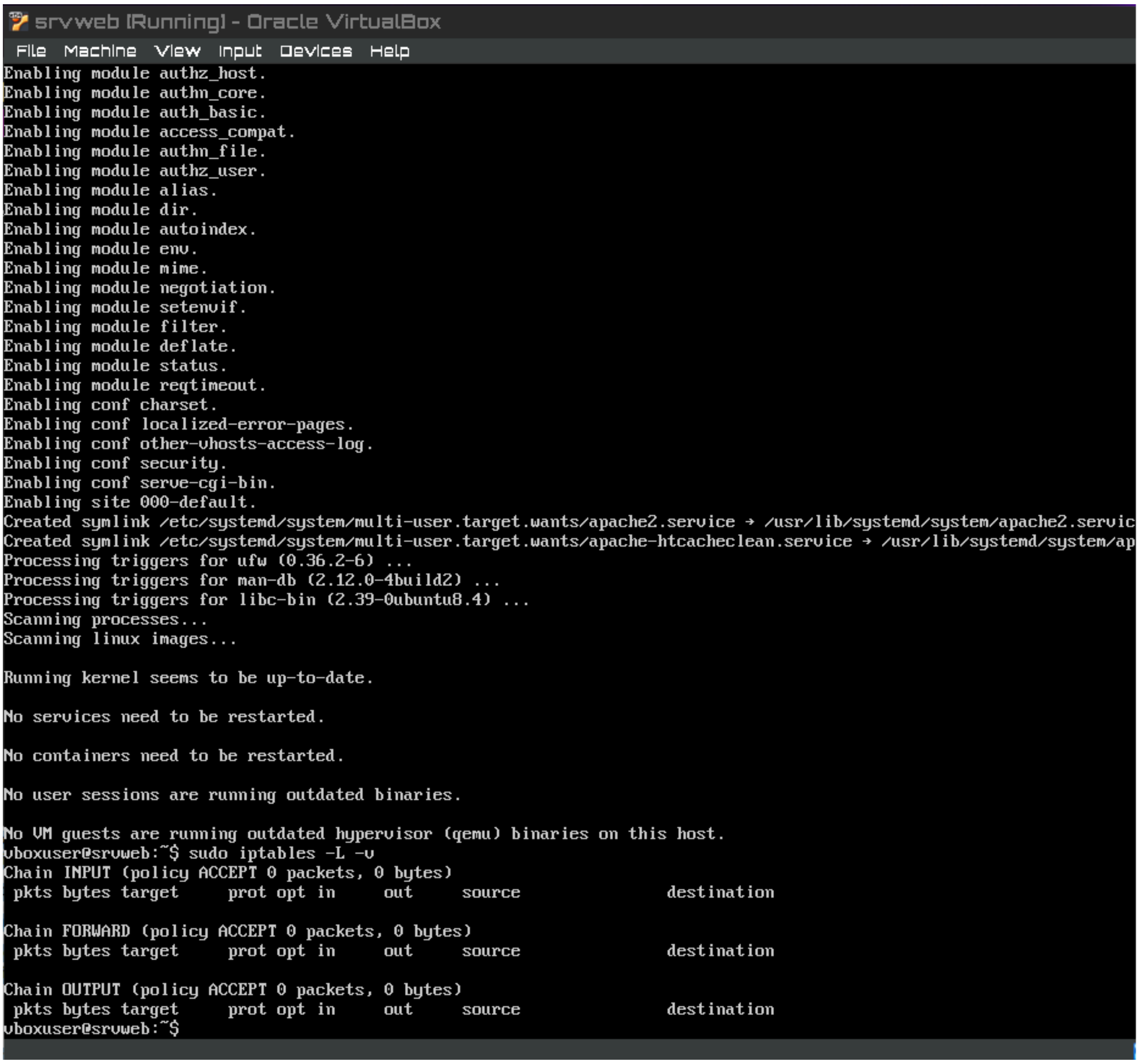
Configuración de reglas iptables para servidor web seguro (Ubuntu Server 22.04)

Pasos realizados:

1. Creación de VM: Se creó una máquina virtual llamada srvweb con Ubuntu Server 22.04.
2. Instalación de Apache2: Se instaló el servidor web con sudo apt install apache2.
3. Verificación inicial de iptables: Se comprobó que no había reglas activas (iptables -L -v).
4. Limpieza de reglas previas: Se ejecutaron comandos iptables -F, -X, etc.
5. Establecimiento de políticas predeterminadas:
    - INPUT y FORWARD: DROP
    - OUTPUT: ACCEPT
6. Reglas añadidas:
    - Permitir puertos 80 y 443 (HTTP/HTTPS).
    - Permitir tráfico ESTABLISHED,RELATED.
7. Guardado persistente: Se instaló iptables-persistent y se guardaron las reglas en /etc/iptables/rules.v4.
8. Verificación final: Se comprobó la tabla de reglas (iptables -L -v).

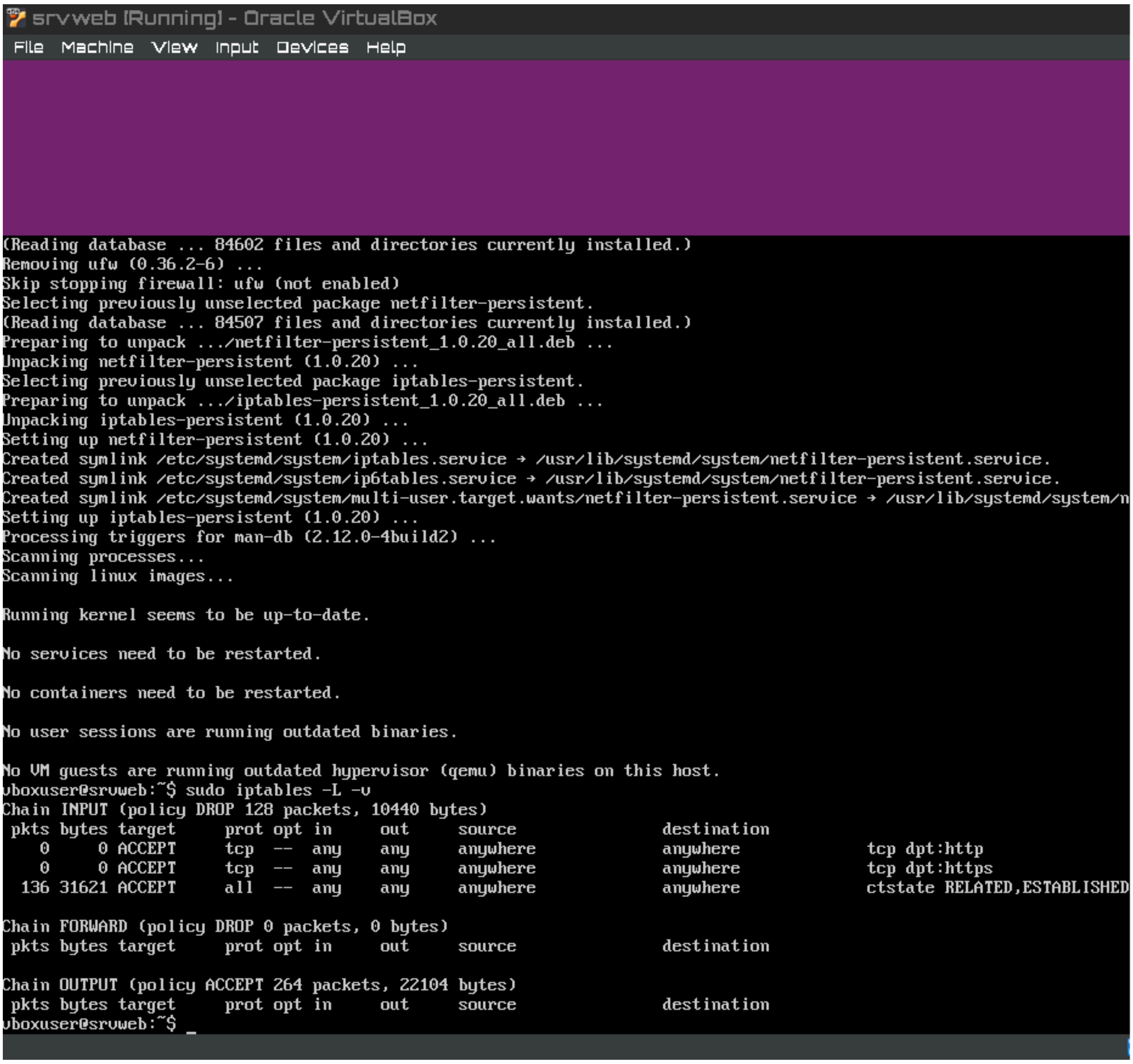
Capturas aportadas:

- Estado inicial de iptables.


srvweb [Running] - Oracle VirtualBox
File Machine View Input Devices Help

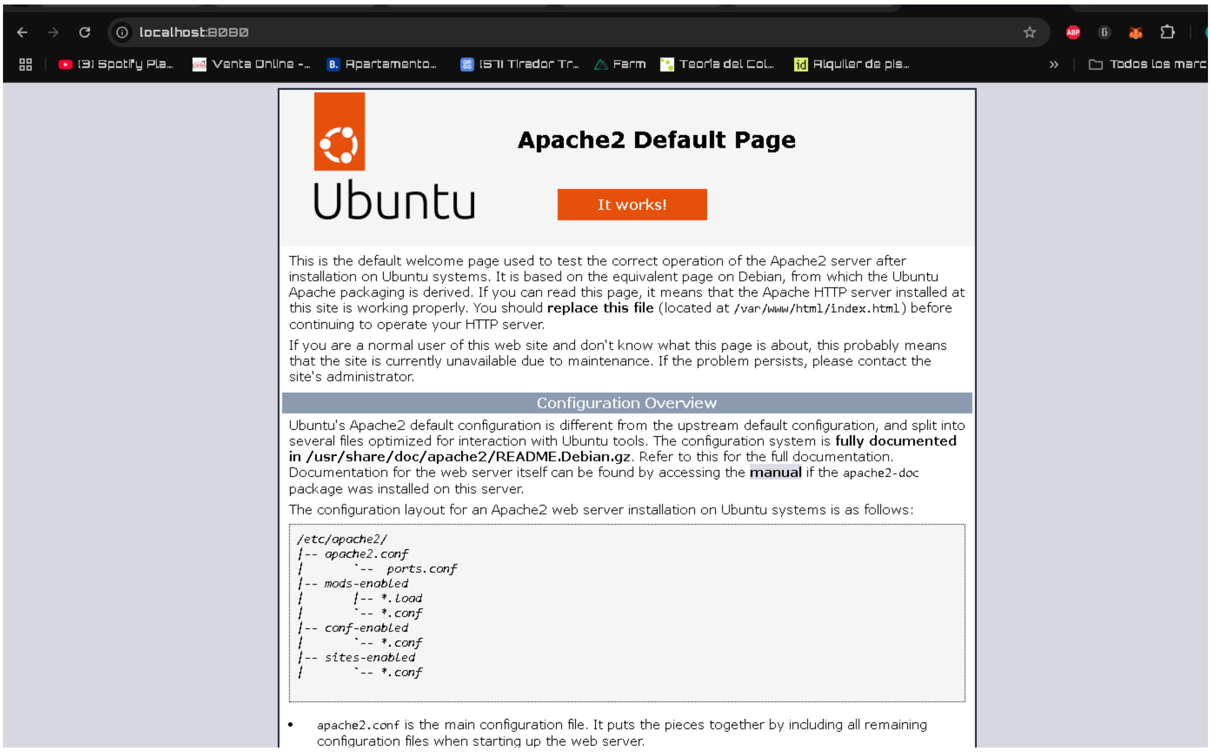
```
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.servic
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/ap
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@srvweb:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
vboxuser@srvweb:~$
```

- Reglas aplicadas tras la configuración.



```
(Reading database ... 84602 files and directories currently installed.)
Removing ufw (0.36.2-6) ...
Skip stopping firewall: ufw (not enabled)
Selecting previously unselected package netfilter-persistent.
(Reading database ... 84507 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.20_all.deb ...
Unpacking netfilter-persistent (1.0.20) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.20_all.deb ...
Unpacking iptables-persistent (1.0.20) ...
Setting up netfilter-persistent (1.0.20) ...
Created symlink /etc/systemd/system/iptables.service → /usr/lib/systemd/system/netfilter-persistent.service.
Created symlink /etc/systemd/system/ip6tables.service → /usr/lib/systemd/system/netfilter-persistent.service.
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /usr/lib/systemd/system/n
Setting up iptables-persistent (1.0.20) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@srvweb:~$ sudo iptables -L -v
Chain INPUT (policy DROP 128 packets, 10440 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
  136 31621 ACCEPT     all  --  any    any     anywhere             anywhere             ctstate RELATED,ESTABLISHED

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 264 packets, 22104 bytes)
 pkts bytes target     prot opt in     out     source               destination
vboxuser@srvweb:~$ _
```

- Página de Apache accesible desde navegador (localhost:8080).



Apache2 Default Page

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

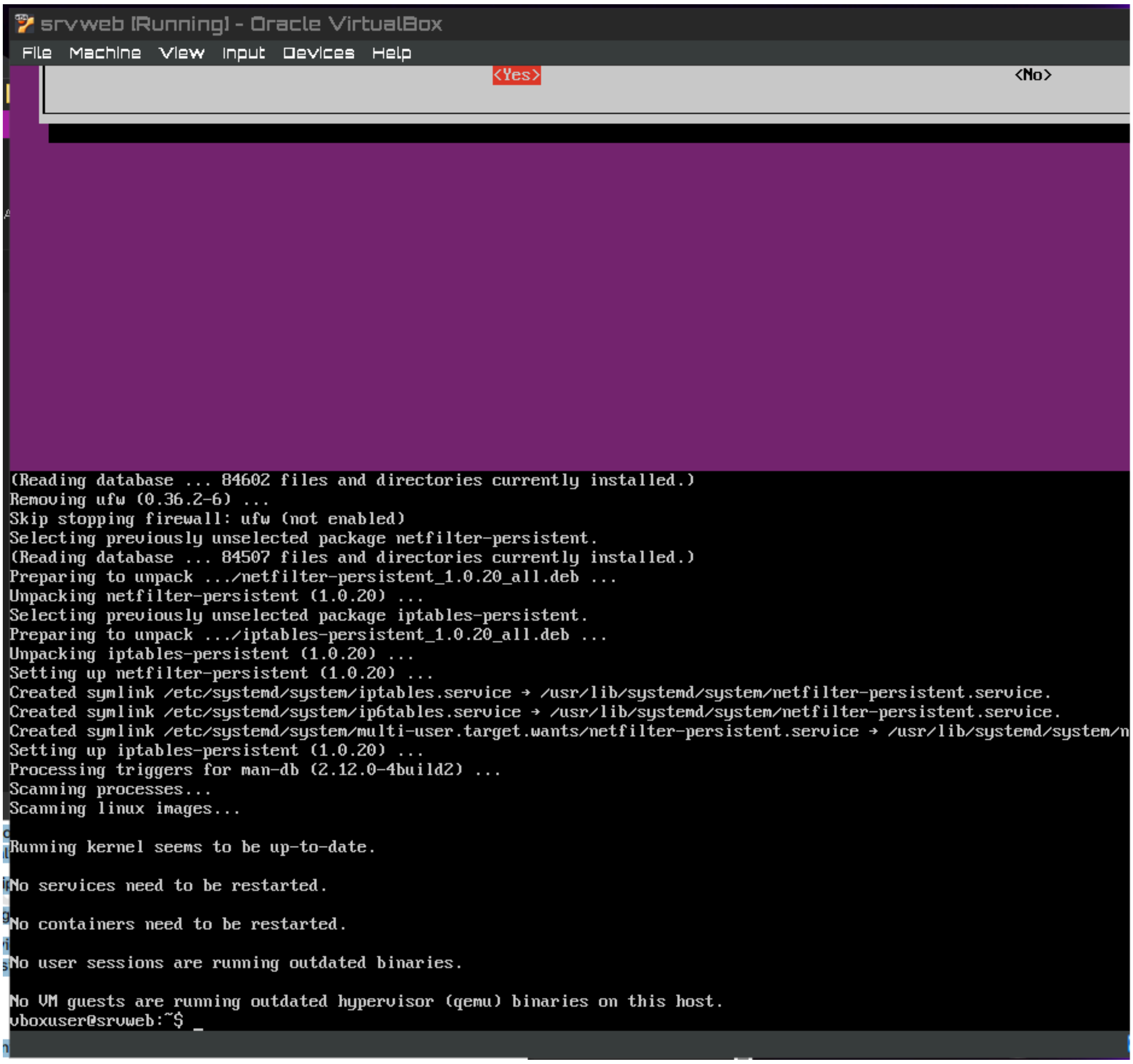
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

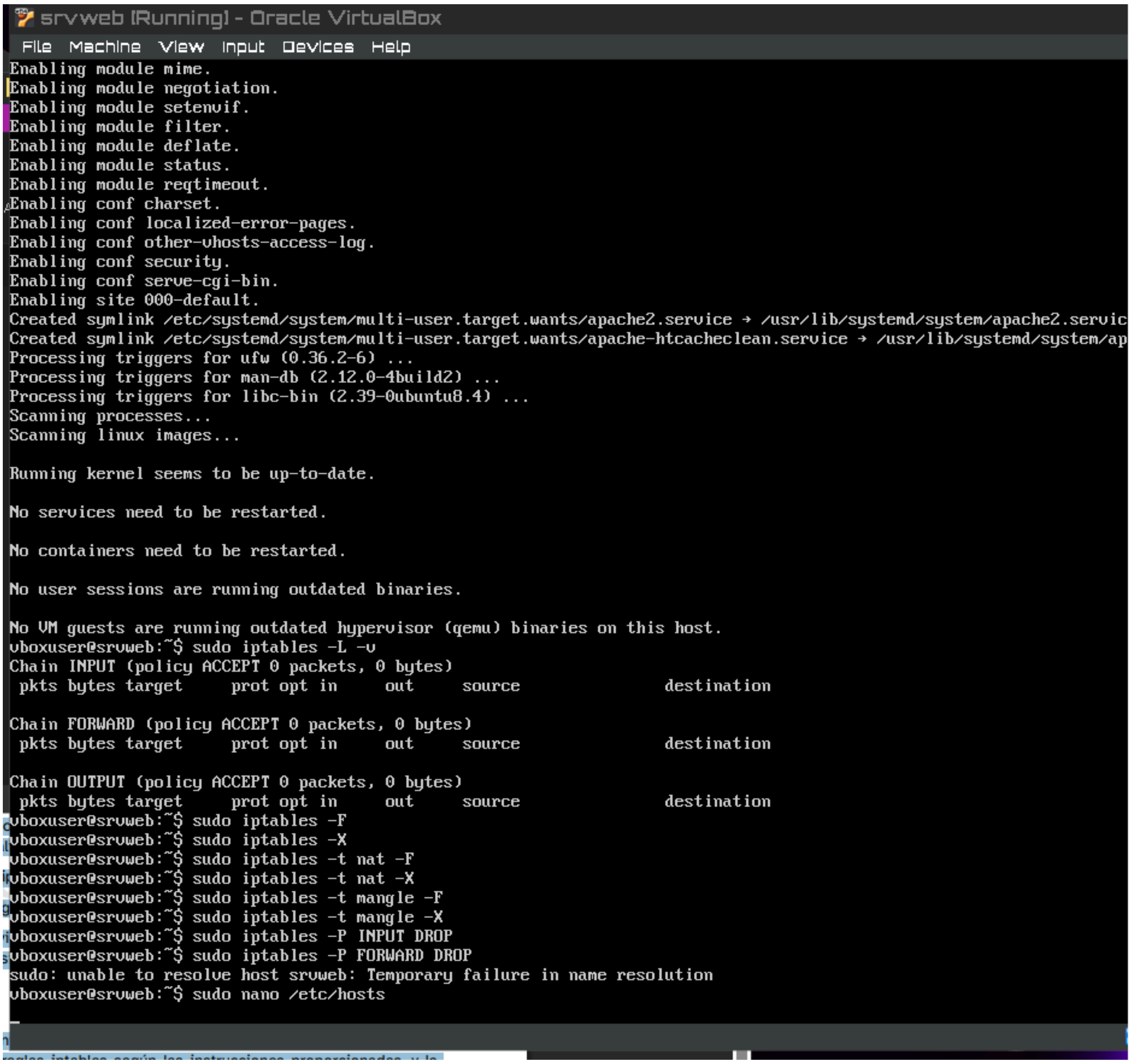
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Problemas encontrados y soluciones aplicadas:

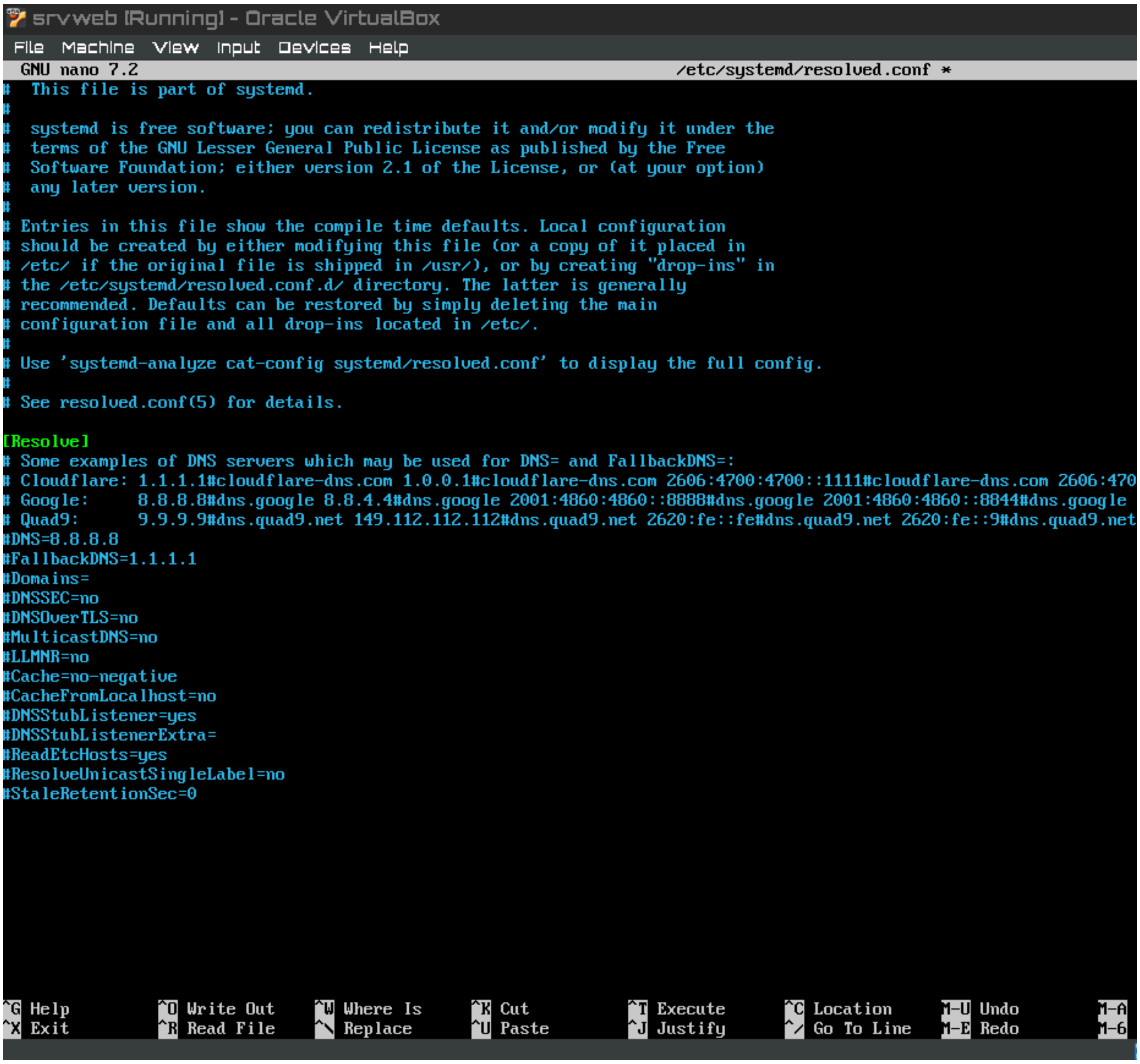
Problema	Solución
sudo: unable to resolve host srvweb	Se corrigió la entrada en /etc/hosts añadiendo 127.0.1.1 srvweb.
Error DNS al instalar paquetes (Temporary failure resolving 'archive.ubuntu.com')	Se editaron los DNS en /etc/systemd/resolved.conf, añadiendo DNS=8.8.8.8 y FallbackDNS=1.1.1.1, reiniciando systemd-resolved.
Al cambiar a adaptador puente, la VM se congelaba	Se restauró NAT y se usó reenvío de puertos para redirigir localhost:8080 al puerto 80 de la VM.



```
(Reading database ... 84602 files and directories currently installed.)
Removing ufw (0.36.2-6) ...
Skip stopping firewall: ufw (not enabled)
Selecting previously unselected package netfilter-persistent.
(Reading database ... 84507 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.20_all.deb ...
Unpacking netfilter-persistent (1.0.20) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.20_all.deb ...
Unpacking iptables-persistent (1.0.20) ...
Setting up netfilter-persistent (1.0.20) ...
Created symlink /etc/systemd/system/iptables.service → /usr/lib/systemd/system/netfilter-persistent.service.
Created symlink /etc/systemd/system/ip6tables.service → /usr/lib/systemd/system/netfilter-persistent.service.
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /usr/lib/systemd/system/n
Setting up iptables-persistent (1.0.20) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@srvweb:~$ _
```


srvweb [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.servic
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/ap
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@srvweb:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
vboxuser@srvweb:~$ sudo iptables -F
vboxuser@srvweb:~$ sudo iptables -X
vboxuser@srvweb:~$ sudo iptables -t nat -F
vboxuser@srvweb:~$ sudo iptables -t nat -X
vboxuser@srvweb:~$ sudo iptables -t mangle -F
vboxuser@srvweb:~$ sudo iptables -t mangle -X
vboxuser@srvweb:~$ sudo iptables -P INPUT DROP
vboxuser@srvweb:~$ sudo iptables -P FORWARD DROP
sudo: unable to resolve host srvweb: Temporary failure in name resolution
vboxuser@srvweb:~$ sudo nano /etc/hosts
_
```



```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it under the
#  terms of the GNU Lesser General Public License as published by the Free
#  Software Foundation; either version 2.1 of the License, or (at your option)
#  any later version.
#
# Entries in this file show the compile time defaults. Local configuration
# should be created by either modifying this file (or a copy of it placed in
# /etc/ if the original file is shipped in /usr/), or by creating "drop-ins" in
# the /etc/systemd/resolved.conf.d/ directory. The latter is generally
# recommended. Defaults can be restored by simply deleting the main
# configuration file and all drop-ins located in /etc/.
#
# Use 'systemd-analyze cat-config systemd/resolved.conf' to display the full config.
#
# See resolved.conf(5) for details.

[Resolve]
# Some examples of DNS servers which may be used for DNS= and FallbackDNS=:
# Cloudflare: 1.1.1.1#cloudflare-dns.com 1.0.0.1#cloudflare-dns.com 2606:4700:4700::1111#cloudflare-dns.com 2606:470
# Google:     8.8.8.8#dns.google 8.8.4.4#dns.google 2001:4860:4860::8888#dns.google 2001:4860:4860::8844#dns.google
# Quad9:      9.9.9.9#dns.quad9.net 149.112.112.112#dns.quad9.net 2620:fe::fe#dns.quad9.net 2620:fe::9#dns.quad9.net
#DNS=8.8.8.8
#FallbackDNS=1.1.1.1
#Domains=
#DNSSEC=no
#DNSOverTLS=no
#MulticastDNS=no
#LLMNR=no
#Cache=no-negative
#CacheFromLocalhost=no
#DNSStubListener=yes
#DNSStubListenerExtra=
#ReadEtcHosts=yes
#ResolveUnicastSingleLabel=no
#StaleRetentionSec=0
```

Bibliografía

1. Configuración básica de iptables

The Debian Administrator's Handbook. (n.d.). *Setting up a Firewall with iptables*. Retrieved June 14, 2025, from https://debian-handbook.info/browse/stable/sect.firewall.html

---

2.Ubuntu Wiki Network

https://help.ubuntu.com/community/Network

3. Instalación y uso de Apache2 en Ubuntu

Apache Software Foundation. (2022). *Apache HTTP Server Documentation*. Retrieved June 14, 2025, from https://httpd.apache.org/docs/