УДК 004.056.53

СИСТЕМИ ВИЯВЛЕННЯ І ЗАПОБІГАННЯ АТАК В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Зоріна Т.І.

DETECTION AND PREVENTION OF ATTACKS IN COMPUTER NETWORKS

Zorina T.

В статті розглянуто системи виявлення атак, технології виявлення атак.Проаналізовано сучасні тенденції розвитку систем виявлення атак.

Ключові слова: *система виявлення атак, захист, методи, аналіз, моніторинг, інформаційна система*

Вступ

Останнім часом світ переконався, що навіть найнадійніші системи захисту не здатні захистити від атак комп'ютерні системи державних і комерційних установ. Одна з причин — у тому, що в більшості систем безпеки застосовують стандартні механізми захисту: ідентифікацію та аутентифікацію, механізми обмеження доступу до інформації згідно з правами суб'єкта і криптографічні механізми.

Звідси потреба в механізмах, які б, доповнюючи традиційні, уможливлювали виявлення спроб несанкціонованого доступу і інформували про це відповідальних за безпеку або реагували у відповідь. Важливо, щоб такі системи могли протистояти атакам, навіть якщо зловмисник уже був аутентифікований та авторизований і з формальної точки зору додержання прав доступу мав необхідні повноваження на свої дії. Ці функції і виконують системи виявлення і запобігання атак.

Системи виявлення комп'ютерних атак - один з найважливіших елементів систем інформаційної безпеки мереж будь-якого сучасного підприємства, враховуючи, як зростає в останні роки число проблем, пов'язаних з комп'ютерною безпекою.

Основна частина

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким будемо розуміти програми, процедури, правила, а також, якщо передбачено, супутніх їм документації та даних, що відносяться до функціонування системи обробки інформації.

Повна назва СВА - це системи виявлення і запобігання атак, так як саме в можливості автоматизованого протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталене назва - система виявлення атак.

Розглянемо докладніше основні можливості, принципи і механізми функціонування, завдання СВА .

Основні можливості, принципи і механізми функціонування систем виявлення атак.

Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей ІБ

– розпізнавання відомих і по можливості невідомих атак і попередження про них персоналу, що відповідає за забезпечення інформаційна безпека (ІБ);

– статистичний аналіз шаблонів аномальних дій;

– моніторинг і аналіз користувальницької, мережевої і системної активності;

– контроль цілісності файлів та інших ресурсів інформаційної системи (ІС);

– аудит системної конфігурації і виявлення вразливостей;

– інсталяцію і підтримку роботи серверів-пасток для запису інформації про порушників;

– зниження навантаження на персонал (або звільнення від неї), що відповідає за ІБ, від поточних рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами ІС;

– надання можливості управління коштами захисту не експертами в області безпеки.

У загальному випадку використання СВА для ІБ інформаційних систем (ІС) забезпечується застосуванням наступних основних механізмів або принципів:

– політика ІБ;

– ідентифікація учасників процесу інформаційної взаємодії;

– контроль доступу учасників процесу інформаційного обміну до ресурсів і рівня цього доступу;

– аудит і моніторинг подій, що відбуваються в процесі обміну інформацією;

– реагування на інциденти при порушенні або підозрі на порушення ІБ;

– управління конфігурацією середовища інформаційного обміну відповідно до вимог ІБ;

– управління користувачами в середовищі інформаційного обміну відповідно до вимог ІБ;

– забезпечення стійкості середовища інформаційного обміну.

Функціонування сучасних СВА з метою забезпечення ІБ ІС зводиться до вирішення таких основних завдань:

– аналіз активності в захищається ІС на предмет появи ознак, що свідчать про спробу вчинення або про реалізацію атаки або про аномальної активності в ІС;

– у разі виявлення ворожих дій або аномальної активністю ти ідентифікація типу атаки або номалії;

– прийняття рішення (самостійно або, в деяких випадках, за допомогою уповноважених осіб) про спосіб блокування реализующейся атаки або аномальної активності та внесення змін до ІС з метою неможливості реалізації подібних атак на ІС;

– блокування атаки або аномалії;

– інформування уповноважених суб'єктів ІС про інцидент при необхідності.

Сучасні технології виявлення атак

Під виявленням атак будемо розуміти процес оцінки подій ІС та її інформаційних потоків, який реалізується за допомогою аналізу журналів реєстрації операційних систем (ОС) і додатків або мережевого трафіку. Реалізація більшості мережевих атак здійснюються в три етапи.

Перший, підготовчий, етап полягає в пошуку передумов для здійснення тієї чи іншої атаки. На даному етапі шукаються уразливості, використання яких робить можливим в принципі реалізацію атаки, яка і складає другий етап. На третьому етапі атака завершується, «заметені» сліди і т. д. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки вважається атакою.

Технології виявлення атак постійно розвиваються і удосконалюються, і ця область постійно залучає нових виробників і розробників. Тільки за 1999-2002 рр.. виникло понад 30 фірм, що пропонують свої послуги в цій галузі, число комерційних і вільно розповсюджуваних СВА наблизилася до сотні. Незважаючи на брак теоретичних основ технології виявлення атак, існують досить ефективні методи, використовувані сьогодні.

Виявлення атак вимагає виконання однієї з двох умов: або знання всіх можливих атак та їх модифікацій, чи розуміння очікуваного поведінки контрольованого об'єкта системи. Всі існуючі технології виявлення мережевих атак можна розділити на два типи: методи на основі сигнатур (зразків і правил); методи на основі аномалій.

Зазвичай в СВА намагаються поєднувати обидві технології, щоб усунути недоліки, властиві кожній окремо. Перевага «аномальних» систем - виявлення невідомих або нових видів атак, які можуть «обійти» СВА. Реєстрація такого роду подій тягне за собою їх аналіз адміністратором, створення для них шаблону і внесення останнього до бази даних СВА. Системи, засновані на методі аномалій, вважаються досить перспективними, але ще розвиваються і перебувають у стадії дослідження.

Розглянемо докладніше технологію виявлення атак на основі сигнатур. Основний підхід до виявлення атак довгий час зводився до опису атаки у вигляді шаблону або сигнатури і пошуку даного шаблону в контрольованому просторі (наприклад, мережевому трафіку або журналі реєстрації). Така СВА може виявити всі відомі атаки, але вона мало пристосована для виявлення нових, ще невідомих, атак.

При розробці СВА, заснованих на цьому підході, виникають дві основні проблеми. Перша полягає у створенні механізму опису сигнатур, тобто мови опису атак, а друга проблема виражається в наступному: як записати атаку, щоб зафіксувати всі можливі її модифікації? У результаті вирішення поставлених у цій роботі завдань описані вище проблеми вдалося усунути.

Схема технології виявлення атак на основі сигнатур показана на рис.1.

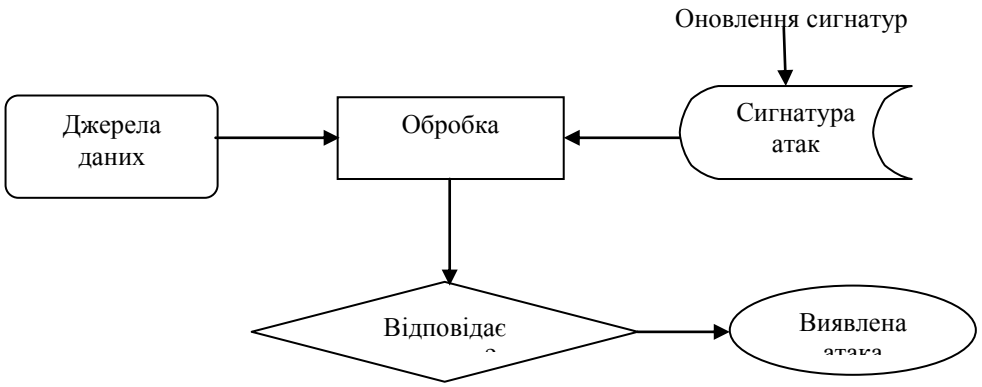

Рис.1. Схема виявлення атак на основі сигнатур

До переваг методу можна віднести точність виявлення атак і високу швидкість аналізу. Основними недоліками є неможливість виявлення нових атак і складність розпізнавання атаки в разі її модифікації, наприклад, зміни послідовності дій або потоку даних.

Розглянемо докладніше технологію виявлення атак на основі аномалій. Дана технологія побудована на припущенні, що аномальна поведінка суб'єкта ІС (системи, програми, користувача), тобто, як правило, атака або яке-небудь ворожу дію часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточну діяльність користувача, хоча існують приклади системи виявлення аномалій в мережевому трафіку.

Традиційне використання цієї технології полягає не в чіткому виявленні атак, а для визначення підозрілої активності, що відрізняється від нормальної. Основна проблема методу полягає в тому, щоб визначити критерій нормальної активності. Необхідно також встановити допустимі відхилення від нормального трафіку, які ще не вважатимуться атакою. У результаті вирішення поставлених у цій роботі завдань описану вище проблему вдалося усунути.

При використанні даної технології виявлення атак можливі два варіанти неправильного виявлення атаки:

– виявлення дії, яка не є атакою, і віднесення його до класу атак;

– пропуск атаки, яка не підпадає під сигнатури атак. Цей випадок набагато більш небезпечний, ніж помилкове віднесення дозволеного дії до класу атак. Підкатегорією такого методу буде аналіз на основі профілів, коли нормальна поведінка визначається для окремих суб'єктів (користувачів / систем). Іноді елементи такого аналізу зустрічаються і в інших методах, скажімо, в розшифровці протоколу, коли виявлений елемент, що не належить наперед визначеним протоколах або порушує правила використання протоколів.

Схема типової системи виявлення аномалій показана на рис. 2.

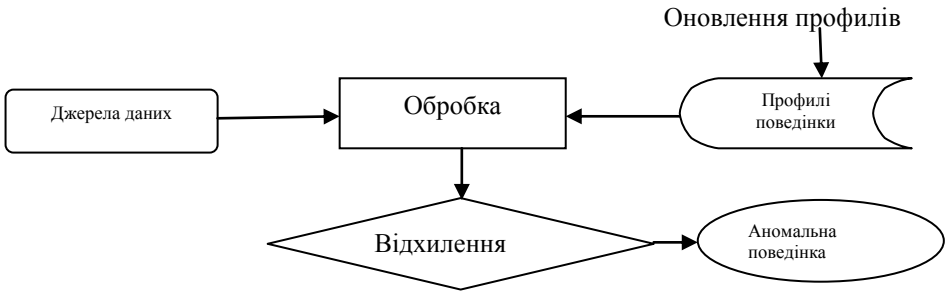

Рис.2. Схема системи виявлення аномальної поведінки

Прикладами аномального поведінки можуть служити велика кількість з'єднань за короткий проміжок часу, високі завантаження центрального процесора і коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не задіюються. Якщо описати профіль нормальної поведінки суб'єкта, то будь-яке відхилення від нього можна охарактеризувати як аномальна поведінка. Однак аномальна поведінка не завжди є атакою.

При використанні даної технології виявлення атак можливі два варіанти неправильного розпізнавання атаки:

– виявлення аномальної поведінки, яке не є атакою, і віднесення його до класу атак;

– пропуск атаки, яка не підпадає під визначення аномальної поведінки. Цей випадок набагато більш небезпечний, ніж помилкове віднесення не аномальної поведінки до класу атак.

Для виявлення аномалій необхідно вирішити два основні завдання:

– побудувати профіль суб'єкта (важко формалізується і потребує багато часу для завдання, що вимагає великої попередньої роботи);

– визначити граничні значення характеристик поведінки суб'єкта для зниження ймовірності появи помилок пропуску атаки і помилкового спрацьовування.

Для виявлення аномалій потрібна постійна реєстрація всіх подій, пов'язаних з діями контрольованого суб'єкта, необхідних для виконання такого роду виявлення, що знижує продуктивність захищається ІС. Подібні системи зазвичай сильно завантажують центральний процесор і задіють великі обсяги дискового простору для зберігання зібраних даних та, в принципі, не застосовні для систем, критичних до швидкодії, що працюють в режимі реального часу.

Основною перевагою технології виявлення аномалій можна вважати те, що коректно налаштований аналізатор дозволить виявляти навіть невідомі атаки і не зажадає додаткової роботи по введенню нових сигнатур і правил атак.

Основні недоліки технології виявлення аномалій:

– не може уявити опис атаки за елементами, швидше Повідомляється те, що відбувається щось підозріле;

– відношення корисної інформації (на основі якої робляться висновки) до марної дуже невелика в більшості випадків;

– значно залежить від середовища функціонування як визначального фактора нормальної поведінки;

– істотна частка помилкових спрацьовувань;

– відносно низька швидкість аналізу;

– трудомістке завдання побудови профілів суб'єктів ІС.

Коротке порівняння технологій виявлення атак наведено в табл. 1

Через відсутність математичних основ та формалізації процесу виявлення несанкціонованих дій та атак можна зробити висновок, що існуючі підходи не орієнтовані на розробку ефективного математичного та програмного забезпечення обчислювальних машин, комплексів і комп'ютерних мереж.

Таблиця 1

Характеристика	Сигнатурні методи	Методи аномалій
Безліч виявлених атак	Обмежується відомими видами атак	Обмежено можливостями налаштування і методами аналізу СВА
Ймовірність пропуску атаки	середня	низька
Ймовірність помилкового спрацьовування	дуже низька	висока
Вимоги до обчислювальних Ресурсів ІС	середні	високі

Тенденції розвитку систем виявлення атак.

Аналіз тенденцій розвитку сучасних СВА дозволив виявити такі основні напрями вдосконалення цих систем.

З розвитком мережевих та інформаційних технологій різко зростає складність ІС і ширина каналів зв'язку. Для корпоративних та науково-дослідних мереж стають нормою гігабітні канали зв'язку, продовжується зростання їх пропускної здатності. Одним з найбільш вузьких місць таких ІС стають СВА, постійно зростають вимоги до їх швидкодії. З ростом ширини каналів зв'язку збільшується і число сигналів тривоги, що потрапляють на консолі засобів захисту, тому виникає гостра необхідність мінімізації помилкових спрацьовувань СВА. Для вирішення цього завдання деякі розробники СВА пропонують системи кореляції подій. Спеціальні «інтелектуальні» модулі СВА в автоматичному режимі здійснюють аналіз даних, що надходять і приймають рішення про наявність або відсутність реальної загрози. Такі модулі зазвичай об'єднують дані від сенсорів СВА з інформацією від сканерів безпеки. Такі системи кореляції існують у компаній Internet Security Systems, Cisco і Symantec. Крім того, існують рішення третіх фірм, які намагаються корелювати дані від засобів захисту різних фірм. Незважаючи на ефективність такого підходу, він досить дорогий у використанні.

У зв'язку з розумінням того факту, що для забезпечення цілісної захисту ІВ від усіляких загроз порушення політики ІБ необхідна інтеграція засобів, що забезпечують захист від різних категорій загроз, в даний час намітилася тенденція інтеграції СВА з іншими засобами захисту для більш повного охоплення і всебічного аналізу стану захищеності корпоративної мережі. Враховуючи, що СВА і антивіруси призначені для вирішення різних аспектів загальної задачі, а також той факт, що шкідливі програми останнім часом все складніше і складніше класифікувати, можна прогнозувати, що протягом найближчих років ці два класи захисних засобів практично зіллються. Вже зараз багато антивіруси вміють виявляти мережеві атаки, СВА ідентифікують мережеві віруси, черв'яки і троянські програми. Аналогічна доля чекає і засоби контролю вмісту, які будуть інтегровані з СВА.

Також намітилася поступова інтеграція міжмережевих екранів і СВА. Експерти вважають, що до кінця 2006 року 60% всіх міжмережевих екранів і СВА будуть об'єднані в рамках єдиної платформи. Також такі платформи будуть опціонально оснащуватися антивірусами і модулями контролю вмісту з метою покриття максимального спектру можливих інтернет-загроз. Такі рішення вже можна знайти і зараз - Proventia M від ISS, Symantec Gateway Security 5400 Series, SmartDefense від Check Point ит. д. До інших тенденціям розвитку СВА можна віднести: «інтелектуалізацію» СВА, інтеграцію з мережевим обладнанням, перехід на програмно-апаратні рішення. Щорічне зростання таких рішень, до числа яких можна віднести Proventia від ISS, Cisco IDS Sensor 4200, NetScreen ЮР і т. д., складе за прогнозами 17,7%.

Одним з важливих етапів розвитку сучасних СВА став розвиток методів виявлення атак на основі виявлення аномалій. Якщо донедавна переважали СВА, що використовують «сигнатурний» підхід, то їм на зміну приходять

«аномальні» рішення, які відстежують в мережевому трафіку або поведінці додатків і процесів всі відхилення від норми. За прогнозами, до кінця 2006 року 50% класичних «сигнатурних» СВА буде замінено на технології, що використовують «аномальний» підхід, а загальне співвідношення сигнатурних і аномальних систем буде один до трьох на користь останніх. Багато СВА вже зараз об'єднують різні методики виявлення несанкціонованої активності - сигнатури, аномалії протоколів, контроль поведінки трафіку і т. д. З часом очікується, що ця тенденція тільки посилиться. Для розгляду основних методів реалізації та виявлення атак виберемо найбільш поширений стек мережевих проколів.

Висновки

Розглянуто та проаналізовано основні можливості, принципи і механізми функціонування, завдання СВА .З аналізу відомих методів і підходів до виявлення атак, а також формальних моделей безпеки зроблено висновок, що їх використання не дозволяє одночасно виявляти як відомі мережеві атаки, так і порушення політики безпеки ІС, тому необхідно розробити модель і методику виявлення несанкціонованих дій і атак, що розширюють функціональні можливості завдання правил виявлення атак і порушень політики безпеки ІС.

Література

1. Бармен С. Разработка правил информационной безопасности. / Пер. с англ. - М., 2002.

2. Губенков А.А. Информационная безопасность, - М., 2005.

3. Джей Бил Short 2.1. Обнаружение вторжений, - М., 2006.

4. Касперски К. Техника сетевых атак. Приемы противодействия. Том 1, - М., 2001.

5. Норткат С. Обнаружение нарушений безопасности в сетях. / Норткаг С., Новак Дж. / Пер. с англ. - М., 2003.

6. Ребекка Бейс Введение в обнаружение атак и анализ защищенности / Пер. Лукацкого А., Цаплева В., http://bugtraq.ru/library/books/ icsa/index.html.

References

1. Barmen S. Razrabotka pravil informacionnoj bezopasnosti. / Per. s angl. - M., 2002.

2. Gubenkov A.A. Informacionnaja bezopasnost', - M., 2005.

3. Dzhej Bil Short 2.1. Obnaruzhenie vtorzhenij, - M., 2006.

4. Kasperski K. Tehnika setevyh atak. Priemy protivodejstvija. Tom 1, - M., 2001.

5. Nortkat S. Obnaruzhenie narushenij bezopasnosti v setjah. / Nortkag S., Novak Dzh. / Per. s angl. - M., 2003.

6. Rebekka Bejs Vvedenie v obnaruzhenie atak i analiz zashhishhennosti / Per. Lukackogo A., Capleva V., http://bugtraq.ru/library/books/ icsa/index.html.

Зорина Т.И.

СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК В КОМПЬЮТЕРНЫХ СЕТЯХ

В статье рассмотрены системы обнаружения атак, технологии обнаружения атак. Проанализированы современные тенденции развития систем обнаружения атак.

***Ключевые слова**: система обнаружения атак, защита, методы, анализ, мониторинг, информационная система*

Zorina T.I.

DETECTION AND PREVENTION OF ATTACKS IN COMPUTER METWORKS

The article deals with intrusion detection systems, attack detection technology. Modern trends of development of attack detection systems.

***Keywords:** system intrusion detection, protection, methods, analysis, monitoring and information system.*

Зоріна Т.І. – Східноукраїнський університет імені Володимира Даля, Луганськ

Рецензент: Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.