序号	章节	课程材料	报告时间	讲授者	报告		演示		备注
					组员1	组员2	组员3	组员4	
1	第一章 漏洞挖掘利用基本知识	1. David Brumley/第二章PPT 2. Eternal War in Memory	2019-9-3	霍玮	~~不可选~~	~~不可选~~	~~不可选~~	~~不可选~~	
2	第二章 模糊测试技术简介	1. 《软件漏洞分析技术》 2. American Fuzzy Lop README	2019-9-3	邹燕燕	~~不可选~~	~~不可选~~	~~不可选~~	~~不可选~~	
3	第三章 控制流劫持漏洞及利用-栈溢出及格式化字符串漏洞	1. Smashing The Stack For Fun And Profit 2. Smashing the Stack in 2011 3. Smashing the stack, an example from 2013 4. StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks	2019-9-10	小组1	俞晨东	孙钰杰	王荣庆	吕坤	
		1. Exploiting Format String Vulnerabilities 2. SEED Book: Wenliang Du. Computer Security: A Hands-on Approach (Chapter 6) 3. ASLR Smack and Laugh Reference	2019-9-10	小组2	刘鹏				
4	第四章 控制流劫持漏洞及利用-堆溢出及其他内存破坏类漏洞	1. Understanding glibc malloc 2. Linux 堆内存管理深入分析 3. Windows 8 Heap Internals	2019-9-17	霍玮	~~不可选~~	~~不可选~~	~~不可选~~	~~不可选~~	
		1. Understanding the heap by breaking it 2. Heap Exploitation 3. Heap Overflows and Double-Free Attacks 4. Exploit writing tutorial part 11 : Heap Spraying Demystified	2019-9-17	小组3	李玉冰	李玥珺	任泽众	范雨琳	
		1. Heap Feng Shui in JavaScript 2. Bypassing Browser Memory Protections: Setting back browser security by 10 years 3. The Art of Leaks: The Return of Heap Feng Shui	2019-9-24	小组4	赵佳旭	曹旭栋	梁朝晖	鲜槟橙	

	章节	课程材料	报告时间	讲授者	报告		演示		备注
					组员1	组员2	组员3	组员4	
5	第五章 代码重用方法	1. Return-Oriented Programming: Systems, Languages, and Applications 2. The Geometry of Innocent Flesh on the Bone: Return-into-libc without Calls (on the x86) 3. Control-Flow Integrity: Precision, Security, and Performance	2019-9-24	小组5	刘心宇	井宇	陈晓惠	侯贵洋	
6	第六章 内核漏洞利用技术介绍	1. FUZE: Towards Facilitating Exploit Generation for Kernel Use-After-Free Vulnerabilities 2. KEPLER: Facilitating Control-flow Hijacking Primitive Evaluation for Linux Kernel Vulnerabilities	2019-10-8	小组6	董超鹏	黄晋涛	李仕杰	胡枭	
7	第七章 模糊测试实践	1. CollAFL: Path Sensitive Fuzzing	2019-10-8	小组7	白云开	张志杰	申卓祥	董国超	
		1. Coverage-based Greybox Fuzzing as Markov Chain Directed Greybox Fuzzing 2. Hawkeye: Towards a Desired Directed Grey-box Fuzzer (CCS 2018)	2019-10-15	小组8	黄振洋	宾浩宇	刘宸睿	丁子恒	
		1. FairFuzz: A Targeted Mutation Strategy for Increasing Greybox Fuzz Testing Coverage 2. REDQUEEN: Fuzzing with Input-to-State Correspondence (NDSS2019) 3. T-Fuzz: fuzzing by program transformation (S&P 2018)	2019-10-15	小组9	李文灏	李兆轩	何玮	陈沛茹	
		1. MOPT: Optimize Mutation Scheduling for Fuzzers 2. VUzzer: Application-aware Evolutionary Fuzzing	2019-10-22	小组10	薄德芳	周怡	王立岩	石鑫	
8	第八章 总结		2019-10-22	霍玮	~~不可选~~	~~不可选~~	~~不可选~~	~~不可选~~	