1300 - Teaching Old Shellcode New Tricks

Friday at 13:00 in Track 2
45 minutes | Demo
Josh Pitts*Hacker*

Metasploit x86 shellcode has been defeated by EMET and other techniques not only in exploit payloads but through using those payloads in non-exploit situations (e.g. binary payload generation, PowerShell deployment, etc..). This talk describes taking Metasploit payloads (minus Stephen Fewer's hash API), incorporating techniques to bypass Caller/EAF[+] checks (post ASLR/DEP bypass) and merging those techniques together with automation to make something better.
Josh Pitts
Josh Pitts has over 15 years experience conducting physical and IT security assessments, IT security operations support, penetration testing, malware analysis, reverse engineering and forensics. Josh has worked in US Government contracting, commercial consulting, and silicon valley startups. He likes to write code that patches code with other code via The Backdoor Factory (BDF), has co-authored an open-source environmental keying framework (EBOWLA), and once served in the US Marines.

@midnite_runr

#defcon25/by_track/track2/friday #defcon25/By_Day/_Friday