УДК 004.056.5:378.3

В. В. Подтопельный, И. А. Ветров

ОПРЕДЕЛЕНИЕ ПРИГОДНОСТИ ПРАВИЛ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ И ИХ МАТЕМАТИЧЕСКАЯ ОЦЕНКА

Поступила в редакцию 16.04.2021 г.
Рецензия от 30.04.2021 г.

Рассмотрены проблемы, возникающие при выявлении сетевых атак с помощью систем обнаружения вторжений в корпоративной сети предприятия. Рассмотрены особенности формирования сигнатур сетевых атак. Исследуется проблема совпадения параметров сетевых вторжений и параметров поврежденных пакетов. Для оценки пригодности правил обнаружения сетевых атак и последующего их контроля предложен способ модернизации компонентного состава систем обнаружения вторжений. Рассмотрен способ математической оценки пригодности правил обнаружения сетевых атак.

The article deals with the problems that arise when detecting network attacks using intrusion detection systems in the corporate network of an enterprise. The features of the formation of signatures of network attacks are considered. The problem of coincidence of parameters of network intrusions and parameters of damaged packets is investigated. To assess the suitability of the rules for detecting network attacks and their subsequent control, a method for upgrading the component composition of intrusion detection systems has been redesigned. A method of mathematical evaluation of the suitability of the rules for detecting network attacks is considered.

Ключевые слова: риск, информационная система, сетевая атака, сетевое вторжение, модуль

Keywords: risk, information system, network attack, network intrusion, module

Введение

На современном этапе развития технологии защиты сетевых данных системы обнаружения сетевых вторжений (СОВ) разрабатываются как комплексное (многосоставное) программное решение. Функционал подобных систем может расширяться за счет подключаемых специфических дополнений (модулей), при этом каждое дополнение реализует какой-либо отдельный функционал. Типовая архитектура систем обнаружения вторжений предполагает следующий набор основных модулей:

— модуль захвата сетевого трафика;
— модуль анализа захваченного трафика;
— модуль базы правил, сетевых сигнатур;
— дополнительные подключаемые модули.

Основные задачи приведенных модулей следующие: получить данные о трафике, разобрать его и с помощью модуля анализа выявить

маркеры (особенные признаки, данные сетевых пакетов), свидетельствующие о присутствии вредоносного воздействия на защищаемые ресурсы. Принадлежность маркеров к указателям на атаки определяется путем сравнения полученного с присутствующими в базе СОВ данными правил в том порядке и в том контексте, который предполагает правило базы.

Анализируются следующие события и параметры правил, их особенности [5]:

— запрос к закрытым портам;

— непредусмотренная алгоритмом протокола TCP последовательность флагов (если соединение отсутствует и при этом принимается пакет с флагом, отличным от SYN, то это означает нарушения порядка соединения, что указывает на ведение атакующих действий);

— большое количество попыток подключиться к портам сетевых служб (открыть соединения) за один промежуток времени;

— неправильные контрольные суммы пакетов протоколов транспортного уровня (TCP, UDP);

— неправильная последовательность флагов TCP-протокола при отладке сеанса (неправильная последовательность флагов при открытии соединения или в ходе соединения, например ACK пакет до SYN);

— попытки открытия соединений с одного порта сетевого узла к другому порту того же узла;

— обращение с портов, которые открыты для передачи данных;

— совпадение IP-адреса назначения сетевого пакета любой сетевой службы с IP-адресом хоста;

— последовательный опрос портов и др.

Некоторые сетевые параметры могут определяться как маркеры атаки только тогда, когда они используются совместно с другими маркерами или при определенных условиях их проявления. При этом их фиксация может указывать на простую ошибку передачи данных в сети. Таким образом, само выявление сигнатурных маркеров в некоторых случаях не гарантирует того, что атака была в действительности. Более того, повышается вероятность получения ошибочных сетевых пакетов при работе в сетях большого масштаба, а также при некорректной настройке маршрутизирующих устройств. Поэтому, чтобы снизить большое количество ложных срабатываний СОВ, многие маркеры могут намеренно не учитываться при настройке правил фильтрации сетевых пакетов. Соответственно, при эксплуатации системы обнаружения вторжений довольно часто возникают ситуации, при которых малозаметные (плохо интерпретируемые) сетевые атаки оказываются успешными. При этом СОВ остается работоспособной и может отсеивать большой массив других атак.

Определение специфики подготовки безопасного активного аудита информационной безопасности АСУТП

Очевидно, что успешность нападения может зависеть не только от наличия незарегистрированных уязвимостей в компонентах корпоративных информационных сетей, но и от некорректных правил систем

обнаружения атак, неправильно или недостаточно полно описывающих признаки атакующих воздействий. Некорректность описания может быть связана с множеством различных факторов, в том числе и новизной атаки. Параметры таких нападений могут быть неизвестны специалистам информационной безопасности. Более того, сами драйверы операционной системы могут по-разному реагировать на воздействие различных атакующих систем (в таблице 1 приведены особенности реагирования различных операционных систем на операции сетевой разведки) [5].

Таблица 1

Вывод Nmap на запрос с определенными флагами

Комбинация флагов	Операционная система		
	Linux с версией ядра 4.4.0	Windows 7	MAC OS X
SYN + URG + PSH	open	filtered	open
SYN + ACK + PSH	closed	closed	closed
SYN + FIN + PSH	filtered	filtered	filtered
SYN+ FIN + RST	filtered	filtered	filtered
ACK + FIN + RST	filtered	filtered	filtered
ACK + FIN + PSH	closed	filtered	closed

В другом случае описание параметра времени в правиле резко осложняется неравномерной зависимостью скорости сканирования от количества портов тестируемого сетевого узла. В таблице 2 можно видеть сильный разброс значений времени отклика при полуоткрытом SYN-сканировании с помощью утилиты Nmap. На показатели сканирования могут влиять следующие факторы [5]:

— показатель загрузки трафика в сети в период сканирования;

— пропускная способность сетевого интерфейса;

— количество пакетов, которые отправляет Nmap в данный промежуток времени.

Таблица 2

Результаты полуоткрытого SYN-сканирования

Число портов	Среднее значение, с	Раунд								
		1	2	3	4	5	6	7	8	9
1	0,63	0,63	0,65	0,62	0,62	0,63	0,64	0,61	0,63	0,65
10	1,82	1,82	1,82	1,80	1,83	1,86	1,82	1,82	1,80	1,79
100	2,05	2,04	2,06	2,05	2,04	2,07	2,05	2,05	2,04	2,04
250	2,37	2,43	2,40	2,30	2,25	2,40	2,40	2,32	2,41	2,43
500	5,45	6,21	6,20	6,20	3,16	6,19	3,11	3,14	3,14	11,71
750	7,83	9,20	8,61	8,60	8,00	7,81	7,69	7,82	4,10	8,60
1000	19,91	33,71	11,89	9,49	11,11	11,12	9,49	35,37	21,80	35,25
1500	27,54	14,23	16,53	16,75	34,12	14,21	16,52	49,80	45,27	40,45
2000	54,58	18,32	90,14	41,97	37,50	71,81	13,21	74,13	84,42	59,74

При анализе трафика следует рассматривать период аномальной нагрузки и количество сетевых пакетов за контрольный период. Эти параметры не всегда явно сигнализируют об атаке, и их значение может зависеть от не связанных с вредоносной деятельностью факторов.

К параметрам, которые однозначно (явно) маркируют присутствие вредоносной активности или ошибочная интерпретация которых наименее вероятна, можно отнести:

1) наборы флагов, которые не соответствуют стандарту соединения по TCP-протоколу (RFC-793);

2) наличие в TCP-пакете порта узла-источника, равного 0 (нельзя использовать нулевой порт);

3) несоответствие указанных контрольных сумм пакетов их оригинальным суммам.

Таким образом, среди маркеров сетевых атак можно выделить два типа: явные и косвенные. Очевидно, что не все косвенные маркеры можно игнорировать. Однако при намеренном учете в правилах всех косвенных признаков вероятность ошибки при определении атаки будет возрастать. Подобная ситуация складывается со множеством различных правил разнотипных сетевых атак. Требуется ввести в систему обнаружения механизм с функциями экспертной системы, который позволит определить успешность работы базы правил СОВ по итогам аудита инцидентов с указанием необходимости коррекции отдельных наборов правил (их параметров).

Для анализа корректности работы правил можно применить методы определения надежности информационных систем. Предполагается, что период, учитываемый в расчетах, охватывает заранее заданный период [3]. Тогда интенсивность отказов работы СОВ будет рассматриваться как интенсивность (среднее число) фиксаций пропущенных атак при последующем определении статистики инцидентов за контрольный период времени. Поскольку отказы функции распознавания СОВ касаются отдельных видов атак и, соответственно, правил, сопряженных с выявлением этих атак, то для каждого набора этих правил будет своя величина интенсивности отказов. Соответственно, интенсивность отказов СОВ равна сумме интенсивностей отказов каждого набора правил, сработавшего некорректно, что фиксируется в результатах аудита корпоративной системы. Сумма интенсивностей отказов рассчитывается следующим образом [6]:

$$A = \sum_{i=1}^{n} a_i , \qquad (1)$$

где A — интенсивность отказа СОВ всей базы правил; a_i — интенсивность отказа одного набора правил для одной атаки (определяется после аудита).

Вероятность исправной работы базы наборов правил $P(t)$ в течение заданного периода t с учетом интенсивности отказов по набору правил определяется следующим образом:

$$P(t) = e^{-At}. \qquad (2)$$

Учитывая специфичность множества различных правил СОВ, можно рассчитать для каждого набора правил вероятность исправной работы ($p_i(t)$) и вычислить вероятность исправной работы базы правил в целом для системы. Исходя из практического использования СОВ, можно сказать, что достаточно одного пропуска атаки, чтобы признать, во-первых, базу правил скомпрометированной, а во-вторых, подтвердить необходимость модификации правил скомпрометированного блока. При этом заданный критерий не означает, что рассчитывать вероятность исправной работы всех наборов правил не нужно, поскольку в действительности применение любого набора правил не исключает вероятность возникновения ошибки.

Помня о множестве ошибочных информационных пакетов, присутствующих в сети, следует отметить, что не все события, связанные с инцидентами безопасности, могут считаться признаками атаки и, соответственно, являться достаточной причиной для внесения изменений в базу правил СОВ, но при этом и игнорировать их нельзя.

Для решения задачи по определению целесообразности внесения изменений в описание маркеров правил (характеристики или условия в правиле) можно использовать один из методов формализации риска, суть которого состоит в определении порога допустимости поражения системы и использовании его для разделения рисков на избыточные и допустимые. Формула определения риска каждого блока правил в этом случае следующая [3]:

$$R_i = P_{ni} * I_j, \tag{3}$$

где i – номер пары; P_{ni} – вероятность реализации угрозы по отношению к «парному» активу; I_j – воздействие реализации этой угрозы на актив; R_i – величина риска.

В качестве «воздействия реализации угрозы на актив» можно использовать параметр, указывающий на компрометацию правил. Он принимает значение 0 или 1. Поскольку риски с параметром компрометации 0 нивелируются, целесообразно рассматривать риски правил СОВ со параметром компрометации 1, которые будут равны заданной в формуле вероятности неисправной работы. Порог допустимости определяется как величина вероятности появления ошибочного пакета при отсутствии реализации атакующих воздействий (R_a). Тогда риски считаются допустимыми, если для всех i-пар $R_i \le R_a$. Соответственно, избыточные риски, которые требуется нейтрализовать, будут превышать значение R_a [3].

Далее необходимо определить период между двумя ближайшими по времени зарегистрированными маркерами неопознанных атак, между которыми должен быть хотя бы один маркер опознанного нападения СОВ. Присутствие в данном случае зарегистрированного маркера атаки необходимо для того, чтобы подтвердить работоспособность базовых наборов правил, иначе расположенные подряд маркеры атак, не обработанные системой, будут указывать на тотальную неработоспособность базы правил СОВ.

Период между двумя ближайшими по времени неопознанными атаками указывает на время успешной работы СОВ при активной фильтрации трафика до первой фиксации маркера неопознанного в дальнейшем нападения. Данный параметр называется «наработка на отказ правил» (H). Он фактически указывает время актуальности сигнатурной базы правил и в целом работоспособности системы и рассчитывается по следующей формуле [6]:

$$H = \frac{1}{A}. \quad (4)$$

Параметр времени восстановления H_r будет оцениваться как время, которое потребуется для актуализации правил обнаружения атак (его следует рассматривать как показатель нивелирования канала несанкционированного доступа). При этом система должна получить новые модификации правил (правила с корректно обработанными параметрами). Параметр времени восстановления позволяет определить коэффициент готовности возобновления правильной фильтрации входящих пакетов (K_w) и выявить, насколько этот коэффициент готовности соответствует тому показателю, который бы означал возможность возобновления работы системы без каких-либо критических повреждений. Таким образом, коэффициент готовности СОВ возобновить корректную фильтрацию сетевых данных будет рассчитываться по формуле

$$K_w = \frac{H}{(H - H_r)}. \quad (5)$$

Соответственно, можно также вычислить коэффициент неготовности (K_{nw}) системы (неподготовленности базы правил) к возобновлению фильтрации сетевых данных:

$$K_{nw} = 1 - K_w. \quad (6)$$

Приведенный математический аппарат можно использовать для определения эффективности работы базы правил уже после обнаружения проблем в области безопасности сетевой инфраструктуры предприятия, то есть после аудита. Решение о внесении изменений в правила СОВ, очевидно, должен принимать специалист в области информационной безопасности. Использование математических методов в отдельном модуле для определения успешности работы набора правил СОВ позволяет увеличить эффективность механизмов обна ружения сетевых атак и снизить вероятность ошибочных подтверждений нападений.

Выводы

Таким образом, прежде чем вводить в эксплуатацию СОВ в корпоративной сети на граничном узле или на узле внутреннего сегмента, требуется решить ряд дополнительных задач, связанных с определени-

ем правильности работы базы правил механизмов защиты сетевой инфраструктуры. Первоначально необходимо собрать статистку отказов СОВ за контрольный период (*t*). Затем требуется выявить целесообразность встраивания в СОВ модуля, контролирующего эффективность работы правил системы обнаружения. При положительном решении нужно, используя функционал дополнительного модуля (механизма) оценки эффективности правил системы защиты, определить, насколько необходимо внесение изменений в базу правил СОВ. Механизм оценки эффективности правил СОВ предполагает выявление следующих параметров:

— сумма интенсивностей отказов каждого набора правил;

— вероятность исправной работы базы наборов правил;

— порог допустимости (величина вероятности появления сетевого пакета с ошибкой);

— время наработки на отказ базы правил;

— коэффициент готовности СОВ возобновить корректную фильтрацию сетевых данных.

Список литературы

1. *Аверичников В.И., Рытов М.Ю., Кувылкин А.В., Рудановский М.В.* Аудит информационной безопасности органов исполнительной власти : учеб. пособие. М., 2011.

2. *Астахов А.* Введение в аудит информационной безопасности. 2018 // GlobalTrust Solutions. URL: http://globaltrust.ru (дата обращения: 29.01.2018).

3. *Галатенко В.А.* Управление рисками: обзор употребительных подходов (ч. 2) // Jet Info. 2006. №12. URL: https://www.jetinfo.ru/upravlenie-riskami-obzor-upotrebitelnykh-podkhodov-chast-2/ (дата обращения: 12.11.2020).

4. *Горбачев И.Е., Глухов А.П.* Моделирование процессов нарушения информационной безопасности критической инфраструктуры // Тр. СПИИРАН. М., 2015. Вып. 1 (38). С. 112—135.

5. *Программа* для обнаружения методов скрытой сетевой разведки : свид. о гос. регистр. программы для ЭВМ №2017661931 / Н.А. Котов, В.В. Подтопельный ; заявитель и правообладатель Федеральное государственное автономное образовательное учреждение высшего образования «Балтийский федеральный университет им. Иммануила Канта» ; заявка №2017618776 ; заявл. 30.08.2017 ; опубл. 25.10.2017.

6. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. СПб., 2004.

Об авторах

Владислав Владимирович Подтопельный — ст. преп., Балтийская государственная академия рыбопромыслового флота ФГБОУ ВО «КГТУ», Россия.

E-mail: ionpvv@mail.ru

Игорь Анатольевич Ветров — канд. техн. наук, доц., Балтийский федеральный университет им. И. Канта, Россия.

E-mail: vetrov.gosha2009@yandex.ru

The authors

Vladislav V. Podtopelny, Assistant Professor, Baltic State Academy of Fishing Fleet, Russia.
E-mail: ionpvv@mail.ru

Dr Igor A. Vetrov, Associate Professor, Immanuel Kant Baltic Federal University, Russia.
E-mail: vetrov.gosha2009@yandex.ru