31 – Shellcode Analysis 2

Shellcode Encodings
NOP Sleds
Finding Shellcode
Quiz: FizzBuzz

• Write a program that prints the numbers from 1 to 100. But for multiples of three print “Fizz” instead of the number and for the multiples of five print “Buzz”. For numbers which are multiples of both three and five print “FizzBuzz”
Shellcode Encodings

- During many exploits, shellcode will be copied in memory using strcpy or its equivalent, that is, a loop that copies a string until a null byte is found. In such a case, the shellcode must contain no zero bytes.

- Two common methods of achieving this:
  - Encode each nibble as a printable characters (as was done in Lab19-01.bin. (Desirable because this can yield values in a fixed range such as printable characters.)
  - xor the shellcode with a fixed byte value. (The value must not be any value appearing in the shellcode instructions. Why?)
NOP Sleds

• Shellcode is often prefixed by a long sequence of single-byte instructions such as `nop` (0x90). This is done because the placement of the code in memory may not be exactly known, but a branch to code near the beginning may be able to be arranged in the vulnerable target program.

• Shellcode may substitute another instruction sequence instead to avoid detection. Opcodes in the 0x40 to 0x4f are single-byte increments and decrements that also fall in the range of ASCII characters. e.g. "MALCODE" = 4D 41 4C 43 4F 44 4E 45
Finding Shellcode

- Javascript that contains shellcode often uses a unicode unescape \%u\u{yy}xx (big-endian notation for two bytes) to represent unicode characters. Ascii unescape \%xx can be mixed with unicode unescape.

- Shellcode is often injected into code using the sequence of calls VirtualAllocEx, WriteProcessMemory, and CreateRemoteThread. Finding these function calls and their arguments can help you locate shellcode.

- Sometimes shellcode is embedded in other files (tiff images, pdf documents, RTF documents). See, for example, POC || GTFO 0x02 which is both a document and an operating system.
Next Time

- More Exercises. (I'll announce.)
- Quiz on shellcode chapter (again), so read it one more time.