Exercise 4.3: Block traffic to a service with TCP Wrappers and prove it is blocked

Use **TCP Wrappers** to block access to FTP daemon and prove it is blocked

Solution 4.3

NOTE: The **TCP Wrappers** option is disabled by default in **Ubuntu** and **Debian**. You must add the following line to the end of the `/etc/vsftpd.conf` file to enable this feature.

```
tcp_wrappers=yes
```

1. Start a service

   ```
   # /etc/init.d/vsftpd start
   ```

2. Check port with **telnet**

   ```
   $ telnet localhost ftp
   ```

3. Block the port by adding the following line to `/etc/hosts.deny`

   ```
   vsftpd: ALL
   ```

   NOTE: On **OpenSUSE** the version of **vsftpd** is not compiled with **TCP Wrappers** support. You may alternatively use the following **iptables** command to block the FTP traffic.

   ```
   # iptables -A INPUT -m tcp -p tcp --dport ftp -j REJECT
   ```

4. Check port with **telnet**

   ```
   $ telnet localhost ftp
   ```

   You should get a connection refused message. Note: The loopback may still work, use a different adapter.

5. Remove the line from `/etc/hosts.deny` to clean up the exercise. Or if you created an **iptables** rule to block traffic, flush the rules:

   ```
   # iptables -F
   ```