Назначение и общий алгоритм работы системы

Система предназначена для автоматизации сканирования заданного перечня ip-адресов на предмет открытых портов баз данных (далее – БД). При нахождении таких БД производится попытка подключения к ним по заданным словарям логинов и паролей. При успешном подключении происходит запрос перечня имеющихся БД на сканируемой. Полученная информация записывается в log-файл в формате txt.

Работа ПО выполняется посредством консоли ОС Linux. ЯП – Python3.8.

Перечень БД:

* MongoDB
* Elasticsearch
* MySQL
* PostgreSQL

Перечень компонентов системы, их назначение и основные характеристики

В качестве входной информации выступают ip-адреса (ключ -i), логины (ключ -l), пароли (ключ -p) в виде текстовых файлов, а также файл с настройками setting.conf для конфигурации, где можно настроить порты по умолчанию для конкретных БД, задержку по времени между сканированием адресов, название и путь к GeoIP-БД в формате .mmdb для поиска информации по конкретному ip-адресу и очистку log-файла log.txt перед сканированием.

Программная часть системы состоит из двух скриптов:

1. scan\_v4.py для непосредственно сканирования
2. hacking.py, в котором определены функции для выполния подключения к БД и записи результатов в log-файл.

Так как в файле с адресами должна быть возможность помимо единичных адресов указывать диапазоны адресов в разных форматах (например: 192.168.0.0/24, 10.10.5-7.100-150, 172.16.0.5/32 и т.д.), то в файл ip\_all.txt собираются автоматически все простые ip-адреса, полученные из этих диапазонов.

Для хранения ip-адресов, на которых был обнаружен хотя бы один порт используется файл csv.txt, куда складывается данная информация в виде <ip-адрес>:<открытые порты через запятую>:

104.244.53.18:27017

190.202.40.53:5432,27017

В сборку также включены файлы:

* GeoIP2-City.mmdb – БД для поиска информации по конкретному ip-адресу;
* install.sh – установщик\_1 (Внимание! Устанавливает python3.8 и python3-pip + зависимости);
* ip.txt – подборка ip-адресов для тестирования;
* logins.txt и top-usernames-shortlist.txt – топ популярных логинов для тестирования;
* password.txt и xato-net-10-million-passwords-10.txt – топ популярных паролей для тестирования;
* requirements.txt – установщик\_2 с зависимостями.

Алгоритм работы системы:

1. Очистка файлов ip\_all.txt и csv.txt.
2. Открытие файла с ip-адресами, предоставленного пользователем, преобразование диапазонов ip-адресов в перечень, запись полученной информации в файл ip\_all.txt.
3. Очистка файла log.txt (если задано в настройках).
4. Сканирование портов ip-адресов из файла ip\_all.txt путём установки tcp-соединения с использованием SOCK\_STREAM (сокета для протокола TCP). Ожидание ответа по умолчанию – 1 секунда.
5. Запись в файл csv.txt при нахождении хотя бы одного открытого порта.
6. Запись в файл log.txt информации о тех адресах, на которых были найдены открытые порты, поиск ip-адреса по БД GeoIP2-City.mmdb для определения страны, к которой он принадлежит.
7. Подключение к БД по данным файла csv.txt (ip-адрес и порт), запись результатов в log.txt (тип найденной БД, подошедшая связка логин/пароль). Запрос перечня имеющихся БД при успешном подключении.
8. Вывод информации о времени работы программы в виде log-файла:

--------------------

ip: 85.192.12.42

country: Russia

open\_port: 3306 --- MySQL

.kibana\_1

.kibana\_task\_manager

gl-events\_0

gl-system-events\_0

graylog\_0

open\_port: 9200 --- Elasticsearch

В программе также реализован цветной вывод в консоль во время сканирования и во время попытки подключения к БД.

Установка программы:

Совет: используйте виртуальное окружение! (virtualenv)

1 способ (Внимание! Устанавливает python3.8 и python3-pip + зависимости):

chmod +x install.sh

bash ./ install.sh

2 способ:

pip3 install -r requirements.txt

Пример запуска программы:

python3 scan\_v4.py -i ip.txt -l logins.txt -p password.txt

python3 sasha.py -l logins.txt -p password.txt