УДК004.457+004.7

Мєшков В.І., аспірант спеціальності 122 Комп'ютерні науки
Науковий керівник: Корнієнко В.І., д.т.н., професор кафедри безпеки інформації та телекомунікацій
(Національний технічний університет «Дніпровська політехніка», Дніпро, Україна)

СУЧАСНІ СИСТЕМИ МОНІТОРИНГУ ТРАФІКУ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Розвиток мережевих технологій супроводжується появою нових типів атак на комп'ютерні мережі. Різноманітні методи вторгнень у комп'ютерні мережі підприємств та їх реалізація у вигляді направлених атак викликає необхідність удосконалення існуючих засобів захисту інформаціїу корпоративних мережах.

Для підвищення захищеності у комп'ютерній мережі мають бути встановлені та налаштовані різні засоби моніторингу роботи всіх елементів мережі, такі як: система збору інформації про події, помилки та збоїв в системі, системи моніторингу трафіку, системи перевірки доступності мережевих вузлів, системи розмежування доступу, системи балансування навантаження, системи виявлення атак та їх запобігання.

Засоби моніторингу повинні бути розроблені та впроваджені в комп'ютерної мережі на етапі проєктування та підтримуватись в актуальному стані під час експлуатації.

Моніторинг мережевого трафіку є важливою процедурою при адмініструванні комп'ютерної мережі. До сучасних систем моніторингу можна віднести:

1. Network Olympus (рис.1) – програмний додаток[1] працює як мережева служба і має веб-інтерфейс. Особливість роботи – має конструктор сценаріїв, за його допомогою можна розробити план-схему моніторингу будь-якої конфігурації, для того щоб була можливість виявляти проблемні місця, а також автоматизувати процес їх усунення. За допомогою сенсора, який надає інформацію про стан мережі – сценарій генерує різні повідомлення та дії, які спрямовані на вирішення поставлених завдань. Кожен елемент ланцюжка може бути налаштований у реальному часі і відразу застосованийна всіх пристроях мережі, за якими закріплений сценарій. Мережева активність буде записана у журнал подій і спеціальні звіти.

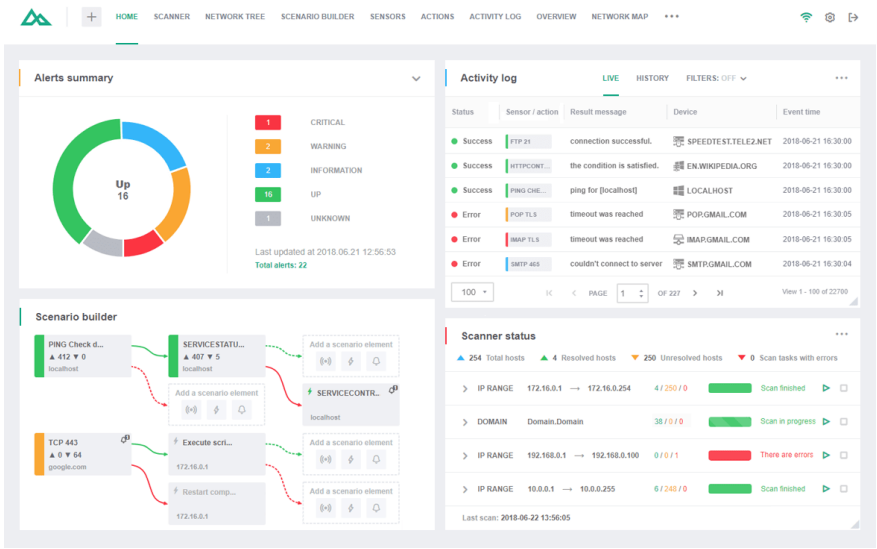

Рисунок 1 – NetworkOlympus

2. Observium (рис. 2) – робота програмного додатка [2] заснована на використанні протоколу SNMP, дозволяє дослідити стан мережі в режимі реального часу та виконати аналіз рівня її продуктивності. Observium може бути інтегрованим з обладнанням провідних розробників Windows, Linux, FreeBSD, Cisco, Dell, HP, Juniper, тощо. Маючи зручний графічний інтерфейс, ця програма надає системному адміністратору багато варіантів для налаштувань,наприклад, отримання данихза протоколом SNMP, необхідним для збору інформації про стан мережі. Також адміністратору надається можливість отримати доступ до технічних характеристик обладнання, яке підключено до комп'ютерної мережі. Звіти, які сформовані за допомогою аналізу журналу подій системи, програмний додаток може представляти у вигляді діаграм і графіків.

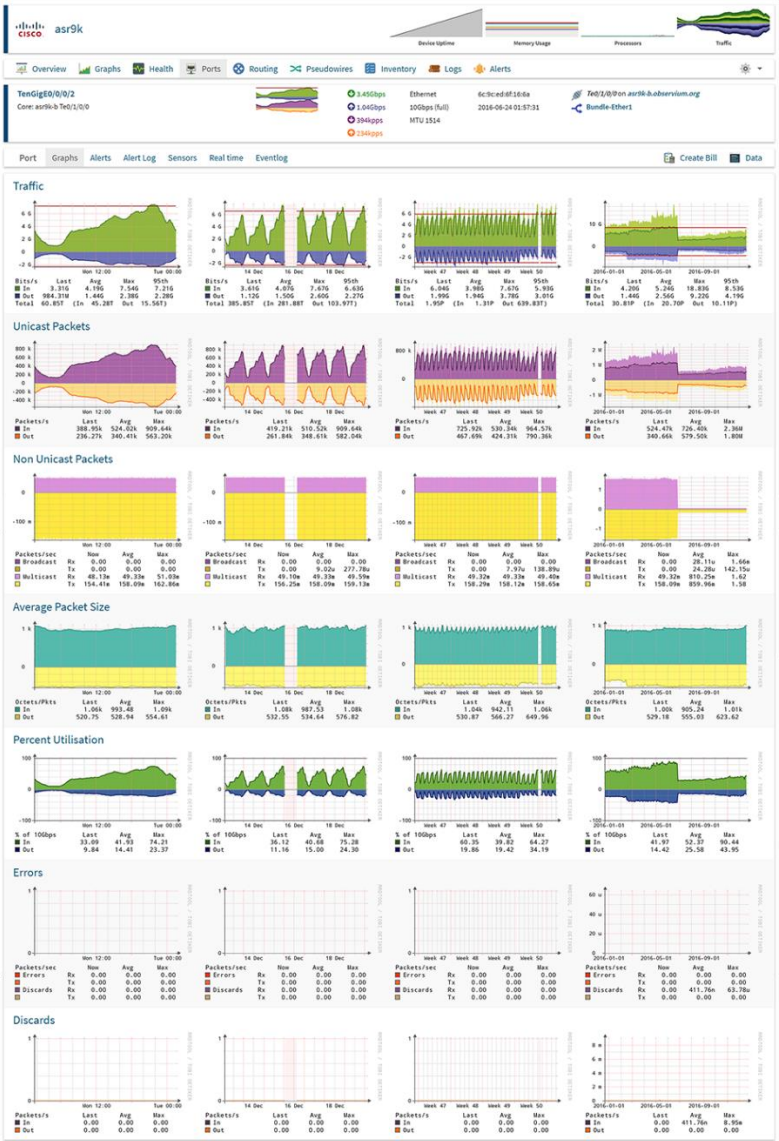

Рисунок 2 – Observium

3. Nagios (рис. 3) – цей програмний додаток [3] є рішенням для моніторингу комп'ютерної мережі, управління яким реалізоване за допомогою веб-інтерфейсу. Додаток має детальну документацію, що дає змогу швидко пройти навчання та опанувати функціонал. За допомогою Nagios системний адміністратор отримує можливість віддалено налаштовувати обсяги навантаження на користувацькета/або мережеве обладнання,а саме – мережеві комутатори, маршрутизатори, сервери, стежити за ступенем завантаженості пам'яті на серверах баз даних, стежити за фізичними показниками мережевого обладнання тощо. Щодо виявлення мережевих аномалій,

Nagios автоматично відправляє попереджувальні повідомлення на встановлену адміністратором адресу електронної пошти чи мобільний телефон.

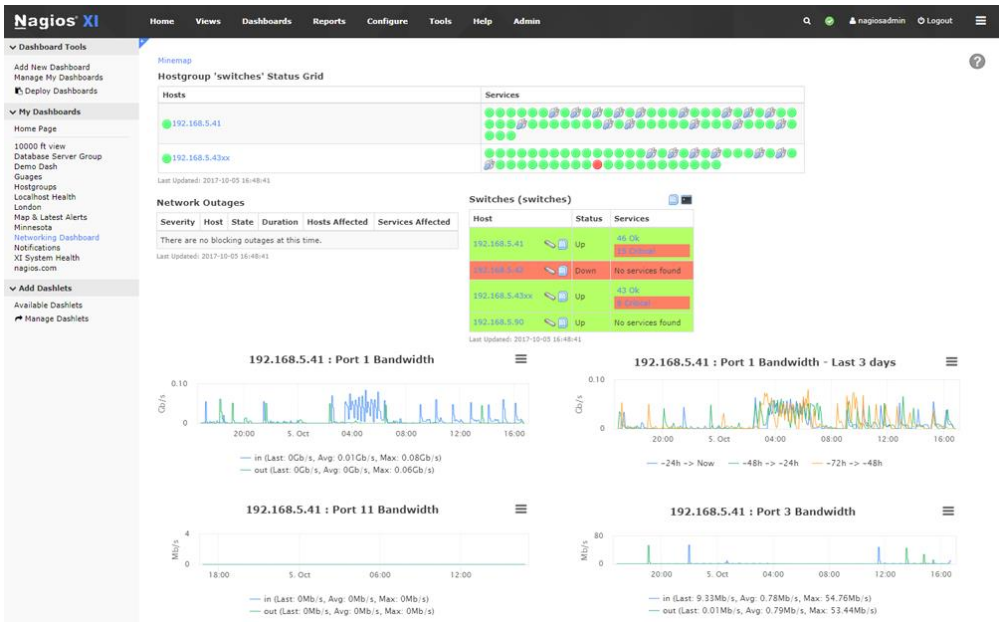

Рисунок 3 – Nagios

4. PRTG (рис. 4) – програмний додаток [4] сумісний з пристроями на базі ОС Windows та призначений для моніторингу мереж. Основні функції мережевих сервісів які реалізовані у PRTG – це інспекція пакетів, виконання аналізута збереження отриманих статистичних даних в базу даних, перегляд карти комп'ютерної мережі в режимі реального часу (також доступна функція отримання історії подій у мережі), збір технічних параметрів про пристрої, які підключені до мережі, а також виконання аналізу рівня навантаження на обладнання мережі.

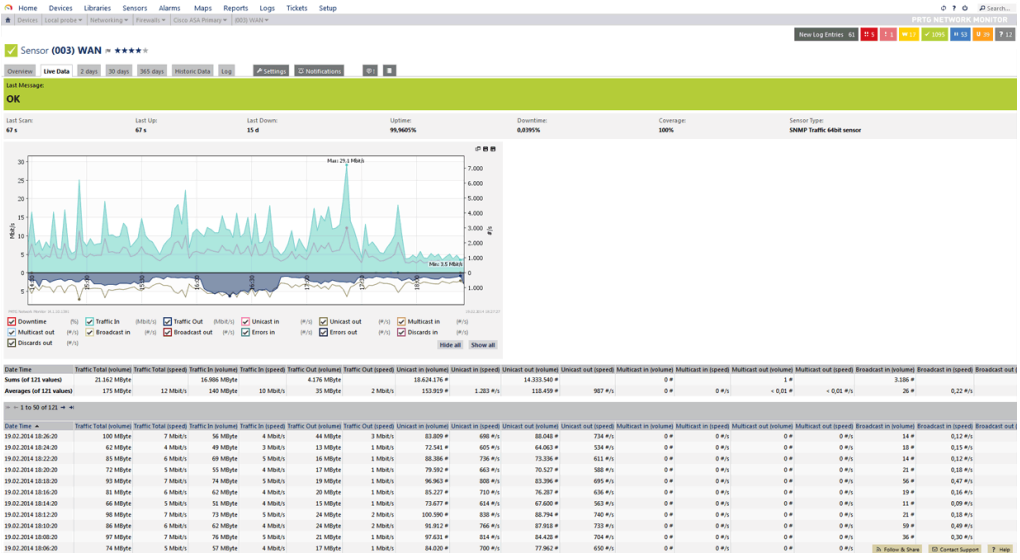

Рисунок 4 – PRTG

5. WireShark – програмний додаток – аналізатор трафіку [5] надає користувачам велику кількість функцій в області мережевої діагностики. Він підтримує роботу з системами на базі UNIX/Windows/macOS. Розгорнувши і налаштувавши його на сервері підприємства, можна отримати централізований елемент для моніторингу мережевого трафіку та визначати найдрібніші зміни в роботі комп'ютерної мережі при аналізі

мережевих протоколах. При використанні WireShark, системний адміністратор отримує інструмент, який дає змогу,на ранніх етапах виявляти і ідентифікувати проблеми, що виникли в комп'ютерній мережі підприємства.

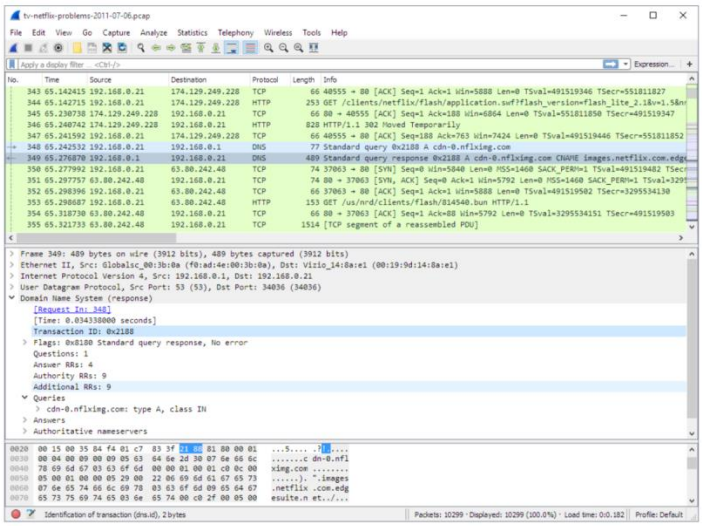

Рисунок 5 – WireShark

До переваг зазначених систем моніторингу мережевого трафіку комп'ютерної мережі можна віднести: можливість використання групових сенсорів (Network Olympus, Observium, Nagios, PRTG), конструктор сценаріїв (Network Olympus, PRTG), отримання графічних звітів про стан мережі (Network Olympus, Observium, Nagios, PRTG), інтеграція з операційними системами Windows/Unix/MacOS (NetworkOlympus, Observium, Nagios, PRTG, Wireshark).

Список використаних джерел:

1. Techpaper. Network Olympus Documentation // URL: https://docs.network-olympus.com/techpaper (дата звернення: 05.02.2023).

2. Observium. // Documentation / URL:https://docs.observium.org/(дата звернення: 05.02.2023).

3. NagiosDocumentation// Official manuals, documentation, video tutorials, and FAQs for Nagios solutions / URL:https://www.nagios.org/documentation/(дата звернення: 05.02.2023).

4. PRTGSupport // Get started with PRTG / URL:https://www.paessler.com/support/getting-started(дата звернення: 05.02.2023).

5. WiresharkDocumentation // URL: https://www.wireshark.org/docs/(дата звернення: 05.02.2023).

УДК 004.89: 004.3

Павлова О.О., д.ф., старший викладач кафедри комп'ютерної інженерії та інформаційних систем
(*Хмельницький національний університет, м. Хмельницький, Україна*)

МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ КІБЕРФІЗИЧНОЇ СИСТЕМИ РОЗУМНОГО ПАРКУВАННЯ

На сучасному етапі розвитку галузі інформаційних технологій питанням безпеки необхідно приділяти значну увагу. Особливо це є важливим під час розробки критичного