ДОСЛІДЖЕННЯ МОДЕЛЕЙ ТА МЕТОДІВ НЕСАНКЦІОНОВАНОГО ВТОРГНЕННЯ В ІНФОРМАЦІЙНІ СИСТЕМИ

Брик М.В., Колесніков К.В.
Черкаський державний технологічний університет, Черкаси, Україна

З розвитком інформаційних технологій відбувається і розвиток кіберзлочинності, яка використовує у своїх протизаконних діях вразливості інформаційних систем.Незважаючи на розробку спеціальних програмно-апаратних засобів захисту, кількість нових методів реалізації атак постійно зростає.

Метою роботиє аналіз найбільш розповсюджених типів кібератак.

Denial-of-Service (відмова в обслуговуванні) - це метод, який використовується для порушення доступу користувачів до обраної мережі або веб-ресурсу [1, 2] . Як правило, це досягається шляхом перевантаження цілі, (часто веб-сервера) величезною кількістю трафіку або шляхом відправки шкідливих запитів, які призводять до відмови або до збою роботи цільового ресурсу. Одними із методів DoS-атаки є: ICMP-флуд,SYN-флуд, перезавантаження буфера. DistributedDenial-of-Service атакаполягає в тому, що під час DDoS-атаки багато шкідливих машин цілеспрямовані на один ресурс. Атака розподіленої відмови в обслуговуванні (DDoS) набагато більш успішна в руйнуванні мети, ніж атака DoS, що виходить з одного джерела. Такий метод набагато важче відстежити атаку, оскільки вона надходить з декількох точок [3].

Отруєння кешу DNS – атака наDNS-сервер, для здійсненняякоїзловмисник, використовуючи недостатньо надійну конфігурацію служби серверу, вносить модифікації до DNS-кешу. Таким чином, усі клієнти DNS-серверу отримують контент зловмисника не зважаючи на те, що звертались за вірним посиланням.

Перехоплення сесії – це спосіб використання чужої сесії, при якому зловмисник вторгається в сесію між двома іншими вузлами. Зловмисник може отримати дійсний ідентифікатор сесії, який використовується для входу в систему і доступу до конфіденційної інформації [4].

Список літератури

1. S. Gavrylenko, V. Chelack, N. Bilogorskiy. Дослідження методів вторгнення в комп'ютерні системи, засноване на показнику Херста// Сучасні інформаційні системи, Том 1, № 2 (2017) > DOI: https://doi.org/10.20998/2522-9052.2017.2.10

2. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы / А.Е. Боршевников // Современные тенденции технических наук: материалы Междунар. науч. конф. – Уфа: Лето, 2011.

3. Mozhaev O. Multiservise network security metric / O. Mozhaev, H. Kuchuk, N. Kuchuk, M. Mozhaev, M. Lohvynenco // IEEE Advanced information and communication technologies-2017. Proc. of the 2th Int. Conf. – Lviv, 2017. – P. 133-136.

4. Лукацкий, А.В. Обнаружение атак, БХВ-Петербург, С.-Пб, 2001, 624 с.