Building Drivers with EWDK

Developed and Presented by :

CodeMachine

Security Research, Development and Training

www.codemachine.com
twitter.com/codemachineinc
facebook.com/codemachineinc

Build, Deploy and Debug Drivers

- Launch a Enterprise WDK build window
- Build the driver (msbuild /p:configuration=debug /p:platform=x64 /p:targetversion=windows10)
- Copy the driver binary to the VM's staging directory
- Copy the driver from the staging directory to the c:\windows\system32\drivers directory
- Copy scripts\install.driver.cmd to the VM's staging directory
- Install the driver in the VM (install.driver.cmd ***driver***)
  - Do not include the (.sys) extension
- Start the driver (sc start ***driver***)
- Test and Debug the driver
- Stop the driver (sc stop ***driver***)

Build, Deploy and Debug Steps