ARP Cache Poisoning Attack Lab Report

管箫 18307130012 2018级信息安全

**一、Task Set 1: ARP Cache Poisoning**

1、Network Setting

建立虚拟机之间的虚拟网络连接。三台虚拟机MAB构成一个虚拟子网。

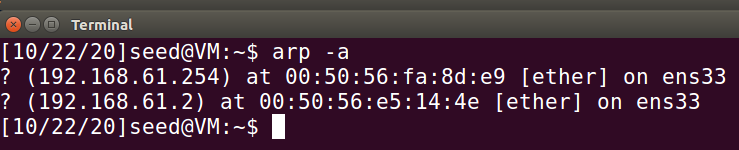
M：IP：192.168.61.138，MAC：00:0c:29:01:41:ae

A：IP：192.168.61.139，MAC：00:0c:29:a3:8a:e6

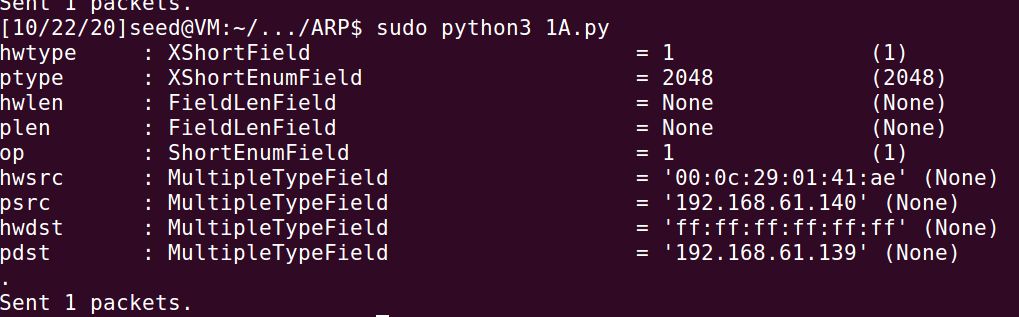
B：IP：192.168.61.140，MAC：00:0c:29:aa:55:ad

其中M作为攻击发起者，A、B两机作为受害者

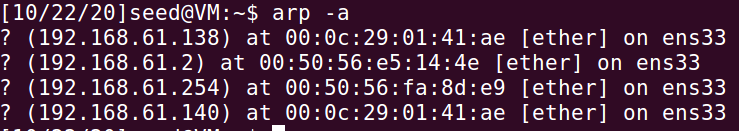
查看A机的ARP表



2、Task1：using ARP request

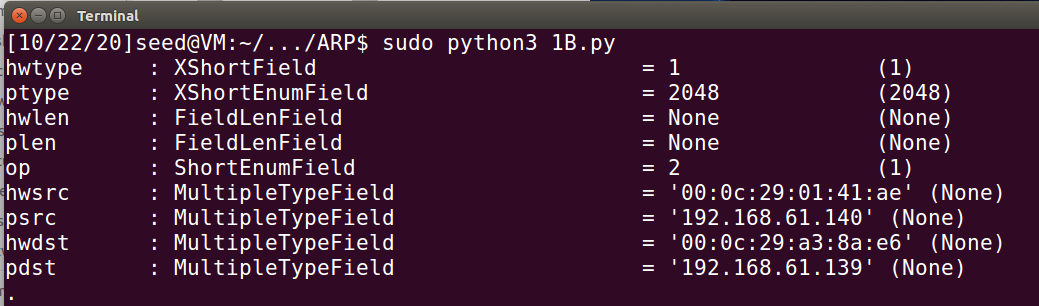


在主机M上构造如上的ARP request包发送到A，观察到在A主机上ARP cache新增记录如下：

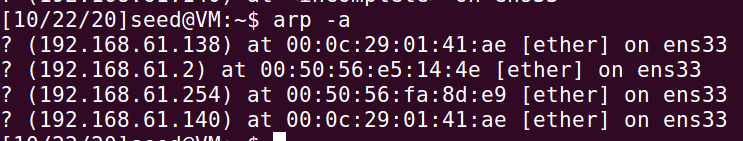


B的ip成功联系到了M的MAC地址，但同时新增了一条M的ip地址和M的MAC地址的关联记录。

3、Task2：using ARP reply

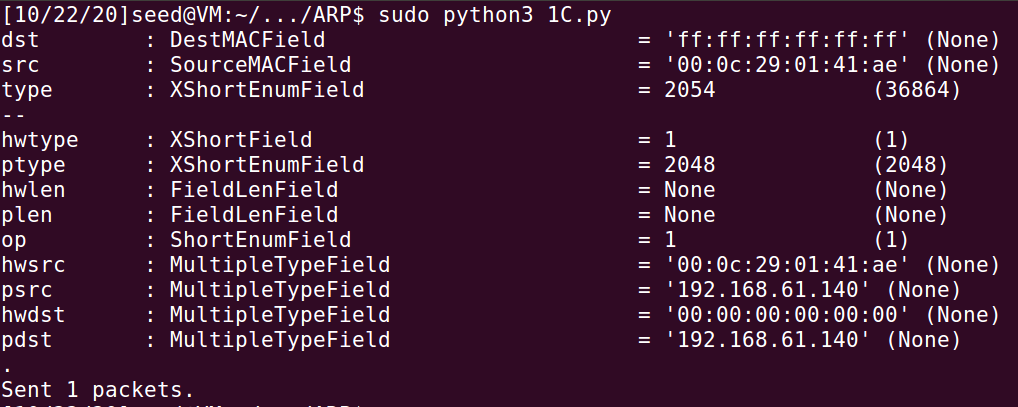


同样的，构造ARP响应包，观察到主机A的arp表产生如下变化：

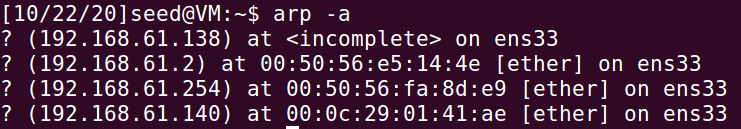


与Task1中情况相似。

4、Task3：using ARP gratuitous message



构造ARP gratuitous包并发送，观察到主机A上的新ARP表：



发现主机M的MAC地址绑定到了主机B的ip地址上，并且未生成主机M的MAC地址与主机M的ip地址之间的关联记录。

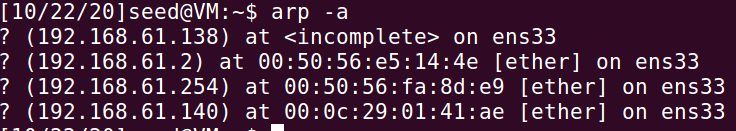
明显，这一方式适合进行ARP欺骗攻击，具有较好的隐蔽性。

**二、Task Set 2: MITM Attack on Telnet using ARP Cache Poisoning**

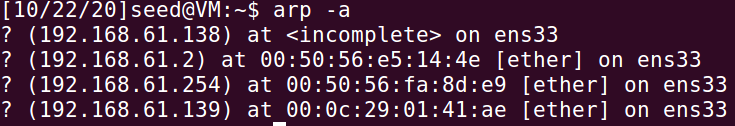
1、Step1：Launch the ARP cache poisoning attack

对主机A和主机B建立ARP欺骗。

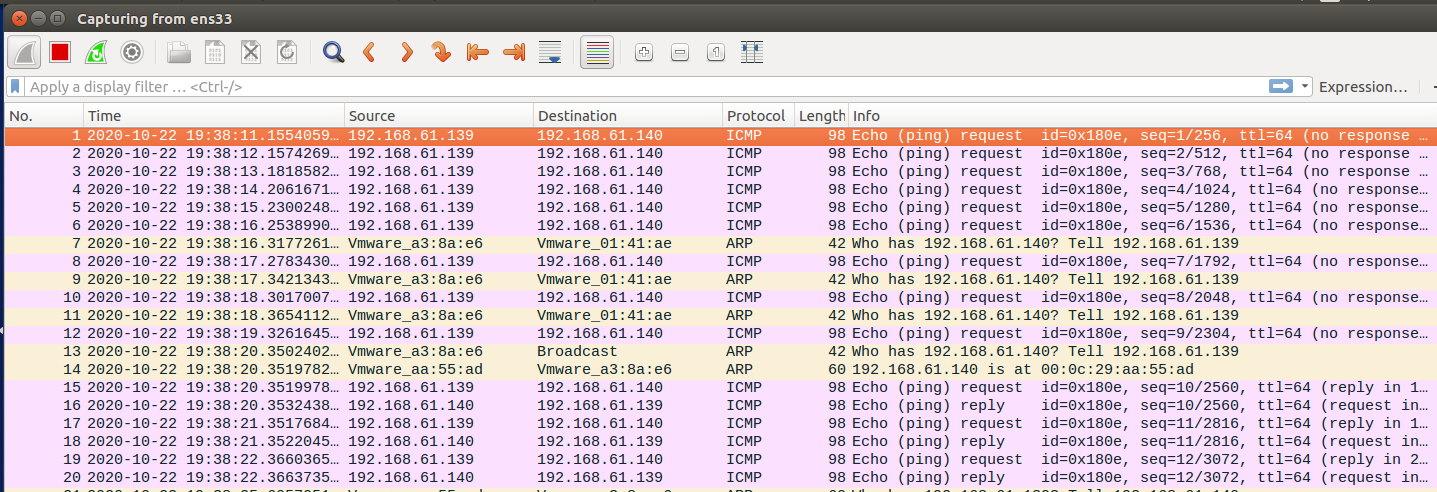
主机A：



主机B：



2、Step2：Testing



我们可以观察到Ping指令发送的ICMP请求包在多次超时后，系统发送了ARP包寻求192.168.61.140的MAC地址，三次对当前地址发送未收到回应后，进行了广播并收到了主机B的回复，两机建立了正确的ARP表，并产生了正确的ICMP请求响应。

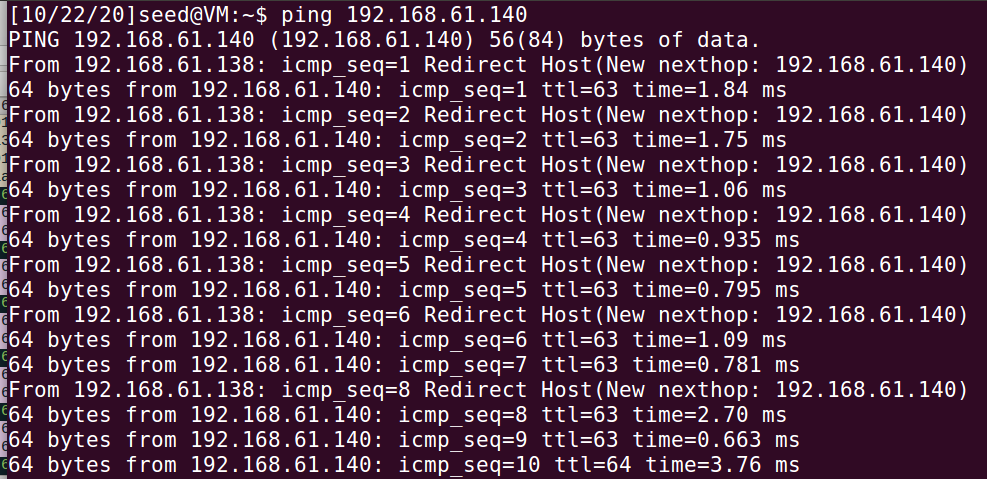
3、Step3：Turn on IP forwarding

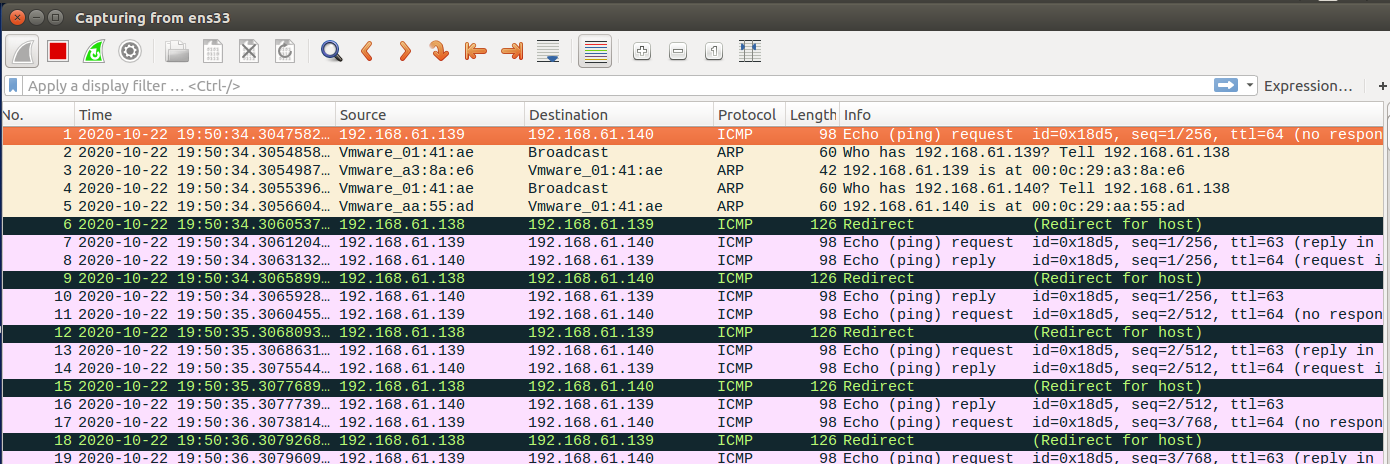
重新建立ARP欺骗，并开启ip forward。



观察到

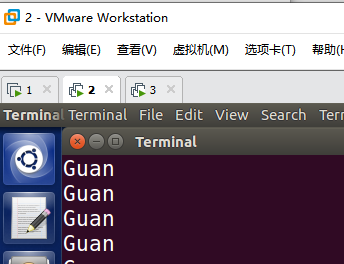
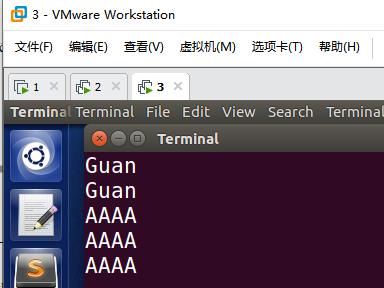
多次接收到来自192.168.61.138的重定向消息。





4、Step4：Launch the MITM attack

**三、Task Set 3: MITM Attack on Netcat using ARP Cache Poisoning**



完成更换，代码见文件。