БПОУ РА «Горно-Алтайский государственный политехнический колледж им. М. З. Гнездилова»

Модуль обнаружения вредоносного ПО в сетевом трафике

Выполнила: студентка группы 1077
Шабыков Алан Артурович
Руководитель: Завчук Ирина Петровна

Цели и задачи работы

Целью работы является модуль обнаружения вредоносного программного обеспечения в сетевом трафике.

Задачи:

- Определить основные угрозы информационной безопасности
- Изучить проблемы обеспечения безопасности сети
- Исследовать современные методики анализа сетевого трафика

Угрозы информационной безопасности

- *Отсутствие блокировки компьютера на время отсутствия пользователя.*
- *Несанкционированное отключение элементов защиты пользователями*
- *Использование сомнительного программного обеспечения*
- *Отсутствие разграничения доступа*

Системы мониторинга и анализ сетевого трафика

- *Системы управления сетью* (Network Management Systems)
- *Встроенные системы диагностики и управления* (Embedded systems)
- *Анализаторы протоколов* (Protocol analyzers)
- *Многофункциональные устройства анализа и диагностики.*

Оборудование для диагностики и сертификации кабельных систем

Системы обнаружения и предотвращения вторжений

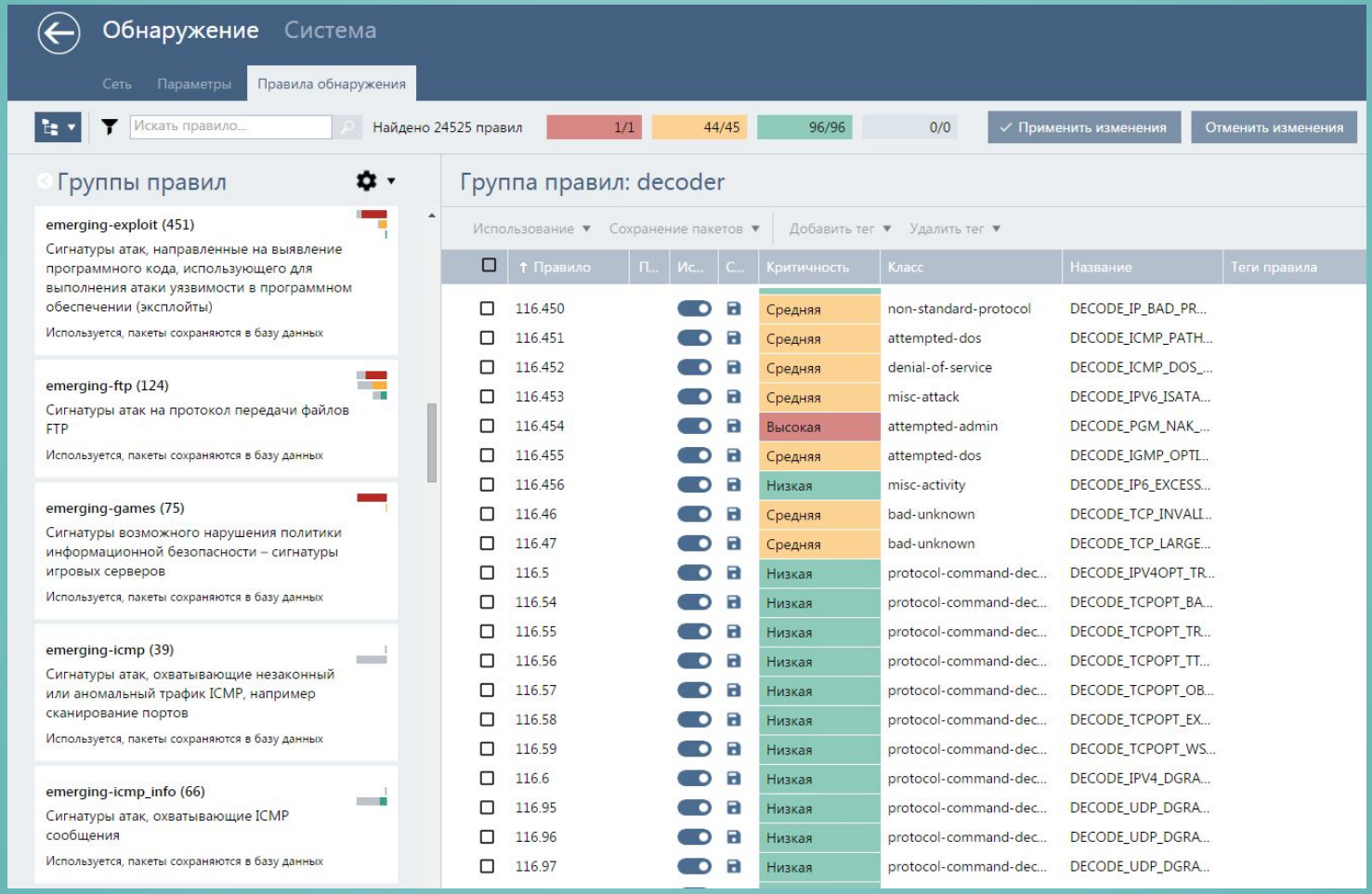
Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS))

Система предотвращения вторжений (СПВ) (англ. Intrusion Prevention System (IPS))

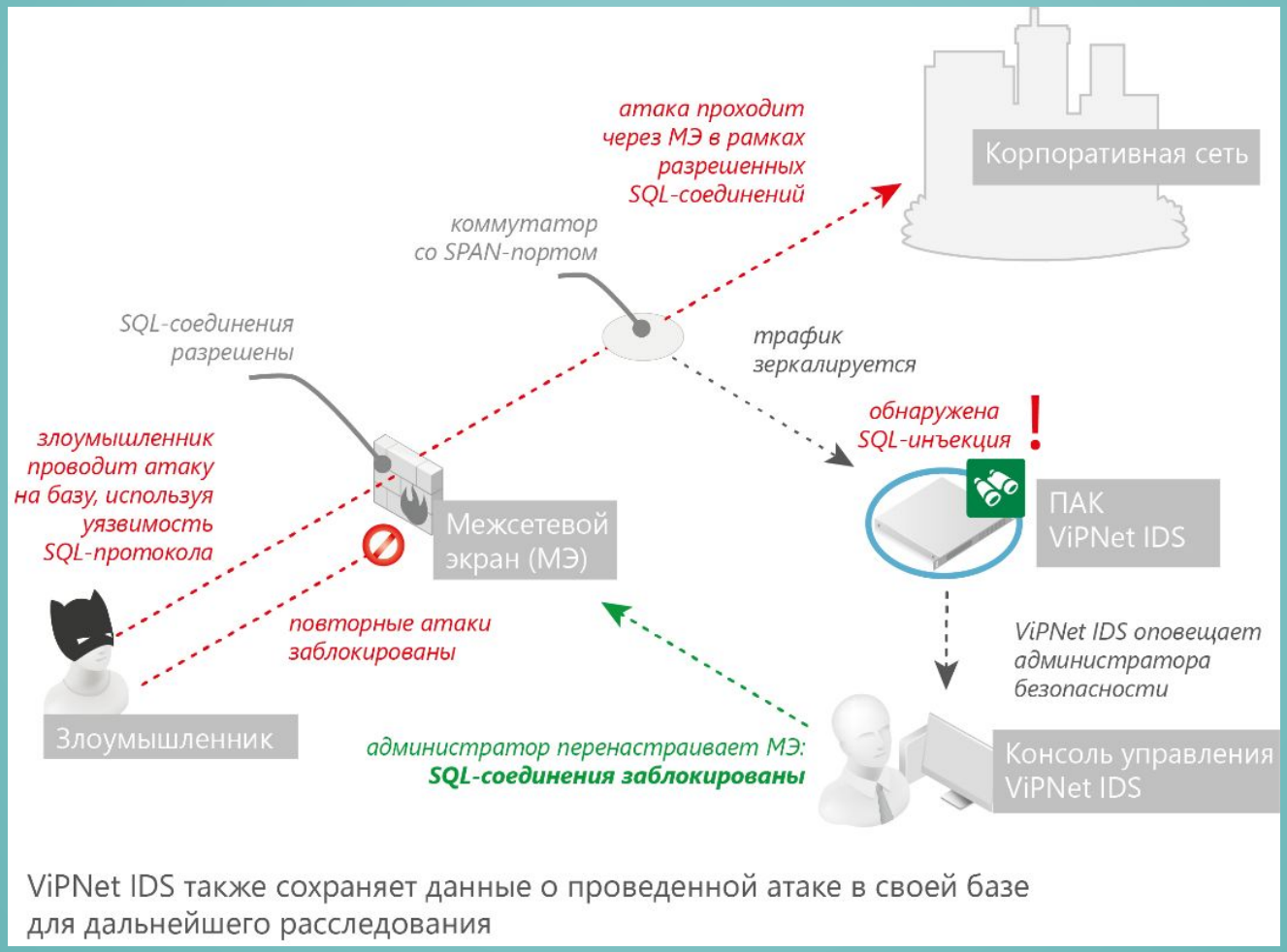
Методики обнаружения аномального и злоумышленного поведения пользователей

ViPNet
IDS

ViPNet IDS


Обнаружение
Система
Сеть
Параметры
Правила обнаружения
Искать правило...
Найдено 24525 правил
1/1
44/45
96/96
0/0
Применить изменения
Отменить изменения
Группы правил
emerging-exploit (451)
Сигнатуры атак, направленные на выявление программного кода, использующего для выполнения атаки уязвимости в программном обеспечении (эксплойты)
Используется, пакеты сохраняются в базу данных
emerging-ftp (124)
Сигнатуры атак на протокол передачи файлов FTP
Используется, пакеты сохраняются в базу данных
emerging-games (75)
Сигнатуры возможного нарушения политики информационной безопасности – сигнатуры игровых серверов
Используется, пакеты сохраняются в базу данных
emerging-icmp (39)
Сигнатуры атак, охватывающие незаконный или аномальный трафик ICMP, например сканирование портов
Используется, пакеты сохраняются в базу данных
emerging-icmp_info (66)
Сигнатуры атак, охватывающие ICMP сообщения
Используется, пакеты сохраняются в базу данных
Группа правил: decoder
Использование
Сохранение пакетов
Добавить тег
Удалить тег
Правило
Критичность
Класс
Название
Теги правила
116.450 Средняя non-standard-protocol DECODE_IP_BAD_PR...
116.451 Средняя attempted-dos DECODE_ICMP_PATH...
116.452 Средняя denial-of-service DECODE_ICMP_DOS_...
116.453 Средняя misc-attack DECODE_IPV6_ISATA...
116.454 Высокая attempted-admin DECODE_PGM_NAK_...
116.455 Средняя attempted-dos DECODE_IGMP_OPTI...
116.456 Низкая misc-activity DECODE_IP6_EXCESS...
116.46 Средняя bad-unknown DECODE_TCP_INVALI...
116.47 Средняя bad-unknown DECODE_TCP_LARGE...
116.5 Низкая protocol-command-dec... DECODE_IPV4OPT_TR...
116.54 Низкая protocol-command-dec... DECODE_TCPOPT_BA...
116.55 Низкая protocol-command-dec... DECODE_TCPOPT_TR...
116.56 Низкая protocol-command-dec... DECODE_TCPOPT_TT...
116.57 Низкая protocol-command-dec... DECODE_TCPOPT_OB...
116.58 Низкая protocol-command-dec... DECODE_TCPOPT_EX...
116.59 Низкая protocol-command-dec... DECODE_TCPOPT_WS...
116.6 Низкая protocol-command-dec... DECODE_IPV4_DGRA...
116.95 Низкая protocol-command-dec... DECODE_UDP_DGRA...
116.96 Низкая protocol-command-dec... DECODE_UDP_DGRA...
116.97 Низкая protocol-command-dec... DECODE_UDP_DGRA...

Обнаружение атаки и предотвращение ее развития



ViPNet IDS также сохраняет данные о проведенной атаке в своей базе для дальнейшего расследования

БПОУ РА «Горно-Алтайский государственный политехнический колледж им. М. З. Гнездилова»

Механизм управления продажами продукции предприятия

Выполнила: студентка группы 1077
Шабыков Алан Артурович
Руководитель: Завчук Ирина Петровна