ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ OPENGFW ЩОДО ВИЯВЛЕННЯ СУЧАСНИХ ПРОТОКОЛІВ ОБФУСКАЦІЇ МЕРЕЖЕВОГО ТРАФІКУ

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

Сучасний розвиток технічних засобів мережевої цензури та систем глибокого аналізу пакетів зумовлює постійне удосконалення протоколів обфускації мережевого трафіку. Протоколи обфускації нового покоління, такі як Hysteria V2 та стек протоколів Xray/V2Ray, розроблені для максимальної імітації легітимного вебтрафіку, що суттєво ускладнює їх виявлення [1]. У зв'язку з цим традиційні системи виявлення мережевих вторгнень (NIDS) та стандартні мережеві фільтри на основі сигнатурного аналізу стають практично неефективними, що створює нові виклики для моніторингу мережевої безпеки [2-4]. **Метою доповіді** є експериментальна перевірка здатності імітаційної моделі цензора OpenGFW виявляти обфускований мережевий трафік, згенерований протоколами VLESS з розширенням XTLS-Reality та Hysteria V2, а також пошук комплексних методів їх детектування.

В ході практичних експериментів базова архітектура OpenGFW не продемонструвала достатньої ефективності у класифікації обфускованого трафіку як аномального, оскільки зазначені протоколи успішно обходять сигнатурний аналіз та імітують легітимні з'єднання. Отримані результати свідчать, що для виявлення подібних обфускованих VPN-тунелів є необхідною інтеграція більш просунутих рішень, зокрема платформ розширеного виявлення і реагування (XDR/EDR). Окрім цього, критично важливим є впровадження методів активного зондування (active probing), індивідуально змодельованих для кожного протоколу обфускації.

Для підвищення ймовірності виявлення обфускованого трафіку варто поєднувати застосування методів активного втручання разом з одночасною інтеграцією пасивних методів аналізу трафіку, наприклад, виявлення специфічних характеристик мережевого з'єднання, таких як використання самопідписаних сертифікатів тощо.

Список літератури

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

2. Sina Ahmadi. «Network Intrusion Detection in Cloud Environments: A Comparative Analysis of Approaches». International journal of advanced computer science and applications. 2024. 15 (3). DOI: 10.14569/IJACSA.2024.0150301.

3. Wails, Ryan, et al. «Censorship evasion with unidentified protocol generation». 34th USENIX Security Symposium (USENIX Security 25). pp. 763-782. 2025.

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