СОЦИАЛЬНЫЕ СЕТИ, КАК ИСТОЧНИК ИНФОРМАЦИИ ДЛЯ СОЦИОТЕХНИЧЕСКИХ МЕТОДИК ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ И ПОИСКА УЯЗВИМОСТЕЙ В СИСТЕМЕ

Кармаз Е. В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Яшин К. Д. – кандидат технич. наук, доцент

Цель работы: разработка методики поиска уязвимости для оценки уровня защищенности информационной системы.

Тестирование на проникновение – частный случай аудита информационной безопасности. Процесс тестирования на проникновение является моделированием реальных действий злоумышленника – поиск уязвимостей системы защиты и их последующая эксплуатация. Эта услуга позволяет получить независимую оценку и экспертное заключение о состоянии защищенности информации ограниченного распространения.

Разведкой в тестировании на проникновение является сбор информации из открытых источников, необходимой для составления сценария атаки на целевую организацию.

В понятии тестирования на проникновение используется термин «футпринтинг» (англ. footprinting) – это определенная техника получения информации об информационных системах и лицах, которым эти системы принадлежат. В некоторых методологиях социальные сети выделяют в отдельный этап футпринтинга. С помощью социальных сетей можно получать информацию, как с помощью социальной инженерии, так и с помощью обычных методов.

Какая информация может быть получена? Ответ весьма интересен – возможности ограничены только знаниями пользователей данной сети. Т.е. (теоретически) в соц. сети можно узнать всё, что знают все ее пользователи вместе взятые. Поистине безграничные возможности для конкурентной разведки. Конечно же нужно помнить о искажении информации и о дезинформации. Поэтому получаемые в социальных сетях данные нужно перепроверять, а также изучать автора этих данных на предмет его возможностей и заинтересованности [1]. Ниже приведена схема, какую информацию может извлечь злоумышленник из информации, находящейся в социальных сетях (см. рис. 1).

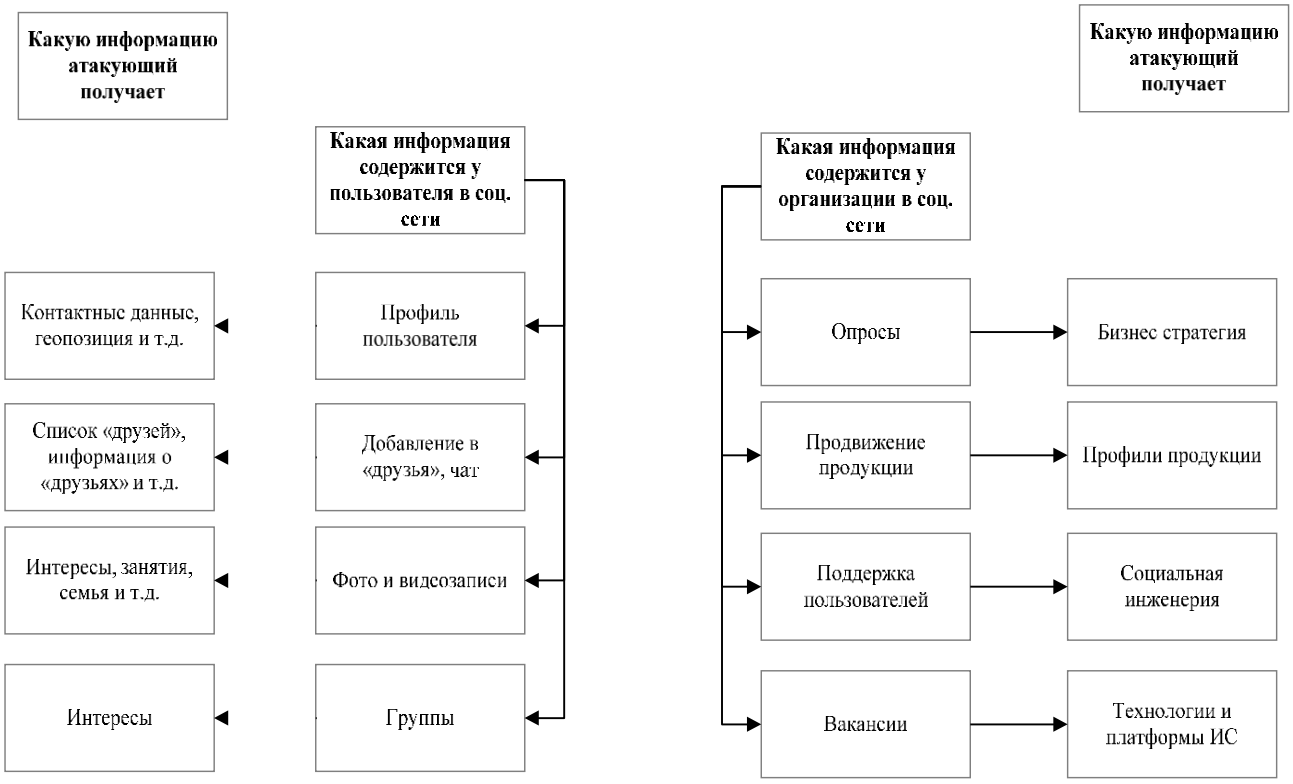

Рисунок 4.1 – Схема получения информации из социальных сетей

Основной вопрос состоит в том, каким образом эту информацию добыть. Путей не так много, но они достаточно эффективны. Это пассивный способ (прямой поиск) и активный (общение).

Говоря о прямом поиске, имеется ввиду поиск, по ключевым словам с использованием поисковых сервисов самой сети или внешних поисковиков.

Какие данные о человеке можно получить в социальной сети? Самые разнообразные: всё, что может о себе сообщить сам исследуемый человек, или информация людей его знающих. Это могут быть:

1) Установочные данные человека: ФИО, дата, место рождения, фото (люди сами часто их оставляют). При этом, полагают, что защищают свои данные, оставляя на одном форуме дату рождения, на другом форуме имя, на третьем форуме ICQ, и при этом везде регистрируются под одним ником.

2) Компетенции — образование, опыт работы, достижения. Порой, это происходит таким образом и с такими подробностями и детализацией, что и трудовая книжка не нужна. И вновь срабатывает тот же эффект – в одном месте один комплект, в другом чуть измененный, в третьем еще с каким-то изменением. Автор уже и забыл, где и что оставлял, а материал остался. Нужно его только собрать, сравнить и выявить те самые нестыковки. Именно в нестыковках будет самое интересное [2].

3) Связи — родственные, дружеские, рабочие.

4) Особенности личности — предпочтения, хобби, взгляды, убеждения.

Материала для исследования предостаточно. А если добавить сюда еще и высказывания на форумах, в блогах и микроблогах по интересующим вас проблемам, то фактически можно составить полное представление об исследуемом объекте.

О компаниях (организациях) тоже можно найти в социальных сетях много информации:

1) Контактные и установочные данные самой компании. Их оставляют и официальные представители компании, и ее сотрудники, и ее клиенты-конкуренты-поставщики. А при таком огромном и неконтролируемом круге знающих в открытый доступ попадают не только официальные данные.

2) Кто сотрудники, кто ТОПы, кто исполнители, как с кем связаться. Эти данные оставляют и их обладатели, и сторонние люди, к которым относятся, в том числе, и обиженные сотрудники, и недовольные клиенты.

3) Внутренняя обстановка офиса, взаимоотношения внутри коллектива. Размеры офиса, его наполнение имуществом и сотрудниками, активность этих сотрудников и активность телефонных переговоров, присутствие клиентов и работа с ними, корпоративный стиль – всё это является косвенным указанием на размеры и доходность компании. И всё это можно узнать посредством социальных сетей.

4) Места проведения корпоративных мероприятий и стиль проведения таких мероприятий тоже дают материал для умозаключений относительно компании. И эти данные также могут быть получены в соцсетях.

Ресурсы организации (финансовые, имущественные, административные) так или иначе могут стать понятны, если использовать возможности социальных сетей [3].

С помощью объединения методов социальной инженерии и социальных сетей мы можем узнать IP-адрес “жертвы”. Для этого, выходим с лицом на контакт в социальной сети с помощью специальных сервисов, передаем “жертве” сформированную ссылку, отправляем его на переадресацию на другой сайт, а сами получаем IP-адрес “жертвы”. Этот способ возможен, если интересуемый объект плохо разбирается в информационных технологиях.

При тестировании на базе социотехнических методов используются методы социальной инженерии, используя «человеческий фактор». Осуществляются санкционированные попытки получения несанкционированного доступа к корпоративной сети и защищаемым активам целевой организации. Методы, как правило, направлены на пользователей конечных систем и позволяют определить реакцию персонала в различных штатных и нештатных ситуациях, уровень осведомленности и знаний персонала о требованиях безопасности.

Из этого следует, что необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности. Проведение инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила информационной безопасности.

Данная разработка методики поиска уязвимости эффективна и служит рекомендательной основой для оценки уровня защищенности любой информационной системы.

Список использованных источников:

1. Ходашинский, и. Методы нечеткого извлечения знаний в задачах обнаружения вторжений / И.А. Ходашинский, И.В. Горбунов, Р.В. Мещеряков // Вопросы защиты информации. – М.: ФГУП ВИНИ, 2012. – № 1. –С. 45–50.

2. Футпринтинг – в поисках ваших целей [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/422897.php/.

3. Соцсети как инструмент конкурентной разведки [Электронный ресурс]. – Режим доступа: http://www.marketing.spb.ru/lib-comm/internet/twit_ci.htm/.