**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**

This project is comprised of using tools for identification , information gathering and exploitation of any system with exploitable loop holes .

To achieve this task the majority of the operation is performed using metaspoitable or commonly knows as msf-console. For obtaining and identification of the target tool such as Nmap is used. This tool performs searches in a network to identify the targets IP as well as the open and closed ports that are available in a target IP.

Also one can get operating system details as well as any available application names as well as version information which will help in identifying the correct payload which will help in target exploit.

For this project three different platform are to be selected and operations are to be performed on them. For simplifying the operation those target machines are either in the virtual state or as a local machine.

The operation of payload selection and exploit implementation are similar for all system. The differences will only come from the different exploit that are available in the target’s system.

**Description of the project**

The Objectives of this project are as follows :-

1. Find systems with different configurations and find there respective IP addresses
2. Use tools such as Nmap to identify the target information such as OS details , open ports and versions details for better selection of exploits .
3. See the information collected to figure out which of the following ports, application can be exploited by using Search function in MSF console followed by the name of the payload you see fit .
4. Locate the following payload from the given list of payloads and figure out which is the most applicable of them. Also check for the operation technique
5. Select the payload by using command “use” along with the name of the payload mentioned or the ID of the following payload
6. Now, use the command “show options” to see the following requirement and the selected default Lhost and Lport
7. If the preselected Jhost & Lport is not as your Target then select them by using “set Lhost <Ip>” and “set Lport <Ip>”
8. Now, you can use “Show Option” to verify the options once again
9. Use “show targets” for various options available sand select any one of them by using “use” along with options number
10. Now after all that use the keyword “Exploit” to start the exploit Sequence.

**Scope of the project**

This Project will go into this following things:

1. Searching for targets which are suitable for exploit.
2. Using tools such as Nmap for analyzing the target and getting there respective IP’s details.
3. Searching for vulnerabilities in those targets and finding exploitable options.
4. Verifying that those exploitable exploits are available as payloads in the console if using.
5. Search for the exploit or system description such as OS information or port related details in the

available database such as msfconsole db.

1. If found then use it or if not then search for any other compatible exploits that are suitable.
2. Now set the target details such as target’s IP , etc.. , and finally
3. Exploit . This will cause a direct root access link to the target machine for any further action.

**System Description**

There are two differently configured system being used :

1. Windows 11(beta-early\_access): This system has multiple libraries and packages installed for smooth and easy operation of tools and procedures. This include – nmap, Metasploit – framework , msfconsole in terminal , Zenmap, wireshark .
2. Kali-linux – This system does not have any additional components installed as this operating system comes preinstalled with all essential tools, hence no modification needed except nominal updation.

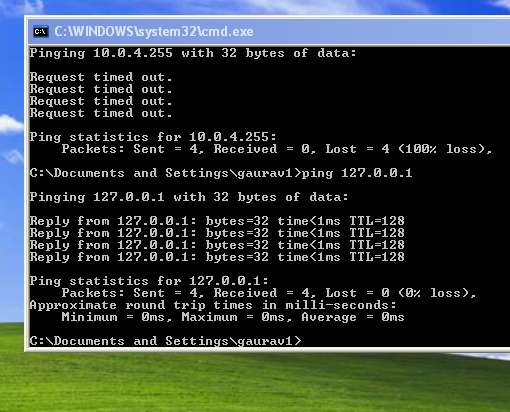
**Target system description**

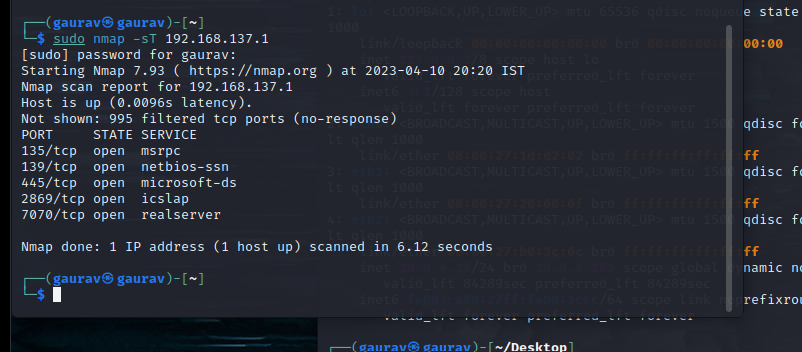
The target systems are as follows:

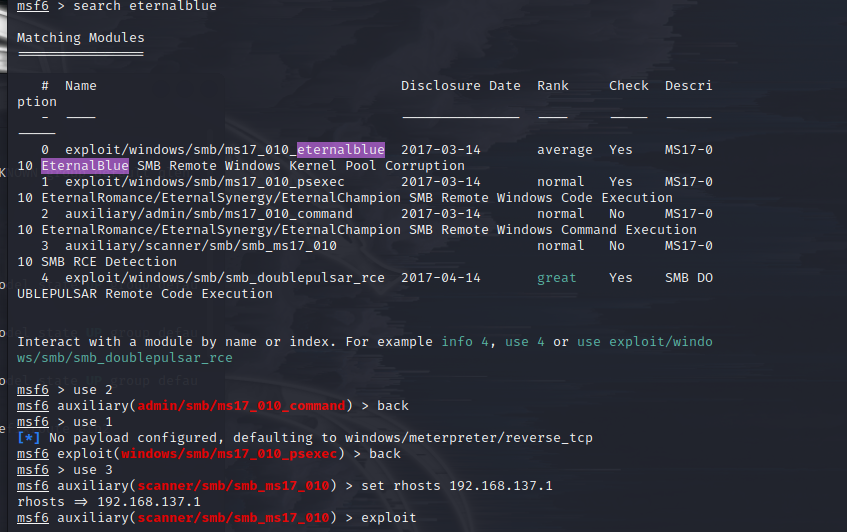
1. Windows XP – configured to run in local virtualized environment. Network adapter running in bridged configuration.
2. Metasploitable 2 - configured to run in local virtualized environment. Network adapter running in bridged configuration.
3. Linux Mint - configured to run in local virtualized environment. Network adapter running in bridged configuration.
4. Linux Lite - configured to run in local virtualized environment. Network adapter running in bridged configuration.

**System snapshots**

WindowsXP exploit

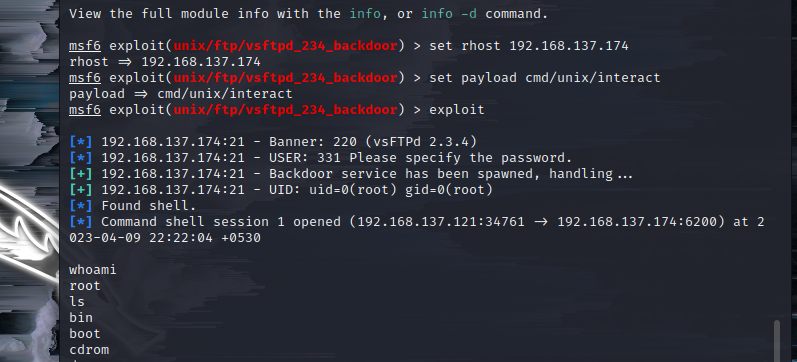


****

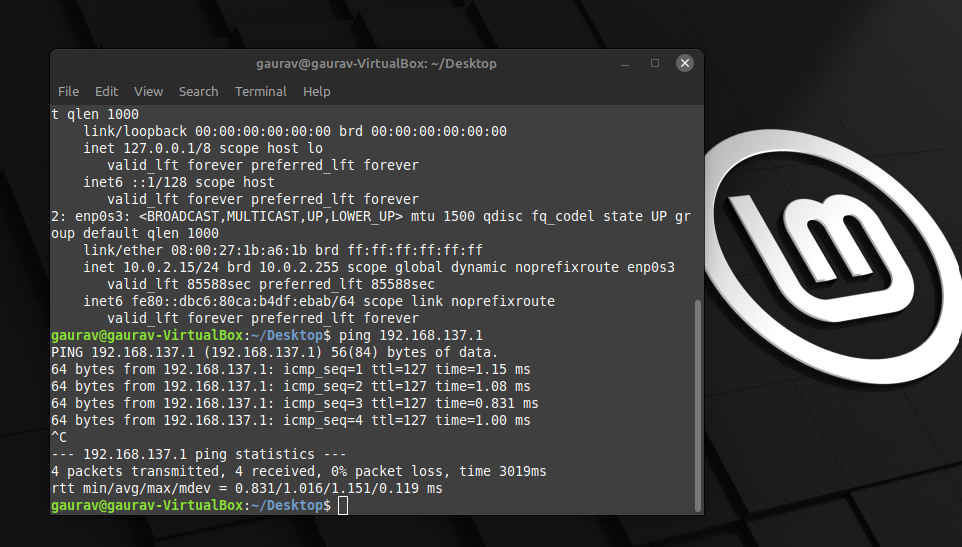
****

Metaspoitable 2





Linux-Mint



Text

Description automatically generated

Linux-Lite

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

**Reference/ Bibliography**

1. unix.stackexchange.com
2. docs.rapid7.com
3. [hackingarticles.in](http://www.hackingarticles.in)
4. [blackmoreops.com](http://www.blackmoreops.com)

**GITHUB LINK**

https://github.com/gauravmukherjee089/Gaurav\_CA3\_OpenSource.git