2.3.4 ARP 缓存污染

进行网络线路监听时我最喜欢的技术，就是 ARP 缓存污染。我们将在第 6 章中详细介绍 ARP 协议，但在这里会进行一个简要的解释，以帮助了解这种技术是如何工作的。

1．ARP 查询过程

在第 1 章里，我们介绍了 OSI 参考模型中在第 2 层与第 3 层上数据包址的两种主要方式。这些第 2 层地址，或称为 MAC 地址，无论你在使用种第 3 层寻址方案，都会与之协同工作。

在本书中，按照行业标准术语，我们将第 3 层寻址方案称为 IP 寻址系统。网络上的所有设备相互通信时在第 3 层上均使用 IP 地址。由于交换机在 OSI 模型的第 2 层上工作，它们只识别第 2 层上的 MAC 地址，因此网络设备必须在它们创建的数据包中包含这些信息。当这些设备在不知道通信方的 MAC 地址时，必须要通过已知的第 3 层 IP 地址来进行查询，这样才能通过交换机将流量传递给相应的设备。

这些翻译过程就是通过第 2 层上的 ARP 协议来实施的。连接到以太网网络上计算机的 ARP 查询过程，是从一台计算机想要与另一台进行通信时开始的。发起通信的计算机首先检查自己的 ARP 缓存，查看它是否已经有对方 IP 地址对应的 MAC 地址。

如果不存在，它将往数据链路层广播地址 FF:FF:FF:FF:FF:FF 发送一个 ARP 广播请求包，作为一个广播数据包，它会被这个特定的以太网广播域上的台计算机接收，这个请求包问道：「某某 IP 地址的 MAC 地址是什么?」

没有匹配到目标 IP 地址的计算机会简单地选择丢弃这个请求包。而目标计算机则选择答复这个数据包，通过 ARP 应答告知它的 MAC 地址。此时，发起通信的计算机就获取到了数据链路层的寻址信息，便可以利用它远端计算机进行通信，同时将这些信息保存在 ARP 缓存中，来加速以后的网络访问。

2．ARP 缓存污染是如何工作的

ARP 缓存污染，有时也被称为 ARP 欺骗，是一种在交换网络中监听流量的高级方法。这种方法通过发送包含虚假 MAC 地址（第二层）的 ARP 息，来劫持其他计算机的流量。图 2-10 显示了 ARP 缓存污染的具体过程

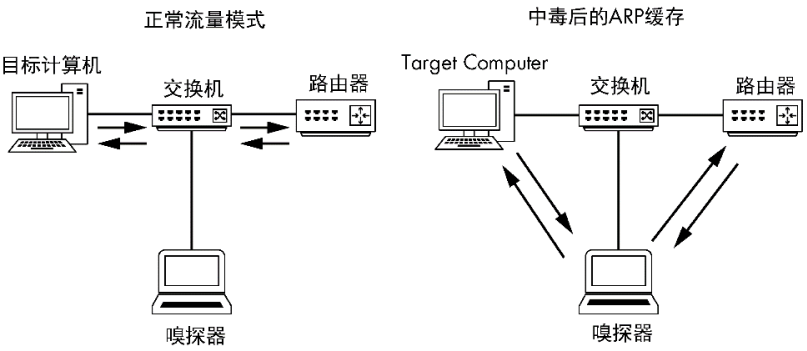

图 2-10　ARP 缓存污染允许你拦截目标计算机的流量

ARP 缓存污染是一种在交换式网络中进行监听的高级技术。它通常由
击者使用，向客户端系统发送虚假地址的数据包，来截获特定的网络流量
或者对目标进行拒绝服务攻击（DoS）。然而，它也可以是一种在交换式网
络中捕获目标系统数据包的方法。

3．使用 Cain & Abel 软件

当试图进行 ARP 缓存污染时，第一步你需要获得一些必要的工具来
集相关信息。在我们的演示中，我们将使用一款流行的安全工具 Cain &
Abel，可以从 oxid.it 下载获得。这款软件也支持 Windows 系统。你可
根据网站上的指引，来下载和安装这款软件。

> 注意
>
> 当你试图去下载这款软件的时候，计算机的杀毒软件或浏览器有可能会把 Cain & Abel 误报
> 恶意或黑客工具。该工具有多种用途，包括一些可能被认为是邪恶的。但在这里，这款工具对
> 的系统没有威胁。

在使用 Cain & Abel 软件之前，你需要收集某些信息，包括嗅探分析
系统的 IP 地址，你所希望嗅探网络流量的远程计算机的 IP 地址，以及远
计算机所连接的上游路由器。

当第一次打开 Cain & Abel 软件时，你会发现在软件窗口的顶端有着
系列的标签页（ARP 缓存污染攻击只是强大的 Cain & Abel 软件的其中一
功能）。为了演示例子，我们将切换到「嗅探器」选项页上。当单击此选
卡时，你应该会看到一个空表，如图 2-11 所示。

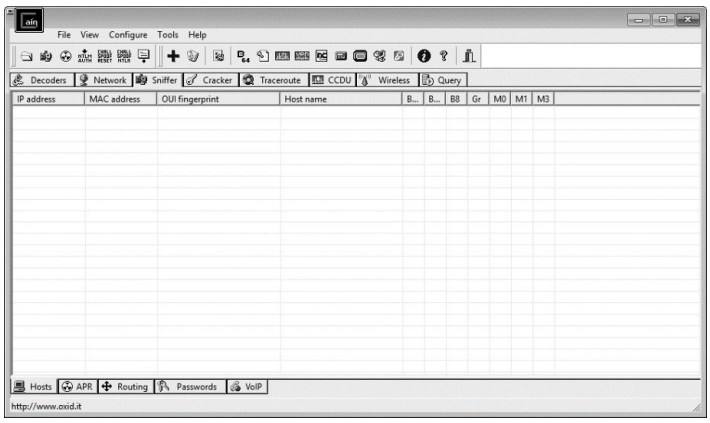

图 2-11　Cain & Abel 软件主窗口中的「嗅探器」选项卡

要完成此表，你需要激活这款软件的内置嗅探器，扫描你的网络并扫活跃主机。请按以下步骤进行操作以完成上述目标。

（1）单击工具栏上左起第二个图标，类似网卡形状的那个。

（2）你会被要求选择你希望进行嗅探的网络接口。这个接口应该连接你所希望进行 ARP 缓存污染的网络。选择这个网络接口，然后点击 OK 按钮。（要确保按下这个按钮，以激活 Cain & Abel 软件内置的嗅探器。）

（3）要建立在你的网络上可用主机的列表，单击加号（+）图标。MAC 地址扫描器对话框将会出现，如图 2-12 所示。请选择「All hosts in my subnet」圆形按钮（或者选择特定的地址范围），单击 OK 继续。

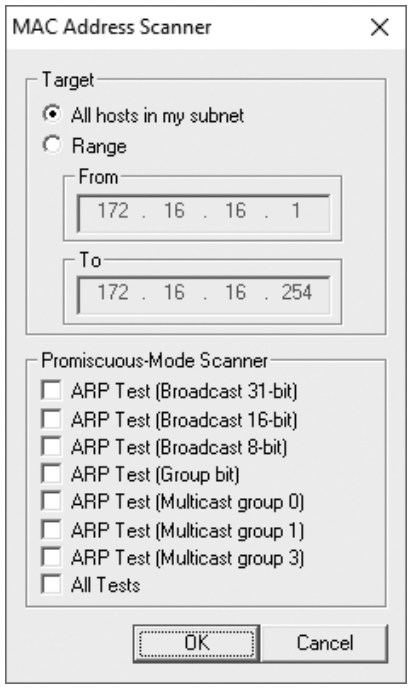

图 2-12　Cain & Abel 网络发现工具

一些 Windows 10 用户报告 Cain & Abel 无法确定他们的网络接口的地址，因此无法完成这个过程。如果您有这个问题，那么在配置网络接口

时，您将看到接口的 IP 地址是 0.0.0.0。

为此，采取以下步骤解决。

（1） 如果 Cain & Abel 是打开的，请关闭它。

（2） 在桌面搜索栏输入 ncpa.cpl，打开网络连接对话框。

（3） 右键单击要嗅探的网络界面，并单击 Properties。

（4） 双击 Internet Protocol Version 4 （TCP/IPv4）。

（5） 单击 Advanced 按钮并选择 DNS 选项卡。

（6） 选择 Use this connection』s DNS suffix in DNS registration 旁的复选框来激活它。

（7） 单击 OK 退出打开的对话框，重新启动 Cain & Abel。

现在表格中应该填满了你所在网络中的所有主机的信息，包括它们的 MAC 地址、IP 地址和供应商信息等。这是你开始进行 ARP 缓存污染的目主机列表。

在程序窗口的底部，你应该会看到另一组选项卡，选择它们将带你到探器标题下的其他窗口。现在，你已经创建了主机列表，接下来可以单击 ARP 选项卡切换至 ARP 窗口中。

在 ARP 窗口中，你会看到两个空的表格。当你完成下面的操作步骤之后，上方的表格中将显示出你的 ARP 缓存污染过程涉及的设备列表，而下方表格则会显示出在你进行中毒攻击的计算机之间的所有通信内容。

进行 ARP 缓存污染攻击，请按照下列步骤进行操作。

（1） 在屏幕上方的空白区域中单击，然后单击程序标准工具栏中的加（+）图标。

（2） 出现的单窗口中会有两个选择栏。在左侧，你可以看到网络上的所有活跃主机的列表。单击你希望进行网络流量嗅探的目标系统 IP 地址，右边的选择栏中将会显示出网络中的所有主机列表，除了你所选择的目标机 IP 地址。

（3） 在右边的选择栏中，单击目标计算机的直接上游路由器（即网关 IP 地址，如图 2-13 所示，然后单击「OK」。这两个设备的 IP 地址现在应会被显示在主程序窗口上方的表格中。

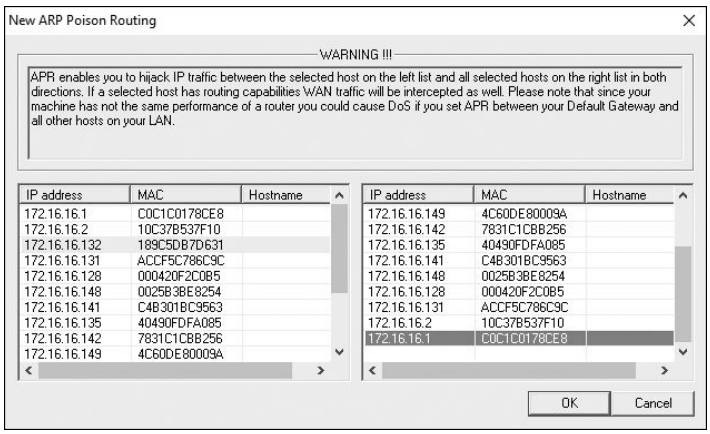

图 2-13　选择你要启用 ARP 缓存污染的目标系统

（4）完成这个过程的最后一步，单击标准工具栏中黄黑相间的辐射符号，这个操作将激活 Cain & Abel 软件的 ARP 缓存污染功能。让你的嗅探器作为从目标系统到它的上游路由器之间所有通信的中间人。

你现在应该就能启动你的数据包嗅探器，并开始分析过程了。当你完流量捕获之后，只需再次单击黄黑相间的辐射图标，便可以停止 ARP 缓存污染过程。

4．关于 ARP 缓存污染的警示

作为 ARP 缓存污染过程的最后警示，你必须要非常清楚实施这个过程中每个系统的角色与作用。在目标设备拥有很高的网络利用流量时，比如一台有着 1Gbit/s 联网线路的文件服务器，不要使用这项技术（尤其当你嗅探分析系统只提供了一条 100Mbit/s 的链路）。

当你使用这个例子中演示的这项技术对网络流量进行重路由时，所有标系统发送和接收的流量都必须先通过你的嗅探分析系统，因此，你的嗅分析系统可能成为整个通信过程中的瓶颈。这种流量重路由会对你进行分的系统造成一种拒绝服务攻击式的影响，将导致网络性能下降以及分析数不完备。

> 注意
>
> 你可以使用一个被称为非对称路由的功能，来避免所有的网络流量经过你的嗅探分析器。对于这种技术的更多信息，请参阅 oxid.it 用户手册。