Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ОТЧЕТ О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ №2**

**по дисциплине**  
 **«Технологии проектирования программного обеспечения»**

Работу выполнил студент группы 35/2 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т. Э. Айрапетов

Направление подготовки: 02.03.03 Математическое обеспечение и администрирование информационных систем

Отчет принял   
доц. каф. ИТ            А. Н. Полетайкин

Тема: Анализ существующих компьютерных разработок.

Цель: ознакомление с существующими разработками подобных программных решений по выбранной теме, приобретение навыков анализа существующих компьютерных разработок.

Задание:

1. Выполнить системное описание существующих подобных программных систем (не менее двух), которые могут быть применены к данному объекту управления; выделить основные преимущества и недостатки представленных систем.

2. Выполнить сравнительную характеристику описанных систем. Результаты сравнительного анализа представить в табличной форме. Набор основных показателей для сравнения:

* назначение системы;
* эффективность системы;
* гибкость системы;
* защищенность системы;
* живучесть системы;
* надежность системы;
* открытость системы;
* оптимальность использования ресурсов;
* удобство пользовательского интерфейса системы;
* стоимость системы (в том числе затраты на тех. поддержку);
* эргономичность.

3. Сделать вывод о возможности или невозможности использования этих систем на выбранном объекте информатизации.

Индивидуальная тема: ПС обнаружения вторжений в компьютерной сети.

**1. Системное описание существующих программных систем.** *Классическая IDS — Snort*. Это система с открытым кодом, созданная еще в 1998 году. Система Snort разрабатывалась как независимое ПО, а в 2008 году ее приобрела компания Cisco, которая теперь является партнером и разработчиком. Snort лучше подходит маленьким и средним компаниям. Утилита включает в себя сниффер пакетов, поддерживает настройку правил и многое другое. Snort — инструмент для тех, кто ищет понятную и функциональную систему предотвращения вторжений.

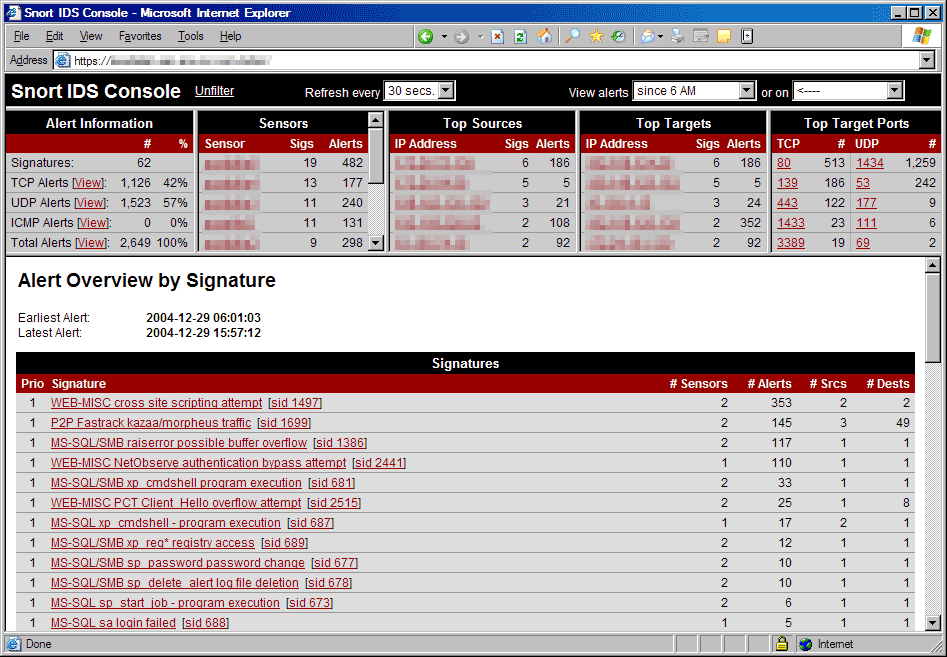


Рисунок 1 – IDS Snort

*Zeek.* Полностью бесплатная IDS с открытым исходным кодом. Поддерживает работу как в стандартном режиме обнаружения вторжений, так и в режиме обнаружения вредоносных сигнатур. Zeek может также обнаруживать события и позволяет задавать собственные скрипты политик. Недостаток Zeek — сложность общения с инструментом, так как разработка ведется с упором на функциональность, а не графический интерфейс.

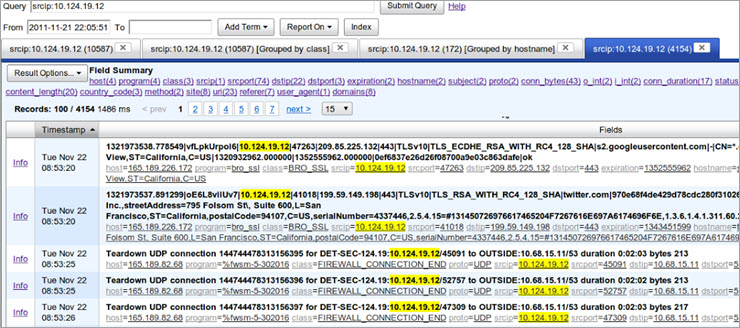


Рисунок 2 – IDS Zeek

*McAfee Network Security Platform*. Если вы большая компания, располагающая значительным бюджетом, можете рассмотреть McAfee Network Security Platform со стартовой ценой около $10 000. IDS блокирует огромное количество угроз, доступ к вредоносным сайтам, предотвращает DDoS-атаки и т. д. В силу монументальности McAfee Network Security Platform может замедлять работу сети, поэтому тут требуется решить, что более значимо — интеграция с другими сервисами или максимальная безопасность.

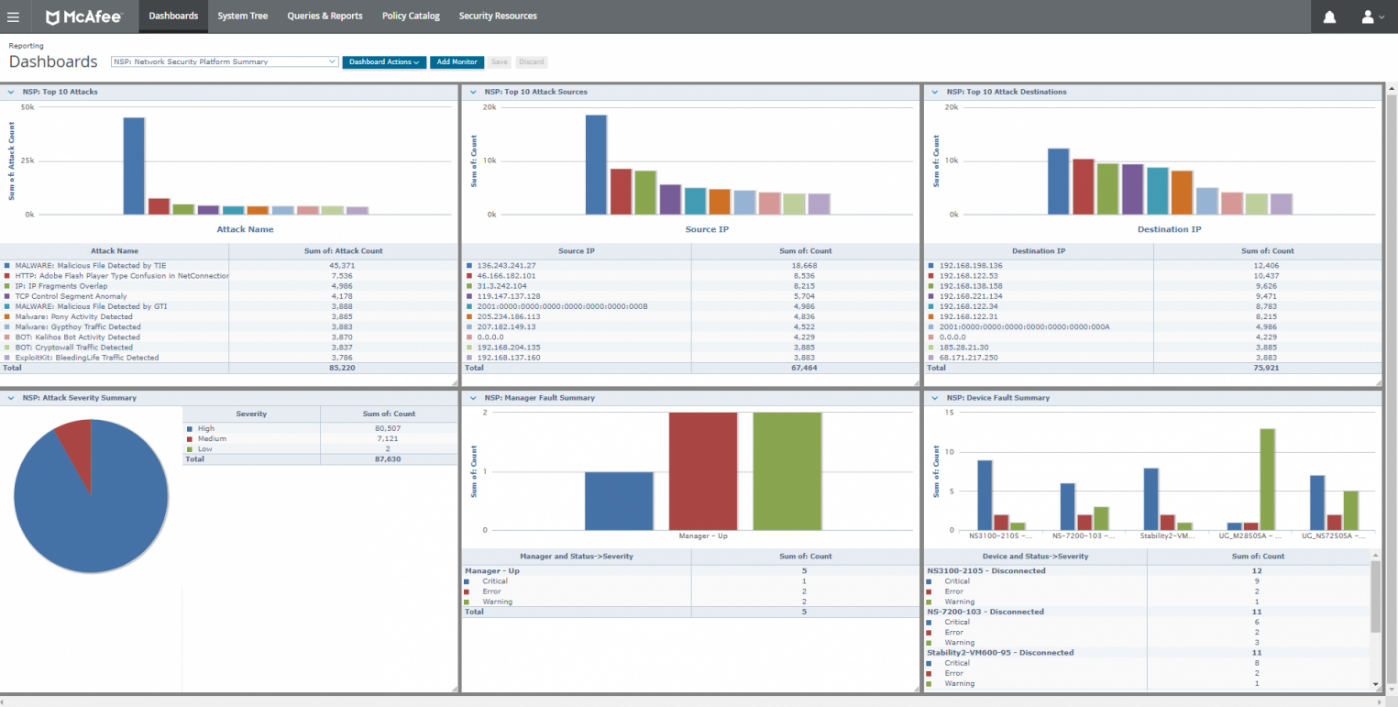


Рисунок 3 – IDS McAffee NSP

*Suricata* — довольно молодая система, и это ее преимущество. В Suricata нет большого количества legacy-кода, также система использует более новые разработки, чем у конкурентов. Благодаря этому Suricata работает быстрее. Кроме того, разработчики позаботились о совместимости со стандартными утилитами анализа результатов. Это значит, что Suricata поддерживает те же модули, что и Snort. Она способна выявлять угрозы по сигнатурам и подходит для средних и больших компаний.



Рисунок 4 – IDS Suricata

**2. Сравнительный анализ.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название/  Показатель | Snort | Zeek | McAffee NSP | Suricata |
| Работоспособность | подходит для маленьких-средних компаний | подходит для многих сценариев | покрывает практически любой сценарий | подходит для многих сценариев |
| Надежность | функционирует при средних нагрузках | выдерживает большие нагрузки | выдерживает DDoS-атаки | выдерживает большие нагрузки |
| Открытость | система открыта | система открыта | система закрыта | система открыта |
| Удобность интерфейса | интуитивно понятен | отсутствует удобный | интуитивно понятен | интуитивно понятен |
| Цена | бесплатно | бесплатно | 10000$ | бесплатно |
| Долговечность | требует доработок для более серьезных сценариев | доработки скорее всего не потребуются | долговечна | требует доработок для более серьезных сценариев |

**3. Выводы.** Любая из приведенных выше системы могут быть использованы на выбранном объекте информатизации, однако для реализации системы обнаружения вторжений при условии возникновения ранее неизвестных атак, они могут оказаться не слишком эффективными.