

# УЧЕБНОЕ ПОСОБИЕ

для высших учебных заведений

СПЕЦИАЛЬНОСТЬ



## Системы обнаружения компьютерных атак



А. С. Коллеров, Н. И. Синадский, Д. А. Хорьков

# Оглавление

Введение.....	3
<b>1. Выявление сетевых атак путем анализа трафика...</b>	<b>5</b>
1.1. Понятие и систематика компьютерных атак.....	5
1.2. Этапы сетевой атаки .....	11
1.2.1. Исследование сетевой топологии .....	11
1.2.2. Обнаружение доступных сетевых служб .....	16
1.2.3. Выявление уязвимых мест атакуемой системы .....	20
1.3. Реализации атак .....	21
1.3.1. Атаки типа «отказ в обслуживании» .....	21
1.3.2. Выявление атаки на протокол SMB .....	23
<b>2. Системы обнаружения атак .....</b>	<b>27</b>
2.1. Основные типы СОА .....	27
2.1.1. Сигнатурный анализ и обнаружение аномалий .....	27
2.1.2. Обнаружение в реальном времени и отложенный анализ .....	31
2.1.3. Локальные и сетевые системы обнаружения атак ...	32
2.1.4. Распределенные системы обнаружения атак .....	33
2.2. Многоагентные СОА .....	35
2.2.1. Понятие многоагентной СОА и ее использование для обнаружения комплексных атак.....	35
2.2.2. Существующие реализации многоагентных СОА ....	36
2.3. Алгоритмы и модели СОА .....	37
2.3.1. Методы потенциальных функций .....	39
2.3.2. Методы опорных векторов SVM .....	39
2.3.3. Нейронные сети .....	40
2.3.4. Алгоритмы выравнивания последовательностей ....	41
2.3.5. Кластерный анализ .....	42
2.3.6. Обнаружение атак, основанное на скрытой модели Маркова .....	43
2.3.7. Метод MARS .....	44
2.3.8. Система запроса процессов PQS .....	44
2.3.9. Использование аппарата нечеткой логики для обнаружения атак .....	45

2.4. Параметры сетевого трафика, анализируемые COA ..	47
<b>3. Эксплуатация COA ..</b>	<b>49</b>
3.1. Система обнаружения атак Snort ..	49
3.1.1. Установка и запуск программы ..	49
3.1.2. Описание языка правил ..	50
3.1.3. Использование COA Snort ..	57
3.1.4. Использование препроцессоров Snort ..	59
3.2. Система обнаружения атак Suricata ..	62
3.2.1. Установка и настройка Suricata ..	62
3.2.2. Использование COA Suricata ..	64
3.3. Настройка комплекса Cisco IDS Sensor ..	66
3.3.1. Назначение COA Cisco IDS Sensor ..	66
3.3.2. Аппаратная часть COA Cisco IDS 4215 Sensor ..	69
3.3.3. Предварительная настройка COA Cisco IDS Sensor в режиме командной строки ..	71
3.3.4. Настройка COA Cisco IDS Sensor в режиме Web-интерфейса ..	77
3.4. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco IDS Sensor ..	80
3.4.1. Сигнатуры компьютерных атак COA Cisco IDS Sensor ..	80
3.4.2. Обнаружение атак исследования сетевой топологии ..	84
3.5. Обнаружение компьютерных атак на узлы сети с использованием комплекса Cisco MARS ..	88
3.5.1. Назначение комплекса Cisco MARS ..	88
3.5.2. Аппаратная часть комплекса Cisco MARS ..	90
3.5.3. Структура лабораторного стенда ..	91
3.5.4. Настройка ОС Windows 2003 Server ..	93
3.5.5. Настройка сетевых интерфейсов Cisco MARS ..	96
3.5.6. Настройка сетевого взаимодействия устройств Cisco IDS Sensor, Cisco MARS и сервера Windows 2003 Server ..	97
3.5.7. Создание сигнатуры компьютерной атаки в COA Cisco IDS Sensor ..	99
3.5.8. Имитация и обнаружение атакующего воздействия ..	100
3.6. Обнаружение компьютерных атак на узлы сети с использованием COA Cisco Security Agent и Cisco MARS ..	105
3.6.1. Назначение COA Cisco Security Agent ..	105
3.6.2. Структура лабораторного стенда ..	106
3.6.3. Настройка сетевых интерфейсов Cisco MARS ..	107

---

3.6.4. Подключение к интерфейсу центра управления CSA	108
3.6.5. Интерфейс центра управления CSA .....	112
Вопросы для проверки знаний .....	113
Обозначения и сокращения .....	118
Литература .....	119