Разметка сетевого трафика для анализа состояния ИБ

Качалин Алексей

ЗАО "ПМ"

Анализ трафика - теория

- Классическая задача
- Методы анализа (примеры)
  - По исходным «знаниям»
    - Обнаружение аномалий
    - Обнаружение злоупотреблений
    - Релевантные метрики
  - По подходу
- Выводы анализа: трафик, узлы, сеть
    - Количественный анализ
      - Тарификация
    - Качественный анализ
      - Обнаружение атак и вирусов
    - Топологии, карты потоков и взаимодействий
- Наличие инструментария

Предпосылки – практика

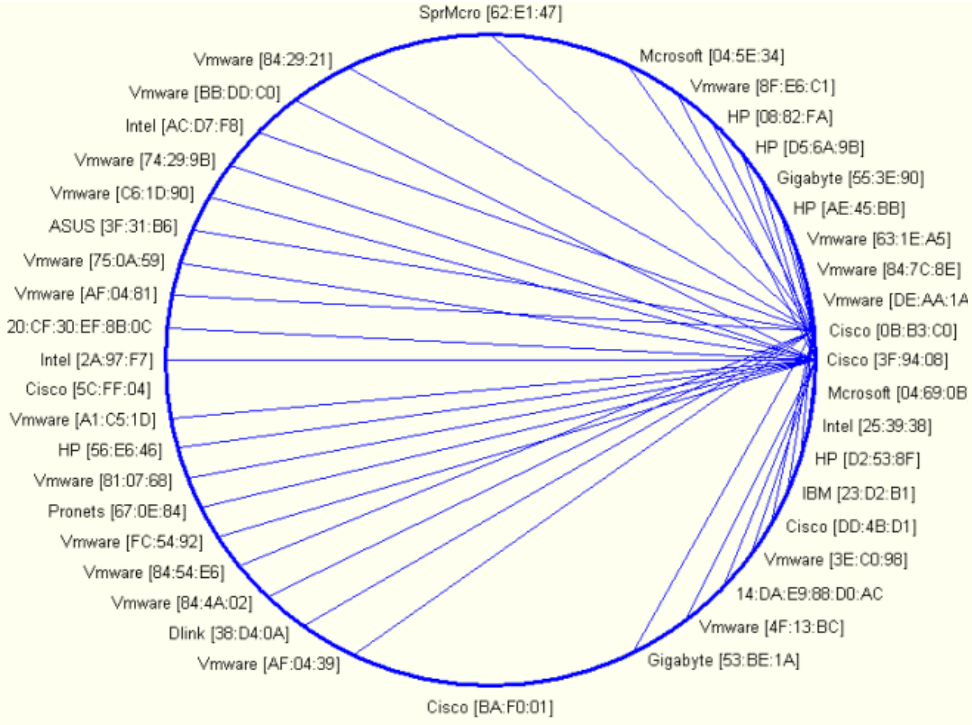
- «Приходим» в неизвестную (в т.ч. администраторам) ИС
  - Не установлены/не обслуживаются системы анализа трафика
- Ограничения при работе
  - Минимум вмешательства в работу сети (пассивный съем)
  - Наличие гипотез, эффективно проверяемых на уровне сети
- Наблюдение ограничено
  - по времени – сроки, энтропия ИС
  - по объектам
  - по спектру наблюдения и детальности наблюдения
- Адекватность средств задаче
  - Отложенный анализ
  - Сравнение замеров сделанных в разное время
- Практическая ценность
  - Универсальность, неинвазивность
  - Унификация наблюдения узлов с различными ОС
  - Задачи аудита ИС, расследование инцидентов

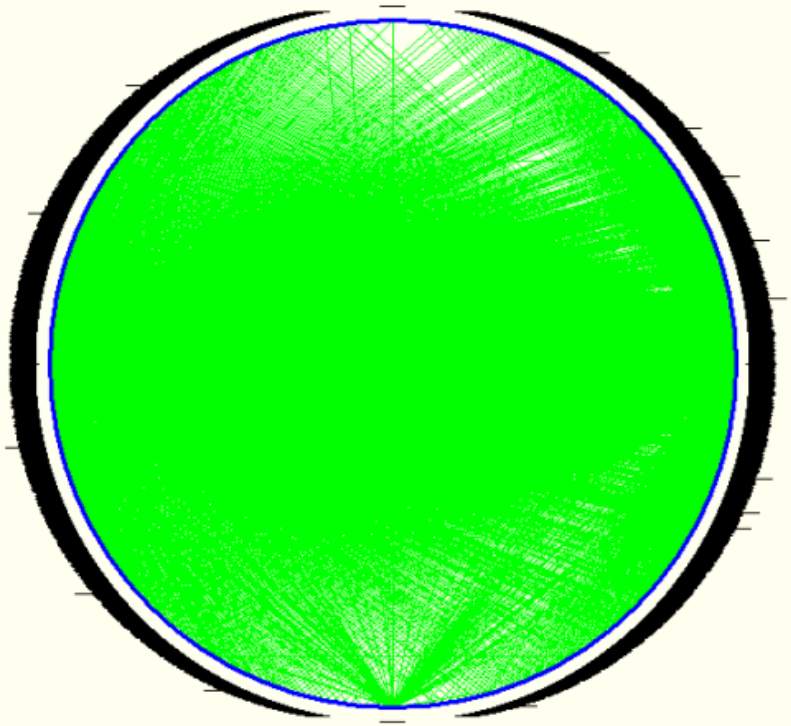
Актуальность задачи

- Проблемы технического характера
  - Корректная интерпретация адресной информации
  - Объемы хранимых данных
- Проблемы теоретического характера
  - Сопоставление
  - Применимость методов анализа (ограничения по вычислительной сложности)

Практика: системы мониторинга ИС?

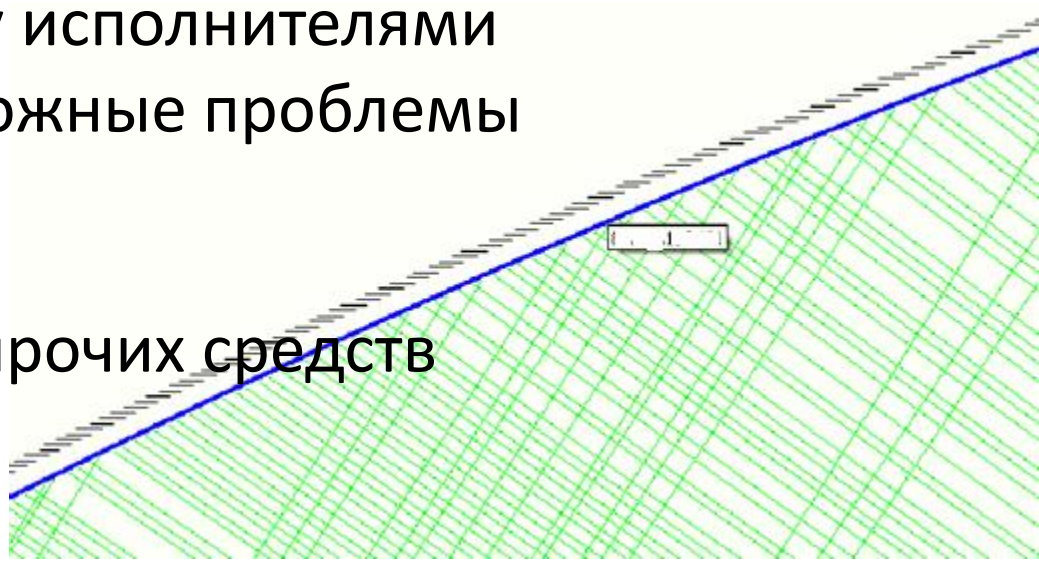
- 20 минут наблюдения, 300 узлов





Идея

- Получить статическую картину поведения объектов ИБ
- Искать не где светло: аналог «pentest attack-tree optimization» для трафика
- Уменьшить «стог сена»
- Разделить работу между исполнителями
- Остаются технически-сложные проблемы
  - Сопоставление узлов
  - Шифрование
- Дополнить вход/выход прочих средств аудита ИБ



Цели

- Собрать и систематизировать toolchain
- Дать аналитикам формализацию и методику для работы
- Разработать модель анализа (выбрать набор моделей), применимую на практике
- … пригодную для описания многошаговых и многоуровневых условий
- Систематизация аналитических сценариев
- …
- Разработка ПО

Процесс решения задачи

Сбор

- Точки подключения (внешний канал или точки в ИС)
- Окно наблюдения (непрерывное)
- Фильтрация на этапе сбора

Обработка

- Фильтрация
- Обрезка
- Разбивка и агрегация по объектам исследования

Разметка

- Автоматическая
- Ручная

Предположения

- Периодичность поведения
  - Объектов
  - Групп объектов
- Наличие паттернов в поведении
  - Технологических
  - «Человеческих»
- Существует «серая зона»
  - Выявление роли узлов
  - Задачи «вне поля зрения» ABC и COA
- Возможность сопоставления описаний поведения на разных уровнях

Разметка трафика: профили и метки

- Выделение сопоставление, именование сетевых объектов
- Сетевое взаимодействие. Паттерны сетевого взаимодействия (communication patterns): выявление server/client, обнаружение p2p
- Профили объектов и взаимодействий
  - сопоставления объектов и взаимодействий
  - Объектов – участников взаимодействий
  - Взаимодействий, связанных объектом
- Обобщенный профиль ИС
  - Карта потоков данных
  - Объекты взаимодействия вне ИС
- Сопоставление проекций

Примеры

- Анализ stepping-stone атак
- In-Out-In паттерны
- Аномальные активности – повод для анализа объектов-участинков
- Выявление теневых бизнес-процессов

Проблемы и решения

- Полнота наблюдения
  - Асимметричная маршрутизация
- Погрешности определения потоков, сессий, сервисов
  - Ограничения наблюдения
- Идентификация
  - Нестандартные порты, случайные порты
- Интерпретация
  - Шифрование/туннелирование
- Изменчивость
  - Перераспределение IP-адресов в сети в течение ее наблюдения.
  - Нестабильность загрузки сети во время наблюдения
  - Изменчивость поведения узлов

Спасибо за внимание!

Инструментальные исследования

Расследование инцидентов

Исследование ПО

Внешний и внутренний мониторинг ИС

http://advancedmonitoring.ru
info@advancedmonitoring.ru
+7 495 737 61 97