

NIST 特别出版物

800-115

**NIST**

**National Institute of  
Standards and Technology**

Technology Administration  
U.S. Department of Commerce

**信息安全测试和评价**

**技术指南**

**国家标准和技术研究所的建议**

**Karen Scarfone  
Murugiah Souppaya  
Amanda Cody**

---

## 计算机安全

---

国家标准和技术研究所  
信息技术实验室  
计算机安全处

Gaithersburg, MD 20899-8930

2008 年 9 月



美国商务部  
部长: Carlos M. Gutierrez

国家标准和技术研究所  
副主任: Patrick D. Gallagher博士

# 目录

## 执行摘要

### 1. 概述

- 1.1 权限
- 1.2 目的和适用范围
- 1.3 适用对象
- 1.4 本文的篇章结构

### 2. 安全测试和查验综述

- 2.1 信息安全评价方法
- 2.2 用于技术评价的技术手段
- 2.3 测试和查验比较
- 2.4 测试的角度
  - 2.4.1 外部的和内部的
  - 2.4.2 公开的和隐蔽的

### 3. 审查技术

- 3.1 文件审查
- 3.2 日志审查
- 3.3 规则集审查
- 3.4 系统配置审查
- 3.5 网络嗅探
- 3.6 文件完整性检查
- 3.7 总结

### 4. 目标识别和分析技术

- 4.1 网络发现
- 4.2 网络端口和服务识别
- 4.3 漏洞扫描
- 4.4 无线扫描
  - 4.4.1 被动无线扫描
  - 4.4.2 主动无线扫描
  - 4.4.3 无线设备位置跟踪
  - 4.4.4 蓝牙扫描
- 4.5 总结

### 5. 目标漏洞验证技术

- 5.1 口令破解
- 5.2 渗透测试
  - 5.2.1 渗透测试的各个阶段
  - 5.2.2 渗透测试的后勤准备
- 5.3 社会工程
- 5.4 总结

### 6. 安全评价规划

- 6.1 制定一项安全评价策略
- 6.2 评价的优先顺序排列和进度表安排

- 6.3 挑选和定制技术手段
- 6.4 评价的后勤准备
  - 6.4.1 评价员的挑选和技能
  - 6.4.2 地点选择
  - 6.4.3 技术工具和资源选择
- 6.5 评价计划的制定
- 6.6 法律方面的考虑
- 6.7 总结
- 7. 安全评价的执行**
  - 7.1 协调
  - 7.2 评价
  - 7.3 分析
  - 7.4 数据处理
    - 7.4.1 数据收集
    - 7.4.2 数据保存
    - 7.4.3 数据传输
    - 7.4.4 数据销毁
- 8. 测试后活动**
  - 8.1 抑制建议
  - 8.2 报告
  - 8.3 补救/抑制
- 附录 A 活套件安全测试 CD 盘**
- 附录 B 合约规则模板**
- 附录 C 应用安全测试和查验**
- 附录 D 远程访问测试**
- 附录 E 参考资料**
- 附录 F 术语表**
- 附录 G 缩写词和缩略语**