Informática Forense y Auditoría

Grado en Ingeniería Informática del Software

Escuela de Ingeniería Informática de Oviedo

Práctica 1: Instalación del entorno de pruebas

Introducción

El propósito de la presente práctica es instalar y configurar el entorno de pruebas en el que se realizarán el resto de prácticas a lo largo del curso. Para ello cada alumno dispone de un equipo de sobremesa con conexión a Internet que tiene como SO instalado Windows 10. El alumno accede a dicho equipo a través de una cuenta en el dominio uniovi. Dicha cuenta es el UOXXXXX del usuario y como contraseña, la contraseña que tiene en el correo corporativo de la Universidad. En dicho equipo se encuentra instalado el software base necesario para realizar la mayoría de las tareas más habituales. Sin embargo, la cuenta que utiliza el alumno para iniciar sesión en el dominio es una cuenta no privilegiada y por tanto no dispone de permisos para realizar determinadas tareas (adición y eliminación de programas, configuración de los interfaces de red, etc.) para los cuales es necesario disponer de privilegios de administración. Por ello, la mayoría de las prácticas se realizarán sobre máquinas virtuales que creará el propio alumno. Para posteriores sesiones deberá sentarse en la misma máquina física o bien salvar las máquinas virtuales en un dispositivo externo antes de abandonar la sesión de prácticas.

Creación de una plataforma de análisis forense

1. Descargue la imagen iso de **Caine 13** del campus virtual (**Recursos Prácticas - Práctica 1**).

2. Configure una máquina virtual en Virtual Box con un disco duro virtual de 80GB y una memoria RAM de 4GB. La nueva máquina virtual se llamará **IFA-AU-XX** (donde XX es el número del puesto físico que ocupa en el aula de prácticas) para diferenciarla de otras máquinas virtuales que pueda crear para otras asignaturas (**en el caso de que realice las prácticas en su equipo personal sustituya XX por su nombre y apellidos sin espacios en blanco**). Haga que la unidad de CD/DVD virtual esté vinculada a la imagen iso de Caine descargada.

3. Arranque la máquina virtual y una vez se haya cargado el SO Caine, realice las siguientes tareas:
   a) Lance la aplicación Keyboard desde el escritorio y seleccione como disposición para su teclado el idioma español.

b) Cambie la resolución de la pantalla a 1360x768.

4. Podemos trabajar con CAINE sin tener la necesidad de instalarlo en la máquina virtual. Simplemente no debe apagar la máquina virtual al terminar la sesión, solo deberá pausarla para mantener todas las configuraciones realizadas hasta el momento. En caso de querer instalar CAINE en una máquina para utilizarla como plataforma de análisis forense, debemos proceder a realizar una serie de pasos que explicaremos a continuación en este ejercicio. Antes de instalar CAINE debe desbloquear el disco de destino para permitir su escritura (recuerde que en el primer ejercicio añadió un disco duro virtual de 80GB a su máquina virtual). Para ello puede utilizar el programa **Unblock** (**Forensic Tools->Discos->Unblock**) del cual también dispone de un acceso directo en el escritorio, o bien abra una terminal desde la línea de comando y escriba el siguiente comando: **sudo blockdev --setrw /dev/sdX** (donde X dependerá del número de dispositivo SATA o SCSI correspondiente a su disco duro virtual). En el escritorio encontrará un acceso directo llamado **Install CAINE 22.04** que le permite iniciar el proceso de instalación de CAINE en el disco duro seleccionado. Cuando llegue el momento de crear la cuenta del primer usuario, cree una cuenta con su **nombre y la primera inicial de cada uno de sus dos apellidos** (ej.: Si el alumno se llama Juan Español Asturias el nombre de la cuenta debe ser **juanea**). Como contraseña establezca **Practicas2024**.

5. Si hemos realizado con éxito la instalación, tenemos una máquina virtual operativa para realizar las prácticas. Como a lo largo del curso se puede desconfigurar o producirse errores que la dejen en un estado no operativo, vamos a crear una instantánea de la misma. Para ello el software de virtualización nos ofrece la posibilidad de crear estas instantáneas que son una suerte de copias de seguridad del estado en el que se encontraba la máquina virtual (SO, programas, datos, etc.) en un instante concreto. Cree una instantánea y llame a dicha instantánea **Base** y establezca como comentario "**Maquina virtual de IFA-AU después de haber instalado SO y haber configurado la red. password: Practicas2024**".

6. Descargue la aplicación Rufus (https://rufus.ie/). Esta es una aplicación que le permitirá crear unidades USB arrancables a partir de imágenes ISO. Abra el archivo descargado, no es necesaria la instalación. El ejecutable está firmado digitalmente y la firma debería indicar:
   - Akeo Consulting
   - Pete-Batard- Open Source Developer

   a) Cree, utilizando Rufus, un USB arrancable con la imagen ISO de Caine. Para ello deberá disponer de un USB que no utilice con al menos 4GB de espacio libre con formato FAT32.
   b) Una vez haya creado el USB arrancable, pruebe el mismo intentando arrancar en un equipo de su propiedad (ej.: un portátil), para lo cual deberá modificar el orden de arranque de la BIOS. Normalmente el menú de arranque está accesible pulsando F12 durante el inicio del ordenador, si bien en algunos equipos se debe pulsar otra tecla.
   c) Compruebe que es capaz de iniciar el equipo desde el USB que acaba de crear con la utilidad Rufus.

Instalación de las máquinas de pruebas

Máquina Linux Ubuntu Desktop

7. Una de las máquinas virtuales en las que desarrollaremos los siguientes guiones de prácticas correrá el SO Linux correspondiente a la distribución Ubuntu 22.04 LTS. Para instalar este sistema operativo necesitamos disponer de una imagen de instalación. Descargue del Campus Virtual (**Recursos Prácticas - Práctica 1**) la imagen iso de dicha versión del SO Ubuntu. Cree una máquina virtual con las siguientes características:

   - 2GB de RAM
   - 50 GB de disco duro virtual.
   - 1 tarjeta de red en modo puente (bridge).
   - 1 unidad de DVD no mapeada a la unidad física

   La nueva máquina virtual se llamará **IFA-UD-XX** (donde XX es el número del puesto físico que ocupa en el aula de prácticas) para diferenciarla de otras máquinas virtuales que pueda crear para otras asignaturas (**en el caso de que realice las prácticas en su equipo personal sustituya XX por su nombre y apellidos sin espacios en blanco**). Una vez hecho esto vincule el DVD de la máquina virtual a la imagen iso del CD de instalación de Ubuntu que descargó previamente.

   Una vez creada la máquina virtual y vinculada la imagen iso del DVD de instalación a la misma, podemos comenzar el proceso de instalación. Para ello inicie la máquina virtual (pulse sobre el botón Play en la barra de herramientas de VirtualBox). Se iniciará la máquina virtual como si de una máquina física se tratase. Transcurridos unos segundos verá el logo de Ubuntu en pantalla y comenzará el proceso de instalación. Si eso no fuese así, habría que cambiar el orden de arranque de los dispositivos en la BIOS de la máquina virtual. En caso de que le ocurra esto último, diríjase al profesor para que este le ayude a solventar el problema.

   El proceso de instalación de Ubuntu consta de 7 pasos entre los cuales cabe resaltar los siguientes:

   - **Elección del idioma de instalación**

     Elección de la configuración del teclado (probar que se escriben correctamente los siguientes caracteres: ñ,:,|,@, ,&,%,$,[,],{,},(,). En caso de no ser así elegir otra configuración de teclado en español).

   - **Elección de la zona horaria**
   - **Particionado del disco duro. Siga las instrucciones del profesor en este apartado.**
   - **Nombre de máquina**

     El nombre de la máquina Linux será **IFA-UD-XX** donde XX es el número de puesto físico que ocupa en el aula.

- **Cuenta inicial**

  El nombre de la primera cuenta será su nombre y la primera inicial de cada uno de sus dos apellidos (Ej. Si ud. se llama Pedro Español Asturias la cuenta sería **pedroea**). Su contraseña será **Practicas2024**.

Una vez realizados estos pasos básicos de instalación comienza la configuración e instalación de los paquetes que componen el sistema operativo. Transcurridos unos minutos finalizará la misma y la máquina virtual se reiniciará. Pruebe a ingresar en el sistema recién instalado con la cuenta de alumno. Abra el icono de la red en la barra de notificación superior y configure el interfaz de red para que obtenga una IP dinámica por DHCP. Cierre el diálogo de configuración de la red y reinicie la misma si es necesario (puede para ello desactivar y luego volver a activar el interfaz de red). Abra una terminal y compruebe la configuración de sus interfaces de red mediante el comando ***ip a***. Pruebe que tiene conexión de red haciendo un **ping** a la pasarela de su subred. Abra un navegador e intente acceder a una página web en Internet. Si no ha tenido problemas al realizar las acciones anteriores tendrá configurada correctamente la red en su máquina virtual. En caso contrario, o bien no estableció el adaptador virtual en modo puente (bridge) o bien tiene mal configurado el DHCP para su interfaz de red en la máquina virtual. En cualquiera de estos dos casos, avise el profesor si no puede solucionarlo por sí mismo.

8. Cree una instantánea de la máquina virtual anterior y llame a dicha instantánea **Base** y establezca como comentario **"Máquina virtual de IFA-UD después de haber instalado SO y haber configurado la red. Usuario: alumno, password: Practicas2024"**.

Firmado por GARCIA TAMARGO, MARCO ANTONIO (FIRMA) el día 03/09/2024 con un certificado emitido por AC DNIE 006