靶机精讲：ZION_1靶机 writeup

一.arp-scan进行扫描靶机

```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -I eth0 -l
[sudo] kali 的密码：
Interface: eth0, type: EN10MB, MAC: 00:0c:29:9c:ad:b4, IPv4: 192.168.28.50
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.28.47   00:0c:29:c4:b8:7e       VMware, Inc.
192.168.28.140  e6:41:b2:54:93:c1       (Unknown: locally administered)
192.168.28.214  6c:cd:0e:fb:e3:b1       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 2.025 seconds (126.42 hosts/sec). 3 responded
```

其中**192.168.28.47**为目标靶机

二.端口扫描与脚本扫描

1.使用namp进行端口tcp扫描

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sT -sV -O -p- --min-rate=10000  192.168.28.47
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-29 10:07 EDT
Nmap scan report for 192.168.28.47
Host is up (0.0014s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
80/tcp open  http    Apache httpd (PHP 7.4.5)
MAC Address: 00:0C:29:C4:B8:7E (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5.1
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9, Linux 5.1
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.08 seconds
```

2.为了更加全面我们在使用upd扫描

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU --min-rate=10000 192.168.28.47
[sudo] kali 的密码：
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-29 10:08 EDT
Nmap scan report for 192.168.28.47
Host is up (0.00033s latency).
Not shown: 998 open|filtered udp ports (no-response)
PORT   STATE  SERVICE
22/udp closed ssh
80/udp closed http
MAC Address: 00:0C:29:C4:B8:7E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
```

3.使用nmap默认脚本扫描

```
文件  动作  编辑  查看  帮助
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=vuln 192.168.28.47
[sudo] kali 的密码：
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-29 10:07 EDT
Nmap scan report for 192.168.28.47
Host is up (0.00031s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
MAC Address: 00:0C:29:C4:B8:7E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 41.39 seconds
```

4.分析

由上述扫描得到，目标靶机开放了22与80端口，分别运行的服务是openssh 8.0 与apache （php 7.4.5），Linux内核可能是3，4或5，脚本扫描没有什么漏洞。由于只开放了两个端口，我们一般优先从80端口开始撕口子，22端口则没有什么办法（字典爆破效率太低且不知道结果）。

四.进行目录爆破

这里我使用dirb进行默认字典目录爆破

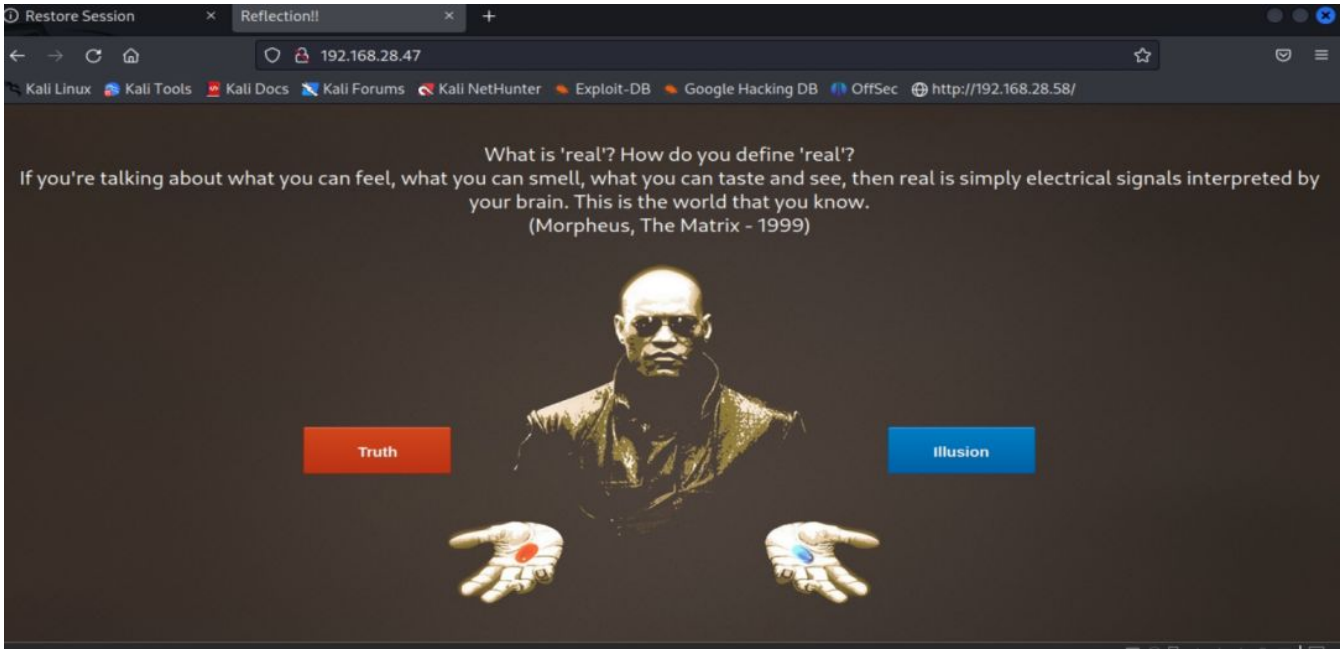
得到一些令人兴奋的文件：

- http://192.168.28.47/cgi-bin/ (CODE:403|SIZE:4518)
- http://192.168.28.47/index (CODE:200|SIZE:886)
- http://192.168.28.47/index.php (CODE:200|SIZE:886)
- http://192.168.28.47/robots (CODE:200|SIZE:13)
- http://192.168.28.47/robots.txt (CODE:200|SIZE:13)

robots.txt绝对值得我们一看

五.信息汇总

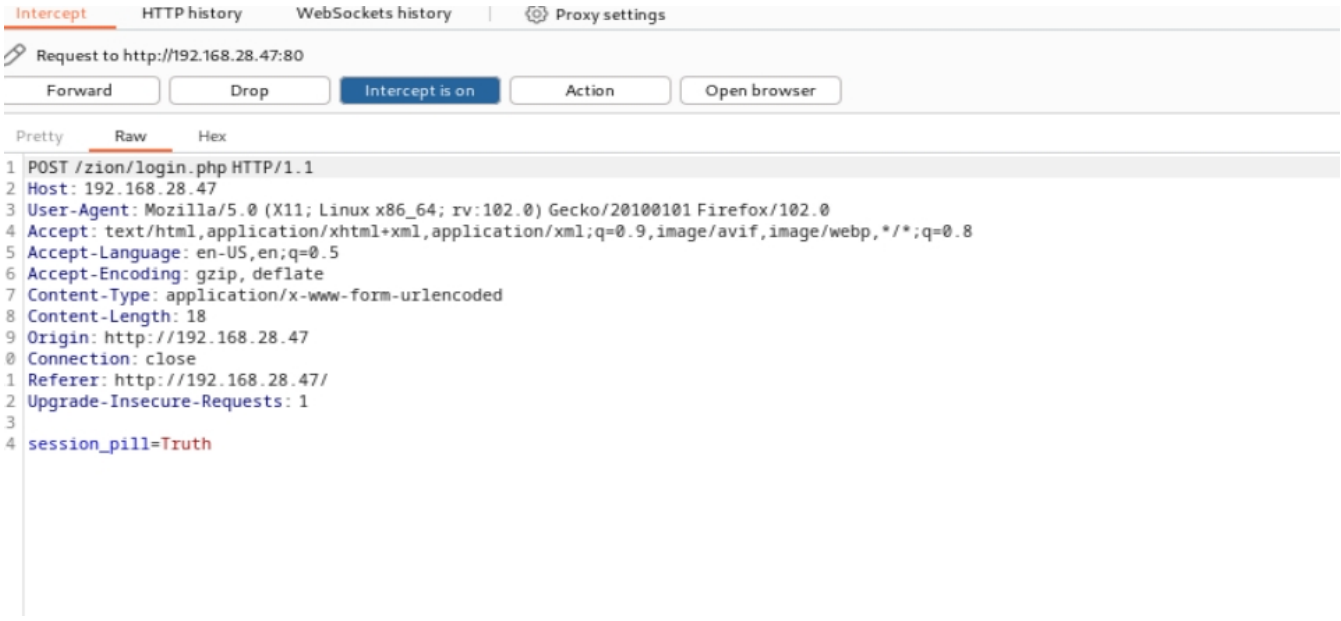
1.主页信息

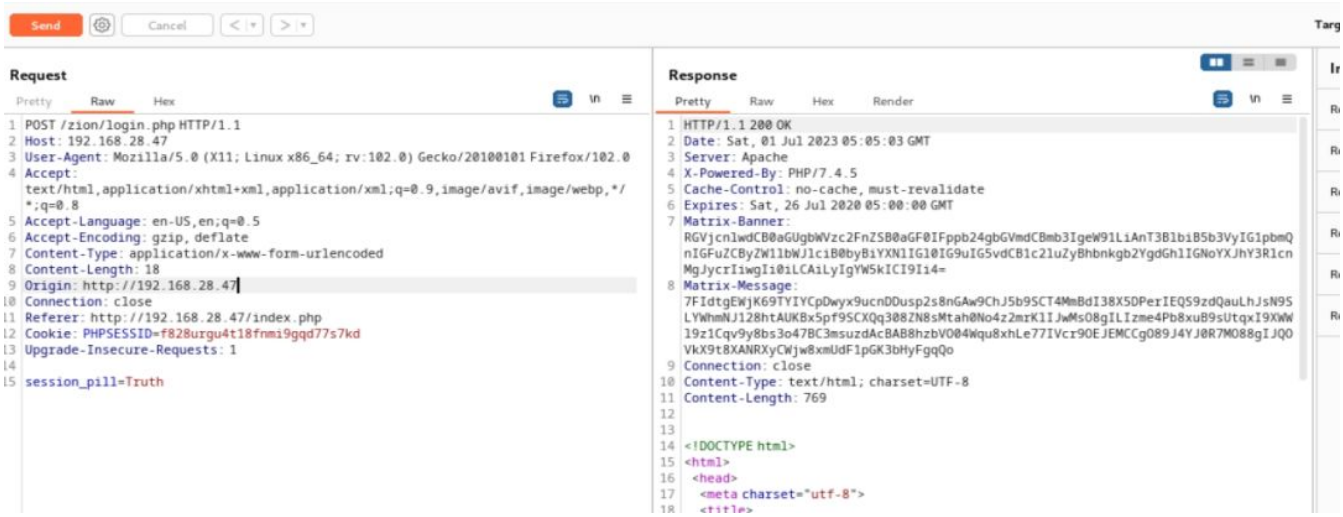


显然在这里除了一些对'real'的疑问外，还有一张背景图和两个按钮外就没有其他可用信息了，那我们开启burp suite开启抓包

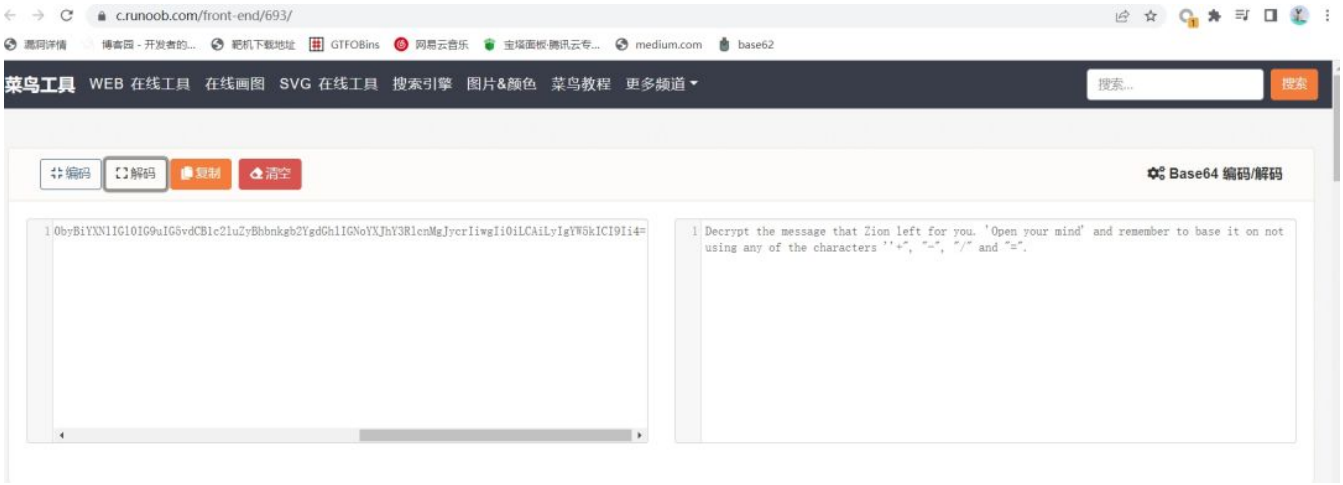
1).按钮的信息

当我们点击按钮后，burpsuite抓包得到这些

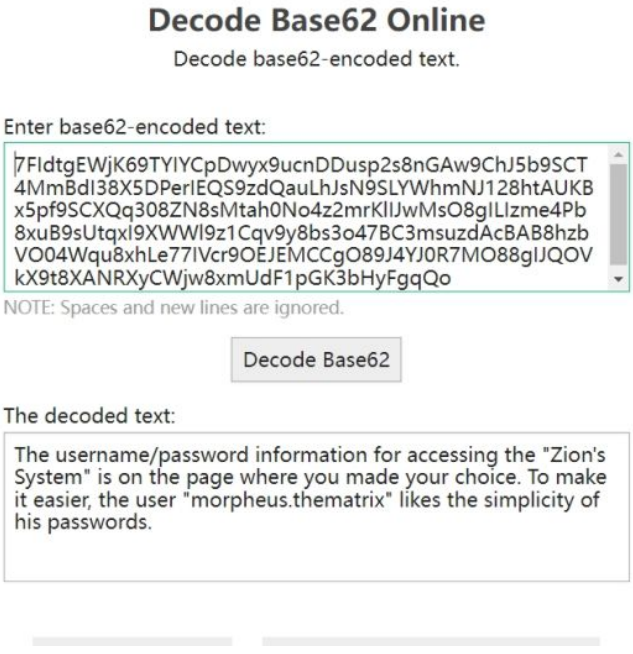




可以看出response是有密文的，分别是base64和base62，破译后，第一个是



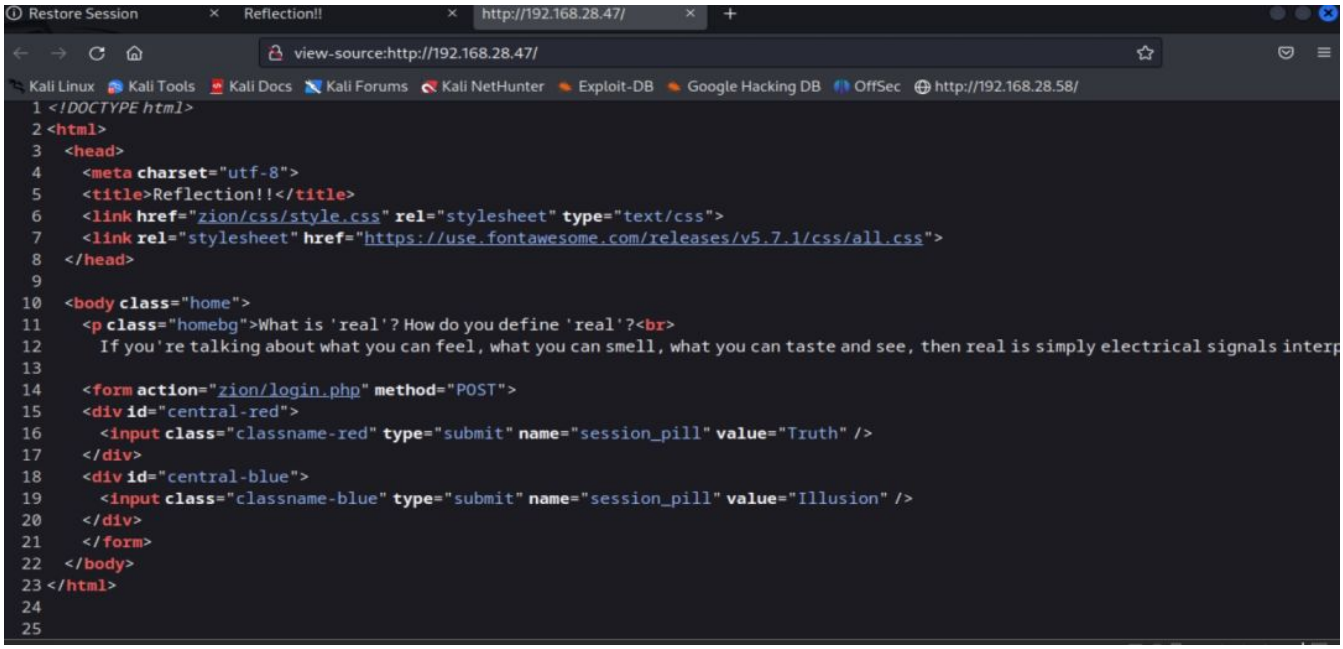
第二个是



从上述信息可知，一个用户名：morpheus.thematrix

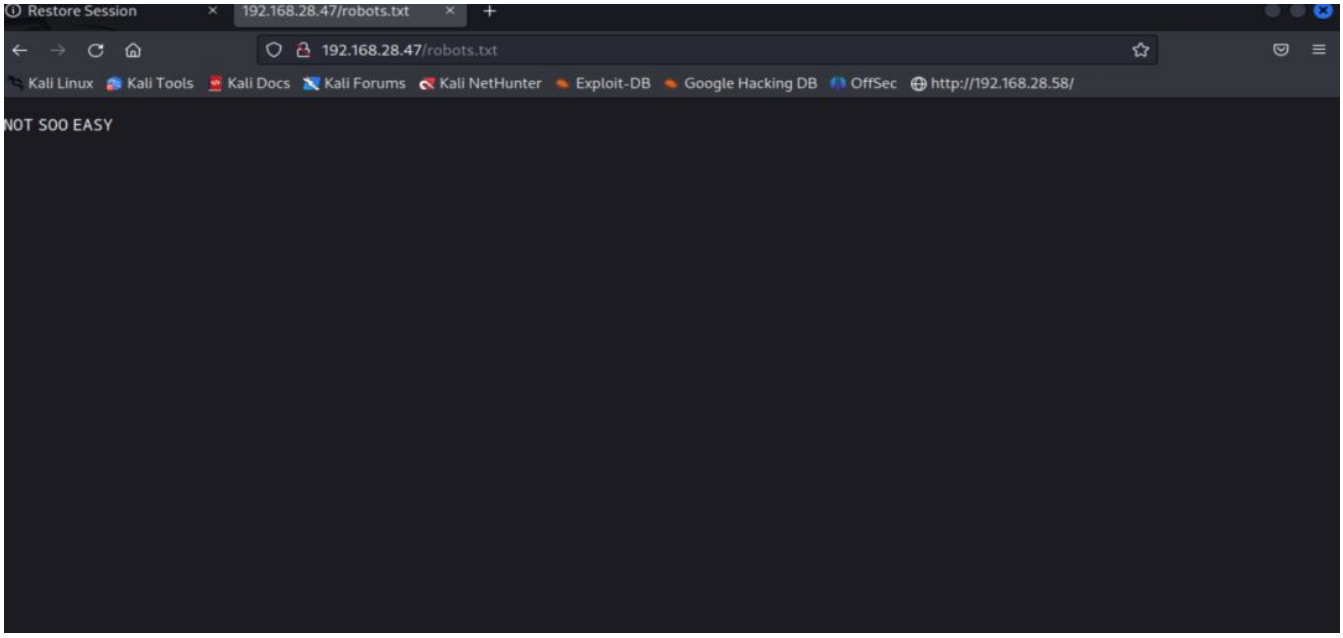
此外他说他设置的密码很简单，那么我们用cewl根据网站生成一个密码典：

2),检查源码



并没有发现令人感兴趣的东西。

2.robotas.txt文件



好吧，没东西，被嘲讽了。（robots文件也是这样）

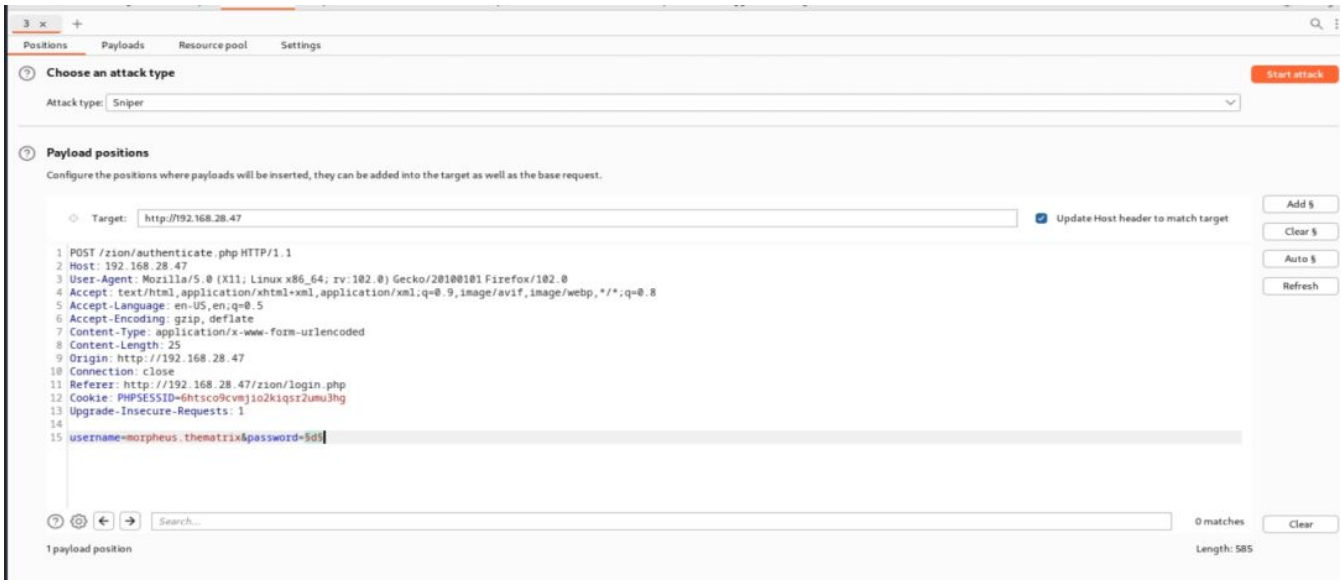
五.跟据已有信息采取措施

1).web密码爆破

现在我们有用户名和一个密码典，这里我采取使用burp suite爆破，当然hydra也不错。

(1).intruder配置

a.先把登录包抓到在发送到intruder模块

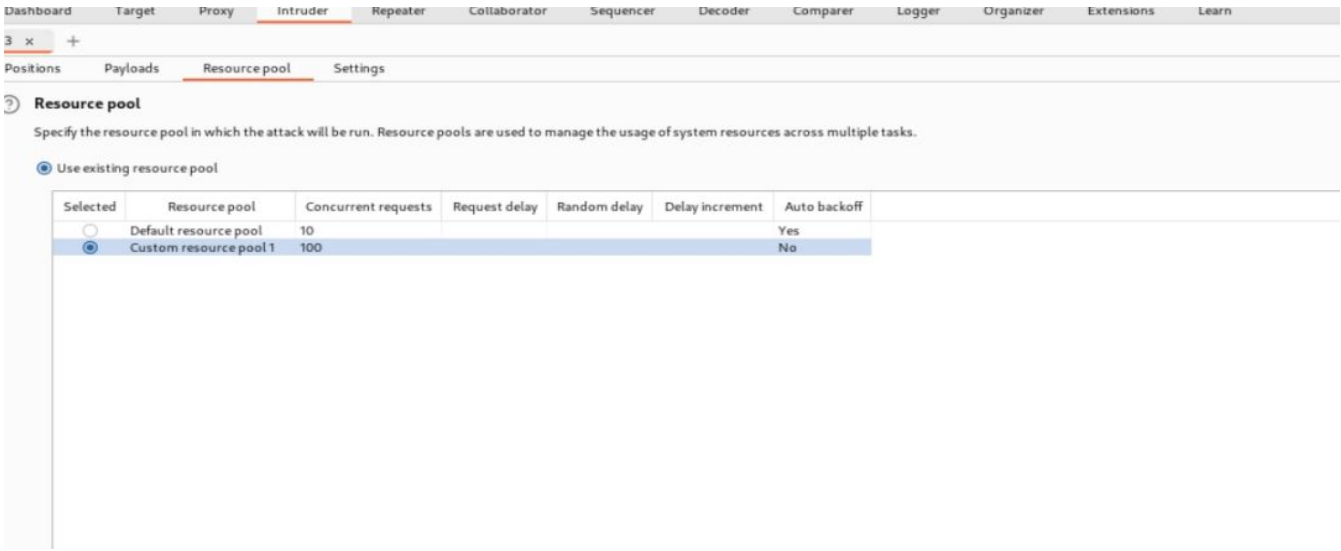


b.payloads配置

在payload setting【simple list】load我们的passwd字典

c.resource pool配置

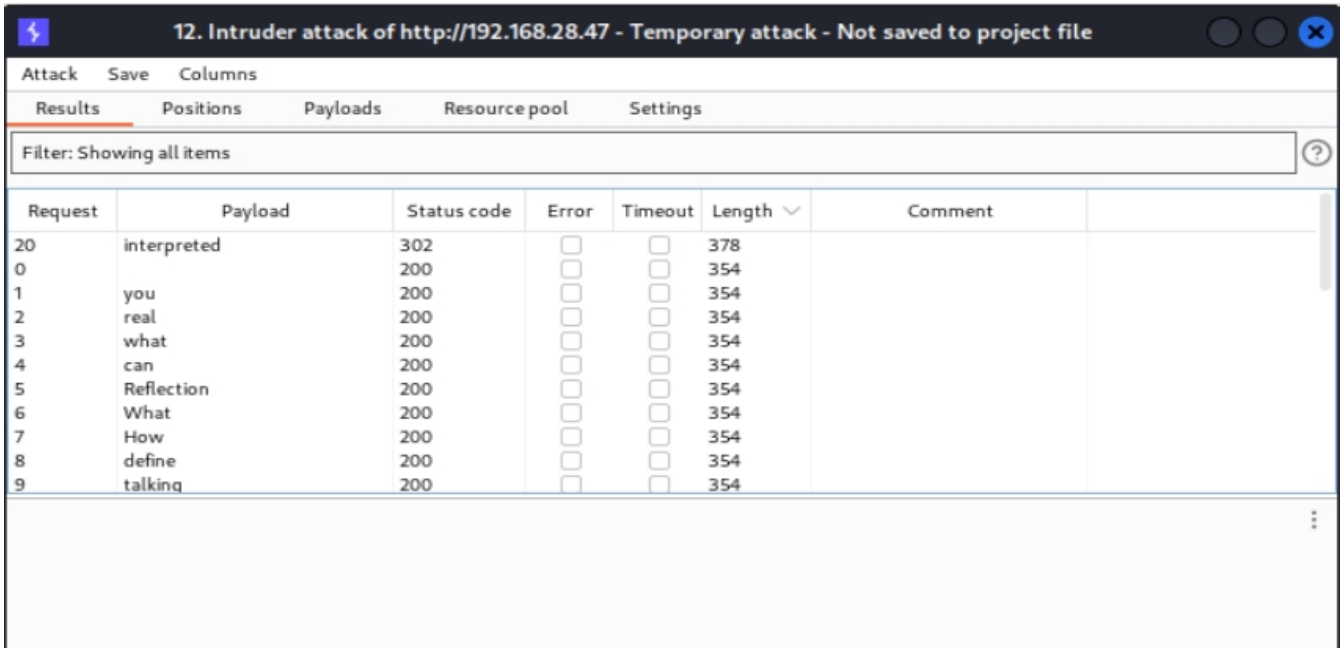
这个设置是用来配置每秒发包和延时发包的，那我配置每秒发包100（最大999），不延时。



d.开始爆破

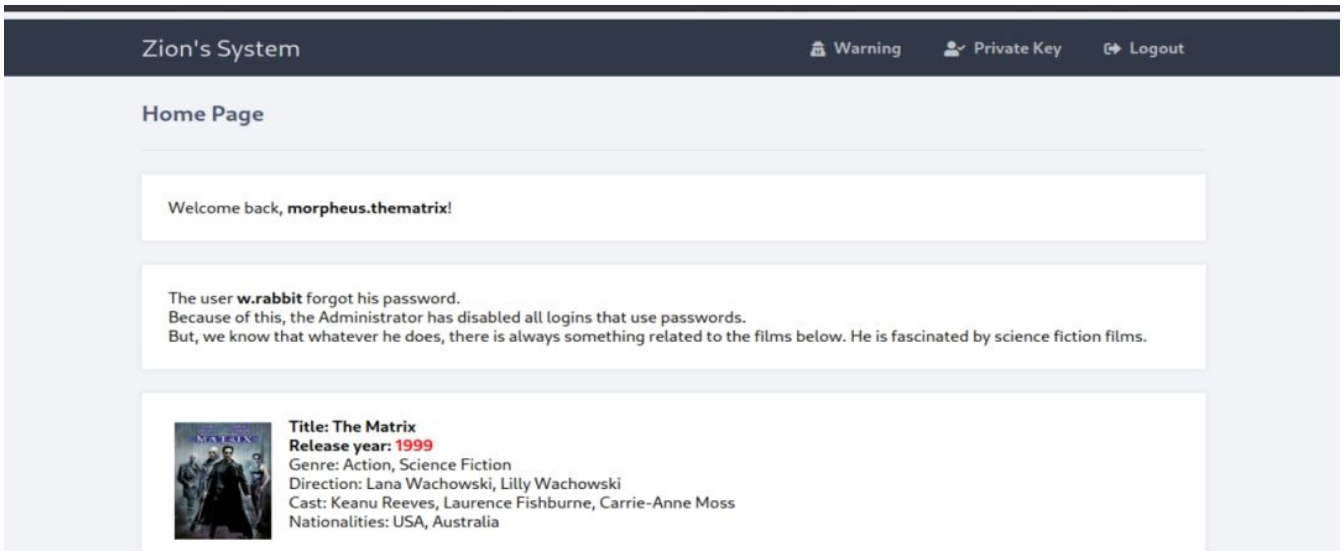
点击右上方红色按钮 start attack

e.得到密码

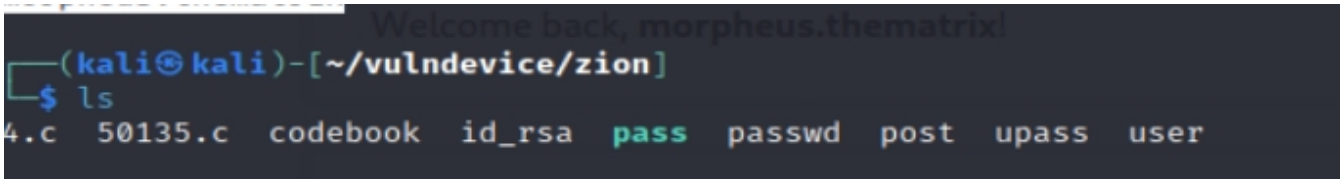


密码：interpreted

六.查看网站

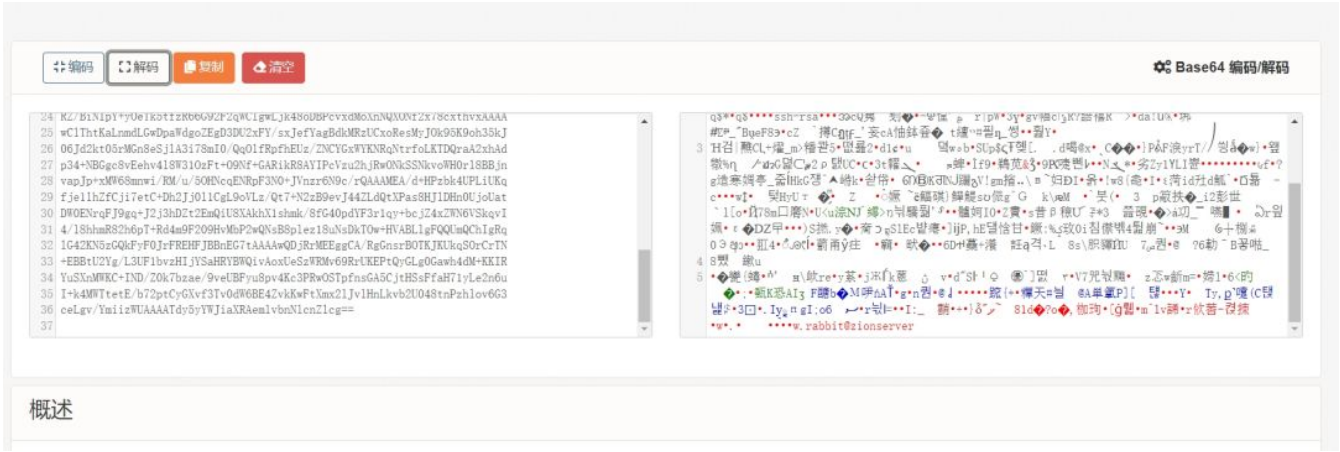


仔细研究，我们发现右上角有private key，欧克，那么我们可以用ssh私匙登录了。我把它复制下来，放在*idrsa* 。



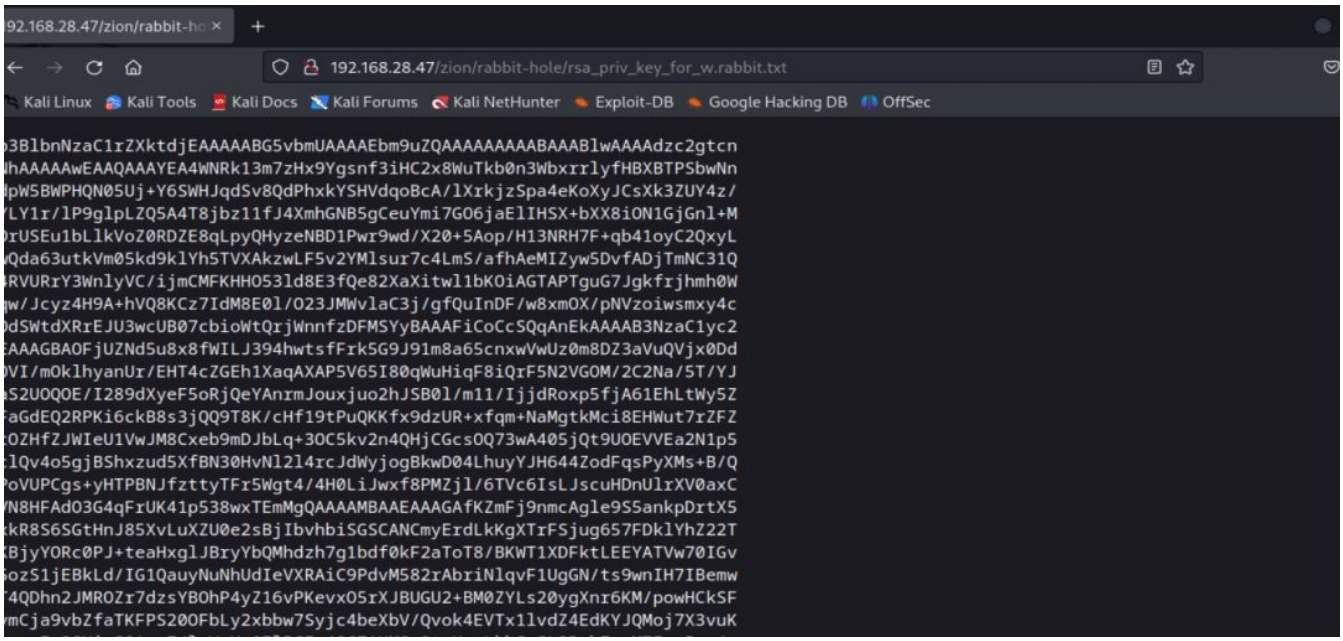
这里要注意ssh私匙格式，如果只复制了不行还要添加这些

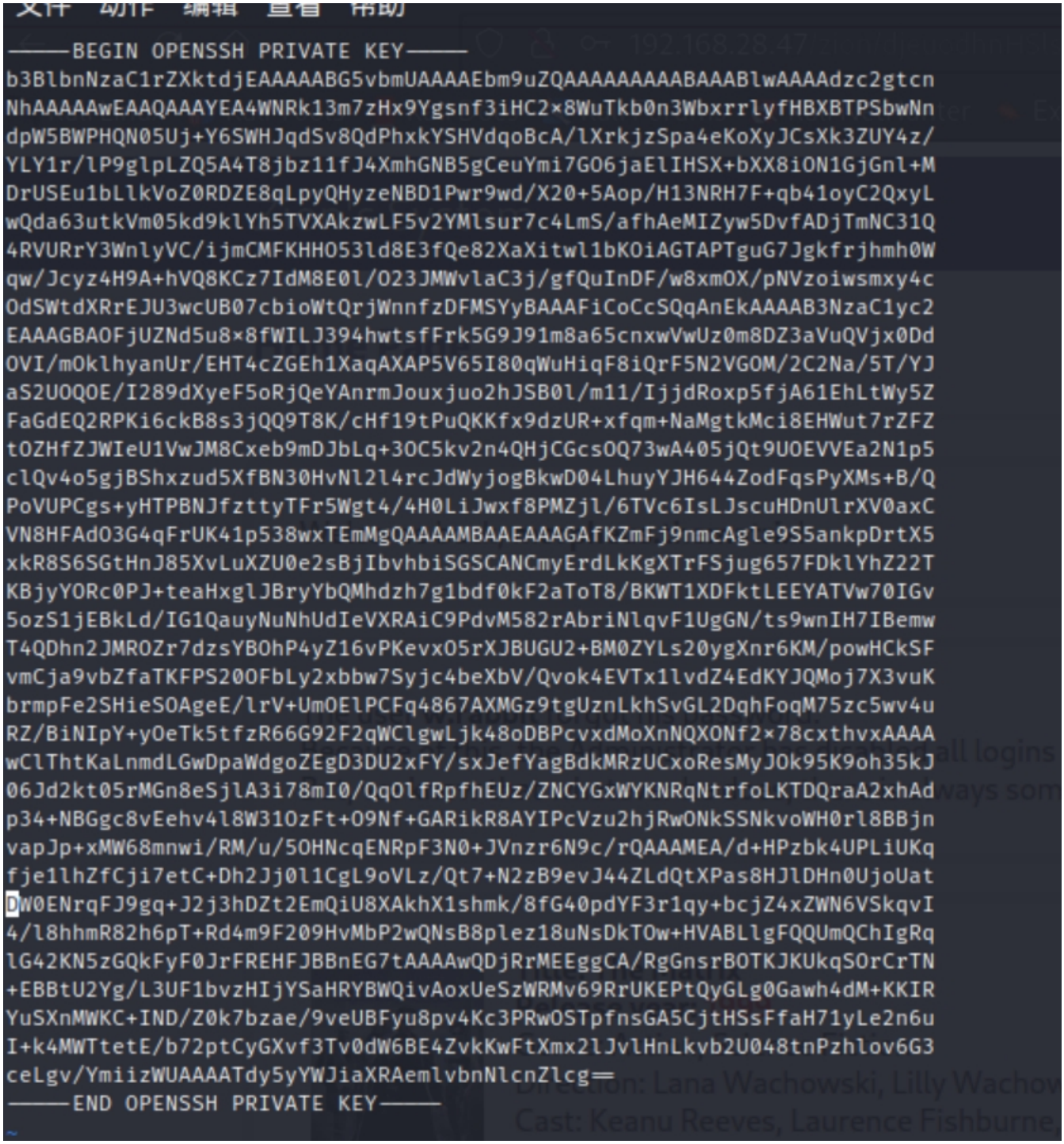
咱们用base64解码



发现用户是w.rabbit.

其实网址那有，但是你要有这个意识。





上面-----BEGIN　OPENSHH　PRIVATE KEY-----

下面-----END OPENSSH PRIVATE KEY-----

权限也只能设置为700，本用户使用，不然也会报错，权限过大。

七.ssh 登录

使用如下命令：`ssh w.rabbit@192.168.28.47 -i id_rsa`

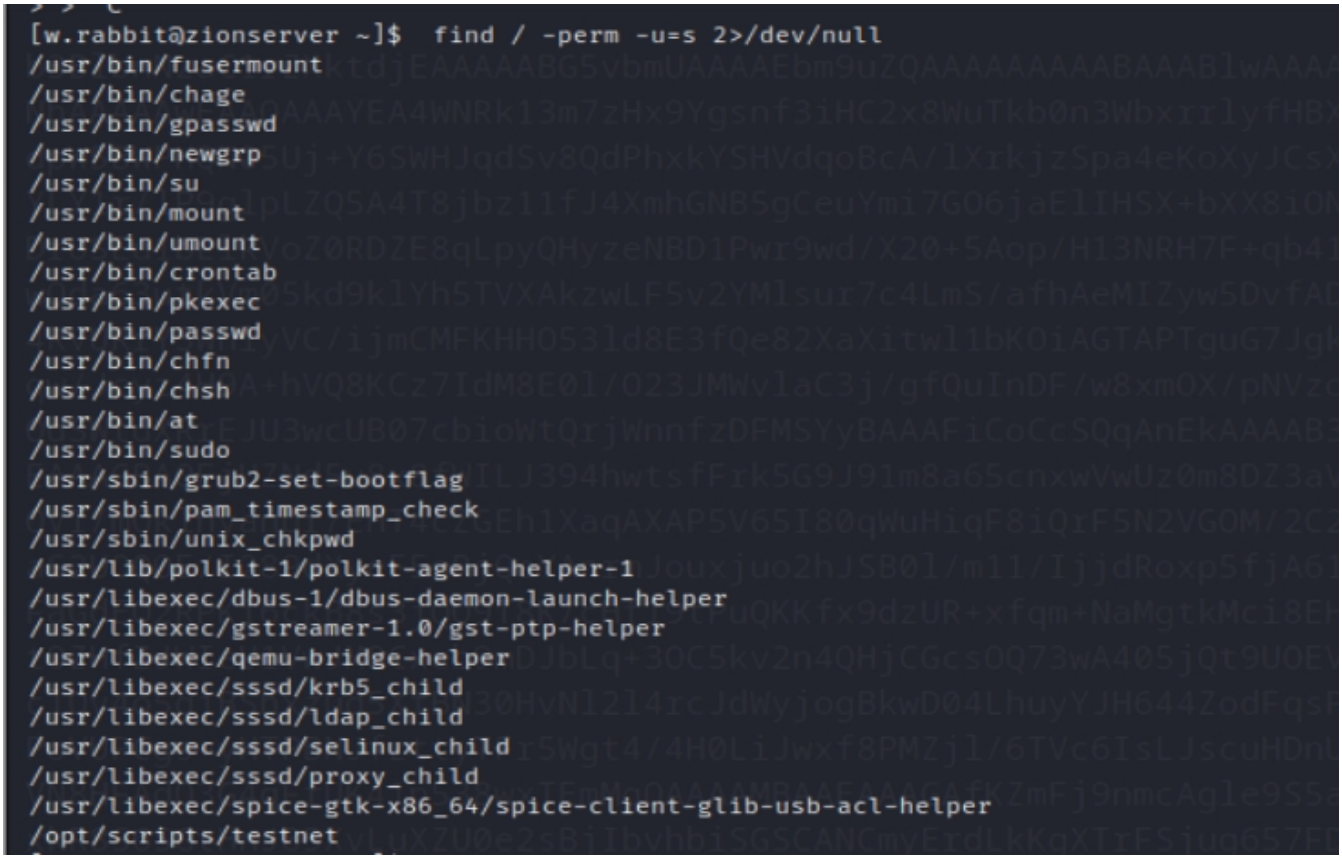
八.capture falg

查看当前目录下有啥，发现waring.txt

直接告诉我们flag在dozer用户目录下，

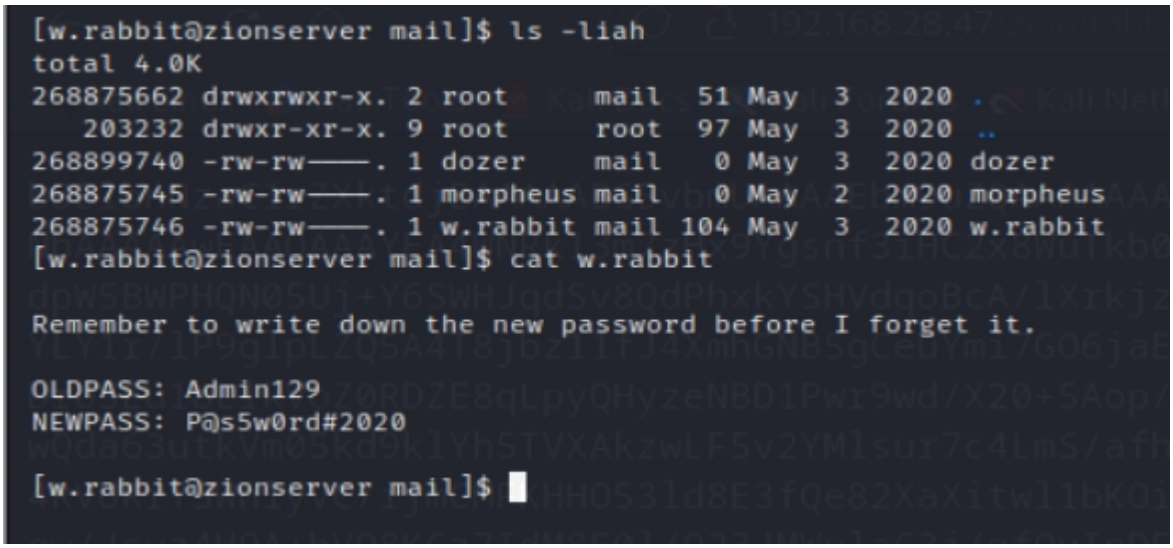
尝试`cd /home/dozer`,发现没有权限。

回到 / 下，尝试`sudo -l`看有没有sudo提权，结果是需要密码，只能先放下。在尝试`find / -perm -u=s -type f 2>/dev/null`,看有没有suid提权，结果



底下的`/opt/script/testnet`引起我的注意，但是用查看权限是744，里面的内容也没有重要内容，只好作罢。

那么我进入/var 目录下。看看有没有有用的信息，发现了mail



我们得到了w.rabbit的密码。

在尝试`sudo -l`,输入密码，发现

```
文件  动作  编辑  查看  帮助
[w.rabbit@zionserver mail]$ ls -liah
total 4.0K
268875662 drwxrwxr-x. 2 root     mail  51 May  3  2020 .
   203232 drwxr-xr-x. 9 root     root  97 May  3  2020 ..
268899740 -rw-rw----. 1 dozer    mail   0 May  3  2020 dozer
268875745 -rw-rw----. 1 morpheus mail   0 May  2  2020 morpheus
268875746 -rw-rw----. 1 w.rabbit mail 104 May  3  2020 w.rabbit
[w.rabbit@zionserver mail]$ cat w.rabbit

Remember to write down the new password before I forget it.

OLDPASS: Admin129
NEWPASS: P@s5w0rd#2020

[w.rabbit@zionserver mail]$ sudo -l
[sudo] password for w.rabbit:
Sorry, try again.
[sudo] password for w.rabbit:
User w.rabbit may run the following commands on zionserver:
    (dozer) /bin/cp
[w.rabbit@zionserver mail]$
```

我们可以一dozer的身份执行，/bin/cp，熟悉 **cp**命令的应该知道**--no-preserve**这个参数，这里不做过多解释，可自行百度。那么我们执行`sudo -u dozer /bin/cp --no-preserve=all /home/dozer/flag.txt /tmp/flag.txt`

```
[w.rabbit@zionserver tmp]$ cat flag4.txt

__      __   _
\ \        / /__| | ___ ___  _ __ ___   ___
 \ \  /\  / / _ \ |/ __/ _ \| '_ ` _ \ / _ \
  \ \/  \/ /  __/ | (_| (_) | | | | | |  __/
   \_/\_/ \___|_|\___\___/|_| |_| |_|\___|

 _____   _____ _           _____
|_   _| |_   _| |__   ___|  ___|__  _ __
  | |/ _ \| | '_ \ / _ \ |_ / _ \| '_ \
  | | (_) | | | | |  __/ _| (_) | | | |
  |_|\___/|_| |_| |_|\___|_|\___/|_| |_|

_____________________________________________
Congratulations!!

Hope you enjoyed Zion:1. Just wanted to send a big thanks out there
to all those who have privied feedback, and who have taken time to
complete these little challenges.

If you enjoyed this CTF, send me a tweet via @mrhenrike

So, take your award:

flag = challUG{Th1nk_0u7_0f_th3_60x}
```

拿到flag。