Práctica 1

Seguridad en Linux: Preparación del entorno.

Antes de empezar

Estas tareas comenzarán a realizarse durante las clases prácticas y, la parte que no dé tiempo a finalizar en ese horario, se terminarán como trabajo individual del alumno.

Lo más conveniente para la correcta realización de la práctica es que se utilicen los ordenadores de los laboratorios. Vamos a establecer conexiones entre las diferentes máquinas por lo que, si preferís llevar vuestro propio ordenador, debéis conectaros a la red a través de cable.

Instalación de Kali Linux

1. Nos descargamos la imagen iso de 64 bit:

   https://www.kali.org/downloads/

2. Comprobamos que la firma sha256 del iso que nos hemos descargado mediante http://download.cnet.com/MD5-SHA-Checksum-Utility/3001-2092_4-10911445.html o cualquier otro programa.
3. Creamos una máquina virtual para arrancar desde la imagen con VirtualBox:
   - Nombre: KL-UOXXXXX
   - Tipo: Linux.
   - Versión: Debian (64bits).
   - RAM: 2GB.
   - Disco duro: Crear un disco virtual ahora.

- Tamaño: 50GB
- Tipo: VMDK, reservado dinámicamente.

4. Configuramos la máquina que acabamos de crear:
   - Sistema/Procesador/Características extendidas, habilitamos PAE/NX y añadimos un procesador más para tener un total de dos.
   - En Red/Adaptador 1 lo configuramos como Adaptador Puente, Modo Promiscuo/ Permitir todo.
   - En Pantalla/Memoria de Vídeo le damos 128MB y habilitamos la aceleración 3D.
   - Para arrancar desde el CD: Almacenamiento/ Controlador IDE, hacemos clic en Vacío y en la Unidad óptica le especificamos la iso que nos hemos descargado.
5. Arrancamos la máquina y seguimos los pasos de instalación del sistema operativo:
   - Install (NO en modo gráfico)
   - Elegimos el idioma que queramos, le ponemos como nombre de la máquina: KL-UOXXXXXX, dejamos en blanco el nombre del dominio y ponemos contraseña al root.
   - Particionado de discos: Guiado – utilizar todo el disco / Seleccionamos el disco correspondiente (sólo habrá uno) / Separar particiones /home, /var y /tmp / Finalizar el particionado y escribir los datos en el disco. Esperamos a que instale el sistema operativo.
   - Utilizamos una réplica de red, dejamos el Proxy en blanco e instalamos el GRUB en el registro principal de arranque (/dev/sda)
   - Iniciamos sesión como root y la contraseña que hemos puesto.
6. En la línea de comandos ejecuta *fdisk -l* para ver la tabla de particiones y *lsblk -l* para ver a qué partición corresponde cada directorio.

7. Estudia los directorios de runlevel en /etc/ para ver el orden de ejecución de servicios según el nivel de ejecución.
8. Mira los permisos de cualquier archivo con la orden *ls*
9. Actualizamos la base de datos de los paquetes que podemos instalar: *sudo apt-get update*
10. Ejecuta la ayuda del comando *netstat*.
11. Ejecuta *netstat –nlp* para monitorizar las conexiones de red.
12. Ejecuta la ayuda para el comando *systemctl*
13. Comprueba los servicios habilitados y que se están ejecutando en el sistema con:
    - *systemctl list-unit-files --type=service | grep enabled*
14. Comprobamos que el servidor ssh no está activo. Para activarlo:
    - systemctl enable ssh.socket
15. Editamos la configuración del servidor ssh para que **NO** permita iniciar sesión con la cuenta root:
    - *sudo nano /etc/ssh/sshd_config*
    - Localizamos en la sección Authentication la opción PermitRootLogin y la deshabilitamos de la siguiente manera:

      PermitRootLogin no
16. Guardamos los cambios como antes: Ctrl+X,S,Enter.
17. Ya que **NO** es recomendable iniciar sesión con la cuenta root, es la cuenta más privilegiada en sistemas UNIX, vamos a crear una cuenta de usuario con nuestro UO y un usuario genérico al que vamos a llamar almnossi:
    - *adduser uoxxxxxx* (donde uoxxxxx es el uo correspondiente)
    - *adduser alumnossi* (le ponemos como contraseña “seguridad”)
18. Una vez hemos creado los usuarios tenemos que añadir nuestro UO al grupo de superusuarios:

    usermod -a -G sudo uoxxxxxx

19. Cerramos la sesión root e iniciamos sesión con nuestro UO con los nuevos privilegios de administración.
20. Para ver que usuarios pueden hacer sudo ejecutar la orden: *sudo visudo*
21. Échale un vistazo al fichero de contraseña shadow: *sudo cat /etc/shadow*
22. Para obtener información acerca de las contraseñas de los usuarios: *sudo chage -l nombreusuario*
23. Nos conectamos a la máquina de tu compañero de al lado:

    ssh alumnossi@ipdelamaquinadetucompañero
24. Estando conectados a la máquina remota podemos dejar un mensaje para demostrar que pasamos por allí. Para eso podemos ejecutar la orden

    echo -e "El alumno con UOxxxx pasó por aqui\nUn saludo" | tee -a saludo.txt

25. **OPCIONAL**: Añadimos una contraseña a GRUB. OJO: Si olvidamos la contraseña GRUB no podremos acceder al sistema por lo que sería conveniente tomar una instantánea de la máquina en este punto.
    - Generamos una contraseña encriptada: *grub-mkpasswd-pbkdf2* y la copiamos seleccionándola.
    - Editamos el fichero /etc/grub.d/40_custom: *sudo nano /etc/grub.d/40_custom* y al final ponemos la configuración de inicio de sesión:

      set superusers =”uoxxxxxx”

      password_pbkdf2 uoxxxxxxx *lacontraseñacifradaquehemoscopiado*

      (para pegar lo que hemos copiado anteriormente basta con clic derecho)

    - Guardamos los cambios como antes: Ctrl+X,S,Enter.
    - Actualizamos el GRUB: *sudo update-grub*
    - Reiniciamos para comprobar los cambios en el GRUB.