ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ SIEM-СИСТЕМ ЩОДО ВИЯВЛЕННЯ СУЧАСНИХ ПРОТОКОЛІВ ОБФУСКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

Пліщенко В.С., Настенко А.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасний розвиток мережевих технологій, зокрема VPN-тунелів, супроводжується появою протоколів обфускації нового покоління - таких як Xray (з REALITY) та Hysteria V2 - призначених для повної імітації легітимного трафіку. Це робить традиційні мережеві системи виявлення та запобігання вторгнень (NIDS/NIPS), що ґрунтуються на сигнатурному аналізі, практично неефективними [1]. Унаслідок цього виникають додаткові ризики для периметру безпеки організацій, оскільки обфусковані канали залишаються непоміченими [2]. Обмежена здатність традиційних SIEM-систем виявляти обфускований трафік зумовлює потребу в перегляді архітектурних підходів до моніторингу безпеки корпоративних мереж.

Метою доповіді є експериментальна перевірка здатності традиційних NIDS/NIPS- і SIEM-систем виявляти обфускований мережевий трафік. **В доповіді** наводяться результати експериментів із виявлення VPN-трафіку, обфускованого за протоколами Xray та Hysteria-V2, у тестовому середовищі, побудованому на основі віддалених віртуальних серверів хмарних провайдерів. Отримані результати демонструють неспроможність стандартних NIDS/NIPS- і SIEM-систем виявляти такий трафік, оскільки обидва протоколи успішно обходять методи виявлення на основі розпізнавання TLS-відбитків (JA3/JA3S) завдяки імітації TLS-рукостискання з легітимними веб-серверами. Водночас, відповідно до сучасних досліджень [3, 4] перспективним є впровадження модулів UEBA, DPI-систем та методів машинного навчання, що дозволить класифікувати потоки обфускованого трафіку як аномальні. Перевірка ефективності застосування зазначених технологій у складі SIEM-систем становить актуальний напрям подальших досліджень.

Список літератури

1. Сєвєрінов, О. В., & Хрєнов, А. Г. (2014). Аналіз сучасних систем виявлення вторгнень. Системи обробки інформації, (6), 122-124.

2. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., Ahmad, F. «Network intrusion detection system: A systematic study of machine learning and deep learning approaches». Transactions on Emerging Telecommunications Technologies, 32(1), e4150. 2021 (First published 16 Oct 2020). DOI: 10.1002/ett.4150.

3. Song, W., Beshley, M., Przystupa, K., Beshley, H., Kochan, O., Pryslupskyi, A., Pieniak, D., & Su, J. «A Software Deep Packet Inspection System for Network Traffic Analysis and Anomaly Detection». Sensors, 20(6), 1637. 2020. DOI: 10.3390/s20061637.

4. L. Al-Bakhat and S. Almuhammadi. «Intrusion Detection on QUIC Traffic: A Machine Learning Approach». 2022 7th International Conference on Data Science and Machine Learning Applications (CDMA). pp. 194-199. 2022. DOI: 10.1109/CDMA54072.2022.00037.