

Forum: [Hack Forums](#)

Thread: [Methods of code injection and places/books to learn about them](#)

hansbald - *October 18, 2018, 9:00 am*

Hello,

I am currently in university learning netsec and advanced cryptography as part of my CS.

I know of a few code injection methods:

Process Hollowing (runPE)

Process Doppelganging

Atombombing

Now, I want to REALLY understand them. I dont want to copy some RunPE code and alter it slightly, I want to really learn how these things work.

Is there a place or book you can recommend that explains everything about how Windows handles executables, what every part of the PE Header does etc etc

I find this really interesting and want to learn more

HFDone - *October 18, 2018, 10:21 am*

https://en.wikipedia.org/wiki/Portable_Executable

<https://docs.microsoft.com/en-us/windows/desktop/debug/pe-format>

"I dont want to copy some RunPE code and alter it slightly, I want to really learn how these things work."

copy some RunPE code and learn how these things work.

use ide break points ...