

12.3 漏洞利用

攻击者是吃饭还是喝粥，就要看漏洞利用阶段的表现了。攻击者已经研究并侦察好目标，并发现了准备利用的漏洞，期望以此进入目标系统。在本章剩下的篇幅里，我们将关注在一些漏洞利用技术中捕获的数据包。这些漏洞包括近期的 Microsoft 漏洞、通过 ARP 缓存污染攻击重定向流量，以及盗窃数据的远程访问特洛伊木马。