9.2.5 DNS 区域传送

DNS 区域是一个 DNS 服务器所授权管理的名字空间（或是一组 DNS 名称）。举例来说，Emma’s Diner 这个网站可能由一个 DNS 服务器对 emmasdiner.com 负责。这样，无论是 Emma’s Diner 内部或者外部的设备，如果希望将 emmasdiner.com 解析成 IP 地址，都需要和这个区域的权威，也就是这个 DNS 服务器联系。如果 Emma’s Diner 发展壮大了，它可能会增加一个 DNS 服务器，专门用来处理其名字空间的 email 部分，比如 mail.emmasdiner.com，那么这个服务器，就成为这个邮件子区域的权威。如果必要的话，还可以为子域名添加更多的 DNS 服务器，如图 9-19 所示。

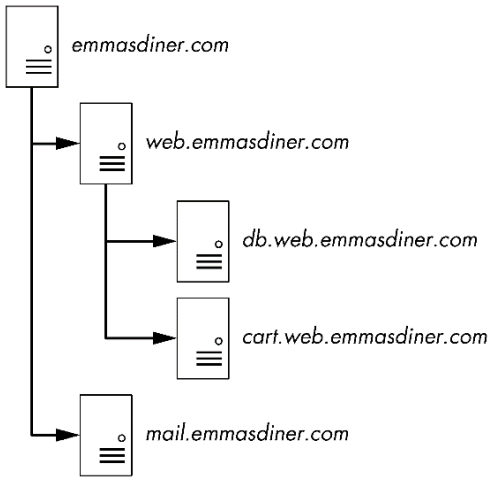

图 9-19　DNS 区域划分名称空间的责任

区域传送指的是通常出于冗余备份的需要，在两台设备之间传送区域数据。举例来说，在拥有多个 DNS 服务器的组织中，管理员通常都会配置一台备用 DNS 服务器，用来维护一份主服务器 DNS 信息的副本，以防止主 DNS 服务器不可用。主要存在两种区域传送。

完整区域传送（AXFR）：这个类型的传送将整个区域在设备间进行传送。

增量区域传送（IXFR）：这个类型的传送仅传送区域信息的一部分。

文件 dns_axfr.pcap 包含了一个主机 172.16.16.164 和 172.16.16.139 之间进行完整区域传送的例子。

当第一眼看这个文件时，你可能会怀疑是否开错了文件，因为你所见到的是 TCP 数据包而不是 UDP 数据包。虽然 DNS 基于 UDP 协议，但它在比

如区域传送的一些任务中也会使用 TCP 协议，因为 TCP 对于规模数据的传输更加可靠。这个捕获文件中的前 3 个数据包是 TCP 的三次握手。

第四个数据包开始在 172.16.16.164 和 172.16.16.139 之间进行实际的区域传送。这个数据包并不包含任何 DNS 信息。由于区域传送请求的数据包中的数据由多个数据包所发送，因此这个数据包被标记为重组装 PDU 的 TCP 分片。数据包 4 和 6 包含了数据包的数据。数据包 5 是对于数据包 4 被成功接收的确认。这些数据包以这种方式显示出来是因为 Wireshark 出于可读性的考虑将 TCP 数据包如此解析并呈现。这里我们可以将数据包 6 作为完整的 DNS 区域传送请求，如图 9-20 所示。

区域传送请求是典型的查询，但它请求的是 AXFR 类型而不是单一记录类型，这意味着它希望从服务器接收全部 DNS 区域。服务器在数据包 7 中回复了区域记录，如图 9-21 所示。正如你所见到的那样，区域传送包含了相当多的数据，并且这还是一个很简单的例子！ 在区域传送完成之后，捕获文件以 TCP 连接的终止过程作为结束。

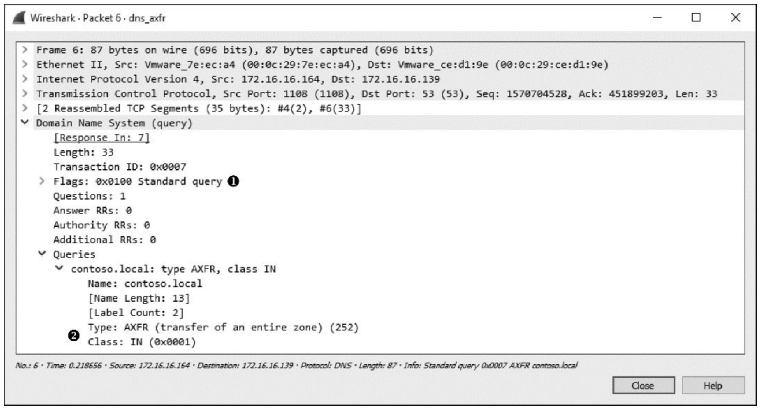

图 9-20　DNS 完整区域传送请求

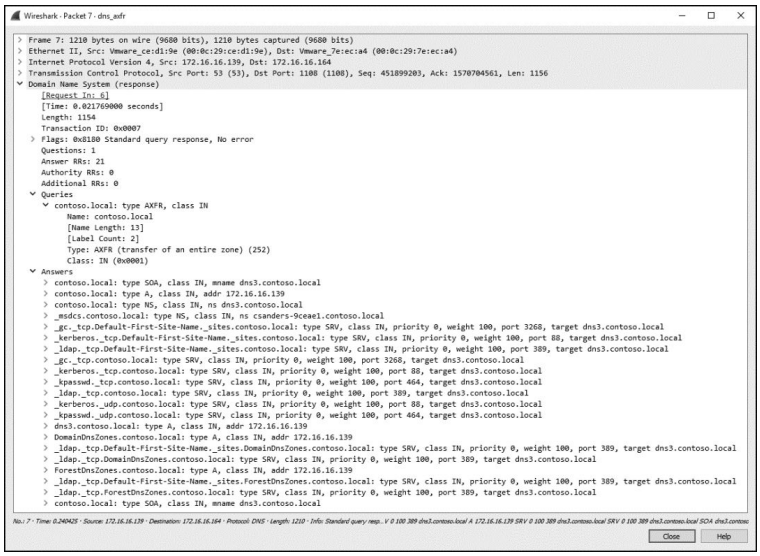

图 9-21　正在进行的 DNS 完整区域传送

警告

区域传送的数据如果落入他人手中可能会很危险。举例来说，通过枚举一个 DNS 服务器，你可以绘出整个网络的基础结构。