前　言 Preface

本书致力于介绍如何使用 Kali Linux 对网络执行渗透测试。渗透测试可以模拟内部或外部的恶意攻击者对网络或系统进行攻击。不同于漏洞评估，渗透测试包括漏洞利用阶段。因此，漏洞是存在的，而且如果不采取相应的措施将会有很大风险。

在这本书中，“渗透测试人员”“攻击者”和“黑客”使用完全相同的技术及工具评估网络和数据系统的安全性。他们之间唯一的区别是他们的目标——数据网络的安全或数据的外泄。

大多数的测试人员和攻击者遵循一个非正式的、开源的或专门定义的测试方法，指导测试过程。下面的一些方法有其固有的优势：

- 测试过程的部分方法可以自动生成（例如，测试人员可以经常使用 ping 扫描发现潜在的目标；因此，这可以作为脚本利用），鼓励测试人员把重点放在发现和利用漏洞的技术创新上。
- 结果是可重复的，允许反复比较，交叉验证测试的结果，确定随着时间的推移，目标的安全性是否有所改善。
- 定义的方法在时间和人员的要求方面是可见的，鼓励成本控制并使成本最小化。
- 测试方法已经预先获得客户批准，在对网络或数据造成任何损害时测试人员免责。

正式的方法包括以下著名的例子：

- Kevin Orrey 的渗透测试框架：这种方法为测试人员提供一个渗透测试的序列步骤，以及工具的超链接和相关命令。更多信息请参见 www.vulnerabilityassessment.co.uk。
- 信息系统安全评估框架（Information Systems Security Assessment Framework，ISSAF）：这个综合性指南的目标是单一的网络测试，更多信息请参见 www.oissg.org。
- NIST SP 800-115，信息安全测试和评估技术手册：完成于 2008 年，这种四步走的方法