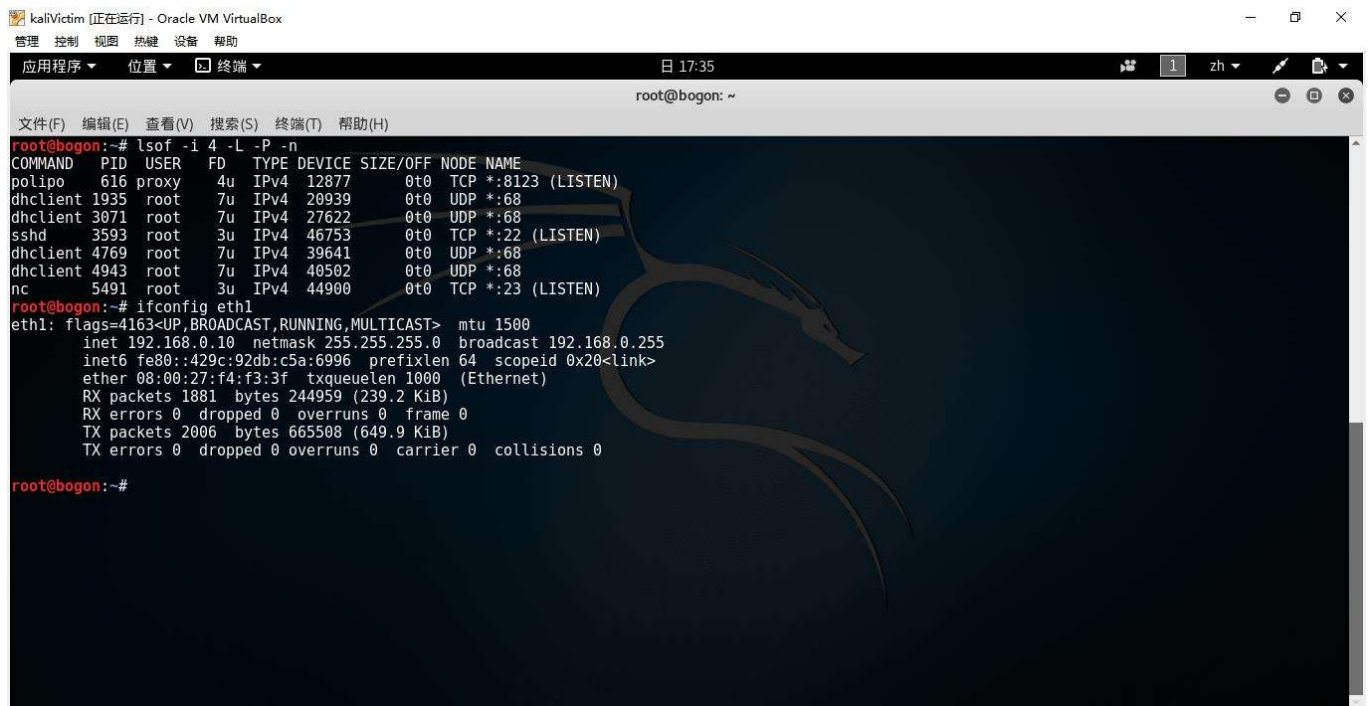


实验二 动手编程实现：TCP connect scan/TCP stealth scan/TCP XMAS scan/UDP scan

一、目标主机IP地址与端口开放情况



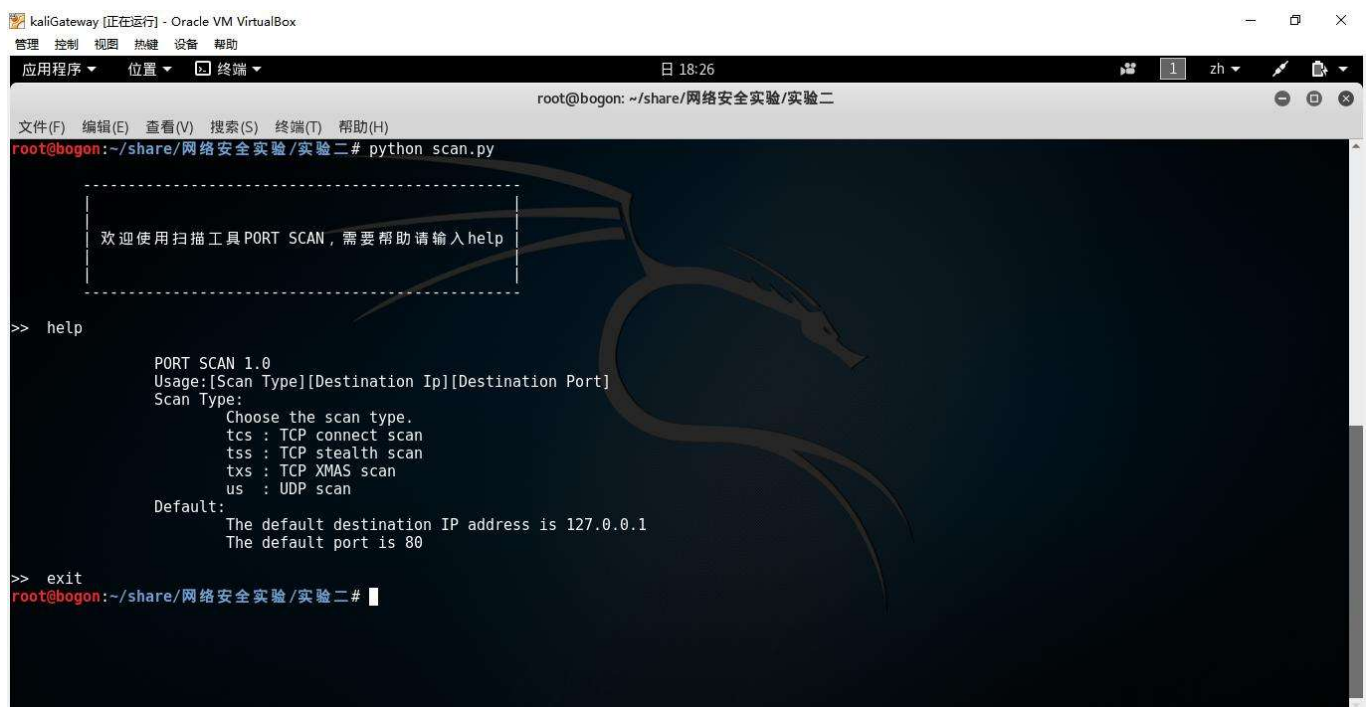
The screenshot shows a terminal window titled 'kaliVictim [正在运行] - Oracle VM VirtualBox'. The user is root@bogon. The terminal displays the output of the 'lsof -i 4 -L -P -n' command, which lists listening ports and the processes using them. It also shows the output of the 'ifconfig eth1' command, displaying network interface details for eth1.

```
root@bogon:~# lsof -i 4 -L -P -n
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
polipo 616 proxy 4u IPv4 12877 0t0 TCP *:8123 (LISTEN)
dhclient 1935 root 7u IPv4 20939 0t0 UDP *:68
dhclient 3071 root 7u IPv4 27622 0t0 UDP *:68
sshd 3593 root 3u IPv4 46753 0t0 TCP *:22 (LISTEN)
dhclient 4769 root 7u IPv4 39641 0t0 UDP *:68
dhclient 4943 root 7u IPv4 40502 0t0 UDP *:68
nc 5491 root 3u IPv4 44900 0t0 TCP *:23 (LISTEN)

root@bogon:~# ifconfig eth1
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 1881 bytes 244959 (239.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2006 bytes 665508 (649.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@bogon:~#
```

二、工具基本使用方法



The screenshot shows a terminal window titled 'kaliGateway [正在运行] - Oracle VM VirtualBox'. The user is root@bogon. The terminal displays the output of the 'python scan.py' command, which shows a welcome message and the usage of the 'PORT SCAN' tool. The user enters 'help' to see the usage instructions, which include the scan type and default destination IP and port.

```
root@bogon:~/share/网络安全实验/实验二# python scan.py

欢迎使用扫描工具PORT SCAN，需要帮助请输入help

>> help

PORT SCAN 1.0
Usage:[Scan Type][Destination Ip][Destination Port]
Scan Type:
    Choose the scan type.
    tcs : TCP connect scan
    tss : TCP stealth scan
    txs : TCP XMAS scan
    us  : UDP scan
Default:
    The default destination IP address is 127.0.0.1
    The default port is 80

>> exit
root@bogon:~/share/网络安全实验/实验二#
```

三、扫描关闭端口结果

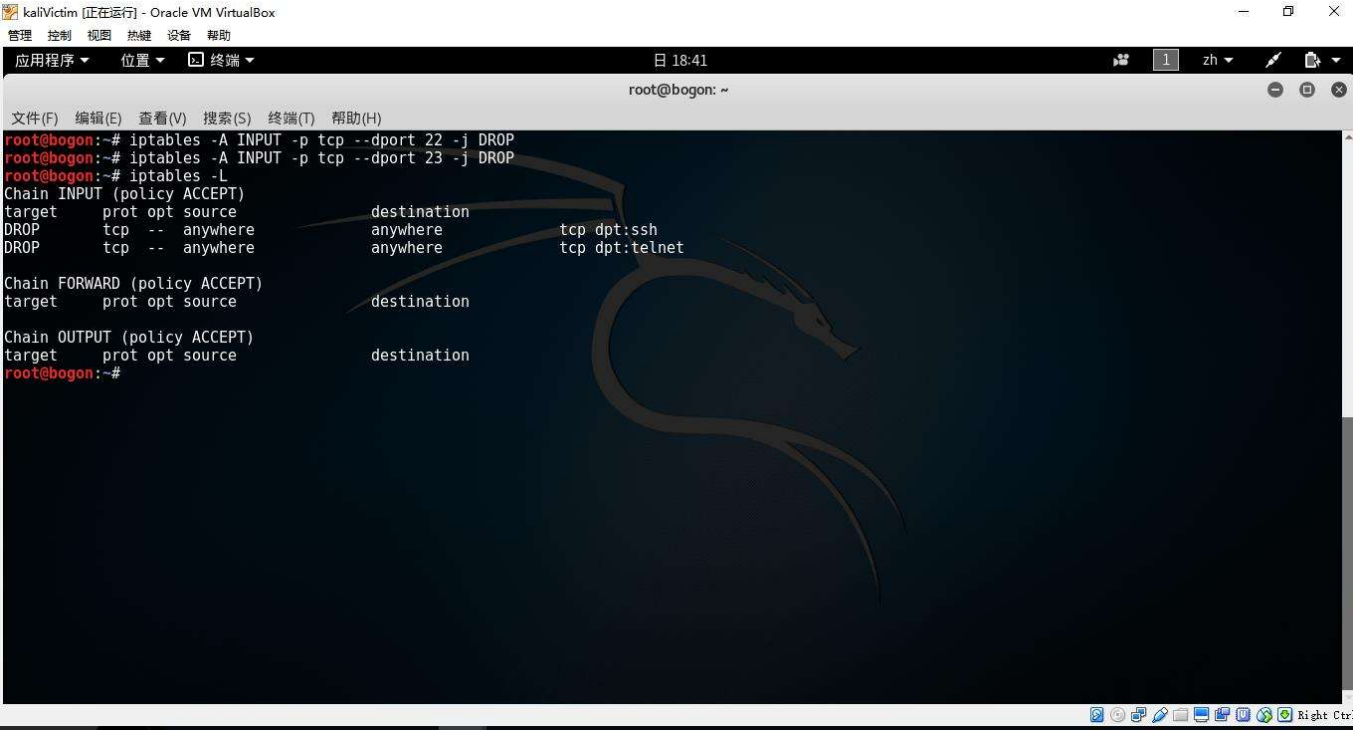


四、扫描开放端口结果



五、扫描添加过滤规则后端口情况

- 添加的过滤规则



• 扫描结果



六、代码

代码片段展示