Вербальная модель процесса защиты SMTP-сервера от сетевой разведки

А. А. Горбачев, e-mail: druzhochek123@yandex.ru

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

Аннотация. *Защита серверов электронной почты клиент-серверных информационных сетей специального назначения от деструктивных воздействий является важной задачей обеспечения информационной безопасности. В статье приведена вербальная модель процесса проактивной защиты сервера электронной почты от сетевой разведки.*

Ключевые слова: *электронная почта, SMTP-сервер, сетевая разведка, проактивная защита.*

Введение

В настоящее время защита клиент-серверных информационных сетей специального назначения от сетевой разведки приобретает все большее значение. Активизация разведывательной деятельности обусловлена совокупностью существующих факторов и условий, влияющих на информационную безопасность клиент-серверных информационных сетей специального назначения, таких как, открытость протоколов обмена информацией и архитектуры объектов информатизации, наличие техники иностранного производства, входящих в состав объектов информатизации, непрерывное развитие технологий и эволюция информационных потребностей пользователей.

Существующие реактивные методы защиты информации от сетевой разведки, базирующиеся на реагировании (обнаружении, оповещении и блокировании несанкционированных воздействий) на факт ведения сетевой разведки, а также на организационно-запрещающих регламентах, недостаточно эффективны по отношению к динамично развивающимся методам и средствам сетевой разведки [1-8].

Одним из перспективных направлений противодействия средствам сетевой разведки является применение сетевых «ловушек» («network tarpits»), активно воздействующих на средства сетевой разведки, замедляющих работу и истощающих вычислительный ресурс средств разведки (так называемые «проактивные» средства защиты информационных систем) [9-11].

С целью выбора оптимальных параметров функционирования средств проактивной защиты клиент-серверных информационных сетей специального назначения существует необходимость разработки вербальной модели процесса защиты SMTP-сервера от сетевой разведки.

1. Разработка вербальной модели процесса защиты SMTP-сервера

Область применения. Модель может быть использована в информационных системах передачи электронной почты, функционирующих на основе стека сетевых протоколов TCP/IP, с целью снижения результативности сетевой разведки.

Постановка задачи. Принцип работы системы передачи электронной почты основан на простом протоколе передачи электронной почты SMTP («Simple Mail Transfer Protocol») прикладного уровня стека протоколов TCP/IP. Базовая схема работы системы передачи электронной почты представлена на рисунке 1.

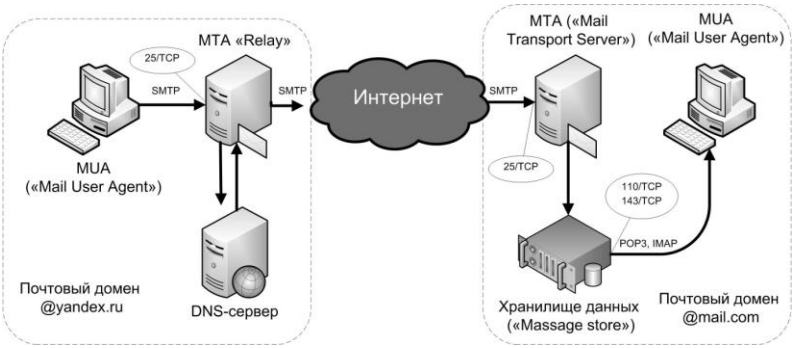

Рис. 1. Принципиальная схема работы системы электронной почты

Когда у клиента имеется почтовое сообщение для передачи, он организует двусторонний канал связи с сервером SMTP, инициализируя TCP-соединение с 25 портом сервера. Передача почтовых сообщений от пользовательского почтового агента клиента («Mail User Agent») почтовому серверу или агенту доставки почты («Mail Transfer Agent»), а также между промежуточными агентами доставки почты («MTA Relay») осуществляется по протоколу SMTP. Адресация почтовых сообщений основана на использовании клиентом идентификаторов (имен) почтовых доменов получателя сообщения, к примеру, «IvanPetrov@mail.com». Маршрутизация сообщений осуществляется на основе MX-записей («Mail eXchenge») в службе DNS, где имени домена электронной почты

соответствует доменное имя почтового сервера. Получение электронных сообщений пользовательским почтовым агентом адресата осуществляется с использованием протоколов POP3 или IMAP с организацией TCP-соединения через порты 110 и 143 соответственно.

Основными информационными угрозами для системы передачи электронной почты является массовая рассылка спама, сканирование сети и сетевая атака типа «отказ в обслуживании», которые строго говоря, взаимосвязаны друг с другом [12-17]. «Спам» - это массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желание ее получать. Распространение массовой рассылки нежелательной электронной почты влияет на все рассмотренные элементы системы электронной почты, в частности, замедляет работу агентов доставки почты, заполняет хранилища данных, снижает пропускную способность сети, что может привести к отказу в обслуживании клиентов. Также под распространением спама может быть замаскировано распространение вредоносного программного обеспечения, так как спам-сообщения имеют сложную структуру для обхода системы фильтрации почтовых серверов, схожую со структурой вирусов.

Описание структуры модели. Разработанная модель описывает процесс защиты клиент-серверных информационных сетей специального назначения от сетевой разведки за счет применения методов проактивной защиты, имитирующих канал связи с плохим качеством. Имитация осуществляется с использованием различных механизмов замедления сетевого соединения между злоумышленником и SMTP-сервером в ходе почтовой транзакции [18-23]. К примеру, одним из механизмов замедления почтовой транзакции является использование специального формата откликов сервера в ходе сеанса связи. В соответствии со спецификацией протокола SMTP сеанс связи между сервером и клиентом осуществляется в текстовом режиме с использованием следующих основных команд: EHLO, MAIL, RCPT, DATA [24-30].

Сервер отвечает на команды клиента откликами с особым форматом командных строк, где первые три цифры представляют собой код отклика, а следующая часть строки состоит из осмысленного текста (комментария). Если между кодом и текстом отклика установлен пробел, то сервер закончил свой ответ, если дефис, то клиент должен ожидать от сервера дополнительные командные строки, то есть сервер возвращает многострочный отклик. На рисунке 2 представлен пример SMTP-сессии, где строки с 5 по 10 являются многострочным откликом.

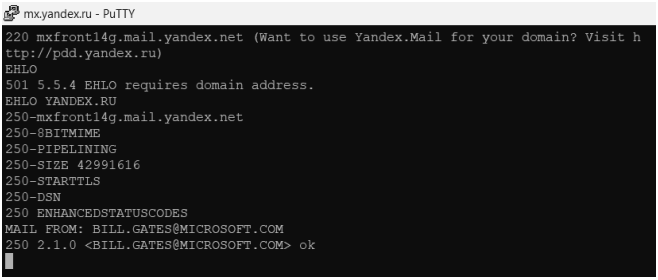

Рис. 2. Пример SMTP-сессии при отправке почтовых сообщений

На рисунке 3 представлена обобщенная блок-схема, включающая действия злоумышленника и противодействие им со стороны средств проактивной защиты SMTP-сервера, составляющая основу вербальной модели защиты SMTP-сервера от сетевой разведки.

Рис. 3. Обобщенная блок-схема, включающая действия злоумышленника и противодействие им со стороны средств проактивной защиты SMTP-сервера

На первоначальном этапе настройки осуществляются записи в конфигурационном файле (блок 1): в «черном списке», сформированном по аналогии с таблицей маршрутизации статически осуществляется запись адресных пространств известных IP-адресов спамеров, устанавливаются величины задержки между отправкой строк многострочных откликов, определяется максимальное количество рабочих портов и другие конфигурационные данные.

На следующем этапе происходит инициировании сеанса с использованием протокола TCP и сетевого порта сервиса электронной почты 25 (блок 2).

Далее происходит проверка IP-адреса почтового клиента в соответствии с таблицей адресов источников распространения спама (блок 3).

На следующем этапе происходит инициирование клиента посредством получения запроса «EHLO (HELO)» (блок 4).

Далее, если IP-адрес не содержится в таблице (блок 5), то почтовая транзакция осуществляется без реализации задержек в многострочных откликах сервера (блок 7).

Если сопоставляемый IP-адрес содержится в таблице «черного списка», то реализуется механизм задержки многострочных откликов сервера, после инициирования клиента программной оболочной перехватываются многострочные отклики и направляются клиенту с заданной величиной задержки (блок 6).

Величина задержки может колебаться от нескольких секунд до нескольких дней, исчерпывая вычислительные и временные ресурсы злоумышленников. На заключительном этапе происходит фиксация результатов почтовой транзакции (блок 8).

Тем не менее, различные виды средств проактивной защиты имеют свои недостатки: несовершенный механизм идентификации злоумышленника, а именно - использование статических записей в таблице, наличие демаскирующих признаков, ограниченное воздействие ловушки на распределенную сеть спам-ботов и другие.

Разработанная вербальная модель защиты сервера передачи электронной почты от сетевой разведки за счет использования средств проактивной защиты позволяет составить математическую модель исследуемого процесса с целью определения оптимальных параметров и режимов функционирования средств защиты.

Дальнейшие исследования в данном направлении автор предполагает сосредоточить на разработке математической модели способа защиты клиент-серверных информационных систем от сетевой разведки с использованием аппарата случайных процессов.

Заключение

Таким образом, разработанная вербальная модель позволяет перейти к разработке математической модели функционирования SMTP-сервера в условиях воздействия средств сетевой разведки с целью формирования требований к техническим характеристикам средств проактивной защиты и определения оптимальных и режимов их функционирования.

Литература

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. тр. участников VIII Междунар. научно-практической конф. "Научные чтения имени профессора Н. Е. Жуковского" (Краснодар, 20–21 декабря 2017 г.). – Краснодар, 2018. – С. 47–52.
3. Sokolovsky, S. P. Hiding computer network proactive security tools unmasking features / S. P. Sokolovsky, R. V. Maximov, A. L. Gavrilov // CEUR Workshop Proceedings : сб. тр. участников конф. "Secure information technologies 2017 (BIT 2017)" (Москва, 6-7 декабря 2017 г.). – Москва, 2017. – С. 88-92.
4. Способ защиты вычислительных сетей [Текст] : пат. 2696330 Российская Федерация : МПК G 06 F 21/50, G 06 F 21/60, H 04 L 9/00 / Соколовский С. П. [и др.] ; заявитель и патентообладатель Краснодарск. высш. воен. училище. – № 2018128075 ; заявл. 31.07.18 ; опубл. 01.08.19, Бюл. № 22. – 30 с.
5. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines / S. P. Sokolovsky [et al.] // Вопросы кибербезопасности. – 2019. – № 1 (29). – С. 10-17.
6. Маскирование идентификаторов канального уровня средств проактивной защиты интегрированных сетей связи специального назначения / С. П. Соколовский [и др.] // Вестник Воронежского института ФСИН России. – 2018. – № 3. – С. 81-89.
7. 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.

8. 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.

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

10. 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). (Москва, 6-7 декабря 2017 г.). – Москва, 2017. – С. 83-87.

11. Iskolnyy, B. B. Survivability Assessment of Distributed Information and Telecommunication Networks / B. B. Iskolnyy, R. V. Maximov, S. R. Sharifullin // Selected Papers of the VIII All-Russian Conference with International Participation "Secure Information Technologies" (BIT 2017). (Москва, 6-7 декабря 2017 г.). – Москва, 2017. – С. 59-65.

12. Искольный, Б. Б. Оценка живучести распределенных информационно-телекоммуникационных сетей / Б. Б. Искольный, Р. В. Максимов, С. Р. Шарифуллин // Вопросы кибербезопасности. – 2017. – № 5 (24). – С. 72-82.

13. 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.

14. 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 : сб. тр. XXIV Международной научно-технической конференции. (Воронеж, 17-19 апреля 2018 г.). – Воронеж, 2018. – С. 169-179.

15. Соколовский, С.П. Модель конфликта в информационной сфере / С. П. Соколовский, С. Р. Шарифуллин, Е. С. Маленков // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета Ю.А. Гагарина в космос : сборник научных статей "VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета

Ю.А. Гагарина в космос" (Краснодар, 12-13 апреля 2018 г.). – Краснодар, 2018. – С. 299-304.

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

17. Катунцев С. Л. Моделирование способа обфускации идентификаторов сетевых устройств в интересах минимизации компрометирующих признаков средств проактивной защиты вычислительных сетей / С. Л. Катунцев, Д. Н. Орехов, С. П. Соколовский // Научные труды Кубанского государственного технологического университета. – 2018. – № 3. – С. 239-248.

18. Моделирование системы конфликтных взаимодействий в информационной системе критического применения / С. С. Кочедыков [и др.] // Вестник Воронежского института ФСИН России. – 2017. – № 4. – С. 74-84.

19. Устранение интервальной неопределенности при распознавании признаков угроз безопасности информационным телекоммуникационным системам / С. П. Соколовский [и др.] // Системы управления и информационные технологии. – 2007. – № 3. – С. 70-73.

20. Душкин, А. В. Способ распознавания вредоносных воздействий на информационную систему / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Телекоммуникации. – 2011. – № 10. – С. 25-28.

21. Усов, Н. А. Моделирование процесса функционирования устройства выявления несанкционированных воздействий на информационную телекоммуникационную систему / Н. А. Усов, С. П. Соколовский // Информатика: проблемы, методология, технологии : материалы XV Международной научно-методической конференции (Воронеж, 12-13 февраля 2015 г.). – Воронеж, 2015. – С. 224-227.

22. Душкин, А. В. Нейросетевая реализация модуля выявления несанкционированных воздействий на информационную телекоммуникационную систему специального назначения / А. В. Душкин, С. П. Соколовский // Информация и безопасность. – 2010. – № 1. – С. 123-126.

23. Соколовский, С. П. Применение адаптивных нечетких систем в вопросах разработки средств выявления несанкционированных воздействий на информацию / С. П. Соколовский, Н. А. Усов // Информатика: проблемы, методология, технологии : материалы XVI

Международной научно-методической конференции (Воронеж, 11-12 февраля 2016 г.). – Воронеж, 2016. – С. 259-264.

24. Результаты анализа способов компрометации средств защиты информации / А. Л. Гаврилов [и др.] // Технические и технологические системы : материалы девятой Международной научной конференции «ТТС-17» (Краснодар, 22-24 ноября 2017 г.). – Краснодар, 2017. – С. 117–121.

25. Разработка программного обеспечения для оценки бескомпроматности средств сетевой защиты / А. Л. Гаврилов [и др.] // Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции (Воронеж, 8-9 февраля 2018 г.). – Воронеж, 2018. – Т. 4. – С. 91–95.

26. Разработка программного обеспечения для компрометации средств сетевой разведки / С. П. Соколовский [и др.] // VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета Ю.А. Гагарина в космос : сборник научных статей "VIII Международная научно-практическая конференция молодых ученых, посвященная 57-й годовщине полета Ю.А. Гагарина в космос" (Краснодар, 12-13 апреля 2018 г.). – Краснодар, 2018. – С. 264-268.

27. Душкин, А. В. Особенности оценки времени противодействия несанкционированным воздействиям на информационные телекоммуникационные системы / А. В. Душкин, М. Ю. Петшауэр, С. П. Соколовский // Информация и безопасность. – 2009. – № 2. – С. 305-308.

28. Душкин, А. В. Модель функционирования системы распознавания угроз безопасности информационно-телекоммуникационной системе / А. В. Душкин, С. В. Скрыль, С. П. Соколовский // Вестник Воронежского государственного технического университета. – 2006. – № 12. – С. 167-170.

29. Душкин, А. В. Способ повышения эффективности распознавания несанкционированных воздействий на информационную телекоммуникационную систему специального назначения в условиях ограничения временного и вычислительного ресурса / А. В. Душкин, В. Н. Похващев, С. П. Соколовский // Информация и безопасность. – 2010. – № 1. – С. 97-102.

30. Процессы высоконадежной обработки информации объектно-реляционных структур критически важных сегментов информационной инфраструктуры / А. С. Дубровин [и др.] // Вестник Воронежского института ФСИН России. – 2017. – № 2. – С. 55-61.