**УДК 004**

# ОХОТА ЗА ИНФОРМАЦИЕЙ ИЛИ OSINT В НАШЕ ВРЕМЯ

Мещеряков Г.В., студент гр. ИТб-202, IV курс
Научный руководитель: Ванеев О.Н., к.н., доцент,
Кузбасский государственный технический университет
имени Т.Ф. Горбачева,
Кемерово

**Значение OSINT в современном мире:**

1) **Важность доступа к информации в цифровую эпоху:**

В современном мире цифровые технологии играют ключевую роль в различных сферах жизни. От бизнеса и журналистики до безопасности и разведки, информация становится неотъемлемой частью нашего понимания окружающего мира и принятия важных решений. Особое внимание уделяется использованию открытых источников информации для осуществления разведки с открытым исходным кодом (OSINT).

OSINT - это уникальный инструмент, предлагающий многочисленные преимущества, которые связаны с его многообразием и простотой использования. Среди открытых источников данных можно выделить разнообразные источники информации, такие как новостные статьи, публикации в социальных сетях, правительственные отчеты и блоги. Это подчеркивает важность OSINT как источника информации, который может предложить данные, недоступные другим методам сбора информации.

Необходимо осознать, что применение OSINT не ограничивается сферой разведки и безопасности. Этот инструмент находит широкое применение в различных областях деятельности, что подчеркивает его универсальность и значимость.

- В расследовании коррупции, OSINT поможет в журналистике, выявлении скрытых фактов и отслеживании тенденций.

- В бизнесе, OSINT может использоваться для анализа конкурентов, оценки рыночных тенденций и обнаружения новых возможностей.

- В научных исследованиях, OSINT поможет проанализировать социальные тенденции, публикации и мнения экспертов.

- Необходимо осознавать ограничения и риски при использовании OSINT, несмотря на все преимущества.

- Неправомерное использование информации, ненадлежащий сбор данных и вторжение в частную жизнь могут иметь серьезные последствия для людей и организаций.

- Поэтому этика и законность играют важную роль в использовании OSINT.

В мире современности, OSINT представляет собой инструмент анализа информации, который обладает огромной мощью. С его помощью можно получить ценные данные и принимать обоснованные решения в различных сферах деятельности.

Осведомительные информационные инструменты (ОИИ) являются неотъемлемой частью исследовательской работы, предоставляя доступ к обширному объему информации. Взглянем на то, как ОИИ могут принести пользу в анализе и исследовании:

1) Широкий доступ к информации: ОИИ предоставляют доступ к разнообразной и свежей информации о событиях, новостях, трендах и других ключевых аспектах. Это помогает исследователям быть в курсе последних событий и тенденций в различных областях.

2) Многообразие источников: ОИИ объединяют в себе разнообразные ресурсы, включая официальные источники, медиа, социальные сети, блоги и другие. Это способствует получению различных точек зрения на изучаемую проблему или тему, обогащая исследовательский процесс.

1) Анализ общественного мнения и трендов: Открытые источники информации могут помочь исследователям выявить тенденции в общественном мнении, проанализировать предпочтения и поведение людей, а также спрогнозировать развитие событий.

2) Исследование конкурентной среды: В сфере бизнеса использование открытой информации позволяет проводить анализ конкурентов, изучать рыночные условия, оценивать потребности потребителей и открывать новые возможности.

3) Проверка фактов и подтверждение информации: Доступ к открытой информации помогает проверить факты, подтвердить достоверность информации и избежать распространения ложной информации путем сравнения различных источников.

1) Расширение доступа к информации: Открытые источники информации играют ключевую роль в современном анализе и исследованиях путем обеспечения исследователям доступа к разнообразным и актуальным данным из множества источников.

2) Повышение качества выводов: Получение ценных инсайтов и информации от открытых источников помогает исследователям принимать обоснованные решения и делать выводы на основе фактов, улучшая качество аналитических выводов в различных областях деятельности.

Путь к пентесту начинается с первого шага – определение области тестирования и сбор информации о цели. После заключения договора, первоначальные сведения включают в себя:

- Название компании.

- Сфера деятельности компании.

- Доменное имя компании.

Интернет-поиск может расширить наши возможности и позволит:

- Создать множество доменов и поддоменов из одного исходного домена.

- Исследование новых подходов к поиску информации.
- Анализ интересных путей в области веб-разработки и API.
- Определение технологического стека: ПО, аппаратуры, языков программирования.
- Поиск активных учетных записей в целевых веб-приложениях.
- Выявление потенциальных уязвимостей.

2) **Этика:**

Однако необходимо учитывать и те сложности, которые могут возникнуть при использовании открытых источников информации. Проблемы конфиденциальности и этики занимают центральное место в дискурсе об OSINT:

- Вторжение в частную жизнь: необдуманный сбор личной информации может нарушить право на приватность.

- Ненадлежащий сбор данных: использование недостоверной или искаженной информации может привести к неправильным выводам и действиям.

- Неправомерное использование информации: применение собранных данных в целях, противоречащих закону или моральным нормам, может иметь серьезные юридические и этические последствия.

**Майндмап по OSINT:**

Поиск в интернете – это не только простое использование поисковых систем, но и сложный процесс, требующий профессионального подхода. Многие исследователи делятся своими методами и стратегиями в поиске информации. На протяжении нескольких лет доступны различные майндмапы и статьи, помогающие в эффективном использовании интернет-ресурсов. Ссылка на подборку таких майндмапов представлена здесь, и несмотря на время, они остаются актуальными.

OSINT Framework - это мощный инструмент, созданный как циклический процесс для поиска информации. Каждый новый IP адрес или доменное имя требует пройти те же шаги, что и ранее найденная информация.

Самый известный майндмап для осинта - OSINT Framework, объединивший различные сайты, утилиты и базы данных. Он предлагает ответы на любые вопросы по осинту.

Однако следует отметить, что OSINT Framework ориентирован на страны вроде США и не учитывает особенности России.

3) **Пассивная разведка:**

1) В процессе пассивной разведки отсутствует любое вмешательство в цель. Не передаем пакеты посредством компьютера, не проводим резолвинг доменных имен на серверах цели, не пингуем ее айпишники, не заходим в веб-приложения и даже не обращаем внимание на двери офиса.

Примеры этапа пассивной разведки:

- Поиск в Google и "хакерских" поисковых системах.

- Исследование баз данных с утечками.

- Анализ вакансий на HH и linkedIn.

- Извлечение метаданных из публично доступных файлов и многое другое.

**Разведка средствами OSINT:**

**1) Начало: Никнейм**

Допустим в начальной точке мы имеет только никнейм юзера по которому хотим найти информацию, для начала прогоним данный никнейм через 2 инструмента(тут стоит отметить что для более лучшего результата, необходимо использовать алгоритмы мутации что бы подобрать похожие никнеймы на изначальный, для примера был взят Мой никнейм).

**Maigret:**

Инструмент Maigret - это довольно мощное и гибкое средство для анализа данных с социальных платформ, он был специально разработан для сбора информации, анализа активности Пользователей и поиска зависимостей. Данный инструмент поддерживает более 3000 сайтов для поиска по Никнейму пользователя.

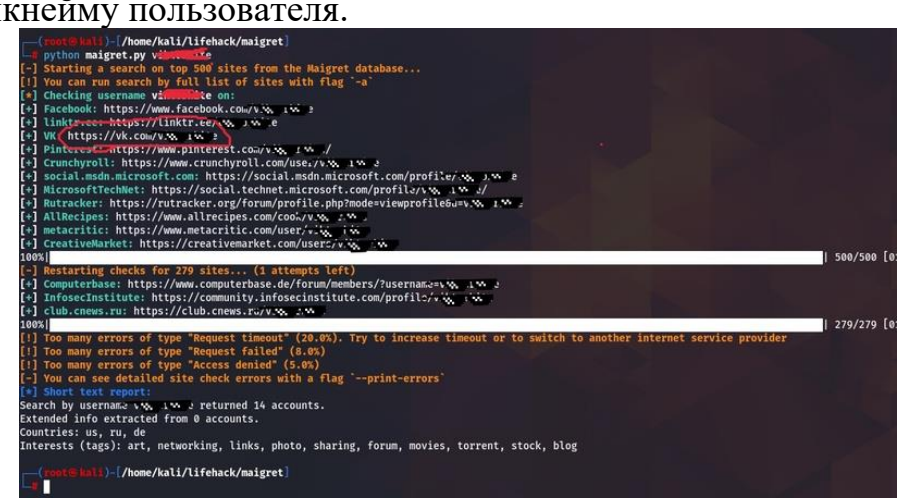


Рис. 1 «Пример работы Maigret»

На данном скриншоте мы можем наблюдать что через данную утилиту мы нашли 14 ссылок.

**Mr.Holmes**

Mr.Holmes - это проект, направленный на сбор информации из открытых источников о социальных сетях, телефонных номерах, доменах и IP-адресах с использованием Google Dorks.

Данный инструмент был назван в честь всеми известного сыщика. Инструмент имеет хороший функционал так же устанавливается как на Windows так и на Unix(В том числе и Termux). Естественно мы будем работать на Linux


Рис. 2 «Стартовая страница Mr.Holmes»

Выбираем пункт 1. В данном примере я не стал использовать прокси-сервер.


Рис. 3 «Пример работы Mr. Holmes»

У инструмента имеется неплохое решение с ведением локальной базы данных. Давайте как раз и воспользуемся ей и выберем 5 пункт.


Рис. 4 «Запуск GUI Mr.Holmes»

Можно наблюдать что сервер был запущен на 5001 порту, когда мы перейдём по этому адресу, у нас выскочит форма авторизации в панель управления базой данных.


Рис. 5 «Страница авторизации в GUI»

Выбираем поиск по Username и вводим никнейм по которому проводили поиск.

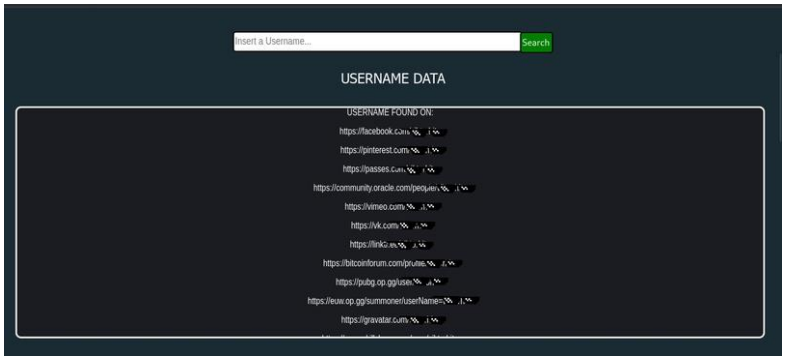


Рис. 6 «Поиск по псевдониму»

Так же в результате поиска можно получить фотографии пользователя с его страниц и сверять с другими сервисами. Так же можно воспользоваться пунктом PEOPLE-OSINT под номером 10.

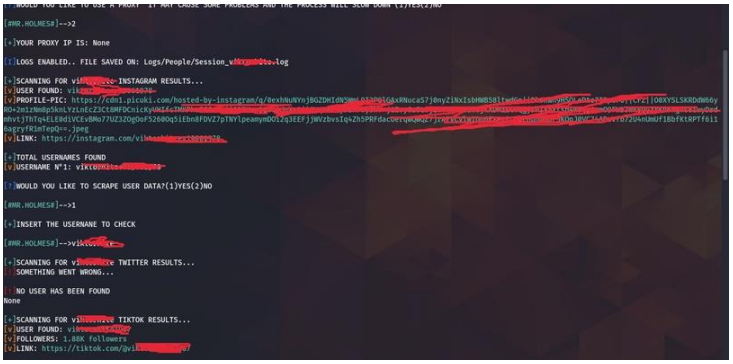


Рис. 7 «Поиск по фотографии»

**2) Подбор почты:**

Из вашего «Никнейма» можно получить данные о вашей почте, а т.к в современном мире большая часть авторизаций, регистраций и т.д, происходит именно через почту то как ИБ-специалист мы имеем огромный потенциал для получения информации о человеке.

Первым делом стоит проверить валидность почты Gmail. На валидность почту можно проверить в Mr.Holmes или другой утилитой которая для этого подходит.

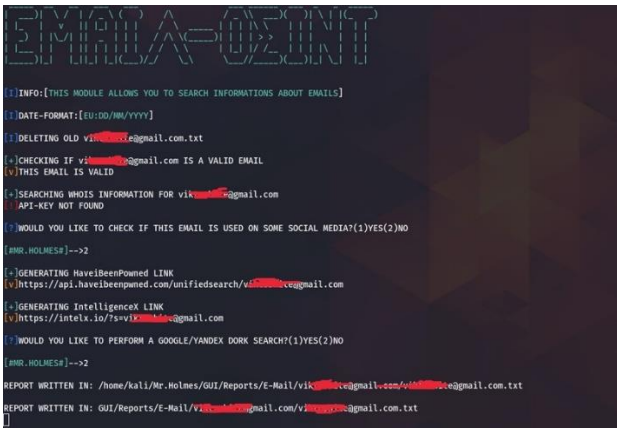


Рис. 8 «Проверка валидности почты»

Как мы можем наблюдать почта существует а значит мы можем позволить себе копать дальше и просмотреть на каких сервисах и сайтах она зарегистрирована.

- Ghunt

Ghunt - это инновационный инструмент, который позволяет вам получить доступ к разнообразной информации, связанной с gmail-адресами пользователей. С его помощью можно узнать не только имя владельца и его идентификаторы, но и просмотреть активные сервисы Google, такие как YouTube, Photos, Maps и другие. Кроме того, Ghunt предоставляет возможность получить данные о местоположении, содержимом Google документов, намеченных встречах в календаре и многом другом.

Заходим в аккаунт Google и при помощи специального плагина авторизуемся в нашем инструменте. И после чего производим поиск по интересующей нас электронной почте.

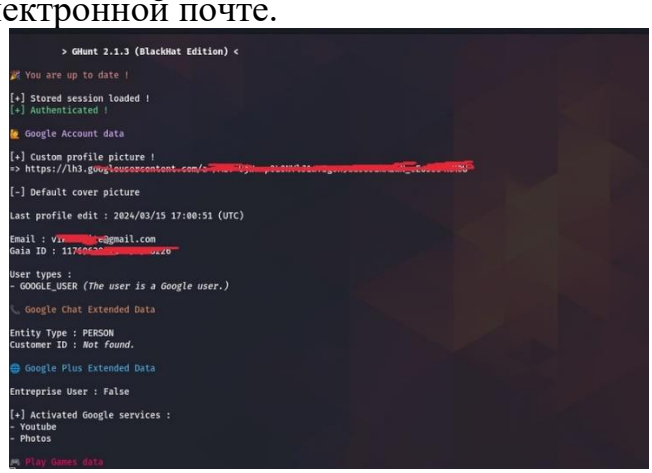


Рис. 8 «Поиск связанных с почтой Аккаунтов»

Как мы можем видеть в этот раз Ghunt выдал мало информации касательно почты но мы можем наблюдать на каких сервисах она была зарегистрирована.

**Заключение:**

В данной статье мы увидели, как легко и эффективно проводить поиск информации, используя только терминал. Этот пример показывает, что осуществление интеллектуальных расследований в цифровой среде не требует сложных программ и интерфейсов. Мы раскрываем новые возможности использования подобных методов в различных областях, таких как кибербезопасность, расследования преступлений, аналитика рынка и другие. Наш опыт наглядно иллюстрирует, что даже без специализированных инструментов можно достичь значительных результатов в анализе данных.

**Список литературы:**

1. Документация Mr.Holmes. [Электронный ресурс] URL: https://github.com/Lucksi/Mr.Holmes
2. Документация Maigret. [Электронный ресурс] URL: https://github.com/soxoj/maigret
3. Документация Ghunt. [Электронный ресурс] URL: https://github.com/mxrch/GHunt
4. Документация Kali Linux. [Электронный ресурс] URL: https://www.kali.org/docs/