**ANEXO I**

**Práctica 1: Hardening.**

**Reactivos**

* **¿Cuál es la finalidad de configurar los permisos del archivo /etc/shadow a 600?**

A) Permitir que todos los usuarios accedan al archivo.

**B) Evitar que usuarios no autorizados lean o escriban en el archivo.**

C) Permitir únicamente lecturas por parte de procesos del sistema.

D) Hacer que el archivo sea ejecutable para todos los usuarios.

* **¿Qué sucede al deshabilitar la autenticación por contraseña en el archivo /etc/ssh/sshd\_config?**

**A) Los usuarios solo podrán acceder mediante claves SSH.**

B) Se elimina la posibilidad de acceder al servidor.

C) El puerto SSH cambia automáticamente al puerto 22.

D) Se habilita el acceso como **root.**

* **¿Cuál es el propósito de restringir los recursos de un usuario en /etc/security/limits.conf?**

**A) Evitar que el usuario consuma todos los recursos del sistema.**

B) Mejorar la velocidad de procesamiento de archivos del usuario.

C) Permitir acceso al servidor solo en horarios específicos.

D) Configurar automáticamente los permisos de los usuarios.

* **¿Qué comando permite verificar las reglas activas del firewall UFW?**

A) sudo ufw enable

B) sudo ufw list-rules

**C) sudo ufw status verbose**

D) sudo ufw allow