Práctica Seguridade Informática
Allow Boot dispositivo extraíble: CD/DVD/USB - GNU/Linux

ESCENARIO

Máquina virtual ou física:
RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado
Sistema operativo instalado: GNU/Linux 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.

NOTAS:

- **Instalación por defecto**: A instalación do sistema operativo GNU/Linux realizouse por defecto, é dicir, seguindo os pasos do instalador:
  - Táboa de particións msdos
  - Unha partición primaria e unha lóxica:
    - Raíz do sistema: /dev/sda1 (/). Formato: ext4
    - Swap: /dev/sda5 (swap). Formato: swap
  - Nome de usuario: usuario
  - Nome computador: usuario-pc
  - Contrasinal: abc123. (Ollo que o contrasinal ten un caracter punto final)
- **Apagado normal do sistema operativo**: Para un correcto funcionamento da práctica o sistema operativo GNU/Linux debe ser apagado sen inconsistencias evitando problemas no sistema de ficheiros ext4.
- **Práctica chroot**

Práctica

Arrancar coa Kali Live amd64

1. Na contorna gráfica abrir un terminal e executar:

$ setxkbmap es #Cambiar o mapa de teclado ao idioma español.
$ sudo su - #Acceder á consola de root(administrador) a través dos permisos configurados co comando sudo (/etc/sudoers, visudo)
# mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
# fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.
# mkdir /mnt/recuperar #Crear o directorio /mnt/recuperar.
# mount -t auto /dev/sda1 /mnt/recuperar #Montar a partición 1 do disco duro /dev/sda no directorio da live /mnt/recuperar. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe..
# mount --bind /dev /mnt/recuperar/dev # Montar o cartafol /dev dentro de /mnt/recuperar/dev para poder ter acceso a todos os dispositivos recoñecidos pola distribución live.
A opción --bind permite facer uso do mesmo sistema de ficheiros en 2 lugares distintos. Por exemplo, /dev pode ser empregado en /dev e en /mnt/recuperar/dev
mount --bind /proc /mnt/recuperar/proc #Montar o cartafol /proc dentro de /mnt/recuperar/proc para poder ter acceso ao kernel grazas a distribución live.
mount --bind /sys /mnt/recuperar/sys #Montar o cartafol /sys dentro de /mnt/recuperar/sys para poder ter acceso ao kernel grazas a distribución live.
chroot /mnt/recuperar /bin/bash #Crear a xaula chroot. Con este comando creamos unha xaula: un entorno pechado para a distribución Linux dentro de recuperar, de tal xeito, que unha vez dentro da xaula soamente existe ésta, e dicir, soamente existe a distribución Linux instalada no disco duro /dev/sda a recuperar, xa non estamos traballando na Live.
passwd usuario #Modificar o contrasinal do usuario de nome usuario. Pór como contrasinal 1234. Repetir o contrasinal. Ollo: Non aparecen asteriscos nin outro tipo de caracteres para impedir saber cantos e cales caracteres estamos a escribir.
passwd root #Modificar o contrasinal do usuario root. Pór como contrasinal 1234. Repetir o contrasinal. Ollo: Non aparecen asteriscos nin outro tipo de caracteres para impedir saber cantos e cales caracteres estamos a escribir.
exit #Saír da xaula chroot para voltar á consola local do usuario root.
umount /mnt/recuperar/dev /mnt/recuperar/proc /mnt/recuperar/sys /mnt/recuperar #Desmontar as unidades montadas.
init 0 #Comando para enviar o runlevel (nivel de execución) do sistema operativo ao nivel 0, equivalente a apagar o sistema.

Arrancar a máquina GNU/Linux sen o dispositivo extraíble conectado

$ Comprobar que agora o contrasinal do usuario de nome **usuario** foi modificada.

$ Comprobar que agora o contrasinal do usuario **root** foi modificada.

Ricardo Feijoo Costa