### 第十课

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 主题 | 二进制漏洞的挖掘和利用 | | 负责人 | |  | |
| 授课方式 | 课程+实践 | | 主讲老师级别 | |  | |
| 总课时 | 48 | 理论课时 | 24 | 实践课时 | | 24 |
| 先修课程： | | | | | | |
| 计算机系统安全基础，软件安全，计算机应用系统安全 | | | | | | |
| 课程目标： | | | | | | |
| 1. 漏洞攻击实践 2. 了解各类保护机制的对抗与演进； 3. 掌握漏洞利用环境的搭建与工具使用； 4. 简单的漏洞挖掘； 5. 理解栈溢出、堆溢出、格式化字符串、UAF、整数溢出等各类漏洞的原理与利用技巧； 6. 掌握不同平台下漏洞利用技巧。 | | | | | | |
| 课程内容： | | | | | | |
| 1. 缓冲区溢出漏洞（8课时）  （1）函数调用栈  （2）栈溢出的概念和各类保护机制  （3）rop，srop，brop  （4）堆的实现  （5）unlink，hof，堆喷，uaf，fastbin  2. 其他漏洞（8课时）  （1）格式化字符串  （2）整数溢出  （3）业务逻辑漏洞  （4）条件竞争  3. 漏洞挖掘（8课时）  （1）静态分析  （2）普通fuzz  （3）符号执行fuzz  （4）智能fuzz | | | | | | |
| 课后作业实践: | | | | | | |
|  | | | | | | |
| 实验内容： | | | | | | |
| 1. 漏洞攻击实践（16课时） 2. 漏洞利用工具使用 3. Shellcode开发 4. 栈溢出漏洞 5. 堆溢出漏洞 6. 格式化字符串，整数溢出 7. Windows平台漏洞利用 8. android平台漏洞 9. 内核漏洞利用 10. 路由器漏洞利用 11. Fuzz AFL（8课时） | | | | | | |
| 考核方法： | | | | | | |
| 考试（理论+实践） | | | | | | |
| 参考书籍 | | | | | | |
|  | | | | | | |