УДК 004.77

Малініч І. П.
Месюра В. І.
Малініч П. П.

ПРОБЛЕМИ СТВОРЕННЯ СЕРЕДОВИЩ ДЛЯ ВИЗНАЧЕННЯ ТИПУ СКАНУВАЛЬНОЇ АКТИВНОСТІ, ЩО ЗДІЙСНЮЄТЬСЯ ПРИ СКАНУВАННІ МЕРЕЖ

Вінницький національний технічний університет

Анотація

При роботі програмного забезпечення для сканування комп'ютерних мереж відбувається генерація мережевого трафіку різних видів. Для його подальшого дослідження необхідно здійснювати поділ на окремі види сканування: вертикальний, горизонтальний та сканування служб. Існує кілька методів визначення видів сканувального трафіку, зокрема з фіксацію часових проміжків та алгоритмічний. Розглянуто проблеми реалізації кожного з них при побудові віртуальних середовищ для збору даних.

Ключові слова: сканування комп'ютерних мереж, мережевий трафік, віртуальні мережеві середовища

Abstract

During use of scanning software for computer networks, network traffic of different types is generated. For its further study it is necessary to divide into separate types of scanning: vertical, horizontal and scanning of services. There are several methods for determining the types of scanning traffic, including time-lapse and algorithmic. The problems of application of each of them during building of virtual environments for data mining are reviewed.

Keywords: network scanning, network traffic, virtual network environments

Вступ

Різні додатки та скрипти для сканування комп'ютерних мереж можуть проявляти різну мережеву активність під час роботи. Для вивчення їх мережевої активності найбільш доцільним є побудова випробувального середовища для збору даних. Серед мережевих сканерів, яким приділено увагу є Nmap [1], Spiceworks IP Scanner, Advanced IP Scanner, Lizard Network Scanner, а також різні реалізації сканерів у вигляді скриптів.

При створенні віртуального середовища приділено увагу структурній схемі подібного середовища у статті [2], де було створено однорангову віртуальну мережу у вигляді єдиного широкомовного домену. Визначено найбільш продуктивні варіанти збору трафіку у подібних конфігураціях мереж завдяки наявності схожих варіантів у попередніх дослідженнях [3].

Необхідність пошуку та вирішення проблем створення середовищ для визначення типу сканувальної активності зумовлена потребою отримання найбільш точних даних про належність пакетів до кожної з фаз сканування мережі тим чи іншим програмним забезпеченням.

З огляду на залежність мережевої активності сканувального програмного забезпечення від архітектури випробувальної мережі також є потреба у максимальному наближенні віртуальних

середовищ до реальних умов віддаленого сканування для отримання найбільш практичних результатів.

Результати

При проектуванні віртуального випробувального середовища для визначення типу сканувальної активності досить важливим є визначення архітектури віртуальної мережі, що в свою чергу може впливати на процес сканування. Деякі сканери, такі як Nmap при виконанні горизонтального сканування на доступність хостів у одноранговій Ethernet-мережі замість надсилання пакетів ICMP Echo Request або деяких видів TCP-пінгу можуть виконувати сканування на другому рівні моделі Моделі OSI і використовувати протокол ARP, подібно до утиліти Arping [4].

Як наслідок для побудови середовища з віртуальних машин для визначення типу сканувальної активності використано віртуальну мережу з поділом на різні широкомовні домени шляхом використання віртуального маршрутизатора з перехопленням та фіксацією пакетів (рис. 1).

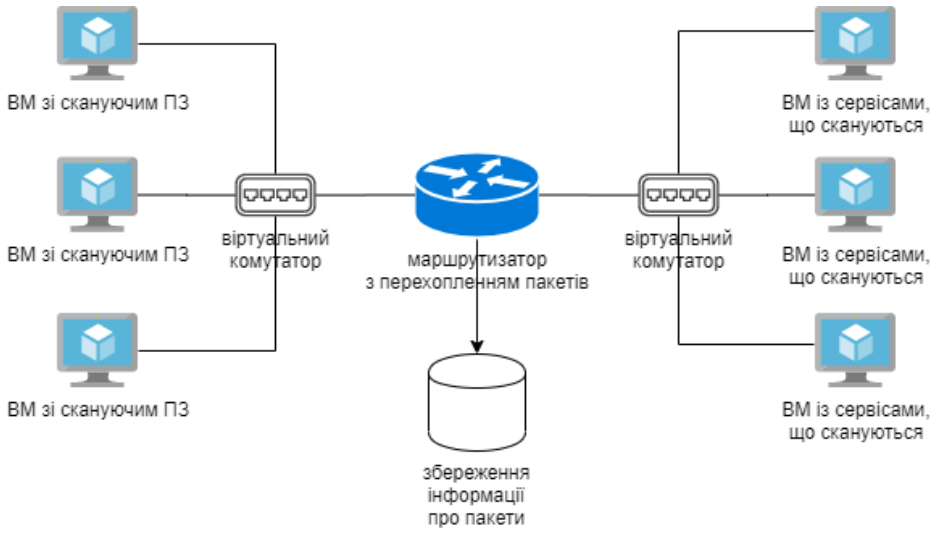

Рисунок 1 – Схема організації віртуального середовища для збору пакетів

Розподіл інформації про пакети, що проходять по мережі, по окремим фазам сканування є можливим завдяки методам визначення видів сканувального трафіку, зокрема з фіксацію часових проміжків та алгоритмічний. Кожен з методів має свої переваги та недоліки.

Метод з використанням фіксації часових проміжків використовує фіксацію часу передачі кожного пакету, а також відслідковує час зміни станів самої програми, яка здійснює сканування. Для відслідковування зміни станів програми можна використовувати як засоби відлагодження, якщо проект має відкритий поточний код, так і обробку повідомлень інтерфейсу командного рядка, якщо поточний код не є відкритим.

Перевагою даного методу є його простота реалізації. Однак він має багато недоліків, які досить негативно відзначаються на точності його роботи. Найбільш суттєвим є затримка пакетів при їх подальшій передачі в мережу та подальшому їх перехопленні. У деяких конфігураціях затримка перевищила 100 мс, що в свою чергу призвело до неправильного маркування належності пакетів до різних фаз сканування. Іншим недоліком є несумісність даного методу з паралельним

виконанням сканувальних завдань, що в свою чергу може також призвести до неправильного визначення належності пакету до конкретної фази.

Алгоритмічний метод має значно більше переваг у точності, але потребує створення алгоритмів для визначення належності кожного пакету до конкретної фази. Даний метод є більш надійним при затримці пакетів та при паралельному виконанні сканувальних завдань. Недоліками даного методу є необхідність підлаштовувати алгоритм виявлення для максимального покриття мережевої активності всього програмного забезпечення, за допомогою якого здійснюється сканування, щоб зменшити до мінімуму кількість пакетів, які неможливо віднести до жодної з фаз.

Незважаючи на простоту реалізації, метод з використанням фіксації часових проміжків уступає алгоритмічному у точності визначення належності пакетів мережевого трафіку до різних фаз сканування та не є пристосованим до роботи паралельних сканувальних задач.

Висновки

Розглянуто проблеми створення середовищ для визначення типу сканувальної активності, що здійснюється при скануванні мереж при використанні таких методів як фіксації часових проміжків та алгоритмічного. Приділено увагу роботі сканувального програмного забезпечення у різних конфігураціях віртуальних мереж. Визначено найбільш оптимальні конфігурації побудови віртуальних середовищ для визначення типу сканувальної активності різного програмного забезпечення. Розглянуто переваги та недоліки різних методів визначення належності пакетів мережевого трафіку до різних фаз сканування. Завдяки перевагам алгоритмічного методу, йому надано перевагу у подальшій роботі над його удосконаленням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gordon Fyodor Lyon. Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning [Text] / Lyon G. F. — Insecure, 2009. Sunnyvale, CA, USA — 464 p.
2. Singh, R. R., Tomar, D. S. Port Scanning Attack Analysis with Dempster-Shafer Evidence Theory [Text] / R. R. Singh, D. S. Tomar // International Journal of Applied Engineering Research. – 12(16). – 2017. – pp.5900-5904
3. Малініч І. П. Ін’єктивний метод отримання даних користувацького досвіду в ігрових симуляторах комп’ютерних мереж [Текст] / І. П. Малініч, В. І. Месюра // Вісник Вінницького політехнічного інституту. – 2019. – No 5. – С. 49-54.
4. Arping. Матеріал з Вікіпедії, вільної енциклопедії. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Arping.

Малініч Ілля Павлович, асистент кафедри комп’ютерних наук, Вінницький національний технічний університет, м. Вінниця, malinich@vntu.edu.ua

Месюра Володимир Іванович, кандидат технічних наук, професор кафедри комп’ютерних наук, Вінницький національний технічний університет, м. Вінниця

Малініч Павло Павлович, студент групи 1ПІ-18б, факультет ІТКІ, Вінницький національний технічний університет, м. Вінниця

Malinich Illia, assistant lecturer of Computer Sciences Department, Vinnytsia National Technical University, Vinnytsia, malinich@vntu.edu.ua

Mesyura Volodymyr, PhD, professor of Computer Sciences Department, Vinnytsia National Technical University, Vinnytsia

Malinich Pavlo, group 1PI-18b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia