Міністерство освіти і науки України

Харківський національний автомобільно-дорожній університет

«КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ І МЕХАТРОНІКА»

(30 травня 2019 р.)

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Харків,

2019

УДК 004:629:656:658

Комп'ютерні технології і мехатроніка. Збірник наукових праць за матеріалами міжнародної науково-практичної конференції. – Харків, ХНАДУ, 2019. – 282 с.

Збірник містить результати теоретичних та практичних наукових досліджень та розробок, які були виконані науково-педагогічними працівниками вищої школи, науковими співробітниками, докторантами, аспірантами, магістрантами, студентами ті фахівцями різних організацій і підприємств.

Для викладачів, наукових працівників, докторантів, аспірантів, магістрантів, студентів, фахівців.

Матеріали доповідей конференції відтворено з авторських оригіналів

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

УДК 004

РОЗРОБКА ЗАСОБІВ ВИЗНАЧЕННЯ КОМП'ЮТЕРНИХ АТАК НА ОСНОВІ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКУ

Черняк Т.О., асистент кафедри прикладної математики та інформатики, ДонНТУ

Хоронеко Д.С., магістрант, ДонНТУ

Актуальність дослідження полягає в тому, що останнім часом поряд з удосконаленням корпоративних і відомчих мереж збільшується і ризик реалізації різних типів загроз їхній безпеці. У зв'язку з цим системи виявлення вторгнень (СВВ), крім миттєвого виявлення атак, повинні надавати всі можливі дані про хост, що атакується, і задовольняти цілому набору жорстких вимог. Сьогодні з'являється величезна кількість нових методів ініціювання атак, при цьому формуються нові вимоги до таких методів, тому потрібні більш ефективні підходи до розробки СВВ. Спостерігається широке розповсюдження інструментів в сучасних СВВ, що аналізують відомі сигнатури, в цілому демонструють високу продуктивність, але не здатні виявити невідому атаку.

Предметом дослідження є захист інформаційної системи від комп'ютерних атак з використанням нейронних мереж.

Об'єктом дослідження є принципи аналізу мережевого трафіку та побудови нейронної мережі, що аналізує трафік з метою виявлення мережевої атаки.

Наукова новизна роботи полягає в тому, що для виявлення комп'ютерних атак запропоноване використання багатошарового персептрону, а також те, що експериментальні випробування здійснювалися на випробуваній базі даних KDD Cup1999 Data.

Метою роботи є розробка системи виявлення комп'ютерних атак на основі аналізу мережевого трафіку за допомогою нейронної мережі.

Комп'ютерні атаки – це реальна та зростаюча загроза, з якою стикаються компанії в усьому світі. Зазначені атаки реалізуються великою кількістю програмних агентів, розміщених на хостах, які зловмисник скомпрометував раніше. Реалізація цих атак може привести не тільки до виходу з ладу окремих хостів і служб, а й зупинити роботу кореневих DNS-серверів і викликати часткове/повне припинення роботи мережі Інтернет. У зв'язку з критичністю та нетривіальністю даного класу атак, побудова ефективних засобів захисту від них являє собою складну науково-технічну проблему. Захист на рівні маршрутизаторів (наприклад, від DDoS-атак) вже досить успішно реалізували компанії Cisco Systems і Arbor Networks, але в цілому порушена проблема атак на сьогоднішній день, як і раніше, стоїть дуже гостро для більшості компаній.

Необхідно зазначити, що існує досить багато різних видів атак на відмову, кожна з яких використовує певну особливість побудови мережі або уразливості програмного забезпечення. Наприклад, атаки можуть здійснюватися шляхом безпосередньої пересилки великої кількості пакетів, використання проміжних вузлів, передачі занадто довгих, некоректних пакетів або великої кількості трудомістких запитів. З останніх тенденцій можна відзначити появу атак погіршення якості та низькочастотних атак і, безумовно, цей процес буде тривати, вимагаючи нових досліджень і розробки нових методів протидії.

Для успішного функціонування системи захисту від атак на відмову надзвичайно важливо виділити безліч припущень про систему, яка підлягає захисту. Очевидно, що захист систем різного типу повинен бути побудований на основі різних принципів, з урахуванням типових характеристик, класів атак, що спрямовані проти систем вказаного типу, вимог до функціонування систем захисту. Як правило, ці припущення стосуються нормальної роботи системи, що підлягає захисту. Виділення наведених емпіричних характеристик істотно полегшує процес виявлення атак за умови збереження їх відповідності реальному стану системи.

Слід відмітити також кілька базових припущень, що використовуються в усіх системах захисту. Перше з них полягає в тому, що атаки взаємопов'язані з незвичайним використанням системи, тому їхні дії істотно відрізняється від типової роботи.

Проаналізувавши вимоги, які пред'являються до систем виявлення мережевих атак на підставі аналізу мережевого трафіку, були сформульовані вимоги до розроблюваної системі: система повинна вчитися на «хорошому» трафіку; враховувати IP-адресу, з якої йде запит; враховувати кількість запитів з однієї IP-адреси; враховувати країну-джерело запиту; враховувати метод запиту; враховувати адреси підмережі; визначати сторінку входу на сайт, тип браузера, тип операційної системи.

В межах даної роботи передбачений нейромережевий аналіз мережевого трафіку. У зв'язку з цим в роботі необхідно вирішити такі завдання: визначити тип нейронної мережі, яка буде найбільш ефективною для здійснення подальшого аналізу; визначити основні характеристики нейронної мережі – кількість нейронів вхідного шару, кількість прихованих шарів, кількість нейронів в прихованих шарах, кількість нейронів вихідного шару; визначити тип навчання; визначити вихідні дані для проведення аналізу; визначити середу побудови нейронної мережі; виконати побудову мережі та виконати процедуру її навчання; проаналізувати отриману вибірку.

Висновки. В подальшому, для виявлення мережевих атак, планується використання засобів, що базуються на застосуванні методів штучного інтелекту – нейронних мереж. Нейронні мережі здатні до навчання та класифікації. Мережі, навчені на обмеженому обсязі даних, показують хороші результати виявлення різних типів мережевих атак. Визначення мережевих атак системи виконується шляхом аналізу мережевого трафіку та надалі приймається рішення про можливу наявну загрозу.

Література: 1. Дасгупта Д. Искусственные иммунные системы и их применение / Д. Дасгупта. – Москва : ФИЗМАТЛИТ, 2006. – 344 с. **2.** Гаценко О.Ю Защита информации. Основы организационного управления / О.Ю. Гаценко. – Санкт-Петербург : Сентябрь, 2001. – 228 с.

ЗМІСТ

НАУКОВЕ ВИДАННЯ

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗА МАТЕРІАЛАМИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ «КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ І МЕХАТРОНІКА»

Конференцію проведено згідно з планом проведення міжнародних, всеукраїнських науково-практичних і науково-методичних конференцій і семінарів Харківського національного автомобільно-дорожнього університету у 2019 р. (посвідчення УкрІНТЕІ № 666 від 20 грудня 2018 р.)

Відповідальний за випуск д.т.н., проф. Ніконов О.Я.

Науковий редактор д.т.н., проф. Ніконов О.Я.

Технічний редактор Мнушка О.В.