УДК 004.056:355.451

МЕТОДИКА ПРОВЕДЕННЯ ПАСИВНОГО OSINT ЗА ДОПОМОГОЮ ПАКЕТУ KALI LINUX

Гонтарь І. А.
Науковий керівник – к.т.н. доцент Снігуров А. В.
Харківський національний університет радіоелектроніки, каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків, Україна
тел. +38(067) 546-86-35

There are many different ways to access the system. Many believe that to gain access to servers or services, you only need to know how to program. It does not. The very first step in attacking or auditing a target is gathering information about the target. Open source intelligence is an intelligence discipline that deals with intelligence generated from publicly available information that is collected, used, and disseminated to appropriate audiences in a timely manner to address specific intelligence and information requirements.

OSINT також являється розвідувальною інформацією, розробленою на основі відкритого збору та аналізу загальнодоступної інформації та інформації з відкритих джерел. OSINT є похідним від систематичного збору, обробки та аналізу загальнодоступної відповідної інформації у відповідь на вимоги розвідки. Два важливі пов'язані терміни – це інформація з відкритого джерела та загальнодоступна інформація [1]:

−відкрите джерело — це будь-яка особа або група, яка надає інформацію без очікування конфіденційності — інформація, стосунки чи те й інше не захищені від публічного розголошення. Інформація з відкритих джерел може бути загальнодоступною, але не вся загальнодоступна інформація є відкритою. Під відкритими джерелами розуміються загальнодоступні носії інформації і не обмежуються фізичними особами;

−загальнодоступна інформація — це дані, факти, інструкції чи інші матеріали, опубліковані або транслюванні для загального користування; доступний на запит для члена широкої громадськості; законно побачений або почутий будь-яким випадковим спостерігачем; або оприлюднити на зустрічі, відкритій для широкої публіки.

Збір даних OSINT зазвичай здійснюється шляхом моніторингу, аналізу даних і досліджень. Виробництво з відкритим кодом підтримує розвідувальну інформацію з усіх джерел і безперервну діяльність процесу розвідки (генерування розвідувальних знань, аналіз, оцінка та поширення).

Сьогодні будь-яка інформація про людину або його життя вже зберігається в глобальній мережі. Виходячи з цих даних, дана особа може стати метою для хакерів і може піддаватися вербовкам або іншим прийомом соціальної інженерії для досягнення цілей злочинців.

Корпоративна пошта є сильним інструментом для нанесення збитку будь-якій компанії. Кожен співробітник може випадково виявитися тією вразливістю, якою можуть скористатися злочинці. Доступ до цього

електронного ящику може виявлятися явно у великих компаніях, де співробітники більше, що означає, велика ймовірність подати до зловмисних цілей. Для аналізу та виявлення подібних цілей існують сервіси, які аналізують, порівнюють і заносять інформацію у свої бази даних. Паролі, як і особисті дані, співробітники можуть використовувати із-за користування ненадійними ресурсами, тощо. Приклади, описані нижче, є рішеннями з відкритим кодом для пошуку співробітників їх корпоративних ящиків для електронних листів [2]:

−hunter.io – пошук корпоративних користувачів;

−bluto - виконує перерахунок адрес електронної пошти на основі цільного домену, в даний час використовуючи пошукові системи Bing і Google, а також збирає дані зі служб Email Hunter і LinkedIn.

Після досягнення цілей, хакер має великий арсенал для можливої атаки на потенційну ціль:

−спам;

−blackmailing;

−крадіжка пароля.

Після визначення списків потенційних цілей хакер збирає дані про цілі:

−соціальні мережі та їх зміст;

−особисті почтові скриньки.

У світі існує величезна кількість злитих паролів користувачів у відкритому доступі. Із-за того, що, в основному, люди ставлять всюди повторюваного пароля, можна методом перебору підібрати потенційний пароль від корпоративного облікового запису. Існує база даних, яка містить у собі понад 1.4 мільярда імейлів і паролів, отриманих з різних ресурсів. Це рішення називається Breach-parse. Breach-parse – відкрита база даних потенційних злитих паролів користувачів різних поштових скриньок та їх доменів. Наприклад, потенційна мета – це провідний програміст у системі авторизації у дослідженій компанії. Доступ до ресурсів, як база даних, є тільки через VPN, до якого можна отримати, через 3rd party авторизацію на корпоративному обліковому записі. Корпоративні облікові записи несуть у собі не тільки інфрмацію, але й доступ до підсистем компанії для розуміння вразливості системи з боку аудитора або зловмисних цілей з боку хакера.

Список використаних джерел:

1. Open Source Intelligence (OSINT). (2023, 28 лютого) OSINT Techniques. https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/

2. 15 top open-source intelligence tools. (2021, 28 червня). https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-intelligence-tools.html