**Hacking**

**ético**

# 

### 

[**Very easy**](#_ncqwc238sads) **1**

[**Reconocimiento**](#_c3ekxf3z7unr) **2**

|  |
| --- |
| Reconocimiento |
| Máquinas en la red |
|  |
| Análisis de las máquinas |
|  |
|  |
| Análisis de máquina víctima |
|  |
| Información sobre el servicio web |
|  |
| Flag 1 |
|  |
| fuzzing |
| **gobuster dir -u http://$ip -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt -x php,txt,html,jpg,js -x '404,403' > dirbu\_dir** |
|  |
| **gobuster dir -u http://$ip -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,html,jpg,js -x '404,403' > dirbu\_dirlis2** |
|  |
| Páginas |
| assets |
| **http://10.0.2.15/assets/** |
|  |
| **admin\_area** |
| **flag 2** |
|  |
| **uploaded\_files** |
|  |
| **robots.txt** |
|  |
| **Index - login.php** |
|  |
| Con las credenciales 1 que ya tenemos podemos registrarnos |
|  |
| Tenemos un sistema para subir archivos y nos recuerda a una ruta en la que parece que nos da acceso a archivos del servidor. |
| Preparamos una webshell, kali nos facilita algunas |
|  |
| La personalizamos con nuestra ip |
|  |
| Subimos el archivo desde el index |
|  |
| Escuchamos por nc a la futura webshell |
|  |
| Lo ejecutamos desde /uploaded\_files |
|  |
| Resultado |
|  |
| Listamos usuarios |
| **cat /etc/passwd | grep -v nologin | grep -v false** |
|  |
| Usuario demouser |
|  |
| * 1 es un archivo de configuración de apache * .hide |
| Credenciales |
|  |
| El flag 4 es: {7845658974123568974185412} |
|  |
| **su** no necesita ser ejecutado como root así que probamos cambiar de usuarios |
|  |
| **Usuario root** |
|  |
|  |

| Nº | usuarios | Contraseñas |
| --- | --- | --- |
| 1 | admin | 3v1l\_H@ck3r |
| 2 | demouser | 3vilH@ksor |
| 3 | root | 3vilH@ksor |