



Защита от вторжений
Расследование компьютерных преступлений
Кевин Мандиа, Крис Проспис
Изд. «ЛОРИ» / 2005 / 585582229X

Содержание

Благодарности
Предисловие
Введение

ЧАСТЬ I ВВЕДЕНИЕ В ПРОБЛЕМУ

Глава 1 Конкретный пример: Свои и чужие
Противодействие атакам
Реальный инцидент
Итоги

Глава 2 Введение в реагирование на компьютерные инциденты
Цели реагирования на инцидент
Методология реакции на инцидент
Подготовка к инциденту
Выявление инцидентов
Первоначальная реакция
Формирование стратегии реакции на инцидент
Судебное дублирование
Исследование
Сетевой мониторинг
Восстановление
Выбор стратегии восстановления
Отчет
Итоги

Глава 3 Подготовка к реагированию на компьютерный инцидент
Идентификация жизненно важных активов компании
Подготовка отдельных хостов
Подготовка сети
Установка подходящей политики и процедур безопасности
Создание набора инструментов для реагирования на инциденты
Формирование команды реагирования на инциденты
Итоги

ЧАСТЬ II БАЗОВЫЕ ЗНАНИЯ

Глава 4 Рекомендации по исследованию
Проведение первичной оценки
Список вопросов при уведомлении об инциденте
Исследование инцидента
Формулировка стратегии реагирования
Итоги

Глава 5 Компьютерный судебный процесс
Учимся обращаться с доказательствами
Выполнение начального реагирования
Выполнение судебного дублирования
Использование Safelock
Использование утилит UNIX для судебного дублирования
Использование Encase
Выполнение судебного анализа
Итоги

Глава 6 Изучение сетевых протоколов, ловушки и трассировка
Понимание TCP/IP
Инкапсуляция
Использование сетевого анализатора
Реализация ловушек и трассировки
Итоги

Глава 7 Выполнение сетевого наблюдения
Зачем выполнять сетевое наблюдение?
Доказательство на основе сети
Сетевая судебная экспертиза
Настройка системы
Выполнение наблюдения
Интерпретация сетевой атаки
Итоги

Глава 8 Дополнительные методы сетевого наблюдения
Цели профессиональных атакующих
Скрытое устройство каналов ICMP
Скрытое устройство каналов TCP без состояния
Скрытое устройство каналов HTTP
Обнаружение незаконных серверов
Итоги

ЧАСТЬ III ИССЛЕДОВАНИЕ СИСТЕМ

Глава 9 Начальное реагирование в системе Windows NT/2000

Создание инструментального набора реагирования

Сохранение информации полученной во время начального реагирования

Получение изменчивых данных до судебного дублирования

Выполнение углубленного, реального реагирования

Требуется ли выполнять судебное дублирование?

Итоги

Глава 10 Исследование системы Windows NT/2000

Где располагаются доказательства в системах Windows NT/2000

Настройка судебной рабочей станции

Выполнение исследования Windows NT/2000

Аудит файлов и кража информации

Действия в случае увольнения сотрудника

Итоги

Глава 11 Начальное реагирование в системах UNIX

Создание инструментального набора реагирования

Хранение информации, полученной во время начального реагирования

Получение изменчивых данных до судебного дублирования

Выполнение углубленного реагирования на действующей системе

Итоги

Глава 12 Исследование систем UNIX

Подготовка к критическому рассмотрению восстановленного образа

Проведение исследования UNIX

Итоги

ЧАСТЬ IV ИССЛЕДОВАНИЕ НЕЗАВИСИМЫХ ОТ ПЛАТФОРМЫ ТЕХНОЛОГИЙ

Глава 13 Исследование маршрутизаторов

Получение изменчивых данных до выключения питания

Поиск доказательства

Использование маршрутизаторов в качестве инструментов ответа

Итоги

Глава 14 Исследование Web-атак

До выключения питания

Поиск доказательств

Итоги

Глава 15 Исследование серверов приложений

Исследование инцидентов с сервером имен доменов

Исследование инцидентов с серверами FTP

Исследование инцидентов со службой RPC

Использование записей программ сетевого общения для исследования инцидентов

Обработка инцидентов, включающих Microsoft Office

Определение источника атак на приложения

Восстановление скомпрометированных серверов приложений
Итоги

Глава 16 Исследование инструментов хакера
Как компилируются файлы
Статический анализ утилит хакеров
Динамический анализ утилит хакеров
Итоги

ЧАСТЬ V ПРИЛОЖЕНИЯ

Приложение А Установление идентичности в киберпространстве

Исследование IP – адресов

Исследование адресов MAP

Трассировка e-mail

Исследование адресов e-mail, псевдонимов, имен пользователей и имен хостов

Раскрытие анонимности по юридическим каналам

Приложение В Политики информационной безопасности и политики допустимого использования

Области политики информационной безопасности

Политика допустимого использования

Приложение С Законодательные акты о компьютерных преступлениях

Федеральные законы о компьютерном вторжении

Федеральные законы об интеллектуальной собственности

Приложение D Организации реагирования