УДК 004.056:004.7

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ ВИЯВЛЕННЯ ШКІДЛИВИХ МЕРЕЖНИХ ПАКЕТІВ

Матвейченко А. Є.
e-mail: artur.matveichenko@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

This work presents a comparative analysis of current network packet analyzers, addressing the increasing complexity of network infrastructures and the growing demand for effective cybersecurity monitoring. In light of rising cyber threats, the research emphasizes the necessity for a comprehensive approach to traffic analysis that not only deciphers detailed protocol data but also offers intuitive monitoring for a broad range of users. An evaluation of popular tools, such as Wireshark, Tcpdump, Nmap, Kismet, NetworkMiner, and SolarWinds Network Performance Monitor, reveals unique strengths and limitations pertinent to various operational environments. The work identifies key criteria for efficiency, including performance, analysis depth, user-friendliness, protocol support, cost, and platform independence.

З кожним роком зростає роль кібербезпеки, оскільки сучасні мережі стають все більш уразливими до кібератак та інших загроз у цифровому просторі. Аналіз мережних пакетів набуває особливої актуальності в умовах зростаючого обсягу трафіку та складності мережевих протоколів. Для забезпечення ефективного моніторингу та своєчасного виявлення аномалій використовують різноманітні аналізатори мережних пакетів, кожен з яких має свої особливості та переваги.

В роботі проаналізовано засоби для аналізу трафіку, які задовольняють різноманітні потреби – від детального аналізу пакетів до моніторингу мережевої інфраструктури. Сучасний ринок пропонує різні засоби аналізу мережного трафіку: графічні інтерфейси та консольні аналізатори. Популярні рішення включають Wireshark[1], Tcpdump[2], Nmap[5], Kismet[3], NetworkMiner та SolarWinds Network Performance Monitor[4], кожен з яких має специфічне призначення.

Основні властивості інструментів для аналізу пакетів, а також критерії вибору залежно від конкретних потреб, від детального технічного аналізу до інтуїтивно зрозумілих рішень для масового користувача, наведені в табл. 1.

Таблиця 1 – Порівняння інструментів для виявлення шкідливих пакетів

Інструмент	**Тип інтерфейсу**	**Основне призначення**	**Особливості**	**Цільова аудиторія**
Wireshark	Графічний	Детальний аналіз пакетів	Розширений розбір протоколів, фільтри	Інженери, аналітики,

Інструмент	Тип інтерфейсу	Основне призначення	Особливості	Цільова аудиторія
				дослідники
Tcpdump	Командний	Легке захоплення пакетів	Швидкість, скриптування	Адміністратори серверів
Nmap	Командний/GUI	Сканування мереж, виявлення вразливостей	Детекція хостів, портів, ОС	Фахівці з кібербезпеки
Kismet	Командний/GUI	Аналіз бездротових мереж	Виявлення прихованих SSID, IDS	Фахівці з Wi-Fi мереж
NetworkMiner	Графічний	Пасивний аналіз	Відновлення файлів, збір даних сесій	Фахівці з цифрової криміналістики
SolarWinds Network Performance Monitor	Графічний	Моніторинг продуктивності мережі	Детальна аналітика, звітність, оповіщення	Керівники мереж, IT-адміністратори

Під час війни ми стикаємося з новими викликами не лише через наземні бойові дії, а й у кіберпросторі, де ворожі хакери активно атакують нашу країну. Тому виникає нагальна потреба у рішенні, яке дозволить аналізувати мережевий трафік на предмет потенційних загроз та здійснювати превентивне блокування шкідливих запитів. Існує потреба створення застосунку, який виступатиме у ролі інтелектуального аналітичного центру. Такий застосунок має бути зручним не лише для професійних розробників та спеціалістів з кібербезпеки, але й для звичайних користувачів, які можуть стати жертвами кібернападів. Ідеальний продукт має поєднувати в собі найкращі практики сучасних аналізаторів, забезпечуючи: детальну аналітику**;** систему превентивного блокування; розумне логування та сповіщення; зручність використання. Таким чином, новий застосунок має стати комплексним рішенням для забезпечення кібербезпеки, яке поєднає потужні аналітичні функції, превентивні заходи та зручний інтерфейс для користувачів усіх категорій.

Список використаних джерел:

1. Wireshark. URL: https://www.wireshark.org/ (дата звертання: 05.03.2025).
2. Tcpdump. URL: https://www.tcpdump.org/manpages/tcpdump.1.html (дата звертання: 05.03.2025).
3. Kismet. URL: https://www.kismetwireless.net (дата звертання: 05.03.2025).
4. SolarWinds Network Performance Monitor. URL:

https://www.solarwinds.com/network-performance-monitor (дата звертання: 05.03.2025).
5. NMAP. URL: https://nmap.org/docs.html (дата звертання: 05.03.2025).