International Conference on Information and Knowledge Management. New York : Association for Computing Machinery, 2020. P. 2725–2732.
6. Essa E., Omar K., Alqahtani A. Fake news detection based on a hybrid BERT and LightGBM models // Complex & Intelligent Systems. 2023. Vol. 9. P. 6581–6592.
7. Leite, J. A., Razuvayevskaya, O., Bontcheva, K., Scarton, C. EUvsDisinfo: A dataset for multilingual detection of pro-Kremlin disinformation in news articles. Proceedings of the 33rd ACM International Conference on Information and Knowledge Management. New York: Association for Computing Machinery, 2024, pp. 5380–5384.
8. Kyslyi, R., Romanyshyn, N., Sydorskyi, V. The UNLP 2025 Shared Task on Detecting Social Media Manipulation. Proceedings of the Fourth Ukrainian Natural Language Processing Workshop, 2025, pp. 105–111. URL: https://aclanthology.org/2025.unlp-1.12.pdf.

Середовище для аналізу атак на SDN-орієнтовані системи

УДК 004.056:004.7

Юрій Кльоц[1], Сергій Мостовий[2]

Хмельницький національний університет,
[1]klots@khmnu.edu.ua, [2] serhii.mostovyi@khmnu.edu.ua

Сучасні мережеві інфраструктури дедалі частіше використовують централізовані засоби керування, моніторингу та конфігурування обладнання, що наближає їх до принципів програмно-конфігурованих мереж. Одним із прикладів такої системи є Omada Controller, який забезпечує централізоване керування маршрутизаторами, комутаторами, точками доступу та бездротовими клієнтами. Концентрація керуючих функцій в одному компоненті підвищує зручність адміністрування, однак одночасно формує критичну точку впливу для потенційних атак.

Атаки на SDN-системи можуть бути спрямовані на порушення доступності контролера, зміну або блокування службової взаємодії між контролером і мережевими пристроями, імітацію легітимної активності, перевантаження каналів керування або виявлення вразливих сервісів. Особливу складність становить те, що частина атакувального трафіку за окремими ознаками може бути подібною до нормальних службових процесів, зокрема реєстрації пристроїв, оновлення станів, обміну телеметрією або підключення клієнтів. Тому дослідження таких атак потребує не лише фіксації факту аномальної активності, а й аналізу варіативності нормального трафіку в умовах реальної або наближеної до реальної мережевої інфраструктури [2].

Використання готових наборів пакетів для розроблення методів виявлення та протидії атакам не завжди забезпечує достатню достовірність результатів. Такі набори часто не враховують особливостей конкретного контролера, моделі мережевого обладнання, структури службового обміну, кількості клієнтів, типів підключення та характеру адміністративних дій. Крім того, у відкритих датасетах зазвичай складно встановити точний контекст формування трафіку, умови проведення атаки та відповідність отриманих пакетів реальним

сценаріям експлуатації. Це обмежує можливість коректної оцінки ефективності алгоритмів виявлення аномалій і може призводити до надмірної кількості хибних спрацювань або пропуску специфічних для конкретної системи атак.

На рис. 1 представлено структурну схему експериментальної мережі для дослідження нормального та аномального трафіку, пов'язаного з роботою Omada Controller. Центральним елементом схеми є маршрутизатор TP-Link, до якого підключено вхідний інтернет-канал, машину з установленим Omada Controller, звичайний комутатор, PoE-комутатор, а також окремі машини для збору пакетів. Така побудова дає змогу відтворювати типові умови функціонування мережі з централізованим керуванням та одночасно фіксувати трафік у ключових точках інфраструктури.

У нижній частині схеми показано клієнтську частину мережі. До звичайного комутатора підключено два дротові ПК, а до PoE-комутатора – дві точки доступу, через які працюють декілька Wi-Fi-клієнтів. Один із внутрішніх вузлів позначено як досліджуваний пристрій, трафік якого може окремо дзеркалюватися на машину збору пакетів. Це дозволяє аналізувати поведінку конкретного пристрою в умовах штатної роботи або під час моделювання атакувальної активності.

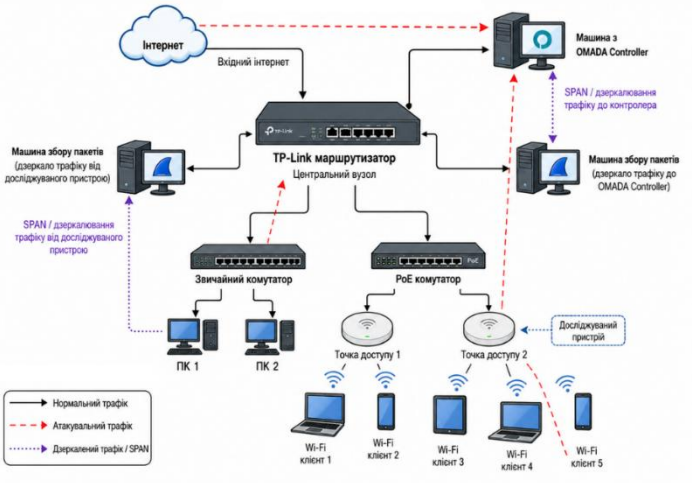

Рис.1. Схема дослідження трафіку та збору пакетів

Окремо на рисунку виділено машини збору пакетів. Одна з них призначена для фіксації дзеркального трафіку, що надходить до Omada Controller, інша – для збору трафіку від досліджуваного пристрою. Для позначення різних типів потоків використано умовні лінії: суцільні стрілки відповідають нормальному мережевому трафіку, пунктирні червоні стрілки – атакувальному трафіку, а фіолетові пунктирні лінії – дзеркальованому трафіку/SPAN. Така схема відображає можливість одночасного дослідження штатної взаємодії між компонентами мережі та виявлення змін у трафіку під час атак на контролер або окремі мережеві пристрої.

Отже, дослідження атак на SDN-орієнтовані системи керування мережею є актуальним, оскільки централізація функцій адміністрування, моніторингу та керування трафіком підвищує критичність контролера як об'єкта захисту. На прикладі Omada Controller показано, що використання лише готових наборів пакетів не завжди забезпечує достовірність результатів, адже вони можуть не враховувати особливості конкретної топології, службової взаємодії пристроїв і реальних умов експлуатації. Запропонована експериментальна схема дає змогу формувати власний набір даних, фіксувати нормальний та атакувальний трафік у ключових точках мережі й створює основу для подальшої розробки методів виявлення аномалій та протидії атакам на системи централізованого керування мережею.

1. Mansoor, A., Anbar, M., Bahashwan, A. A., Alabsi, B. A., & Rihan, S. D. A. (2023). Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller. Systems, 11(6), 296. https://doi.org/10.3390/systems11060296

Дослідження вразливостей протоколів динамічної маршрутизації

УДК 004.056.

Сергій Мостовий[1], Сергій Савченко[2]

Хмельницький національний університет,
[1]serhii.mostovyi@khmnu.edu.ua, [2]sserggii@yahoo.com

Корпоративні мережі постійно піддаються впливу різноманітних загроз, які можуть призвести до порушення конфіденційності, цілісності або доступності мережевих сервісів. У контексті динамічної маршрутизації ці загрози мають критичне значення, оскільки впливають на механізми обміну маршрутною інформацією, що є основою функціонування будь-якої IP-мережі. Завдяки використанню динамічних протоколів маршрутизації, таких як RIP, OSPF, IS-IS, EIGRP, та BGP [1,3], забезпечується автоматичне оновлення таблиць маршрутизації в реальному часі, що дозволяє адаптувати мережу до змін. Однак, ці самі властивості роблять протоколи маршрутизації вразливими до різноманітних атак, що можуть порушити їхню функціональність і безпеку.

Загрози у корпоративних мережах можна умовно класифікувати на кілька груп, кожна з яких стосується певних аспектів функціонування мережі.

Перша група загроз стосується маршрутизаторів та мережевого обладнання. Ці загрози включають атаки, метою яких є виведення маршрутизатора з ладу або отримання доступу до його конфігурації [1].

Друга група загроз - загрози цілісності маршрутної інформації. Зловмисники можуть змінювати або підмінювати маршрутні оголошення, що суттєво впливає на мережу. У межах динамічної маршрутизації подібні дії можуть спричинити перехоплення трафіку, його перенаправлення або повне блокування комунікацій [1].

Третя група загроз - загрози доступності. Атаки типу DoS (Denial of Service) та DDoS (Distributed Denial of Service) можуть спричинити перевантаження маршрутних процесів, що призводить до зниження продуктивності або відмови