УДК 004.056.5

Мохнін Микита Ігорович, студент гр. 125м-16-1,

Науковий керівник: Святошенко В.О., ст. викл. кафедри безпеки інформації та телекомунікацій

(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕННЯ В РЕАЛЬНОМУ ЧАСІ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Ця стаття дає ознайомитися з вразливістю мереж та методом завдяки якому можна цьому запобігти.

***Ключові слова* – Мобільний агент; Комп'ютерні мережі; Модель виявлення вторгнення**

ВСТУП

З мінливої індустрією телекомунікацій і зростанням популярності комп'ютеризованих додатків, велика кількість досліджень було проведено по застосуванню біологічно методів і систем на основі агентів систем комп'ютерного зв'язку, Мотивація даної роботи є дослідити, як біологічними методи в поєднанні з мобільним агентом можна використовувати електронну FFI ciently для розробки майбутніх поколінь систем виявлення вторгнень для комп'ютера комунікативних мереж.

ПРОПОНОВАНА МОДЕЛЬ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Запропонована модель заснована на поєднанні мобільних парадигм агента і біологічно натхненної методики, заснованої на парадигмі імунної системи людини. У нашій моделі для системного аудиту використовується секвенційний аналіз реєстрів журналів, а для цілей моніторингу використовується схема виявлення аномалій. Основні особливості нашої моделі IDS полягають в наступному:

- Модель виявлення аномалій.
- Архітектура на основі розподілених агентів і хостів.
- Компонент генерації відповіді.

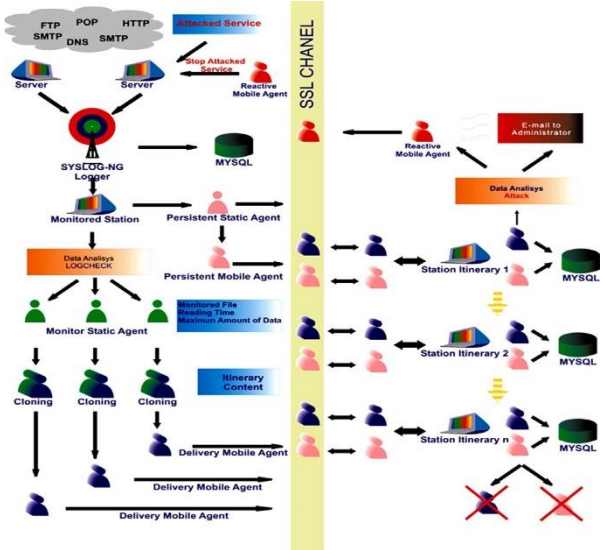

Рисунок 1. Схема моделі

На рисунку 1 зображені основні компоненти пропонованої моделі IDS, яка включає в себе не тільки служби FTP, DNS, HTTP, POP3 е SMTP, але також сервери, на яких запущено інструмент генерації журналів (Syslog-ng), які відповідають для

отримання реєстраційних операцій для різних серверів і сервісів і визначення їх відповідної функції генерації подій.

ЕКСПЕРЕМЕНТАЛЬНІ РЕЗУЛЬТАТИ

В даних експериментах ми розглянули зміни розміру агента, включаючи загальний час передачі в мережі з використанням різних смуг пропускання, тобто Ethernet 10 Мбіт / с, Ethernet 100 Мбіт / с і Ethernet 1000 Мбіт / с. Для кожного мережевого сценарію ми варіювали розміри сегмента агента від 0 КБ до 2000 КБ. Експерименти, які ми проводили, складаються в реєстрації часу передачі агентів між двома комп'ютерами з використанням декартового продукту між розміром агента і швидкістю мережі.

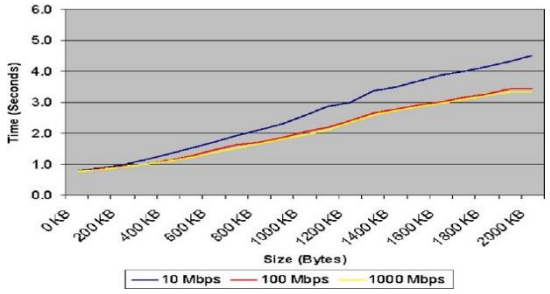

Рисунок 2. Ефективність передачі

На рисунку 2 зображено ефективність передачі агента, змінюючи розміри агентів і швидкість мережі, використовуючи сокет без SSL в якості моделі зв'язку. Як видно, наші результати показують, що продуктивність агента в повному обсязі лінійні, оскільки мережі Ethernet 100 Мбіт / с і 1000 Мбіт / с показують аналогічну продуктивність для передачі агента, в той час як 10 Мбіт / с демонструють аналогічну поведінку в початкових сегментах, а потім значно погіршуються. Щоб довести ці спостереження, було застосовано статистичний метод Круськала-Уолліса для груп результатів, отриманих в інтервалі [0 КВ, 2000. КБ] при використанні декількох значень передачі (10 Мбіт / с, 100 Мбіт / с і 1000 Мбіт / с) з 95% -ним інтервалом узгодження.

ВИСНОВКИ

У цій роботі була розроблена модель виявлення вторгнень, засновану на парадигмі імунної системи людини, та показано, як біологічно натхненні методи в поєднанні з технологіями мобільних агентів можуть поліпшити безпеку складних комп'ютерних комунікаційних мереж, а також те, як ці методи можуть бути використовується для розробки майбутніх поколінь систем виявлення вторгнень для комп'ютерних мереж зв'язку. Дана система виявлення вторгнень і комунікацій на основі реального часу заснована на хості і використовує парадигму виявлення аномалій.

ПЕРЕЛІК ПОСИЛАНЬ

1. A. Boukerche, K.R.L. Jucá, J.B.M. Sobral, M.S.M.A. Notare, Biological inspired based intrusion detection models for mobile telecommunication systems, in: IEEE Proceedings of the Int'l Parellel and Distributed Processing Symposium and Workshops, 2015.

2. J. Kim, P. Bentley, Evaluating negative selection in an artificial immune system for network intrusion detection, in Proceedings of the Genetic and Evolutionary Computation Conference, pp. 1330–1337, 2016.

Central loghost mini how to. http://www.campin.net/newlog- check.html#newlogcheck/, 2016.