УДК 004.056

В.А. ТИХОМИРОВ, Н.Г. МИЛОСЛАВСКАЯ

Национальный исследовательский ядерный университет «МИФИ», Москва

ПОСТРОЕНИЕ ПРОЦЕССА УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ АКТИВОВ ТИПОВОЙ ИТКС НА ОСНОВЕ ГРАФОВЫХ МОДЕЛЕЙ КОМПЬЮТЕРНЫХ АТАК

Предложены подходы к приоритизации уязвимостей активов информационно-телекоммуникационных сетей (ИТКС) на основе анализа разработанного гиперграфа компьютерных атак (КА) и рассмотрению связей между этими уязвимостями при попытке злоумышленника реализовать КА. Исследованы основные характеристики получившегося гиперграфа КА.

Введение

Анализ показал, что существующие методы построения графов КА не подходят для задач ранжирования уязвимостей активов ИТКС, поскольку они не позволяют управлять уязвимостями, а строят пути КА с использованием всех возможных техник и тактик. Эти модели не могут в реальном времени и автоматизированном режиме обрабатывать информацию об уязвимостях. Также не решены проблемы вычислительной сложности, обработки циклических зависимостей и интеграции вероятностных методов оценки. Актуальность исследования обусловлена необходимостью разработать процесс управления уязвимостями активов ИТКС, который бы учитывал не только критичность уязвимости для конкретного актива, но и то, как уязвимость сочетается с другими уязвимостями и некорректными конфигурациями.

Постановка задачи

Цель исследования – рассмотрев основы моделирования графов КА, провести систематический анализ современных подходов к построению и анализу графов КА, включая их классификацию, сравнение и математический аппарат оценки критичности маршрутов КА. Для достижения поставленной цели решались следующие задачи: анализ существующих подходов к описанию графов КА, формулирование методики создания графа КА для задач управления уязвимостями активов ИТКС, разработка алгоритма построения гиперграфа КА [1] и процесса управления уязвимостями [2] с применением графов КА.

Результаты исследования

В рамках исследования проанализированы актуальные подходы к формированию графов КА [3]. В результате выявлено, что существующие подходы к построению графов КА нерелевантны для выбранной задачи приоритизации уязвимостей активов ИТКС. Предложен новый подход к построению графов КА, с учетом специфики задачи приоритизации уязвимостей в рамках процесса управления уязвимостями активов ИТКС. Основа графа – это хостовой граф, который описывает возможные сетевые взаимодействия серверов между собой. В то же время, каждую вершину графа можно рассмотреть, как граф зависимостей эксплуатации, основанный на уязвимостях. В итоге получен гиперграф – пара $H = (X, E)$, где X − множество вершин, а E − семейство подмножеств X, называемых гиперребрами [1]. С учетом особенностей двухуровневого гиперграфа (уровень хоста и уровень сети) разработан алгоритм приоритизации уязвимостей на основе степени посредничества уязвимости в графе.

Выявление многофакторных уязвимостей активов ИТКС, как и выявление уязвимостей архитектуры ИТКС, в автоматизированном режиме возможны лишь при учете связей между разными активами и их уязвимостями, которые злоумышленник может проэксплуатировать при проведении КА. Выявить такие связи можно при помощи построенной графовой модели перемещения злоумышленника в ИТКС организации, включая использование базы данных *CVE*.

Заключение

Созданы методика формирования графа КА, ее формализованное представление и модель гиперграфа КА. На этой основе и NIST SP 1800-5 разработан процесс управления уязвимостями активов ИТКС. Далее предлагаемая модель и алгоритм оценки и приоритизации уязвимостей будут реализованы на практике.

Список литературы

1. Hypergraphs: Combinatorics of Finite Sets [Hypergraphes: Combinatoire des ensembles finis] / Claude Berge. Amsterdam: North-Holland, 1989. 255 p. (North-Holland Mathematical Library; vol. 45). – ISBN 0- 444-87489-5

2. О безопасности критической информационной инфраструктуры Российской Федерации [федер. закон от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.; одобрен Советом Федерации 19 июля 2017 г.]. – 2017.

3. Zenitani K. Attack graph analysis: an explanatory guide. Computers & Security. 2023. Vol. 126. DOI: 10.1016/j.cose.2022.103081.