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.

- **Сайт не работает.** Базу сайтов с почтовыми адресами владельцев легко превратить в переходы на любой другой сайт. Отправляем письма с текстом «Почему-то страница вашего сайта www.site.ru/random.html не работает!» Ну и классический прием: в тексте ссылки жертва видит свой сайт, а сама ссылка ведет на другой URL.

- **Фейковая подписка на рассылку.** О фишинге путем заманивания на фейк-страницу вы уже наверное знаете. Вот совсем легкий способ заставить пользователя перейти на сайт по ссылке в письме

- **Претекстинг** – это действие, отработанное по заранее составленному сценарию (претексту). В результате цель (жертва) должна выдать определённую информацию, или совершить определённое действие. Этот вид атак применяется обычно по телефону.

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. Только заголовок лабораторной работы. Без нумерации © 2017 Компания Cisco и/или ее дочерние компании. Все права защищены. Этот документ является общедоступной информацией Cisco.

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.

Социальная инженерия – способ получения доступа к конфидециальной информации, паролям, банковским и другим защищенным данным и системам. Киберпреступники используют социальную инженерию для проведения таргетированных атак (атаки на инфраструктуру компаний или государственных структур). Они заранее тщательно изучают средства защиты этой организации.

Примеры социальной инженерии

Наверняка вы слышали про спам с «актами выполненных работ» или договорами, в которые вшиты трояны. Такой рассылкой бухгалтеров уже не удивишь. Или всплывающие окна с «рекомендациями» скачать плагин для просмотра видео — это уже скучно. Я разработал несколько менее очевидных сценариев и представляю их здесь в качестве пищи для размышлений. Надеюсь, что они не станут руководством к действию, а, наоборот, помогут сделать Рунет безопаснее.

Верифицированный отправитель
Иногда администраторы сайтов по недосмотру не включают фильтрацию поля «Имя» в форме регистрации (скажем, при подписке на рассылку или при отправке какой-нибудь заявки). Вместо имени можно вставить текст (иногда килобайты текста) и ссылку на вредоносный сайт. В поле email вставляем адрес жертвы. После регистрации этому человеку придет письмо от сервиса: «Здравствуйте, уважаемый…», а дальше — наш текст и ссылка. Сообщение от сервиса будет в самом низу.

Как это превратить в оружие массового поражения?

Элементарно. Вот один случай из моей практики. В одном из поисковиков в декабре 2017 года была обнаружена возможность отправки сообщений через форму привязки запасного email. До того как я выслал отчет по программе bug bounty, имелась возможность отправлять 150 тысяч сообщений в сутки — нужно было только немного автоматизировать заполнение формы.

Этот трюк позволяет отправлять мошеннические письма с настоящего адреса техподдержки сайта, со всеми цифровыми подписями, шифрованием и так далее. Вот только вся верхняя часть оказывается написанной злоумышленником. Такие письма приходили и мне, причем не только от крупных компаний вроде booking.com или paypal.com, но и от менее именитых сайтов.

Шаг 3:

1. Анализ способов предотвращения применения социальной инженерии Приняты ли в вашей компании или школе процедуры, призванные предотвращать применение социальной инженерии?

Скорее нет

2. Если да, в чем заключаются эти процедуры?

_____
_____
_____
_____
_____
_____
_____

3. Найдите в Интернете процедуры, принятые в организациях для того, чтобы предотвратить получение доступа к конфиденциальной информации при помощи социальной инженерии. Перечислите найденное. Осуществление защиты от атак социальной инженерии

Для начала создать политику безопасности, нужно сделать ее доступной персоналу и добиться ее исполнения, при этом главная задача — обучить персонал политике ИБ.

Безопасность компании — общее дело, поэтому донесите ее основы до всех отделов и пользователей, особенно тех, кто работает вне офисной среды.