06-Metasploit Lab 01 Setup

Security questions

Please explain the purpose of the following msfvenom options

`-e x86/shikata_ga_nai` This is a encoder used to change the binary order, substitute, XOR, dynamic block ordering, reorder, etc.

- cmd/brace
- cmd/echo
- cmd/generic_sh
- cmd/ifs
- cmd/perl
- cmd/powershell_base64
- cmd/printf_php_mq
- generic/eicar
- generic/none
- mipsbe/byte_xori
- mipsbe/longxor
- mipsle/byte_xori
- mipsle/longxor
- php/base64
- ppc/longxor
- ppc/longxor_tag
- ruby/base64
- sparc/longxor_tag
- x64/xor
- x64/xor_context
- x64/xor_dynamic
- x64/zutto_dekiru
- x86/add_sub

- x86/alpha_mixed
- x86/alpha_upper
- x86/avoid_underscore_tolower
- x86/avoid_utf8_tolower
- x86/bloxor
- x86/bmp_polyglot
- x86/call4_dword_xor
- x86/context_cpuid
- x86/context_stat
- x86/context_time
- x86/countdown
- x86/fnstenv_mov
- x86/jmp_call_additive
- x86/nonalpha
- x86/nonupper
- x86/opt_sub
- x86/service
- x86/shikata_ga_nai
- x86/single_static_bit
- x86/unicode_mixed
- x86/unicode_upper
- x86/xor_dynamic

`--encrypt rc4 --encrypt-key hacker` This encrypt the binary file with the given algorithm and key

`-x cmd.exe` Sets a custom binary template to use