ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

В течение многих лет исследователи занимаются разработкой методов распознавания лиц, однако данная проблема до сих пор остается актуальной. Это связано с тем, что условия съемки лиц могут быть разнообразными и изменчивыми: освещение, угол обзора, возраст, выражение лица и другие факторы могут сильно влиять на процесс распознавания. При проектировании систем распознавания лиц часто стараются ограничить эти факторы, однако основной интерес представляет именно распознавание лиц на фотографиях, сделанных в неконтролируемых условиях. Благодаря прогрессу в области глубокого машинного обучения и появлению больших наборов данных для тренировки систем, в последние годы наблюдается значительный прогресс в этой области.

Данный метод мультибиометрической идентификации позволяет повысить безопасность аутентификации путем объединения нескольких биометрических данных человека с помощью нейронных сетей, что в свою очередь обеспечивает быстродействие и достаточную точность обработки.

Список использованных источников

1. Кухарев Г.А., Каменская Е.И., Матвеев Ю.Н., Щеголева Н.Л. Методы обработки и распознавания изображений лиц в задачах биометрии. – М.: Политехника, 2013. – 416 с.

2. Галушкин А. И. Нейронные сети: основы теории. / А. И. Галушкин. – Москва : Горячая линия-Телеком, 2019. – 456 с. – ISBN 978-5-9912-0082-0

3. Рыбалко С. Использование OpenCV и Face Recognition в системах распознавания лиц на одноплатных компьютерах типа Raspberry Pi / С. Рыбалко // Evergreens.com.ua : электронный журнал. – URL: https://evergreens.com.ua/ru/articles/open-cv-face-recognition.html. – Дата публикации: 25.01.2021.

РАЗРАБОТКА ИНСТРУМЕНТА OSINT ДЛЯ АВТОМАТИЧЕСКОГО СБОРА ИНФОРМАЦИИ ИЗ ОБЩЕДОСТУПНЫХ ИСТОЧНИКОВ

Акылбек Бота Алтынбековна
akylbek.ba@mail.ru
Научный сотрудник Института теоретической математики
и научных вычислений ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Шахметова Г.Б.

OSINT - это набор методов и техник, которые позволяют эффективно использовать свободно доступные источники информации.[1] В области кибербезопасности и сбора разведывательных данных открытые источники информации (OSINT) представляют собой сбор, анализ и использование публично доступной информации из различных онлайн и офлайн источников. В отличие от традиционных методов разведки, которые полагаются на классифицированные или конфиденциальные данные, OSINT использует открыто доступную информацию для выявления инсайтов, оценки рисков и поддержки процессов принятия решений.

Инструменты OSINT служат нескольким целям и находят применение в различных областях, включая кибербезопасность, правоохранительную деятельность, корпоративную разведку и конкурентный анализ. Вот некоторые ключевые цели и применения инструментов OSINT:

1. **Угрозовая Разведка:** Инструменты OSINT позволяют специалистам по кибербезопасностимониторить и анализировать онлайн-активности, выявляя потенциальные угрозы, уязвимости и злоумышленников. Путем сбора информации с форумов, социальных сетей и других открытых источников, они помогают предотвратить атаки и защитить информацию.

2. **Исследование Конкурентов:** В бизнесе инструменты OSINT используются для анализа деятельности конкурентов, их стратегий маркетинга, отзывов клиентов и других

аспектов. Это позволяет компаниям принимать информированные решения, улучшать свои продукты и услуги и оставаться конкурентоспособными на рынке.

3. **Поиск Уязвимостей:** Пентестеры и специалисты по безопасности используют инструменты OSINT для исследования возможных уязвимостей в информационной инфраструктуре. Они могут использовать открытую информацию для поиска слабых мест в системах, софтвере и процессах, что помогает укрепить защиту и предотвратить возможные атаки.

4. **Расследование Преступлений:** Правоохранительные органы используют OSINT для расследования преступлений, идентификации подозреваемых и сбора доказательств. Путем анализа информации из социальных сетей, отчетов СМИ и других источников, они могут провести подробное расследование и привлечь виновных к ответственности.

Разведка с открытым исходным кодом (OSINT) - это дисциплина сбора разведывательных данных, которая включает сбор информации из открытых источников и ее анализ для получения полезных разведданных. Конкретный термин "открытый" относится к общедоступным источникам, в отличие от засекреченных источников. OSINT включает в себя широкий спектр информации и источников. Благодаря Интернету основную часть аналитических данных для прогнозирования можно получить из общедоступных, несекретных источников. Революция в информационных технологиях делает открытые источники более доступными, повсеместными и ценными, что позволяет получать открытые данные с меньшими затратами, чем когда-либо прежде. Фактически, мониторам больше не нужна дорогостоящая инфраструктура антенн для прослушивания радио, просмотра телевидения или сбора текстовых данных из интернет-газет и журналов [2].

В мире кибербезопасности и сбора разведывательных данных открытые источники информации (OSINT) являются неотъемлемой частью. Они позволяют получать доступ к обширной базе публичной информации из разнообразных источников, что помогает выявлять интересные факты, анализировать уязвимости и облегчать процесс принятия решений. Существует огромное количество различных инструментов, наиболее известные это:

Maltego представляет собой инструмент с графическим интерфейсом, который обеспечивает визуализацию и анализ данных. Этот инструмент предоставляет широкий спектр функций для сбора информации из различных источников, что делает его удобным инструментом для проведения исследований. Однако, бесплатная версия Maltego имеет некоторые ограничения по функционалу и количеству запросов.

Shodan - это поисковая система, специализирующаяся на обнаружении устройств и сервисов в Интернете. С помощью Shodan можно найти уязвимости и потенциальные угрозы в сети. Хотя этот инструмент предоставляет ценную информацию, доступ к его расширенным функциям может потребовать платной подписки.

Recon-ng - мощный инструмент для автоматизации сбора информации из различных источников. Он обладает большим количеством модулей для различных задач в области OSINT. Несмотря на свою мощность, некоторые пользователи могут столкнуться с ограничениями или нестабильной работой при использовании некоторых источников данных.

При разработке инструментов OSINT следует уделять приоритетное внимание интеграции правовых и этических гарантий для обеспечения соответствия требованиям и признания в обществе [3]. Исследования OSINT ценны для извлечения информации из открытых исходных данных, предлагая информацию о потенциальных деловых партнерах, клиентах, поставщиках и сотрудниках [4]. Кроме того, государственный сектор, особенно правоохранительные органы, признает важность методов OSINT для расширения возможностей расследования и эффективного противодействия криминальным угрозам [5].

Изучив основы работы различных инструментов OSINT, автор предлагает свой инструмент, Passive, который помогает в автоматизации сбора разнообразной информации из открытых источников. Passive предназначен для эффективного сбора следующих типов информации:

1. **Персональные данные:** Инструмент Passive способен автоматически собирать персональные данные, такие как имена, адреса, номера телефонов и электронные адреса, из различных открытых источников, включая каталоги и базы данных.

2. Passive проводит анализ исследуемого имени пользователя в социальных сетях, определяя его наличие и активность на популярных платформах, таких как Facebook, Twitter, LinkedIn, Instagram и других.

3. **Связи между данными:** Passive также способен автоматически связывать полученные данные между собой, создавая цельную картину информации о целевом объекте.

Предлагаемый инструмент OSINT разрабатывается для эффективного сбора и анализа открытой информации из различных источников. Основной целью инструмента является обеспечение возможности получения ценных данных для кибербезопасности, разведки и анализа конкурентов. Данный продукт состоит из двух модулей: Модуль распознавания IP – адресов и модуль проверки имен пользователей.

Продукт Passive написан на языке программирования Go (или Golang). Go представляет собой эффективный, современный и простой в использовании язык программирования, который обладает мощными инструментами для создания высокопроизводительных приложений.

Преимущества использования Go для разработки Passive включают в себя:

- Простоту и понятность синтаксиса, что облегчает разработку и поддержку кода.
- Высокую производительность и низкое потребление ресурсов, что важно для приложений, выполняющих большое количество запросов к различным источникам данных.
- Поддержку параллельных вычислений и конкурентности, что полезно для эффективного сбора информации из нескольких источников одновременно.
- Наличие обширной стандартной библиотеки, включающей инструменты для работы с сетью, обработки данных и создания веб-сервисов.

Модульпроверкииименпользователей:

- Анализирует введенные имена пользователя на наличие упоминаний в социальных сетях.
- Выводит сообщение, показывая в каких социальных сетях были выявлены учетные записи с такими именем, прилагая ссылку

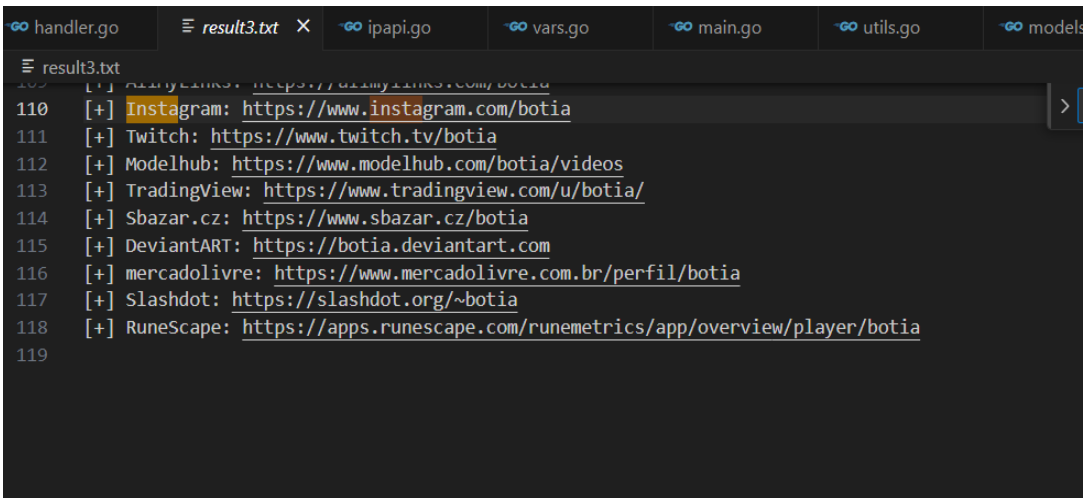
Далее представлен участок кода из функции Discord, которая выполняет проверку наличия пользователя в базе данных Discord:

```
funcDiscord(usernamestring) {
                                                                                jsonStr:=
[]byte(`{"username":"`+username+`","username":"asdsadsad","password":"q1e31e12r13*","invite":null,"co
nsent":true,"date_of_birth":"1973-05-
09","gift_code_sku_id":null,"captcha_key":null,"promotional_username_opt_in":false}`)

        client:=&http.Client{}
          r, err:=http.NewRequest("POST", utils.DiscordEndpoint, bytes.NewBuffer(jsonStr)) // URL-
encoded payload
        iferr!=nil {
           log.Fatal(err)
        }
        r.Header.Add("Content-Type", "application/json")
            r.Header.Add("User-Agent", "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36")
        r.Header.Add("X-Debug-Options", "bugReporterEnabled")

        res, err:=client.Do(r)
        iferr!=nil {
           log.Fatal(err)
        }
```

```
    deferres.Body.Close()
    ifres.StatusCode==400 {
      body, err:=io.ReadAll(res.Body)
      iferr!=nil {
        log.Fatal(err)
      }
      varresponsemodels.DiscordResponse
      json.Unmarshal(body, &response)
      iflen(response.Errors.Username.Errors) >0 {
        ifresponse.Errors.Username.Errors[0].Code=="username_ALREADY_REGISTERED" {
          utils.Social_result=append(utils.Social_result, "Discord \U0001f440")
        } else {
          utils.Social_result=append(utils.Social_result, "Discord [Not here!]")
        }
      } else {
        utils.Social_result=append(utils.Social_result, "Discord [Not here!]")
      }
    } elseifres.StatusCode==429 {
      utils.Social_result=append(utils.Social_result, "Discord [Rate limited!]")
    } else {
      utils.Social_result=append(utils.Social_result, "Discord [Couldn't check!]")
    }
  }

  funcgetCSRFToken() string {
    client:=&http.Client{}
    req, _:=http.NewRequest("GET", utils.InstagramCSRFEndpoint, nil)
      req.Header.Set("User-Agent", "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36")
    res, err:=client.Do(req)
    iferr!=nil {
      log.Fatal(err)
    }
    body, err:=io.ReadAll(res.Body)
    iferr!=nil {
      log.Fatal(err)
    }
    deferres.Body.Close()
    ifres.StatusCode==200 {
      re:=regexp.MustCompile(`(?m){\\"config\\":{\\"csrf_token\\":\\"(.*?)\\"`)
      match:=re.FindStringSubmatch(string(body))
      iflen(match) >0 {
        returnmatch[1]
      }
   }
   return""
  }
```

Этот участок кода выполняет POST-запрос к серверу Discord, передавая в теле запроса информацию о проверяемом пользователе. После получения ответа он анализирует статус ответа и соответствующим образом обрабатывает результат.

Результат работы данной функции:



1-рисунок. Результат работы инструмента в файле txt при вводных данных "botia"

В заключение можно сказать, что разработка инструмента OSINT для автоматического сбора информации из общедоступных источников представляет значимый шаг в области кибербезопасности и разведывательного анализа. Этот инструмент обладает способностью эффективно извлекать и анализировать различные виды данных из разнообразных онлайн-ресурсов, что позволяет специалистам получать ценные сведения для выявления угроз, оценки рисков и принятия обоснованных решений.

Автоматизация процесса сбора информации снижает временные и человеческие затраты, делая его более эффективным и масштабируемым. Разработанный инструмент способствует улучшению работы специалистов по кибербезопасности, аналитиков и расследователей, обеспечивая им возможность оперативного доступа к обширной базе данных для выявления угроз и решения сложных задач.

Таким образом, разработка инструмента OSINT для автоматического сбора информации из общедоступных источников имеет большой потенциал в области кибербезопасности и разведывательного анализа, и его использование может значительно усилить возможности специалистов по защите информации и обеспечить более надежную защиту цифровых активов.

Список использованных источников

1. Open Source Intelligence (OSINT): retour aux sources - Olivier Le Deuff, RayyaRoumanos

2. A multilanguage platform for Open Source Intelligence - N. Baldini, F. Neri, Massimo Pettoni

3. Design Science Research towards Privacy by Design in Maritime Surveillance ICT Systems - Rajamäki 2019 ISIJ

4. What is Open-Source Intelligence and How it Can Prevent Frauds -Chalicheemala,2022

Surveillance and falsification implications for open source intelligence investigationsBayer, Akhgar – 2015Commun. ACM

ОБЗОР МЕТОДОВ ОБНАРУЖЕНИЯ СТЕГАНОГРАФИИ В МУЛЬТИМЕДИЙНЫХ ФАЙЛАХ

Асанов Әділбек Жанболатұлы
asanovadilbek66@gmail.com
Магистрант ЕНУ имени Л.Н. Гумилева, факультета информационных технологий, кафедра информационной безопасности, специальности «Системы информационной безопасности», Астана, Казахстан.