Entorno de trabajo y familiarización para la siguiente práctica:

En esta práctica se trabajará usando máquinas virtuales utilizando VirtualBox en los ordenadores del laboratorio.

Creación de la máquina virtual:

Descargue la máquina virtual
de http://fry.tlm.unavarra.es/~mikel/tlm/vms/sec2014/tlm_basic.ova

En el directorio /opt encontrará una carpeta llamada ssi/practica. Copie ahí el archivo tlm_basic.ova

Recuerde que la cuota de su cuenta es de 500MB, no deje archivos grandes en tu carpeta de descargas o escritorio.

Abra ahora VirtualBox.

Configure primero como carpeta predeterminada para las máquinas virtuales una dentro de /opt/ssi/practicas (pude hacerlo desde Archivo -> preferencias -> General)

Desde File seleccione la opción Import Appliance. Selecciones el archivo tlm_basic.ova. Pulse Next. En esa pantalla verá un resumen de las características la máquina virtual. Asegúrese de cambiar las rutas de los dos discos duros que aparecen (Virtual Disk Image). Esas rutas deben estar dentro de la carpeta /opt/ssi/.

Marque la opción de reinicializar la dirección MAC y pulse Import.

Configuración de red:

VirtualBox nos permite elegir las siguientes configuraciones de red (accesibles con la máquina apagada en el apartado Red de la configuración)

1. **No conectado**.
   VirtualBox muestra un adaptador de red pero sin conexión. (cable desconectado)
2. **"Network Address Translation" (NAT)**
   Permite funcionalidad básica desde el sistema operativo Huésped. Navegar por internet acceder al correo, descargar ficheros.
3. **Adaptador puente**
   Simula una conexión física real a la red, asignando una IP al sistema operativo huésped.
4. **Red interna**
   Similar al Adaptador puente, se puede comunicar directamente con el mundo exterior con la salvedad de que ese mundo exterior está restringido a las máquinas virtuales conectadas en la misma red interna. Esta limitación viene justificada por seguridad y velocidad.
5. **Adaptador sólo-anfitrión**
   Es una mezcla entre los tipos "Adaptador puente" e "interna". Para crearlo hace falta tener antes configurado un nuevo host: File-> Preferences -> Network y pulsar Add host only network. Aparecerá en pantalla vboxnet0 que será vuestro interfaz de red. Si vboxnet0 no aparece es que s necesario crearlo desde Archivo -> Preferencias -> red -> Redes solo anfitrión.

Cuando sea necesario conectarse a internet para hacer instalaciones, configure la red como NAT.

Cuando sea necesario tener conectividad entre varias máquinas virtuales, seleccione Solo Anfitrión.

Con esto ya tiene la máquina virtual creada. Puede iniciarle pulsando Start.

Como primer paso utilice esto para crear una máquina de trabajo, cambiar las contraseñas y crear algún usuario en ella. La máquina proporcionada tiene usuario tlm/tlm.

Cree dos máquinas de trabajo (puede mantener una máquina patrón y clonarla cuando lo necesite). Compruebe que puede que tiene conectividad con internet si selecciona NAT y que es posible tener conectividad entre las 2 máquinas y el host si selecciona Solo Anfitrión.

Para la siguiente práctica utilizaremos las máquinas virtuales que ya tenemos creadas:

Configuracion de SSH:
Configure el servidor de ssh en una máquina y compruebe que puede entrar desde otras. Instale el paquete ssh : sudo apt-get install openssh-server -> es posible que antes necesita hacer sudo apt-get update

- Aprenda como hacer usuarios en esa distribución de UNIX:
- Aprenda como configurar en el servidor que sólo puedan entrar algunos usuarios o algunas máquinas. Asi como los parámetros de configuración que le resulten interesantes

Puede editar archivos desde la máquina anfitriona utilizando los siguiente:

gedit sftp://VM_USUARIO@ruta completa del archivo a editar &

Debe construir una máquina con varios usuarios, algunos tienen que poder entrar por ssh y debe poder hacer que otros no tengan acceso por ssh. Para hacer algo como root debería entrar por ssh y luego hacerse root. Con `su` o `sudo`.

Aparte de probar todas las opciones de ssh que le parezcan interesantes, aprenda como configurar en un usuario que la autentificación sea con una clave pública y privada en lugar de una contraseña.

Ataques de login:
Utilice hydra o medusa para atacar su máquina.

Pruebe como se usan los diccionarios. Pruebe a atacar con fuerza bruta una contraseña de 3 caracteres.

Defensas:
Pruebe diferentes defensas contra estos ataques.

- Configure que solo algunos usuarios puedan entrar.
- Pruebe a cambiar el puerto del servidor de ssh.
- Pruebe a cambiar los parámetros de SSH que afectan a la velocidad con que un atacante puede intentar contraseñas.
- Pruebe a buscar, instalar y configurar monitores de login que corten el acceso a quien haga varios intentos de acceso fallidos.
- Mire que es el port-knocking y pruébelo

Reconocimiento de red:
Pruebe la herramienta `nmap` (https://nmap.org/man/es/) desde la máquina atacante para escanear puertos de máquinas virtuales e identificación de sistemas operativos. Active servicios en el servidor y compruebe si puede descubrirlos, incluso ocultándolos en puertos altos e incluso en UDP.