# ЗБІР ТА АНАЛІЗ ДАНИХ З МЕРЕЖІ HONEYPOT

Русанов Г.О.
Науковий керівник – к.т.н., доц. Федюшин О.І.
Харківський національний університет радіоелектроніки
(61666, м. Харків, пр. Науки 14, каф. Безпеки інформаційних технологій,
тел. (057) 702-14-25, email: d_its@nure.ua)

The given work is dedicated to the means of collecting and analyzing the data received from honeypots. The tools and methods used by hackers to achieve their goals – be it a simple challenge or terrorism acts – are constantly changing and new ones appear that might not be publicly known. The data gathered from these honeypots can later be used for analysis which can give the honeypot owners the clue about these methods and tools used by hackers, to be able to protect the real systems against these kinds of attacks.

Системи honeypot (англ. - горщик з медом) – це ресурси, які використовуються як своєрідна «приманка» для хакерів. Вони не містять ніякої насправді важливої інформації, ізольовані від справжніх серверів або баз даних, хоча зовні створюють видимість зворотнього. Простими словами, це ресурси, задача яких бути атакованими [1]. Їх мета полягає в скануванні будь-яких дій, які хакер застосовує для виконання несанкційних дій в бік honeypot-у. Мережі, що містять декілька таких систем, також називають honeynets.

Honeypot системи можуть бути реалізовані за допомогою програмного забезпечення з різними можливостями: від емуляції роботи окремих сервісів операційної системи або роботи мережних служб до образів окремих операційних систем та емуляції окремих серверів на фізичній обчислювальній машині.

Актуальним питанням для подібних систем є побудова системи збору та зберігання даних від honeypot-ів, що емулюють роботу потенційних сервісів-мішеней від низького до високого рівнів.

Метою даної роботи є аналіз та систематизація даних від різних моделей honeypot-ів для забезпечення подальшої їх обробки та зберігання. Для цього запропоновано схему збирання та перетворення даних від різних honeypot систем для колекціювання та виведення у наочному вигляді на екран робочого місця адміністратора за допомогою web-застосунку.

Дані, що збираються з honeypot-ів мають не тільки містити будь-які деталі, що можуть бути використані для аналізу, але й бути чітко структурованими для можливості проведення такого аналізу. Цього можна досягти спеціальними колекторами – програмними додатками, кожен з яких прив’язаний до свого honeypot-у, він збирає дані з його локальних логів або бази даних, форматує їх відповідно до визначеної структури та передає до центрального серверу баз даних для аналізу.

Структура даних, що передаються, має давати змогу детального їх аналізу. Для цього використовується ряд різних метрик (для прикладу в таблиці 1 запропоновані деякі з них [2]).

Таблиця 1. –Набір метрик для аналізу

| Постановка проблеми | Аналіз |
|---|---|
| Найбільш імовірні джерела атак | IP-адреси; доменні імена, URL-адреси; User-агенти; операційні системи; відбитки (fingerprints) |
| Ціль атаки | IP адреси; порти, транспортні протоколи; служби, процеси; вразливості |
| Частота та тривалість атаки | Частота спам - повідомлення, email за одиницю часу; аналіз трафіку - його розмір, кількість запитів та відповідей тощо за одиницю часу; тривалості окремих сесій, інтервалів між ними |
| Порівняння поширення | Графіки атак; графіки поширення |
| Виявлення шаблонів атак | Метод головних компонент (PCA); символьна агрегатна апроксимація (SAX); метод найбільшої спільної підпослідовності (LCS) |
| Виявлення основної причини | ISN (номер початкової послідовності); когерентність кластерів; EIP |

Більша частина даних потребує детального аналізу для виявлення основної причини атаки, тому дані, що приймаються та аналізуються запропонованою системою від різних honeypot-ів допомагають вирішити цю нетривіальну задачу. Для складних мереж honeypot-ів необхідно використовувати більш складний математичний апарат, такий як пошук асоціативних правил, нейронні мережі тощо, тому цей напрямок розвитку потребує подальших досліджень.

Список використаної літератури:

1. Spitzner L. The Honeynet Project: trapping the hackers [Електронний ресурс] / Lance Spitzner // IEEE. – 2003. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/1193207.

2. A Survey on Honeypot Software and Data Analysis [Електронний ресурс] / [M. Nawrocki, M. Wählisch, T. Schmidt та ін.] // arXiv. – 2016. – Режим доступу до ресурсу: https://arxiv.org/pdf/1608.06249.pdf.