УДК 004.6, 004.89

І.І. Сех, М.Б. Герович, Л.В. Федисів, О.А. Пелещак
Західноукраїнський національний університет, Україна

БАЗИ ДАНИХ АТАК ДЛЯ НАВЧАННЯ ТА ТЕСТУВАННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

I.I. Sekh, M.B. Herovych, L.V. Fedysiv, O.A. Peleshchak

ATTACK DATABASES FOR TRAINING AND TESTING INTELLIGENT INTRUSION DETECTION SYSTEMS

Сьогодні безпровідні мережі передачі даних, зокрема з використанням технології Інтернет Речей, продовжують стрімко розвиватися, що пояснюється їх доступністю, простотою підключення користувачів і поширенням мобільних пристроїв. Проте безпровідне середовище передачі в силу своїх особливостей створює потенційні умови для прослуховування мережевого трафіку і неконтрольованого підключення до безпровідної мережі зловмисників, що знаходяться в зоні її дії. Крім того, такі мережі піддаються багатьом типам атак, у тому числі внаслідок недосконалості протоколів передачі даних.

Всього ж за останні п’ять років число мережевих атак виросло в декілька разів. Рядові користувачі і невеликі організації, як правило, обмежуються використанням антивірусного програмного забезпечення, яке на сучасному етапі розвитку має ряд додаткових модулів захисту (вбудовані міжмережеві екрани, перевірка електронної пошти і т. д.). Великі підприємства вимушені купляти дорогі системи виявлення і запобігання атакам. Системи виявлення атак можуть бути реалізовані як на основі моделі виявлення відомих ознак (сигнатур), так і на основі виявлення відхилень від нормальної поведінки (аномалій). Бази даних перших містять тисячі ознак атак, при цьому їх використання підвищує вимоги до апаратного забезпечення і помітно уповільнює швидкість обробки мережевого трафіку, тому частенько більшість правил адміністратор інформаційної безпеки відключає, що веде до підвищення ризику здійснення атаки. У свою чергу, технологія виявлення аномалій забезпечує захист від нових, невідомих вірусів і мережевих атак, але системи, побудовані на основі цього методу, можуть видавати велику кількість помилкових спрацювань.

Атаки на безпровідні локальні мережі розділені на дві групи: атаки фізичного і канального рівня, що є специфічними для безпровідних мереж; атаки з мережевого по прикладний рівні, властиві будь-якій технології організації локальних мереж, у тому числі Ethernet.

В якості зразків атак з мережевого по прикладний рівні в роботі використана вдосконалена база сигнатур NSL KDD-2009 [1], побудована на основі бази KDD-99, створена за ініціативою американського агентства перспективних оборонних дослідницьких проектів (DARPA) [2]. Для проведення досліджень в області виявлення вторгнень агентством був зібраний набір даних про з’єднання, що охоплює широкий спектр різних вторгнень, змодельованих в середовищі, що імітує мережу Військово-повітряних сил США. База містить близько 4 гігабайт стислих даних про мережевий трафік.

Репрезентативність бази KDD-99 досить спірна. Важливим недоліком в наборі даних KDD-99 є величезна кількість надмірних записів (близько 78% і 75% записів в навчальній і тестовій вибірці відповідно), що викликає зміщення роботи алгоритмів класифікації у бік розпізнавання поширеніших записів і пропускання рідкісних. Крім того, із-за великого об’єму навчальної вибірки дослідники зазвичай розділяють її на частини і використовують їх для тестування ефективності алгоритмів класифікації, що у результаті призводить до недостовірних результатів експериментів.

Вище згадані проблеми вирішені у базі NSL KDD-2009 [1]. Вона містить навчальний і тестовий набори, що складаються з окремих вибраних записів про з’єднання бази KDD-99. Кожне з’єднання позначене як нормальне або як якийсь тип атаки з чотирьох наступних категорій атак: відмова в обслуговуванні (Denial of Service, DoS); несанкціоноване

отримання прав користувача (Remote to Local, R2L); несанкціоноване підвищення прав користувача до суперкористувача (User to Root, U2R); зондування (Probe). Детальний опис атак представлений в [3].

Проте, для навчання і тестування систем виявлення атак у безпровідній мережі потрібна також вибірка безпровідних атак, специфічних для мереж 802.11, тобто атак канального рівня. Для вирішення задачі формування такої вибірки можна використати тестову локальну безпровідну мережу. Середовищем генерації атак може бути ноутбук з набором спеціальних утиліт для тестування на проникнення в мережу і безпровідним адаптером в режимі моніторингу. Для перехоплення і аналізу кадрів з метою формування бази сигнатур атак можна використати другий ноутбук з безпровідним адаптером в пасивному режимі моніторингу. Зібрані кадри необхідно представити у вигляді, що використовується у базі NSL KDD-2009.

У свою чергу, атаки на безпровідні сенсорні мережі можна розділити на активні та пасивні. Активні атаки це загальні атаки, атаки на кластерну мережу та атаки на систему захисту мережі. Згідно з цими даними наступні атаки можуть завдати найбільшого несприятливого впливу при реалізації зловмисником: атака Сібіли (Sybil attack), атака блокування вузла, атака блокування вузла з наявністю умов, тунельна атака, атака відмова в обслуговуванні. Отримати базу даних атак на безпровідні сенсорні мережі можна використовуючи систему моделювання Network Simulator-2 (NS-2), яка дозволяє модифікувати вихідний код, додаючи необхідні дії з пакетами, надає можливість моделювати необхідні атаки [4].

Отже, поширення безпровідних мереж призводить до необхідності приділяти активну увагу вирішенню властивих їм проблем інформаційної безпеки. При цьому існуючі засоби захисту, у тому числі комерційні безпровідні системи виявлення атак, не забезпечують повноцінного захисту. Тому актуальними задачами є підвищення ефективності виявлення вторгнень у безпровідних мережах шляхом розробки сучасних методів та засобів вирішення цієї задачі. Перспективним є використання нейромережевих технологій, що доведено на практиці [5].

Література:

1. The NSL-KDD Data Set [Електронний ресурс]. – Режим доступу: http://nsl.cs.unb.ca/NSL-KDD.

2. KDD cup 99 Intrusion detection data set [Електронний ресурс]. – Режим доступу: http://kdd.ics.uci.edu/databases/kddcup99.

3. Lincoln Laboratory. DARPA Intrusion Detection Evaluation. [Електронний ресурс]. – Режим доступу: http://www.ll.mit.edu/mission/communications/cyber/ CSTcorpora/ideval/docs/attackDB.html.

4. Issariyakul T., Hossain E. Introduction to Network Simulator 2 (NS2). In: Introduction to Network Simulator NS2. Springer, Boston, MA. 2012. https://doi.org/10.1007/978-1-4614-1406-3_2.

5. Komar M., Kochan V., Dubchak L., Sachenko A., Golovko V., Bezobrazov S., Romanets I. High performance adaptive system for cyber attacks detection. The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : Proceedings (Bucharest, Romania, September 21-23, 2017). Bucharest, 2017. Vol. 2. Pp. 853-858.