Seguridad y Alta Disponibilidad - CFGS ASIR: fail2ban

FAIL2BAN:

Realiza las siguientes acciones:

- Crea un contenedor LXD con las siguientes características:
  - de nombre *tunombre-f2b* (reemplaza *tunombre* por tu nombre y las iniciales de tus apellidos, por ejemplo *manuelgr-f2b*)
  - corre Ubuntu 20.04
  - ponle contraseña al usuario `ubuntu`
  - autoriza el acceso por ssh usando contraseñas
  - haz una foto llamada *acceso.png* donde se vea la siguiente secuencia de acciones:
    - ejecutas el comando `lxc ls -c n,4,s,l,P,m`
    - accedes por ssh al contenedor como usuario `ubuntu`
- En el contenedor *tunombre-f2b c*onfigura::
  - fail2ban para proteger el servicio ssh revisando los últimos 15 minutos de log y que proceda a 'banear' durante 2 horas a todos aquellos equipos que fallen 4 veces en la autenticación.

    NOTA: haz que esos parámetros afecten únicamente al servicio ssh.
  - Syslog para desactivar la reducción de mensajes repetidos.
- Realiza la siguiente secuencia de acciones:
  - Accede por ssh desde el equipo anfitrión y provoca el bloqueo. Acto seguido haz un vídeo *fail2ban* donde se vea sin borrar la terminal en ningún momento:
    - Cadena de reglas iptables de fail2ban donde aparece bloqueada la IP (únicamente la cadena de usuario que crea fail2ban).
    - Comandos fail2ban para ver el estado del jail sshd y desbloquear la IP anterior.
  - Haz una foto llamanda *fail2ban.png* donde se muestren las líneas del fichero de log de fail2ban donde se ve que se ha creado una regla temporal de baneo y su posterior desbloqueo manual. Usa el editor de imágenes para resaltar la línea donde se informa del bloqueo y la línea donde se informa del desbloqueo.

Entrega:

- archivo/s de configuración de fail2ban y syslog modificado/s.
- foto *acceso.png*
- vídeo *fail2ban*
- foto *fail2ban.png*.