Тези доповідей 54-ої конференції молодих дослідників ОНПУ-магістрантів “Сучасні інформаційні технології та телекомунікаційні мережі” //Одеса: ОНПУ, 2019, вип. 54.
Секція 4 - аналіз та синтез інформаційно-аналітиних систем.

СИСТЕМИ ВИЯВЛЕННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ АНАЛІЗУ СТАНІВ СИСТЕМИ

РАЗРАБОТКА СИСТЕМЫ ОБНАРУЖЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АНАЛИЗА СОСТОЯНИЙ СИСТЕМЫ

DEVELOPMENT OF AN INFORMATION MODEL FOR AN INFORMATION SECURITY INCIDENT DETECTION SYSTEM BASED ON AN ANALYSIS OF SYSTEM CONDITIONS

Науковий керівник - доцент кафедри Радіотехнічних пристроїв
Агаджанян А.Р., Агаджанян А.Р., Aghajanian A.R.
Студент – Лозан А.Е., Лозан А.Э., Lozan A.E.,
Карнаушенко М.О., Карнаушенко Н.О., Karnaushenko N.O.

Анотація: Розглянуто архітектура побудови систем виявлення вторгнення і методи, які використовуються для виявлення інцидентів інформаційної безпеки.
Ключові слова: система виявлення вторгнення, архітектура СВВ, сигнатурний метод, поведінковий метод, інформаційна система.

Аннотация: Рассмотрена архитектура построения систем обнаружения вторжения и методы, которые используются для выявления инцидентов информационной безопасности.
Ключевые слова: система обнаружения вторжения, архитектура СОВ, сигнатурный метод, поведенческий метод, информационная система.

Abstract: The architecture of intrusion detection systems and the methods that are used to identify information security incidents are considered.
Key words: intrusion detection system, IDS architecture, signature method, behavioral method, information system.

Система виявлення вторгнень (СВВ) може бути реалізована, як програмне рішення, так і в якості апаратного засобу.

Дана система призначена для виявлення фактів несанкціонованого доступу до комп'ютерної системи, з подальшою можливістю управляти ресурсами скомпрометованої системи. Більш відомим терміном СВВ є Intrusion Detection System (IDS).

Система виявлення вторгнень використовується в якості додаткового рівеня захисту для виявлення мережевих атак [1].

Зазвичай архітектура СВВ включає:

- сенсорну підсистему, з метою збору даних про події, пов'язані з безпекою, що захищається системою;

- підсистему аналізу, з метою виявлення атак та підозрілих дій на основі даних від сенсорів;

- сховище, що забезпечує накопичення первинних подій і результатів аналізу;

- консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом захищеності системи та СВВ, переглядати виявлені підсистемою аналізу інциденти [2].

Сучасні методи виявлення вторгнень базуються на кількох основних принципах. Сигнатурний метод полягає в описі атаки, як особливої моделі або сигнатури, в якості якої може застосовуватися символьний ряд. Суть даного методу полягає в накопиченні вихідних даних за допомогою мережевих або вузлових датчиків, результати зберігаются в базі даних сигнатури, а потім здійснюється пошук сигнатури атаки.

Поведінковий метод, не використовує моделі іформаційних атак, натомість стан моделі стандартного функціювання інформаційної системи (ІС). Принцип таких методів базується на порівнянні станів системи в стандартному режимі роботи і станом системи в реальному часі, якщо виявляються невідповідності в ході роботи системи, ситуація розглядається, як атака. Перевага даного методу полягає у виявлені великої ймовірності нової атаки, без змін параметрів моделі. Створити детальну модель штатного режиму функціювання інформаційної системи дуже складно.

На стадії вторгнення виявити атаку можливо за допомогою, як сигнатурних, так і поведінкових методів. Будь-яке вторгнення характеризується певними ознаками, які, з одного боку, можна представити у вигляді сигнатури, а з іншого - описати як відхилення від штатної поведінки ІС. Найбільш ефективним є поєднання обох методів, при цьому для отримання необхідних вихідних даних застосовні будь-які (вузлові або мережеві) датчики.

Список літератури

1. Расторгуев С.П. Основы информационной безопасности / С.П. Расторгуев. – М.: Академия, 2007. – 160 с.
2. Кевин М. Защита от вторжений. Расследование компьютерных преступлений / М. Кевин, К. Просис. – СПб.: Лори, 2005. – 476 с.
3. Куприянов А.И. Основы защиты информации / А.И. Куприянов, А.В. Сахаров, В.А. Щевцов. – М.: Академия, 2006. – 180 с.
4. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – Казань: Юниор, 2003. – 504 с.
5. Белов Е.Б. Основы информационной безопасности / Е.Б. Белов, В.П. Лось., 2006. – 544 с.
6. Касперски К. Техника сетевых атак / К. Касперски. – М.: Клио, 2007. – 300с.