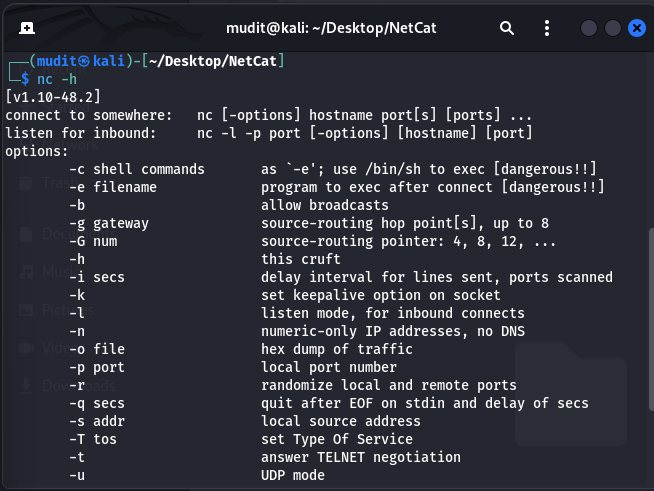
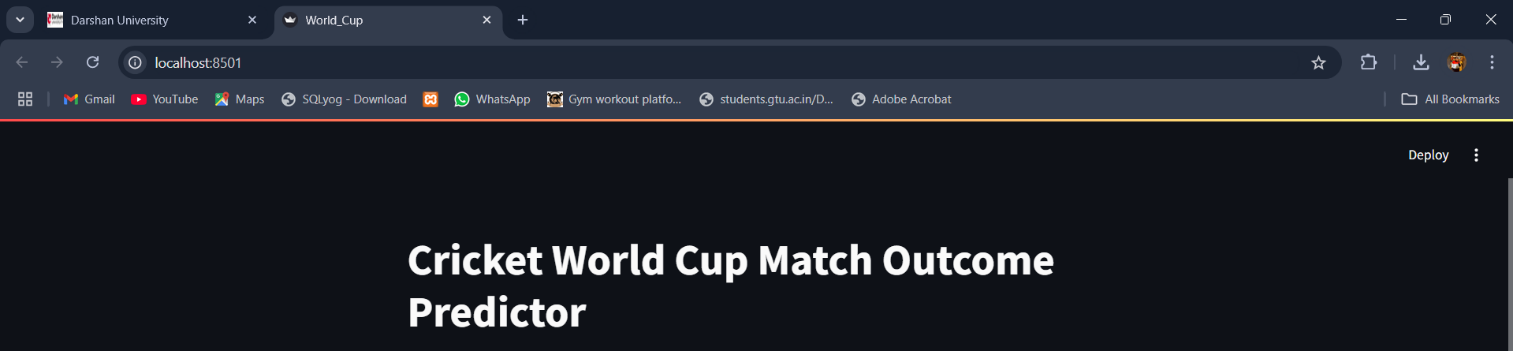
**Lab Practical 3:**

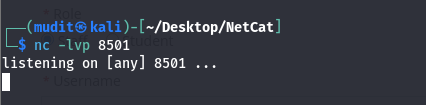
Perform Netcat and metasploit tool for scanning system vulnerability.

* NetCat:
* nc -h: It is used to get information about netcat command.

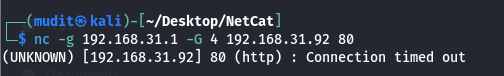


* nc -lvp <port>: it can be used for listen local port on web Browser.

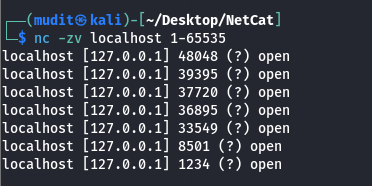
3 



* nc -g: It can be use to connect with port via gateway.



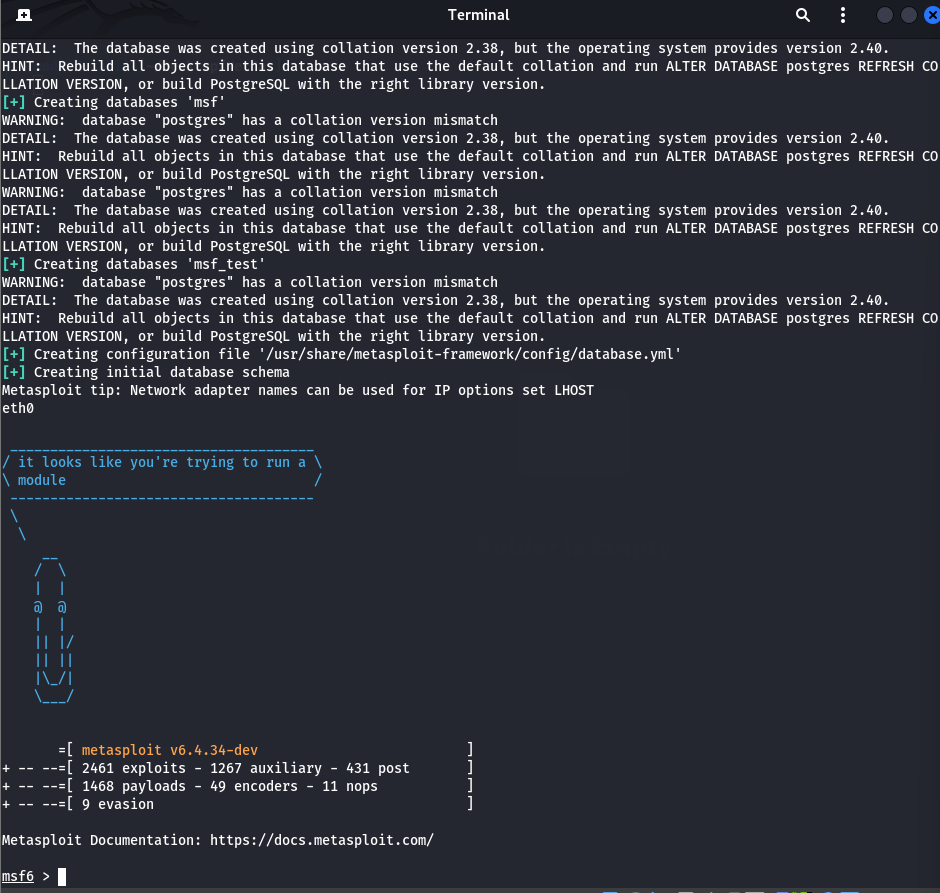
* nc -zv localhost 1-65535: This scans all ports (1-65535) and tells you which ones are open.



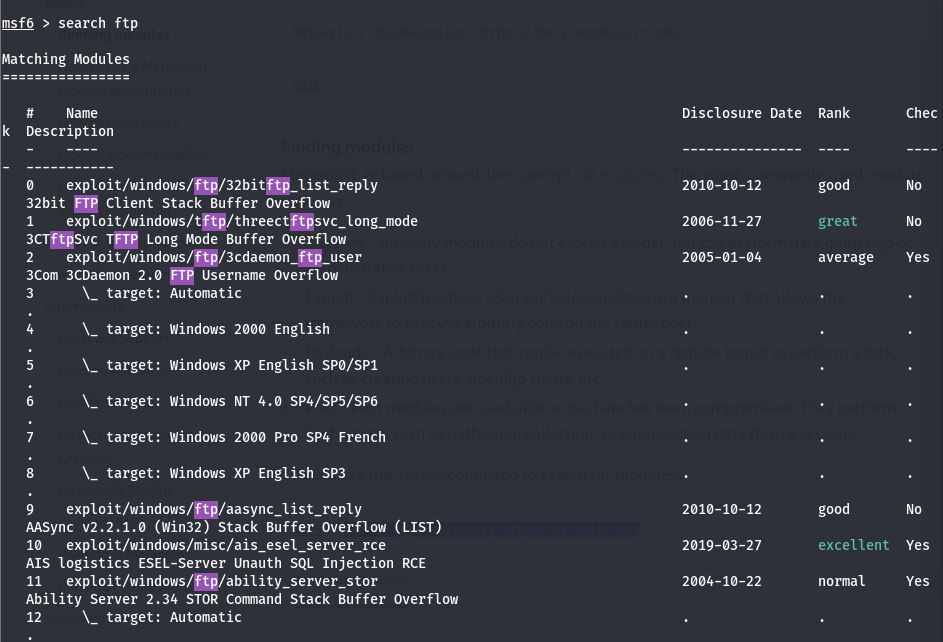
* echo -e "GET / HTTP/1.1\r\nHost: localhost\r\n\r\n" | nc localhost 80:
  + Replace 80 with the port where your HTTP server is running.



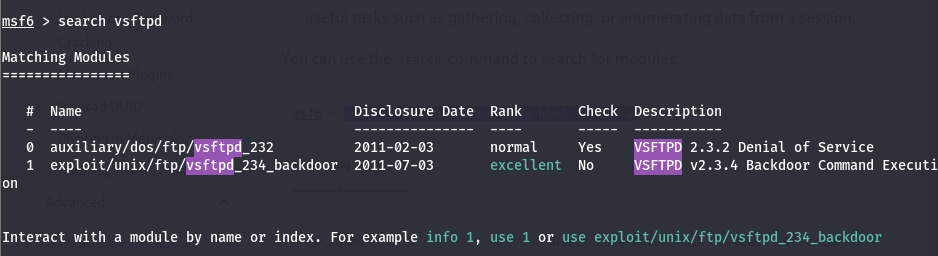
2. Metasploit:



* Search FTP:
  + This command lists all FTP-related modules, including **exploits**, **auxiliary tools** (like brute force or enumeration), and **post-exploitation modules**. For example, auxiliary/scanner/ftp/anonymous checks for anonymous FTP access.



* search vsftpd:
  + This will list modules related to the **vsftpd** service, such as the well-known **exploit/unix/ftp/vsftpd\_234\_backdoor**, which targets a backdoor in **vsftpd v2.3.4** to gain shell access.



* Use 1: it can use 1 option in given options:
* Set RHOTS: Set ip address in RHOTS

