ICSSH

INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE

SCIENCE, TECHNOLOGY AND SOCIETY: CHALLENGES AND PROSPECTS FOR DEVELOPMENT IN THE MODERN WORLD

Book of abstracts

December 6, 2024

Tampere,
Finland

INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE

SCIENCE, TECHNOLOGY AND SOCIETY: CHALLENGES AND PROSPECTS FOR DEVELOPMENT IN THE MODERN WORLD

Book of abstracts

December 6, 2024
Tampere,
Finland

UDC 37:082.2(06)

International scientific-practical conference "Science, technology and society: challenges and prospects for development in the modern world": conference proceedings (Tampere, Finland, December 6, 2024). Tampere, Finland: Scholarly Publisher ICSSH, 2024. 91 pages.

The proceedings of the International scientific-practical conference "Science, technology and society: challenges and prospects for development in the modern world" featured the materials of participants from:

Alfred Nobel University
Berdiansk State Pedagogical University
Bogomolets National Medical University
Dnipro State Medical University
Ivan Franko National University of Lviv
Kharkiv National Air Force University named after Ivan Kozhedub
Kharkiv National Medical University
Kherson State University
Khmelnytsky National University
Kryvyi Rih City Clinical Hospital № 2 of Kryvyi Rih City Council
Kryvyi Rih Educational and Research Institute of Donetsk State University of Internal Affairs
Kyiv National University of Construction and Architecture
Lviv National University of Environmental Management
Lviv State University of Physical Culture named after Ivan Bobersky
Marzeev Institute of Public Health of the National Academy of Medical Sciences of Ukraine
Municipal Higher Education Institution "Dnipro Academy of Continuing Education" of the Dnipro Regional Council
Municipal Institution "Kharkiv Humanitarian and Pedagogical Academy" of the Kharkiv Regional Council
Mykhailo Drahomanov Ukrainian State University
Narodytskyy kindergarten of Narodytskyy village council
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
National University of Pharmacy
Pavlo Tychyna Uman State Pedagogical University
Polissya National University
Private higher education institution "European University"
Pylyp Orlyk International Classical University
SHEI Priazovsky State Technical University
State institution "O. S. Kolomiychenko institute of otolaryngology of national academy of medical sciences of Ukraine"
State Institution "Institute of Forensic Psychiatry of the Ministry of Health of Ukraine"
State University "Kyiv Aviation Institute"
Taras Shevchenko National University of Chernihiv Collegium
Taras Shevchenko National University of Kyiv
Ternopil Volodymyr Hnatiuk National Pedagogical University
Ukraine National University "Yuriy Kondratyuk Poltava Polytechnic"
Ukrainian Military Medical Academy
Ukrainian State Flight Academy
University of Economics and Law "KROK"
Uzhhorod National University
V. I. Vernadsky Taurida National University
V. N. Karazin Kharkiv National University
Vozianov Institute of Urology of the National Academy of Medical Sciences of Ukraine
Yuriy Fedkovych Chernivtsi National University
Zhytomyr State University named after Ivan Franko

Офіційний сайт: http://www.economics.in.ua

SECTION 12 INFORMATION TECHNOLOGIES

УДК 004.89

Ланде Д. В.
д.т.н.,
Золотов І. К.
бакалавр
КПІ ім. Ігоря Сікорського, ІПРІ НАН України

РОЗРОБКА МЕТОДОЛОГІЧНИХ ЗАСАД АУДИТУ КІБЕРБЕЗПЕКИ НА БАЗІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ

Сучасні корпоративні мережі є складними та вразливими до кіберзагроз, які постійно еволюціонують. Традиційні методи аудиту безпеки часто не завжди можуть впоратися із новими викликами, що ставить під загрозу критичні ресурси. Інноваційні підходи, зокрема застосування генеративного штучного інтелекту (ГШІ), дозволяють автоматизувати процеси аудиту кібербезпеки та прогнозувати сценарії можливих атак зловмисників. У цьому дослідженні пропонується методологія аудиту кібербезпеки корпоративних мереж на базі ГШІ, використовуючи моделювання мережевих з'єднань, аналіз вразливостей та оцінку ймовірності атак.

Метою дослідження є розробка методології та технологічних рішень для автоматизованого аудиту кібербезпеки корпоративних мереж за допомогою ГШІ. Зокрема, пропонується підхід, що полягає у створенні моделі мережі із зазначенням вузлів, зв’язків, критичності ресурсів та вразливостей, на основі якої здійснюється оцінка можливих сценаріїв атак.

Серед досліджень, де застосовуються моделі ГШІ для прогнозування кіберзагроз, варто відзначити роботу [1], де йдеться про кіберрозвідку загроз (Cyber Threat Intelligence, CTI), для чого застосвуються великі мовні моделі (LLMs). У роботі [2] йдеться про застосування ГШІ для оцінки ймовірностей зловмисних переходів між вузлами корпоративної мережі. У роботі [3] демонструєтьсяі як моделі ГШІ можуть бути використані для створення семантичних мереж, які допомагають передбачати потенційні сценарії атак. Також у цій роботі запропоновано концепцію "рою віртуальних експертів", яка базується на ідеї колективного інтелекту, коли кілька моделей ГШІ або віртуальних агентів співпрацюють для вирішення задачі. JSON (JavaScript Object Notation) є стандартним форматом для зберігання та обміну структурованими даними і широко застосовується для опису об'єктів кіберзахисту. [4] описують використання подібних форматів даних для аналізу логів і вразливостей в інформаційних системах. Розрахунок ризиків кібербезпеки є складним процесом, який потребує врахування ймовірностей реалізації різних сценаріїв атак, оцінки вразливостей та критичності ресурсів. У [5] розглядають методи оцінки ризиків на основі моделювання сценаріїв загроз за допомогою ChatGPT.

Методологія

Запропонована методологія аудиту кібербезпеки базується на використанні ГШІ для моделювання кіберзагроз та прогнозування можливих сценаріїв атак. Ключовими етапами методології є моделювання корпоративної мережі, генерація сценаріїв можливих атак, оцінка ймовірності атак, ранжування отриманих сценаріїв. Для моделювання корпоративної мережі створюється JSON-структура, які описує вузли мережі (сервери, маршрутизатори, хаби тощо), їхні параметри (IP-адреси, операційні системи, вразливості, рівень захищеності) та зв’язки між ними. Генерація сценаріїв атак здійснюється шляхом використання генеративного ГШІ для моделювання можливих шляхів дій зловмисників у мережі. Цей процес включає

використання рою віртуальних експертів, які допомагають ідентифікувати можливі шляхи проникнення. Для оцінки ймовірності атак застосовується алгоритм, за допомогою якого розраховуються ймовірності переходів зловмисників між вузлами та оцінює ризики досягнення критичних ресурсів мережі. На основі розрахованих ймовірностей сценарії атак ранжуються за рівнем ризику, що дозволяє фахівцям з безпеки зосередитися на найбільш небезпечних загрозах.

Математична модель

Мережа представлена у вигляді графа $G=(V,E)$ де V — це вузли (сервери, хаби, маршрутизатори), а E — це зв'язки між ними. Для кожного вузла визначається функція критичності $C(v)$, яка відображає важливість вузла у корпоративній мережі. Зв’язки характеризуються ймовірністю атаки $P(e)$, яка залежить від шифрування, вразливостей та інших параметрів з’єднання. Процес прогнозування сценаріїв атак здійснюється за допомогою пошуку можливих шляхів Π у графі, де для кожного шляху розраховується ймовірність успішної атаки

$$P(\Pi) = \prod_{e \in \Pi} P(e)$$

Далі використовується ранжування шляхів на основі ймовірності та критичності ресурсів, до яких ці шляхи ведуть.

Технологічні засади

Запропонована методологія реалізується у вигляді програмного застосунку, що дозволяє завантажити структуру корпоративної мережі у форматі JSON, після чого система генерує сценарії атак за допомогою генеративного ШІ та розраховує ймовірності. Основні технологічні рішення також включають автоматизоване моделювання вузлів і зв’язків мережі; генерацію сценаріїв атак із застосуванням рою віртуальних експертів; оцінку ймовірності атак та ранжування сценаріїв на основі критичності ресурсів.

Висновки

Застосування генеративного ШІ для аудиту кібербезпеки забезпечує автоматизовану оцінку ризиків і прогнозування можливих сценаріїв атак. Запропонована методологія може стати основою для створення нових інструментів аудиту кібербезпеки, що нададуть фахівцям з безпеки інформацію щодо вразливостей та можливих шляхів проникнення зловмисників.

Список літератури

1. Shafee, Samaneh, Alysson Bessani, and Pedro M. Ferreira. "Evaluation of LLM-based chatbots for OSINT-based Cyber Threat Awareness." Expert Systems with Applications (2024): 125509. DOI: 10.1016/j.eswa.2024.125509

2. Ланде Д.В., Новіков О.М., Алексейчук Л.Б. Визначення коефіцієнтів логіко-ймовірнісних моделей кібербезпеки з використанням віртуальних експертів. Theoretical and Applied Cybersecurity. Матеріали другої всеукраїнської науково-практичної конференції (TACS-2024). - Київ: Інжиніринг, 2024. - С. 11-20.ISBN 978-966-2344-98-1

3. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3

4. Ramsdale, Andrew, Stavros Shiaeles, and Nicholas Kolokotronis. "A comparative analysis of cyber-threat intelligence sources, formats and languages." Electronics 9.5 (2020): 824. DOI: 10.3390/electronics9050824

5. Naito, Takeru, Rei Watanabe, and Takuho Mitsunaga. "Llm-based attack scenarios generator with it asset management and vulnerability information." In 2023 6th International Conference on Signal Processing and Information Security (ICSPIS), pp. 99-103. IEEE, 2023. DOI: 10.1109/ICSPIS60075.2023.10344019