УДК 004.056:355.451

МЕТОДИКА ПРОВЕДЕННЯ АУДИТУ НА СЕРВЕРАХ ЗА ДОПОМОГОЮ ПАКЕТУ KALI LINUX

Гонтарь І. А.
Науковий керівник – к.т.н. доцент Снігуров А. В.
Харківський національний університет радіоелектроніки, каф. Інфокомунікаційної інженерії імені В.В. Поповського, м. Харків, Україна
тел. +38(067) 546-86-35

There are a huge number of programs and operating systems that act as servers for receiving, processing and storing information. Every such system is a potential target for attackers. One of the main problems is the untimely update of the program, operating systems, etc. Such inactivity can cause: gaining access to the system, data theft, infection of the system, etc. This article examines ways to gain control over a server through untimely server updates using Apache as an example.

Виправлення сервера або виправлення сервера оновлює програмне забезпечення сервера для виправлення помилок, оновлення версій або покращення функцій та продуктивності. Виправлення помилок також передбачає усунення вразливостей системи безпеки та усунення помилок, які можуть становити загрозу для даних та інформації компанії.

Таким чином, ми можемо сказати, що є п'ять основних причин для оновлення сервера [1]:

−щоб усунути конкретну помилку чи недолік у коді обробки ядра;

−щоб підвищити стабільність, функції та функції серверної операційної системи чи будь-якої її програми;

−розробники програмного забезпечення та операційних систем випускають виправлення та оновлення щоразу, коли виявляються вразливості; їх слід швидко встановити;

−для видалення розповсюдженого програмного забезпечення – непотрібного коду та програм – для оптимізації розміру та споживання ресурсів основних компонентів операційної системи;

−для удосконалення існуючих процесів виправлення – можливо, служби Windows Server Update Services (WSUS) не працюють чи не працюють належним чином; можливо, він взагалі не працює. Інструмент управління виправленнями третьої сторони може взяти на себе роботу або навіть перевершити такі рідні служби виправлення.

У цій статті як приклад буде розглядатися HTTP-сервер Apache. Apache — це безкоштовне міжплатформне програмне забезпечення веб-сервера з відкритим кодом, випущене згідно з умовами ліцензії Apache 2.0. Apache розробляється та підтримується відкритою спільнотою розробників під егідою Apache Software Foundation [2]. Переважна більшість екземплярів HTTP-сервера Apache працює на дистрибутиві Linux, але поточні версії

також працюють на Microsoft Windows, OpenVMS та широкому спектрі Unix-подібних систем. Попередні версії також працювали на NetWare та інших операційних системах, включаючи порти до мейнфреймів.

Кожна версія програми або операційної системи має потенційно вразливість, яку зловмисник може скористатися. Оновлення систем є не тільки додаванням нових можливостей сервісу, але може в собі нести оновлення системи для перекриття потенційних проломів у безпеці. Хакери намагаються знайти можливі вразливості в безпеці в кожній версії програми для своєї вигоди. Такі дані, як знайдена вразливість або навіть її використання може бути викладена в мережу. Щоб розглянути це питання детальніше, нижче буде розглянуто способи ідентифікації версії операційної системи або програми, використовуючи операційну систему Kali Linux, як інструмент для тестування на проникнення:

−nmap -T4 -A -p- 192.182.131.105 – дана команда шукатиме порти, операційну систему або програму та їх версію в рамках IP адреси 192.182.131.105;

−nikto -h #domain – дана команда є безплатним аналізатором вразливості веб-ресурсів і також надає операційну систему або програму та їх версію в рамках #domain.

Після ідентифікації операційної системи та їх версії, як тестувальники на проникнення, потрібно перевірити чи існують якісь експреси для цієї версії системи. Для пошуку, існують величезна кількість ресурсів. Нижче є кілька найбільш популярних прикладів:

−exploit-db.com – сайт, який зберігає в собі величезну кількість експоїтів у відкритому доступі, які допомагають провести тестування на проникнення на різних ступенях зануреності;

−searchspoilts apache 1.3 – команда для Kali Linux, яка шукає можливі експлоїти для Apache сервера для версії 1.3.

На основі зібраної інформації, залежно від вже знайдених експлоїтів, хакер має можливість скористатися вразливістю сервера через несвоєчасне оновлення та отримати доступ до сервера, файлам конфігурації інших серверів, які знаходяться на даному сервері, отримання даних з інших сервісів, впроваджені зараженого програмного забезпечення. забезпечення та тд.

Список використаних джерел:

1. What is Patch Management and Why is it Important?. (2021, 1 вересня). https://jumpcloud.com/blog/what-is-patch-management.

2. Apache HTTP Server. (2010, вересень). https://en.wikipedia.org/wiki/Apache_HTTP_Server.