Секція 1

ПОГЛИБЛЕНИЙ АНАЛІЗ МЕТОДІВ ТЕХНІЧНОГО OSINT ТА RECON ДЛЯ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

Луговцов Д. В.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Шостак А. В.

Актуальність. В умовах експоненційного зростання кіберзагроз та ускладнення векторів атак, методологія технічного OSINT (Open Source Intelligence) та Recon (reconnaissance) набуває критичного значення для проактивного виявлення вразливостей в інформаційних системах [1]. Інтеграція цих методів створює комплексний підхід до розвідки загроз, що дозволяє організаціям випереджати потенційні атаки та зміцнювати свою кібер стійкість у динамічному середовищі загроз.

Метою даної роботи є дослідження сучасних методів технічного OSINT та Recon для ефективного виявлення вразливостей інформаційних систем і мереж.

Основні положення. Технічний OSINT (Open-Source Intelligence) та Recon (Reconnaissance) є ключовими інструментами кібербезпеки, які дозволяють виявляти слабкі місця у системах на основі загальнодоступної інформації. OSINT передбачає збір даних з відкритих джерел (доменні записи, субдомени, IP-адреси, тощо), а Recon дозволяє глибше оцінити цільову систему, забезпечуючи проактивний підхід до захисту інфраструктури [2]. Одним із основних методів у технічному OSINT є «воронка»: процес починається із широкого збору даних, які потім проходять фільтрацію та аналіз для виділення найбільш релевантної інформації [3]. Такий підхід дає змогу зосередитися на критичних точках і зменшити обсяг хибнопозитивних результатів. Автоматизація процесів збору та аналізу за допомогою інструментів (наприклад: Censys, Nuclei, Nmap) підвищує ефективність та швидкість, що дозволяє обробляти великі обсяги інформації і зменшує ризик людських помилок. Інтеграція результатів OSINT та Recon у загальну стратегію кібербезпеки організації дозволяє не тільки захищати внутрішню інфраструктуру, а й здійснювати зовнішній моніторинг, що значно посилює захист від потенційних атак.

Висновки. Поглиблене застосування методів технічного OSINT та Recon дозволяє значно підвищити ефективність процесу виявлення вразливостей. Важливо впроваджувати систематичний підхід до

використання цих інструментів для створення більш безпечного середовища.

Список літератури

1. Open-Source Intelligence (OSINT) Report. *Vercara*. URL – https://vercara.com/resources/vercaras-open-source-intelligence-osint-report-november-1-november-7-2024 (дата звернення: 10.10.2024).
2. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», Том 1(25), С. 19-50. DOI: https://doi.org/10.28925/2663-4023.2024.25.1950.
3. Mukhopadhyay A., Luther K. OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment. 2024. DOI: https://doi.org/10.48550/arXiv.2409.11672.

Відомості про авторів

Луговцов Денис Васильович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», d.v.luhovtsov@student.csn.khai.edu
Шостак Анатолій Васильович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», к.т.н., доцент, a.shostak@csn.khai.edu