First I have run the command “ip a “ for the scan of ip address on my system.



Then after I have performed a nmap scan for the ip address then I have found the ip address of the doubletrouble vm machine. Then I have performed a netdiscover for the range then I have got the ip addressof the machine



After getting the ip address of the machine then I have performed the nmap command to discover the open ports

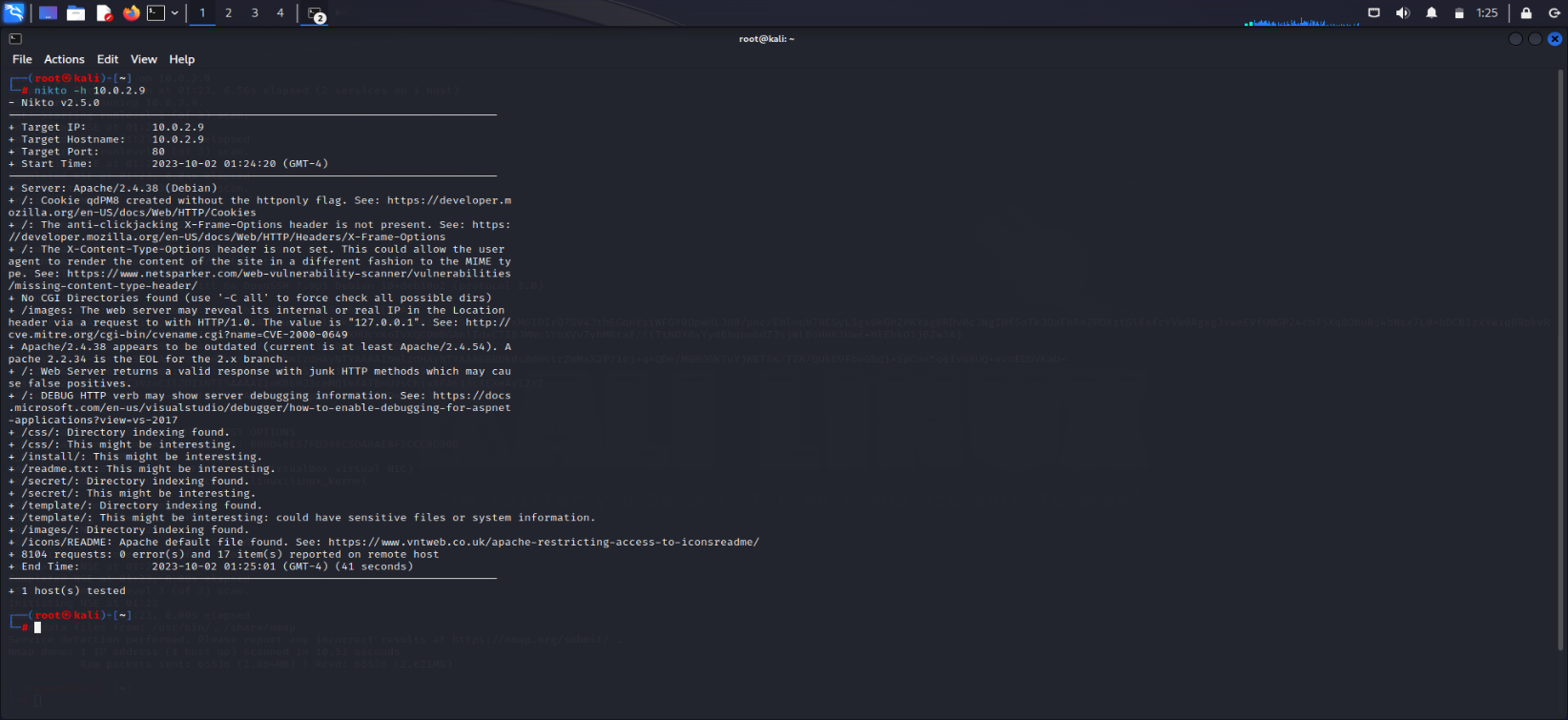
The command is “nmap -p- -n -vvv -sCV -o /root/scan1” . I have run this command to even save the output in a file and this is the output of the command



A screenshot of a computer

Description automatically generated

Then I have found the two open ports of which one is 22-ssh and the other is 80-http .As the http port open we can open the ip address in the browser. Then after I have performed a nikto scan for the ip address to check the vulnerabilities.

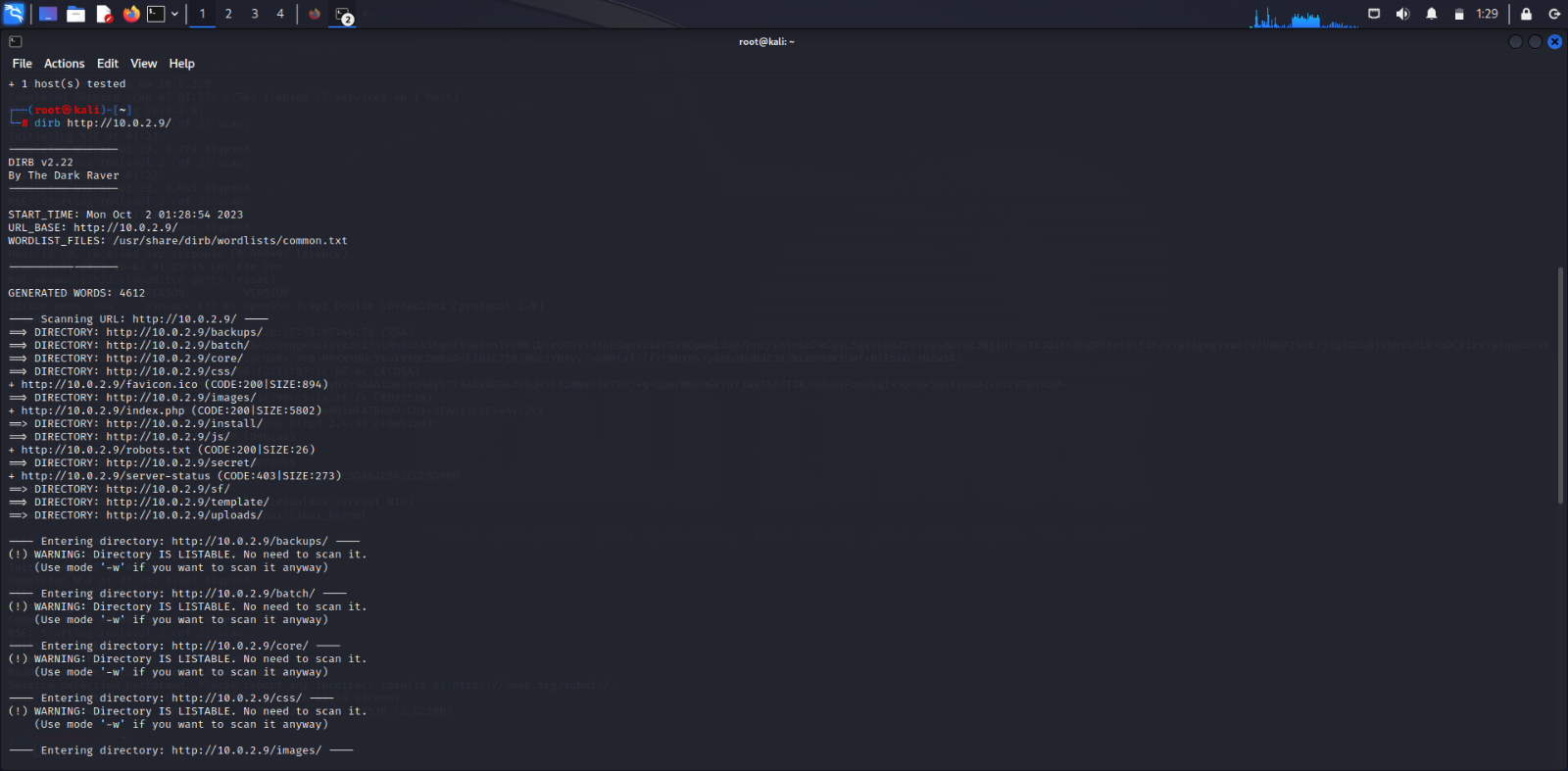


After performing the nikto scan then I have found the /secret folder which might be interesting after changing the ip address to “10.0.2.9/secret” I have found a image.

A computer screen shot of a white screen

Description automatically generated

After this I have performed a dirb command for the enumeration.



Then after I have downloaded the image and performed the steghide command and found that it had a password to extract the image so I have performed a stegseek command using the rockyou file which is by default saved as rockyou.txt.gz I have unzipped it and found password as “92camaro”

A screenshot of a computer

Description automatically generated

After this I have got a file of credits .txt which consists of the credentials of the user which I have used to login into the machine.



After getting the credentials I have logged into the machine then I have found that the upload of the image does not have a specific format to upload so we can perform even a reverse shell attack and even get a reverse connection and then gain the complete access of the system.

A screenshot of a computer

Description automatically generated

After this step I have downloaded the php reverse shell from the git hub and change the ip address to my attacker machine address and then download the python file from the exploit-db.com then after running both the files a have gained the complete access to the machine and I have got the access as the root user to the machine .

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated