12.1 网络侦察

攻击者采取的第一步行动是深入研究目标系统。这一步又叫「网络踩点」，通常使用各式各样的公开资源来完成，比如目标公司的主页或者 Google。这个研究完成后，攻击者通常开始扫描目标 IP 地址（或者域名）的开放端口或运行服务。

通过扫描，攻击者可以确定目标是否在线并且可达。例如，想象一下，一位银行大盗盯上了位于缅因街 123 号的目标——本市规模很大的银行。他花费数星期时间精心策划此次抢劫，却在抵达目的地后才发现银行已经搬迁到了万安街 555 号。还可以想象一个更糟糕的场景，劫匪计划在正常上班时间步行进入银行，以便对金库下手，刚到银行门口却发现今天歇业。确保目标在线并且可达是我们必须要解决的一个问题。

扫描的另一个重要收获是，它告诉了攻击者目标开放了哪些端口。回到我们刚才类比的银行劫匪，想一想，如果劫匪出现在银行门口，却对整幢楼的布局一无所知，会怎么样？他无法进入大楼，因为他不知道物理防御的弱点在哪里。

在本节中，我们会讨论如何用一些典型的扫描技术识别主机和它们开放的端口号，以及网络上的漏洞。

> 注意
>
> 到目前为止，本书说的「连接两端」都是指发送者和接收者，或者客户端和服务器。而本章提到的「连接两端」却是指攻击者或受害者。