

# Seguridad en Sistemas de Información: Tarea 1

Jorge E. Chávez Saab

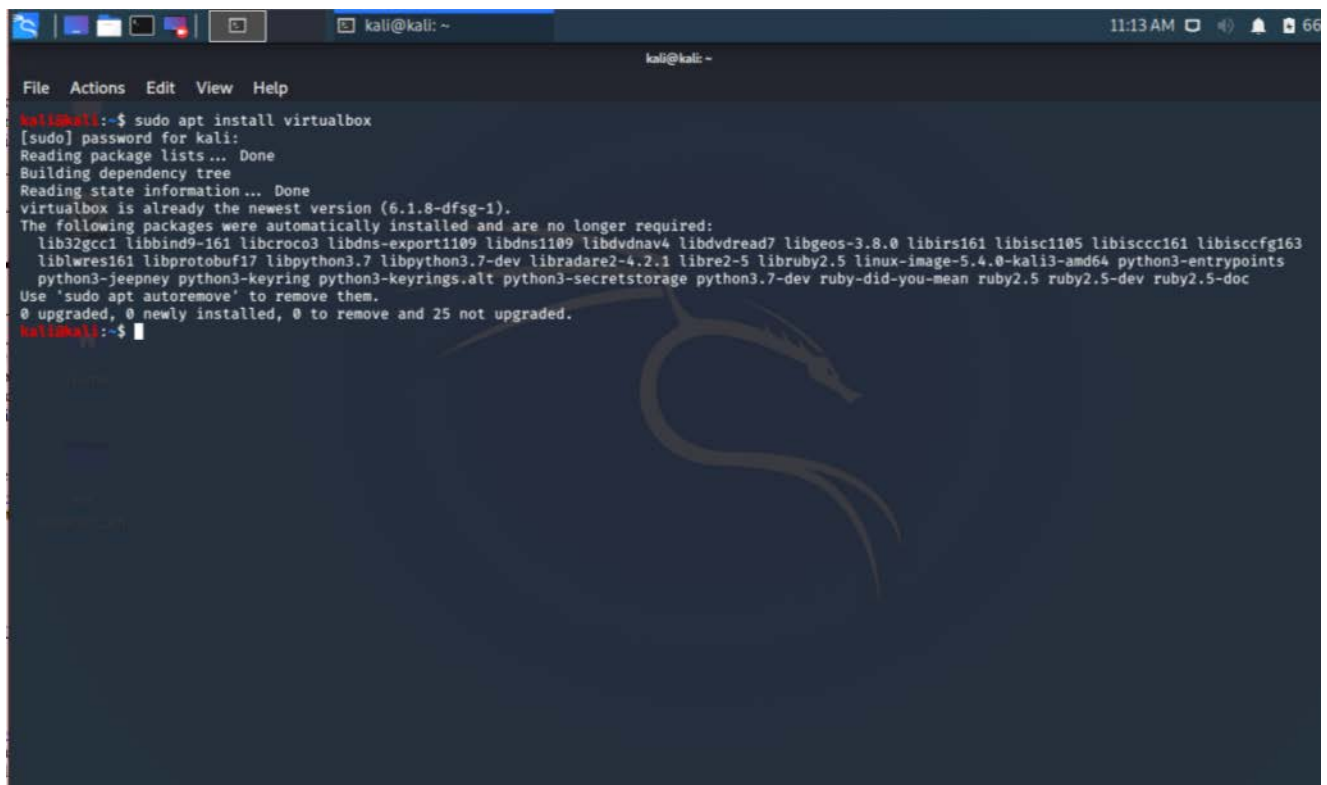
CINVESTAV-IPN

10 de Junio 2020

En esta práctica realizamos los pasos para generar una imagen de un sistema Linux mínimo usando la distribución Kali y el arrancador Grub, y posteriormente lo iniciamos en una máquina virtual usando Virtual Box.

## 1. Instalacion de VirtualBox

Primero verificamos que VirtualBox ya está instalado en la máquina:



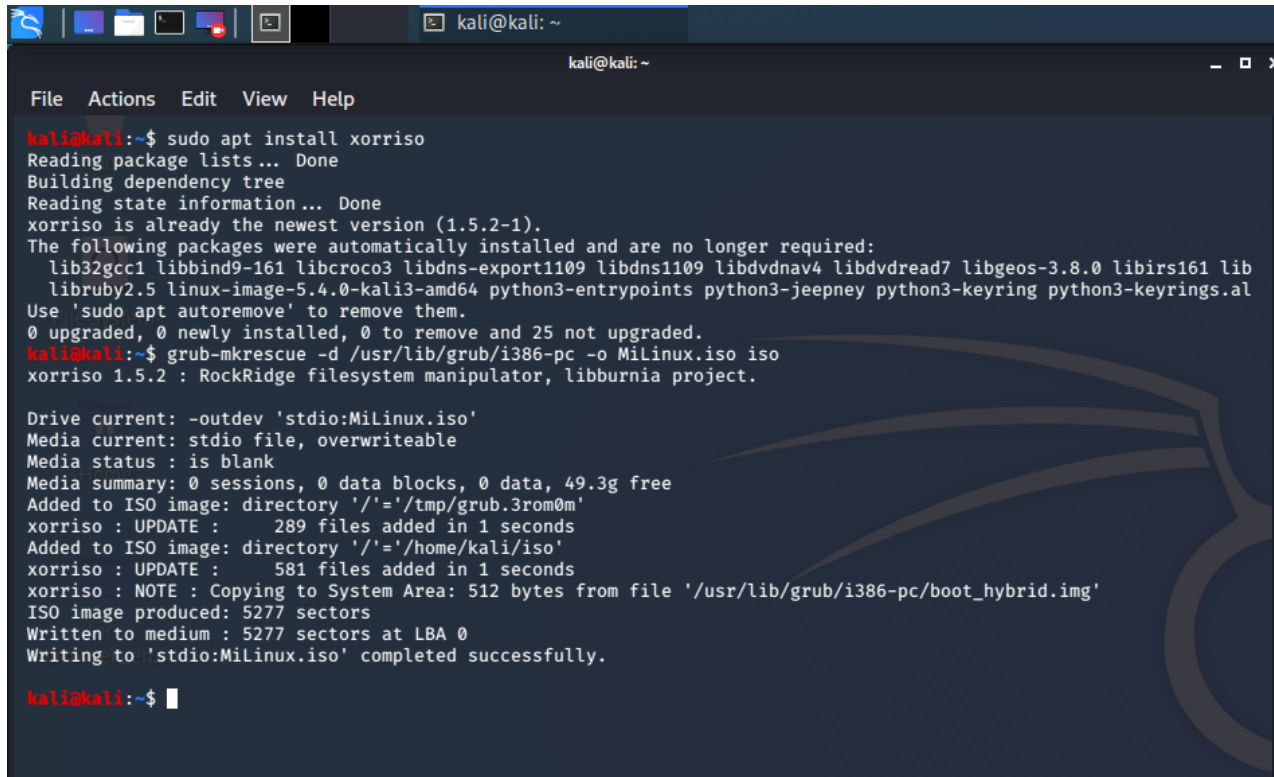
```
kali@kali:~$ sudo apt install virtualbox
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
virtualbox is already the newest version (6.1.8-dfsg-1).
The following packages were automatically installed and are no longer required:
 lib32gcc1 libbind9-161 libcroco3 libdns-export1109 libdns1109 libdvdnav4 libdvdread7 libgeos-3.8.0 libirs161 libisc1105 libisccc161 libiscfg163
 liblwres161 libprotobuf17 libpython3.7 libpython3.7-dev libradare2-4.2.1 libre2-5 libruby2.5 linux-image-5.4.0-kali3-amd64 python3-entrypoints
 python3-jeepney python3-keyring python3-keyrings.alt python3-secretstorage python3.7-dev ruby-did-you-mean ruby2.5 ruby2.5-dev ruby2.5-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 25 not upgraded.
kali@kali:~$
```

## 2. Creación del archivo .iso

Descargamos el archivo .iso disponible usando el comando `wget`, después lo montamos usando



```
grub-mkrescue -d /usr/lib/grub/i386-pc -o MiLinux.iso iso
```



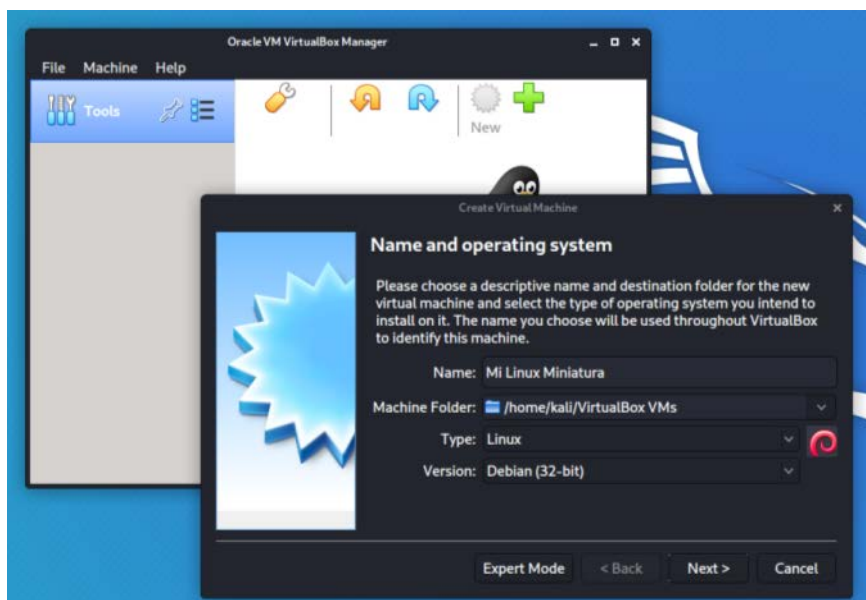
```
kali@kali:~$ sudo apt install xorriso
Reading package lists... Done
Building dependency tree
Reading state information... Done
xorriso is already the newest version (1.5.2-1).
The following packages were automatically installed and are no longer required:
  lib32gcc1 libbind9-161 libcroco3 libdns-export1109 libdns1109 libdvdnv4 libdvdread7 libgeos-3.8.0 libirs161 lib
  libruby2.5 linux-image-5.4.0-kali3-amd64 python3-entrypoints python3-jeepney python3-keyring python3-keyrings.al
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 25 not upgraded.
kali@kali:~$ grub-mkrescue -d /usr/lib/grub/i386-pc -o MiLinux.iso iso
xorriso 1.5.2 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:MiLinux.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 49.3g free
Added to ISO image: directory '/'='/tmp/grub.3rom0m'
xorriso : UPDATE :      289 files added in 1 seconds
Added to ISO image: directory '/'='/home/kali/iso'
xorriso : UPDATE :      581 files added in 1 seconds
xorriso : NOTE : Copying to System Area: 512 bytes from file '/usr/lib/grub/i386-pc/boot_hybrid.img'
ISO image produced: 5277 sectors
Written to medium : 5277 sectors at LBA 0
Writing to 'stdio:MiLinux.iso' completed successfully.

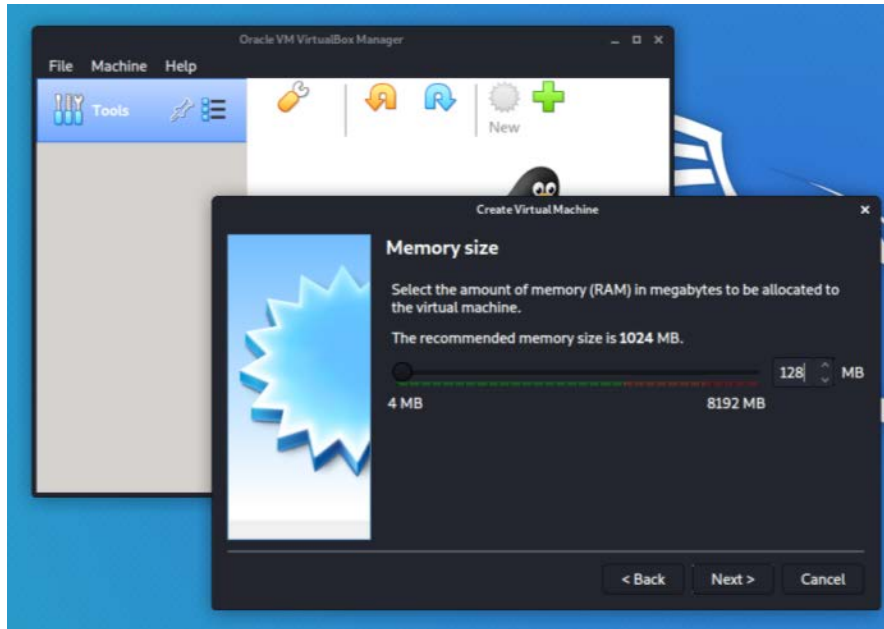
kali@kali:~$
```

### 3. Creación de la Máquina Virtual

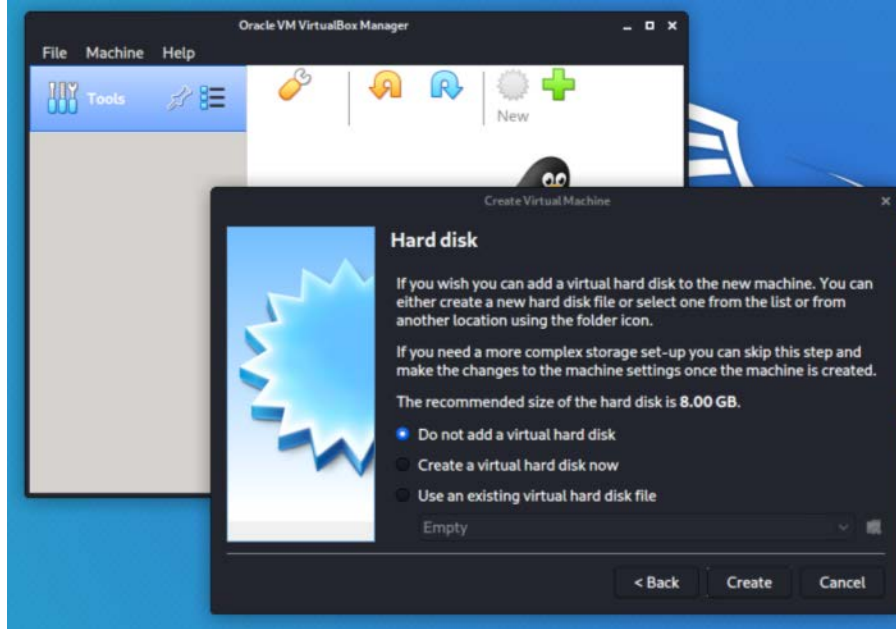
Ejecutamos VirtualBox y elegimos la opción para crear una nueva máquina.



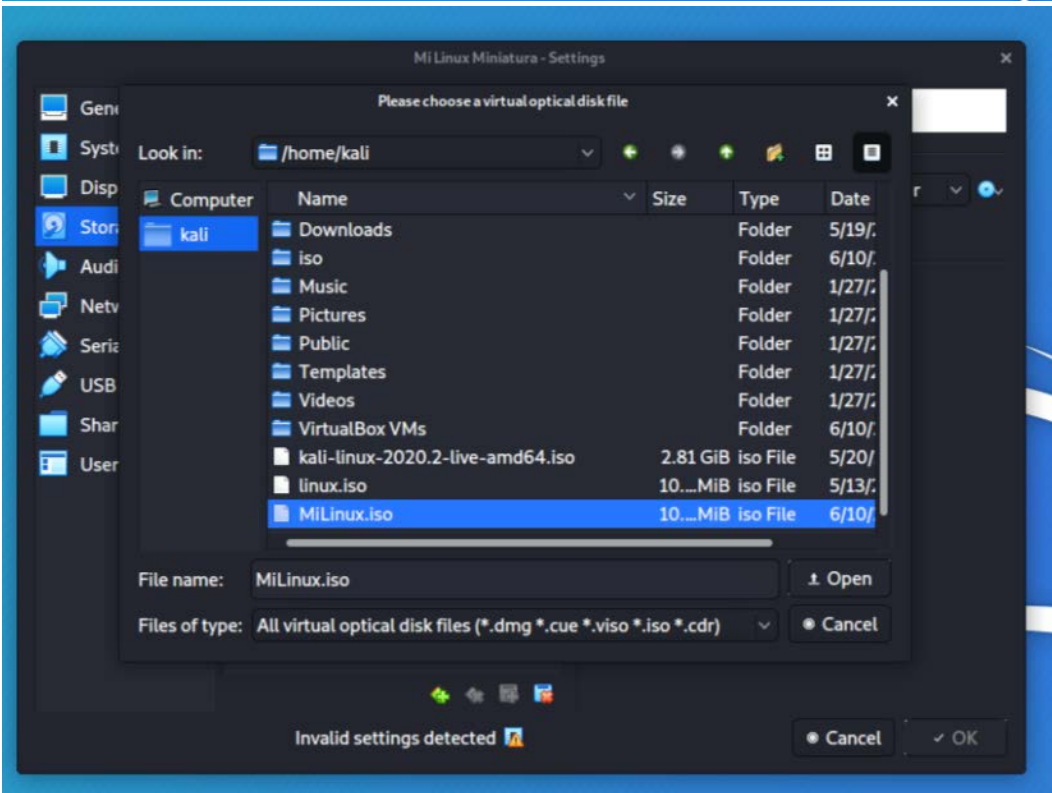
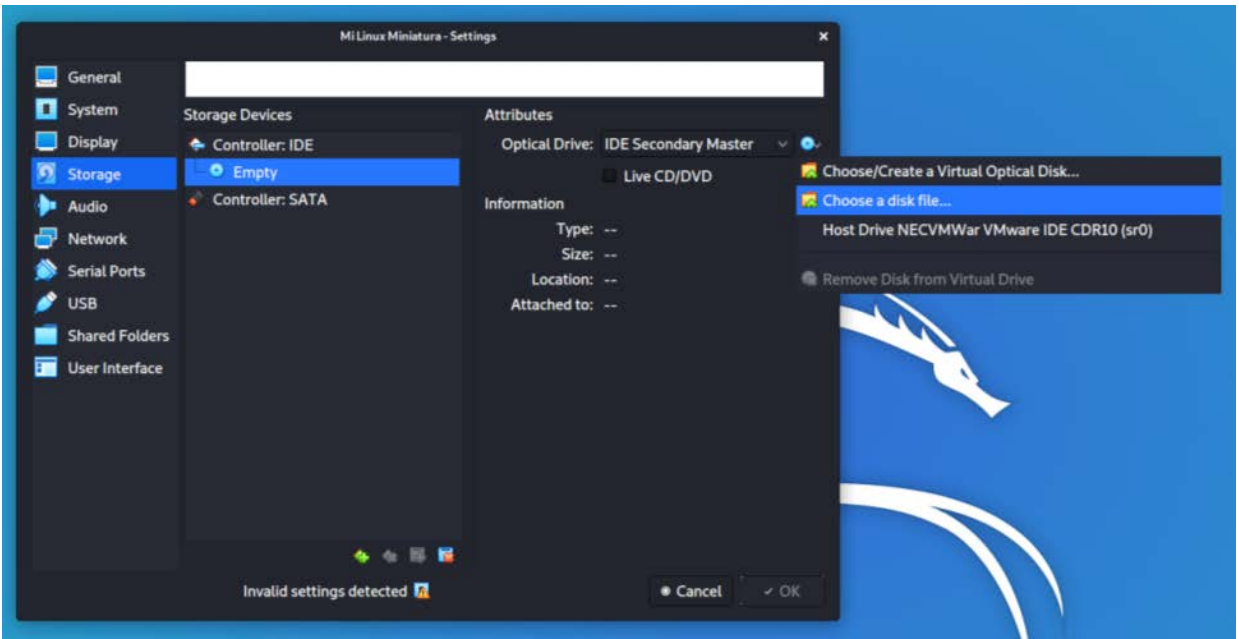
Asignamos 128 MB de memoria



y elegimos la opción para no agregar ningún disco duro.



Una vez creada la máquina vamos a su configuración y bajo el menú Storage>Controller: IDE>Empty elegimos la opción para añadir un archivo de imagen, y seleccionamos el MiLinux .img que acabamos de generar.



Finalmente arrancamos la máquina, y confirmamos los cambios en los mensajes.

```
GNU GRUB version 2.04-5kali1

*Mi Linux Miniatura

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 1s.
```

```
Booting 'Mi Linux Miniatura'
Cargando..
```

Como se esperaba, entramos en Kernel panic inmediatamente porque no hemos hecho un sistema de archivos.

```
[ 0.468596] rtc_cmos 00:01: setting system clock to 2020-06-10T19:02:09 UTC
1591815729)
[ 0.468694] List of all partitions:
[ 0.468717] No filesystem could mount root, tried:
[ 0.468718]
[ 0.468760] Kernel panic - not syncing: UFS: Unable to mount root fs on unknown-block(0,0)
[ 0.468804] CPU: 0 PID: 1 Comm: swapper/0 Not tainted 5.5.0-kali2-amd64 #1 Debian 5.5.17-1kali1
[ 0.468849] Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 02/27/2020
[ 0.468902] Call Trace:
[ 0.468925] dump_stack+0x66/0x90
[ 0.468947] panic+0x101/0x2d7
[ 0.468969] mount_block_root+0x310/0x31f
[ 0.468994] prepare_namespace+0x136/0x165
[ 0.469020] kernel_init_freeable+0x1cd/0x1d8
[ 0.469046] ? rest_init+0xaa/0xaa
[ 0.469068] kernel_init+0xa/0x106
[ 0.469091] ret_from_fork+0x35/0x40
[ 0.469158] Kernel Offset: 0x35c00000 from 0xffffffff81000000 (relocation range: 0xffffffff80000000-0xffffffffbfffffff)
[ 0.469281] ---[ end Kernel panic - not syncing: UFS: Unable to mount root fs on unknown-block(0,0) ]---
```