0.908 ms
64 bytes from 192.168.136.4: icmp_seq=11 ttl=64 time=0.985 ms

--- 192.168.136.4 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10005ms
rtt min/avg/max/mdev = 0.908/1.779/7.875/1.937 ms
```