АНАЛІЗ ПЕРСПЕКТИВНИХ МЕТОДІВ ПОШУКУ ВРАЗЛИВОСТЕЙ У КОРПОРАТИВНИХ МЕРЕЖАХ

Руженцев В.І., Поздняков Р.О.
Харківський національний університет радіоелектроніки, Харків, Україна

В роботі розглянуті основні методи пошуку вразливостей у корпоративних комунікаційних мережах.

Об'єктом дослідження є процес побудови та функціонування корпоративної мережі підприємства та пошук розповсюджених вразливостей, що протидіють нормальній роботі мережі.

Предмет дослідження – методи та засоби розпізнавання і пошуку розглянутих вразливостей.

Оцінка захищеності корпоративної інфраструктури потребує часу та високої кваліфікації фахівців з ІБ. Використовуються засоби аналізу захищеності - спеціальні системи, які в автоматизованому режимі виявляють відкриті мережеві порти та доступні служби, уразливості в програмному забезпеченні, а також недоліки конфігурації обладнання, серверів та засобів захисту. Сучасні засоби аналізу захищеності дозволяють проводити сканування інформаційних систем у різних режимах залежно від конкретного завдання — мережне сканування, системні перевірки, контроль за відповідністю стандартам безпеки [1].

Методи відкритого пошуку і керування вразливостей у мережі дозволяють здійснити безперервний, про активний та автоматизований процес, який забезпечує захист комп'ютерних систем, мереж та корпоративних програм від кібератак і порушень безпеки даних [2]. Для керування загрозами та вразливостями, використовується низка інструментів і рішень для запобігання кіберзагрозам та їх усунення або превентивних дій для їх адміністрування.

В результаті проведеного аналізу, та вивченню основних типів загроз було виявлено основні критерії методів пошуку вразливостей, до яких входять: виявлення й інвентаризація ресурсів, сканування вразливостей, керування виправленнями, керування конфігурацією, керування інцидентами та подіями безпеки, тестові атаки та аналіз існуючих кіберзагроз. Сумісні з даними критеріями методології охоплюють найбільших спектр захищеності корпоративної мережі, виявлення відповідних вразливостей і превентивне реагування відповідні інциденти ІБ.

Список літератури

1. А. В. Жилін, О. М. Шаповал, О. А. Успенський "Технології захисту інформації в інформаційно-телекомунікаційних системах" – Київ – 2020 – С.38

2. N. Olifer, V. Olifer "Computer Networks: Principles, Technologies and Protocols for Network Design – Wiley, 2006. – С. 933-940.