Morozov Konstantin Yuryevich, Povolzhskiy State University of Telecommunications and Informatics, 26, 3 floor, Kirov Avenue, Samara, 443010, Russian Federation; Applicant for the PhD degree in Technical Sciences. Tel. +7 846 203-20-26. E-mail: mky@siprs.ru

References

1. Shinakov Yu.S. Crest factor of OFDM signals and harmonic distortion in radio equipment of wireless access systems. *Tsifrovaja obrabotka signalov*, 2012, no. 4, pp. 60–64. (In Russ.)
2. Väänänen O. Digital modulators with crest factor reduction techniques. Diss. Dr. of Science in Technology. Helsinki University of Technology, Electronic Circuit Design Laboratory, Report 42, Espoo, 2006, 127 p.
3. GOST R 54462–2011. Digital Radio Broadcasting System DRM. Requirements and Parameters. Moscow: Standartinform, 2013, 416 p. (In Russ.)
4. ETSI EN 302 245 V2.1.1 (2018-06) Transmitting equipment for the Digital Radio Mondiale (DRM) sound broadcasting service; Harmonised Standard for access to radio spectrum. 26 p. URL: https://www.etsi.org/deliver/etsi_en/302200_302299/302245/02.01.01_60 (accessed: 02.02.2021).
5. Rules for the use of broadcasting systems. Part I. Rules for the use of terrestrial digital broadcasting transmitters operating in the frequency ranges 0.1485-0.2835 MHz; 0.5265-1.6065 MHz; 3.95-26.10 MHz. 16 p. URL: https://digital.gov.ru/ru/documents/4058 (accessed: 02.02.2021).
6. Recommendation ITU-R BS.1660-8 (06/2019) Technical basis for planning terrestrial digital sound broadcasting in the VHF band. 86 p. URL: https://www.itu.int/dms_pubrec/itu-r/rec/bs/R-REC-BS.1660-8-201906-I!!PDF-pdf (accessed: 02.02.2021).
7. Buzov A.L., Morozov K.Yu. Crest factor reduction techniques in DRM broadcast transmitters. *Radiotehnika*, 2019, no. 6 (7), pp. 24–29. (In Russ.)
8. Väänänen O., Vankka J., Halonen K. Simple Algorithm for Peak Windowing and its application in GSM, EDGE and WCDMA systems. *IEE Proceedings Communications*, 2005, vol. 152, no. 3, pp. 357–362.
9. Morozov K.Yu. Optimal filtering while limiting the crest factor of the DRM + signal. *Physics of Wave Processes and Radio Systems*, 2020, vol. 23, no. 3, pp. 82–89. (In Russ.)
10. Van Nee R., Prasad R. *OFDM for Wireless Multimedia Communications*. Norwood: Artech House Publishers, 2000, 280 p.

Received 11.01.2021

ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 004.056.53

ВЫЯВЛЕНИЕ DOS-АТАК С ПОМОЩЬЮ АНАЛИЗА СТАТИСТИЧЕСКИХ ХАРАКТЕРИСТИК ТРАФИКА

Поздняк И.С., Плаван А.И.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: i.pozdnyak@psuti.ru

В настоящее время количество проводимых каждый день атак во всем мире постоянно увеличивается. Причем злоумышленники используют наряду со старыми способами и инструментами новые, ранее неизвестные. Обнаружить их становится все сложнее. В данной статье рассматривается проблема выявления аномальной составляющей в трафике, обусловленной деятельностью злоумышленников или неисправностями сети. Для этого проводится моделирование атаки типа отказ в обслуживании и осуществляется захват соответствующего трафика с целью его дальнейшего анализа. Сравниваются статистические характеристики трафика, соответствующего нормальному состоянию системы и состоянию активной атаки. По результатам анализа делается вывод о нали-

чии статистических зависимостей в определенных параметрах сетевого трафика, позволяющих сделать вывод об обнаружении аномальной составляющей, причины которой необходимо выяснять.

Ключевые слова: *анализ трафика, DoS-атака, системы обнаружения вторжений, статистические характеристики, коэффициенты корреляции, информационная безопасность*

Введение

В повседневной жизни мы практически постоянно взаимодействуем с различными информационными потоками. Различные информационные системы банков, государственных и частных предприятий, образовательных учреждений, транспорта для качественного и своевременного предоставления услуг хранят и обрабатывают очень большие объемы информации. Данные проходят через десятки и сотни разнородных сетей различного уровня, и чем длиннее этот путь, тем сложнее контролировать, как и куда передается информация. При передаче информации могут возникать различные нештатные ситуации, например, выход сетевого оборудования из строя или хакерские атаки. Эти ситуации могут привести к значительным потерям для организаций.

Для противодействия злоумышленникам создаются сложные многоуровневые системы защиты информации. В состав этих систем входят различные средства защиты информации: антивирусы, межсетевые экраны, системы обнаружения и предотвращения вторжений, системы предотвращения утечек данных (DLP-системы), криптографические средства защиты, виртуальные частные сети и т. д.

Защита от атак

Для обеспечения корректной работы всех связанных систем хранения, обработки и передачи данных должны соблюдаться три ключевых свойства информации: конфиденциальность, целостность и доступность. Нарушение хотя бы одного из этих свойств уже может привести к сбоям в работе системы.

В процессе эксплуатации информационной системы необходимо обеспечивать ее работоспособность, то есть диагностировать работу сети и подключенных к ней серверов, рабочих станций и иных устройств, а также защищать ресурсы сети от реализации угроз безопасности. Для достижения своих целей злоумышленники используют богатый набор средств, включающий различные программные и аппаратные средства, методы социальной инженерии. Инструменты злоумышленников постоянно совершенствуются и модернизируются, появляются новые средства и методы проведения атак. Это создает дополнительное требование к средствам зашиты информационных систем – они должны эффективно выявлять как существующие, так и ранее неизвестные виды атак.

Подходящие под это требование средства защиты информации используют общий подход – выявление отклонений от «нормального» состояния информационных ресурсов сети, или аномалий. Эти аномалии могут быть вызваны сбоями в работе аппаратного и программного обеспечения, а также хакерскими атаками.

Системы обнаружения вторжений

Системы обнаружения вторжений (СОВ) – это множество аппаратных и программных средств, позволяющих собирать информацию из различных точек защищаемой компьютерной сети и анализировать эту информацию для выявления попыток нарушения режима информационной безопасности.

Существует несколько классификаций СОВ. Одна из них представлена на рисунке 1, в которой деление происходит по функциональным и нефункциональным признакам.

Кроме того, по механизму анализа параметров трафика СОВ делятся на два типа – обнаружение аномалий и обнаружение злоупотреблений (сигнатур злонамеренных действий). Преимуществом метода обнаружения аномалий по сравнению с обнаружением сигнатур является возможность обнаруживать ранее не встречавшиеся атаки. При использовании данного механизма анализа создается образ нормального состояния системы, с которым в дальнейшем будут анализироваться и сравниваться все действия в системе. Признаком атаки может являться отклонение текущих показателей от показателей образа на определенное значение. Также могут использоваться и другие методы оценки [2]:

– статистические методы;
– интеллектуальный анализ данных;
– методы искусственного интеллекта;
– вейвлет-анализ;
– визуальный анализ данных.

Достаточно подробно методы обнаружения атак описаны в [3].

Статистический анализ трафика

Статистические методы анализа являются наиболее востребованными при обнаружении

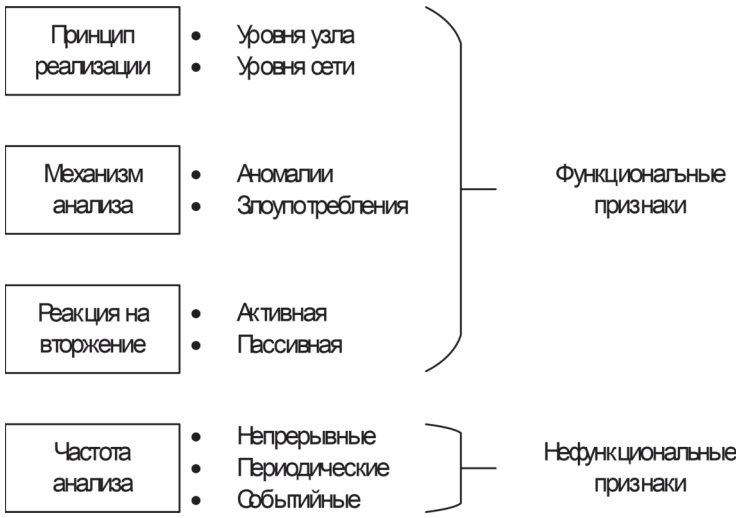

Рисунок 1. Классификация СОВ

вторжений, так как позволяют достаточно гибко подходить к этому процессу. В различных мультисервисных сетях применяется мониторинг трафика с целью предотвращения возникающих в процессе эксплуатации сбоев и поддержания доступности информационной системы на требуемом уровне.

Анализ сетевого трафика позволяет охарактеризовать известные конструктивные особенности сети, выявить неизвестные и внести изменения в ее структуру на основании полученных результатов. Результат анализа сетевого трафика может предоставить основания для изменения существующих бизнес-процессов [4]. Для захвата и анализа трафика применяются специальные утилиты, снифферы (traceroute, iperf, tcpdump, Wireshark, Snort) и специальные протоколы (SNMP, NetFlow, sFlow).

Так как процесс передачи пакетов в сети по сути представляет собой поток событий, для исследования трафика можно применять стандартные методы математической статистики. При этом интенсивность поступления пакетов в сети может быть представлена как случайный процесс. Данные, полученные в результате серии экспериментов, как раз и являются объектом исследования в прикладной статистике.

Кроме того, при исследовании трафика может использоваться корреляционный анализ – статистический метод изучения взаимосвязи между двумя и более случайными величинами. При анализе сетевого трафика в качестве случайных величин выступают различные параметры последовательности пакетов либо характеристики сетевых устройств.

Охарактеризовать эти случайные величины позволяет, например, корреляционный анализ. Между случайными переменными может существовать неявная взаимосвязь, то есть изменение закона распределения одной переменной также повлечет за собой изменение закона распределения другой. Сила и направление такой зависимости определяются коэффициентом корреляции, который может иметь любое значение из интервала [–1,0; 1,0]. Нулевое значение указывает на отсутствие корреляции, значение, близкое к единице на сильную взаимосвязь. Знак коэффициента определяет направление связи.

Корреляционный анализ позволяет установить лишь наличие статистической взаимосвязи, но это не позволяет делать вывод о наличии реальной причинно-следственной связи двух случайных величин. Кроме расчета коэффициентов корреляции необходимо также выполнять проверку их значимости, в основе которой лежит принцип проверки статистических гипотез.

В случае, когда исследуемым объектом является сетевой трафик, возникает два следующих возможных варианта.

1. Трафик характерен для нормального состояния системы.

2. Трафик не характерен для нормального состояния системы.

Рассмотрение таких задач в математической постановке приводит к понятию статистической гипотезы. С точки зрения статистики обнаружение изменений опирается на тестовые гипотезы H_0 – утверждающей, что изменений нет, и H_1 – что изменения есть. Разработка таких гипотез требует априорного знания распределения вероятностей изменений. Если такого знания нет, необходимо прибегать к оценке распределения, то есть наиболее подходящему значению по результатам серии наблюдений.

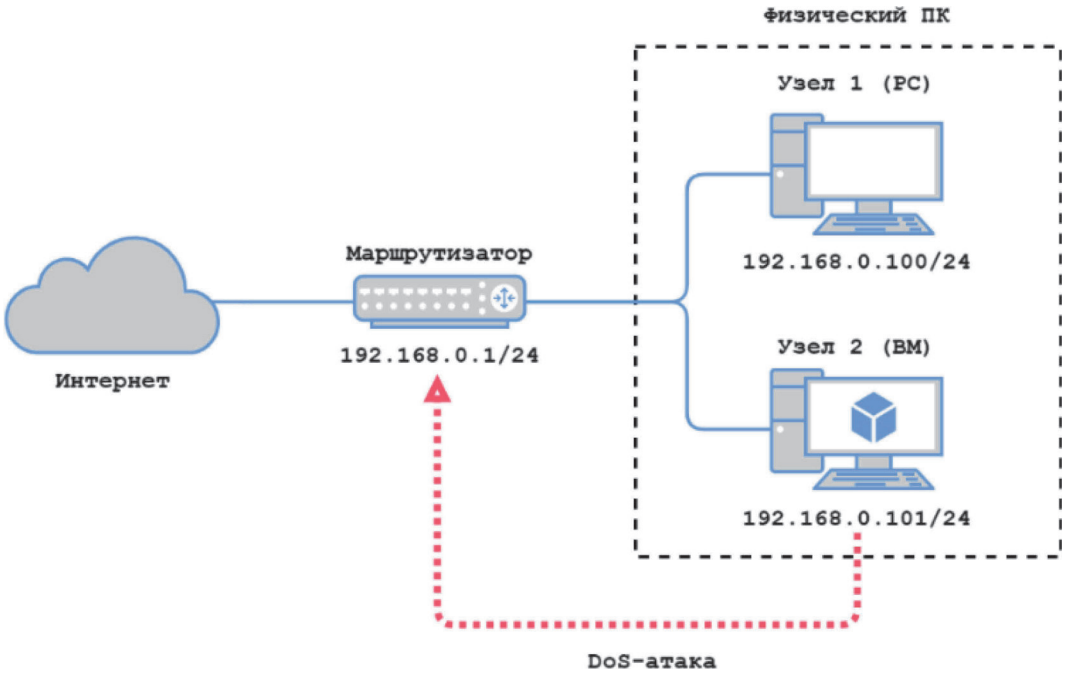

Рисунок 2. Структура сети исследования

Статистический критерий – это правило, по которому принимается решение о принятии истинной и отклонении ложной гипотезы с наиболее высокой вероятностью. Критерии делятся на параметрические и непараметрические [5]. Для оценки эффективности применения статистических критериев вводится понятие ошибок первого и второго рода. В контексте систем информационной безопасности они представляются как следующие ситуации:

– легальные пользователи классифицируются как злоумышленники (ошибка первого рода);

– злоумышленники классифицируются как легальные пользователи (ошибка второго рода).

Для оценки эффективности алгоритмов классификации (то есть отнесение текущего сетевого трафика к нормальному или аномальному) часто применяются ROC-кривые [6]. ROC-кривая (кривая ошибок) – это график, отражающий соотношение между долей верных срабатываний (чувствительностью) и долей ложных срабатываний системы (специфичностью).

Все эти понятия в большей или меньшей степени применяются при статистическом анализе трафика.

Моделирование DoS-атаки

Моделирование проводилось в домашней сети, состоящей из двух узлов и маршрутизатора. Один узел является реальной машиной, а второй – виртуальной машиной (ВМ), расположенной на том же компьютере (см. рисунок 2). На ВМ будут имитироваться действия злоумышленника, направленные на сетевой маршрутизатор с целью блокировки доступа во внешнюю сеть.

В работе исследовалась интенсивность сетевого трафика, характерного для нормальной активности (просмотр веб-страниц и потокового видео), а также проводилось его сравнение с трафиком, соответствующим состоянию активной DoS-атаки (SYN-, RST-, FIN- и ICMP-flood).

Для моделирования DoS-атак использовалась консольная утилита hping3. Она позволяет генерировать пакеты ICMP/UDP/TCP, посылать их и анализировать полученные ответы. Утилита Hping3 входит в состав дистрибутива Kali Linux и является одним из стандартных инструментов для проверки безопасности сети.

Соответствующие команды запуска представлены в работе [7; 8]. Для захвата трафика была использована программа Wireshark. Для определения математического ожидания, среднеквадратического отклонения (СКО), коэффициентов корреляции была написана программа на языке Java, которая также позволяет строить графики по полученным значениям. Для исследования была выбрана характеристика сетевого трафика, описывающая длительность между моментами поступления пакетов τ [9; 10].

Захват трафика для сценариев нормального поведения системы не предполагает каких-то особенных действий и выполняется в программе Wireshark на используемом по умолчанию сетевом интерфейсе компьютера. Для захвата трафика в сценариях, относящихся к аномальному поведению системы, будет проведено моделирование DoS-атак различных видов [11]:

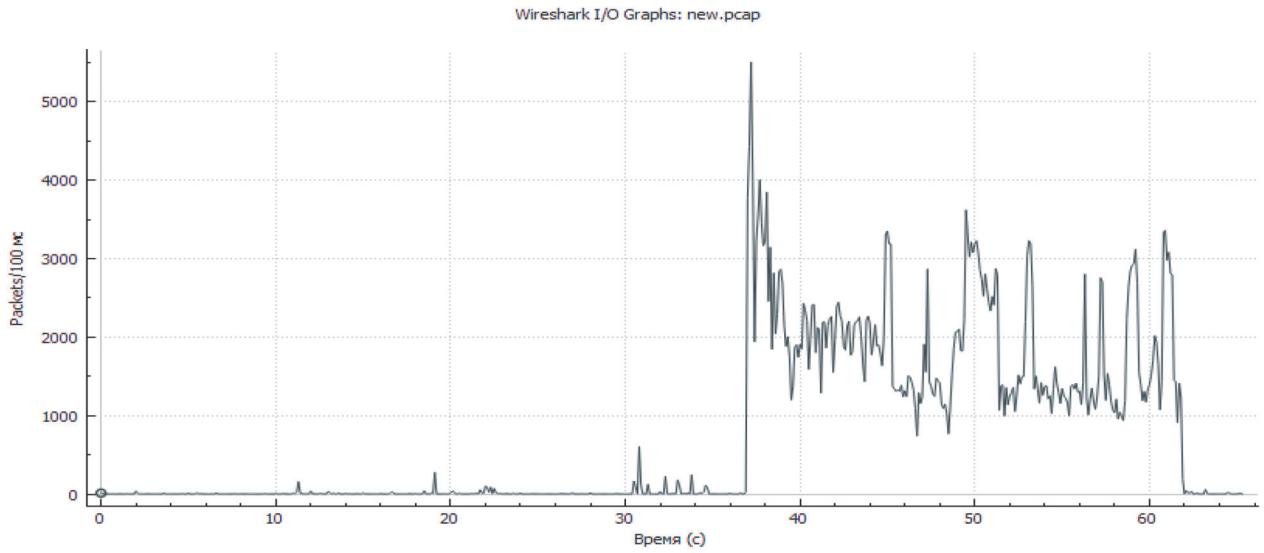

Рисунок 3. Интенсивность поступления пакетов при атаке SYN-flood

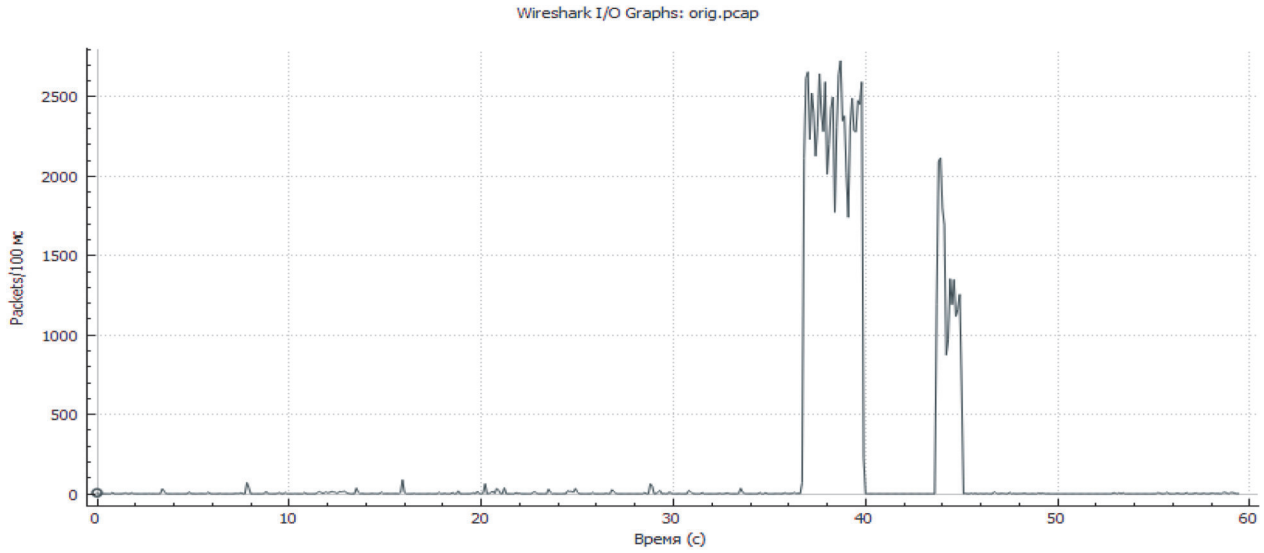

Рисунок 4. Интенсивность поступления пакетов при атаке ICMP-flood

– *SYN-flood* – суть данной атаки заключается в отправке большого количества SYN-запросов (запросов на подключение по протоколу TCP) в короткий срок;

– *RST-flood* – в случае данной атаки, злоумышленник посылает большое количество TCP-пакетов с установленным флагом RST (reset). Сервер вынужден выделять значительное количество системных ресурсов для сопоставления входящих пакетов с текущими открытыми соединениями, что приводит к потере производительности сервера и к его частичной недоступности;

– *FIN-flood* – атака данного типа эксплуатирует ту же особенность обработки TCP-пакетов сетевыми устройствами, что и RST-flood, но злоумышленник устанавливает в пакетах флаг FIN (finish);

– *ICMP-flood* – суть данной атаки состоит в том, что злоумышленник отправляет большое количество небольших по объему ICMP-пакетов.

На рисунках 3 и 4 представлены графики интенсивности поступления пакетов (при проведении атак типа SYN-flood и ICMP-flood соответственно), на которых можно четко выделить момент начала атаки. Так как в этот момент происходит резкое изменение интенсивности поступления пакетов, можно считать, что система сразу переходит в аномальное состояние и рассмотрение промежуточного(переходного) состояния невозможно.

При анализе математического ожидания и СКО последовательности τ для нормальной и аномальной активности в сети было выявлено, что при наличии атаки оба этих показателя уменьшаются более чем в сто раз, что является

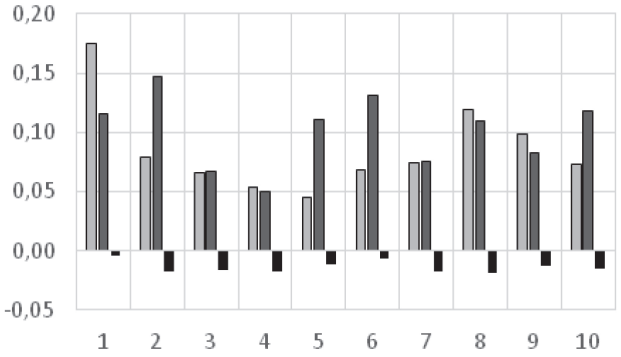

Рисунок 5. Коэффициенты корреляции при атаке SYN-flood

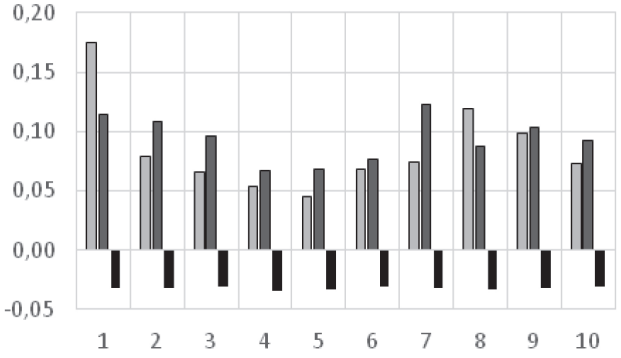

Рисунок 6. Коэффициенты корреляции при атаке RST-flood

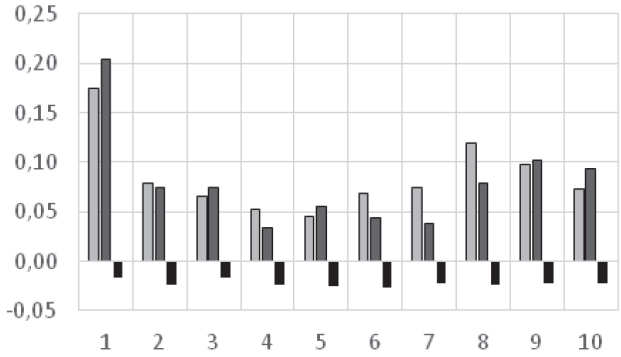

Рисунок 7. Коэффициенты корреляции при атаке FIN-flood

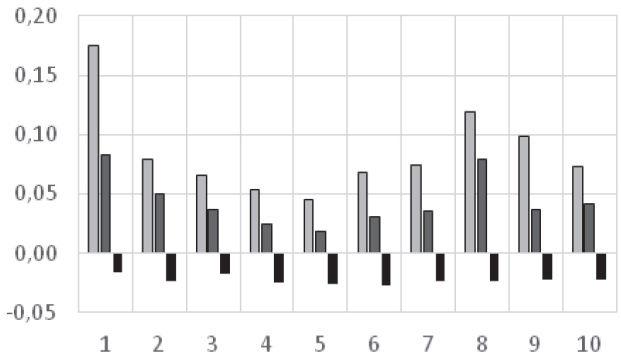

Рисунок 8. Коэффициенты корреляции при атаке ICMP-flood

вполне характерным для данного вида вторжения. На рисунках 5–8 представлены значения коэффициентов корреляции τ, рассчитанные при разных сценариях: белым цветом выделены значения, соответствующие нормальному трафику, серым – смеси нормального трафика и трафика атаки и черным – трафику, в котором присутствуют лишь пакеты DoS-атаки.

По графикам видно, что коэффициенты корреляции меняют свое значение для трафика, который является смесью нормального трафика и трафика атаки (серые столбцы), что говорит об изменении характера наблюдаемой последовательности. Следует заметить, что коэффициенты корреляции трафика, в котором присутствуют только пакеты DoS-атаки (черные столбцы), значительно отличаются от показателей трафика нормальной активности.

Заключение

Рассмотренные статистические характеристики исследуемого трафика при проведении DoS-атаки значительно отличаются от тех же показателей трафика с нормальной активностью, что является поводом для дальнейшего более детального анализа изучаемых последовательностей с целью исключения ошибок первого рода.

Эффективность предложенного метода обнаружения аномалий зависит от выбора анализируемого параметра трафика, а также от характеристик самого трафика, соответствующего нормальной активности. Возможно предположить, что в сети предприятия трафик имеет более устойчивую статистическую картину, чем в домашней сети, в которой проводилось моделирование. Так, если «нормальный» трафик неоднороден и имеет неустойчивую во времени структуру (не стационарен), метод обнаружения аномалий на основе анализа корреляционных коэффициентов может приводить к ложноположительным срабатываниям.

Эффективность обнаружения изменений в параметрах сетевого трафика можно повысить при помощи метода «скользящего окна», если рассматривать только определенный интервал значений, то есть часть трафика, характеризующую начало или конец атаки, и сдвигать этот интервал во времени.

Литература

1. Bocetta S. So long, ransomware: organizations brace for cryptojacking. URL: https://www.dataversity.net/so-long-ransomware-organizations-brace-for-cryptojacking (дата обращения: 28.08.2020).

2. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений в компьютерные сети (сетевые аномалии). М.: Горячая линия–Телеком, 2013. 220 с.
3. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИ РАН. 2016. № 45. С. 207–244.
4. Real-time network anomaly detection system using machine learning / S. Zhao [et al.] // 11th International Conference on the Design of Reliable Communication Networks (DRCN). Kansas City, MO. 2015. P. 267–270.
5. Стукач О.В. Проверка статистических гипотез. URL: http://ieee.tpu.ru/system/hypotez.htm (дата обращения: 22.07.2020).
6. Brownlee J. How to use ROC curves and precision-recall curves for classification in Python. URL: https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-classification-in-python (дата обращения: 22.07.2020).
7. hping3 – тестирование сети. URL: http://its27.ru/2019/05/27/hping3-testing-network (дата обращения: 20.06.2020).
8. hping3 Package Description. URL: https://tools.kali.org/information-gathering/hping3 (дата обращения: 20.06.2020).
9. Карташевский В.Г., Поздняк И.С. Фильтрация наблюдаемого трафика как способ обнаружения вторжений // Вестник УрФО. 2019. № 1 (31). С. 17–22.
10. Карташевский В.Г. Основы теории массового обслуживания. М.: Горячая линия–Телеком, 2013. 130 с.
11. Шапиро Л. Атаки DDoS. Часть 2. Арсенал противника // БИТ. 2015. № 6. С. 24–27.

Получено 21.09.2020

Поздняк Ирина Сергеевна, к.т.н., доцент кафедры информационной безопасности (ИБ), Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 927 657-24-27. E-mail: i.pozdnyak@psuti.ru

Плаван Алексей Игоревич, аспирант кафедры ИБ ПГУТИ. 443010, Российская Федерация, г. Самара, ул. Л. Толстого, 23. Тел. +7 927 736-50-55. E-mail: aleksej.plavan@ya.ru

IDENTIFICATION OF DOS ATTACKS BY ANALYSIS OF SOME STATISTICAL CHARACTERISTICS OF TRAFFIC

Pozdnyak I.S., Plavan A.I.
Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation
E-mail: i.pozdnyak@psuti.ru

Currently, the number of attacks carried out every day around the world is constantly increasing. Moreover, cybercriminals use new, previously unknown methods along with old methods and tools. It's getting harder and harder to spot them. This article discusses the problem of identifying an anomalous component in traffic caused by the activities of intruders or network failures. For this, a denial-of-service attack is simulated and the corresponding traffic is captured for further analysis. The statistical characteristics of traffic corresponding to the normal state of the system and the state of an active attack are compared. Based on the results of the analysis, it is concluded that there are statistical dependencies in certain parameters of network traffic, which make it possible to conclude that an anomalous component has been detected.

Keywords: *traffic analysis, DoS attack, intrusion detection systems, statistical characteristics, correlation coefficients, information security*

DOI: 10.18469/ikt.2021.19.1.10

Pozdnyak Irina Sergeevna, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; Associate Professor of Information Security Department, PhD in Technical Science. Tel. +7 927 657-24-27. E-mail: i.pozdnyak@psuti.ru

Plavan Aleksey Igorevich, Povolzhskiy State University of Telecommunications and Informatics, 23, L. Tolstoy Street, Samara, 443010, Russian Federation; PhD Student of Information Security Department. Tel. +7 927 736-50-55. E-mail: aleksej.plavan@ya.ru

References

1. Bocetta S. So long, ransomware: organizations brace for cryptojacking. URL: https://www.dataversity.net/so-long-ransomware-organizations-brace-for-cryptojacking (accessed: 28.08.2020).
2. Sheluhin O.I., Sakalema D.Zh., Filinova A.S. *Detection of Intrusions into Computer Networks (Network Anomalies)*. Moscow: Gorjachaja linija–Telekom, 2013, 220 p. (In Russ.)
3. Branitskij A.A., Kotenko I.V. Analysis and classification of methods for detecting network attacks. *Trudy SPII RAN*, 2016, no. 45, pp. 207–244. (In Russ.)
4. Zhao S. et al. Real-time network anomaly detection system using machine learning. *11th International Conference on the Design of Reliable Communication Networks (DRCN)*, Kansas City, MO, 2015, pp. 267–270.
5. Stukach O.V. Testing statistical hypotheses. URL: http://ieee.tpu.ru/system/hypotez.htm (accessed: 22.07.2020). (In Russ.)
6. Brownlee J. How to use ROC curves and precision-recall curves for classification in Python. URL: https://machinelearningmastery.com/roc-curves-and-precision-recall-curves-for-classification-in-python (accessed: 22.07.2020).
7. hping3 – network testing. URL: http://its27.ru/2019/05/27/hping3-testing-network (accessed: 20.06.2020). (In Russ.)
8. hping3 Package Description. URL: https://tools.kali.org/information-gathering/hping3 (accessed: 20.06.2020).
9. Kartashevskij V.G., Pozdnjak I.S. Filtering monitored traffic as a way to detect intrusions. *Vestnik UrFO*, 2019, no. 1 (31), pp. 17–22. (In Russ.)
10. Kartashevskij V.G. *Basics of Queuing Theory*. Moscow: Gorjachaja linija–Telekom, 2013, 130 p. (In Russ.)
11. Shapiro L. DDoS attacks. Part 2. Arsenal of the enemy. *BIT*, 2015, no. 6, pp. 24–27. (In Russ.)

Received 21.09.2020

УДК 004.4

РАЗРАБОТКА МЕТОДА МОНИТОРИНГА АНОМАЛЬНОГО ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ В РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЕ: ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ

Ряполова Е.И., Преснов А.А., Цветкова К.Е.
Оренбургский филиал Поволжского государственного университета телекоммуникаций и информатики, Оренбург, РФ
E-mail: presnov.aleksey@mail.ru

Статья посвящена разработке системы мониторинга аномального поведения пользователя в распределенных информационно-вычислительных системах и построению математической модели разрабатываемой системы. Проведен анализ современных методов поведения пользователя информационной системы. Главное внимание уделено тому, что существующие методы защиты информационных систем имеют ряд недостатков, исправить которые возможно при использовании разрабатываемого метода, который осуществляет защиту как от внутренних, так и от внешних нарушителей. Для разработки системы мониторинга аномального поведения пользователя в распределенных информационно-вычислительных системах необходимо решить ряд задач: провести анализ методов мониторинга поведения пользователей в информационной системе; построить целевую функцию и выбрать критерии для оценки качества методов анализа аномального поведения пользователей. В исследовании использованы методы теории информационной безопасности, теории автоматов, теории распознавания образов и теории проектирования вычислительных систем.