2.5 部署嗅探器的实践指南

我们已经介绍了在交换式网络中捕获网络流量的 4 种不同方法。我们可以再增加一种方式，适用于我们仅仅在单个系统上安装嗅探器软件并监听这台系统流入流出的流量。在某个特定场景中，你可能不太容易确定应该用上述这 5 种方法中的哪种才是最合适的。表 2-2 提供了每种部署方法的通用准则。

作为分析师，我们需要尽可能地隐蔽。最理想的境界是，我们采集需要的数据，而不留下任何的脚印。这就像是法医在调查时不想对犯罪现场造成任何破坏。我们也不希望破坏捕获的网络流量。

表 2-2 在交换式网络环境中进行数据包嗅探的指导准则

技术	指导准则
端口镜像	● 通常是首选的，因为它不会留下网络脚印痕迹，也不会因此而产生额外的数据包。 ● 可以在不让客户端脱机下线的情况下进行配置，非常便于镜像路由器或者服务器端口。
集线器输出	● 当你不需要考虑主机暂时下线带来的后果时适用。 ● 当你必须捕获多台主机的流量时是低效率的，因为碰撞和丢包会导致性能低下。 ● 可能会导致现代的 100/1000Mbit/s 主机丢失数据包，因为大多数真正的集线器都只是 10Mbit/s 的。
使用网络分流器	● 当你不需要考虑主机暂时下线带来的后果时适用。 ● 当你需要嗅探光纤通信时，这是唯一选项。 ● 由于网络分流器就是为了网络监听嗅探而设计的，而且能够跟上现代网络速度，因此这种方法比起集线器输出要更优一些。 ● 在预算紧张时，这种方法的成本会过于高昂

术	
ARP 缓存污染	● 这会被认为是非常草率的，因为它涉及网络上注入数据包，并通过重路由网络流量流经你的嗅探器。 ● 在你需要一个暂时性快速实施的方法，能够将一个设备的网络流量进行捕获，而又不用将其下线，同时端口镜像又不被支持的时候，这种方法会是一个高效的选择。
直接安装	● 一般不建议，因为如果一台主机存在故障和问题，这个问题可能会导致数据包被丢弃，或是被配置成它们无法被准确展示的样子。 ● 主机的网卡不需要设置在混杂模式。 ● 在进行环境测试、评估和审查性能，或是检查在其他地方捕获的数据包文件时，这是最佳方案。

当在后面章节中逐步面对一些实际场景时，我们将会对逐个案例进行详细分析，来讨论捕获数据最好的方式。目前来说，我们在图 2-15 中给出的流程图应该能够帮助你决定用来捕获流量的最佳方法。请记住，这个流程图只是一个简单的通用参考，并不涵盖所有用来监听网络线路的可能方法。