УДК 004.75

АНАЛІЗ ІСНУЮЧИХ ЗАСОБІВ ПОШУКУ ВРАЗЛИВОСТЕЙ

Цаволик Т.Г.[1)], Ващук В.С.[2)]
Тернопільський національний економічний університет
[1)] к.т.н. викладач, [2)]магістрант

I. Постановка проблеми

На сьогоднішній день компанії не приділяють питанню безпеки інформації в мережі належної уваги, часто починаючи вживати заходи тільки після витоку або ж втраті інформації.

Щоб забезпечити або ж усунути наявні проблеми, пов'язаніз захистом інформації, у даній темі буде розглянуто рішення для діагностики та моніторингу комп'ютерної мережі, так звані сканери – програмні або апаратні засоби, які сканують систему на предмет виявлення можливих проблем в безпеці, що дозволяють виявляти, оцінювати і усувати вразливості в мережі.

До основних завдань сканерів відносяться [1]: ідентифікація та аналіз загроз, інвентаризація ресурсів (програмне забезпечення, мережеві пристрої, операційна система), формування звітів з описом вразливостей та варіанти вирішення вразливостей системи.

Існує два основних механізми роботи сканерів вразливостей [1]: сканування –пасивний аналіз, що представляє собою збір інформації про порти, операційні системи, версії програмного забезпечення, отримані дані порівнюються з правилами визначення інформації про порти, програмне забезпечення та ін. компоненти системи та формується висновок про наявність або відсутність вразливостей; зондування – активний аналіз, що представляє собою імітацію атаки на систему, яка перевіряється. Тому важливою задачею при тестуванні системи на проникнення є аналіз засобів пошуку вразливостей. Отже задача щодо аналізу засобів пошуку вразливостей є актуальною та потребує додаткового дослідження.

II. Мета роботи

Метою роботи є аналіз існуючих засобів пошуку вразливостей при тестуванні на проникнення систем.

III. Аналіз існуючих засобів пошуку вразливостей

Для різних етапів перевірки системи на наявність вразливостей існують різні засоби пошуку, починаючи від сканерів портів до комплексних систем, які складаються з сканерів портів, засобів пошуку експлойтів для вразливостей.

Прикладами засобів пошуку вразливостей можуть бути: Metasploit Framework – інструмент для перевірки та експлуатації вразливостей [2]; програма для дослідження мережі Nmap – дозволяє визначити хости мережі, встановлені служби та їх версії а також яку операційні системи вони використовують [3]

Засоби пошуку та експлуатації вразливостей можуть бути зібрані в спеціальних операційних системах (ОС), призначених для аналізу захищеності та проведення тестувань комп'ютерних систем на проникнення. Існують такі операційні системи для проведення тестування тестування комп'ютерних систем на проникнення:ОС BlackArchLinux; ОС ParrotSecurity OS; ОС BlackBox; ОС KaliLinux [4-8].

Висновок

У роботі приведено аналіз існуючих засобів пошуку вразливостей систем. Таким чином, існують два варіанта пошуку вразливостей – використовувати сканери або ж використовувати засоби, які входять до спеціальних ОС, таких як KaliLinux, та ін.

Список використаних джерел

1. А.В.Лукацький - «Як працює сканер безпеки» [Електронний ресурс]. – Режим доступу: http://citforum.ck.ua/internet/securities/scaner.shtml
2. Довідкове керівництво сканера nmap [Електронний ресурс]. – Режим доступу: https://nmap.org/man/ru/index.html
3. Getting started with Burp Suite [Електронний ресурс]. – Режим доступу: https://portswigger.net/burp/help/suite_gettingstarted
4. Metasploit Basics [Електронний ресурс]. – Режим доступу: https://metasploit.help.rapid7.com/docs/metasploit-basics
5. Офіційний сайт виробника Kali Linux [Електронний ресурс]. Режим доступу –https://www.kali.org
6. Офіційний сайт виробника BlackArch [Електронний ресурс].Режим доступу –https://blackarch.org/index.html
7. Офіційний сайт виробника Parrot Security [Електронний ресурс].Режим доступу – https://www.parrotsec.org
8. Офіційний сайт виробника BlackBox [Електронний ресурс].Режим доступу – https://www.blackbox.com/en-us