

МЕТОД ВИЯВЛЕННЯ АНОМАЛЬНОЇ ПОВЕДІНКИ В ЛОКАЛЬНІЙ МЕРЕЖІ

В. І. Батинчук¹, О. М. Барановський¹

¹ Національний технічний університет України «Київський політехнічний інститут»

Анотація

У даній роботі розглядаються системи виявлення вторгнень на основі аномалій. Описуються їх основні переваги та недоліки. Запропоновано метод модифікації системи виявлення вторгнень для покращення її ефективності та зменшення кількості хибних спрацювань.

Ключові слова: система виявлення вторгнень, атака, аномальна поведінка, метрика

Вступ

За оцінками McAfee річний збиток світової економіки від кіберзлочинності нараховує понад 445 млрд доларів. Найнижче можливе значення вказане у розмірі 375 млрд, а найгірше припущення нараховує 575 млрд доларів [1].

Проведено розрахунки, за результатами яких, кіберзлочинність дає змогу реалізувати 1425 % інвестиційних внесків, що робить дану сферу ще більш привабливою для злочинців.

Що стосується України, за даними УБК, в 2013 році сума лише заявленого матеріального збитку склала близько 19 млн грн, а за I півріччя 2014 року – близько 10 млн грн.

Дана статистика вказує на те, що існуючі антивірусні рішення, мережеві фаєрволи, системи виявлення вторгнень не допомагають захистити інформацію належним чином. Причиною цього є неготовність даних рішень до протистояння новим типам атак, інсайдерським атакам, неможливість врахування людського фактору, та великий проміжок часу між виходом нового вірусу чи експлоїту та виходом відповідного оновлення.

Саме тому необхідні дослідження в сфері систем виявлення вторгнень на основі аномалій, оскільки вони надають можливість реагувати на атаки «нульового дня», для яких ще нема сигнатур, «низькі і повільні» атаки, при яких атакуючий залишається нижче порогу спрацювання засобів моніторингу, та локальні атаки, від авторизованих користувачів.

1. Системи виявлення вторгнень

Система виявлення вторгнень (англ. Intrusion Detection System (IDS)) – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу (вторгнення або мережевої атаки) в комп'ютерну систему або мережу.

IDS на основі статистичних аномалій (statistical anomaly-based IDS) – це системи, засновані на поведінці. Вони не використовують сигнатури. Замість

цього вони створюють профіль «нормальної» діяльності, працюючи в режимі навчання. Цей профіль будується на основі постійного аналізу того, що відбувається в середовищі діяльності. Точність профілю і якість захисту залежить від часу знаходження IDS в режимі навчання. Після створення профілю, весь наступний трафік і діяльність порівнюються з ним. Все, що не схоже на профіль, вважається атакою, про яку надсилається відповідне повідомлення [2].

Такі IDS використовують складні статистичні алгоритми, вишукуючи аномалії в мережевому трафіку і діях користувачів. Кожному пакету присвоюється рейтинг його «аномальності», який вказує на ступінь його відхилення від нормального профілю. Якщо рейтинг вище певного порогу «нормальної» поведінки, виконується заздалегідь визначена дія.

Універсальність моделі IDS на основі аномалій полягає в тому, що вона не залежить від особливостей тієї чи іншої системи, прикладного оточення, вразливостей системи та програм, типів вторгнення, а також здатності виявляти порушення безпеки в широких межах – від спроб проникнення ззовні до внутрішніх зловживань.

Модель включає в себе профілі представлення поведінки суб'єктів по відношенню до об'єктів в термінах метричних і статистичних моделей і правила для отримання знань про цю поведінку із записів аудиту для виявлення аномальної поведінки [3].

Метрика – це випадкова змінна X , що представляє деяку кількісну міру того, що сталося за період. Періодом може бути як фіксований інтервал часу (хвилини, дні, тижні і ін.), так і час між двома аудитов'язаними подіями (наприклад, час між входом в систему і виходом з неї). Є три типи метрик:

- лічильник подій (наприклад, кількість логінів в годину);
- часовий інтервал (наприклад, між логінами);
- вимір ресурсу (наприклад, кількість надрукованих сторінок).

Мета статистичної моделі – визначити, чи є нове спостереження x_{n+1} змінної X аномальним в порівнянні з попередніми спостереженнями.

Основні моделі що використовуються:

- операційна модель
- модель середнього значення та середньоквадратичного відхилення
- багатоваріаційна модель
- модель Марківського процесу
- модель часових серій

2. Модель середнього значення та середньоквадратичного відхилення

Модель середнього значення та середньоквадратичного відхилення забезпечує незалежність оцінки аномальності поведінки від апріорних знань, проста в реалізації та має високу швидкість роботи. Тому для дослідження було обрано саме цю модель.

Дана модель базується на тому, що все, що ми знаємо про попередні спостереження (x_1, \dots, x_n) деякої величини – це її середнє значення $\mu = \frac{\sum x_i}{n}$ та середньоквадратичне відхилення $\sigma = \sqrt{\frac{x_1^2 + \dots + x_n^2}{n-1} - \mu^2}$. Тоді нове спостереження є аномальним, якщо воно не вкладається в межах довірчого інтервалу $\mu + d \cdot \sigma$, де d - деяка константа [3]. Модель може бути застосована для вимірювання лічильників подій, часових інтервалів і ресурсів що використовуються. Аномальність поведінки залежить від значення довірчого інтервалу, і як наслідок, поняття аномальності для користувачів системи може відрізнятися.

2.1. Модифікація моделі

Якість профілю IDS на основі аномалій характеризується кількістю похибок першого або другого роду, що в свою чергу вимагає висококваліфікованого персоналу та значних затрат людських ресурсів, для зменшення кількості хибних спрацювань. Це пов'язано з складністю навчання IDS, та тим, що в мережі постійно відбуваються зміни. Часто це призводить до того, що компанії просто відключають свої IDS, через те, що вони вимагають вкрай багато часу для своєї належної підтримки.

Зменшення кількості хибних спрацювань такої IDS пропонується за рахунок врахування часових характеристик окермої доби, днів тижня, числа місяця, та дня року. Дана пропозиція впливає з особливостей організації робочого часу на кожному підприємстві.

Так, наприклад, слід враховувати, що під час обідньої перерви на підприємстві, активність користувачів стає мінімальною. Також важливо зазначити, що вкінці робочого тижня, активність користувачів може бути нижчою, або навпаки вищою, залежно від організації звітнього процесу робітників підприємства. Число місяця та день року можуть впливати на кількість проведених платіжних та звітніх операцій, як в кінці місяця чи року, так і перед календарним святом.

Під час навчання IDS аналізує не лише події, часовий інтервал і ресурси, але і вищевказані часові

характеристики. Таким чином, дії користувачів аналізуються в порівнянні з «нормальною» поведінкою в той же часу доби, якщо система виявляє дію, яка виходить за межі визначеного довірчого інтервалу, вона порівнюється з довірчим інтервалом цього ж дня тиждень тому, місяць тому, та рік тому. Якщо дана дія проходить всі зазначені довірчі інтервали, то вона визначається як аномальна.

Результат роботи

Результатом роботи є IDS на основі аномалій створена на персональному комп'ютері. Систему було створено за допомогою Snort – програмного продукту для створення IDS. Дана IDS навчалась таким чином, що робоча машина працювала лише в денний час, та знаходилась в стані сну вночі. У денний час комп'ютер проводив операцію сканування локальної мережі рівно о першій годині дня.

Через деякий час, після початку системи, комп'ютер було увімкнено уночі, та проведено ту саму операцію сканування локальної мережі. В результаті таких дій Snort визначив дану операцію як аномальну. Отже на практиці визначено, що розроблена модель допомагає виявляти аномалії на основі часових характеристик окремої доби.

Для подальшого випробування ефективності побудованої моделі необхідний більший проміжок часу, та більше обчислювальних ресурсів. Тому розвиток даної моделі, та дослідження її ефективності на практиці знаходиться в процесі.

Висновки

Таким чином в роботі пропонується використання системи виявлення вторгнень на основі аномалій як додатковий спосіб захисту комп'ютерної системи та мережі. Запропонований метод модифікації моделі середнього значення та середньоквадратичного відхилення дозволяє значно зменшити кількість хибних спрацювань та покращити ефективність системи виявлення вторгнень на основі аномалій завдяки більш детальній порівняльній характеристиці дій користувачів з «нормальною» поведінкою. На практиці було побудовано запропоновану модель, та доведено її ефективність для часових характеристик доби. Хоч така модифікація вимагає додаткових обчислювальних ресурсів, проте вона допомагає заощадити людські ресурси, що може позитивно відобразитись на оперативності реагування персоналу з інформаційної безпеки.

Перелік використаних джерел

1. Net Losses: Estimating the Global Cost of Cyber-crime — TECHmarcLabs— 2014.
2. Практика информационной безопасности — Мониторинг управления доступом: Выявление вторжений, 2011.
3. Архипов А. Е., Ишутин А. Системы обнаружения вторжения — 2006. — № 13.