УДК 004.056 DOI: 10.31673/2412-4338.2023.015360

Запорожченко М.М.
Державний університет телекомунікацій, Київ

МІСЦЕ OSINT В ЖИТТЄВОМУ ЦИКЛІ КІБЕРАТАКИ

Анотація. *Протягом останніх років можна спостерігати тенденцію до зростання кількості кібератак на організації та окремих користувачів. В багатьох випадках ключовим фактором реалізації інциденту інформаційної безпеки є проведення зловмисником ефективної підготовки до кібератаки: вибір цілі, розвідка, тобто отримання будь-якої інформації, яка може знадобитися при плануванні атаки, озброєння на основі виявлених механізмів захисту, використовуваного програмного та апаратного забезпечення тощо, а також доставка, тобто вибір способу, яким чином шкідливе програмне забезпечення попаде до жертви і які кроки знадобляться для його подальшої активації. Володіння значною кількістю важливої та критичної для організації з точки зору забезпечення безпеки інформацією надає зловмиснику можливість вибору оптимального сценарію атаки і значно підвищує шанси на її успіх.*

Проблема полягає в тому, що сучасні методи та інструменти OSINT дозволяють знайти майже будь-яку інформацію, яка захищена неналежним чином, що значно підвищує ризики особливо для організацій, яким важко контролювати всю інформацію, яка публікується її співробітниками в соціальних мережах, розкривається на інтерв'ю чи випадково потрапляє до Інтернету. Втім, більшість інструментів для розвідки доступні не лише зловмисникам, тому етичні хакери та пентестери також можуть використовувати інструменти OSINT для перевірки вразливих місць організації та вдосконалення її захисту, до того, як цими вразливостями скористаються зловмисники.

В статті досліджені основні методи розвідки на основі відкритих джерел, розглянуто найбільш поширені та найчастіше використовувані інструменти OSINT, проведено опис життєвого циклу кібератаки та визначено етапи, які потребують застосування інструментів OSINT при проведенні аудиту інформаційної безпеки організації та тестів на проникнення.

Ключові слова: *кібербезпека; соціальна інженерія; OSINT; життєвий цикл кібератаки; розвідка; тестування на проникнення.*

Zaporozhchenko M.M.
State University of Telecommunications, Kyiv

THE PLACE OF OSINT IN THE CYBER KILL CHAIN

Abstract. *In recent years, there has been a trend towards an increase in the number of cyber attacks on organizations and individual users. In many cases, a key factor in the implementation of an information security incident is the attacker's effective preparation for a cyber attack: target selection, reconnaissance, i.e. obtaining any information that may be needed when planning an attack, weaponization based on discovered defense mechanisms, software and hardware, etc. and delivery, i.e. choosing how the malware will reach the victim and what steps will be required to activate it further. Having a significant amount of important and critical information for the organization from the point of view of ensuring security provides the attacker with the opportunity to choose the optimal attack scenario and significantly increases the chances of its success.*

The problem is that today's OSINT methods and tools allow you to find almost any information that is not protected in a real way, which significantly increases the risks, especially for organizations

that find it difficult to control all the information that their employees post on social networks, disclose in interviews or accidentally enters the Internet. However, most intelligence tools are not only available to attackers, so ethical hackers and penetration testers can also use OSINT tools to examine an organization's vulnerabilities and improve its defenses before attackers exploit those vulnerabilities.

The article examines the main methods of intelligence based on open sources, considers the most common and most often used OSINT tools, describes the life cycle of a cyber attack and defines the stages that require the use of OSINT tools when conducting an audit of the organization's information security and penetration tests.

Keywords: *cyber security; social engineering; OSINT; Cyber Kill Chain; reconnaissance; penetration testing.*

1. Постановка проблеми

Будь-яка кібератака починаються з вибору зловмисником цілі – компанії чи особи, стосовно якої буде проведена подальша атака, і пошуку інформації про неї. Для зловмисників від того, наскільки якісно було проведено розвідку, залежить успішність атаки вцілому, для пентестерів – ефективність проведення тестів на проникнення, а також ефективність відпрацювання окремих векторів атак (соціальна інженерія, брутфорс, атаки на Web-додатки тощо), що дозволить виявити вразливі місця і впровадити контрзаходи для вдосконалення системи захисту [1].

У контексті кібербезпеки OSINT найчастіше застосовується для збору публічних даних про компанію з відкритих джерел, причому до таких даних відноситься не тільки електронна пошта співробітників, але й інформація про IP-адреси, DNS-імена, домени та субдомени, зареєстровані за компанією, відкриті порти та сервіси на них, публічні експлойти до знайдених сервісів, наявні механізми безпеки, факти компрометації поштових адрес, конфіденційні документи тощо.

Через вдосконалення методів злому зростає кількість кіберінцидентів, від яких страждають організації та окремі користувачі мережі Інтернет. Завдяки доступності послуг типу Ransomware-as-a-Service або Phishing-as-a-Service, які не вимагають володіння широкими технічними знаннями, зростає і кількість кіберпорушників, а доступність інструментів OSINT дозволяє їм довгий час накопичувати інформацію про ціль і планувати кібератаку, залишаючись непоміченими. Це створює загрозу для організацій, більшість з яких навіть не здогадується про значну кількість інформації про неї, доступну в мережі.

Важливо визначити місце OSINT в процесі реалізації кібератаки – її життєвому циклі, а також дослідити інструменти, які можуть використовуватися для пошуку інформації по відкритим джерелам, оскільки вони є доволі ефективним способом попередити потенційні атаки за рахунок вчасного виявлення вразливих місць завдяки тестам на проникнення.

2. Аналіз останніх досліджень і публікацій

Завдяки стрімкому розвитку IT-технологій в області OSINT (розвідки по відкритим джерелам) відбуваються постійні зміни та вдосконалення. Загалом останні дослідження в даній галузі приділяють велику увагу різноманітним інструментам та методам, які використовуються для збору, фільтрації, аналізу та інтерпретації інформації з відкритих джерел.

Деякі з цих досліджень приділяють увагу етичним та юридичним питанням, пов’язаним з використанням відкритих джерел інформації в різних сферах, включаючи національну безпеку, медицину та охорону здоров'я, бізнес та маркетинг та ін., в той час як інші сфокусовані на розробці нових методів та технологій, таких як автоматичне розпізнавання обличчя, комп’ютерний зір та аналіз текстів природною мовою.

Ці інструменти можуть бути використані для аналізу та класифікації інформації з відкритих джерел, що дозволяє визначати тенденції та тренди, виявляти підозрілі активності та прогнозувати майбутні події.

До наукових розвідок, присвячених OSINT, можна віднести публікації авторів: Joseph Poppy [3], Pavan Kashyap, Vinesha Selvarajah [5], Rahul Awati [6], Isaac Odun-Ayo [8], Mike Elgan [9], Victoria Robert, Olumide Adeosun.

3. Мета і задачі дослідження

Метою дослідження є визначення ролі OSINT у життєвому циклі кібератаки, а також аналіз методів OSINT, які можуть бути використані при етичному хакінгу та при проведенні тестів на проникнення для визначення вразливих місць інформаційних систем організації.

4. Результати дослідження

Термін «життєвий цикл кібератаки» («cyber kill chain») ілюструє структуру успішної кібератаки, тобто фактично це процес, якому слідує зловмисник, від розвідки до досягнення своєї мети, будь то крадіжка даних чи запуск шкідливого програмного забезпечення. Вперше цей термін було запропоновано використовувати як частину моделі Intelligence Driven Defense для виявлення та попередження процесів кібервторгнення. В даній моделі визначаються кроки, які повинен здійснити зловмисник для успішної реалізації кібератаки. Ця модель також дозволяє зрозуміти, що для того, щоб розірвати ланцюжок кібератаки, достатньо заблокувати діяльність зловмисника на будь-якому з етапів, оскільки для успішної реалізації атаки він повинен пройти через всі етапи. Дана модель визначає такі основні етапи кібератаки: розвідка, підготовка, доставка, експлуатація, закріплення, отримання управління та виконання дій в системі жертви (рис. 1).

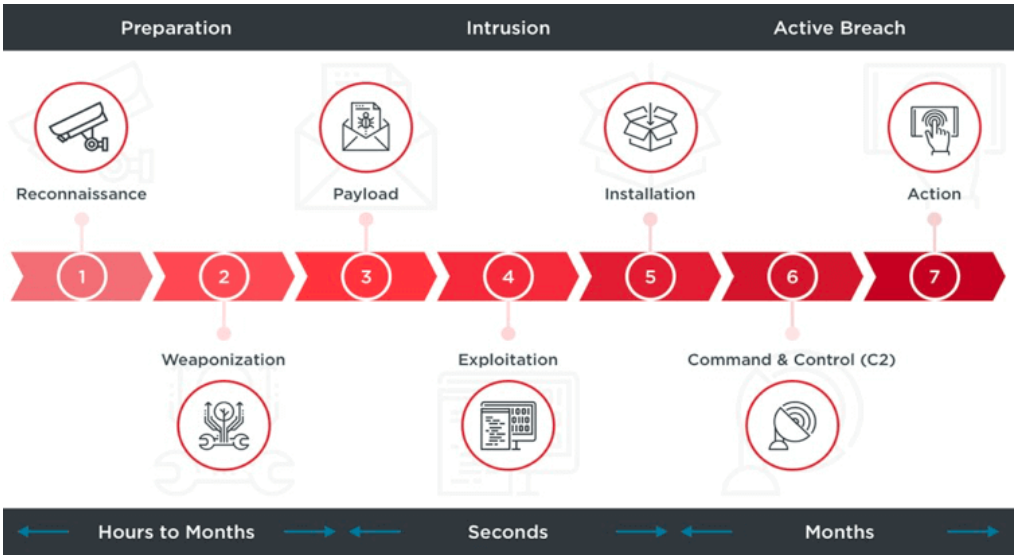

Рис. 1. Життєвий цикл кібератаки

Перші етапи моделі передбачають здебільшого підготовчу діяльність. Так, етап розвідки може включати дуже багато різноманітних методів, найбільш поширеним з яких є сканування, метою якого є виявлення відомих вразливостей, неправильної конфігурації програмних і апаратних засобів, застарілого програмного забезпечення та інших вразливих місць, які можуть допомогти у реалізації кібератаки. Також збирається вся доступна інформація про ціль, в тому числі визначаються особливості цільової організації, специфічні вимоги до галузі, до якої вона належить, які технології в ній використовуються, досліджується активність компанії та її співробітників в соціальних мережах, блогах, форумах тощо. Збір такої інформації призначений для того, щоб виявити найбільш вразливі місця системи захисту організації,

визначити найбільш ймовірні з точки зору успішності методи атаки і обрати з них оптимальні з точку зору необхідних для проведення кібератаки ресурсів та інвестицій [2].

Другий етап – етап вибору чи розробки інструментів для атаки. Сучасний стан кіберзлочинності значно полегшує роботу зловмисникам, оскільки якщо раніше вони повинні були володіти значною кількістю знань для написання зловмисного коду, його впровадження в інформаційну систему організації та подальшої крадіжки даних, то сьогодні всі інструменти для злому – готові ботнети, набори експлойтів, утиліти для модифікації шкідливих програм, модулі шифрування та інші – доступні для покупки в даркнеті, тобто навіть людина, яка не володіє спеціальними технічними навичками, може скористатися цими послугами. Існує навіть таке явище, як вимагання як послуга (RaaS, Ransomware as a Service), результатом якої є потрапляння шкідливого програмного забезпечення на комп'ютер жертви, шифрування даних та вимагання викупу за їх дешифровку. У разі, якщо зловмисник скористається такою послугою, він отримає готовий продукт і йому не потрібно буде нічого розробляти.

Також підвищує ймовірність злому той факт, що хакери підписані на оновлення програмного забезпечення і отримують патчі з виправленням вразливостей одні з перших. За допомогою реверс-інжинірингу вони виявляють, де розробниками була знайдена проблема, досліджують цю вразливість та або створюють новий експлойт безпосередньо під неї, або модифікують вже існуючий. Враховуючи те, що нерідко оновлення програмного забезпечення корпоративними та приватними користувачами здійснюється з затримкою, зловмисники мають час на дослідження оновлення, створення експлойту та проведення атаки на об'єкти із застарілим програмним забезпеченням.

Третім етапом є доставка шкідливого програмного забезпечення в мережу організації. Способом, який найчастіше використовується для цього, є відправлення співробітникам шкідливого електронного листа і використання прийомів соціальної інженерії для того, щоб у співробітника виникло бажання чи необхідність відкрити прикріплений до листа файл чи архів, перейти за посиланням, виконати певні вказані в листі дії. У разі проведення ефективної розвідки можна значно підвищити відгук на відправлені листи, замаскувавши його таким чином, що навіть підготовлений співробітник буде впевнений, що листа адресовано йому від легітимного джерела. Допомогти при створенні шкідливого електронного листа може будь-яка інформація: назва банку, в якому обслуговується співробітник організації, його хобі, інтереси, імена друзів та колег, робочі задачі, які він має виконувати, ЗМІ, які він читає тощо. Чим більше інформації буде знайдено про конкретного співробітника, тим більш правдоподібного листа можна написати.

Четвертим етапом життєвого циклу кібератаки є злом. Його сутність полягає в тому, що співробітник компанії або приватний користувач завантажує чи відкриває файл, програму або архів, прикріплений до електронного листа, або ж переходить за посиланням, тим самим він активує шкідливу програму і надає зловмиснику доступ та контроль над зараженою машиною.

П'ятим етапом є встановлення та розгортання шкідливого програмного забезпечення на уже контрольовану зловмисником машину. Даний етап передбачає завантаження зловмисником невистачаючих модулів та забезпечення постійної присутності в мережі. Таку активність зловмисника важко виявити, оскільки завантажуванні файли можуть маскуватися під легітимні, імітуючи повсякденну активність користувачів.

Шостим етапом є отримання зловмисником повного контролю над зараженими машинами та можливості управління: він може відправляти команди, завантажувати нові модулі для атаки, отримувати інформацію про комп'ютери та встановлене на них програмне забезпечення тощо. Зловмисник залежно від цілей, які він переслідує, може маскуватися в мережі достатньо довгий час для визначення подальших векторів атак, наприклад, зараження інших комп'ютерів, отримання доступу до інтернет-банкінгу, промислових систем, крадіжки даних тощо.

На сьомому етапі зловмисник досягає своїх цілей: завантажує необхідну йому інформацію, шифрує дані, починає шантажувати користувача чи організацію, отримує викуп за розшифровку даних, створює ботнети тощо.

Провести успішну атаку, тобто здійснити всі сім кроків життєвого циклу кібератаки, майже неможливо без ретельної підготовки, яка включає в себе етапи розвідки, озброєння та доставки шкідливого програмного забезпечення. Для цього можуть використовуватися різноманітні методи та інструменти OSINT. Зловмиснику не просто потрібно знайти сайт компанії чи сторінки деяких її співробітників в соціальних мережах, йому також необхідно застосувати всі навички розвідки, включаючи і спілкування, для маніпулювання співробітниками організації чи окремими користувачами, тобто використовувати прийоми соціальної інженерії [3].

Методи OSINT можна умовно поділити на дві категорії: пасивні й активні. До пасивних методів належать ті, які передбачають здійснення пошуку інформації лише по загальнодоступним джерелам і не потребують взаємодії з об'єктом атаки. До таких методів можна віднести:

- пошук відкритих персональних даних співробітників компанії у соціальних мережах, месенджерах і будь-яких інших відкритих джерелах;
- збір інформації про діяльність, структуру компанії, її працівників, керівництво, підрядників з відкритих пошукових систем;
- аналіз активності об'єкта у соціальних мережах, форумах, блогах та інших віртуальних платформах;
- перегляд збережених копій сайтів в пошукових системах для аналізу їх на предмет змін з поточною інформацією;
- отримання геолокаційних даних, використовуючи загальнодоступні сервіси, наприклад, Google Maps.

Перелічені методи являють собою лише малу частину пасивних методів розвідки, проте навіть вони у сукупності зі знаннями атакуючого та вмінням їх використовувати можуть сильно допомогти йому при проведенні підготовки до кібератаки [4].

Активні методи OSINT передбачають більш глибокий пошук та аналіз інформації, до того ж, деякі з них потребують контакту з цільової компанією або особою, що є доволі ризикованим заходом, оскільки якщо ціль щось запідозрить, весь цикл атаки може перерватися на етапі розвідки. Так, у випадку пасивних методів можна було знайти тільки загальну інформацію про ціль з відкритих джерел, а при застосуванні активних методів атакуючий повинен самостійно діставати інформацію про ціль, тому такі методи потребують більше часу, зусиль та ресурсів, проте і надають більш детальну інформацію. До активних методів розвідки можна віднести:

- збір даних на закритих платних ресурсах;
- застосування спеціальних сервісів та програм, які здійснюють активний вплив на об'єкт, наприклад, автоматично реєструються на сайті;
- застосування сервісів, які сканують файли, програми, сайти на наявність вірусів;
- створення сайтів-підробок, каналів у месенджерах з метою збору даних про користувачів;
- безпосередній контакт з ціллю.

Якщо можна зрозуміти з опису, пасивні методи являють собою легший шлях збору даних, а активні – більш складний та ризикований з точки зору виявлення спроби кібератаки.

Кожна група методів використовує певні інструменти для проведення розвідки. Серед найчастіше застосовуваних можна виділити Shodan, Maltego, Google Dorks, Metagoofil. Для успішної розвідки рекомендується використовувати комбінацію цих та багатьох інших інструментів.

Shodan – це одна з найбільш популярних пошукових систем для OSINT, яка індексує всі підключені до мережі обчислювальні пристрої, наприклад, маршрутизатори, веб-камери та камери відеоспостереження, сервери, IoT-девайси тощо та дозволяє знаходити їх через різноманітні пошукові запити та фільтри. Shodan охоплює значну частину адресного простору Ipv4 і намагається знайти кожний пристрій, підключений до Інтернету, та отримати його

«цифровий відбиток», використовуючи такі ж інструменти сканування, як і утиліта nmap. Сканери Shodan визначають, які мережеві служби надає кожний знайдений Інтернет-пристрій, а також збирають інформацію, яка може допомогти у ідентифікації використовуваного цими пристроями програмного та апаратного забезпечення. Вся ця інформація зберігається в базі даних Shodan, що дозволяє користувачам здійснювати пошук пристроїв, які використовують задане програмне забезпечення чи обладнання [5].

В першу чергу Shodan збирає інформацію про доступні служби веб-серверів (HTTP/HTTPS – порти 80, 8080, 443, 8443), FTP (порт 21), SSH (порт 22), Telnet (порт 23), SNMP (порт 161), IMAP (порт 143, 993), SMTP (порт 25), SIP (порт 5060), RTSP (порт 554).

Наявність такої інформації у вільному доступі може як принести користь, так і нанести шкоду. Наприклад, дослідники можуть використовувати цю інформацію для оцінки рівня розповсюдженості тих чи інших пристроїв, веб-інструментів, операційних систем або виявляти рівень проникнення Інтернету у будь-які населені пункти з точністю до кварталу. В той же час зловмисники, які створюють експлойт під конкретне програмне забезпечення, можуть використовувати інформацію з бази даних Shodan для пошуку потенційних жертв.

Maltego – інший потужний інструмент OSINT та комп'ютерної криміналістики, який використовується для пошуку інформації і формування графу на основі аналізу взаємозв'язків між людьми, організаціями, сайтами тощо. (рис. 2).

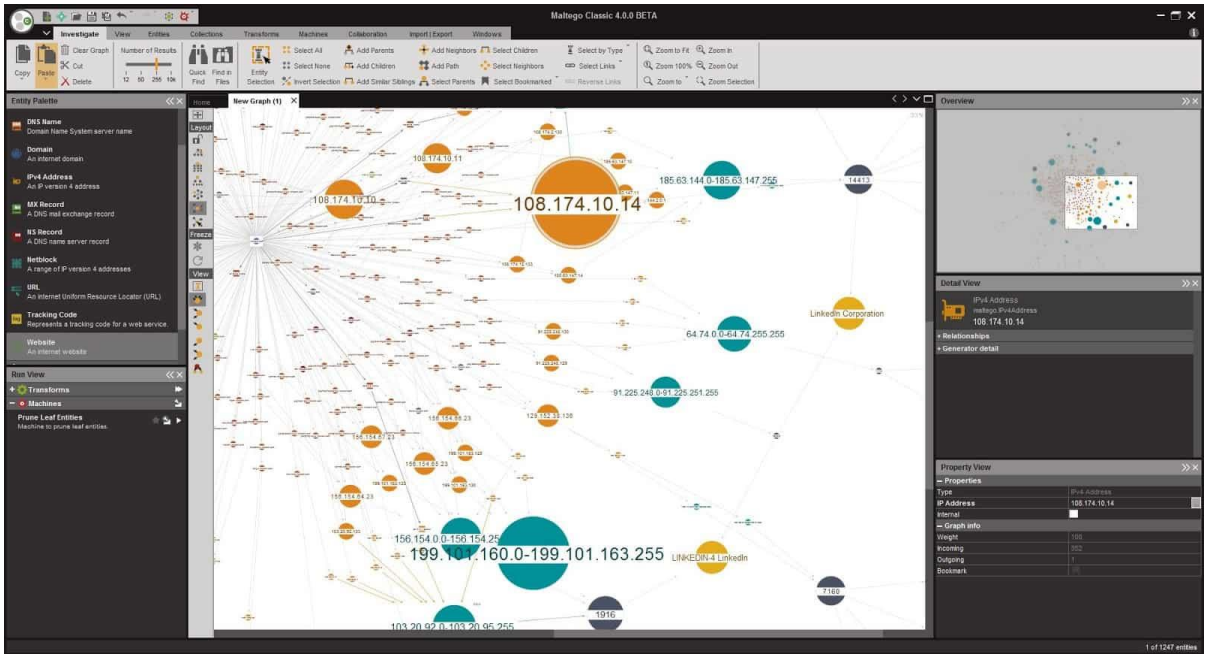

Рис. 2. Візуальна карта Maltego

Дане програмне забезпечення використовується в онлайн-розслідуваннях та розвідці для автоматизації процесу та пошуку зв'язків між частинами інформації, які розміщені в різних джерелах мережі Інтернет. Тобто, даний інструмент на основі заданих параметрів здійснює пошук інформації, збирає знайдені дані в схему, після чого будує логічні зв'язки між ними.

Google Dork Queries (GDQ) – це набір запитів, який дозволяє виявити те, що належним чином не сховано від пошукових роботів. Для пошуку інформації можна застосовувати багато команд, проте до найчастіше використовуваних належать [6]:

- inurl – дана команда вказує на те, що пошуковий запит повинен міститися в адресі сторінки чи сайту;
- intitle – дана команда вказує на те, що пошуковий запит повинен міститися в заголовку сторінки;
- site – дана команда здійснює пошук по конкретному заданому сайту;

- ext або filetype – дана команда здійснює пошук файлів конкретного типу (.docx, .pdf, .xls тощо).

За допомогою комбінації подібних команд можна знайти багато того, що може допомогти зловмисникам при реалізації кібератаки: проблеми сайтів, вразливості, навіть логіни та паролі користувачів та адміністраторів у разі їх неналежного захисту.

Metagoofil – це інструмент, який використовується для того, щоб витягувати інформацію з документів формату doc, xls, ppt, pdf, opd, ods, які знаходяться на цільовій сторінці чи на будь-якому загальнодоступному сайті. Даний інструмент використовує Google для пошуку документів, після чого завантажує їх та аналізує метадані, в результаті чого надає можливість знайти конфіденційні дані, наприклад, імена користувачів, електронні листи тощо, і показує шлях до файлів, що дозволяє дізнатися про операційну систему, мережеві імена, спільні ресурси та багато іншого.

Часто застосовується для проведення розвідки OSINT Framework [7], який містить в собі різноманітні сайти, утиліти, бази даних, які можуть бути корисні при розвідці (рис.3).

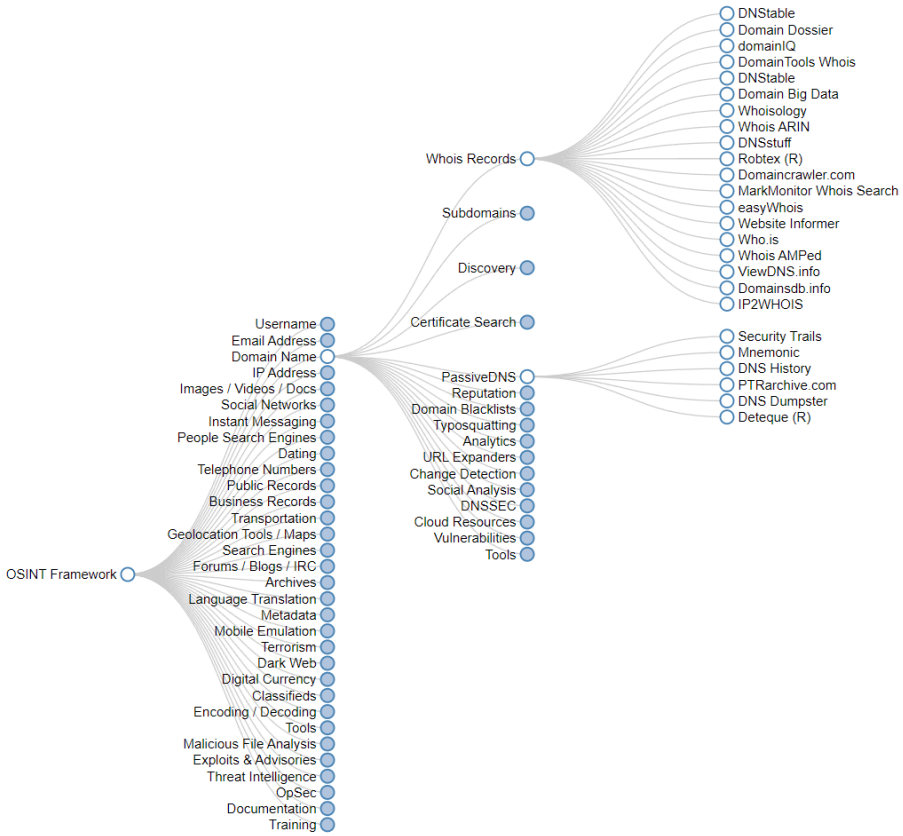

Рис. 3. OSINT Framework

5. Висновки і перспективи подальших досліджень

Всі перелічені вище інструменти та методи допомагають зловмисникам краще підготувати атаку на організацію, втім ці інструменти також доступні і спеціалістам з кібербезпеки. Періодичне проведення аудитів та тестів на проникнення може допомогти виявити потенційні недоліки мережевого периметру організації раніше, ніж ними скористаються зловмисники. А оскільки виявити кібератаку на етапі підготовки вкрай важко, необхідно подбати про те, щоб у разі проведення розвідки зловмисник отримав мінімальну кількість інформації про організацію та її співробітників, а також іншої інформації, яка тим чи іншим чином може посприяти успішній реалізації атаки.

Таким чином, застосування методів та інструментів OSINT при проведенні тестів на проникнення дозволяє захистити будь-яку область, починаючи з території компанії, підвищити анонімність в Інтернеті, захистити співробітників компанії від соціальної інженерії. Знання

того, яка інформація про компанію, що представляє ризик для забезпечення її інформаційної безпеки, наявна в загальнодоступних джерелах, є ключовим фактором для блокування етапу розвідки і, відповідно, повному попередженню кібератаки.

Подальше більш детальне дослідження сучасних інструментів OSINT є необхідним для отримання кращого розуміння того, як захистити свої інформаційні ресурси та протидіяти розвідці з боку кіберпорушників.

Список використаних джерел:

1. ENISA Threat Landscape. 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
2. Penetration Testing with Open-Source Intelligence (OSINT): Tips, Tools, and Techniques. URL: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-open-source-intelligence-osint/
3. Joseph Poppy. What is the cyber kill chain and why is it important? 2019. URL: https://www.bulletproof.co.uk/blog/what-is-the-cyber-kill-chain
4. OSINT: технологія збору та аналізу даних з відкритих джерел. 2022. URL: https://softlist.com.ua/articles/osint-tekhnologiya-sbora-i-analiza-dannyh-iz-otkrytyh-istochnikov/
5. Pavan Kashyap, Vinesha Selvarajah. Analysis of Different Methods of Reconnaissance 2021. URL: https://www.atlantis-press.com/article/125960844.pdf
6. Rahul Awati. Google dork query. 2022. URL: https://www.techtarget.com/whatis/definition/Google-dork-query
7. W. Mazurczyk. Cyber Reconnaissance Techniques 2021. URL: https://dl.acm.org/doi/pdf/10.1145/3418293
8. Isaac Odun-Ayo. Evaluating Common Reconnaissance Tools and Techniques for Information Gathering. 2021. URL: https://thescipub.com/pdf/jcssp.2022.103.115.pdf
9. Mike Elgan. Malicious Reconnaissance: What It Is and How To Stop It? 2022. URL: https://securityintelligence.com/articles/malicious-reconnaissance-protection-guide/
10. Разведка и сбор информации — обзор инструментария OSINT. 2020. URL: https://defcon.ru/penetration-testing/14235/

References:

1. ENISA Threat Landscape. 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
2. Penetration Testing with Open-Source Intelligence (OSINT): Tips, Tools, and Techniques. URL: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/penetration-testing-open-source-intelligence-osint/
3. Joseph Poppy. What is the cyber kill chain and why is it important? 2019. URL: https://www.bulletproof.co.uk/blog/what-is-the-cyber-kill-chain
4. OSINT: technology of data collection and analysis from open sources. 2022. URL: https://softlist.com.ua/articles/osint-tekhnologiya-sbora-i-analiza-dannyh-iz-otkrytyh-istochnikov/
5. Pavan Kashyap, Vinesha Selvarajah. Analysis of Different Methods of Reconnaissance 2021. URL: https://www.atlantis-press.com/article/125960844.pdf
6. Rahul Awati. Google dork query. 2022. URL: https://www.techtarget.com/whatis/definition/Google-dork-query
7. W. Mazurczyk. Cyber Reconnaissance Techniques 2021. URL: https://dl.acm.org/doi/pdf/10.1145/3418293
8. Isaac Odun-Ayo. Evaluating Common Reconnaissance Tools and Techniques for Information Gathering. 2021. URL: https://thescipub.com/pdf/jcssp.2022.103.115.pdf
9. Mike Elgan. Malicious Reconnaissance: What It Is and How To Stop It? 2022. URL: https://securityintelligence.com/articles/malicious-reconnaissance-protection-guide/
10. Reconnaissance and information gathering – OSINT toolkit review. 2020. URL: https://defcon.ru/penetration-testing/14235/