1500 - Assembly Language is Too High Level

Friday at 15:00 in 101 Track
45 minutes | Demo, Tool, Exploit
XlogicX*Machine Hacker*

Do you have a collection of vulnerable programs that you have not yet been able to exploit? There may yet still be hope. This talk will show you how to look deeper (lower level). If you've ever heard experts say how x86 assembly language is just a one-to-one relationship to its machine-code, then we need to have a talk. This is that talk; gruesome detail on how an assembly instruction can have multiple valid representations in machine-code and vice versa. You can also just take my word for it, ignore the details like a bro, and use the tool that will be released for this talk: the Interactive Redundant Assembler (irasm). You can just copy the alternate machine code from the tool and use it in other tools like mona, use it to give yourself more options for self-modifying code, fork Hydan (stego) and give it more variety, or to create peace on earth.
XlogicX
XlogicX hacks at anything low level. He's unmasked sanitized IP addresses in packets (because checksums) and crafts his own pcaps with just xxd. He feeds complete garbage to forensic tools, AV products, decompression software, and intrusion detection systems. He made evil strings more evil (with automation) to exploit high consumption regular expressions. Lately he has been declaring war on assembly language (calling it too high-level) and doing all kinds of ignorant things with machine code. More information can be found on xlogicx.net

@XlogicX

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday