Группа: БСБО-03-22

Студенты: Бердникова Екатерина, Денисенко Софья, Анисифоров Евгений

OSINT (Open Source Intelligence) — это методология, которая использует общедоступные данные и информацию для извлечения и анализа различных сведений о людях, организациях и событиях.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Название, ссылка | Назначение | Условия использования |
| 1 | Maryam,  https://github.com/saeeddhqan/Maryam | OWASP Maryam — это модульный фреймворк с открытым исходным кодом, основанный на OSINT и сборе данных. Он предназначен для обеспечения надежной среды для быстрого и тщательного сбора данных из открытых источников и поисковых систем. | Maryam является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий |
| 2 | Snoop, https://github.com/snooppr/snoop | Snoop — это один из самых быстрых и мощных инструментов для поиска по имени. | Snoop является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий. |
| 3 | tookie-osint, https://github.com/Alfredredbird/tookie-osint | Tookie-osint имеет простой в использовании пользовательский интерфейс и очень прямолинеен. Основная идея Tookie-osint заключается в обнаружении имен пользователей, которые запрашиваются из входных данных. Он обнаруживает все учетные записи пользователей на разных веб-сайтах. | tookie-osint является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий. |
| 4 | earch4faces, https://search4faces.com/ | earch4faces - сервис поиска людей в интернете по фотографии. | Доступный всем онлайн сервис. Существуют различные способы взаимодействия с сервисом: веб-интерфейс и JSON-RPC АПИ. |
| 5 | 2gis, https://2gis.ru/moscow | Подходит для поиска какого-либо малого бизнеса, т.к. там отмечены даже границы помещений внутри здания, в котором сидит компания. | Сервис бесплатный и доступен всем. |
| 6 | Maltego, https://www.maltego.com/ | Maltego фокусируется на поиске конкретных взаимосвязей между активами, людьми, компаниями и доменами веб-сайтов. Большинство основных платформ OSINT предоставляют Maltego API. | Имеет 3 варианта начала использования:  1) Community, Бесплатная версия Community Edition  2) Professional, лучше всего подходит для индивидуальных исследователей и небольших групп за 5000 евро в год  3) Organization, лучше всего подходит для больших команд и государственных организаций (цены в открытом доступе нет) |
| 7 | DorkSearch, https://dorksearch.com/ | DorkSearch —инструмент для автоматизации и подсказок при составлении расширенных операторов поиска.  С его помощью можно находить конкретные уязвимости в безопасности и открытые данные. | Сервис бесплатный и доступен всем. |
| 8 | ScamSearch.io, https://scamsearch.io/ | ScamSearch - это бесплатная общедоступная база данных с информацией о мошенниках, включая их адреса электронной почты, номера телефонов, логины, веб-сайты и криптоадресы. | Сервис бесплатный и доступен всем. |
| 9 | Spiderfoot, https://github.com/smicallef/spiderfoot | Spiderfoot может извлекать данные из нескольких разных источников для сбора информации о различных онлайн-ресурсах. Он ищет IP-адреса, диапазоны CIDR, домены, поддомены, ASN, адреса электронной почты и номера телефонов. | Spiderfoot является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий. |
| 10 | Builtiwth, https://trends.builtwith.com/ | Builtiwth может определить, какие технологические стеки используются на различных веб-сайтах и платформах. | Сервис бесплатный и доступен всем. |
| 11 | Intelligence X, https://intelx.io/ | Intelligence X архивирует исторические версии веб-сайтов в Интернете, но также включает утечку данных, которые обычно удаляются довольно быстро. | Сервис можно использовать бесплатно, но тогда не будут доступны некоторые функции. Для большего функционала можно купить продукт за 2500, 5000, 7500 или за 20000 долларов в год |
| 12 | Grep.app, https://grep.app/ | Grep.app может выполнять поиск по всем репозиториям git | Сервис бесплатный и доступен всем. |
| 13 | theHarvester, https://github.com/laramies/theHarvester | theHarvester — это инструмент для сбора e-mail адресов, имён поддоменов, виртуальных хостов, открытых портов/банеров и имён работников из различных открытых источников (поисковые системы, сервера ключей pgp). | theHarvester является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий. |
| 14 | Searchcode, https://searchcode.com/ | Searchcode выполняет поиск в исходном коде, быстро находя полезные забытые фрагменты | Инструмент бесплатный и доступен всем. |
| 15 | Shodan, https://www.shodan.io/ | Shodan — поисковая система, позволяющая пользователям искать различные типы серверов (веб-камеры, маршрутизаторы, серверы и так далее), подключённых к сети Интернет, с использованием различных фильтров. | Для использования необходимо оформить подписку за 69, 359 или 1099 долларов в месяц. |
| 16 | Metagoofil, https://github.com/opsdisk/metagoofil | Metagoofil - инструмент для извлечения метаданных из документов, загруженных на веб-сайты. | Сервис бесплатный и доступен всем. |
| 17 | FOCA, https://github.com/ElevenPaths/FOCA | FOCA - инструмент для сбора информации о доменных именах, IP-адресах, электронных почтовых адресах и многое другое. | Сервис бесплатный и доступен всем. |
| 18 | Stalkface, https://stalkface.com/en/ | StalkFace — это инструмент, который показывает личные данные по URL-адресу профиля или фотографии в Facebook. | Сервис бесплатный и доступен всем. |
| 19 | GHunt, https://github.com/mxrch/GHunt | Ghunt — поиск информации о владельце Google аккаунта. | GHunt можно использовать без предварительных условий. |
| 20 | Nmap, https://nmap.org/ | Nmap — один из самых популярных сетевых сканеров, который используется для сканирования сетей и портов. Его интеграция с OSINT помогает собирать данные о сетевой инфраструктуре и выявлять уязвимости. | Nmap является открытым исходным кодом разведки (OSINT), поэтому его можно легко использовать без предварительных условий. |

**Выявление 15 наиболее эффективных инструментов OSINT на основе их преимуществ/недостатков и актуальности.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Название, ссылка | Назначение | Условия использования | Работа инструмента | Выявленные преимущества | Выявленны е недостатки |
| 1 | Maryam,  https://github.com/saeeddhqan/Maryam | OWASP Maryam — это модульный фреймворк. Он предназначен для обеспечения надежной среды для быстрого и тщательного сбора данных из открытых источников и поисковых систем. | Открытый исходный код. | + | - Грамотный и структурированный сбор информации из данных. Фреймворк собирает данные систематическим образом.  - Возможность найти файлы документов (PDF-файлы, текстовые файлы и т. д.). Для этого используется модуль docs\_search.  - Возможность перебрать DNS-записи с помощью модуля dnsbrute.  - Поиск информации на сайте (Regex-поиск) с помощью модуля crawl\_pages. | - Инструмент требует, чтобы в системе был установлен Python, поскольку он основан на нём.  - При многократном использовании функции Maryam поисковые системы могут определить бота и выдать ошибки CAPTCHA. |
| 2 | Snoop, https://github.com/snooppr/snoop | Snoop — это один из самых быстрых и мощных инструментов для поиска по имени. | Открытый исходный код. | + | - Расширенная база данных.  В полной версии инструмент выслеживает наличие пользователя на более чем 3700 интернет-ресурсах.  - Ускоренный поиск. При скорости интернет-соединения не менее 12 Мбит/с поиск по имени пользователя в полной базе Snoop в quick-режиме занимает менее минуты.  - Простой функционал. Пользователь скачивает софт, указывает цель и получает результат | - Ограниченная лицензия. Код написан на языке Python и распространяется под лицензией, ограничивающей применение только для личного пользования.  - Проблемы с некоторыми веб-сайтами. Например, если на них отсутствуют закрывающие теги, сертификаты не продлеваются, а хостинги вовремя не оплачиваются. |
| 3 | tookie-osint, https://github.com/Alfredredbird/tookie-osint | Основная идея Tookie-osint заключается в обнаружении имен пользователей, которые запрашиваются из входных данных. Он обнаруживает все учетные записи пользователей на разных веб-сайтах. | Открытый исходный код. | + | - Простой в использовании интерфейс. Инструмент создан, чтобы помочь новым программистам или пентестерам войти в мир OSINT  - Высокая точность обнаружения учётных записей в социальных сетях — почти 80%. | Многие функции в разработке. |
| 4 | search4faces, https://search4faces.com/ | search4faces - сервис поиска людей в интернете по фотографии. | Сервис бесплатный и доступен всем. | + | - Быстрый поиск профилей в популярных соцсетях. Поддерживаются такие платформы, как «ВКонтакте», «Одноклассники», TikTok и другие.  - Простой интерфейс, не требующий специальных знаний.  - Обширная база данных русскоязычных социальных платформ. | - Отсутствие поиска по лицам на многих платформах социальных сетей (например, Facebook, Instagram и Twitter).  - Неактуальные базы данных (последняя была обновлена в 2022 году). |
| 5 | 2gis, https://2gis.ru/moscow | Подходит для поиска какого-либо малого бизнеса, т.к. там отмечены даже границы помещений внутри здания, в котором сидит компания. | Сервис бесплатный и доступен всем. | + | - Удобный поиск. Пользователи могут быстро находить нужные места и компании благодаря различным фильтрам.  - Подробная информация. 2GIS предоставляет сведения о компаниях, включая контактные данные, отзывы и оценки, что помогает принимать обоснованные решения. | - Неактуальность информации. База данных может не содержать всю необходимую информацию.  - Отсутствие некоторых организаций в базе. |
| 6 | Maltego, https://www.maltego.com/ | Maltego фокусируется на поиске конкретных взаимосвязей между активами, людьми, компаниями и доменами веб-сайтов. Большинство основных платформ OSINT предоставляют Maltego API. | Имеет 3 варианта начала использования:  1) Community, Бесплатная версия Community Edition  2) Professional, лучше всего подходит для индивидуальных исследователей и небольших групп за 5000 евро в год  3) Organization, лучше всего подходит для больших команд и государственных организаций (цены в открытом доступе нет) | + | - Платформа объединяет в себе множество инструментов для проведения OSINT-расследований. Это позволяет пользователям проводить комплексный анализ данных из различных источников, не переключаясь между разными приложениями и сервисами.  - Простота использования. Интуитивно понятный интерфейс и автоматизированные процессы делают Maltego доступным даже для новичков. Встроенные руководства и документация помогают быстро освоить основные функции.  - Широкие возможности анализа. Визуализация данных в виде графов позволяет легко обнаруживать скрытые взаимосвязи и структуры. Maltego предоставляет пользователям мощные инструменты для анализа больших объёмов данных, выявления паттернов и тенденций. | - Ограничения бесплатной версии. В Maltego Community Edition за один раз можно вывести только 12 объектов, при этом они выводятся случайным образом, а не по порядку. |
| 7 | DorkSearch, https://dorksearch.com/ | DorkSearch —инструмент для автоматизации и подсказок при составлении расширенных операторов поиска.  С его помощью можно находить конкретные уязвимости в безопасности и открытые данные. | Сервис бесплатный и доступен всем. | + | -Централизован ная база Google dorks. Помогает специалистам по безопасности находить релевантные запросы для оценок и разведки.  - Возможность создавать собственные запросы. Для этого есть встроенный конструктор, который позволяет комбинировать и создавать новые dorks.  - Настройка диапазона дат. Результаты поиска можно фильтровать по дате, чтобы находить релевантные данные.  - История поиска. Можно отслеживать прошлые запросы и легко экспортировать их. | - Необходи мость ответственного и этичного использования. Незаконное или злонамеренное применение инструмента может привести к юридическим последствиям. |
| 8 | ScamSearch.io, https://scamsearch.io/ | ScamSearch - это бесплатная общедоступная база данных с информацией о мошенниках, включая их адреса электронной почты, номера телефонов, логины, веб-сайты и криптоадресы. | Сервис бесплатный и доступен всем. | + | - Большая база данных с отчётами о мошенниках. В ней зарегистрировано около 10 миллионов мошенников, и их число увеличивается еженедельно.  - Простая панель поиска. Она позволяет искать имя пользователя, адрес электронной почты, крипто-адрес, псевдоним, настоящее имя или веб-сайт в базе данных.  - Мгновенный поиск. Панель поиска раскрывается и предлагает предложения, похожие на поисковый запрос. | - Отсутствие инструментов для продвинутого анализа. |
| 9 | Spiderfoot, https://github.com/smicallef/spiderfoot | Spiderfoot может извлекать данные из нескольких разных источников для сбора информации о различных онлайн-ресурсах. Он ищет IP-адреса, диапазоны CIDR, домены, поддомены, ASN, адреса электронной почты и номера телефонов. | Открытый исходный код. | + | - интеграция с практически всеми доступными источниками данных.  - использование ряда методов для анализа данных, что упрощает их навигацию.  - встроенный веб-сервер для чистого и интуитивно понятного веб-интерфейса, но также можно использовать через командную строку  - более 200 модулей  - YAML-конфигурируемый корреляционный механизм с 37 предопределёнными правилами  - экспорт и импорт ключей API в форматах CSV, JSON и GEXF.  - интеграция TOR для поиска в даркнете.  - возможность вызывать другие инструменты, такие как DNSTwist, Whatweb, Nmap и CMSeeK. | - Сложность первоначальной настройки. |
| 10 | Builtiwth, https://trends.builtwith.com/ | Builtiwth может определить, какие технологические стеки используются на различных веб-сайтах и платформах. | Сервис бесплатный и доступен всем. | + | - позволяет узнать, какие технологии и стратегии используют конкуренты.  - база данных содержит более двух миллионов активных магазинов электронной коммерции, 5000 веб-технологий и более 250 сайтов. | - высокая стоимость.  - риск получения неточных данных, которые могут нанести ущерб бизнесу. |
| 11 | Intelligence X, https://intelx.io/ | Intelligence X архивирует исторические версии веб-сайтов в Интернете, но также включает утечку данных, которые обычно удаляются довольно быстро. | Сервис можно использовать бесплатно, но тогда не будут доступны некоторые функции. Для большего функционала можно купить продукт за 2500, 5000, 7500 или за 20000 долларов в год | + | - Версионное хранилище интернета.  - Расширенная база поиска. Включает даркнет, данные Whois и другие источники.  - Инструменты для анализа данных. Есть возможности для анализа полученных данных, визуализации связей и поддержки при ведении расследований.  - Приватность и безопасность. Intelligence X акцентирует внимание на обеспечении конфиденциальности запросов и защите информации своих пользователей. | - высокая стоимость. |
| 12 | Grep.app, https://grep.app/ | Grep.app может выполнять поиск по всем репозиториям git | Сервис бесплатный и доступен всем. | + | - удобен для разработчиков.  - позволяет искать по точному вхождению и с помощью регулярных выражений.  - индексирует только 0,5 миллиона GitHub-репозиториев, что исключает много шума в результатах. | - малое количество данных для поиска, так как база репозиториев ещё не полностью проиндексирована. |
| 13 | theHarvester, https://github.com/laramies/theHarvester | theHarvester — это инструмент для сбора e-mail адресов, имён поддоменов, виртуальных хостов, открытых портов/банеров и имён работников из различных открытых источников (поисковые системы, сервера ключей pgp). | Открытый исходный код. | + | - Автоматизация сбора данных из многочисленных открытых источников, включая поисковые системы, DNS и различные API. Это экономит время и увеличивает объём собранных данных. | - Необходи мость этичного и легального использования. |
| 14 | Shodan, https://www.shodan.io/ | Shodan — поисковая система, позволяющая пользователям искать различные типы серверов (веб-камеры, маршрутизаторы, серверы и так далее), подключённых к сети Интернет, с использованием различных фильтров. | Для использования необходимо оформить подписку за 69, 359 или 1099 долларов в месяц. | + | - Детальная информация о сетевых устройствах. Инструмент позволяет находить устройства по различным критериям, включая IP-адрес, открытые порты, тип устройства, операционную систему и географическое расположение.  - Визуализация результатов. Функции Shodan Maps и Shodan Images позволяют визуализировать результаты поиска на карте и просматривать изображения с различных устройств, таких как веб-камеры и VNC-серверы.  - API для разработчиков. Shodan предоставляет API, который позволяет автоматизировать сбор данных и интеграцию с другими инструментами.  - Оценка безопасности сетей. Shodan Monitor позволяет отслеживать все устройства, доступные из Интернета в пределах сети, и получать уведомления в реальном времени при появлении новых уязвимых устройств. | - Ограничения бесплатной версии. Без регистрации можно просматривать только первые 10 результатов поисковой выдачи, с бесплатной регистрацией — 50. Неограниченный доступ к результатам поиска возможен только на условиях платной подписки.  - Угроза безопасности незащищённых устройств. Shodan позволяет находить незащищённые роутеры, IP-камеры и другие устройства, использующие установленные по умолчанию логины и пароли. |
| 15 | Nmap, https://nmap.org/ | Nmap — один из самых популярных сетевых сканеров, который используется для сканирования сетей и портов. Его интеграция с OSINT помогает собирать данные о сетевой инфраструктуре и выявлять уязвимости. | Открытый исходный код. | + | - гибкие настройки сканирования (настройка скорости, количества потоков, числа групп для сканирования и т. д.)  - точечное сканирование отдельных хостов.  - возможность параллельного сканирования.  -предопределён ные наборы скриптов для различных задач.  - вывод результатов в пяти различных форматах, включая XML, который можно импортировать в другие инструменты. | - при сканировании группы хостов данные о каком-либо хосте будут недоступны до тех пор, пока не окончится сканирование всей группы.  - при сканировании SYN-пакеты отправляются на целевой порт, и ожидается любой ответный пакет или наступление таймаута, если ответа нет.  - во время сканирования больших сетей с применением флагов для ускорения сканирования Nmap может пропускать открытые порты на хосте и выдавать false-negative результаты. |

**Топ 10 инструментов OSINT — Рейтинг**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Место | Название, ссылка | Назначение | Условия использования | Работа инструмента | Выявленные преимущества | Выявленные недостатки |
| 1 | Maryam (https://github.com/saeeddhqan/Maryam) | Модульный фреймворк для сбора данных из открытых источников и поисковых систем. | Бесплатно, требуется Python. | + | Структурированный сбор информации, поддержка множества модулей. | Требует Python, возможность CAPTCHA при интенсивном использовании. |
| 2 | Maltego (https://www.maltego.com/) | Анализ взаимосвязей между активами, людьми, компаниями и доменами. | Бесплатная версия (ограничена), платная версия от 5000 евро в год. | + | Графическое отображение взаимосвязей, комплексный анализ данных, удобный интерфейс. | Ограничения бесплатной версии, высокая стоимость полной версии. |
| 3 | Spiderfoot (https://github.com/smicallef/spiderfoot) | Автоматизированный сбор данных из множества источников, включая IP, домены, ASN и др. | Бесплатно, требуется настройка. | + | Интеграция более 200 модулей, поддержка TOR, экспорт данных в различных форматах. | Сложная первоначальная настройка. |
| 4 | Shodan (https://www.shodan.io/) | Поиск сетевых устройств и уязвимостей. | Платный (от $69 до $1099 в месяц). | + | Мощный анализ сетевых устройств, поддержка API, визуализация данных. | Ограничения бесплатной версии, высокая стоимость полной версии. |
| 5 | Nmap (https://nmap.org/) | Сканирование сетей и портов для выявления уязвимостей. | Бесплатно, с открытым исходным кодом. | + | Гибкие настройки сканирования, поддержка параллельного сканирования, интеграция с другими инструментами. | Возможны пропуски открытых портов при высокоскоростном сканировании. |
| 6 | theHarvester (https://github.com/laramies/theHarvester) | Сбор данных (e-mail, поддомены, IP и др.) из множества источников. | Бесплатно, с открытым исходным кодом. | + | Автоматизация сбора данных, широкий диапазон источников. | Требует внимательного и этичного использования. |
| 7 | DorkSearch (https://dorksearch.com/) | Автоматизация составления расширенных операторов поиска (Google Dorks). | Бесплатно. | + | Помогает находить уязвимости и открытые данные, настройка диапазона дат, история поиска. | Требует этичного использования, риск юридических последствий при неправильном применении. |
| 8 | **Grep.app** (<https://grep.app/>) | Поиск по всем репозиториям git, точный поиск и использование регулярных выражений. | Бесплатно. | + | Удобен для разработчиков, минимизирует шум в результатах поиска. | Ограниченная база данных, не полностью проиндексированы репозитории. |
| 9 | ScamSearch.io (https://scamsearch.io/) | Поиск информации о мошенниках (e-mail, телефоны, криптоадреса и др.). | Бесплатно. | + | Большая база данных, мгновенный поиск. | Отсутствие инструментов для продвинутого анализа. |
| 10 | search4faces (https://search4faces.com/) | Поиск людей по фотографиям в социальных сетях. | Бесплатно. | + | Быстрый поиск в русскоязычных соцсетях, простой интерфейс. | Ограниченная база данных (не охватывает Facebook, Instagram, Twitter). |