INSTRUCCIONES

- La actividad se debe ejecutar con un u**suario que se denomine con tu nombre de pila**, no con el usuario denominado “usuario”. Debes usar sudo cuando sea necesario.
- Casi todos los subapartados deben incluir al menos una captura de pantalla
- En el caso de que se quiere dejar evidencia de un comando
  - Dicho comando será **el primero** en aparecer en la captura de pantalla
  - Aparecerá como mínimo una línea adicional a la del comando, aunque dicha línea sea el prompt del sistema
  - El espacio vacío de la terminal no aparecerá en la captura
- Todas las capturas de pantalla tendrán como ancho el de la página
- La captura de pantalla irá a continuación del trozo de enunciado correspondiente, ni antes ni a los lados

El incumplimiento de alguna de las instrucciones indicadas, hará que dicha captura no sea usada a efectos de evaluación ni calificación

NOTA: Entre corchetes se indica el peso de cada apartado en la calificación global de la actividad

CRITERIOS DE EVALUACIÓN:

4d) Se han identificado, arrancado y detenido servicios y procesos.

5b) Se han utilizado dispositivos de interconexión de redes.

5c) Se ha configurado el acceso a redes de área extensa.

5d) Se han gestionado puertos de comunicaciones.

5f) Se han aplicado protocolos seguros de comunicaciones.

5g) Se han configurado redes de área local cableadas.

5h) Se han configurado redes de área local inalámbricas

6c) Se han explotado servidores de ficheros, servidores de impresión y servidores de aplicaciones.

6d) Se ha accedido a los servidores utilizando técnicas de conexión remota.

6f) Se han instalado y evaluado utilidades de seguridad básica.

USO DEL FIREWALL UFW

1. [1] Instala el paquete openssh-server, que es un servidor de SSH. Una vez instalado, asegúrate de que el servicio esté corriendo. Después, accede por SSH (con el comando ssh, no con putty) con tu usuario a tu propia máquina desde tu propia máquina. ¿Funciona el acceso?

2. [2] Utiliza **ufw** para aplicar a tu ordenador la configuración típica de firewall para un Linux de Escritorio (denegar tráfico entrante y permitir tráfico saliente). Una vez aplicada la configuración muestra el estado de la configuración del firewall y comprueba que puedes navegar correctamente. Adjunta pantallazos de los comandos necesarios y de un navegador visitando una página web de tu libre elección.

3. [3] Intenta acceder de nuevo a tu ordenador con ssh. ¿Porqué sigue funcionando el acceso si acabamos de configurar el cortafuegos de forma que se deniegue el tráfico entrante?

4. [3] Partiendo de la configuración anterior utiliza **ufw** para abrir los puertos necesarios para poder ofrecer los siguientes servicios:

    4.a) DNS

    4.b) FTP en modo activo

    4.c) SSH

    4.d) HTTP y HTTPS

    Muestra el estado de la configuración del firewall.

5. [4] Partiendo de la configuración anterior debes denegar (deny) los puertos asociados al servicio de FTP y DNS. Muestra el estado de configuración del firewall tras realizar los cambios.

6. [1] Por último, resetea el firewall para dejar el ordenador como al principio.