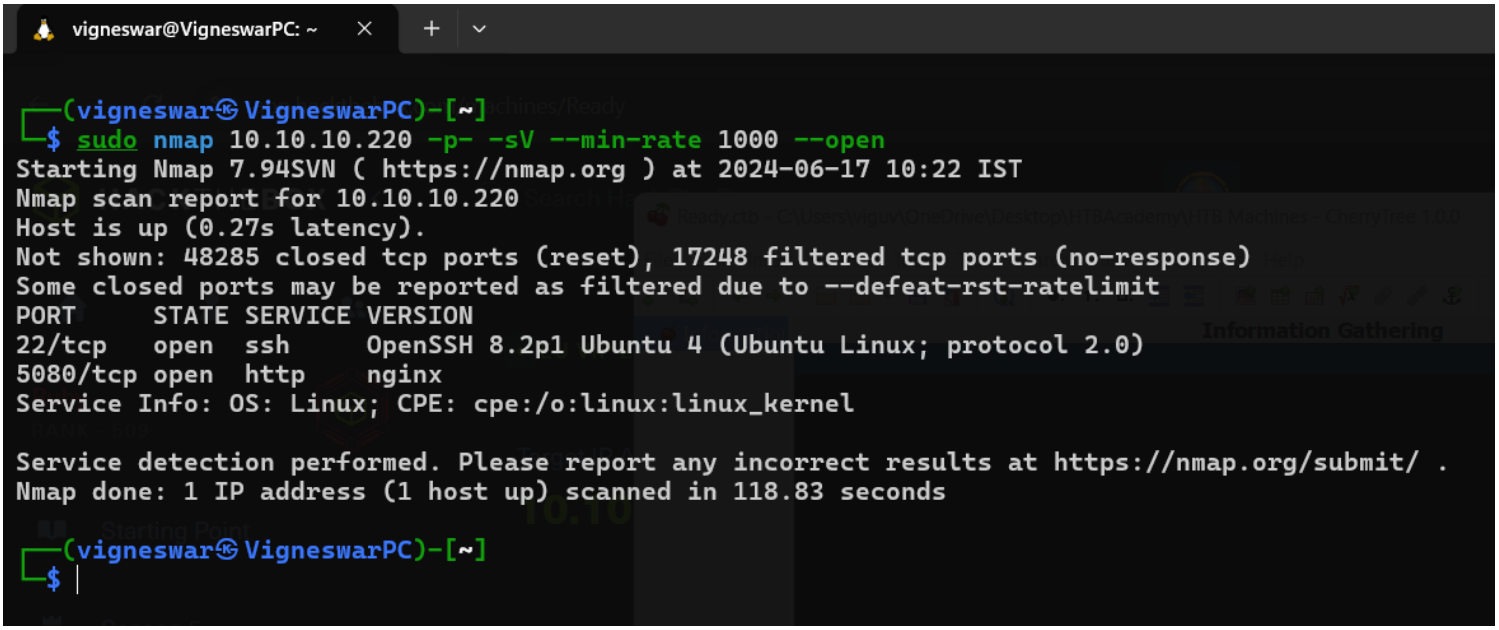
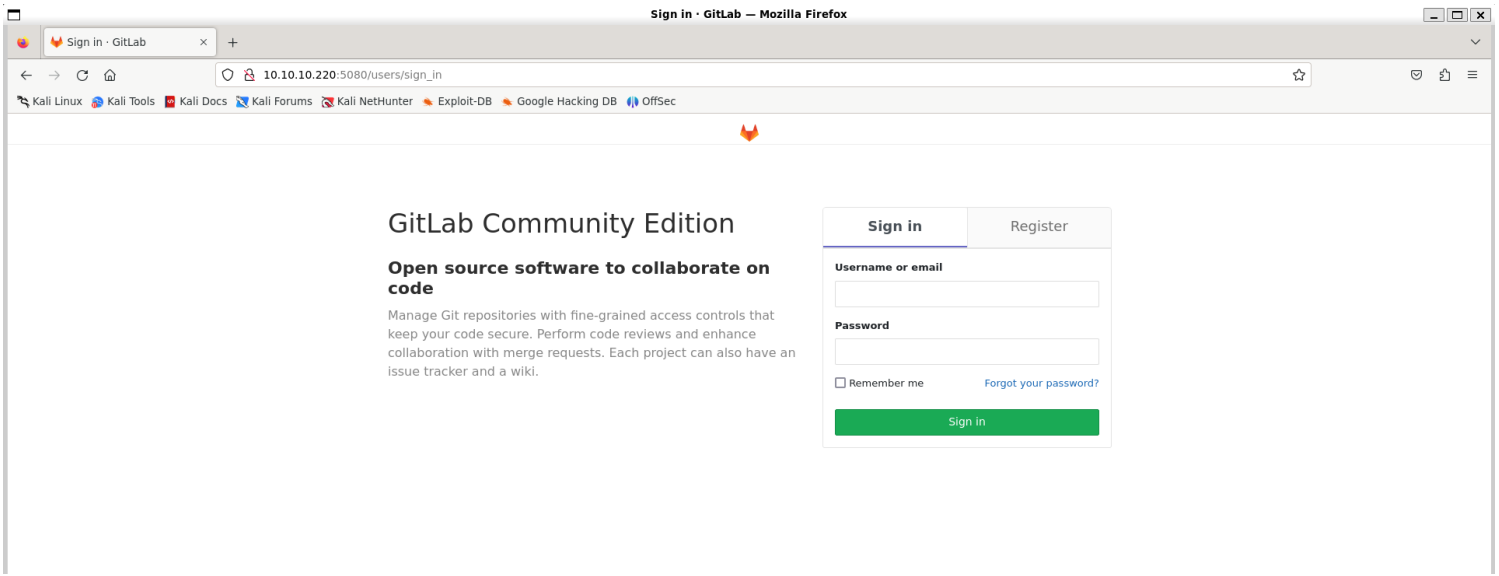
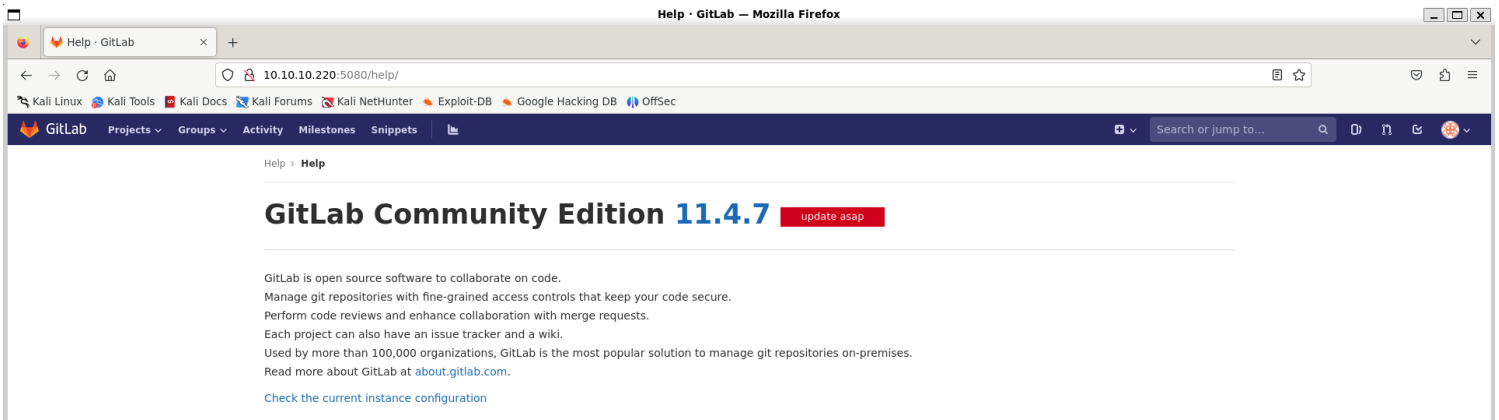
Information Gathering

1) Found open ports



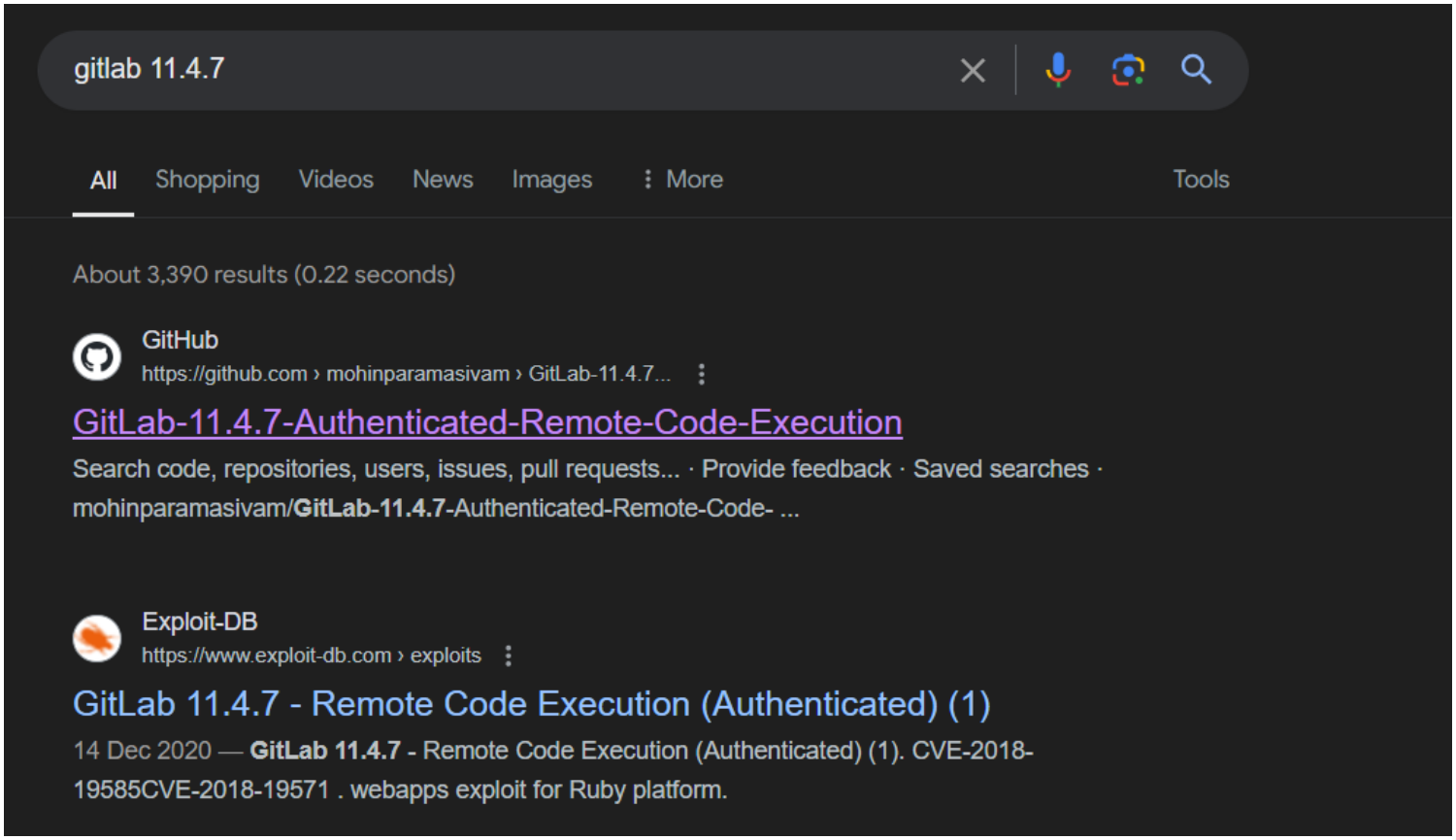
2) Found a gitlab instance





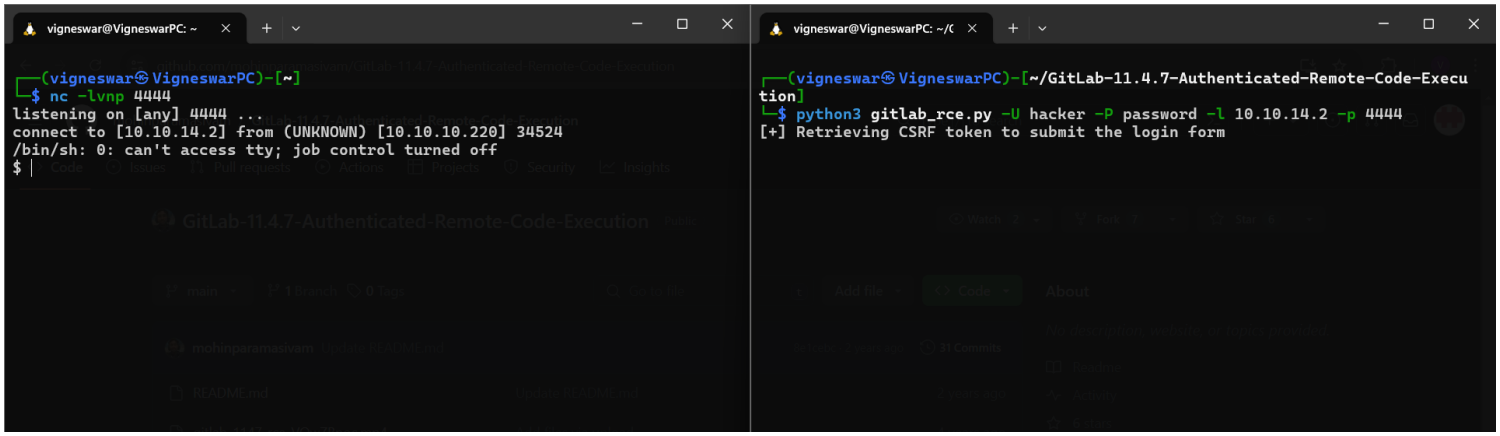
Vulnerability Assessment

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