УДК 381.3

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СЕТИ С ПОМОЩЬЮ ГРАФОВ АТАК

© 2020 А. В. Савенков, Ю. П. Преображенский, О. Н. Чопоров

ОАО «Лебединский ГОК» (Губкин, Россия)
Воронежский институт высоких технологий (Воронеж, Россия)
Воронежский государственный технический университет (Воронеж, Россия)

В данной работе проводится анализ возможностей обеспечения защищенности информационной сети на основе графов атак.

Ключевые слова: защита информации, информационная система, граф.

Графы атак представляют собой важный инструмент проектировщиков и администраторов сети в ходе определения уровня защищенности сетевых структур.

На их базе есть возможности для визуализации путей, по которым нарушитель безопасности может получить доступ к объекту защиты информации.

Благодаря этому, проектировщики и администраторы сети могут обратить внимание на ошибки, допущенные при проектировании сети или уязвимости, возникающие во время эксплуатации информационной сети [1, 2], которые могут нарушителям безопасности предоставить максимальный доступ.

При увеличении информационной сети так же возможно использовании этих графов атак, так как количество ошибок и уязвимостей увеличивается почти линейно.

Используя моделирование, классифицируем уязвимости, строим графы, в результате этого формируем рекомендации по повышению безопасности информационной сети [3].

Чтобы защитить информационную сеть проектировщик или администратор сети должен постараться найти все связи в сети, которые нарушитель может использовать для атак.

Проектировщик или администратор сети имеют преимущество перед нарушителем, так как знают пути прохождения трафика в сети, какие службы запущены и какие есть уязвимости в этих службах.

Савенков Андрей Васильевич – ОАО «Лебединский ГОК», специалист, savvenkovaavv30@yandex.ru.
Преображенский Юрий Петрович – Воронежский институт высоких технологий, профессор, it_pro@vivt.ru.
Чопоров Олег Николаевич – Воронежский государственный технический университет, профессор, choporov_oleg@mail.ru.

Он так же может получить дополнительную информацию о состоянии сети.

Одним из способов получения дополнительной информации о защищенности сети являются графы атак. Существует несколько статей о применении графов атак при анализе защищенности информационной сети [4].

Графы атак показывают, как нарушитель может атаковать информационную сеть, находясь в разных точках самой сети и вне её.

Это помогает выявить критические уязвимости информационной сети и устранить их.

Для построения графов атак используется большое количество предварительных данных.

Но главной проблемой моделирования атак являются трудности, моделирования для режимов реального времени. В данной статье рассмотрим обработку предварительных данных при построении графов атак [5, 6].

Модель защищаемой сети должна содержать:

1. Список описаний хостов.

2. Список связей между хостами. Два основных вида связей -

виртуальные и физические.

3. Зависимости сервисов.

Модель хостов определяется:

1. Программно-аппаратной платформой хоста [7, 8].

2. Списком пользователей с описанием их прав. Если нарушитель внутренний, то его права тоже необходимо включить.

3. Особенностями информации на хостах.

4. Характеристиками политик безопасности.

Модель зависимостей сервисов определяется:

1. Программным обеспечением на некотором хосте [9, 10].

2. Видом зависимости. Она может быть связана с функционированием, доверием и др.

3. Возможными атаками, которые могут быть осуществлены на базе таких отношений.

Когда начинается формирование деревьев атак по каждому из хостов, тогда выбираются соответствующие предварительные данные.

Для каждой из рассмотренных атак определяют уязвимости.

Список уязвимостей может быть создан при помощи открытых баз уязвимостей, например, CVE, NVD, OSVDB и др.

Помимо этого, в качестве источников баз уязвимостей могут рассматриваться сканеры уязвимостей, например, Rapid7 Nexpose, Tenable Nessus Scanner, Nmap и др.

Графы атак строятся на основе применения шаблонов атак в формате CAPEC. Он включает наиболее частым образом наблюдаемые последовательности действий нарушителей.

Есть несколько этапов атак. Первый этап касается сбора информации по доступным хостам.

В этапе нет информации относительно эксплуатации уязвимостей. Для сбора информации используют шаблон CAPEC-292 (Host Discovery).

В нем есть группа разных подходов осуществления сканирования по хостам и портам. В такой группе, например, есть: CAPEC-285 (ICMP Echo Request Ping), CAPEC-296 (ICMP Information Request), CAPEC-299 (TCP SYN Ping) и др.

После составления таблицы по потенциальным атакам для каждого из хостов, делается выбор точек.

Для них нарушитель имеет возможности для получения доступа к сети.

Есть вариант внешнего нарушителя, который не будет иметь возможностей прямым способом вести подключения к локальной сети.

Есть исключения по хостам, для которых существует доступ из сети Интернет.

По каждому из типов нарушителей ведется список возможных целей.

Значит, что модель нарушителя представляется в виде множества пар (тип нарушителя – цель). На базе созданных моделей нарушителей идет формирование графов атак.

Нарушители ограничены в выборах потенциально вероятных атакующих действий из общего множества и этим задается модель нарушителя. Причины ограничений определяются:

1. Знаниями нарушителей, которые они может применять вследствие ограничений сложности уязвимостей [11].

2. Начальное положение нарушителей внутри защищаемой сети. Нарушители могут быть внешними и внутренними.

3. Начальные права нарушителей. Определенные атаки могут быть проведены лишь при том, что существуют определенные прав у нарушителей [12].

Модель знаний нарушителя определяется различными параметрами. Есть связь модели начальных прав нарушителей с такими компонентами:

1. Числом хостов.

2. Элементами компьютерных сетей - хостами.

3. Уровнем прав нарушителей.

Нарушители, которые обладают целью, определяется:

1. Моделями самих нарушителей.

2. Целью нарушителей в ходе осуществления атак.

Момент, в который нарушители будут завершать свои атакующие рассматривается с точки зрения целей нарушителей [13].

Когда выбираются потенциальные пути движения по дереву атак для соответствующих нарушителей, то параметр цели нарушителей дает возможности для определения вероятностных характеристик. Модель цели нарушителей базируется на:

1) хостах – элементах моделей компьютерных сетей;

2) результате атакующих действий.

Результаты атакующих действий рассматриваются в виде отражений по общим целям нарушителей.

Они могут быть промежуточными или конечными.

В качестве примера можно указать получение каких-то прав доступа, кражу или порчу информации, вариант, когда система будет идти к нерабочему состоянию.

Происходит обозначение атрибутов узлов при помощи разных цветов. Их размеры будут пропорциональны количеству скомпрометированных узлов, которые будут вкладываться в прямоугольники.

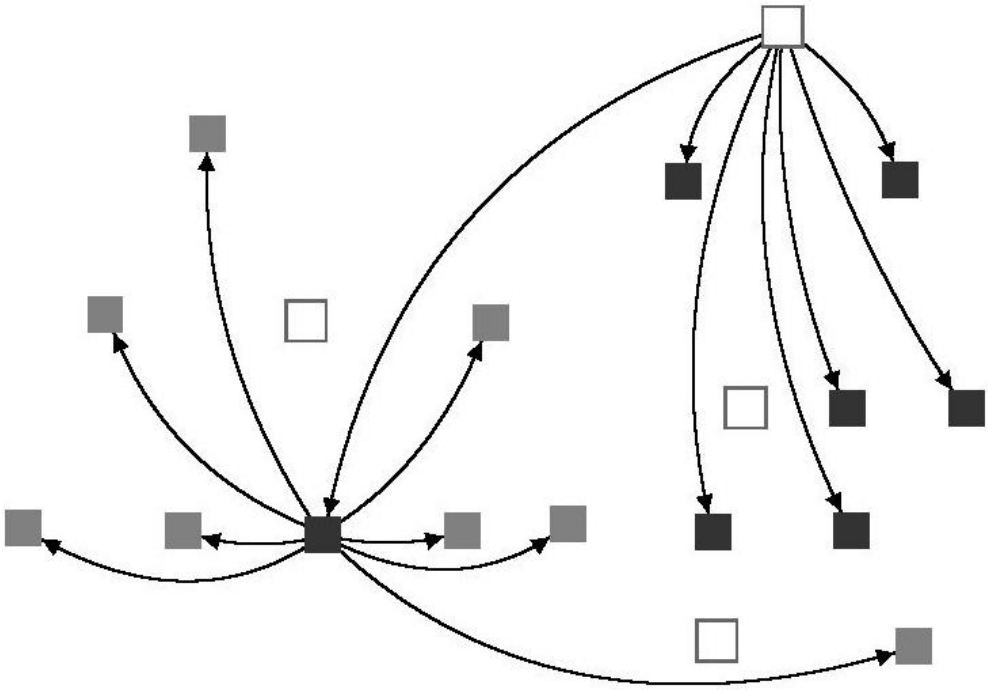

Рисунок 1. Представление графа атак в виде карты деревьев.

Важным направлением исследований должно быть упрощение задачи обновления и анализа элементов, чтобы затраты времени и ресурсов были минимальными.

Добавление потенциальных атак в графы атак производится в том случае, когда будут соблюдены три условия:

1. Защищаемая сеть должна характеризоваться уязвимостями.

Определяется свойствами защищаемой сети.

2. Нарушители должны обладать требуемыми знаниями и ресурсами, чтобы поддерживать атаки. Это определяется свойствами защищаемой сети и моделью нарушителя.

3. Выполнение атаки ведет нарушителей к выполнению их целей.

В случае, когда хост является промежуточной целью, то один вид атаки может привести к реализации другого вида атаки. А в случае, когда хост является конечной целью, то через соединения с другими хостами произойдет утечка информации.

Таким образом, нами проведен анализ возможностей применения графов атак для оценки степени защищенности компьютерных сетей.

ЛИТЕРАТУРА

1. Львович Я. Е. Адаптивное управление Марковскими процессами в конфликтной ситуации / Я. Е. Львович, Ю. П. Преображенский, Р. Ю. Паневин // Вестник Воронежского государственного технического университета. – 2008. – Т. 4. – № 11. – С. 170-171.

2. Казаков Е. Н. Разработка и программная реализации алгоритма оценки уровня сигнала в сети wi-fi / Е. Н. Казаков // Моделирование, оптимизация и информационные технологии. – 2016. – № 1 (12). – С. 13.

3. Кострова В. Н. Оптимизация распределения ресурсов в рамках комплекса общеобразовательных учреждений / В. Н. Кострова, Я. Е. Львович, О. Н. Мосолов // Вестник Воронежского государственного технического университета. – 2007. – Т. 3. – № 8. – С. 174-176.

4. Львович И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

5. Мэн Ц. Анализ методов классификации информации в интернете при решении задач информационного поиска / Ц. Мэн // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (13). – С. 19.

6. Львович Я. Е. Исследование характеристик защищенности мобильных сенсор-

ных сетей / Я. Е. Львович, И. Я. Львович, А. П. Преображенский, Ю. П. Преображенский, О. Н. Чопоров // Радиолокация, навигация, связь. Сборник трудов XXV Международной научно-технической конференции, посвященной 160-летию со дня рождения А. С. Попова. В 6-ти томах. – 2019. – С. 239-244.

7. Потудинский А. В. Модели для определения моментов контроля в многоуровневых организационных системах / А. В. Потудинский, А. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2020. – Т. 8. – № 2 (29). – С. 28-29.

8. Преображенский А. П. Построение модуля расчета для исследования систем мобильной связи / А. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2015. – № 1 (8). – С. 6.

9. Преображенский А. П. О проектировании беспроводных сетей связи на основе методов искусственного интеллекта / А. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2014. – № 4 (7). – С. 13.

10. Преображенский А. П. О процессах оптимизации в мобильных системах связи / А. П. Преображенский, Е. И. Коденцев // Моделирование, оптимизация и информационные технологии. – 2013. – № 3 (3). – С. 6.

11. Преображенский Ю. П. Проблемы доступа к данным в информационных системах компаний / Ю. П. Преображенский // В сборнике: Юность и знания – гарантия успеха - 2020. сборник научных трудов 7-й Международной молодежной научной конференции: в 3 т.– Курск. – 2020. – С. 341-344.

12. Преображенский Ю. П. О системном подходе при внедрении информационных систем в организациях / Ю. П. Преображенский // В сборнике: Молодежь и XXI век - 2020. Материалы X Международной молодежной научной конференции. – 2020. – С. 127-129.

13. Преображенский Ю. П. Теоретические основы увеличения помехозащищённости широкополосных телекоммуникационных оптических систем / Ю. П. Преображенский // Техника и технологии: пути инновационного развития. Сборник научных трудов 9-й Международной научно-практической конференции. В 2-х томах. Отв. редактор А. А. Горохов. – 2020. – С. 100-103.

THE ANALYSIS OF THE SECURITY OF THE INFORMATION NETWORK WITH ATTACK GRAPH

© 2020 A. V. Savenkovn, Yu. P. Preobrazhenskiy, O. N. Choporov

JSC «Lebedinsky GOK» (Gubkin, Russia)
Voronezh Institute of High Technologies (Voronezh, Russia)
Voronezh State Technical University (Voronezh, Russia)

This paper analyzes the possibilities of ensuring the security of an information network based on attack graphs.

Keywords: information protection, information system, graph.