УДК 621.38(62-52)

К.М. Носенко, О.І. Півторак, Т.А. Ліхоузова

ОГЛЯД СИСТЕМ ВИЯВЛЕННЯ АТАК В МЕРЕЖЕВОМУ ТРАФІКУ

Анотація: Розглядаються існуючі засоби моніторингу комп'ютерних атак, що здатні реалізовувати виявлення вразливостей у мережах в автоматичному режимі. Дано короткий огляд сучасних технологій та наведено основні принципи побудови систем виявлення атак.

Ключові слова: інформаційна безпека комп'ютерної мережі, засоби моніторингу комп'ютерних атак.

Постановка задачі

На сьогодні розвиток комп'ютерних мереж впливає на більшість сфер економічної діяльності. Значна кількість підприємств та організацій по всьому світу використовують комп'ютерні мережі для керування виробничими процесами і персоналом, розподілу ресурсів та підключення віддалених користувачів до мережі Internet. Це дає їм ряд очевидних переваг - прискорення виробничих процесів, підвищення мобільності і оперативності доступу до інформації та послуг, можливість віддаленого управління банківськими рахунками, замовлення і оплати товарів і послуг. Це зумовило значне зростання вартості інформації, циркулюючої в комп'ютерних мережах.

Забезпечення працездатності мереж, а також працездатності функціонуючих в них інформаційних систем, залежить не тільки від надійності використовуваної апаратури, але і від здатності мережі протистояти цілеспрямованим діям, які спрямовані на порушення її роботи.

Слід зазначити, що атаки на інформаційні системи з кожним роком стають усе досконалішими, масштабнішими та інтенсивнішими. Тому актуальною є проблема розробки та вдосконалення систем виявлення вторгнень, головним завданням яких є саме виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Постійний стрімкий розвиток методів та способів деструктивного програмного впливу на інформаційні системи зумовлює необхідність проведення порівняльного аналізу типів систем виявлення атак та запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформації.

Системи аналізу захищеності

Системи аналізу захищеності досліджують налаштування елементів захисту операційних систем робочих станцій і серверів, аналізують топологію мережі, шукають незахищені мережеві з'єднання, досліджують налаштування міжмережевих екранів. Дані системи дозволяють значно знизити ризик наявності невиявлених загроз у системі захисту мереж.

ISSN 1560-8956

До сучасних засобів моніторингу комп'ютерних атак відносяться аналізатори трафіку, такі як "сніфери" і системи виявлення атак.

Істотним недоліком даних систем є те, що аналіз трафіку адміністратором безпеки здійснюється практично вручну із застосуванням лише найпростіших засобів автоматизації, таких як аналіз протоколів. У зв'язку з цим дані системи не підходять для моніторингу великих обсягів трафіку мереж масштабу міста.

Рішенням цієї проблеми є застосування засобів моніторингу, здатних аналізувати трафік великого об'єму в режимі реального часу. До таких засобів моніторингу відносяться системи виявлення атак.

Системи виявлення атак (СВА) являють собою окремий клас програмних засобів (ПЗ), під яким розуміють 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 автоматизованої протидії атакам полягає одна з основних переваг таких систем, у порівнянні, наприклад, із засобами, заснованими на людському факторі. Проте надалі буде використовуватися найбільш усталена назва - система виявлення атак.

Використання СВА дозволяє вирішити цілий ряд завдань, що забезпечують досягнення цілей інформаційної безпеки:

- розпізнавання відомих і, по можливості, невідомих атак та попередження персоналу, що відповідає за забезпечення інформаційної безпеки (ІБ);
- статистичний аналіз шаблонів аномальних дій;
- моніторинг і аналіз користувацької, мережевої та системної активності;
- контроль цілісності файлів та інших ресурсів інформаційної системи (ІС);
- аудит системної конфігурації і виявлення вразливостей;
- інсталяція і підтримка роботи серверів-пасток для запису інформації про порушників;
- зниження навантаження на персонал (або звільнення від нього), що відповідає за ІБ, від поточних рутинних операцій з контролю за користувачами, системами і мережами, які є компонентами ІС;
- надання можливості управління функціями захисту не спеціалістам в області інформаційної безпеки.

Сучасні технології виявлення атак

Під виявленням атак розуміють 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 шукають вразливості, використання яких робить можливим в принципі реалізацію атаки, яка і складає другий етап. На третьому етапі атака завершується. При цьому перший і третій етапи самі по собі можуть бути атаками. Наприклад, пошук порушником вразливостей за допомогою сканерів безпеки вже вважається атакою.

Технології виявлення атак постійно розвиваються і удосконалюються, і ця область постійно залучає нових виробників і розробників. Незважаючи на брак теоретичних основ технології виявлення атак, існують досить ефективні методи, що використовують на сьогодні.

Існує кілька способів класифікації систем виявлення атак, кожен з яких заснований на різних характеристиках. Тип слід визначати, виходячи з таких характеристик:

- Спосіб контролю за системою. За способами контролю за системою поділяються на network-based, host-based і application-based.
- Спосіб аналізу. Це частина системи визначення проникнення, яка аналізує події, отримані з джерела інформації, і приймає рішення, чи відбувається проникнення. Способами аналізу є виявлення зловживань (misuse detection) та виявлення аномалій (anomaly detection).
- Затримка в часі між отриманням інформації з джерела та її аналізом і прийняттям рішення. Залежно від затримки в часі, системи виявлення атак діляться на interval-based (або пакетний режим) і real-time.

Більшість комерційних систем виявлення атак є real-time network-based системами.

Виявлення атак вимагає виконання однієї з двох умов: або знання всіх можливих атак та їх модифікацій, чи розуміння очікуваної 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.

Особливістю технології виявлення атак на основі сигнатур є процес 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? Схема технології виявлення атак на основі сигнатур показана на рис. 1.

Переваги:

- Детектори зловживань ефективно визначають атаки і дуже рідко створюють помилкові повідомлення;
- Детектори зловживань швидко й надійно діагностують використання конкретного інструментального засобу або технології атаки. Це дає змогу адміністратору скоригувати заходи для забезпечення безпеки;
- Швидкість аналізу.

Недоліки:

- Оскільки детектори зловживань виявляють лише відомі їм атаки, слід постійно оновлювати їхні бази даних для отримання сигнатур нових атак;
- Більшість детекторів зловживань розроблено так, що вони використовують лише певні сигнатури, а це не дає виявити можливі варіанти атак;

Технологія виявлення атак на основі аномалій побудована на припущенні, що аномальна поведінка суб’єкта ІС (системи, програми, користувача), тобто, як правило, атака або яка-небудь ворожа дія часто проявляється як відхилення від нормальної поведінки. Зазвичай системи виявлення аномальної активності використовують як джерело даних журнали реєстрації і поточна діяльність користувача, хоча існують приклади системи виявлення аномалій в мережевому трафіку.

Традиційне використання цієї технології полягає не в чіткому виявленні атак, а у визначенні підозрілої активності, що відрізняється від нормальної. Основна проблема методу полягає в тому, щоб

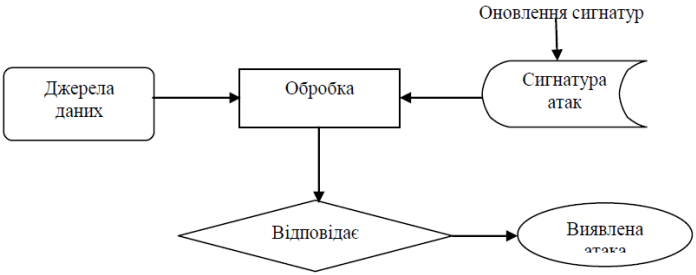

Рис. 1 – Схема виявлення атак на основі сигнатур

визначити критерій нормальної активності. Необхідно також встановити допустимі відхилення від нормального трафіку, які ще не вважатимуться атакою.

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 більш небезпечний, ніж помилкове віднесення дозволеного дії до класу атак. Підкатегорією такого методу є 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 визначеному протоколу або порушує правила використання протоколів.

Схема типової системи виявлення аномалій показана на рис. 2.

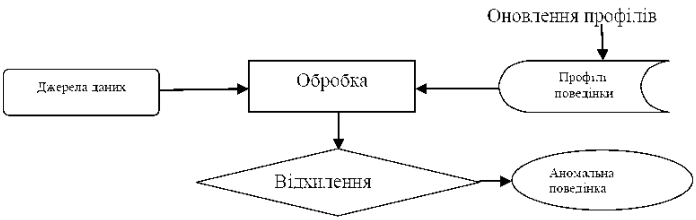

Рис. 2 – Схема системи виявлення аномальної поведінки

Прикладами аномальної поведінки є велика кількість з'єднань за короткий проміжок часу, високі завантаження центрального процесора і коефіцієнт мережевого навантаження або використання периферійних пристроїв, які зазвичай не використовуються.

Якщо описати профіль нормальної поведінки суб'єкта, то будь-яке відхилення від нього можна охарактеризувати як аномальна поведінка.

Переваги:

- СВА, що виявляють аномалії, фіксуючи несподівану поведінку системи, отримують можливість визначати симптоми атак, не маючи відомостей про їхні конкретні деталі;
- Детектори аномалій збирають інформацію, якою в подальшому можуть скористатися детектори зловживань для визначення сигнатур.

Недоліки:

- Під час виявлення аномалій, як правило, створюється велика кількість помилкових сигналів про атаки у разі непередбачуваної поведінки користувачів і мережної активності;
- Цей метод часто потребує певного етапу навчання системи, під час якого визначаються характеристики нормальної поведінки. Якість проведення цього навчання суттєво впливає на подальшу ефективність СВА;
- Не можна реалізувати опис атаки за елементами. Повідомляється те, що відбувається щось підозріле;
- Дана технологія значно залежить від середовища функціонування як визначального фактор анормальної поведінки;
- Відносно низька швидкість аналізу;
- Трудомістке завдання побудови профілів суб'єктів ІС.

Переваги використання СВА порівняно з firewall'ами

Кожен засіб захисту адресовано конкретній загрозі в системі. Більше того, кожен засіб захисту має слабкі та сильні сторони. Тільки комбінуючи їх, можна захиститися від максимально великого спектру атак.

Firewall'и є механізмами створення бар'єру, заступаючи вхід деяких типів мережевого трафіку і дозволяючи інші види трафіку. Створення такого бар'єру відбувається на основі політики firewall'а. Системи виявлення атак служать механізмами моніторингу, спостереження активності та прийняття рішень про те, чи є спостережувані події підозрілими. Вони можуть виявити атакуючих, які обійшли firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить кроки щодо запобігання атаки.

Системи виявлення атак стають необхідним доповненням інфраструктури безпеки в кожній організації. Технології виявлення проникнень не роблять систему абсолютно безпечною. Проте практична користь від систем виявлення атак існує, і не маленька, що доведено експертним методом оцінювання у таблиці 2.

Таблиця 1.

Порівняння методів СВА

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

Швидкість реакції

Важливим елементом в системах виявлення атак є швидкість реакції,що відбувається через певні проміжки часу, тобто пакетно. Швидкість реакції вказує на час, що минув між подіями, які були виявлені монітором, аналізом цих подій і реакцією на них.

У системах, реакція яких відбувається через певні проміжки часу, інформаційний потік від точок моніторингу до інструментів аналізу не є безперервним. У результаті інформація обробляється способом, аналогічним комунікаційним схемами "зберегти і перенаправляти". Багато ранніх host-based систем виявлення атак використовують дану схему хронометражу, тому що вони залежать від записів аудиту в ОС. Засновані на інтервалі системи не виконують ніяких дій, які є результатом аналізу подій.

Real-Time (безперервні) системи виявлення атак обробляють безперервний потік інформації від джерел. Найчастіше це є домінуючою схемою в network-based системах, які отримують інформацію з потоку мережевого трафіку. Термін "реальний час"використовується в тому ж сенсі, що і в системах управління процесом. Це означає, що визначення проникнення, що виконується системами виявлення атак в "реальному часі призводить до результатів досить швидко, що дозволяє виконувати певні дії в автоматичному режимі.

Таблиця 2.

Імовірності подолання загроз різними засобами захисту

Вид атакуючої дії	Засіб захисту			
	Міжмережевий екран	VPN шлюз	СВА	Антивірус
Троянські програми				0,96
Віруси				0,92
DoS-атаки	0,81	0,98	0,98	
DDoS-атаки	0,62	0,79	0,97	
Макровіруси				0,6
IP Spoofing	0,69	0,96	0,95	
DNS Spoofing			0,92	
WEB Spoofing			0,54	
Захоплення мережевих підключень	0,51	0,97	0,93	
Різні види сканування мережі	0,59		0,89	
Порушення конфіденційності даних		0,95		
Автоматичний підбір паролів	0,75		0,91	
Атаки на протоколи			0,79	
Неавторизоване використання прав	0,32		0,91	
Неконтрольоване використання ресурсів	0,53	0,61	0,81	0,64
Неавторизоване використання АС	0,62	0,73	0,79	0,67
Прослуховування мережі		0,92		
Шпигунське ПЗ			0,54	0,97

Висновки

Вибір СВА повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження та порівняльний аналіз сучасних систем виявлення атак та запобігання вторгненням показав, що при вдосконаленні існуючих та проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування інформаційної системи, які підлягають захисту.

 ISSN 1560-8956

Література

1. *Грайворонський М.В., Новіков О.М.* Безпека інформаційно-комунікаційних систем / М.В. Грайворонський – К.: Видавнича група BHV, 2009 – 608 с.
2. *Шаньгин В.Ф.*Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин – М.: ДМК Пресс, 2010 – 544 с.
3. *Ленков С.В.* Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К.: Арий, 2008 – Т.2: Информационная безопасность, 2008 – 344 с.
4. Обзор механизмов реализации и обнаружения атак [Электронный ресурс]. – Режим доступа: http://comp-bez.ru/?p=778
5. *Радченко М.М.* Аналіз системи виявлення вторгнень та комп'ютерних атак / М.М. Радченко, О.І. Іванов, С.І. Прохорський, К.К. Мужеський Междисциплинарные исследования в науке и образовании, 2013. – 379 с.
6. *Юдін О.К.* Захист інформації в мережах передачі даних / О.К. Юдін, Г.Ф. Конахович, О.Г. Корченко / Підручник МОН України. – К.: Видавництво DIRECTLINE, 2009. – 714 с.

Отримано 17.03.2014 р.