Темы которые нужно изучить:

* Поддомены <https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B4%D0%B4%D0%BE%D0%BC%D0%B5%D0%BD>
* Поиск поддоменов <https://habr.com/ru/company/hosting-cafe/blog/312954/>
* Зачем искать директории на сайте <https://tgraph.io/Kak-haknut-na-sajt-na-ehtape-sbora-informacii-11-30>
* Поиск админок на сайте <https://hackware.ru/?p=2633>
* Про протокол FTP <https://ru.wikipedia.org/wiki/FTP>
* Про протокол TELNET <https://ru.wikipedia.org/wiki/Telnet>
* Про HTTP Auth <https://en.wikipedia.org/wiki/Basic_access_authentication>
* Про HTTP Auth <https://developer.mozilla.org/ru/docs/Web/HTTP/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F>
* Про метод перебора паролей <https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D0%BD%D1%8B%D0%B9_%D0%BF%D0%B5%D1%80%D0%B5%D0%B1%D0%BE%D1%80>
* Про многопоточную работу программ <https://ru.wikipedia.org/wiki/%D0%9C%D0%BD%D0%BE%D0%B3%D0%BE%D0%BF%D0%BE%D1%82%D0%BE%D1%87%D0%BD%D0%BE%D1%81%D1%82%D1%8C>
* Словарь директорий использованный в программе <https://github.com/Bo0oM/fuzz.txt>

Программа осуществляет такие вещи:

* Поиск субдоменов на сайте, с помощью открытых источников.
* Поиск директорий на сайте по словарю.
* Поиск директории админки на сайте по словарю.
* Подбор пароля и логина к HTTP Auth.
* Подбор пароля и логина к FTP.
* Подбор пароля и логина к TELNET.
* Многопоточная работа.

Программа основывается на таких библиотеках:

* PySimpleGUIQt – для реализации графического интерфейса. <https://pysimplegui.readthedocs.io/en/latest/>
* Requests – для отправки реквестов к сайтам. <https://requests.readthedocs.io/en/master/>
* Requests\_ntlm – для работы с HTTP Auth. <https://github.com/requests/requests-ntlm>
* Queue – для общения потоков между собой. <https://docs.python.org/3/library/queue.html>
* Threading – для реализации многопоточности. <https://docs.python.org/3/library/threading.html>
* Socket – для работы с сокетами. <https://docs.python.org/3/library/socket.html>
* Ftplib – для работы с FTP протоколом. <https://docs.python.org/3/library/ftplib.html>
* Telnetlib – для работы с TELNET протоколом. <https://docs.python.org/3/library/telnetlib.html>
* Json – для парсинга json формата. <https://docs.python.org/3/library/json.html>
* Re – работа с регулярными выражениями. <https://docs.python.org/3/library/re.html>

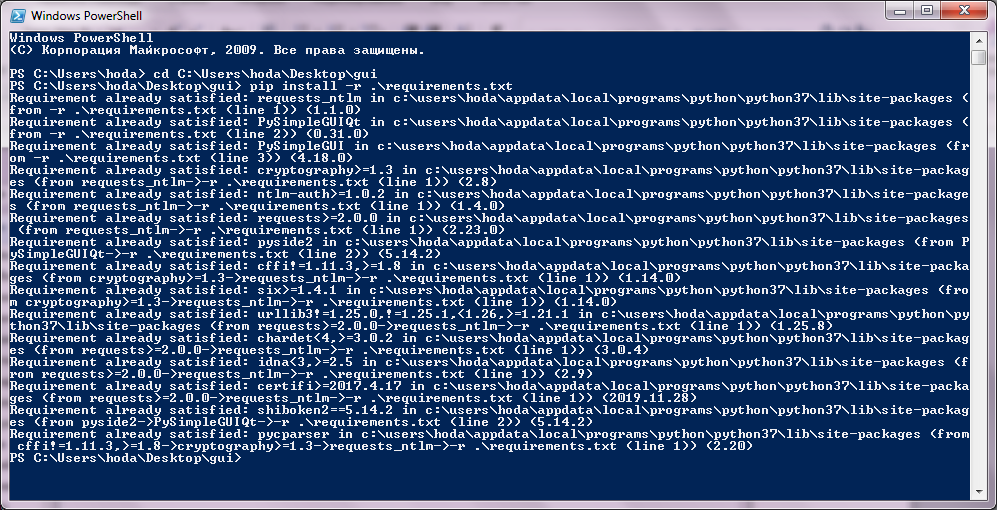
Программа состоит из таких файлов:

* Gui.py – главный файл программы, в нем реализовывается графический интерфейс, многопоточность, обработка нажатий в графическом интерфейсе.
* Lib/dir.py – модуль для поиска директорий на сайте.
* Lib/ftpauth.py – модуль для подбора пароля и логина к FTP.
* Lib/httpauth.py – модуль для подбора пароля и логина к HTTP Auth.
* Lib/subdomain.py – модуль для поиска субдоменнов сайта по открытым источникам.
* Lib/telnetauth.py – модуль для подбора пароля и логина к TELNET.

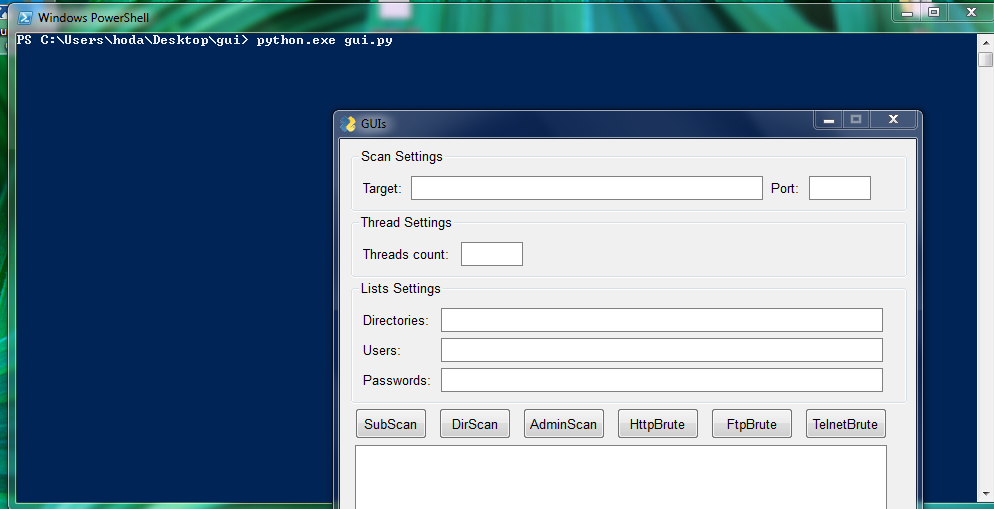
**Установка и запуск**

Для запуска нужно:

* Установить Python3 <https://www.python.org/downloads/release/python-380/>
* Установиться нужные библиотеки, для этого запускаем консоль в папке проекта и выполняем команду pip.exe install –r requirements.txt.



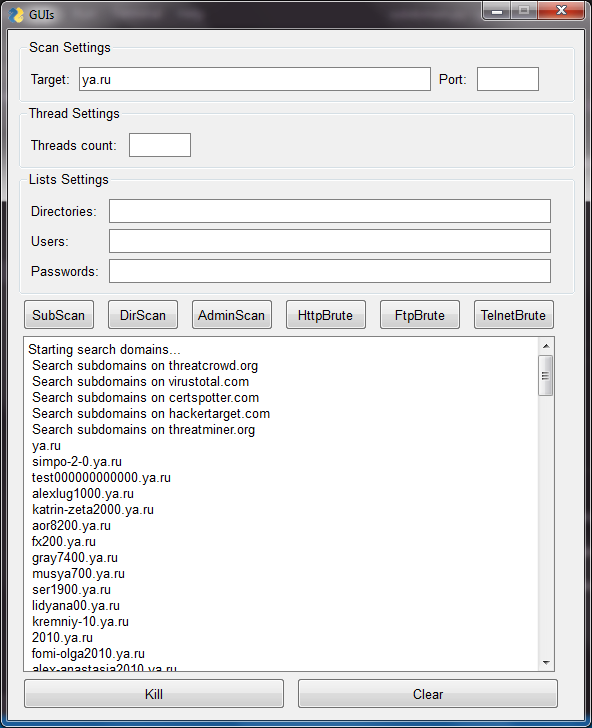
* Для запуска самой программы, нужно выполнить команду python.exe gui.py



**Поиск субдоменнов на сайте**

Для этого интересующий сайт вводится в поле Target, и нажимается кнопка SubScan. Результат сканирования выводится в нижнюю часть окна программы.

Кнопки Kill и Clear нужны, для остановки сканирования, и для очистки окна вывода.



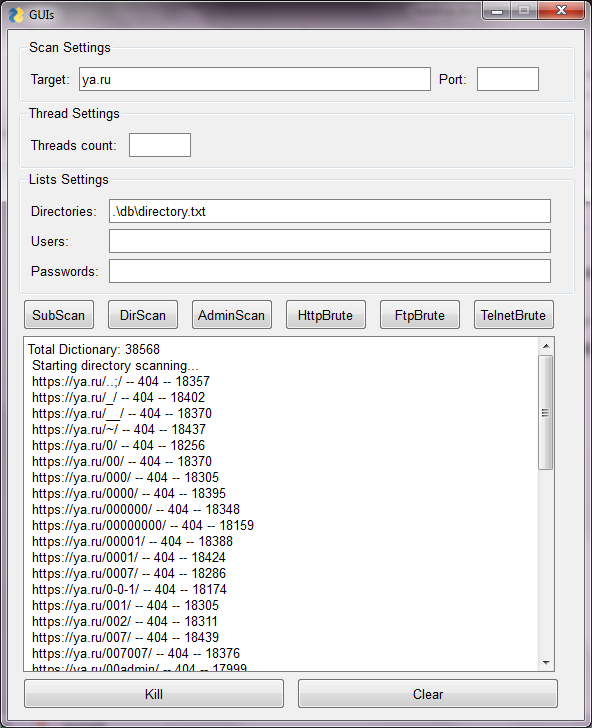
**Поиск директорий на сайте**

Для этого интересующий сайт вводится в поле Target, путь к словарю вводится в поле Directories, и нажимается кнопка DirScan.

Если путь к словарю не будет заполнен, то используется словарь по умолчанию из папки db.

Так же, в поле Thread count можно ввести нужное количество потоков, по умолчанию используется один поток.

Результат сканирования выводится в нижнюю часть окна программы, результат включает в себя URL к которому была попытка подключения, и размер ответа от сервера, а так же статус ответа.



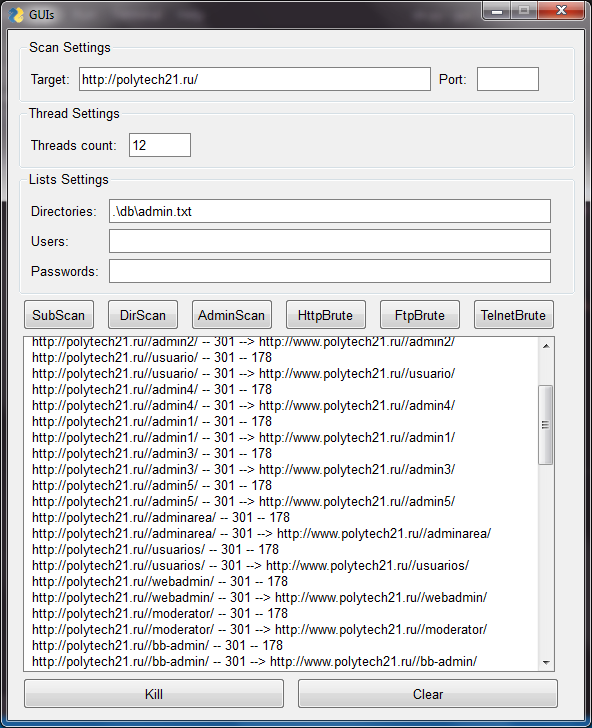
**Поиск директорий администратора на сайте**

Для этого интересующий сайт вводится в поле Target, путь к словарю вводится в поле Directories, и нажимается кнопка AdminScan.

Если путь к словарю не будет заполнен, то используется словарь по умолчанию из папки db.

Так же, в поле Thread count можно ввести нужное количество потоков, по умолчанию используется один поток.

Результат сканирования выводится в нижнюю часть окна программы, результат включает в себя URL к которому была попытка подключения, и размер ответа от сервера, а так же статус ответа.



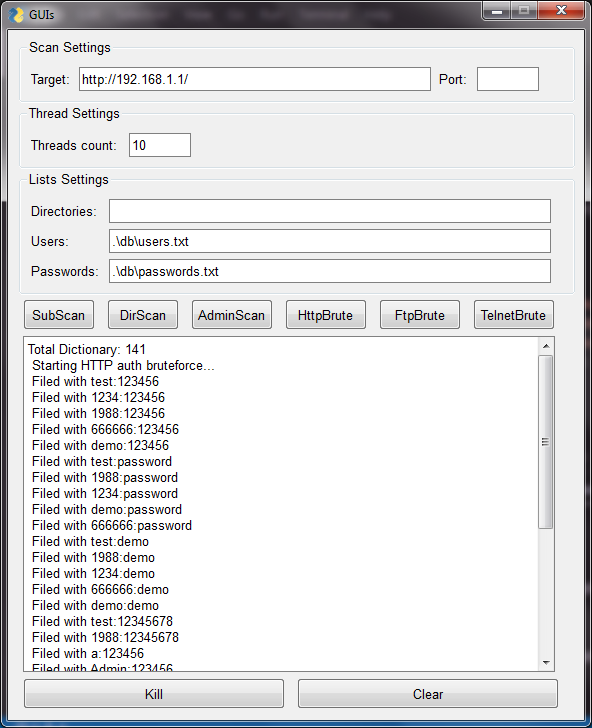
**Подбор пароля и логина к HTTP Auth на сайте**

Для этого интересующий сайт вводится в поле Target, путь к словарю вводится в поля Users и Password, и нажимается кнопка HttpBrute.

Если путь к словарю не будет заполнен, то используется словарь по умолчанию из папки db.

Так же, в поле Thread count можно ввести нужное количество потоков, по умолчанию используется один поток.

Результат сканирования выводится в нижнюю часть окна программы, результат включает в себя успешные попытки подключения и проваленные.



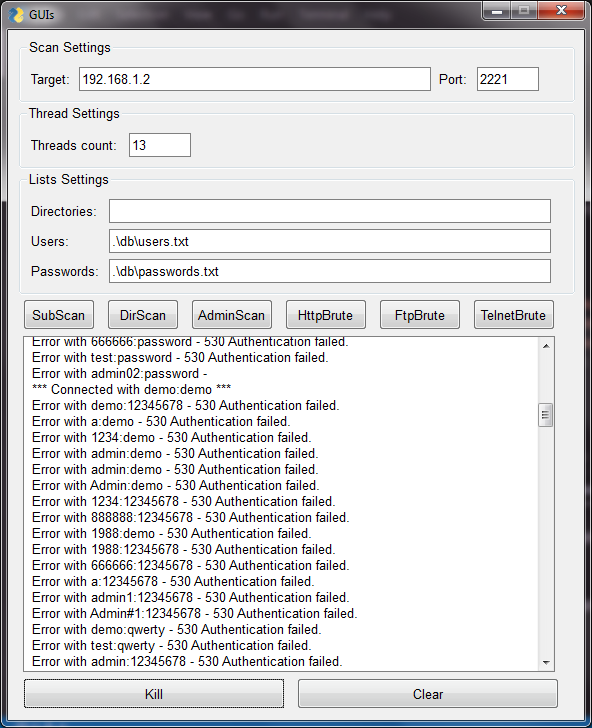
**Подбор пароля и логина к FTP на сервере**

Для этого интересующий IP вводится в поле Target, путь к словарю вводится в поля Users и Password, порт на котором работает FTP вводится в поле Port, и нажимается кнопка FtpBrute.

Если путь к словарю не будет заполнен, то используется словарь по умолчанию из папки db.

Так же, в поле Thread count можно ввести нужное количество потоков, по умолчанию используется один поток.

Результат сканирования выводится в нижнюю часть окна программы, результат включает в себя успешные попытки подключения и проваленные, а так же статус проваленной попытки.



**Подбор пароля и логина к TELNET на сервере**

Для этого интересующий IP вводится в поле Target, путь к словарю вводится в поля Users и Password, порт на котором работает TELNET вводится в поле Port, и нажимается кнопка TelnetBrute.

Если путь к словарю не будет заполнен, то используется словарь по умолчанию из папки db.

Так же, в поле Thread count можно ввести нужное количество потоков, по умолчанию используется один поток.

Результат сканирования выводится в нижнюю часть окна программы, результат включает в себя успешные попытки подключения и проваленные, а так же статус проваленной попытки.

