Обзор

1. Для проведения сбора информации могут использоваться следующие методы: HUMINT (человеческий интеллект) и SIGINT (разведка сигналов). Используются утилиты MAltego & tinfoleak. Creepy. Tinfoleak использовался для сбора разного рода информации о жертве в Twitter'е для дальнейшего проведения атаки электронной почты.

2. Ш.Р. ДАВЛАТОВ, П.В. КУЧИНСКИЙ.СИСТЕМА СБОРА, АНАЛИЗА И ВИЗУАЛИЗАЦИИ ДАННЫХ ОБ УСТРОЙСТВАХ В СЕТИ ИНТЕРНЕТ/ ДОКЛАДЫ БГУИР. 2018, № 6 (116) - представлена система сбора, анализа и визуализации технической информации о подключенных устройствах к сети Интернет на базе платформы Censys.

3. Kanta, A., Coisel, I., & Scanlon, M. (2020). *A survey exploring open source Intelligence for smarter password cracking. Forensic Science International: Digital Investigation, 35, 301075. Использование тулзов OSINT для сбора информации о жертве.*

OSINT tools.

Function	Example Tools	Notable Usage
Automation Suites		
Maltego	https://www.paterva.com/	Entity transformations
theHarvester	https://github.com/laramies/theHarvester	OSINT gathering from multiple sources
Spiderfoot	spiderfoot.net	Scanning and monitoring open data sources
Twitter		
Twitter ID	gettwitterid.com/, tweeterid.com/	Unique numerical identifier
GPS enabled tweets/geocoding	geosocialfootprint.com/	Estimate of likely location based on social check-ins and geocoding
Sleeping Patterns	Sleeping time.org/	Sleeping Patterns of specific user
Record of profile changes	spoonbill.io/	Profile changes of specific users
Trending topics by location	Trends map.com/, tweetarchivist.com/	Tracking and analytics of users and topics
Sentiment analysis on hashtags	Social bearing.com/	Analytics on twitter usage including sentiment analysis and hashtag use
Visualisation of a twitter community	burrrd.com/	Insights including top connected users and top topics
Facebook		
Find Facebook ID	findmyfbid.in/, lookup-id.com/	Unique numerical identifier
Facebook Search	facebook.com/help/821153694683665	Facebook's inherent search tool
Who Posted What	whopostedwhat.com/	Search by date, location or Facebook UID. Works on Instagram too
Email		
Email Format	email-format.com/	Find the email format of a company
Email Permutator	Metric sparrow.com/toolkit/email-permutator/	Permutations of possible email addresses
H8mail	github.com/khast3x/h8mail	Password hunting tool that matches email addresses to leaked passwords
Reverse Email Lookup	Thats them.com/reverse-email-lookup	Returns useful information associated with an email address
We Leak Info	Weleak info.com/	Data breach search engine (search by email, username, password, hash, etc)

4. Gibson, H. (2016). *Acquisition and Preparation of Data for OSINT Investigations. Advanced Sciences and Technologies for Security Applications, 69–93. В статье предлагается использовать следующую методику для сбора информации о жертве с дальнейшим формированием специальной базы данных:*

- Сбор метаданных с вею-сайтов;
- Использование API;

- Использование метода SOCMINT (сбор данных в социальных сетях);

Maltego, CaseFile, Palentir & AxisPro

5. Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE Access, 8, 10282–10304. doi:10.1109/access.2020.2965257

Геопространственный анализ.

Семантический анализ.

Лингвистический анализ

6. Gibson, H., Ramwell, S., & Day, T. (2016). *Analysis, Interpretation and Validation of Open Source Data. Advanced Sciences and Technologies for Security Applications, 95–110.*

В этом документе описываются инструменты и подходы OSINT для поиска конфиденциальной информации о веб-приложении или сети любой организации. В документе описаны действия по сбору информации и способы защиты веб-приложения, организации или сети. Проблема заключалась в том, что, если мы обнаружим утечку такой информации, как учетные данные, токен, ключ API, мы можем легко получить авторизацию для учетной записи администратора / пользователя.

7. Open Source Intelligence Base Cyber Threat Inspection Framework for Critical Infrastructures. Авторы статьи приходят к мнению, что с развитием технологий всё сложнее применять технологию OSINT’а, но при этом не исключается возможность собирать данные по поводу критически важной инфраструктуры из-за несвоевременного обновления программного обеспечения. Для улучшения сбора информации о жертве предлагается обращать внимание на предложенную авторами алгоритм подготовки и применения тулзов информационной разведки.

8. Ivo Vacas, Ibéria Medeiros, Nuno Neve. Detecting Network Threats using OSINT Knowledge-based IDS 2018 14th European Dependable Computing Conference В статье представлен подход к улучшению возможностей

обнаружения IDS за счет использования данных аналитики угроз, собранных из каналов OSINT. Наш подход автоматически обрабатывает данные OSINT, агрегирует и коррелирует их для создания IoA. Впоследствии эти IoA используются для построения правил IDS и черного списка, которые затем устанавливаются в IDS. IDSoSint может обнаруживать незаконные действия, используя полученные знания, предупреждая о таких проблемах, как связь ботнетов и приложения удаленного доступа.

9. Martinez Monterrubio, S. M., Noain-Sánchez, A., Verdú Pérez, E., & González Crespo, R. (2021). Coronavirus fake news detection via MedOSINT check in health care official bulletins with CBR explanation: The way to find the real information source through OSINT, the verifier tool for official journals. Information Sciences, 574, 210–237

На основе данных, представленных из официальных баз данных ООН, предпримается поптыка через OSINT дипфейки о пандемии COVID-19.

10. Magalhães, A., & Magalhães, J. P. (2018). TExtractor: An OSINT Tool to Extract and Analyse Audio/Video Content. Lecture Notes in Electrical Engineering, 3–9.

Сбор и разведка данных: Maltego, Shodan and Censys

Для анализа берется три разных источника: аудиокнига, запись речи и саундтрек. Тулзы: Speech to Text, Web Speech API, Speechlogger and Speechnotes. Чтобы позволить сравнение извлеченного текста и исходного текста, мы использовали инструменты сравнения текста.