Системы обнаружения атак: общие принципы

Денис Гамаюнов

Немного статистики

Первые 6 мест по atlas.arbor.net за 24 часа в октябре 2010 г.:

Страна	**Место**	**Число атак на подсеть**	**Объём сканирований на подсеть**	**Число ботнетов**	**Число попыток фишинга**	**Число DoS-атак**
США	1	979	500Кб	940	40435	0
Китай	2	623	620Кб	49	332	0
Венгрия	3	1	211Кб	11	124	0
Польша	4	4	14Кб	11	5002	0
Россия	**5**	**130**	**81Кб**	**94**	**2600**	**0**
Румыния	6	28	67Кб	28	2297	0

Кому и зачем нужны IDS и IPS?

- Системы обнаружения атак
  - доказательная база для расследования инцидентов
  - мониторинг вредоносной активности
- Требования:
  - Живучесть
  - Полнота обнаружения атак

- Системы предотвращения атак
  - «нормализация» трафика
  - блокирование атак и минимизация ущерба
- Требования:
  - Надёжность
  - Точность/низкий уровень ложных срабатываний

Современные OSS IDS

- Snort: http://www.snort.org/
- Bro IDS: http://www.bro-ids.org/
- Suricata: http://www.openinfosecfoundation.org/
- OSSEC (host only) http://www.ossec.net/

Общие принципы

- Обнаружение злоупотреблений
  - Основа – сигнатурный анализ трафика и/или узловых событий (журналы приложений, сисколлы)
  - Анализаторы протоколов
- Обнаружение аномалий
  - Обучение на примерах нормального функционирования

Сигнатурный анализ

- Простой поиск подстрок
  - strcmp
  - Boyer-Moore
- Словарный поиск
  - Aho-Corasick
- Поиск регулярных выражений
  - PCRE

Обнаружение аномалий

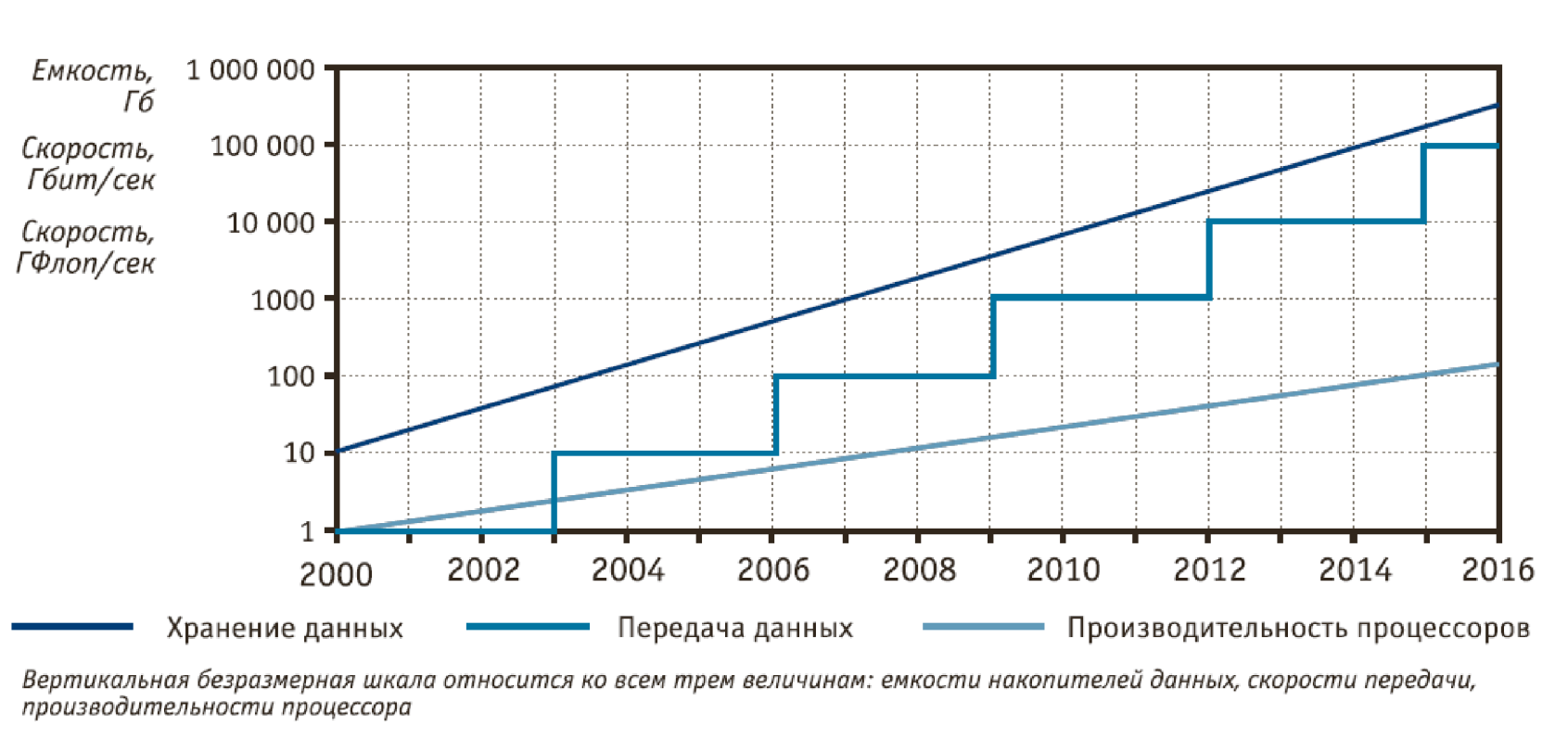
- Основное применение – системы обнаружения DDoS-атак

Snort

Формат сигнатур

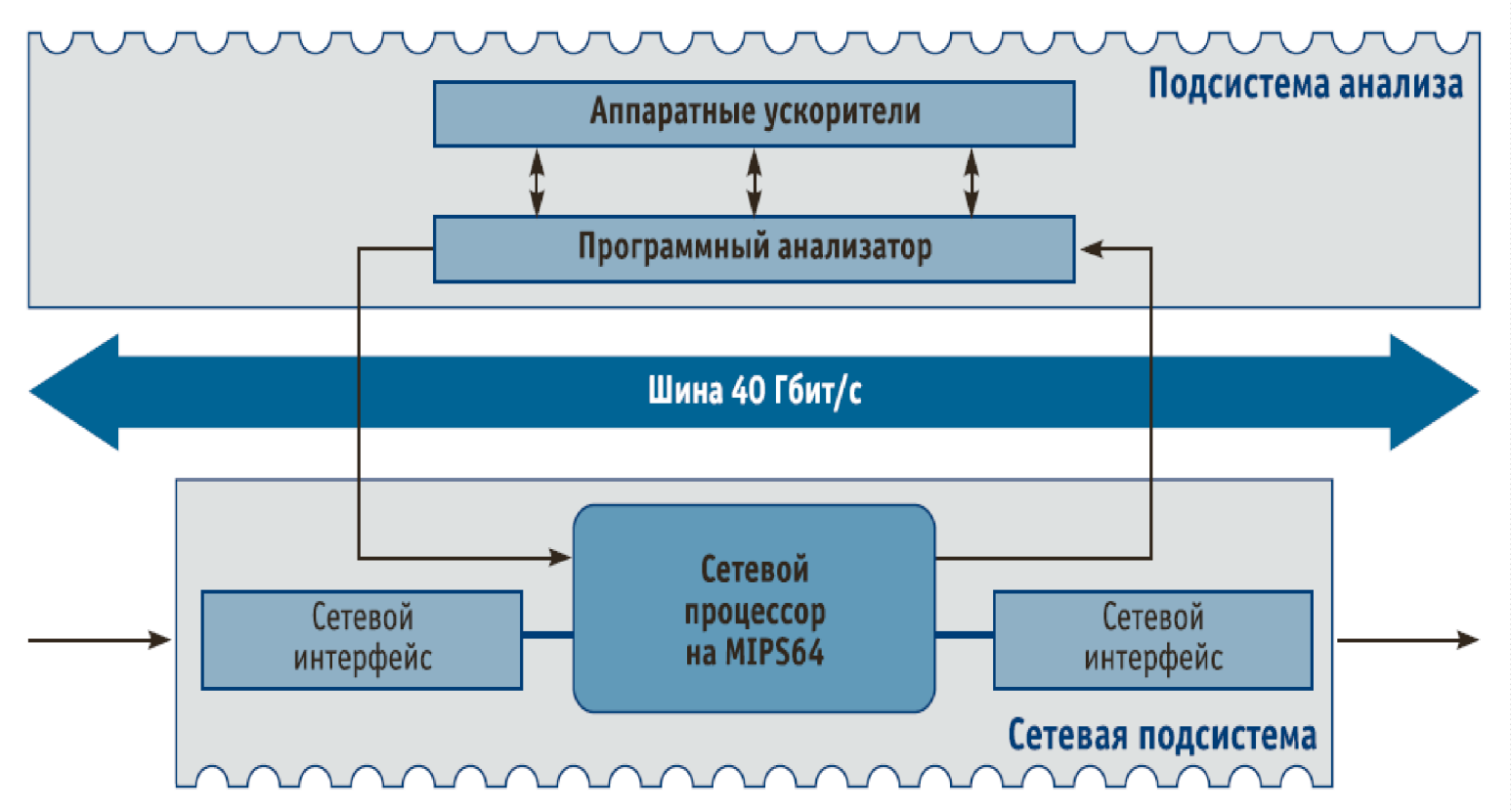
- alert tcp $EXTERNAL_NET 27374 -> $HOME_NET any (msg:"BACKDOOR subseven 22"; flow:to_server,established; content:"|0D 0A|[RPL]002|0D 0A|"; reference:arachnids,485; reference:url,www.hackfix.org/subseven/; classtype:misc-activity; sid:103; rev:7;)
- alert tcp $HOME_NET 16959 -> $EXTERNAL_NET any (msg:"BACKDOOR subseven DEFCON8 2.1 access"; flow:from_server,established; content:"PWD"; classtype:trojan-activity; sid:107; rev:6;)

Анализ трафика – задача реального времени



1GigE: минимальный пакет 64 байта, 672 нс на обработку (худший случай)

Аппаратная поддержка



Задания

- Установить на виртуальную машину:
  - Snort
  - Bro
  - Suricata
- Написать сигнатуру для обнаружения успешных логинов пользователя root через telnet (для тестирования поднять telnetd на DVL)
- Натравить Metasploit на машину с включенными IDS, изучить логи