МЕТОДИКА ВІДДАЛЕНОГО ВИЗНАЧЕННЯ ВЕРСІЇ MYSQL СЕРВЕРА ЗА ДОПОМОГОЮ ПАКЕТА KALI LINUX

Гонтарь І. А., Снігуров А.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: ivan.hontar@nure.ua,
arkadii.snihurov@nure.ua

Abstract

A database is a storage for any information that should be stored and proceeded. A large number of services work directly with the database. It is deployed on the servers on which the database works, for example, on a Linux server. The information that is stored on the server is a potential target for attackers. In order to have access to the server, you need to pass the configuration of the server, and then get access to the database. The correct configuration of servers and services allow reducing the risks of any malicious actions, but even a small piece of information, i.e. a version of servers or services, can become a critical vulnerability, because each version of the operating system or software can contain critical vulnerabilities that can be closed only in new versions. Therefore, such information as the server or service version can be used for malicious actions.

MySQL — це реляційна система керування базами даних. Бази даних є основним сховищем даних для всіх програм. Наприклад, щоразу, коли хтось здійснює пошук в Інтернеті, входить до облікового запису або завершує транзакцію, то система бази даних зберігає інформацію, щоб до неї можна було отримати доступ у майбутньому.

Реляційна база даних зберігає дані в окремих таблицях, а не поміщає всі дані в одну велику комірку. Структура бази даних організована у фізичні файли, оптимізовані для швидкості [1].

Логічна модель даних із такими об'єктами, як таблиці даних, подання, рядки та стовпці, пропонує гнучке середовище програмування. Встановлюються правила, що регулюють відносини між різними полями даних, такі як один до одного, один до багатьох, унікальні, обов'язкові чи необов'язкові та «вказівники» між різними таблицями. База даних забезпечує дотримання цих правил, тож з такою добре розробленою базою даних, ваша програма ніколи не бачить дані, які є неузгодженими, дубльованими, загубленими, застарілими або відсутніми. Фреймворк Metasploit являється потужним інструментом, який використовується тестувальниками на проникнення для дослідження систематичних вразливостей на мережах і серверах: а також може використовуватися хакерами для зловмисних дій. Оскільки це фреймворк із відкритим кодом, він легко налаштований і використовується з більшістю операційних систем. Фреймворк складається з різних моделей та інтерфейсів, які включають msfconsole, msfcli до всіх функцій msf з terminal/cmd, графічний інструмент Java Armitag, який використовується для інтеграції з MSF, і веб-інтерфейс спільноти Metasploit, який підтримує віддалене тестування. Для знаходження версії MySQL серверу, потрібно просканувати мережу для знаходження відкритих портів 3306, який являється стандартним портом для MySQL сервера. Щоб виявити усі відкриті порти, потрібно використати програму nmap, яка являється потужним інструментом для тестування на вразливості. Результатом команди «nmap -p-192.168.31.0/24» будуть просканові IP-адреси в рамках з 192.168.31.0 до 192.168.31.255 та для кожної адреси 66532 портів, які будуть відкриті. На рисунку 1 виведено результат для IP-адреси 192.168.31.214, де існує відкритий 3306 порт з поміткою MySQL сервісом.

Розглянемо 2 варіанти визначення версії MySQL сервера після знаходження IP-адреси серверу, на якому воно розташовано:

- використовування утиліти nmap;
- використовування сканера mysql_version через Metasploit.

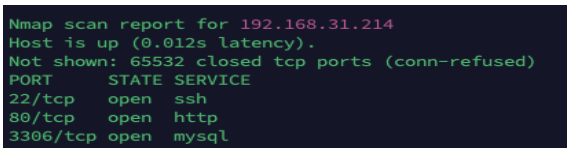

Рис. 1. Результат сканування відкритих портів

У першому варіанті пропонується використання утиліти nmap, яка містить в собі велику кількість інструментів. Один з них, це знаходження версії сервісів чи операційних систем через параметр «-sV». Для знаходження очікуваного результату, потрібно виконати наступну команду «nmap -sV -p 3306 192.168.31.0/24». Результатом першого експерименту являється знаходження версії MySQL серверу та версії операційної системи серверу. На рисунку 2 виведено результат для 192.168.31.214:3306, у якому MySQL сервер має 5.7.42 версію та Linux сервер з версією 18.04.1.

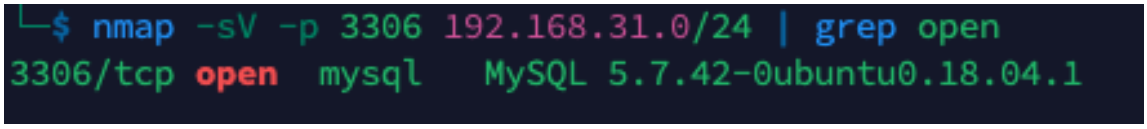

Рис. 2. Результат знаходження версії MySQL сервера через nmap

У другому варіанті, розглядається використовування утиліти Metasploit та модуля сканера. Нижче описанні кроки для визначення версії MySQL сервера за допомогою вище описаних інструментів:

- msfconsole – для запуску Metasploit;
- use scanner/mysql/mysql_version – вибір сканеру для визначення версії MySQL сервера;
- set rhost 192.168.31.214 – встановлення IP-адреси цілі;
- run – запуск сканера.

Результатом другого експерименту являється знаходження версії MySQL сервера та версії операційної системи серверу за допомогою Metasploit та mysql_version сканера. На рисунку 3 виведено результат у віддаленому сервері 192.168.31.214, у якому MySQL сервер має 5.7.42 версію та Linux сервер з версією 18.04.1.

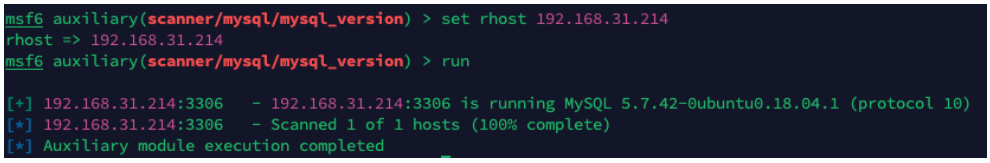

Рис. 3. Результат знаходження версії MySQL сервера через допомогою Metasploit та mysql_version сканер

Визначення точної версії MySQL сервера може викликати цілий ряд проблем: тому що кожна версія має свої вразливості: які потенційно можуть бути закриті у наступній версії.

Один з основних методів протидії визначенню версії сервера – це менеджмент білого листу IP-адрес. Нижче приведені приклади, які допоможуть правильно настроїти MySQL сервер:

- створення користувача для баз даних, доступ до якої можна буде отримати с однієї специфічної IP-адреси, приклад команди«CREATE USER 'testuser'@'remote_ip_address' IDENTIFIED BY 'password';», де «remote_ip_address» це IP-адреса віддаленого користувача;
- додавання IP-адреси віддаленого користувача для білого листу на Linux сервері та підключення тільки по порту бази даних, через наступну команду «ufw allow from remote_ip_address to any port 3306», де «remote_ip_address», це IP-адреса віддаленого користувача.

В даній статті розглядаються методики знаходження версії MySQL сервера через nmap та Metasploit та mysql_version сканер за допомогою пакету Kali Linux. Також розглядаються деякі можливості захисту та правильного менеджменту доступів до серверу чи бази даних.

Література

1. B. R. What Is MySQL and How Does It Work [Електронний ресурс] / Richard B. – 2023. – Режим доступу до ресурсу: https://www.hostinger.com/tutorials/what-is-mysql.