南方科技大学
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

课程详述

COURSE SPECIFICATION

以下课程信息可能根据实际授课需要或在课程检讨之后产生变动。如对课程有任何疑问，请联系授课教师。

The course information as follows may be subject to change, either during the session because of unforeseen circumstances, or following review of the course at the end of the session. Queries about the course should be directed to the course instructor.

1.	**课程名称 Course Title**	**计算机安全 Computer Security**
2.	**授课院系** **Originating Department**	计算机科学与工程系 Department of Computer Science and Engineering
3.	**课程编号** **Course Code**	CS315
4.	**课程学分 Credit Value**	3
5.	**课程类别** **Course Type**	专业选修课 Major Elective Courses
6.	**授课学期** **Semester**	秋季 Fall
7.	**授课语言** **Teaching Language**	中英双语 English & Chinese **（请保留相应选项 Please only keep the relevant information）**
8.	**授课教师、所属学系、联系方式（如属团队授课，请列明其他授课教师）** **Instructor(s), Affiliation& Contact** **（For team teaching, please list all instructors）**	张锋巍，副教授，计算机科学与工程系 Fengwei Zhang, Associate Professor, Department of Computer Science and Engineering
9.	**实验员/助教、所属学系、联系方式** **Tutor/TA(s), Contact**	无 NA / 待公布 To be announced / 已确定的实验员/助教联系方式 Please list all Tutor/TA(s) **（请保留相应选项 Please only keep the relevant information）**
10.	**选课人数限额(可不填)** **Maximum Enrolment（Optional）**	50

11. 授课方式 Delivery Method

	讲授 Lectures	习题/辅导/讨论 Tutorials	实验/实习 Lab/Practical	其它(请具体注明) Other（Please specify）	总学时 Total
学时数 Credit Hours	32		32		64

12. 先修课程、其它学习要求 Pre-requisites or Other Academic Requirements

熟悉 Unix/Linux 系统
Familiar with Unix/Linux systems

13. 后续课程、其它学习规划 Courses for which this course is a pre-requisite

无
None

14. 其它要求修读本课程的学系 Cross-listing Dept.

无
Not applicable for other departments beside CS.

教学大纲及教学日历 SYLLABUS

15. 教学目标 Course Objectives

本课程主要介绍计算机安全的基本原理，以及常见的攻击手段和防御机制。为了更好的加深对真实世界网络攻击的理解，本课程为学生提供一个可以动手测试的实时软件和网络系统环境。本课程将同时教授攻击手段和防御机制，这样让学生理解现实生活中的攻防对抗。本课程教授的内容主要包括的攻击手段（例如：缓冲溢出、dirty COW、 格式字符串、跨站脚本攻击、返回导向编程），黑客基础（例如：扫描和侦察），防御机制（例如：入侵检测系统、防火墙）。本课程将通过高强度的实验，以及使用真实世界的恶意软件，漏洞利用，防御等来训练学生。

This course aims help students to learn the principles of computer security and understand how various security attacks and countermeasures work. It provides hands-on experience in playing with security software and network systems in a live laboratory environment, with the purpose of understating real-world threats. The course will take both offensive and defense methods to help student explore security tools and attacks in practice. It will focus on attacks (e.g., buffer overflow, dirty COW, format-string, XSS, and return oriented programming), hacking fundamentals (e.g., scanning and reconnaissance), defenses (e.g., intrusion detection systems and firewalls). Students are expected to finish intensive lab assignments that use real-world malware, exploits, and defenses.

16. 预达学习成果 Learning Outcomes

本课程将提供真实世界攻防的深度体验。在课程完成时，学生于应该获得以下技能：

- 理解真实世界中的安全漏洞，攻击利用，以及防御体系。
- 具有网络和系统安全试验的动手经历。
- 学习到计算机安全的基本知识，现实安全问题，以及对应的解决方案。

This course offers an in-depth experience of real-world threats and defence. Upon successful completion of this class, the student will gain experience in:

- Understanding on real-world security vulnerabilities, exploits and defence.
- Having hands-on labs in network and system security experiments.
- Learning knowledge of practical security problems and their solutions.

17. **课程内容及教学日历（如授课语言以英文为主，则课程内容介绍可以用英文；如团队教学或模块教学，教学日历须注明主讲人）**
Course Contents (in Parts/Chapters/Sections/Weeks. Please notify name of instructor for course section(s), if this is a team teaching or module course.)

第一周：课程介绍 & 网络数据包截获

- 课程综述介绍
- 实验虚拟机镜像，Kali Linux – 渗透测试的 Linux 版本
- 计算机网络简要介绍
- 网络数据抓包工具以及网络协议分析工具

[Lab 1]网络数据包截获分析和 Wireshark 软件应用：这个实验主要学习抓包工具像 Wireshark，包括它的安装，怎么截获网络数据包，以及怎么分析篡改网络数据包。

第二周：网络扫描和侦察

- 介绍渗透分析的第一步
- 怎么找到目标电脑以及对应的计算机服务
- Nmap: 开源网络安全扫描工具
- OpenVAS: 开源漏洞分析平台
- NESSUS: 漏洞检测扫描工具

[Lab 2]网络扫描和侦察：这个实验主要学习怎么样应用网络安全扫描工具去侦测目标机器的信息，以及怎么样得到可以利用的漏洞。

Lab 1 截止提交

第三周：渗透测试

- 介绍渗透测试的历史
- Metasploit 平台项目
- Armitage: 基于 Metasploit 的网络空间攻击管理系统

[Lab 3] Metasploit 平台：这个实验主要是用 Metasploit 平台，远程的攻击并且控制一台设定的服务器。

Lab 2 截止提交

第四周：安全编程 & 缓冲溢出

- C 语言基础知识
- 程序内存分部
- Unix 调试器：gdb 介绍
- 堆栈攻击

[Lab 4] 缓冲溢出以及防御（第一部分）：这个实验主要是交学生什么是缓冲溢出以及其它的内存漏洞攻击。实验目标是查看一个先前定义好的程序，然后看怎么样才能够利用缓冲溢出漏洞，拿到 Shell。

Lab 3 截止提交

第五周：学期、团队项目建议讨论

- 对于提交的项目建议想法提供反馈意见
- 确定学期项目队伍和主题

[Lab 5] 缓冲溢出以及防御（第二部分）：这个实验主要是交学生什么是缓冲溢出以及其它的内存漏洞攻击。实验目标是查看一个先前定义好的程序，然后看怎么样才能够利用缓冲溢出漏洞，拿到Shell。

第六周：逆向工程和反逆向

- 逆向工程概念介绍
- 安卓编程介绍
- 安卓字节码，Dalvik 执行文件格式（DEX）
- Smali/baksmali: DEX 的编译和反编译器

[Lab 6] 安卓应用重打包和反逆向：本实验将用安卓应用，交学生怎么样是逆向工程和反逆向。首先，学生会要求写一个安卓应用。然后，学生要通过逆向工程往安卓应用中间添加恶意代码。最后，他们将用反逆向工具去保护这个安卓应用。

Lab 4 & 5 截止提交

第七周：物联网安全以及隐私

- 物联网环境下的安全
- Zephyr: 物联网环境下的实时操作系统
- Brillo: 谷歌物联网操作系统
- Contiki: 物联网环境下的开源操作系统

[Lab 7] 物联网环境下的操作系统安全：本实验将用 Zephyr 操作系统作为例子，然后学习物联网操作系统安全。其中，我们将利用一个缓冲溢出漏洞，攻击 Zephyr 操作系统。

Lab 6 截止提交

第八周：无线网络攻击和防御

- 无线网络安全的挑战
- 路由器，热点
- 中间人攻击
- WPA/WPA2 协议的秘钥获取

[Lab 8] 无线网络攻击和防御：本实验会帮助学生学习无线网络的攻击手段，以及对应的防御机制。

Lab 7 截止提交

第九周：防火墙&入侵检测系统（IDS）

- 防火墙，入侵检测系统，入侵防御系统概念

- 基于特征 vs. 基于行为
- IDS 系统的评估标准：误报率，准确率，漏报率，等等

[Lab 9] 防火墙和入侵检测系统：通过这个时间，学生会学习到 Snort 入侵检测系统。Snort 是一个基于特征的检测系统，学生用这个系统对网络的异常行为进行检测分析。

Lab 8 截止提交

第十周：Dirty COW 攻击

- 竞争条件漏洞介绍
- Linux 内核下面的 Copy-on-write 操作

[Lab 10] Dirt COW 攻击：本实验的目标是让学生理解 Dirty COW 攻击，理解竞争条件漏洞攻击，最后学生会利用 Dirt COW 攻击的竞争条件漏洞，获得 root 权限。

Lab 9 截止提交

第十一周：安全编程 & 格式化字符串漏洞

- 字符串漏洞介绍
- 理解程序栈的结构和分布
- 代码注入，恶意代码，回调 Shell

[Lab 11] 格式化字符串漏洞：这个实验会提供给学生一个具有格式化字符串漏洞的程序。学生需要找到这个漏洞，并成功的利用这个漏洞。

Lab 10 截止提交

第十二周：Web 安全

- 跨站点请求伪造攻击（CSRF）
- 跨站脚本攻击（XSS）
- SQL 注入攻击

[Lab 12] 跨站点请求伪造攻击：在这个实验中，学生会利用 CSRF 攻击一个社交网路上面的应用。这个开源的社交网络叫做 Elgg，它其实有对应的防御机制。对于这个实验，我们将关闭这个防御机制。

Lab 11 截止提交

第十三周：Return-to-libc 和返回导向编程

- 不可执行栈空间
- 攻击不需要代码注入和可执行的栈空间
- 返回导向编程概念，以及怎么找到 ROP 的 gadgets

[Lab 13] Return-to-libc 攻击：在这个实验中，学生会得到一个具有缓冲溢出漏洞的程序。根据这个漏洞，学生要利用它和 return-to-libc 的概念，获得 root 权限。

Lab 12 截止提交

第十四周：Return-to-libc 和返回导向编程（继续）

- 不可执行栈空间
- 攻击不需要代码注入和可执行的栈空间
- 返回导向编程概念，以及怎么找到 ROP 的 gadgets

[Lab 13] Return-to-libc 攻击（继续）：在这个实验中，学生会得到一个具有缓冲溢出漏洞的程序。根据这个漏洞，学生要利用它和 return-to-libc 的概念，获得 root 权限。

第十五周：课程实验总结

[Lab 15] 学期/团队报告 1

Lab 13&14 截止提交

第十六周：学期/团队报告 2

[Lab 15] 学期/团队报告 3

Week 1. **Course Overview & Packet Sniffing**

- Course overview and logistics
- Virtual machine images, Kali Linux - penetration testing Linux distribution
- Computer network basics
- Packet sniffing tools and network protocol analyzer.

[Lab 1] Packet Sniffing and Wireshark: This lab uses Wireshark for the experiments, and it covers Wireshark installation, packet capturing, and protocol analysis.

Week 2. **Scanning and Reconnaissance**

- Introduction to penetration testing
- Finding Hosts, Services
- Nmap: the Network Mapper - Free Security Scanner
- OpenVAS: Open Vulnerability Assessment System
- NESSUS: Vulnerability Scanner

[Lab 2] Scanning and Reconnaissance: This lab will learn how to use tools to scan and retrieve information from a targeting system.

Lab 1 Due.

Week 3. **Penetration Testing**

- History of Pen Testing
- Metasploit Framework Project
- Armitage: Cyber Attack Management for Metasploit

[Lab 3] Metasploit Framework: In this lab, the students will learn how to use Metasploit to gain access to a remote machine.

Lab 2 Due.

Week 4. **Secure Coding & Buffer Overflows**

- C language basics
- Program memory layout
- Debugging under Unix: gdb tutorial
- Smashing the Stack for Fun and Profit. Aleph One. In Phrack Volume 7, Issue 49

[Lab 4] Buffer Overflows and Defenses (Part 1): This lab will teach how buffer overflows and other memory vulnerabilities are used to takeover vulnerable programs. The goal is to investigate a program I provide and then figure out how to use it to gain shell access to systems.

Lab 3 Due.

Term/Team Project Proposal Due.

Week 5. **Term/Team Project Proposal Discussion**

- Provide feedback for the project proposal ideas
- Finalized teams/project topics.

[Lab 5] Buffer Overflows and Defenses (Part 2). This lab will teach how buffer overflows and other memory vulnerabilities are used to takeover vulnerable programs. The goal is to investigate a program I provide and then figure out how to use it to gain shell access to systems.

Week 6. **Reverse Engineering and Obfuscation**

- Reverse engineering concepts
- Introduction to Android programming
- Android bytecode, Dalvik executable (DEX)
- Obfuscation and packing techniques
- smali/baksmali: an assembler/disassembler for the DEX.

[Lab 6] Android Application Repackaging and Obfuscation: This lab will teach how to do reverse engineering and obfuscation for Android applications. First, the students will need to write a simple Android application. Then, they will reverse the byte code of the application by adding a malicious function. Lastly, they will use packers to obfuscate the application and protect it from reverse engineering.

Lab 4 & 5 Due.

Week 7. **Internet of Things Security & Privacy**

- Security in IoT environments
- Zephyr: Real Time OS for IoT - A Linux Foundation Collaborative Project
- Brillo: Google's Operating System for the Internet of Things
- Contiki: The Open Source OS for the Internet of Things

[Lab 7] OS Security for the Internet of Things: In this lab, we use Zehpyr as a study example to explore the OS security of IoT devices. Specifically, we will exploit buffer overflow vulnerabilities in an application and understand the security features of Zephyr OS.

Lab 6 Due.

Week 8. **Wireless Exploitation & Defenses**

- Challenges in protecting wireless networks
- Routers, access point

- Man-in-the-middle attacks
- WPA/WPA2 key cracking

[Lab 8] Wireless Exploitation & Defenses: In this lab students will explore ways to perform wireless attacks and understand potential defenses.

Lab 7 Due.

Week 9. **Firewalls & Intrusion Detection Systems (IDS)**

- Firewalls, intrusion detection systems, intrusion prevent systems
- Signature-based vs. anomaly-based
- IDS evaluation metrics: false positive, false negative, true positive, and true negative

[Lab 9] Firewall & Intrusion Detection Systems: In this lab students will explore the Snort Intrusion Detection Systems. The students will study Snort IDS, a signature-based intrusion detection system used to detect network attacks.

Lab 8 Due.

Week 10. **Dirty COW Attack**

- Race condition concepts
- Copy-on-write operation inside Linux kernel

[Lab 10] Dirty COW Attack: The objective of this lab is for students to gain the hands-on experience on the Dirty COW attack, understand the race condition vulnerability exploited by the attack, and gain a deeper understanding of the general race condition security problems. In this lab, students will exploit the Dirty COW race condition vulnerability to gain the root privilege.

Lab 9 Due.

Week 11. **Secure Coding & Format-String Vulnerability**

- Format string vulnerability
- Understanding the layout of the program stack
- Code injection, shellcode, reverse shell

[Lab 11] Format-String Vulnerability: In this lab, students will be given a program with a format-string vulnerability; their task is to develop a scheme to exploit the vulnerability.

Lab 10 Due.

Week 12. **Web Security**

- Cross-site request forgery attack
- Cross-site scripting (XSS)
- SQL Injection attacks

[Lab 12] Cross-Site Request Forgery Attack: In this lab, students will be attacking a social networking web application using the CSRF attack. The open-source social networking application called Elgg has countermeasures against CSRF, but we have turned them off for the purpose of this lab.

Lab 11 Due.

Week 13. **Return-to-libc & Return Oriented Programming**

- Non-executable stack
- Attacks without an executable stack

- ROP concepts and gadgets finding

[Lab 13] Return-to-libc Attack: In this lab, students are given a program with a buffer-overflow vulnerability; their task is to develop a return-to-libc attack to exploit the vulnerability and finally to gain the root privilege.

Lab 12 Due.

Week 14. **Return-to-libc & Return Oriented Programming (Continue)**

- Non-executable stack
- Attacks without an executable stack
- ROP concepts and gadgets finding

[Lab 14] Return-to-libc Attack (continue): In this lab, students are given a program with a buffer-overflow vulnerability; their task is to develop a return-to-libc attack to exploit the vulnerability and finally to gain the root privilege.

Lab 13 Due.

Week 15. **Course Lab Review**

[Lab 15] Term/Team Project Presentations 1

Lab 14 Due.

Week 16. **Term/Team Project Presentation 2**

[Lab 16] Term/Team Project Presentations 3

18. 教材及其它参考资料 Textbook and Supplementary Readings

Wenliang Du, Computer Security: A Hands-on Approach, ISBN-13: 978-1548367947, ISBN-10: 154836794X

课程评估 ASSESSMENT

19. 评估形式 Type of Assessment	评估时间 Time	占考试总成绩百分比 % of final score	违纪处罚 Penalty	备注 Notes
出勤 Attendance				
课堂表现 Class Performance		8%		课堂和试验参与 Class participation 80 points
小测验 Quiz				
课程项目 Projects		20%		课程项目提议 课程项目报告 课程项目结果 Term project proposal Term proposal presentation Term project report 50 + 50 + 100 = 200 points
平时作业 Assignments		72%		12 个高强度的试验 12 intensive labs 12 X 60 = 720 points
期中考试 Mid-Term Test				
期末考试 Final Exam				
期末报告 Final Presentation				
其它（可根据需要改写以上评估方式） Others (The above may be modified as necessary)				

20. 记分方式 GRADING SYSTEM

☑ A. 十三级等级制 Letter Grading
□ B. 二级记分制（通过/不通过） Pass/Fail Grading

课程审批 REVIEW AND APPROVAL

21. 本课程设置已经过以下责任人/委员会审议通过
This Course has been approved by the following person or committee of authority