ПРОГРАМНІ ЗАСОБИ АНАЛІЗУ ЛОКАЛЬНИХ МЕРЕЖ ЩОДО УРАЗЛИВОСТЕЙ

асистент Булага В.А., студент Патлан Є.О.
Харківський національний університет радіоелектроніки,
комп'ютерної радіоінженерії та систем технічного захисту інформації,
м. Харків, Україна
e-mail: victoria.bulaga@nure.ua, yehor.patlan@nure.ua

Abstract. This work is devoted to the analysis of vulnerabilities of local networks through software tools. The goal is to investigate potential threats and identify weaknesses in network security. The researcher uses software tools to automate network scanning, identify vulnerabilities, and provide recommendations for improving security.

Ключові слова: локальна мережа, уразливості, аналіз.

Вступ. В сучасному інформаційному суспільстві локальні мережі (ЛМ) відіграють важливу роль у забезпеченні обміну даними, ресурсами та послугами між комп'ютерами та пристроями в межах певного фізичного простору [1-3], такого як офіс, школа, будинок, підприємство тощо [4, 5].

Загальне визначення локальних мереж та їх важливість:

- локальна мережа (ЛМ) - це комп'ютерна мережа, що об'єднує комп'ютери, сервери та інші пристрої в межах обмеженого фізичного простору, такого як офіс, школа або будинок;
- ЛМ відіграють важливу роль у сучасному світі, забезпечуючи ефективну комунікацію та обмін інформацією;
- уразливості в ЛМ можуть призвести до витоку конфіденційної інформації, несанкціонованого доступу до системи, атак зловмисників та інших негативних наслідків;
- в рамках даної роботи ми розглянемо програмні засоби, які призначені для аналізу уразливостей в локальних мережах.

Таким чином, метою даної роботи є дослідження програмних засобів аналізу локальних мереж щодо уразливостей та їх впливу на забезпечення безпеки ЛМ.

Основна частина. Локальна мережа зазвичай складається з набору комп'ютерів, які підключені до спільної мережевої інфраструктури, такої як комутатори або маршрутизатори. Комп'ютери в ЛМ можуть обмінюватись інформацією, виконувати спільні завдання, друкувати документи на спільному принтері та забезпечувати спільний доступ до ресурсів, таких як файли або бази даних. Один з основних принципів ЛМ - це локальність, тобто обмеженість фізичного простору.

Уразливість в контексті локальних мереж означає наявність слабкого місця або потенційної вразливості, яка може бути використана зловмисниками для несанкціонованого доступу, пошкодження або

викрадення даних, переривання послуг або інших зловмисницьких дій. Уразливості можуть виникати як через технічні недоліки в мережевому обладнанні та програмному забезпеченні, так і через людські помилки або необережне використання ресурсів.

Деякі загальні типи уразливостей, що можуть виявитися в локальних мережах, включають:

- недостатня аутентифікація та авторизація;
- незахищені мережеві протоколи;
- недостатня фізична безпека;
- недостатня оновлення та патчі;
- соціальна інженерія (люди можуть стати слабким ланцюжком у безпеці мережі, коли їхні дії або недії допомагають зловмисникам отримати несанкціонований доступ).

Наведемо огляд деяких таких програмних засобів.

1. Nessus: Nessus є одним з найпопулярніших програмних засобів для аналізу уразливостей.
2. OpenVAS: OpenVAS (Open Vulnerability Assessment System) - це відкрите програмне забезпечення для аналізу уразливостей в мережах.
3. Nmap: Nmap (Network Mapper) - це інструмент для сканування мереж і виявлення живих хостів, відкритих портів та розпізнавання операційних систем.
4. Wireshark: Wireshark - це популярний аналізатор мережевих пакетів, який дозволяє перехоплювати, аналізувати та відстежувати мережевий трафік.
5. Metasploit: Metasploit - це потужний фреймворк для тестування на проникнення, який включає в себе велику кількість експлойтів, модулів та інструментів для використання в різних типах атак.
6. Nikto: Nikto - це веб-сканер з відкритим вихідним кодом, спеціально розроблений для виявлення потенційних уразливостей на веб-серверах.
7. Aircrack-ng: Aircrack-ng - це набір інструментів для аналізу бездротових мереж, зокрема Wi-Fi.
8. Burp Suite: Burp Suite - це інтегроване середовище тестування вразливостей додатків, спеціально розроблене для виявлення уразливостей в веб-додатках.
9. Acunetix: Acunetix - це інструмент для автоматичного сканування веб-додатків з метою виявлення потенційних уразливостей.

Ці програмні засоби представляють лише частину широкого спектру інструментів, доступних для аналізу уразливостей в локальних мережах.

Висновки. У даній роботі було розглянуто тему "Програмні засоби аналізу локальних мереж щодо уразливостей. У процесі дослідження було встановлено, що локальна мережа є важливою складовою сучасної інформаційної інфраструктури. Вона забезпечує зв'язок між комп'ютерами та пристроями, що дозволяє обмінюватися даними та використовувати

спільні ресурси. Однак, разом з розвитком технологій, зростають і загрози безпеці локальних мереж. Уразливості локальних мереж можуть виникати з різних причин, включаючи помилки в конфігурації, недостатній рівень захисту, вразливість програмного забезпечення та недосконаліть протоколів мережі. Ці уразливості можуть призвести до несанкціонованого доступу, пошкодження даних та інших шкідливих наслідків. Застосування програмних засобів аналізу локальних мереж є важливим кроком у забезпеченні безпеки і захисту мережі.

Список використаних джерел.

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

2. N. Jovanovic. (березень 2006). TxtForum: script injection vulnerability. http://www.seclab.tuwien.ac.at/advisories/TUVSA-0603-004.txt

3. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

4. Сердюк С. Л. Цифрова система для митного контролю ручного багажу в аеропортах та зонах підвищеної небезпеки / С. Л. Сердюк, В. А. Булага // Радіоелектроніка та молодь в XXI столітті : матеріали 26-го Міжнародного молодіжного форуму, 24-25 листопада 2022 р. – Харків : ХНУРЕ, 2022. – Т. 3. – С. 132–133.

5. V. Bulaga. Digital System for Customs Inspection of Baggage in High Security Areas // III International Scientific and Practical Conference Theoretical and Applied Aspects of Device Development on Microcontrollers and FPGAs (MC&FPGA), Kharkiv, Ukraine, 2021, pp. 43-46. DOI: 10.35598/mcfpga.2021.015