МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

ЯВОРСЬКИЙ РУСЛАН ІВАНОВИЧ

УДК 004.056

ОГЛЯД ЗАГРОЗ ДЛЯ ЗАХИЩЕНОСТІ ПРОГРАМНИХ СИСТЕМ ТА ЗАСОБІВ ЗАХИСТУ ВІД ЗОВНІШНЬОГО ПРОНИКНЕННЯ У ХМАРНИХ СЕРВІСАХ

125 "Кібербезпека”

Автореферат
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль
2019

Роботу виконано на кафедрі кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: доктор технічних наук, доцент кафедри кібербезпеки **Александер Марек Богуслав**, Тернопільський національний технічний університет імені Івана Пулюя

Рецензент: д.т.н., професор кафедри комп'ютерних наук Приймак М.В. **_____,** Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 26 грудня 2019 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії № ____ у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус № 1, ауд. 806.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Віртуалізація дає ряд переваг, ніж традиційні системи. Віртуалізація дозволяє одночасно запускати кілька операційних систем. Більше того, віртуалізація пропонує покращені, оптимізовані та дешеві послуги для клієнтів завдяки підтримці наданні своїх послуг, як абстрактної хмари у. Екземпляри серверів і сервісів в цьому випадку називаються віртуальними машинами (VM). Кожна VM має власну операційну систему та прикладні програми. Ініціюється VM для кожного користувача. Таким чином практично кожен користувач має доступ до віртуального комп'ютера. Монітор VM або гіпервізор – це модуль, що управляє VM та координує одночасну роботу операційних систем на одній фізичній машині.

Ризики щодо безпеки можуть змінюватися залежно від типу використовуваного гіпервізора. Підтримуваний гіпервізор розміщений в операційній системі. Ця віртуалізована інфраструктура піддається більшій загрозі, ніж звичайна традиційна операційна система. Віртуальні машини розміщуються на фізичному хості, і вони можуть комунікувати одна з одною. Ця комунікація дозволяє здійснювати атаки зловмисників. Тому тема роботи є актуальною з точки зору захисту віртуальних сервісів від вторгнень шкідливого програмного забезпечення.

Мета роботи: розгляд теоретичних та практичних засад технології виявлення інфікованих комп'ютерів, формалізацію створення методик виявлення атак на віртуальні сервіси.

Для досягнення вказаної мети в рамках дипломної роботи було сформульовано та розв’язано наступні задачі:

- розглянути основні загрози систем, що надають віртуальні сервіси;
- розглянути методи виявлення атак на хмарні мережеві сервіси;
- виконати аналіз інструментів виявлення вторгнень;
- запропонувати рішення для покращення достовірності спрацювання системи виявлення вторгнень.

Об’єкт, методи та джерела дослідження: процес виявлення шкідливого програмного забезпечення.

Методи дослідження. Для досягнення мети дипломної роботи використовувались:

– методи узагальнення та аналізу – при проведенні огляду стану загроз для віртуальних мережевих сервісів;

– формалізації та математичного моделювання – при розробці методу виявлення вторгнень на основі статистичних методів.

Предмет дослідження: способи виявлення вторгнень на основі різноманітних підходів і принципів.

Наукова новизна отриманих результатів.

Наукова новизна полягає у вирішенні задачі систематизації відомостей про засоби виявлення та запобігання атак на хмарні мережеві сервіси. При цьому було отримано такі результати:

– на основі класифікації загроз запропоновано використовувати системи виявлення вторгнень на основі нейронних мереж;

– виокремлено переваги та недоліки систем виявлення вторгнень на основі різних принципів;

– вироблено рекомендації стосовно використання систем виявлення вторгнень.

Практичне значення отриманих результатів.

Всі розроблені методи можуть бути доведені до практичного впровадження у складі системи захисту від зловмисного вторгнення. Така система дозволить мінімізувати ризики захищеності систем на основі віртуальних сервісів.

Апробація. Основні положення роботи доповідались, розглядались та обговорювались на науковій конференції Тернопільського національного технічного університету. Результати дипломної роботи опубліковані у 1 науковій праці, яка є тезами студентської наукової конференції, яка проводились у ТНТУ.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 7 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – ____ арк. формату А4.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі розкрито актуальність теми, окреслено основні завдання на дипломну роботу.

В першому розділі виконано аналітичний аналіз поставленого завдання та систематизовано матеріал, що стосується систем виявлення вторгнень на мережеві хмарні сервіси.

В другому розділі описано аналіз методів виявлення аномалій у віртуальних системах. Основну увагу приділено нейронним мережам та аспектам виявлення атак на віртуальні служби з використанням нейронних мереж

В розділі практичної реалізації Описано методи та системи для визначення аномальної мережі. Проаналізовано різні підходи до виявлення аномалій на основі статистичних підходів, машинного навчання, класифікації, кластеризації

В частині «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання планування робіт по охороні праці та аналіз небезпек природного походження та антропогенного походження.

В частині «Екологія» проаналізовано сучасний екологічний стан України, розглянуто питання забруднення довкілля, що виникає внаслідок використання комп'ютерної техніки, а також запропоновано заходи зі зменшення цього негативного впливу.

У загальних висновках щодо дипломної роботи описано прийняті в проекті технічні рішення і організаційно-технічні заходи, які забезпечують виконання завдання; оригінальні технічні рішення, прийняті автором в процесі роботи; технічні рішення роботи, які можуть бути впроваджені практично.

В додатках до пояснювальної записки приведено копії тез доповідей на студентській науковій конференції.

ВИСНОВКИ

У процесі виконання дипломної роботи було отримано наступні результати.

Методи кластеризації, які використовують лише звичайні мітки, часто можуть бути ефективнішими, ніж методи, засновані на класифікації. У ситуаціях, коли визначити хороший показник відстані важко, класифікація або статистичні методи можуть бути кращим вибором. Однак на успіх статистичних методів значною мірою впливає застосовність статистичних припущень у конкретних сценаріях реального життя.

Для реального часу виявлення вторгнень, складність аномалії процесу виявлення грає життєво важливу роль. У разі класифікації, кластеризації та статистичних методів, хоча навчання є дорогим, вони все ще прийнятні, оскільки тестування проходить швидко, а навчання в режимі офлайн. На відміну від таких методів, як найближчий сусід та спектральні методи, які не мають фази навчання, мають дорогу фазу тестування, яка може бути обмеженням у реальній обстановці.

Методи виявлення аномалій зазвичай передбачають, що аномалії даних є рідкісними порівняно із звичайними випадками. Взагалі такі припущення справедливі, але не завжди. Часто непідконтрольні методи страждають від великої помилкової частоти тривоги, коли аномалії знаходяться у великій кількості. Для виявлення об'ємних аномалій можуть застосовуватися методи, що працюють в режимах, що контролюються.

Більшість існуючих IDS для провідникового середовища працюють трьома способами: трафік рівня потоку або аналіз даних на рівні пакета, аналіз даних, аналіз протоколу або перевірка корисного навантаження. Кожна з цих категорій має свої переваги та обмеження. Отже, гібридизація цих (наприклад, аналіз рівня протоколу з подальшим аналізом трафіку на рівні потоку) може дати кращі показники з точки зору відомого (з високою швидкістю виявлення), а також невідомого виявлення атаки.

IDS, здатна ідентифікувати як відомі, так і невідомі атаки, повинна використовувати як під контролем (навчання, засноване на правилах чи підписах), так і без нагляду (кластеризація або групування) на декількох рівнях для роботи в режимі реального часу з низькою помилковою помилкою. показники тривоги.

Розробник IDS повинен вибирати основні компоненти, метод (и), методи або базу правила / підпису / профілю для подолання чотирьох важливих обмежень: суб'єктивна ефективність, обмежена масштабованість, ефективність залежно від сценарію та обмежена безпека.

Ефективність кращої ІДС повинна встановлюватися як якісно, так і кількісно.

Краща класифікація або метод ідентифікації аномалій дозволяє нам настроїти її (відповідні нормальні профілі, пороги тощо) залежно від сценарію мережі.

Хоча дослідницькою спільнотою було розроблено багато методів та систем, все ж існує низка відкритих дослідницьких питань та проблем. Відповідність показників

продуктивності є загальновизнаним недоліком у виявленні вторгнень. Оцінюючи ІДС, три найважливіші якості, які потрібно виміряти, – це повнота, коректність та продуктивність. Поточний стан сучасного виявлення вторгнень обмежує оцінку нових систем тестуванням неповних наборів даних, які тестують вузько визначені компоненти системи. Деякі системи, засновані на аномалії, були протестовані за допомогою надуманих наборів даних. Така оцінка обмежена якістю набору даних, щодо якої оцінюється система. Побудова об'єктивного набору даних, що є об'єктивним, реалістичним та всеосяжним, є надзвичайно складним завданням.

Деякі важливі питання ми розбираємо як виклики та перелічуємо їх нижче.

I. Обмеження часу виконання є важливою проблемою для NIDS. Не втрачаючи жодних пакетів, IDS у реальному часі повинен бути в ідеалі здатним захоплювати та перевіряти кожен пакет.

II. Більшість NIDSів та мережевих методів виявлення вторгнень в мережу залежать від середовища. В ідеалі система чи метод повинні бути незалежними від середовища.

III. Характер аномалій постійно змінюється, оскільки зловмисники адаптують свої мережеві атаки, щоб уникнути існуючих рішень виявлення вторгнень. Отже, адаптованість NIDS або методу виявлення необхідна для оновлення з поточними аномаліями, що зустрічаються в локальній мережі або Інтернеті.

IV. В ідеалі, NIDS або метод виявлення повинен уникати високої кількості помилкових тривог. Однак не можна повністю врятуватися від помилкових тривог, навіть якщо йому потрібно прагнути до цього в будь-якому середовищі та полегшити адаптивність під час виконання. Це ще один виклик для спільноти розвитку NIDS.

VI. Підготовка об'єктивного набору даних про вторгнення в мережу з усіма ненормальними варіаціями профілів – ще одне складне завдання. Кількість нормальних випадків зазвичай велика, і їх частка із випадками нападу дуже перекошена у існуючих загальнодоступних наборах даних про вторгнення. Лише кілька наборів даних про вторгнення з достатньою кількістю інформації про атаку доступні загальнодоступним. Таким чином, існує загальна потреба у контрольних наборах даних про вторгнення для оцінки NIDS та методів виявлення.

1. Розробка відповідного та швидкого методу вибору функцій для кожного класу атаки – наступна проблема.

2. Вибір відповідної кількості некорельованих, неупереджених класифікаторів з пулу класифікаторів шляхом формування гіпотези класифікатора для побудови ефективного підходу ансамблю для виявлення мережевої аномалії є додатковим завданням.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Яворський Р. Проблеми інформаційної безпеки при розгортанні системи виявлення вторгнень [Текст] / Р. Яворський, В. Амбок, В. Леньо. Матеріали науково-технічної конференції «Інформаційні моделі, системи та технології» Тернопільського національного технічного університету імені Івана Пулюя. – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2019. – с. 108.

АНОТАЦІЯ

У магістерській роботі виконано дослідження способів забезпечення необхідного рівня захищеності хмарних сервісів, які доступні через мережеві з'єднання. Виконано огляд і класифікація матеріалу стосовно способів впливу шкідливого програмного забезпечення на мережеві хмарні сервіси та вироблено рекомендації стосовно використання систем виявлення вторгнень на основі різних принципів.

В дипломній роботі показано актуальність оцінювання рівня захищеності хмарних сервісів. Пропонується спосіб відбору характеристик та методів роботи систем виявлення вторгнень на основі нейромереж та статистичних методів.

Ключові слова: ЗАГРОЗА, НЕЙРОННА МЕРЕЖА, КЛАСИФІКАЦІЯ, СТАТИСТИЧЕНІ МЕТОДИ, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ.

ANNOTATION

The master's thesis investigates how to provide the required security level of cloud services that are accessible through network connections. The material was reviewed and classified regarding the ways in which malware could affect the network cloud services, and recommendations were made regarding the use of intrusion detection systems based on various principles.

The diploma thesis shows the relevance of assessing the security level of cloud services. A method of selecting the characteristics and methods of operation of neural network based intrusion detection systems and statistical methods are proposed.

Key words: THREAT, NEURAL NETWORK, CLASSIFICATION, STATISTICAL METHODS, INTRUSION DETECTION SYSTEM.