# 

**Лабораторная работа. Социальная инженерия**

**Задача**

В этой лабораторной работе вы изучите примеры социальной инженерии, определите пути ее определения

и противодействия ей.

**Ресурсы**

 Компьютер с доступом в Интернет

**Шаг 1: Примеры социальной инженерии**

Термин «социальная инженерия» в сфере информационной безопасности используется для описания техник,

применяемых человеком (или группой людей) для манипулирования другими людьми с целью получения доступа или компрометации информации об организации или ее информационных системах. Злоумышленника, который использует эту технологию, обычно трудно определить, он может называть себя новым сотрудником, сотрудником обслуживающего персонала или исследователем. Социальный инженер может даже предоставлять документы, подтверждающие его личность. Втираясь в доверие и задавая вопросы, он или она могут собрать достаточно

информации для внедрения в информационную сеть организации.

С помощью любого браузера найдите информацию о случаях применения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.

**1. Претекстинг** – действие по заранее созданному плану. Злоумышленник продумывает всё до мелочей. Что он будет говорить, продумывает своё новое "я", а так же реакцию жертвы.

**2**. **Кви про кво** – метод, использующий неквалифицированность и неопытность жертвы. Например, человек звонит в офис «из отдела техподдержки», и тоже сообщает, что в компьютере либо уязвимость, либо просто интересуется о наличии ошибок. А далее просто командует, что нужно делать, причём присутствие самого "синжера" необязательно, сам сотрудник сам себе навредит.

**3. Дорожное яблоко** – техника, которая эксплуатирует любопытство жертвы, и является слегка переделанным трояном. Единственное отличие – человек не получает «посылку», а сам её находит. Например, объект «случайно» находит в лифте диск с названием “Информация о сотрудника 2011, только для служебного пользования”. Прежде чем этот честный гражданин отнесёт диск начальству (а может и не отнесёт), он обязательно глянет на содержимое, и тоже подцепит вирус. А тем более, если и отнесёт этот диск, есть вероятность заразить и начальство, и всю компанию. Такой метод не очень распространён, но и такие случаи бывают.

**Шаг 2: Определение признаков социальной инженерии**

Социальные инженеры – не что иное, как воры или шпионы. Вместо того чтобы получить доступ к вашей сети

через Интернет, они пытаются получить его, используя желание человека быть любезным. И хотя пример ниже не относится к сетевой безопасности, он показывает, каким образом ничего не подозревающий человек может невольно разгласить конфиденциальную информацию.

*«Это кафе было достаточно тихим, и я, одетый в костюм, сел за свободный столик. Я поставил портфель на стол и ждал подходящую жертву. Вскоре подобная жертва появилась – вместе с подругой они расположились за соседним столиком. Она положила сумочку на соседний стул, пододвинула его поближе и все время держала руку на сумочке.*

*Через несколько минут ее подруга вышла в уборную. Жертва [цель] осталась одна, и я подал Алексу и Джесс сигнал. Играя роль парочки, Алекс и Джесс спросили у жертвы, сможет ли она их сфотографировать вместе. Она с радостью согласилась. Она убрала руку с сумочки, взяла камеру и сфотографировала «счастливую парочку». В это время я, пользуясь ее невнимательностью, нагнулся, взял ее сумочку, положил в портфель и закрыл его.Жертва даже не замечала пропажи в то время, как Алекс и Джесс уходили из кафе. После этого Алекс пошел на парковку неподалеку.*

*Прошло немного времени, прежде чем она поняла, что ее сумочка пропала. Она начала паниковать, повсюду суетливо искать сумочку. Это было именно то, на что я надеялся. Я спросил, не нужна ли ей моя помощь.*

*Она спросила, не видел ли я что-то. Я сказал, что не видел, но убедил присесть и подумать о том, что было в той сумочке. Телефон. Косметика. Немного наличных. Кредитные карты. Бинго!*

*Я спросил, в каком банке она обслуживалась, а затем объявил, что работаю на этот банк. Какая удача! Я убедил ее в том, что все будет хорошо, но ей нужно прямо сейчас заблокировать свою кредитную карту. Я позвонил по номеру «техподдержки», по которому на самом деле ответил Алекс, и передал ей свой телефон.*

*Алекс находился в фургоне на парковке. Магнитола на приборной панели воспроизводила шум офиса. Он уверил жертву, что ее карту можно с легкостью заблокировать, но для того, чтобы подтвердить ее личность, требуется ввести PIN-код на клавиатуре телефона, с которого она звонит. На клавиатуре моего телефона.*

*Когда мы получили ее ПИН-код, я ушел. Если бы мы были реальными ворами, мы бы могли получить доступ к ее счету при помощи банкомата или покупок с подтверждением PIN-кодом. К счастью для нее, это было всего лишь ТВ-шоу».*

«Взлом или социальная инженерия – автор Christopher Hadnagy http://www.hackersgarage.com/

hacking-vs-social-engineering.html

*На заметку: «Те, кто возводят стены, думают иначе, чем те, кто пытаются преодолеть эту стену снизу, сверху, вокруг или сквозь нее». Paul Wilson – The Real Hustle*

Найдите способы определения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.

**Претекстинг,** **Кви про кво** (услуга за услугу)**,** **Обратная социальная инженерия.**

**Обратная социальная инженерия** - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью».

**Претекстинг** - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие.

**Кви про кво** (услуга за услугу) - данная техника предполагает обращение злоумышленника к пользователю. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

**Шаг 3: Анализ способов предотвращения применения социальной инженерии**

Приняты ли в вашей компании или школе процедуры, призванные предотвращать применение социальной инженерии?

Да.

Если да, в чем заключаются эти процедуры?

Основным способом защиты от методов социальной инженерии является обучение сотрудников. Все работники компании должны быть предупреждены об опасности раскрытия персональной информации и конфиденциальной информации компании, а также о способах предотвращения утечки данных.

Найдите в Интернете процедуры, принятые в организациях для того, чтобы предотвратить получение доступа

к конфиденциальной информации при помощи социальной инженерии. Перечислите найденное.

* **Пользовательские учетные данные являются собственностью компании.**

Всем сотрудникам в день приема на работу должно быть разъяснено то, что те логины и пароли, которые им выдали, нельзя использовать в других целях (на web-сайтах, для личной почты и т.п), передавать третьим лицам или другим сотрудникам компании, которые не имеют на это право. Например, очень часто, уходя в отпуск, сотрудник может передать свои авторизационные данные своему коллеге для того, чтобы тот смог выполнить некоторую работу или посмотреть определенные данные в момент его отсутствия.

* **Необходимо проводить вступительные и регулярные обучения сотрудников компании, направленные на повышения знаний по информационной безопасности**.

Проведение таких инструктажей позволит сотрудникам компании иметь актуальные данные о существующих методах социальной инженерии, а также не забывать основные правила по информационной безопасности.

* **Обязательным является наличие регламентов по безопасности, а также инструкций, к которым пользователь должен всегда иметь доступ. В инструкциях должны быть описаны действия сотрудников при возникновении той или иной ситуации.**

Например, в регламенте можно прописать, что необходимо делать и куда обращаться при попытке третьего лица запросить конфиденциальную информацию или учетные данные сотрудников. Такие действия позволят вычислить злоумышленника и не допустить утечку информации.

* **На компьютерах сотрудников всегда должно быть актуальное антивирусное программное обеспечение.**

На компьютерах сотрудников также необходимо установить брандмауэр.

* **В корпоративной сети компании необходимо использовать системы обнаружения и предотвращения атак.**

Также необходимо использовать системы предотвращения утечек конфиденциальной информации. Все это позволит снизить риск возникновения фитиновых атак.

* **Все сотрудники должны быть проинструктированы, как вести себя с посетителями.**

Необходимы четкие правила для установления личности посетителя и его сопровождения. Посетителей всегда должен сопровождать кто-то из сотрудников компании. Если сотрудник встречает неизвестного ему посетителя, он должен в корректной форме поинтересоваться, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетители в службу безопасности.

* **Необходимо максимально ограничить права пользователя в системе.**

Например, можно ограничить доступ к web-сайтам и запретить использование съемных носителей. Ведь, если сотрудник не сможет попасть на фишинговый сайт или использовать на компьютере флеш-накопитель с «троянской программой», то и потерять личные данные он также не сможет.

Исходя из всего перечисленного, можно сделать вывод: основной способ защиты от социальной инженерии – это обучение сотрудников. Необходимо знать и помнить, что незнание не освобождает от ответственности. Каждый пользователь системы должен знать об опасности раскрытия конфиденциальной информации и знать способы, которые помогут предотвратить утечку. Предупрежден – значит вооружен!