

《安全审核与风险分析》目录



全书由 9 章组成，主要内容包括：安全审核入门、审核过程、系统资源侦查、审核服务器渗透和攻击技术、控制阶段的安全审核、审核和日志分析、审核结果、入侵检测系统、早期预警与事件响应。

本书具有教材和技术资料双重特征，既可以作为网站安全管理的培训、自学教材，又可以是网络工程技术人员和安全管理的技术参考资料。

本书内容新颖，实例丰富，语言文字通俗易懂；各单元重点、难点突出，原理、技术和方法的阐述融于丰富的实例之中，并配有习题；书中安排有实验，便于教学和自学。

第 1 单元：安全审核入门	1-1
课前问题	1-2
审核人员的工作	1-3
审核人员的职责和前瞻性	1-3
风险评估	1-6
风险评估阶段	1-14
差距分析	1-15
划分资产风险等级	1-16
进行安全审核所要考虑的事项	1-17
获得最高管理者的支持	1-18
获取客户信息的反馈	1-19
单元练习	1-21
第 2 单元：审核过程	2-1
课前问题	2-2
检查书面安全策略	2-3

美国威凯普斯公司北京代表处

中国·北京·朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>

划分资产等级.....	2-5
识别业务重点.....	2-9
使用现有安全管理控制体系.....	2-9
配置基于网络和主机的漏洞扫描和分析软件.....	2-11
实施网络级和主机级安全扫描.....	2-16
考虑路由器和防火墙的安全配置.....	2-19
确定电话服务系统或集成系统的安全等级.....	2-23
评估现有备份机制的执行效率.....	2-24
安全审核阶段.....	2-24
单元练习.....	2-26
第 3 单元：系统资源侦查.....	3-1
课前问题.....	3-2
侦查方法.....	3-3
安全扫描.....	3-4
物理侦查.....	3-25
采访面谈.....	3-26
企业级审核工具.....	3-27
社会工程.....	3-34
你能获得什么信息.....	3-36
单元练习.....	3-42
第 4 单元：审核服务器渗透和攻击技术.....	4-1
课前问题.....	4-2
网络渗透技术.....	4-3
攻击特征和审核.....	4-3

美国威凯普斯公司北京代表处

中国·北京·朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>

危及安全的服务	4-3
易受攻击的目标	4-4
路由器	4-4
数据库	4-5
Web 服务器和 FTP 服务器	4-6
电子邮件服务器	4-7
名称服务	4-8
审核系统 BUG	4-9
审核 Trap Door 和 rootkit	4-9
审核拒绝服务攻击	4-11
结合所有攻击制定审核策略	4-13
拒绝服务和 TCP/IP 堆栈	4-16
单元练习	4-23
第 5 单元：控制阶段的安全审核	5-1
课前问题	5-2
网络控制	5-3
控制阶段的目标	5-3
控制方法	5-15
渗透到其他系统	5-26
控制阶段的审核	5-27
单元练习	5-35
第 6 单元：审核和日志分析	6-1
课前问题	6-2
日志分析	6-3

美国威凯普斯公司北京代表处

中国·北京·朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>

建立基线.....	6-3
防火墙和路由器日志.....	6-3
操作系统日志.....	6-3
日志过滤.....	6-12
审核可疑活动.....	6-17
其他类型的日志.....	6-18
日志的存储.....	6-18
审核对系统性能的影响.....	6-18
单元练习.....	6-21
第 7 单元：审核结果	7-1
课前问题.....	7-2
建立审核报告.....	7-3
收集客户意见.....	7-3
制定详细审核报告.....	7-3
推荐的审核方案.....	7-4
建立审核步骤.....	7-5
安全审核和安全标准.....	7-6
增强路由器安全.....	7-9
实施主动检测.....	7-10
主机审核解决方案.....	7-11
升级和替代服务.....	7-19
单元练习.....	7-25
第 8 单元：入侵检测系统	8-1
课前问题.....	8-2

美国威凯普斯公司北京代表处

中国·北京·朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>

入侵检测系统的概念.....	8-3
入侵检测的分类.....	8-4
建立一个有效的入侵检测体系.....	8-8
创建和配置 IDS 规则.....	8-10
IDS 的动作与行为.....	8-10
IDS 主动审核和被动审核.....	8-10
入侵检测系统常用的检测方法.....	8-11
基于内核的入侵检测系统 (LIDS).....	8-13
入侵检测技术发展方向.....	8-17
知名的入侵检测系统软件.....	8-19
如何选择入侵检测产品.....	8-22
单元练习.....	8-35
第 9 单元：早期预警与事件响应.....	9-1
课前问题.....	9-2
为不可避免的状况做准备.....	9-3
蜜网.....	9-4
配置问题.....	9-11
做好响应计划.....	9-11
建立响应策略.....	9-11
提前做决定.....	9-12
保持镇定.....	9-12
做出正确的反应.....	9-12
记录下所有的事件.....	9-13
分析攻击的形式.....	9-13

美国威凯普斯公司北京代表处

中国·北京·朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>

确定攻击的范围.....	9-14
制止和牵制黑客活动.....	9-14
实施响应计划.....	9-14
分析和学习.....	9-16
建立容灾备份计划.....	9-16
常用容灾备份技术.....	9-16
单元练习.....	9-21

美国威凯普斯公司北京代表处

中国.北京.朝阳区建国门外秀水街一号建外外交公寓 1-4-42/43 100600

Tel: 86.10.85325600 Fax: 86.10.8532.5300

<http://www.CIWchina.com> <http://www.CIWcertified.com>