Práctica Seguridade Informática Allow Boot dispositivo extraíble: CD/DVD/USB chntpw

ESCENARIO

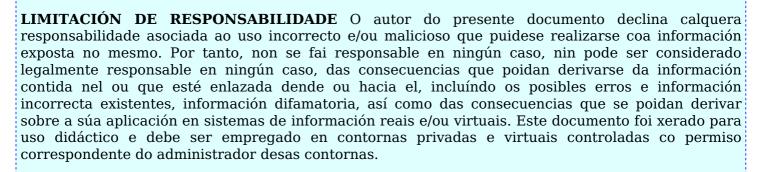
Máquina virtual ou física:

RAM ≤ 2048MB CPU ≤ 2 PAE/NX habilitado Sistema operativo instalado: Microsoft Windows 64bits

Rede: DHCP (NAT)

ISO/CD/DVD/USB: Live amd64 - Calquera distribución baseada en Debian

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



NOTAS:

Instalación por defecto: A instalación do sistema operativo Microsoft Windows realizouse po	or
defecto, é dicir, seguindo os pasos do instalador.	

Avisar ao docente para a revisión \square_1

Apagado normal do sistema operativo: Para un correcto funcionamento da práctica o sistema
operativo Microsoft Windows debe ser apagado sen inconsistencias evitando problemas no sistema
de ficheiros NTFS.

Avisar ao docente para a revisión \square_2

1. Arrancar coa distro Live amd64 baseada en Debian

2. Abrir un terminal e executar:

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

- # fdisk -l /dev/sda #Lista a táboa de particións do disco /dev/sda e logo remata.
- # mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali.
- # mount -t auto /dev/sda2 /mnt #Montar a partición 2 do disco duro /dev/sda no directorio da live /mnt. Coa opción -t auto solicitamos ao comando mount a autodetección do sistema de ficheiros de montaxe. Poderiamos tamén empregar o comando ntfs-3g /dev/sda2 /mnt , o cal xa traballa directamente co sistema de ficheiros NTFS..
- # mount #Amosar os sistemas de ficheiros montados, é dicir, os que está a usar e podemos empregar neste sistema operativo live Kali. Neste caso verificamos que a última liña refírese ao punto de montaxe /mnt onde podemos traballar coa partición /dev/sda2.
- # cd /mnt/Windows/System32/config #Acceder ao directorio do sistema operativo Microsoft Windows C:\Windows\System32\config, o cal está montado en /mnt/Windows/System32/config
- # ls -l SAM #Listar de forma extendida o ficheiro SAM, o cal é o administrador de contas de seguridade (SAM): unha base de datos que atópase en equipos que executan sistemas operativos Microsoft Windows e que almacenan as contas de usuario e os descriptores de seguridade dos usuarios no equipo local.
- # file SAM #Determinar que tipo de ficheiro é o ficheiro SAM. Neste caso é un ficheiro de rexistro Microsoft Windows, NT/2000 ou superior.

	# dhclient -v eth0 #Solicitar a configuración de rede por DHCP para a interface eth0. A opción -v(verbose) amosa a saída do comando en modo detallado.
	# apt-get update #Actualizar o listado de paquetes dos repositorios (/etc/apt/sources.list, /etc/apt/sources.list.d/) # apt-cache search chntpw #Buscar calquera paquete que coincida co patrón de búsqueda chntpw # apt-get -y install chntpw #Instalar o paquete chntpw, é dicir, instalar o programa chntpw. Co parámetro -y automaticamente asumimos yes a calquera pregunta que ocorra na instalación do paquete. # chntpw -l SAM #Listar todos os usuarios da base de datos SAM e saír. O comando chtnpw é unha utilidade que permite sobreescribir contrasinais de sistemas operativos Microsoft Windows
	Avisar ao docente para a revisión \square_3
	# chntpw -u Administrador SAM #Modificar o usuario Administrador, o cal debe existir na SAM, é dicir, debe existir na saída do comando anterior.
	No menú que aparece escollemos as opcións $1 \to \mathbf{q} \to \mathbf{y}$ para pór o contrasinal en branco, e grabar os cambios á SAM. Poderiamos tamén executar o comando chntpw -i SAM , o que nos permite interactuar co programa e elixir distintas opcións de menú.
	# cd #Acceder ao directorio de traballo do usuario, neste caso, acceder a /root # umount /mnt #Desmontar (deixar de facer uso) a partición primaria /dev/sda2 que estaba montada en /mnt
	Avisar ao docente para a revisión \square_4
	# init 0 #Apagar a máquina enviando o sinal de apagado mediante o runlevel 0
3.	Arrancar a máquina Windows sen o dispositivo extraíble conectado
4.	Comprobar que agora o contrasinal do usuario de nome Administrador foi modificada, é dicir, comprobar que o usuario <i>Administrador</i> accede sen contrasinal.
5.	Avisar ao docente para a revisión \square_5
6.	Que é o que acontece se o sistema operativo Microsoft Windows é un servidor de dominio? Por que?
7.	Avisar ao docente para a revisión \square_6



This work is licensed under a **Creative Commons Attribution-ShareAlike 4.0 International License**