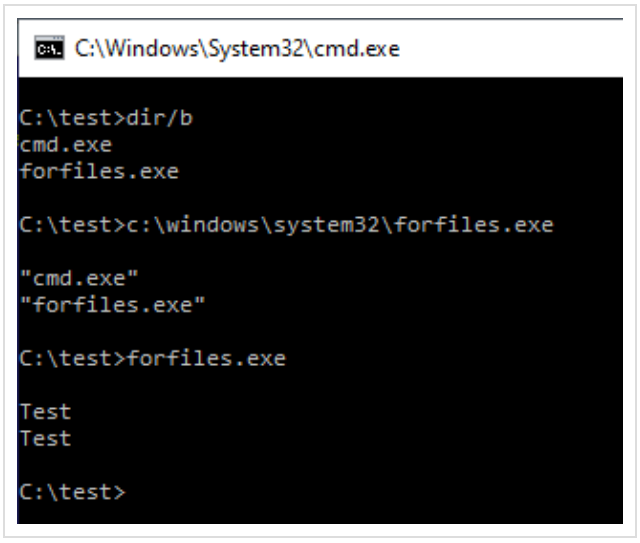
1 little known secret of forfiles.exe

The *forfiles.exe* program is a well-known lolbin. Its power comes from the */c* command line argument that helps to specify a command that we want to execute for each item found by the program when it enumerates directories.

The less known fact about *forfiles.exe* is that executing the program itself, without any option, leads to *cmd.exe* being spawn for every item enumerated. This is because its default command is *cmd /c echo @file*.

As such, one can copy *forfiles.exe* to a different directory, and place malicious *cmd.exe* there. Running *forfiles.exe* without any command line argument (or a combination without */c* argument) will still launch malicious *cmd.exe*!



This entry was posted in **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.