

Maltego — это инструмент для построения и анализа связей между различными субъектами и объектами. Её особенностями являются: визуализирование полученных данных, разведка на основе открытых источников, комбинирование для глубокого анализа данных полученных из закрытых и открытых источников, автоматический анализ открытых источников и автоматическое построение взаимосвязей между обнаруженными объектами.

Maltego позволяет собрать воедино информацию полученную из открытых и закрытых источников, она позволяет визуализировать агрегированные данные.

Maltego предлагает пользователю беспрецедентную информацию.

Информация — это средство воздействия. Информация — это сила.

- Maltego — это программа, которая может быть использована для выявления отношений и реальных связей между:
 - Людьми
 - Группами людей (социальные сети)
 - Компаниями
 - Организациями
 - Веб-сайтами
 - Интернет инфраструктурами, такими как:
 - Доменами
 - DNS именами

- Сетевыми блоками
- IP адресами
- Факторами
- Аффилированности
- Документами и файлами
- Эти объекты связываются на основе разведки по открытым источникам.
- Maltego — проста и быстра в установке, она использует Java, а, следовательно, работает на Windows, Mac и Linux.
- Maltego имеет графический интерфейс, которые позволяет видеть взаимосвязи между объектами мгновенном и точно, а это даёт возможность проследить скрытые связи.
- Используя графический пользовательский интерфейс (GUI), вы с лёгкостью увидите все взаимоотношения, даже если они разделены тремя или четырьмя уровнями.
- Maltego уникальна от того, что она использует мощный и гибкий фреймворк, который делает возможной настройку под себя. По сути Maltego может быть адаптирована под ваши собственные, уникальные требования.

Выполнение работы.

Необходимо запустить виртуальную машину Kali Linux. Пароль и логин для авторизации в системе root:toor

Вариант брать согласно журналу из файла Variants.txt.

1. Можно запустить из меню или набрать в консоли

\$ maltego

Нас встречает мастер:



Нажимаем далее. Нам нужно ввести e-mail и пароль.

Maltego_Chlorine

Welcome to Maltego!

Startup wizard - Login (1 of 2)

Enter your details below to log in to the Maltego Community Server
Or if you have not done so yet, [register here](#)

Login

* Email Address

Password

Crate

SoFull

* Solve captcha

< Back

Next >

Finish

Cancel

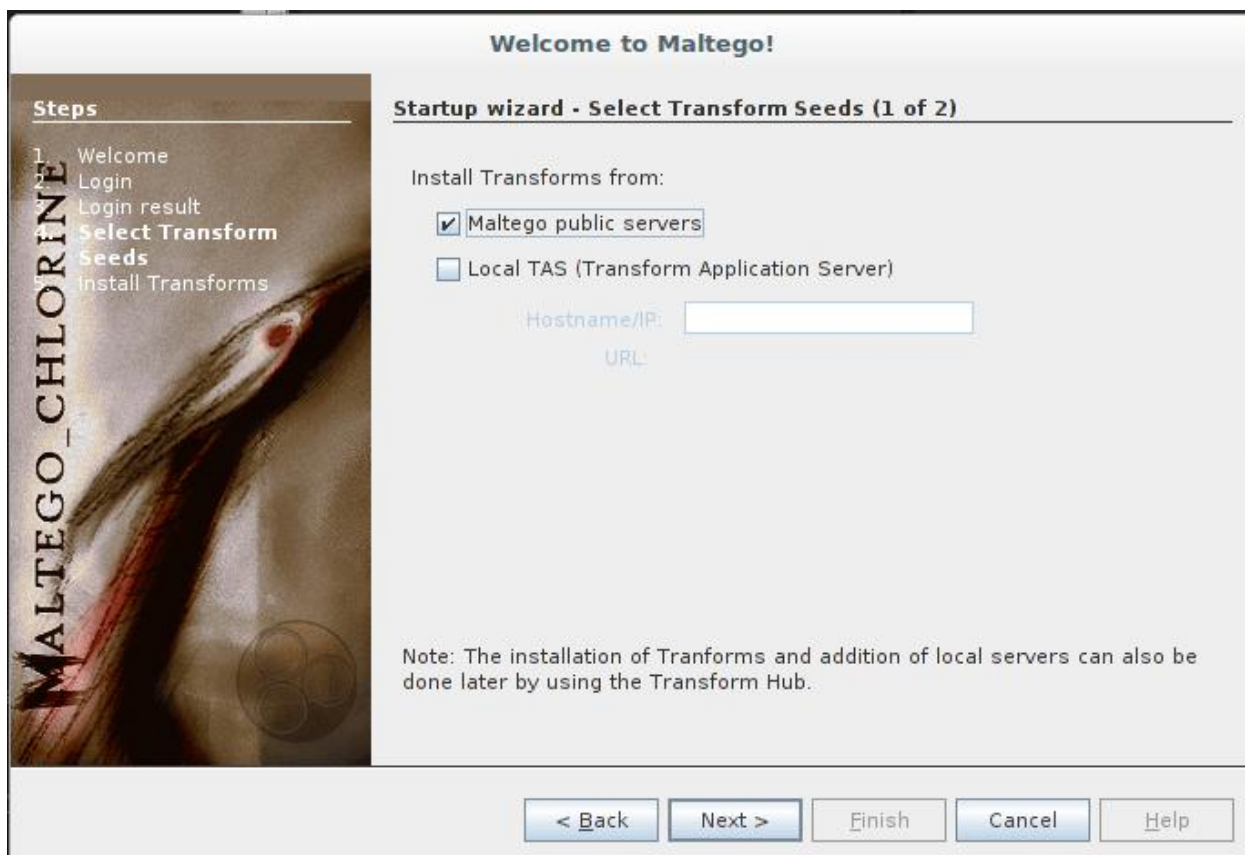
Help

Данные для входа:

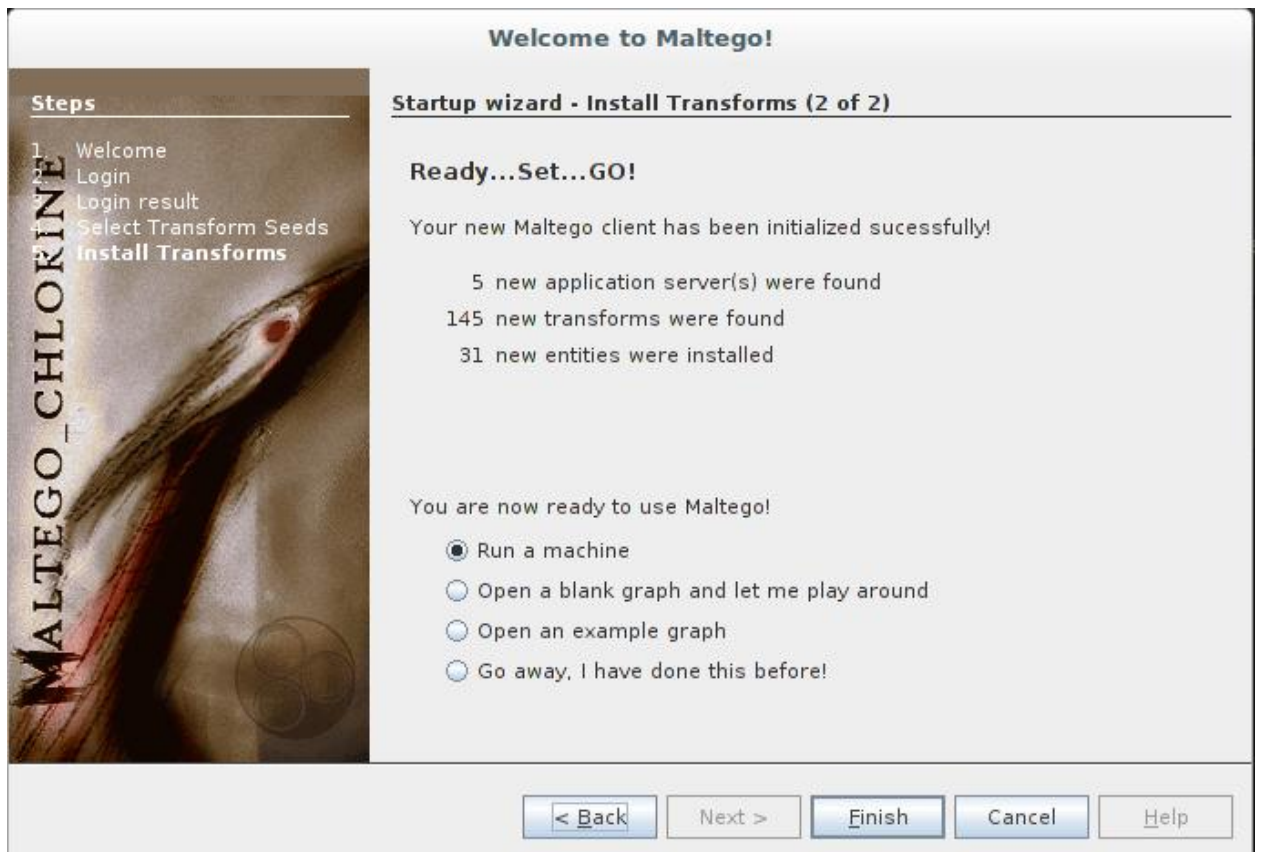
Email: sibsutis.biut@gmail.com

Password: test123

Вводим данные, нажимаем далее. Отмечаем Maltego public servers, далее:



Видим что для запуска машины все готово, кликаем финиш.



А здесь нас встречает запуск новой машины.



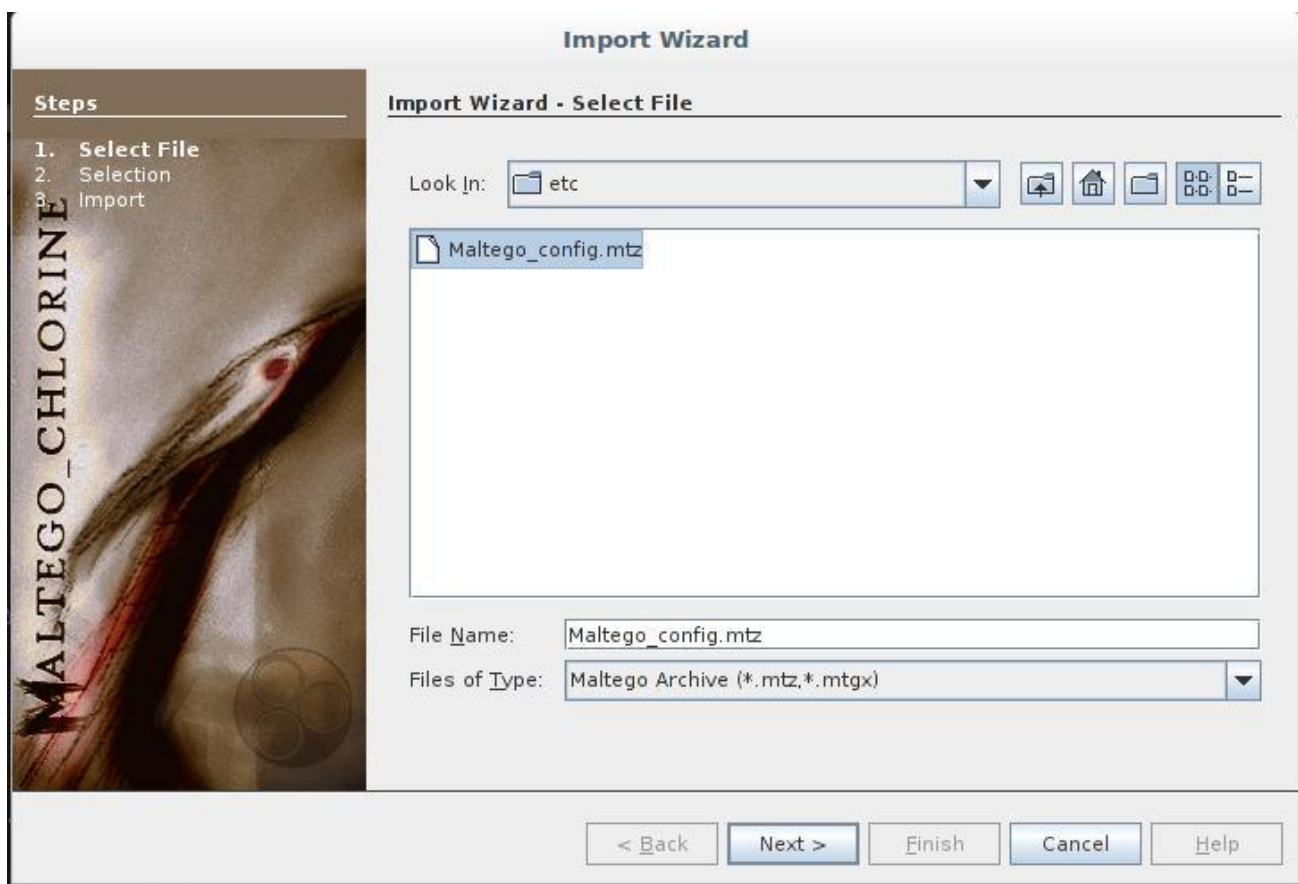
Закроем его. Давайте импортируем настройки. Нам говорят об ограничении, но оно убирается, если сделать импорт настроек.



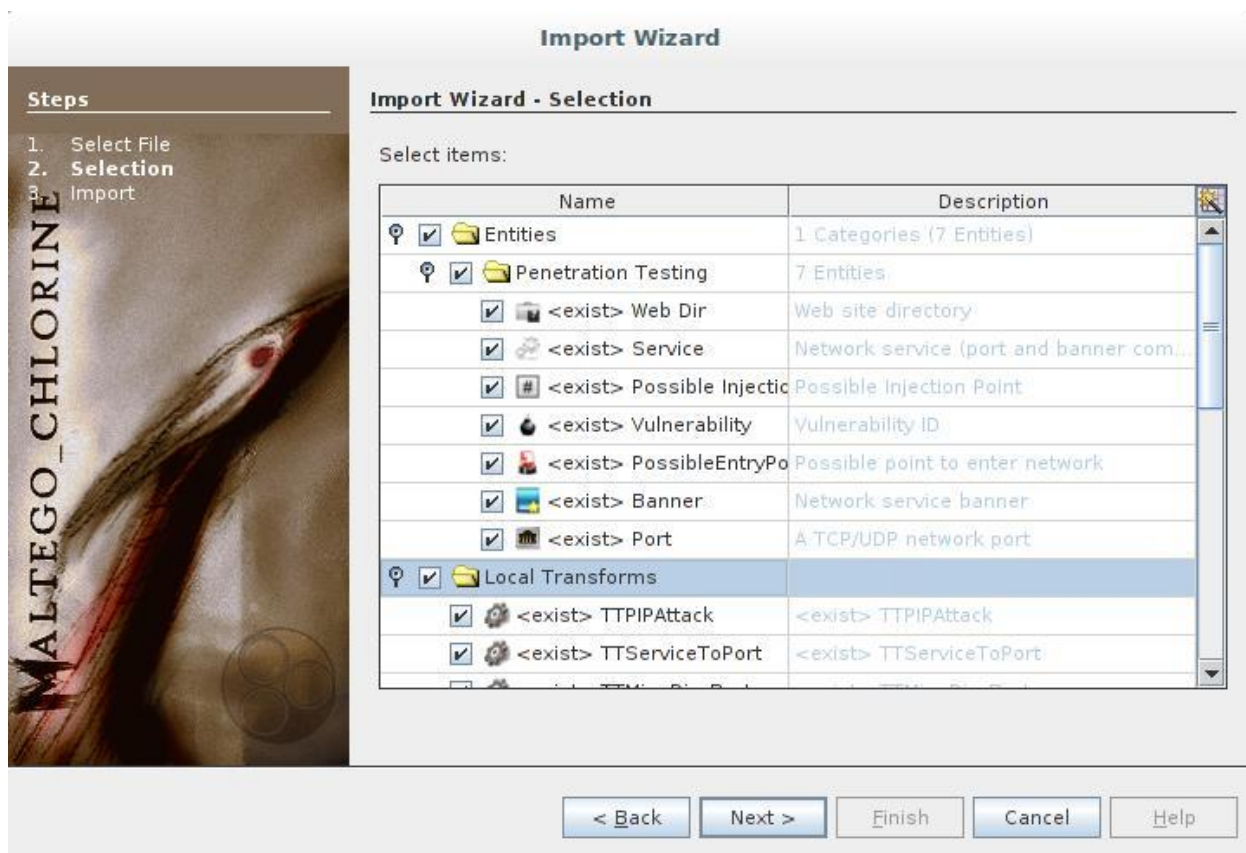
Нажмите ОК.

Чтобы импортировать настройки в левом верхнем углу нажмите на глобус/шар (кнопка приложения). Далее Импорт -> Импорт конфигурации, выберите файл лежащий по адресу /opt/Teeth/etc/Maltego_config.mtz. (Можно пропустить этот пункт и поставить галочку Don't show again).

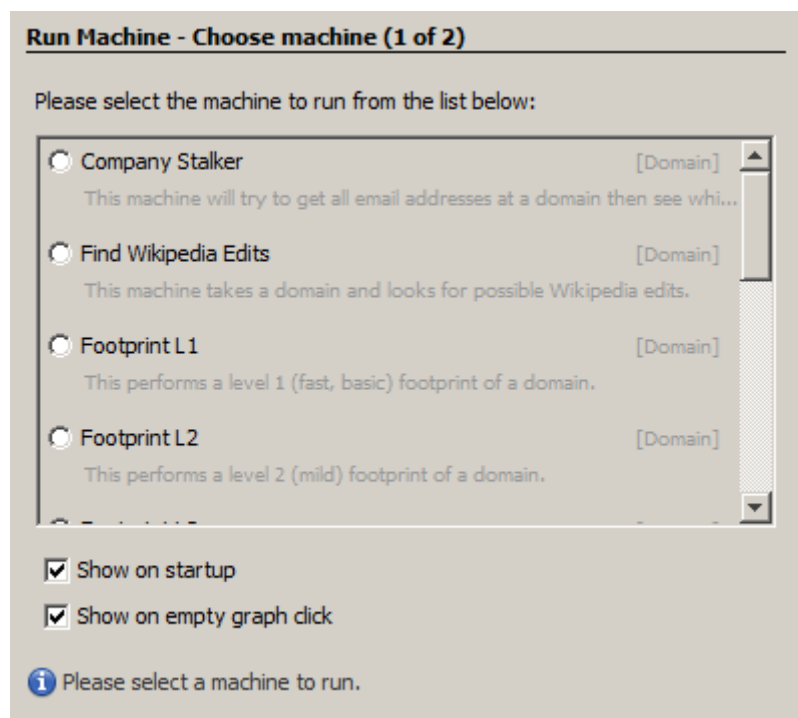
Нажмите Далее.



Поставьте галочки где нужно. Например – везде.



Теперь нажимаем запустить машину.

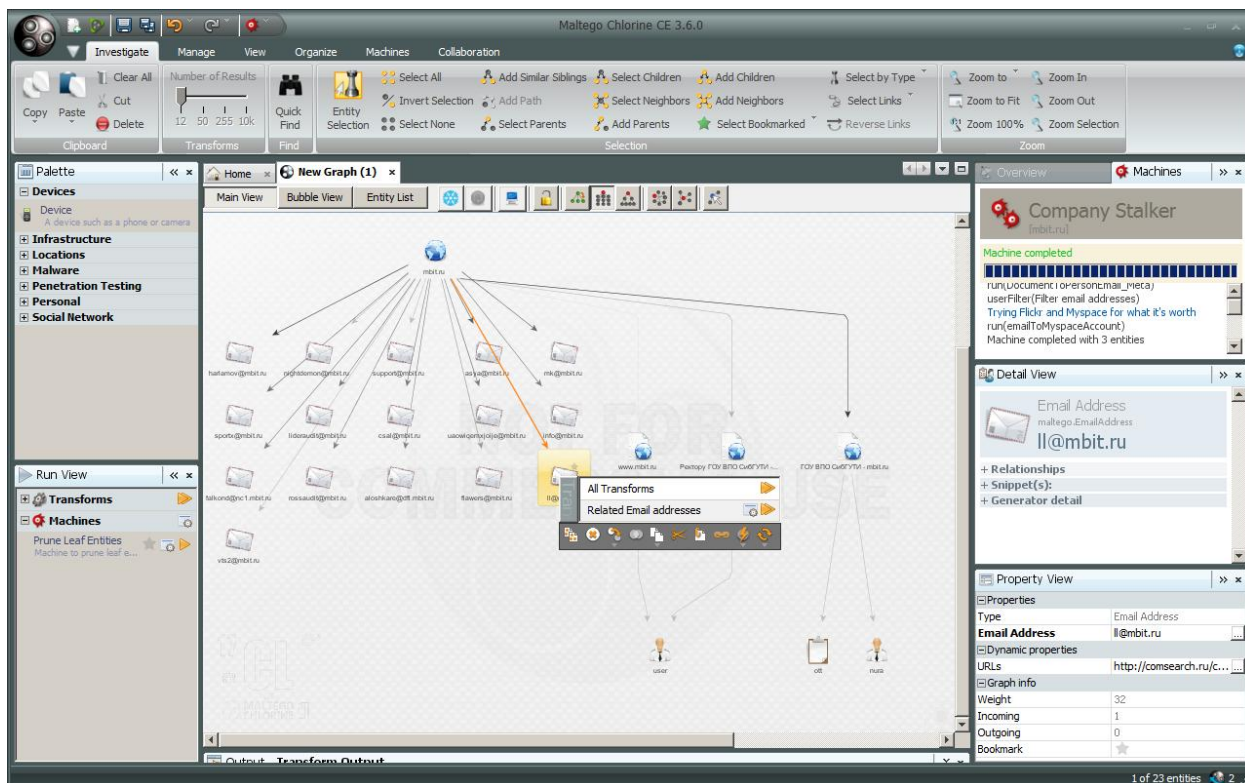


Доступные пункты:

- Company Stalker: Машина попытается собрать все адреса e-mail на домене, потом попробует их сопоставить с данными в социальных сетях. Также собираются документы и извлекаются метаданные. Нужно ввести домен.
- Find Wikipedia Edits: Эта машина берёт домен и ищет возможные правки в Википедии.
- Footprint L1: Производится первый уровень (быстрый, простой) снятия «отпечатков пальцев» с домена.
- Footprint L2: Производится второй уровень (мягкий) снятия «отпечатков пальцев» с домена.
- Footprint L3: Производится третий уровень (интенсивный) снятия «отпечатков пальцев» с домена. Это занимает время и потребляет ресурсы. Используйте осторожно.
- Footprint XXL: Машина впрягается в действительно тяжёлую работу по действительно большим целям, которые hostят свою собственную инфраструктуру. Машина пытается получить отпечатки пальцев просматривая SPF записи в надежде на нетблоки, а также на обратное делегирование DNS к их серверам имён. Это **ОЧЕНЬ** важно — внимательно смотреть на пользовательские фильтры, которые представлены перед вами, в противном случае вы **ОБЯЗАТЕЛЬНО** получите ложные срабатывания. Результатом работы этой машины может стать масса графиков поэтому, пожалуйста: 1) будьте терпеливы, 2) имейте много оперативной памяти.
- Person — Email Address: Пытается получить чей-либо e-mail адрес и найти, где он используется в Интернете. Нужно ввести адрес почты.
- Prune Leaf Entities: Prune Leaf Entities
- Twitter Digger X: Работает по псевдониму (или псевдонимам) Twitter. Анализирует твиты.
- Twitter Digger Y: Работает по псевдонимам Twitter. Находит твиты и анализирует их.
- Twitter Monitor: Машина мониторит Твиттер на хештеги или на заданные вхождения имени, упомянутые во фразах. Нужно ввести фразу.
- URL To Network And Domain Information

2. Согласно варианту, просканировать и проанализировать всю полученную информацию по одному из доменов. Режим сканирования Company Stalker или Footprint 1.

В ходе работы машины, будут появляться новые объекты. По каждому объекту можно кликнуть правой кнопкой и выбрать дополнительные действия, например, All Transforms:



3. Проанализировать полученную информацию, пометить ключевые объекты.

4. Выбрать режим Person — Email Address, используя полученные в ходе выполнения пункта 2 Email адреса, произвести сканирование. (В случае отсутствия адресов в пункте 2 – выбрать любой на ваше усмотрение. В некоторых случаях программа может не найти зависимости.)

5. Выбрать режим Twitter Digger Y/ Twitter Monitor. Подать любые входные параметры, посмотреть результат.