# ДОДАТОК А

Графічний матеріал атестаційної роботи

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

АТТЕСТАЦІЙНА РОБОТА МАГІСТРА

на тему:

# Методи виявлення атак на комп’ютерну мережу

Виконав: ст. гр. КСМзм-19-1
Жукова І.Ю.

Керівник: доц. каф. ЕОМ
Голубничий Д.Ю.

## Мета, об’єкт та предмет роботи

- Метою дипломного проекту є дослідження методів виявлення атак в комп’ютерній мережі та розробка системи виявлення атак на мережеві ресурси із застосуванням нейромережевих технологій.
- Об'єктом дослідження дипломного проекту є спроектована і навчена нейронна мережа.
- Предметом дослідження виступає мережевий трафік.

# Класифікації атак:

- 1) віддалене проникнення;
- 2) локальне проникнення;
- 3) віддалена відмова в обслуговуванні;
- 4) локальна відмова в обслуговуванні;
- 5) атаки з використанням мережевих сканерів);
- 6) атаки з використанням сканерів вразливостей;
- 7) атаки з використанням зломщиків паролів;
- 8) атаки з використанням аналізаторів протоколів (sniffers)

Класифікація від Internet Security Systems, Inc.:

- 1) збір інформації;
- 2) спроби несанкціонованого доступу;
- 3) відмова в обслуговуванні;
- 4) із підозрілою активністю;
- 5) системні атаки.

За типом програмного середовища:

- вразливості в операційній системі;
- вразливості в певному сервісі;
- вразливості в певному програмному забезпеченні


3

За характером вразливості, використовуваної для реалізації атаки:

- "чорні ходи" (Backdoors);
- помилки в CGI-скриптах;
- атаки типу "відмова в обслуговуванні";
- помилки в FTP-серверах;
- наявність на комп'ютері сервісу Finger або помилки в програмах, що реалізують цей сервіс;
- помилки в реалізації міжмережевих екранів;
- помилки, що дозволяють користувачеві, що має термінальний вхід на даний сервер, отримати права адміністратора;
- помилки, що дозволяють атакуючому віддалено отримати права адміністратора;
- інші помилки, які не ввійшли в інші категорії;
- помилки в NIS-серверах;
- помилки в RPC-серверах;
- вразливості, що дозволяють атакуючому віддалено отримати будь-який файл з сервера;
- помилки в SMTP-серверах;
- невикористовувані сервіси (Useless services).

За типом атаки:

- локальні (Host Based);
- віддалені (Network Based).

- За характером дій, використовуваних в атаці:
- "чорні ходи" (Backdoors);
- атаки типу "відмова в обслуговуванні" (Denial of Service, DoS);
- розподілені атаки типу "відмова в обслуговуванні" (Distributed Denial of Service);
- потенційно незахищена операційна система (OS Sensor);
- неавторизований доступ (Unauthorized Access Attempts);

За ступенем ризику:

- високий (High);
- середній (Medium);
- низький (Low);

4

# Методи виявлення атак:

Метод сигнатурного аналізу - зіставлення реальної сигнатури (в конкретній точці пристрою), відображеної на дисплеї сигнатурного аналізатора, з еталонною сигнатурою цієї точки.

Статистичний метод - використання вже розробленого і перевіреного апарату математичної статистики і адаптація до поведінки суб'єкта.

Нейромережеві методи - аналіз інформації та оцінка узгодженості даних з характеристиками, які нейромережа навчена розпізнавати

Штучні імунні системи – використання різноманітних механізмів навчання, пам'яті і асоціативного пошуку для вирішення завдань розпізнаванія і класифікації.

Графові моделі атак - побудова графа, який містить всі відомі сценарії атак, на основі певного характеру коректності системи.

Експертні системи - набор правил, які охоплюють знання людини-експерта.

Кластерний аналіз - метод інтелектуального аналізу даних, що дозволяє групувати об'єкти в кластери на підставі обраної міри схожості між об'єктами.

| | Рівень нагляду за системою | Верифікуємість | Адитивність | Стійкість | Обчислювальна складність |
|---|---|---|---|---|---|
| Аналіз сигнатур | Host; Network; Application | + | - | глобальна | O(logn) |
| Статистичний контроль | Host; Network | - | + | локальна | O(n) |
| Нейромережеві методи | Host; Network; Application | + | + | локальна | O(n) |
| Штучні імунні системи | Host; Network | - | + | локальна | O(n) |
| Графові моделі атак | Host; Network; Application | + | + | локальна | NP |
| Методи кластерного аналізу | Host; Network; Application | - | + | локальна | O(n) |
| Експертні системи | Host; Network | + | + | глобальна | NP |

**5**

# Системи виявлення мережевих атак:

**Bro** - мережева система виявлення атак. Вона є набором модулів декомпозиції даних різних мережевих протоколів (від мережевого до прикладного рівня) і набором сигнатур над подіями відповідних протоколів.

**OSSEC** - первісно орієнтована на виявлення атак рівня системи (вузлових). Вона найбільш нова з розглянутих систем. Включає набір аналізаторів для різних джерел даних, контроль цілісності файлової системи, сигнатури відомих троянських закладок (rootkits) та ін.

**STAT** - експериментальна університетська розробка, і найбільш "стара" з даних систем - перші публікації датуються 1992 роком. Система включає набір компонентів виявлення атак різних рівнів – мережний (NETSTAT), вузловий (USTAT, WINSTAT), додатків (WEBSTAT), тобто є класичною гібридною системою.

**Prelude** - гібридна, тобто здатна виявити атаки як на рівні системи, так і на рівні мережі. Система спочатку розроблялася як самостійна СВА, але в даний час є високорівневою надбудовою над відкритими СВА і системами контролю цілісності.

**Snort** - чисто мережева СВА і, окрім основної бази описів атак, має набір підключаємих модулів для виявлення специфічних атак або таких, що реалізовують альтернативні методи виявлення. Найбільш популярна на сьогоднішній день некомерційна СВА.

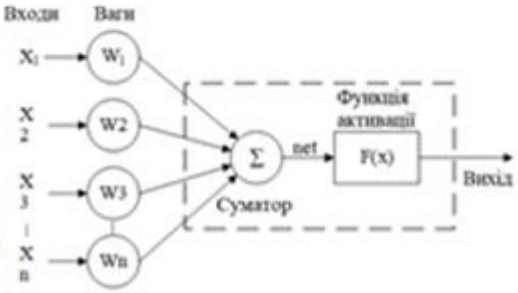
| | Класи атак | Рівень спостереження за системою | Метод виявлення | Адаптивність | Масштабованість | Реакція | Захист |
|---|---|---|---|---|---|---|---|
| Bro | [illegible] | Системний | Сигнатурний | - | - | - | - |
| OSSEC | [illegible] | Системний | Сигнатурний | +/- | + | - | - |
| STAT | [illegible] | Системний, мережевий | Сигнатурний, аналіз переходів станів | - | + | + | SSL |
| Prelude | [illegible] | Системний, мережевий | Сигнатурний | - | + | + | SSL, Libnids |
| Snort | [illegible] | Мережевий | Сигнатурний | - | - | + | - |

**6**

Нейронні мережі - це один з напрямків досліджень в області штучного інтелекту, заснований на спробах відтворити нервову систему людини, а саме: здатність нервової системи навчатися та виправляти помилки, що дозволяє змоделювати, хоча і досить грубо, роботу людського мозку.

До завдань, що вирішують нейронні мережі, можна віднести:

- розпізнавання образів і класифікація;
- завдання кластеризації;
- апроксимація функцій;
- оптимізація.



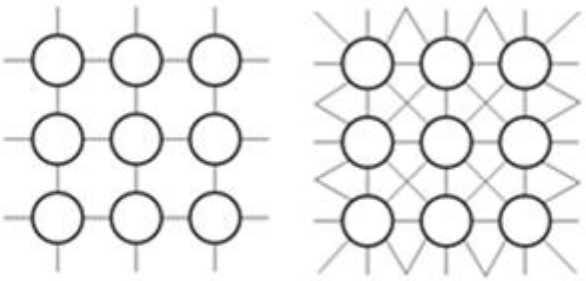

Нейронна мережа складається з нейронів. Кожен нейрон є елементарною структурною одиницею нейронної мережі. Процес навчання мережі зводиться до зміни вагових коефіцієнтів Wn. NET в даному випадку і є результат обчислень нейрона. Результати обчислення передаються на вихід через функцію активації.

Функція активації нейрона - це функція, яка обчислює вихідний сигнал нейрона. На вхід цієї функції подається сума всіх добутків сигналів і ваг цих сигналів.

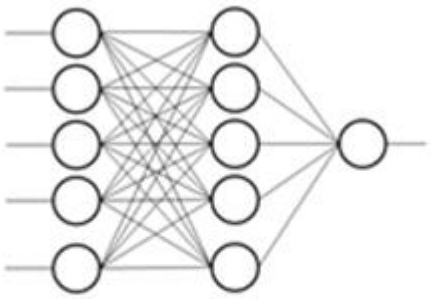
Можна виділити наступні функції активації :

1. Одиничний стрибок або жорстка порогова функція: $Out = \begin{cases} 0, NET < \theta \\ 0, NET \geq \theta \end{cases}$
2. Сигмоїдальна функція або сигмоїд: $Out = \frac{1}{1+e^{-NET}}$
3. Гіперболічний тангенс: $Out = th(NET)$ або $Out = \frac{e^{NET} - e^{-NET}}{e^{NET} + e^{-NET}}$

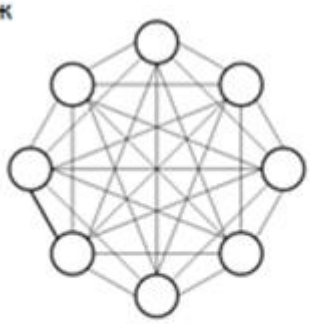
**7**



Структурна схема
слабозв'язаних мереж



Структурна схема
багатошарової мережі



Структурна схема
повнозв'язної мережі

**8**

## Існують два концептуальних підходи до навчання нейронних мереж: навчання з вчителем і навчання без вчителя.

Навчання нейронної мережі з вчителем передбачає, що для кожного вхідного вектора з навчальної множини існує необхідне значення вихідного вектора. Ці вектора утворюють навчальну пару і ваги в мережі змінюються до тих пір, поки прийнятний рівень відхилення між векторами не буде досягнутий.


Навчання нейронної мережі без вчителя передбачає те, що навчальна безліч складається тільки з вхідних векторів. Алгоритм навчання мережі підлаштовує ваги так, щоб виходили узгоджені вихідні вектори.

При цьому дотримується наступна послідовність подій:

1) в нейронну мережу надходять зовнішні сигнали (вхідні параметри);

2) вільні параметри мережі змінюються;

3) після змін нейронна мережа приймає вхідні сигнали вже іншим чином.


9

## Інструменти розробки


10

# Апробація результатів




Голубничий Д.Ю. Оцінка складності методів виявлення атак / А.В. Власов, В.Ф. Третяк, Д.М. Запара, І.Ю. Жукова // Scientific Collection «InterConf», (37): with the Proceedings of the 1st International Scientific and Practical Conference «Recent Scientific Investigation» (December 6-8, 2020). – Oslo, Norway: Dagens naeringsliv forlag, 2020. – Pp. 1061 – 1070. https://ojs.ukrlogos.in.ua/index.php/interconf/issue/view/6-8.12.2020

**11**

# ВИСНОВКИ

У процесі виконання роботи були вирішені завдання:

1. Проведено аналіз існуючих атак, методів та систем їх виявлення.
2. Досліджено технології і програмне забезпечення використане для розробки компонентів системи.
3. Спроектована і розроблена програма збирача даних.
4. Спроектована і розроблена програма аналізатор.
5. Спроектовано і розроблено веб додаток для перегляду підозрілої активності.
6. Спроектовані і розроблені дві моделі нейронних мереж.

Моделі здатні аналізувати дані з мережі, навіть якщо дані неповні або перекручені. Кожна модель може проводити аналіз в нелінійній формі. Обидві ці характеристики важливі для використання в мережних технологіях, де інформація часто піддається випадковим помилкам обладнання.

**12**