网络安全工程与实践

段海新

duanhx@tsinghua.edu.cn

清华大学网络研究院

群聊：网络安全工程与实践
2024 课程群

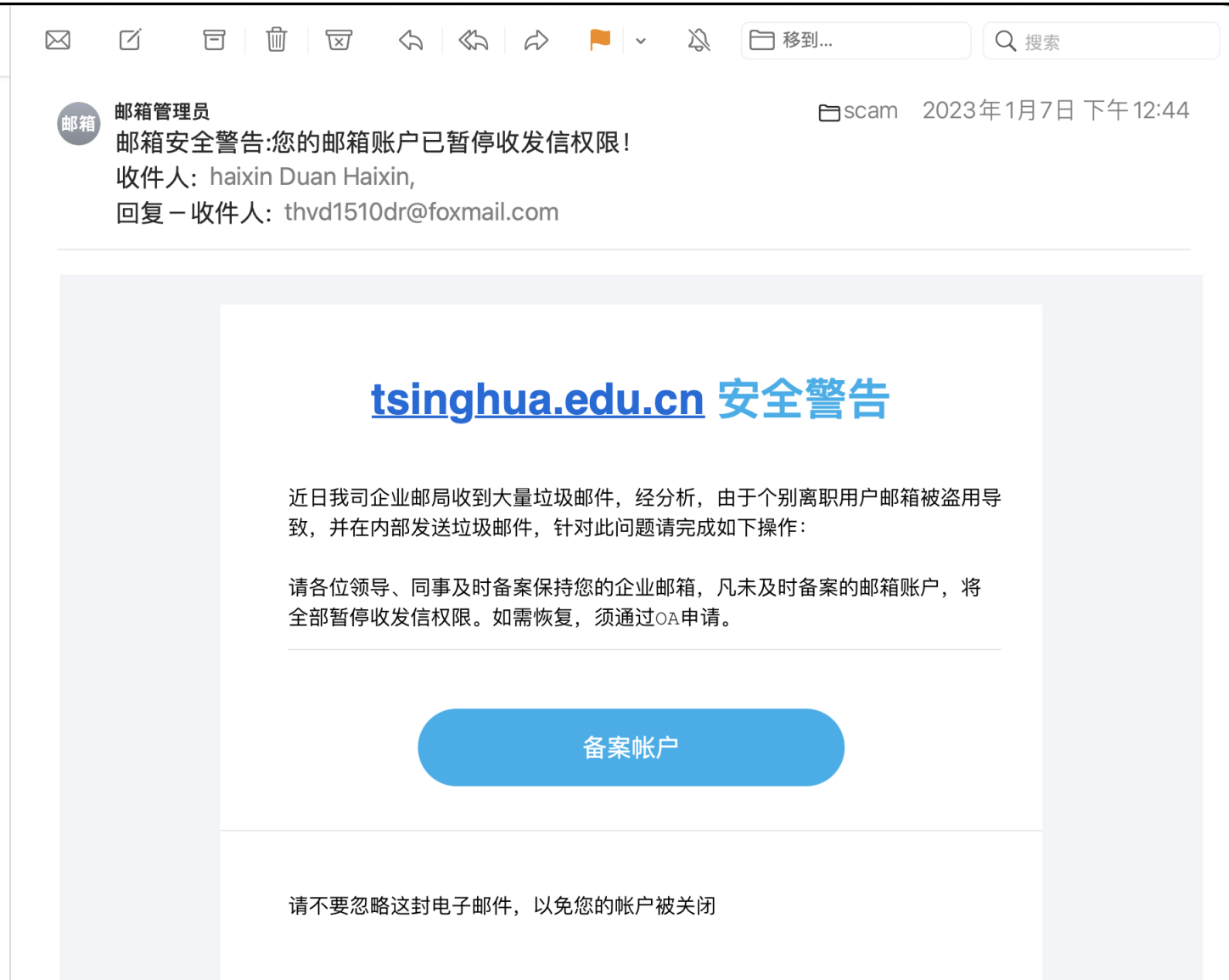
课程信息

- 主讲教师：
  - 段海新，教授：duanhx@tsinghua.edu.cn
  - 张　超，副教授:chaoz@tsinghua.edu.cn
  - 办公室：FIT楼 3-211
- 助教：
  - 邢云鹏，王浩铭
- 时间：第1-16周星期四第6节(7:20-8:55pm)
- 地点：六教6A214

网络空间安全的攻防对抗

- 国家网络空间中的对抗
  - 2013年斯诺登事件
  - 俄乌网络战
- 企业网络和信息安全防护
- 网络犯罪、地下产业、个人隐私防护

你收到多少这样的邮件？



scam — tsinghua.edu.cn
46封邮件

移到...
搜索

邮箱系统 2023/4/15
邮箱管理
《邮箱转移通知》 邮箱系统将在4月15日至16日进行维护、升级、转移至新服务器。 【现需要对邮箱进行报备】 为了避免重要邮件丢失，请及...

升级通知！ 2023/4/13
安全升级：请及时更新邮箱证书，...
系统通知 尊敬的用户您好！ 为加强网络安全管理，提高系统的安全性和稳定性，保障收发畅通，为用户提供优质的服务，现即将启用新版系统，有关事...

Salem Mohamed 2023/4/9
Hello, I Need Your Assistance And...
Greeting Dear Friend, My Name is Mr.Salem Mohamed. from Damascus Syria, and I have now resigned from the government. I am a member of...

邮箱管理员 2023/1/7
邮箱安全警告:您的邮箱账户已暂停...
tsinghua.edu.cn 安全警告 近日我司企业邮局收到大量垃圾邮件，经分析，由于个别离职用户邮箱被盗用导致，并在内部发送垃圾邮件，针对此问题请完...

系统管理员 2023/1/5
duanhx@tsinghua.edu.cn您的密...
tsinghua.edu.cn 密码通知。 你好, duanhx@tsinghua.edu.cn 您的密码 duanhx@tsinghua.edu.cn今天到期请按照以下说明保留您的当前密码并...

邮箱 **邮箱管理员**
scam 2023年1月7日 下午12:44
邮箱安全警告:您的邮箱账户已暂停收发信权限！
收件人：haixin Duan Haixin,
回复－收件人：thvd1510dr@foxmail.com

tsinghua.edu.cn 安全警告

近日我司企业邮局收到大量垃圾邮件，经分析，由于个别离职用户邮箱被盗用导致，并在内部发送垃圾邮件，针对此问题请完成如下操作：

请各位领导、同事及时备案保持您的企业邮箱，凡未及时备案的邮箱账户，将全部暂停收发信权限。如需恢复，须通过OA申请。

备案帐户

请不要忽略这封电子邮件，以免您的帐户被关闭

改变世界的邮件门事件

希拉里团队的竞选主席约翰·波德斯塔收到一封看似来自Google的警告邮件称，有人试图侵入他的账号，需要立即更改邮箱密码。波德斯塔的助手将警告邮件转给技术人员后，得到回复：“这是一封合法邮件”。
随后，波德斯塔的助手放心点开邮件中的钓鱼链接，将波德斯塔近十年来的6000余封邮件拱手送给了黑客。

http://www.sic.gov.cn/News/91/7894.htm

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

ACM:2022年全球安全岗位缺人180万

Chapter 1: Introduction to Cybersecurity Education

By all accounts, the world faces a current and growing workforce shortage of qualified cybersecurity professionals and practitioners. In fact, both government and non-government sources project nearly 1.8 million cybersecurity-related positions going unfilled by 2022[1]. The workforce demand is acute, immediate, and growing[2]. In order to develop the required talent, academic departments across the spectrum of computing disciplines are launching initiatives to establish new cybersecurity programs or courses of study within existing programs. Whether developing full new programs, defining new concentrations within existing programs, or augmenting existing course content, these institutions need curricular guidance based on a comprehensive view of the cybersecurity field, the specific demands of the base discipline, and the relationship between the curriculum and cybersecurity workforce frameworks.

In August 2015, the Association for Computing Machinery (ACM) Education Board recognized this urgent need and took measures to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education.

For nearly five decades, starting with Computer Science 1968[3], the ACM education initiative has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines. Currently, ACM curricular volumes provide recommendations in computer science, computer engineering, information systems, information technology, and software engineering. The ACM Computing Curricula 2005 Report (CC2005), currently being updated, provides an overview of the curriculum guidelines for each of these five computing disciplines[4]. This volume, CSEC2017, represents an expansion of the ACM education initiative to include the first set of global curricular recommendations in cybersecurity education.

Due to the highly dynamic nature of cybersecurity, it is strongly recommended that these curricular guidelines be reviewed within five years of the publication date.

1.1 The Joint Task Force

The CSEC2017 Joint Task Force on Cybersecurity Education (JTF) was officially launched in September 2015 as a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS)[5], Association for Information Systems Special Interest Group on Information

[1] See, for example, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html
[2] (ISC)2 Report available here: https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf
[3] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197.
[4] ACM Computing Disciplines Overview: http://acm.org/education/curricula-recommendations
[5] IEEE CS website: https://www.computer.org/

ACM CSEC 2017 Curricular

- 1968, ACM Education Board
- 2005, curriculum guidelines for 5 computing sub-disciplines
- 2015, CSEC2017 Joint Task Force on Cybersecurity Education

2005
1.Computer Engineering
2.Computer Science
3.Information Systems
4.Information Technology
5.Software Engineering

2017
1. Computer Engineering
2. Computer Science
3. Cybersecurity
4. Information Systems
5. Information Technology
6. Software Engineering

CMU：63门Cybersecurity课程

- Available to both undergraduate and graduate students
- https://www.cylab.cmu.edu/education/courses.html

1. Foundations of Privacy
2. Engineering Privacy in Software
3. Information Security
4. Privacy Policy Law and Technology
5. Secure Coding
6. Applied Information Assurance
7. Information Security Risk Management
8. Information Security Policy and Management
9. Introduction to Cyber Intelligence
10. Network Security and Management
11. Intro to Software Reverse Engineering
12. Host Based Forensics
13. Network Forensics
14. Web Application Security & Performance
15. Cyber Forensics and Incident Response
16. Introduction to Privacy Engineering: from Policy to Code to Quality to Value
17. Elements of Web Security
18. Elements of Browser Security
19. Cybersecurity Research Seminar
20. Introduction to Computer and Network Security
21. Secure Programming
22. Information Security and Privacy
23. Introduction to Computer and Network Security and Applied Cryptography
24. Theoretical Cryptography
25. Formal Foundations of Software Security
26. Social Engineering
27. Software Security Engineering
28. Engineering Runtime Malware Analysis
29. Introduction to Computer Security
30. Introduction to Information Security
31. Introduction to Hardware Security
32. Wireless network security
33. Mobile Security
34. Introduction to Computer Security
35. Network Security
36. Software Security
37. Applied Cryptography
38. Malware, Defense, and Vulnerability Analysis
39. Usable Privacy and Security
40. Cybersecurity and the Future of the Internet
41. Data Privacy
42. Web Application Security
43. Analytical Social Science and National Security
44. Cybersecurity Policy
45. Introduction to Information Security
46. Information Security Compliance and Training
47. Information Security Policy and Governance
48. Software and Security
49. Cryptography
50. Introduction to Information Security Management
51. Internet Security
52. Network and Internet Security
53. Cybersecurity in Critical Infrastructure
54. Privacy in the Digital Age
55. Defensive Hacking
56. Network Security Analysis
57. Information Warfare
58. Information Assurance Policy
59. Network Situational Awareness
60. Introduction to Information Security Training and Awareness
61. Ethical Penetration Testing
62. Network Defenses
63. Special Topics in Cryptography: Blockchain and Cryptocurrencies

网络空间安全学科成立的背景

- **信息安全专业**，本科教育，1998增设
- **网络空间安全一级学科**，研究生教育，2015年增设

国务院学位委员会
教育部 文件

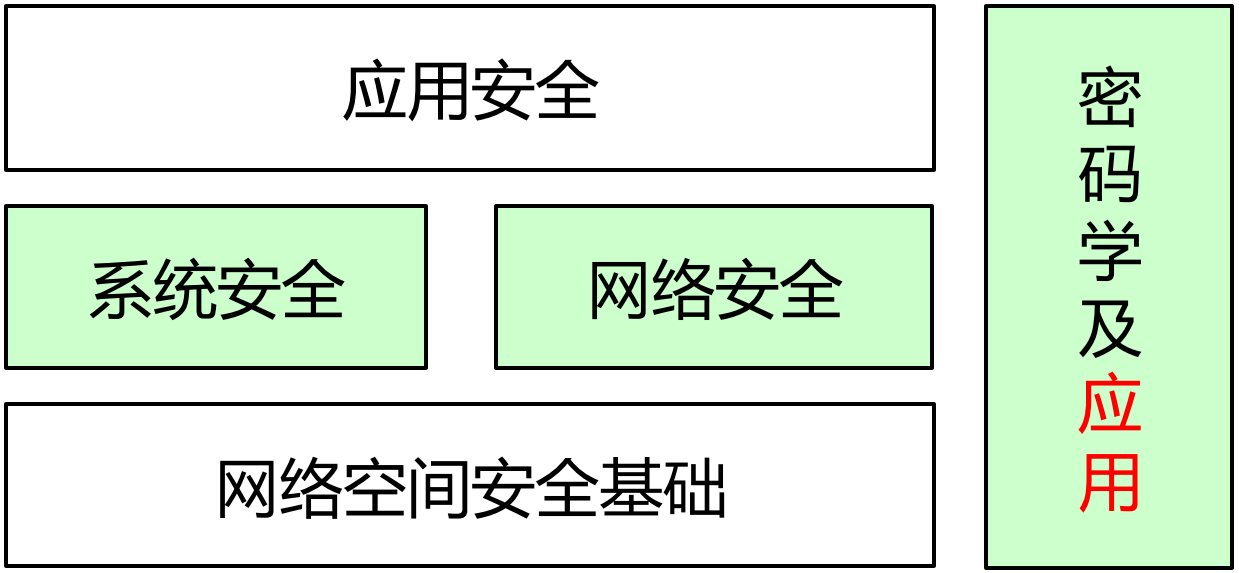
学位〔2015〕11号

国务院学位委员会 教育部
关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

网络空间安全学科主要学科方向



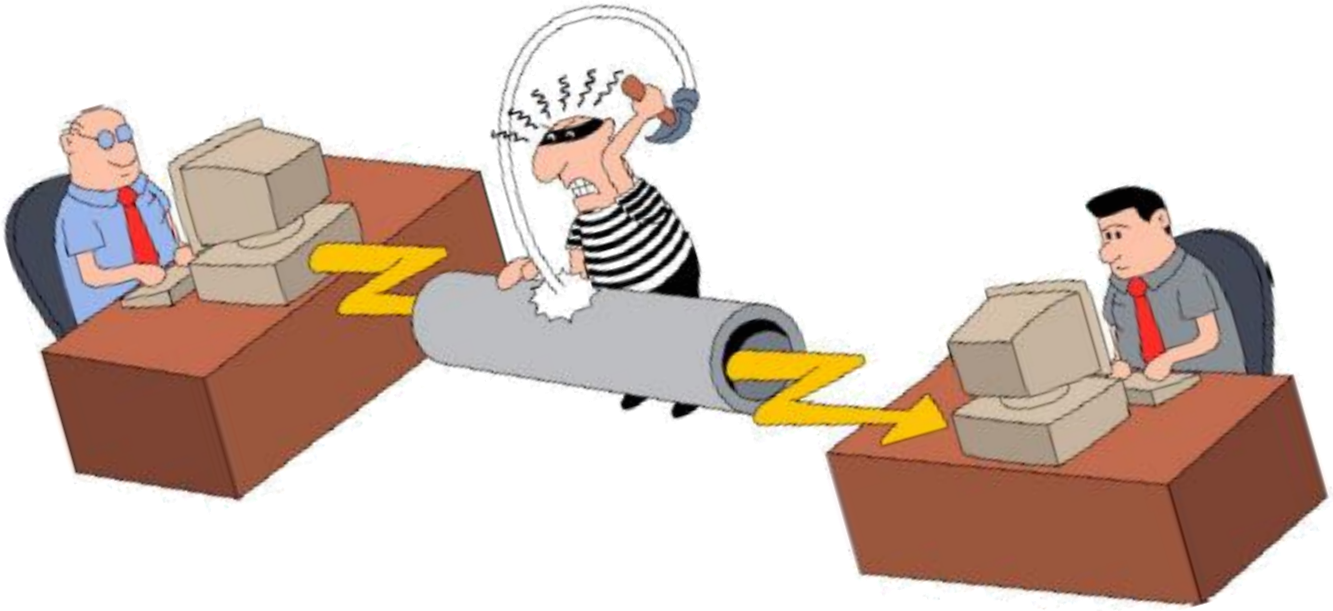
- 安全基础为其他方向的研究提供理论、架构和方法学指导
- 密码学及应用是为系统/网络/应用安全提供密码安全机制
- 系统安全保证网络空间中的单元计算系统的安全
- 网络安全保证网络自身和传输信息的安全
- 应用安全保证大型应用系统的安全，也是安全的综合应用

系统安全

- 端系统：计算机、手机、智能家电、汽车…
- 硬件安全（如CPU），软件安全（OS，APP）

网络安全

- 关注中间系统、通信协议的安全
- 中间系统：交换机、路由器、DNS、CDN等
- 通信协议：DNS、HTTP、SMTP、TLS等



课程主要内容（1）

- 基本概念和常用工具
- 局域网中的安全问题
  - 交换机工作原理及问题
  - ARP欺骗及防范
  - DHCP攻击及防范
  - 其他局域网攻击
- TCP/IP安全与入侵检测
  - IP 的分片问题
  - IP 地址假冒问题
  - IPv6 安全
  - TCP序列号预测与劫持
- 域名系统安全
  - DNS基本工作原理
  - 国际域名系统治理
  - DNS 常见攻击概要
  - DNS缓存污染攻击
  - DNS 反射放大攻击
  - DNSSEC原理
- 常用密码算法与PKI
  - 常用密码算法
  - 公钥基础设施（PKI）
  - 针对PKI的攻击

课程主要内容（2）

- 安全通信协议与VPN
  - TLS工作原理
  - TLS VPN
  - 其他VPN
- Web 安全
  - HTTP协议概要
  - 认证与Cookie
  - 客户端攻击
  - 服务器端的攻击
- 软件安全
  - 软件安全概述
  - 栈溢出漏洞与利用
  - 智能化分析方法

课程实验（待更新和讨论）

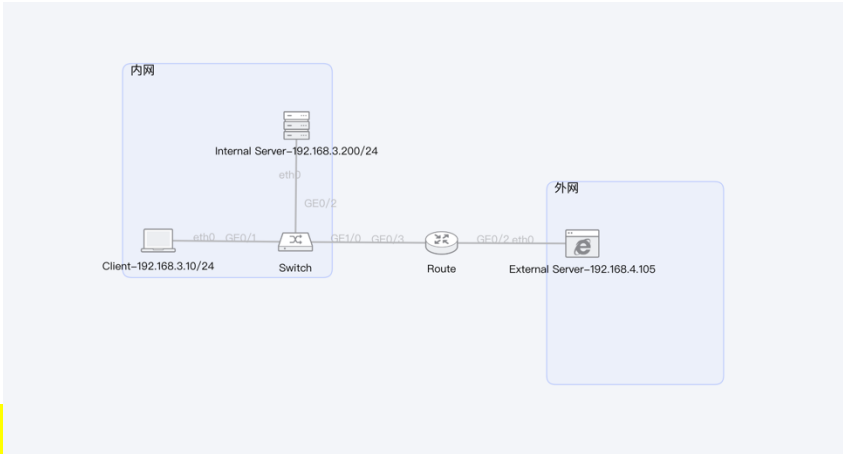
1. 流量分析与数据包构造工具
2. 局域网攻击及口令破解
3. DNS缓存污染攻击与防范
4. 虚拟专用网络（VPN）
5. Web 网站安全
6. 软件漏洞分析与利用

实验要求

- 每人一个实验环境，独立完成
- 提交实验报告
  - 主要操作步骤
  - 关键步骤截图
  - 问题和探索
- 实验结束后选择2位同学分享
  - 课堂演示、讲解
  - 优秀者有奖励

实验平台: 爱慕乐（iMOOL.com.cn）

- 自带电脑终端，接入远程实验环境



实验平台： imool.com.cn
用户名和口令已通过邮件发送到邮箱

实验一：计算机网络基础及常用工具

王浩铭 | 15 | 2024-09-06 09:14 - 2024-10-08 09:14

0个
提交任务

0分
总得分

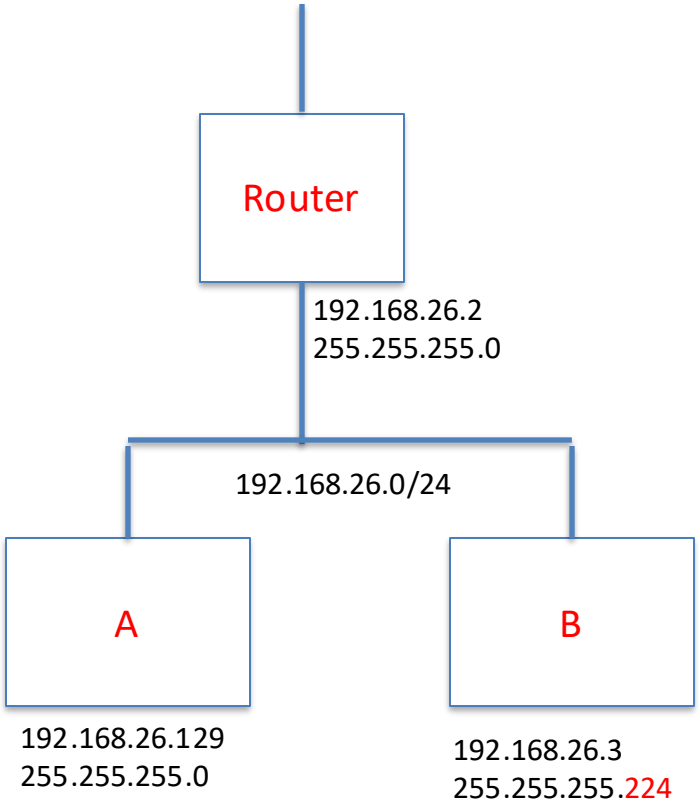
名
排名

加入小组

学习内容

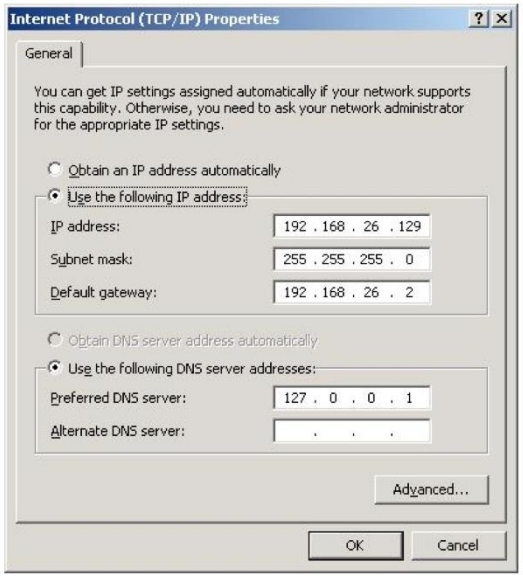
1. 实验1：使用tcpdump分析ICMP流量
2. 实验2：使用wireshark分析Web访问过程流量
3. 实验3：使用Scapy构造ICMP Echo Request数据包
4. 实验4：Smurf攻击
5. 实验5：使用Burpsuite更改HTTP请求

掩码配错了会怎样？

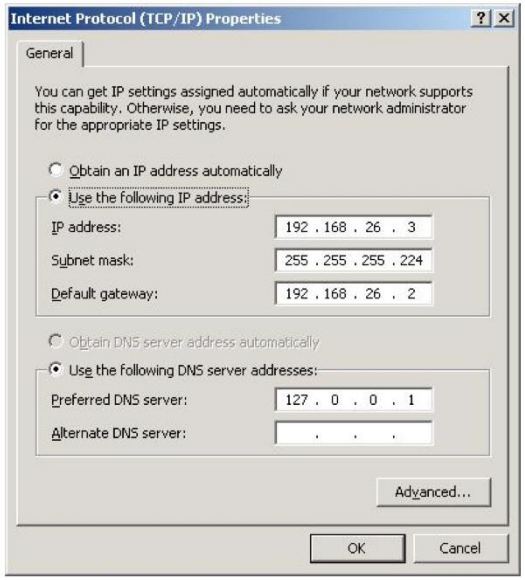


两台服务器 A 和 B 的网络配置如下（见图 1），B 的子网掩码本应该是 255.255.255.0，被不小心配成了 255.255.255.224。它们还能正常通信吗？

服务器 A：



服务器 B：



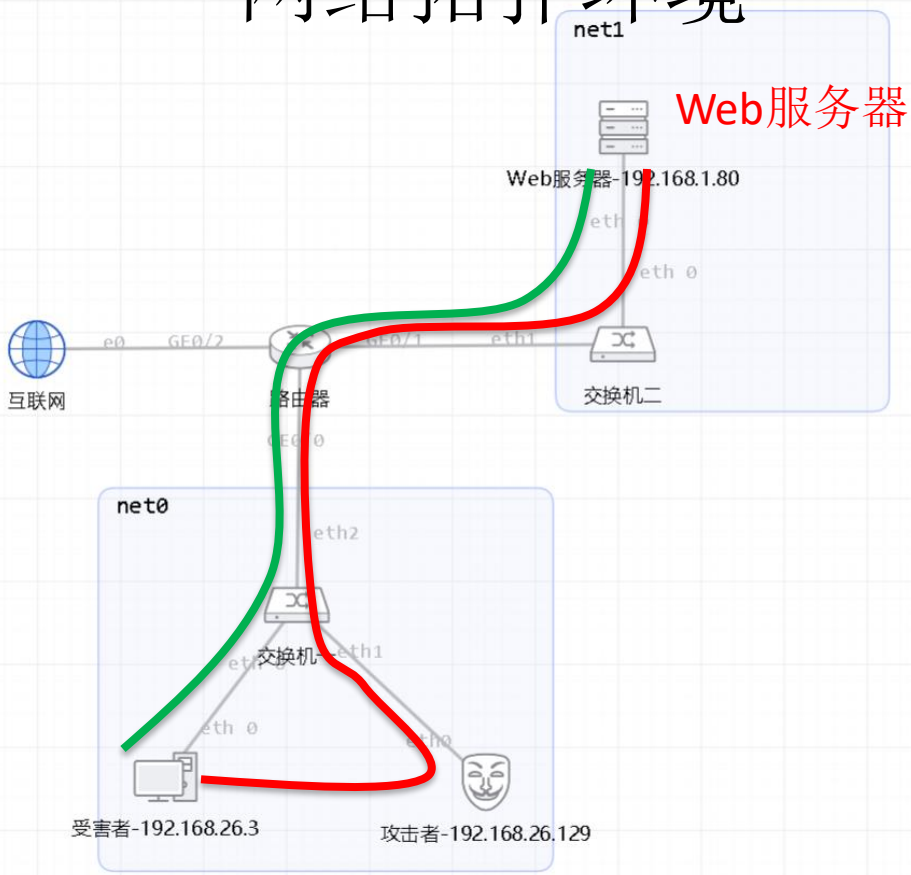
Ping 192.168.26.3

Ping 192.168.26.129

Lab2: 局域网攻击及口令破解

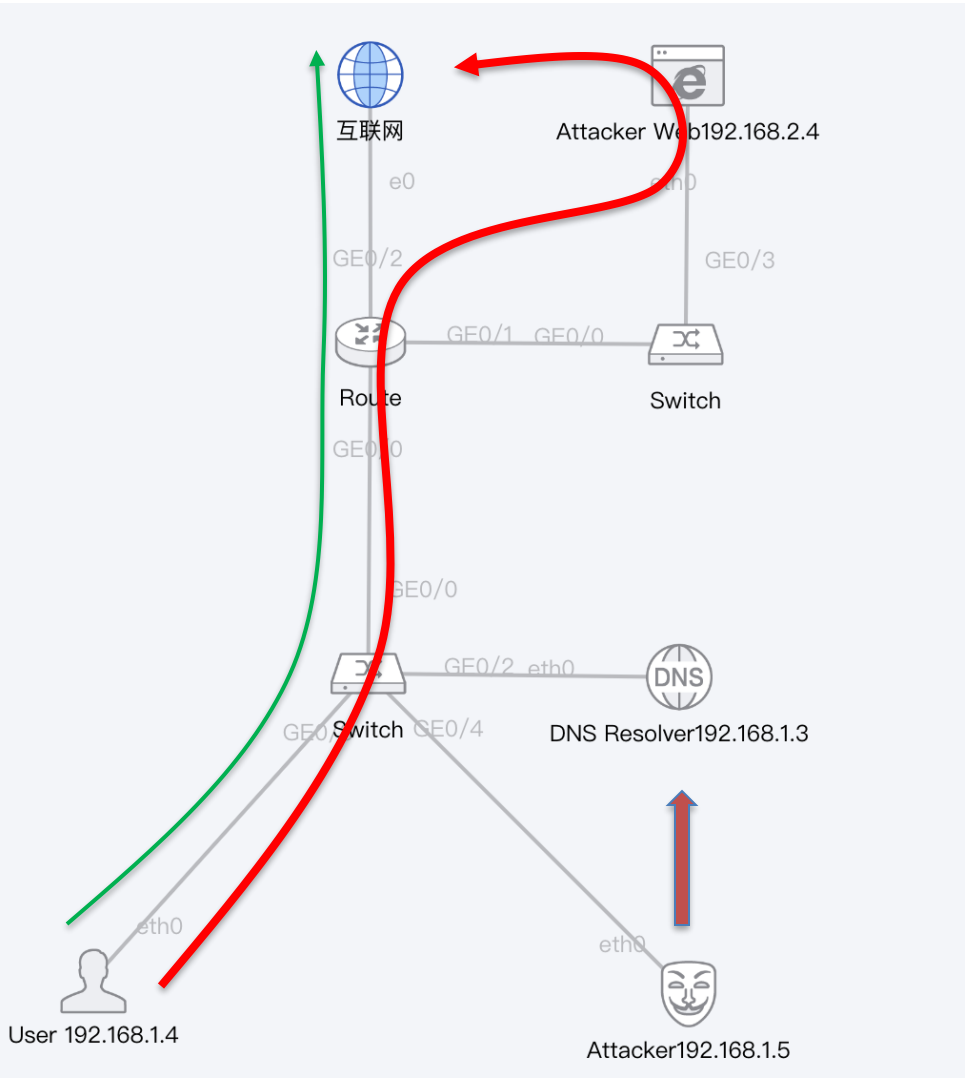
- 基础知识
  - 以太网交换机工作原理
  - ARP协议的作用
  - ARP欺骗攻击及防御措施
  - MD5摘要访问认证口令破解
- 局域网安全实践
  - 基于Scapy的ARP报文欺骗攻击
  - 网络报文嗅探与口令猜解
  - 进阶：ARP欺骗攻击防御方案

- 网络拓扑环境



局域网内攻击者利用ARP欺骗，充当中间人劫持受害者与Web服务器通信流量

Lab3: DNS缓存污染攻击与防范



- 域名系统DNS工作原理
- DNS常见攻击
- 完成缓存污染攻击

Prerequisite

- Computer Networks：TCP/IP
- Programing：C/C++，python，Go,…
- OS：Linux/Unix
- Software or tools
  - Wireshark, tcpdump, …
  - Burp suite …

期末考试成绩计算

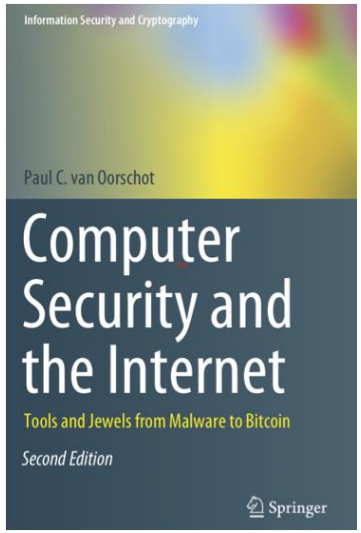
- 平时的实验/作业: 90%
  - Lab Report, Code /script
- 课堂参与和表现: 10%
- **考试课！** 不及格会影响研究生入学
- 期末无法补实验，环境重构需大量时间和计算资源

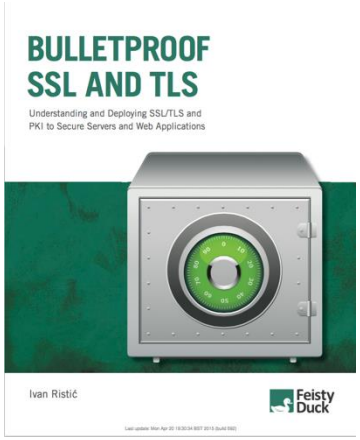
伦理和道德

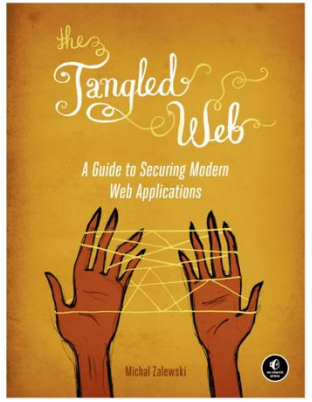
- 了解网络安全法律
- 网络安全研究的伦理和道德
- 尊重他人，不侵犯他人隐私
- 在受控的环境下攻击测试
- 测试不能影响生产系统
- 负责任的漏洞披露
- 为自己的行为负责

参考资料

- 以课件及指定的在线文档为主（每年更新）
- Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, 2nd Edition
  - https://people.scs.carleton.ca/~paulv/toolsjewels.html
- 计算机安全导论：深度实践，杜文亮，高等教育出版社
- 密码学基础方向
  - Bulletproof SSL and TLS (E-book)
- Web 安全
  - The Tangled Web(Ebook)







Q & A

群聊：网络安全工程与实践
2024 课程群

该二维码7天内(9月12日前)有效，重新进入将更新