GANPAT UNIVERSITY
INFORMATION TECHNOLOGY
B. TECH. SEMESTER-VI
2CEIT6PE7: ETHICAL HACKING

PRACTICAL – 1

Aim : Virtual Lab Building using VMWare workstation.

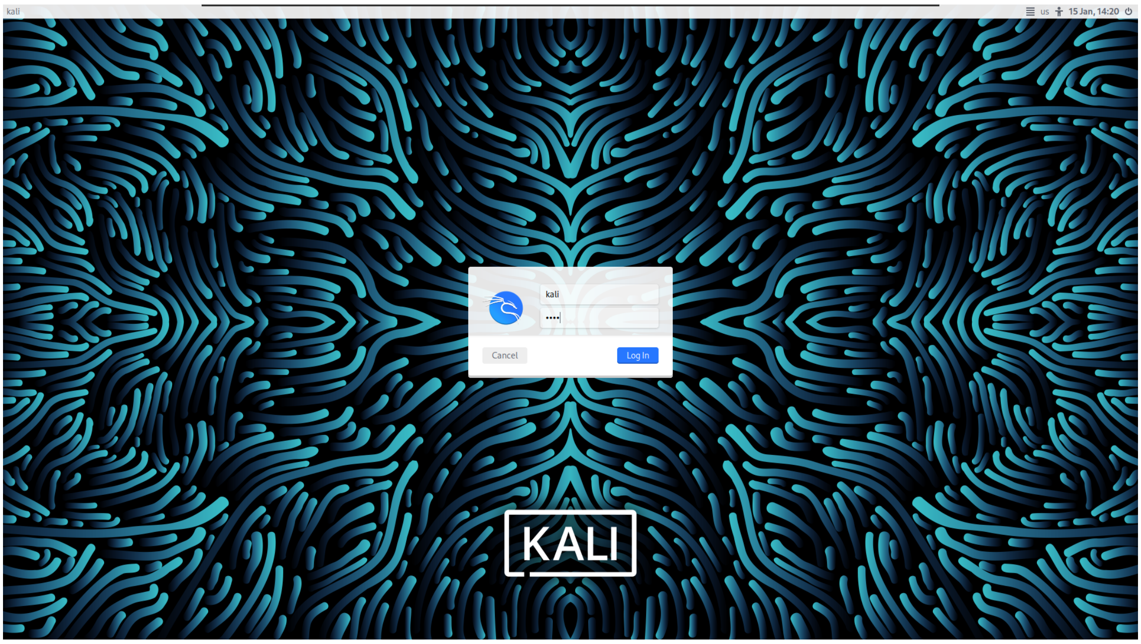
Install VMware

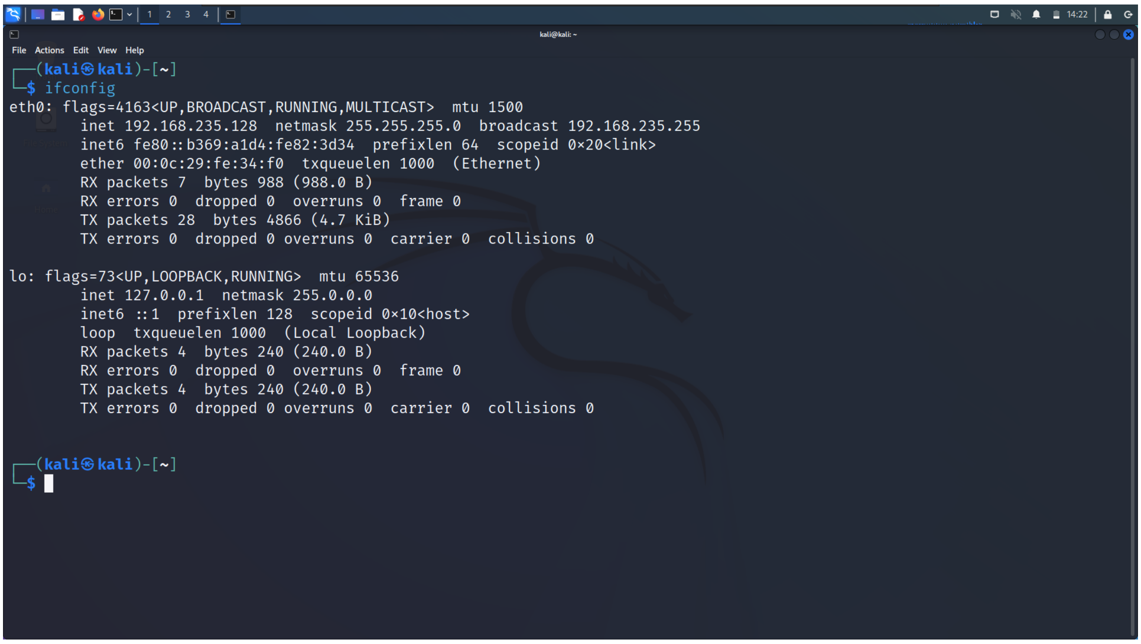
The following OSs are required to install:

1. Kali linux
2. Metasploitable 2
3. Metasploitable 3
4. Windows 10
5. Windows 7

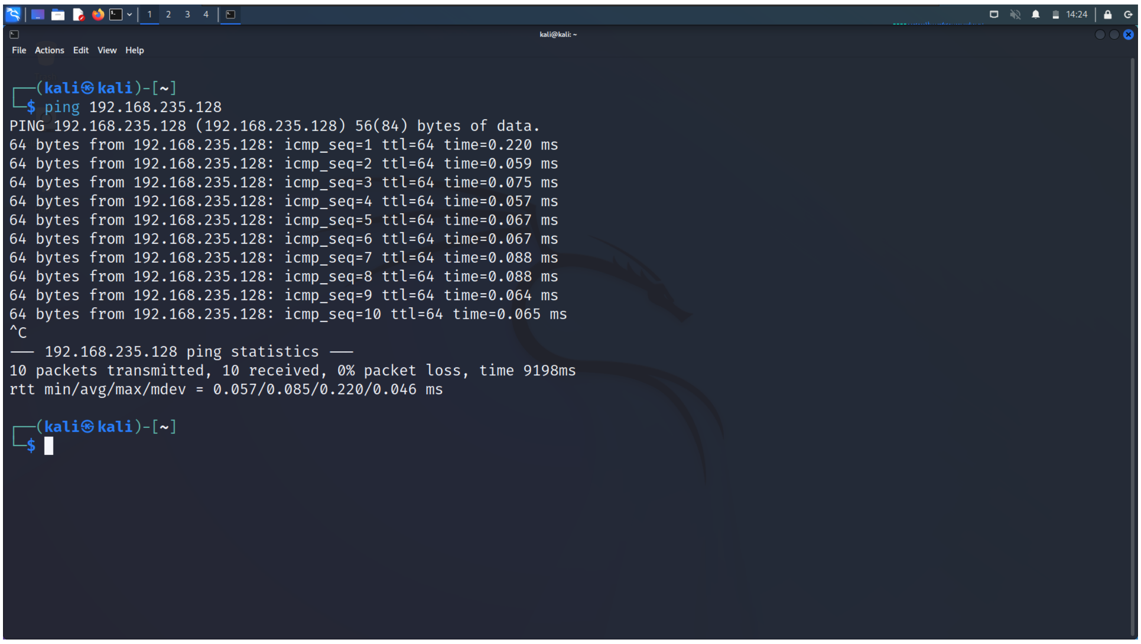
Note: Set the Network adapter to the NAT network and enable the DHCP so, VMware automatically gives IP addresses to each machine. To enable DHCP to go to Virtual Network Editor with administrator privileges.

1. Kali Linux



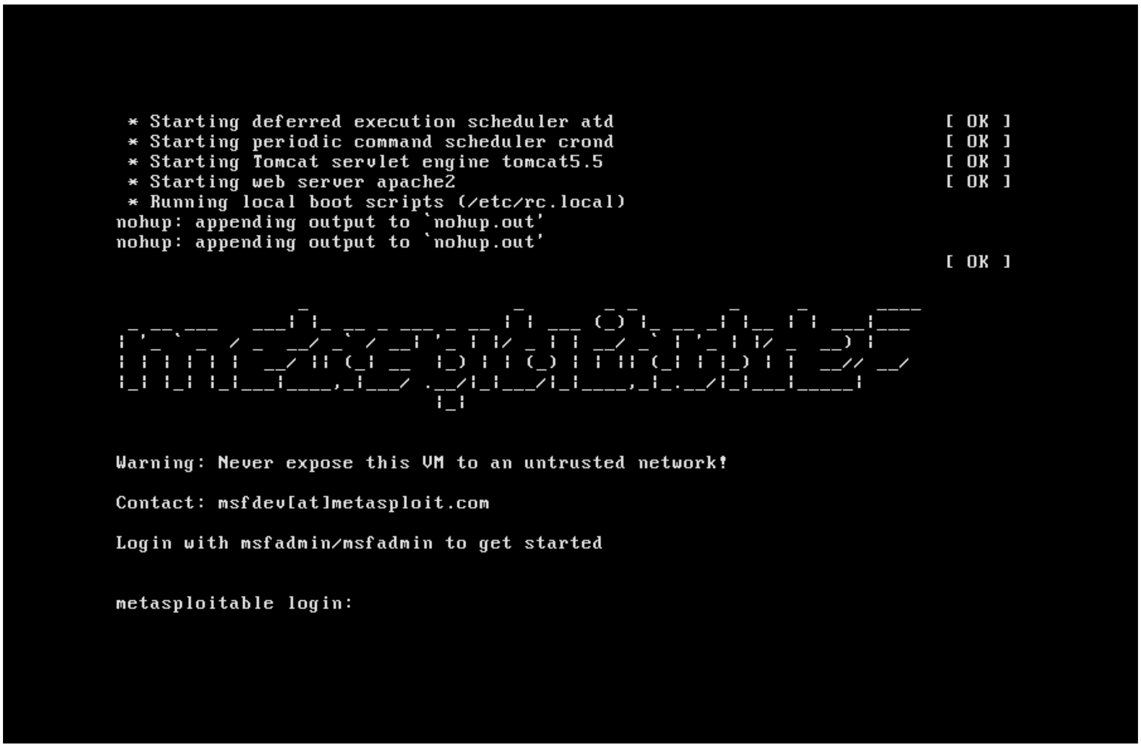


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.235.128  netmask 255.255.255.0  broadcast 192.168.235.255
        inet6 fe80::b369:a1d4:fe82:3d34  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:fe:34:f0  txqueuelen 1000  (Ethernet)
        RX packets 7  bytes 988 (988.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 28  bytes 4866 (4.7 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ ▌
```

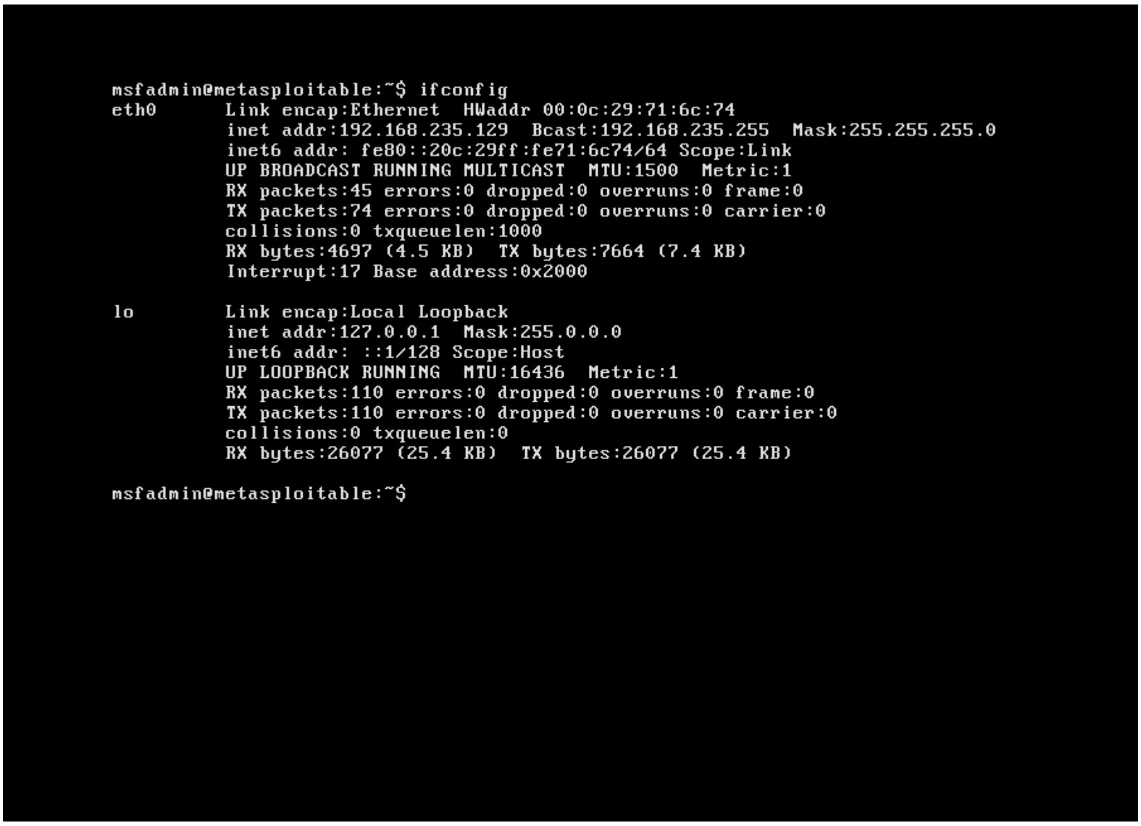


```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.235.128
PING 192.168.235.128 (192.168.235.128) 56(84) bytes of data.
64 bytes from 192.168.235.128: icmp_seq=1 ttl=64 time=0.220 ms
64 bytes from 192.168.235.128: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.235.128: icmp_seq=3 ttl=64 time=0.075 ms
64 bytes from 192.168.235.128: icmp_seq=4 ttl=64 time=0.057 ms
64 bytes from 192.168.235.128: icmp_seq=5 ttl=64 time=0.067 ms
64 bytes from 192.168.235.128: icmp_seq=6 ttl=64 time=0.067 ms
64 bytes from 192.168.235.128: icmp_seq=7 ttl=64 time=0.088 ms
64 bytes from 192.168.235.128: icmp_seq=8 ttl=64 time=0.088 ms
64 bytes from 192.168.235.128: icmp_seq=9 ttl=64 time=0.064 ms
64 bytes from 192.168.235.128: icmp_seq=10 ttl=64 time=0.065 ms
^C
── 192.168.235.128 ping statistics ──
10 packets transmitted, 10 received, 0% packet loss, time 9198ms
rtt min/avg/max/mdev = 0.057/0.085/0.220/0.046 ms

┌──(kali㉿kali)-[~]
└─$ ▌
```

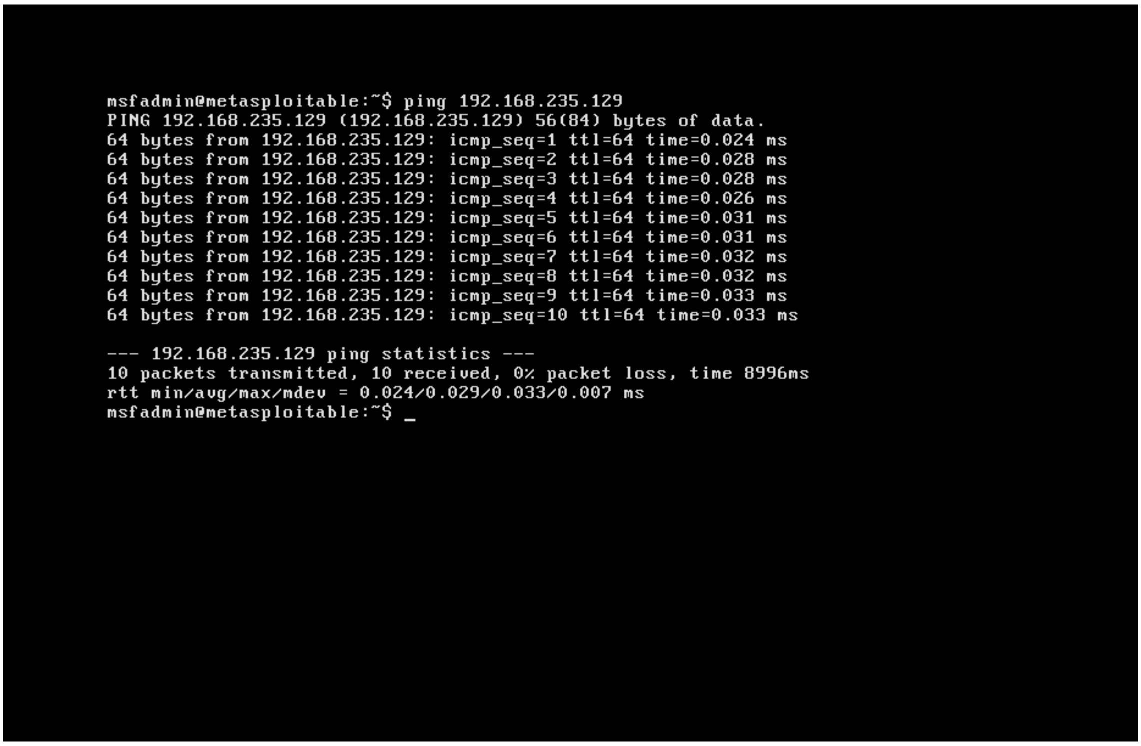
2. Metasploitable 2



```
 * Starting deferred execution scheduler atd                              [ OK ]
 * 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:
```

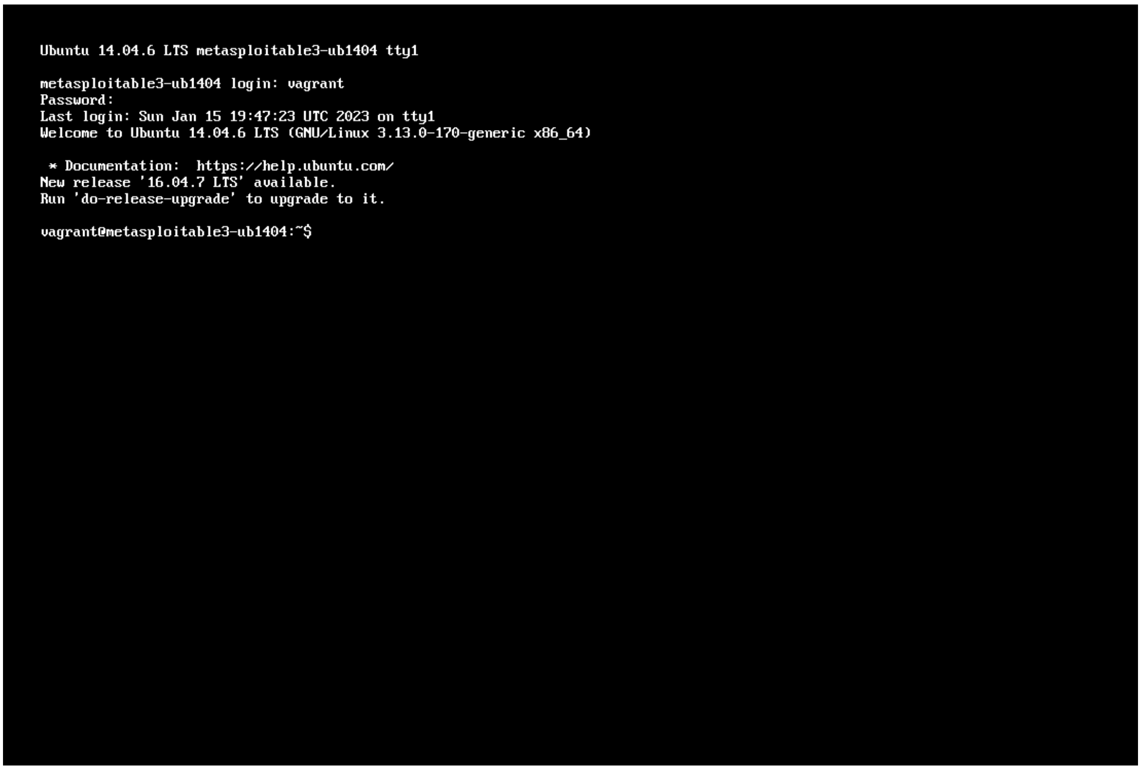


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:71:6c:74
          inet addr:192.168.235.129  Bcast:192.168.235.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe71:6c74/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:45 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4697 (4.5 KB)  TX bytes:7664 (7.4 KB)
          Interrupt:17 Base address:0x2000

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:110 errors:0 dropped:0 overruns:0 frame:0
          TX packets:110 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26077 (25.4 KB)  TX bytes:26077 (25.4 KB)

msfadmin@metasploitable:~$
```

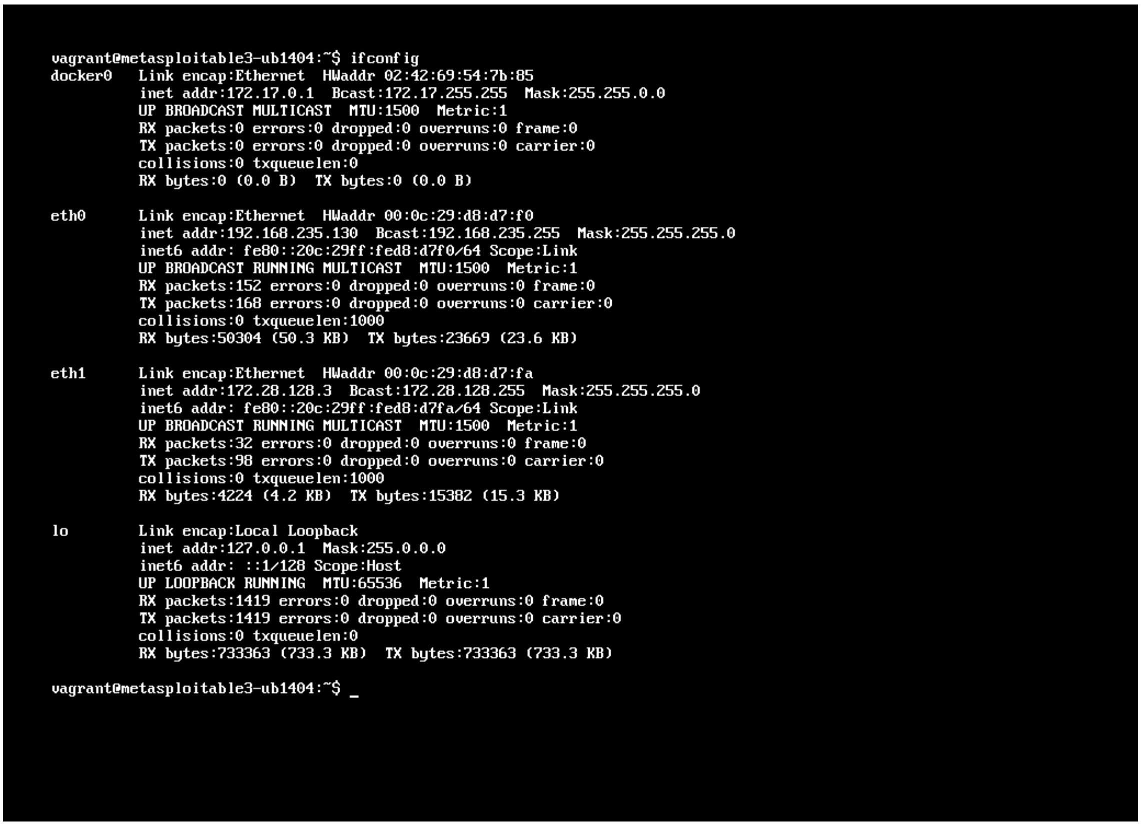


```
msfadmin@metasploitable:~$ ping 192.168.235.129
PING 192.168.235.129 (192.168.235.129) 56(84) bytes of data.
64 bytes from 192.168.235.129: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 192.168.235.129: icmp_seq=2 ttl=64 time=0.028 ms
64 bytes from 192.168.235.129: icmp_seq=3 ttl=64 time=0.028 ms
64 bytes from 192.168.235.129: icmp_seq=4 ttl=64 time=0.026 ms
64 bytes from 192.168.235.129: icmp_seq=5 ttl=64 time=0.031 ms
64 bytes from 192.168.235.129: icmp_seq=6 ttl=64 time=0.031 ms
64 bytes from 192.168.235.129: icmp_seq=7 ttl=64 time=0.032 ms
64 bytes from 192.168.235.129: icmp_seq=8 ttl=64 time=0.032 ms
64 bytes from 192.168.235.129: icmp_seq=9 ttl=64 time=0.033 ms
64 bytes from 192.168.235.129: icmp_seq=10 ttl=64 time=0.033 ms

--- 192.168.235.129 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 8996ms
rtt min/avg/max/mdev = 0.024/0.029/0.033/0.007 ms
msfadmin@metasploitable:~$ _
```

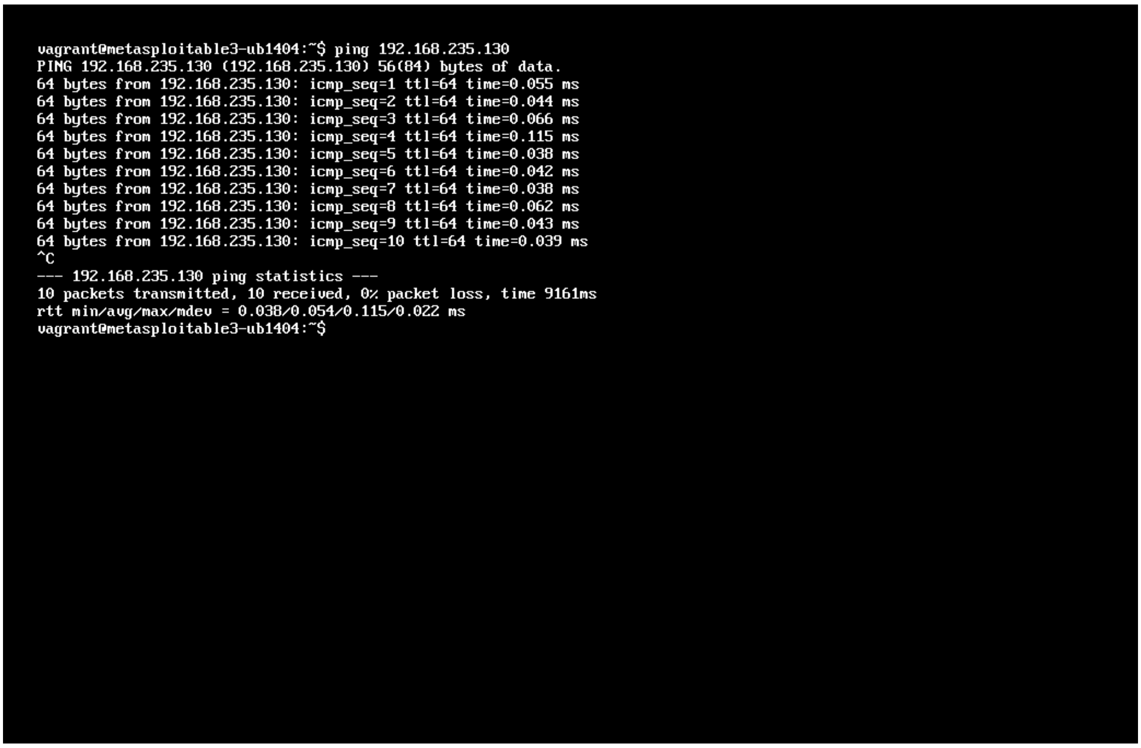
3. Metasploitable 3



```
Ubuntu 14.04.6 LTS metasploitable3-ub1404 tty1

metasploitable3-ub1404 login: vagrant
Password:
Last login: Sun Jan 15 19:47:23 UTC 2023 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 3.13.0-170-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

vagrant@metasploitable3-ub1404:~$
```

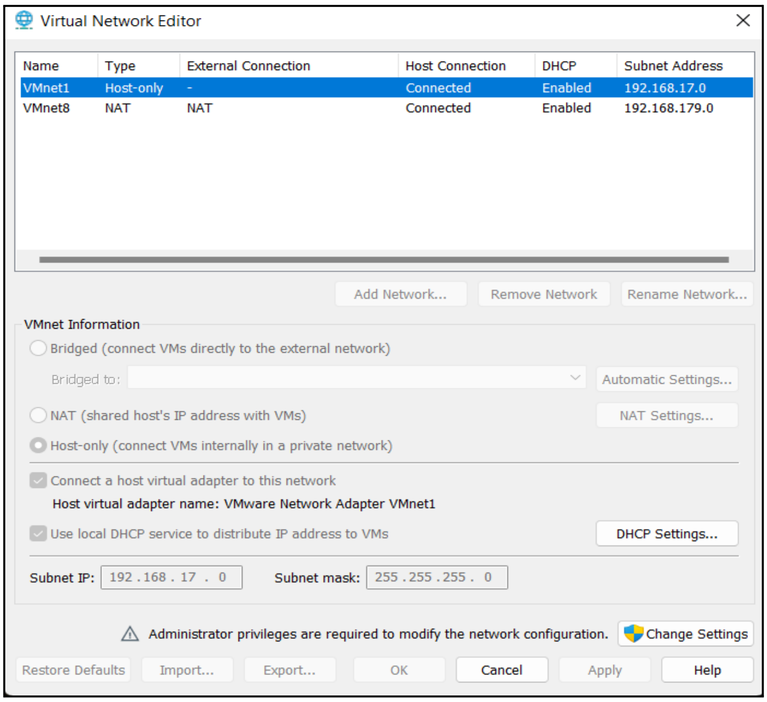


```
vagrant@metasploitable3-ub1404:~$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:69:54:7b:85
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eth0      Link encap:Ethernet  HWaddr 00:0c:29:d8:d7:f0
          inet addr:192.168.235.130  Bcast:192.168.235.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed8:d7f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:168 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50304 (50.3 KB)  TX bytes:23669 (23.6 KB)

eth1      Link encap:Ethernet  HWaddr 00:0c:29:d8:d7:fa
          inet addr:172.28.128.3  Bcast:172.28.128.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed8:d7fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4224 (4.2 KB)  TX bytes:15382 (15.3 KB)

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:65536  Metric:1
          RX packets:1419 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1419 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:733363 (733.3 KB)  TX bytes:733363 (733.3 KB)

vagrant@metasploitable3-ub1404:~$ _
```



```
vagrant@metasploitable3-ub1404:~$ ping 192.168.235.130
PING 192.168.235.130 (192.168.235.130) 56(84) bytes of data.
64 bytes from 192.168.235.130: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from 192.168.235.130: icmp_seq=2 ttl=64 time=0.044 ms
64 bytes from 192.168.235.130: icmp_seq=3 ttl=64 time=0.066 ms
64 bytes from 192.168.235.130: icmp_seq=4 ttl=64 time=0.115 ms
64 bytes from 192.168.235.130: icmp_seq=5 ttl=64 time=0.038 ms
64 bytes from 192.168.235.130: icmp_seq=6 ttl=64 time=0.042 ms
64 bytes from 192.168.235.130: icmp_seq=7 ttl=64 time=0.038 ms
64 bytes from 192.168.235.130: icmp_seq=8 ttl=64 time=0.062 ms
64 bytes from 192.168.235.130: icmp_seq=9 ttl=64 time=0.043 ms
64 bytes from 192.168.235.130: icmp_seq=10 ttl=64 time=0.039 ms
^C
--- 192.168.235.130 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9161ms
rtt min/avg/max/mdev = 0.038/0.054/0.115/0.022 ms
vagrant@metasploitable3-ub1404:~$
```

Virtual Network Editor :



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	192.168.17.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.179.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to:

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

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

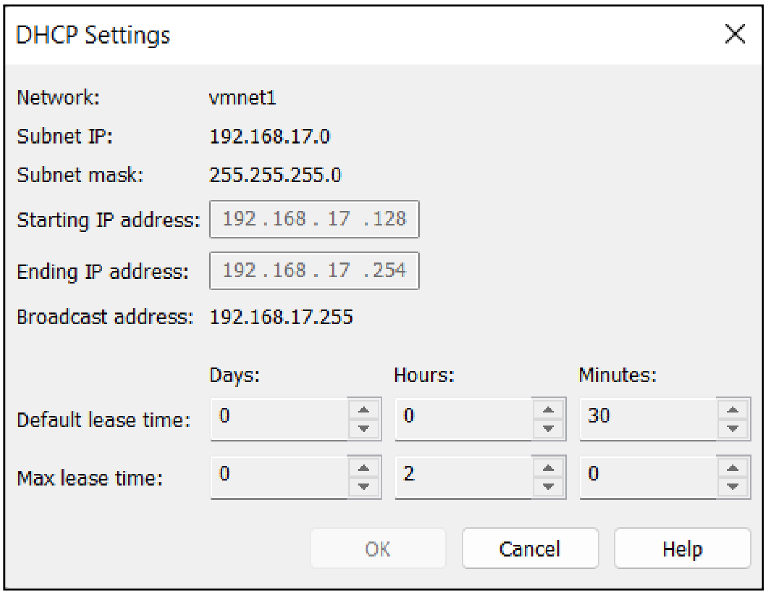
☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet1

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 17 . 0 Subnet mask: 255 . 255 . 255 . 0

⚠ Administrator privileges are required to modify the network configuration.



DHCP Settings

Network: vmnet1

Subnet IP: 192.168.17.0

Subnet mask: 255.255.255.0

Starting IP address: 192 . 168 . 17 . 128

Ending IP address: 192 . 168 . 17 . 254

Broadcast address: 192.168.17.255

	Days:	Hours:	Minutes:
Default lease time:	0	0	30
Max lease time:	0	2	0

Definitions :

1. **Ifconfig/Ipconfig :**
   The utilities known as ipconfig (in Windows), and ifconfig (in Unix/Linux/Mac) will display the current configuration of TCP/IP on a given workstation—including the current IP address, DNS configuration, Windows Internet Naming Service (WINS) configuration, and default gateway.
   - **Syntax (Windows)** : ipconfig
   - **Syntax (Unix/Linux/Mac)** : ifconfig

2. **Ping :**
   A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration.
   - **Syntax** : ping <website/Host-Address>

3. **NAT Connection :**
   NAT stands for network address translation. It's a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.

4. **Bridged Connection :**
   Bridged networking connects a virtual machine to a network by using the network adapter on the host system. If the host system is on a network, bridged networking is often the easiest way to give the virtual machine access to that network.

5. **Host Only Connection :**
   Host-only networking is useful if you need to set up an isolated virtual network. In a host-only network, the virtual machine and the host virtual network adapter are connected to a private Ethernet network. The network is completely contained within the host system.