CLASS 6

Buffer Overflow Lab 2

吴瑞欣-E41614059

1、 详细解释一下 JIT spray 以及 heap spray 是什么?

Heap Spray 漏洞攻击技术的一部分。名为堆喷。Heap Spray 是在 shellcode 的前面加上大量的 slide code（滑板指令）【一般为 NOP{\90}】，组成一个注入代码段。然后向系统申请大量内存，并且反复用注入代码段来填充。这样就使得进程的地址空间被大量的注入代码所占据。然后结合其他的漏洞攻击技术控制程序流，使得程序执行到堆上，最终将导致 shellcode 的执行。

JIT 是 just in time,即时编译技术。使用该技术，可以加速 java 程序的运行速度。 在执行时 JIT 会把翻译过的机器码保存起来，已备下次使用，因此从理论上来说，使用该 JIT 技术能够接近纯编译技术。

JIT apray 的相关资料网上较少，没有查出明确的定义。

2、 解释一下老的 windows 操作系统下面利用 SEH 绕过 DEP 的原理和过程。

SEH：【structured exception handing】结构化处理异常，操作系统给程序设计者提供的异常处理机制。

DEP 是数据执行保护的缩写，【Data Execution Prevention】。 他是一套软硬件技术，能够在内存上执行额外检查以帮助防止在系统上运行恶意代码。其基本原理是将数据所在内存页标识为不可执行，当程序溢出成功转入 shellcode 时，程序会尝试在数据页面上执行指令，此时 CPU 就会抛出异常，而不是去执行恶意指令。

利用 SEH 绕过 DEP 的原理和过程。如下：

启用 DEP 后，就不能使用 pop pop re 地址了，而应采用 pop reg/pop reg/pop esp/ret 指令的地址，指令 pop esp 可以改变堆栈指针，ret 将执行流转移到 nseh 中的地址上（用关闭 NX 例程的地址覆盖 nseh，用指向 pop/pop/pop esp/ret 指令的指针覆盖异常处理器）。