DOI: https://doi.org/10.26642/ten-2024-1(93)-246-254
УДК 004.056

Є.М. Трокоз, ст. викладач
О.А. Покотило, ст. викладач
Н.О. Щур, ст. викладач
Державний університет «Житомирська політехніка»

Моделювання загроз канального рівня в OWASP Threat Dragon з розробкою стратегії захисту

(Представлено: д.т.н., доц., Воротніков В.В.)

Моделювання загроз є важливим процесом, коли йде мова про забезпечення безпеки мережі на всіх рівнях, адже воно дозволяє визначити потенційні вразливості та загрози, які можуть впливати на конфіденційність, цілісність та доступність даних. Забезпечення захисту канального рівня є особливо важливим, оскільки саме він відповідає за передачу даних між пристроями в локальній мережі. З метою ефективного виявлення та усунення його вразливостей, запропоновано варіант побудови моделі загроз в середовищі OWASP Threat Dragon, яке надає можливості її візуалізації та дієвого управління ризиками. Для ідентифікації загроз обрано модель STRIDE, також запропоновано шкалу для оцінювання їх ризиків. Для забезпечення більшого розуміння вразливостей за побудованою моделлю згенеровано звіт, який дає можливість ефективного аналізу поточної інформації. Завдяки моделюванню загроз канального рівня вдалося розробити ефективні рішення для підвищення мережевої безпеки. Це дозволить запобігти потенційним атакам цього рівня та зменшити можливі ризики. Створена модель загроз може бути використана в багатьох практичних сценаріях, зокрема для проведення поглибленого аналізу каналів передачі даних та виявлення можливих шляхів атак. Також її доцільно використовувати для оцінки ризиків та розроблення стратегій захисту, що передбачатимуть застосування шифрування, контролю доступу та аутентифікації. Крім того, модель може покращити навчання співробітників, підвищуючи їх обізнаність щодо захищеності мережевої інфраструктури.

Ключові слова: *модель загроз; атаки; канальний рівень моделі OSI; OWASP Threat Dragon.*

Актуальність теми. Стрімкий розвиток технологій зв'язку та збільшення складності мережевих інфраструктур викликає серйозне занепокоєння щодо безпеки мережі. Багато організацій впроваджують заходи безпеки саме на вищих рівнях моделі OSI (Open Systems Interconnection). Канальний рівень, хоч і належить до нижчих рівнів, але є критично важливим для забезпечення ефективної та безпечної передачі даних. Тому його вразливості можуть мати суттєві наслідки для мережі. Враховуючи це, побудова моделі загроз, яка дозволить виявити можливі слабкі місця та розробити стратегію захисту для пом'якшення ризиків, є досить важливим заданням.

Аналіз останніх досліджень та публікацій, на які спираються автори. Зокрема, аналіз досліджень за вказаною тематикою показав, що атаки на канальний рівень мережі постійно вдосконалюються, що призводить до необхідності розробки ефективних моделей загроз та впровадження надійних заходів безпеки. Авторами статті [1] розглянуто та проаналізовано існуючі моделі мережних атак з метою визначення перспектив використання моделей, які мають специфічні властивості: можливість оцінки ймовірності атаки, визначення стратегії виявлення атаки та зручний формальний опис для автоматизації управління захистом. На основі цього аналізу вибрано найбільш адекватні моделі для автоматизації заходів захисту.

У роботі П.В. Кучернюк [2] наведено перелік типових загроз комп'ютерним мережам на фізичному і канальному рівнях моделі OSI, а також проведено аналіз особливостей методів і технологій захисту. Отримані результати дозволяють прийняти рішення стосовно вибору методів захисту для мереж з різним призначенням та вимогами до захисту інформації. В публікації В.Фарбітник, А.Лагун [3] розглядаються аспекти захисту інформації, включаючи причини, цілі та методи. Також досліджуються основні моделі захисту інформації, велика увага приділяється проблемам, що виникають у процесі їх створення на прикладі комп'ютерної мережі захищеної лабораторії.

Праця Nataliya Shevchenko, Timothy A. Chick, Paige O'Riordan, Thomas Patrick Scanlon та Carol Woody [4] присвячена розгляду дванадцяти різних методів моделювання загроз та їх особливостей. Вибір найбільш оптимального методу має базуватися на багатьох критеріях, зокрема, кількості часу на моделювання, наявному практичному досвіді та ін. В публікації Yassine Ayachi, El Hassane Ettifouri, Jamal Berrich та Bouchentouf Toumi [5] основною метою є створення загальної моделі найбільш відомих та небезпечних вебатак з метою їх кращого розуміння та задля прийняття найадаптованіших до бізнесу

та технічного середовища стратегій безпеки. Отримані результати можуть бути корисними і для оцінювання систем виявлення вторгнень.

У статті Mahapara Mahak та Yashwant Singh [6] обґрунтовується необхідність забезпечення безпеки та конфіденційності IoT. Крім того, авторами переоцінюються деякі з існуючих моделей загроз і методологій оцінки ризиків. Робота Krasen Parvanov та Chrysostomos Tsagkidis [7] демонструє важливість кібербезпеки для IoT, зокрема звертається увага на моделювання загроз та оцінку вразливостей у процесі розробки програмного забезпечення. Проведене авторами дослідження показує, що існує потреба в належній інтеграції моделювання загроз у загальний процес розробки та у запровадженні систематичного підходу до оцінки вразливостей та тестування безпеки.

Метою статті є дослідження процесу побудови моделі загроз канального рівня у спеціалізованому програмному середовищі OWASP Threat Dragon з метою розробки ефективної стратегії захисту мережевих інфраструктур. Для досягнення поставленої мети необхідно визначити можливі загрози та потенційні наслідки, які вони можуть спричинити, і, на базі цієї інформації, побудувати діаграму, яку надалі використовувати для визначення методів та засобів захисту, які будуть найбільш ефективними.

Викладення основного матеріалу. Моделювання загроз є одним з ключових процесів, який надає можливість проводити аналіз, попереджувати або нейтралізувати потенційні загрози безпеці на рівні мережевої інфраструктури. Воно спрощує процес розуміння вразливостей, ідентифікації ризиків та подальшої розробки ефективної стратегії захисту, а також забезпечує можливість передбачення атак та їх завчасного пом'якшення.

Для побудови моделі загроз канального рівня потрібно уважно розглянути всі аспекти мережевої інфраструктури, а також налаштування протоколів, що використовуються для комутації даних. Важливо врахувати різноманітні сценарії атак та можливі наслідки їх реалізації, щоб забезпечити повноту та об'єктивність аналізу.

Канальний рівень – це другий рівень моделі OSI, який відповідає за передачу даних між двома пристроями, що безпосередньо підключені в межах однієї локальної мережі через різні фізичні засоби зв'язку, зокрема кабелі та бездротові з'єднання. На цьому рівні інформація з кадрів перетворюється на біти для подальшої передачі через мережу, а також відбувається виявлення та виправлення помилок.

На канальному рівні можуть виникати загрози, що впливатимуть на нормальне функціонування мережі та безпеку передачі даних. Вони призводять до порушення конфіденційності, цілісності та доступності мережної інформації, а також до відмови в обслуговуванні. Атаки на канальний рівень найчастіше полягають у підробці зловмисником дійсних облікових даних або у спробі імітувати легальний запит, щоб перехопити мережевий трафік. Вони можуть бути спрямовані на комутатори та маршрутизатори, на пристрої другого рівня моделі OSI (мережеві адаптери, мости, концентратори та ін.) або використовувати вразливості в протоколах канального рівня, щоб порушити роботу мережі, отримати несанкціонований доступ до ресурсів або розповсюдити шкідливе програмне забезпечення.

Основними незахищеними точками комутаторів є алгоритм прозорого моста, таблиця комутації та вхідні й вихідні буфери. Зазвичай саме ці слабкі місця стають об'єктами атак на канальний рівень. Вразливості канального рівня створюють можливість для здійснення різноманітних атак, серед яких варто виокремити такі категорії:

1. Атаки на MAC-адреси та таблицю комутації спрямовані на використання або зміну MAC-адрес пристроїв для перехоплення або несанкціонованої модифікації трафіку (MAC-Flooding, MAC-Sniffing) або мають на меті переповнення та маніпулювання CAM-таблицею комутатора (CAM Overflow);
2. Атаки на протокол STP використовують вразливості протоколу STP (недостатній рівень аутентифікації, авторизації, заходів безпеки) для маніпуляцій шляхами в мережевому дереві (STP MiTM, STP Provocated Sniffing, STP DoS);
3. Атаки на протокол DHCP спрямовані на вичерпання пулу доступних IP-адрес, що може спричинити тимчасову відмову в обслуговуванні, або на створення нелегітимного DHCP-сервера з метою видачі недійсної мережевої інформації (DHCP Starvation/DHCP Exhaustion, DHCP DoS, DHCP Server Spoofing/Rogue DHCP Server);
4. Атаки на протокол ARP проводяться для маніпуляції або зміни IP- та MAC-адрес та спотворення зв'язків між ними шляхом маскування зловмисника під легітимний хост (ARP-Flooding, ARP-Spoofing, ARP-Poisoning) [8].

У таблиці 1 наведено порівняльну характеристику основних типів атак за такими критеріями, як мета, спосіб їх здійснення та потенційні наслідки для мережі. Після визначення основних атак на канальний рівень мережі, наступним кроком є вибір середовища моделювання для їх оцінки та подальшого аналізу. Важливо обрати таке програмне забезпечення, яке відображає реальні умови та конфігурації мережі, враховуючи різноманітні типи пристроїв та протоколів. Крім того, воно має підтримувати методологію моделювання загроз STRIDE, яка буде використана надалі [9]. Для цього дослідження було обрано спеціалізоване програмне забезпечення OWASP Threat Dragon, яке дозволить побудувати модель загроз, враховуючи результати аналізу, наведені вище.

Таблиця 1

Атаки на канальний рівень моделі OSI

Тип атаки	Мета атаки	Спосіб здійснення	Потенційні наслідки
MAC-Flooding	Переповнення таблиць комутації на комутаторі	Генерація і відправлення великої кількості широкомовних кадрів на комутатор	Зниження швидкості мережі, відмова в обслуговуванні легітимних запитів
MAC-Sniffing	Отримання несанкціонованого доступу до мережних ресурсів	Підробка MAC-адреси адаптера відправника іншою MAC-адресою	Порушення конфіденційності або цілісності даних
CAM Overflow	Переповнення таблиць комутації на комутаторі	Формування і передача потоку кадрів з унікальними адресами відправника в мережу	Відмова в обслуговуванні легітимних запитів, зниження продуктивності мережі
STP MiTM	Отримання несанкціонованого доступу до трафіку	Використання технік «Man-in-the-Middle» для маніпулювання STP	Перенаправлення трафіку до атакуючого пристрою
STP Provocated Sniffing	Перехоплення трафіку для прослуховування	Відправка BPDU в мережу, щоб примусити інші пристрої переключитися на небезпечний порт	Можливість зловживання конфіденційністю та інформацією про користувачів
STP DoS	Створення перешкод нормальному функціонуванню STP	Відправлення фальшивих керуючих пакетів для виклику відмови в роботі STP	Відмова в обслуговуванні, зниження швидкості мережі
DHCP Starvation / DHCP Exhaustion	Спроба зайняти всі доступні адреси IP або ресурси DHCP-сервера	Генерація унікальних ідентифікуючих повідомлень з різними MAC-адресами відправника	Відсутність можливості новим пристроям отримати IP-адреси
DHCP DoS	Надмірне навантаження DHCP-сервера або мережі DHCP-запитами	Відправка великої кількості DHCPDISCOVER-пакетів з різними MAC-адресами	Відсутність можливості новим пристроям отримати IP-адреси, відмова в обслуговуванні мережі
DHCP Server Spoofing / Rogue DHCP Server	Перехоплення ролі легального DHCP-сервера для зловмисного	Розгортання фальшивого DHCP-сервера у мережі ближче до кінцевого пристрою	Недоступність легітимного DHCP-сервера, надання невірної мережевої конфігурації клієнтам
ARP-Flooding	Переповнення ARP-таблиць на пристроях	Відправлення великої кількості підробних ARP-запитів у мережу	Перекривання легітимних ARP-запитів, зменшення продуктивності мережі
ARP-Spoofing	Виведення з ладу легітимних вузлів мережі	Підробка ARP-відповідей з метою перенаправлення трафіку	Перехоплення чутливої інформації, відмова у можливості передачі трафіку
ARP-Poisoning	Перенаправлення трафіку на пристрій зловмисника	Відправлення фальшивих ARP-пакетів для сповільнення роботи мережі	Несанкціоноване використання переспрямованого трафіку

Побудуємо модель загроз канального рівня для мережі без налаштувань функцій безпеки. До елементів цієї ІКС належать: комутатор, локальна мережа з встановленим DHCP-сервером, файл конфігурації комутатора, таблиця комутації, ARP-таблиця, робоча станція легального користувача, робоча станція зловмисника з встановленими аналізатором трафіку та інструментами для проведення атак. Важливо на діаграмі загроз зазначити потоки даних між елементами ІКС: вхідні та вихідні кадри, зчитування та запис у сховища даних, повідомлення протоколів ARP, STP та DHCP. Діаграма елементів ІКС з потоками даних між ними наведена на рисунку 1.

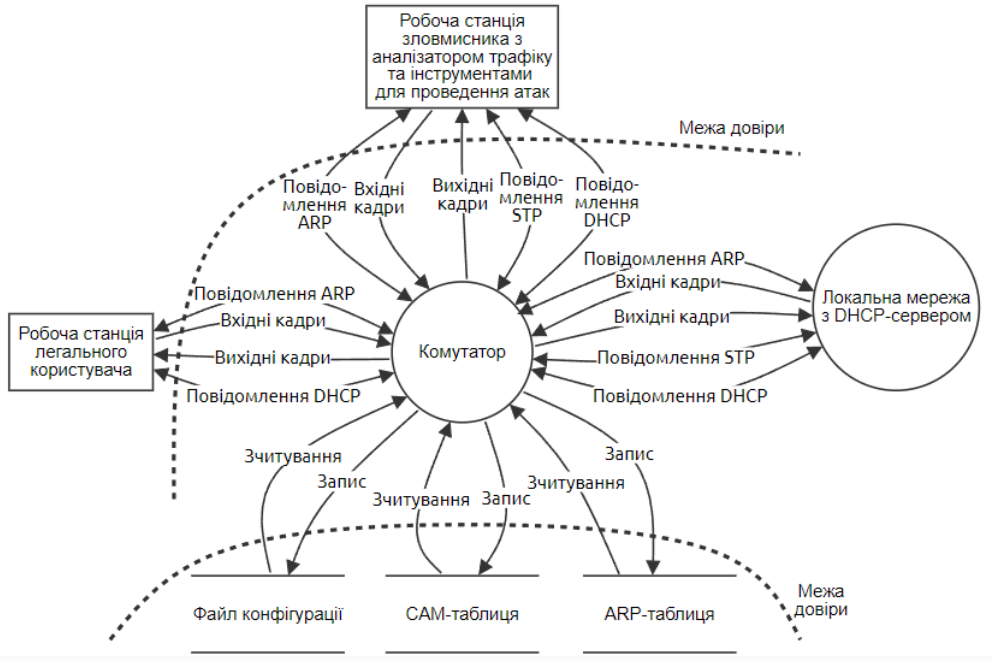

Рис. 1. Діаграма елементів ІКС з потоками даних

Проаналізувавши вразливості та атаки на протоколи канального рівня, перейдемо до визначення критичних елементів ІКС (з відкритими загрозами) та типу загроз. Критичними елементами для цієї ІКС є робоча станція легального користувача, комутатор, локальна мережа з DHCP-сервером, CAM-таблиця та ARP-таблиця.

Для ідентифікації загроз було використано модель STRIDE, що використовується для аналізу та оцінки безпеки інформаційних систем. Вона допомагає ідентифікувати потенційні загрози та вразливості, які можуть виникнути внаслідок атак або недоліків у системі. Основні складові методики STRIDE є абревіатурою:

1. Spoofing Identity (підробка ідентичності): атаки, які спрямовані на підробку або використання інших ідентифікаторів для отримання несанкціонованого доступу до ресурсів;
2. Tampering with Data (підробка даних): це атаки, коли зловмисник маніпулює даними в системі, змінюючи їх в недозволений спосіб;
3. Repudiation (заперечення або відмова від авторства): ситуації, коли сторона відмовляється визнавати факт виконання певної дії, такі як відмова від відповідальності за виконання дій у системі;
4. Information Disclosure (розголошення інформації): атаки, що спрямовані на незаконне отримання доступу до конфіденційної інформації;
5. Denial of Service (відмова в обслуговуванні): атаки, які спрямовані на перешкоджання нормальному функціонуванню системи або відмову в обслуговуванні легітимних користувачів;
6. Elevation of Privilege (підвищення привілеїв): це атаки, коли зловмисник намагається отримати більше привілеїв або доступу до системи, ніж у нього має бути [10].

Згідно з методикою STRIDE визначені загрози належать або до типу Denial of Service (відмова в обслуговуванні), або Spoofing Identity (підробка ідентичності).

Кількісну оцінку рівня загрози було проведено за такою шкалою:

- 1 – низький рівень загрози;
- 3 – середній рівень загрози;
- 5 – високий рівень загрози.

При додаванні загрози до елементів ІКС зазначається її назва, тип згідно з методикою STRIDE, статус (невизначений / відкрита /пом'якшена), рівень, пріоритет (низький, середній, високий), короткий опис та методи пом'якшення. Всі загрози будуть відкритими, оскільки за основу береться мережа без налаштувань засобів захисту. Пріоритет загрози обирається згідно з рівнем потенційного впливу цієї загрози на стан безпеки ІКС. На рисунку 2 показано процес додавання загроз реалізації атак на протокол ARP, для інших загроз – процес аналогічний.

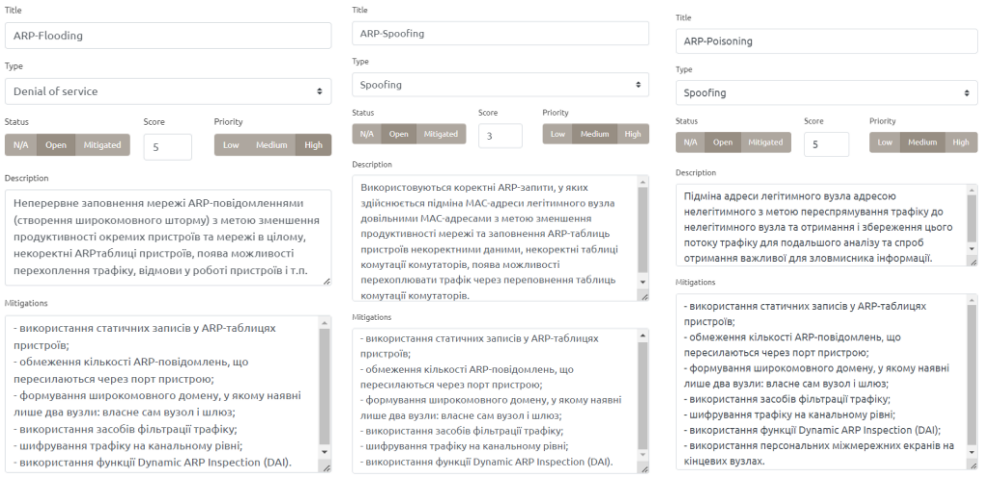

Рис. 2. Загрози реалізації атак на протокол ARP

Після того, як було додано загрози, критичні елементи ІКС на діаграмі будуть виділені червоним кольором (рис. 3).

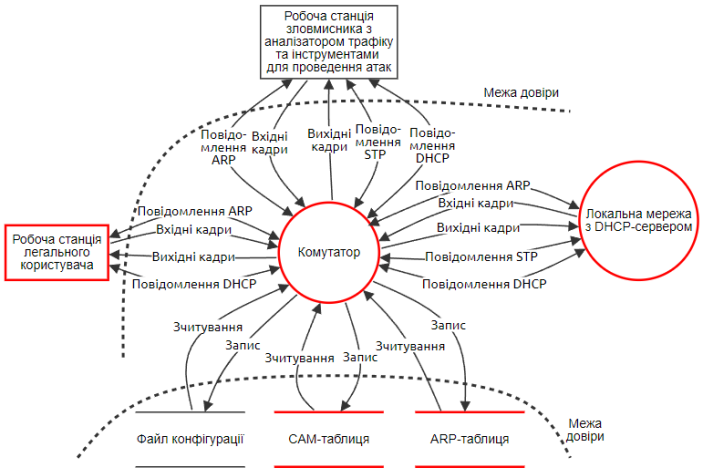

Рис. 3. Діаграма загроз канального рівня

Для того, щоб переглянути усі додані загрози для окремого критичного елемента ІКС, потрібно вибрати / виділити цей елемент і ці загрози будуть показані у вікні Threats. Приклад виведення загроз, які можуть порушити роботу комутатора, представлено на рисунку 4.

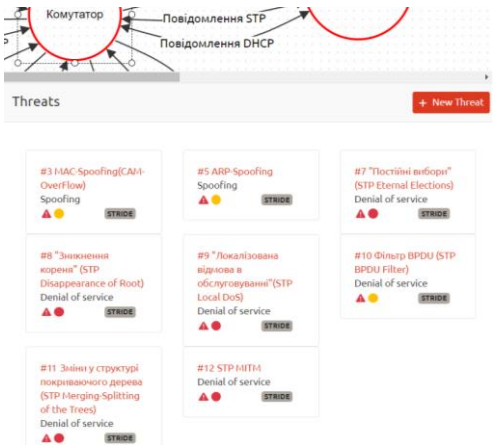

Рис. 4. Загрози комутатору

Для зручності перегляду поточної інформації по загрозах, є можливість зробити звіт по створеній моделі. В ньому буде виведено короткe резюме по загрозах (загальна кількість, кількість пом'якшених / усунутих загроз, кількість відкритих загроз, кількість відкритих загроз з високим, середнім, низьким та невизначеним пріоритетами), створена діаграма та опис загроз для кожного елемента ІКС (назва, її тип, пріоритет, статус, рівень та методи / способи пом'якшення). Приклад опису загроз для елемента ІКС «Робоча станція легального користувача» наведено на рисунку 5.

Робоча станція легального користувача (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	MAC-Spoofing(MAC-Sniffing)	Spoofing	High	Open	5	Підміна зловмисником MAC-адреси власного інтерфейсу на MAC-адресу інтерфейсу легального користувача з метою перехоплення трафіку.	- формування статичних записів в таблиці комутації; - використання функції, яка дає можливість зазначити MAC-адреси кінцевих вузлів, яким дозволено передавати дані через певний порт.
6	ARP-Poisoning	Spoofing	Medium	Open	5	Підміна адреси легітимного вузла адресою нелегітимного з метою перенаправлення трафіку до нелегітимного вузла та отримання і збереження цього потоку трафіку для подальшого аналізу та спроб отримання важливої для зловмисника інформації.	- використання статичних записів у ARP-таблицях пристроїв; - обмеження кількості ARP-повідомлень, що пересилаються через порт пристрою; - формування широкомовного домену, у якому наявні лише два вузли: власне сам вузол і шлюз; - використання засобів фільтрації трафіку; - шифрування трафіку на канальному рівні; - використання функції Dynamic ARP Inspection (DAI); - використання персональних міжмережних екранів на кінцевих вузлах.
15	DHCP Server Spoofing/Rogue DHCP Server	Spoofing	High	Open	5	Якщо фальшивий сервер встановлено в мережі, за замовчуванням, він отримує повідомлення DHCPDISCOVER від клієнтів що шукають IP-адресу, яку можна отримати. На цій стадії відбувається змагання між фальшивим та істинним DHCP серверами. По причині того, що клієнт знаходиться ближче до фальшивого сервера, то більш ймовірно що фальшивий сервер отримає перемогу.	- розробка загальної схеми IP-адресації та чіткий розподіл IPадрес між вузлами мережі; - налагодження ручного виділення IP-адрес на DHCP-сервері мережі; - використання функції Port Security на комутаторах мережі; - використання функції DHCP-Snooping на комутаторах мережі.

Рис. 5. Опис загроз для елемента ІКС «Робоча станція легального користувача»

Відповідно до визначених вразливостей, загроз та варіантів їх пом'якшення, було запропоновано таку стратегію захисту:

1. Захист від атаки MAC-Flooding:
   - налаштування комутаторів на обмеження кількості дозволених MAC-адрес на кожному порті з використанням функції Port Security;
   - розділення мережі на VLAN для обмеження розповсюдження атаки на весь мережевий сегмент;
   - використання систем моніторингу мережевого трафіку для виявлення аномальних змін у рівні активності або надмірного трафіку, які можуть свідчити про атаку;
   - використання інтелектуальних комутаторів, які можуть автоматично виявляти та обмежувати незвичайну активність на портах;
   - налаштування Rate Limiting на комутаторах для обмеження швидкості прийняття вхідного трафіку на портах;
2. Захист від атаки MAC-Spoofing:
   - блокування неправомірного трафіку шляхом визначення списку дозволених MAC-адрес на кожному порті;
   - використання протоколу 802.1X для вимагання аутентифікації користувачів перед наданням доступу до мережі;
   - реалізація Network Access Control (NAC), яка дозволяє перевіряти стан пристроїв та вимагати виконання обов'язкових вимог перед наданням доступу до мережі;
   - встановлення статичних MAC-адрес у таблицях комутаторів для критичних пристроїв;
3. Захист від атак на протокол ARP:
   - конфігурація ARP Inspection на комутаторах для перевірки відповідності між IP-адресами та MAC-адресами в ARP-пакетах;
   - ручне встановлення статичних ARP-записів на критичних мережевих пристроях для уникнення маніпуляцій зловмисників;
   - використання Dynamic ARP Inspection (DAI) для перевірки та аутентифікації ARP-пакетів перед їх пересиланням;

- використання Private VLANs (PVLANs) з метою обмежити зв'язок між різними пристроями в мережі;
- регулярний моніторинг ARP-трафіку у мережі, який може допомогти вчасно виявити аномальність в ARP-відповідях або спотворення ARP-таблиць;

4. Захист від атак на протокол STP:

- налаштування BPDU Guard на портах комутаторів для автоматичного блокування портів, які приймають неправомірні BPDU-пакети;
- налаштування Root Guard на портах, які не мають бути частиною шляху до кореневого комутатора, що запобігає зміні кореневого комутатора через ці порти;
- налаштування Loop Guard на портах, які налаштовані в режимі резервного або альтернативного порту з метою захисту від атак на спотворення топології мережі;
- використання Portfast на портах, які підключені до групи пристроїв, таких як кінцеві пристрої або сервери, що допомагає уникнути проблем з автоконфігурацією STP і зменшити час переходу до активного стану;
- налаштування фільтрації BPDU на портах, що призначені для клієнтських пристроїв, які не підтримують STP;
- налаштування Port Security на портах комутаторів для обмеження кількості дозволених MAC-адрес на порті;
- регулярний моніторинг STP-пакетів у мережі для виявлення аномальної активності або спроби атак на протокол STP;

5. Захист від атак на протокол DHCP:

- налаштування DHCP Snooping на комутаторах для перевірки легітимності DHCP-відповідей і блокування неправомірних DHCP-пакетів;
- використання DHCP Relay Agent на маршрутизаторах або комутаторах для пересилання DHCP-запитів до відповідного DHCP-сервера;
- налаштування DHCPv6 Guard на інтерфейсах маршрутизаторів або комутаторів для перевірки легітимності DHCPv6-пакетів;
- використання аутентифікації 802.1X для перевірки легітимності пристроїв перед наданням доступу до мережі;
- встановлення статичних DHCP-записів на DHCP-сервері для прив'язки певних IP-адрес до конкретних MAC-адрес;
- регулярний моніторинг DHCP-трафіку у мережі.

Ці стратегії захисту від атак канального рівня можна комбінувати та налаштовувати відповідно до конкретних потреб і характеристик мережі. Важливо постійно оновлювати програмне забезпечення мережевого обладнання та проводити моніторинг безпеки мережі для виявлення та запобігання новим загрозам.

Висновки та перспективи подальших досліджень. У ході роботи було проведено аналіз загроз канального рівня та визначено атаки, які можуть вплинути на безпеку мережевої інфраструктури. Для ідентифікації загроз було використано модель STRIDE та визначено шкалу для кількісної оцінки їх рівня. Побудована діаграма дозволила візуалізувати загальну структуру, а додавання до її елементів відповідних загроз допомогло розробити ефективну стратегію захисту.

Подальші дослідження можуть бути спрямовані на розробку більш автоматизованих інструментів для виявлення та пом'якшення загроз, які легко інтегруватимуться у мережеві системи. Крім того, перспективним напрямом є створення стратегій захисту, які охоплюють не лише канальний рівень, а й інші рівні моделі OSI для забезпечення комплексної безпеки мереж.

Список використаної літератури:

1. *Казакова Н.* Аналіз методів моделювання кібернетичних атак / *Н.Казакова, Ю.Щербина, О.Фразе-Фразенко* // Інформаційні технології та комп'ютерне моделювання : матеріали статей Міжнародної науково-практичної конференції, 20–25 травня. – Івано-Франківськ, 2019 [Електронний ресурс]. – Режим доступу : https://eprints.cdu.edu.ua/4180/1/zbirnyk2019.pdf#page=184.
2. *Кучернюк П.В.* Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні) / *П.В. Кучернюк* // Мікросистеми, Електроніка та Акустика. – 2017. – № 6. DOI: 10.20535/2523-4455.2017.22.6.113191.
3. *Фарбітник В.* Дослідження основних проблем при побудові моделей захисту інформації в комп'ютерній мережі захищеної лабораторії / *В.Фарбітник, А.Лагун* // Інформаційна безпека та інформаційні технології : збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, 26 листопада. – Львів, 2021 [Електронний ресурс]. – Режим доступу : http://surl.li/sqkow.

4. Threat modeling: a summary of available methods / *N.Shevchenko, T.A. Chick, P.O'Riordan and other*. – Pittsburgh, United States : Carnegie Mellon University Software Engineering Institute, 2018 [Electronic resourse]. – Access mode : https://apps.dtic.mil/sti/pdfs/AD1084024.pdf.
5. Modeling the OWASP Most Critical WEB Attacks / *Y.Ayachi, E.H. Ettifouri, J.Berrich, B.Toumi* // Information Systems and Technologies to Support Learning: Proceedings of EMENA-ISTL. – 2018. – Vol. 111. DOI: 10.1007/978-3-030-03577-8_49.
6. *Mahak M.* Threat Modelling and Risk Assessment in Internet of Things: A review / *M.Mahak, Y.Singh* // Proceedings of Second International Conference on Computing, Communications, and Cyber-Security : Lecture Notes in Networks and Systems. – 2021. – Vol. 203. DOI: 10.1007/978-981-16-0733-2_21.
7. *Parvanov K.A.* Threat modelling and vulnerability assessment for IoT solutions: a case study / *K.A. Parvanov, C.Tsagkidis*. – 2022 [Electronic resourse]. – Access mode : https://gupea.ub.gu.se/handle/2077/72699.
8. Network Security – Data Link Layer [Electronic resourse]. – Access mode : https://www.tutorialspoint.com/network_security/network_security_data_link_layer.htm.
9. *Покотило О.А.* Порівняльний аналіз програмного забезпечення для моделювання загроз / *О.А. Покотило, Є.М. Байлюк, Н.О. Щур* // Вісник Хмельницького національного університету. – 2023. – № 4 [Електронний ресурс]. – Режим доступу : http://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/09/323-268-277.pdf.
10. Threat Modeling Methodology: STRIDE [Electronic resourse]. – Access mode : https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride.

References:

1. Kazakova, N., Shcherbyna, Yu. and Fraze-Frazenko, O. (2019), «Analiz Metodiv Modeliuvannia Kibernetychnykh Atak», *Informatsiini tekhnolohii ta kompiuterne modeliuvannia*, materialy statei Mizhnarodnoi naukovo-praktychnoi konferentsii, 20–25 travnia, Ivano-Frankivsk, [Online], available at: https://eprints.cdu.edu.ua/4180/1/zbirnyk2019.pdf#page=184
2. Kucherniuk, P.V. (2017), «Metody i tekhnolohii zakhystu kompiuternykh merezh (fizychnyi ta kanalnyi rivni)», *Mikrosystemy, Elektronika ta Akustyka*, No. 6, doi: 10.20535/2523-4455.2017.22.6.113191.
3. Farbitnyk, V. and Lahun, A. (2021), «Doslidzhennia osnovnykh problem pry pobudovi modelei zakhystu informatsii v kompiuternii merezhi zakhyshchenoi laboratorii», *Informatsiina bezpeka ta informatsiini tekhnolohii*, zbirnyk tez dopovidei V Vseukrainskoi naukovo-praktychnoi konferentsii molodykh uchenykh, studentiv i kursantiv, 26 lystopada, Lviv, [Online], available at: http://surl.li/sqkow
4. Shevchenko, N., Chick, T.A., O'Riordan, P., et al. (2018), *Threat modeling: a summary of available methods*, Carnegie Mellon University Software Engineering Institute, Pittsburgh, United States, [Online], available at: https://apps.dtic.mil/sti/pdfs/AD1084024.pdf
5. Ayachi, Y., Ettifouri, E.H., Berrich, J. and Toumi, B. (2018), «Modeling the OWASP Most Critical WEB Attacks», *Information Systems and Technologies to Support Learning: Proceedings of EMENA-ISTL*, Vol. 111, doi: 10.1007/978-3-030-03577-8_49.
6. Mahak, M. and Singh, Y. (2021), «Threat Modelling and Risk Assessment in Internet of Things: A review», *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*, Lecture Notes in Networks and Systems, Vol. 203, doi: 10.1007/978-981-16-0733-2_21.
7. Parvanov, K.A. and Tsagkidis, C. (2022), «Threat modelling and vulnerability assessment for IoT solutions: a case study», [Online], available at: https://gupea.ub.gu.se/handle/2077/72699
8. «Network Security – Data Link Layer», [Online], available at: https://www.tutorialspoint.com/network_security/network_security_data_link_layer.htm
9. Pokotylo, O.A, Bailiuk, Ye.M. and Shchur, N.O. (2023), «Porivnialnyi analiz prohramnoho zabezpechennia dlia modeliuvannia zahroz», *Visnyk Khmelnytskoho natsionalnoho universytetu*, No 4, [Online], available at: http://journals.khnu.km.ua/vestnik/wp-content/uploads/2023/09/323-268-277.pdf
10. «Threat Modeling Methodology: STRIDE», [Online], available at: https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride

Трокоз Єлизавета Максимівна – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0000-0002-4961-7816.

Наукові інтереси:

- захист інформації в інформаційно-комунікаційних системах;
- проєктування, побудова та експлуатація комп'ютерних мереж.

Покотило Олександра Андріївна – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0000-0002-1587-235X.

Наукові інтереси:

- інформаційна безпека;
- прикладна криптологія.

Щур Наталія Олександрівна – старший викладач кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка».

https://orcid.org/0000-0002-1182-4799.

Наукові інтереси:

- криптографічний захист даних;
- інформаційна безпека.

Trokoz Ye.M., Pokotylo O.A., Shchur N.O.

Modelling link-level threats in OWASP Threat Dragon with the development of a protection strategy

Threat modelling is an important process when it comes to securing a network at all levels, as it helps identify potential vulnerabilities and threats that could affect the confidentiality, integrity and availability of data. Ensuring the protection of the data link layer is particularly important, as it is responsible for the transmission of data between devices on a local network. In order to effectively identify and eliminate its vulnerabilities, we propose a variant of building a threat model in the OWASP Threat Dragon environment, which provides opportunities for its visualisation and effective risk management. The STRIDE model is chosen to identify threats, and a scale for assessing their risks is proposed. To provide a better understanding of vulnerabilities, a report was generated based on the model, which allows for effective analysis of current information. Thanks to the modelling of link-level threats, we managed to develop effective solutions to improve network security. This will prevent potential attacks at this level and reduce possible risks. The created threat model can be used in many practical scenarios, including in-depth analysis of data transmission channels and identification of possible attack paths. It can also be used to assess risks and develop protection strategies that include encryption, access control and authentication. In addition, the model can improve employee training by raising their awareness of the security of network infrastructure.

Keywords: threat model; attacks; link layer of the OSI model; OWASP Threat Dragon.

Стаття надійшла до редакції 17.04.2024.