

## 实验一 基于VirtualBox的网络攻防基础环境搭建实例讲解（改）

### 一、实验目的

熟悉virtualBox操作系统网络连接方式，掌握网关的配置和网络拓扑结构，搭建起基于VB的网络攻防实验环境。

### 二、实验要求及完成情况

- 节点：靶机、网关、攻击者主机 ok
  - 连通性
    - 靶机可以直接访问攻击者主机 ok
    - 攻击者主机无法直接访问靶机 ok
    - 网关可以直接访问攻击者主机和靶机 ok
    - 靶机的所有对外上下行流量必须经过网关 ok
    - 所有节点均可以访问互联网 ok
  - 其他要求
    - 所有节点制作成基础镜像（多重加载的虚拟硬盘）ok

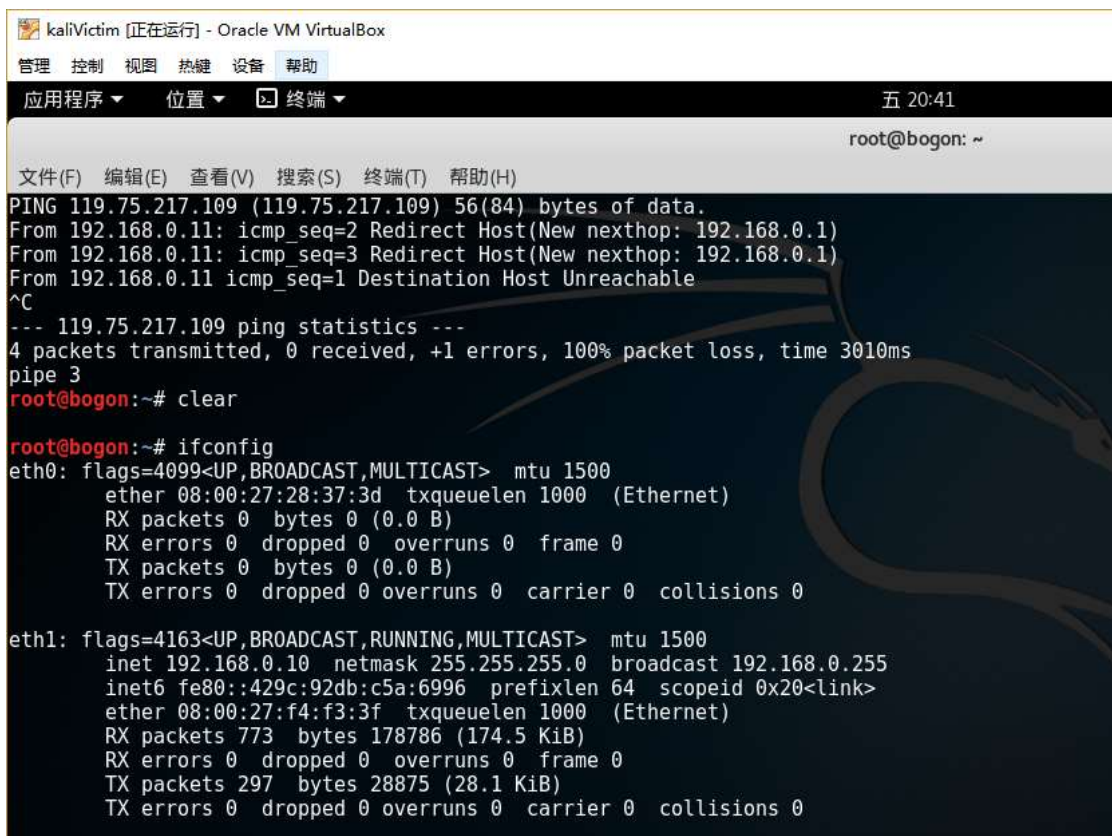
### 三、实验结果展示

#### 1、节点

（1）靶机（KaliVictim）

配置方法：手动

- Eth1（内部网络）：IP 192.168.0.10 网关 192.168.0.11



```
kaliVictim [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾ 五 20:41
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
PING 119.75.217.109 (119.75.217.109) 56(84) bytes of data.
From 192.168.0.11: icmp_seq=2 Redirect Host(New nexthop: 192.168.0.1)
From 192.168.0.11: icmp_seq=3 Redirect Host(New nexthop: 192.168.0.1)
From 192.168.0.11 icmp_seq=1 Destination Host Unreachable
^C
--- 119.75.217.109 ping statistics ---
4 packets transmitted, 0 received, +1 errors, 100% packet loss, time 3010ms
pipe 3
root@bogon:~# clear

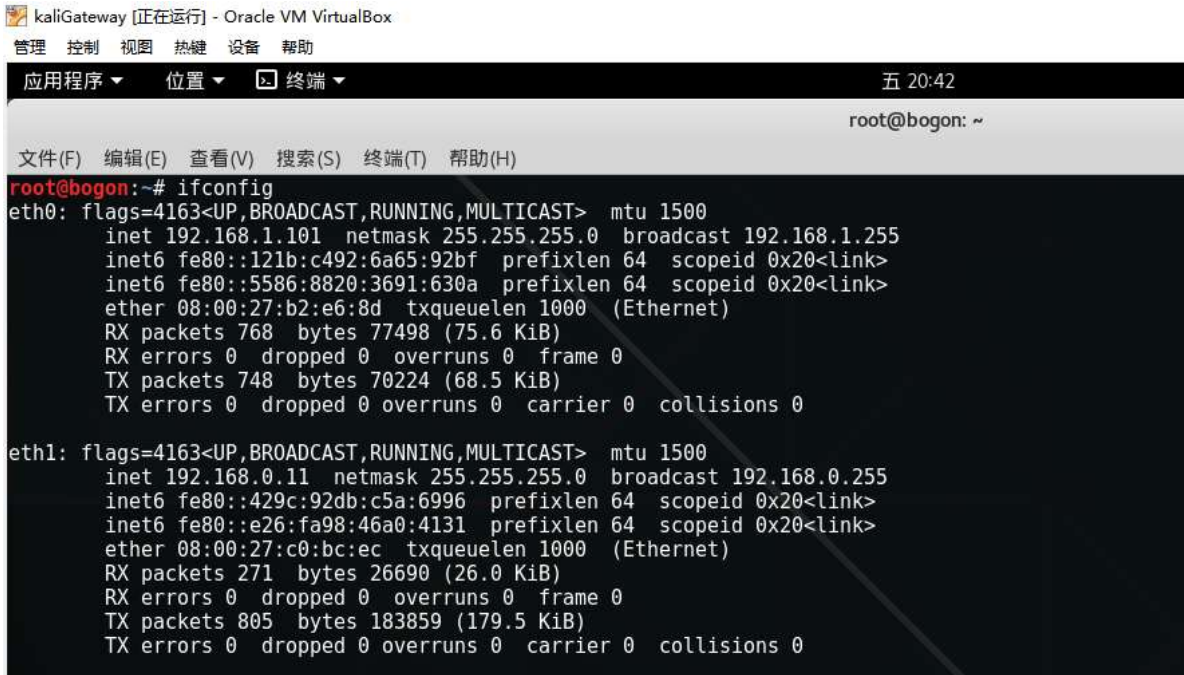
root@bogon:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:28:37:3d txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.10 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::429c:92db:c5a:6996 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:f4:f3:3f txqueuelen 1000 (Ethernet)
    RX packets 773 bytes 178786 (174.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 297 bytes 28875 (28.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

（2）网关（KaliGateway）

配置方法：dhcp（dhclient）

- Eth0（桥接网络）：IP 192.168.1.101 网关 192.168.1.1
- Eth1（内部网络）：IP 192.168.0.11 网关 192.168.0.1



```

kaliGateway [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端 五 20:42
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@bogon:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::121b:c492:6a65:92bf prefixlen 64 scopeid 0x20<link>
    inet6 fe80::5586:8820:3691:630a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:b2:e6:8d txqueuelen 1000 (Ethernet)
    RX packets 768 bytes 77498 (75.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 748 bytes 70224 (68.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

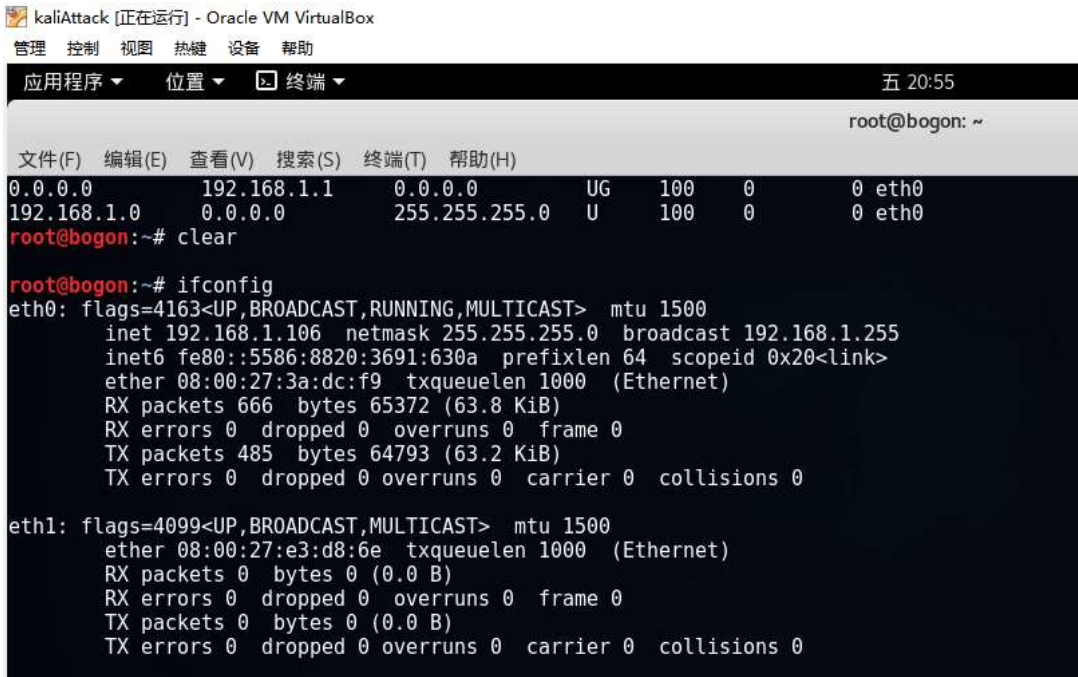
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.11 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::429c:92db:c5a:6996 prefixlen 64 scopeid 0x20<link>
    inet6 fe80::e26:fa98:46a0:4131 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:c0:bc:ec txqueuelen 1000 (Ethernet)
    RX packets 271 bytes 26690 (26.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 805 bytes 183859 (179.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

(3) 攻击者主机 (KaliAttack)

配置方法: dhcp (dhclient)

- Eth0 (桥接网络): IP 192.168.1.106 网关 192.168.1.1



```

kaliAttack [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 位置 终端 五 20:55
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
0.0.0.0 192.168.1.1 0.0.0.0 UG 100 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
root@bogon:~# clear

root@bogon:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.106 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::5586:8820:3691:630a prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:3a:dc:f9 txqueuelen 1000 (Ethernet)
    RX packets 666 bytes 65372 (63.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 485 bytes 64793 (63.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 08:00:27:e3:d8:6e txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

2、连通性

- 靶机可以直接访问攻击者主机

kaliVictim [正在运行] - Oracle VM VirtualBox

管理 控制 视图 热键 设备 帮助

应用程序 ▾ 位置 ▾ 终端 ▾ 四 21:25

root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
root@bogon:~# ping 192.168.1.106
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_seq=1 ttl=64 time=0.277 ms
64 bytes from 192.168.1.106: icmp_seq=2 ttl=64 time=0.646 ms
64 bytes from 192.168.1.106: icmp_seq=3 ttl=64 time=0.671 ms
64 bytes from 192.168.1.106: icmp_seq=4 ttl=64 time=0.558 ms
64 bytes from 192.168.1.106: icmp_seq=5 ttl=64 time=0.635 ms
^C
--- 192.168.1.106 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.277/0.557/0.671/0.146 ms
root@bogon:~#
```

- 攻击者主机无法直接访问靶机

kaliAttack [正在运行] - Oracle VM VirtualBox

管理 控制 视图 热键 设备 帮助

应用程序 ▾ 位置 ▾ 终端 ▾ 五 21:00

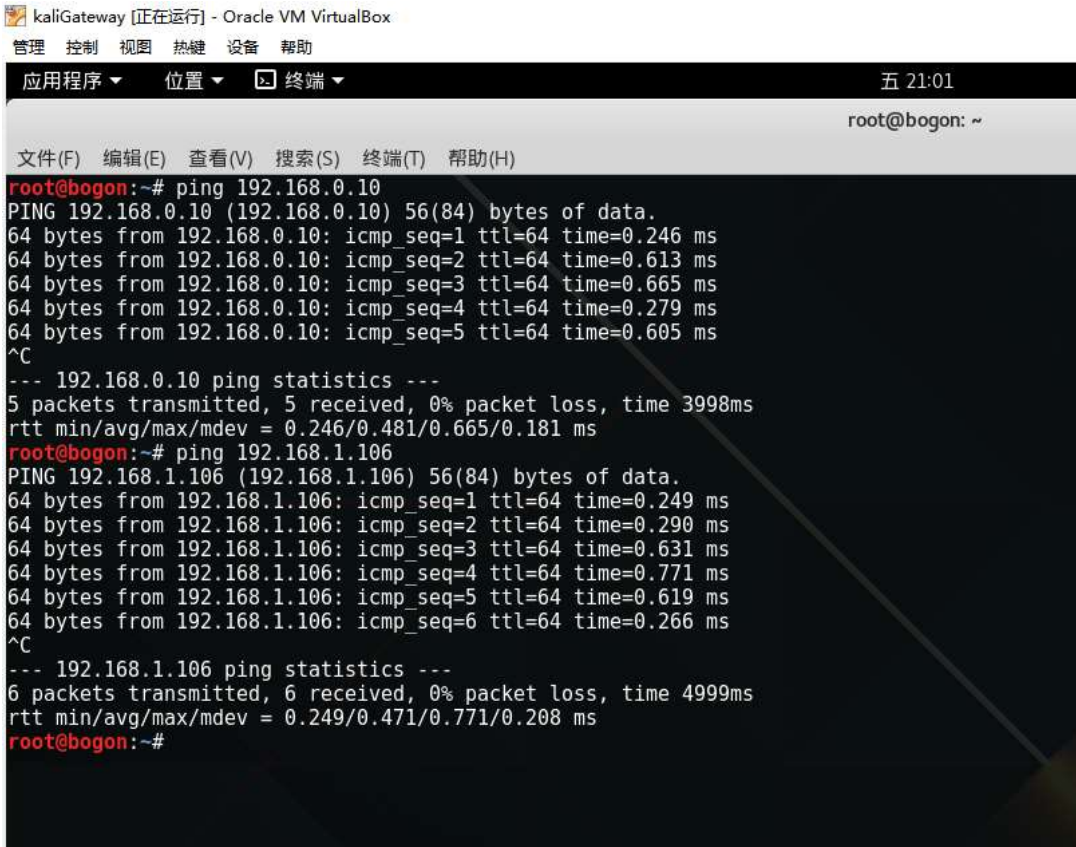
root@bogon: ~

文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

```
root@bogon:~# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
^C
--- 192.168.0.10 ping statistics ---
51 packets transmitted, 0 received, 100% packet loss, time 50338ms
root@bogon:~#
```

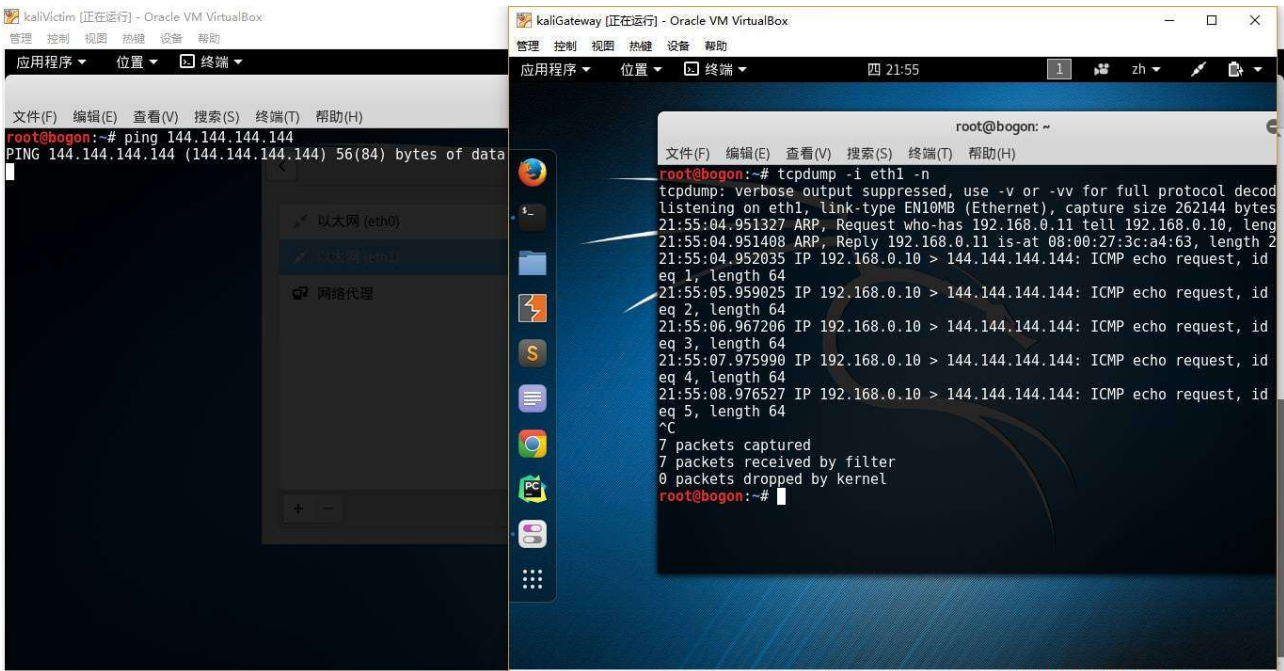
- 网关可以直接访问攻击者主机和靶机





```
kaliGateway [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾ 五 21:01
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@bogon:~# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data:
64 bytes from 192.168.0.10: icmp_seq=1 ttl=64 time=0.246 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=64 time=0.613 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=64 time=0.665 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=64 time=0.279 ms
64 bytes from 192.168.0.10: icmp_seq=5 ttl=64 time=0.605 ms
^C
--- 192.168.0.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3998ms
rtt min/avg/max/mdev = 0.246/0.481/0.665/0.181 ms
root@bogon:~# ping 192.168.1.106
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data:
64 bytes from 192.168.1.106: icmp_seq=1 ttl=64 time=0.249 ms
64 bytes from 192.168.1.106: icmp_seq=2 ttl=64 time=0.290 ms
64 bytes from 192.168.1.106: icmp_seq=3 ttl=64 time=0.631 ms
64 bytes from 192.168.1.106: icmp_seq=4 ttl=64 time=0.771 ms
64 bytes from 192.168.1.106: icmp_seq=5 ttl=64 time=0.619 ms
64 bytes from 192.168.1.106: icmp_seq=6 ttl=64 time=0.266 ms
^C
--- 192.168.1.106 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.249/0.471/0.771/0.208 ms
root@bogon:~#
```

- 靶机的所有对外上下行流量必须经过网关

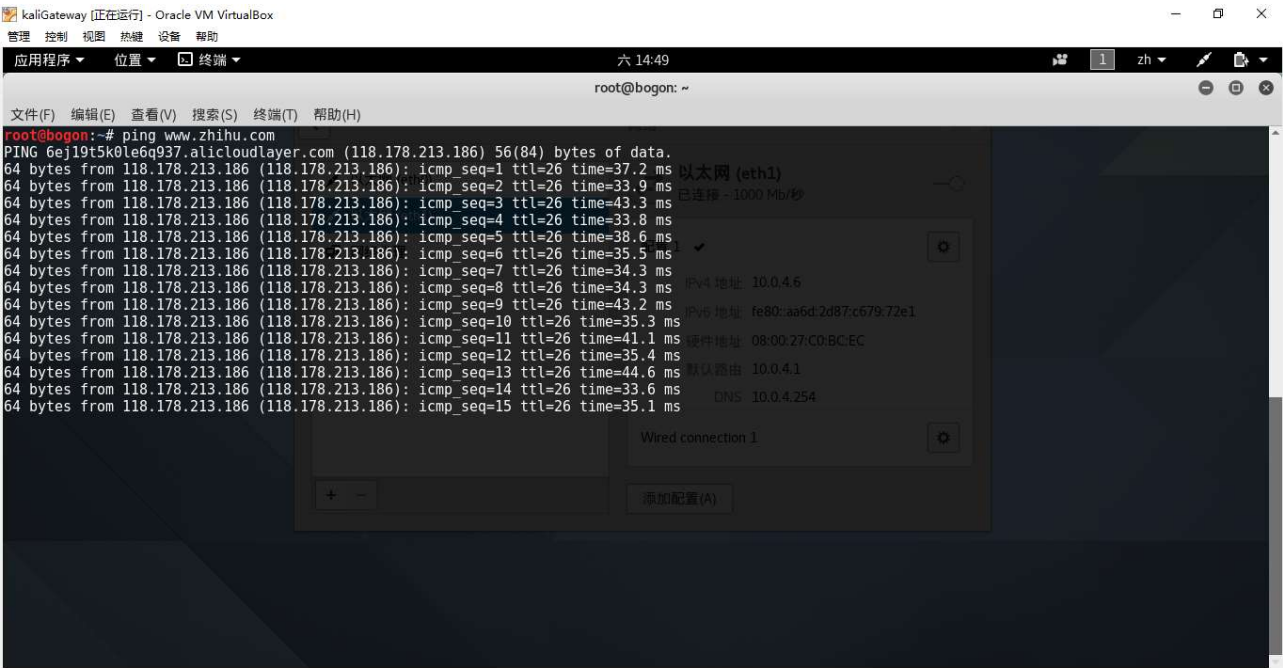


```
kaliVictim [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@bogon:~# ping 144.144.144.144
PING 144.144.144.144 (144.144.144.144) 56(84) bytes of data:
^C
--- 144.144.144.144 ping statistics ---
0 packets transmitted, 0 received, 100% packet loss, time 0ms
root@bogon:~#

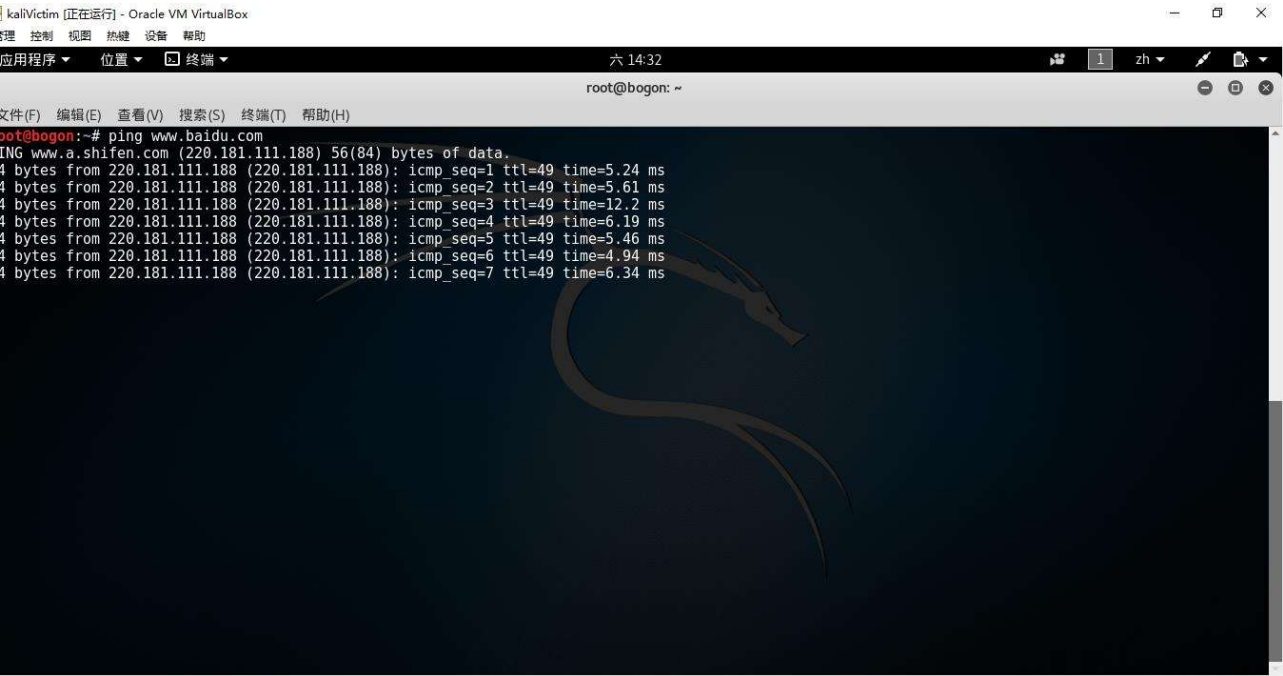
kaliGateway [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
应用程序 ▾ 位置 ▾ 终端 ▾ 四 21:55
root@bogon: ~
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@bogon:~# tcpdump -i eth1 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decoding
listening on eth1, link-type EN10MB (Ethernet), capture size 262144 bytes
21:55:04.951327 ARP, Request who-has 192.168.0.11 tell 192.168.0.10, length 28
21:55:04.951408 ARP, Reply 192.168.0.11 is-at 08:00:27:3c:a4:63, length 28
21:55:04.952035 IP 192.168.0.10 > 144.144.144.144: ICMP echo request, id 1, length 64
21:55:05.959025 IP 192.168.0.10 > 144.144.144.144: ICMP echo request, id 2, length 64
21:55:06.967206 IP 192.168.0.10 > 144.144.144.144: ICMP echo request, id 3, length 64
21:55:07.975990 IP 192.168.0.10 > 144.144.144.144: ICMP echo request, id 4, length 64
21:55:08.976527 IP 192.168.0.10 > 144.144.144.144: ICMP echo request, id 5, length 64
^C
7 packets captured
7 packets received by filter
0 packets dropped by kernel
root@bogon:~#
```

- 所有节点均可以访问互联网

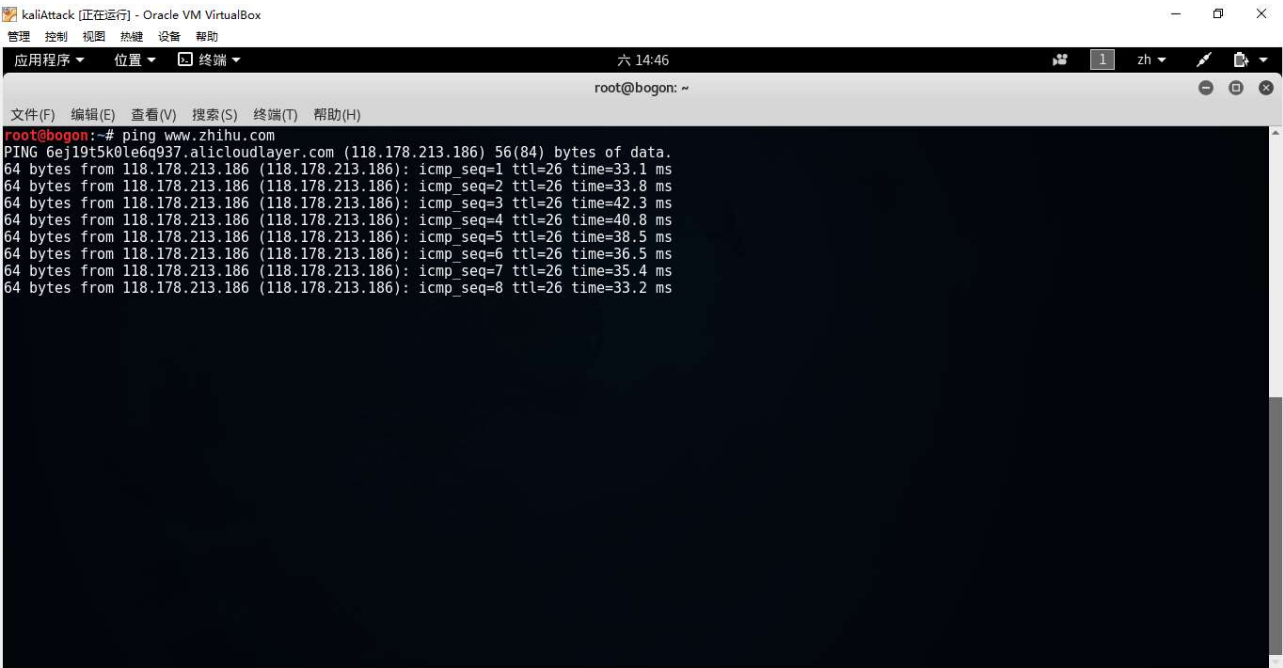
(1) 网关



(2) 靶机



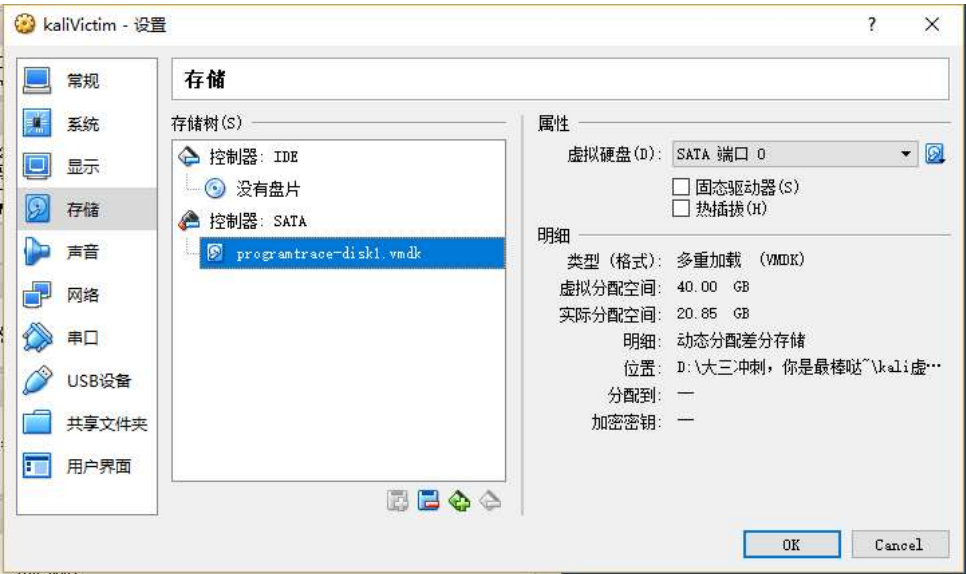
(3) 攻击者主机



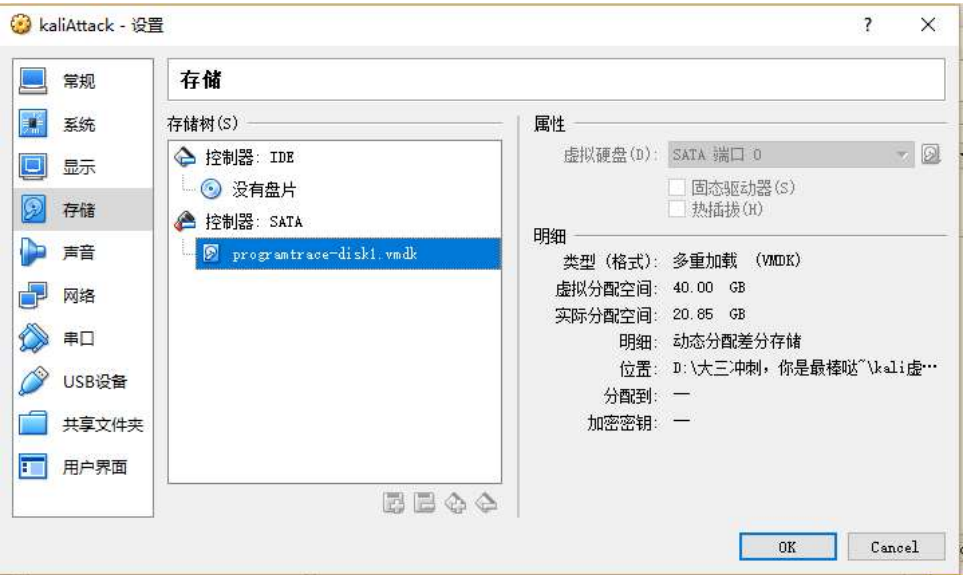
3、其他要求

- 所有节点制作成基础镜像（多重加载的虚拟硬盘）

(1) 靶机

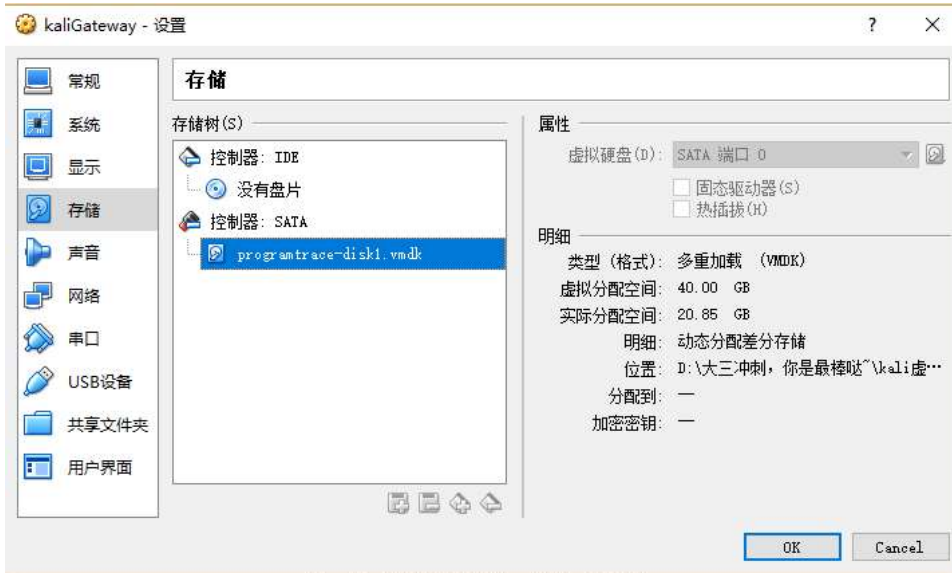


(2) 攻击者





### (3) 网关



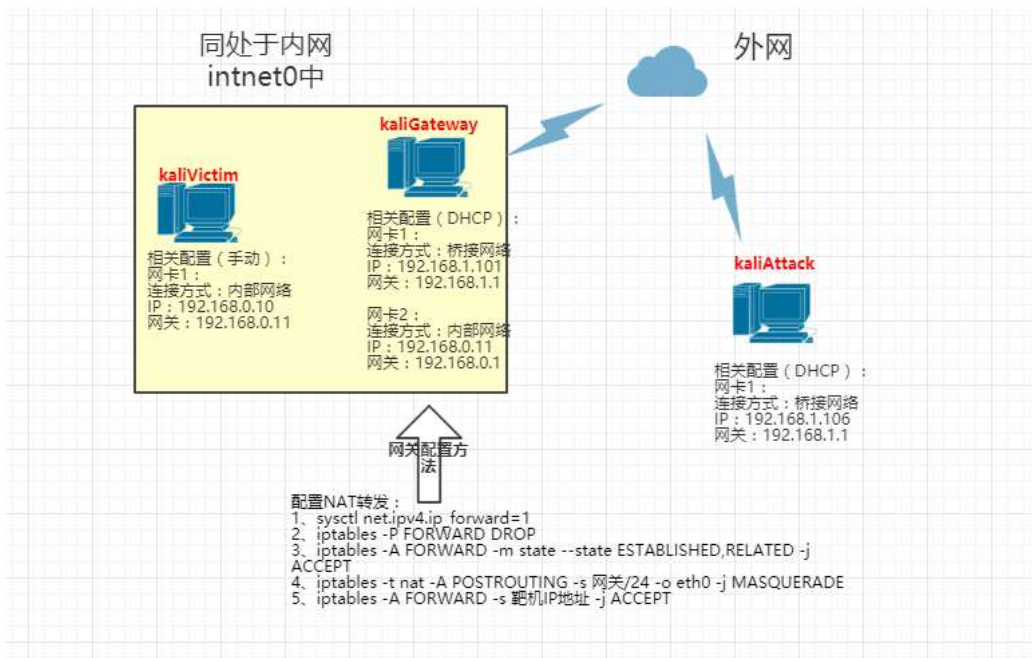
## 四、实验步骤

### 1、为网关配置NAT转发服务

在网关上操作：

- (1) 打开linux的转发功能: `sysctl net.ipv4.ip_forward=1`
- (2) 将FORWARD链的策略设置为DROP, 这样做的目的是做到对内网ip的控制: `iptables -P FORWARD DROP`
- (3) 这条规则规定允许任何地址到任何地址的确认包和关联包通过: `iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT`
- (4) 源地址转换: `iptables -t nat -A POSTROUTING -s 网关/24 -o eth0 -j MASQUERADE`
- (5) 允许特定IP地址(靶机)访问internet: `iptables -A FORWARD -s 靶机IP地址 -j ACCEPT`

## 配置流程图



2、所有节点制作成基础镜像（见链接）

[https://github.com/BiancaGuo/BiancaGuo.github.io/blob/master/\\_posts/VirtualBox%E8%99%9A%E6%8B%9F%E6%9C%BA%E5%A4%9A%E9%87%8D%E5%8A%A](https://github.com/BiancaGuo/BiancaGuo.github.io/blob/master/_posts/VirtualBox%E8%99%9A%E6%8B%9F%E6%9C%BA%E5%A4%9A%E9%87%8D%E5%8A%A)