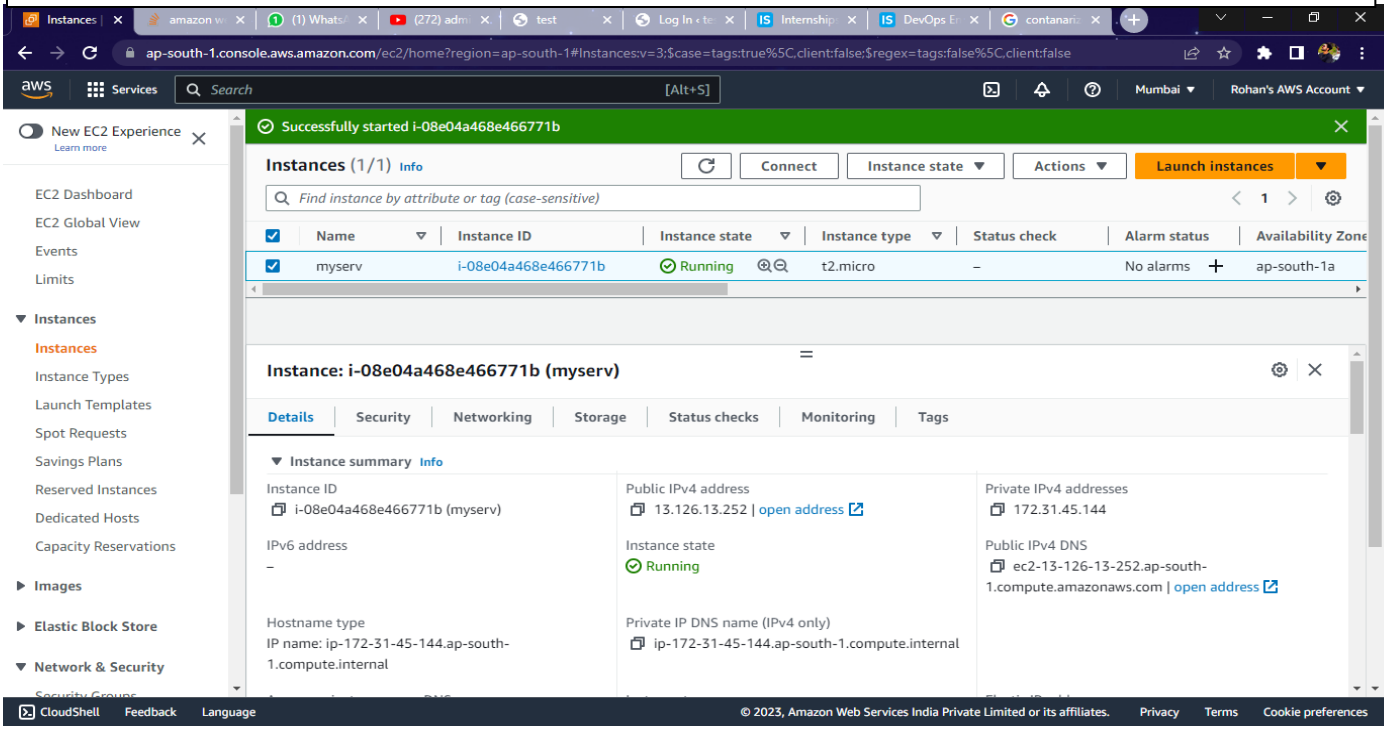
Project

Name:- Rohan Kamble **Github:- https://github.com/rohankamble103** **Linkedin:- https://www.linkedin.com/in/rohan-kamble-79705a217/**

The problem statement requires deploying a sample WordPress website, protecting it with a Nginx reverse proxy, and allowing admin login from a specific IP address only. Additionally, the candidate must enable log rotation, write a script to analyze Nginx logs, and provide a report.

1. First of all create a instance of your desired size and configure it as per your need.



Successfully started i-08e04a468e466771b

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
myserv	i-08e04a468e466771b	Running	t2.micro	–	No alarms	ap-south-1a

Instance: i-08e04a468e466771b (myserv)

Instance summary Info

Instance ID: i-08e04a468e466771b (myserv)

Public IPv4 address: 13.126.13.252 | open address

Private IPv4 addresses: 172.31.45.144

IPv6 address: –

Instance state: Running

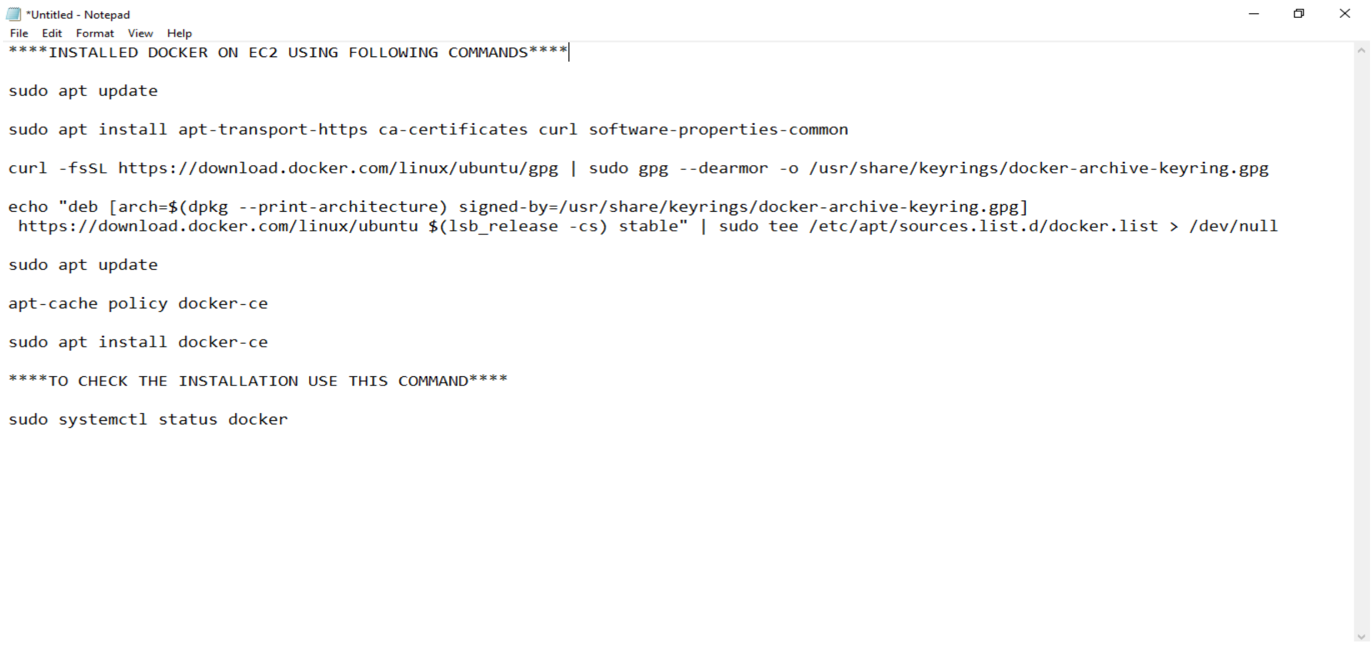
Public IPv4 DNS: ec2-13-126-13-252.ap-south-1.compute.amazonaws.com | open address

Hostname type: IP name: ip-172-31-45-144.ap-south-1.compute.internal

Private IP DNS name (IPv4 only): ip-172-31-45-144.ap-south-1.compute.internal

2. We need to install docker and docker-compose using following commands to containerize the Images

#sudo apt install docker-compose -y

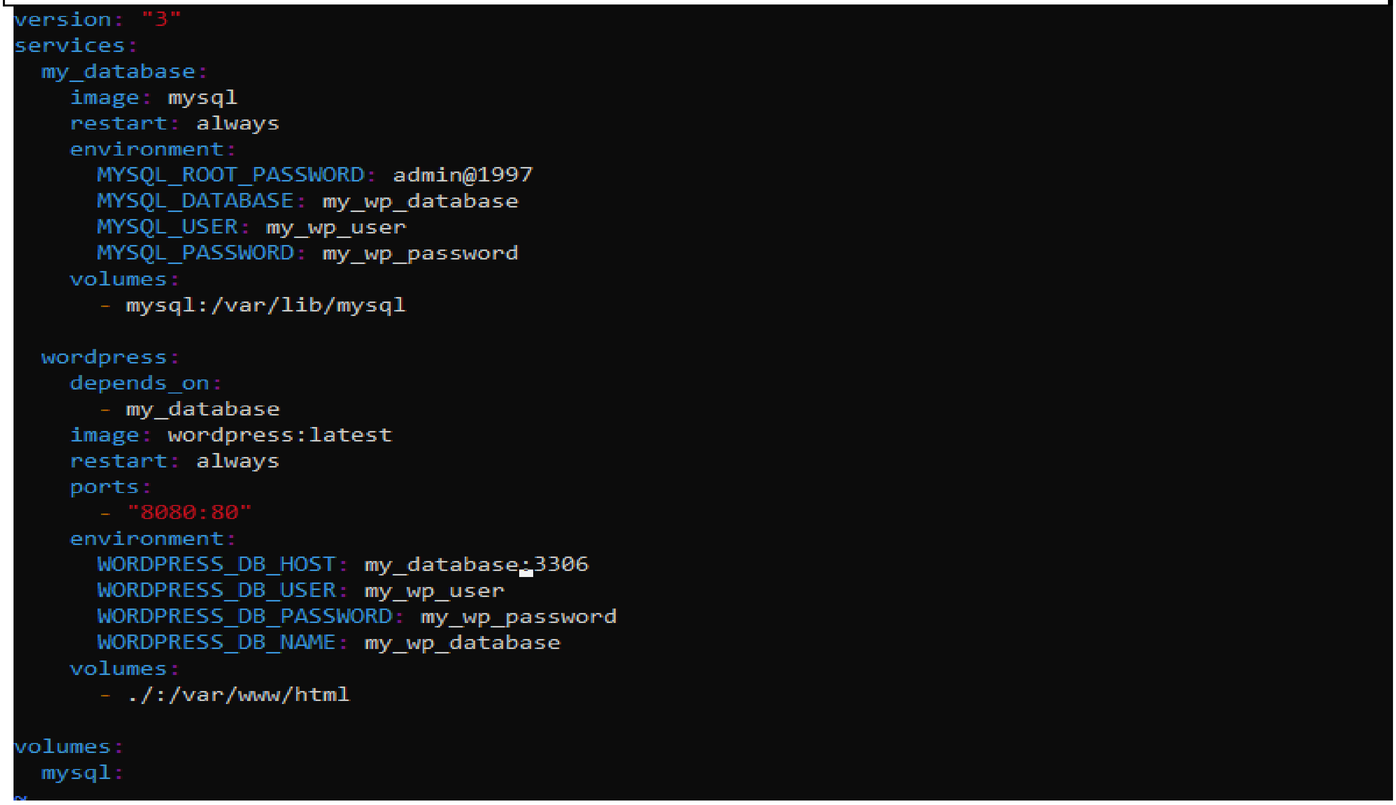


```
****INSTALLED DOCKER ON EC2 USING FOLLOWING COMMANDS****

sudo apt update

sudo apt install apt-transport-https ca-certificates curl software-properties-common

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg

echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg]
 https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

sudo apt update

apt-cache policy docker-ce

sudo apt install docker-ce

****TO CHECK THE INSTALLATION USE THIS COMMAND****

sudo systemctl status docker
```

3. Creating a folder named as compose and in that folder I have created a docker-compose file named as docker-compose.yml by using commands

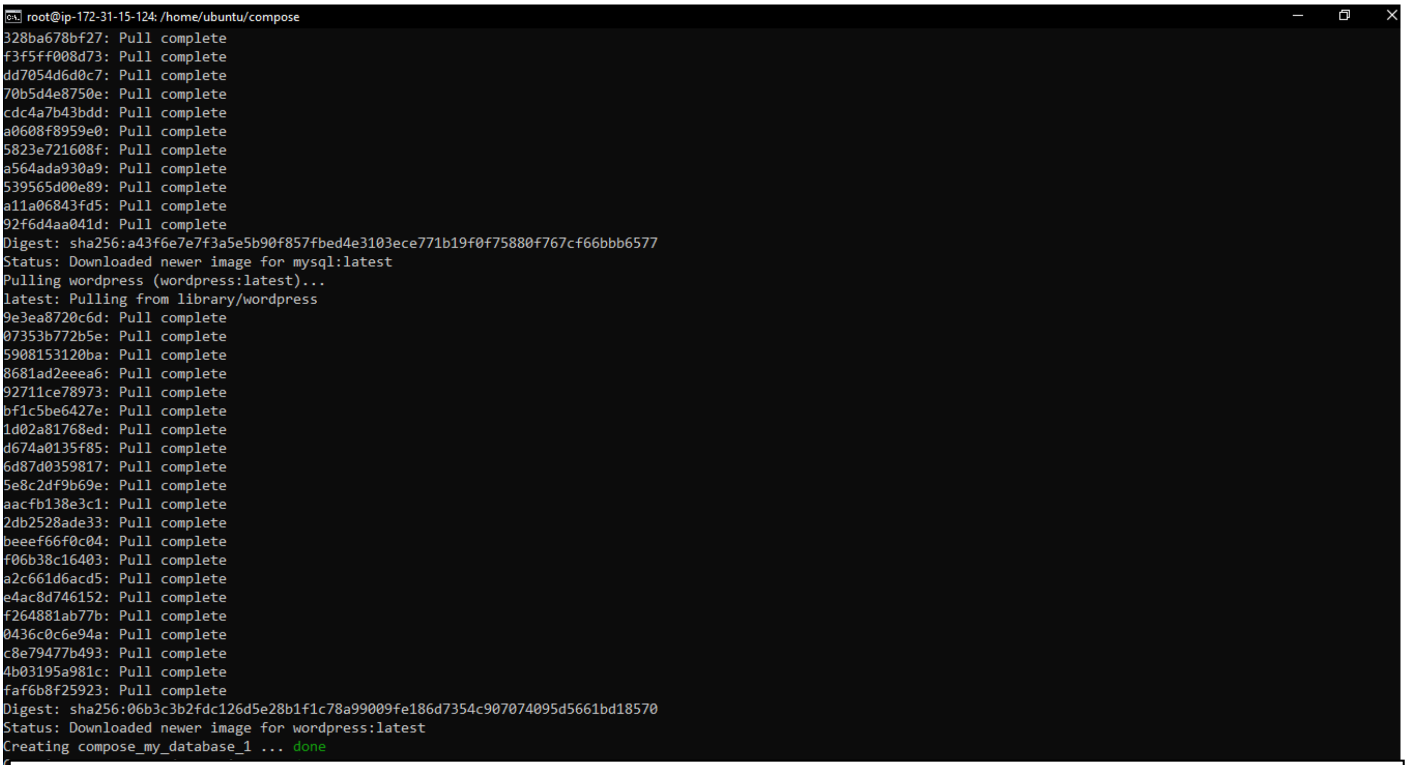
#mkdir compose

#vi docker-compose.yml



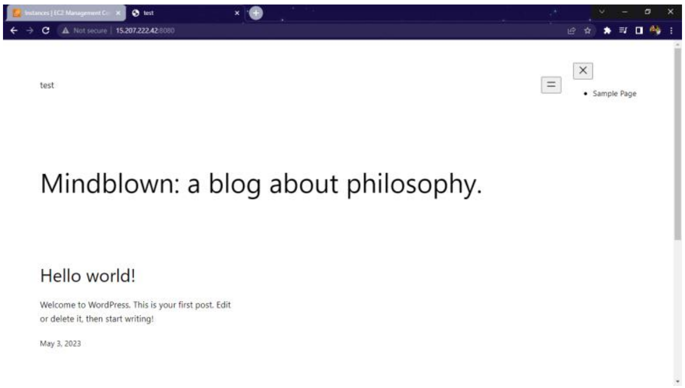
```
version: "3"
services:
  my_database:
    image: mysql
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: admin@1997
      MYSQL_DATABASE: my_wp_database
      MYSQL_USER: my_wp_user
      MYSQL_PASSWORD: my_wp_password
    volumes:
      - mysql:/var/lib/mysql

  wordpress:
    depends_on:
      - my_database
    image: wordpress:latest
    restart: always
    ports:
      - "8080:80"
    environment:
      WORDPRESS_DB_HOST: my_database:3306
      WORDPRESS_DB_USER: my_wp_user
      WORDPRESS_DB_PASSWORD: my_wp_password
      WORDPRESS_DB_NAME: my_wp_database
    volumes:
      - ./:/var/www/html

volumes:
  mysql:
```

4. Launching two containers of wordpress sample website and database with the help of docker compose



```
328ba678bf27: Pull complete
f3f5ff008d73: Pull complete
dd7054d6d0c7: Pull complete
70b5d4e8750e: Pull complete
cdc4a7b43bdd: Pull complete
a0608f8959e0: Pull complete
5823e721608f: Pull complete
a564ada930a9: Pull complete
539565d00e89: Pull complete
a11a06843fd5: Pull complete
92f6d4aa041d: Pull complete
Digest: sha256:a43f6e7e7f3a5e5b90f857fbed4e3103ece771b19f0f75880f767cf66bbb6577
Status: Downloaded newer image for mysql:latest
Pulling wordpress (wordpress:latest)...
latest: Pulling from library/wordpress
9e3ea8720c6d: Pull complete
07353b772b5e: Pull complete
5908153120ba: Pull complete
8681ad2eeea6: Pull complete
92711ce78973: Pull complete
bf1c5be6427e: Pull complete
1d02a81768ed: Pull complete
d674a0135f85: Pull complete
6d87d0359817: Pull complete
5e8c2df9b69e: Pull complete
aacfb138e3c1: Pull complete
2db2528ade33: Pull complete
beeef66f0c04: Pull complete
f06b38c16403: Pull complete
a2c661d6acd5: Pull complete
e4ac8d746152: Pull complete
f264881ab77b: Pull complete
0436c0c6e94a: Pull complete
c8e79477b493: Pull complete
4b03195a981c: Pull complete
faf6b8f25923: Pull complete
Digest: sha256:06b3c3b2fdc126d5e28b1f1c78a99009fe186d7354c907074095d5661bd18570
Status: Downloaded newer image for wordpress:latest
Creating compose_my_database_1 ... done
```

5. Create Admin User for the wordpress sample website and launching both the admin page and the website page


Instances | EC2 Management Co
test
Not secure | 15.207.222.42:8080

test

☰ ✕

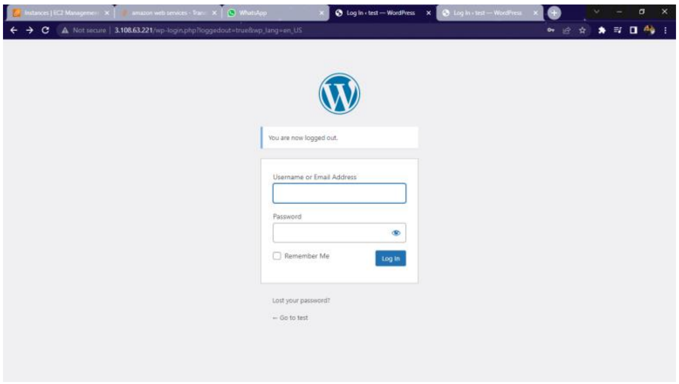
- Sample Page

Mindblown: a blog about philosophy.

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

May 3, 2023


Instances | EC2 Managemen
amazon web services - Tran
WhatsApp
Log In ‹ test — WordPress
Log In ‹ test — WordPress
Not secure | 3.108.63.221/wp-login.php?loggedout=true&wp_lang=en_US

You are now logged out.

Username or Email Address

Password

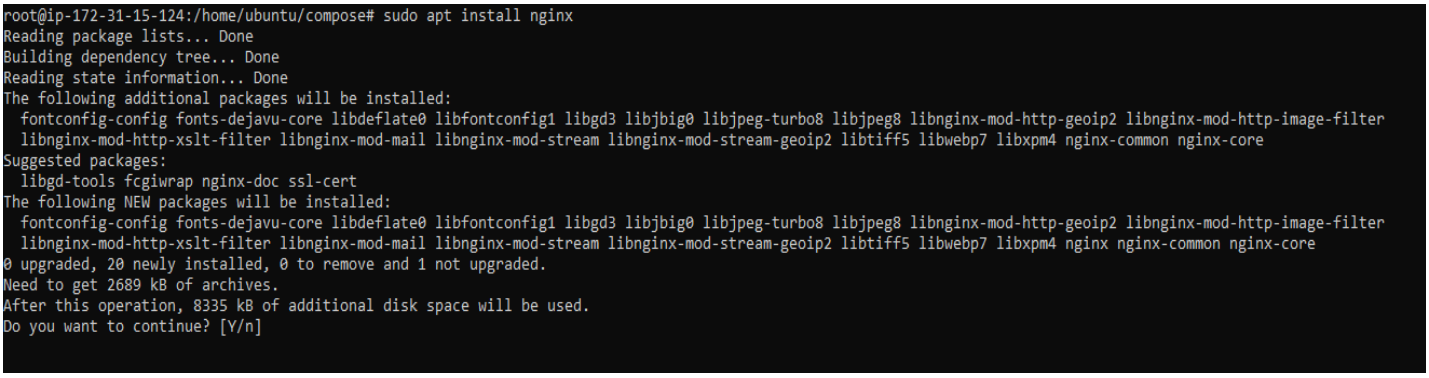
□ Remember Me

Log In

Lost your password?

← Go to test

6. Installing Nginx web server to apply security in the form of reverse proxy to the container.

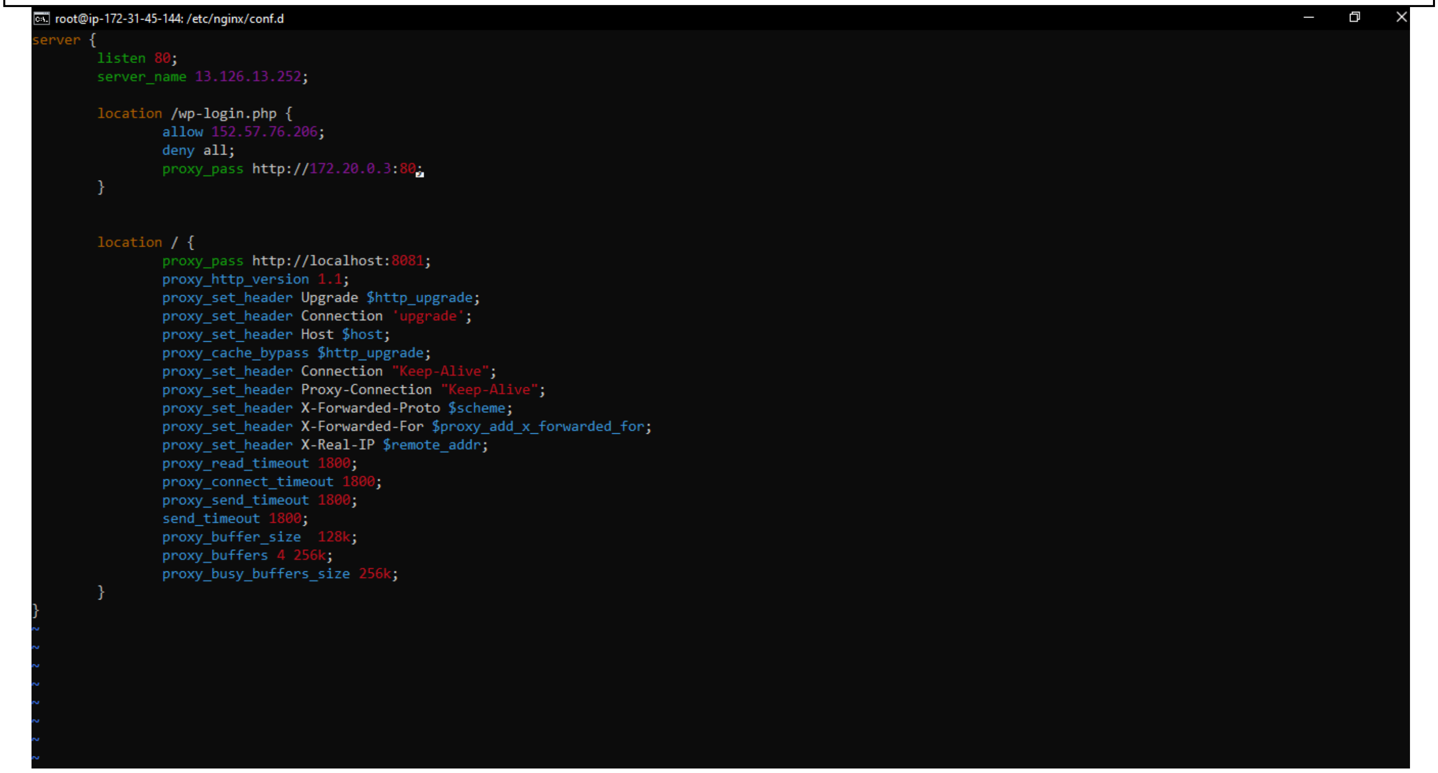


```
root@ip-172-31-15-124:/home/ubuntu/compose# sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip2 libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2 libtiff5 libwebp7 libxpm4 nginx-common nginx-core
Suggested packages:
  libgd-tools fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-geoip2 libnginx-mod-http-image-filter
  libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream libnginx-mod-stream-geoip2 libtiff5 libwebp7 libxpm4 nginx nginx-common nginx-core
0 upgraded, 20 newly installed, 0 to remove and 1 not upgraded.
Need to get 2689 kB of archives.
After this operation, 8335 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

7. Creating a conf file in the "/etc/nginx/conf.d/wordpress.rohan.conf", By using this file we are applying reverse proxy and also we are restricting the admin access of the website using allow "private IP";

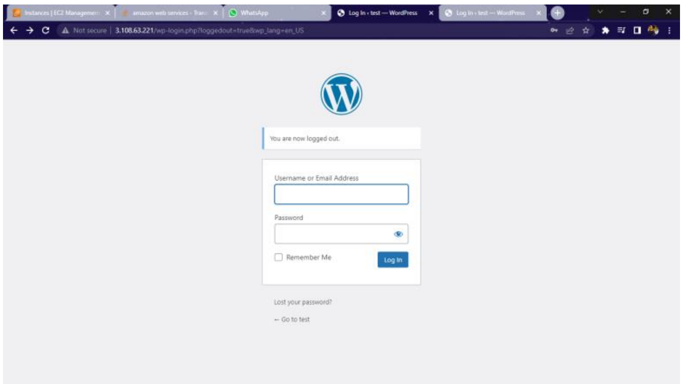
Nginx also look for wp-login.php in the localserver and not able to find the webpage,

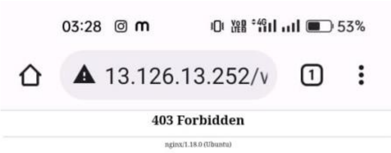
So we have to give the containers Ip (172.20.0.3:port) so that nginx can look for wp-login.php in container



```
server {
        listen 80;
        server_name 13.126.13.252;

        location /wp-login.php {
                allow 152.57.76.206;
                deny all;
                proxy_pass http://172.20.0.3:80;
        }


        location / {
                proxy_pass http://localhost:8081;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
                proxy_set_header Connection "Keep-Alive";
                proxy_set_header Proxy-Connection "Keep-Alive";
                proxy_set_header X-Forwarded-Proto $scheme;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_read_timeout 1800;
                proxy_connect_timeout 1800;
                proxy_send_timeout 1800;
                send_timeout 1800;
                proxy_buffer_size  128k;
                proxy_buffers 4 256k;
                proxy_busy_buffers_size 256k;
        }
}
~
~
~
~
~
~
~
~
```

8. Check the syntax by “ nginx –t ” and if the test is ok then restart the nginx by command systemctl restart nginx, ow you don’t need to mention port in the address bar and also no one else can find the admin page

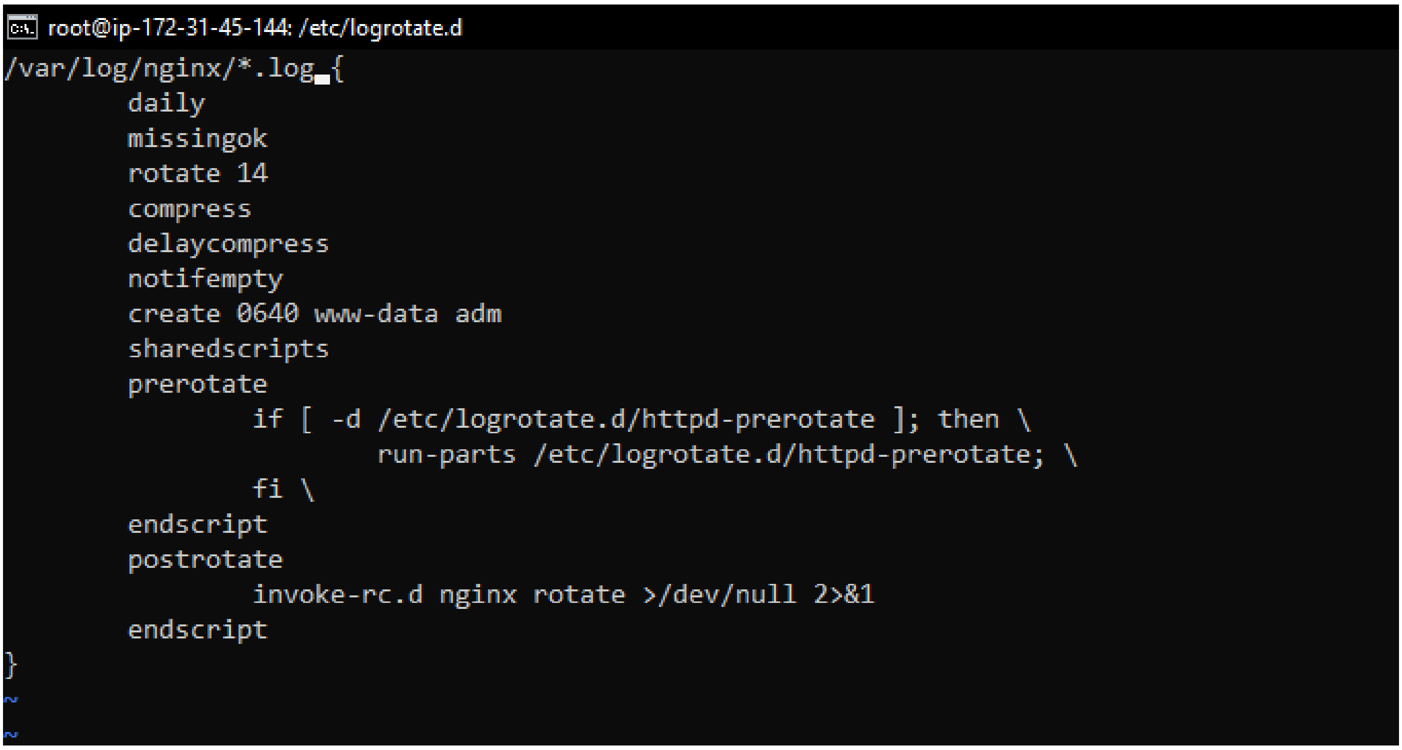

Not secure | 3.108.63.221/wp-login.php?loggedout=true&wp_lang=en_US
You are now logged out.
Username or Email Address
Password
Remember Me
Log In
Lost your password?
← Go to test



403 Forbidden

nginx/1.18.0 (Ubuntu)

9. Create a file nginx in /etc/logrotate.d/ and you will mention each and every detail of information you want from logs, for example :-



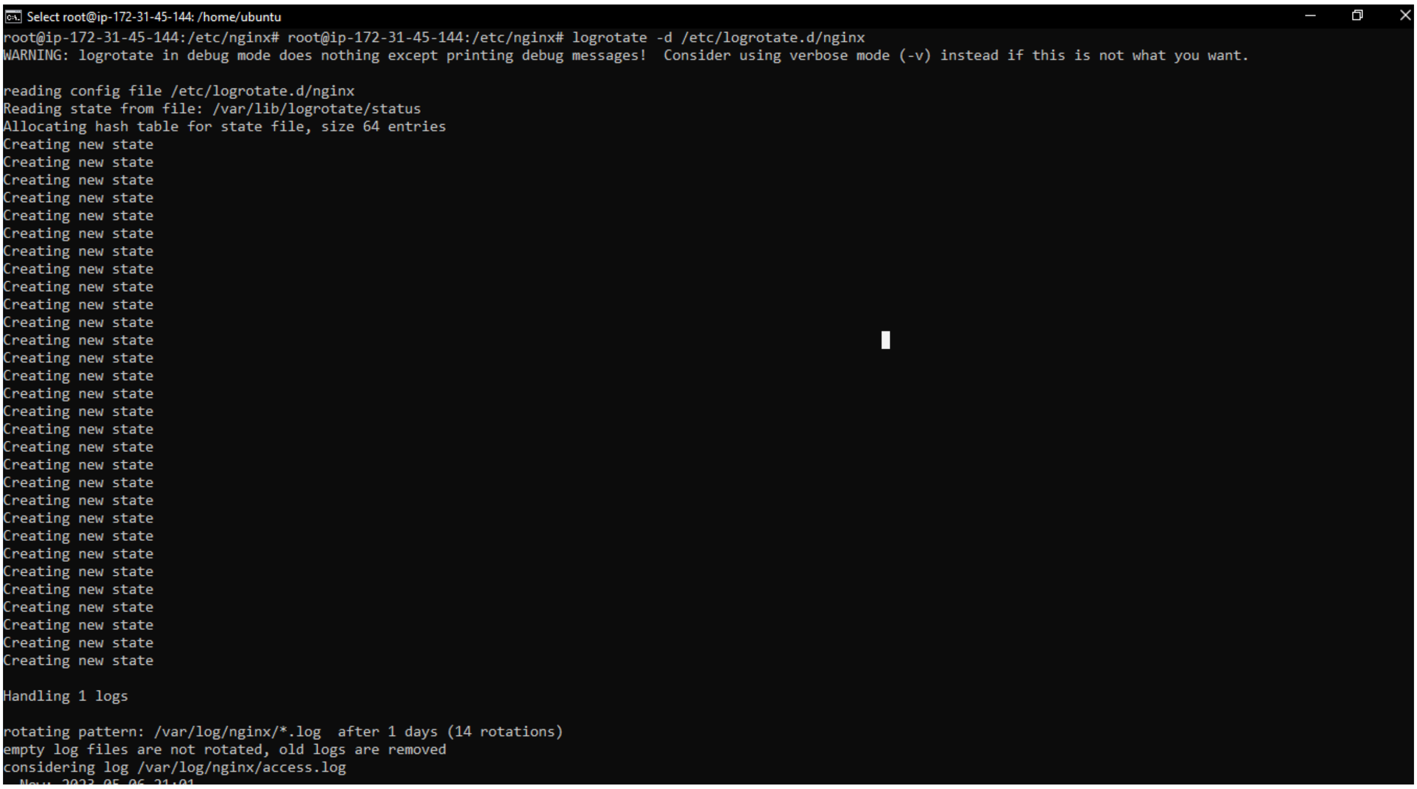
```
/var/log/nginx/*.log {
        daily
        missingok
        rotate 14
        compress
        delaycompress
        notifempty
        create 0640 www-data adm
        sharedscripts
        prerotate
                if [ -d /etc/logrotate.d/httpd-prerotate ]; then \
                        run-parts /etc/logrotate.d/httpd-prerotate; \
                fi \
        endscript
        postrotate
                invoke-rc.d nginx rotate >/dev/null 2>&1
        endscript
}
~
~
```

daily**:- log files should be rotated every day. ***missingok**:- log file is missing, the rotation should proceed without throwing an error. ***rotate 14**:- maximum of 14 rotated logs should be kept. ***compress**:- rotated log files should be compressed. * **delaycompress**:-compression of rotated log files should be delayed until the next rotation cycle.notifempty**:- rotated log files should not be rotated if they are empty. ***create**:- create log with given permissions.***sharedscripts**:- **postrotate** script should only be run once after all logs have been rotated.***prerotate**:- commands enclosed in the block should be executed before the log files are rotated.***postrotate**:- commands enclosed in the block should be executed after the log files have been rotated.

10. Test the configuration using the following command and also enable it with the second command.

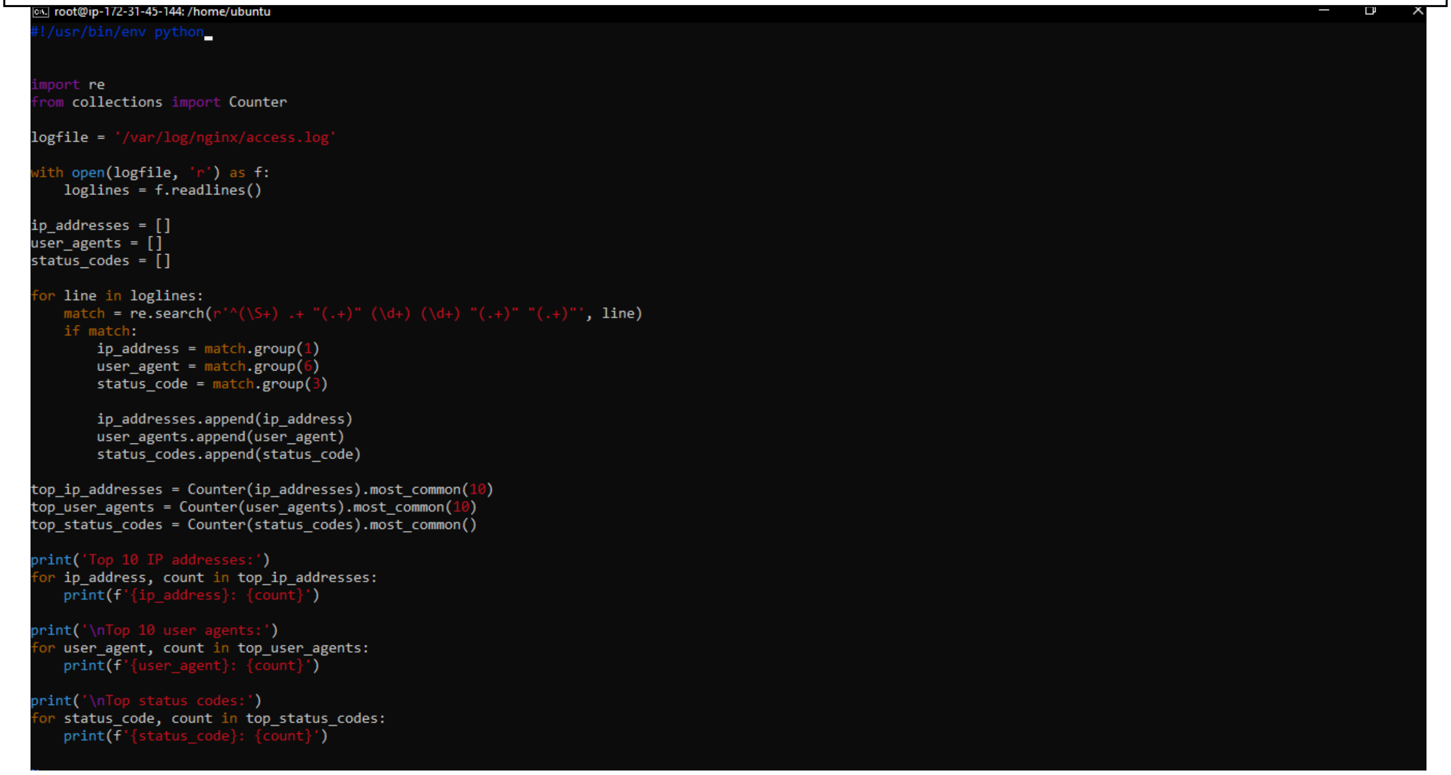
# logrotate -d /etc/logrotate.d/nginx

# logrotate /etc/logrotate.d/nginx



```
root@ip-172-31-45-144:/etc/nginx# root@ip-172-31-45-144:/etc/nginx# logrotate -d /etc/logrotate.d/nginx
WARNING: logrotate in debug mode does nothing except printing debug messages!  Consider using verbose mode (-v) instead if this is not what you want.

reading config file /etc/logrotate.d/nginx
Reading state from file: /var/lib/logrotate/status
Allocating hash table for state file, size 64 entries
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state
Creating new state

Handling 1 logs

rotating pattern: /var/log/nginx/*.log  after 1 days (14 rotations)
empty log files are not rotated, old logs are removed
considering log /var/log/nginx/access.log
  Now: 2023-05-06 21:01
```

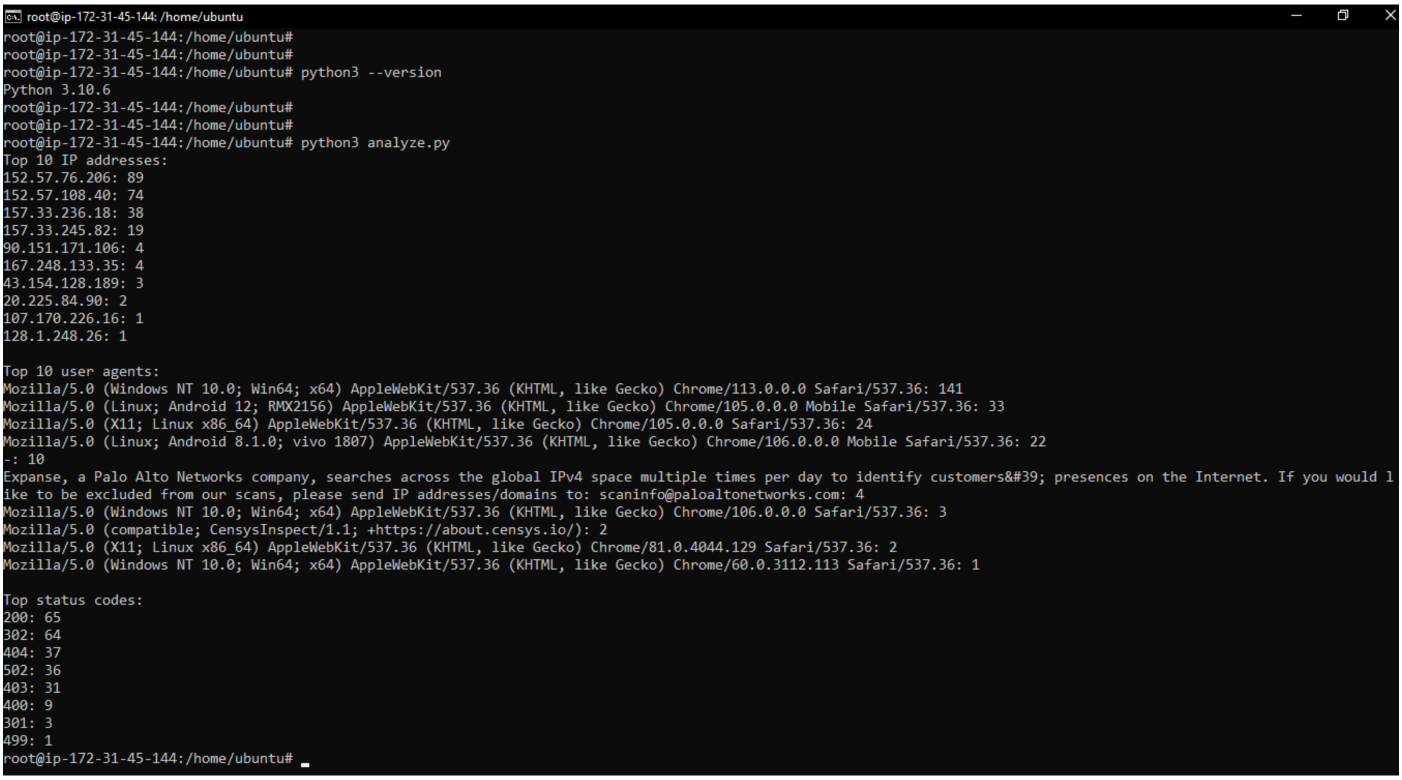
11. Create a Python Script to analyse the logs according to our need and print the output



```
#!/usr/bin/env python


import re
from collections import Counter

logfile = '/var/log/nginx/access.log'

with open(logfile, 'r') as f:
    loglines = f.readlines()

ip_addresses = []
user_agents = []
status_codes = []

for line in loglines:
    match = re.search(r'^(\S+) .+ "(.+)" (\d+) (\d+) "(.+)" "(.+)"', line)
    if match:
        ip_address = match.group(1)
        user_agent = match.group(6)
        status_code = match.group(3)

        ip_addresses.append(ip_address)
        user_agents.append(user_agent)
        status_codes.append(status_code)

top_ip_addresses = Counter(ip_addresses).most_common(10)
top_user_agents = Counter(user_agents).most_common(10)
top_status_codes = Counter(status_codes).most_common()

print('Top 10 IP addresses:')
for ip_address, count in top_ip_addresses:
    print(f'{ip_address}: {count}')

print('\nTop 10 user agents:')
for user_agent, count in top_user_agents:
    print(f'{user_agent}: {count}')

print('\nTop status codes:')
for status_code, count in top_status_codes:
    print(f'{status_code}: {count}')
```

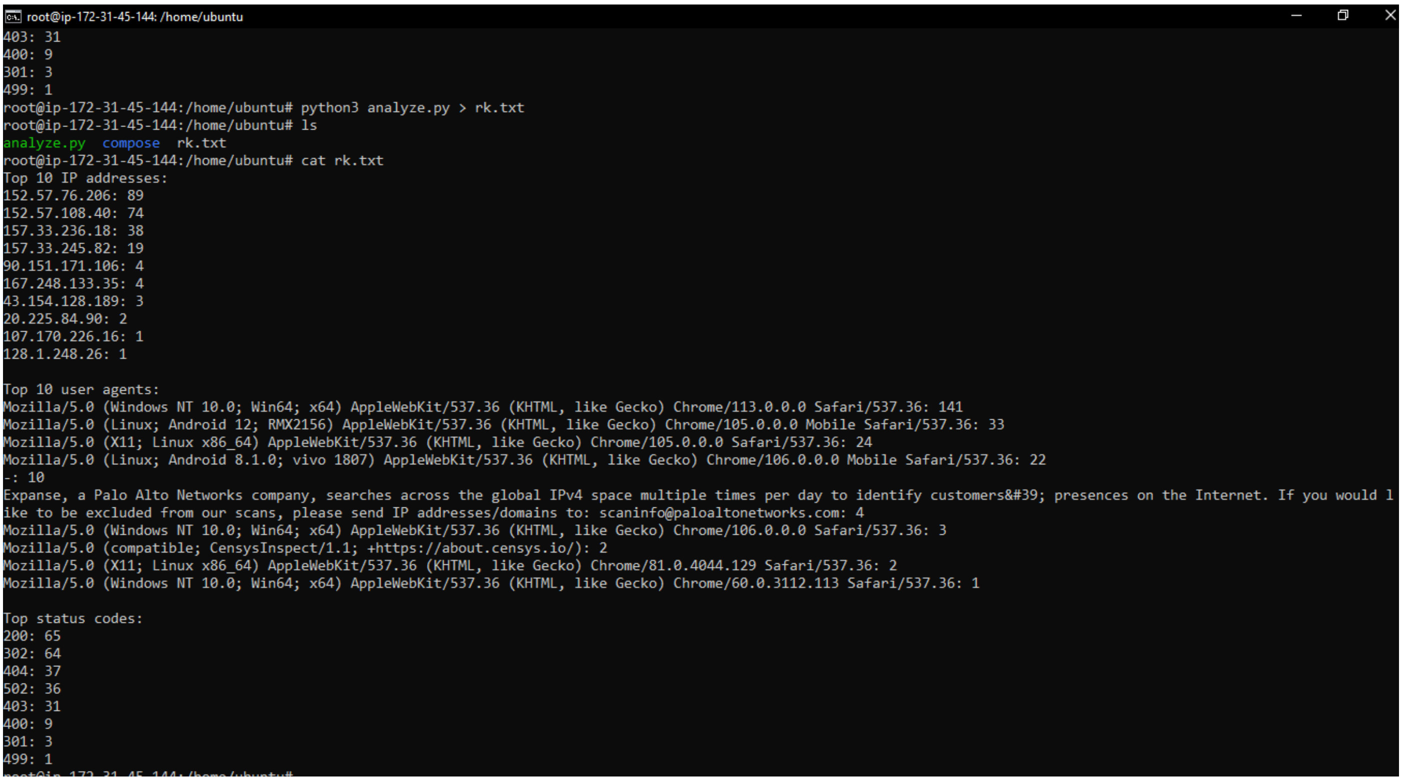
12. To Execute the file we need to change the permission of the file and add execute permission by using following command

#chmod 755 analyze.py

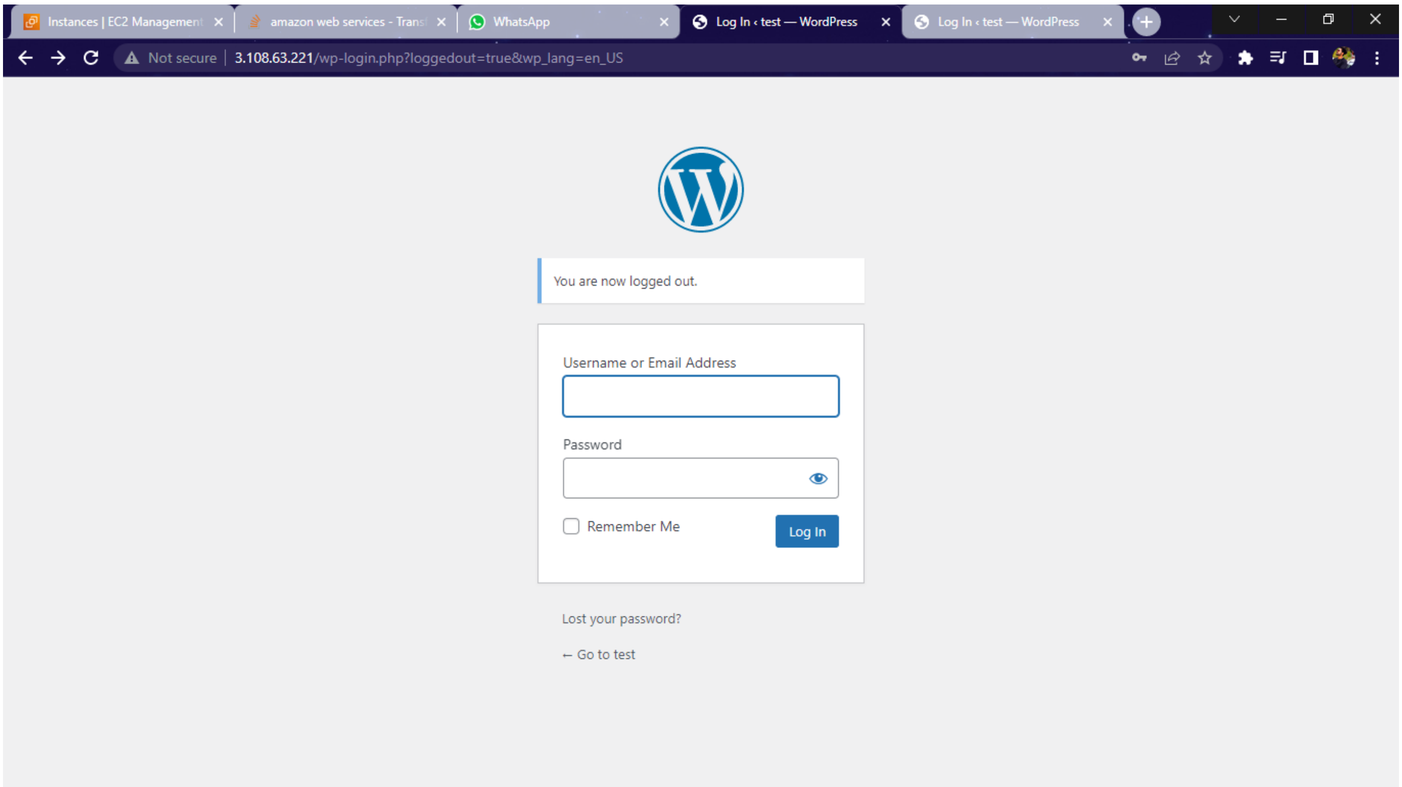


```
root@ip-172-31-45-144:/home/ubuntu#
root@ip-172-31-45-144:/home/ubuntu#
root@ip-172-31-45-144:/home/ubuntu# python3 --version
Python 3.10.6
root@ip-172-31-45-144:/home/ubuntu#
root@ip-172-31-45-144:/home/ubuntu#
root@ip-172-31-45-144:/home/ubuntu# python3 analyze.py
Top 10 IP addresses:
152.57.76.206: 89
152.57.108.40: 74
157.33.236.18: 38
157.33.245.82: 19
90.151.171.106: 4
167.248.133.35: 4
43.154.128.189: 3
20.225.84.90: 2
107.170.226.16: 1
128.1.248.26: 1

Top 10 user agents:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36: 141
Mozilla/5.0 (Linux; Android 12; RMX2156) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Mobile Safari/537.36: 33
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36: 24
Mozilla/5.0 (Linux; Android 8.1.0; vivo 1807) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36: 22
-: 10
Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers&#39; presences on the Internet. If you would l
ike to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com: 4
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36: 3
Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/): 2
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36: 2
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36: 1

Top status codes:
200: 65
302: 64
404: 37
502: 36
403: 31
400: 9
301: 3
499: 1
root@ip-172-31-45-144:/home/ubuntu# _
```

13. To Run the script we need to check is ther python installed or not, If it is not we need to install it to our system



```
403: 31
400: 9
301: 3
499: 1
root@ip-172-31-45-144:/home/ubuntu# python3 analyze.py > rk.txt
root@ip-172-31-45-144:/home/ubuntu# ls
analyze.py  compose  rk.txt
root@ip-172-31-45-144:/home/ubuntu# cat rk.txt
Top 10 IP addresses:
152.57.76.206: 89
152.57.108.40: 74
157.33.236.18: 38
157.33.245.82: 19
90.151.171.106: 4
167.248.133.35: 4
43.154.128.189: 3
20.225.84.90: 2
107.170.226.16: 1
128.1.248.26: 1

Top 10 user agents:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36: 141
Mozilla/5.0 (Linux; Android 12; RMX2156) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Mobile Safari/537.36: 33
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36: 24
Mozilla/5.0 (Linux; Android 8.1.0; vivo 1807) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Mobile Safari/537.36: 22
-: 10
Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers&#39; presences on the Internet. If you would l
ike to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com: 4
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36: 3
Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/): 2
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36: 2
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36: 1

Top status codes:
200: 65
302: 64
404: 37
502: 36
403: 31
400: 9
301: 3
499: 1
root@ip-172-31-45-144:/home/ubuntu#
```



Instances | EC2 Management
amazon web services - Trans
WhatsApp
Log In ‹ test — WordPress
Log In ‹ test — WordPress
Not secure
3.108.63.221/wp-login.php?loggedout=true&wp_lang=en_US

You are now logged out.

Username or Email Address

Password

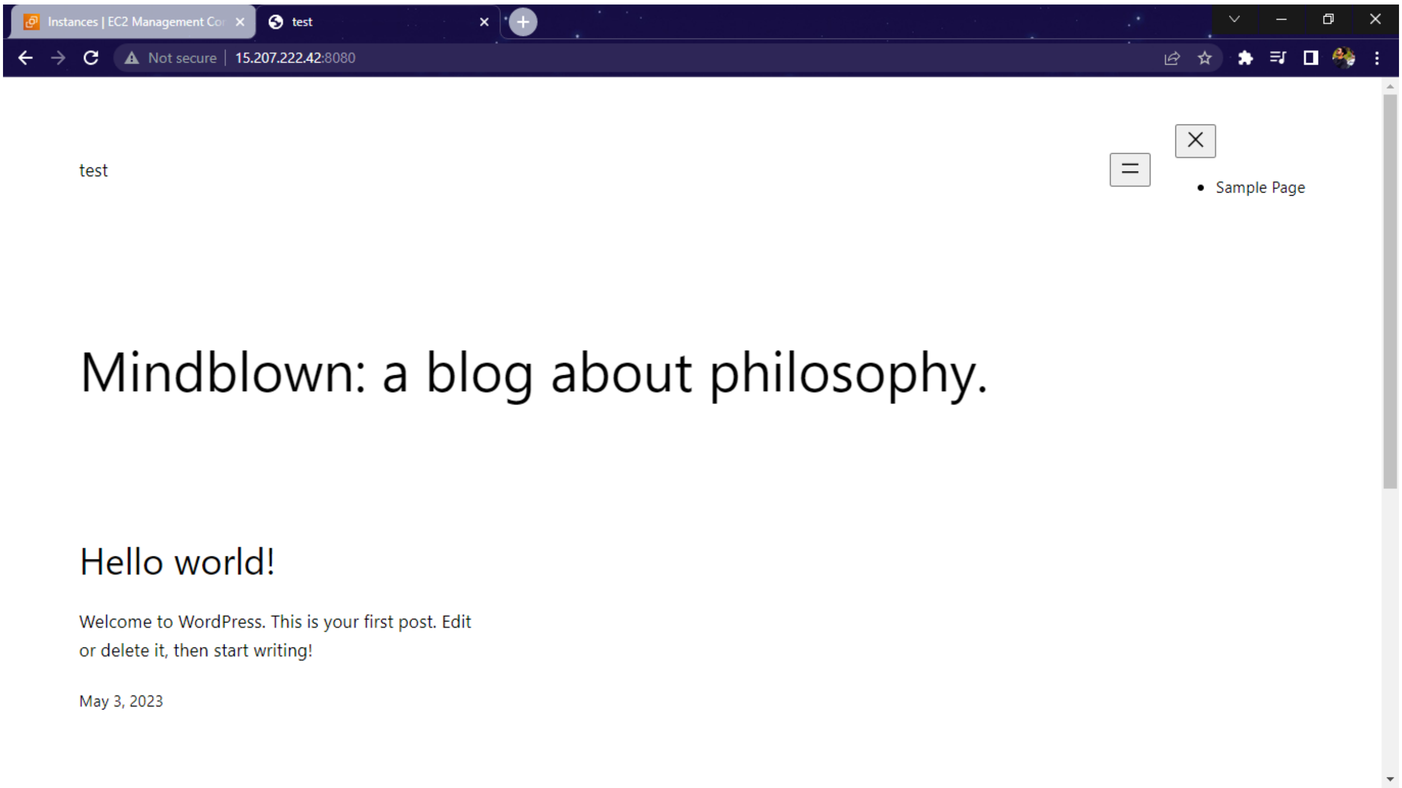
□ Remember Me

Log In

Lost your password?

← Go to test

14. Run the script by command “python3 analyze.py” and it will print the output as you needed and you can also story the output of the file into another file by using “python3 analyze.py > rk.txt” and the data will be stored in the file



test

- Sample Page

Mindblown: a blog about philosophy.

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

May 3, 2023

Regards,

Rohan Kamble