Симуляция медленных Сетевых атак

Матюха Д. В., студент кафедры безопасных информационных технологий Университета ИТМО, denisych259@yandex.ru

Аннотация

В данной статье рассматривается тема симуляции медленных сетевых атак с целью проведения эксперимента для выявления изменения характеристик сети во время проведения атаки. Симулятор может изменять соотношение легитимного и вредоносного трафика, моделируя реальную среду. Параметры, с которыми симулятор реализует атаку, можно изменять динамически. В результате проведения экспериментов и использованием симулятора планируется выявить подходы к детектированию медленных сетевых атак на уровне магистралей с большим объемом проходящего трафика.

Введение

«Медленные» сетевые атаки держат открытыми множественные подключения к целевому серверу, вызывая нагрузку, а в последствии отказ в обслуживании [1]. На текущий момент разработаны и описаны методы противодействия таким атакам на уровне сервера, однако в открытых источниках нет методов детектирования медленных сетевых атак на уровне магистралей с большим объемом проходящего трафика. Сложность детектирования обусловлена ключевыми особенностями такого рода атак. Воздействие растянуто во времени, то есть сложно выделить какие-то пики в потоке трафика. Атакующие запросы на сетевом уровне не отличаются от легитимных, они, как правило, имеют подобный размер и структуру. В большинстве случаев отсутствуют какие-либо явные признаки влияния извне на промежуточные элементы сети, в то время как суммарная нагрузка на жертву позволяет вызывать отказ в обслуживании, например, за счет сложности вычислений на сервере (SSL renegotiatiom). В некоторых случаях происходит «усиление» - злоумышленник порождает большее воздействие при затрачивании меньших ресурсов.

В настоящее время существует множество таких атак (HTTP Flood, SSL/TLS renegotiation, SMTP Flood, DNS amplification и т.д.). У каждой из них существуют свои особенности, они используют различные сетевые

протоколы и зависят от ряда условий. Для разработки эффективного противодействия необходимо:

1. Формально описать эти атаки;
2. Разработать инструментарий, позволяющий их воспроизвести;
3. Изменяя входные и промежуточные параметры, исследовать атаку с точки зрения воздействия на целевую систему и ключевые узлы сети, в которой она проводится;

Симулятор

Особенности реализации

Симулятор - программное средство, принимающее на вход конфигурацию атаки (её формальное описание, параметры атаки и настройки системы-симулятора), обрабатывающее её и реализующее в некоторой исследуемой среде.

Разработка ведётся с использованием средств языка Python 2.7. в среде linux.

Симулятор включает в себя:

- обертку, отвечающую за интерпретацию конфигурации атаки и управление настройками атаки;
- динамический конфигуратор атаки;
- модуль симуляции естественной среды атаки;

На вход программе подается конфигурационный файл в формате json, в котором в обязательных полях описывается название атаки, её словесное описание, протокол, а массив опций содержит объекты, каждый из которых описывает параметры атаки. Таким образом можно статически задать несколько конфигураций для одной атаки. Симулятор может запускать готовые бинарные файлы, путь и аргументы для которых указаны в опциональных полях «program» и «args» соответственно, а также выполнять скрипты python, записанные в конфигурационном файле.

Для создания имитационной модели атаки необходимо воссоздать сеть, близкую к реальной. За это отвечает модуль симуляции естественной среды атаки. На текущем этапе можно задавать в конфигурационном файле соотношение вредоносного трафика к легитимному, таким образом получается «естественный» трафик в канале передачи данных. В дальнейшем изменяя это соотношение можно будет следить за

изменениями в характеристиках атаки и делать определенные выводы о её детектировании.

Атака в симуляторе будет проводится в соответствии со сценарием, который может рефлексивно менять ее параметры. Для этого разрабатывается динамический конфигуратор атаки. После проведения одной атаки, в зависимости от её результатов должна генерироваться новая конфигурация и на её основе будет проведена следующая атака.

Данная система должна быть расширяема в дальнейшем.

Модель симулятора

Для соотношения среды симулятора с реальной средой следует ввести несколько производных от заданных в конфигураторе атаки параметров.

$$\mathbf{P_L + P_M = 1} \quad \mathbf{(1)}$$

Формула (1) отражает соотношение вредоносного трафика и легитимного, который генерирует симулятор. Меняя это соотношение, мы сможем следить за изменениями характеристик магистрали, что даст некоторое понимание о возможностях детектирования вредоносного трафика в общем потоке. Отсюда следует формула (2):

$$\mathbf{P_C} = \frac{P_{Mc}}{P_{Lc}} \quad \mathbf{(2)}$$

Это такое отношение вредоносного трафика к легитимному, при котором изменение характеристик сети не заметно монитору. Для хорошо настроенной системы мониторинга в идеальных условиях данное отношение должно стремиться к нулю.

$$\boldsymbol{\mu} = \frac{n \bullet P_{Mi}}{t_i} \quad \mathbf{(3)}$$

Где n – количество потоков в рамках одной конфигурации, P_{Mi} – количество трафика, генерируемого одной атакой, t_i – время, затрачиваемое симулятором на проведение атаки. Формула (3) является отношением для характеристики интенсивности μ. Интенсивность показывает количество вредоносного трафика, генерируемого симулятором в единицу времени.

Симуляция атаки SSL renegotiation

В ходе эксперимента с использованием симулятора медленных сетевых атак была проведена атака SSL renegotiation. На вход симулятору подавался конфигурационный файл с параметрами атаки и бинарный файл, реализующий её.

Пример конфигурационного файла для атаки типа «SSL\TLS renegotiation»:

```
{
  "name": "ssl renegotiation",
  "descr": "ssl renegotiation attack",
  "protocol": "ssl/tls",
  "options": [
    {
      "threads": "2",
      "timeout":"8000",
      "programm": "/path/ssl_attack_binary",
      "args": "-r target.ru 443"
    },
    {…}
  ]
}
```

Атака такого типа загружает целевой сервер сложными вычислениями. Как видно из конфигурационного файла симулятор должен запустить два атакующих потока с задержкой в 8 секунд. При этом успех атаки можно отследить по росту cpu на целевом сервере.

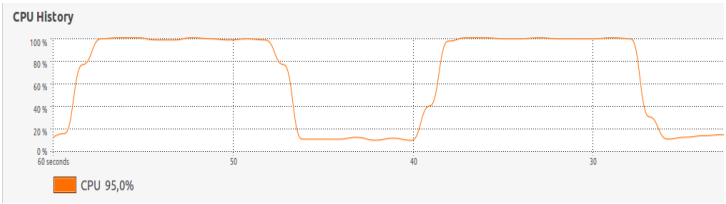

Рисунок 1: Рост cpu при успешном проведении атак.

Как видно из графика cpu (см. Рис. 1), атака с использованием заданных параметров была успешно проведена.

Заключение

Проблема детектирования медленных сетевых атак на уровне магистралей с большим объемом проходящего трафика является

актуальной и мало описанной в открытых источниках. Для того, чтобы научиться детектировать такого рода атаки следует получить характеристики сети в момент их проведения. Необходимо провести эксперимент, в ходе которого бы эта атака воспроизводилась. Меняя параметры, можно следить за изменениями этих характеристик. Для проведения атаки в среде, близкой к реальной, а также для динамического изменения параметров разрабатывается программа-симулятор. В статье был описан принцип работы симулятора медленных сетевых атак, а также была проведена демонстрация его работы на упрощенном примере атаки SSL renegotiation.

Литература

1. Slowloris (computer security) [Электронный ресурс] // Wikipedia, the free encyclopedia – URL: https://en.wikipedia.org/wiki/Slowloris_(computer_security) (дата обращения: 20.02.2016).
2. *Д.И. Котенко, И.В. Котенко, И.Б. Саенко* Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы // Труды СПИИРАН. 2012. Вып. 3(22). ISSN 2078-9181 (печ.)