科来

第 10 章
如何找出 ARP 病毒攻击

科来官微
CSNA 公众号
400-6869-069
www.colasoft.com.cn
support@colasoft.com.cn

ARP 协议对网络通讯具有重要的意义，然而不法分子通过伪造 IP 地址和 MAC 地址可以实现 ARP 欺骗，严重影响网络的正常传输和安全。ARP 欺骗的危害很大，可让攻击者取得局域网上的数据封包，甚至可篡改封包让网络上特定计算机或所有计算机无法正常连接。实践证明，通过网络分析技术，对网络流量进行数据包级的分析，对解决 ARP 欺骗问题是行之有效的。

10.1 问题描述

某用户使用办公机访问服务器时，会出现网络时断时续的现象。办公机是通过 DHCP 来获取 IP 地址的，当访问中断时，需要重新获取一下 IP 地址才可以连通，但持续不久又会中断。

该用户的网络环境比较简单，如下图所示。

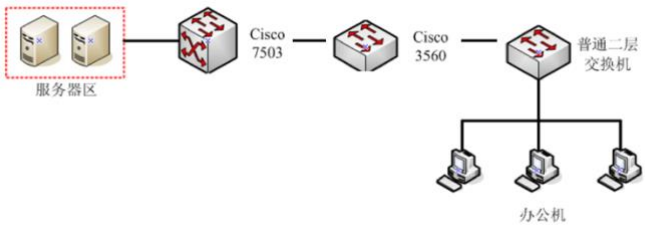

图 10-1

办公机的网段是 X.X.200.X/24，网关地址是 Cisco 3560 上的 X.X.200.254，服务器的地址段为 X.X.144.X/24。

10.2 分析过程

10.2.1 分析测试

在出现故障时，科来网络分析工程师尝试 Ping 服务器地址及办公机的网关地址，发现均无法 Ping 通。通过查看办公机的 ARP 表，发现网关地址对应的 MAC 地址全为 0，如下图所示。

```
C:\Documents and Settings\Administrator>ping       .200.254

Pinging       .200.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for       .200.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>arp -a

Interface: 0.0.0.0 --- 0x3
  Internet Address      Physical Address      Type
  192.168.200.254       00-00-00-00-00-00     dynamic
```

图　10-2

通过上面的分析测试我们了解到：当办公机无法访问服务器时，办公机连网关也无法 Ping 通。办公机中网关的 MAC 地址全为 0，即办公机没有学习到网关的 MAC 地址，因此办公机无法跟网关进行通信，从而导致主机无法连通服务器。

10.2.2　数据分析

正常连接时，办公机应该有网关的 IP 地址和 MAC 地址的 ARP 映射表。当连接失败时，办公机通过该表没有学习到网关的 MAC 地址。因此，造成该故障的原因很可能是网络中存在 ARP 欺骗！为了验证网络是否存在 ARP 欺骗，科来网络分析工程师通过在交换机 3560 上做端口镜像来抓取交互的数据包，具体部署如下图所示。

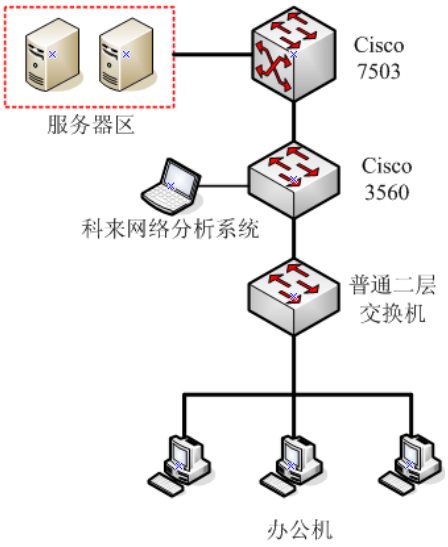

图　10-3

如上图所示，因为办公机连到交换机 3560 的端口是 f 0/46，所以将该端口

镜像到端口 f0/25，然后把科来网络分析系统接到 f0/25 端口上捕获通信的数据包。

科来网络分析工程师在分析数据包时，发现网络中存在大量的 IP 冲突，如下图所示。

图　10-4

通过诊断视图中的提示，发现产生冲突的源 IP 地址是故障网段的网关地址，如下图所示。

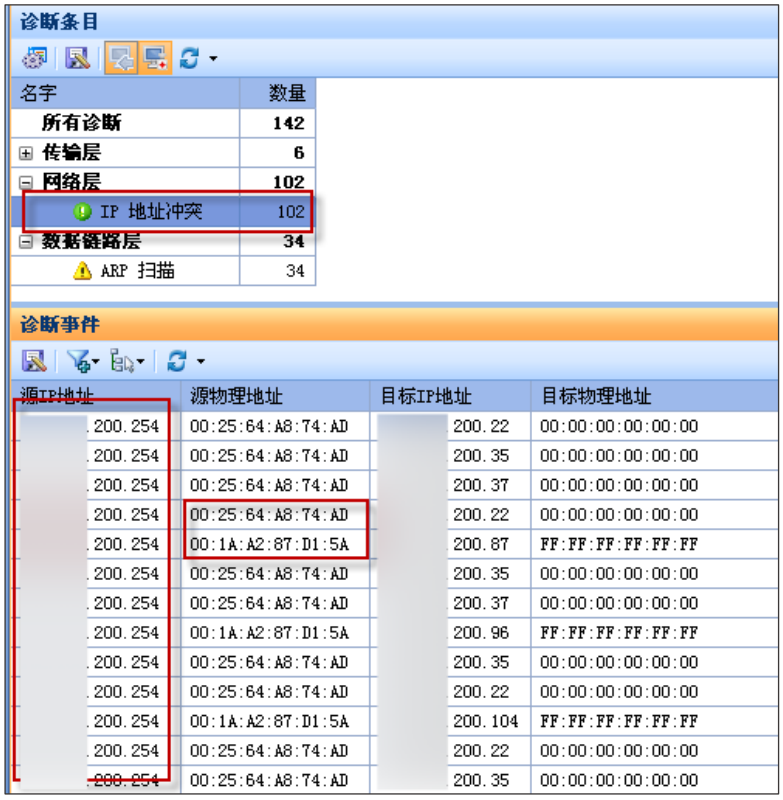

图　10-5

通过观察上图，发现 X.X.200.254 对应的 MAC 地址有两个：一个是

00:25:64:A8:74:AD，另一个是 00:1A:A2:87:D1:5A。对此具体分析可以发现：MAC 地址为 00:25:64:A8:74:AD 的主机对应的 IP 地址为 X.X.200.33，如下图所示。

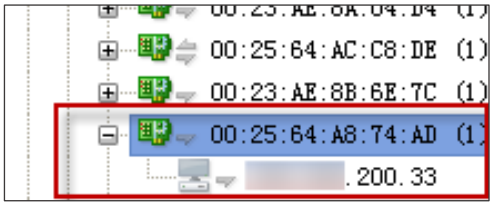

图 10-6

00:1A:A2:87:D1:5A 才是 X.X.200.254 真实的 MAC 地址。

因为办公机向错误的网关地址发送了请求，网关没有响应办公机的请求，所以导致办公机学习不到正确网关的 MAC 地址，如下图所示。

```
C:\Documents and Settings\Administrator>ping .200.254

Pinging .200.254 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for .200.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>arp -a

Interface: 0.0.0.0 --- 0x3
  Internet Address      Physical Address      Type
  192.168.200.254       00-00-00-00-00-00     dynamic
```

图 10-7

导致网络不通的原因就是由于 X.X.200.33 这台办公机进行 ARP 欺骗造成的。

10.3 分析结论

通过上面的分析，可以看出 MAC 地址为 00:25:64:A8:74:AD，IP 地址为 X.X.200.33 的这台办公机中了 ARP 病毒，将自己伪装成网关，欺骗网段内的其他办公机。对于 ARP 病毒的处理，只要定位到病毒主机，我们就可以通过 ARP 专杀工具进行查杀来解决这类问题。而最好的预防办法就是能够在内网主机安装杀毒软件，并且及时的更新病毒库，同时给主机打上安全补丁，防止再次出现。

10.4 价值

ARP 攻击在十年前就已经存在，至今为止仍被攻击者广泛使用。如何应对 ARP 攻击，已成为网络安全管理者深思的问题。而网络流量分析技术正是检测这类攻击的有效手段：无论怎样的攻击方式，都会产生网络数据。通过对数据的完整记录及分析，就能找到攻击过程和攻击源，从而采取针对性措施进行弥补。

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 GartnerNPMD 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区