МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ПОЗДНЯКОВ ЕЛЬДАР РАФИСОВИЧ

Допускається до захисту:
Завідувач кафедри
інформаційних технологій,
к.т.н., доцент,
_____Нескородєва Т. В.
«__»_____20__р.

МЕТОДИКА ПІДБОРУ ІНСТРУМЕНТАРІЮ OSINT

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Науковий керівник:
Барибін О. І.,
к.т.н., доцент кафедри
інформаційних технологій

_____
(підпис)

Оцінка : _____ / _____ / _____
(бали/за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____
(підпис)

Вінниця 2021

АНОТАЦІЯ

Поздняков Е. Р. Методика підбору інструментарію OSINT. Спеціальність 125 Кібербезпека. Донецький національний університет імені Василя Стуса. Вінниця. 2021 рік.

У бакалаврській роботі на основі аналізу найпоширеніших інструментів OSINT запропонована методика оцінювання кожного інструменту, яка включає в себе 6 факторів. Кожному з факторів відведено від одного до 4 рівнів оцінок. В результаті оцінювання з'ясовано, що найбільший рейтинг для використання мають Google Dorks, Maltego, Spiderfoot, але використання того чи іншого інструментарію має бути засновано на оцінці за кожною складовою.

Ключові слова. OSINT, інструмент.

Табл. 1, Рис. 15, Бібліограф.: 27 найм.

Pozdniakov E.R. Methods of OSINT tool selection. Specialty 125 Cybersecurity. Vasyl Stus Donetsk National University. Vinnitsa. 2021.

In the bachelor's work on the basis of the analysis of the most widespread OSINT tools the technique of an estimation of each implant including 6 factors is offered. For every factor from to 4 assesment levels is allocated. As a result of the evaluation, it was found that the highest rating for the use of Google Dorks, Maltego, Spiderfoot, showed that the other was adapted to the evaluation of each component.

Keywords. OSINT, tool.

Tab. 1, Fig. 15, Bibliographer: 27 items.

ЗМІСТ

ВСТУП

Актуальність OSINT. В даний час існує диверсифікація послуг, що пропонуються в Інтернеті, що призвело до еволюції зростаючої маси цифрових даних [1]. До цих даних можна отримати доступ за допомогою інтерфейсів програмування програм (API) або різних служб, додатків тощо. Наприклад, люди, які користуються послугами, доступними в Інтернеті, для реєстрації сайтів, що цікавлять, подорожей, політичних чи релігійних належність, фотографій, серед інших джерел розкриття інформації, що мають явно публічний характер, можна знайти. Однак не всі знають, що значна частина цієї інформації відкрито відкрита і може використовуватися приватними особами чи організаціями з різними цілями [2]. Це означає, що вся інформація, опублікована в соціальних мережах, дискусійних форумах та групових чатах, серед інших джерел, є безкоштовною та доступною для всіх, враховуючи обмеження, які можуть застосовуватися [3]. Тим не менше, навіть коли знайдені великі обсяги даних, вони самі по собі вважаються неоціненим матеріалом, отриманим із будь-якого джерела. Проте, коли такі дані опрацьовуються та обробляються, набуваючи сенсу та корисності, вони перетворюються на інформацію. Крім того, якщо до цього додаються досвід, розуміння та кодифікація, така інформація стає знанням.

Після того, як це стає доступним людині, зацікавленій у тому, щоб допомогти процесу прийняття рішень, відбувається розвідка [4–6]. Діяльність збору та співвіднесення такої інформації за допомогою інструментів називається розвідкою з відкритим кодом (OSINT) [6]. Хоча ця робота зі збору та співвіднесення інформації не є нещодавньою діяльністю, можна навести ще деякі сучасні визначення OSINT. «Некласифікована інформація, яка була навмисно виявлено, дискриміновано, перегнано та розповсюджено серед вибраної аудиторії для вирішення конкретного питання »[7,8].

`«Збирати, обробляти та співвідносити публічну інформацію з відкритих джерел даних, таких як ЗМІ, соціальні мережі, форуми та блоги, державні державні дані, публікації чи комерційні дані» [9].

Мета бакалаврської роботи: запропонувати методику підбору інструментарію OSINT та рекомендації щодо його використання. Відповідно до мети можна сформулювати наступні завдання:

1. Визначити ключові аспекти OSINT, його методи, етапи, джерела.
2. Запропонувати перелік факторів, які впливають на прийняття рішення, щодо обрання інструментарію та визначити рівні їх оцінки.
3. Надати рекомендації для користувачів інструментів OSINT в залежності від його зручності.

Об’єктом бакалаврської роботи є OSINT інструментарій.

Предметом бакалаврської роботи є фактори, які впливають на прийняття рішень, щодо обрання інструментарію OSINT.

РОЗДІЛ 1 ОСНОВНІ ВІДОМОСТІ

1.1 Що таке OSINT

Інтелектуальна система з відкритим кодом (OSINT) - це дисципліна збору розвідувальних даних, яка полягає у зборі необроблених даних, доступних кожному із загальнодоступних джерел. Подальшою обробкою та аналізом ці необроблені дані перетворюються на діючі інтелектуальні знання; або іншими словами, в розвідувальний продукт, який є вирішальним сегментом розвідувальної діяльності. Кінцевий розвідувальний продукт, який найчастіше називають розвідувальною інформацією, водночас є вінцем складної якісної розвідувальної роботи, оскільки завдяки своєчасній класифікації та розподілу розвідувальних знань серед кінцевих користувачів процес прийняття рішень спрощується, робиться швидшим та простішим , не лише коли йдеться про різні політичні рішення, а й про різноманітні ділові рішення. Цим актом завершується традиційний розвідувальний процес. Попереднє - це отримання запиту, встановлення фактів, їх обробка та аналіз з подальшим початком нового циклу[10].

1.2 Чому OSINT важливий

OSINT має вирішальне значення у відстеженні цього інформаційного хаосу. Є три основні важливі завдання в рамках OSINT, які IT має виконати, і для задоволення цих потреб було розроблено широкий спектр інструментів OSINT. Більшість інструментів виконують усі три функції, хоча багато перевершуються в одній конкретній галузі.

Виявлення публічних активів

Їх найпоширеніша функція - допомагати IT-командам виявляти активи, що стоять перед громадськістю, і картографувати, якою інформацією володіє кожна,

що може сприяти появі потенційної поверхні атаки. Загалом, вони не намагаються шукати такі речі, як уразливості програм або проводити тестування на проникнення. Їх основна робота - це запис інформації, яку інформацію хтось міг би публічно знайти в активах компанії або про активи компанії, не вдаючись до злому.

Вторинною функцією, яку виконують деякі інструменти OSINT, є пошук відповідної інформації за межами організації, наприклад, у публікаціях у соціальних мережах або в доменах та місцях, які можуть бути поза жорстко визначеною мережею. Організації, які здійснили багато поглинань, об'єднавши IT-активи компанії, з якою вони об'єднуються, могли б знайти цю функцію дуже корисною. З огляду на надзвичайний ріст і популярність соціальних медіа, пошук конфіденційної інформації поза периметром компанії, мабуть, корисний майже для будь-якої групи.

Зібрати виявлену інформацію у діючу форму

Нарешті, деякі інструменти OSINT допомагають згрупувати та згрупувати всю виявлену інформацію в корисну та ефективну інформацію. Запуск сканування OSINT для великого підприємства може дати сотні тисяч результатів, особливо якщо включені як внутрішні, так і зовнішні активи. Поєднання всіх цих даних і можливість впоратися з найсерйознішими проблемами може бути надзвичайно корисним.

1.3 Етапи OSINT

Крок 1: Забезпеченість - OSINT Toolkit

Хороша стратегія OSINT повинна бути підтримана надійним набором інструментів для збору інтелекту. Групи безпеки, журналісти та слідчі дуже віддані своїм улюбленим інструментам онлайн-дослідження. Оскільки багато досліджень проводиться в Інтернеті, веб-інструменти є робочими конями для збору та організації даних для OSINT.

Основний набір інструментів OSINT повинен включати:

Доступ до традиційних джерел новин, таких як Google

Google - Карти, Пошук, Зображення

Платформа соціального моніторингу з можливостями геозонування -

Крок 2: Систематичність

Тут не дивно. Будь-який журналіст міг би сказати вам, що систематичний підхід до OSINT є першорядним для добре округленої та добре дослідженої історії.

Поінформованість - Ситуаційна та контекстна обізнаність є основою для уникнення хибного сприйняття та побудови неупередженої історії.

Формування гіпотези. Сформулюйте робочу гіпотезу, а потім спробуйте не просто довести, а й спростувати свою робочу гіпотезу та переглянути її протягом усього процесу.

Картування дискурсу. Зберіть якомога більше даних від якомога більшої кількості залучених людей, щоб ви могли наочно уявити та зрозуміти ситуацію в цілому.

Оцінка даних. Ніколи не приймайте думки однієї людини за номіналом. Виконайте кроки, що призвели до висновку, і ви повинні судити про те, чи правильні методологія та презентація.

Прозорість. По можливості цитуйте, звідки взялася ваша інформація та як ви дійшли висновків.

Крок 3: Розглядання геолокації

Геолокація може бути неймовірно цінним активом для вашої стратегії OSINT. Фотографії чи відеоролики, якими публічно діляться соціальні медіа, часто містять інформацію про місця розташування фотографій. Інструменти OSINT з можливостями геозонування дозволяють користувачам намалювати віртуальний периметр навколо своїх цікавих місць та отримувати уявлення, характерні для цього регіону. Ця розвідка, що базується на розташуванні, є важливою для дослідників та аналітиків і особливо корисна в процесі перевірки, яка веде нас до наступного кроку в повній стратегії OSINT

Крок 4: Перевірка

Найкращий спосіб перевірити те, що ви бачите в Інтернеті, - це щось на зразок перехресної перевірки з натовпу. Якщо багато людей повідомляють про те саме або подібне за подією, ви маєте вагомі підстави вважати, що події, про які повідомляється, відповідають дійсності.

Крок 5: Дотримування конфіденційності

При обладнанні набору інструментів OSINT важливо вибрати інструменти, які відповідають загальносвітовим стандартам конфіденційності. Деякі компанії зберігають загальнодоступні дані, що означає, що вони зберігають інформацію про користувачів соціальних мереж, навіть якщо користувачі видаляли або змінювали свою інформацію в мережі. Echosec - це одна платформа, яка збирає лише опубліковані загальнодоступні дані із соціальних мереж і не зберігає дані. [11].

1.4 Сторони, які зацікавлені в OSINT інформації

OSINT може бути корисним для різних людей. Ми коротко їх перелічимо та згадаємо, що спонукає кожного до пошуку ресурсів OSINT.

1. Уряд: Урядові органи, особливо військові відомства, вважаються найбільшим споживачем OSINT-джерел. Урядам потрібні джерела OSINT для різних цілей, таких як національна безпека, боротьба з тероризмом, кіберстеження терористів, розуміння поглядів вітчизняної та іноземної громадськості на різні теми, надання політикам необхідної інформації для впливу на їх внутрішню та зовнішню політику та використання іноземних ЗМІ, таких як телебачення, для отримання миттєві переклади різних подій, що відбуваються зовні.

2. Міжнародні організації: Міжнародні організації, такі як ООН, використовують джерела OSINT для підтримки миротворчих операцій по всьому світу. Гуманітарні організації, такі як Міжнародний Червоний Хрест, використовують джерела OSINT, щоб допомогти їм у їхніх зусиллях у час кризи

або катастрофи. Вони використовують розвідку OSINT для захисту свого ланцюжка поставок від терористичних груп шляхом аналізу сайтів соціальних мереж та програм обміну повідомленнями в Інтернеті для прогнозування майбутніх терористичних дій.

3. Правоохоронні органи: поліція використовує джерела OSINT для захисту громадян від зловживань, сексуального насильства, викрадення особистих даних та інших злочинів. Це можна зробити, відстежуючи у соціальних мережах цікаві ключові слова та фотографії, щоб запобігти злочинам до їх ескалації.

4. Бізнес-корпорації. Інформація - це сила, і корпорації використовують джерела OSINT для дослідження нових ринків, моніторингу діяльності конкурентів, планування маркетингової діяльності та прогнозування всього, що може вплинути на їх поточну діяльність та майбутнє зростання. Компанії також використовують інформацію OSINT для інших нефінансових цілей, таких як:

A. Боротися проти витоку даних, знаючи, що ділова конфіденційна інформація та вразливі місця безпеки їхніх мереж є причиною майбутніх кіберзагроз.

B. Створити свої стратегії розвідки загроз шляхом аналізу джерел OSINT як ззовні, так і всередині організації, а потім комбінуючи цю інформацію з іншою інформацією для реалізації ефективної політики управління кіберризиками, яка допомагає їм захищати свої фінансові інтереси, репутацію та клієнтську базу .

5. Тестери на проникнення та хакери / злочинні організації Black Hat: OSINT широко використовується хакерами та тестувальниками проникнення для збору інформації про конкретну ціль в Інтернеті. Це також вважається цінним інструментом для допомоги у здійсненні атак соціальної інженерії. Перший етап будь-якої методології тестування на проникнення починається з розвідки (іншими словами, з OSINT).

6. Люди, які підозрюють про конфіденційність: це звичайні люди, які, можливо, захочуть перевірити, як сторонні можуть проникнути в їх обчислювальні пристрої та що їхній провайдер знає про них. Вони також повинні знати рівень свого впливу в Інтернеті, щоб подолати будь-яку прогалину в безпеці

та видалити будь-які приватні дані, які могли бути ненавмисно опубліковані. OSINT - чудовий інструмент для того, щоб побачити, як ваша цифрова ідентичність виглядає у зовнішньому світі, дозволяючи вам зберігати свою приватність. Люди також можуть використовувати OSINT для боротьби з викраденням особистих даних, наприклад, у випадку, якщо хтось видає себе за вас.

7. Терористичні організації: Терористи використовують джерела OSINT для планування атак, збору інформації про цілі перед нападом на них (наприклад, при використанні супутникових зображень, таких як Карти Google для дослідження місця розташування цілі), залучення більшої кількості бійців, аналізуючи сайти в соціальних мережах, отримують військову інформацію, виявлену випадково уряди (наприклад, як будувати бомби) та поширюють свою пропаганду по всьому світу, використовуючи різні засоби масової інформації.

1.5 Джерела OSINT

Те, що дані з відкритим кодом існують, це не означає, що це обов'язково прямий доступ. Визначення даних, необхідних для просування розслідування, є першим кроком у визначенні, яке є найкращим джерелом та методом отримання таких даних. Крім того, доступ до потрібних даних, але наявність їх у непридатному форматі значно уповільнить наступну фазу аналізу, і, отже, розгляд способу повернення даних також є важливим фактором. У цьому розділі описано деякі процеси отримання різних типів даних з відкритим кодом.

1.5.1 Підтримка пошуків вручну

Іноді ручний пошук забирає занадто багато часу, вимагає занадто багато (людських) ресурсів, а набір результатів занадто широкий, щоб люди могли переглядати один сайт, наступний і наступний, поки вони не знайдуть потрібну

інформації. Налаштування веб-сканера, який іноді називають павуком, автоматизує цей процес, переходячи за цими посиланнями, або без розбору, або за деякими заздалегідь визначеними правилами.

Веб-сканери зазвичай починаються з ряду початкових початкових URL-адрес, з яких сканер почне. Потім сканер сканує сторінку, якщо потрібно, завантажує вміст, визначає нові URL-адреси на цій сторінці, а потім переходить до цих URL-адрес і повторює процес. Веб-сканери можуть бути налаштовані таким чином, щоб вони відповідали шаблону пошуку на глибину або ширину. Як правило, після широкого пошуку, обмеженого певною кількістю рівнів, швидше за все, можна досягти трохи кращих результатів, оскільки це обмежує сканер наближення до початкового списку URL-адрес. Подальші обмеження можуть бути застосовані до сканерів, такі як обмеження їх до певного списку доменів, забезпечення того, щоб сканери підпорядковувались файлу robots.txt і обмежували типи посилань, за якими можна переходити, наприклад, ігноруючи посилання, які переходять до JavaScript або інших файлів, що не належать до HTML. Крім того, якщо насіннєву URL-адресу ідентифікують із вмістом, який, ймовірно, зміниться з часом, може бути доцільним повторне сканування через певні проміжки часу. Залежно від типу контенту це може бути від одного разу на годину до одного разу на місяць або менше. Якщо цей збір даних буде позначений часом, це також забезпечить хорошу можливість дослідити, як конкретні дані змінюються з часом. Веб-сканери забезпечують хорошу початкову точку для розслідування OSINT, якщо слідчий знає, що в Інтернеті є значна кількість інформації про тему, яка їх цікавить, але вони не мають часу переходити за посиланнями вручну або читати кожну сторінку визначити, доречно це чи ні. Об’єднання веб-сканера з процесором, який визначає, чи буде сторінка релевантною, також є хорошим способом зменшити набір результатів та виключити посилання, які мають мало вмісту, пов’язаного з початковим пошуком. Такі методи, як категоризація та вилучення інформації, можуть допомогти визначити, чи може сторінка бути корисною для слідчого.

1.5.2 Веб-метадані

Метадані на веб-сторінках, іноді їх також називають мікроданими, структурованими соціальними даними або „розширеними фрагментами", надають інформацію про вміст веб-сторінки у визначеному форматі. Він є частиною того, що називається семантичною павутиною. Використання розмітки, наприклад, популяризованої schema.org, означає, що в HTML веб-сторінки є певні теги, що описують вміст цієї веб-сторінки. Це може бути настільки простим, як включення заголовка, автора та опису або більш складним, включаючи націнку для організацій, книг, серіалів, продуктів, місць розташування та багато іншого. Окрім „речей", націнка може також містити інформацію про дії, які можна здійснити на веб-сторінці. Twitter і Facebook створили власні версії метаданих, які можуть бути включені у веб-сторінки, відомі як Card Markup і Open Graph. Крім того, як HTML5, так і WAI-ARIA (спеціальна розмітка, спрямована на допомогу тим, хто використовує допоміжні технології для перегляду в Інтернеті) обидва мають покажчики, які допоможуть синтаксичним аналізаторам HTML зрозуміти (і машинно прочитати) вміст. Хоча ці націнки часто використовують маркетологи, намагаючись просувати свої сторінки ефективніше, ми також можемо подумати, що це означає для дослідника OSINT? По-перше, якщо під час веб-сканування повертається безліч веб-сторінок, кожна з цих сторінок матиме різні способи організації вмісту на сторінці, що ускладнює вилучення основного вмісту цієї сторінки без сторонніх відомостей. Використання цих тегів у процесі вилучення інформації дозволить надійно витягнути, щонайменше, точний заголовок, опис, автора та інше для статті, яку ви шукаєте. Звичайно, слідчий (і сканер) не завжди може здійснювати пошук на сайтах новин, що містять ці націнки; однак їх також можуть використовувати форуми та блоги

1.5.3 APIs

API або інтерфейси прикладного програмування - один із найпоширеніших способів отримання даних. Наприклад, для отримання даних результатів пошуку від Bing, їх API пошуку забезпечує автоматичний доступ до їх результатів за певним запитом. У Twitter ви можете використовувати їх REST або потоковий API, або ви можете використовувати графічний API Facebook. Pipl (шукач людей) також має власний API, і багато інших служб, що дозволяють доступ до даних, також забезпечують доступ через API. Доступ до API зазвичай вимагає попередньої реєстрації ключа API для цієї конкретної послуги. Тоді кожен ключ матиме обмеження, що обмежують обсяг даних, які ви можете запитувати або отримувати протягом певного періоду часу. Після закінчення цього періоду часу ви зможете запускати запити щодо API та отримувати інформацію, яка вас цікавить.

1.5.4 Відкриті дані

Протягом останніх 10 років рух до відкритих даних набирав темпів. Щось бентежить, відкриті дані - це лише підмножина даних з відкритим кодом, про які ми говоримо в OSINT. Зазвичай відкриті дані стають доступними, оскільки докладено зусиль (або навіть вимога) для публікації таких даних у машиночитаному форматі для підвищення прозорості в організаціях. Отже, відкриті дані можуть бути ще одним цінним ресурсом в арсеналі слідчого з відкритим кодом. Хоча, звичайно, велика частина цих даних є дуже агрегованою та анонімізованою, все ще можуть бути приховані корисні фрагменти. Такі дані, як місцеве самоврядування, витрачають дані, які малі компанії та індивідуальні підприємці мають контракти на послуги в межах місцевого самоврядування (та інших областей), які потім можна простежити до конкретних людей. Наприклад, Компанія House7 тепер публікує основні дані про компанію, яку кожен може

завантажити та здійснити пошук: для невеликих компаній адреса кореспонденції часто відповідає їхній домашній адресі, таким чином надаючи цю інформацію кожному, хто хоче її шукати. Також ми не повинні забувати про інші види відкритих даних, які можуть не мати безпосереднього відношення до розслідування, але допомагають зрозуміти середовище, яке оточує розслідування. Сюди входять географічні дані, такі як дані, опубліковані Geonames8 або Ordnance Survey у Великобританії, 9 які можна використовувати для перетворення назв місць у координати широти та довготи або навпаки. Такі дані, як погода та інші екологічні дані, супутник, вигляд вулиць та інші зображення також можуть бути корисними. Сайти для обміну фотографіями, такі як Flickr та Instagram, також можуть надавати корисні контекстні дані.

1.5.5 Соціальні мережі

Більше, ніж будь-який інший ресурс з відкритим кодом, дані, розміщені в соціальних мережах, можуть бути скарбницею інформації про певні події, людей та їхні стосунки. . Лондонські заворушення 2011 року підкреслили нездатність правоохоронних органів мати справу з інформацією, розміщеною в соціальних мережах, і той факт, що їй бракує робочої сили, процедур та процесів для вилучення даних із соціальних мереж та перетворення їх на дієвий інтелект, який би дозволив їм зрозуміти динаміку безладів і, отже, дозволив їм реагувати швидше та активніше (HMIC 2011). Як було підкреслено у цій справі (та інших великих кризових подіях, таких як терористичні атаки), ми зазначаємо, що навіть перший крок ефективного та ефективного збору даних із соціальних мереж не є тривіальним завданням. Ми коротко обговоримо деякі методи отримання даних із найпоширеніших сайтів соціальних мереж. Як обговорювалося вище, більшість сайтів соціальних мереж роблять (деякі) свої дані доступними через API. Такі торговельні посередники, як Gnip та Datasift, забезпечують більш повний доступ до даних соціальних мереж. Однак ці дані також мають необов’язково незначну

ціну. Дані також можна отримувати з соціальних мереж "на льоту", але це дуже багато даних, які доступні на даний момент і можуть бути не тими, що існували тиждень тому чи тиждень у майбутньому (Shein 2013). Отримання твітів із Twitter - це, мабуть, найкращий приклад цього ефемерного характеру даних у соціальних мережах, хоча тимчасовий період, протягом якого дані залишаються доступними (не платячи за це, - отже, це не справді ефемерно, як існує така служба, як Snapchat оскільки дані все ще доступні для тих, хто їх справді хоче), залежить від способу доступу до даних. Twitter пропонує дві основні служби API: REST API та Streaming API. API REST дозволяють користувачам взаємодіяти з Twitter за допомогою доступу та оновлення даних. Нас більше цікавить доступ до даних. API надають можливість завантажувати дані про друзів та послідовників конкретного користувача, твіти, які вони розмістили або позначили як обрані, та створені ними списки. Twitter також робить доступним API пошуку, за допомогою якого користувачі можуть завантажувати значну частину всіх твітів, використовуючи певне ключове слово або хештег. Потім ці твіти можна додатково звузити, використовуючи специфікації геолокацій, настроїв, періодів часу тощо. 15 Обмеження щодо API пошуку полягає в тому, що доступні лише твіти приблизно за останній тиждень.

Що стосується простого доступу до API пошуку, Twitter Archiver є доповненням до Google Sheets, яке дозволяє вводити пошукові запити та повертати їх у форматі таблиці з текстом твіту, користувачем та ім'ям користувача, датою та часом, коли він твідів id та деяку основну інформацію про користувача. Подібним чином, NodeXL17 - це доповнення для візуалізації мережі для Microsoft Excel, яке забезпечує функцію імпорту даних безпосередньо з API Twitter (Hansen et al. 2010). Такі інструменти можуть бути корисними для дослідника з відкритим кодом, оскільки вони мають низький бар’єр для входу та надають користувачеві дані у звичному форматі, які зазвичай можна легко імпортувати в інші інструменти.

Доступ до даних Facebook через їх графічний API набагато більш обмежений, ніж Twitter, з точки зору видів інформації, до яких можна отримати

доступ. Незважаючи на те, що інформація та публікації, зроблені на загальнодоступних сторінках та подіях, є легкодоступними, дані про друзів або з часової шкали конкретних людей не надаються, незалежно від того, встановлена цією інформацією в їх профілі загальнодоступність чи ні. Таким чином, слідчий отримує ширший обсяг даних шляхом допиту сторінки профілю користувача вручну та переходу від посилання до посилання. Однак захопити та керувати цією інформацією набагато складніше, ніж отримати доступ до неї через API, і, схоже, ще не існує рішень, які ефективно фіксують ці дані та залишаються в межах умов використання Facebook - сканування самого Facebook категорично заборонено (Warden 2010) . Крім того, кількість інформації, яку ви можете прочитати на сторінці людини у Facebook, залежить від того, ввійшли ви в службу чи ні. Кількість доступної інформації обмежується, коли ви не ввійшли в систему.

Незважаючи на те, що LinkedIn - це професійна соціальна мережа, інформація, яка розповсюджується на платформі, як правило, деталізується, як показано в ICWatch 20, де викладено особисту інформацію, доступну в Інтернеті тим, хто входить до спільноти розвідки. Отже, якщо ті, хто працює в розвідувальному співтоваристві, потенційно настільки розхитані щодо власного конфіденційності, то, ймовірно, багато хто з інших громадян також буде. Тому в певних ситуаціях LinkedIn також слід вважати цінним джерелом OSINT. Як ми бачимо, багата кількість інформації, доступна на сайтах соціальних медіа, та її відносна простота доступу при отриманні або принаймні перегляді цих даних робить її золотою шахтою з точки зору розслідувань.

1.5.6 Традиційні ЗМІ

Доступ до традиційних ЗМІ простіший, ніж будь-коли, тому що більшість газет та медіаорганізацій мають присутність в Інтернеті, де вони відтворюють статті, які, наприклад, можуть бути включені в газету того дня. Ці джерела новин

часто каталогізуються через RSS-канали, а деякі навіть мають власні API, такі як BBC, Guardian, Associated Press та New York Times, серед інших. Ця простота доступу, яка варіюється від великих організацій, таких як перераховані вище, до значно менших місцевих газет, які можуть містити більш конкретну інформацію, особливо важливу для слідчих, значно покращує швидкість розповсюдження інформації в будь-якій точці світу. Окрім індивідуального пошуку веб-сайтів, агрегатори новин, такі як European Media Monitor, Глобальна база даних про події, мову та тон (GDELT) та, в меншій мірі, BBC Monitoring забезпечують більш широкий доступ до баз даних з усього світу, які вже можуть бути були попередньо перекладені на англійську мову.

1.5.7 Платні дані та дані про згоду

Слово «відкритий» в інтелекту з відкритим кодом не слід плутати зі словом «вільний». Таким чином, цілком прийнятно розглядати джерела, які існують лише за платною стіною, як ключові відкриті джерела. Насправді, ці дані, зокрема, можуть дати перевагу слідчим, оскільки люди не можуть обов’язково контролювати або навіть знати про дані, які ці приватні компанії зберігають на них, і, отже, вони не можуть вживати заходів для їх видалення. Сюди входять такі дані, як «Світова перевірка» Thomson Reuters «World Check», яка збирає дані про осіб, які вважаються групами ризику, таких як підозрювані терористи або члени організованої злочинності.

Представлені дані - це підмножина платних даних. Згоджені бази даних, такі як ті, що надаються LexisNexis, GBG, 192.com та Experian, як правило, вимагають оплати за доступ до певних записів або передплати, яка дозволяє певну кількість пошукових запитів на місяць, наприклад. Ці бази даних можуть містити інформацію про компанії, людей, номери телефонів, адреси, адреси електронної пошти та іншу особисту інформацію, яку люди погодились зробити доступною. Потім ці бази даних можуть бути використані працівниками правоохоронних

органів для підтвердження або розширення знань, які вони можуть мати про особу, яка цікавить[14].

1.6 Загальні напрямки, в яких публікується OSINT

Для огляду загальних категорій або підрайон, в яких публікуються ресурси OSINT, були розглянуті метадані, надані семи різними базами даних (Taylor & Francis Group, Sage Journals, Sage Knowledge, Springer, Scopus, Web of Science та Redalyc). Згідно з цим оглядом, бази даних Taylor & Francis Group, Springer, Scopus та Web of Science мають більший охоплення в підрайонах публікації ресурсів OSINT. З іншого боку, Scopus має найбільшу кількість ресурсів, опублікованих у різних підрайонах OSINT. Рисунок 1 визначає галузі комп'ютерних наук та політики, а також міжнародні відносини як такі, що мають основну бібліографічну продукцію, показуючи, що OSINT базується на двох макросценаріях:

(a) у системному дослідженні для опису та перетворення інформації за допомогою програми комп'ютера системи; та

(b) у його використанні та застосуванні в глобальному контексті, враховуючи існуючу складну динаміку.

Однак, враховуючи сучасні умови наростання проблем безпеки та оборони, а також корисності, яку OSINT довів для вирішення цих проблем, як це видно з [15], яка є Агентством Європейського Союзу з підготовки правоохоронних органів, це не постановляється виявляється, що багато процесів, що виконуються в інших областях, не повністю документально задокументовані.

Рисунок 1 - Категорії публікацій OSINT

РОЗДІЛ 2 ІНСТРУМЕНТИ ТА МЕТОДИ OSINT

2.1 Фактори інструментів

Існує багато інструментів OSINT. У бакалаврській роботі буде розглянуто 10 найпопулярніших інструментів. На основі розглянутих інструментів OSINT можна розробити їх рейтинг. Для цього буде висунуто декілька факторів які будуть впливати на рейтинг цього інструменту. Буде розглянуто такі фактори:

1. Які операційні системи підтримує інструмент.
2. Складність використання.
3. Наявність графічного інтерфейсу.
4. Доступність.
5. Коли програмний продукт оновлювався востаннє.
6. Наскільки конфіденційною буде отримана інформація.

Далі для кожного фактору буде створена оцінка, за допомогою яких і буде визначено наскільки зручно використовувати інструмент.

1. Які операційні системи підтримує інструмент. Підтримка тільки однієї ОС(1), підтримка двох з трьох ОС(3), підтримка Windows, Linux, MacOS(5).

2. Складність використання. Потрібні навички роботи в мережі та програмування навички роботи в мережі та програмування (1), потрібні деякі технічні навички (3), досвідчений користувач комп’ютера (5), не потрібні технічні знання (6).

3. Наявність графічного інтерфейсу. Немає графічного інтерфейсу(1), є графічний інтерфейс(3).

4. Доступність. Не можна знайти у відкритій мережі(3), можна знайти у відкритій мережі(5).

5. Коли програмний продукт оновлювався востаннє. Більше двох років назад(2), від 1,5 до 2 років(4), від 1 до 1,5 років(6), від 0,5 до 1 року(8)б менше ніж 0,5 роки(10).

6. Наскільки конфіденційна буде отримана інформація. Розкрито мінімальні нечутливі дані (2), розкрито мінімальні критичні дані (4), розкрито великі нечутливі дані (6), розкрито великі критичні дані (7), усі дані розкрито (9)

2.2 Maltego

OSINT Tools aMaltego була створена Paterva і використовується правоохоронними органами, експертами з безпеки та соціальними інженерами для збору та розповсюдження інформації з відкритим кодом. Він може збирати великі обсяги інформації з різних джерел і використовувати різні методи для отримання графічних, легко помітних результатів. Maltego надає бібліотеку перетворень для дослідження даних з відкритим кодом і представляє ці дані у графічному форматі, який підходить для аналізу відносин та видобутку даних. Ці зміни вбудовані і можуть бути також змінені залежно від необхідності.

Maltego написаний на Java і працює з усіма операційними системами. Він поставляється попередньо встановленим у Kali Linux. Maltego широко використовується завдяки своїй приємній та зрозумілій моделі взаємозв'язку сутності, яка представляє всі відповідні деталі. Ключовою метою цього додатка є дослідження реальних відносин між людьми, веб-сторінок або доменів організацій, мереж та Інтернет-інфраструктури. Додаток може також зосередитись на зв’язку між обліковими записами соціальних мереж, API розвідки з відкритим кодом, приватними даними, що розміщуються самостійно, та вузлами комп’ютерних мереж. Завдяки інтеграціям від різних партнерів по обробці даних, Maltego розширює свій обсяг даних до неймовірної міри та методів [15].

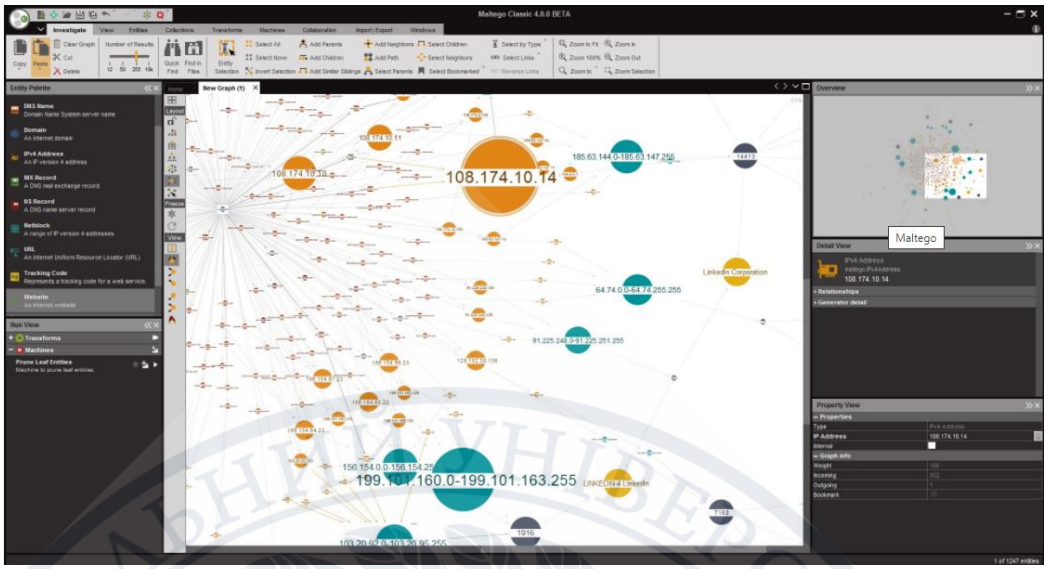

Рисунок 2 – Робоче вікно Maltego

Maltego - це програма, яка може бути використана для виявлення відносин та реальних зв'язків між:

- Людьми
- Групами людей (соціальні мережі)
- Компаніями
- Організаціями
- Веб-сайтами

Інтернет-інфраструктури, такі як:

  - Доменами
  - DNS іменами
  - Мережевими блоками
  - IP адресами

- Факторами
- Аффілірованості
- Документами та файлами
- Ці об'єкти зв'язуються на основі розробок за відкритим джерелом.
- Maltego - проста та швидка програма в установках, яка використовує Java, а, відповідно, працює на Windows, Mac та Linux.

• Maltego має графічний інтерфейс, який дозволяє побачити взаємозв'язок між об'єктами прогнозованого і точного, що дає можливість простежити приховані зв'язки.

• Використовуючи графічний користувацький інтерфейс (GUI), ви з легкістю використовуєте всі взаємозв'язки, навіть якщо вони розділені на трем або на рівні вмісту.

• Maltego унікальна від того, що вона використовує потужний та гнучкий фреймворк, який робить можливу настройку під себе. Після використання Maltego може бути адаптована під ваші власні, унікальні вимоги [19].

На основі вище наведеної інформації було виставлено оцінки для інструменту. Так як Maltego встановлюється для кожної з трьох популярних операційних систем, має графічний інтерфейс, що дуже спрощує використання, та не дуже важкий у використанні, то інструмент отримав досить високий бал і може використовуватись багатьма людьми навіть без спеціальної підоготовки.

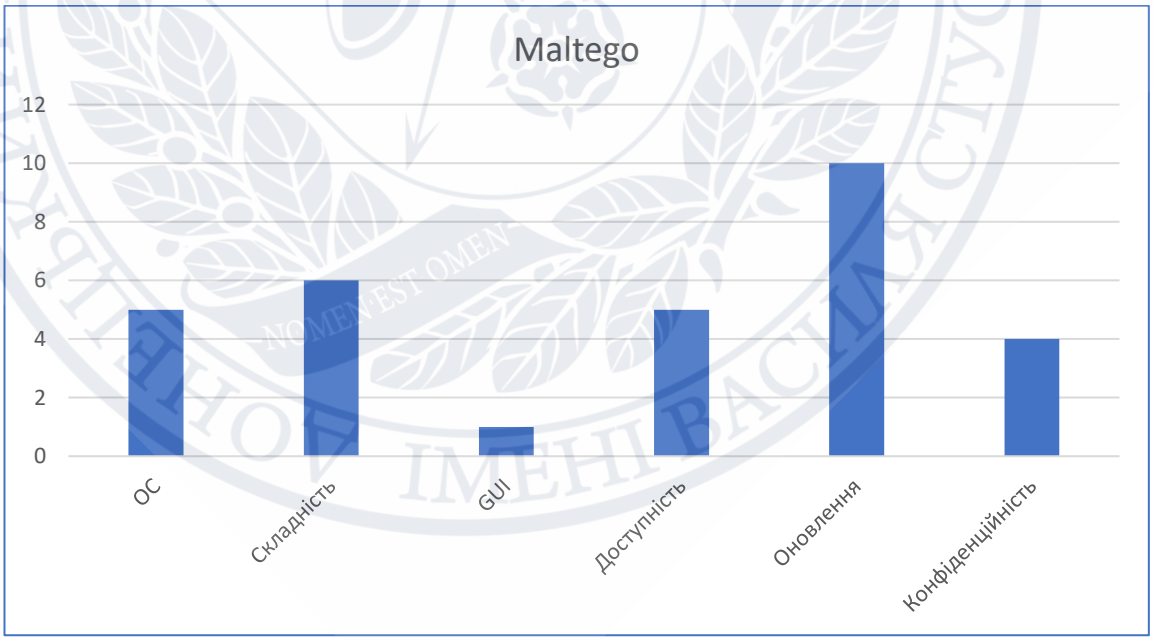

Рисунок 3 – Оцінка інструмента Maltego

2.3 Google Dorks

Пошукові системи справді надають нам багато інформації, і Google популярний серед усіх, що використовується для збору інформації про ціль. Google Dorks - це один з найкорисніших інструментів розвідки з відкритим кодом, який надає таку інформацію за допомогою деяких дивовижних операторів, і він існує з 2002 року. Dork допомагає ефективно здійснювати більш цільові пошуки.

Даний приклад збору і аналізу інформації, який виступає як інструмент OSINT, є не вразливістю Google і не пристроєм для злому хостингу сайтів. Навпаки, він виступає в ролі звичайного пошукового процесу даних з розширеними можливостями. І це не в новинку, так як існує величезна кількість веб-сайтів, яким вже більше десятка років і вони служать як сховища для вивчення і використання Google Hacking.

У той час як пошукові системи індексують, зберігають хедери і вміст сторінок, і пов'язують їх між собою для оптимальних пошукових запитів. Але на жаль, мережеві павуки будь-яких пошукових систем налаштовані індексувати абсолютно всю знайдену інформацію. Навіть незважаючи на те, що у адміністраторів веб ресурсів не було ніяких намірів публікувати цей матеріал.

Однак найцікавіше в Google Dorking, так це величезний обсяг інформації, який може допомогти кожному в процесі вивчення пошукового процесу Google. Може допомогти новачкам в пошуку зниклих родичів, а може навчити яким чином можна отримати інформацію для власної вигоди. Загалом, кожен ресурс цікавий і дивний за своїм і може допомогти кожному в тому, що саме він шукає.

Використовуючи Google Dorks можна знайти від контролерів віддаленого доступу різних заводських механізмів до конфігураційних інтерфейсів важливих систем. Є припущення про те, що величезна кількість інформації, викладеної в мережі, ніхто і ніколи не знайде.

Однак, давайте розберемося по порядку. Уявіть собі нову камеру відеоспостереження, яка дає змогу відтворювати її трансляцію на телефоні в будь-який час. Ви налаштовуєте і підключаєтеся до неї через Wi-Fi, і завантажуєте

додаток, для аутентифікації входу в систему камери спостереження. Після цього можна отримати доступ до цієї ж камері з будь-якої точки світу.

На задньому плані не все виглядає таким простим. Камера надсилає запит на китайський сервер і відтворює відео в режимі реального часу, дозволяючи увійти в систему і відкрити відеотрансляцію, розміщену на сервері в Китаї, з вашого телефону. Цей сервер може не вимагати пароля для доступу до каналу з вашої веб-камери, що робить її загальнодоступною для всіх, хто шукає текст, що міститься на сторінці перегляду камери.

І на жаль, Google безжально ефективний в пошуку будь-яких пристроїв в Інтернеті, які працюють на серверах HTTP і HTTPS. І оскільки більшість цих пристроїв містять певну веб платформу для їх налаштування, це означає, що багато речей, які не призначені бути в Google, в кінцевому підсумку виявляються там.

Безумовно, найсерйозніший тип файлів, це той, який несе в собі облікові дані користувачів або ж всієї компанії. Зазвичай це відбувається двома способами. У першому, сервер налаштований неправильно і виставляє свої адміністративні логи або журнали у відкритому доступі в Інтернеті. Коли паролі змінюються або користувач не може увійти в систему, ці архіви можуть витекти разом з обліковими даними.

Другий варіант відбувається тоді, коли конфігураційні файли, що містять ту ж інформацію (логіни, паролі, найменування баз даних і т.д.), стають загальнодоступними. Це файли повинні бути обов'язково приховані від будь-якого публічного доступу, так як в них часто залишають важливу інформацію. Будь-яка з цих помилок може призвести до того, що зловмисник знайде дані лазівки і отримає всю потрібну інформацію.

Дана стаття ілюструє використання Google Dorks, для того щоб показати не тільки як знаходити всі ці файли, але і наскільки бувають уразливі платформи, що містять інформацію у вигляді списку адрес, електронної пошти, картинок і навіть переліку веб-камер у відкритому доступі[16].

Google Dorks часто називають GHDB (база даних злому Google) і спеціально призначена для тестувальників пера на етапі збору інформації.

Ось деякі з його операторів:

Ext: Це використовується для визначення того, яке розширення файлу шукати конкретно.

Intext: використовується для пошуку певного тексту на сторінці.

Тип файлу: використовується для пошуку конкретних типів файлів, які користувач повинен шукати.

Inurl: використовується для отримання веб-сторінок із певним текстом у їх URL-адресах.

Intitle: використовується для отримання веб-сторінок, у заголовку яких є певний текст.

Пошукові системи також індексують файли журналів, а dorks можуть отримати до них доступ для виявлення вразливостей та прихованих даних[17].

Google Dorks – це інструмент від Google. Google – одна з найпопулярніших пошукових систем. Цей інструмент досить простий у використанні і тому може використовуватись багатьма користувачами.

Рисунок 4 – Приклад пошуку

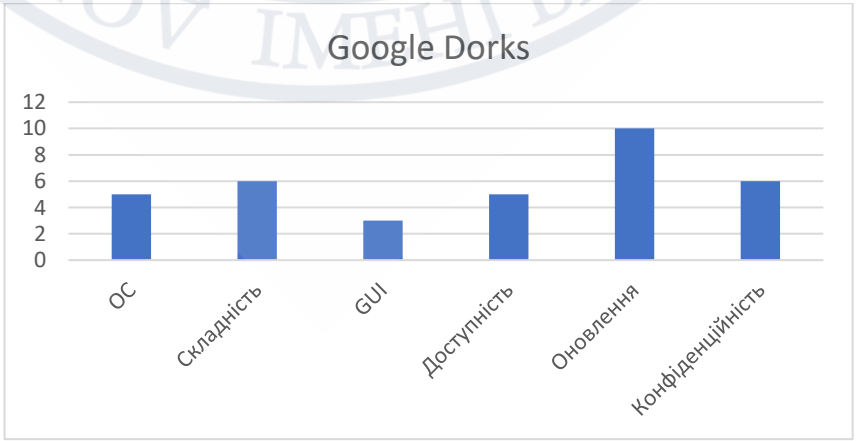

Рисунок 5 – Оцінка інструмента Google Dorks

2.4 Recon-ng Package Description

Recon-ng - це повнофункціональний фреймворк веб-розвідки, написаний на Python. У комплексі незалежних модулів, взаємодії з базовими даними, зручних вбудованих функцій, інтерактивної допомоги та завершення команди. Recon-ng забезпечує потужне окруження, під час якого розробляється на основі відкритих веб-джерел, може бути проведено швидко і досконало.

Зв'язок схожості з Metasploit Framework, завдяки цьому потрібно менше часу на навчання для влаштування фреймворку. Тем не менше, він трохи інший. Recon-ng не ставить за мету конкурувати з існуючими фреймворками, він створений виключно для розведки на основі відкритих веб-джерел. Якщо ви бажаєте використати уявлення, використовуйте Metasploit Framework. Якщо вам потрібна соціальна інженерія, використовуйте Social-Engineer Toolkit. Якщо ви провокуєте розвідку, використовуйте Recon-ng!

Recon-ng - це повністю модульний фреймворк, який робить написання нових модулів простим навіть для початківців розробників на Python'e. Каждый модуль - це підклас класу "модуль". Клас "модуль" - це настроєний інтерпретатор "cmd", потужний вбудований функціонал, що забезпечує прості інтерфейси для популярних завдань, таких як стандартизований вивід, взаємодія з базовими даними, створення веб-запрошень та управління API ключами. Таким чином, вся трудна робота вже зроблена. Створення модулів - це просто і займається трохи менше кількох хвилин[20].

Тип інформації, яка може бути зібрана з цими модулями, включає:

- контакти;
- облікові дані; профілі соціальних мереж;
- IP адреса; зворотний IP-адреса;
- інформація WHOIS; інформація про порти.
- Recon-ng також може шукати певні уразливості в цільовому веб-додатку, такі як:

- міжсайтовий скриптинг;
- PunkSPIDER; GHDB (Google Hacking Database).

Recon-ng - це модульна структура, яка може збирати детальну інформацію про цільових веб-додатках і окремих осіб, це відмінний інструмент для OSINT (розвідка на основі відкритих джерел) [21].

Recon-ng – це специфічний інструмент який знаходить інформацію про доменні імена, IPадреси. Він не дуже складний у використанні, але підтримує лише одну операційну систему та не має графічної оболонки. Це ускладнює використання.

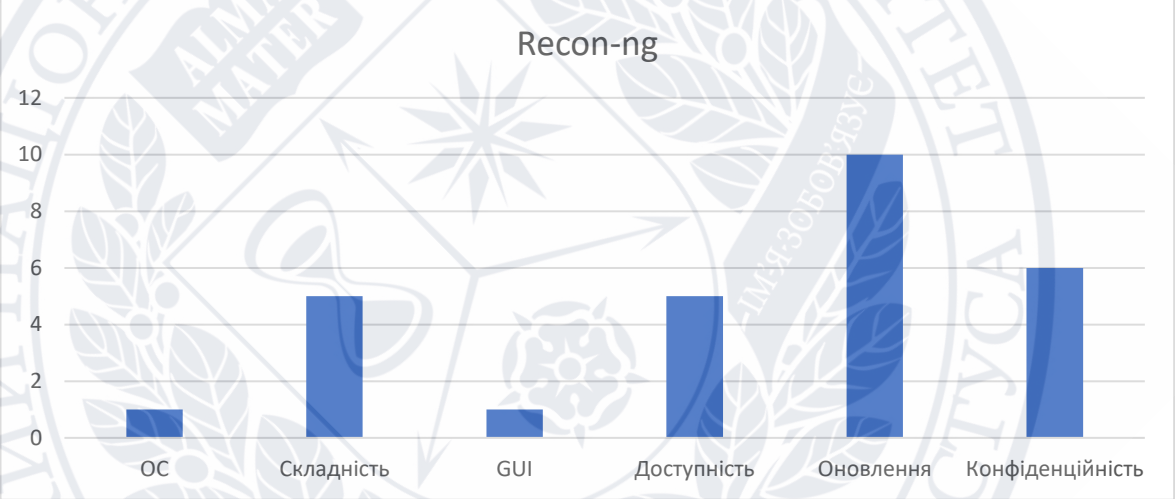

Рисунок 6 – Оцінка інструмента Recon-ng

2.5 theHarvester

theHarvester - це інструмент для збору e-mail адрес, імен піддоменів, віртуальних хостів, відкритих портів / банерів і імен працівників з різних відкритих джерел (пошукові системи, сервера ключів pgp).

Це по-справжньому простий інструмент, але ефективний на ранніх етапах тестування на проникнення або щоб дізнатися, яку інформацію можуть зібрати про вашу компанію через Інтернет.

Джерелами є:

пасивні:

- google: пошукова машина Google - www.google.com
- googleCSE: спеціальний пошук Google
- google-profiles: пошукова система Google, специфічний пошук за профілями Google
- bing: пошукова система Microsoft - www.bing.com
- bingapi: пошукова система Microsoft, через API (вам потрібно додати ваш ключ в файл discovery / bingsearch.py)
- dogpile: пошукова система Dogpile - www.dogpile.com
- pgp: сервер ключів pgp - mit.edu
- linkedin: пошукова система Google, специфічний пошук по користувачах Linkedin
- vhost: пошук Bing по віртуальним хостам
- twitter: Twitter акаунти, пов'язані із зазначеним доменом (використовується пошук Google)
- googleplus: користувачі, які працюють в цільової компанії (використовує пошук Google)
- yahoo: пошукова система Yahoo
- baidu: пошукова система Baidu
- shodan: пошукова система Shodan, шукає порти і банери виявлених хостів (http://www.shodanhq.com/)

активні:

- брут-форс DNS: цей плагін запустить перебір по словнику
- зворотне перетворення DNS: зворотне перетворення виявлених ip для пошуку імен хостів
- DNS TDL розширення: перерахування за словником TLD
- Модулі, для роботи котрої потрібні API ключі:
- googleCSE: Вам потрібно створити Google Custom Search engine (CSE) і додати ваш Google API ключ і CSE ID в плагін (discovery / googleCSE.py)

• shodan: Вам потрібно ввести ваш API ключ в discovery / shodansearch.py[22]

theHarvester використовується для пошуку різної інформації зв'язаної з DNS записами доменів. Він встановлюється лише на одну операційну систему та не має графічної оболонки. Для використання застосовують команди unix що може бути важко для звичайного користувача, але для людини яка має хоч якийсь досвід роботи з Linux терміналом, це не має зробити якихось перешкод.

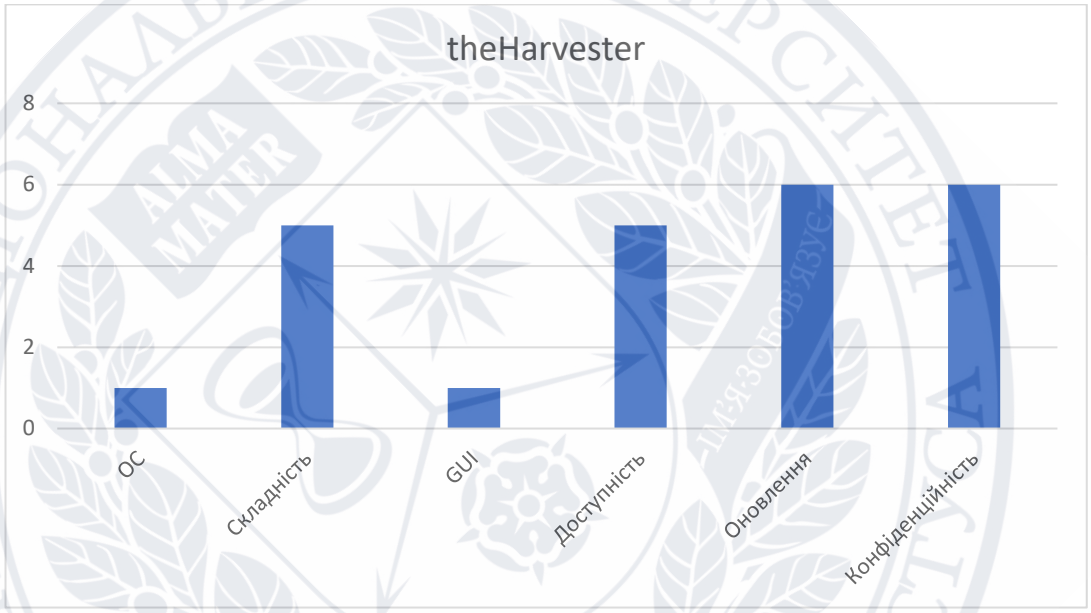

Рисунок 7 – Оцінка інструмента theHarvester

2.6 Shodan

Shodan - це пошукова система для пристроїв, підключених до Інтернету. Веб-пошукові системи, такі як Google і Bing, чудово підходять для пошуку веб-сайтів. Але що, якщо вам цікаво виміряти, які країни стають більш зв'язаними? Або якщо ви хочете знати, яка версія Microsoft IIS є найпопулярнішою? Або ви хочете знайти контрольні сервери для зловмисного програмного забезпечення? Можливо, виникла нова вразливість, і ви хочете побачити, на скільки хостів це може вплинути? Традиційні веб-пошукові системи не дозволяють відповісти на ці запитання.

Shodan збирає інформацію про всі пристрої, безпосередньо підключені до Інтернету. Якщо пристрій підключено безпосередньо до Інтернету, тоді Shodan запитує його щодо різної загальнодоступної інформації. Типи приладів, які індексуються, можуть надзвичайно відрізнятися: від невеликих робочих столів до атомних електростанцій і всього іншого.

То що тоді індекс Шодана? Основна маса даних береться з банерів, які є метаданими про програмне забезпечення, яке працює на пристрої. Це може бути інформація про серверне програмне забезпечення, які параметри підтримує послуга, привітальне повідомлення або щось інше, що клієнт хотів би знати перед взаємодією з сервером.

Інформація, отримана від цих послуг, застосовується у багатьох сферах:

- Безпека мережі: слідкуйте за всіма пристроями у вашій компанії, які стикаються з Інтернетом
- Дослідження ринку: з’ясуйте, які товари люди використовують у реальному світі
- Кібер-ризик: включіть онлайн-показник ваших продавців як метрику ризику
- Інтернет речей: відстежуйте зростаюче використання розумних пристроїв
- Відстеження програм-вимагачів: виміряйте, на скільки пристроїв вплинуло програм-вимагачів

Як ви можете сказати, варіанти використання даних різні. Ми пропонуємо платформу, яка забезпечує точну, послідовну та актуальну інформацію про пристрої, що працюють в Інтернеті - вам вирішувати, який тип інформації вас найбільше цікавить[23].

Shodan дуже схожий на звичайно пошуковик, але вимагає спеціального синтаксису, і тому для використання цього інструменту потрібні впевнені навички роботи з комп’ютером. Але також, він має графічний інтерфейс, що спрощує його використання.

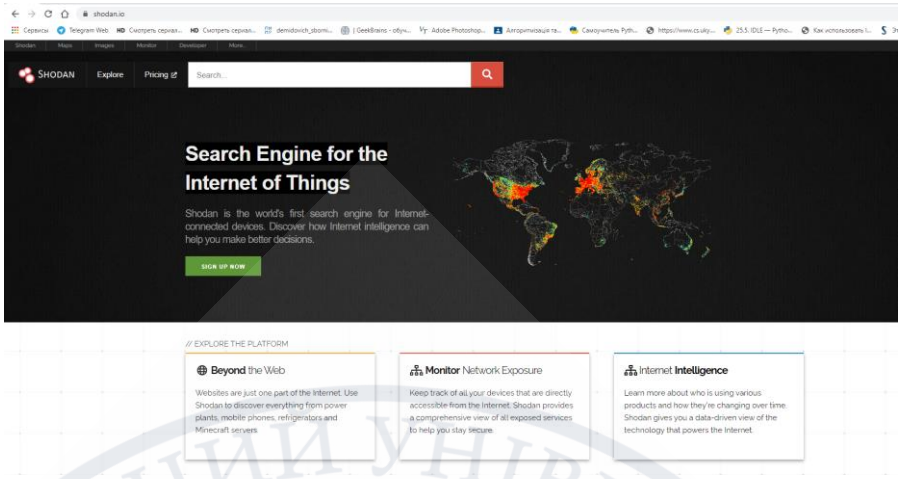

Рисунок 8 – Вебсайт Shodan.io

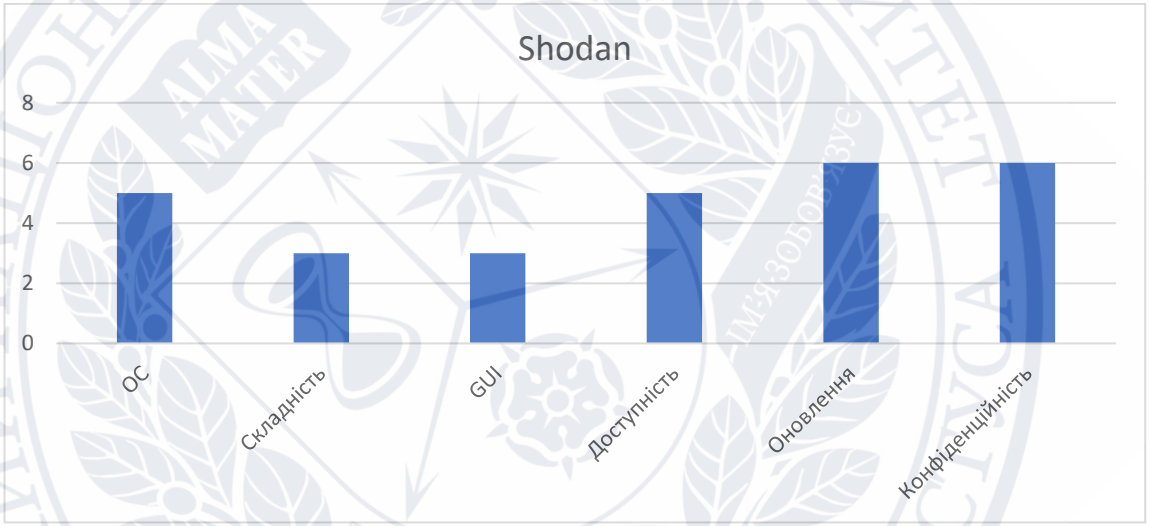

Рисунок 9 – Оцінка інструмента Shodan

2.7 Metagoofil

Metagoofil - чудовий інструмент збору інформації, який можна використовувати для вилучення тонн інформації з документів Word, PDF-файлів, таблиць Excel, зображень .jpg та багатьох інших форматів. Отже, Metagoofil може надати багато плідної інформації під час тестування на проникнення, просто скануючи зібрані файли.

Metagoofil вже існує в Kali Linux і є чудовим інструментом для аналізу файлів метаданих у них. Ці метадані - це лише деякі дані про файл, які

використовуються програмами. Мета-дані не можуть бути переглянуті користувачем, а також не будуть корисними для користувача. Його там буде використовувати програма.

Metagoofil може використовуватися для отримання метаінформації з різних форматів, таких як word, pdf, .jpg тощо, включаючи веб-сторінки HTML[24].

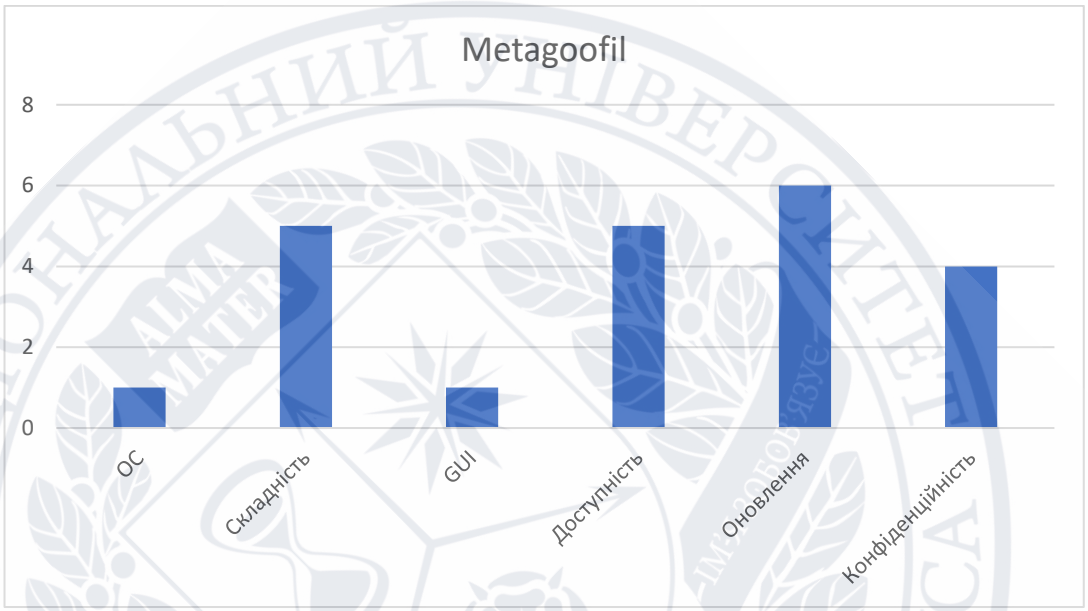

Рисунок 10 – Оцінка інструмента Metagoofil

2.7 nMap

По суті, Nmap - це інструмент мережевого сканування, який використовує IP-пакети для ідентифікації всіх підключених до мережі пристроїв та надання інформації про служби та операційні системи, на яких вони працюють.

Програма найчастіше використовується через інтерфейс командного рядка (хоча доступні також інтерфейси графічного інтерфейсу) і доступна для багатьох різних операційних систем, таких як Linux, Free BSD та Gentoo. Його популярність також підкріпила активна та захоплена спільнота підтримки користувачів.

Nmap був розроблений для корпоративних мереж і може сканувати тисячі підключених пристроїв. Однак в останні роки Nmap все частіше використовується

меншими компаніями. Зокрема, зростання IoT тепер означає, що мережі, що використовуються цими компаніями, стали більш складними, а отже, їх важче захистити.

Це означає, що Nmap зараз використовується в багатьох інструментах моніторингу веб-сайтів для аудиту трафіку між веб-серверами та пристроями IoT. Нещодавня поява бот-мереж IoT, подібно до Mirai, також стимулювала інтерес до Nmap, не в останню чергу через його здатність допитувати пристрої, підключені через протокол UPnP, та виділяти будь-які пристрої, які можуть бути шкідливими.

На практичному рівні Nmap використовується для надання детальної інформації в реальному часі у ваших мережах та на підключених до них пристроях.

Основне використання Nmap можна розділити на три основні процеси. По-перше, програма надає вам детальну інформацію про кожен IP, активний у ваших мережах, і кожен IP потім може бути відсканований. Це дозволяє адміністраторам перевірити, чи використовується IP-адресом законною службою чи зовнішнім зловмисником.

По-друге, Nmap надає інформацію про вашу мережу в цілому. Він може використовуватися для надання списку активних хостів і відкритих портів, а також для ідентифікації ОС кожного підключеного пристрою. Це робить його цінним інструментом постійного моніторингу системи, а також критичною частиною пентестування. Nmap може використовуватися поряд із фреймворком Metasploit, наприклад, для перевірки, а потім для усунення вразливостей мережі.

По-третє, Nmap також став цінним інструментом для користувачів, які хочуть захистити особисті та ділові веб-сайти. Використання Nmap для сканування власного веб-сервера, особливо якщо ви розміщуєте веб-сайт у себе вдома, по суті імітує процес, який хакер використовував би для атаки на ваш сайт. «Атакувати» таким чином власний сайт - це потужний спосіб виявлення вразливих місць безпеки.

Nmap є простим у використанні, і більшість інструментів, які він пропонує, знайомі системним адміністраторам з інших програм. Перевага Nmap полягає в

тому, що він об'єднує широкий спектр цих інструментів в одну програму, а не змушує вас переходити між окремими та дискретними інструментами моніторингу мережі.

Для того, щоб використовувати Nmap, ви повинні бути знайомі з інтерфейсами командного рядка. Більшість досвідчених користувачів можуть писати сценарії для автоматизації загальних завдань, але це не потрібно для базового моніторингу мережі [25].

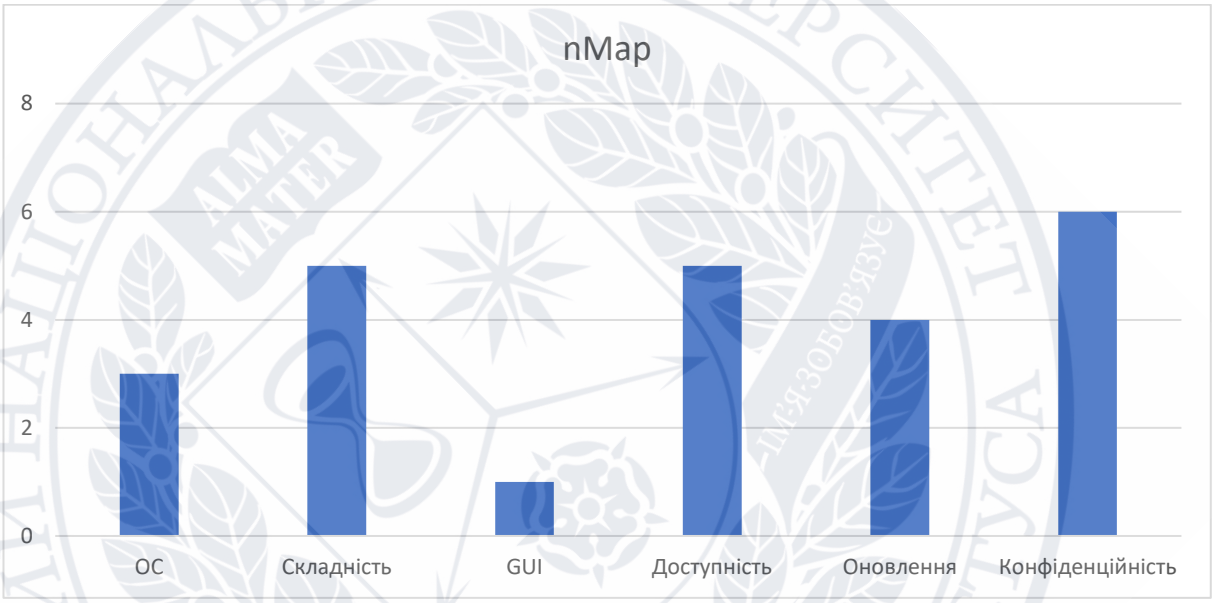

Рисунок 11 – Оцінка інструмента nMap

2.8 Spiderfoot

Spiderfoot - це інструмент, написаний Стівом Мікаллефом, який автоматизує весь процес OSINT.

Оскільки в Інтернеті є маса даних, доступних для різних служб, мереж та протоколів збір усієї цієї інформації з будь-якого окремого місця і кожного разу стає досить трудомістким завданням.

Саме тоді SpiderFoot приходить на допомогу, оскільки його можна використовувати для автоматизації процесу збору OSINT, щоб знайти що-небудь про вашу ціль, централізовану в одному єдиному інструменті.

Для автоматизації OSINT Spiderfoot запитує понад 100 відкритих джерел інформації та обробляє всі дані розвідки з імен доменів, електронних адрес, імен, IP-адрес, серверів DNS та багато іншого.

Вкажіть ціль, виберіть модулі для запуску, і Spiderfoot виконає за вас всю роботу, зібравши всі дані, щоб створити повний профіль усього, що ви досліджуєте.

Інструменти OSINT, такі як Spiderfoot, особливо корисні для передачі інформації про будь-яку ціль, виявлення можливих витоків даних або виявлення повних вразливостей, наявних у їх мережі або додатках.

Ця інформація може бути корисною під час проведення тесту на проникнення, аудиту власної мережі або авторизованої мережі третьої сторони.

Основні характеристики Spiderfoot

• Відкритий код: цей інструмент безпеки написаний на Python і розміщений на Github. Найкраще те, що це відкритий код, а це означає, що кожен може внести свій внесок у його покращення.

• Мультиплатформа: Spiderfoot можна запускати як в операційних системах Linux, так і в Windows.

• Веб-інтерфейс: за замовчуванням Spiderfoot можна запускати з інтерфейсу CLI, однак він також підтримує крутий веб-інтерфейс для тих, хто хоче простоти використання, вишуканих піктограм та насиченої графічної візуалізації.

• Підтримка модулів: він працює, включаючи понад 100+ модулів, що може допомогти виконати майже будь-який тест проти цільової мережі. Модулі SpiderFoot були запрограмовані на взаємодію один з одним, дозволяючи всім пов'язаним модулям обмінюватися однаковими даними про ціль.

• Документація: на відміну від інших інструментів OSINT, Spiderfoot був не тільки добре написаний з точки зору коду, він має чудову область документації, яка дозволить вам виявити, прочитати та зрозуміти, як все працює, включаючи процес встановлення, використання, модулі тощо.

• Spiderfoot HX: хоча стандартна версія буде працювати в будь-якому середовищі, ви також можете запустити Spiderfoot на власній хмарній платформі, що розміщується самостійно, яка включає в себе більш розширені функції, ніж сама розміщена версія[26].

•

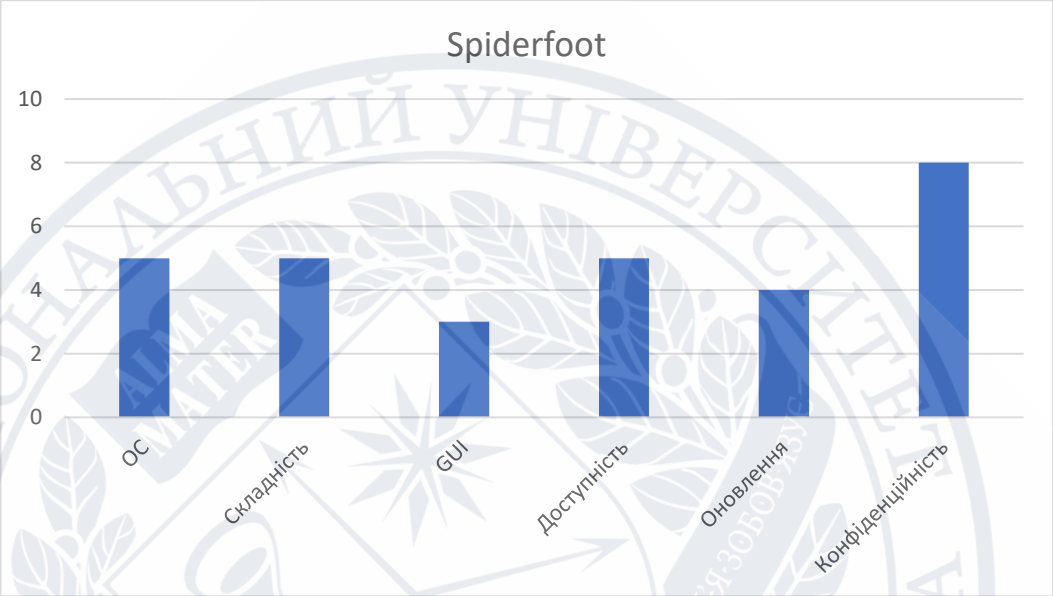

Рисунок 12 – Оцінка інструмента Spiderfoot

2.9 WebShag

Webshag - це багатопотоковий багатоплатформенний інструмент аудиту веб-серверів. Написаний на Python, він збирає загальнокорисні функції для аудиту веб-серверів, такі як сканування веб-сайтів, сканування URL-адреси або розмивання файлів.

Webshag можна використовувати для сканування веб-сервера в HTTP або HTTPS, через проксі-сервер та за допомогою аутентифікації HTTP (Basic та Digest). На додаток до цього він пропонує інноваційні функції ухилення IDS, спрямовані на ускладнення кореляції між запитом (наприклад, використання іншого випадкового проксі-сервера HTTP для кожного запиту).

Він також надає інноваційні функціональні можливості, такі як можливість отримання списку доменних імен, розміщених на цільовій машині, та розмивання

файлів за допомогою динамічно генерованих імен файлів (на додаток до загальних розбіжностей на основі списку).

Сканер URL-адрес Webshag та розширювач файлів спрямовані на зменшення кількості помилкових спрацьовувань і, таким чином, отримання чистіших наборів результатів. Для цього webshag реалізує механізм відбитків пальців веб-сторінки, стійкий до змін вмісту. Потім цей механізм відбитків пальців використовується в алгоритмі видалення помилково позитивних даних, спеціально призначеному для роботи з “м'якими” відповідями сервера 404.

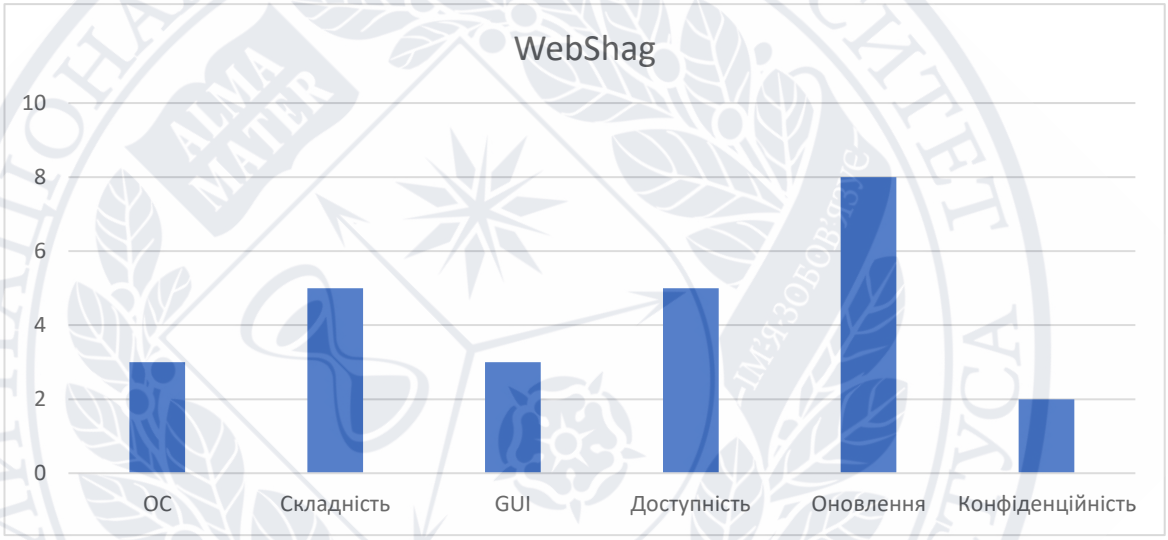

Рисунок 13 – Оцінка інструмента WebShag

2.10 Unicornscan

Сканування портів - одна з найпопулярніших тактик, яку використовують хакери чорних шапок. Отже, він також часто використовується в етичному злому для перевірки систем на наявність вразливостей. Кілька інструментів полегшують сканування портів, nmap, NetCat, Zenmap, будучи помітною кількістю.

Але сьогодні ми поговоримо про ще один чудовий сканер портів: Unicornscan та про те, як використовувати його під час наступної спроби сканування портів. Як і інші популярні інструменти для сканування портів, такі як nmap, він має кілька чудових функцій, унікальних для нього самого. Однією з

таких особливостей є те, що він може розсилати пакети та отримувати їх через два різні потоки, на відміну від інших сканерів портів.

Відомий своїми можливостями асинхронного сканування TCP та UDP, Unicornscan дозволяє своїм користувачам виявляти деталі мережевих систем за допомогою альтернативних протоколів сканування.

Атрибути Unicornscan

• Перш ніж ми намагатимемося сканувати мережу та порти за допомогою Unicornscan, виділимо деякі його визначальні особливості:

• Асинхронне сканування TCP без стану із кожним із прапорів TCP або комбінацій прапорів

• Асинхронне сканування UDP, специфічне для протоколу

• чудовий інтерфейс для вимірювання відповіді від стимулу з підтримкою TCP / IP

• Активне та пасивне віддалене виявлення ОС та додатків

• Журналювання та фільтрація файлів PCAP

• здатний надсилати пакети з відбитками пальців ОС, відмінними від ОС хоста.

• Вихід реляційної бази даних для зберігання результатів сканування

• Налаштовувана підтримка модуля, яка підходить відповідно до системи, яка перевіряється

• Індивідуальні подання набору даних.

• Має свій стек TCP / IP, що є відмінною рисою, яка відрізняє його від інших сканерів портів

• Поставляється вбудованою в Kali Linux, завантажувати не потрібно[27].

•

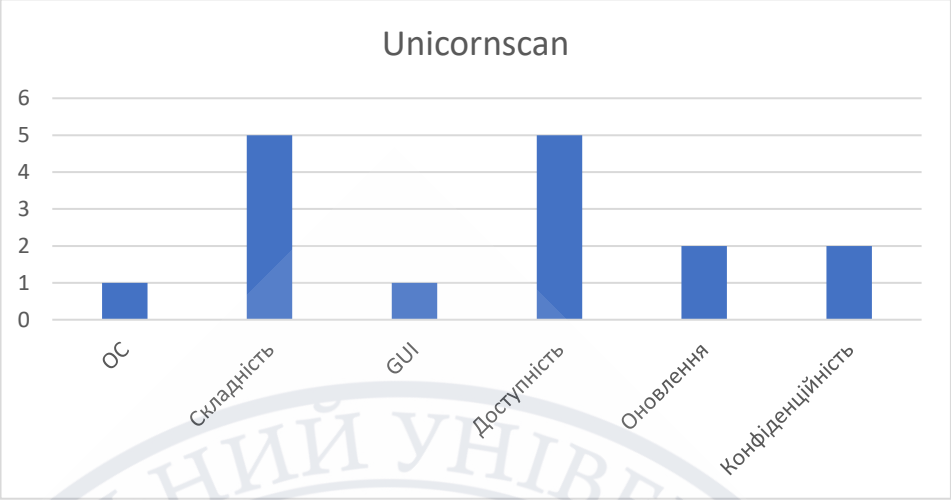

Рисунок 14 – Оцінка інструмента Unicornscan

2.11 Порівняння інструментів OSINT

На основі отриманих результатів отримуємо таблицю порівнянь.

Таблиця 2.1 – Порівняння інструментів OSINT

	ОС	Складність	GUI	Доступність	Оновлення	Конфіденційність	Сума
Maltego	5	3	1	5	10	4	28
Google Dorks	5	1	3	5	10	6	30
Recon-ng	1	3	1	5	10	6	26
theHarvester	1	3	1	5	6	6	22
Shodan	5	3	3	5	6	6	28
Metagoofil	1	3	1	5	6	4	20
nMap	3	3	1	5	4	6	22
Spiderfoot	5	3	3	5	4	8	28
WebShag	3	3	3	5	8	2	24
Unicornscan	1	3	1	5	2	2	14

Також, для наглядності створимо діаграму порівнянь.

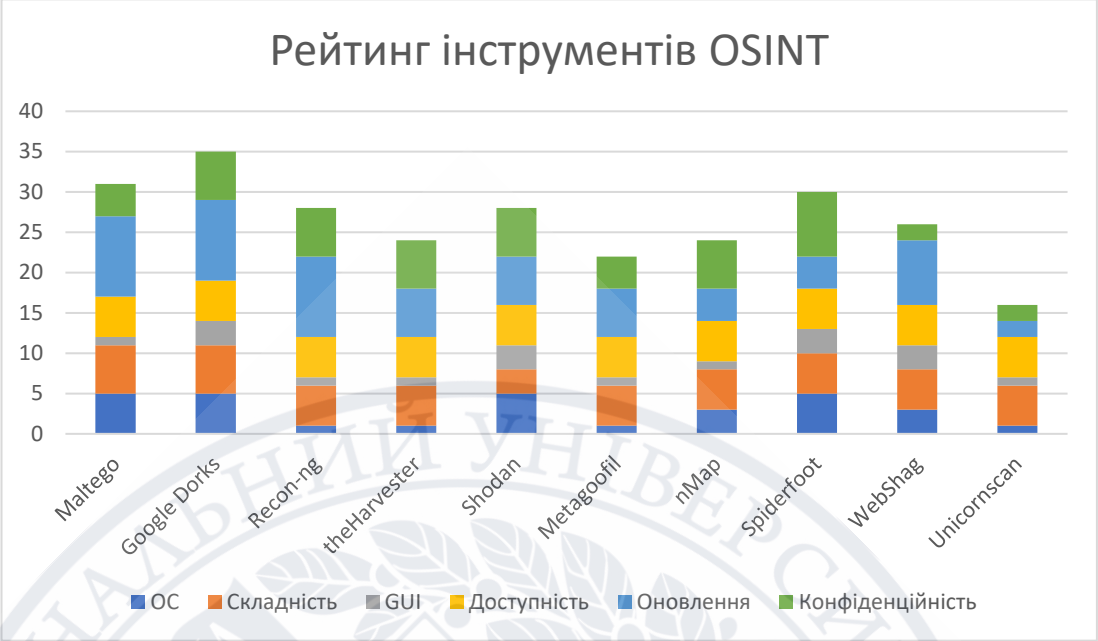

Рисунок 15 – Порівняння інструментів OSINT

На основі отриманих результатів можна зрозуміти який інструмент OSINT буде зручніше для використання. Але кожний інструмент має свої особливості та в деяких випадках краще використати той, що більше підходить для знаходження потрібної інформації, а не той що зручніше. Наприклад, Google Dorks зручний для використання, та має графічний інтерфейс, але його не можна використовувати для сканування відкритих портів. Для цієї задачі краще використати nmap або Unicorscan. Якщо ж користувачу потрібно знайти інформацію про домен, наприклад WHOIS, то ми можемо використати Recon-ng. Бувають випадки, коли інформація вже знайдена, але треба отримати ільш детальну інформацію, то для цього можна використати Metagoofil – інструмент збору інформації, призначений для виведення метаданих документів (PDF, DOC, XLS, PPT, DOCX, PPTX, XLSX). Потужною пошуково системою є Shodan, але його зручно використовувати тоді, коли користувач може чітко сформувати потрібний запит, це є особливістю цього інструменту OSINT.

ВИСНОВКИ

1. На основі проведеної роботи було з’ясовано, що на даний момент OSINT є дуже популярним методом пошуку інформації. Оскільки технологія зростає з кожним днем, виникає потреба у швидкому та конкретному зборі інформації, і це збільшує потребу в OSINT. Використовуючи OSINT, ми можемо отримати важливу інформацію за лічені хвилини, що можливо лише шляхом глибокого аналізу в газетах, журналах, галузевих бюлетенях, соціальних мережах, телевізійних стенограмах та блогах. Було з’ясовано, що для застосування OSINT на практиці використовуються різноманітні інструменти і підбір інструменту під кожний окремий випадок є проблемним питанням тому, що немає єдиного підходу до підбору.

2. На основі аналізу найпоширеніших інструментів OSINT запропонована методика оцінювання кожного інструменту, яка включає в себе 6 факторів:

1. Які операційні системи підтримує інструмент.
2. Складність використання.
3. Наявність графічного інтерфейсу.
4. Доступність.
5. Коли програмний продукт оновлювався востаннє.
6. Наскільки конфіденційною буде отримана інформація.

Кожному з факторів відведено від одного до 4 рівнів оцінок.

3. В результаті оцінювання з’ясовано, що найбільший рейтинг для використання мають Google Dorks, Maltego, Spiderfoot, але використання того чи іншого інструментарію має бути засновано на оцінці за кожною складовою. Також, треба розуміти, що деякі інструменти вузько спеціалізовані для отримання конкретної інформації, і тому, для того, щоб результат пошуку був максимально точний, треба дивитись, який інструмент для чого призначений.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pune, M.; Open Source Intelligence (OSINT). Market Research Report-Global Forecast to 2023—Market Analysis, Scope, Stake, Progress, Trends and Forecast to 2023. Market Research Future. 2020. Available online: https://www.marketresearchfuture.com/reports/open-source-intelligence-market-4545
2. Pastorino, C. Técnicas y Herramientas OSINT Para la Investigación en Internet. Welivesecurity by ESET. 2019. Available online: https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-invest igacion-internet/
3. Passi, H. Top. 10 Popular Open Source Intelligence (OSINT) Tools. GreyCampus. 2018. Available online: https://www.greycampus.com/blog/information-security/top-open-source-intelligence-tools
4. Portillo, I.; Nykiel, W. From Zero to OSINT Hero. Universidad de Alcalá de Henares. 2019. Available online: https://es.slideshare.net/WiktorNykielLION/from-zero-to-osint-hero-universidad-de-alcal-de-henares-i van-portillo-morales-y-wiktor-nykiel
5. Pastor-Galindo, J.; Nespoli, P.; Gomez Marmo, F.; Martinez Perez, G. OSINT Is the Next Internet Goldmine: Spain as an Unexplored Territory. V Jornadas Nacionales de Investigación en Ciberseguridad. 2019. Available online: https://www.researchgate.net/publication/333703698_OSINT_is_the_next_Internet_goldmine_Spa in_as_an_unexplored_territory
6. Norton, R. Guide to Open Source Intelligence. Intell. J. US Intell. Stud. 2011, 18, 65–67. Available online: https://www.afio.com/publications/Norton_Open_Source_in_AFIO_INTEL_WinterSpring2011.pdf
7. NATO. Open Source Intelligence Handbook; North Atlantic Treaty Organization: Brussels, Belgium, 2001. Available online:

http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NA TO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

8. Korkisch, F. NATO Gets Better Intelligence; Center for Foreign and Defense Policy: Vienna, Austria, 2010. Available online: https://natowatch.org/sites/default/files/NATO_Gets_Better_Intell_April_PDP_0.pdf
9. Pastor-Galindo, J.; Nespoli, P.; Gomez Marmol, F.; Martinez Perez, G. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access 2020, 8, 10282–10304. [CrossRef]
10. Tomislav Ivanjko Department of Information and Communication Sciences, Faculty of Humanities and Social Sciences, University of Zagreb Ivana Lučića 3, Zagreb, Croatia
11. How To Build An OSINT Strategy In 5 Steps [Електронний ресурс]. Режим доступу: https://www.echosec.net/blog/osint-strategy (дата звернення 01.05.2021)
12. An Introduction To Open Source Intelligence (OSINT) Gathering [Електронний ресурс]. Режим доступу: https://www.secjuice.com/introduction-to-open-source-intelligence-osint/ (дата звернення 01.05.2021)
13. European Union Agency for Law Enforcement Training. OSINT. 2019. Available online: https://www.cepol.Eeuropa.eu/tags/osine (дата звернення 03.05.2021)
14. Babak Akhgar P. Saskia Bayerl Fraser Sampson Editors, Open Source Intelligence Investigation
15. OSINT Tools and Techniques [Електронний ресурс]. Режим доступу: https://linuxhint.com/osint-tools-and-techniques/ (дата звернення 05.05.2021)

16. Google Dorking или используем Гугл на максимум [Електронний ресурс]. Режим доступу: https://habr.com/ru/company/postuf/blog/510766/ (дата звернення 08.05.2021)
17. Top 10 OSINT Tools - Open Source Intelligence [Електронний ресурс]. Режим доступу: https://mindmajix.com/osint-tools (дата звернення 09.05.2021)
18. 8 top open source intelligence tools [Електронний ресурс]. Режим доступу: https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html (дата звернення 10.05.2021)
19. Maltego Teeth Package Description [Електронний ресурс]. Режим доступу: https://tools.kali.org/information-gathering/maltego-teeth (дата звернення 12.05.2021)
20. Recon-ng Package Description [Електронний ресурс]. Режим доступу: https://tools.kali.org/information-gathering/recon-ng (дата звернення 13.05.2021)
21. Recon-ng — инструмент интеллектуальной системы отслеживания [Електронний ресурс]. Режим доступу: https://www.make-info.com/recon-ng-osint-tool/ (дата звернення 15.05.2021)
22. theHarvester [Електронний ресурс]. Режим доступу: https://kali.tools/?p=2286 (дата звернення 17.05.2021)
23. theHarvester [Електронний ресурс]. Режим доступу: https://help.shodan.io/the-basics/what-is-shodan (дата звернення 19.05.2021)
24. Metagoofil Tutorial : Extract Information from Docs,Images [Електронний ресурс]. Режим доступу: https://www.hackingloops.com/metagoofil-tutorial-extract-information-from-docsimages-and-more/ (дата звернення 21.05.2021)
25. How to Use Nmap: Commands and Tutorial Guide [Електронний ресурс]. Режим доступу: https://www.varonis.com/blog/nmap-commands/ (дата звернення 23.05.2021)

26. Spiderfoot, an Open Source Intelligence Automation Tool [Електронний ресурс]. Режим доступу: https://securitytrails.com/blog/spiderfoot-osint-automation-tool (дата звернення 25.05.2021)
27. Unicornscan: A beginner's guide [Електронний ресурс]. Режим доступу: https://linuxhint.com/unicornscan_beginner_tutorial/ (дата звернення 28.05.2021)