ОБМАННЫЕ СПОСОБЫ УКЛОНЕНИЯ ОТ СИГНАТУРНЫХ ПРАВИЛ СЕТЕВЫХ СИСТЕМ ОБНАРУЖЕНИЯ АТАК

Выступающий: Браницкий А.А.

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук

РусКрипто

Солнечногорск, 22 марта 2018 г.

Актуальность

- Функционирование большинства СОА основано на сигнатурных правилах (сопоставлении с образцом, пороговом анализе)
- Разнообразие видов и настроек защищаемых ОС затрудняет анализ проходящих через СОА сетевых потоков
- Наличие в сети устаревшего оборудования и маломощных маршрутизаторов с малыми значениями максимально допустимых размеров IP-пакетов (Maximum Transmission Unit, MTU) приводит к сильнофрагментированному трафику
- Требуется (1) разработать тестовые сценарии сетевых атак, компрометирующих сетевой стек СОА, (2) выполнить экспериментальное исследование открытых СОА с целью проверки их способности корректно обрабатывать „нестандартные“ пакеты, (3) предложить рекомендации для избежания возникновения случаев таких атак

Атаки на сетевые СОА

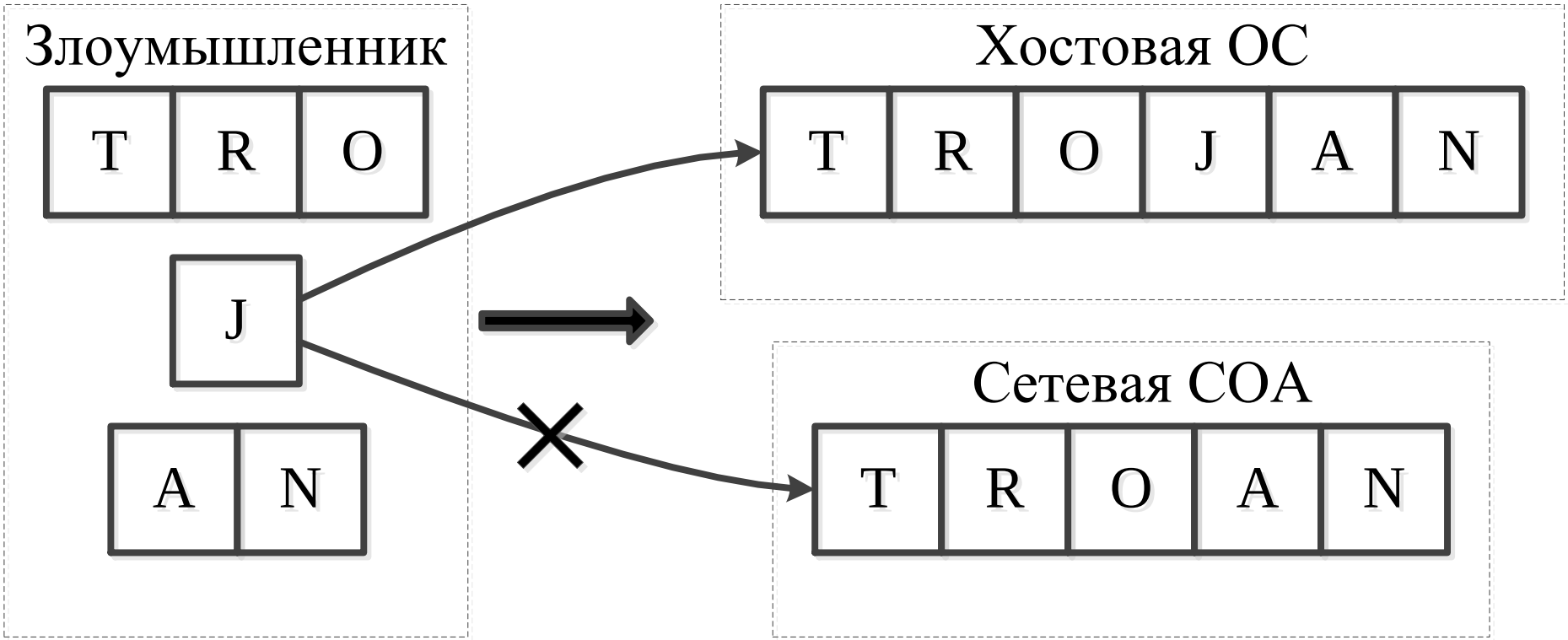
Атаки на сигнатурные СОА:

- **Атаки со скрытием (insertion attacks)**
- **Атаки со вставкой (evasion attacks)**
- Атаки на сетевой стек СОА
- DoS-атаки

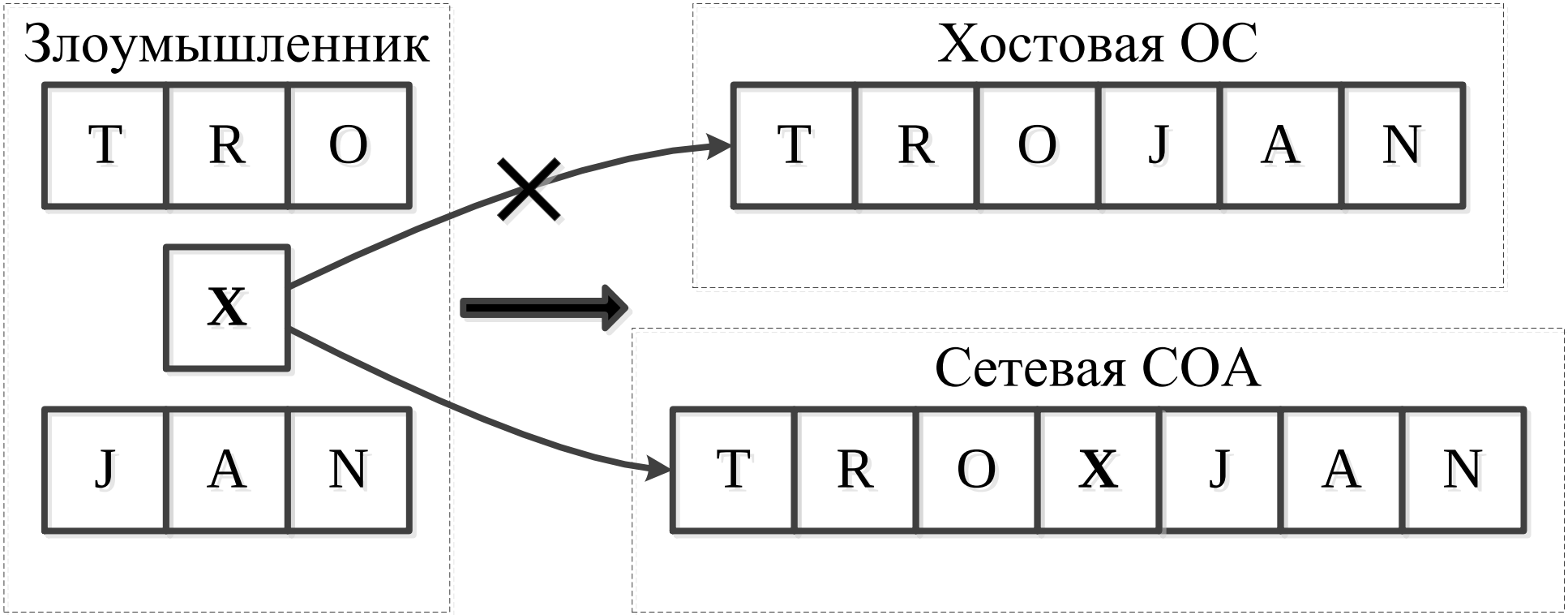
Атаки на эвристические СОА:

- Состязательные атаки (adversarial attacks)
- Отравление модели (poisoning the model)
- Атаки „кипяченой лягушки“ (frog-boiling attacks)
- DoS-атаки

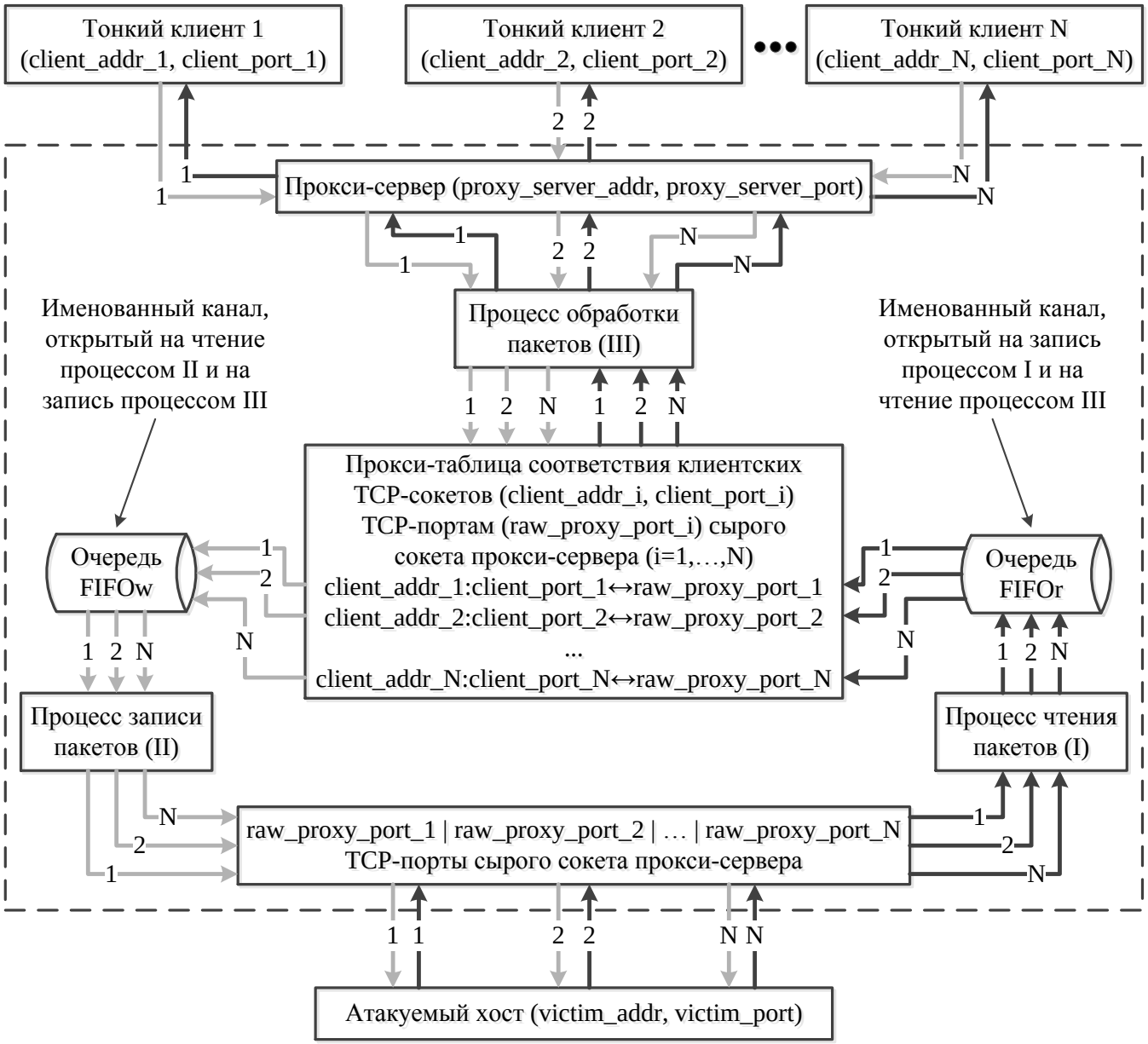
Атака со скрытием



Атака со вставкой



Асинхронный прозрачный прокси-сервер TCP-сессий



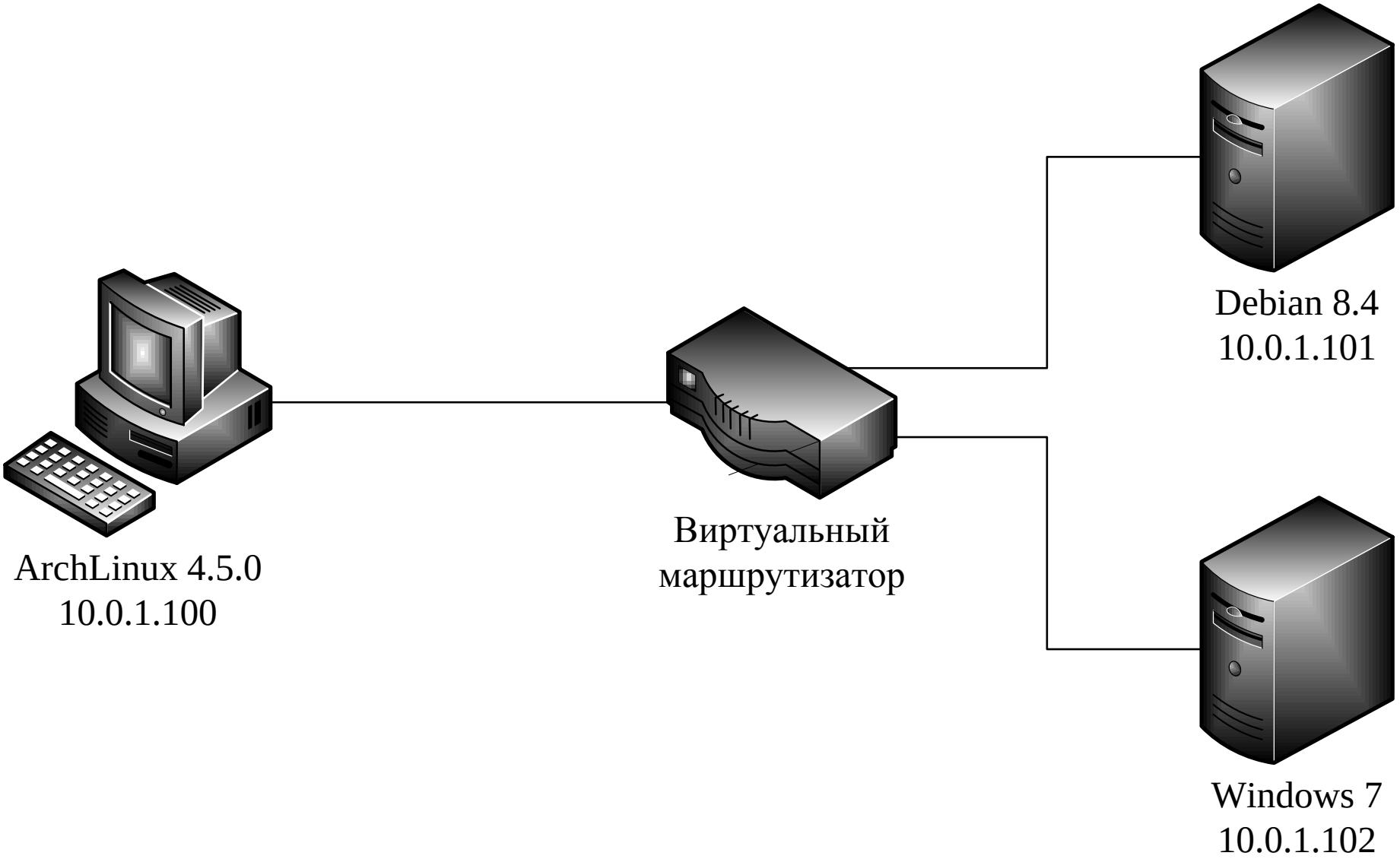
Особенности разработанного инструмента

- Частичная эмуляция TCP/IP-взаимодействия на уровне сырых сокетов
- Прозрачное проксирование TCP-соединений с возможностью анонимного сокрытия IP-адреса источника генерации атак
- Асинхронная и однопоточная обработка поступающих от тонких клиентов запросов
- Генерация тестовых последовательностей низкоуровневых сетевых атак, покрывающих четыре уровня модели OSI

Отличия разработанного инструмента

Характеристика	Сравниваемые инструменты		
	fragroute/ fragrouter	hping3	Разработанный инструмент
Наличие клиент-серверной архитектуры	–	–	+
Поддержка проксирования TCP-соединений	–	–	+
Покрываемые уровни модели OSI	3, 4	3, 4	2, 3, 4, 7
Трансформация пакетов внутри TCP-сессий	–	–	+
Наличие функции сканирования	–	+	–

Программный стенд



Сигнатурные правила Snort и Suricata

```
# test_examples.rules
alert tcp $EXTERNAL_NET any -> $HOME_NET 80 ( \
msg:"WEB test attack"; flow:to_server,established; \
content:"GET /secret.html"; fast_pattern; \
sid:1000003; rev:1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 21 ( \
msg:"FTP test attack"; flow:to_server,established; \
content:"RETR confidential_info.txt"; fast_pattern; \
sid:1000004; rev:1;)
```

Сигнатурные правила Bro

```
# test_examples.sig
signature 1000003-1 {
ip-proto == tcp
src-ip != 10.0.1.101 # local_nets
dst-ip == 10.0.1.101 # local_nets
dst-port == 80
event "WEB test attack"
tcp-state established,originator
payload /.*GET \/secret\.html/
}
signature 1000004-1 {
ip-proto == tcp
src-ip != 10.0.1.101 # local_nets
dst-ip == 10.0.1.101 # local_nets
dst-port == 21
event "FTP test attack"
tcp-state established,originator
payload
/.*RETR confidential_info\.txt/
}
```

```
# test_examples.bro
@load base/frameworks/signatures
@load-sigs ./test_examples.sig
module TestExamples;
global log_file: file;
event bro_init() {
log_file = open(fmt(
"test_examples_%s.log",
current_time()));
}
event bro_done() {
close(log_file);
}
event signature_match(
state: signature_state, msg: string,
data: string) &priority=5 {
print log_file, fmt(
"%s alert %s", current_time(), msg);
flush_all();
}
```

Выводы по экспериментам

- Bro не обрабатывает данные, передаваемые в первом пакете TCP-сессии
- Обход сигнатурных правил Snort возможен при помощи отправки большого числа полностью наслаивающихся друг на друга IP-фрагментов (опция overlap_limit), а также при помощи задания временного таймаута, используемого для удаления просроченных TCP-сессий
- Атака „вываливания за пределы TCP-сессии“ характерна только для СОА Suricata и Bro под ОС Linux
- Ни одна из исследованных сетевых СОА не имеет числа пропуска атак, равного нулю

Рекомендации

- Игнорирование фрагментированных IP-пакетов (`MF=1||IP_OFFSET>0`) средствами МЭ:
```
# включение правила
iptables -A INPUT "4&0x3FFF=1:0x3FFF" -j DROP
# отключение правила
iptables -D INPUT "4&0x3FFF=1:0x3FFF" -j DROP
```
- Установка нулевого таймаута для сборки фрагментированных пакетов:
`echo 0 > /proc/sys/net/ipv4/ipfrag_time`
(В ответ отправляется ICMP-пакет с кодом 1 („Fragment reassembly time exceeded“) и типом 11 („Time-to-live exceeded“))
- Замена сетевых СОА хостовыми (OSSEC, Samhain)
- Использование сетевых СОА с настройками, максимально приближенными к настройкам сетевого стека защищаемой ОС

Заключение

- Рассмотрены сценарии сетевых атак, компрометирующих сетевой стек СОА, предложены рекомендации по предотвращению таких атак
- Направление дальнейших исследований — совершенствование асинхронного прозрачного прокси-сервера TCP-сессий (добавление функционала обработки и формирования IP- и TCP-опций, ...), расширение списка тестируемых СОА и сценариев атак

Список литературы

- Ptacek T. H., Newsham T. N. Insertion, evasion, and denial of service: Eluding network intrusion detection: tech rep. / SECURE NETWORKS INC CALGARY ALBERTA — 1998.
- Northcutt S., Novak J. Network intrusion detection. – Sams Publishing, 2002. — 512 pp.
- Barreno M. [et al.] Can machine learning be secure? // Proceedings of the 2006 ACM Symposium on Information, computer and communications security. — 2006. — Pp. 16–25.
- Moosavi-Dezfooli S. M., Fawzi A., Frossard P. Deepfool: a simple and accurate method to fool deep neural networks // Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). — 2016. — Pp. 2574–2582.
- Chan-Tin E. [et al.] The frog-boiling attack: Limitations of secure network coordinate systems // ACM Transactions on Information and System Security (TISSEC). — 2011. — Vol. 14, no. 3.

Контактная информация

Браницкий А.А.
Санкт-Петербургский институт информатики и автоматизации Российской академии наук
branitskiy@comsec.spb.ru
Работа выполнена при финансовой поддержке РФФИ (проекты 15-07-07451, 16 37-00338) и бюджетных тем № 0073-2015-0004