DOI 10.62731/mcnd-17.05.2024.008

СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK

Тимощук Віталій Дмитрович
ORCID ID: 0009-0007-2858-9434
здобувач першого рівня вищої освіти
факультету прикладних інформаційних технологій та електроінженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Долінський Андрій Михайлович
ORCID ID: 0009-0003-4230-0183
здобувач третього рівня вищої освіти
факультету комп'ютерно-інформаційних систем і програмної інженерії
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Науковий керівник: Тимощук Дмитро Іванович
ORCID ID: 0000-0003-0246-2236
старший викладач кафедри кібербезпеки
Тернопільський національний технічний університет імені Івана Пулюя, Україна

Зростання кількості та складності кіберзагроз ставить перед організаціями важливе завдання захисту мережевої інфраструктури від різноманітних атак. Однією з таких загроз є DoS-атаки, які спрямовані на перевантаження ресурсів мережі та призводять до відмови в обслуговуванні реальних користувачів. У цьому контексті важливо розробити ефективні засоби виявлення та зменшення впливу DoS-атак на рівні мережевого обладнання.

В роботі проведено аналіз різноманітних типів DoS-атак, їхніх характеристик та впливу на мережеву інфраструктуру [1]. Серед яких особливо виділяються атаки на доступність, такі як TCP SYN Flood, ICMP Flood, та UDP Flood. Ці атаки можуть викликати перевантаження каналів зв'язку та ресурсів пристроїв, що веде до відмови в обслуговуванні для законних користувачів [2]. Дослідницький процес включав аналіз впливу цих атак на окремі рівні моделі OSI, що дозволило краще зрозуміти їхні наслідки та визначити ефективні методи протидії.

Було розроблено та налаштовано тестове середовище для моделювання DoS атак. Це середовище включало в себе гіпервізор VMware ESXi, на якому були створені наступні віртуальні машини: маршрутизатор MikroTik CHR, Ubuntu Linux з вебсервером, DNS-сервером та SSH, а також Windows 10 для тестування якості зв'язку під час атаки. [3]. Базовою платформою для розробки системи зменшення впливу DoS-атак було обрано маршрутизатор MikroTik CHR [4]. Це обґрунтовано широким функціоналом даного маршрутизатора та можливістю програмування на скриптовій мові.

Під час моделювання атак за допомогою Parrot Security без системи зменшення впливу DoS-атак спостерігалось значне використання ресурсів маршрутизатора MikroTik (рис. 1).

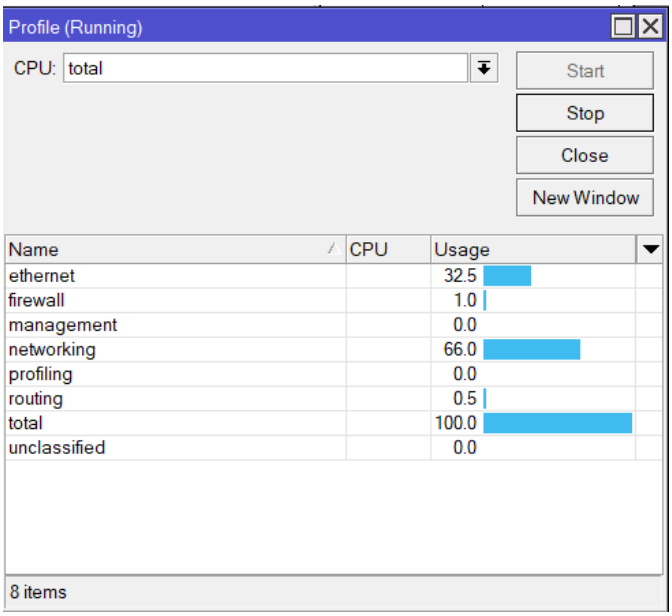

Рис 1. **Використання ресурсів маршрутизатора MikroTik без налаштованого механізму зменшення впливу DoS-атак**

Розроблена методика виявлення та зменшення впливу DoS-атак на основі маршрутизаторів MikroTik включає в себе аналіз трафіку, виявлення аномалій та застосування механізмів обмеження та блокування шкідливого трафіку. Основною метою дослідження було визначення ефективних заходів захисту від DoS-атак на рівні маршрутизатора MikroTik.

Результати досліджень свідчать про ефективність розроблених механізмів захисту. Маршрутизатор MikroTik зумів ефективно фільтрувати трафік та виявляти аномальну активність, що дозволило зменшити вплив DoS-атак як на мережеву інфраструктуру загалом, так і на маршрутизатор MikroTik (рис. 2)

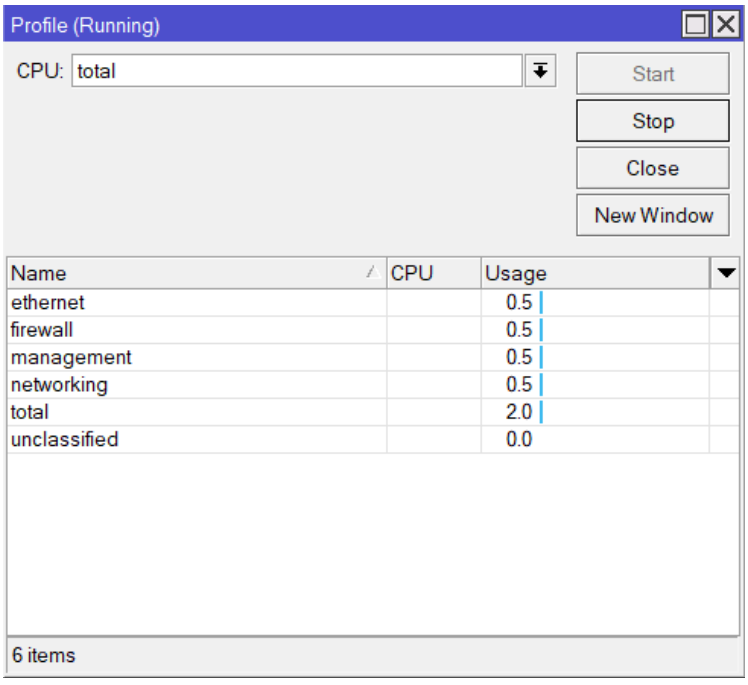

Рис 2. **Використання ресурсів маршрутизатора MikroTik з налаштованим механізмом зменшення впливу DoS-атак**

Маршрутизатори з функцією брандмауера зазвичай є першими лініями оборони мережі, тому їх захист від атак є важливим для забезпечення нормальної роботи всієї мережевої інфраструктури.

Висновки. Запропонована методика є ефективним інструментом для захисту мережевої інфраструктури від шкідливого впливу атак на відмову в обслуговуванні. Отримані результати мають практичне значення для адміністраторів мереж та спеціалістів з інформаційної безпеки, які займаються захистом від DoS-атак. Подальші дослідження будуть включати розширення аналізу інших типів атак та вдосконалення методів їх виявлення та протидії на рівні мережевої інфраструктури.

Список використаних джерел:

1. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. *Collection of scientific papers «SCIENTIA»*, (November 24, 2023; Kraków, Poland), 130-130.
2. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. *Матеріали конференцій МНЛ*, (3 листопада 2023 р., м. Вінниця), 177-178.
3. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. *Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології "Тернопільського національного технічного університету імені Івана Пулюя*, 95-95.
4. Cloud hosted router, CHR - routeros - mikrotik documentation. (б.д.). Взято з https://help.mikrotik.com/docs/display/ROS/Cloud+Hosted+Router,+CHR