

Всем салют!

Сегодня речь пойдет о Telegram и Instagram.

Лекция 2 «Взлом Telegram и Instagram»

Telegram

Акк от телеги мы можем увести следующими способами из прошлой лекции:

1. Стиллер, используя Azorult, TeleShadow 2.

Пройденный нами Azorult обладает нужной нам опцией (Стиллер куки-файлов Telegram, по которым можно попасть на аккаунт).

**Как вы понимаете, для этого способа у человека на ПК должна быть установлена прилага Telegram Desktop.*

Есть вариант перехвата сессии используя TeleShadow 2, он более простой и делает все ровно так же. Рассмотрим его ниже

2. Дубликат симки.

**Нужно знать номер телефона жертвы, что далеко не всегда возможно.*

3. Взлом протокола связи SS7.

Грубо говоря, перехват сигнала базовой станции оператора. Все инфу поступающую на телефон можно перехватить, даже звонки.

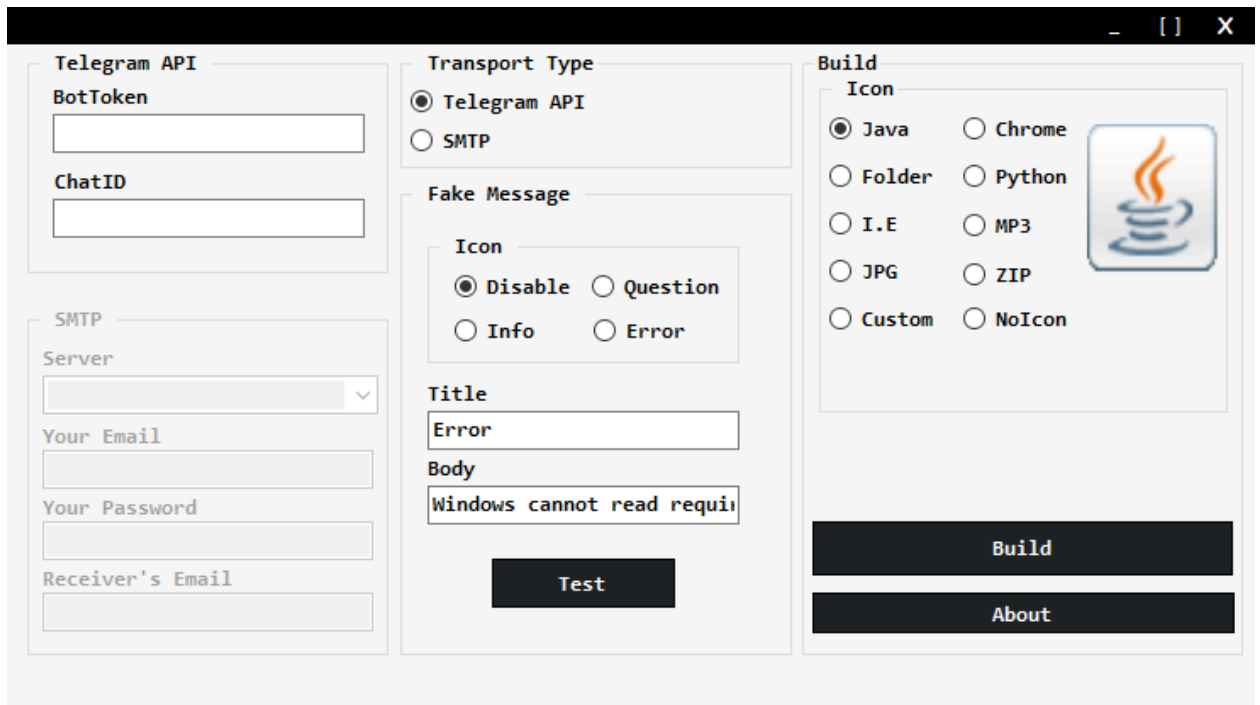
**Данный метод мы рассматривать не будем из-за его сложности. Возможно в будущем сделаем отдельный курс на эту тему.*

TeleShadow 2. Руководство.

Перехват телеграмм сессии еще никогда не был так прост в реализации, прога очень проста и эффективна.

Главные достоинства данного ПО:

- Обход двухфакторной аутентификации
- Обход пароля для входа в аккаунт
- Поддержка официальной версии Telegram Desktop, а так же iGram.
- Смена иконки стиллера
- Поддержка Telegram API и фейковых сообщений.



Вот так выглядит наш стиллер.

Первое, что нас интересует:

Transport Type – это то, как будет происходить доставка данных нам.

Тут два варианта:

1. Телеграм апиай – используя бота, будет идти прямо в наш телеграм.

**Чтобы получить идентификатор пользователя (свой) или GroupChat, просто отправьте /my_id в телеграмм бота @get_id_bot.*

2. SMTP – используя электронную почту.

Fake Message – то, что будет высказывать у жертвы при запуске стиллера.

Icon – иконка стиллера

Когда ввели все данные – жмем **Build** и генерируем наш стиллер.

Взлом Instagram

Фишинг

Используем сайт Z-Shadow, что бы не заморачиваться с хостингом и прочим.

Шаг 1: Создайте аккаунт на z-shadow.info

Applications ▾ Places ▾ Firefox ESR ▾ Thu 10:31

Register - z-shadow.us - Mozilla Firefox

z-shadow.info/register

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

Username:

Password:

Confirm Password:

Email:

Age: 15 ▾

Country: Afghanistan ▾

Captcha:

Pub - Ads

Waiting for www.google.com...

Шаг 2: После регистрации ваш аккаунт будет выглядеть примерно, как на изображении ниже.

Applications ▾ Places ▾ Firefox ESR ▾ Thu 10:34

Home - z-shadow.us - Mozilla Firefox

z-shadow.info/index.php

Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Getting Started

martinumusime

Username: martinumusime

Total victims: 25

Victims Of Today: 0

Total ZPoints: 0

Total Pages: 0/5

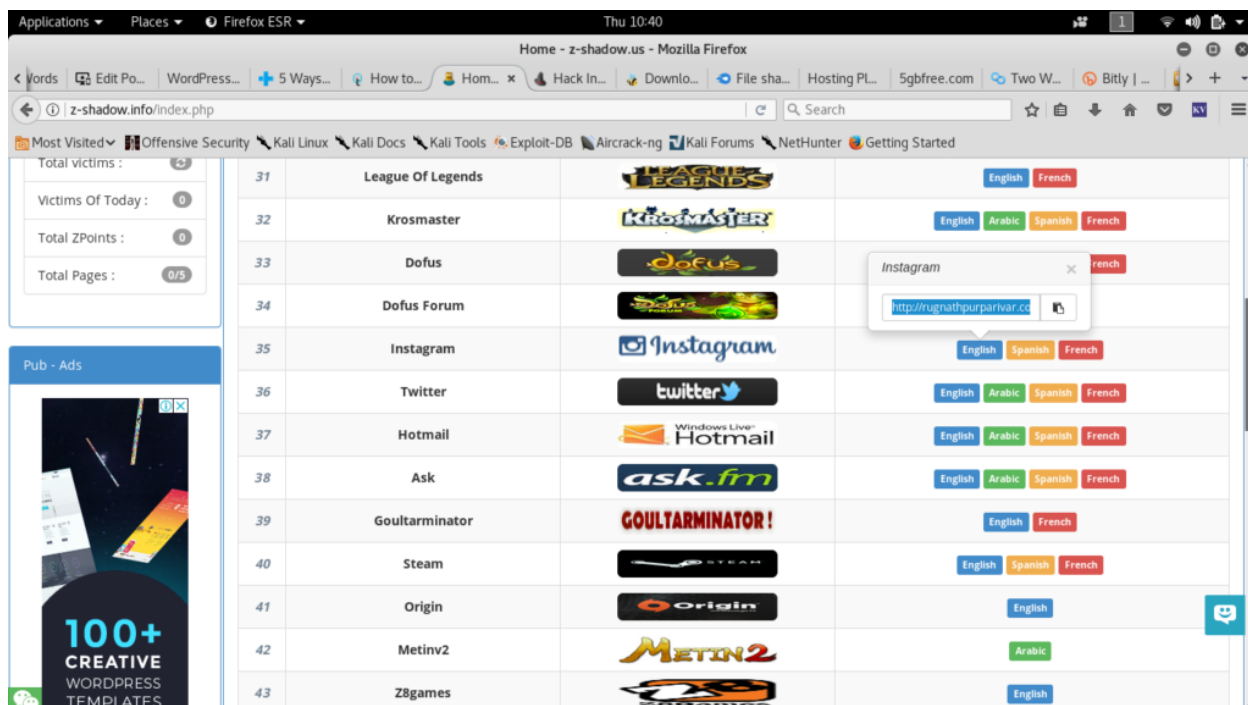
Pub - Ads

Transferring data from z-shadow.info...

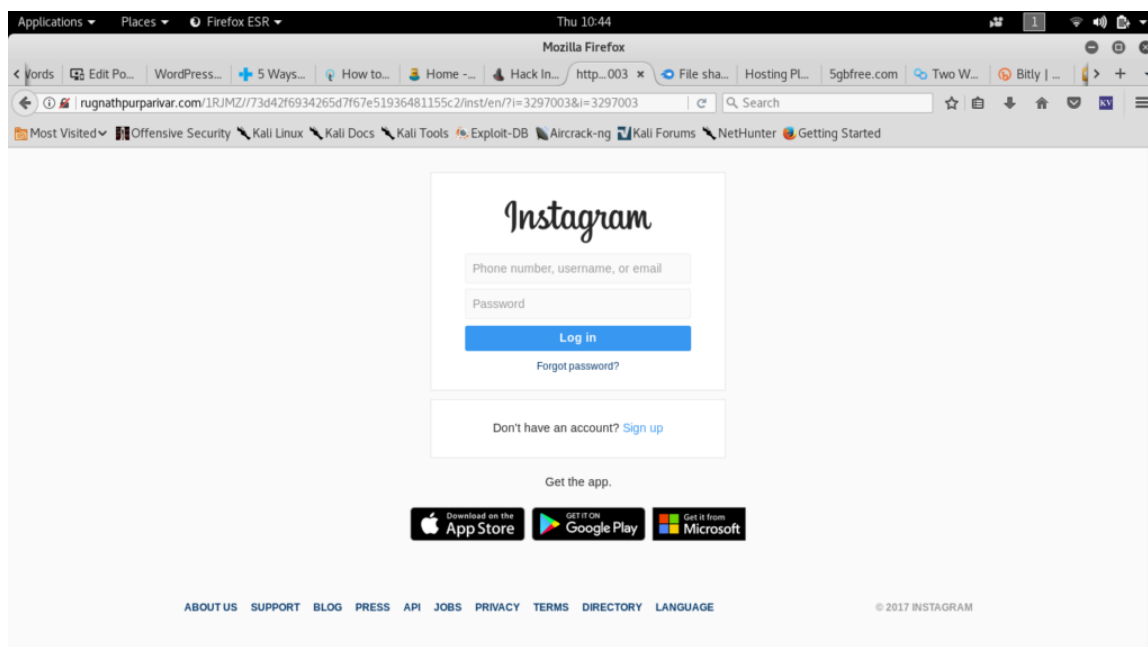
Links get updated automatically every 6 hours.

#	Website Description	Website Logo	Links
1	Facebook	facebook	English Arabic Spanish French
2	Facebook Colors	facebook	English Arabic Spanish French
3	Facebook Colors1	facebook	English
4	HappyFarm	الفرجة المرحلة	English Arabic
5	Pool Live Tour Free Coins	POOL	English Arabic Spanish French
6	8ball pool	8ball pool	English Arabic Spanish French
7	Facebook Add Likes	Add Fans	English Arabic Spanish French
8	Facebook Add Friends	Add Friends	English Arabic Spanish French
	Facebook Add Followers	Add 1000 followers to your account	English Arabic Spanish French

Шаг 3: Листайте вниз и выберите страницу номер 3 > Number 35 (Instagram) > Нажмите «English» > Нажмите Ctrl + C (чтобы скопировать ссылку)



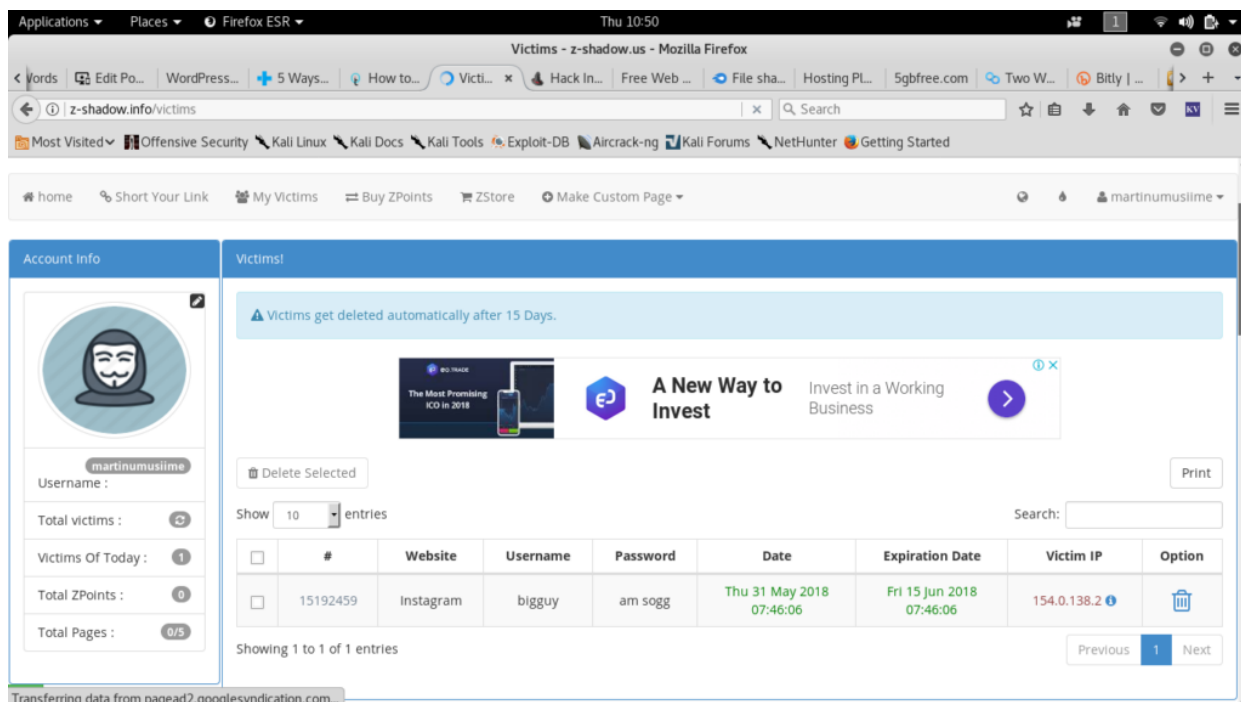
Шаг 4: Откройте новое окно и нажмите Ctrl + V, чтобы вставить ссылку в URL-пространство.



Как просмотреть взломанные никнеймы и пароли

Для того, чтобы увидеть количество взломанных жертв, вернитесь на домашнюю страницу вашего аккаунта и обновите «Total Victim» под

фотографией вашего профиля. Нажмите на вкладку My Victims вверху страницы, затем нажмите Продолжить.

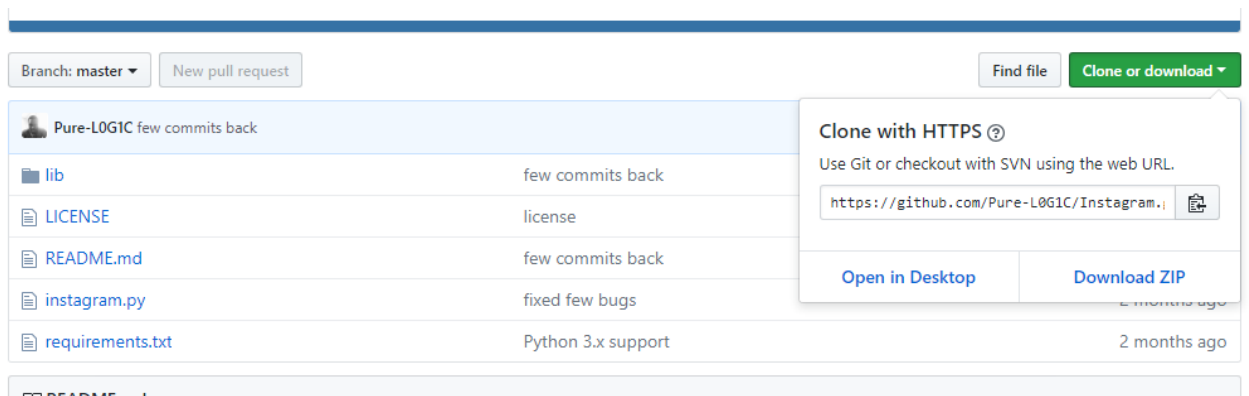


Теперь взлом паролей и аккаунтов Инстаграм выглядит веселым и простым занятием, не так ли? Как это работает? Просто скопируйте ссылку из третьего шага и отправьте ее по whatsapp или СМС, уговаривая вашу цель нажать на нее. Поздравляем, вы взломали ваш первый Инстаграм аккаунт сегодня.

Брутфорс

Сразу предупреждаю, что этот метод атаки простой, но занимает много времени

Шаг 1: Загрузите эту программу <https://github.com/Ethical-H4CK3R/Instagram.git> из git-репозитория на ваш компьютер. Так, как показано на рисунке ниже.



Далее, вам нужно распаковать файл, для этого откройте окно терминала и напишите следующую команду: `chmod -R 755 Instagram && cd Instagram`

```
root@Kali:~# chmod -R 755 Instagram && cd Instagram
root@Kali:~/Instagram#
```

Шаг

2: Выполняем программу. Для того, чтобы открыть программу, напишите команду `ls`, чтобы увидеть, что находится внутри папки.

```
root@Kali:~/Instagram# ls
Core  README.md  instagram.py
root@Kali:~/Instagram#
```

Далее, запустите программу

`Instagram.py`, набрав команду в терминале `python Instagram.py`.

Вы получите сообщение об ошибке, не волнуйтесь.

Это произошло, потому что мы не предоставили программе текстовый файл. Так как это программа использует брутфорс метод для взлома Инстаграма, то нам необходимо предоставить словарь, чтобы программа могла им воспользоваться.

Шаг 3: Получаем текстовый файл. Для этого загрузите «`daniel miessler passwords github`» и выберите первый результат. Прямо как на скриншоте ниже.

Google search results for "daniel miessler passwords github". The search bar shows the query, and the results list several GitHub repositories related to security assessments, including "SecLists" and "Passwords". A red arrow points to the "Tools" tab in the search results.

Google search results for "daniel miessler passwords github". The search bar shows the query, and the results list several GitHub repositories related to security assessments, including "SecLists" and "Passwords". A red arrow points to the "Tools" tab in the search results.

Перейдите в папку Passwords и выберите один из текстовых файлов, в котором не менее 10 миллионов паролей. Чем больше, тем лучше.

g0tm1k Close #200 - Attribution for @erose1337 Latest commit c196a6e a day ago		
Discovery	Quick move about	3 months ago
Fuzzing	Added numeric combinations	3 months ago
IOCs	rename 's/_/-/g'	10 months ago
Miscellaneous	Quick move about	3 days ago
Passwords	Added CIRT default usernames/passwords from https://cirt.net/passwords	2 days ago
Pattern-Matching	Close #106 - XXE-Fuzzing / Grep PHP Auditing	3 months ago
Payloads	Merge pull request #197 from g0tm1k/zip	9 days ago
Usernames	Added CIRT default usernames/passwords from https://cirt.net/passwords	2 days ago
Web-Shells	Set file permissions	4 months ago
.gitignore	Quick move about	3 days ago
CONTRIBUTING.md	Update CONTRIBUTING.md	9 days ago
LICENSE	Create LICENSE	9 days ago
README.md	Close #200 - Attribution for @erose1337	a day ago

Для того, чтобы сохранить файл, скопируйте пароли в текстовый редактор и сохраните с разрешением .txt в Instagram папку, которая должна находиться в домашней директории.

Шаг 4: Время взломать Инстаграм аккаунт. Откройте терминал и напишите следующую команду: `cd Instagram`. В соответствующей папке напишите команду `ls`, чтобы убедиться, что текстовый файл находится в нужной папке.

Для того, чтобы выполнить программу напишите:
Python Instagram.py Username Thetextfile.txt

С этого момента брутфорс атака началась. В терминале будет отображаться номер попытки и текущий пробный пароль.



```
[!] Brute Force In Progress ...  
[ - ] [REDACTED]  
[ - ] [REDACTED]  
[ - ] Attempts: 13  
[ - ] Password Found: True  
root@kali:~/Desktop/Instagram#
```

Если вы получаете ошибки, такие как Core.tor, импортируйте TorManager, затем установите механизацию с помощью:

pip install mechanize,

установите запросы с:

pip install request,

установите Tor с помощью:

sudo apt-get install tor