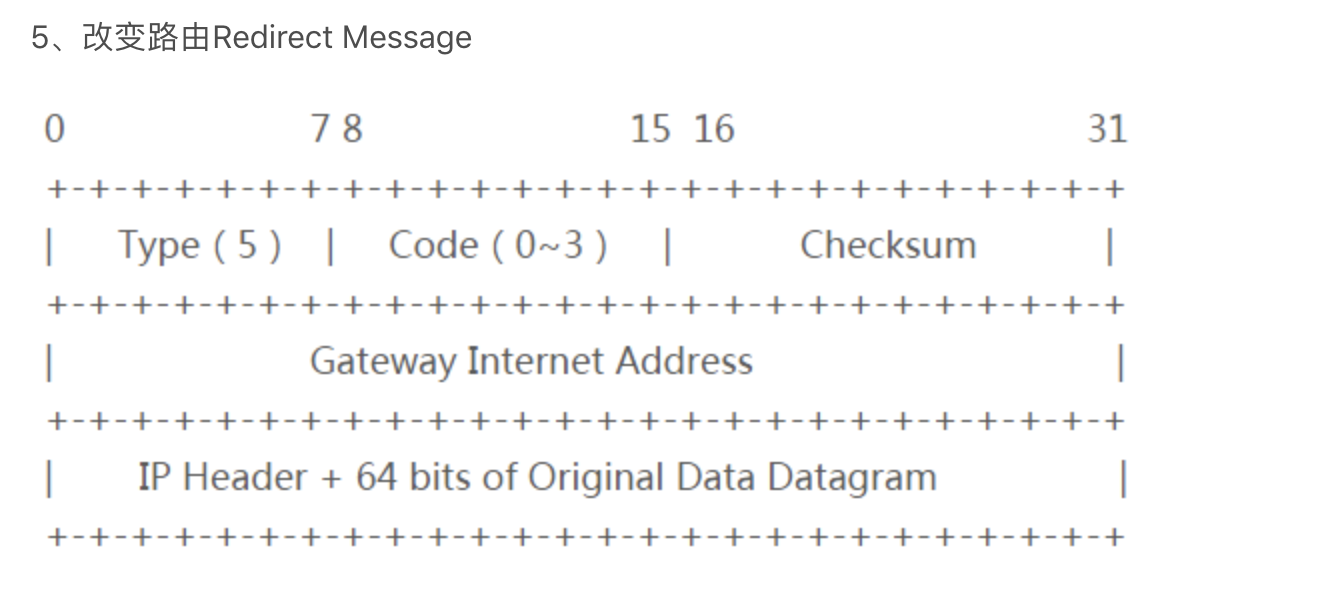
**lab[3]-report**

——57118207 魏宇萌

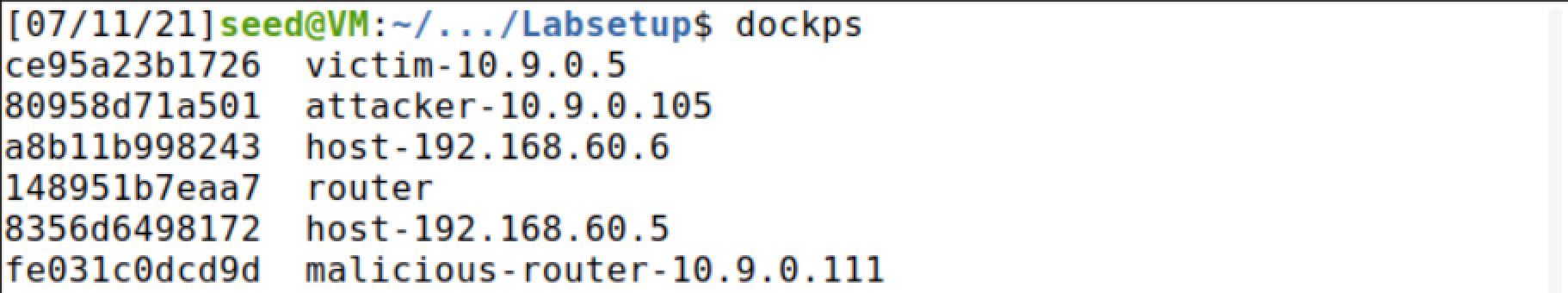
**Task 1**

（1）实验内容：实现ICMP redirect攻击

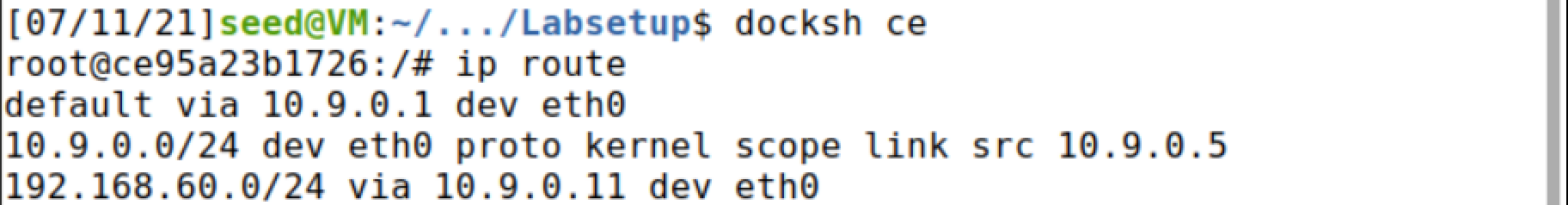
（2）代码：根据ICMP重定向报文和样例代码，确定ICMP type为5，ICMP code为0；redirect报文要从路由器发出才有可能被接收，所以根据container的配置，IP报文源地址为原路由10.9.0.11，IP报文目的地址为victim主机10.9.0.5，新路由为10.9.0.111；redirect报文的内容中为路由器接收到的报文内容，所以其源地址为victim主机10.9.0.5，目的地址为victim主机欲通信的主机192.168.10.5。



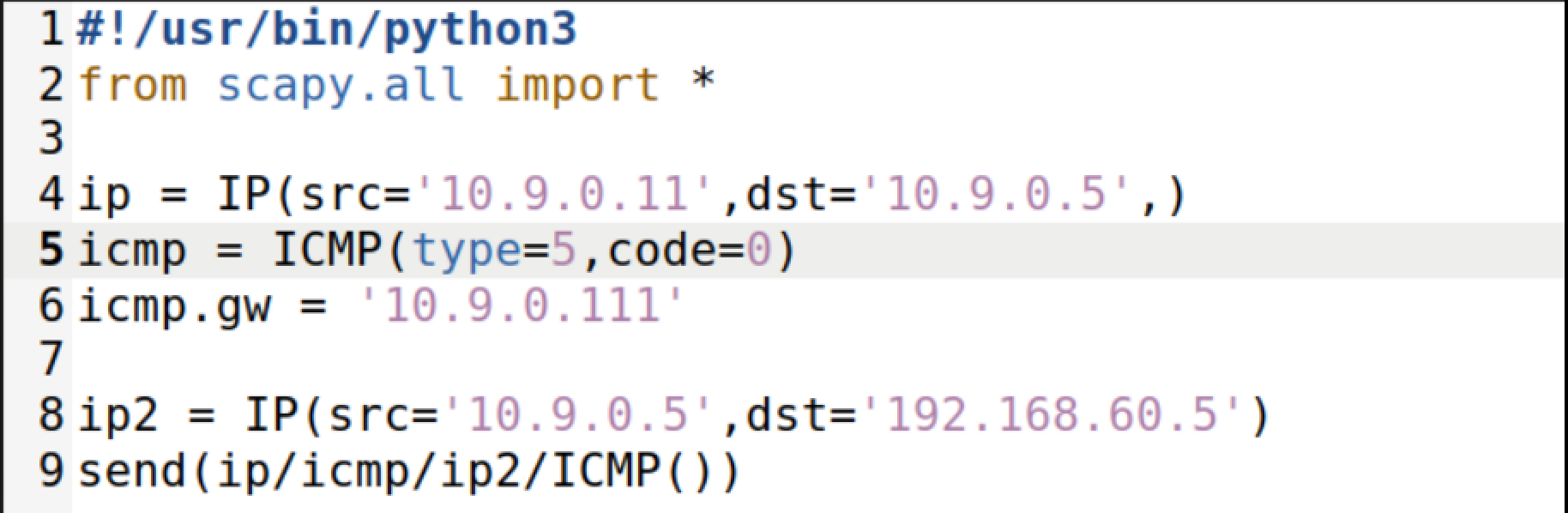
ICMP重定向报文格式



container配置信息

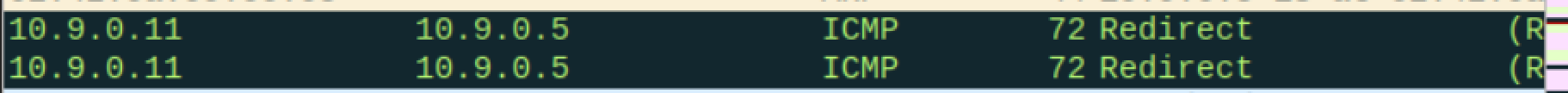


victim主机的路由信息

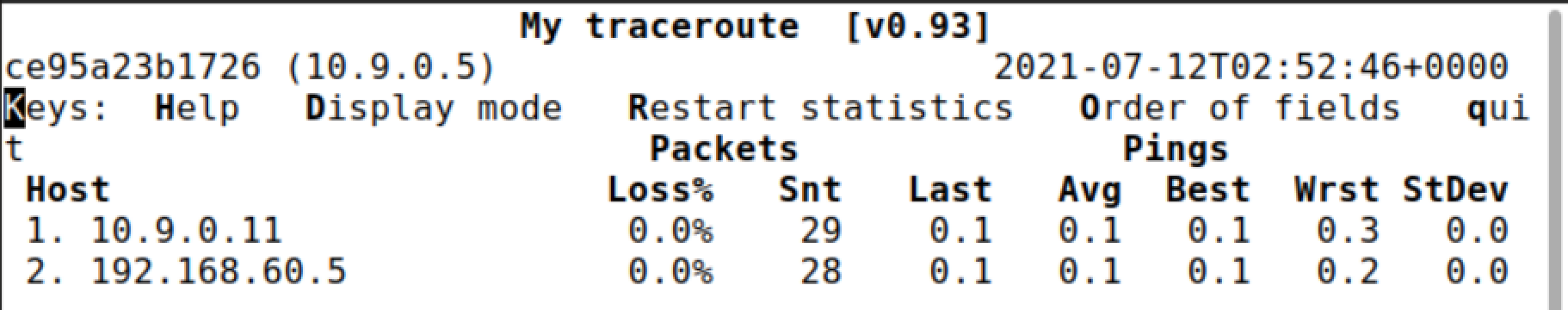


redirect.py

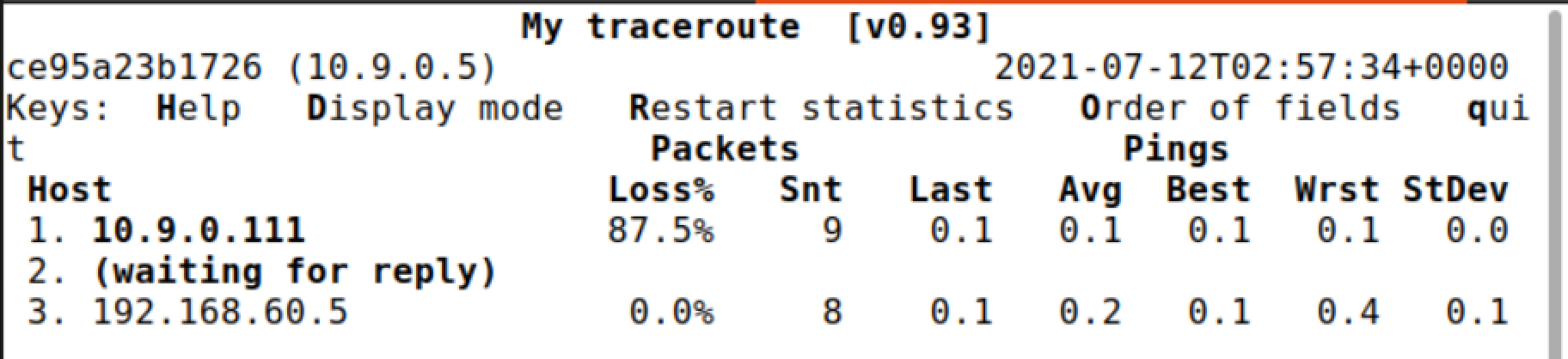
（3）程序执行情况：执行程序，发现伪造redirect报文成功发出，但当不ping 192.168.60.5时，ICMP redirect攻击无法成功；当ping 192.168.60.5时，ICMP redict攻击成功，前往192.168.60.0/24的路由被更改为10.9.0.111



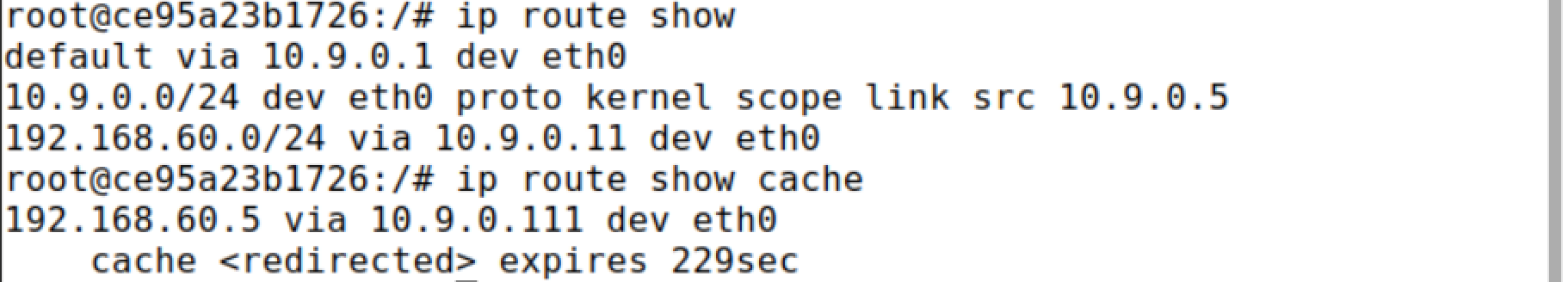
伪造的redirect报文发出



不ping 192.168.60.5时，ICMP redirect攻击失败



ping 192.168.60.5时，ICMP redirect攻击成功

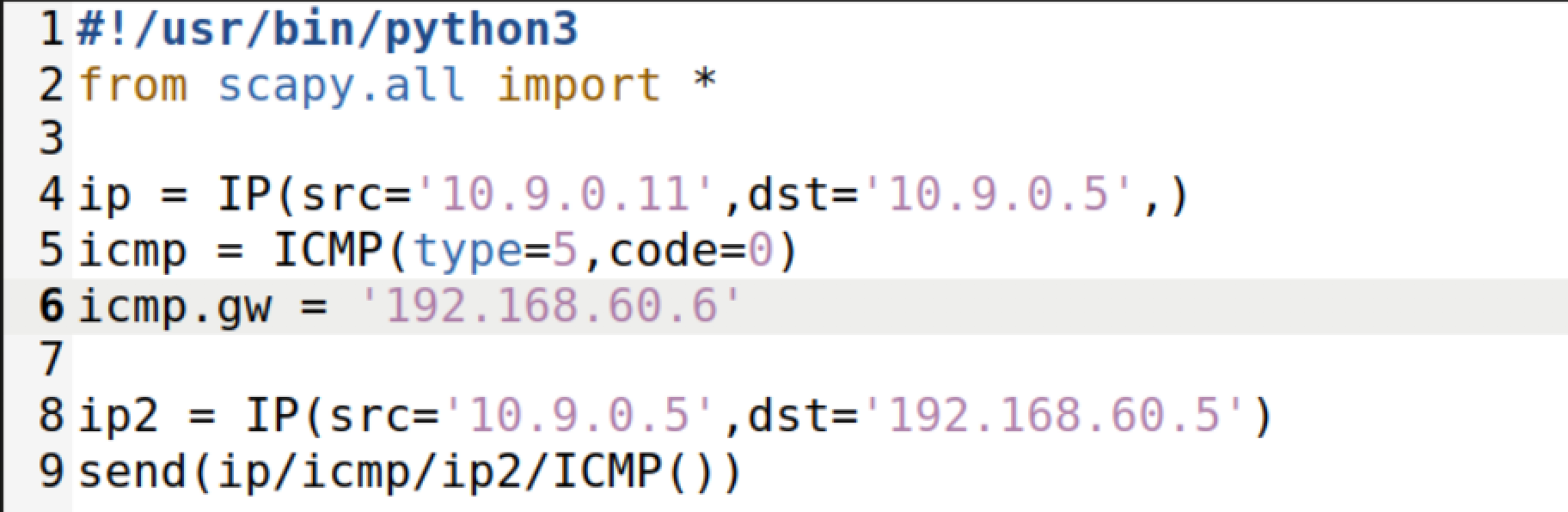


victim主机中路由cache中路由信息被更改

**Question 1**

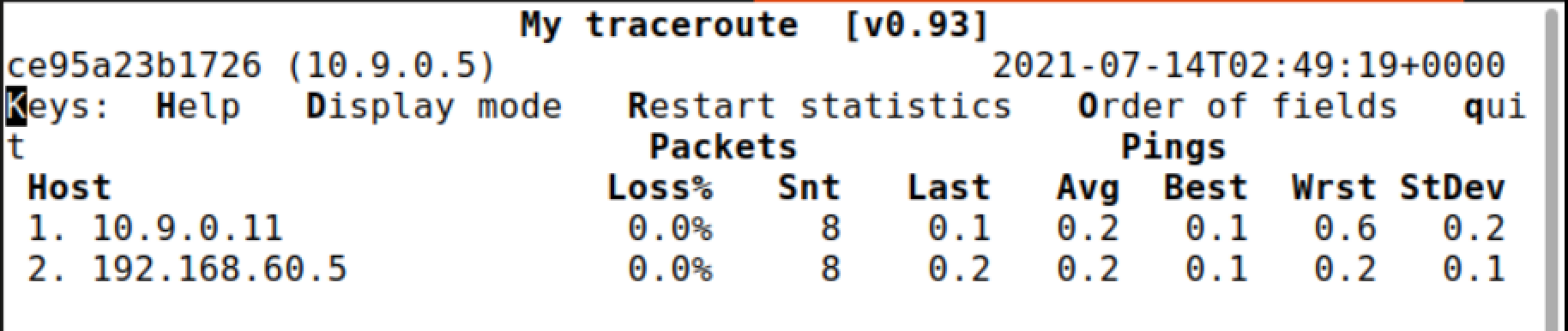
（1）实验内容：探究ICMP redirect攻击是否可以将路由redirect到非本网段的IP地址。

（2）代码：将路由redirect到非本网段的主机192.168.60.5。

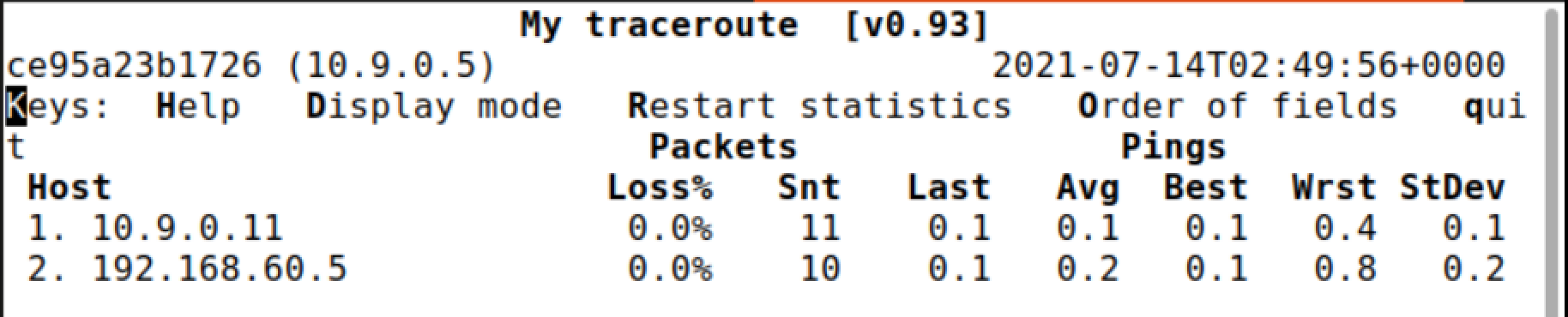


redirect.py

（3）程序执行情况：先不执行程序，查看到主机192.168.60.6的路由，路由器为10.9.0.11；再在ping 192.168.60.5的同时执行程序，查看到主机192.168.60.6的路由，路由器仍然为10.9.0.11，证明ICMP redirect攻击不可以将路由redirect到非本网段的IP地址上。

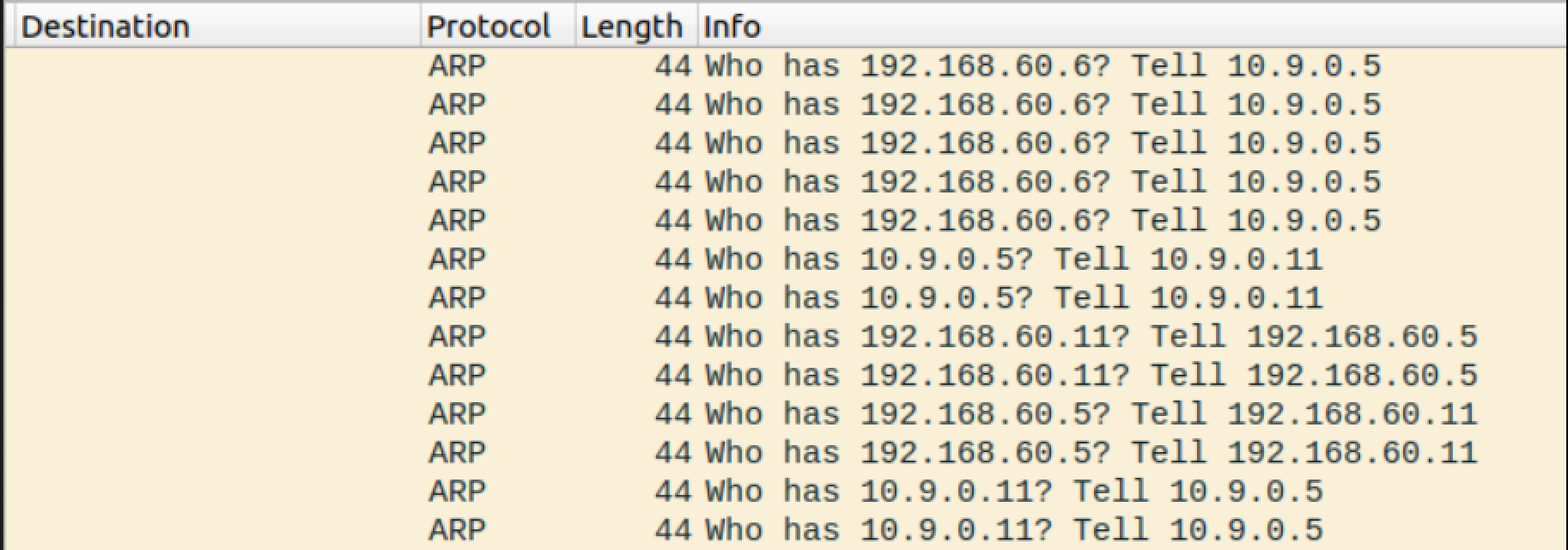


未执行程序前路由情况



程序执行后路由不变

（4）原因：通过Wireshark发现，伪造的redirect报文发出后，victim主机收到该报文后会ARP重定向的路由的MAC，但无回应，便会再ARP原来路由的MAC。通过程序执行情况知victim主机的路由未发生改变，而且查看routing cache，并没有重定向项。所以，victim主机接收到redirect报文后，先ARP新路由MAC，未发现新路由MAC后，不更新routing cache，则路由情况不会发生改变。

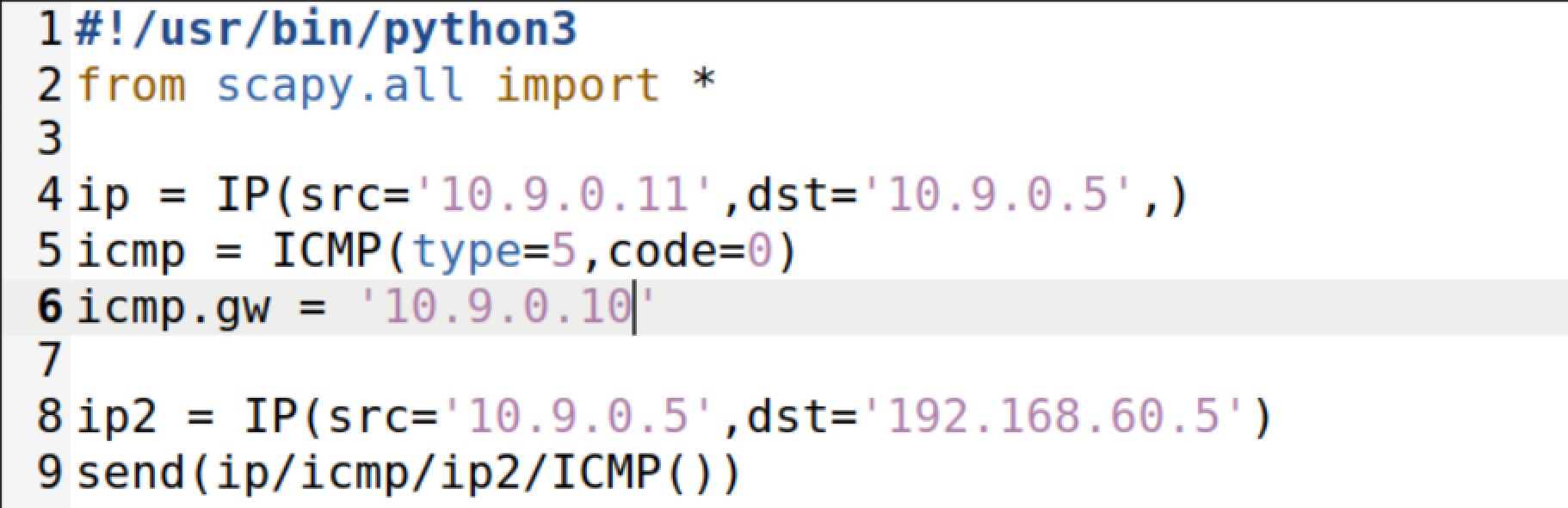


victim主机接收到redirect报文后ARP信息

**Question 2**

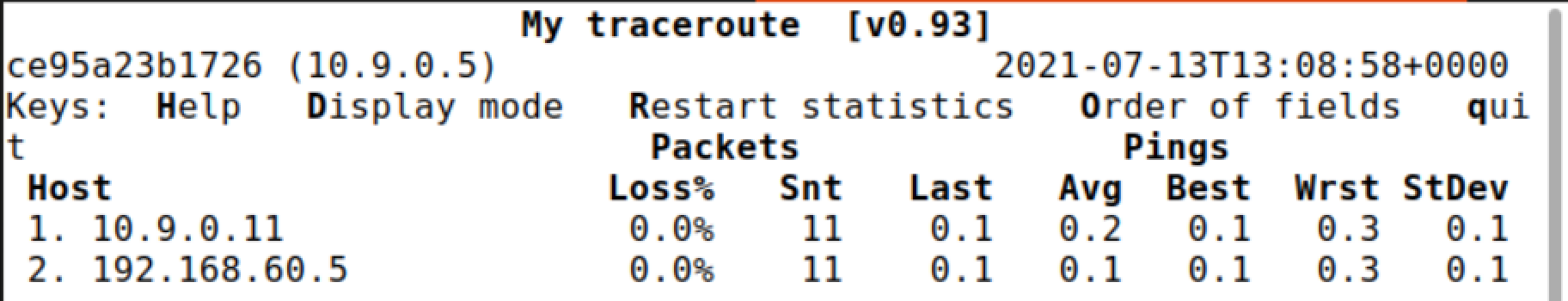
（1）实验内容：探究ICMP redirect攻击是否可以将路由redirect到本网段不存在或下线的IP地址。

（2）代码：将路由redirect到本网段不可达的主机10.9.0.10。



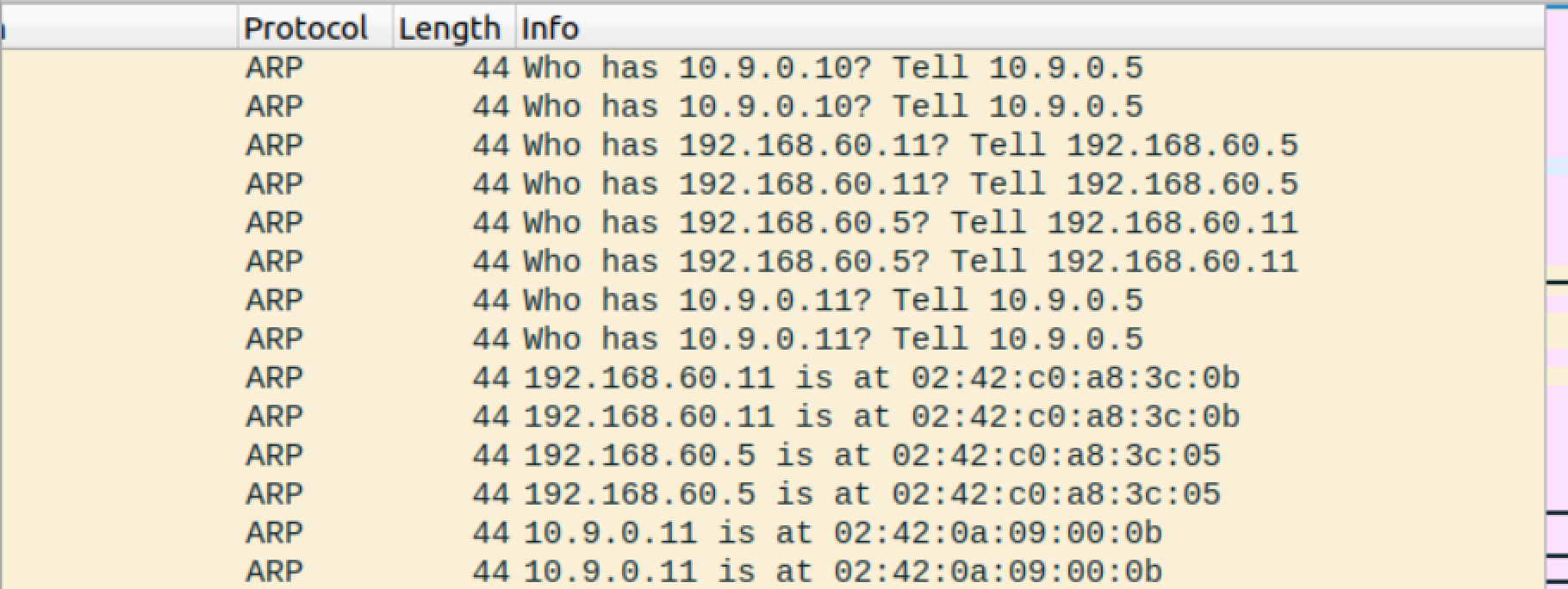
redirect.py

（3）程序执行情况：在ping 192.168.60.5的同时执行程序，查看到主机192.168.60.5的路由，路由器仍然为10.9.0.11，证明ICMP redirect攻击不可以将路由redirect到本网段不存在的IP地址上。



程序执行后路由不变

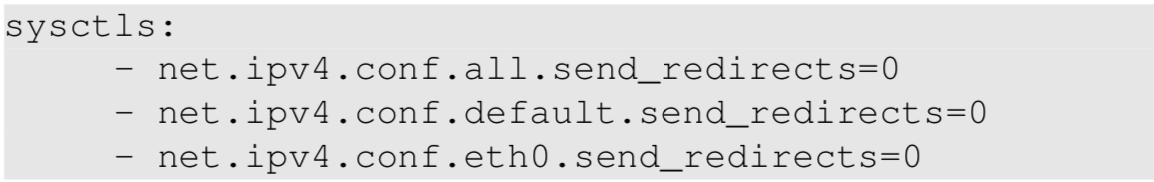
（4）原因：与Question 2的情况相同。通过Wireshark发现，伪造的redirect报文发出后，victim主机收到该报文后会ARP重定向的路由的MAC，但无回应，便会再ARP原来路由的MAC。通过程序执行情况知victim主机的路由未发生改变，而且查看routing cache，并没有重定向项。所以，victim主机接收到redirect报文后，先ARP新路由MAC，未发现新路由MAC后，不更新routing cache，则路由情况不会发生改变。



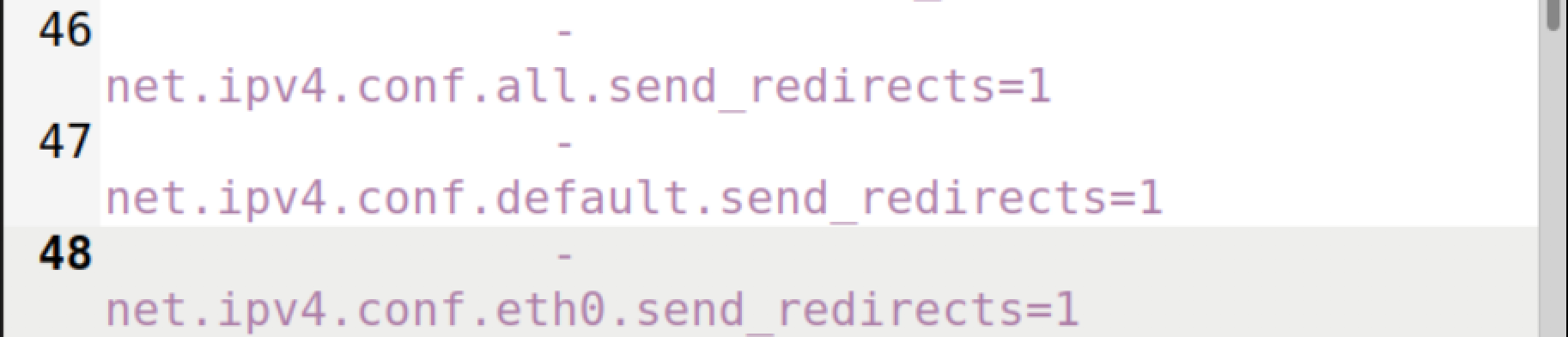
victim主机接收到redirect报文后ARP信息

**Question 3**

（1）实验内容：探究下列配置的意义，以及将这些配置值改为1对ICMP redirect攻击的影响。

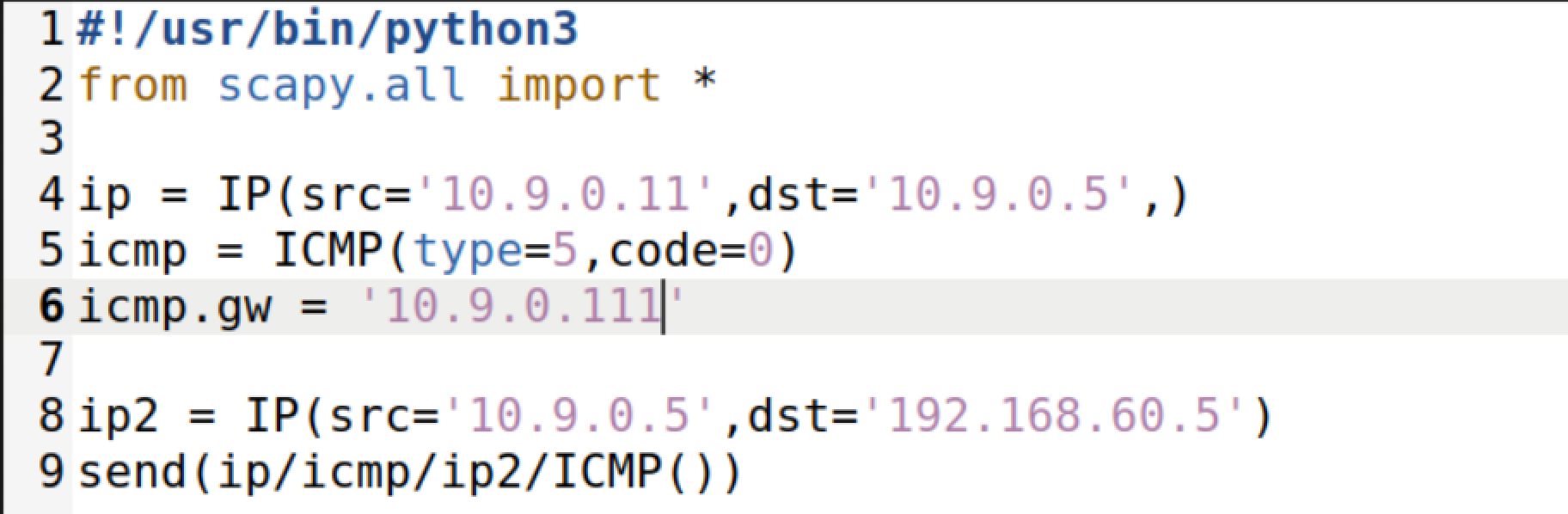


需要修改的配置



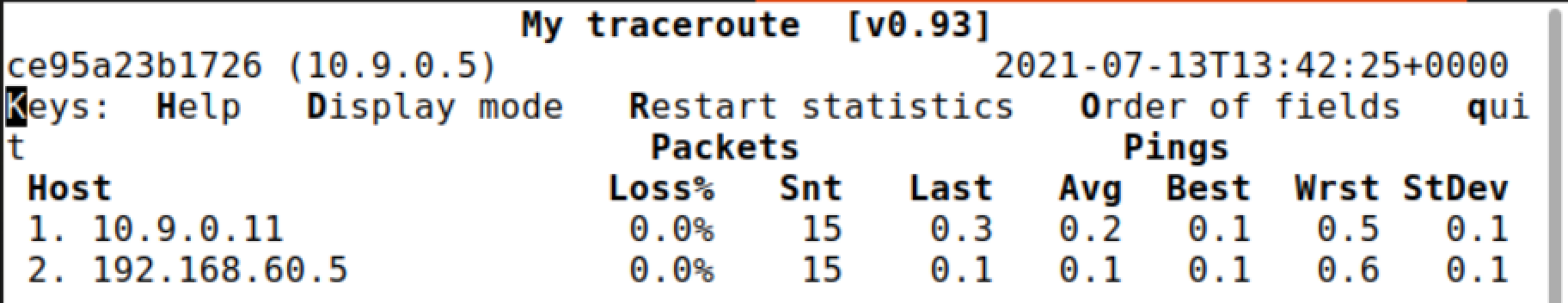
修改后的配置

（2）代码：与Task 1的代码相同，redirect路由为malicious router 10.9.0.111。



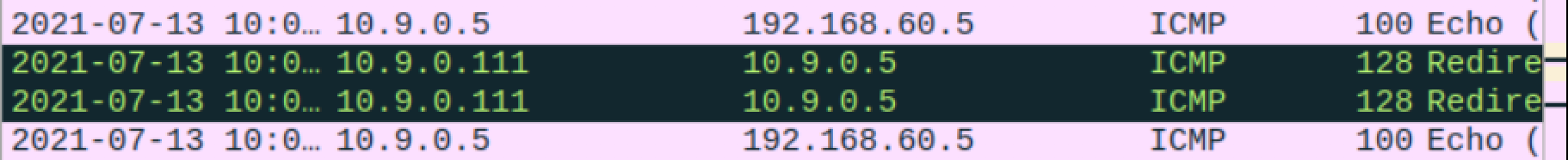
redirect.py

（3）程序执行情况：在ping 192.168.60.5的同时执行程序，查看从victim主机到目标主机192.168.60.5的路由，路由器仍然为10.9.0.11，证明改变配置值为1后，ICMP redirect攻击失败。



程序执行后路由不变

（4）原因：上述配置意为是否允许主机发送重定向报文的设置，设置值为0是不允许，设置值为1是允许。通过Wireshark抓包发现，流量中不仅有伪造的redirect报文，当victim主机查看到192.168.60.5主机的路由时，还有 malicious router发给victim主机的redirect报文，该报文通知victim主机又恢复了正确的路由，而在配置设置值为0时该报文是不存在的。所以，由于malicious router并不是192.168.60.0/24网络的默认路由，在配置设置值为1的情况下，当有其他主机将malicious router当作通往192.168.60.0/24网络的默认路由时，malicious router会向该主机发送redirect报文以告知其正确的路由，这样ICMP redirect攻击就会失败。



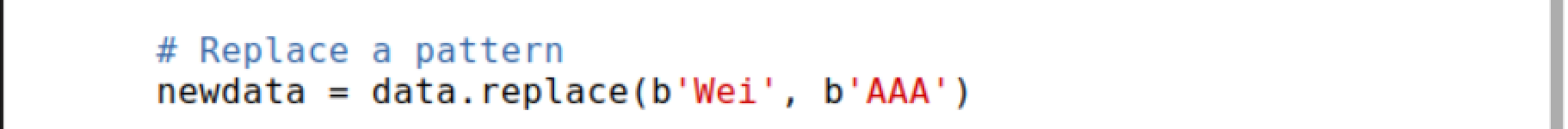
malicious router发送的redirect报文

**Task 2**

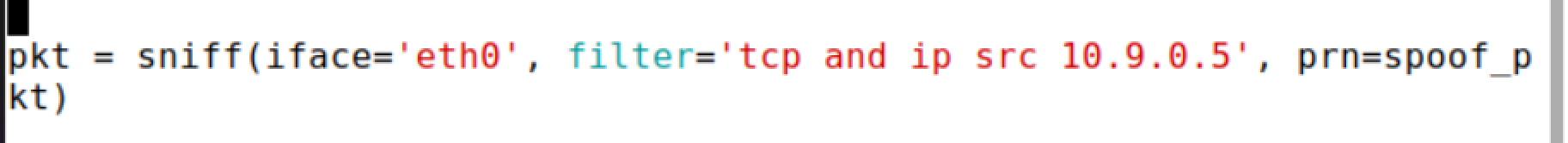
（1）实验内容：基于ICMP redirect攻击成功的结果，借用malicoius router实现MITM。

（2）代码与程序执行情况：首先要先实现ICMP redirect攻击，将中间路由变为malicoius router（注意：redirect报文改变routing cache，cache项有时长限制，应在有效时长内进行接下来的攻击）。

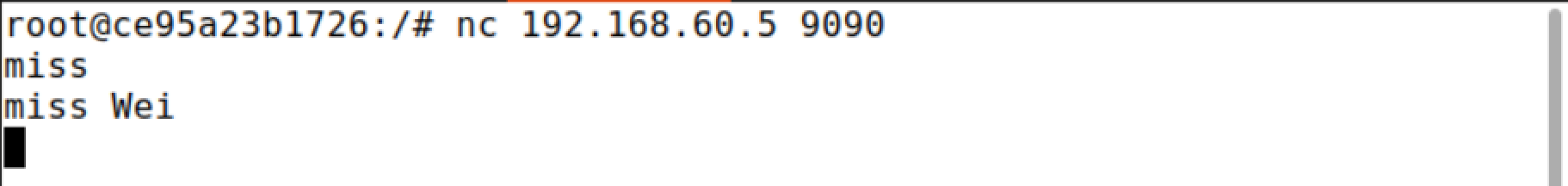
然后修改示例代码中的模式替代段，再修改filter以提高报文效率，先在filter中使用IP。从victim主机向目标外网主机发送信息，发现模式Wei被正确替换为AAA，证明MITM成功。但是进程开始无止尽发送报文，这是因为无论是原报文还是经MITM替换过的报文，其源IP都是victim主机，filter反复嗅探到原报文和经MITM替换过的报文，所以会不停的发送报文。



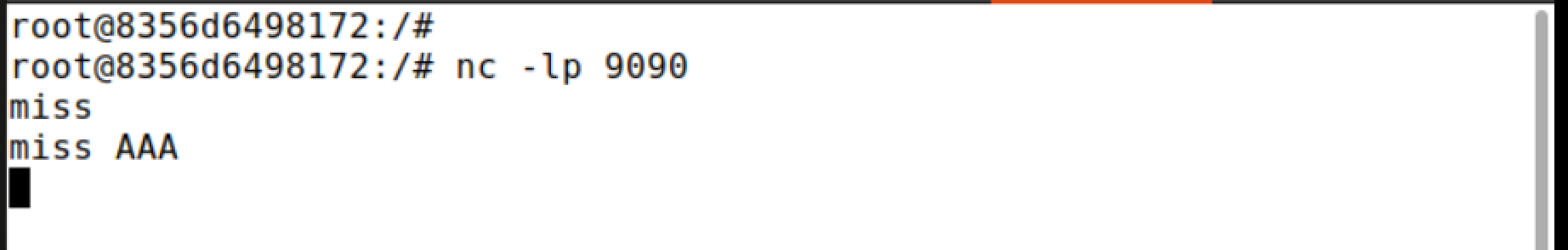
模式替代段



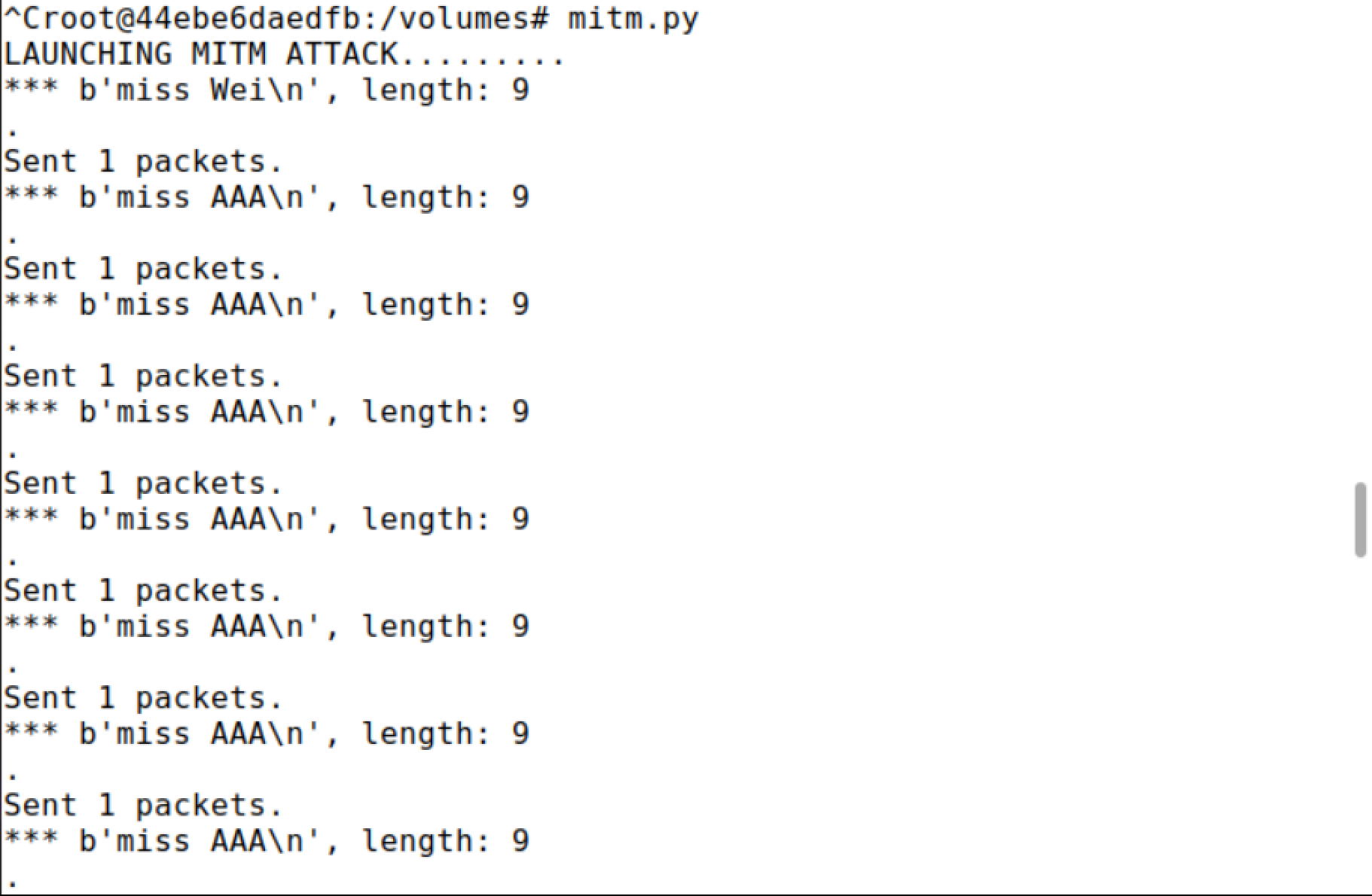
使用vicm主机IP的filter



victim主机发送信息

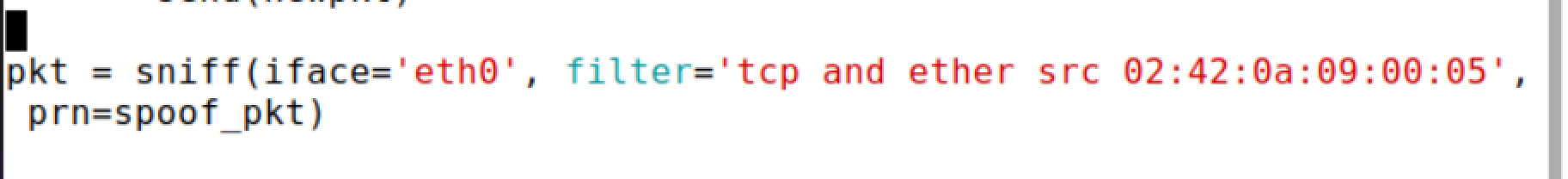


目标主机接收到被替换的信息

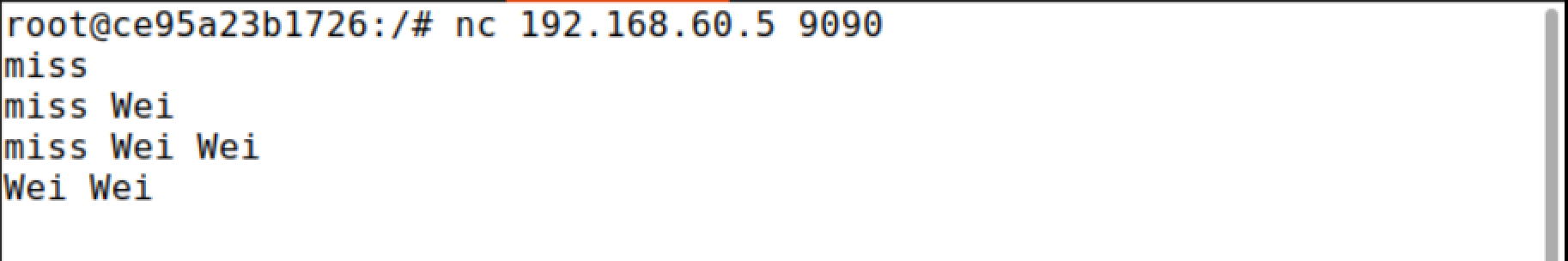


进程不断发送报文

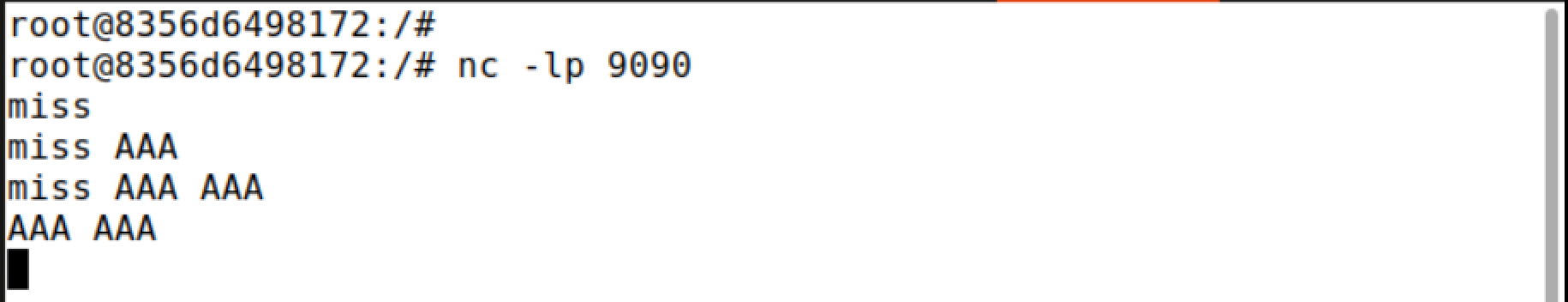
在filter中使用MAC地址，从victim主机向目标外网主机发送信息，发现模式Wei被正确替换为AAA，证明MITM成功，而且进程每次只发送一个报文，是正确的情况。这是因为，经MITM替换的报文的MAC地址是malicoius router的MAC地址，而非victim主机的MAC地址。



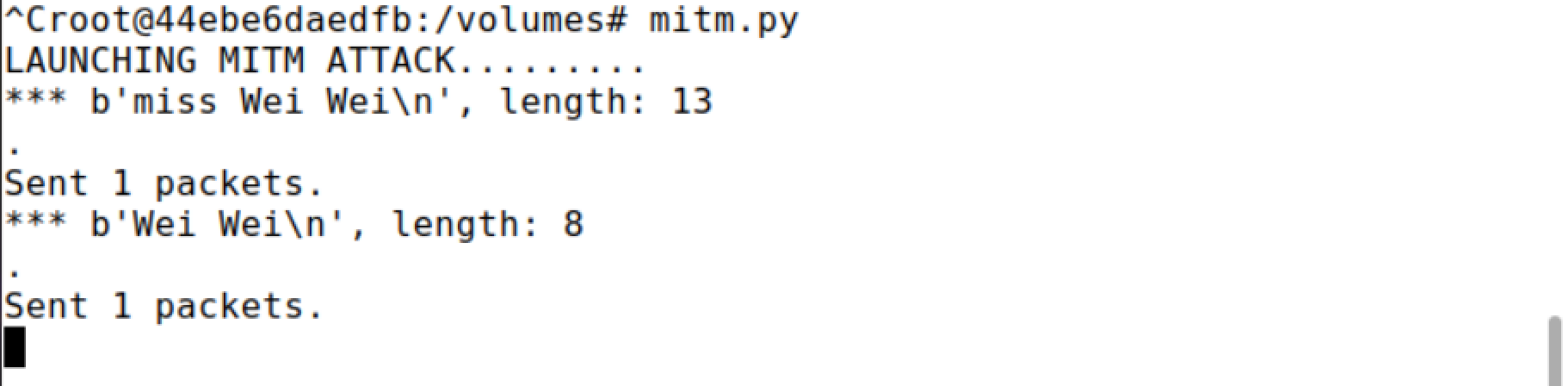
使用victim主机MAC地址的filter



victim主机发送信息



目标主机接收到被替换的信息

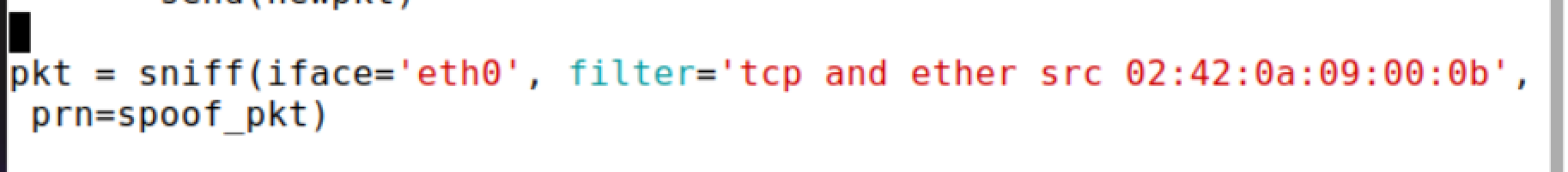


进程每次只发送一个报文

**Question 4**

（1）实验内容：探究MITM中应捕获哪一方向的数据报文。

（2）代码：使用目标主机MAC地址的filter，即捕获来自目标主机192.168.60.5发送的报文。

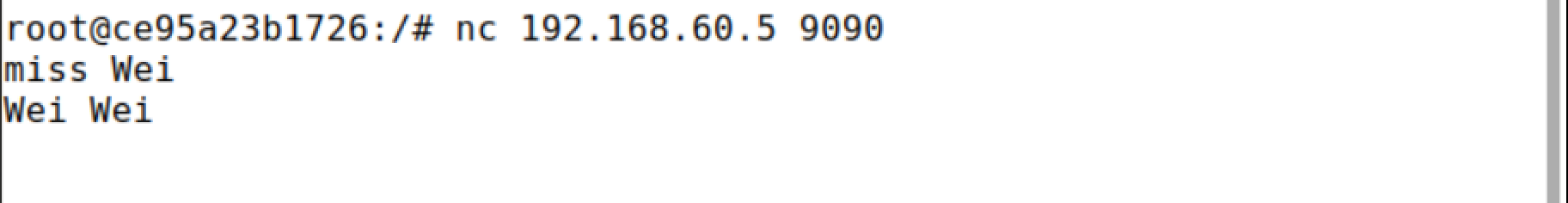


使用目标主机MAC地址的filter

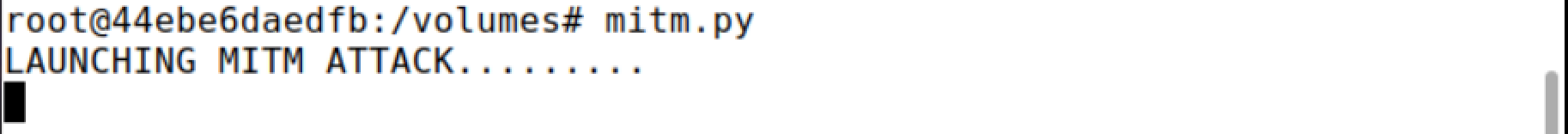
（3）程序执行情况：从目标主机192.168.60.5向victim 主机发送第一条信息miss Wei，victim 主机收到该消息，但进程并没有捕获到该报文。从victim 主机向目标主机192.168.60.5发送第二条信息Wei Wei，目标主机并没有收到该消息，因为malicous router配置被修改，并不会自动转发该报文，而且因为filter此报文不会被处理。



目标主机信息情况

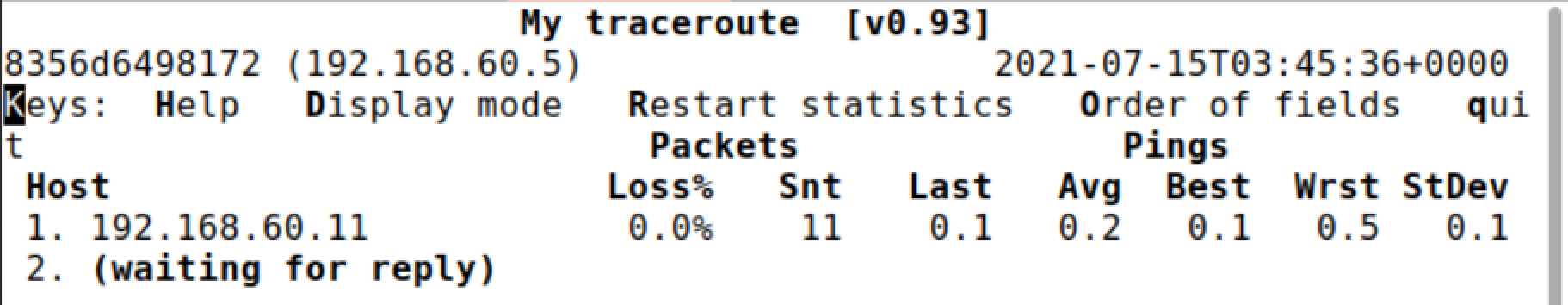


victim主机信息情况



进程执行情况

（4）MITM中应捕获从victim 主机方向来的报文，因为ICMP redirect攻击改变的是victim 主机的路由，没有更改目标主机的路由，从目标主机发送出的报文不可能是也不会经过malicious router。



目标主机路由并非malicious router

**Question 5**

如Task 2所示，使用victim主机的MAC地址是正确的做法，因为victim主机发送的报文和malicious router发送的报文具有相同的源IP地址，而MAC地址不同。