12.2.1 ARP 缓存污染攻击

在第 7 章中，我们讨论了 ARP 协议是如何将网络中的 IP 地址映射成 MAC 地址的，在第 2 章中，我们讨论了将 ARP 缓存污染攻击作为监听主机流量的方法。ARP 缓存污染攻击是网络工程师高效实用的工具。然而，若有恶意企图，它也是一个非常致命的中间人攻击（man-in-the-middle，MITM）方法。

在 MITM 攻击中，攻击者重定向两台主机间的流量，试图在传输过程中拦截或修改。MITM 攻击有多种形式，包括会话劫持、DNS 欺骗，以及 SSL 劫持。

ARP 缓存污染攻击之所以有效，是因为特意构造的 ARP 数据包使两台主机相信它们在互相通信，而实际上它们却是与一个在中间转发数据包的第三方通信。

文件 arppoison.pcap 包含了 ARP 缓存污染攻击的一个例子。当打开它时，第一眼你会发现这些流量看起来很正常。然而，如果你跟进这些数据包，就会发现我们的受害者 172.16.0.107 在浏览 Google 并执行搜索。搜索的结果导致了一些 HTTP 流量，并夹杂一些 DNS 查询。

我们知道 ARP 缓存污染攻击是发生在第二层的技术，所以如果只是在 Packet List 面板里随意浏览，恐怕很难发现任何异常。因此，我们在 Packet List 面板里增加几列，过程如下。

（1）选择**Edit->Preferences**。

（2）单击 Preferences 窗口左边的**Columns**。

（3）单击**Add**。

（4）输入`Source MAC`并按回车键。

（5）在**Field type**下拉列表里，选择**Hw src addr (resolved)**。

（6）单击新增加的项，拖动它到**Source**列后面。

（7）单击**Add**。

（8）输入`Dest MAC`并按回车键。

（9）在**Field type**下拉列表里，选择**Hw dest addr (resolved)**。

（10）单击新增加的项，拖动它到**Destination**列后面。

（11）单击**OK**使改动生效。

当完成这些步骤时，你的屏幕应该跟图 12-8 一样。你现在应该有额外的两列，分别显示了数据包的来源 MAC 地址和目标 MAC 地址。

如果你还打开了 MAC 地址解析，应该会看到通信设备的 MAC 地址表明它是 Dell 或 Cisco 硬件。这是很重要的，因为当我们滚动整个捕获记录时，这些信息在数据包 54 就开始改变了。我们看到了一些奇怪的 ARP 流量，在 Dell 主机（受害者）和新出现的 HP 主机（攻击者）之间交互，如图 12-9 所示。

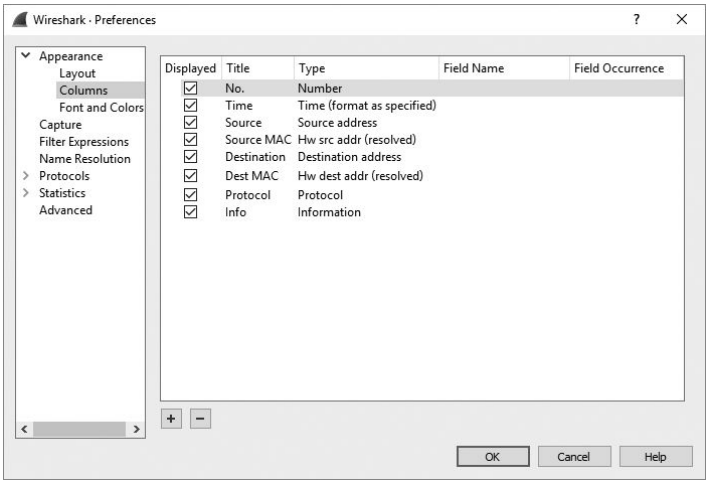

图 12-8　Column 配置屏幕，包含了新增的来源和目标硬件地址列

图 12-9　Dell 设备和 HP 设备间奇怪的 ARP 流量

在进一步深入之前，注意一下这次通信中涉及的端点，由表 12-3 列出。

表 12-3　监视的端点

角色	设备类型	IP 地址	MAC 地址
受害者	Dell	172.16.0.107	00:21:70:c0:56:f0

角色	设备类型	IP 地址	MAC 地址
路由器 攻击者	Cisco HP	172.16.0.1 未知	00:26:0b:21:07:33 00:25:b3:bf:91:ee

是什么使流量变得奇怪呢？回忆一下我们在第 6 章对 ARP 的讨论，ARP 数据包有两种类型：请求和响应。请求数据包在网络上广播给所有主机，用以发现包含特定 IP 地址的机器的 MAC 地址。接着，响应信息作为单播数据包发给请求的设备。在这个背景下，我们从通信序列中发现了一些奇怪的事情，参见图 12-16。

首先，数据包 54 是 MAC 地址为 00:25:b3:bf:91:ee 的攻击者发送的 ARP 请求，它作为单播数据包直接发送给 MAC 地址为 00:21:70:c0:56:f0 的受害者 ❶。这种类型的请求本应该广播给网络上所有主机，但它却只是直接发给了受害者。我们又注意到虽然这个数据包是攻击者发送的，并且在 ARP 头部包含了攻击者的 MAC 地址，但它却列出了路由器的 IP 地址，而不是它自己的。

紧随这个数据包的是受害者发给攻击者的响应，包含它的 MAC 地址信息 ❷。最诡异的事情出现在数据包 56 里：攻击者给受害者发送了一个包含未请求 ARP 响应的数据包，告诉它 172.16.0.1 对应的 MAC 地址是 00:25:b3:bf:91:ee❸。问题是 172.16.0.1 对应的 MAC 地址不是 00:25:b3:bf:91:ee 而应该是 00:26:0b:31:07:33。因为在之前的数据包捕获中我们看到过路由器 172.16.0.1 与受害者的通信，所以我们知道事实本应如此。由于 ARP 协议内在的不安全性（它的 ARP 表接收未请求的更新），因此现在受害者会将本应发送到路由器的流量发送给攻击者。

> 注意
>
> 因为这些数据包是从受害者机器上捕获的，所以你实际上没有看到事情的全貌。要使攻击生效，攻击者必须给路由器发送同样序列的数据包，骗它认为攻击者就是受害者。但我们需要在路由器（或攻击者）捕获才能看到这些数据包。

一旦两头都上当，受害者和路由器间的通信就会流经攻击者，如图 12-10 所示。

数据包 57 可以确认攻击取得成功。当你用神秘的 ARP 通信之前发送的数据包（比如数据包 40，参见图 12-11）与它比较时，就会发现远程服务

器（Google）的 IP 地址是一样的 ❶，但目标 MAC 地址却变化了 ❷。MAC 地址的变化告诉我们，现在的流量抵达路由器之前将被路由到攻击者。

这个攻击如此狡猾，以至它很难被检测。要想发现它，你通常需要专门配置 IDS 的帮助，或者在设备上运行能检测 ARP 表项突然变化的软件。因为你很可能会想利用 ARP 缓存污染攻击来捕获网络上的数据包以便分析，所以了解如何使用这种技术也是很重要的。

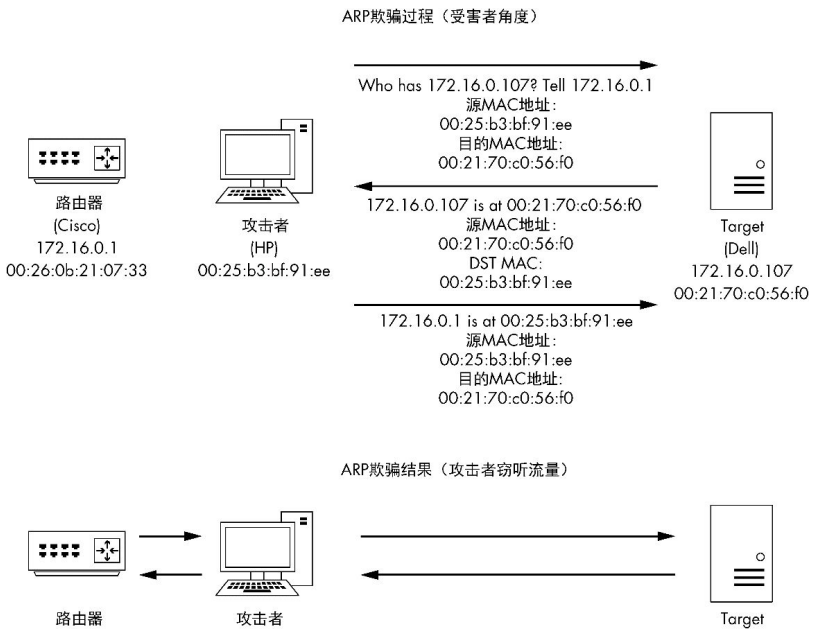

图 12-10　ARP 缓存污染导致 MITM 攻击

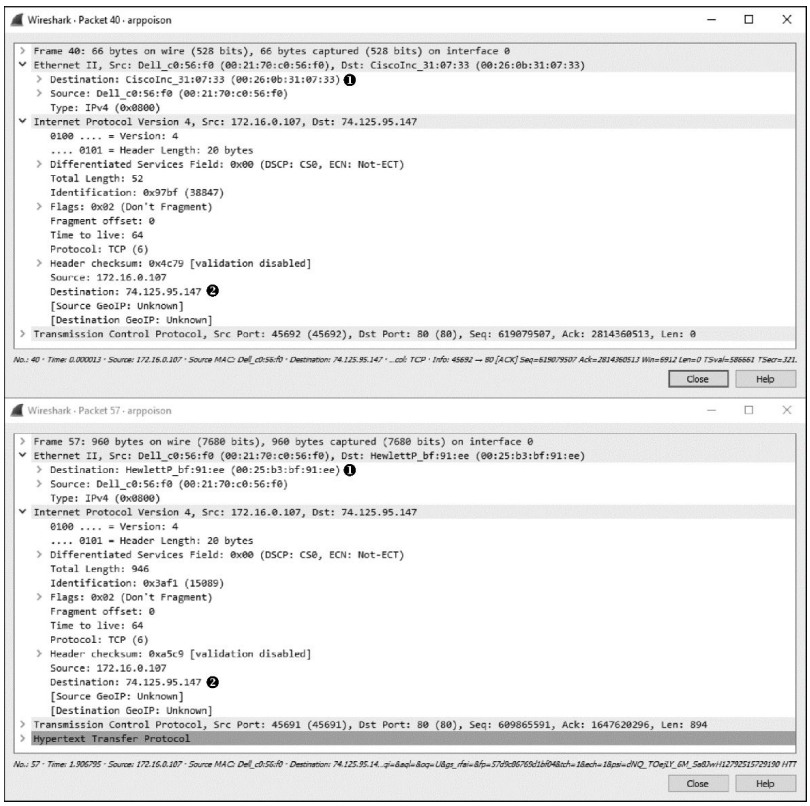

图 12-11　目标 MAC 地址的变化说明这次攻击是成功的

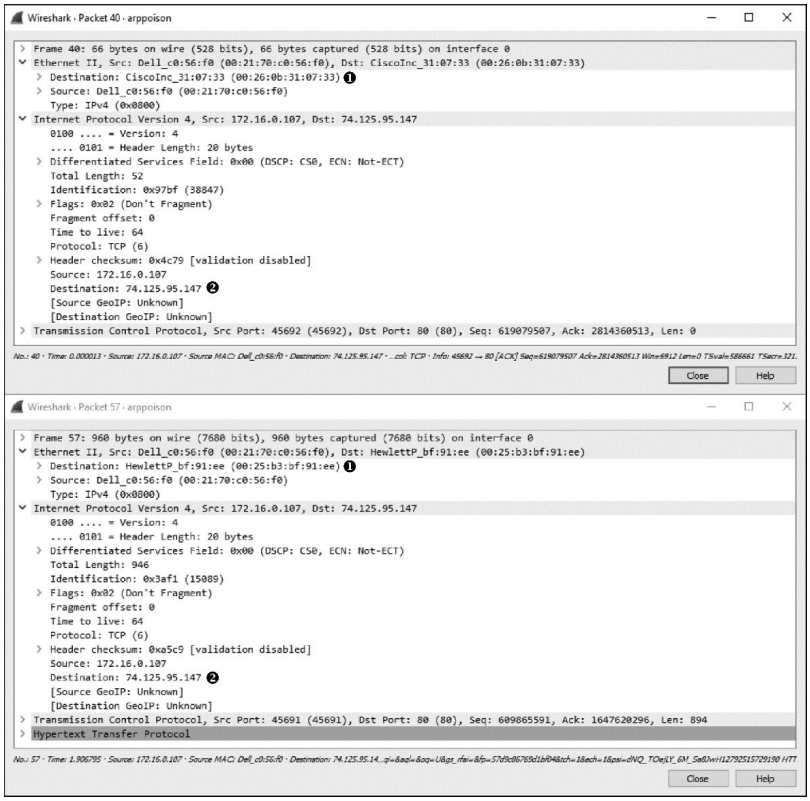

图 12-11　目标 MAC 地址的变化说明这次攻击是成功的（续）