УДК 004.056.53

ВИКОРИСТАННЯ ХАНІПОТІВ ДЛЯ ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК

Єлизавета Шаєц, Ольга Лунгол

Донецький державний університет внутрішніх справ, м. Кропивницький, Україна

Анотація. *Виявлення вторгнень є важливою складовою інформаційної безпеки. Системи виявлення мережевих вторгнень використовується для моніторингу мереж на наявність атак або вторгнень, щоб вжити відповідних заходів для їх попередження та уникнення. Одним із способів виявлення мережевих атак є використання ханіпотів.*

Ключові слова: *ханіопти, інформаційна безпека, технологія обману, мережеві атаки.*

Abstract. *Detection of intrusions is an important component of information security. Network intrusion detection systems are used to monitor networks for attacks or intrusions in order to take appropriate measures to prevent and avoid them. One of the ways to detect network attacks is the use of honeypots.*

Keywords: *honeypots, information security, deception technology, network attacks.*

З розвитком мережевих технологій і додатків та зважаючи на те, що ми живемо в період гібридної війни, фактор виявлення мережевих атак є надзвичайно актуальним. Кількість і серйозність мережевих атак на території України значно зросла з початку 2022 року. Як ключовий метод у сфері мережевої безпеки, система виявлення мережевих атак відіграє надзвичайно важливу роль у захисті як персональних даних, так і даних організацій та установ, в тому числі державного рівня. Навколишнє середовище постійно розвивається та змінюється завдяки новим технологіям та Інтернету [1]. Продукти виявлення вторгнень – це інструменти, які допомагають керувати загрозами та вразливими місцями в цьому мінливому інформаційному середовищі.

Мережеві атаки будемо розглядати як спробу зловмисників отримати несанкціонований доступ до мережі організації або установи з метою викрадення, пошкодження даних, спостережень за діями користувачів мережі або виконання інших шкідливих дій. Наслідком пасивної мережевої атаки є отримання зловмисниками доступу до мережі з контролем або викраденням конфіденційної інформації, але не змінюючи дані, залишаючи їх недоторканими. У випадку активної мережевої атаки зловмисники не лише отримують неавторизований доступ, але й можуть змінювати дані, видаляючи, шифруючи чи іншим чином пошкоджуючи їх. Отримання зловмисниками неавторизованого доступу до пристроїв користувачів, організацій чи

установ, відбувається часто з їх компрометацією шляхом зараження шкідливим програмним забезпеченням. Зараження шкідливим програмним забезпеченням дозволяє зловмисникам скомпрометувати системи, викрасти дані та завдати значної шкоди користувачу чи групі користувачів [2].

Існують різні методи захисту мереж, такі як поділ мережі на зони відповідно до вимог безпеки, регулювання доступу до мережі Інтернет через проксі-сервер, розміщення брандмауера на кожному з'єднанні мережевих зон, використання трансляції мережевих адрес, що дозволяє переводити внутрішні IP-адреси в адреси, доступні в загальнодоступних мережах, відстеження вхідного, вихідного та внутрішнього мережевого трафіку з можливістю автоматичного виявлення загроз і розуміння їх контексту та впливу, застосування технології обману, тобто створення приманок у власній мережі, спокушаючи зловмисників скористатися ними тощо. Ідея створення приманок полягає у тому, що зловмисників навмисно перенаправляють в спеціально створене ІТ-середовище ще до того, як вони змогли проникнути в реальну інформаційну інфраструктуру організації чи установи. У цьому фіктивному середовищі фахівці служби кібербезпеки мають змогу спостерігати за зловмисниками, щоб визначити їхню мотивацію, методи та, в деяких випадках, навіть особу та замовників. Однією з технологій обману є використання приманки, або ханіпоту (honeypot). Він має вигляд справжньої комп'ютерної системи з програмами та даними, що змушує злочинців ІТ-простору вважати, що це реальна ціль. Наприклад, ханіпот може представляти собою систему виставлення рахунків клієнтам певної організації, що є улюбленою мішенню для кібератак злочинців, які хочуть заволодіти даними кредитних карток. Коли хакери використовують приманку, їх можна відстежити та вивчити, спрогнозувати поведінку, щоб зробити реальну мережу більш безпечною. Інший спосіб зацікавлення кіберзловмисника, це навмисне створення вразливостей у мережі. Наприклад, ханіпот може мати порти, які відповідають на сканування портів або слабкі паролі. Вразливі порти можуть бути залишені відкритими, щоб спонукати зловмисників проникнути до середовища ханіпот, а не до реальної мережі певної організації. Отже, ханіпоти у виявленні мережевих атак являються тим інформаційним інструментом, який може допомогти користувачу або спеціалістам із захисту мережі зрозуміти існуючі загрози та можливі загрози для певної організації.

Ханіпоти класифікують на основі їхнього розміщення та участі кіберзловмисника [4]:

– дослідницькі, які використовуються для аналізу хакерських атак і застосування різних способів запобігання цим атакам;

– виробничі, які розміщуються у виробничих мережах разом із сервером. Ці приманки діють як зовнішня пастка для зловмисників, що склада-

ється з неправдивої інформації та дає час адміністраторам на усунення ймовірної вразливості.

Залежно від взаємодії ханітопи можна поділити на:

− приманки з низьким рівнем взаємодії, які дають кіберзловмиснику дуже мало інформації про мережу. Цей ханітоп лише імітує послуги, які часто запитують зловмисники. Основна операційна система не задіяна в системах з низьким рівнем взаємодії. Такі приманки не потребують багато ресурсів і їх легко можна розміщати. Єдиним недоліком цих приманок є те, що досвідчені хакери можуть легко ідентифікувати подібні приманки та уникнути їх використання;

− приманки із середньою взаємодією дозволяють кіберзловмиснику виконувати більше дій порівняно з попереднім варіантом;

− приманки з високою взаємодією спрямовані на те, щоб кіберзловмисник витратив багато часу на роботу з ханітопом, у цей час фахівці з безпеки отримують багато інформації про самих хакерів. Ці приманки включають операційну систему в реальному часі, тому вони є порівняно ризикованими, якщо хакер ідентифікує ханіпот [4]. Недоліком таких приманок також є те, що вони є досить дорогими у вартості та складними у реалізації.

До переваг використання приманок ханітопів при виявленні мережевих атак можна віднести: ханітопи збирають дані лише тоді, коли із ними хтось взаємодіє; у ханіпотів немає помилкових спрацьовувань, тому що будь-яка діяльність з ними є несанкціонованою, зважаючи на мету їх створення; вони не потребують багато ресурсів; не має значення, чи використовує зловмисник шифрування, оскільки діяльність з приманкою в будь-якому випадку буде зафіксовано.

Інформаційні джерела

1. Meeragandhi, G. & K.Srivatsa,. (2018). Detecting and preventing attacks using network intrusion detection systems. International Journal of Computer Science and Security.

2. Network Attacks and Network Security Threats. URL: https://www.cynet.com/network-attacks/network-attacks-and-network-security-threats/ (Дата звернення: 17.11.2022).

3. What is deception? Deception Technology from Austria. URL: https://cybertrap.com/en/deception-technology/ (Дата звернення: 15.11.2022).

4. What is Honeypot? Geeksforgeeks. URL: https://www.geeksforgeeks.org (Дата звернення: 19.11.2022).

5. Honeypots: The sweet spot in network security. John Harrison, Symantec Corp. URL: https://www.computerworld.com/article/2573345/honeypots--the-sweet-spot-in-network-security.html (Дата звернення: 19.11.2022).