МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний технологічний університет
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Інститут комп`ютерної інженерії, автоматизації, робототехніки та програмування ім.П.Н.Платонова

XXIV Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

18-19 квітня 2024 р.

УДК 004.49

ІНСТРУМЕНТИ OSINT FRAMEWORK

ЖИВИЛО Є.О. (zhivilka@i.ua), **ДАМЯН М. Ю.** (kqmaksym1029@gmail.com)
Національний університет "Полтавська політехніка ім. Ю. Кондратюка"

Будь-яка кібератака починається з розвідки, причому спочатку з пасивного збору даних, а потім з їх аналізу. Якщо діяти "наосліп", то це значить плодити помилку за помилкою. Але використання OSINT це ще й спосіб відповіді зловмисникам; недаремно кажуть, що озброєний той, хто попереджений. Збір даних про себе чи компанію – це чудовий спосіб зрозуміти, які саме дані доступні хакерам.

Отже в роботі розглянуто деякі з основних інструментів OSINT, які є частиною цього процесу. Використовуючи їх правильно і осмислено, можна ефективно збирати дані з різних онлайн-джерел, включаючи соціальні мережі, пошукові системи, різні каталоги, реєстри і бази даних.

Загалом, розуміння процесів та алгоритмів, на яких побудований фреймворк OSINT, дозволяє більш структуровано та ефективно впроваджувати методи відкритої розвідки, а також збирати інформацію на основі відкритих джерел в Інтернеті.

Постановка проблеми. Сьогоднішнє життєве середовище суспільства знаходиться в новій ері існування – цифровій. Спілкування з рідними та друзями онлайн, здійснення покупок, пошук інформації, гра в ігри, планування маршрутів, все це неможливо відтворити без використання сучасних інформаційних технологій.

Сьогоднішня реальність така, що людям, які хочуть дізнатися про вас більше інформації, вже не потрібно збирати інформацію за різними матеріальними джерелами. Ви самі "викладете" на себе ті, чи інші світлини у соціальних мережах, оприлюдните коментарі під постами друзів і т.д. При цьому зловмиснику потрібно лише проаналізувати весь той контент, який ви даєте йому і структурувати його.

Щоб впевнено існувати та діяти в такому середовищі, ми повинні знати і вміти застосовувати на практиці основні принципи безпечної поведінки в ньому.

Виклад суті дослідження. Розробка дієвої стратегії захисту будь-якої комунікаційної системи чи мережі є доволі серйозним і відповідальним завданням. При цьому вагому роль відіграє інформація яка розповсюджена у відкритих джерелах, що до її активів в цілому, відповідно до всих її складових. OSINT – це ідеальне рішення щодо збору даних з відкритих джерел. Одночасно це є навичкою і методом, які є обов'язковими для ефективної роботи будь якого спеціаліста сфери захисту інформації та кібербезпеки.

Таким чином, Open Source Intelligence – це набір інструментів і ресурсів, спрямованих на виявлення потенційних кібервразливостей у комунікаційних системах організації/компанії, а також на пошук прогалин у політиці безпеки, незалежно від того, чи йдеться про захист корпоративної мережі, або перевірку її на вразливості. Можна сказати, що інструменти платформи зосереджені на проактивних заходах з виявлення та стримування загальних кіберризиків.

За цих обставин основною функцією, доступною через офіційний веб-сайт, є компіляція загальнодоступної інформації з різних онлайн-джерел. Фреймоврк включає понад 150 ресурсів що розділені на 32 категорії. На додаток, кожна категорія містить від 1 до 5 підкатегорії в яких міститься посилання на інструмент пов'язаний з назвою розділу.

Структурований за системною методологією OSINT Framework класифікує зібрану інформацію відповідно до:

- джерела;
- актуальності;
- типу;
- контексту.

За своєю суттю OSINT Framework зосереджується на використанні безкоштовної низки інструментів і методів для аналізу відкритих даних. Нижче пропонується розглянути декілька потужних інструментів фреймворк Open Source Intelligence, а саме:

- Osintgram – цей інструмент знаходиться в категорії "Social Networks", в підкатегорії "Instagram". Дане програмне забезпечення збирає інформацію про особу в соціальній мережі Instagram використовуючи нікнейм цілі. Дана утиліта візуалізує аналіз активності та публікацій користувачів.

- theHarvester – інструмент знаходиться в категорії "Email Address", в підкатегорії "Emails Search". Ця утиліта збирає інформацію про електронні адреси, домени, піддомени тощо.

- Shodan – пошукова система знаходиться в категорії "IP & MAC Address", в підкатегорії "Host/Port Discovery". Даний інструмент виконує пошук за допомогою IP-адреси, домену або ключовим словам, які можуть бути в банерах, заголовках тощо.

- Maltego – розташований в категорії "Tools". Цей візуальний аналітичний інструмент для збору та аналізу великих обсягів даних між різними об'єктами, такими як люди, організації, місця, домени, IP-адреси та інше. Основна мета даного інструмента це надання допомоги користувачам зрозуміти, взаємозв'язки різних об'єктів та їх ідентифікація.

- Photon – знаходиться в категорії "Tools", в підкатегорії "OSINT Automation". Це інструмент для вилучення URL-адрес з веб-сайтів та збору метаданих з них. Крім того, Photon може здійснювати видобування метаданих з отриманих URL-адрес, таких як заголовки, мова, кількість запитів, кодування тощо.

Отже, OSINT Framework – це складний та корисний інструмент, який використовує можливості загальнодоступних даних для збору розвідувальної інформації. Використовується не тільки у військовій розвідці, а також в різних секторах будь-якої держави, таких як уряд, правоохоронні органи та корпоративний світ. Враховуючи етичні міркування, що лежать в його основі, і здатність об'єднуватися з іншими методами кібербезпеки, звичайно, що OSINT є незамінним інструментом сьогодення.

Висновки. Сучасні пошукові системи орієнтовані на отримання конфіденційних даних за територіальним розподілом. В цілому їх інструменти та ресурси надають локалізовані та адаптовані результати пошуку, що відповідають їхнім відповідним регіонам. Розглядаючи фреймворк Open Source Intelligence необхідно зробити наголос, що це складна та змістовно наповнена онлайн платформа з доволі дієвими інструментами та ресурсами.

В зазначеній роботі була розглянута лише частина інструментів з різних категорій ресурсів згрупованих Джастіном Нордіном. Але при цьому їх можна об'єднати з іншими методами кібербезпеки, що дозволить обґрунтовано прийняти рішення і здійснити превентивні упереджувальні заходи реагуючи на потенційні кіберзагрози.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. GitHub – Datalux/Osintgram: Osintgram is a OSINT tool on Instagram. It offers an interactive shell to perform analysis on Instagram account of any users by its nickname // https://github.com/Datalux/Osintgram.

2. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security // Vol. 5 (13 (125)) (2023): Eastern-European Journal of Enterprise Technologies. P. 65–76.

3. GitHub – laramies/theHarvester: E-mails, subdomains and names Harvester – OSINT // https://github.com/laramies/theHarvester.

4. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems // 5(9-119) (2022): Eastern-European Journal of Enterprise Technologies. P. 34–44.