УДК 004.78

СКАНУВАННЯ ТА АНАЛІЗ ПРИСТРОЇВ ЛОКАЛЬНОЇ МЕРЕЖІ

Балабуха І.О.
email: ihor.balabukha@nure.ua
Науковий керівник – к.т.н., ас. Кобилін І. О.
Харківський національний університет радіоелектроніки, каф. ІНФ,
м. Харків, Україна

This study presents a methodology for scanning and analyzing local network devices using ARP requests and Nmap. The approach enables accurate identification of active devices, including MAC addresses, operating systems, and open ports. The use of Scapy and Nmap ensures efficient data collection and network visualization. Device classification based on MAC addresses helps determine hardware manufacturers and device types. The proposed method enhances network security, simplifies monitoring, and improves administrative efficiency. It is applicable for corporate network analysis, threat detection, and unauthorized access prevention.

У сучасному цифровому світі питання аналізу та моніторингу локальних мереж набуває особливої актуальності. Захист та ефективне управління мережею вимагають застосування інструментів, здатних виявляти та ідентифікувати активні пристрої, оцінювати їхню доступність та потенційні загрози. Дослідження спрямоване на розробку методики сканування та аналізу мережевих вузлів, що базується на використанні ARP-запитів та сканування Nmap. Даний підхід забезпечує отримання детальної інформації про пристрої у локальній мережі, включаючи MAC-адреси, операційні системи та відкриті порти.

Аналіз мережевих середовищ є одним із ключових завдань адміністрування інформаційної інфраструктури. Виявлення активних пристроїв та їх ідентифікація дають можливість оперативно реагувати на підозрілі підключення, оцінювати ризики та покращувати загальну безпеку мережі. У межах дослідження представлено алгоритм сканування мережевих вузлів із застосуванням бібліотек Scapy та Nmap, що дозволяють точно та швидко отримувати дані про мережеві компоненти.

Методика аналізу передбачає використання ARP-запитів, які є ефективним механізмом для швидкого виявлення пристроїв у межах локальної мережі. Подальший детальний аналіз здійснюється за допомогою Nmap, що дозволяє визначити відкриті порти, активні сервіси та тип операційної системи пристрою. Для отримання розширеної інформації реалізовано агресивний режим сканування, який забезпечує глибший рівень перевірки мережевих вузлів.

Класифікація знайдених пристроїв виконується на основі отриманих MAC-адрес, що дає змогу визначити виробника обладнання та тип при-

строю (сервер, персональний комп’ютер, маршрутизатор, мобільний пристрій тощо). Отримані результати подаються у вигляді графічної візуалізації, яка включає мережеву топологію та спеціальний індикатор статусу сканування, що відображає поточний етап аналізу мережі.

Таблиця 1 – Виявлені пристрої у локальній мережі

IP	MAC	OS	Виробник	Тип
192.168.1.1	00:1A:2B:3C:4D:5E	Linux	TP-Link	Router
192.168.1.2	00:1A:2B:3C:4D:5F	Windows	Dell	Computer
192.168.1.3	00:1A:2B:3C:4D:60	macOS	Apple	Computer

На рис. 1 представлено графічну візуалізацію результатів сканування, що демонструє взаємозв’язки між пристроями в межах локальної мережі.

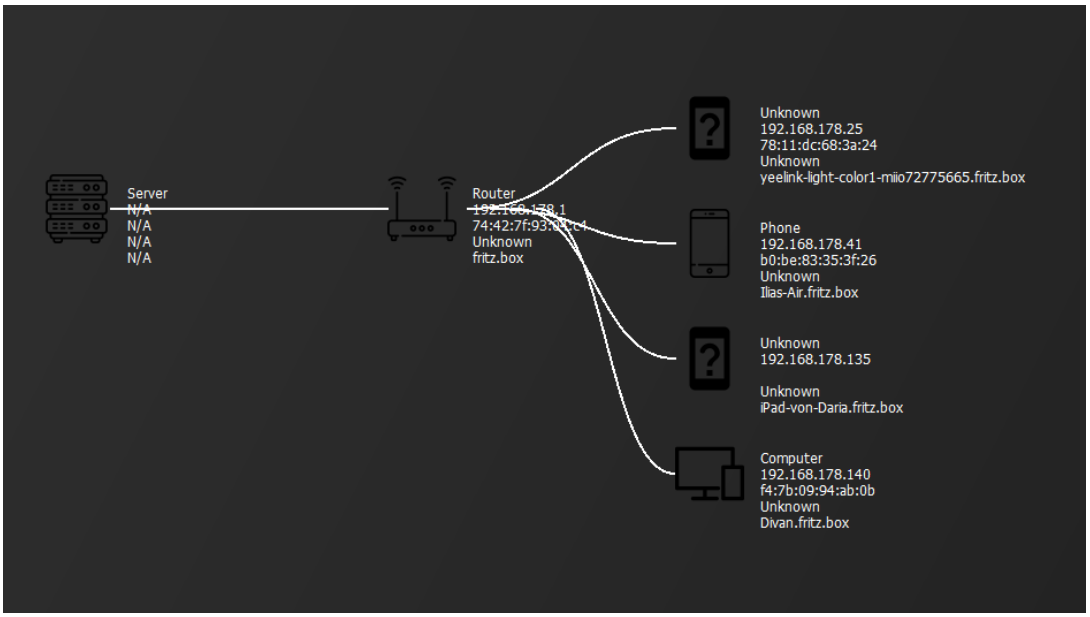

Рисунок 1 – Виявлені пристрої в локальній мережі (Візуалізація)

Запропонована методика дозволяє значно спростити та автоматизувати процес аналізу локальної мережі. Використання ARP-запитів у поєднанні з Nmap забезпечує високу точність визначення пристроїв та їх характеристик, що значно підвищує рівень мережевої безпеки та ефективність адміністрування. Крім того, застосування графічного представлення результатів робить процес аналізу більш наочним і зрозумілим.

Досліджений підхід має широкий спектр застосування, зокрема:

- Використання для моніторингу та аналізу локальних мереж підприємств та організацій.
- Виявлення та усунення потенційних загроз інформаційній безпеці.
- Підвищення ефективності управління мережею та зниження ризиків несанкціонованого доступу.