2019 Spring Software Secure

> 该课程引进自雪城大学的软件安全课程。记录最后期末开始的内容。

课程结束掌握的技能

- 使用gdb调试程序
  - info breakpoint 查看断点信息
  - del breakpoint n 删除断电
  - b *0xddddddddd 下断点
  - b func_name 函数入口断点
  - disas main 查看main函数汇编代码
  - run args 带参数运行
  - x/40xw $esp 查看栈信息
- 条件竞争漏洞（dirtycow）
- 格式化字符串漏洞
- 缓冲区溢出漏洞（ret2lib，jmp esp）
- 整形溢出漏洞
- UAF（Spring未讲解）

期末考试题目说明

> 本学期只有12次课，最后考试题目有4道，本人做出来3道，有1题未解答。

- 第一题考察点在于整形溢出和缓冲区溢出。做法是利用缓冲区溢出覆盖函数返回地址为shellcode地址，shellcode藏在环境变量中。
- 第二题考察点只有格式化字符串。利用%hn写入返回地址为shellcode地址。
- 第三题重点考察jmp esp，缓冲区溢出并且要栈上的值覆盖成原值。shellocde藏在栈中。
- 第四题考察利用ret2lib。构造栈中的数据，例外execl函数产生新进程返回必须是有效的函数地址（exit）。

Pre

感谢老师认真授课，从Pre也能学到很多东西。

- 堆喷射攻击，arm平台以及x64平台的栈攻击手段。
- `setuid seteuid setreuid`函数的差别和联系
- `system exexve fork`函数的差别和联系
- `O_WRONLY | O_CREAT | O_EXCL` liunx下open函数的几个模式
- `fprintf printf sprintf snprintf vprintf`函数的差别

总结

课程入门二级制漏洞，去pwnable.kr上也完成了第一层题目。也完成了攻防世界第一层题目。学习了pwntools，srop比较高级一点的栈溢出的攻击手段。堆溢出一直没接触，说到底还是菜。

其他问题

- gdb调试suid程序为啥不能获得root权限
- 栈保护的各种机制
- 地址空间随机化
- 寻找系统中的suid程序
- passwd文件格式
- GOT表的作用