1.) Para realizar este ejercicio hemos modificado el puerto del servidor ssh y hemos establecido el puerto 5000 como puerto de dicho servidor.

Para encender el servidor, hemos puesto el siguiente comando en la terminal de la máquina que actuaba como servidor: “sudo /etc/init.d/ssh start”.

Para conectarnos remotamente, hemos usado el siguiente comando: “ssh usuario@10.162.91.11” debido que hemos tenido que usar la red externa porque lo he intentado hacer con mi portátil y no me ha dejado acceder a la red interna.

Luego, hemos intentado realizar la conexión ssh mediante PuTTY y ha resultado satisfactorio.

Si queremos provocar un enjaulamiento en la carpeta de Descargas al usuario “usuario” se haría de la siguiente forma:

```
#Subsystem      sftp    /usr/libexec/openssh/sftp-server
Subsystem sftp internal-sftp
```

Ahora vamos a agregar la jaula para nuestro usuario agregando las siguientes líneas:

```
# Jaula usuario Descargas
Match usuario Descargas
ChrootDirectory %h
AllowTcpForwarding no
ForceCommand internal-sftp
X11Forwarding no
```

Luego, habría que eliminar la shell del usuario en el fichero passwd.

2.) 2.2.) Podemos ver como se encuentran corriendo 84 procesos en el sistema del profesor ya que no hemos sido capaces de montar el servidor webmin en nuestro portátil.

2.5.) Entramos en la configuración y establecemos los logins y logouts como elementos importantes del sistema, por lo que, al salir y volver a entrar, al revisar los logs, podemos ver que se ha recogido nuestra ip como un evento de login.

2.8.) En el menú desplegable de la izquierda seleccionamos la pestaña “System logs” dentro de la pestaña “System”. Una vez dentro podemos ver la ruta donde se encuentran guardados los archivos de log. En dicha tabla, podemos ver si están o no activos en la columna “Active?”.

2.11.) El puerto de escucha del servidor virtual de Apache es el 80, el de ssh es el 22.

2.15.) No hay cortafuegos instalado. Lo podemos encontrar en el menú desplegable de la izquierda en “Networking”.

3.) - Sobre un equipo: nmap -Pn 192.168.1.111
- Sobre varios equipos: nmap -sP 192.168.33-95
- Sobre toda la red: nmap -sP 192.168.1.0/24

La opción -Pn se usa para saber cuantos hosts hay conectados a la red.

La opción -sP se usa para que hacer un ping a todos los hosts de la red y aparecen aquellos hosts que responden a dicho ping.

Zenmap es una interfaz gráfica para realizar las mismas pruebas que hemos realizado por consola, por lo que obtenemos los mismos resultado en zenmap que en nmap.