

Taller BRS - Backup MBR - Microsoft Windows



ESCENARIO

Máquina virtual ou física:

RAM \leq 2048MB CPU \leq 2 PAE/NX habilitado

Sistema operativo instalado: Microsoft Windows 64bits

ISO/CD/DVD/USB: Kali Live amd64

BIOS: Permite arranque dispositivo extraíble: CD/DVD, USB



LIMITACIÓN DE RESPONSABILIDADE O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

1. Realizar os puntos 1, 2 e 3 da práctica **1-Taller-BRS-Practica-Allow-Boot-CD-USB-Windows.pdf**



2. Unha vez comprobado o correcto arranque do sistema realizamos un apagado normal do sistema operativo

Backup MBR

3. Arrancar coa Kali Live amd64

Na contorna gráfica abrir un terminal e executar:

kali@kali:~\$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.

kali@kali:~\$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)

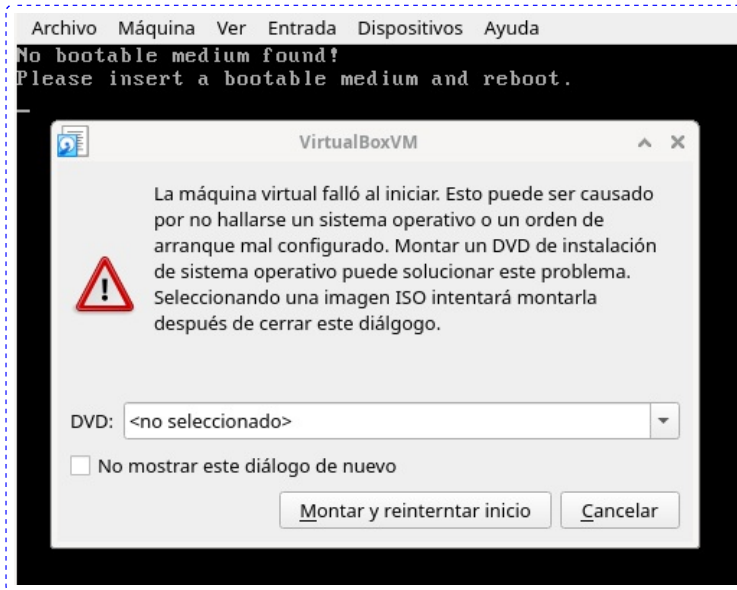
root@kali:~# dd if=/dev/sda of=/home/kali/Desktop/backup-mbr.dd bs=512 count=1 status=progress

#Crear mediante o comando *dd* un ficheiro baleiro chamado *backup-mbr.dd* (if=input file), na ruta */home/kali/Desktop*, de 512B co volcado do MBR do dispositivo */dev/sda* (of=output file). O parámetro *bs=512* establece o tamaño do bloque a 512 bytes e *count=1* especifica que se copie 1 bloque. O indicador *status=progress* amosa o progreso do proceso.

4. Mediante o uso de "Carpetas Compartidas" de VirtualBox copiar o ficheiro *backup-mbr.dd*, situado no escritorio do usuario *kali*, a un cartafol do voso sistema operativo anfitrión.

MBR corrupto

5. Imos provocar o mal funcionamento do MBR. Así, executar na anterior consola de *root*
`root@kali:~# dd if=/dev/zero of=/dev/sda bs=512 count=1 status=progress` #Corromper o MBR mediante o comando *dd*. O parámetro *bs=512* establece o tamaño do bloque a 512 bytes e *count=1* especifica que se copie 1 bloque. O dispositivo */dev/zero* en if(input file) fai que se volquen bytes "ceros" no MBR no dispositivo */dev/sda* (of=output file). O indicador *status=progress* amosa o progreso do proceso.
`root@kali:~# init 0` Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.
6. Arrancar co sistema operativo Microsoft Windows instalado no disco duro. Agora o MBR está corrupto polo cal non podemos arrancar o sistema operativo xa que non existe información sobre o particionado nin o xestor de arranque.



Recuperación do MBR

7. Arrancar coa Kali Live amd64
8. Mediante o uso de "Carpetas Compartidas" de VirtualBox copiar o ficheiro *backup-mbr.dd* do voso sistema operativo anfitrión ao Escritorio (do usuario *kali*)
9. Na contorna gráfica abrir un terminal e executar:
`kali@kali:~$ setxkbmap es` #Cambiar o mapa de teclado ao idioma español.
`kali@kali:~$ sudo su -` #Acceder á consola de root(administrador) a través dos permisos configurados co comando `sudo` (/etc/sudoers, visudo)
`root@kali:~# dd if=/home/kali/Desktop/backup-mbr.dd of=/dev/sda bs=512 count=1 status=progress` #Volcar mediante o comando *dd* o ficheiro chamado *backup-mbr.dd* (if=input file) de 512B ao MBR do dispositivo */dev/sda* (of=output file). O parámetro *bs=512* establece o tamaño do bloque a 512 bytes e *count=1* especifica que se copie 1 bloque. O indicador *status=progress* amosa o progreso do proceso.
`root@kali:~# init 0` Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.
10. Comprobar que é posible de novo arrancar co sistema operativo Microsoft Windows instalado no disco duro debido á recuperación do MBR.