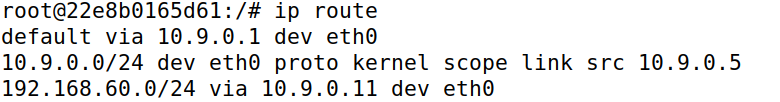
**ICMP Redirect Attack Lab**

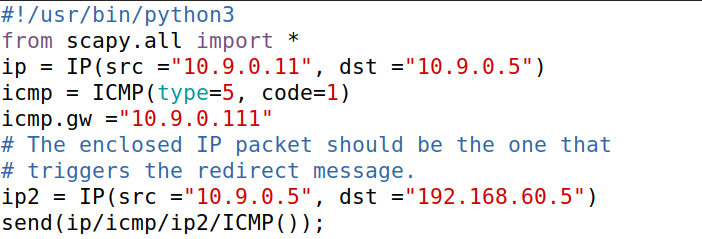
57118112 王怡乐

**Task 1: Launching ICMP Redirect Attack**

使用ip route命令查看受害者主机的路由表

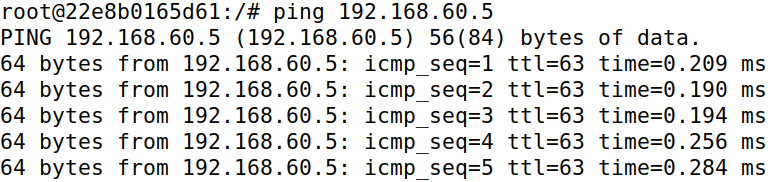


根据路由表构建攻击代码如下

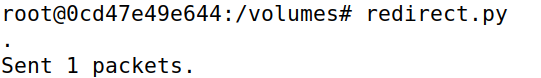


其中设置icmp重定向的源ip地址为局域网网关即10.9.0.11，目的地址为受害者主机ip，指定的新恶意网关地址为10.9.0.111。ip2的原宿地址即为受害者主机当前发送数据包相对应的ip地址。

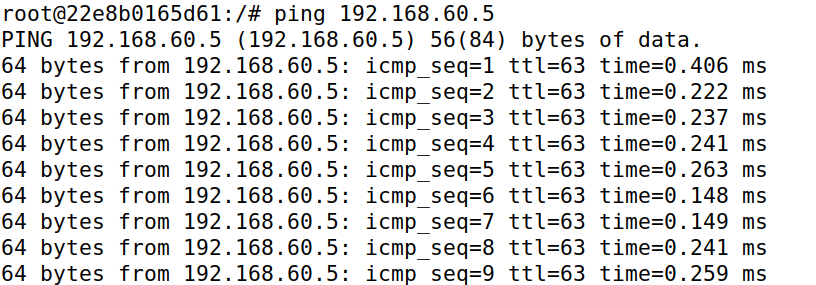
攻击之前，在受害者主机中ping 192.168.60.5



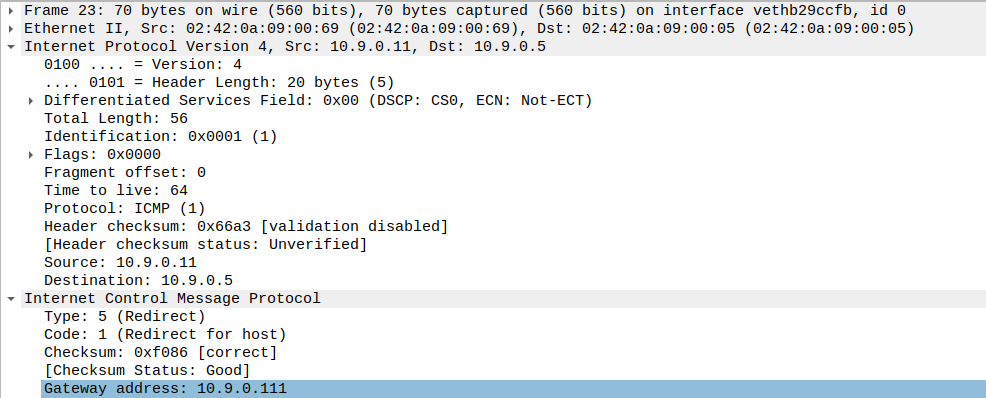
攻击者主机中执行攻击程序



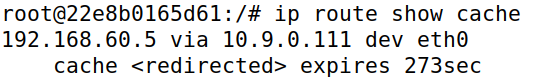
在受害者主机中ping 192.168.60.5



在wireshark中捕获到的重定向报文如下

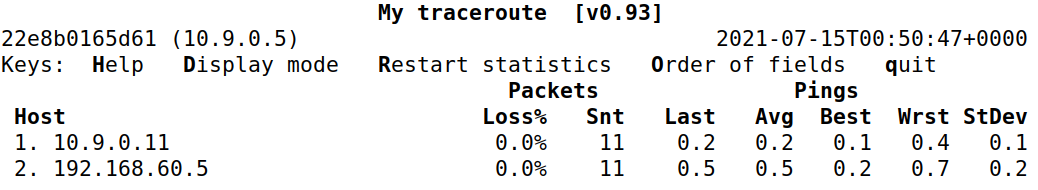


查看受害者主机的路由缓存，发送至192.168.60.5的数据包的网关已被重定向

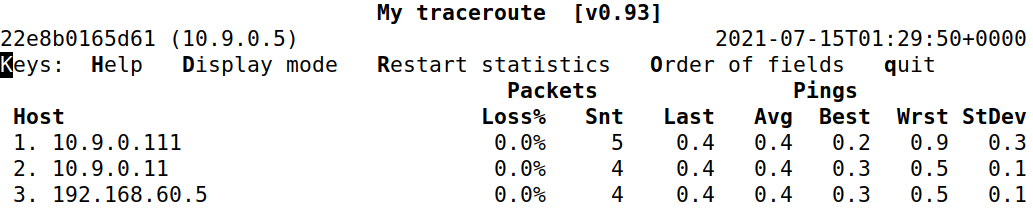


使用mtr -n 192.168.60.5 命令对比攻击前后的路由

攻击前：



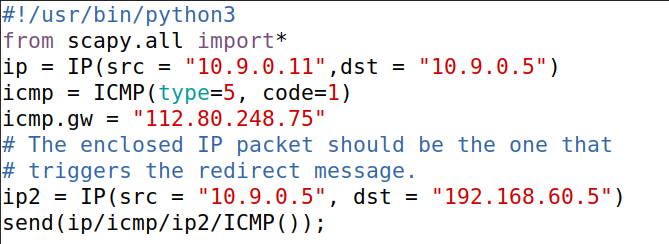
攻击后：



**问题回答：**

1. 可以使用ICMP重定向攻击重定向到远程机器吗?即分配给icmp.gw的IP地址是一台不在本地局域网内的计算机。请出示您的实验结果，并说明您的观察结果。

修改攻击程序如下，其中icmp.gw的IP地址更改为[www.baidu.com](http://www.baidu.com)的IP



重新发起攻击，没有产生路由缓存



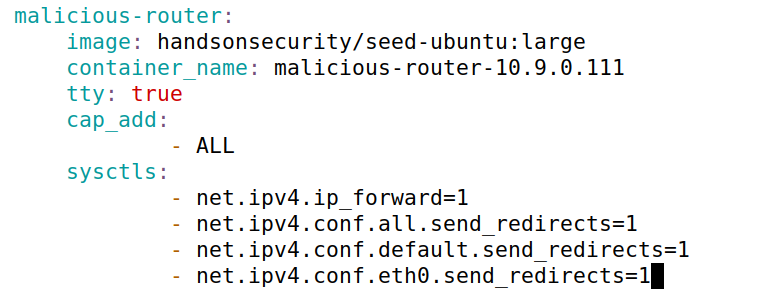
1. 是否可以使用ICMP重定向攻击来重定向到同一网络中不存在的计算机?即分配给icmp.gw的IP地址是一台离线或不存在的本地计算机。请出示您的实验结果，并说明您的观察结果。

将icmp.gw的IP地址更改为1.2.3.4，攻击结果与第一个实验相同，没有产生路由缓存，攻击失败



1. 如果你看一下docker-compose.yml文件，您将发现恶意路由器容器的以下条目。这些条目的目的是什么?请将它们的值改为1，并重新发起攻击。请描述并解释你的观察结果。

这些条目的目的是关闭icmp重定向，将它们的值修改为1则代表允许发送重定向消息。



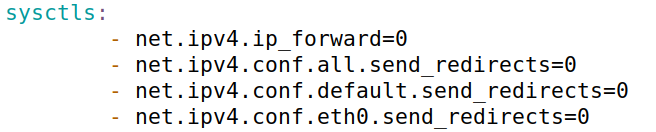
重新发起攻击，发现攻击失败



可能的原因是开启恶意路由器的重定向功能后，恶意路由器重定向到原网关上，导致重定向攻击失败。

**Task 2: Launching the MITM Attack**

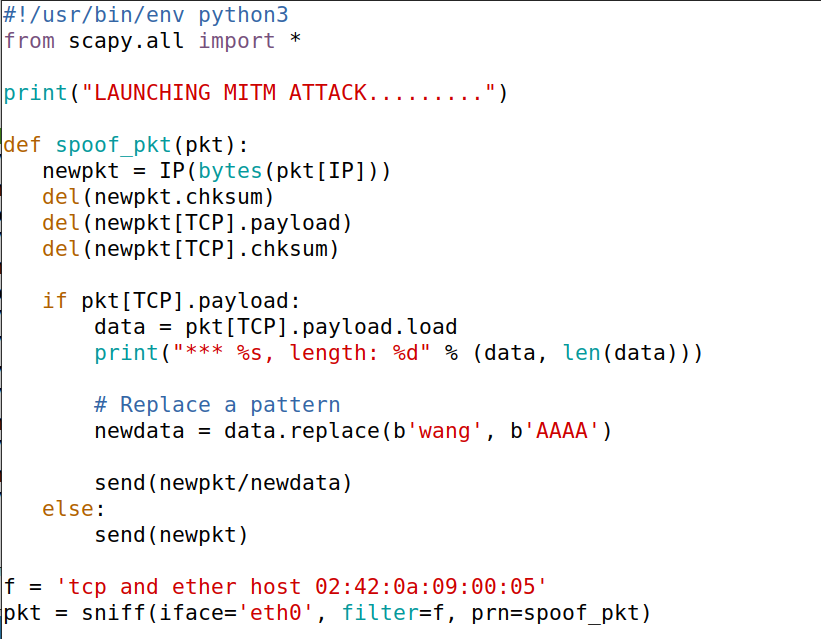
修改docker-compose.yml文件，将net.ipv4.ip\_forward的值更改为0，禁用恶意路由器的ip转发，并重启容器。



首先，同task1，对受害者主机进行icmp重定向攻击

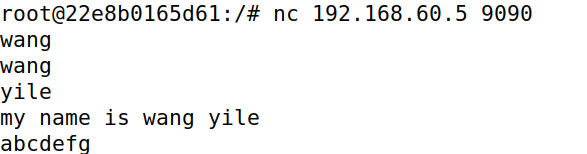
在目标容器192.168.60.5中执行命令nc -lp 9090，在受害者主机上执行命令nc 192.168.60.5 9090

在恶意路由器中执行攻击程序如下，其中将报文中的字符串“wang”更改为“AAAA”。同时为了避免捕获自己发出的报文，修改过滤规则，只捕获mac地址为被攻击主机mac地址的报文

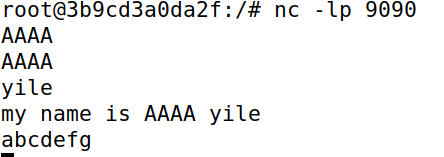


在恶意路由器上执行攻击程序。执行后受害者主机、目的主机及恶意路由器的输出如下所示

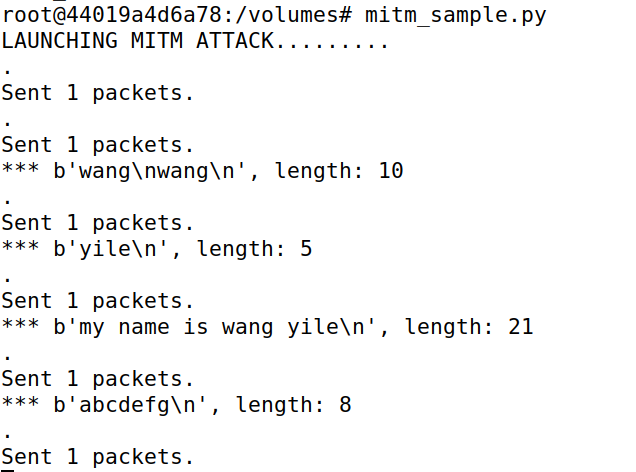
受害者主机：



目的主机：



恶意路由器：



**问题回答：**

1. 在MITM程序中，您只需要捕获一个方向的流量。请指明方向，并说明原因。

只需捕获从受害者主机到目的主机的流量。这是因为恶意路由器的ip转发功能被关闭，恶意路由器收到来自受害者主机的数据包后，不会转发给目的主机，因此目的主机不会回复受害者主机，也就不会有从目的主机到受害者主机的流量。

1. 在MITM程序中，当你从A(10.9.0.5)捕获nc流量时，你可以在过滤器中使用A的IP地址或MAC地址。其中一个选择是不好的，会产生问题，即使两个选择都可能有效。请两种都试一下，用你的实验结果来说明哪一种选择是正确的，并解释你的结论。

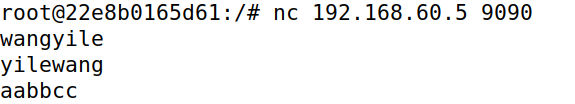
上述实验实现的是用mac地址进行过滤。用ip地址进行过滤的实验过程如下：

将过滤条件更改为

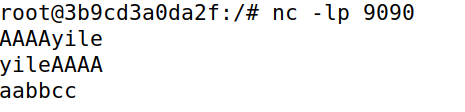


攻击结果如下

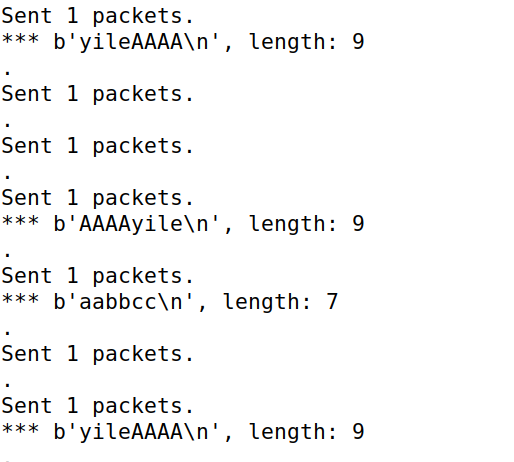
受害者主机：



目的主机：



恶意路由器：



发现使用ip地址进行过滤时攻击成功，但恶意路由器会不停地发送数据包。这是因为攻击程序伪造的数据包的ip地址与受害主机的ip地址相同，因此程序在捕捉来自受害主机数据包的同时，也会不断捕捉自己伪造的数据包。所以，选择mac地址进行过滤是正确的。