Práctica 9: Control de acceso a los servicios I: Xinetd y TCPWrappers.

El objetivo de la práctica es configurar el servidor xinetd y los envolventes de acceso (tcpwrappers) para que permitan el acceso a una serie de servicios por parte de unos ordenadores y la denegación de los mismos a otros ordenadores.

Para un correcto funcionamiento de la práctica, es condición indispensable detener el cortafuegos (iptables) del sistema. Para ello, debéis ejecutar el comando:

```
systemctl stop iptables.service
```

Una vez detenido el cortafuegos debéis formar una "red privada", la cual estará compuesta por vuestro ordenador y otro ordenador de prácticas, con cuyo usuario os habréis puesto de acuerdo para formar entre ambos ordenadores la "red privada".

Una vez llegados a este punto, se solicita que se configure el ordenador de forma que el servidor xinetd permita:

- El servicio de *daytime*, bajo el protocolo TCP, para todos los ordenadores del departamento de informática de la universidad de Valencia.
- El servicio de *echo*, bajo el protocolo TCP, para los ordenadores de la red privada.
- El servicio de *telnet* para todos los ordenadores de la red, pero con las siguientes condiciones:
  - El servicio debe estar activo solo de 8:00 a 20:00 horas[1].
  - Debe permitir un máximo de 2 conexiones simultáneas desde un mismo ordenador.
  - Debe permitir un máximo de 3 conexiones totales.

El resto de servicios que proporciona xinetd deben estar deshabilitados[2]. Para conseguir que el servidor xinetd lea las modificaciones que realicemos en la configuración, podemos ejecutar el comando:

```
systemctl restart xinetd.service
```

El cual detiene y arranca el servidor con la nueva configuración. Para comprobar el correcto funcionamiento de las restricciones insertadas podéis utilizar el comando *telnet* ejecutando la conexión al puerto adecuado en cada caso (7 para *echo*, 13 para *daytime* y 23 para *telnet*, aunque este es el puerto por defecto y no hace falta especificarlo).

Una vez configurado de forma correcta el servidor xinetd, se deberán configurar los envolventes de acceso (tcpwrappers), de forma que:

[1] Para comprobar su funcionamiento, habilitarlo en un intervalo pequeño de tiempo, 5 minutos por ejemplo, y probar a utilizar el servicio durante ese intervalo y fuera de ese intervalo.
[2] Para comprobar los servicios que se encuentran habilitados podéis ejecutar el comando *nmap localhost*.

- Se limite el acceso al servicio de *telnet*, de forma que solo los ordenadores del laboratorio de prácticas puedan conectarse al mismo[3].
- Se permita el acceso al resto de servicios proporcionados por el servidor *xinetd*.
- Se permita el acceso al servidor de SSH (*sshd*) a los ordenadores del departamento de informática de la universidad de Valencia[4].
- Se deniegue el acceso al resto de servicios existentes en el ordenador, escribiendo en el fichero */tmp/tcpwrapper.log* la hora en que se produjo la solicitud bloqueada, el nombre del servicio solicitado y la dirección IP del ordenador que realizó la solicitud de acceso.

Comprobar que el funcionamiento del envolvente de acceso es correcto y que permite el acceso y denegación de servicios según las reglas indicadas.

[3] Recordar que todos los ordenadores del laboratorio de prácticas responden al patrón de nombres lab114pcXX.informat.uv.es, donde XX son dos dígitos decimales.
[4] Para arrancar el servidor de SSH basta con ejecutar el comando *systemctl start sshd.service*.