Байлюк Є. М., ст. викладач
кафедри комп'ютерної інженерії та кібербезпеки
Покотило О. А., ст. викладач
кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

ПОБУДОВА МОДЕЛІ ЗАГРОЗ ДЛЯ АТАК MAC-FLOODING ТА MAC-SPOOFING З ВИКОРИСТАННЯМ OWASP THREAT-DRAGON

Кожного дня інформаційно-комунікаційні системи та мережі піддаються величезній кількості кібератак. Зловмисники використовують різноманітні методи та способи для їх реалізації. Зокрема, це вразливості різних алгоритмів та протоколів. Метою таких кібератак є виведення з ладу всієї мережі чи її частини, або отримання доступу до конфіденційної чи таємної інформації. При цьому, зловмисники в більшості випадків здійснюють кібератаки, які найпростіше реалізувати.

Досить популярними є атаки канального рівня, найбільш відомими серед яких є MAC-Flooding та MAC-Spoofing. Такі атаки відносяться до атак відмови в обслуговуванні. При успішній їх реалізації, вся мережа може бути недоступною, або значно зменшується її продуктивність, в результаті чого, легальні користувачі не матимуть доступу до ресурсів спільного користування. Обидва типи атак використовують вразливості алгоритму прозорого моста, за яким працюють комутатори. При реалізації атаки MAC-Flooding зловмисником в мережу надсилається потік широкомовних (або групових чи унікальних з невідомими адресами призначення) кадрів. В результаті генерується великий об'єм трафіку, що значно навантажує обчислювальні ресурси комутатора і призводить до відмови у доступі до ресурсів мережі [1]. Атака MAC-Spoofing більше орієнтована на таблицю комутації. При реалізації даної атаки зловмисник може мати на меті або переповнення таблиці комутації(CAM OverFlow), шляхом надсилання в мережу потоку кадрів з унікальними адресами відправника, або перехоплення мережного трафіку(MAC-Sniffing) для отримання необхідної інформації[2].

Першим кроком для попередження або усунення загроз будь-якого типу є побудова моделі загроз. Для цього було обрано OWASP Threat-Dragon, що є найбільш зручним інструментом моделювання загроз з усіх наявних на даний момент. Спочатку було визначено усі елементи та потоки даних, які можуть брати участь під час реалізації вищезгаданих атак. Окрім того, було зроблено припущення, що зловмисник буде проводити атаки за допомогою відповідних утиліт ОС Kali Linux. Створена діаграма загроз наведена на рис.1.

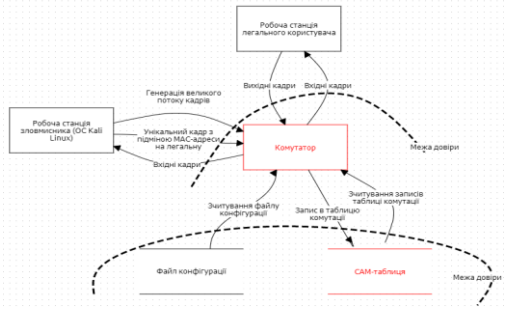

Рис.1. Діаграма загроз, побудована за допомогою програми OWASP Threat-Dragon

Окрім того, OWASP Threat-Dragon дає можливість описати загрози будь-якому елементу діаграми загроз з врахуванням типу загроз, їх рівня та з можливими діями(порадами) для пом'якшення чи усунення загрози. Визначені загрози з їх описом показані на рис.2.

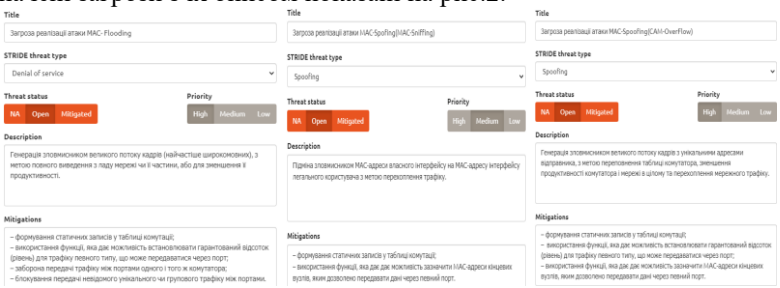

Рис.2. Загрози реалізації атак MAC-Flooding та MAC-Spoofing

В результаті проведеного дослідження було визначено механізми, способи та засоби реалізації атак MAC-Flooding та MAC-Spoofing. На основі досліджень побудовано модель загроз за допомогою OWASP Threat-Dragon. Крім того, було визначено методи та способи пом'якшення даних загроз. Створена модель загроз допоможе при плануванні заходів забезпечення безпеки роботи комутаторів.

Список використаних джерел

1.MAC Flooding Program. URL: https://cybercademy.org/mac-flooding-program-project-overview/ (дата звернення 20.11.2022).
What is MAC spoofing? URL: https://www.ionos.com/digitalguide/server/know-how/what-is-mac-spoofing/ (дата звернення 20.11.2022).