

中华人民共和国国家标准

中华人民共和国

GB/T 36627—2018

信息安全技术
网络安全等级保护测试评估技术指南

technology—

Information security

classified cybersecurity protection

Testing and evaluation technical guide for

2018-09-07 发布

2018-04-01 实施

国家市场监督管理总局

发布

中国合格评定国家认可委员会

目 次

前言	III	引言	III
1 范围	IV	1 范围	IV
2 规范性引用文件	1	2 规范性引用文件	1
3 术语和定义、缩略语	1	3 术语和定义、缩略语	1
3.1 术语和定义	1	3.1 术语和定义	1
3.2 缩略语	2	3.2 缩略语	2
4 概述	2	4 概述	2
4.1 技术分类	2	4.1 技术分类	2
4.2 技术选择	2	4.2 技术选择	2
5 等级测评要求	2	5 等级测评要求	2

前言

[illegible]


 铁路作为交通经济大动脉，以高质量服务助力春运

1. **Identify the main components of the system.** The system consists of a **client** and a **server**. The client is responsible for sending requests to the server, and the server is responsible for processing these requests and returning responses.

中国医药有限公司 上海分公司 地址：上海南京路100号

1. **Introduction**
 2. **Background**
 3. **Methodology**
 4. **Results**
 5. **Discussion**
 6. **Conclusion**
 7. **References**
 8. **Appendix**
 9. **Figure 1**
 10. **Figure 2**
 11. **Figure 3**
 12. **Figure 4**
 13. **Figure 5**
 14. **Figure 6**
 15. **Figure 7**
 16. **Figure 8**
 17. **Figure 9**
 18. **Figure 10**
 19. **Figure 11**
 20. **Figure 12**
 21. **Figure 13**
 22. **Figure 14**
 23. **Figure 15**
 24. **Figure 16**
 25. **Figure 17**
 26. **Figure 18**
 27. **Figure 19**
 28. **Figure 20**
 29. **Figure 21**
 30. **Figure 22**
 31. **Figure 23**
 32. **Figure 24**
 33. **Figure 25**
 34. **Figure 26**
 35. **Figure 27**
 36. **Figure 28**
 37. **Figure 29**
 38. **Figure 30**
 39. **Figure 31**
 40. **Figure 32**
 41. **Figure 33**
 42. **Figure 34**
 43. **Figure 35**
 44. **Figure 36**
 45. **Figure 37**
 46. **Figure 38**
 47. **Figure 39**
 48. **Figure 40**
 49. **Figure 41**
 50. **Figure 42**
 51. **Figure 43**
 52. **Figure 44**
 53. **Figure 45**
 54. **Figure 46**
 55. **Figure 47**
 56. **Figure 48**
 57. **Figure 49**
 58. **Figure 50**
 59. **Figure 51**
 60. **Figure 52**
 61. **Figure 53**
 62. **Figure 54**
 63. **Figure 55**
 64. **Figure 56**
 65. **Figure 57**
 66. **Figure 58**
 67. **Figure 59**
 68. **Figure 60**
 69. **Figure 61**
 70. **Figure 62**
 71. **Figure 63**
 72. **Figure 64**
 73. **Figure 65**
 74. **Figure 66**
 75. **Figure 67**
 76. **Figure 68**
 77. **Figure 69**
 78. **Figure 70**
 79. **Figure 71**
 80. **Figure 72**
 81. **Figure 73**
 82. **Figure 74**
 83. **Figure 75**
 84. **Figure 76**
 85. **Figure 77**
 86. **Figure 78**
 87. **Figure 79**
 88. **Figure 80**
 89. **Figure 81**
 90. **Figure 82**
 91. **Figure 83**
 92. **Figure 84**
 93. **Figure 85**
 94. **Figure 86**
 95. **Figure 87**
 96. **Figure 88**
 97. **Figure 89**
 98. **Figure 90**
 99. **Figure 91**
 100. **Figure 92**
 101. **Figure 93**
 102. **Figure 94**
 103. **Figure 95**
 104. **Figure 96**
 105. **Figure 97**
 106. **Figure 98**
 107. **Figure 99**
 108. **Figure 100**
 109. **Figure 101**
 110. **Figure 102**
 111. **Figure 103**
 112. **Figure 104**
 113. **Figure 105**
 114. **Figure 106**
 115. **Figure 107**
 116. **Figure 108**
 117. **Figure 109**
 118. **Figure 110**
 119. **Figure 111**
 120. **Figure 112**
 121. **Figure 113**
 122. **Figure 114**
 123. **Figure 115**
 124. **Figure 116**
 125. **Figure 117**
 126. **Figure 118**
 127. **Figure 119**
 128. **Figure 120**
 129. **Figure 121**
 130. **Figure 122**
 131. **Figure 123**
 132. **Figure 124**
 133. **Figure 125**
 134. **Figure 126**
 135. **Figure 127**
 136. **Figure 128**
 137. **Figure 129**
 138. **Figure 130**
 139. **Figure 131**
 140. **Figure 132**
 141. **Figure 133**
 142. **Figure 134**
 143. **Figure 135**
 144. **Figure 136**
 145. **Figure 137**
 146. **Figure 138**
 147. **Figure 139**
 148. **Figure 140**
 149. **Figure 141**
 150. **Figure 142**
 151. **Figure 143**
 152. **Figure 144**
 153. **Figure 145**
 154. **Figure 146**
 155. **Figure 147**
 156. **Figure 148**
 157. **Figure 149**
 158. **Figure 150**
 159. **Figure 151**
 160. **Figure 152**
 161. **Figure 153**
 162. **Figure 154**
 163. **Figure 155**
 164. **Figure 156**
 165. **Figure 157**
 166. **Figure 158**
 167. **Figure 159**
 168. **Figure 160**
 169. **Figure 161**
 170. **Figure 162**
 171. **Figure 163**
 172. **Figure 164**
 173. **Figure 165**
 174. **Figure 166**
 175. **Figure 167**
 176. **Figure 168**
 177. **Figure 169**
 178. **Figure 170**
 179. **Figure 171**
 180. **Figure 172**
 181. **Figure 173**
 182. **Figure 174**
 183. **Figure 175**
 184. **Figure 176**
 185. **Figure 177**
 186. **Figure 178**
 187. **Figure 179**
 188. **Figure 180**
 189. **Figure 181**
 190. **Figure 182**
 191. **Figure 183**
 192. **Figure 184**
 193. **Figure 185**
 194. **Figure 186**
 195. **Figure 187**
 196. **Figure 188**
 197. **Figure 189**
 198. **Figure 190**
 199. **Figure 191**
 200. **Figure 192**
 201. **Figure 193**
 202. **Figure 194**
 203. **Figure 195**
 204. **Figure 196**
 205. **Figure 197**
 206. **Figure 198**
 207. **Figure 199**
 208. **Figure 200**
 209. **Figure 201**
 210. **Figure 202**
 211. **Figure 203**
 212. **Figure 204**
 213. **Figure 205**
 214. **Figure 206**
 215. **Figure 207**
 216. **Figure 208**
 217. **Figure 209**

引 言

网络安全等级保护测评过程包括测评准备活动、方案编制活动、现场测评活动、报告编制活动四个

信息安全技术

网络安全等级保护测试评估技术指南

1 范围

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。

GB 17859—1999 信息安全等级保护基本要求

GB 35118—2017 网络安全等级保护基本要求

3 术语和定义、缩略语

3.1 术语和定义

和定义适用于本文件。

GB 17859—1999 及 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1.1

字典式攻击 dictionary attack

在破解口令时,逐一尝试用户自定义词库中的单词或短语的攻击方式

3.1.2

文件完整性检查 file integrity checking

3.1.3

3.1.4

源地址 rule set

3.1.5

测试对象 target testing and evaluation

等级保护实施过程中不同阶段的工作对象,主要是与等级保护实施相关的系统、设备、网络、人员等

3.2 缩略语

下列缩略语适用于本文件。

漏洞库(China National Vulnerability Database)	CNVD; 国家信息安全漏洞库
域名系统(Domain Name System)	DNS; 域名系统(Domain Name System)
分布式拒绝服务(Distributed Denial of Service)	DDoS; 分布式拒绝服务
报文协议(Internet Control Message Protocol)	ICMP; Internet 控制报文协议
入侵检测系统(Intrusion Detection System)	IDS; 入侵检测系统
入侵防御系统(Intrusion Prevention System)	IPS; 入侵防御系统
安全外壳协议(Secure Shell)	SSH; 安全外壳协议(Secure Shell)
服务集标识(Service Set Identifier)	SSID; 服务集标识(Service Set Identifier)
结构化查询语言(Structured Query Language)	SQL; 结构化查询语言(Structured Query Language)
虚拟专用网络(Virtual Private Network)	VPN; 虚拟专用网络(Virtual Private Network)

4 概述

4.1 技术分类

可用于等级测评的测评技术分为以下三类。

1. 文档检查技术：通过检查被测对象的文档，了解其安全策略、管理制度、技术措施等。	2. 配置检查技术：通过检查被测对象的配置，了解其安全配置、系统参数、网络设置等。
3. 漏洞扫描技术：通过扫描被测对象的漏洞，了解其安全漏洞、系统弱点、安全风险等。	4. 渗透测试技术：通过模拟攻击者的行为，验证漏洞的存在性和可利用性。
5. 社会工程学：通过利用人的心理弱点，获取敏感信息、系统权限等。	6. 物理攻击：通过物理手段，破坏被测对象的硬件设施、窃取数据等。

4.2 技术选择

1. 文档检查技术：适用于所有等级的测评，是基础性的技术。	2. 配置检查技术：适用于所有等级的测评，是基础性的技术。
3. 漏洞扫描技术：适用于所有等级的测评，是基础性的技术。	4. 渗透测试技术：适用于高级别的测评，是进阶性的技术。
5. 社会工程学：适用于高级别的测评，是进阶性的技术。	6. 物理攻击：适用于高级别的测评，是进阶性的技术。

5 等级测评要求

5.1 检查技术

5.1.1 文档检查

保护对象运营单位提供的文档，评价其策略和措施的技术准确性。文档检查的主要功能是基于等级

和完整性。进行文档检查时,可考虑以下评估要素:

a) 检查对象的安全策略,是系统的防御策略,还是为系统提供技术支持的防御策略;

b) 检查对象的安全策略是否满足国家法律法规和标准规范的要求;

c) 检查对象的安全策略是否经过审批,审批流程是否完整,审批记录是否完整;

d) 检查对象的安全策略是否经过更新,更新流程是否完整,更新记录是否完整;

e) 检查对象的安全策略是否经过培训;

f) 检查对象的安全策略是否经过演练;

g) 检查对象的安全策略是否经过评估;

h) 检查对象的安全策略是否经过备案;

i) 检查对象的安全策略是否经过发布;

j) 检查对象的安全策略是否经过实施;

k) 检查对象的安全策略是否经过监督;

l) 检查对象的安全策略是否经过改进;

m) 检查对象的安全策略是否经过总结;

n) 检查对象的安全策略是否经过归档;

o) 检查对象的安全策略是否经过销毁;

p) 检查对象的安全策略是否经过备份;

q) 检查对象的安全策略是否经过恢复;

r) 检查对象的安全策略是否经过验证;

s) 检查对象的安全策略是否经过测试;

t) 检查对象的安全策略是否经过部署;

u) 检查对象的安全策略是否经过维护;

v) 检查对象的安全策略是否经过更新;

w) 检查对象的安全策略是否经过发布;

x) 检查对象的安全策略是否经过实施;

y) 检查对象的安全策略是否经过监督;

z) 检查对象的安全策略是否经过改进;

aa) 检查对象的安全策略是否经过总结;

ab) 检查对象的安全策略是否经过归档;

ac) 检查对象的安全策略是否经过销毁;

ad) 检查对象的安全策略是否经过备份;

ae) 检查对象的安全策略是否经过恢复;

af) 检查对象的安全策略是否经过验证;

ag) 检查对象的安全策略是否经过测试;

ah) 检查对象的安全策略是否经过部署;

ai) 检查对象的安全策略是否经过维护;

aj) 检查对象的安全策略是否经过更新;

ak) 检查对象的安全策略是否经过发布;

al) 检查对象的安全策略是否经过实施;

am) 检查对象的安全策略是否经过监督;

an) 检查对象的安全策略是否经过改进;

ao) 检查对象的安全策略是否经过总结;

ap) 检查对象的安全策略是否经过归档;

aq) 检查对象的安全策略是否经过销毁;

ar) 检查对象的安全策略是否经过备份;

as) 检查对象的安全策略是否经过恢复;

at) 检查对象的安全策略是否经过验证;

au) 检查对象的安全策略是否经过测试;

av) 检查对象的安全策略是否经过部署;

aw) 检查对象的安全策略是否经过维护;

5.1.3 规则集检查

规则集的漏洞,检查对象包括网络设备、安全设

备、操作系统、数据库系统、应用系统、移动终端

等。检查对象的安全策略是否满足国家法律法规

和标准规范的要求,审批流程是否完整,审批

记录是否完整,更新流程是否完整,更新记录

是否完整,培训记录是否完整,演练记录是否

完整,评估记录是否完整,备案记录是否完整,

发布记录是否完整,实施记录是否完整,监督

记录是否完整,改进记录是否完整,总结记录

是否完整,归档记录是否完整,销毁记录是否

完整,备份记录是否完整,恢复记录是否完整,

验证记录是否完整,测试记录是否完整,部署

记录是否完整,维护记录是否完整,更新记录

是否完整,发布记录是否完整,实施记录是否

完整,监督记录是否完整,改进记录是否完整,

总结记录是否完整,归档记录是否完整,销毁

记录是否完整,备份记录是否完整,恢复记录

是否完整,验证记录是否完整,测试记录是否

完整,部署记录是否完整,维护记录是否完整,

更新记录是否完整,发布记录是否完整,实施

规则集检查的主要功能是发现基于规则集的安全控

制策略、策略集、策略集及策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

的策略集、策略集的策略集、策略集的策略集、

策略集的策略集、策略集的策略集、策略集的策略

集、策略集的策略集、策略集的策略集、策略集

访问规则；
 存储在操作系统的用户数据，在操作系统的支持下，它能够实现细粒度的强制访问

相同的访
 2) 以立体形

见前注。

2) 日志数据应存储在能可靠的用户数据，在故障排除时系统的其他部分应能访问。

5.1.4 配置检查

配置检查是指对系统配置进行检查，以确保系统配置符合安全要求。配置检查应包括以下内容：

- 1) 检查系统配置是否符合安全要求。
- 2) 检查系统配置是否符合国家有关标准。
- 3) 检查系统配置是否符合行业有关标准。
- 4) 检查系统配置是否符合企业有关标准。
- 5) 检查系统配置是否符合用户有关标准。

5.1.5 文件完整性检查

文件完整性检查是指对系统文件完整性进行检查，以确保系统文件完整性。文件完整性检查应包括以下内容：

- 1) 检查系统文件完整性是否符合安全要求。
- 2) 检查系统文件完整性是否符合国家有关标准。
- 3) 检查系统文件完整性是否符合行业有关标准。
- 4) 检查系统文件完整性是否符合企业有关标准。
- 5) 检查系统文件完整性是否符合用户有关标准。

5.1.6 密码检查

密码检查是指对系统密码进行检查，以确保系统密码安全。密码检查应包括以下内容：

- 1) 检查系统密码是否符合安全要求。
- 2) 检查系统密码是否符合国家有关标准。
- 3) 检查系统密码是否符合行业有关标准。
- 4) 检查系统密码是否符合企业有关标准。
- 5) 检查系统密码是否符合用户有关标准。

5.2 安全检测技术

5.2.1 网络嗅探

网络嗅探的主要功能是实时监控网络流量，收集、识别网络中传输的数据，检测系统和网络

安全事件，并生成安全事件报告。网络嗅探技术广泛应用于网络安全检测、入侵检测和应急响应

等领域。网络嗅探技术可以实现对网络流量的实时监控，及时发现异常流量和攻击行为。

网络嗅探技术的主要优点是：实时监控网络流量，及时发现异常流量和攻击行为。

网络嗅探技术的主要缺点是：只能检测网络流量，无法检测系统内部的安全事件。

口及端口的状态。——

d) 在网络边界处部署网络嗅探器,用以评估进出网络的流量;

去陪山遊仁德廟雙園故址探要 田川河什海礁海邊這具的楓面春

5.2.2 网络端口和服务识别

、相关服务与应用程序。进行网络

网络端口和服务识别的主要功能是识别活动设备上开放的端口。端口和服务识别时,可考虑以下评估要素和评估原则:

a) 对主机及存在潜在漏洞的端口进行识别, 以便于确定渗透型

50 在試圖努力界外執行掃描時，就使用命令，例如，重裝。

5.2.3 漏洞扫描

2011年12月15日 星期四

© 2004 Blackwell Publishing Ltd, *Journal of Internal Medicine* 255: 111–118

一、从《说文解字》看“美”字

[illegible]

②三翻四拍前,扫描设备应更新升级

d) 依据湿润扫描工具的湿润分析原理, 检测评估对象故障。

—他因患肝病而設法去印度打獵健康——

5.2.4 无线扫描

[illegible]

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

5.3 漏洞验证技术

5.3.1 口令破解

口令破解技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

5.3.2 渗透测试

渗透测试技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

5.3.3 系统漏洞扫描

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

5.3.2 渗透测试

渗透测试的主要功能是通过模拟恶意黑客的攻击方法，攻击等级保护对象的应用程序、系统或者网络，以验证系统的安全性和完整性。

5.3.3 系统漏洞扫描

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

5.3.3 系统漏洞扫描

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

系统漏洞扫描技术主要功能是在系统运行过程中通过系统日志、数据库、应用程序、配置文件、系统文件、网络流量等方式获取系统口令，并对口令进行破解。

5.3.3 远程访问测试

远程访问测试的主要功能是评估远程访问方法中的漏洞,发现未授权的接入方式。进行远程访问

测试时,应采取以下步骤:

a) 发现除 VBN、SSH 远程桌面规则之外是否存在其他的非授权的接入方式。

通过 b) 发现未授权的远程访问服务,通过端口扫描定级经常用于进行远程访问的开放的端口。

附录 A
(资料性附录)
测评后活动

4. a. $\text{NaOH} + \text{H}_2\text{SO}_4 \rightarrow \text{Na}_2\text{SO}_4 + \text{H}_2\text{O}$

A. 板内应力(六分制)

定和排除误报,对漏洞进行分类,并确定产生漏洞的原因,此外,找出漏洞。以下列举了常见的造成漏洞的根本原因,包括:

测评结果分析的主要目标是确
在整个测评中需要立即处理的严重

定 额 编 制 总 则 及 各 分 部 分 定 额 的 编 制 说 明 书 均 在 本 册 附 录 中 有 详 细 说 明 书 及 图 表 。

1. 一般情形: 若 α 是 A 的特征值, β 是 B 的特征值, 则 $\alpha + \beta$ 是 $A + B$ 的特征值, $\alpha\beta$ 是 AB 的特征值.

Kristin A. Brownlee, Julia M. Dwyer, J. Scott Armstrong, Robert C.

三、我國目前之失業現象與經濟政策

安全配置策略

c) 缺乏安全基準,同類的系統使用了不一或部

离开或不满足安全要求,直至满足安全要求为止。

③ 在系统开发时经常需要维护某些数据,如系统

1000



系统松存在缺陷,如安全投入未能有效汇集或至系统运行如前,安全投入仍难有效发挥。

樂全堂

本会受理「聯合聲明」後，本會即與各股東簽訂「聯合聲明」，並由本會代為辦理各項登記手續，包括：(1) 辦理「聯合聲明」之登記；(2) 辦理「聯合聲明」之變更登記；(3) 辦理「聯合聲明」之註銷登記；(4) 辦理「聯合聲明」之其他登記事項。

喜在喧喧藉流木，不知滲透幽篁清淨心。

Figure 1

[illegible]

2013年12月10日 星期二

A horizontal strip of six small, square, black and white photographs. From left to right: 1. A person sitting on a bench. 2. A person standing in a field. 3. A person sitting on a bench. 4. A person standing in a field. 5. A person sitting on a bench. 6. A person standing in a field.

— 125 —

A.2 提出改进建议

© 2006 Pearson Education, Inc. All rights reserved. Printed in the United States of America. This publication is protected by copyright. Any unauthorized reproduction or distribution without the written permission of Pearson Education, Inc., may cause severe penalties under applicable law.

Figure 1. The effect of the number of trials on the number of correct responses.

A.3 报告

在测评结果分析完成之后,宜生成包括系统安全问题、漏洞及其改进建议的报告。测评结果可用于以下几个方面:

- a) 作为实施改正措施的参考;
- b) 制定改进措施以修补确认的漏洞;
- c) 作为测速对象运营单位为使等级保护对象满足安全要求而采取改进措施的基准。

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was significantly higher than the number of incorrect responses in all cases. Error bars represent the standard error of the mean.

[illegible]

B.1 综述

模拟攻击者,利用攻击者常用的工具和技
术,对单一漏洞,大量做渗透测试试

渗透测试是一种安全性测试,在该类测试中,测试人员将模
拟攻击者常用的工具和技
术,对单一漏洞,大量做渗透测试试

复杂程度

b) 攻击者需要突破系统所面临的大体

e) 可减少系统威胁的其他对策;

d) 防御者能够检测攻击者并做出反应

的能力

还需要丰富的专业知识和技能,尽管有经验的测试

渗透测试是一种非常重要的安全测试,测试人

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

测试人员在渗透测试中,通常

这个阶段的渗透攻击测试过程通常包括规划、发现、攻击和报告四个阶段。

图 B.1 渗透测试阶段

图 B.1 渗透测试阶段

B.2.1 概述

见图 B.1 所示

渗透测试通常包括规划、发现、攻击、报告四个阶段,如

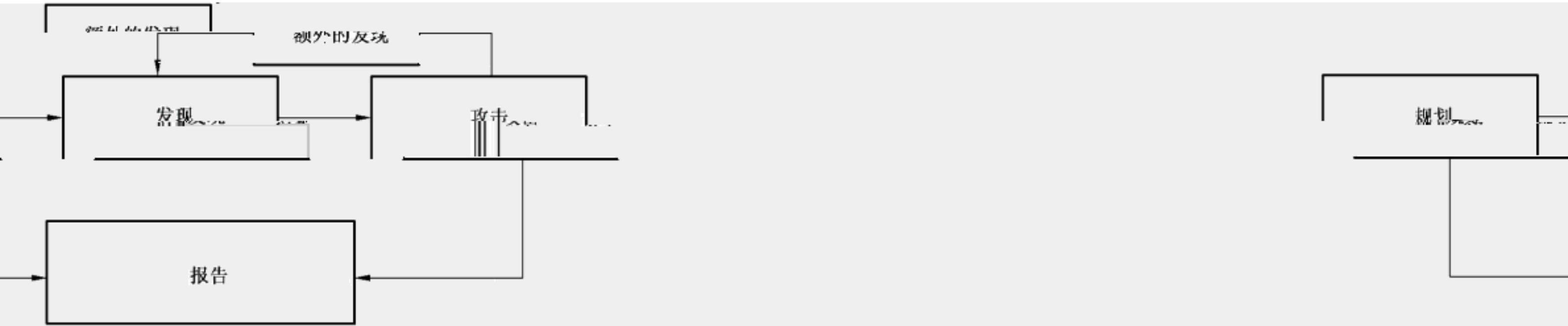


图 B.1 渗透测试的四个阶段

B.2.2 规划阶段

在规划阶段,确定规则,管理层审批定稿,记录在案,并设定测试目标。规划阶段为一个成功的渗透
测试奠定基础,在渗透测试发生之前进行测试。

□ □ □ 42 70 74 84

363 452 559

渗透测试的发现阶段包括两个部分：

[illegible]

1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2677, 2678, 2679, 26

第三, 数据是决策制定和运营优化的关键。通过收集和分析运营数据, 企业可以识别瓶颈、优化流程、提高资源利用率, 从而实现运营效率的提升。

B.2.4 攻击阶段

柱状土且经采测定的核子土段段且。今通过升原生确实的泥泥池。止燃木。进而按常港在

— *Journal of the American Medical Association*, 1997

[illegible]

B.2.5 報告除毀

B.3 渗透测试方案

渗透测试方案宜侧重于在应用程序、系统或网络中的设计和实现中,定位和挖掘出可利用的漏洞缺

2022 年 12 月 16 日 星期五 第 16 期

1. *Journal of the American Medical Association*, 1997; 277: 1001-1005.

Figure 1. The effect of the number of trials on the number of correct responses. The number of correct responses was plotted against the number of trials for each condition. The number of correct responses increased with the number of trials for all conditions. The number of correct responses was highest for the condition with the highest number of trials (10 trials) and lowest for the condition with the lowest number of trials (2 trials).

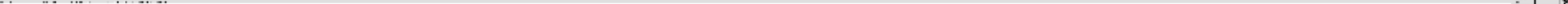
[illegible][illegible]

[illegible]

Figure 1. The effect of the number of iterations on the accuracy of the proposed algorithm. The accuracy of the proposed algorithm increases with the number of iterations. The accuracy of the proposed algorithm is 100% when the number of iterations is 100.

R 4 渗透测试风险

常会利用攻击者常用的工具和技术来对被测系统和数据发动真实攻击。在渗透测试过程中,测试人员通





在 对

B.5 渗透测试风险规避



1. 2010年10月1日起，凡在中华人民共和国境内销售货物或者提供加工、修理修配劳务以及进口货物的单位和个人，均应按照《中华人民共和国增值税暂行条例》及实施细则缴纳增值税。

1. 四川成都: 蜀人生活, 2010. 6. 10. 2. 四川成都: 蜀人生活, 2010. 6. 10.

An aerial photograph of a city skyline, likely New York City, showing a wide river (the Hudson River) and a large bridge (the George Washington Bridge) spanning it. The city buildings are visible on the opposite bank. The image is oriented horizontally.

000000

GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[1] GB

GB/T 20270—2006 信息安全技术 网络基础安全技术要求

[2] GB

GB/T 20271—2006 信息安全技术 网络信息安全技术要求

[3] GB

GB/T 20272—2006 信息安全技术 数据库安全技术要求

[4] GB

GB/T 20273—2006 信息安全技术 云计算安全技术要求

[5] GB

GB/T 20274—2006 信息安全技术 物联网安全技术要求

[6] GB

GB/T 20275—2006 信息安全技术 即时通信安全技术要求

[7] GB

GB/T 20276—2006 信息安全技术 网络钓鱼安全技术要求

[8] GB

GB/T 20277—2006 信息安全技术 网络蠕虫安全技术要求

[9] GB

GB/T 20278—2006 信息安全技术 网络病毒安全技术要求

[10] GB

GB/T 20279—2006 信息安全技术 网络木马安全技术要求

[11] GB

GB/T 20280—2006 信息安全技术 网络僵尸网络安全技术要求

[12] GB

GB/T 20281—2006 信息安全技术 网络垃圾邮件安全技术要求

[13] GB

GB/T 20282—2006 信息安全技术 网络垃圾短信安全技术要求

[14] GB

GB/T 20283—2006 信息安全技术 网络垃圾电话安全技术要求

[15] GB

GB/T 20284—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[16] GB

GB/T 20285—2006 信息安全技术 网络垃圾短信网关安全技术要求

[17] GB

GB/T 20286—2006 信息安全技术 网络垃圾电话网关安全技术要求

[18] GB

GB/T 20287—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[19] GB

GB/T 20288—2006 信息安全技术 网络垃圾短信网关安全技术要求

[20] GB

GB/T 20289—2006 信息安全技术 网络垃圾电话网关安全技术要求

[21] GB

GB/T 20290—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[22] GB

GB/T 20291—2006 信息安全技术 网络垃圾短信网关安全技术要求

[23] GB

GB/T 20292—2006 信息安全技术 网络垃圾电话网关安全技术要求

[24] GB

GB/T 20293—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[25] GB

GB/T 20294—2006 信息安全技术 网络垃圾短信网关安全技术要求

[26] GB

GB/T 20295—2006 信息安全技术 网络垃圾电话网关安全技术要求

[27] GB

GB/T 20296—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[28] GB

GB/T 20297—2006 信息安全技术 网络垃圾短信网关安全技术要求

[29] GB

GB/T 20298—2006 信息安全技术 网络垃圾电话网关安全技术要求

[30] GB

GB/T 20299—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[31] GB

GB/T 20300—2006 信息安全技术 网络垃圾短信网关安全技术要求

[32] GB

GB/T 20301—2006 信息安全技术 网络垃圾电话网关安全技术要求

[33] GB

GB/T 20302—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[34] GB

GB/T 20303—2006 信息安全技术 网络垃圾短信网关安全技术要求

[35] GB

GB/T 20304—2006 信息安全技术 网络垃圾电话网关安全技术要求

[36] GB

GB/T 20305—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[37] GB

GB/T 20306—2006 信息安全技术 网络垃圾短信网关安全技术要求

[38] GB

GB/T 20307—2006 信息安全技术 网络垃圾电话网关安全技术要求

[39] GB

GB/T 20308—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[40] GB

GB/T 20309—2006 信息安全技术 网络垃圾短信网关安全技术要求

[41] GB

GB/T 20310—2006 信息安全技术 网络垃圾电话网关安全技术要求

[42] GB

GB/T 20311—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[43] GB

GB/T 20312—2006 信息安全技术 网络垃圾短信网关安全技术要求

[44] GB

GB/T 20313—2006 信息安全技术 网络垃圾电话网关安全技术要求

[45] GB

GB/T 20314—2006 信息安全技术 网络垃圾邮件网关安全技术要求

[46] GB

GB/T 20315—2006 信息安全技术 网络垃圾短信网关安全技术要求

[47] GB

GB/T 20316—2006 信息安全技术 网络垃圾电话网关安全技术要求

[48] GB

中 华 人 民 共 和 国

国 家 标 准

信息安全技术

网络安全等级保护测试评估技术指南

GB/T 36627—2018

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

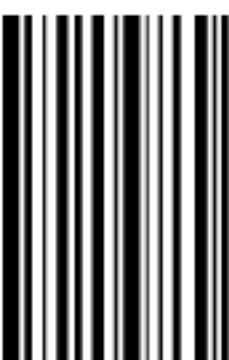
网址: www.spc.org.cn

服务热线: 400-168-0010

2018年9月第一版

*

书号: 155066 · 1-61231



GB/T 36627—2018

中国标准出版社

版权受保护 侵权必究

