Секція 7. Комп'ютерні технології інформаційної безпеки

УДК 681.3

ПРОГРАМНА СИСТЕМА ДЛЯ МОДЕЛЮВАННЯ ЗАХИЩЕНОСТІ ЛОКАЛЬНОЇ МЕРЕЖІ

Волошин М.Я.[1)], Маслияк Ю.Б.[2)]
Тернопільський національний економічний університет
[1)] магістрант; [2)] магістр

I. Постановка задачі

Із бурхливим розвитком на сьогоднішній день мережевих технологій, зокрема як розширення асортименту апаратного та програмного забезпечення мереж, так і збільшення територіального мережевого покриття, суттєво зростає актуальність захисту мереж від несанкціонованого доступу та різного роду атак [1, 3].

II. Мета роботи

Метою дослідження є підвищити захищеність локальної мережі на основі розробки програмної системи, яка дає можливість моделювати ситуації несанкціонованого доступу до ресурсів мережі та різного роду атак.

III. Особливості програмної реалізації системи

Проведено аналіз найбільш поширених видів локальних комп'ютерних мереж та технологій передачі даних у них. Вказано на засоби захисту мереж, зокрема програмні та апаратні рішення, а також правильність побудови мережевої архітектури. Переважна більшість існуючих програмно-апаратних комплексів захисту розроблені на основі операційної системи LINUX [2].

У результаті проведеного аналізу та узагальнення видів атак на комп'ютерні мережі, побудовані на основі протоколів TCP/IP та ARP, виділено декілька з них, які є найтиповішими та найпоширенішими для мережевих операційних систем сімейства Windows, це – широкомовний шторм (Broadcast Storm), багатоадресний шторм (Multicast Storm), ARP-спуфінг (ARP-Spoofing) [4].

Запропоновано розробити програмну систему, яка для операційних систем Windows, на модельному рівні імітує вказані типи атак на мережу та перевіряє правильність роботи мережних ресурсів. Структура програмної системи зображена на рисунку 1.

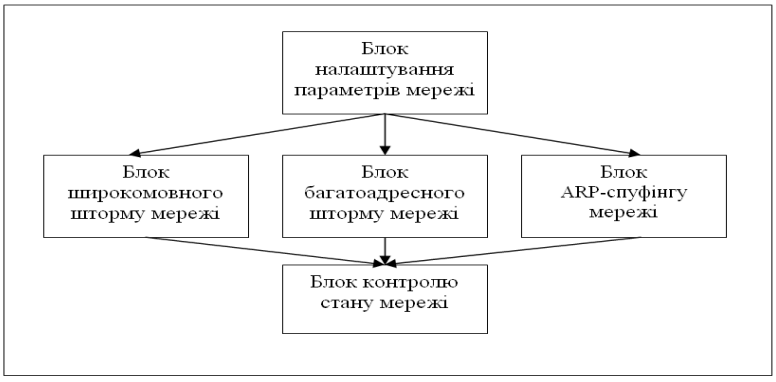

Рисунок 1 - Структура програмної системи

Програмна реалізація виконана на мові C# із використанням бібліотеки PCcap, яка дозволяє аналізувати дані з трафіку на мережевій карті.

Висновок

У роботі представлено задачу створення програмної системи для підвищення захищеності ресурсів локальної мережі від різного роду атак.

Список використаних джерел

1. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О.Г. Корченко, Г.Ф. Конахович. - Видавництво Інтерсервіс, 2009. -716 с.
2. Новіков О.М. Безпека інформаційно-комунікаційних систем / О.М. Новіков, М.В. Грайворонський. - Видавництво BHV, 2009. - 608 с.
3. Конахович Г. Ф. Защита информации в телекоммуникационных системах. - МК-Пресс, 2005. - 288 с.
4. Норткат С. Обнаружение нарушений безопасности в сетях / С. Норткат, Д. Новак. - Вильямс, 2003. - 448 с.

УДК 004.9

КРИТЕРІЙ ЕФЕКТИВНОСТІ ДЛЯ ВИЗНАЧЕННЯ СТІЙКОСТІ БЛОКОВИХ ШИФРІВ НА ОСНОВІ ВНЕСЕНИХ ЗМІН СТАТИСТИЧНИХ ХАРАКТЕРИСТИК ШИФРОВАНОГО ТЕКСТУ

Глухова О.В.[1)], Лозинський А.Я.[2)], Яремкевич Р.І.[3)], Ігнатович А.О.[4)]

Національний університет «Львівська політехніка»

[1)] бакалавр; [2), 3)] магістр; [4)]аспірант.

І. Постановка проблеми

Стійкість шифрів звичайно оцінюють за критерієм, який визначає необхідні ресурси для визначення типу шифру, визначення ключа і дешифрацію тексту. Деякі шифри дають велику кількість можливих варіантів ключів (наприклад – мільйони і десятки мільйонів варіантів). Якщо раніше такі кількості закривали будь-які перспективи роботи з такими шифрами, то зараз ситуація корінним чином змінилася. На сьогоднішній день таке питання вирішується масованими атаками з використанням великої кількості технічних і людських ресурсів. Відомо, що в багатьох країнах світу сформовані кібер-війська, які мають можливість масованими атаками з погодженими діапазонами дослідних процедур розкривати шифри, які мають мільйони варіантів можливих ключів. Такі кібер-війська сформовані в КНР, РФ, США, і т.д. Багато країн і не афішують такі питання, але зрозуміло, що в сучасних умовах вижити без серйозного інформаційного захисту просто неможливо.

ІІ. Мета роботи

В криптографії відомі тисячі шифрів, використовуються сотні сучасних комп'ютерних шифрів. Важливо скрити не тільки ключ, але і використаний метод шифрування. Такі підходи вимагають нові оціночні критерії нових методів шифрування. На сучасному етапі зрозуміло, що майже всі шифри можна розкрити – справа тільки в затрачених ресурсах і часі. Дуже важливим є маскування використаного методу шифрування. Це вже є елемент боротьби не з криптографами, а з кібер-військами, які за досить короткі терміни відкривають складні сучасні шифри (RSA, DES, AES, мережа Фейстеля і т.д.). Метою є пошук і оцінка ефективності шрифтів, в яких виконується як шифрування з допомогою сучасних шифрів, так і маскування використаних методів шифрування інформації.

ІІІ. Особливості реалізації

Розглянемо використання запропонованого критерію ефективності на основі шифру Хілла. Шифр Хілла з точки ефективності і надійності, якщо розглядати його як ручний шифр – він є досить трудомісткий і тому неефективний. Надійність цього шифру також має слабі місця. Спосіб шифрування на основі шифру Хілла – поліграмний блоковий шифр підстановки, заснований на лінійній алгебрі. Цей спосіб шифрування давав можливість зашифровувати більш ніж k символів за один цикл. Шифрування інформації відбувається наступним чином. Кожній букві відкритого тексту присвоюється число. Для латинського алфавіту часто використовується найпростіша схема: A = 0, B = 1, ..., Z = 25, але це не є істотною властивістю шифру. Блок з μ букв розглядається як μ-мірний вектор і множиться