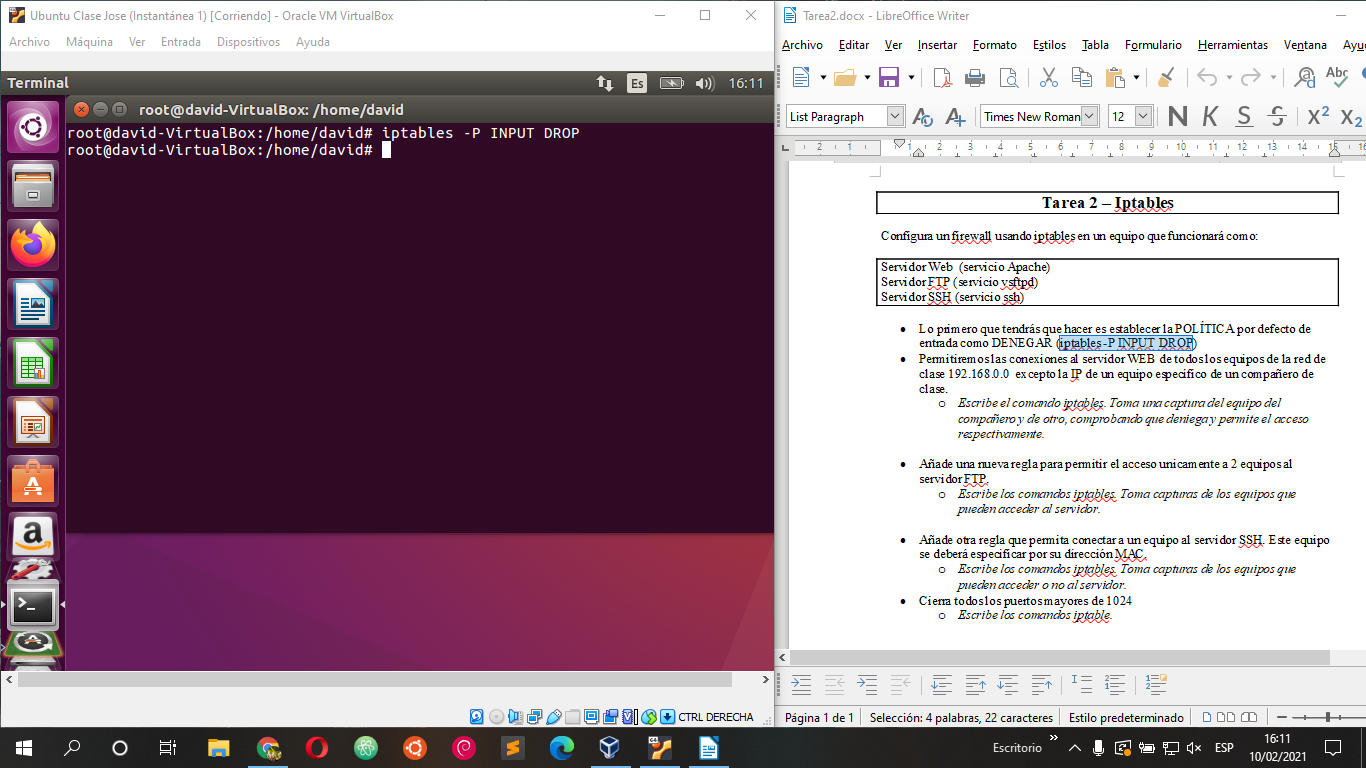
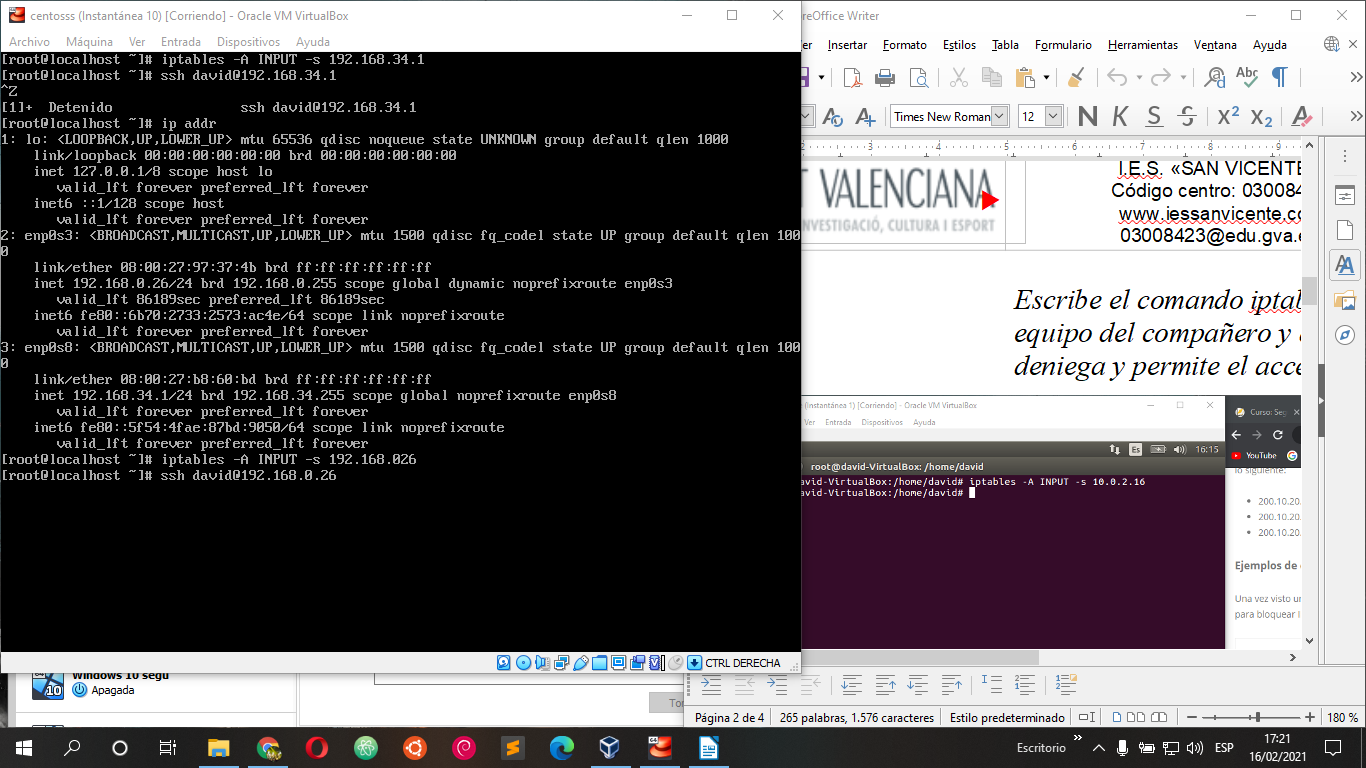
**Tarea 2 – Iptables**

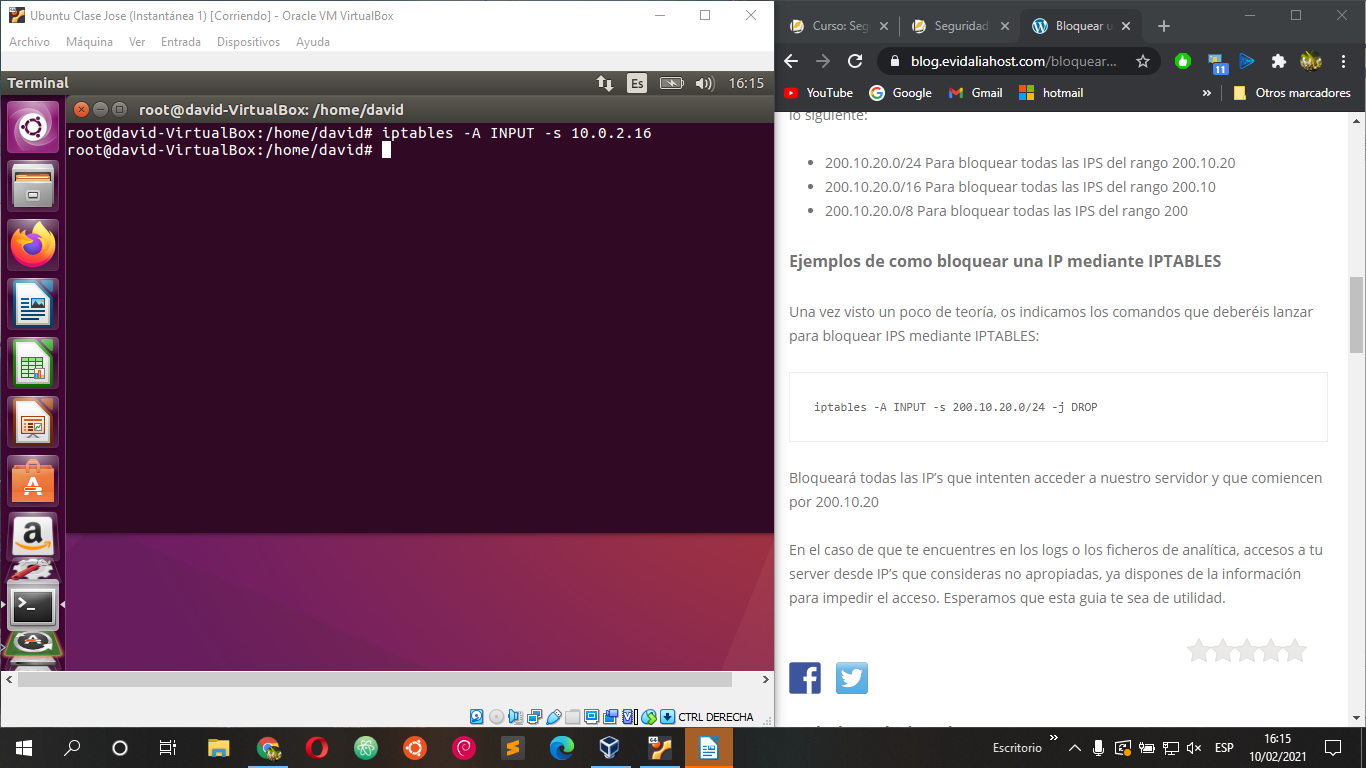
Configura un firewall usando iptables en un equipo que funcionará como:

Servidor Web (servicio Apache)  
Servidor FTP (servicio vsftpd)  
Servidor SSH (servicio ssh)

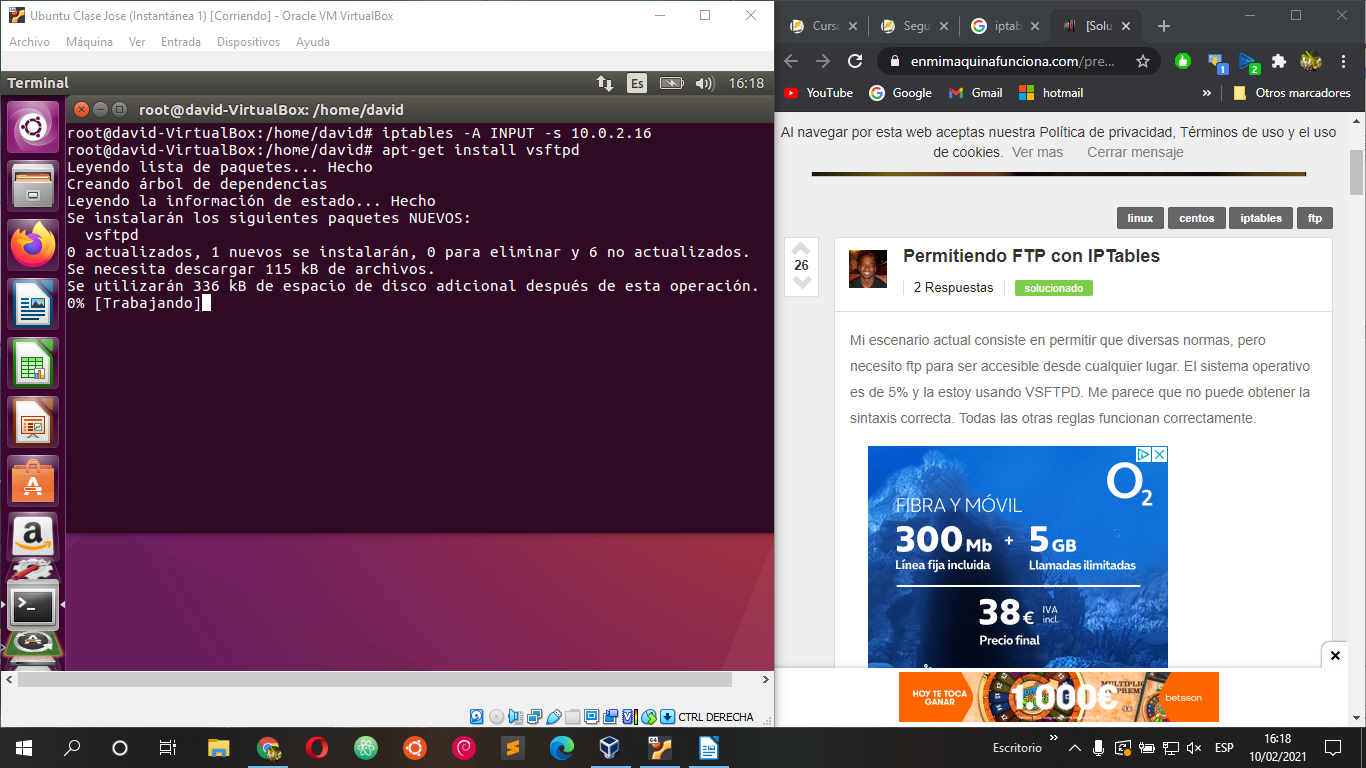
* Lo primero que tendrás que hacer es establecer la POLÍTICA por defecto de entrada como DENEGAR (iptables -P INPUT DROP)

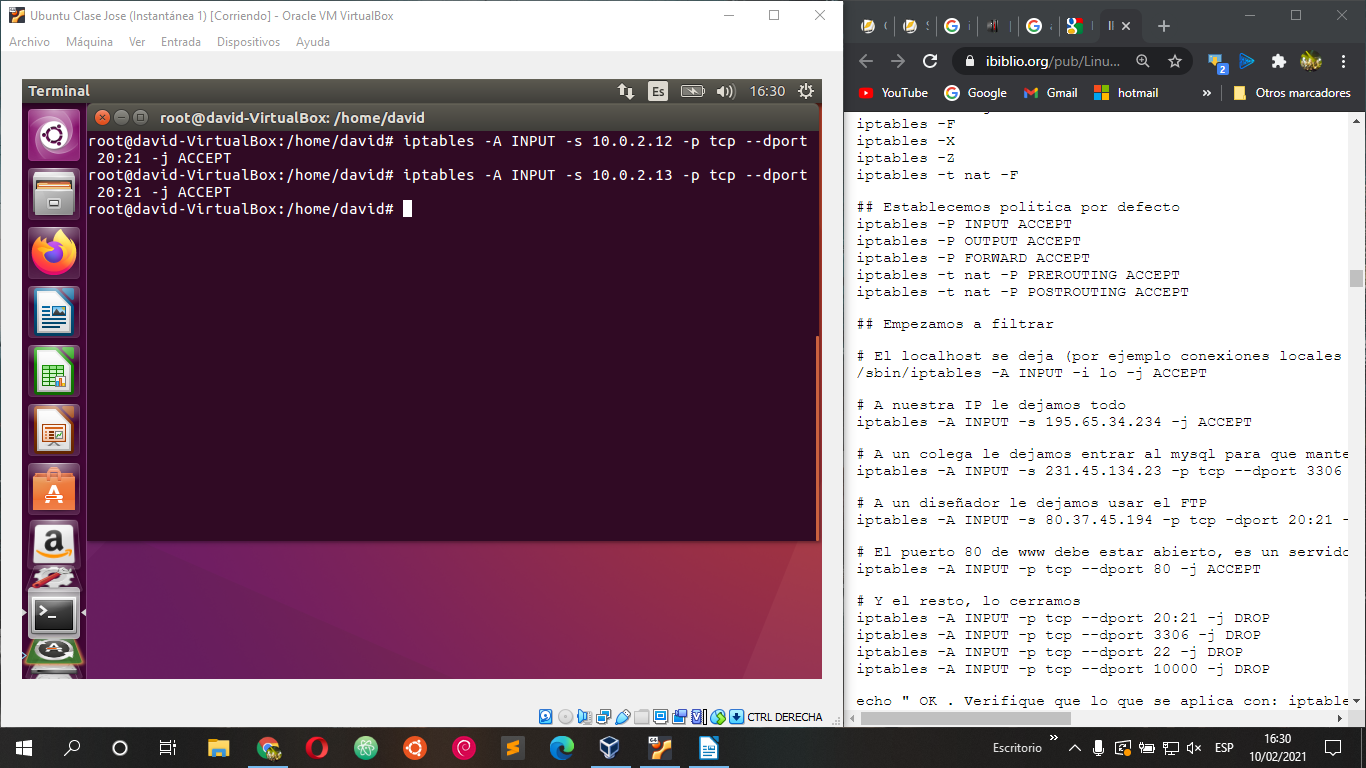


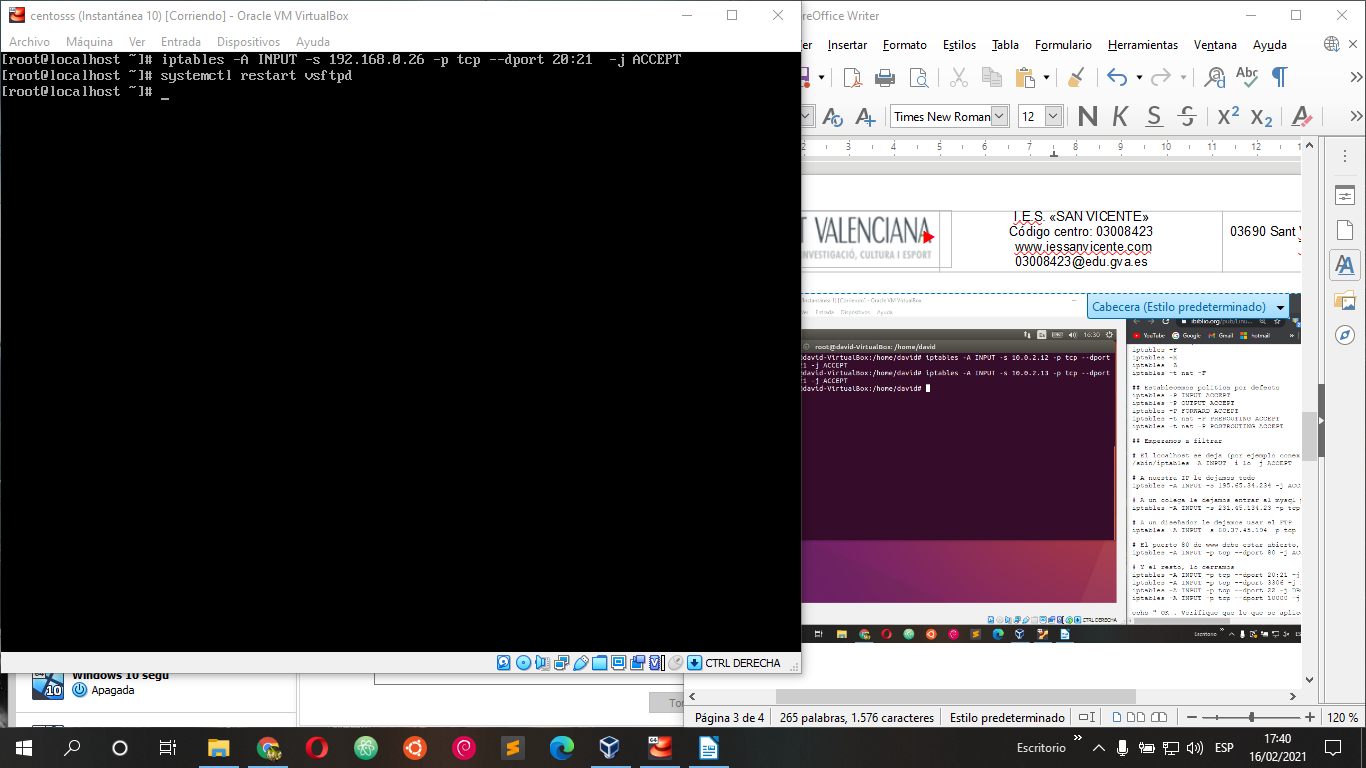
* Permitiremos las conexiones al servidor WEB de todos los equipos de la red de clase 192.168.0.0 excepto la IP de un equipo específico de un compañero de clase.

*Escribe el comando iptables. Toma una captura del equipo del compañero y de otro, comprobando que deniega y permite el acceso respectivamente.*

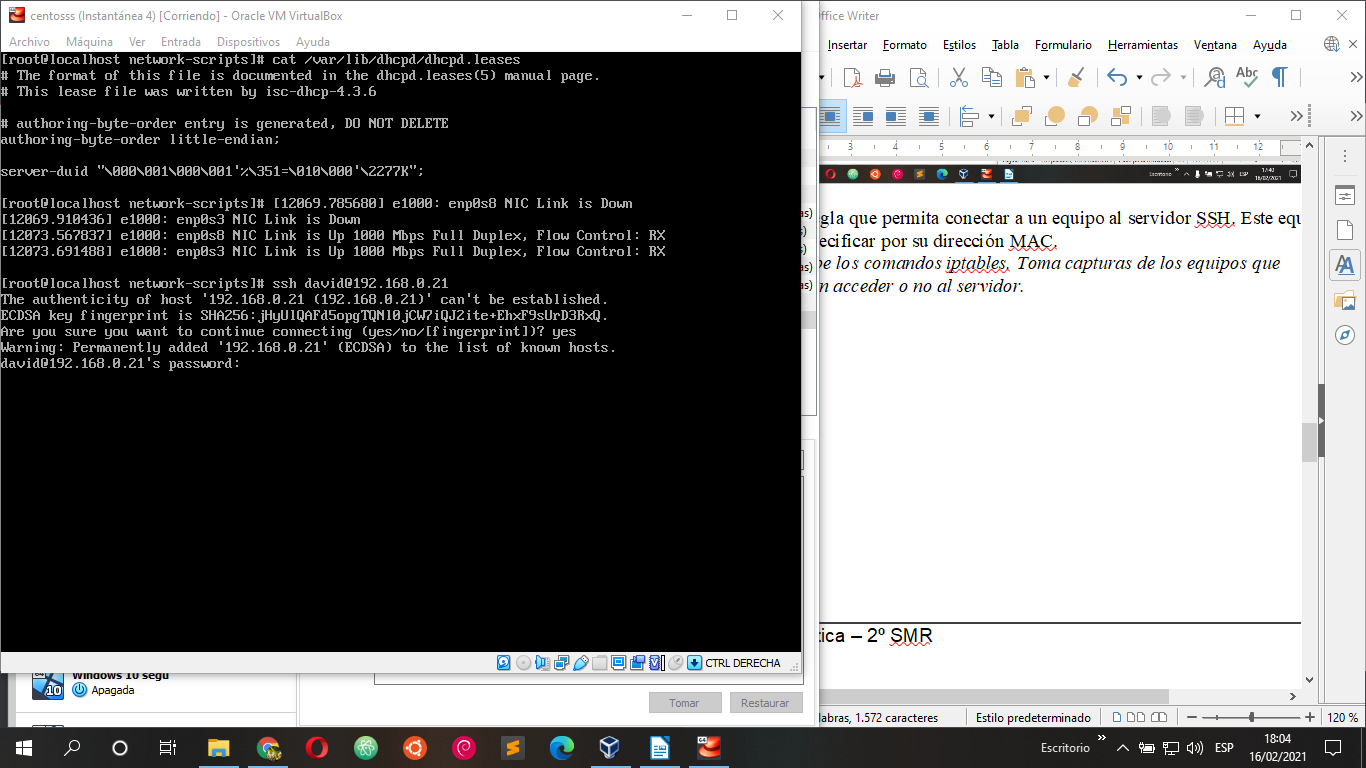
* Añade una nueva regla para permitir el acceso unicamente a 2 equipos al servidor FTP.
  + *Escribe los comandos iptables. Toma capturas de los equipos que pueden acceder al servidor.*

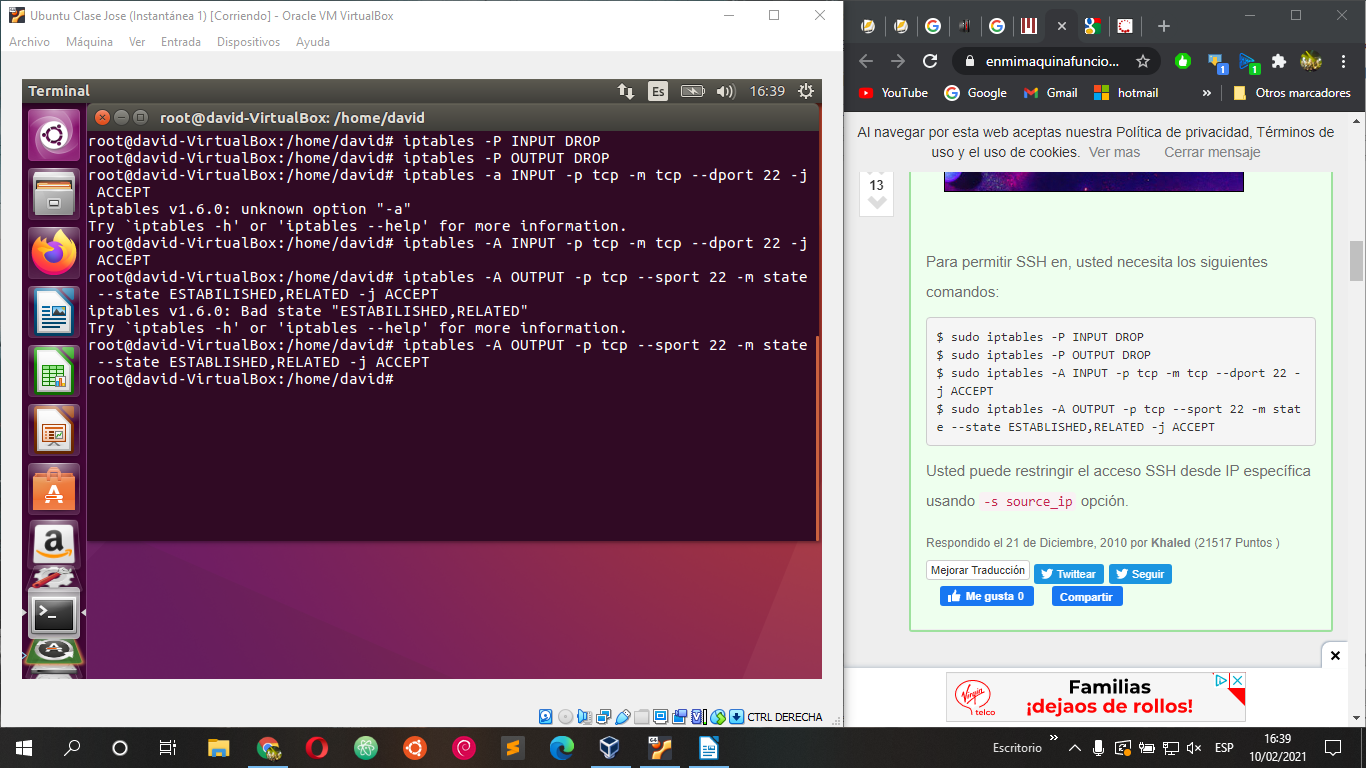
**



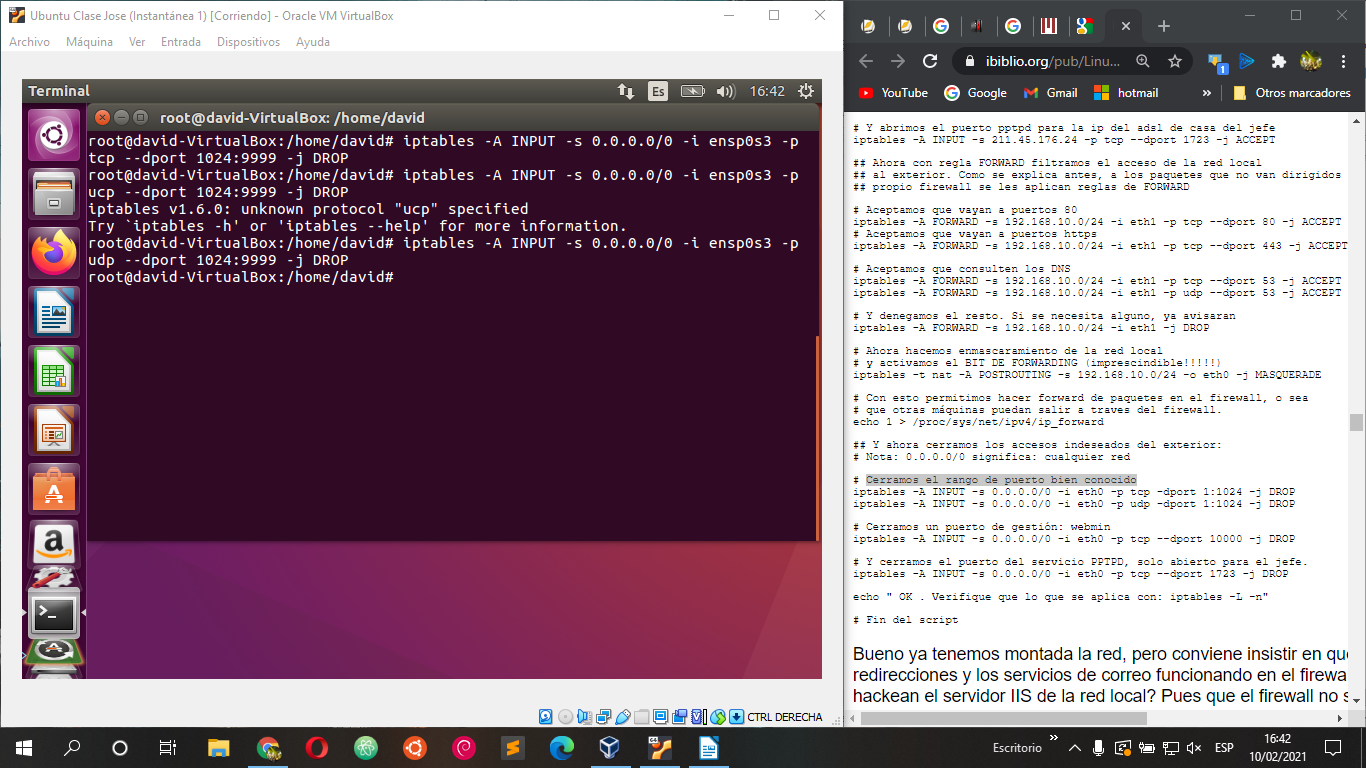


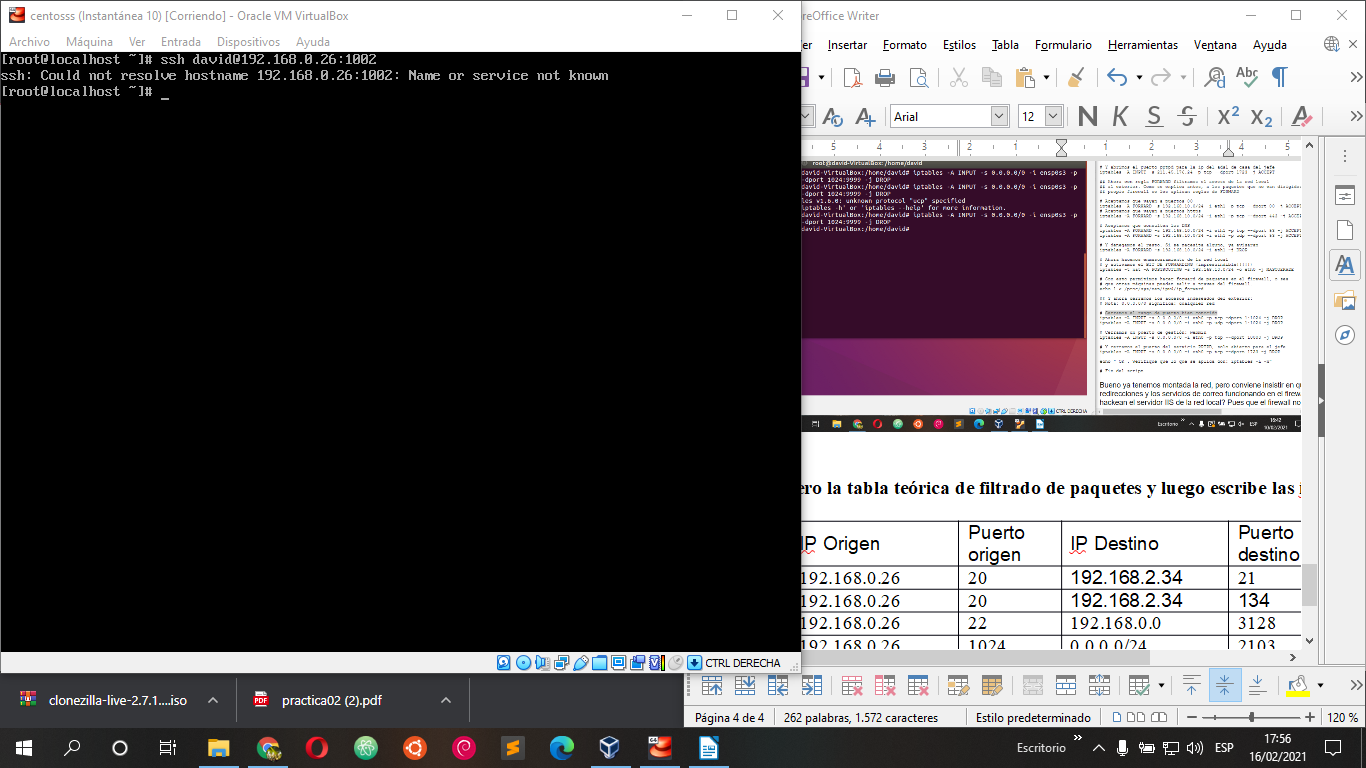
* Añade otra regla que permita conectar a un equipo al servidor SSH. Este equipo se deberá especificar por su dirección MAC.
  + *Escribe los comandos iptables. Toma capturas de los equipos que pueden acceder o no al servidor.*

**

**

* Cierra todos los puertos mayores de 1024
  + *Escribe los comandos iptable.*





**Realiza primero la tabla teórica de filtrado de paquetes y luego escribe las iptables.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Número Regla | IP Origen | Puerto origen | IP Destino | Puerto destino | Acción |
| 1 | 192.168.0.26 | 20 | 192.168.2.34 | 21 | drop |
| 2 | 192.168.0.26 | 20 | 192.168.2.34 | 134 | accept |
| 3 | 192.168.0.26 | 22 | 192.168.0.0 | 3128 | accept |
| 4 | 192.168.0.26 | 1024 | 0.0.0.0/24 | 2103 | drop |