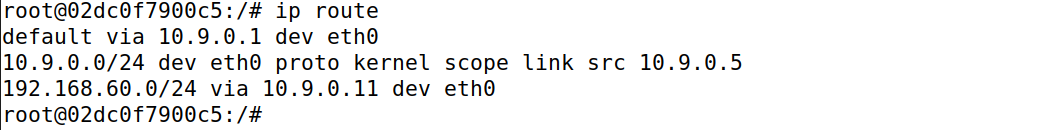
Lab3

57118111王雯

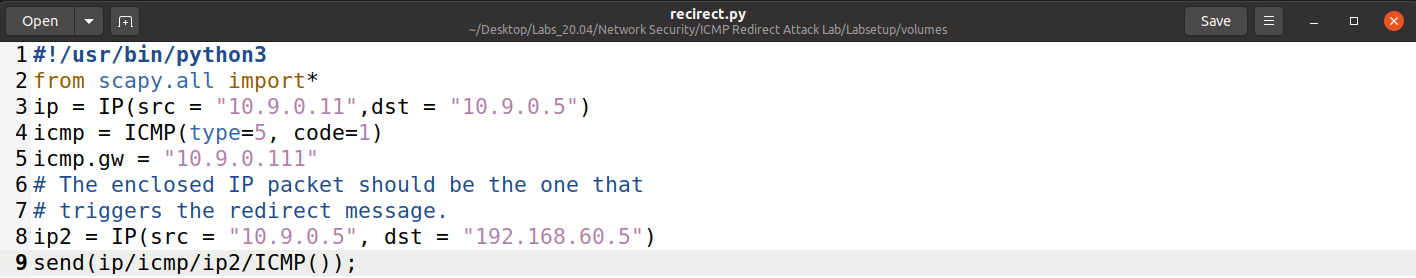
Task 1: Launching ICMP Redirect Attack

代码实现：

（1）使用IP route命令查看受害者主机的路由器：



攻击代码如下：

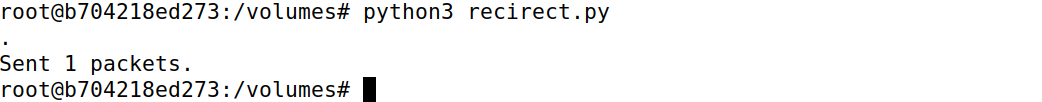


（2）进行重定向攻击

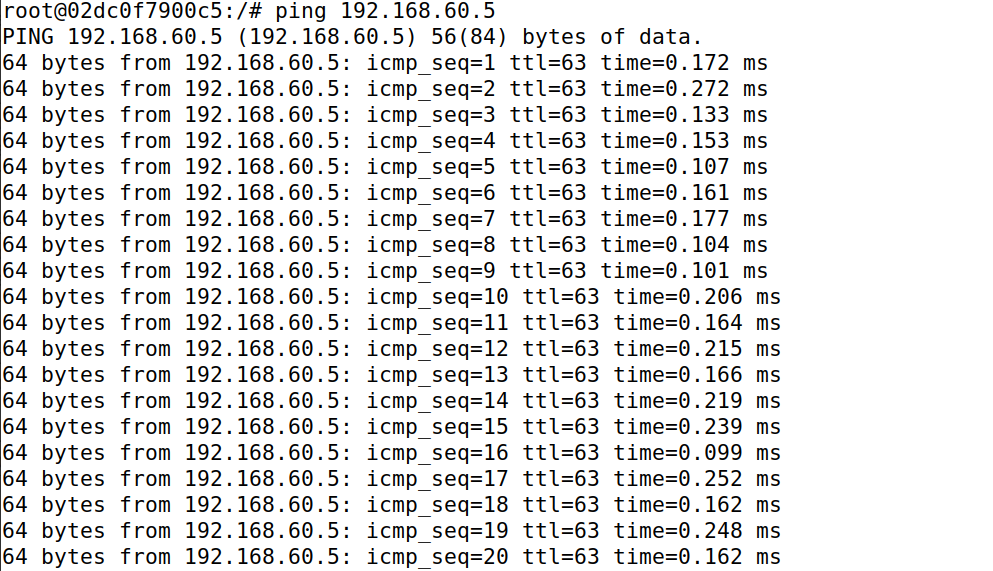
在发起攻击之前，在被攻击主机中ping 192.168.60.5，然后在攻击主机中

执行攻击程序。

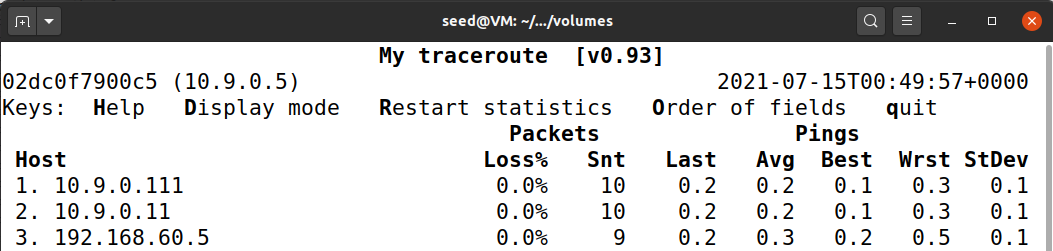
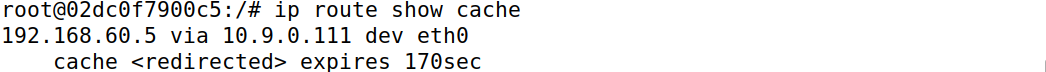
攻击者的输出：



受害者的输出：



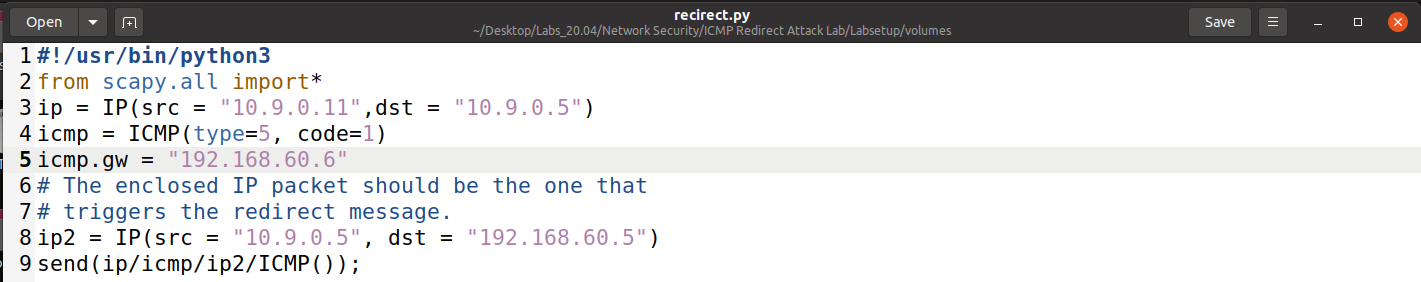
使用ip route show cache命令查看攻击后的路由缓存：发现发送至192.168.60.5 的数据包的网关已经被重定向为恶意路由器地址。



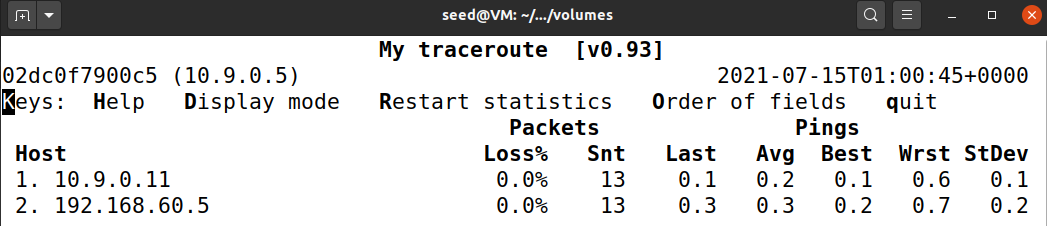
（3）问题回答

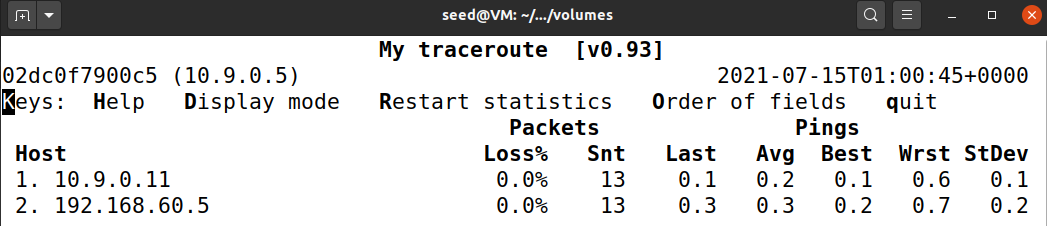
问题1:可以使用ICMP 重定向攻击重定向到远程机器吗？也就是说，分配给icmp.gw 的IP 地址是一台不在本地局域网上的计算机。

答：将icmp.gw改为192.168.60.6，重新运行查看



重新运行，运行后发现没有产生路由缓存。

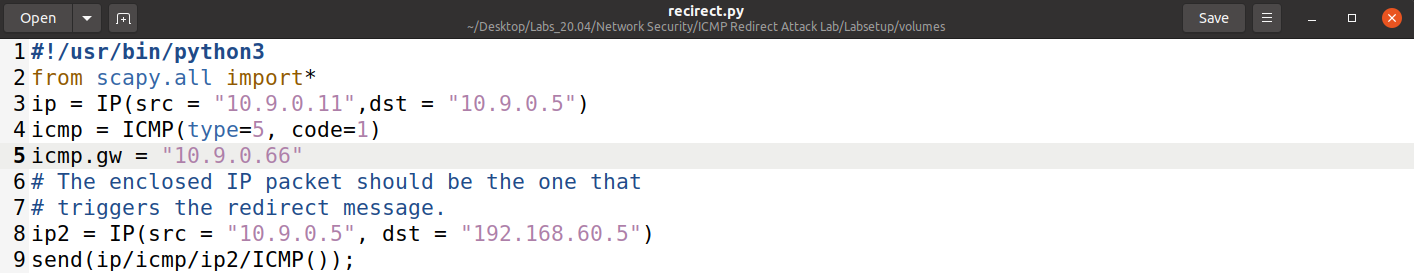


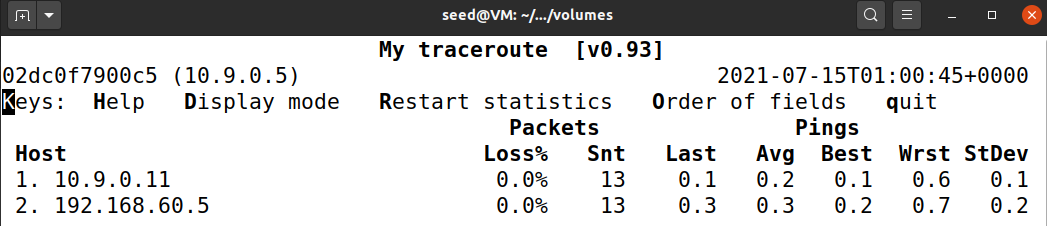


问题2:您可以使用ICMP 重定向攻击来重定向到同一网络上不存在的机器吗？也就是说，分配给icmp.gw 的IP 地址是脱机或不存在的本地计算机。

答：将icmp.gw 修改为不存在的本地地址10.9.0.66,结果与第一个问题的

实验结果相同，无法重定向。由于无法到达该地址，无法作为网关，所以无法重定向

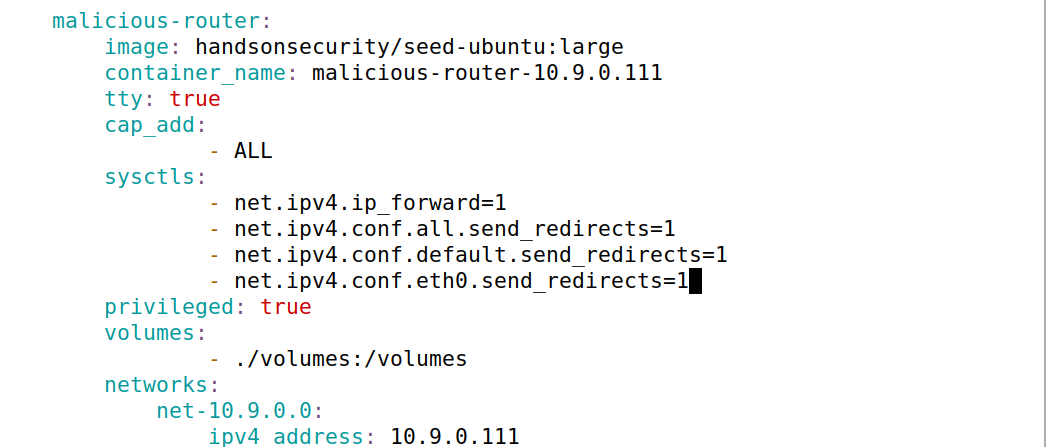






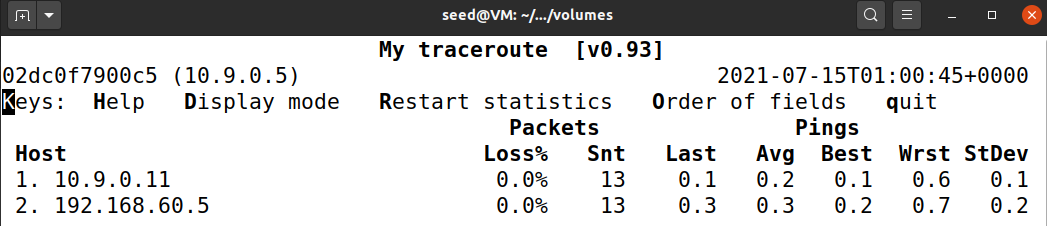
问题3:如果您查看docker-compose.yml 文件，您会发现恶意路由器容器的以下条目。这些条目的目的是什么？请将它们的值更改为1，然后再次发起攻击。请描述并解释你的观察。

答：将与重定向有关的三个参数的值设置为1



重启docker。重新攻击，进行重定向攻击，发现重定向失败

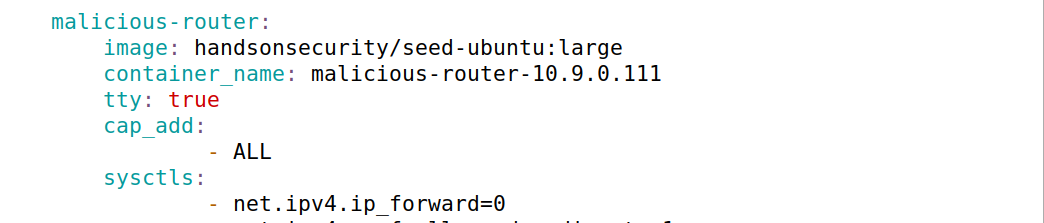




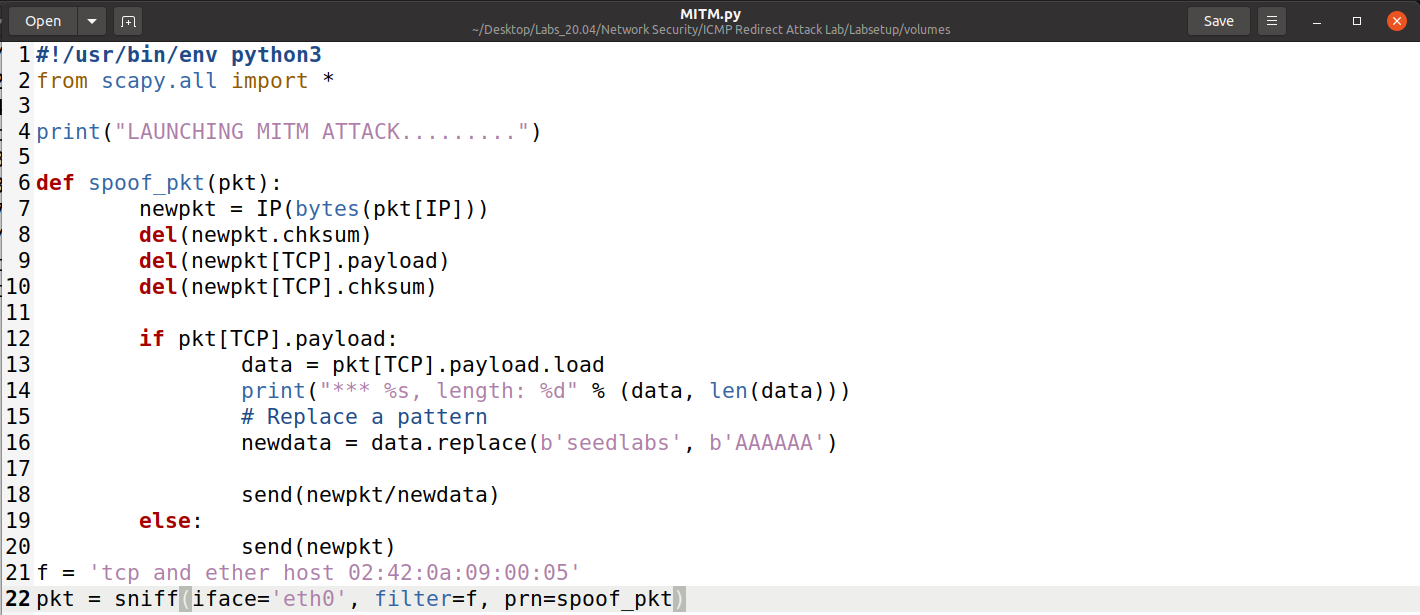
Task 2: Launching the MITM Attack

（1）中间人攻击

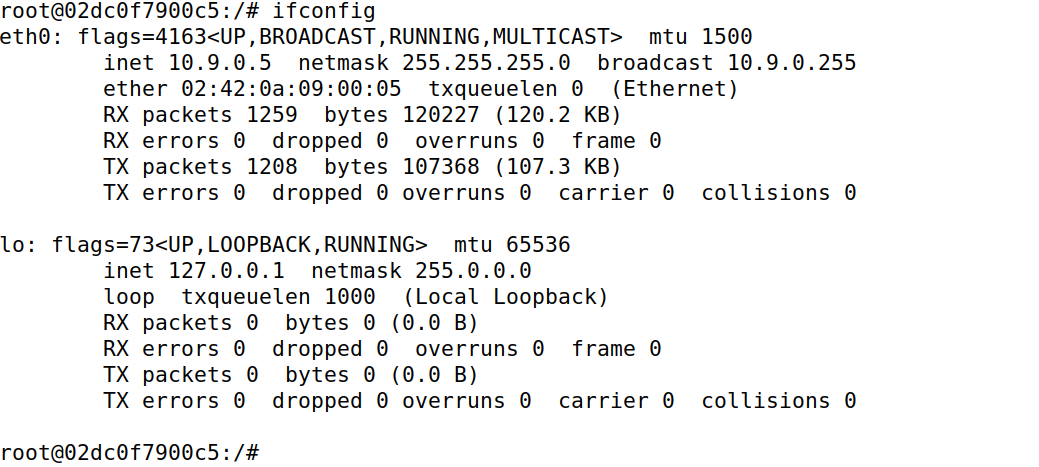
首先，恶意路由上禁用IP转发



重启docker。在重定向的基础上，在恶意路由上执行MITM攻击程序，受害者主机和目的主机进行TCP连接。MITM攻击代码如下：

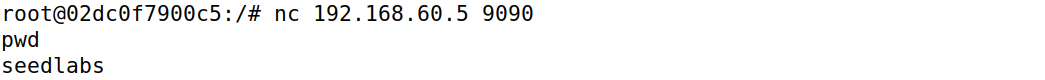


受害者的主机的MAC地址可以通过ifconfig查看：

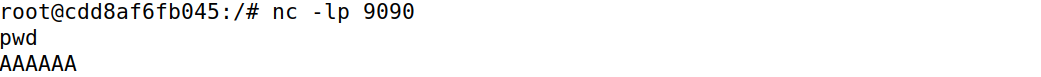


执行程序后被攻击主机、目的主机以及恶意路由器输入输出分别如下：

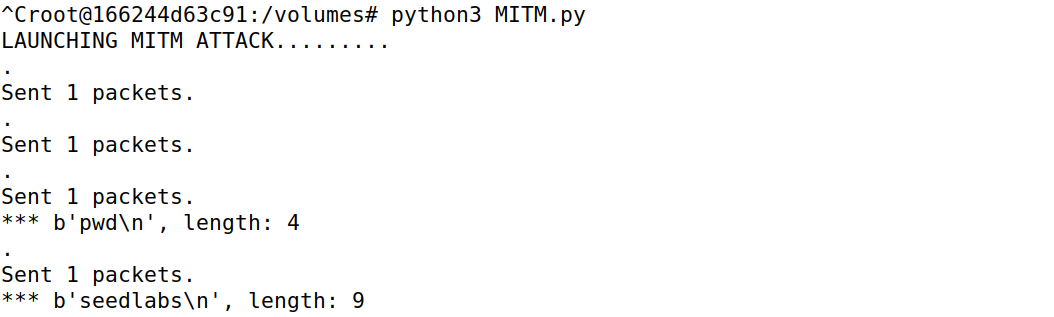
受害者主机：



目的主机：



恶意路由器：



（2）问题回答

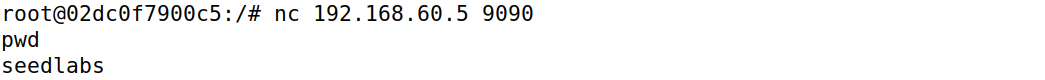
问题4:在你的MITM 计划中，你只需要捕捉一个方向的流量。请指出哪个方向，并解释原因。

答：在MITM程序中，只需要捕捉去往目的主机，即192.168.60.5的流量，因为这个方向的流量上有携带了受害者主机输入数据的报文

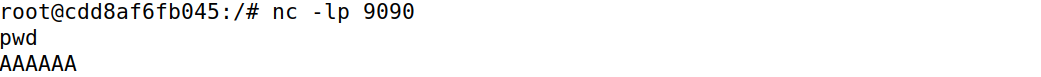
问题5:在MITM 程序中，当您从A (10.9.0.5)捕获nc 流量时，您可以在过滤器中使用A 的IP 地址或MAC 地址。其中一个选择不好，会产生问题，尽管两个选择都可能奏效。请两者都试一试，用你的实验结果来说明哪个选择是正确的，并请解释你的结论。

答：首先将过滤器改为tcp and src host 10.9.0.5，重新运行并进行tcp连接后，结果如下

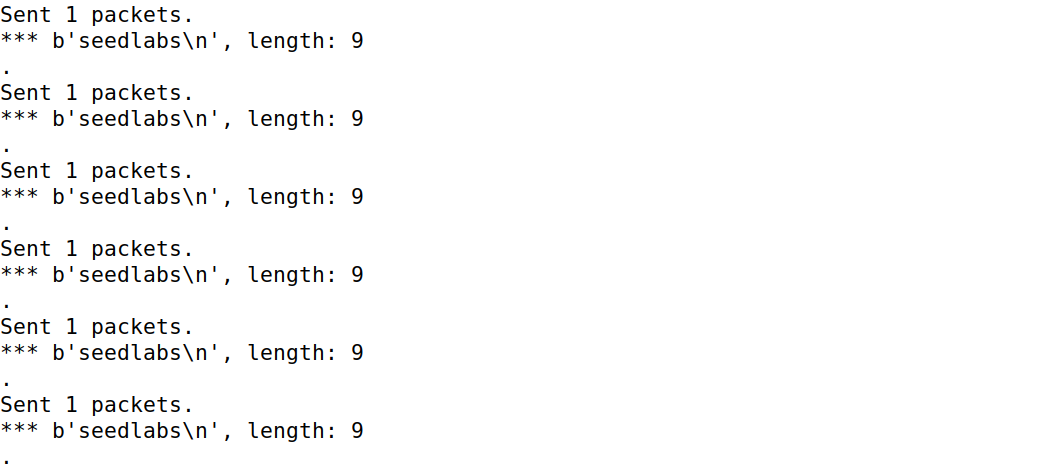
受害者主机：



目的主机：



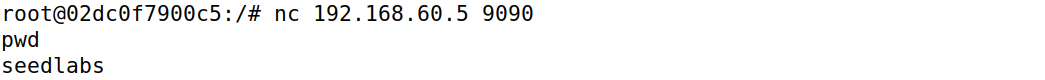
恶意路由器：



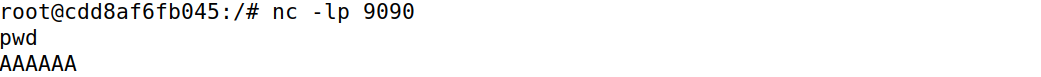
可以发现攻击可以正常进行，“seedlabs”字符串被成功替换。但是我们也发现了问题，前面我们使用mac 地址过滤时，我们每发送一行信息，恶意路由器也发送一个数据包，但是使用ip 地址过滤时，恶意路由器会不停地发送数据包，这会浪费我们的性能

再将过滤器改为tcp and ether src 02:42:0a:09:00:05

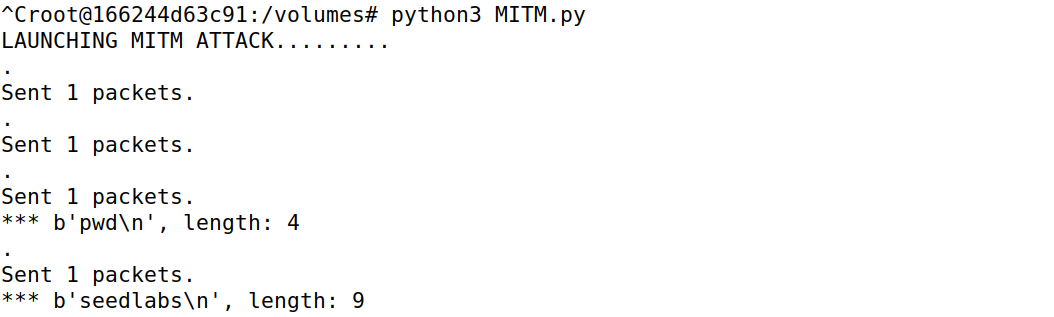
受害者主机：



目的主机：



恶意路由器：



发现中间攻击人攻击成功，被成功篡改。