Academic Year: 2022-23 **Semester: V**
Class / Branch: TE IT
Subject: Security Lab (SL)
Subject Lab Incharge: Prof. Apeksha Mohite

EXPERIMENT NO. 8

Aim: To demonstrate Computer Security System Honeypots and Web Vulnerability

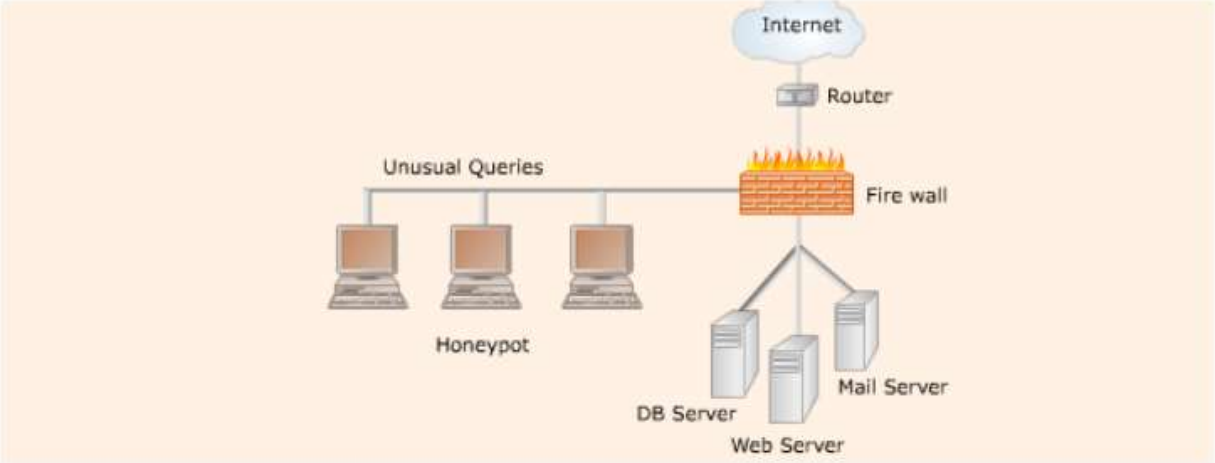
SQL Injection.Theory:

SQL Injection is a code injection technique where an attacker executes malicious SQL queries that control a web application's database. With the right set of queries, a user can gain access to information stored in databases. SQLMAP tests whether a 'GET' parameter is vulnerable to SQL Injection.

SQL injection is a hacking technique where an attacker can insert SQL commands through a URL tobe executed by the database. This bug or vulnerability occurs because all programmers or webmasters do web programming such as the filtering of variables in the web. A database is a collection of information stored on a computer or web server systematically that is useful for obtaining information from the database.

SQLMap is an open source penetration test tool that automates the process of detecting and exploiting weaknesses in SQL injection and taking over the server database. So sqlmap is a tool thatcan automatically detect and exploit SQL injection bugs. by doing a SQL injection attack an attacker can take over and manipulate a database on a server.

HoneyPots:



Honeypots are information system resource intended to be compromised. For this reason, they are kept outside the firewall of a normal network. When the firewall identifies an unusual pattern, it forwards the requests to the honeypot instead of dropping it.

Within the honeypot the cracker is free to perform all mischief. The job of the administrator is to analyze the log reports generated by the honeypot tools and then trace back to the attacker.