

Tutorial

Tanto el Obligatorio 1 como los siguientes serán evaluados sobre una máquina virtual VMware con una instalación de BackTrack Linux (<http://www.backtrack-linux.org/>). Los siguientes son los pasos para su instalación en un PC o Mac con algún VMware instalado (VMplayer, VMware Workstation, etc.).

- Obtener la máquina virtual para el primer obligatorio, las opciones son:

1. comprar el CD en el quisco del CEI o,
2. bajar la imagen iso del BackTrack 3 desde el sitio oficial

<http://www.backtrack-linux.org/download.php?fname=bt3>

y luego bajar desde el sitio del curso los cuatro archivos necesarios, tres para VMPlayer y uno para el Obligatorio:

- floppy.flp, RC2009.vmx, slack.nvram
- captureFING.pcap

Grabar en un CD o pendrive los cuatro archivos mencionados (bt3-final.iso , floppy.flp, RC2009.vmx y slack.nvram).

Suponiendo que en este momento se tienen todos los archivos necesarios en un CD (si lo tiene en un USB es similar), los pasos a seguir son:

- Poner el CD en la lectora de CD/DVD y desde línea de comandos ejecutar

```
mount /media/dvdrom
```

(recuerde que antes de retirarse, luego de apagar la máquina virtual, deberá ejecutar el comando `umount /media/dvdrom`)

- Copiar los archivos captureFING.pcap, floppy.flp, RC2009.vmx, slack.nvram que vienen en el CD a su home.
- Modifique en el archivo RC2009.vmx las siguientes líneas, según la configuración del PC.

```
ide1:0.fileName = "/media/cdrom/bt3-final.iso"
```

- Ejecute el vmplayer, seleccione abrir una máquina virtual existente y luego seleccione el archivo RC2009.vmx.
- A continuación comenzará a bootear la imagen y levanta el entorno gráfico.
- si el browser no obtiene paginas web recuerde ver la configuración del proxy en el navegador.

DADO QUE LOS CONTENIDOS SE BORRAN AL REINICIAR LA MÁQUINA SE DEBE TENER CUIDADO DE COPIAR A UN ALMACENAMIENTO NO VOLÁTIL TODOS LOS RESULTADOS QUE SE OBTUVIERON.

Para transferir archivos entre el SO anfitrión y la máquina virtual se puede configurar la máquina virtual para que vea el USB. Si no fuera posible, lo siguiente siempre funciona.

Primero debe asegurarse de que el servicio SSH esté funcionando en la máquina virtual, de lo contrario debe iniciarlo. Inicio -> Services -> SSH -> Start SSHD

El usuario es `root`
y la password `toor`

Para sacar archivos de la imagen del vmplayer:

- si tiene conexión a Internet puede usar webmail por ejemplo o,
- hacer un `scp` a la maquina real. Por ejemplo si el grupo 06 de redes ejecuta un comando y se guarda la salida en un `/root/salida.txt` (dentro del vmplayer), entonces deberá usar el siguiente comando dentro del vmplayer para pasarlo a la máquina real:

```
scp /root/salida.txt redes06@192.168.185.1:~/
```

Para ingresar archivos al vmplayer:

- si tiene conexión a internet puede usar webmail por ejemplo
- hacer un `scp` a la maquina real, por ejemplo si el grupo 06 de redes quiere poner dentro de la máquina virtual el archivo de captura que nosotros les damos y dejarlo en `/root/`. Debe ejecutar dentro del vmplayer el siguiente comando:

```
scp redes06@192.168.185.1:/ruta/real/captureFING.pcap /root/
```