# 基于 VirtualBox 的网络攻防基础环境搭建

## 实验目的

- 掌握 VirtualBox 虚拟机的安装与使用；
- 掌握 VirtualBox 的虚拟网络类型和按需配置；
- 掌握 VirtualBox 的虚拟硬盘多重加载；

## 实验环境

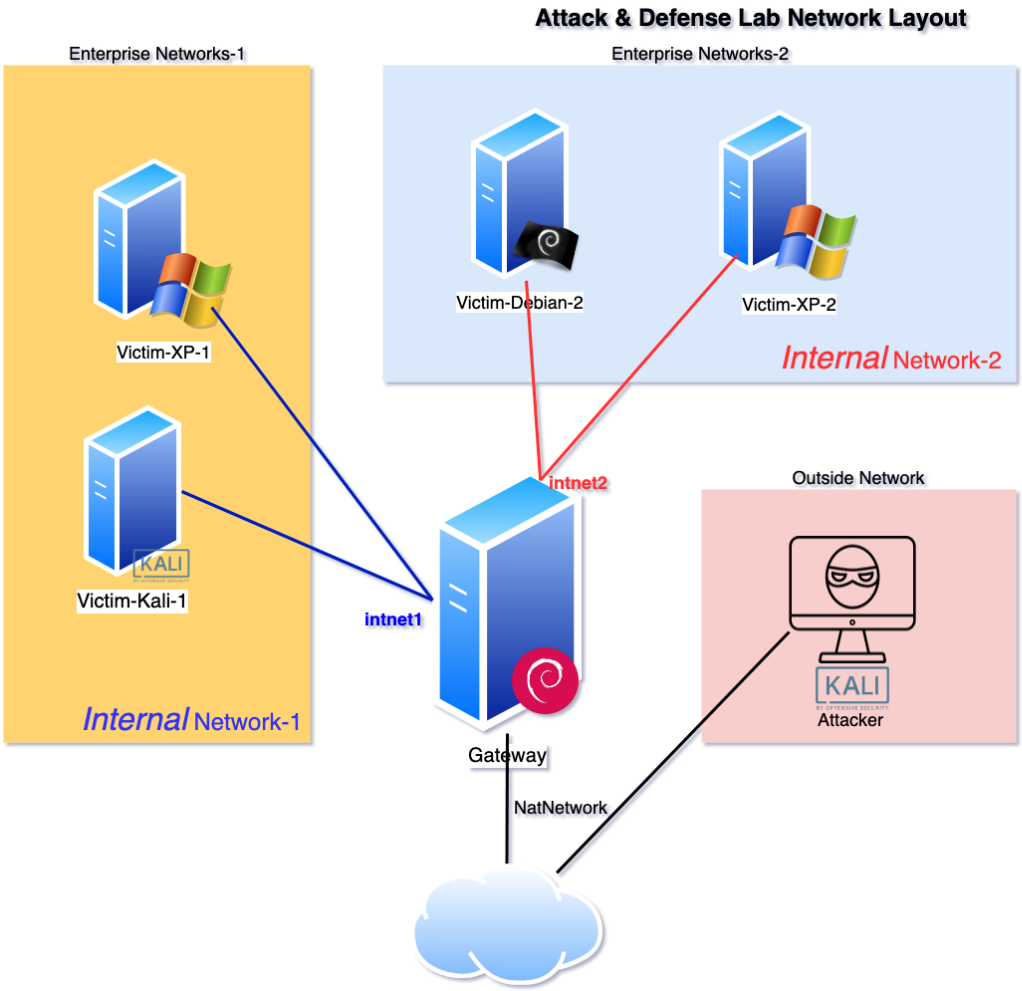
以下是本次实验需要使用的网络节点说明和主要软件举例：

- VirtualBox 虚拟机
- 攻击者主机（Attacker）：Kali Rolling 2019.2
- 网关（Gateway, GW）：Debian Buster
- 靶机（Victim）：win7 / Debian / Kali

## 实验要求

- 虚拟硬盘配置成多重加载，效果如下图所示；


- 搭建满足如下拓扑图所示的虚拟机网络拓扑；



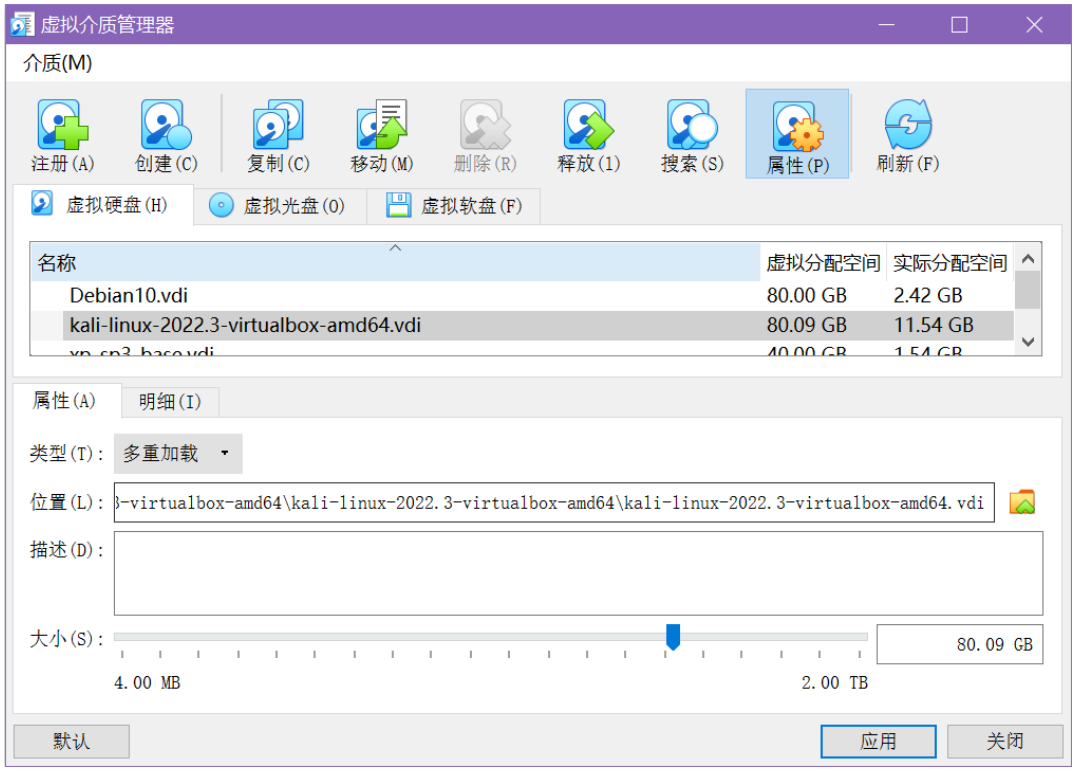

> 根据实验宿主机的性能条件，可以适度精简靶机数量

- 完成以下网络连通性测试；
  - [x] 靶机可以直接访问攻击者主机
  - [x] 攻击者主机无法直接访问靶机
  - [x] 网关可以直接访问攻击者主机和靶机
  - [x] 靶机的所有对外上下行流量必须经过网关
  - [x] 所有节点均可以访问互联网

# 实验过程

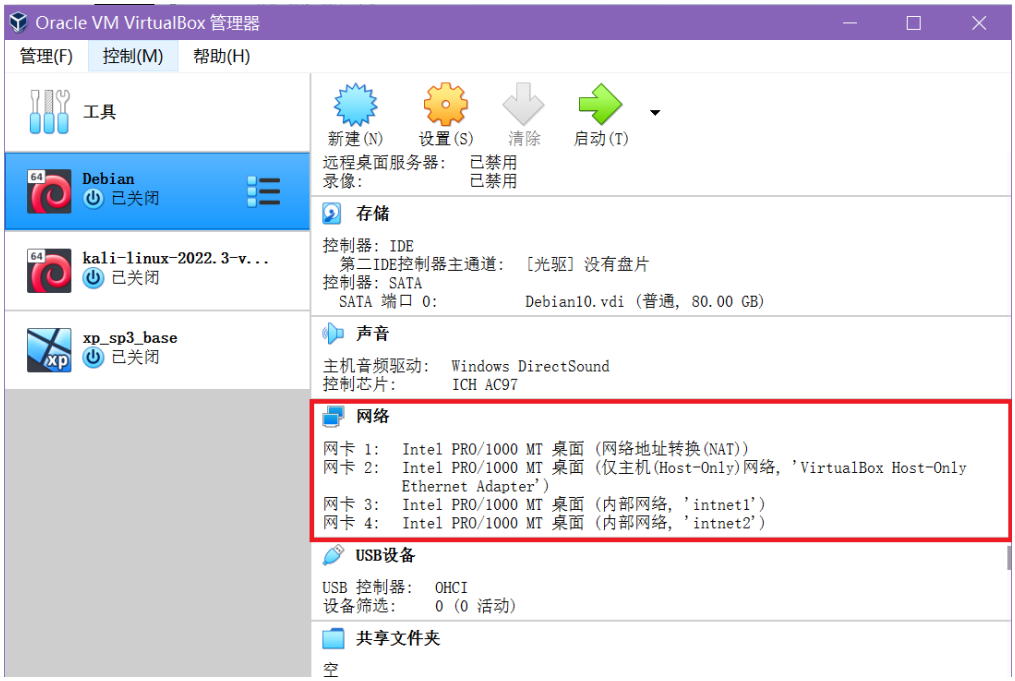
- **将虚拟硬盘配置成多重加载**
  - 在VirtualBox上方的管理中，选择虚拟介质管理


- 选中需要的虚拟盘，在属性处将类型修改为多个加载并应用。

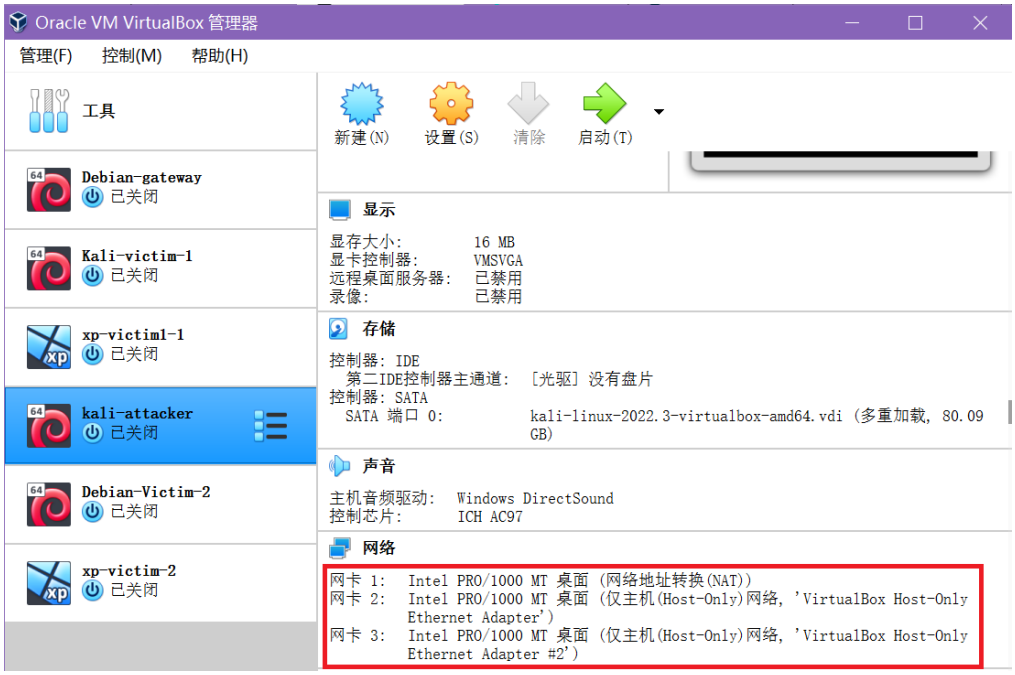



- 结果

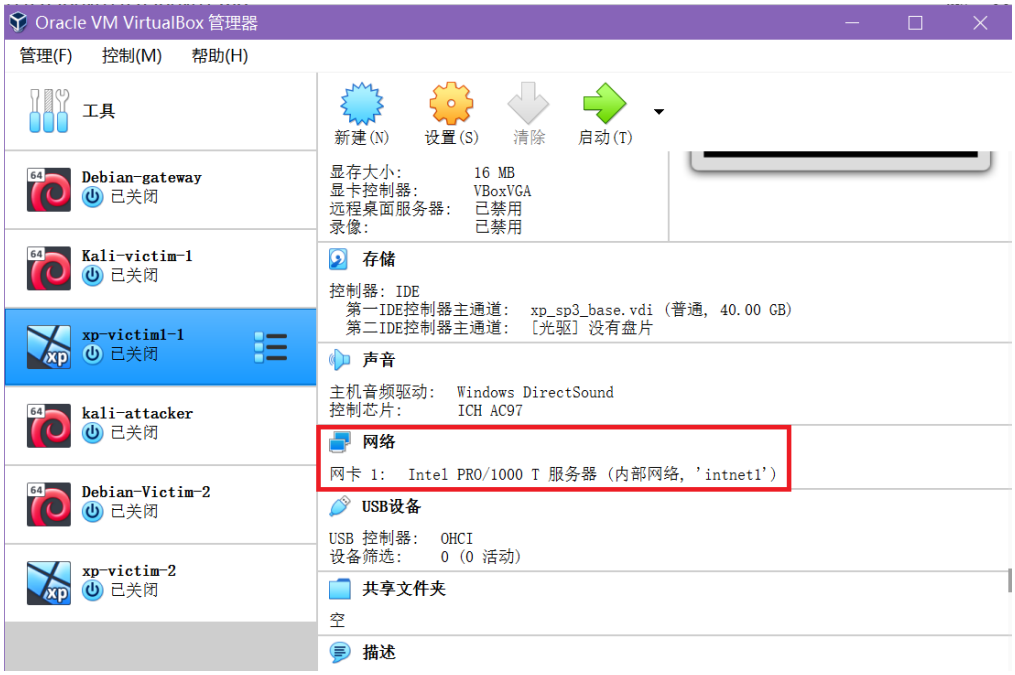

- **搭建虚拟机网络拓扑**
  - 在每台虚拟机的设置中对网卡进行配置
    - 网关网卡配置（4块网卡）如图：

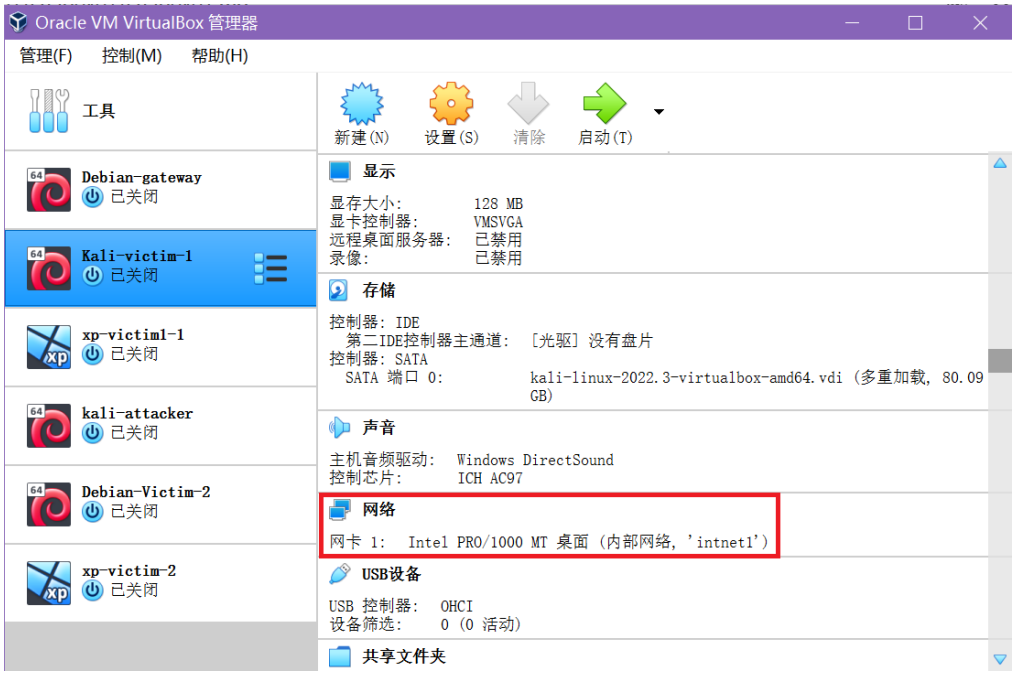



    - 攻击者网卡配置（3块卡）如图




- 受害主机都仅需一张网卡
- 将受害主机分为两组，两个局域网中
  - Victim-XP-1和Victim-Kali-1在Intnet1
  - Victim-XP-2和Victim-Debian-2在Intnet2

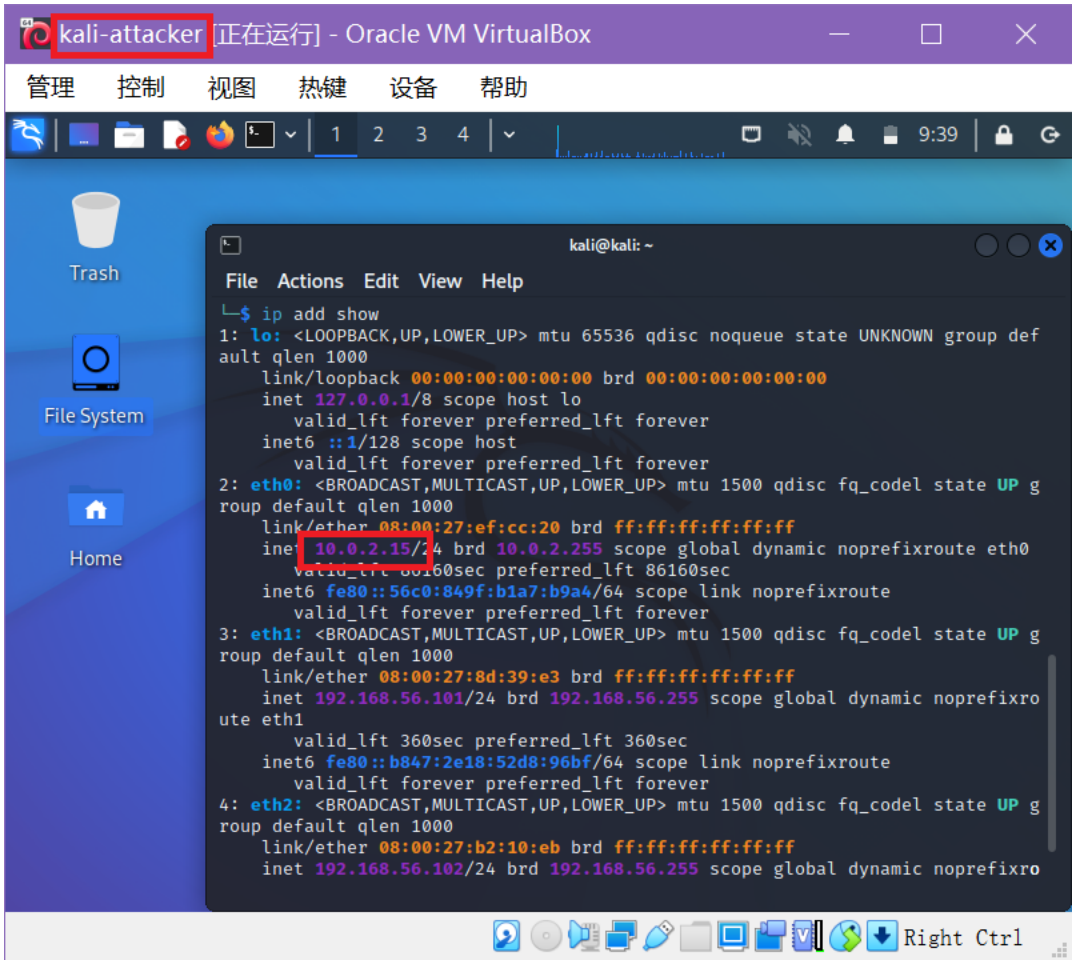


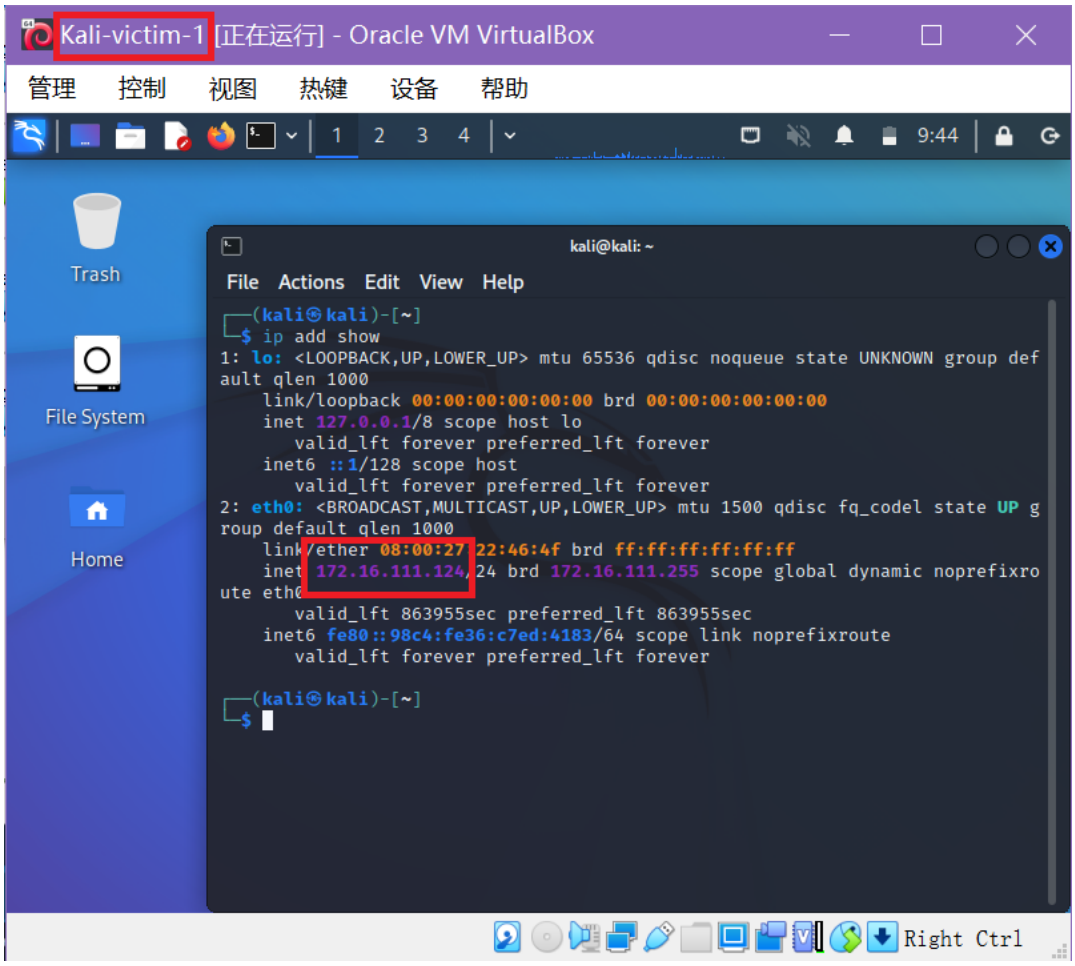

Oracle VM VirtualBox 管理器
管理(F) 控制(M) 帮助(H)
工具
Debian-gateway
已关闭
Kali-victim-1
已关闭
xp-victim1-1
已关闭
kali-attacker
已关闭
Debian-Victim-2
已关闭
xp-victim-2
已关闭
新建(N) 设置(S) 清除 启动(T)
显示
显存大小: 128 MB
显卡控制器: VMSVGA
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第二IDE控制器主通道: [光驱] 没有盘片
控制器: SATA
SATA 端口 0: kali-linux-2022.3-virtualbox-amd64.vdi (多重加载, 80.09 GB)
声音
主机音频驱动: Windows DirectSound
控制芯片: ICH AC97
网络
网卡 1: Intel PRO/1000 MT 桌面 (内部网络, 'intnet1')
USB设备
USB 控制器: OHCI
设备筛选: 0 (0 活动)
共享文件夹

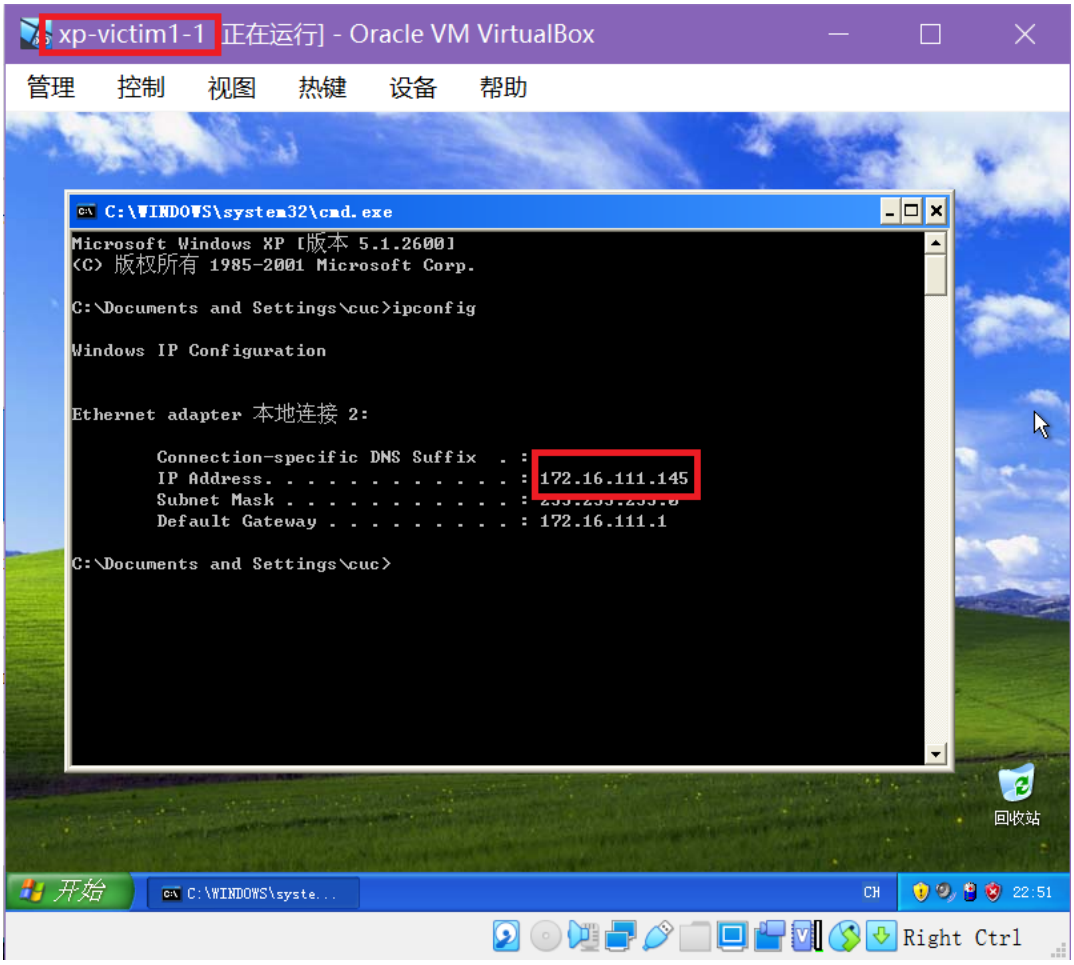

Oracle VM VirtualBox 管理器
管理(F) 控制(M) 帮助(H)
工具
Debian-gateway
已关闭
Kali-victim-1
已关闭
xp-victim1-1
已关闭
kali-attacker
已关闭
Debian-Victim-2
已关闭
xp-victim-2
已关闭
新建(N) 设置(S) 清除 启动(T)
显卡控制器: VBoxVGA
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第一IDE控制器主通道: xp_sp3_base.vdi (普通, 40.00 GB)
第二IDE控制器主通道: [光驱] 没有盘片
声音
主机音频驱动: Windows DirectSound
控制芯片: ICH AC97
网络
网卡 1: Intel PRO/1000 T 服务器 (内部网络, 'intnet2')
USB设备
USB 控制器: OHCI
设备筛选: 0 (0 活动)
共享文件夹
空
描述
空

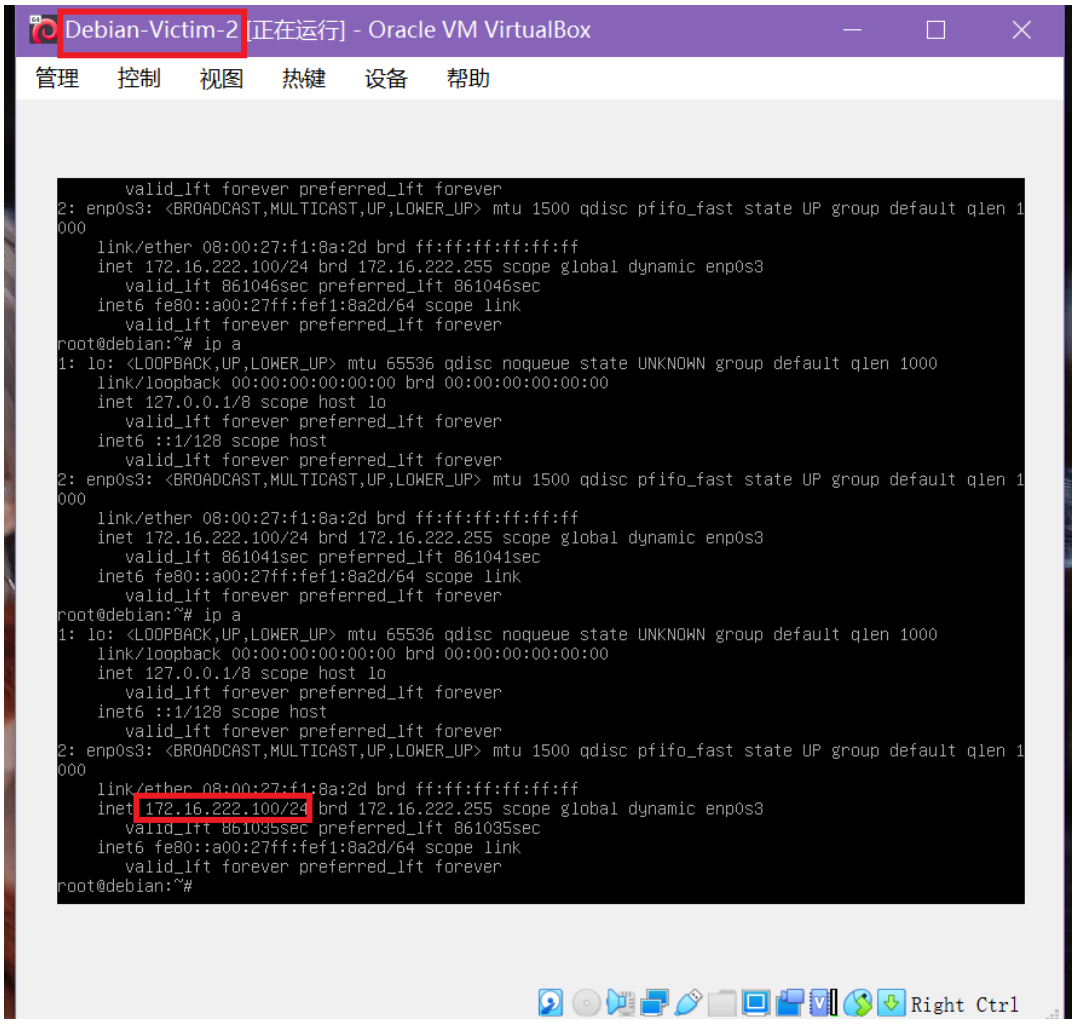

Oracle VM VirtualBox 管理器
管理(F) 控制(M) 帮助(H)
工具
Debian-gateway
已关闭
Kali-victim-1
已关闭
xp-victim1-1
已关闭
kali-attacker
已关闭
Debian-Victim-2
已关闭
xp-victim-2
已关闭
新建(N) 设置(S) 清除 启动(T)
显示
显存大小: 16 MB
显卡控制器: VMSVGA
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: IDE
第二IDE控制器主通道: [光驱] 没有盘片
控制器: SATA
SATA 端口 0: Debian10.vdi (普通, 80.00 GB)
声音
主机音频驱动: Windows DirectSound
控制芯片: ICH AC97
网络
网卡 1: Intel PRO/1000 MT 桌面 (内部网络, 'intnet2')
USB设备
USB 控制器: OHCI
设备筛选: 0 (0 活动)
共享文件夹

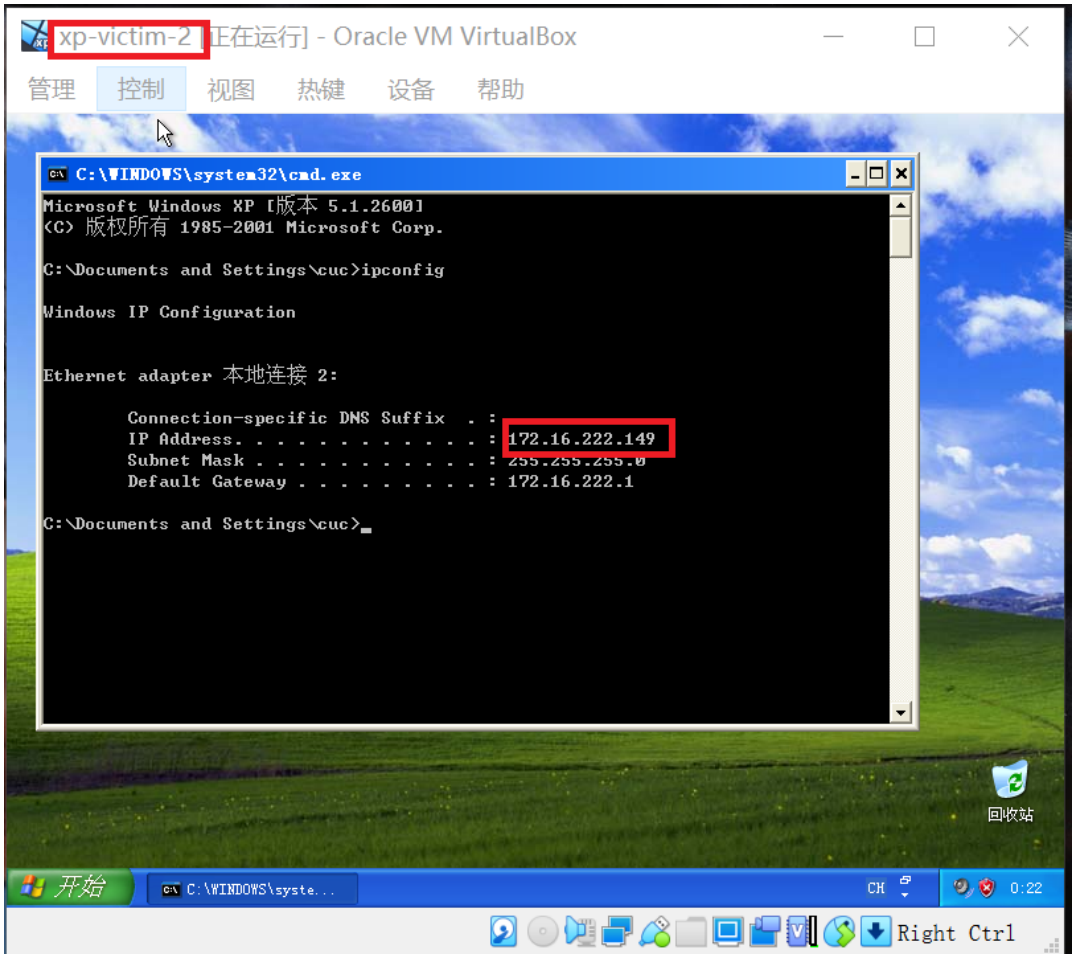
- **测试网络连通性**
  - 查询各主机的IP



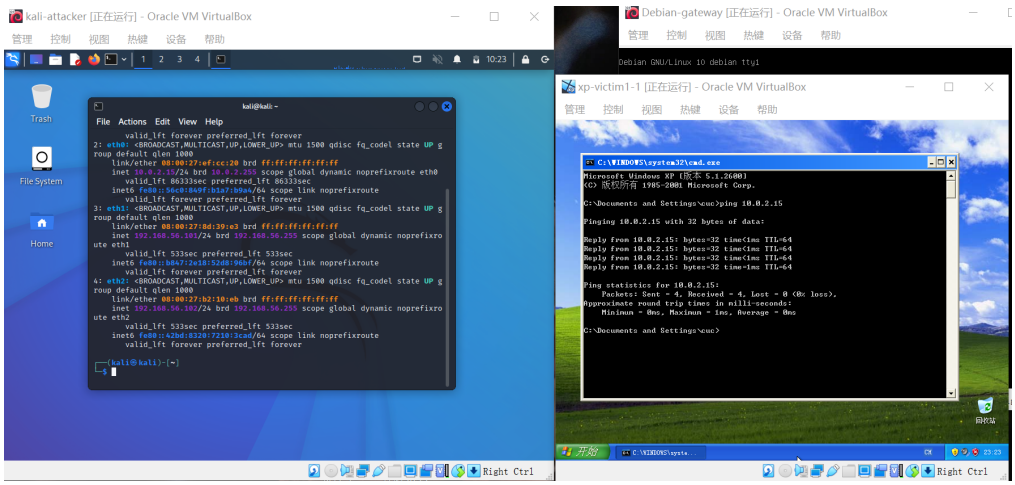




xp-victim1-1 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\cuc>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接 2:
Connection-specific DNS Suffix . :
IP Address. . . . . : 172.16.111.145
Subnet Mask . . . . . :
Default Gateway . . . . . : 172.16.111.1
C:\Documents and Settings\cuc>
回收站
开始
C:\WINDOWS\syste...
CH
22:51
Right Ctrl

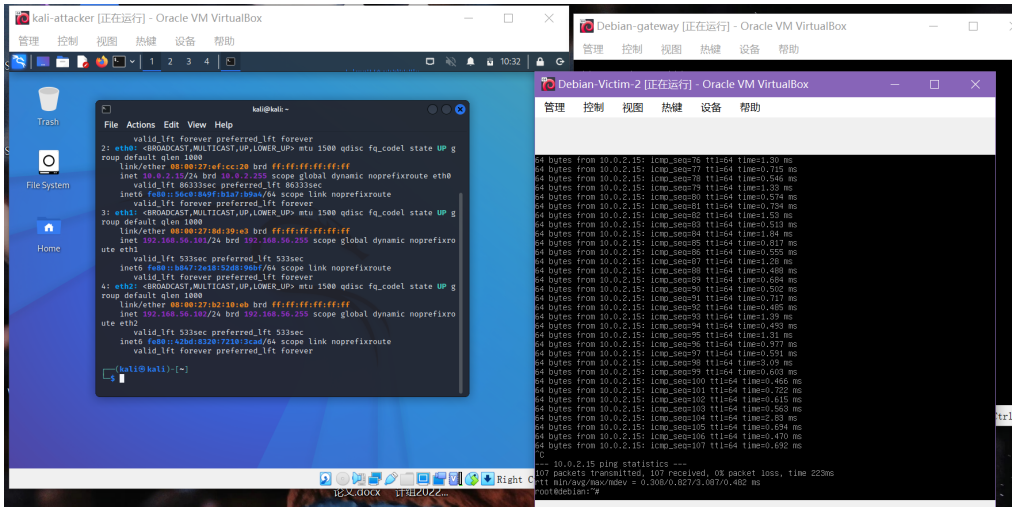

Debian-Victim-2 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:f1:8a:2d brd ff:ff:ff:ff:ff:ff
inet 172.16.222.100/24 brd 172.16.222.255 scope global dynamic enp0s3
valid_lft 861046sec preferred_lft 861046sec
inet6 fe80::a00:27ff:fef1:8a2d/64 scope link
valid_lft forever preferred_lft forever
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:f1:8a:2d brd ff:ff:ff:ff:ff:ff
inet 172.16.222.100/24 brd 172.16.222.255 scope global dynamic enp0s3
valid_lft 861041sec preferred_lft 861041sec
inet6 fe80::a00:27ff:fef1:8a2d/64 scope link
valid_lft forever preferred_lft forever
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:f1:8a:2d brd ff:ff:ff:ff:ff:ff
inet 172.16.222.100/24 brd 172.16.222.255 scope global dynamic enp0s3
valid_lft 861035sec preferred_lft 861035sec
inet6 fe80::a00:27ff:fef1:8a2d/64 scope link
valid_lft forever preferred_lft forever
root@debian:~#
Right Ctrl



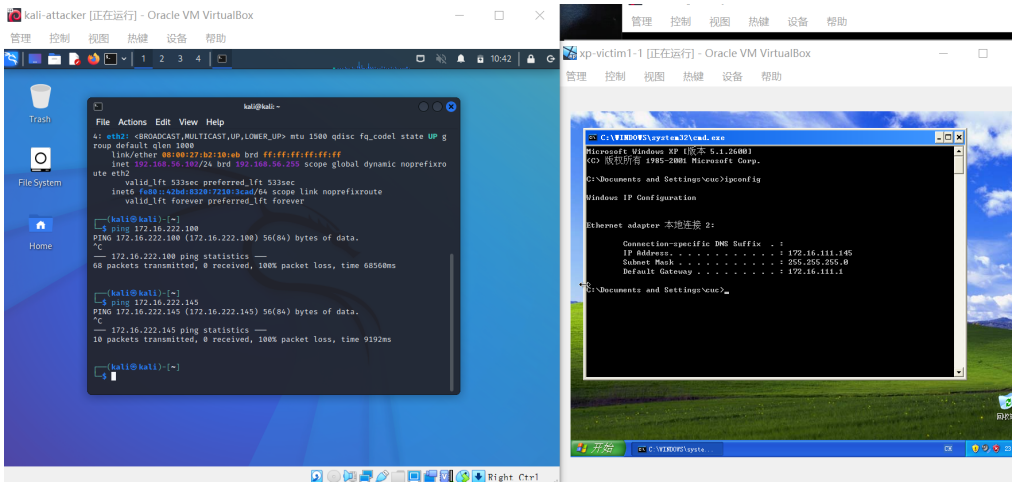

- 靶机可以直接访问攻击者主机
  - 局域网1内的靶机访问



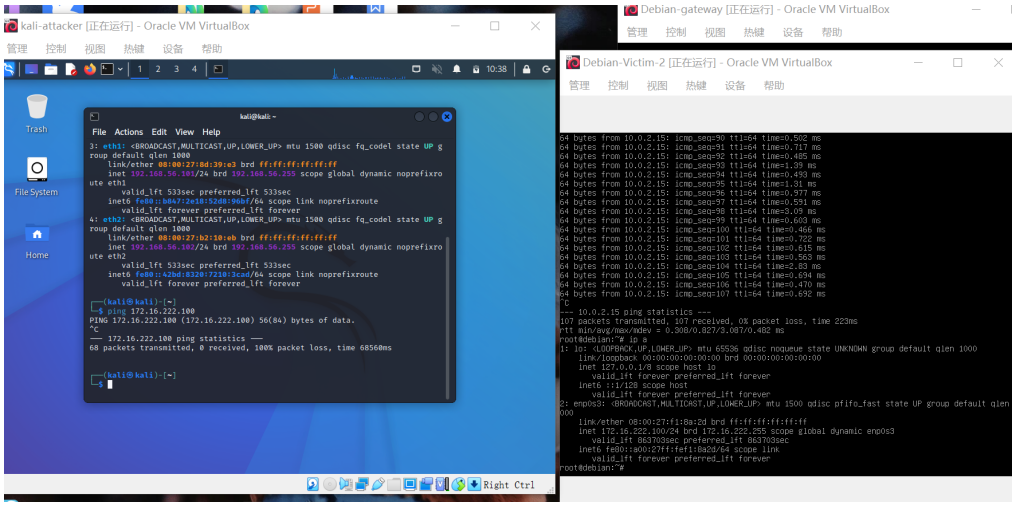

  - 局域网2内的靶机访问



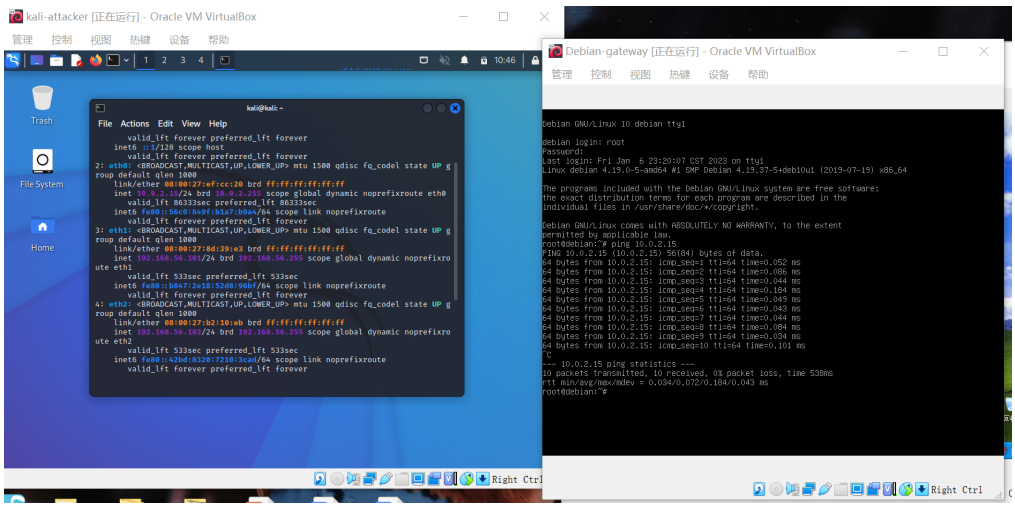

- 攻击者主机无法直接访问靶机
  - 访问局域网1内的靶机



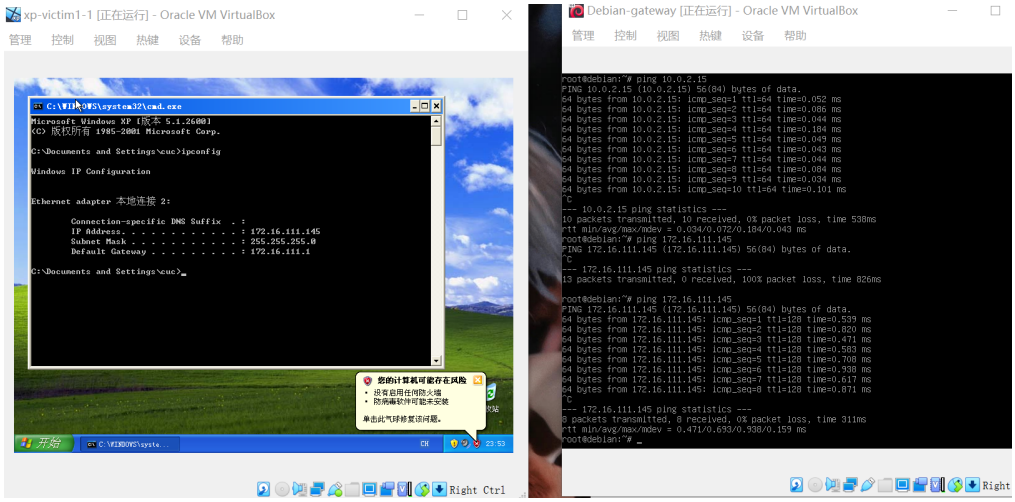

  - 访问局域网2内的靶机



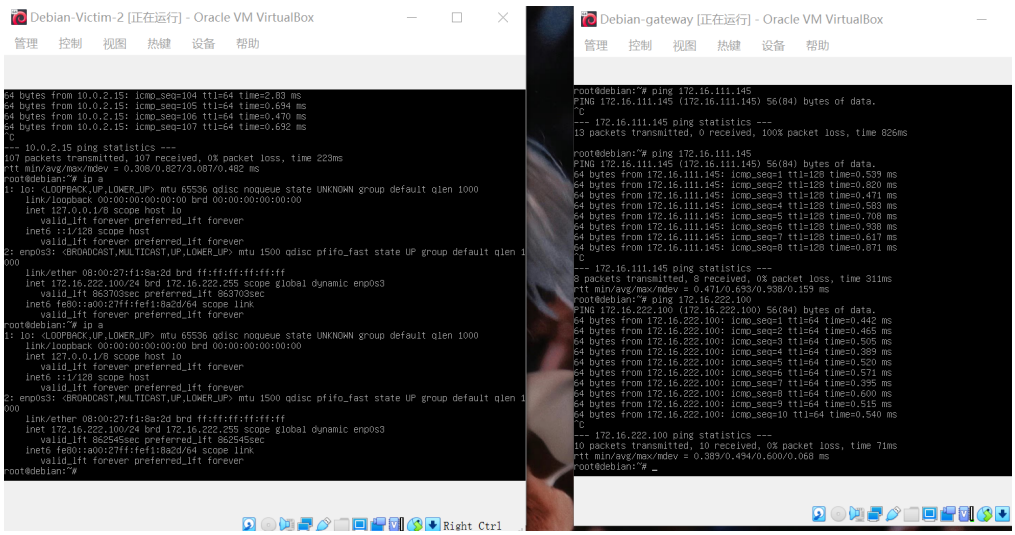

- 网关可以直接访问攻击者主机和靶机
  - 访问攻击者主机



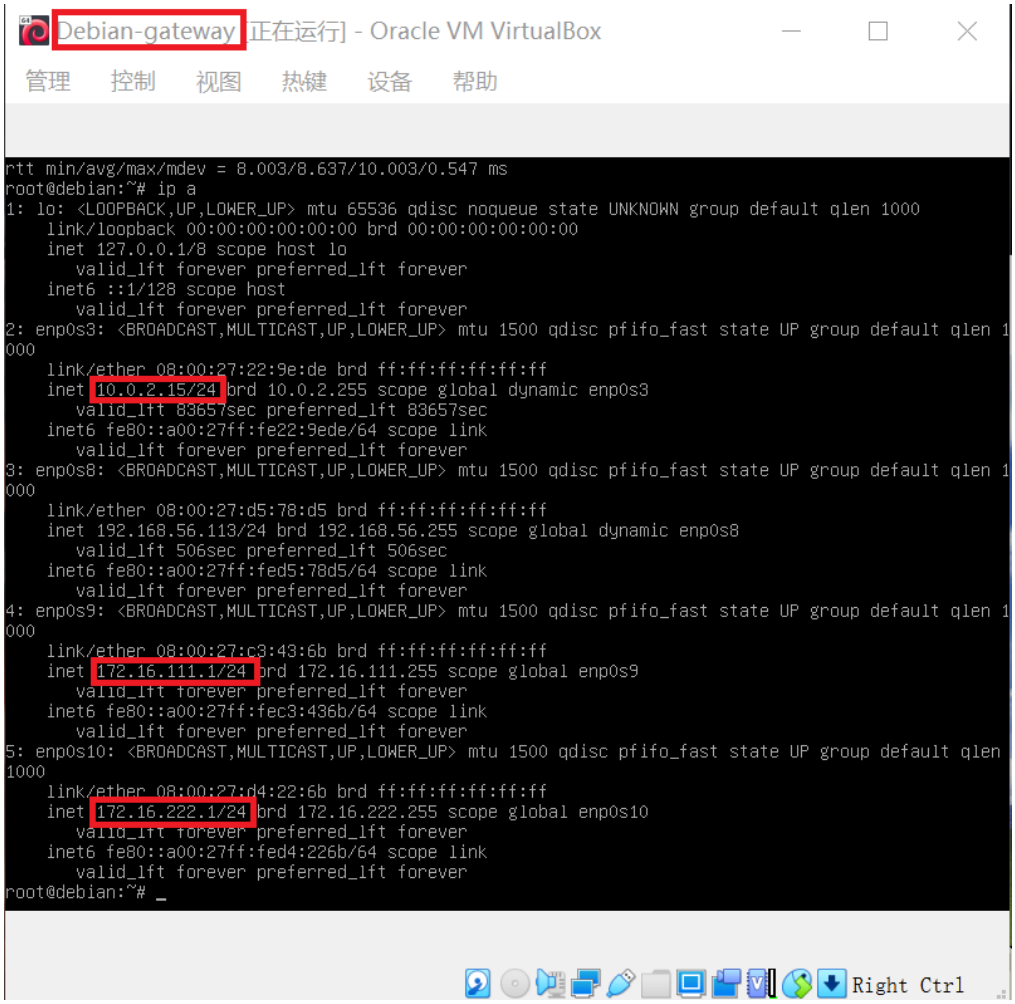

- 访问局域网1内的靶机



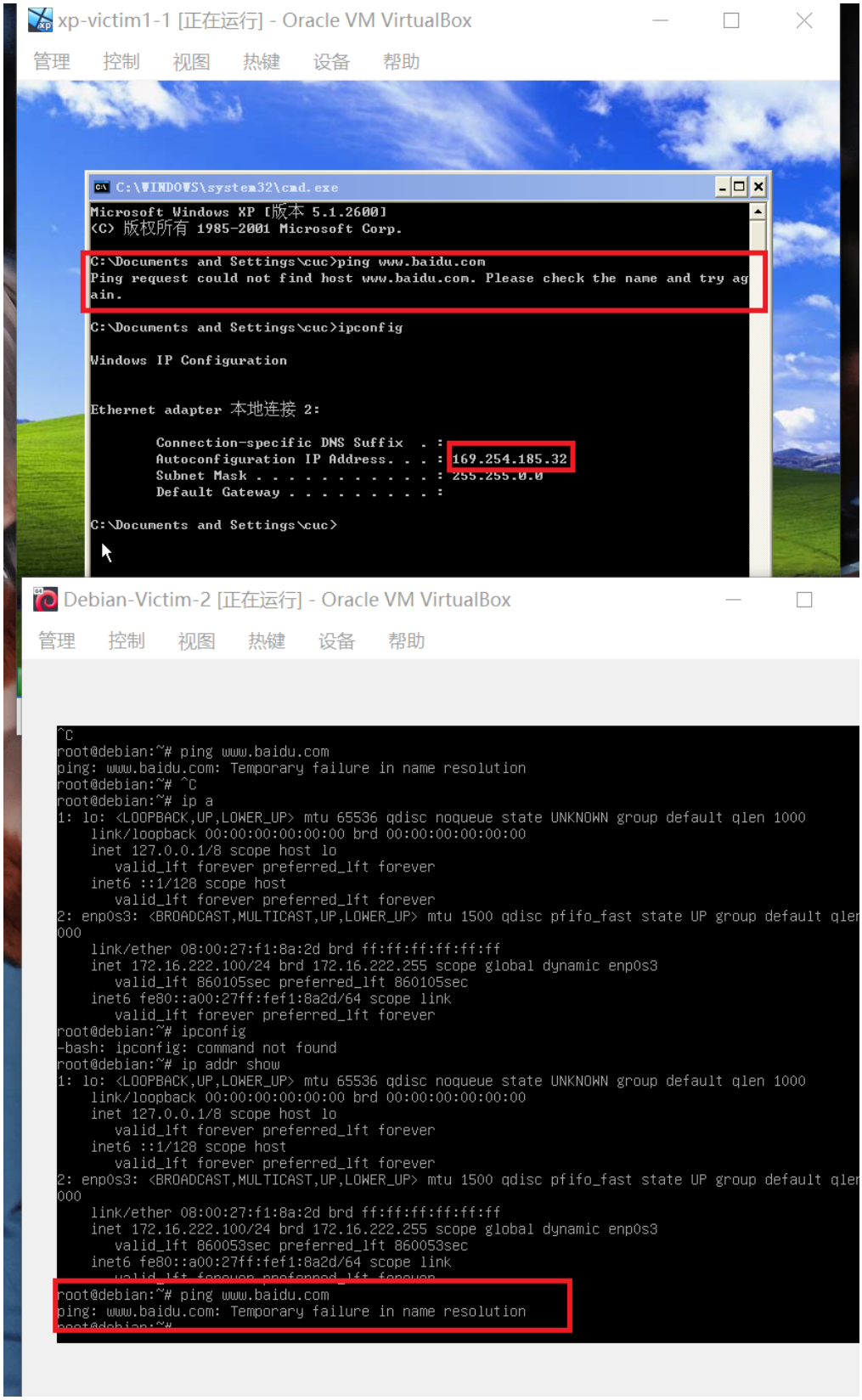

- 访问局域网2内的靶机



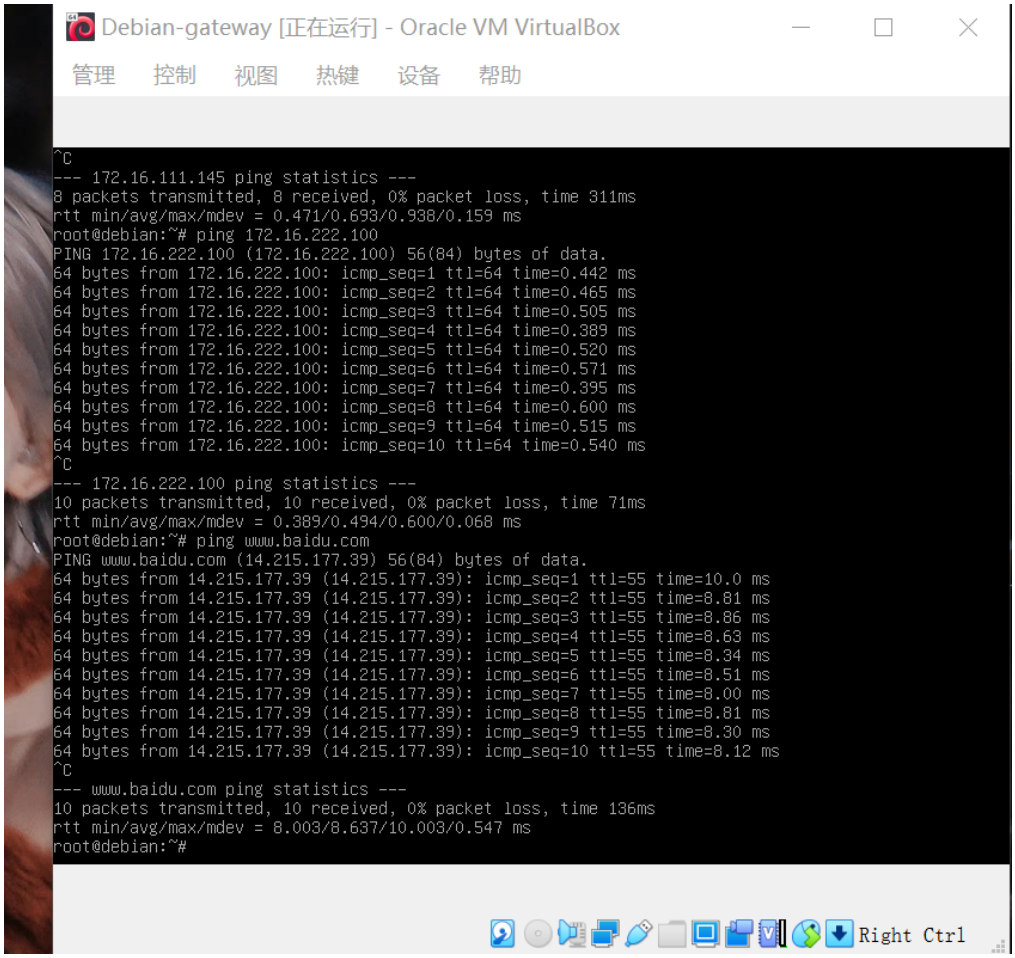

- 靶机的所有对外上下行流量必须经过网关
  - 通过观察可以发现，靶机的网关ip 被设置为Gateway enp0 的ip，靶机本身不能上网，靶机只能经由网关对外访问。



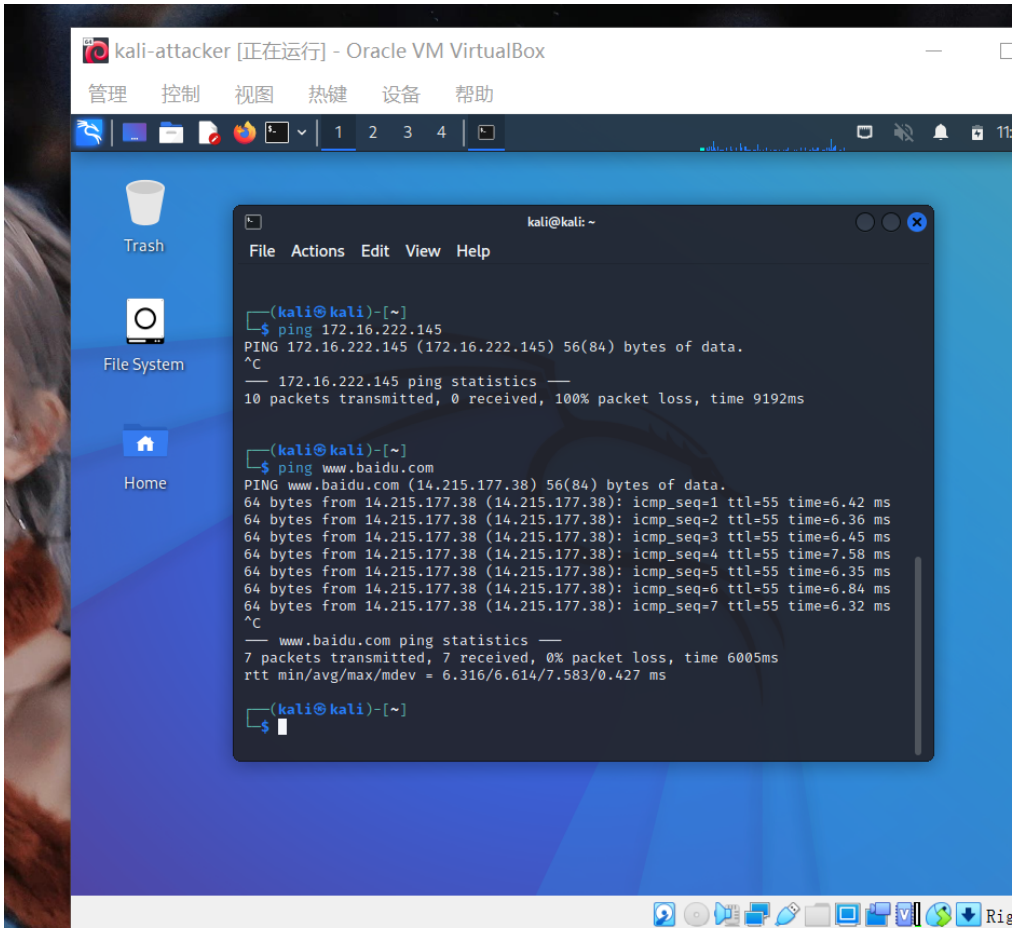

- 关闭网关后不再能访问互联网，且靶机的ip地址是169开头的，不是原来的172，是自动获取的



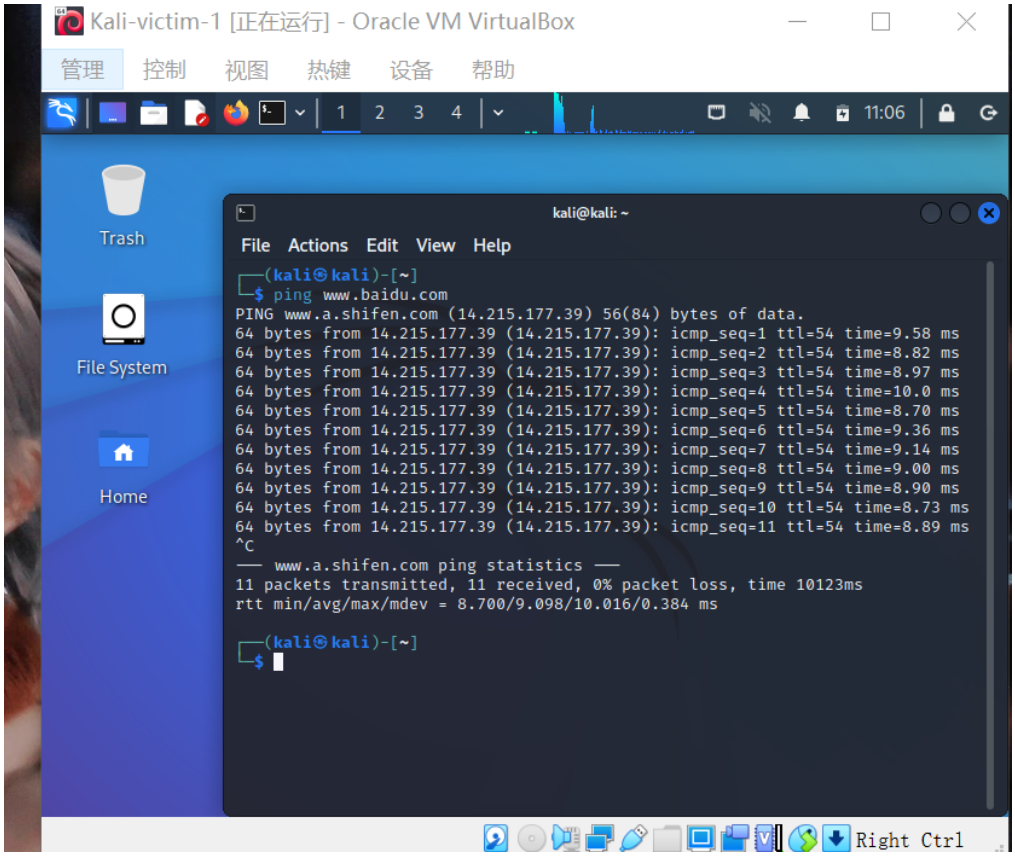

- 所有结点均可以访问互联网
  - 网关

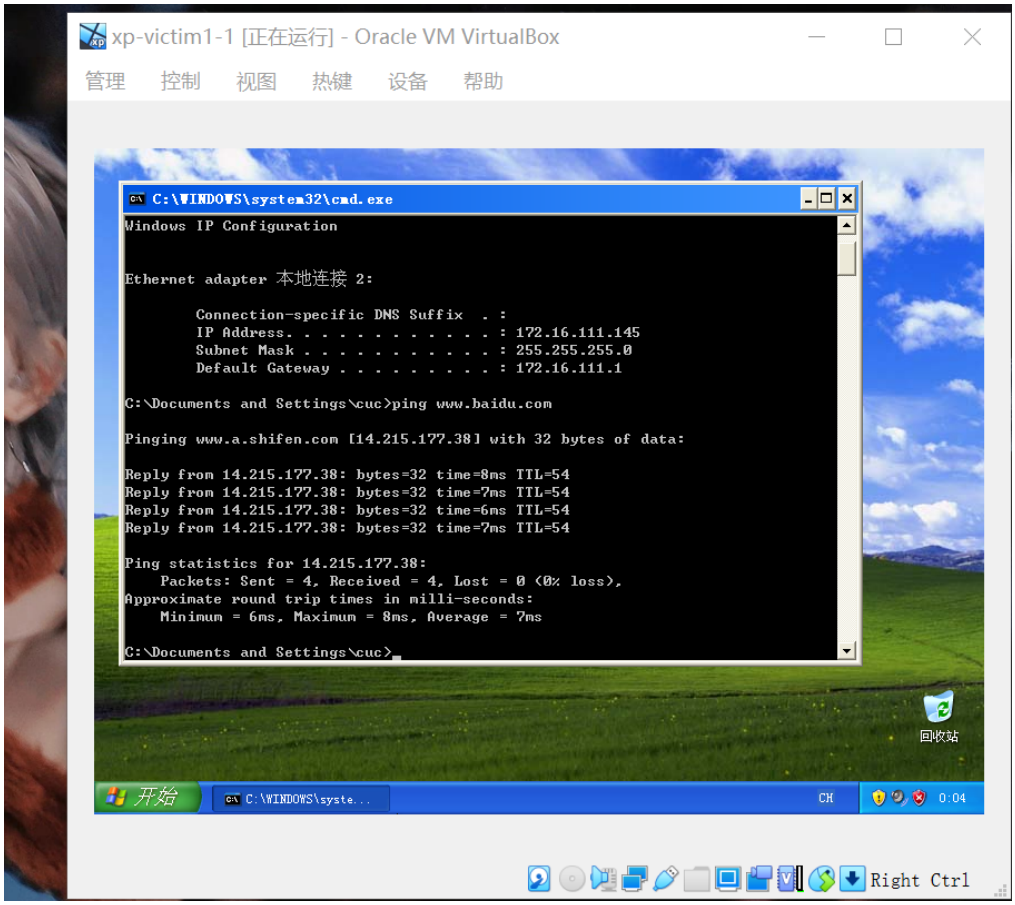

Debian-gateway [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
^C
--- 172.16.111.145 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 311ms
rtt min/avg/max/mdev = 0.471/0.693/0.938/0.159 ms
root@debian:~# ping 172.16.222.100
PING 172.16.222.100 (172.16.222.100) 56(84) bytes of data.
64 bytes from 172.16.222.100: icmp_seq=1 ttl=64 time=0.442 ms
64 bytes from 172.16.222.100: icmp_seq=2 ttl=64 time=0.465 ms
64 bytes from 172.16.222.100: icmp_seq=3 ttl=64 time=0.505 ms
64 bytes from 172.16.222.100: icmp_seq=4 ttl=64 time=0.389 ms
64 bytes from 172.16.222.100: icmp_seq=5 ttl=64 time=0.520 ms
64 bytes from 172.16.222.100: icmp_seq=6 ttl=64 time=0.571 ms
64 bytes from 172.16.222.100: icmp_seq=7 ttl=64 time=0.395 ms
64 bytes from 172.16.222.100: icmp_seq=8 ttl=64 time=0.600 ms
64 bytes from 172.16.222.100: icmp_seq=9 ttl=64 time=0.515 ms
64 bytes from 172.16.222.100: icmp_seq=10 ttl=64 time=0.540 ms
^C
--- 172.16.222.100 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 71ms
rtt min/avg/max/mdev = 0.389/0.494/0.600/0.068 ms
root@debian:~# ping www.baidu.com
PING www.baidu.com (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=1 ttl=55 time=10.0 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=2 ttl=55 time=8.81 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=3 ttl=55 time=8.86 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=4 ttl=55 time=8.63 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=5 ttl=55 time=8.34 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=6 ttl=55 time=8.51 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=7 ttl=55 time=8.00 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=8 ttl=55 time=8.81 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=9 ttl=55 time=8.30 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=10 ttl=55 time=8.12 ms
^C
--- www.baidu.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 136ms
rtt min/avg/max/mdev = 8.003/8.637/10.003/0.547 ms
root@debian:~#
Right Ctrl

- 攻击者主机

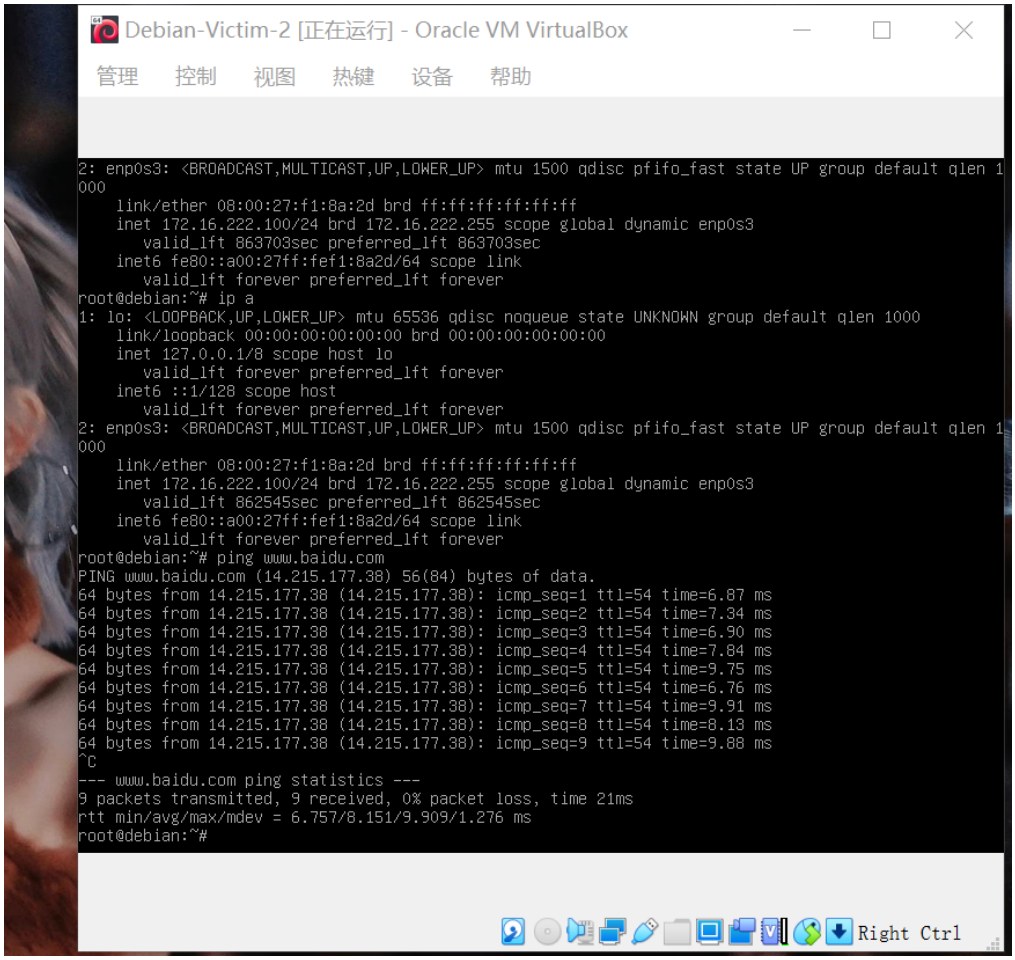

kali-attacker [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping 172.16.222.145
PING 172.16.222.145 (172.16.222.145) 56(84) bytes of data.
^C
— 172.16.222.145 ping statistics —
10 packets transmitted, 0 received, 100% packet loss, time 9192ms
(kali㉿kali)-[~]
$ ping www.baidu.com
PING www.baidu.com (14.215.177.38) 56(84) bytes of data.
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=1 ttl=55 time=6.42 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=2 ttl=55 time=6.36 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=3 ttl=55 time=6.45 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=4 ttl=55 time=7.58 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=5 ttl=55 time=6.35 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=6 ttl=55 time=6.84 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=7 ttl=55 time=6.32 ms
^C
— www.baidu.com ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6005ms
rtt min/avg/max/mdev = 6.316/6.614/7.583/0.427 ms
(kali㉿kali)-[~]
$

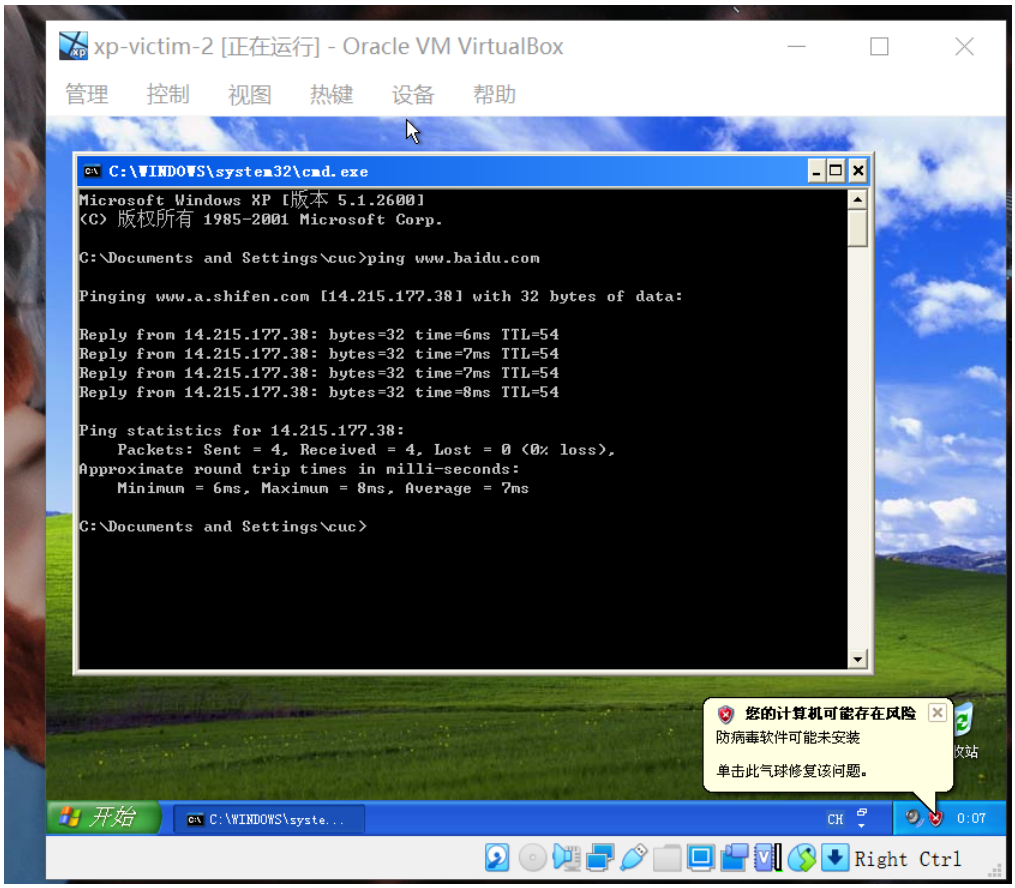
- 局域网1


Kali-victim-1 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
11:06
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ping www.baidu.com
PING www.a.shifen.com (14.215.177.39) 56(84) bytes of data.
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=1 ttl=54 time=9.58 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=2 ttl=54 time=8.82 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=3 ttl=54 time=8.97 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=4 ttl=54 time=10.0 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=5 ttl=54 time=8.70 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=6 ttl=54 time=9.36 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=7 ttl=54 time=9.14 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=8 ttl=54 time=9.00 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=9 ttl=54 time=8.90 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=10 ttl=54 time=8.73 ms
64 bytes from 14.215.177.39 (14.215.177.39): icmp_seq=11 ttl=54 time=8.89 ms
^C
— www.a.shifen.com ping statistics —
11 packets transmitted, 11 received, 0% packet loss, time 10123ms
rtt min/avg/max/mdev = 8.700/9.098/10.016/0.384 ms
(kali㉿kali)-[~]
$
Right Ctrl


xp-victim1-1 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
C:\WINDOWS\system32\cmd.exe
Windows IP Configuration
Ethernet adapter 本地连接 2:
Connection-specific DNS Suffix . :
IP Address. . . . . : 172.16.111.145
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.111.1
C:\Documents and Settings\cuc>ping www.baidu.com
Pinging www.a.shifen.com [14.215.177.38] with 32 bytes of data:
Reply from 14.215.177.38: bytes=32 time=8ms TTL=54
Reply from 14.215.177.38: bytes=32 time=7ms TTL=54
Reply from 14.215.177.38: bytes=32 time=6ms TTL=54
Reply from 14.215.177.38: bytes=32 time=7ms TTL=54
Ping statistics for 14.215.177.38:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 8ms, Average = 7ms
C:\Documents and Settings\cuc>
回收站
开始
CH
0:04
Right Ctrl

- 局域网2


Debian-Victim-2 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
link/ether 08:00:27:f1:8a:2d brd ff:ff:ff:ff:ff:ff
inet 172.16.222.100/24 brd 172.16.222.255 scope global dynamic enp0s3
valid_lft 863703sec preferred_lft 863703sec
inet6 fe80::a00:27ff:fef1:8a2d/64 scope link
valid_lft forever preferred_lft forever
root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
000
link/ether 08:00:27:f1:8a:2d brd ff:ff:ff:ff:ff:ff
inet 172.16.222.100/24 brd 172.16.222.255 scope global dynamic enp0s3
valid_lft 862545sec preferred_lft 862545sec
inet6 fe80::a00:27ff:fef1:8a2d/64 scope link
valid_lft forever preferred_lft forever
root@debian:~# ping www.baidu.com
PING www.baidu.com (14.215.177.38) 56(84) bytes of data.
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=1 ttl=54 time=6.87 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=2 ttl=54 time=7.34 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=3 ttl=54 time=6.90 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=4 ttl=54 time=7.84 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=5 ttl=54 time=9.75 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=6 ttl=54 time=6.76 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=7 ttl=54 time=9.91 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=8 ttl=54 time=8.13 ms
64 bytes from 14.215.177.38 (14.215.177.38): icmp_seq=9 ttl=54 time=9.88 ms
^C
--- www.baidu.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 6.757/8.151/9.909/1.276 ms
root@debian:~#
Right Ctrl


xp-victim-2 [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.
C:\Documents and Settings\cuc>ping www.baidu.com
Pinging www.a.shifen.com [14.215.177.38] with 32 bytes of data:
Reply from 14.215.177.38: bytes=32 time=6ms TTL=54
Reply from 14.215.177.38: bytes=32 time=7ms TTL=54
Reply from 14.215.177.38: bytes=32 time=7ms TTL=54
Reply from 14.215.177.38: bytes=32 time=8ms TTL=54
Ping statistics for 14.215.177.38:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 8ms, Average = 7ms
C:\Documents and Settings\cuc>
您的计算机可能存在风险
防病毒软件可能未安装
单击此气球修复该问题。
开始
C:\WINDOWS\syste...
CH
0:07
Right Ctrl

## 实验中出现的问题

- 网关无法访问局域网1中的Windows XP

  查询资料得可能是XP的防火墙所致，关闭防火墙即可