УДК 004.93

М. В. Гикава

ВПЛИВ АТАК НА КОМП'ЮТЕРНУ МЕРЕЖУ ТА МЕТОДИ ЇХ ДОСЛІДЖЕННЯ

Вінницький національний технічний університет

Анотація

У даній роботі описуються вплив атак на комп'ютерну мережу, методи перевірки та запобігання атаки. Розглянуто питання про атаку переповнення буферу, можливий підхід для визначення ступіню пошкоджень та визначення необхідних дій для усунення атаки та її наслідків.

Ключові слова: переповнення буферу, лінійна регресія.

Abstract

This paper describes impact of attacks on computer network, test methods and prevention of attacks. The question of buffer overflow attacks, a possible approach to determine the extent of damage and determine the necessary actions to address the attack and its aftermath.

Keywords: buffer overflow, linear regression.

Забезпечення працездатності мережі і функціонуючих в ній інформаційних систем, залежить не тільки від надійності апаратури, а й від здатності мережі протистояти цілеспрямованим діям, які спрямовані на порушення її роботи [2].

Метою даного дослідження є збільшення швидкості виявлення та усунення наслідків атаки на комп'ютерну мережу. Об'єктом дослідження являються атаки та їхній вплив на комп'ютерну мережу.

Без належних заходів безпеки комп'ютерам в мережі загрожують самі різні фактори. Загрози безпеки можуть бути як внутрішніми, так і зовнішніми. Однією із самих серйозних являється загроза несанкціонованого доступу ззовні, в мережу, організації зломщиків (хакерів). Друга загроза – комп'ютерні віруси. Вони здатні спричинити значних збитків, а деякі з них можуть знищити всі файли в мережі [2].

Переповнення буфера давно відоме в області комп'ютерної безпеки. Навіть перший само-поширюючий Інтернет-черв'як - Черв'як Моріса 1988 року - використовував переповнення буфера в Unix-демоні finger для поширення між машинами. Двадцять сім років по тому, переповнення буфера залишається джерелом проблем [3].

Переповнення стека/буфера (stack/buffer overflow) — це аномальна ситуація, коли процес намагається записати свої дані за межі буфера фіксованої довжини. В результаті надлишкові дані записуються поверх сусідніх даних. Заміщені таким чином дані можуть бути іншими буферами, змінними, даними про роботу програми, що може призвести до аварійного завершення програми або одержання невірних результатів. Також переповнення може бути викликане вхідними даними, спеціально розробленими для виконання шкідливого коду чи щоб змусити програму поводитися непередбачувано [4, 5].

Переповнення буфера в стеку відбувається, коли перевірка виходу за межі не проводиться над даними, записуваними в статичний буфер. Якщо обсяг копійованих в стек даних перевершує розмір буфера, комп'ютер продовжує перезаписувати стек до тих пір, поки не досягне NUL-символу, переписуючи інші значення в стеку і деякі покажчики, які говорять програмі, що робити далі [1].

Проблема переповнення буфера найчастіше виникає в програмах підтримки, які є зовнішніми по відношенню до JVM. Сама JVM часто пишеться на мові C для конкретної платформи, тобто без належної уваги до деталей реалізації машина JVM може сама виявитися вразливою для атак на переповнення буфера.

Крім JVM, численні проблеми переповнення буфера характерні для систем, в яких використовується Java, і конкретно для програм підтримки роботи з Java.

Для дослідження характеру поведінки системи під дією атаки, найбільш доцільно використовувати принцип регресії.

При проведенні простої лінійної регресії основною задачею є визначення параметрів b і a. Після визначення цих параметрів, наприклад, можна спрогнозувати показник Y, що буде через один місяць або рік. Як відомо, найпростіша функція - лінійна функція, так що ми будемо шукати функцію виду:

$$K = f(x_1, x_2, m_1, m_2, a, b) \quad (1)$$

де x_1, x_2 – вхідні параметри системи;

m_1, m_2 – параметри атаки;

a, b – параметри, які визначають наслідки дії атаки;

При проведенні простої лінійної регресії основною задачею є визначення параметрів b і a. Після визначення цих параметрів, наприклад, можна спрогнозувати показник Y. Такий підхід лінійної регресії дозволяє визначити ступінь пошкоджень та спрогнозувати необхідні дії для усунення атаки та її наслідків.

Для отримання оцінки параметрів лінійної функції регресії взята вибірка, яка складається з векторних змінних (X,Y)

$$Y = a + b \times X \quad (2)$$

де $X = f(m_1, m_2)$ – характеристика системи, що дозволяє визначити напрямок та інтенсивність процесу атаки.

Отже, на початковому етапі потік інформації аналізується на наявність атаки. Якщо пошкоджень не виявлено передається інформація. Якщо виявлено атаку, визначається, які вона спричинила і спричинить в майбутньому можливі пошкодження. Визначаються методи нейтралізації атаки та пошкоджень. Після остаточної перевірки даних відправляється інформація адресату.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Joshua Hulse. Переполнение буфера [Електронний ресурс] / Joshua Hulse — Режим доступу: http:// securitylab.ru/analytics/421994.php
2. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, лето 2011. — С. 8-13.
3. Peter Bright. How security flaws work: The buffer overflow [Електронний ресурс] / Peter Bright. — Режим доступу: https://habrahabr.ru/post/266591
4. Кадер М. Типы сетевых атак, их описания и средства борьбы [Електронний ресурс] / М. Кадер. — Режим доступу: http://vmw.cnews.info/reviews/free/oldcom/security/ciscoattacks.shtml.
5. Колищак А. Атаки на переполнение буфера [Електронний ресурс] / Колищак А. — Режим доступу: https://securityvulns.ru/articles/bo.asp

Гикава Марія Вікторівна – факультет інформаційних технологій та комп'ютерної інженерії, група 2КН-16 м, Вінницький національний технічний університет, м. Вінниця, e-mail: maria.gykava@gmail.com

Науковий керівник: ***Суприган Олена Іванівна*** – к. т. н., доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.

Mariia V. Hykava – Department of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia e-mail: maria.gykava@gmail.com

Supervisor: ***Elena I. Supryhan*** – Cand Sc., Assistant Professor of the Chair of Computer Science, Vinnytsia National Technical University. Vinnytsia.