УДК 004.42

А. А. Цыганков[1]*

Метод активного анализа информационных систем

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: aatsygankov@mephi.ru

Аннотация. Проверка аутентичности объектов информационных систем является одним из первых шагов обеспечения информационной безопасности сетевой инфраструктуры предприятия. Нарушение подлинности данных о сетевом объекте, включая его параметры, представляет серьезный риск для всей системы, увеличивая вероятность несанкционированного доступа. В работе рассматривается метод активного анализа информационных систем. Целью исследования является проверка аутентичности объектов сетевой инфраструктуры предприятия. В рамках исследования проанализированы уязвимости протоколов транспортного уровня стека TCP/IP, приведены рекомендации по использованию библиотек с открытым исходным кодом для осуществления межсетевого взаимодействия. На обзор вынесен метод активного анализа информационных систем, а также изложен подход к его разработке. Метод может быть использован при проведении аудита безопасности сетевой инфраструктуры предприятия для проверки соответствия фактических параметров объектов заявленным. Область применимости включает информационные системы, функционирующие на базе стека протоколов TCP/IP.

Ключевые слова: tcp, udp, libnet, libpcap, network security

A. A. Tsygankov[1]*

Method for Active Analysis of Information Systems

[1] National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russian Federation
* e-mail: aatsygankov@mephi.ru

Abstract. Verifying the authenticity of information system objects is one of the first steps in ensuring the information security of an enterprise's network infrastructure. Violation of the authenticity of data about a network object, including its parameters, poses a serious risk to the entire system, increasing the likelihood of unauthorized access. The paper considers the method of active analysis of information systems. The purpose of the study is to verify the authenticity of the enterprise network infrastructure objects. The study analyzes the vulnerabilities of transport layer protocols of the TCP/IP stack, provides recommendations on the use of opensource libraries for inter-network communication. The method of active analysis of information systems is reviewed, and the approach to its development is outlined. The method can be used in conducting security audits of the enterprise network infrastructure to verify the compliance of the actual parameters of objects with the declared ones. The area of applicability includes information systems functioning on the basis of TCP/IP protocol stack.

Keywords: tcp, udp, libnet, libpcap, network security

Введение

Развитие информационных технологий стимулирует государственные учреждения и частные компании расширять собственную информационную инфраструктуру для поддержания уровня экономической конкурентоспособности, что увеличивает поверхность для осуществления потенциальной атаки злоумышленником и усложняет работу по обеспечению безопасности предприятия. Большинство сетевых инфраструктур функционируют на базе стека протоколов TCP/IP, обладающего существенными уязвимостями [1–3]. Эксплуатация данных уязвимостей, в частности использование методов сканирования портов с использованием протоколов транспортного уровня эталонной модели взаимодействия открытых систем OSI (англ. The Open Systems Interconnection model) протокола управления передачей TCP (англ. Transmission Control Protocol) и протокола пользовательских дейтаграмм UDP (англ. User Datagram Protocol) [4], возможна не только злоумышленниками при осуществлении разведки сетевого периметра на предмет возможных точек входа, но и специалистами по сетевой безопасности в рамках проверки аутентичности объектов сетевой инфраструктуры.

Согласно отчету компании Positive Technologies «Актуальные киберугрозы: IV квартал 2023 года», 89 % атак на компьютеры, серверы и сетевое оборудование предприятий прошли успешно. Актуальность проблемы обеспечения сетевой информационной безопасности также подтверждается нормативно-правовыми актами, направленными на регламентацию процесса осуществления информационной безопасности, в частности, Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказом Федеральной службы безопасности Российской Федерации от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств» и Указом Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Приведенные факты указывают на растущую потребность в разработке решений для осуществления активного анализа информационных систем.

Моделирование предметной области

Не существует унифицированного подхода к осуществлению аудита безопасности информационных систем, а применение существующих алгоритмов зависит от начальных условий и целей [5]. В рамках исследования данный процесс рассматривается с точки зрения обеспечения сетевой информационной безопасности и обсуждается с научно-технической, но не с нормативно-правовой позиции. С целью рассмотрения обобщенного алгоритма проведения подготовительных мероприятий к аудиту безопасности информационных систем предлагается к рассмотрению BPMN-диаграмма на верхнем уровне абстракции проверки аутентичности объектов сетевой инфраструктуры предприятия [6] (рис. 1).

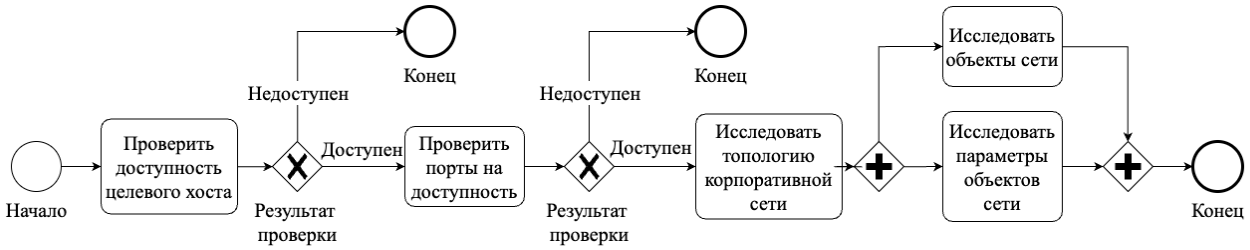

Рис. 1. BPMN-диаграмма проверки аутентичности объектов сетевой инфраструктуры предприятия

В предложенной модели производится декомпозиция цели на атомарные прикладные задачи и рассматривается их реализация с позиции злоумышленника, проводящего разведку системы без заведомых знаний о топологии и объектах корпоративной сети. В рамках исследования рассматривается реализация метода проверки портов на доступность с учетом уязвимостей протоколов транспортного уровня стека TCP/IP.

Постановка задачи

Вышеописанная проблема требует разработки прикладного решения для осуществления разведки поверхности сети. В связи с этим целью исследования является разработка метода активного анализа, обеспечивающего аутентичность объектов сетевой инфраструктуры предприятия.

В рамках декомпозиции цели на задачи выделены этапы работы:

1) систематизация проблематики;

2) проектирование программной реализации минимально жизнеспособного продукта MVP №1 (англ. Minimum Viable Product);

3) разработка прототипа метода активного анализа.

Также стоит отметить, что программная реализация должна использовать актуальные библиотеки с открытым исходным кодом и быть масштабируемой.

Уязвимости протоколов транспортного уровня стека TCP/IP

Следует отметить, что уязвимости, описываемые в данной работе, присутствуют у систем, функционирующих на базе стека TCP/IP, реализованных с учетом технических спецификаций и стандартов, описанных в официальных документах рабочей группы по проектированию Интернета IETF (англ. Internet Engineering Task Force), в котором содержатся спецификации и организационные замечания по темам, связанным с интернетом и компьютерными сетями RFC (англ. Request for Comments) 793 и RFC 768 соответственно [7]. Первый метод исследования состояния порта, который будет использован в данной работе, реализует проверку порта на доступность путем обрывания процесса трехстороннего рукопожатия, предусмотренного в стандарте протокола TCP. (рис. 2).

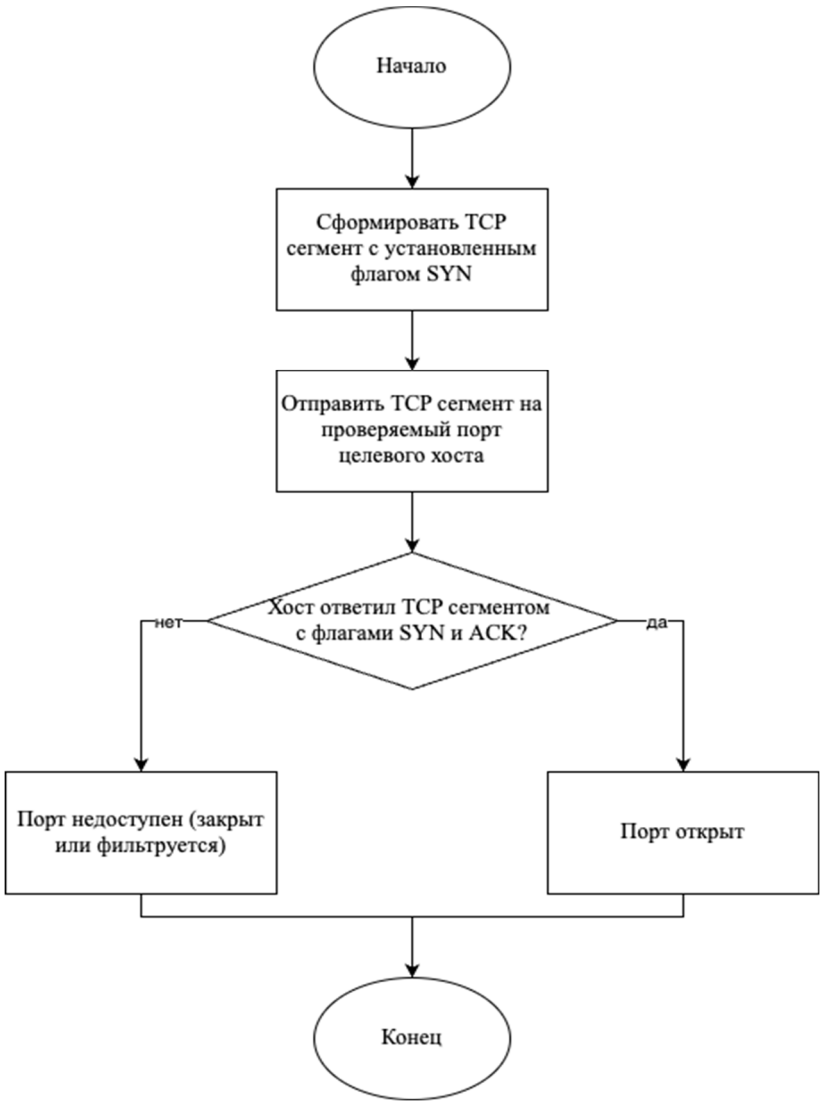

Рис. 2. Метод сканирования с использованием полуоткрытых соединений

Метод использует полуоткрытые соединения (англ. half-open connection), инициируя его установление, но не переходя в состояние подключения. В случае, если при отправке TCP сегмента с установленным флагом SYN порт прослушивается, хост обязан вернуть TCP сегмент с соответствующими флагами – в противном случае порт недоступен.

Второй метод исследования состояния порта, который будет применен в данной работе (рис. 3), использует уязвимость, связанную с отправкой ответной дейтаграммы целевым хостом при попытке отправки UDP дейтаграммы на недоступный порт.

В данной ситуации хост обязан вернуть сообщение о недоступности ICMP-порта. В противном случае, при достижении порта назначения ответ в стандартах протокола не предусмотрен.

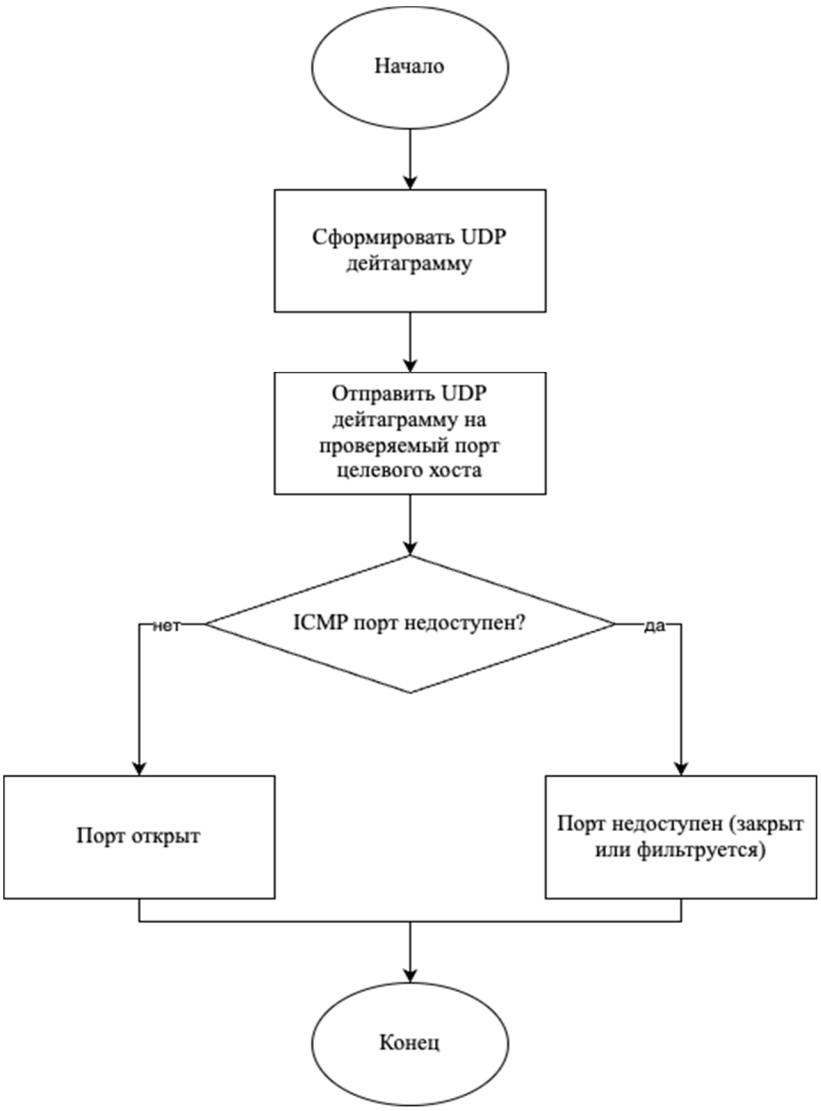

Рис. 3. Метод сканирования с использованием UDP дейтаграмм

Следует отметить, что все вышеописанные уязвимости будут зафиксированы в журналах событий большинства систем [8].

Выбор технологического стека

На этапе выбора технологического стека произведено проектирование метода активного анализа информационных систем, однако в рамках данной работы сделан упор на выбор библиотек.

При реализации алгоритмов проверки портов на доступность для эксплуатации уязвимостей протоколов транспортного уровня стека TCP/IP [9] требуется выстроить межсетевое взаимодействие хоста, реализующего разведку, и объектов сетевой инфраструктуры предприятия. Наиболее распространенными библиотеками с открытым исходным кодом для языка C являются:

1) socket.h – стандартная библиотека Unix-подобных операционных систем, позволяющая осуществлять взаимодействие с сетевыми объектами на высоком уровне;

2) libdnet.h – библиотека с открытым исходным кодом, предоставляющая портативный интерфейс для низкоуровневых сетевых процедур. На данный момент не поддерживается разработчиком [10];

3) libnet.h – кроссплатформенная низкоуровневая библиотека с открытым исходным кодом, используемая для создания, обработки и отправки сырых пакетов [11];

4) pcap.h – кроссплатформенная библиотека с открытым исходным кодом, используемая для захвата пакетов [12].

При условии поддержки разработчиком библиотеки libnet, рекомендуется использовать именно ее для формирования и отправки пакетов. Для захвата ответов от целевой машины рекомендуется использовать библиотеку libpcap, созданную для разработки функций пассивного анализа трафика (снифферов).

С целью сохранения состояний проекта на этапе разработки рекомендуется к использованию распределенная система управления версиями Git и веб-сервис для хостинга IT-проектов GitHub.

Архитектура прототипа

Реализация прототипа метода активного анализа информационных систем предлагает разработку двух модулей, отвечающих за реализацию каждого из алгоритмов сканирования. Требуемыми для корректной работы программы параметрами являются IP-адрес целевой машины и порт (диапазон портов) назначения [13]. Таким образом, предлагается архитектура, содержащая модули:

1) обработки событий;
2) формирования TCP сегмента с установленным флагом SYN;
3) формирования UDP дейтаграммы;
4) отправки пакета с предварительным формированием IP заголовка;
5) захвата пакета и обработки информации, содержащейся в нем.

При реализации пунктов 2-4 требуется использовать библиотеку libnet. Libpcap же рекомендуется рассматривать как интерфейс для захвата пакетов в п. 5.

Разработка прототипа

На первом шаге взаимодействия с libnet требуется инициализировать библиотеку путем вызова функции libnet_init(), передав в качестве параметров LIBNET_RAW4 (константа для определения взаимодействия с интерфейсом сырых сокетов для интернет протокола 4 версии IPv4 (англ. Internet Protocol version 4)), имя сетевого интерфейса и буфер для принятия ошибок (статический массив символов размером LIBNET_ERRBUF_SIZE). Имя используемого сетевого интерфейса можно получить, предварительно вызвав функцию pcap_findalldevs(), которая возвращает список доступных интерфейсов.

При приведении доменного имени или IP-адреса к упорядоченному по байтам адресу, который принимается в качестве параметра функциями библиотеки, используется функция libnet_name2addr4(). В качестве параметров в неё передается контекст libnet (возвращаемое значение функции libnet_init()), строка, со-

держащая IP-адрес или доменное имя, и константа LIBNET_RESOLVE, разрешающая взаимодействие с системой доменных имен DNS (англ. Domain Name System).

Декомпозиция реализации функции отправки TCP-сегмента на атомарные подзадачи:

1) собрать TCP-сегмент с помощью функции libnet_build_tcp(), в качестве параметров в которую передаются порт отправки и порт назначения, флаги, контекст libnet, тэг протокола и иные стандартные поля TCP, не требуемые в рамках отправки сырого пакета;

2) собрать IP-пакет функцией libnet_autobuild_ip(), принимающей размер пакета, указание на используемый протокол на вышестоящем уровне, IP-адрес назначения и контекст libnet.

Формирование UDP дейтаграммы реализуется с помощью функции libnet_build_udp() с аналогичным п. 1 синтаксисом.

Отправка IP пакета осуществляется функцией libnet_write(). Контроль возникновения ошибок реализуется с учетом возвращаемых представленными функциями значений [14].

Декомпозиция реализации функции сниффинга ответа целевого хоста:

1) начать фиксировать приходящий трафик на интерфейс, выбранный при отправке пакета функцией pcap_open_live(), передав в нее имя интерфейса, размер буфера для принимаемого сообщения, флаг неразборчивого режима и время таймаута для чтения;

2) получить адрес сети, передав в функцию pcap_lookupnet() имя интерфейса, IP-адрес и маску;

3) скомпилировать фильтр и установить его функциями pcap_compile() и pcap_setfilter() соответственно;

4) захватить следующий пакет, удовлетворяющий фильтру с помощью функции pcap_next() [15].

В данном разделе рассмотрен процесс разработки MVP №1.

Заключение и обсуждение

В ходе научно-практических изысканий был рассмотрен процесс проверки подлинности информации о сетевых объектах, а также разработан прототип системы на базе метода активного анализа информационных систем, реализованный с использованием библиотек libnet и libpcap. Получившаяся в результате работы программа является масштабируемой, что открывает возможность ее дополнения иными методами сканирования портов, добавления возможностей тестирования хостов на доступность проверки аутентичности параметров объектов сетевой инфраструктуры.

В работу интегрирована поддерживаемая автором кроссплатформенная библиотека с открытым исходным кодом, что является конкурентным преимуществом перед существующими сетевыми сканерами, большинство из которых функционируют на libdnet.

Область применения полученного решения включает информационные системы, функционирующие на базе стека протоколов TCP/IP.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня, Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия / Е. А. Басыня // Защита информации. Инсайд. – 2021. – № 5(101). – С. 16-25.

2. Басыня, Е. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации / Е. А. Басыня, В. Е. Хиценко, А. А. Рудковский // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2019. – Т. 22, № 2. – С. 45-51.

3. Басыня Е. А. Распределенная система сбора, обработки и анализа событий информационной безопасности сетевой инфраструктуры предприятия //Безопасность информационных технологий. – 2018. – Т. 25. – №. 4. – С. 42-51.

4. De Vivo M. et al. A review of port scanning techniques //ACM SIGCOMM Computer Communication Review. – 1999. – V. 29. – N. 2. – PP. 41-48.

5. Alzahrani, M. E. Auditing Albaha University network security using in-house developed penetration tool. // Journal of Physics: Conference Series. Vol. 978. No. 1. IOP Publishing, 2018.

6. Lo E. C., Marchand M. Security audit: a case study [information systems] //Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No. 04CH37513). – IEEE, 2004. – V. 1. – PP. 193-196.

7. Yeung K. H., Fung D., Wong K. Y. Tools for attacking layer 2 network infrastructure //Proceedings of the international multiconference of engineers and computer scientists. – 2008. – V. 2. – PP. 1-6.

8. Liu W. T. Research on Remote Operating System Detection Using Libnet //2009 International Conference on Industrial and Information Systems. – IEEE, 2009. – PP. 101-103.

9. Alcock S., Lorier P., Nelson R. Libtrace: A packet capture and analysis library //ACM SIGCOMM Computer Communication Review. – 2012. – V. 42. – No. 2. – PP. 42-48.

10. Liao S. et al. A comprehensive detection approach of nmap: Principles, rules and experiments //2020 international conference on cyber-enabled distributed computing and knowledge discovery (CyberC). – IEEE, 2020. – PP. 64-71.

11. Anbar M. et al. Investigating study on network scanning techniques //International Journal of Digital Content Technology and its Applications. – 2013. – V. 7. – No. 9. – P. 312.

12. Gadge J., Patil A. A. Port scan detection //2008 16th IEEE international conference on networks. – IEEE, 2008. – PP. 1-6.

13. Gallo M. et al. NaNET: socket API and protocol stack for process-to-content network communication //Proceedings of the 1st ACM Conference on Information-Centric Networking. – 2014. – PP. 185-186.

14. LIU W. T. Design of network testing system based on libnet //Proceedings of 2008 International Symposium on Distributed Computing and Applications for Business Engineering and Science. – 2008.

15. Garcia L. M. Programming with libpcap-sniffing the network from our own application //Hakin9-Computer Security Magazine. – 2008. – V. 2. – P. 2008.