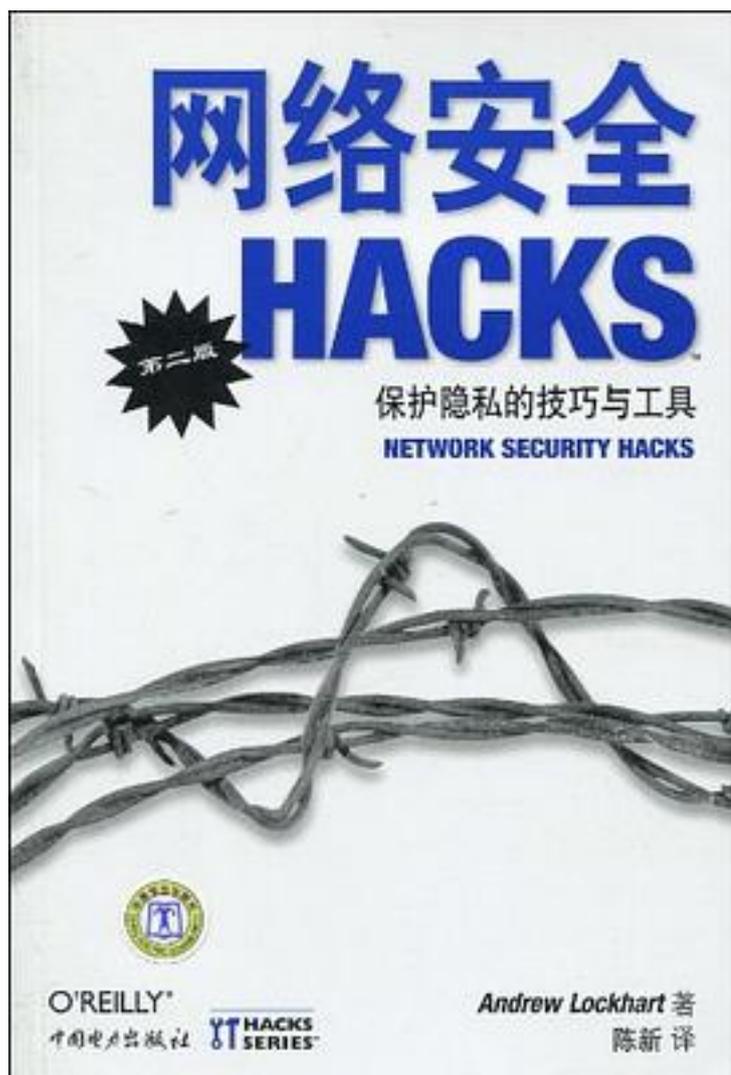


网络安全HACKS



[网络安全HACKS_下载链接1](#)

著者:洛克哈特

出版者:中国电力出版社

出版时间:2010-3

装帧:

isbn:9787508392790

《网络安全Hacks(第2版)》内容简介：入侵者用于网络攻击的技术在发展，因此用于保护自己 and 网络的工具和方法也必须及时修改以跟上步伐。《网络安全Hacks(第2版)》更新了所有系统关键的工具，并为两年前不存在的问题提供了灵活的解决方案。

新版本展示了如何检测网络入侵者的存在，使用强加密保护网络和数据，甚至要为可能的系统破坏者设下埋伏。相比以前的版本，新版本更大、更广泛，并更具有实用性，它陈述了125个真实世界的工具和技巧，专家就是用这些手段来加强他们对攻击者的防护。

在《网络安全Hacks(第2版)》中，您将看到一些很有用的检测并处理入侵者的技术，学到以下内容：

- 通过躲避网络流量分析和加密电子邮件来保护隐私。
- 通过captive portal(强制网络门户)共享无线网络，使用良好粒度的鉴别来保护无线网络。
- 建立看起来容易遭受攻击的虚拟网络(蜜罐)，来转移攻击者注意力，或者迷惑攻击者。
- 加强Linux、BSD和Windows主机安全，防范攻击。
- 使用先进的入侵检测系统监视网络和服务。
- 使用强VPN解决方案通过互联网安全地连接两个远程站点。
- 检测系统漏洞，当系统遭受攻击时如何进行响应和恢复。

要获取更有效的安全工具，需要学习攻击者使用的最新技术。《网络安全Hacks(第2版)》提供了维持网络安全可靠所需的信息。

作者介绍:

Andrew Lockhart原来居住在美国南卡罗莱纳州,1现在居住于美国科罗拉多州北部.Andrew在那里学习了如何审计反汇编后的二进制文件,1并努力防止由于天气寒冷而被冻死.他拥有科罗拉多州立大学计算机系的理学学士学位,1并担任该州某些小型公司的安全顾问.1现在当不写作的时候,1他在Network Chemistry公司担当资深安全分析员,1该公司是无线安全解决方案最主要的提供商.Andrew还是无线漏洞及其应用项目(<http://www.0wirelessve.0org>)的编辑委员会成员之一,1并经常为他们刊登在Network-World上的无线安全专栏(<http://www.0networkworld.0com/topics/wireless-Security.0html>)出力.在业余时间,1他为一个名为Snort-Wireless(<http://snort-wireless.0org>)的项目组工作.该项目组主要研究如何为流行的开源IDS Snort增加无线入侵检测功能.

目录: 荣誉

前言

第1章 unix系统主机安全

1 保障mount点安全(初级难度)

2 扫描suid及sgid程序(初级难度)

3 扫描具有全局可写和组可写权限的目录(初级难度)

4 使用posix的acl(access control list. 访问控制表)来创建灵活的权限层次(中级难度)

5 保护日志不被篡改(初级难度)

- 6 授权管理员角色(初级难度)
 - 7 自动验证加密签名(中级难度)
 - 8 检查监听的服务(初级难度)
 - 9 阻止服务绑定某个接口(中级难度)
 - 10 采用沙盒(sandbox)环境来限制服务(高级难度)
 - 11 使用具有mysql验证源的proftpd工具(中级难度)
 - 12 防止堆栈粉碎攻击(高级难度)
 - 13 使用grsecurity锁定内核(高级难度)
 - 14 使用grsecurity工具限制应用程序(高级难度)
 - 15 使用systrace工具限制系统调用(高级难度)
 - 16 自动创建systrace工具的策略(高级难度)
 - 17 使用pam控制登录访问(中级难度)
 - 18 限制用户对scp和sftp的访问(高级难度)
 - 19 为身份认证使用一次性使用的密码(高级难度)
 - 20 限制shell环境(中级难度)
 - 21 加强对用户和组的资源的限制(中级难度)
 - 22 自动更新系统(初级难度)
- ## 第2章 windows系统主机安全
- 23 检查服务器所应用的补丁(中级难度)
 - 24 使用组策略来配置自动更新(初级难度)
 - 25 获得当前打开的文件及其进程的列表(初级难度)
 - 26 列出正在运行的服务和开放的端口(初级难度)
 - 27 启用系统审核功能(初级难度)
 - 28 枚举自动运行程序(中级难度)
 - 29 保障事件日志的安全(初级难度)
 - 30 修改日志文件大小的最大值(初级难度)
 - 31 备份和清除事件日志(中级难度)
 - 32 禁用默认共享(初级难度)
 - 33 加密临时文件夹(初级难度)
 - 34 备份efs(中级难度)
 - 35 在关机时清除页面文件(中级难度)
 - 36 检查永不过期的密码(中级难度)
- ## 第3章 隐私与匿名
- 37 躲避流量分析(中级难度)
 - 38 通过tor挖掘隧道ssh(初级难度)
 - 39 无缝加密文件系统(初级难度)
 - 40 预防网络钓鱼(中级难度)
 - 41 采用更少的密码来使用web(初级难度)
 - 42 使用thunderbird加密电子邮件(初级难度)
 - 43 在mac os x系统下加密电子邮件(初级难度)
- ## 第4章 防火墙
- 44 使用netfilter防火墙(初级难度)
 - 45 使用openbsd的防火墙packetfilter(初级难度)
 - 46 使用windows防火墙保护计算机(初级难度)
 - 47 关闭开放的端口和阻止协议(初级难度)
 - 48 替换windows防火墙(高级难度)
 - 49 建立身份认证网关(中级难度)
 - 50 使得网络自治化(中级难度)
 - 51 测试防火墙(中级难度)
 - 52 使用netfilter过滤物理地址(中级难度)
 - 53 阻止tor(高级难度)
- ## 第5章 加密与安全服务
- 54 使用ssl加密imap和pop(高级难度)
 - 55 采用sendmail使用支持tls的smtp(高级难度)

- 56 采用qmail使用支持tls的smtp(高级难度)
- 57 使用ssl和suexec来安装apache服务器(高级难度)
- 58 保障bind服务器的安全(高级难度)
- 59 安装小巧并安全的dns服务器(高级难度)
- 60 保障mysql服务器的安全(高级难度)
- 61 在unix系统下安全地共享文件(高级难度)

第6章 网络安全

- 62 检测arp欺骗攻击(初级难度)
- 63 建立静态arp表(中级难度)
- 64 保护ssh不受暴力攻击(高级难度)
- 65 欺骗远程操作系统检测软件(高级难度)
- 66 维持网络的产品清单(初级难度)
- 67 扫描网络漏洞(中级难度)
- 68 保持服务器时钟同步(初级难度)
- 69 创建自己的ca(初级难度)
- 70 向客户端发布您的ca证书(中级难度)
- 71 使用证书服务备份与恢复ca(中级难度)
- 72 远程检测以太网嗅探器(高级难度)
- 73 帮助追踪攻击者(初级难度)
- 74 在unix服务器上扫描病毒(中级难度)
- 75 追踪漏洞(初级难度)

第7章 无线安全

- 76 使您的便利无线路由器变成一个智能安全平台(高级难度)
- 77 为无线网络使用良好粒度的身份认证(高级难度)
- 78 配置captive portal(高级难度)

第8章 日志

- 79 运行集中式syslog服务器(中级难度)
- 80 操纵syslog工具(初级难度)
- 81 将windows系统整合到syslog基础设置中(中级难度)
- 82 自动归纳总结日志(中级难度)
- 83 自动监视日志(中级难度)
- 84 聚合来自远程站点的日志(高级难度)
- 85 使用进程记账技术来记录用户活动(中级难度)
- 86 集中监控服务器的安全形势(高级难度)

第9章 监视和趋势

- 87 监视可用性(中级难度)
- 88 趋势图(高级难度)
- 89 实时监控网络状况(初级难度)
- 90 使用防火墙规则收集统计信息(高级难度)
- 91 远程嗅探以太网(中级难度)

第10章 安全隧道

- 92 在linux系统下配置ipsec(中级难度)
- 93 在freebsd系统下配置ipsec(中级难度)
- 94 在openbsd系统下配置ipsec(中级难度)
- 95 使用openswan进行随机加密(高级难度)
- 96 通过ssh转发并加密流量(初级难度)
- 97 使用ssh客户密钥自动登录(初级难度)
- 98 通过ssh使用squid代理(中级难度)
- 99 将ssh用作socks代理(初级难度)
- 100 使用ssl加密流量，并为流量建立隧道(初级难度)
- 101 使用http内部的隧道连接(初级难度)
- 102 使用vtun和ssh建立隧道(中级难度)
- 103 自动生成vtun配置(中级难度)
- 104 创建跨平台的vpn(高级难度)

- 105 使用ppp隧道(中级难度)
- 第11章 网络入侵检测
- 106 使用snort进行入侵检测(中级难度)
- 107 持续关注报警(中级难度)
- 108 实时监视ids(高级难度)
- 109 管理探测器网络(高级难度)
- 110 编写您自己的snort规则(中级难度)
- 111 使用snort_inline来防御入侵和容侵(高级难度)
- 112 使用snortsam实现自动化的动态防火墙(高级难度)
- 113 检测异常行为(中级难度)
- 114 自动升级snort的规则库(中级难度)
- 115 创建一个分布式stealth探测代理网络{高级难度}
- 116 利用barnyard在高性能环境中使用snort(高级难度)
- 117 检测和阻止对web应用程序的入侵(中级难度)
- 118 扫描网络流量，发现病毒(高级难度)
- 119 模拟一个包含多个有漏洞主机的网络(高级难度)
- 120 记录honeypot活动(高级难度)
- 第12章 恢复与响应
- 121 镜像挂载的文件系统(中级难度)
- 122 检验文件完整性，寻找遭受破坏的文件(中级难度)
- 123 使用rpm寻找遭受破坏的程序包(初级难度)
- 124 查找系统中的rootkit(中级难度)
- 125 寻找网络的所有者(初级难度)
- • • • • [\(收起\)](#)

[网络安全HACKS 下载链接1](#)

标签

安全

网络安全

黑客

计算机

网络安全HACKS

信息安全

linux

计算机科学

评论

适合网管读的，防，非攻

浪费。

排班不行，没有重点，泛泛而谈

可以翻翻，但是只是各个主题用不同章讲不同工具的使用，相当于是一些tips，内容略过时

有启发，不通的思路，国内未必适用

信息略过时。

很早之前看的

[网络安全HACKS 下载链接1](#)

书评

书中很多实用的网络安全小技巧，有windows的，也有linux的。推荐对网络安全感兴趣的可以看看。在《网络安全Hacks

(第2版)》中，您将看到一些很有用的检测并处理入侵者的技术，学到以下内容：

- 通过躲避网络流量分析和加密电子邮件来保护隐私。
- 通过captive porta...

[网络安全HACKS_下载链接1](#)