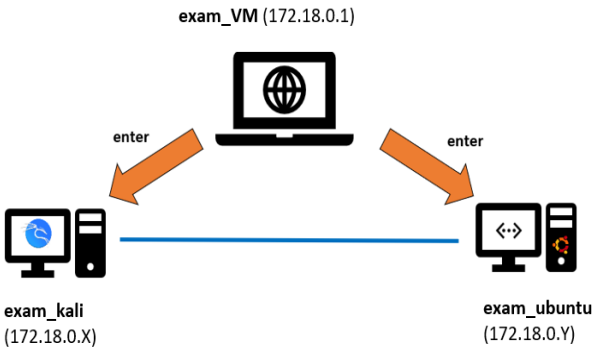
Seguridad de Sistemas Informáticos. Examen Práctico Convocatoria Ordinaria 2022

Nombre y Apellidos:

UO:

Instrucciones:

El siguiente esquema muestra la infraestructura que se le proporciona para este examen, consistente en **una MV idéntica a la usada en prácticas** con 2 contenedores también similares. Para acceder a ellos, en el escritorio de la máquina virtual verá un fichero comprimido **`exam.zip` que deberá descomprimir** con la clave que se dirá al empezar el examen. Dentro de él verá la carpeta `exam/lab_exam`. **El contenido de esta carpeta contiene el laboratorio que tendrás que manejar en este examen, compuesto por:**



- Un contenedor *Kali*.
- Un contendor *Ubuntu* con una copia de la web de nuestra escuela.

Los contenedores ya están construidos, por lo que **basta hacer un `build_lab.sh` para poner en marcha la infraestructura** (**NO ES NECESARIO hacer un `prepare_lab.sh`**). Al igual que en prácticas, puede entrar en sesión en ambos con los scripts `enter_kali.sh` y `enter_ubuntu.sh` proporcionados.

Las IPs de los tres componentes de nuestra infraestructura son las que aparecen en la imagen, si bien X e Y pueden ser 2 o 3 en función del orden en el que se arranquen los contenedores. **Recuerde que puede traer todo el material desarrollado en las prácticas como ayuda para hacer este examen.**

Entrega:

Debe entregar **un único fichero PDF** en la tarea habilitada en el campus virtual con las **capturas de pantalla y explicaciones necesarias** que demuestren que ha hecho cada ejercicio. Se recomienda abrir un fichero *Word* desde el primer momento del examen e ir completando capturas y explicaciones a medida que se vayan haciendo ejercicios, grabando a menudo para evitar perder información. Puede luego **guardar como PDF** el fichero para la entrega.

Ejercicios:

1) **En la página web alojada en el contenedor *Ubuntu* un administrador despistado ha usado mal el mecanismo estándar que existe para que *Google* u otros buscadores no indexen ciertas páginas de sitios web, pretendiendo ocultar un dato secreto con el mismo. Localice ese mecanismo y qué está ocultando (1 punto).**

2) **Bonifacia (también conocida como `ssiuser`) pretende mandar un mensaje a Anacleto manifestándole su amor eterno y quiere utilizar la infraestructura de clave pública para ello. Bonifacia tiene la clave pública de Anacleto, pero el muy ignorante se la ha mandado en un fichero cifrado mediante clave simétrica que puedes encontrar en la carpeta `/exam`, llamado `clave_pública_anacleto2022.asc.asc`. A pesar de su amor ciego, Bonifacia es consciente de las limitaciones de Anacleto y sabe que siempre utiliza la misma *password* para todo, incluso para autenticarse en el sistema. Demuestre que puede implementar el siguiente procedimiento para conseguir mandar el mensaje de amor (1,5 puntos)**
   - **Crear, mediante `useradd` un usuario en la MV de nombre `anacleto` y cuya password hasheada es `'$1$marina22$FNBWK1hFyaa4U.BEdgTL71'`. Puede encontrar esta hash dentro de la carpeta `/exam` en el fichero `hash_anacleto.txt`. No es necesario ningún parámetro más que la password y el nombre del usuario, pero ¡OJO!, utiliza comillas simples (entrecomillado fuerte), para suministrar la password.**
   - **Atacar mediante `john` a los ficheros del sistema, tal y como hicimos en prácticas, para averiguar la password de `anacleto` de la MV. Para ello utiliza el fichero `diccionario.txt` de la carpeta `/exam`. `john` está instalado tanto en la MV como en ambos contenedores, elije el que quieras para ello.**

- **Descifrar, con la password obtenida en el paso anterior, la clave pública de `anacleto`.**
- **Importar la clave pública obtenida de `anacleto` y cifrar la declaración de amor de Bonifacia (sirve un simple `.txt` 😊) para el susodicho agente secreto.**

3) Sirviéndose de la ayuda de la guía CIS de *Ubuntu* si lo estima necesario (proporcionada en la carpeta `exam`), haga las siguientes operaciones de seguridad manual en la máquina virtual (1,5 puntos)

a. **Cambie la configuración del servidor SSH para que:**
   i. **Se desactive el acceso en modo gráfico.**
   ii. **El número máximo de intentos de autenticación sea 6.**
   iii. **El número máximo de sesiones sea 3 o menos.**
   iv. **Se desactive el login con la cuenta `root`.**
b. **Evalúe el nivel de seguridad con `lynis`.**

4) En la carpeta `exam` de la máquina virtual se le entrega un fichero ZIP llamado `U_CAN_Ubuntu_18-04_LTS_V2R5_STIG_Ansible.zip`. Es el STIG aplicable con *Ansible* idéntico al visto en los laboratorios. La máquina tiene además ya instalados el paquete `oscap` y su GUI *Oscap Workbench* ya instalados. Para completar el ejercicio se le pide (1,5 puntos):

- **Evalúe el estado actual de la máquina virtual con *Oscap Workbench* y el perfil CIS tal y como vimos en clase, y entregue una captura donde se vea la puntuación final (porcentaje) obtenida. En la carpeta `exam` está el fichero `scap-security-guide-0.1.59-oval-5.10.zip` idéntico al que usamos en prácticas.**
- **Clone o haga un *snapshot* de la MV, de forma que pueda Vd. volver al estado inicial en caso necesario.**
- **Aplique los controles de seguridad contenidos en el ZIP del STIG, escribiendo en el informe de resultados qué ha hecho para ello. *Ansible* ya está instalado en la máquina virtual.**
- **Reevalúe la MV con estos controles aplicados usando el mismo perfil anterior y muestre la nueva puntuación (porcentaje) final.**

5) Para hacer este ejercicio la máquina virtual tiene `firewalld` y su GUI vistos en prácticas ya instalados. Usando dichas herramientas haga lo siguiente (1,5 puntos):

- **Entre en la consola del contenedor `exam_ubuntu` y compruebe que puede hacer `ssh` a la máquina virtual**
- **Abra el GUI del firewall y, en la zona `docker`, prohíba la comunicación del contenedor anterior con la máquina virtual para dicho servicio `ssh` solo bajo IPv4, indicando en los resultados como lo ha hecho.**
- **Haga de nuevo el paso anterior, pero comprobando ahora que la conexión no es posible, y que el *firewall* está haciendo su trabajo.**

6) En el contenedor `exam_ubuntu` hay un servidor web *Apache* con `mod_security2` instalado. Con ello se pide probar solamente que el motor de `mod_security2` funciona agregando una nueva regla a mano al WAF que se dispare cuando el valor del parámetro "rick" en una URL sea una cadena que contenga la palabra "pickle". El WAF deberá devolver una página de error con el estado *HTTP 406 Not Acceptable*. Además, se deberá registrar el incidente con el siguiente mensaje "I'm a pickle Rick!". Dispara esta regla a posta (1,5 puntos)

7) El usuario `ssiuser`, inconscientemente, decide activar el bit SUID al comando 'date' con la idea de que se pueda ejecutar con privilegios, aunque no se tengan. Un malote, tras estudiar cómo se pueden utilizar comandos de *Linux* para hacer el mal, se entera de que el comando `date` tiene el bit SUID activado. Demuestre cómo podría acceder al contenido del fichero donde se almacenan las contraseñas de los usuarios del sistema en estas circunstancias. En la carpeta `/exam` tiene un fichero que le puede ayudar a hacerlo (1,5 puntos)