Utilidades

- http://technet.microsoft.com/es-es/sysinternals/bb795534

PStools

https://learn.microsoft.com/es-es/sysinternals/downloads/pstools

Paquete con diversas herramientas:

- PsExec : ejecución de procesos de forma remota
- PsFile : muestra los archivos abiertos de forma remota
- PsGetSid : muestra el SID de un equipo o un usuario
- PsInfo : lista de información sobre un sistema
- PsPing : medición del rendimiento de la red.
- PsKill : eliminación de procesos por nombre o identificador de proceso
- PsList : enumerar información detallada sobre los procesos
- PsLoggedOn : consulte quién ha iniciado sesión localmente y a través del uso compartido de recursos (se incluye el origen completo).
- PsLogList : volcado de registros de eventos
- PsPasswd : cambia las contraseñas de la cuenta
- PsService : ver y controlar los servicios
- PsShutdown : apaga y, opcionalmente, reinicia un equipo.
- PsSuspend : suspende los procesos
- PsUptime: muestra cuánto tiempo se ha estado ejecutando un sistema desde su último reinicio (la funcionalidad de PsUptime se ha incorporado a PsInfo).

https://archive.geant.org/projects/gn3/geant/services/edupert/Documents/PSNC_psping-for-edupert-vc-v1.pdf

PSPing

```
psping destino:puerto
```

Monitorización

GhostBuster

Permite ver ventanas ocultas que pueden ser utilizadas por troyanos para enviar y recibir comandos

```
ghostbuster.exe -r
```

el -r identifica ventanas ocultas cuya clase sea 'IEFrame' o 'ConsoleWindowClass'

http://sbdtools.googlecode.com/files/GhostBuster.zip

Registro

- Autoruns permite desactivar programas del arranque de windows
  http://technet.microsoft.com/es-es/sysinternals/bb963902.aspx

Enlaces

http://www.securitybydefault.com/search/label/herramientas

UNIX

Diversas herramientas de unix portadas a windows http://unxutils.sourceforge.net/

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=windows:herramientas

Last update: **282023/03/ 11:10**