УДК 004.056.53
Н. Бурмістрова; Р. Козак, к.т.н., доцент
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ МАШИННОГО НАВЧАННЯ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ: ФРЕЙМВОРК SHENNINA

UDC 004.056.53
N. Burmistrova, student of gr. СБм-61; R. Kozak, Ph.D., Assoc. Prof.

USING MACHINE LEARNING FOR PENETRATION TESTING: SHENNINA FRAMEWORK

Автоматизація процесів пентесту із застосуванням машинного навчання відкриває нові можливості для досягнення цілей кібербезпеки. Фреймворк Shennina, що використовує машинне навчання для адаптивного виявлення та експлуатації вразливостей, є одним із новітніх рішень у цій сфері, що потребує дослідження його ефективності та можливостей. Автоматизоване тестування на проникнення не лише сприяє оперативності й ефективності тестування, але й дозволяє значно розширити його масштаби, що особливо важливо для комплексних систем, де необхідна всеосяжна безпекова перевірка [1].

Метою дослідження був аналіз можливостей та обмежень фреймворку Shennina для автоматизованого тестування на проникнення в порівнянні зі сканером вразливостей Nessus. Дослідження спрямоване на оцінку ефективності використання Shennina для реальної експлуатації вразливостей та визначення сценаріїв, у яких цей фреймворк є найбільш доцільним [2].

Для тестування та порівняння ефективності інструментів Shennina та Nessus було обрано віртуальну машину Metasploitable 2, яка є навмисно вразливою версією операційної системи Ubuntu Linux, спеціально створеною для навчальних цілей у сфері кібербезпеки та тестування на проникнення. Ця віртуальна машина дозволяє відпрацьовувати навички виявлення та експлуатації вразливостей у безпечному та контрольованому середовищі.

У процесі дослідження використовували два основних інструменти: Nessus і Shennina, які виконували сканування в контрольованому середовищі [3]. Алгоритм дослідження передбачав чітко структуровані етапи, що забезпечують повноту аналізу та можливість порівняння результатів між обраними інструментами.

З метою оцінки роботи Shennina та Nessus було сформовано метрики, які дозволяють провести об'єктивне порівняння цих інструментів: кількість виявлених вразливостей, час виконання сканування, глибина аналізу, покриття тестової системи, споживання системних ресурсів.

У результаті дослідження встановлено, що фреймворк Shennina, завдяки інтеграції з Metasploit і можливості автоматичної експлуатації, продемонстрував гнучкість у виявленні та використанні не лише стандартних, але й штучно створених вразливостей конфігураційного характеру. Однак охоплення виявлених уразливостей було вужчим, ніж сканера вразливостей Nessus. Це свідчить про необхідність комплексного підходу: використання Nessus для широкого виявлення вразливостей і аналізу відповідності до CVE, а Shennina – для перевірки можливості експлуатації та оцінки практичного ризику для інформаційних систем.

Література

1. Yaacoub J.-P. A., Noura H. N., Salman O., Chehab A. A Survey on Ethical Hacking: Issues and Challenges // A Preprint. American University of Beirut, Electrical and Computer Engineering Department, Beirut, Lebanon. 2020.
2. The Usage of Machine Learning on Penetration Testing Automation // Proceedings of the 2023 3rd International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS). August 2023.
3. AI-Powered Penetration Testing using Shennina: From Simulation to Validation // Proceedings of the 2024 ACM Conference. July 2024.

.