МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
Університет Інформатики і прикладних знань, м.Лодзь, Польща
Національний технічний університет України «Київський політехнічний інститут»
Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції

Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р**.** - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

Проведення та впровадження тестування на ефективність і стійкість є важливою задачею. Охарактеризовано декілька підходів і методик щодо таких дій. Отриманні в роботі результати можуть бути використані при відборі та підготовці операторів безпілотних літальних апаратів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методика коммуникативных и организаторских склонностей. [Электронный ресурс]. Доступно: http://www.miu.by/kaf_new/mpp/014.pdf.
2. Самооцінка психічних станів за методикою Г. Айзенка[Электронный ресурс]. Доступно: https://onlinetestpad.com/ua/testview/76436-samooc%D1%96nka-psikh%D1%96chnikh-stan%D1%96v-za-metodikoyu-g-ajzenka
3. Методика Т. Елерса*:* "Діагностика мотивації до уникнення невдач". [Электронный ресурс]. Доступно: http://personal.in.ua/article.php?ida=508.
4. В. М. Кичак, С. М. Злепко, В. І. Макогон, "Технологія психофізіологічного відбору операторів безпілотних літальних апаратів", *Technical sciences*, 232-236 с., 2019.
5. О. Н. Романюк, Л. Г. Коваль, С.В. Котлик, А.В. Марущак, та В. А Шмалюх. "Комп'ютерна програма для тренування операторів БПЛА в ігровій формі". *Матеріали І Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів «Комп'ютерні ігри та мультимедіа як інноваційний підхід до комунікації»*. Одеса, 25-26 березня 2021 р. - Одеса, Видавництво ОНАХТ, 2021 р. – с.17-18.

УДК 004.451.7:004.7

ПАСИВНИЙ МЕРЕЖЕВИЙ АНАЛІЗ ТА ЗАСОБИ ЙОГО ВДОСКОНАЛЕННЯ

ЖОЛНЕР І. Д., МИРУТЕНКО Л. В., ШЕСТАК Я.В.
(*ivzholner@gmail.com, myrutenko.lara@gmail.com, lucenko.y@ukr.net*),
Київський національний університет ім. Тараса Шевченка

Із розвитком мережевих технологій та збільшенням обсягів інформації, що передається через мережу, виникає потреба в поглибленому аналізі трафіку. Було розглянуто пасивний метод аналізу мережі, проаналізовано його переваги та недоліки в порівнянні з активним методом. Для усунення існуючих недоліків даного методу було запропоновано використання нейронних мереж, які, вірно відкалібрувавши вагу нейронів, зможуть робити точні передбачення на рахунок рівня загрози подій у мережі, та використання ідентифікації (fingerprinting) по заголовкам пакетів отримуючи інформацію про ОС користувача, дивлячись на те яким чином конфігурований зміст відправленого пакету.

У сучасному світі важко уявити своє життя без інформаційних технологій, включаючи мережеві технології, які, в свою чергу, потребують постійного розвитку та вдосконалення. Це призводить до ускладнення їх структури та збільшення розмірів, а також до потреби розробки інструментів, що дозволять як локалізувати проблеми, які виникають у мережах, так і проаналізувати причини їх появи. Таку задачу на сьогоднішній день вирішують мережеві аналізатори, перевагами використання яких є можливість проводити накопичення, обробку, класифікацію, контроль і модифікацію мережевих пакетів в залежності від їх вмісту в реальному часі. Але при використанні наряду з перевагами аналізатори мають і ряд недоліків. Однією з основних проблем є те, що для використання таких аналізаторів треба

«влучно» та актуально вибрати місце для розміщення мережевих сенсорів, які будуть зчитувати необхідну інформацію та здійснювати при цьому мінімальний вплив на пропускну здатність критичних точок системи. Крім того, слід звернути увагу, що навіть при вдалому виборі розміщення, спеціалістам з кібербезпеки (security analyst) необхідно також проаналізувати отриману інформацію та визначити рівень загрози кожної неправомірної дії.

Таким чином, можна зробити висновок, що навіть маючи персонал, який буде займатись розслідуванням та нейтралізацією загроз, можлива неправильна ідентифікація дій користувачів у мережі як загроз, або ж навпаки (false positive, false negative). Даний недолік можна вирішити за допомогою технологій побудови нейронних мереж на основі дата-сету для подальшого використання нейронної мережі в ідентифікації рівня загроз різних мережевих подій (events), які, в залежності від степені загрози, зможуть запропонувати можливі вектори нападу та захисту. Також хотілось би відмітити, що у сканерах безпеки майже не реалізуються методи ідентифікації користувачів по різним заголовкам пакетів (fingerprinting). Дана технологія могла б підвищити ефективність розслідувань подій, а також допомогти в ідентифікації правопорушників (або хоча б пристроїв, які вони використовують). Запровадження таких вдосконалень можливо на рівні середовища накопичення обробки та класифікації перехоплених пакетів.

Слід звернути увагу на те, що методи пасивного мережевого аналізу працюють так, як і активні методи побудови карт. Пасивні методи ґрунтуються на сценарії «запит-відповідь», вони покладаються на чужій запит, а потім збирають відповіді. В активному сценарії об'єкт відповідає на запит додатка, який будує карти мережі, що є ефективним. У сценарії пасивного мережевого аналізу об'єкт відповідає на запити в результаті нормального функціонування мережевих додатків. В обох випадках отримуються дані про вибір потрібного порту і службах, потоках з'єднань, інформацію про час, за якими можна зробити припущення про робочі характеристики мережі. Пасивний метод дозволяє також зробити те, що неможливо зробити за допомогою активного методу: можна бачити мережу з точки зору користувача і вивчати поведінку додатків в ході звичайних операцій. Такі аналізатори зазвичай перехоплюють мережевий трафік, сприймаючи не адресовані їм пакети даних, переводячи свою мережеву картку в нерозбірливий режим. Або ж використовують встановлені у робочій мережі датчики, для перехоплення трафіку та подальшого їх логування.

Але пасивний аналіз також має свої недоліки. Для проведення пасивного аналізу потрібно вставити апаратний або програмний датчик в досліджувану мережу. Датчики повинні бути розміщені в топології мережі так, щоб через них проходив корисний трафік, що не є тривіальним завданням в сучасних мережах. І нарешті, інструментарій для пасивного аналізу набагато менш розвинений, ніж традиційні методи активного аналізу, тому що вимагають значних зусиль від аналітика для розміщення датчиків, збору даних і аналізу результатів. Такі фактори формують виникнення наведених недоліків.

Виправлення відбувається при використанні глибоких нейронних мереж, або ж нейронних мереж натренованих на трафіку, що циркулює у мережі підприємства. Використовуючи цей метод, аналіз та ідентифікація загроз може бути значно спрощена за допомогою нейронної мережі. Такі мережі можуть бути натреновані за допомогою використання різних методів. Наприклад: метод тренування по дельта-правилу, MNIST або по базі данних (Modified National Institute of Standards and Technology), з «вчителем» або без нього. Одним з таких методів є написання штучного інтелекту, який, навчений на реальному мережевому трафіку, буде генерувати різноманітний трафік, включаючи шкідливий а також корегувати вагу нейронів. А потім використання цього штучного інтелекту для генерування дата-сету тренування нейронної мережі, що буде спрощувати аналіз. Другий метод – написання такого дата-сету вручну, враховуючи потреби та найчастіші загрози безпеці підприємства, використовуючи базу даних загроз, яка містить вже відомі загрози всередині мережевого трафіку, що аналізуємо.

Таким чином, ми розглянули метод аналізу за допомогою переведення мережевої карти в нерозбірливий режим та метод розставляння сенсорів при пасивному мережевому аналізу. Виявлені деякі недоліки пасивного аналізу та запропоновано методи їх вирішення, а саме для вирішення проблеми аналізу загроз безпеці надаються методи використання нейронної мережі, як допоміжний інструмент у аналізі. Запропоновано використання ідентифікації користувачів мережі по заголовкам пакетів, що вони відправляють, для полегшення розслідувань та ідентифікації пристроїв з яких відбувалися неправомірні дії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Alexander J. Beecroft, Passive Fingerprinting of Computer Network Reconnaissance Tools, Monterey, CA 93943-5000, 2009, 89 p.
[2] A. Bremler-Barr, Y. Harchol, D. Hay, Y. Koral, Deep packet inspection as a service, 2014, p. 271.
[3]: Пассивный анализ сети. [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.securitylab.ru/analytics/350448.php
[4] Исследование угроз безопасности и атак в сетях [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/ru-ru/research/analytics/ss7-vulnerability-2018/
[5] Colin J. Bennett, Andrew Clement, Kate Milberry, Introduction to Cyber-Surveillance. Cyber Surveillance in Everyday Life, 2012, 21 p.
[6] Network Intrusion Detection Signatures. [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: http://www.symantec.com/connect/articles/network-intrusion-detection-signatures-partfive.

УДК 004.738.5

АНАЛІЗ ХМАРНОЇ ТЕХНОЛОГІЇ GOOGLE DRIVE

РОМАНЮК О. Н., БОРИСОВА К. О., КАТЄЛЬНІКОВ Д. І. (*rom8591@gmail.com*)
Вінницький національний технічний університет

У статті розглянуто одне із найвідоміших хмарних сховищ даних та порівняно його з аналогічним продуктом від компанії Microsoft.

Хмарні сервіси [1-7], що дозволяють перенести обчислювальні ресурси й дані на віддалені інтернет-сервери, в останні роки стали одним з основних трендів розвитку IT-технологій. Щоб скористатися можливостями технологій, людині достатньо бути там, де є Інтернет, і мати пристрій, в якому є інтернет-браузер.

За даними аналітичного агентства *Research and Markets, очікується зростання глобального ринку хмарних обчислень від $371,4 млрд. у 2020 році до $832,1 млрд. у 2025 [1]. Необхідність у хмарних технологіях збільшилась внаслідок закриття офісів, шкіл і підприємств у зв'язку із пандемією COVID-19. Працівники використовують хмарні платформи для обміну даними та знаннями і спілкування протягом локдаунів.*

Одним із найпоширеніших подібних сервісів є хмарні сховища даних. *Хмарне сховище даних* – це модель зберігання цифрових даних в онлайновому просторі, що охоплює кілька серверів та місце розташувань, і зазвичай підтримується хостинг-компанією [2]. Таким чином, замість розміщення файлів на фізичних носіях пам'яті, здійснюється поступове перенесення інструментів і результатів роботи у хмарний простір задля підвищення їх доступності. Крім цього, втрата документа абсолютно виключена при хмарному зберіганні, коли копія документа завжди доступна на сервері та може бути легко знайдена засобами

XXI Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.