УДК 004.057.4
ББК 32.973

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ СКАНИРОВАНИЯ ПОРТОВ

Ирина Сергеевна Кожевникова

Магистрант кафедры телекоммуникационных систем,
Волгоградский государственный университет
matuny77@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Алексей Олегович Пасюк

Ассистент кафедры телекоммуникационных систем,
Волгоградский государственный университет
molodoj88@gmail.com
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Ключевые слова: атака, обнаружение сканирования, вероятностный метод, статистический метод, эффективность.

Сканирование портов является подготовительным этапом перед проведением атаки [2]. От качества сканирования напрямую зависит успех реализации атаки, так как основными последствиями сканирования портов являются: получение списка открытых портов, списка закрытых портов, списка сервисов на портах хоста, предположительное определение типа и версии ОС [3].

На сегодняшний день проблема обнаружения сканирования портов на раннем этапе проведения является брешью при защите информации [1]. Не существует единого и комплексного подхода для обнаружения всех видов сканирования. Таким образом, целью данного исследования является создание алгоритма обнаружения сетевых аномалий, возникающих в процессе несанкционированного сканирования портов.

Исходя из этого, областью данного исследования является информационная защита устройств телекоммуникации, объектом исследования – ПЭВМ с сетевым интерфейсом, а предметом исследования – обнаружение процесса сканирования портов.

Для достижения поставленной цели, необходимо решить следующие задачи:

1. Провести анализ информационной системы предприятия.
2. Провести анализ угроз, связанных со сканированием портов.
3. Провести анализ механизмов защиты от сканирования портов в информационной системе предприятия.
4. Провести анализ существующих алгоритмов обнаружения сканирования портов.
5. Разработать математическую модель алгоритма обнаружения сканирования портов.
6. Разработать программное средство, реализующее алгоритм обнаружения сканирования портов.
7. Определить задачи экспериментальных исследований.
8. Провести экспериментальные исследования.
9. Провести анализ результатов экспериментальных исследований.

Существуют два алгоритма обнаружения сканирования портов: sa-, или вероятностный, метод, nt-, или статистический, метод [4].

В рамках данного исследования разрабатываемый алгоритм будет создан на основе статистического метода, поскольку он эффективно обнаруживает все виды сканирования портов.

Предполагается, что разработанный алгоритм, позволит увеличить уровень эффективности обнаружения сканирования на 20 %, что снизит вероятность реализации угроз и повысит уровень информационной безопасности сети.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ угроз, связанных со сканированием портов / В. С. Оладько, Е. В. Ананьин, И. С. Кожевникова, Л. В. Датская // Первые шаги в науку третьего тысячелетия : материалы XI Всерос. студ. науч.-практ. конф. с междунар. участием. – Нефтекамск, 2015. – С. 58.

2. Бредихин, С. В. Обнаружение сканеров в ip-сетях методом последовательного статистического анализа / С. В. Бредихин, В. И. Костин, Н. Г. Щербакова // Вестник НГУ. Серия: Информационные технологии. – 2009. – Т. 7, вып. 4. – С. 15.

3. Никишова, А. В. Программный комплекс обнаружения атак на основе анализа данных реестра / А. В. Никишова, А. Е. Чурилина // Вестник Волгоградского государственного университета. Серия 10. Инновационная деятельность. – 2012. – № 6. – С. 153.

4. Шлюзы безопасности: новая волна // Журнал сетевых решений/LAN. – 2010. – № 9.

RESEARCH OF THE PORT SCANNING DETECTION METHODS

Irina Sergeevna Kozhevnikova

Master Student, Department of Telecommunication Systems,
Volgograd State University
matuny77@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Alexey Olegovich Pasyuk

Lecturer Assistant, Department of Telecommunication Systems,
Volgograd State University
molodoj88@gmail.com
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Key words: attack, port scanning detection, probability method, statistical method, efficiency.