Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.455.2 : 004.056

Трафимук
Максим Павлович

# Имитация и мониторинг дестабилизирующих воздействий на сетевые ресурсы в ООО «Белатра»

**АВТОРЕФЕРАТ**
на соискание степени магистра информатики и вычислительной техники по специальности 1-40 81 02 «Технологии виртуализации и облачных вычислений»

_____

Научный руководитель

Селезнев И. Л.

доцент, к.т.н

_____

Минск 2019

# ВВЕДЕНИЕ

Современные тенденции развития информационных технологий предполагают максимальную виртуализацию и абстрагирование от конкретных рабочих станций и все больший переход к облачным и сетевым системам хранения и обработки данных. Эти решения сопряжены с меньшим риском потери информации и большей вычислительной мощностью таких систем, а также с их независимостью от географического местоположения пользователя и мощности его личного устройства, взаимодействующего с системой.

Основополагающими принципами систем хранения данных и центров обработки данных являются: безопасность, надежность и доступность. Для обеспечения надежности используются дублирующие компоненты, для обеспечения безопасности различные виды аутентификации и шифрования, а для обеспечения доступности многие организации не предпринимают практически ничего, что является серьезной проблемой, потому что этот аспект является самым легкодоступным для внешних вредоносных действий.

В данной работе рассматриваются различные способы дестабилизации сетевого ресурса, преимущественно являющиеся вариантами снижения доступности, так как стабильность является одной из основных составляющих понятия «доступность» для сетевого ресурса.

Существует несколько семейств причин снижения доступности:

1. DoS и DDoS - атака типа «отказ в обслуживании» и распределенная атака типа «отказ в обслуживании» соответственно.
2. Эксплоиты – недоработки в программных модулях систем и устройств.

Первое рассматриваемое семейство причин снижения доступности, организованные злоумышленниками или соперниками называется Distributed Denial of Service (DDoS), распределенная атака типа «отказ в обслуживании». Иными словами, когда злоумышленник загружает канал доступа к ресурсу клиенты не могут воспользоваться этим ресурсом, таким образом нарушается принцип доступности. В случае DDoS злоумышленник использует большое количество атакующих устройств для повышения успеха.

Второе рассматриваемое семейство – эксплоиты, недоработки в программных модулях, позволяющие использовать их нестандартным негативным образом. Рассмотрение всех возможных эксплоитов едва ли возможно в рамках одной работы, поскольку их существенно больше чем существующих программных средств, и количество обнаруженных

постоянно увеличивается, однако наиболее яркие представители этого семейства будут рассмотрены и реализованы.

Целью этого проекта является разработка программного комплекса, из атакующего модуля, позволяющего эмулировать дестабилизирующие воздействия на сетевые ресурсы для получения необходимого опыта системными администраторами и проверки надежности уже выстроенной защиты, и модуля мониторинга для проверки результативности работы. В ходе создания проекта необходимо учитывать, что от масштабных атак нет надежной защиты, и для них нужно большое количество участников, таким образом на ресурсы, не являющиеся всемирно востребованными такие атаки не производятся. Также в качестве отрицательного эффекта объема всемирной сети является ее статичность, таким образом эмуляции самых распространенных видов атак достаточно для подготовки к 90% угроз доступности.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы исследования:**

Современные тенденции развития информационных технологий предполагают максимальную виртуализацию и абстрагирование от конкретных рабочих станций и все больший переход к облачным и сетевым системам хранения и обработки данных. Эти решения сопряжены с меньшим риском потери информации и большей вычислительной мощностью таких систем, а также с их независимостью от географического местоположения пользователя и мощности его личного устройства, взаимодействующего с системой.

Основополагающими принципами систем хранения данных и центров обработки данных являются: безопасность, надежность и доступность. Для обеспечения безопасности и надежности существует огромное количество программных и аппаратных средств, а для обеспечения доступности их крайне мало. Обеспечение доступности – задача системного администратора и, для того чтобы успешно противостоять вредоносным воздействиям, ему нужно иметь возможность воспроизвести атаку и проанализировать ее алгоритм. В данной работе решения этого вопроса рассматриваются различные способы дестабилизации сетевого ресурса, преимущественно являющиеся вариантами снижения доступности, так как стабильность является одной из основных составляющих понятия «доступность» для сетевого ресурса. А также реализован модуль мониторинга для определения результативности.

**Цели и задачи работы:**

Целью работы является разработка программного комплекса позволяющего совершать дестабилизирующие воздействия на сетевые ресурсы, а так же мониторинг их успешности. В соответствие с поставленной целью в работе сформулированы и решены следующие задачи:

1. Проанализировать возможные дестабилизирующие воздействия и методы мониторинга сетевых ресурсов
2. Проанализировать и реализовать наиболее перспективные существующие методы.

**Объектом исследования** является сетевая сфера взаимодействия.

**Предметом исследования** выступают методы мониторинга и дестабилизации сетевых ресурсов.

**Научная новизна** диссертационной работы заключается в нахождении новых типов дестабилизирующих воздействий и анализе актуальности существующих видов этих воздействий в настоящий момент.

**Положения выносимые на защиту:**

1. Существующие методы дестабилизации сетевых ресурсов и их особенности.
2. Программная реализация актуальных методов дестабилизации сетевых ресурсов.

**Апробация результатов диссертации**

Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: 55-я юбилейная научная конференция аспирантов, магистрантов и студентов БГУИР (Минск, 2019).

**Опубликованность результатов исследования**

По результатам исследований, представленных в диссертации, опубликовано 2 печатные работы, в том числе 2 тезиса в сборниках и материалах научных конференций.

**Структура и объем диссертации**

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, трех глав и заключения, библиографического списка и приложений. Общий объем диссертации – 61 страниц. Работа содержит 12 рисунков, 1 таблица, 1 приложение. Библиографический список включает 30 наименований, графический материал включает 1 чертеж, 13 слайдов презентации.

# КРАТКОЕ СОДЕРЖАНИЕ

Во **введении** описана актуальность выбранной темы диссертации, а также сфера возможного применения результата работы.

В **общей характеристике** работы сформулированы ее цель и задачи, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе автора, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В **первой главе** представленной работы проводится рассмотрение и анализ существующих методов дестабилизации сетевых ресурсов, среди которых более подробно рассмотрены способы снижения доступности вида «отказ в обслуживании» вследствие их малочисленности, а также несколько типовых уязвимостей, позволяющих вывести целевой ресурс из строя.

Во **второй главе** проводится анализ потенциальной эффективности рассматриваемых методов дестабилизации на основе задокументированных результатов. Также во второй главе происходит выбор реализуемых программно методов атаки для проверки их практической эффективности.

В **третьей главе** описываются требования к программному комплексу в целом, и к каждому его модулю в частности, особенности реализации каждого модуля и их компонентов. Также в третье главе проводятся испытания получившегося в результате разработки программного комплекса, и проводится анализ полученных практических результатов в сравнении с теоретическими данными, рассмотренными во второй главе.

# ЗАКЛЮЧЕНИЕ

Результатом данной магистерской работы стал программный комплекс дестабилизации и мониторинга сетевых ресурсов, а также ряд исследований эффективности различных видов атак в современных реалиях.

В процессе рассмотрения и анализа литературы были найдены наиболее известные, широко используемые и эффективные виды атак. На текущий момент на уровне провайдера отключена возможность подменять исходящий IP адрес, таким образом сводя многие атаки, основанные на больших объемах трафика на нет. По этой причине атаки основанные на UDP или TCP флуде практически не имеют эффективности, поскольку пропускная способность любого сервера как правило выше пропускной способности одного компьютера, а организация большого количества компьютеров в одну структуру для атаки является слишком трудоемким процессом и на современном этапе развития компьютерной безопасности возможен практически только на добровольных условиях. По этой же причине неэффективны атаки с использованием DNS и NTP серверов, которые произвели фурор более десяти лет назад. Кроме того, многие сервера имеют другие виды защиты, например использование TCP протокола для отправки больших пакетов данных.

Так же не удалось добиться хоть сколько-нибудь ярко выраженных результатов для тех видов атак, которые вызвали серьезный общественный резонанс. К таким атакам можно отнести RefRef, HTTP флуд мусорными данными, AhrDosme и некоторые другие. Эти атаки, как правило, связаны с крупными политическими или экономическими конфликтами, в связи с чем защита от них и превентивные меры для их избегания встроены в большинство систем.

Исключением из этого списка можно считать HTTP-POST флуд с использованием GZip бомб, который позволил увеличить время отклика сетевых ресурсов на значения до ста процентов от стандартного. Несмотря на некоторую известность этой атаки вследствие ее результативности при использовании против файлообменников и фотохостингов, она все еще актуальна. Однако неизвестно является ли полученный результат следствием непосредственно использования GZip бомб или увеличения нагрузки на поддержку и обработку соединения, поскольку один файл передается достаточно длительное время, которое подключение остается задействованным и увеличивает нагрузку на канал цели. Данный вопрос

может быть предметом дополнительного анализа и исследований в этой области.

Ожидаемо высокий уровень эффективности продемонстрировала атака SlowLoris, поскольку эффективной защитой от нее является только ограничение количества подключений с одного адреса, чем многие владельцы и администраторы сетевых ресурсов пренебрегают. Однако неожиданным стал факт того, что для успеха атаки понадобилось менее десяти секунд, поскольку атаки такого типа опасны именно за счет длительного воздействия.

Неожиданно высокий уровень эффективности продемонстрировала атака ReCoil, поскольку по результату анализа литературы был сделан вывод что она эффективна, только в случае, когда пропускная способность сетевого канала атакующего выше, чем аналогичная характеристика цели. Однако эффективность данной атаки была подтверждена неоднократно в процессе испытаний.

Так же высокий уровень эффективности продемонстрировали различные виды эксплоитов, направленные на некоторые широко используемые программы и компоненты. В данном проекте успешность этих атак демонстрировал TMOF эксплоит, который был наиболее эффективен среди всех реализованных атак. Однако не все использованные эксплоиты были настолько эффективны, например RefRef был абсолютно неэффективен.

Подытожить можно следующим тезисом: на сегодняшний день наиболее уязвимым является прикладной уровень модели OSI, как самый быстрорастущий, поскольку более низкие уровни многократно выверены и эффективно защищены вследствие своей статичности.

Так же есть некоторое количество выводов, касающихся мониторинга сетевых ресурсов: большая часть современных сетевых ресурсов, доступных в нашей стране, имеет среднее время отклика до двухсот миллисекунд и превышение этого значения чаще всего означает недоступность или чрезмерно высокую загруженность ресурса; практически все современные сетевые ресурсы предоставляющие доступ по протоколу HTTP используют переадресацию и другие способы упрощения доступа к данным, что вызывает сложности при мониторинге, например код ответа, отличный от успешного из 200 серии. Поэтому при мониторинге таких сетевых ресурсов необходимо либо учитывать многочисленные переадресации при попытке обращения и измерения времени доступа, либо допускать что любой код кроме 500 серии является кодом, означающим успешный доступ.

Полученный в результате работы программный комплекс можно развивать далее, добавляя дополнительные виды атак, а также дополнив модуль мониторинга поддержкой переадресации для корректного отображения результата. Самым перспективным направлением развития данного проекта является исследование сетевых уязвимостей с целью найти новые способы атаки, которые неизвестны на текущий момент. Это направление является наиболее полезным поскольку добавляет в проект такие области информационных технологий как машинное обучение, генетические и эволюционные алгоритмы, численные методы, теорию автоматов и многие другие.

# СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Трафимук, М.П. TMOF уязвимость / М. П. Трафимук // Компьютерные системы и сети: материалы 55-й юбилейной научной конференции аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – (приняты к опубликованию).

[2] Трафимук, М.П. SharePoint 2016 OData уязвимость / М. П. Трафимук // Инфокоммуникации: материалы 55-й юбилейной научной конференции аспирантов, магистрантов и студентов, Минск, 22 – 26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2019. – (приняты к опубликованию).