第十五章 安全评估和测试

15.1 创建安全评估和测试程序

- 信息安全团队维护活动的基石就是他们的安全评估和测试程序，用来定期合适机构与重组的安全控制以及这些安全控制可以正常运行以便有效的保护信息资产

15.1.1 安全测试

- 安全测试能够验证控制运行正常：测试包括自动扫描、工具辅助渗透测试和手动测试，安全团队可设计和验证一个综合的评估测试策略
- 安全专家仔细审核测试结果，保证每个测试是成功的

15.1.2 安全评估

- 安全评估是对系统、应用程序或其他测试环境的综合评价
- 安全评估工具的主要产出物是一份用于管理的评估报告，报告以非技术的语音描述评估结果，并且以具体建议作为结论，从而提高被测环境的安全性

15.1.3 安全审计

- 安全审计会使用与安全评估期间相同的许多技术，但必须由独立的审计员执行
- 审计员对安全控制的状态做出的评估应公正、无偏见，他们编写的报告与安全评估报告非常类似
- 内部审计由组织的内部审计人员执行且通常也是为了内部使用

15.2 执行漏洞评估

- 漏洞评估是信息安全专家工具箱的重要测试工具，为安全专家找到系统或应用在技术控制方面的弱点

15.2.1 漏洞扫描

- 漏洞扫描会自动对系统、应用程序和网络进行探测，寻找可能被攻击者利用的弱点
- 漏洞扫描分三种
    - 网络发现扫描：使用多种技术对一系列IP地址进行扫描，搜索配有开放网络端口的系统，不能探测系统漏洞
        - TCP SYN扫描：向每个被扫描的端口发送带有SYN标志设置的单个数据包
        - TCP 连接扫描：向指定端口的远程系统打开一个全连接
        - TCP ACK扫描：发送带有ACK标志设置的单个数据包

        - Xmas 扫描：发送带有FIN、PSH和URG标志设置的数据包
    - 网络漏洞扫描： 在检测到开放端口后继续调查目标系统或网络来查找已知漏洞，还能执行一些测试，来确定系统是否已收到数据库中的每个漏洞影响
    - WEB漏洞扫描：在WEB应用程序中搜寻已知漏洞的专用工具

15.2.2 渗透测试

- 渗透测试：为了试图让安全控制失效，进入目标系统或应用程序来展示缺陷
- 渗透测试分三种
    - 白盒测试：为攻击者提供目标系统的详细情况，缩短了攻击事件并增加了发现安全漏洞的可能性
    - 灰盒测试：部分知识测试
    - 黑盒测试：不为攻击者提供任何信息，模拟外部攻击者在进行攻击之前试图获取业务和技术环境信息的情况

15.3 测试你的软件

- 软件是系统安全的关键组成部分，仔细测试软件对每一个现代组织的机密性、完整性和可用性都是至关重要的

15.3.1 代码审查和测试

- 代码审核和测试可能再缺陷生效并对经营产生负面影响之前发现安全、性能或可靠性缺陷
    - 代码审查：除了写代码的人以外的开发人员进行审查、查找缺陷
    - 静态测试：在不运行软件的情况下通过分析源代码或编译的 应用程序对软件进行评估，通常用来检测常用软件缺陷（如缓冲区溢出）的自动化工具
    - 动态测试：在运行环境中评估软件安全，对部署别人写的应用程序的组织来说说通常是唯一选择
    - 模糊测试：一项专门的动态测试技术，向软件提供许多不同类型的输入，来强调其局限性并发现先前未发现的缺陷
        - 变异模糊测试：从软件的实际操作中提取之前的输入值，对其进行处理以创建模糊输入
        - 智能模糊测试：开发数据模型并创建新的模糊输入

15.3.2 接口测试

- 接口测试是开发复杂软件系统的一个重要部分，接口测试针对接口规范的性能，以确保所有开发工作完成后模块能正常运行
    - 应用编程接口（API）：为代码模块提供一种标准的方式进行交互
    - 用户界面（UI）:为终端用户提供与软件交互的能力，测试包括审查所有的用户界面来验证他们能否正常运作

    - 物理接口：一些操作机器、逻辑控制器或物理世界中其他对象的应用程序存在

15.3.3 误用案例测试：

- 软件测试人员使用称为误用测试案例或滥用用例测试的过程来评估他们的软件对于那些已知风险的脆弱性

15.3.4 测试覆盖率分析

- 软件测试专业人员经常进行测试覆盖率分析，进行估计对新软件进行测试的程度

15.4 实现安全管理过程

15.4.1 日志审核

- 信息安全管理人员应该定期对日志进行审查，特别是敏感功能，以确保特权用户不滥用特例

15.4.2 账户管理

- 账户管理审核确保用户只保留授权权限，而没有发生未经授权的修改

15.4.3 备份验证

- 管理人员定期检查备份的结果，确保过程有效执行，满足组织的数据保护需求

15.4.4 关键性能指标和风险指标

- 安全管理人员应该维持监视关键性指标和风险指标
    - 开放漏洞的数量
    - 解决漏洞的时间
    - 被盗账户的数量
    - 在生产前扫描中发现的软件缺陷数
    - 重复审计发现
    - 访问恶意网站的用户尝试