

**Assignment Submitted by ,**

**Name : MD Faruk Mahmud**

**Reg No : 11900277**

**Roll No : 36**

**Section : KE050**

**Subject: INT301**

**Assignment Submitted to**

**Navjot Kaur**

GitHub Link : <https://github.com/farukzzzz/open_source_project/tree/main>

Question Number : 9

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

**Machine I have used** : I have used Kali operating system for generating payloads and exploitation . Kali Linux basically is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

**About Payload** : A payload is a piece of code or software that is designed to perform a specific action on a target system, such as gaining unauthorized access, stealing data, or causing system damage. In the context of computer security, a payload is typically associated with malware or other malicious software that is used to compromise a system.

To generate a payload, we would typically use a tool or software that is specifically designed for that purpose, such as Metasploit or other open-source exploitation frameworks. These tools allow us to create customized payloads that can be used to exploit vulnerabilities in target systems.

Once a payload has been created, it can be delivered to a target system using various methods, such as email attachments, malicious links, or other social engineering techniques. Once the payload has been executed on the target system, it can then carry out its intended actions, such as providing a remote shell or executing arbitrary code.

It is important to note that the use of payloads and other exploitation tools should only be done for legitimate purposes and with proper authorization and consent. Engaging in unauthorized or illegal activities can have serious legal and ethical consequences.

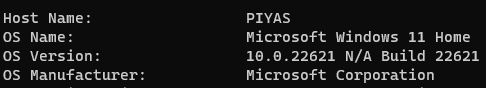
**Scope of the work** : In general, the scope of work for ethical hacking and penetration testing should be clearly defined and agreed upon between the client and the security professional. The scope should specify the objectives of the engagement, the systems and networks that are included, the testing methods and tools that will be used, the rules of engagement, and the expected deliverable.

The scope should also define the limitations of the engagement, such as the systems and networks that are out of scope, the types of attacks that are prohibited, and any legal or ethical constraints that need to be considered.

It is important to ensure that the scope of work is agreed upon in advance and that all parties understand and agree to the objectives, limitations, and expectations of the engagement. This can help to ensure that the engagement is conducted in a safe, legal, and ethical manner, and that the results are meaningful and actionable.

1. **Target System - Windows**

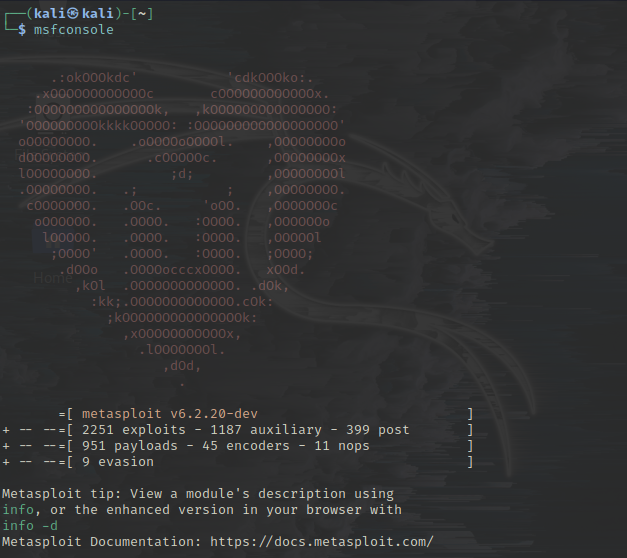
**System Description** : I have use windows 11 as target system and conduct the exploitation . System information are given below :



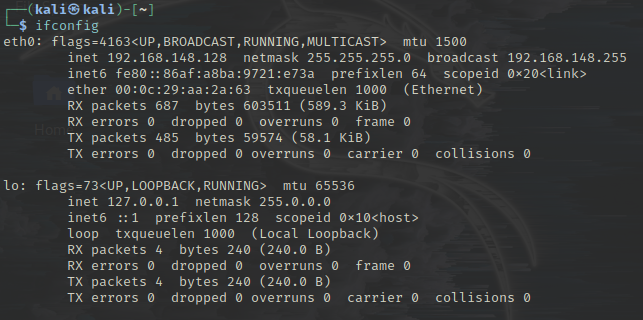
The exploitation based on two steps . First is to make a payload for the target machine and then configure msfconsele for conduct the exploitation .

**First step ( Creating Payload )**

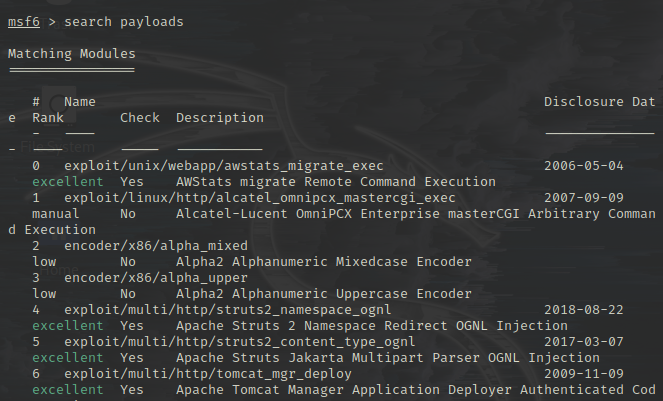
start the msfconsole :



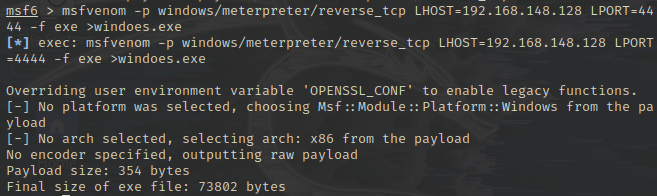
Check the attacker device ip address :



After I need to search a usable payload :



Make the payload into a windows supported exe file .



Here -p flag used to select the payload .

LHOST is for the local host or attacker ip address

LPORT - listening port . the port to listen on for a connection from the target computer.

-f = used for the file format .

Finally a payload created by the name of windows.exe

**Step 2 ( doing Exploitation )**

Enter into the exploit/multi/handler :

IMG_256

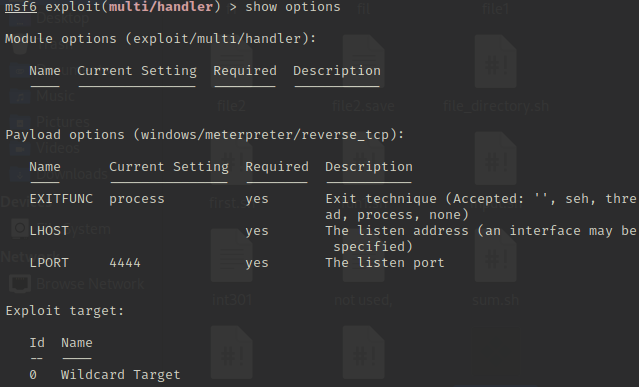
For configuring the attacker machine in ‘multi/handler’ I need to select the payload . And then need to configure the other setting :

IMG_256

Set the attacker LHOST(Listening Host ) :

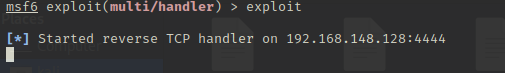
IMG_257

Using show options command I can check the configured options :

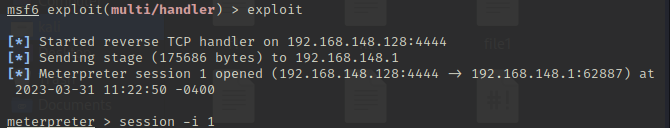


Then type exploit and press enter :

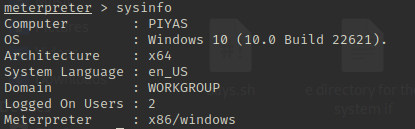
If somehow the windows.exe file clicked by the target machine , session will start immediately .



After clicked by the target machine :



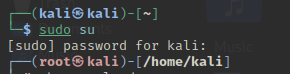
See the target machine information from attacker machine :



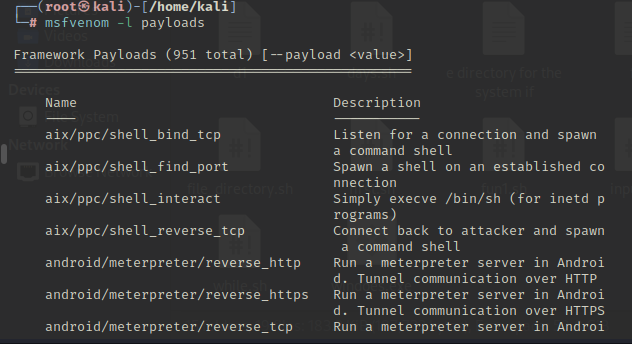
1. **Target System : Android**

First step (make payload ):

* Give the terminal permission to root :

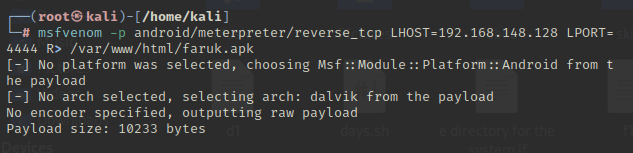


* Then show all the metasploit payloads using command :



It will show all the list of payloads .

* Among them select the suitable payloads related to android reverse tcp .



Set LHOST = (Attacker IP address - 192.168.148.128

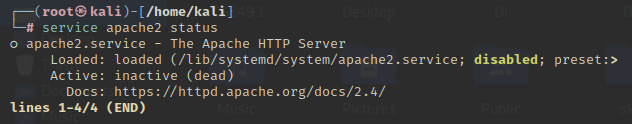
Set LPORT = Listening port . It could be any active port . I have taken 4444

I’m putting my apk file in the apache server . So I have given the server path of apk file path is (/var/www/html/)

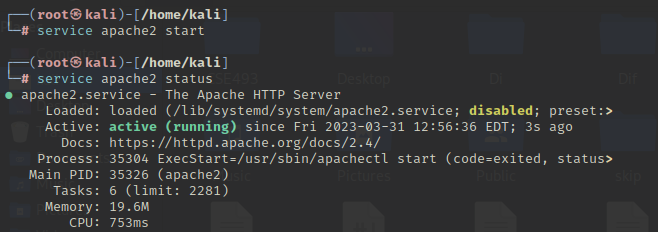
And I put the application name is faruk and the file extension is apk .

After pressing enter it will take some time and create a apk file to the web apache server .

* I need to activate the apache server . So I need to check the server status first . for checking the server status :



As it is showing the server status is inactive so I need to activate the server . By doing this anyone can access the apk file remotely . For activing the server I need to do :

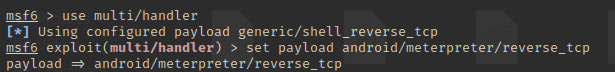


Second Step (Exploiting )

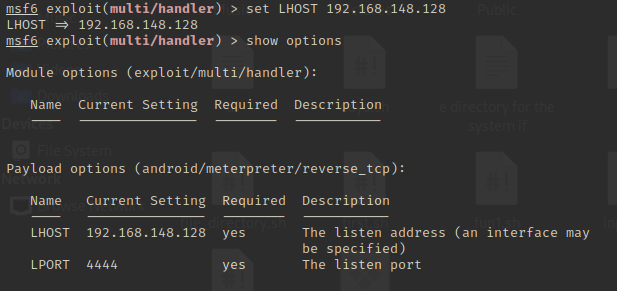
* First I need to enter into the console .



* Then I need to enter into he multi handler and select the payload .



* Then I need to check the options of the payloads and need to select the LHOST and LPORT for the attacker machine .



* After all these I need to type ‘exploit’ and then the session will generate and waiting for the exploitation . When someone will download or receive the apk file and install it session will start and attacker will get the full access of the target android machine .

