УДК 004.738.5

АНАЛІЗ АТАК В ПРОГРАМНО-КЕРОВАНИХ МЕРЕЖАХ

Уривський Л.О., Могилевич В.Д.
Навчально-науковий інститут телекомунікаційних систем КПІ імені Ігоря Сікорського, Україна
E-mail: vadym.vadym63@gmail.com

ANALYSIS OF ATTACKS IN SOFTWARE-DEFINED NETWORKS

Дослідження присвячено аналізу типових атак, які можуть відбуватися в середовищі програмно-керованих мереж. У контексті швидкого розвитку технологій SDN, де управління мережею відокремлено від фізичної інфраструктури та здійснюється програмно, виникають нові виклики у забезпеченні безпеки та захисті мережевих ресурсів.

Постановка задачі. Програмно-керовані мережі (SDN) спрямовані на усунення проблем традиційних мереж (неефективне управління, загрози безпеці, стагнація інновацій через збільшення кількості користувачів, поява динамічних додатків та технологій гетерогенного доступу).

Основна ідея SDN [1, 2] полягає у відокремленні площин керування та передачі даних від мережевих пристроїв.

Площина управління виводиться з комутаторів і консолідується в логічно централізованому контролері. Контролер має інформацію про всю керовану мережу. Комутатори працюють як елементи переадресації і є програмованими. Вони можуть бути запрограмовані для різних цілей за допомогою мережевих додатків, що реалізовані на контролері. Комутатори, кінцеві хости та зв'язки між ними разом утворюють площину даних. Контролер з об'єднаною площиною управління - це або окремий сервер, або група логічно централізованих, але розподілених серверів. Контролер взаємодіє з комутаторами за допомогою інтерфейсів API. У випадку декількох серверів, контролери взаємодіють один з одним за допомогою східних та західних інтерфейсів. Мережеві додатки, що працюють поверх контролера, зв'язуються з ним за допомогою інтерфейсів.

Управління SDN спрямоване на вирішення різноманітних завдань, що стосуються ефективного та гнучкого керування мережевими ресурсами.

Однією з основних переваг SDN є централізоване управління мережевими ресурсами. Замість розподіленого управління на окремих мережевих пристроях, SDN дозволяє централізовано керувати всією мережею через центральний контролер.

SDN забезпечує платформу для розробки додатків безпеки та управління. Дослідники використовують цей аспект SDN для розробки різних фреймворків безпеки. Аналіз науково-технічної літератури показав, що безпеці самої SDN

не приділяється достатня увага в порівнянні з іншими дослідницькими роботами в цій області. Виклики безпеки в SDN є більш загрозливими порівняно з традиційними мережами. У традиційній мережі кілька серверів, що є частиною мережі стають об'єктами атак. На відміну від цього, якщо зловмисники компрометують площину управління SDN, під загрозою опиниться вся керована мережа [3, 4].

Отже, метою дослідження є аналіз та класифікація атак на програмно-керовану мережу.

Результати аналізу атак в мережі SDN.

Можна виділити такі загрози площини управління в SDN:

1. Несанкціонований доступ до контролера. Зловмисники можуть намагатися отримати несанкціонований доступ до контролера SDN, щоб отримати контроль над мережею і впливати на рішення, прийняті контролером.
2. Атаки на протоколи комунікації. Зловмисники можуть атакувати протоколи комунікації, використані в SDN, наприклад, OpenFlow, для впливу на трафік або виконання небажаних дій.
3. Використання вразливостей програмного забезпечення контролера. Наявність вразливостей у програмному забезпеченні контролера може використовуватися зловмисниками для виконання атак, таких як впровадження шкідливого коду або використання вразливостей для незаконного доступу.
4. Атаки на протоколи автентифікації. Зловмисники можуть намагатися атакувати протоколи автентифікації, використані в SDN, для отримання несанкціонованого доступу до системи інтелектуального управління мережею.
5. Атаки на апаратне забезпечення. Зловмисники можуть використовувати атаки на апаратне забезпечення, такі як фізичні атаки або використання вразливостей апаратного забезпечення, для отримання несанкціонованого доступу до контролера або підміни компонентів мережі.
6. Соціально-інженерні атаки. Зловмисники можуть використовувати соціально-інженерні методи, щоб отримати доступ до конфіденційної інформації або впливати на користувачів SDN, наприклад, шляхом фішингу або імітації привілейованих осіб.

Атаки на площину даних в SDN можуть включати наступні види загроз:

1. Атаки на протоколи комутації: атаки, спрямовані на протоколи комутації, такі як OpenFlow, можуть призвести до впливу на шляхи маршрутизації та пересилання даних у мережі SDN. Основне призначення OpenFlow полягає у розмежуванні логіки керування та обробки пакетів, що дозволяє розділити мережевий контроль на централізований контролер та розподілені комутатори.

Завдяки протоколу OpenFlow, контролер SDN може динамічно керувати маршрутизацією трафіку в мережі, встановлюючи правила потоків (flow rules) на комутаторах. Ці правила вказують комутаторам, які дії вони мають

виконувати з пакетами даних, що надходять до них. Наприклад, контролер може встановлювати правила, які вказують комутаторам, яким шляхом маршрутизувати певний тип трафіку або як обробляти пакети в залежності від їх характеристик або вмісту.

Цей підхід дозволяє мережі бути більш гнучкою та динамічною, оскільки правила потоків можуть бути змінені або оновлені централізовано з контролера без необхідності налаштовувати кожен комутатор окремо. Крім того, використання протоколу OpenFlow дозволяє реалізувати більш складні стратегії та забезпечує більший рівень автоматизації управління мережею.

2. Атаки на вузли комутації. Ці атаки спрямовані на вузли комутації, які керують обробкою пакетів даних у мережі SDN. До таких атак можна віднести атаки на самі вузли комутації (зловмисники можуть намагатися використовувати вразливості в програмному або апаратному забезпеченні) або на їхне фізичне середовище. До типових атак на фізичний рівень вузлів комутації SDN можна віднести:

Вплив на фізичні з'єднання та фізичне руйнування вузлів комутації: зловмисники можуть спробувати фізично пошкодити або знищити комутатори та кабелі зв'язку, що може призвести до втрати зв'язку та зниження доступності мережі.

Спроби фізичного доступу*:* атаки можуть включати спроби фізичного доступу до комутаторів з метою незаконного внесення змін у їхню конфігурацію, підключення шкідливих пристроїв або перехоплення мережевого трафіку.

Атаки на фізичний канал зв'язку: зловмисники можуть спробувати перехопити або модифікувати фізичний канал зв'язку між комутаторами або між комутаторами та контролером SDN, наприклад, шляхом використання атак на кабелі зв'язку.

Зловживання фізичними портами: зловмисники можуть намагатися зловживати фізичними портами комутаторів, наприклад, підключенням до них шкідливих пристроїв або спробами отримати несанкціонований доступ до мережі.

Атаки на канал зв'язку (перехоплення): зловмисник може перехопити (щоб отримати доступ до конфіденційної інформації) або модифікувати (щоб змінити маршрутизацію трафіку) трафік між контролером SDN та вузлом комутації.

Відмова в обслуговуванні (DoS): зловмисник може перевантажити вузол комутації фальшивим трафіком, щоб зробити його недоступним для законних користувачів.

Атаки на тунелювання даних: у мережах SDN можуть використовуватися тунелювання для передачі даних між вузлами. Зловмисники можуть намагатися перехоплювати або модифікувати дані, що передаються через ці тунелі, або використовувати їх для здійснення атаки на внутрішню мережу.

3. Атаки на контролер: зловмисник може намагатися атакувати контролер SDN, який керує всією мережею, шляхом використання вразливостей в програмному забезпеченні або переповнення буферів. Це може призвести до збоїв у роботі мережі та втрати контролю над мережею.

4. Атаки на мережеві пристрої: зловмисник може намагатися атакувати мережеві пристрої, такі як файерволи, перехоплювачі пакетів або мережеві монітори, щоб отримати доступ до конфіденційної інформації або вплинути на роботу мережі.

5. Атаки на шифрування даних: зловмисник може намагатися атакувати шифрування даних, що передаються через мережу SDN, для отримання несанкціонованого доступу до конфіденційної інформації або впливу на роботу мережі.

Висновки. Програмно-керовані мережі, як і будь-які інші мережеві середовища, піддаються різноманітним атакам з боку зловмисників.

Основні типи атак в програмно-керованих мережах включають атаки на контролери мережі, перехоплення пакетів, введення некоректної інформації у потокові таблиці, використання вразливостей в програмному забезпеченні та багато інших.

Важливою частиною управління програмно-керованими мережами є розуміння потенційних ризиків та вчасна реакція на атаки шляхом вдосконалення захисних механізмів та використання сучасних технологій кібербезпеки.

Ідентифікація та дослідження атак в програмно-керованих мережах є актуальним та важливим напрямком у галузі кібербезпеки і вимагає подальших досліджень для розробки нових методів захисту та забезпечення стабільності цих мереж.

Література

1. Goransson P., Black C. Software Defined Networks. A Comprehensive Approach: training manual. Publisher Morgan Kaufmann, 2014. – 352 p.
2. Software-Defined Networks. A Systems Approach: training manual / Systems Approach LLC, 2020. – 194 p.
3. Abdulsamad A.A., Salih, T.A. IoT security improvement based on SDN Controller. Eurasian Journal of Engineering and Technology, 2023. № 14. 49 – 56. URL: https://geniusjournals.org/index.php/ejet/article/view/3199.
4. Sheng C., Bai J. Sun Q Software-Defined Wide Area Network Architectures and Technologies: training manual. CRC Press, 2013 . – 460 p.