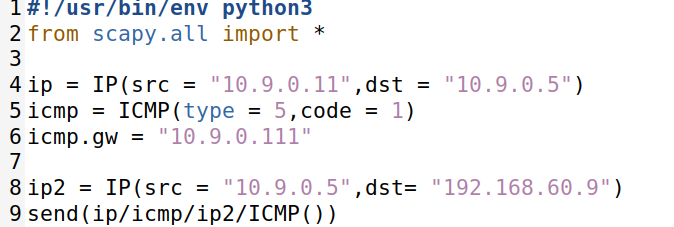
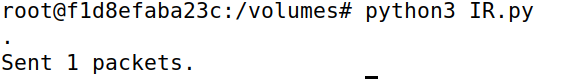
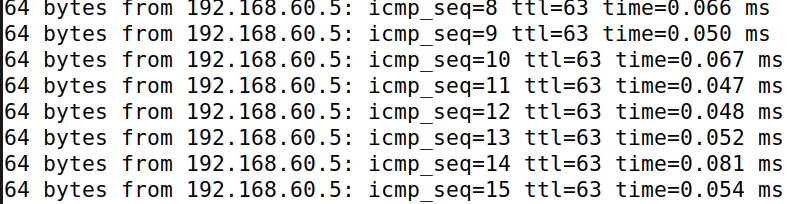
Task1

将py文件补充完整

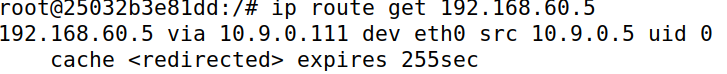


在受害者容器中ping192.168.60.5，同时在攻击者容器中运行以上代码



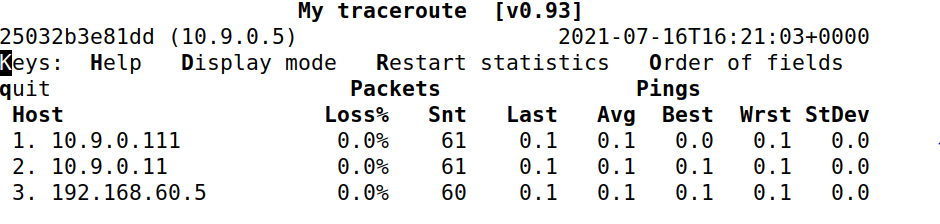


在受害者容器中查看，发现被重定向了



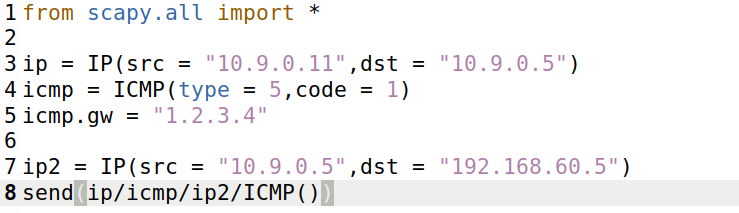
多了一条host





Q1

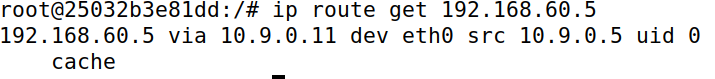
将icmp.gw 改成外网网关



Flush后重新ping

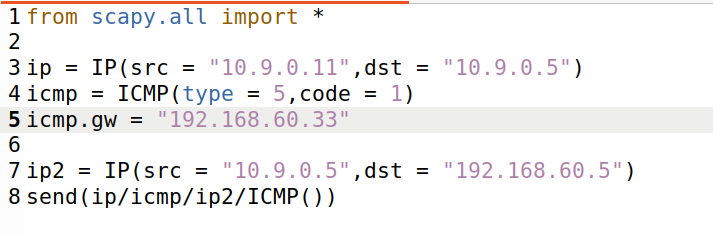


运行后在受害者容器中发现并没有被重定向

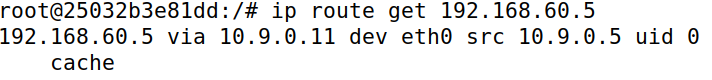


Q2

将icmp.gw改成内网不存在的地址

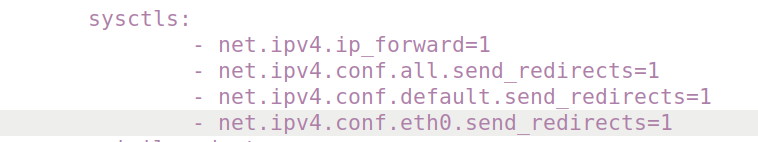


重复Q1中操作，发现并没有被重定向



Q3

将以下值置1

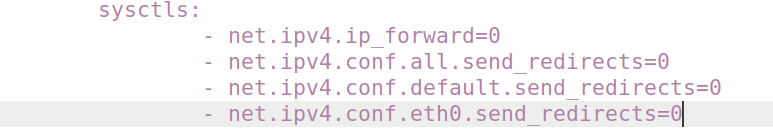


重复之前的操作 然后发现攻击失败

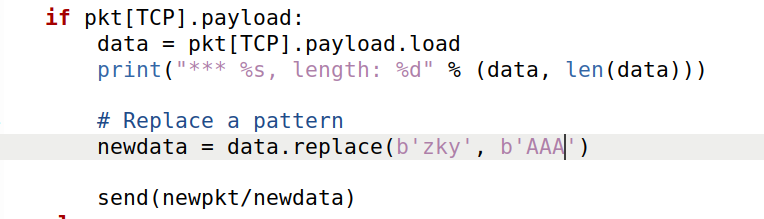
Task2

Q4

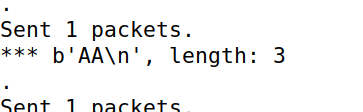
先关掉恶意路由的转发



代码修改成名字

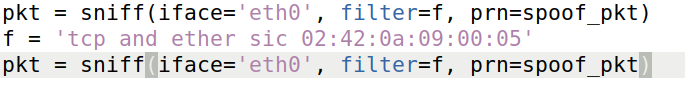


先重定向路由，在恶意路由上运行程序，在受害者容器中跟192.168.60.5nc连接，发送“zky”，发现被替换为“AAA“



Q5

将filter改成victim的MAC地址，添加筛选条件



再重复上述实验发现恶意路由运行时发的包减少，而且不会接收自己发的包