

Оглавление

Введение	20
Глава 1. Как такое могло случиться, или Анатомия преступления	25
Глава 2. Принципы разграничения доступа	33
Глава 3. Базовые сведения	41
Глава 4. Пользователи, права доступа и файловые системы	73
Глава 5. Подключаемые модули аутентификации	99
Глава 6. Одноразовые пароли	135
Глава 7. Учет использования ресурсов	149
Глава 8. Журнальная регистрация	157
Глава 9. Как стать суперпользователем: утилита sudo	169
Глава 10. Защита сетевых служб: демон xinetd	191
Глава 11. Защищенный интерпретатор команд: система SSH	221
Глава 12. Программа Crack	285
Глава 13. Контроль системы: программа Bastille	309
Глава 14. Программа Tripwire	353
Глава 15. Программа ipchains	383
Глава 16. Программа iptables	427
Глава 17. Сетевые сканеры, анализаторы и детекторы	445
Глава 18. Управление журнальными файлами	499
Глава 19. Внедрение средств защиты	523
Приложение А. Web-ресурсы	533
Приложение Б. Программа OPIE	545
Приложение В. Защита сетевых служб: программы TCP_Wrappers и portmap	559
Приложение Г. CFS и TCFS	591
Предметный указатель	616