**LOVELY PROFESSIONAL UNIVERSITY**

**Academic Task-3 (Compulsory)**

**INT301: Open Source Technologies**

**Name: Gaurav Mukherjee**

**Reg\_no:11713082 (Roll\_no:36)**

**Question: 9. 🡪Generate Payload for three different platforms, and exploit windows machine using Metasploit framework/ any open-source software.**

**Introduction**

Metasploit Framework is an open-source penetration testing framework developed by Rapid7. It provides a collection of tools and exploits for security professionals to perform penetration testing and vulnerability assessments on networks, systems, and applications.

The framework includes a wide range of exploits, payloads, encoders, and auxiliary modules that allow security researchers to identify and exploit vulnerabilities in various systems and applications. It supports multiple platforms, including Windows, Linux, and macOS, and provides a command-line interface and a graphical user interface for ease of use.

The Metasploit Framework is widely used by security professionals, penetration testers, and hackers alike for ethical hacking, vulnerability assessment, and penetration testing. Its popularity stems from its flexibility, ease of use, and the fact that it is constantly updated with the latest exploits and vulnerabilities, making it an invaluable tool in the arsenal of any security professional.

Metasploit Framework is a popular open-source penetration testing tool used for exploiting vulnerabilities in computer systems and networks. It provides a wide range of tools and resources for penetration testers, security researchers, and ethical hackers to test and evaluate the security of systems and applications.

The Metasploit Framework allows users to scan and identify vulnerabilities in target systems, then exploit them to gain access to the system or network. It includes a large database of exploits, payloads, and modules that can be used to create customized attacks. The tool also includes features for post-exploitation activities such as data collection, pivoting, and privilege escalation.

Metasploit is designed to be flexible and extensible, allowing users to write their own modules and exploits, and integrate them with the existing framework. It also has a robust community of users and developers who contribute to the development of the tool, including updates to existing exploits and the creation of new ones.

While Metasploit can be used for both legal and illegal activities, it is primarily used by security professionals and ethical hackers to assess the security of computer systems and networks. It is important to use Metasploit only with the permission of the target system owner or network administrator and in compliance with applicable laws and regulations.

**Objective of the project**

**Description of the project**

**Scope of the project**

**System Description**

**Target system description**

**Assumptions and Dependencies (If applicable)**

**Functional/Non-Functional Dependencies (if any)**

**Data set used in support of your project (if any then paste the link)**

**Analysis Report**

**System snapshots and full analysis report**

**Reference/ Bibliography**