УДК 004.04

Д. М. Жаворонок

ВРАЗЛИВОСТІ БЕЗПЕКИ МЕРЕЖЕВОГО РІВНЯ WEB -ДОДАТКІВ

Вінницький національний технічний університет

Анотація

Виявлення та способи усунення вразливостей в додатках, які можуть привести до несанкційонованого доступу до інформації та втрачення конфедиційної інформації, яка має комерційний характер.

Ключові слова: web-додаток, нсд, мережеві екрани, вразливість, атаки.

Abstract

Dentification and methods for addressing vulnerabilities in applications that may lead to unauthorized access to information and loss of confidential information of a commercial nature.

Keywords: web application, unauthorized access to information, scanners, vulnerability, attacks

Виявлення можливих вразливостей мережевого рівня

Такий Web-сервери та Web-сайти - це об’єкти, які постійно піддаються небезпекі. Особливу увагу слід звернути на Web-сервери, серйозну загрозу для яких становлять хакери і віруси. Перші можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і змінити їх вміст, а також вивести з ладу сервер за допомогою розподіленої атаки (DDoS-атака).

Практично у майже будь-якій програмі є вразливості. Наявність вразливостей легко пояснюється через здатність людей допускати помилки. Велике програмне забезпечення (ПЗ) пише не одна людина, а ціла група. І досить часто помилки виникають при компонуванні модулів, створених різними програмістами[1]. Крім того, наявність вразливостей далеко не завжди визначається якістю написання ПЗ.

На сьогоднішній день компанії дуже рідко замислюються про безпеку своєї інформації в мережі і зовсім не приділяють цьому питанню уваги, часто починаючи вживати заходів лише після витоку або втрати важливої інформації.

Способи підвищення безпеки мережевого рівня

Щоб забезпечити або ж усунути існуючу проблему, пов'язану із захистом інформації, застереження від атак зловмисників корпоративного сайту, його бази даних або всередині мережі додатків, буде розглянуто рішення для діагностики вразливостей і моніторингу комп’ютерів в мережі.

Для того, щоб забезпечити високу безпеку мережевого рівня доцільно використовувати спеціальні сканери програмні або апаратні засоби, скануючі систему на предмет виявлення можливих проблем в безпеці [2], що дозволяють виявляти, оцінювати і усувати вразливості в мережі.

Сканери уразливості діляться на дві основні групи:

1. Сканери корпоративних мереж, призначення яких полягає в аналізі мережі на наявність відкритих портів, а також вразливостей в операційних системах і додатках.

2. Сканери уразливості веб-додатків. На даний момент їхня популярність зростає в силу того, що більшість комерційних організацій і банків використовують у своїй діяльності інтернет ресурси, захист яких стає важливим фактором. У цій роботі буде розглянуто більше інформації саме по цій групі.

Висновки

Пропоновані продукти мають всі можливості і засоби для ефективного виявлення і управління виправленнями вразливостей, які створені після аналізу та фільтрації результатів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Khan Khaled M. Managing Web Service Quality: Measuring Outcomes and Effectiveness. / Khaled M. Khan. – IGI Global, 2008. – 418 p.

2. Жуков Ю.В. Основы веб-хакинга. Нападение и за- щита / Юрий Викторович Жуков, 2012. – 206 с.

Жаворонок Дар'я Михайлівна — студентка групи УБ-14б, факультету менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: zhavoronok,dasha@gmail.com

Науковий керівник: ***Поплавський Анатолій Вацлавович*** — кандидат технічних наук, доцент кафедри менеджменту і інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця

Zhavoronok Daria M. — Department of Management and Information Security , Vinnytsia National Technical University, Vinnytsia, email: zhavoronok.dasha@gmail.com .

Supervisor: **Poplavskii Anatoliy V**. — Cand. Sc. (Eng), Assistant Professor of management and safety of the informative systems , Vinnytsia National Technical University,