Алгоритм проактивной защиты FTP-сервера от компьютерных атак

Т.В.Лебедкина, email: alina010570@mail.ru

Краснодарское высшее военное училище
имени генерала армии С.М. Штеменко

Аннотация. *В статье рассматривается алгоритм защиты FTP-сервера на основе управления сетевыми соединениями с нарушителями информационной безопасности. Описывается последовательность действий, поясняющая сущность разработанного алгоритма. Делается вывод о том, что разработанный алгоритм устраняет некоторые из недостатков аналогов и обеспечивает более высокую защищенность FTP-сервера от несанкционированных воздействий за счет имитации канала связи с плохим качеством.*

Ключевые слова: *проактивная защита, вычислительная сеть, компьютерная атака, сетевые соединения, протокол, сетевая разведка.*

Введение

В настоящее время в области компьютерной безопасности особую актуальность набирает разработка принципиально новой технологии, направленной не на обнаружение и реагирование, а на предотвращение компьютерных атак (КА). Одним из направлений этой технологии является применение методов проактивной защиты вычислительных сетей [2-5], реализуемых на этапе проведения злоумышленником сетевой разведки. Его сущность заключается в активном противодействии вредоносным воздействиям, за счет, предотвращения дальнейшей передачи данных злоумышленником по установленному сетевому соединению на время, которое может быть использовано службами информационной безопасности для реализации необходимых мер защиты [9-15].

Алгоритм относится к области информационной безопасности вычислительных сетей и может быть использован в системах обнаружения атак с целью оперативного выявления и противодействия несанкционированным воздействиям на FTP-серверы, в сетях передачи данных типа «Internet».

Описание алгоритма проактивной защиты FTP-сервера

Протокол FTP предназначен для передачи файлов по TCP/IP сетям, построен по архитектуре «клиент-сервер» и использует два TCP соединения для передачи команд и откликов между клиентом и сервером (управляющее соединение), а также для передачи файлов между клиентом и сервером (соединение данных).

В соответствии со спецификацией [6], команды FTP передаются от клиента к серверу по управляющему соединению и состоят из 3 или 4 байт. FTP-сервер отвечает откликом на каждую из полученных команд, который содержит трехзначный номер (передается как три числовых символа), за которым может следовать строка текста и представляет собой подтверждение (или отказ, содержащий сообщение с кодом временной или постоянной ошибки), передаваемое в форме строк от сервера к клиенту через управляющее соединение. Диалог между FTP-клиентом и FTP-сервером осуществляется поэтапно (команда – отклик – команда …).

Текст отклика FTP-сервера на команду FTP-клиента может содержать несколько строк, количество которых не ограничено, но это требует использования для многострочных откликов специального формата, регламентирующего, чтобы каждая строка (кроме последней) начиналась кодом отклика, после которого следует дефис (–), а далее текст. В последней строке вместо дефиса используется пробел, после которого может следовать текст.

После завершения передачи файлов клиент может закрыть подключение или инициировать следующую передачу.

Назначением разработанного алгоритма, является конфигурация параметров соединений FTP-сервера и клиентов в условиях КА, обеспечивающая повышение результативности защиты за счет снижения возможностей злоумышленника по подбору имен и паролей FTP-клиентов.

Наиболее близким аналогом по своей сущности к разработанному алгоритму является алгоритм, описанный в [8], где обеспечивается повышение защищенности сети от несанкционированных воздействий за счет проверки идентификаторов, санкционированных FTP-клиентов, которыми являются уникальные имя пользователя и пароль, и сравнения их с идентификаторами санкционированных FTP-клиентов. При их совпадении предоставляют FTP-клиенту доступ к использованию информационных ресурсов FTP-сервера. В ином случае направляют с FTP-сервера FTP-клиенту отклик об ошибке авторизации.

Недостатками известных алгоритмов является относительно низкая результативность защиты, обусловленная блокированием после

заданного количества ошибок попыток авторизации, что может привести к новым попыткам несанкционированного доступа уже с учетом полученной информации о системе защиты FTP-сервера.

Алгоритм проактивной защиты FTP-сервера, основан на снижении возможностей по подбору имен и паролей несанкционированных FTP-клиентов, что достигается имитацией канала связи с плохим качеством, обеспечивающим значительное увеличение времени для проведения атак с подбором пароля, за счет направления FTP-клиенту, не прошедшему успешную авторизацию, фрагментированного ответного отклика с ложным сообщением о временной ошибке, фрагменты которого направляются через малые интервалы времени задержки, после множества промежуточных откликов. Снижение возможностей злоумышленника по компрометации средств защиты достигается за счет отсутствия блокирования соединения с FTP-клиентом, не прошедшим успешную авторизацию, направлением через малые интервалы времени задержки, исключающими возможность использования малых значений времени тайм-аута ожидания ответного отклика от FTP-сервера, промежуточных откликов перед направлением ответного отклика от FTP-сервера.

Реализация предлагаемого алгоритма проактивной защиты поясняется блок-схемой последовательности действий, представленной на рисунке, где на начальном этапе формируют модуль хранения, модуль обнаружения и анализа, модуль проактивной защиты (блок 1). Модуль хранения предназначен для хранения в ячейках памяти разрешенных идентификаторов FTP-клиентов, предназначенных для идентификации несанкционированных клиентов. Модуль обнаружения и анализа предназначен для сравнения считанных идентификаторов FTP-клиентов с санкционированными и выдачи команды на блок проактивной защиты в случае их несовпадения. Модуль проактивной защиты предназначен для формирования управляющего воздействия, имитирующего канал связи с плохим качеством, значительно увеличивающего продолжительность времени FTP-соединения с несанкционированным FTP-клиентом и расход его вычислительного ресурса, без блокирования или разрыва установленного сетевого соединения со злоумышленником.

На следующем этапе (блок 2), устанавливают сетевые соединения FTP-клиентов с FTP-сервером. Алгоритмы проактивной защиты клиент-серверных вычислительных сетей, реализуемые на транспортном уровне на этапе установления сетевого соединения, предшествующие обмену сообщениями на уровне приложений в процессе FTP-сессии, которые также могут быть применимы для защиты FTP-серверов,

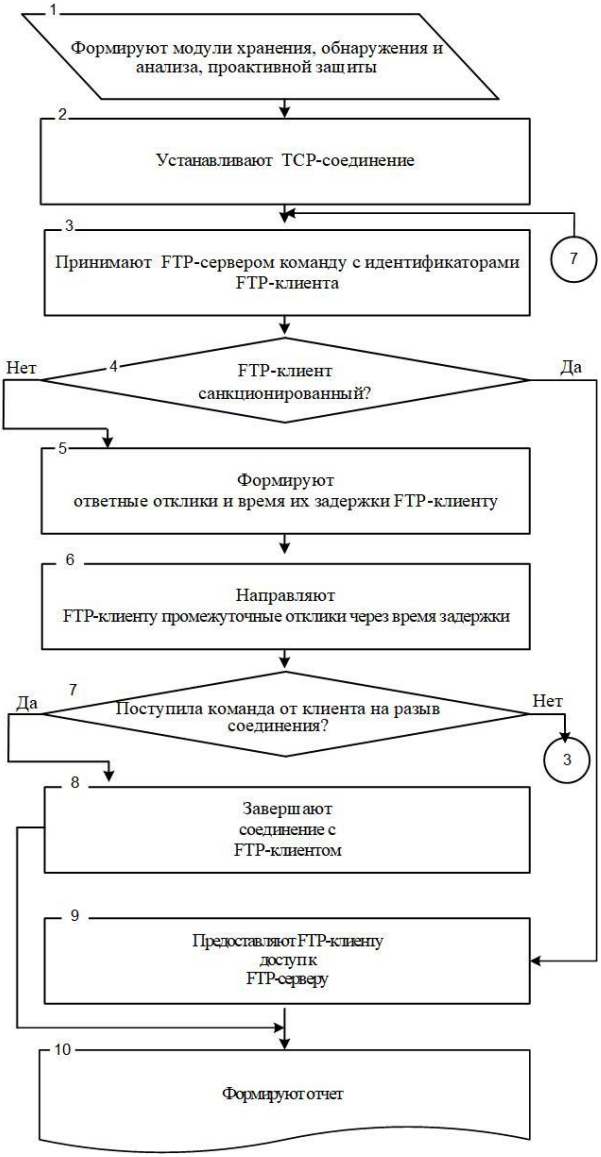

Рисунок. Блок-схема последовательности действий, реализующая алгоритм проактивной защиты FTP-сервера от компьютерных атак

достаточно полно изложены в [1], в связи с чем в настоящей статье не рассматриваются.

После установления соединения FTP-серверу направляют (блок 3) команды с идентификаторами FTP-клиента, далее сравнивают (блок 4) выделенные идентификаторы FTP-клиента с опорными идентификаторами санкционированных FTP-клиентов, если клиент несанкционированный, то формируют (блок 5, 6) ответный отклик FTP-клиенту с ложным сообщением о временной ошибке, с определенным временем задержки. В ином случае FTP-клиенту предоставляется (блок 9) доступ к информационным ресурсам FTP-сервера и формируется отчет. Применение ложных сообщений о временной ошибке в алгоритме является механизмом для увеличения продолжительности времени принудительного диалога со злоумышленником, обеспечивающем дискомфорт для него, а для системы защиты дополнительный временной ресурс, позволяющий ей принять дополнительные меры защиты.

Для повышения результативности защиты за счет снижения вероятности обнаружения злоумышленником факта использования средств защиты, имитируют канал связи с плохим качеством. Для этого, в целях исключения возможности идентификации злоумышленником средств защиты по продолжительным задержкам ответных откликов от FTP-сервера, а также для предотвращения возможности обхода средств защиты за счет установки коротких тайм-аутов ожидания ответных откликов, в предварительно заданные данные дополнительно задают время задержки промежуточных откликов FTP-клиенту. Использование интервалов времени, в течение которого FTP-клиенту будут направлены промежуточные отклики, применяется для увеличения времени диалога с FTP-клиентом, не прошедшим успешную авторизацию на FTP-сервере.

Для исключения возможности обхода средств защиты, за счет установки злоумышленником коротких значений тайм-аутов ожидания ответных откликов от FTP-сервера, значение времени задержки для каждого из промежуточных откликов FTP-клиенту, перед отправкой ответного отклика, выбирают в пределах от 0,1 до 1 секунды.

Для увеличения времени диалогового взаимодействия со злоумышленником количество промежуточных откликов, направляемых FTP-клиенту, перед отправкой ответного отклика, выбирают в пределах от 10000 до 250000.

Для исключения возможности обхода средств защиты, за счет установки злоумышленником коротких значений тайм-аутов ожидания ответных откликов от FTP-сервера, значение времени задержки для

каждого из фрагментов ответного отклика, направляемого FTP-клиенту, выбирают в пределах от 0,1 до 1 секунды.

Для увеличения времени диалогового взаимодействия со злоумышленником величину фрагментов, на которые разбивают ответный отклик FTP-клиенту, выбирают в пределах от 1 до 2 байт.

Для увеличения времени диалогового взаимодействия со злоумышленником, код отклика с ложным сообщением о временной ошибке, выбирают в случайном порядке из кодов группы откликов 4xx (временный сбой), коды откликов известны и описаны [6].

Выводы

В алгоритме проактивной защиты FTP-сервера от КА обеспечивается повышение результативности защиты снижением возможностей злоумышленника по подбору имен и паролей, санкционированных FTP-клиентов. Это достигается имитацией канала связи с плохим качеством, обеспечивающем значительное увеличение времени для проведения атак с подбором пароля, за счет направления FTP-клиенту, не прошедшему успешную авторизацию, фрагментированного ответного отклика с ложным сообщением о временной ошибке, фрагменты которого направляются через малые интервалы времени задержки, после множества промежуточных откликов. Снижение возможностей злоумышленника по компрометации средств защиты вычислительных сетей и их обходу достигается за счет отсутствия блокирования соединения с FTP-клиентом, не прошедшим успешную авторизацию, направлением через малые интервалы времени задержки, исключающими возможность использования злоумышленником малых значений времени тайм-аута ожидания ответного отклика от FTP-сервера, промежуточных откликов перед направлением ответного отклика от FTP-сервера.

Разработанный алгоритм может быть использован в системах обнаружения и предупреждения КА с целью противодействия несанкционированным воздействиям в вычислительных сетях.

Список литературы

1. Максимов, Р. В. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки / Р. В. Максимов, Д. Н Орехов, С. П. Соколовский // Системы управления, связи и безопасности. 2019. № 4. С. 50–99.

2. Соколовский, С.П. Концептуализация проблемы проактивной защиты интегрированных информационных систем / С. П. Соколовский, Д. Н. Орехов // Научные чтения имени профессора Н. Е. Жуковского: сб.

научн. стат. VIII Междунар. науч. метод. конф. (Краснодар, 20–21 декабря 2017 г.). – Краснодар. 2018. С. 47–52.

3. Maximov, R. V. Hiding computer network proactive security tools unmasking features./ R. V. Maximov, S. P. Sokolovsky, L. A. Gavrilov // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Moscow, Bauman Moscow Technical University, 2017, P. 88-92.

4. Максимов, Р. В. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей / Р. В. Максимов, С. П. Соколовский, Д. Н. Орехов // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 2. – Воронеж: ООО «Вэлборн», 2018. С. 169-179.

5. Соколовский, С. П. Способы снижения информативности демаскирующих признаков средств проактивной защиты вычислительных сетей / С. П. Соколовский, А. Л. Гаврилов, Д. Н. Орехов // Научные труды Кубанского государственного технологического университета. 2018. № 3. С. 211-220.

6. RFC 959. File Transfer Protocol (FTP). 1985. URL: https://tools.ietf.org/html/rfc959 (дата обращения: 24.12.2020).

7. RFC 2228. FTP Security Extensions. 1997. URL: https://tools.ietf.org/html/rfc2228 (дата обращения: 25.12.2020).

8. RFC 2577. FTP Security Considerations. 1999. URL: https://tools.ietf.org/html/rfc2577 (дата обращения: 24.12.2020).

9. Соколовский, С. П. Обоснование задач динамического конфигурирования информационных систем для обеспечения их безопасности / С. П. Соколовский, И. С. Ворончихин // Радиоэлектронная борьба в современном мире: сб. тр. участников I Всерос. научно-методич. конф. "Радиоэлектронная борьба в современном мире" (Воронеж, 1-2 октября 2019 г.). – Воронеж, 2019. – С. 300-304.

10. Соколовский, С. П. Поиск новых технических решений по маскированию структуры вычислительных сетей на основе динамического конфигурирования их параметров / С. П. Соколовский, И. С. Ворончихин, А. Д. Гритчин // Решетневские чтения: сб. тр. участников XXIII Междунар. науч.-практич. конф., посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева "Решетневские чтения" (Красноярск, 11-15 ноября 2019 г.). – Красноярск, 2019. – Ч. 2. – С. 447-448.

11. Шерстобитов, Р.С. Маскирование интегрированных сетей связи ведомственного назначения / Р. С. Шерстобитов, С. Р. Шарифуллин,

Р. В. Максимов // Системы управления, связи и безопасности. 2018. № 4. С. 136–175.

12. Sokolovsky, S. P. Moving target defense for securing distributed information systems / S. P. Sokolovsky, I. S. Voronchikhin, A. P. Telenga // Информатика: проблемы, методология, технологии: сб. тр. участников XIX Междунар. научно-методической конф. "Информатика: проблемы, методология, технологии" (Воронеж, 14-15 февраля 2019 г.). – Воронеж, 2019. – С. 639-643.

13. Маскирование структуры распределенных информационных систем в киберпространстве / И.С. Ворончихин [и др.] // Вопросы кибербезопасности. 2019. № 6 (34). С. 92–101.

14. Maximov, R. V. Network Topology Masking in Distributed Information Systems / R. V. Maximov, I. I. Ivanov, S. R. Sharifullin // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). (Moscow, 6-7 December 2017) – Moscow, Bauman Moscow Technical University, 2017. P. 83-87.

15. Максимов, Р. В. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей / Р. В. Максимов, С. П. Соколовский, И. С. Ворончихин // Труды СПИИРАН. 2020. Т. 19. № 5. С. 1018-1049.