ТЕХНІЧНІ НАУКИ

Андрійчук В.В.
студент,
Національний технічний університет України
«Київський політехнічний інститут»

СИСТЕМИ ВИЯВЛЕННЯ КІБЕР АТАК

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.

Проблема захисту інформаційних потоків у комп'ютерних мережах наразі не може вважатись вирішеною, а саме тому, дослідження цього питання є актуальним майже для усіх установ, де необхідне відповідне збереження цілісності та конфіденційності інформації, що передається інформаційними потоками комп'ютерних мереж.

Розроблені правила мають бути доступними для широкого кола користувачів, легкими у використанні та максимально точними у визначенні фактів втручання у роботу комп'ютерної мережі. Об'єктами дослідження є веб-портал з невисокою відвідуваністю та локальна комп'ютерна мережа, а

предметами – набори правил для системи виявлення атак на основі сигнатурних та аномальних методів.

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 сигнатур (signature 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 networkbased 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?

Список використаних джерел:

1. Жигулин Г. П., Новосадов С. Г., Яковлев А. Д. Информационная безопасность – СПб: СПб ГУ ИТМО, 2003. – 315 с.

2. Олифер В. Г., Олифер Н. А. Компьютерные сети – 3-е издание ПИТЕР, 2006. – 958 с.

Білан Т.Р.

аспірант,

Інститут загальної енергетики

ОЦІНКА ВАРІАНТІВ ЗАБЕЗПЕЧЕННЯ ТЕС ВУГІЛЬНИМ ПАЛИВОМ

Забезпечення економіки України вугільним паливом зазнає істотних змін у зв'язку з різким скороченням обсягів власного видобутку з вітчизняних паливних баз, дефіцитом природного газу й необхідністю його заміщення іншими видами палива, зокрема вугіллям, зниженням потреби в паливі, викликаним припиненням функціонування багатьох енергоємнісних виробництв.

При забезпеченні паливом теплових електростанцій необхідно врахувати можливі джерела надходження палива як з вітчизняних паливних баз – вугілля власного видобутку, так і за імпортом. Крім того, дефіцит штатного палива електростанцій може викликати необхідність повної заміни споживаних марок вугілля, що спричинить необхідність заміни котлоагрегату станції, наприклад заміну котла, спроектованого на спалювання антрацитової групи вугілля на котли для газової групи (марка Г).

З метою вибору оптимальних варіантів вуглезабезпечення теплових електростанцій з урахуванням економічної доцільності та надійності постачання перспективних видів палива розроблено економіко-математичну модель.

У загальному випадку паливний баланс теплової генерації ОЕС України означає рівність обсягів потреби у штатному паливі всіх споживачів енергосистеми та обсягів його надходження з можливих джерел постачання – вуглевидобувних підприємств країни та джерел імпортування.

$$\sum_{i=1}^{N_{потр}} y_i^{потр} = \sum_{j=1}^{N_{д.н.}} x_j \,, \qquad (1)$$

де $y_i^{потр}$ – потреба у штатному паливі споживача i, млн т;

x_j – надходження палива з джерела j, млн т;