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.

Переадресация портов

1) Злоупотребления доверием 2) неправильно предоставить доступ

3) Захват хакером общего доступа

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.

Злоупотребления доверием, когда взломанный хост используется для

передачи через межсетевой экран трафика, который в противном случае был бы обязательно от бракован.

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?

Не давать доступ к DMZ не доверенным лицам

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

Основным способом борьбы с переадресацией портов является использование надежных моделей доверия . Кроме того, помешать хакеру установить на хосте свои программные средства может хост-система IDS (HIDS).

