Lab 3 57118226 舒钰淇

Task 1: Launching ICMP Redirect Attack

首先查看受害主机的路由表，可以看到当前通往192.168.60.0网段的主机经由路由器10.9.0.11转发。

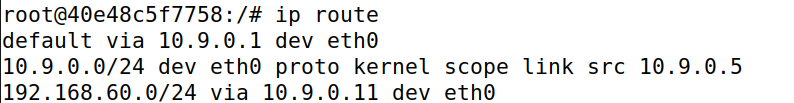


图1.1 受害主机路由表

编写如下图所示的伪造ICMP重定向报文发送程序，由于ICMP重定向报文需要由路由器发出，因此src设置为当前路由器IP地址10.9.0.11，因为是对主机进行重定向，所以type 和code分别设置为5和0，网关设置为恶意主机10.9.0.111，内层则与受害主机需要发送的ICMP请求报文信息相匹配。

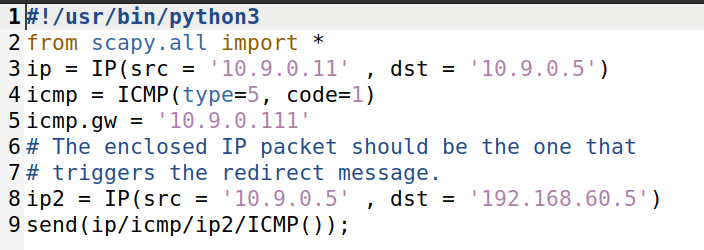


图1.2 task1.py

先在受害主机上ping192.168.60.5，再在恶意主机上运行上述的task1.py程序，可以看到受害主机的路由表缓存已经发生了改变，发往192.168.60.5的报文会先发往10.9.0.111。

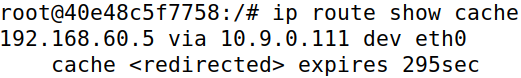


图1.3 受害主机路由缓存

再在受害主机上traceroute 192.168.60.5 ，可以看到报文先发往了恶意主机10.9.0.111。

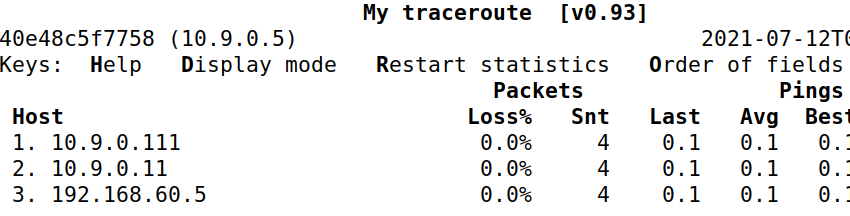


图1.4 受害主机上的traceroute结果

Question1

将重定向报文中的网关改为不在LAN上的主机，172.20.10.10位虚拟机的IP，路由缓存发生改变，但是traceroute时发送到默认网关寻找172.20.10.10，得不到答复。

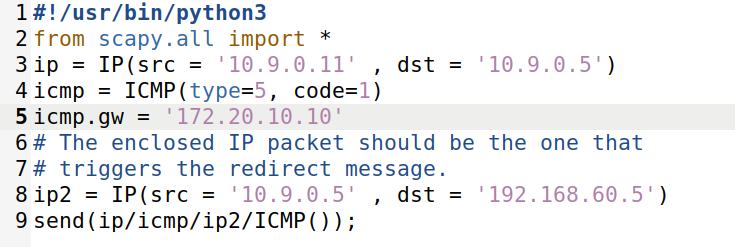


图1.5 网关改为172.20.10.10

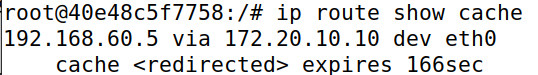
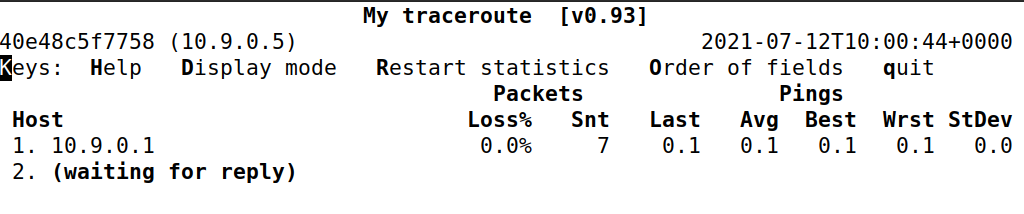


图1.6 受害主机路由缓存

图1.7受害主机上的traceroute结果

Question2 重定向到一个本网段上不存在的主机，路由缓存不会发生修改。

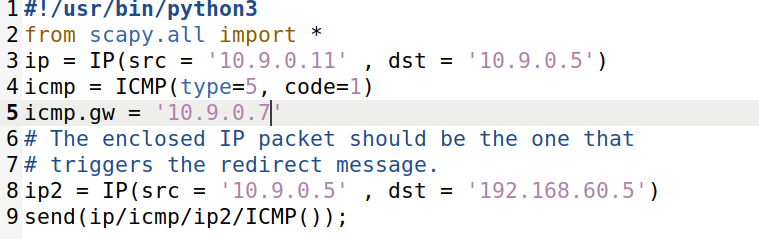


图1.8 网关改为10.9.0.7



图1.9 受害主机路由缓存

Question3

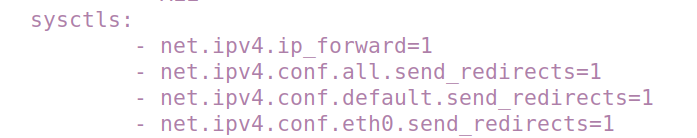
将路由器配置修改如下

图1.10 修改路由器配置

重新进行ICMP重定向攻击，可以发现缓存中还是路由器的地址。

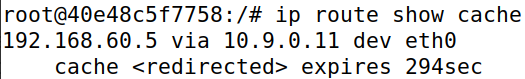


图1.11 受害主机路由缓存

Task 2: Launching the MITM Attack

在对受害主机进行ICMP重定向后，由于路由缓存的存在，可以进行进一步的攻击。如下图所示，在第一步攻击结束后，受害主机发往192.168.60.5的报文会先发送给10.9.0.111。

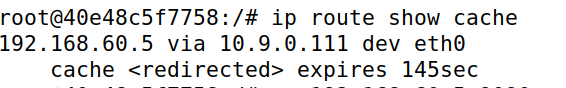


图2.1 受害主机路由缓存

编写如下程序，恶意路由器10.9.0.111监听接口eth0上的tcp报文，当报文内容为Shu时，将其更换为AAA，并转发给报文的目标地址。

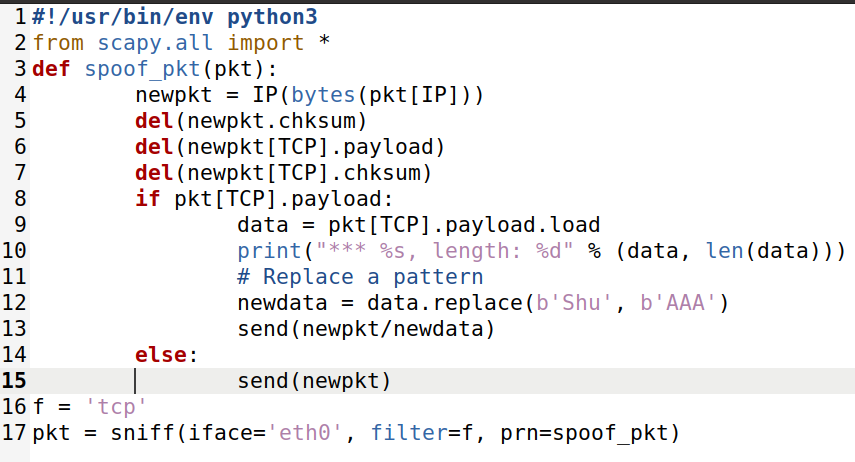


图2.2 task2.py

受害主机与192.168.60.5先以netcat进行连接，在恶意路由器上运行上述程序，在恶意主机上输入Shu并发送，192.168.60.5上显示AAA，而恶意路由器上也显示发送了相应的报文。

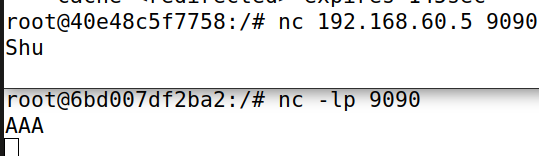


图2.3 netcat连接被干预

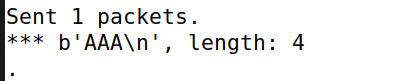


图2.4 恶意路由器转发报文

Question 4

如下图所示，修改恶意路由器运行的转发报文程序，只捕获源地址为10.9.0.5的报文，可以看到攻击成功

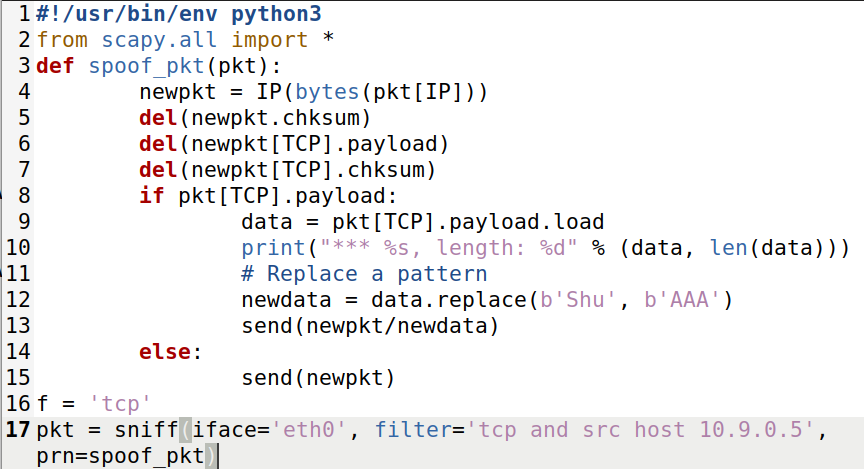


图2.5 修改过滤条件的程序

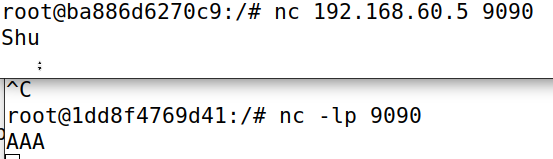


图2.6 攻击成功

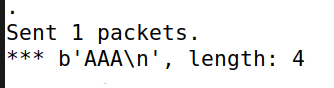


图2.7恶意路由器转发报文

Question 5

上一个Question中使用受害主机IP地址作为过滤条件，当受害主机通过netcat发送目标字符时，可以看到恶意路由器不断发送大量报文，是因为恶意路由器转发的报文也符合该过滤条件，因此会持续触发该转发程序。

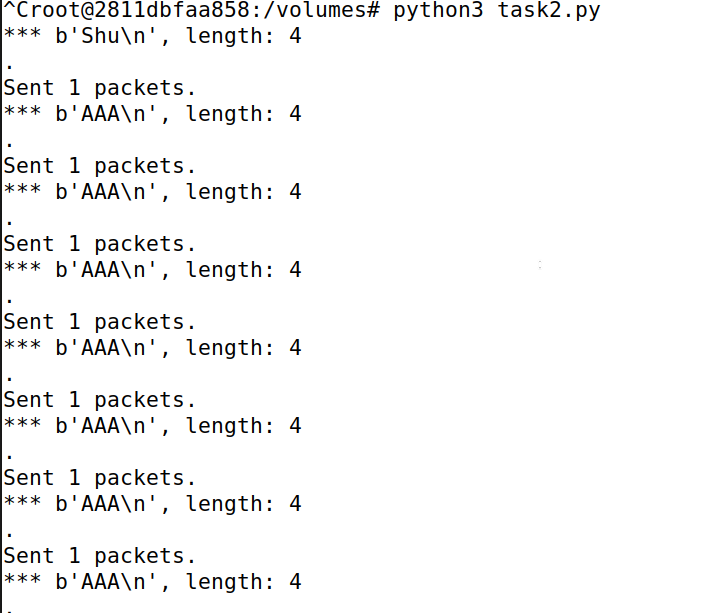


图2.8 恶意路由器持续转发

修改转发报文程序，将受害主机mac地址作为过滤条件

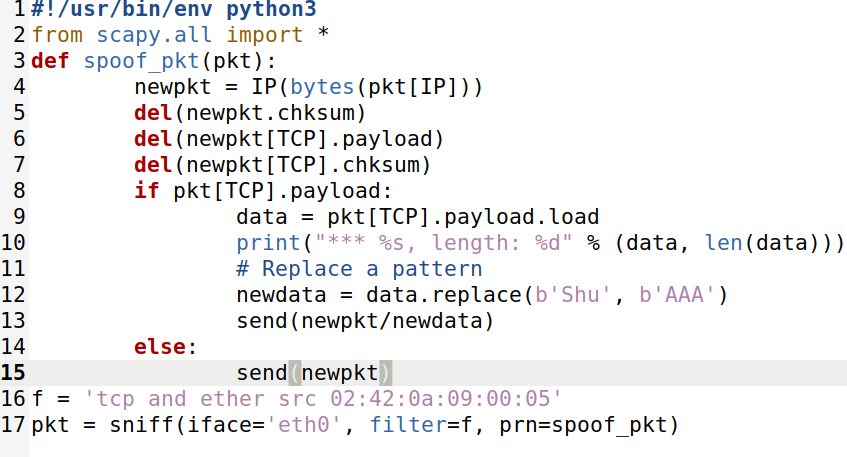


图2.9 修改过滤条件

再次进行攻击，可以看到攻击成功，且恶意路由器不再持续发送报文，说明对MAC地址进行过滤是更好的。

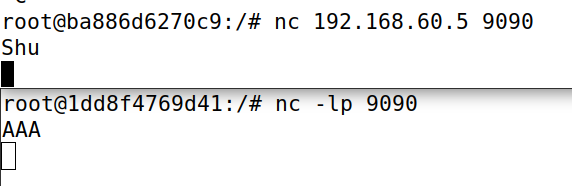


图2.10 攻击成功

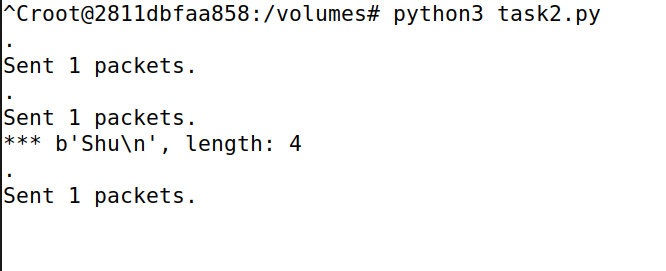


图2.11 恶意路由器转发的报文