coggle
made for free at coggle.it

Windows

Herramientas basicas
- tasklist
- powercfg
- assoc
- ping
- Ipconfig
- netstat
- traceroute
- driverquery
- SFC

Algunos archivos clave
- explorer.exe
- hal.dll
- ntdetect.com
- ntbotdd.sys
- winlogon.exe

Conocerlo nos permite:
- Detectar anomalias
- Analizar instalaciones limpias
- Familiarizarnos con el Sistema
- Entender el proceso de Ararnque

Registro de Eventos — **Tipos**
- Sistema
- Seguridad
- Aplicaciones

Directorios Clave
- C:\Windows\System32\
- C:\Users\{NombreDeusuario}\
- C:\Archivos de Programa\
- C:\Archivos de Programa(x86)

Registro — **Clasificacion**
- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG