12Ф96А6Й	00100101
3Н435РФ83	010001100
8Ф789Ь9Я1	010000010
93Э64НЙ5ЖФ5	00100110110
АО26КЗФ	1000111
Ф83К92АЦЫ1	1001001110
0ГЕ383	011000
8ЕО96Ф6П31Ш9	011001010010
Ш04РЪЗДЗ	10011010
8ГЮФ536	0111000

Для каждой последовательности составляется разность по Хеммингу (табл. 1), на основе которой злоумышленник может выявить наиболее удаленные друг от друга последовательности, возможно претендующие на то, чтобы быть ключом. Цветом в таблице помечены значения, соответствующие максимальной разнице между последовательностями.

Табл. 1. – расстояния по Хеммингу между последовательностями

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1		4	3	2	4	5	2	1	7	3
2			3	3	3	6	2	3	5	4
3				6	5	5	1	2	6	2
4					3	6	1	6	5	4
5						3	5	5	2	7
6							4	7	2	4
7								1	5	1
8									8	2
9										5

В случаях с последовательностями 1 и 9, 5 и 10, 8 и 9 расстояние максимально. Таким образом, получается 5 комбинаций, претендующих на роль потенциального ключа (в том числе комбинация АО26КЗФ, которая соответствует шаблону пользователя). Но это лишь предположение, сделанное на основе первичного приближения. Возможность однозначно указывать конкретные буквы и цифры во много раз затрудняет дальнейший анализ, так как количество комбинаций, претендующих на роль потенциального ключа, приблизится к общему количеству высылаемых комбинаций.

Заключение

Данная схема позволяет идентифицировать непосредственного владельца аккаунта (естественно, лишь в случае сохранения в тайне выбранного шаблона для восстановления), а также не позволяет злоумышленнику, завладевшему чужой электронной почтой, получить доступ к ассоциированному аккаунту целевого ресурса. В случае полной блокировки злоумышленником электронной почты, возможно применение дополнительных организационных мер для восстановления доступа к ресурсу правомочного пользователя.

Литература

1. Учётная запись [Электронный ресурс]. – 2015. – Режим доступа: https://ru.wikipedia.org/wiki/Учётная_запись

2. Принцип Кирхгофа [Электронный ресурс]. – 2013. – Режим доступа: http://www.finam.ru/dictionary/wordf02470/?n=32

3. Брюс Шнайер, Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Текст] / М.: Издательство Триумф, 2002. 816 с.

4. Гмурман В.Е., Теория вероятностей и математическая статистика. Учеб. пособие для вузов. Изд.7-е,стер. / М.: Высш. шк.,1999. - 479 с.

Ю.В. Алейнов

О СПОСОБАХ РАЗМЕЩЕНИЯ ЛОЖНЫХ ЦЕЛЕЙ В СЕТИ ДЛЯ ОБНАРУЖЕНИЯ НАПРАВЛЕННЫХ АТАК

(Самарский государственный технический университет)

В настоящее время можно отметить возрастающую актуальность такого класса угроз, как направленные сетевые атаки (*APT*) [1]. Направленные атаки характеризуются особым типом поведения нарушителя, который старается как можно более незаметно, используя специально подобранные или самостоятельно разработанные инструменты и применяя их как можно точнее, внедриться в сеть конкретного объекта информатизации [2,3].

По мнению ряда исследователей, перспективным методом обнаружения такого типа атак является метод, основанный на внедрении ложных целей (*Honeypot*) в защищаемую сеть [4]. Ложные цели реализуются в виде специальных объектов, не участвующих ни в каких производственных процессах, протекающих в сети и не взаимодействующих в штатном режиме ни с какими другими системами. Среди достоинств данного метода можно отметить:

- возможность обнаружения атак неизвестного типа;
- низкую вероятность ложных срабатываний.

В то же время, использование данного метода осложнено относительно высокой сложностью реализации системы ложных целей (ЛЦ). Особенно следует отметить задачу размещения ловушек в сети. Очевидно, что от того, как размещены ЛЦ, зависит вероятность обнаружения нарушителя.

В рамках исследований на тему создания автоматизированных систем управления ложными целями ряд авторов затрагивал проблему размещения ловушек в сети, в связи с чем, на данный момент имеется несколько подходов к ее решению [4]. Однако анализ работ по этой тематике показывает, что сущест-

вующие подходы не рассматривались в контексте использования ЛЦ для обнаружения атак направленного типа [5].

В связи с этим актуальной является задача выработки критериев применимости той или иной методики размещения ЛЦ для обнаружения атак направленного типа и проведения анализа существующих методик по этим критериям для выбора одной из них или обоснования необходимости разработки новой.

Помимо очевидных критериев, таких как простота реализации методики на практике и наличие количественного показателя эффективности размещения ложных целей, важно определить специальные критерии, на основании которых можно судить о применимости методики в условиях направленной атаки. Эти специальные критерии должны основываться на показателях, вытекающих из характерных свойств атак направленного типа. К таким свойствам относят [1,2]:

- наличие четко определенного объекта атаки;
- привлечение в случае необходимости значительных ресурсов для атаки;
- высокая квалификация атакующих и их осведомленность об атакуемом объекте;

Перечисленные особенности определяют многоступенчатость процесса направленной атаки. Нарушитель, осуществляющий направленную атаку, заинтересован в компрометации определенного подмножества узлов в сети. Эти узлы могут быть недоступны потенциальному нарушителю в начале атаки вследствие реализованной в сети политики разграничения доступа. Таким образом, для доступа к интересующим ресурсам злоумышленник может быть вынужден совершить ряд промежуточных атак на другие ресурсы сети, чтобы, используя их ресурсы, совершить атаку на интересующую цель.

Таким образом, методика размещения ложных целей в сети для обнаружения направленных атак должна учитывать тот факт, что в сети может быть реализована политика разграничения доступа. Другими словами, под размещением ложных систем подразумевается прежде всего распределение их по разным зонам межсетевого экрана.

С учетом этого, предлагается использовать следующий набор критериев для анализа применимости методик размещения ложных целей в сети для обнаружения направленных атак:

- простота реализации метода или алгоритма на практике;
- наличие количественного показателя эффективности размещения ложных целей;
- способность методики определять размещение ложных целей относительно границ зон межсетевого экрана с учетом правил разграничения доступа в сети.

Литература

1. Piggin R. Cyber security trends: What should keep CEOs awake at night //International Journal of Critical Infrastructure Protection. – 2016.

2. Sood, A.K., Enbody, R.J. Targeted Cyberattacks: A Superset of Advanced Persistent Threats // Security & Privacy, IEEE (Volume:11 , Issue: 1) . IEEE, 2013.

3. Медведовский И., Семьянов П., Леонов Д. Атака на Internet. – Litres, 2013.

4. Bringer M.L., Chelmecki, C.A., Fujinoki H A Survey: Recent Advances and Future Trends in Honeypot Research. // International Journal of Computer Network & Information Security. 2012. №4.

5. Алейнов Ю.В., Бондаренко В.В. Применение динамических систем пассивной регистрации сетевых атак для обеспечения безопасности компьютерных сетей // Сборник “Вычислительная техника и новые информационные технологии”. Уфа: УГАТУ, 2011. с. 126-131.

А.А. Бомм

РЕШЕНИЕ ЗАДАЧ БЕЗОПАСНОСТИ В ИГРОВОЙ ОБУЧАЮЩЕЙ СИСТЕМЕ «3DUCATION»

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Развитие современных информационных технологий задает тенденцию разработки не только многофункциональных, но и безопасных приложений, которые способны выдержать конкуренцию на рынке информационных систем. Наряду с тривиальными задачами разработки вэб-приложений, остро стоят вопросы защиты от несанкционированного доступа и утечек данных. Защита информации (62%) и выполнение условий лицензионного соглашения (51%) являются основными причинами для защиты веб-приложений [1]. Одним из самых распространённых для получения несанкционированного доступа способов является использование уязвимостей систем аутентификации пользователей, в результате которых злоумышленники могут не только получить полный или частичный доступ к данным пользователя, но и вызвать сбои работы как отдельных узлов, так и системы в целом. Для решения задач безопасности необходимо полное понимание слабых мест в системе безопасности. Рассмотрению данных задач и посвящена данная работа.

Игровая обучающая система «3Ducation», разработанная на кафедре программных систем СГАУ, входит с информационное пространство школы информатики СГАУ наряду с сайтом Школы Информатики, сайтом дистанционного обучения и автоматизированной информационной системой (АИС) «Школа информатики СГАУ». Для удобства и комфорта конечного пользователя (доступ к различным системам должен осуществляться только через одну учетную запись) была разработана подсистема удаленной авторизации с использованием технологии единого входа (технология OpenID), которая позволяют клиенту перемещаться между различными разделами портала без повторной аутентификации [2].