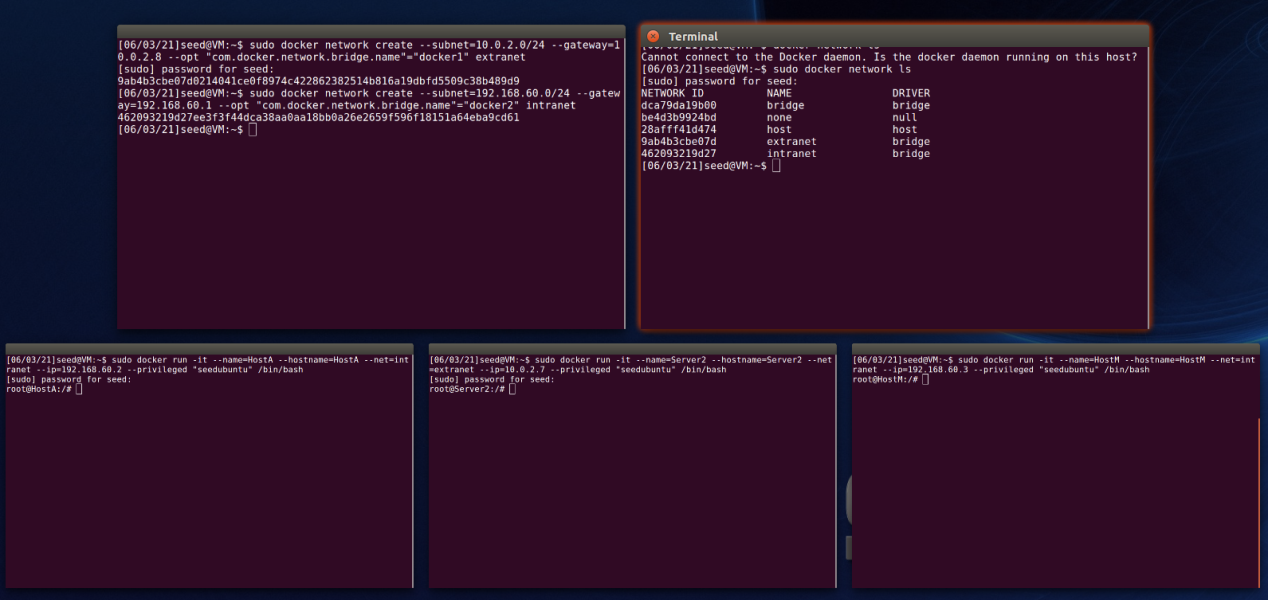
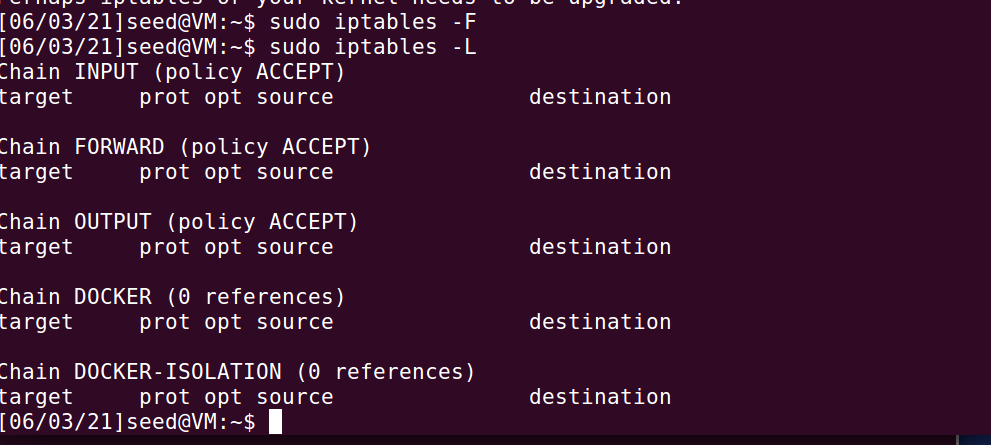
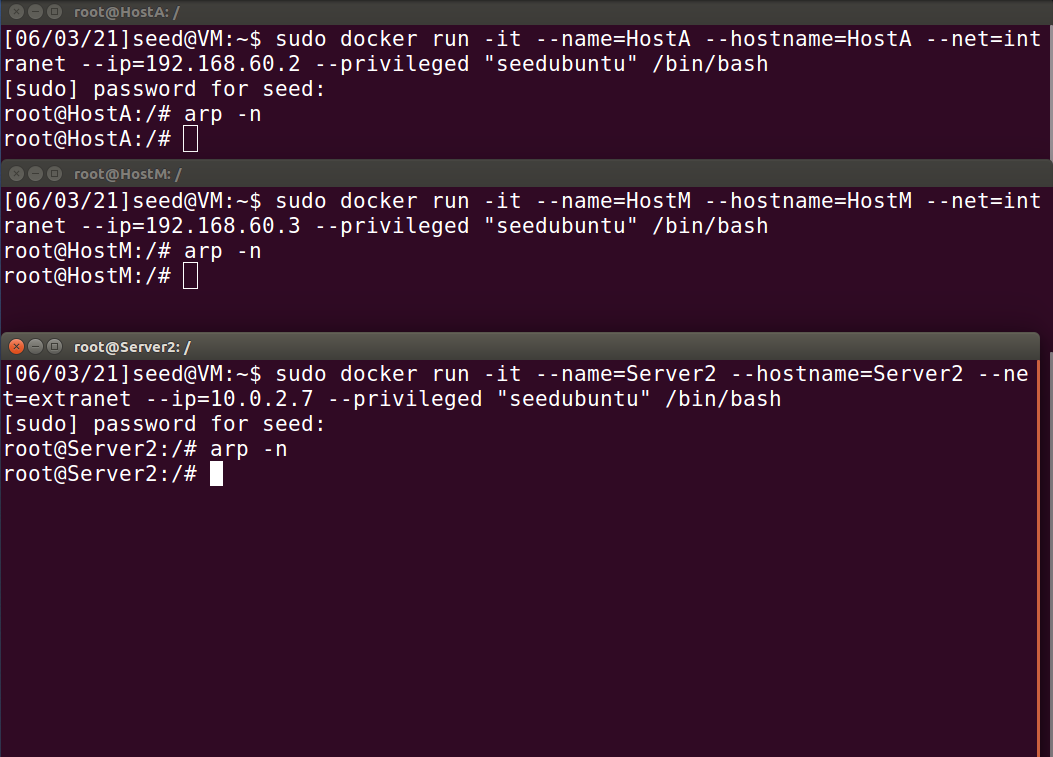
1. 首先通过docker完成实验所需环境的配置



1. 使用iptables命令关闭防火墙，并利用-L参数查看结果

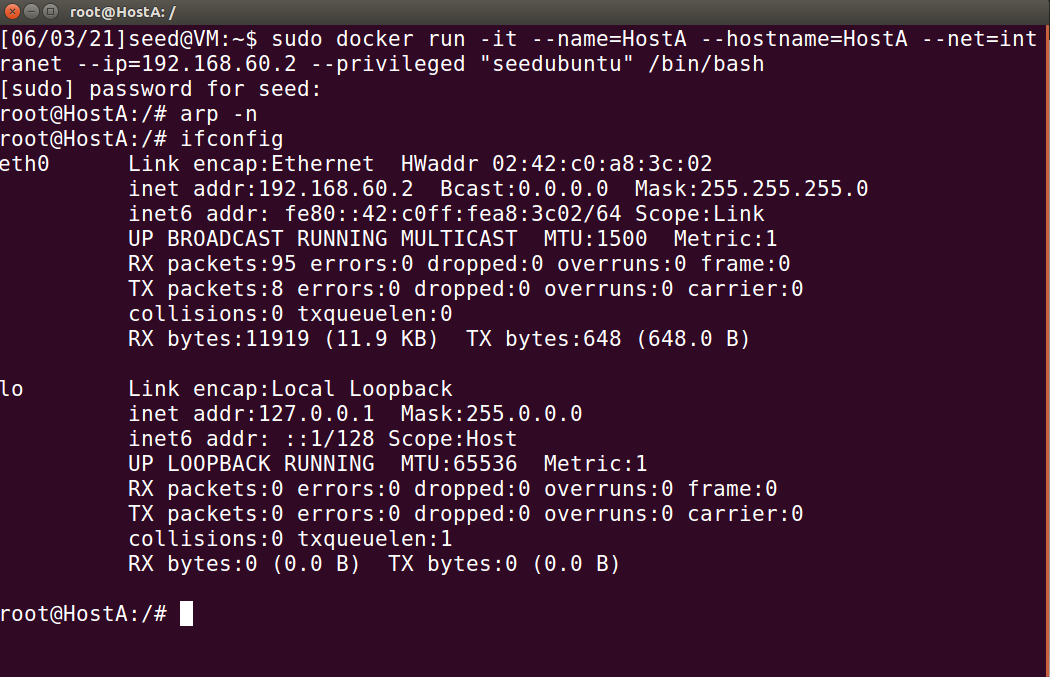


1. 在192.168.60.0/24网段里的虚拟机里使用arp –n命令查看arp缓存，可以看到初始状态下，其中是没有内容的。

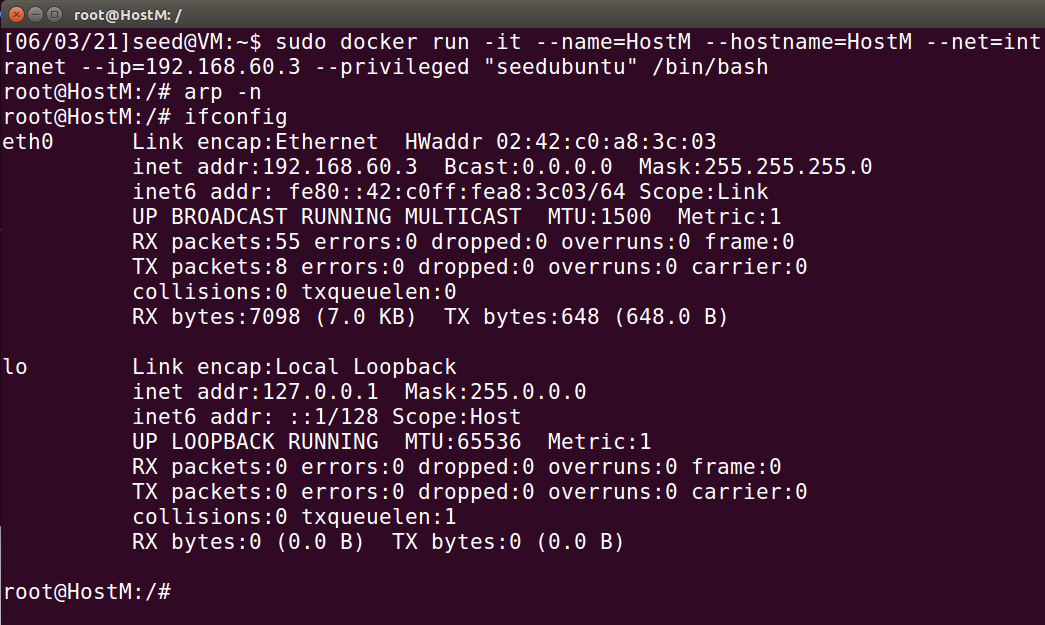


1. 通过ifconfig命令，分别获得192.168.60.0网段下两台主机(docker)的MAC地址

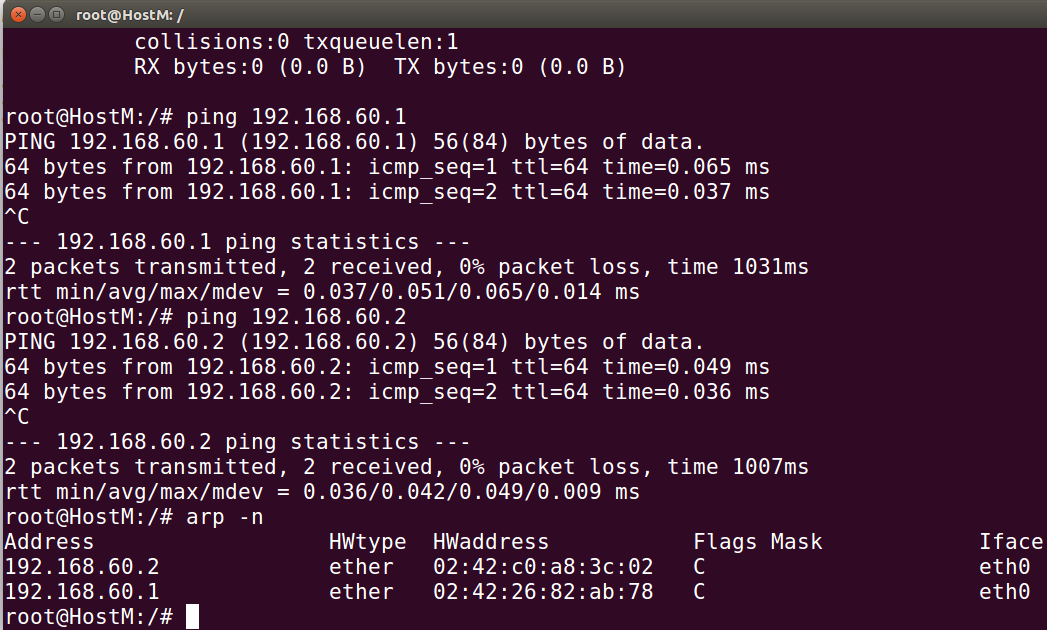
HostA：被攻击者



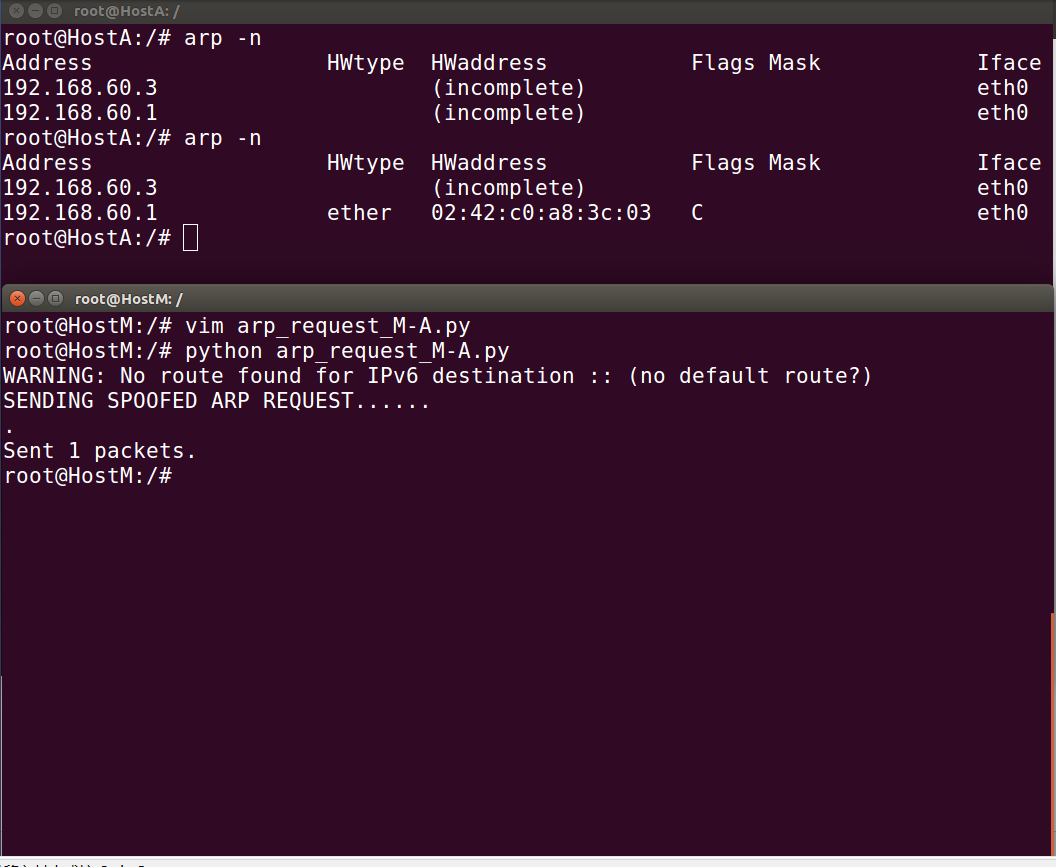
HostM：攻击者



1. 由于处于同一局域网，使用攻击者主机HostM来ping网关192.168.60.1，获得网关的MAC地址，用于脚本中相关地址的填充



1. 在攻击主机HostM上运行arp攻击脚本（图中下半部分），在图中上半部分中借助arp –n命令可以看到在执行arp攻击前后，HostA（被攻击主机）中对于网关的MAC地址arp缓存的区别——其中02:42:c0:a8:3c:03为HostM的MAC地址，表明攻击成功。



1. 执行脚本完成攻击后，使用tcpdump对数据进行监听来检验攻击效果：

在HostA（被攻击主机）上使用ping命令对网关IP发送数据包(图中左侧)，于此同时在HostM打开tcpdump对数据包进行监听，可以看到收到了大量来自于HostA、目的地址为网关IP的数据包(图中右侧)。

