ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ»

(АО «ПМ»)

БАЗА ДАННЫХ СИГНАТУРНЫХ ПРАВИЛ ОБНАРУЖЕНИЯ АТАК AM RULES

Функциональные характеристики базы данных сигнатурных правил обнаружения атак AM Rules на примере ViPNet IDS NS 3.7

На 12 листах

Москва 2023

Аннотация

Настоящий документ описывает функциональные характеристики базы данных сигнатурных правил обнаружения атак AM Rules.

Содержание

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ 4
1 Общие сведения 5
2 Функциональное назначение 6
3 Используемые технические средства и дополнительное программное обеспечение 8
4 Входные данные 10
5 Выходные данные 11
6 Загрузка 12

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения:

АО «ПМ»	Акционерное общество «Перспективный мониторинг»
БРП	База данных сигнатурных правил обнаружения атак AM Rules
СЗИ	Система защиты информации
ИБ	Информационная безопасность

1 Общие сведения

Основным направлением деятельности АО «ПМ» является оценка практической защищённости информационных систем, выявление их уязвимостей при помощи средств инструментального и ручного анализа, реагирование на инциденты безопасности, разработка Программного комплекса автоматизированного поиска, обработки и визуализации данных из открытых источников «Тардис» и Программного комплекса обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire».

Наименование средства - База данных сигнатурных правил обнаружения атак AM Rules.

Формат средства - База данных сигнатурных правил обнаружения атак AM Rules распространяется в файле формата tgz.

2 Функциональное назначение

База данных сигнатурных правил обнаружения атак AM Rules (далее - БРП) предназначена для конфигурирования СЗИ для эффективного обнаружения компьютерных атак и других событий ИБ (далее - События). БРП предоставляет инструкции (далее - Правила), на основе которых СЗИ создает внутреннюю логику обнаружения, а также конфигурационные файлы. События могут быть просмотрены в интерфейсе СЗИ, экспортированы или автоматически отправлены на внешние обработчики.

Функциональные возможности, которые БРП предоставляет СЗИ (согласно Приказу ФСБ России от 6 мая 2019 г. № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»):

- первичная обработка Событий с помощью компонента препроцессоров Snort, настраиваемого с помощью конфигурационных файлов БРП, в частности: обработку поступающих Событий;
- автоматический анализ Событий и выявление компьютерных инцидентов с помощью компонента сигнатурных правил, настраиваемого с помощью Правил БРП, в частности:
  - отбор и фильтрацию Событий с помощью соответствующего синтаксиса Правил;
  - выявление последовательностей разнородных Событий, имеющих логическую связь, которые могут быть значимы для выявления возможных нарушений безопасности информации (корреляция) с помощью функционала flowbits;
  - объединение однородных данных о Событиях (агрегация) с помощью функционала threshold;
  - выявление компьютерных инцидентов, так как Правило является методом (способом) их обнаружения;

– возможность корреляции для распределенных:

- по времени возникновения Событий с помощью функционала threshold и flowbits;
- по месту возникновения Событий с помощью функционала threshold;

– возможность корреляции для последовательности Событий с помощью функционала flowbits.

3 Используемые технические средства и дополнительное программное обеспечение

Клиентская часть - приложение для пользователя СЗИ, эксплуатирующего БРП, работает в браузере на базе Google Chrome, Mozilla Firefox, Microsoft Edge.

Для установки БРП требуется СЗИ ViPNet IDS 3.7 в любом исполнении, как в серверном на физическом сервере, так и виртуальном в соответствии с характеристиками соответствующего варианта ViPNet IDS 3.7.

Минимальная конфигурация виртуальной машины:

– 2 процессора;

– 4 гигабайта оперативной памяти;

– 200 гигабайт объема жесткого диска;

– 4 сетевых интерфейса.

Дополнительным программным обеспечением является средство визуализации AM Ruleset Analyzer. Оно предназначено для ОС Windows 7 / Windows 10 / Windows 11 с графическим интерфейсом для процессоров архитектуры x86-64.

Язык разработки - Python 3.7

Использованные библиотеки из официального Python-репозитория пакетов с открытым исходным кодом PyPI (https://pypi.org/): Matplotlib 3.1.1 (https://pypi.org/project/matplotlib/), Numpy 1.18.2 (https://pypi.org/project/numpy/), Pandas 1.2.4 (https://pypi.org/project/pandas/), PIL 9.5.0 (https://pypi.org/project/Pillow/)

Минимальная конфигурация машины (соответствует минимальной конфигурации Microsoft Windows 10):

– 1 процессор частотой не менее 1 ГГц;

– 2 гигабайта оперативной памяти;

– 20 гигабайт объёма жёсткого диска;

– графическая карта с поддержкой DirectX 9 или новее с драйвером WDDM 1.0 или новее;

– графический дисплей 800 на 600 пикселей.

4 Входные данные

БРП используется для обнаружения Событий в сетевом трафике, захватываемом физической или виртуальной сетевой картой с помощью сетевого интерфейса, работающего по протоколу IP и имеющего IPv4-адрес, а также в качестве входных данных для AM Ruleset Analyzer.

5 Выходные данные

Использование БРП в СЗИ генерирует События, данные о которых могут:

1) выводиться в графический интерфейс СЗИ;

2) отправляться посредством протоколов:

– электронной почты;

– SNMP;

– Syslog;

– CEF;

– ViPNet TIAS.

AM Ruleset Analyzer генерирует файлы формата PDF, содержащие статистические сведения о составе БРП (см. подраздел 4).

6 Загрузка

Загрузка БРП на СЗИ производится согласно инструкции по установке БРП.

Загрузка БРП в АМ Ruleset Analyzer производится с помощью графического интерфейса, посредством нажатия кнопки «Выберите БРП».