УДК 004.93

М. В. Гикава

МЕТОДИ ПЕРЕВІРКИ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ В РЕЖИМІ АТАКИ

Вінницький національний технічний університет

Анотація

У даній роботі описуються основні методи перевірки роботи комп'ютерної мережі в режимі атаки. Розглянуто питання про вплив атаки на мережу, основні способи захисту від атак та їх наслідків. Визначено основні поняття та актуальність даної теми.

Ключові слова: комп'ютерна мережа, мережева атака.

Abstract

This paper describes the basic methods of verification of computer network attack mode. The question of the impact of the attacks on the network, the main ways to protect against attacks and their consequences. The basic concept and relevance of the topic.

Keywords: computer network, network attack.

На сьогоднішній день інформаційні технології проникли в усі сфери життя людини. Їх невід'ємною частиною є глобальна мережа Internet. Одним з головних завдань є забезпечення безпеки поводження інформації всередині мережі. Однією з небезпек для безпеки є мережеві атаки [1].

Знання методів атак необхідне для появи необхідних методів захисту. Багато компаній забезпечують власну безпеку, використовуючи мережеві екрани та механізми шифрування. Вся область мережевої безпеки досить обширна та еволюціонує з кожним кроком. Для початку визначемо основні поняття, а саме, що таке мережева атака та комп'ютерна мережа.

Мережева атака - дія, метою якого є захоплення контролю (підвищення прав) над віддаленою / локальної обчислювальної системою, або її дестабілізація, або відмова в обслуговуванні, а також отримання даних користувачів користуються цією віддаленої / локальної обчислювальної системою [1].

Комп'ютерна мережа (англ. Computer NetWork, від net - мережа і work - робота) - сукупність комп'ютерів, з'єднаних за допомогою каналів зв'язку і засобів комутації в єдину систему для обміну повідомленнями та доступу користувачів до програмних, технічних, інформаційних і організаційних ресурсів мережі [2].

На даний момент виділяють наступні атаки: mailbombing, переповнення буфера, використання спеціалізованих програм (вірусів, сніфферів, троянських коней, поштових черв'яків, rootkit-ів і т.д.), мережева розвідка, IP-спуфинг, man-in-the-middle, ін'єкція (SQL-ін'єкція, PHP- ін'єкція, міжсайтовий скриптинг або XSS-атака, XPath-ін'єкція), відмова в обслуговуванні (DoS- і DDoS-атаки),phishing-атаки [1].

Розглянемо деякі із зазначених атак та визначимо основні способи боротьби з ними.

Для атаки типу man-in-the-middle зловмисникові потрібен доступ до пакетів, що передаються по мережі. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії. Способи боротьби з цією атакою: використання шифрування даних [3].

Атака на переповнення буфера (buffer overflows) ґрунтується на пошуку програмних або системних вразливостей, здатних викликати порушення границь пам'яті і аварійно завершити додаток або виконати довільний бінарний код від імені користувача, під яким працювала вразлива програма. Якщо програма працює під обліковим записом адміністратора, то дана атака може дозволити отримати повний контроль над комп'ютером, на якому виповнюється дана програма [4].

Результатами даної атаки є порушення умов цілісності, доступності, конфіденційності інформації. Методами захисту є використання спеціальних «безпечних» аналогів небезпечних функцій, заборона на виконання коду в області стека, перевірка меж змінних при кожному доступі до них та ін [5].

Проаналізовані основні мережні атаки та способи протидії показали, що не дивлячись на можливість використання комплексних мір по захисту інформаційних систем, тобто цілеспрямованого застосування різних методів і засобів [5,6], найбільш надійним способом захисту комп'ютера є використання перевірених електронних ресурсів і дотримання жорстких умов розмежування привілеїв. Виявлено, що сучасний підхід до побудови систем виявлення мережних вторгнень і виявлення ознак комп'ютерних атак на інформаційні системи сповнений недоліків і вразливостей [6].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы [Текст] / А. Е. Боршевников // Современные тенденции технических наук: материалы междунар. науч. конф. — Уфа, лето 2011. — С. 8-13.
2. Шауцукова Л. З. Информатика. Теория (с задачами и решениями) [Електронний ресурс] / Л. З. Шауцукова. – Режим доступу: http://book.kbsu.ru/theory/
3. 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
4. Колищак А. Атаки на переполнение буфера [Електронний ресурс] / Колищак А. — Режим доступу: https://securityvulns.ru/articles/bo.asp
5. Защита от хакеров корпоративных сетей / [Ахмад Д.М., Дубравский И., Флин Х. и др.] ; под. ред. Р. Рассела. – Компания АйТи; ДМК Пресс. – 2005. – 864 с. - ISBN: 5-98453-015-5, 1-928994-70-9.
6. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при відділеній обробці даних / Я. В. Корпань // Методи захисту інформації в комп'ютерних системах і мережах. — 2015. — Т17, №2. — С. 39 – 46.

Гикава Марія Вікторівна – факультет інформаційних технологій та комп'ютерної інженерії, група 2КН-12б, 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.