

Джуди Новак
Стивен Норткэтт

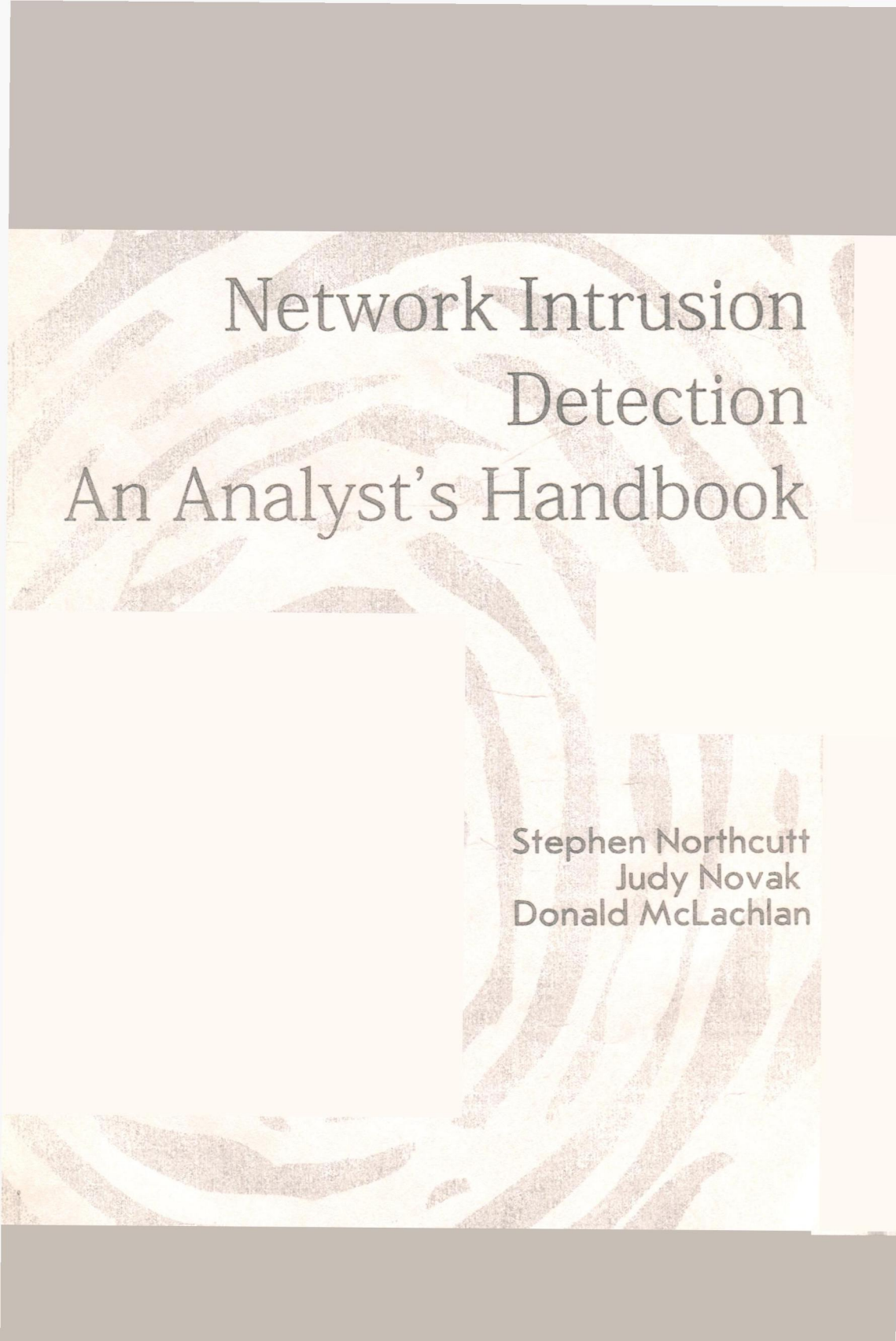


**КАК ОБНАРУЖИТЬ
ВТОРЖЕНИЕ
В СЕТЬ**

Как обнаружить вторжение в сеть

Джуди Новак, Стивен Норткатт, Дональд
Маклахлен

Издательство "ЛОРИ"



Network Intrusion
Detection
An Analyst's Handbook

Stephen Northcutt
Judy Novak
Donald McLachlan

Network Intrusion Detection
An Analyst's Handbook
Second Edition
Stephen Northcutt, Judy Novak, Donald McLachlan
All rights reserved

Как обнаружить вторжение в сеть
Настольная книга специалиста по системному анализу
Джуди Новак, Стивен Норткатт, Дональд Маклахлен

Переводчик И. Дранишников
Корректор Н. Литвинова
Верстка Л. Федерякиной

Copyright © by New riders Publishing. All rights reserved.
201 West 103rd Street, Indianapolis, Indiana 46290
ISBN 0-7357-1008-2

© Издательство "ЛОРИ", 2016

Изд. N : OAI (03)
ЛР N : 070612 30.09.97 г.
ISBN 978-5-85582-323-3

Подписано в печать 01.02.2016, Формат 70x100/16
Гарнитура Нью-Баскервиль, Печать офсетная
Печ.л. 26 Тираж 200

Содержание

Глава 1 Концепции протокола Интернета	1
Модель TCP/IP Интернета	2
Пакетирование	4
Адреса	8
Служебные порты	11
Протоколы IP	13
Система именования доменов	14
Маршрутизация	15
Итоги	17
Глава 2 Введение в TCPdump и TCP	18
TCPdump	18
Введение в TCP	24
Перекосы в работе TCP	30
Итоги	33
Глава 3 Фрагментация	35
Теория фрагментации	35
Злонамеренная фрагментация	43
Итоги	45
Глава 4 ICMP	47
Теория ICMP	47
Методы составления карты сети	50
Нормальные операции ICMP	54
Злонамеренные операции ICMP	57
Блокировать или не блокировать	63
Итоги	64
Глава 5 Стимул и реакция	65
Ожидаемое поведение	66
Связь протоколов	71
Итоги разделов об ожидаемом поведении и о связи протоколов	73

Аномальные стимулы	73
Нестандартный стимул, идентифицирующая операционную систему реакция	76
Итоги	81
Глава 6 DNS	82
Назад к основам — теория DNS	83
Обратный поиск	89
Использование DNS для разведки	93
Опасные ответы DNS	96
Итоги	99
Глава 7 Атака Митника	100
Использование TCP	100
Обнаружение атаки Митника	111
Сетевые системы обнаружения вторжения	111
Хостовые системы обнаружения вторжения	113
Предотвращение атаки Митника	115
Итоги	115
Глава 8 Введение в фильтры и сигнатуры	117
Политика фильтрации	117
Сигнатуры	118
Фильтры, используемые для обнаружения значимых событий	119
Примеры фильтров	120
Пример фильтра Snort	130
Дополнительная настройка фильтров	132
Итоги	135
Глава 9 Вопросы архитектуры	136
Значимые события	137
Ограничения наблюдения	138
Модель низко висящего фрукта	139
Человеческие факторы, ограничивающие возможности детектирования	140
Уровень серьезности	142
Контрмеры	144
Вычисление показателя серьезности	145
Размещение датчиков	148
Выталкивание и вытягивание	150
Консоль аналитика	152
Фильтры отображения	153
Обнаружения вторжения на хостах и в сети	155
Итоги	157

Глава 10	Возможность совместной работы и корреляция	158
Совместная работа нескольких компонентов		159
Коммерческие решения для совместной работы ID-систем		163
Корреляция		164
Базы данных SQL		175
Итоги		179
Глава 11	Сетевые средства обнаружения вторжения	181
Snort		182
Коммерческие инструментальные средства		182
Системы на основе UNIX		186
GOTS		189
Оценка систем обнаружения вторжения		191
Итоги		194
Глава 12	Направления дальнейшего развития	195
Наращение угроз		196
Улучшенные инструменты		197
Уточненное направление нападения		197
Мобильные программные конструкции		198
Внедрение через программы		198
Обмен информацией — наследие Y2K		200
Проверенный член организации		203
Улучшенная реакция		205
Еще раз об антивирусных средствах		206
Аппаратное обнаружение вторжения		206
Эшелонированная защита		207
Программное обнаружение вторжения		208
Мудрые аудиторы		209
Итоги		209
Глава 13	Методы нападения и сканирование для их реализации	210
Ложные тревоги		210
Методы нападения на IMAP		218
Сканирование для реализации методов нападения		222
Одиночный метод — Portmap		225
Итоги		232
Глава 14	Отказ в обслуживании	233
Трассировки грубых атак "отказ в обслуживании"		233
Элегантные атаки		238
Распределенные атаки "отказ в обслуживании"		243
Введение в DDOS		244
Итоги		245