

Taller BRS - Allow Boot CD/DVD/USB

MS Windows - chntpw

ESCENARIO

Máquina virtual ou física:

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

Sistema operativo instalado: Microsoft Windows Server 2019 64bits

Rede: DHCP (NAT)

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

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 **Microsoft Windows Server 2019** realizouse por defecto, é dicir, seguindo os pasos do instalador,
- **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.
- **chntpw**

Práctica

Arrancar coa distro Live amd64 baseada en Debian

1. 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. Poderíamos 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 descriptors 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 chntpw é unha utilidade que permite sobreescribir contrasinais de sistemas operativos Microsoft Windows
# 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:

- **2** para desbloquear (unlock) o usuario
- **1 → q → y** para pór o contrasinal en branco, e grabar os cambios á SAM.

Poderíamos 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
# init 0 #Apagar a máquina enviando o sinal de apagado mediante o runlevel 0
```

Arrancar a máquina Windows sen o dispositivo extraíble conectado

- Comprobar que agora o contrasinal do usuario de nome **Administrador** foi modificada, é dicir, comprobar que o usuario *Administrador* accede sen contrasinal.
- Que é o que acontece se o sistema operativo Microsoft Windows é un servidor de dominio?

Pasaría o mesmo, é dicir, desbloquearíase e eliminaríase o contrasinal, no caso de existir, da **conta local** do usuario Administrador.
O comando **chntpw** serve para modificar soamente contas locais: SAM