网络攻防技术与实践课程

1. 网络攻防技术概述与课程简介

诸葛建伟

zhugejw@gmail.com

个人简介

- 任课教师—诸葛建伟 博士
  - 北京大学计算机研究所副研究员
  - 研究方向：网络与系统安全
  - 北大土著: **97**级本，**01**级硕，**03**转博，**06**留校
  - **80**后老大哥
  - 著名开源团队**The Honeynet Project Full Member, THP Chinese Chapter**技术负责人
  - 主持或参与国家科研项目**10**余项，发表知名国际会议论文/一级期刊论文**20**余篇
  - 就读期间获柯达, 惠普奖学金, 微软学者, **IBM**博士生英才, 五四青年科学奖（挑战杯）竞赛一等奖

内容

1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

课程简介

- 课程名称-《网络攻防技术与实践》
- 课程目的
  - 使得学生能够较为全面地掌握网络与信息安全方向的基础知识框架；
  - 并具备实际的网络攻击、取证分析和安全防护实践技术能力。
- 授课对象：硕博研究生，欢迎高年级本科生旁听

课程简介—主要内容

- 一、绪论
  - **1.** 网络攻防技术概述与课程简介
  - **2.** 网络攻防实验环境
- 二、网络安全攻防
  - **3.** 网络信息收集技术
  - **4.** 网络嗅探与协议分析
  - **5. TCP/IP**网络协议攻击
  - **6.** 网络安全防护技术
- 三、系统安全攻防
  - **7. Linux**操作系统安全攻防
  - **8. Windows**操作系统安全攻防
  - **9.**恶意代码

课程简介—主要内容(2)

- 四、网络攻防技术进阶
  - **10.** 程序安全攻防：缓冲区溢出和**Shellcode**
  - **11. Web**应用安全攻防
  - **12.** 浏览器安全攻防
  - **13.** 无线网络与移动终端安全攻防
- 五、课程总结与团队实践项目展示
  - **14.** 团队实践项目展示

教材和参考书

- 使用教材（非必须购买,ftp提供电子书）
  - 《网络攻防技术与实践》讲义(未完成，电子工业出版社书约)
  - **Stuart Mcclure，Joel Scambray，George Kurtz**著，王吉军 张玉亭 周维续译，**HACKING EXPOSED，5RD EDITION**（黑客大曝光：网络安全机密与解决方案第**5**版），清华大学出版社，**2006**年。　第六版(英文版)
  - 被誉为“信息安全圣经”
- 参考书
  - 《**WINDOWS SERVER 2003**黑客大曝光》，《**LINUX**黑客大曝光》,《**Web**应用黑客大曝光》
  - 《黑客攻防实战入门(第**2**版)》，《黑客攻防实战进阶》
  - 《决战恶意代码》,《密码编码学与网络安全**--**原理与实践第四版》，《黑客防范手册》，《网络渗透技术》，《深入解析**Windows**操作系统》

课程考核方式

- 2人组队方式：9月29日前确定组队，发送给助教登记

- 最后考试成绩＝课堂表现(10) +课外作业(60)+项目实践(30)
- 课堂表现：课堂问答发言与课堂实践发言+出勤情况
- 课外作业: 12次课外实践作业(每次作业10分)，部分作业团队合作，至少完成6次，选取60分最高作业计算实践作业分数
- 项目实践：项目实验技术报告和课堂展示
  - 项目实验技术报告(15分)：任课老师/助教给分
  - 课堂展示(15分)：同学互评
- 认真上课并完成课程作业和团队项目实践的学生都将能够获得良好的分数。
  - 前年平均得分84+，去年平均得分86+
  - 90+(40%)

课程作业

- 作业1: 黑客电影鉴赏和社会工程学(团队)
- 作业2: 网络攻防实验环境搭建和测试(个人)
- 作业3: 网络信息搜索与扫描技术实践(个人)
- 作业4: 解码一次网络扫描/扫描攻防对抗 (个人+团队)
- 作业5: TCP/IP网络协议栈攻击(个人)
- 作业6:分析蜜网网关中防火墙与入侵检测系统配置规则 (个人)

课程作业(2)

- 作业7: Linux操作系统攻防对抗(团队)
- 作业8: Windows操作系统攻防对抗(团队)
- 作业9: 分析一个恶意代码样本(团队)
- 作业10: 分析一个实际的Buffer Overflow漏洞(团队)
- 作业11: SQL注入和XSS攻击(团队)
- 作业12: 网站挂马案例分析(团队)

项目实践选题

- 项目实践选题
  - 可选择建议的实践选题，推荐自主选题
  - 避免重复选题
  - 按照实践工作量、达成效果、社区贡献、报告和展示效果进行综合评分

- 建议参与开源项目或竞赛
  - **Google Summer of Code**
  - **Microsoft 创新杯(Imagine Cup)**
  - “挑战杯”全国大学生课外学术科技作品竞赛
  - 全国大学生信息安全竞赛
  - 全国大学生电子设计竞赛信息安全技术专题邀请赛

前年的项目实践选题

无线网络WEP/WPA破解	6	
网络Sniffer编程实现	3	
无线网查点	2	
Jargon file	2	
Hacker profiling	2	
木马实现	1	
Web跨站内嵌链接分析	1	
恶意代码脱壳器	1	
Rootkit检测工具	1	
PHoneyC工具改进	1	GSoC
Windows exploit工具试验整理	1	
网络信息战调研	1	

去年的项目实践选题

- Capture the Flag
- Gsoc-Nmap调查
- Jargon Files整理
- Java程序缺陷静态分析器
- pdf恶意代码检测 GSoC
- Qebek for Linux
- SQL注入技术攻击及防御措施研究
- TraceExploit自动重放攻击系统 - GSOC
- Windows&Linux渗透攻击资源
- 北大校内无线AP探测
- 钓鱼邮件的分析和识别
- 改进PHoneyC对VBScript的支持
- 黑站(网站攻击)技术的应对
- 互联网免费软件的捆绑安装状况调查
- 基于Winpcap自主开发sniffer
- 基于离散小波的图像数字水印研究
- 集成nmap/nessus/p0f/pads实现网络自动化侦察工具
- 美国黑客文化调查
- 人人网人际关系分析
- 社会工程学案例收集分析
- Web应用的SQL注入攻击与防御
- 网络安全知识竞赛机考系统
- 网页动态图片验证码的自动识别
- 网站上的点击广告分布情况调查分析

Google Summer of Code

- **Know More:**
  - **Google Summer of Code (Google编程之夏)2010开锣**
  - **http://blog.cost.edu.cn/zhugejw**

Google Summer of Code 2009情况

- **Google Summer of Code**
  - **Google支持开源社区研发的一个公益性计划，since 2005**
  - **资助学生($4,500)和开源团队($500)开展暑期开源编码**
  - **http://code.google.com/soc/**
  - **3,300 students from nearly 100 countries**
- **Google Summer of code'09**
  - **2009年3月开始申请, 4月末出结果, 5-8月项目执行期**
  - **400开源团队申请 → 150开源团队受资助 (37.5%)**
  - **5,900学生申请 → 1,000学生受资助(16.9%)→ 85%顺利完成**
  - **The Honeynet Project 首次成功申请，安全 方向3-4个**
  - **55个申请者，最终录用9个，录取率16.3%**
  - **The Honeynet Project Chinese Chapter 3份申请全部命中，8月份全部顺利完成**
  - **其中1项是本课程项目实践后继工作，1项为助教选题**

GSoC 2009 Chinese Chapter Projects

1. Develop and Improve PhoneyC: PhoneyC is a low-interaction client honeypot designed to allow researcher to quickly and easily identify and analyze malicious websites and their malware. We hope to be adding DOM emulation and automated shellcode detection using LibEmu this summer, amongst other features, to help improve detection and performance.
Student: Zhijie Chen
Primary Mentor: Jose Nazario

2. Develop and Improve PhoneyC: PhoneyC is a low-interaction client honeypot designed to allow researcher to quickly and easily identify and analyze malicious websites and their malware. We hope to be adding DOM emulation and automated shellcode detection using LibEmu this summer, amongst other features, to help improve detection and performance..
Student: Geng Wang
Primary Mentor: Jose Nazario

3. Qebek: QEMU Based Sebek: Advanced new data capture technique for virtualized environments, looking to extend our existing work on Sebek for high interaction honeypot I/O capture to the hypervizor layer, for increased stealth and performance.
Student: Chengyu Song
Primary Mentor: Brian Hay

Google Summer of Code 2010情况

- **Google Summer of Code'10 变化**
  - **学生资助金额提高至$5,000**

Google发布GSoC2010学生名单-北大4名学生成功获得资助

2010年4月28日　　3 条评论

Google刚刚正式公开了GSoC 2010受资助学生名单，The Honeynet Project
令人兴奋地拿到了17个学生名额（从去年的9个名额几乎增长了一倍），
具体受资助名单见here!。

在The Honeynet Project最后收到的45份有效申请中，来自中国学生的有8份，
其中北大的5份，最终4名中国学生成功获得了资助，参与The Honeynet Project
的开源程序开发，均为北大的学生，分别为：
Student Proposal Title Mentor
Huilin Zhang Improving PHoneyC—-Detecting and Analyzing Malicious PDF attack jose nazario
Zhongjie Wang Implement TraceExploit: Replay the collected network trace to perform successful exploit Jianwei Zhuge
chengyu song Using hardware virtualization to improve high interaction honeypot data capture system Thanh Nguyen
Wenxin Yang My proposal for infected host detection through DNS analysis Jeff Nathan

祝贺这些同学，并希望他们能够成功完成GSoC项目，并积极参与到开源团队和社区中。

zhugejw　The Honeynet Project, open source
GSoC, open source, The Honeynet Project　120 views

项目实践选题-调研/训练类

- 支持中国高校学生网络安全技能大赛的选题
  - 国外黑客**Capture the Flag**竞赛组织方式和实践过程
  - 网络安全知识与黑客社区文化常识，挑战试题库与解答
  - 古典与现代密码分析技术，挑战试题库与解答
  - 数字图像隐写分析技术，挑战试题库与解答
  - 网络攻击网络流数据集取证分析技术，挑战试题库及解答
  - 二进制逆向分析技术，挑战试题库及解答
  - **Web**应用攻击技术，挑战试题库及解答
- 调查**GFW**机制，以及绕过**GFW**的方法，给出实践技术报告
- **…**

项目实践选题-创新类

- 自主选题，能够解决实际问题，或对开源社区有所贡献，与网络攻防有一丝联系即可
- 前年及去年的项目实践报告及答辩材料，可从课程**FTP**下载

共享资源与交流平台

- 课程共享**FTP**
  - **ftp://222.29.87.30**
  - **u/p=HackingExposed/HackingExposed**
  - 课程内容：**slides, materials**子目录
  - 电子书：**ebooks**子目录
  - 作业数据下载：**exercises**子目录
  - 软件工具下载：**tools**子目录
  - 攻防环境虚拟机镜像下载：**images**子目录(待上传)
  - 黑客电影: **movies**子目录
- 交流平台
  - **BBS**版面：北大未名/课程特区/**HackingExposed**网络攻防技术与实践

内容

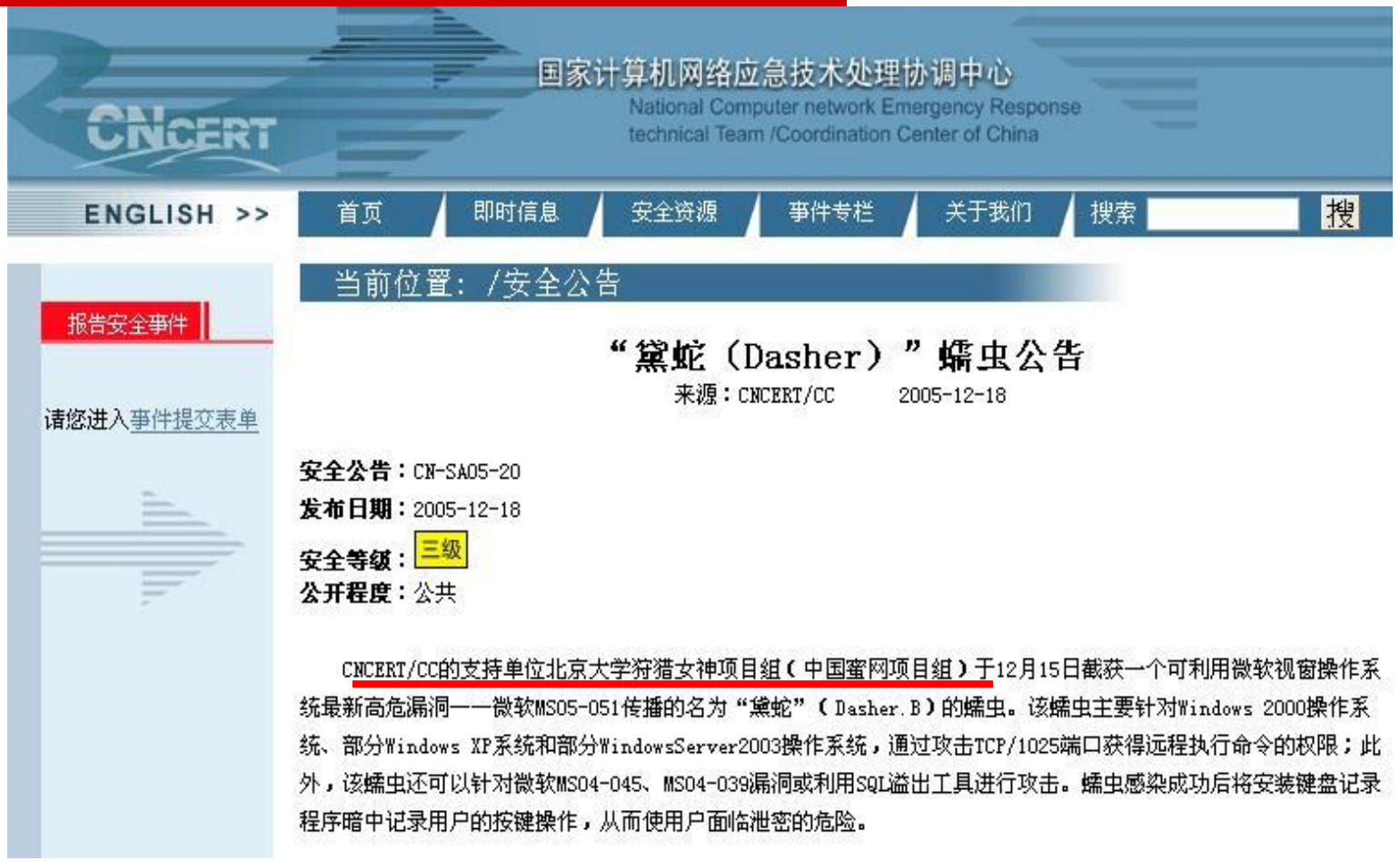
1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

案例演示背景 – 黛蛇蠕虫

- 黛蛇蠕虫(Dasher)：2005年国内爆发的知名蠕虫案例
  - 狩猎女神项目组参与应急处理的第一个实际网络攻击案例

- **2005年12月15日北京时间21:45，狩猎女神项目组国内第一时间截获蠕虫样本**
- **2005年12月16日北京时间10:24，向CNCERT/CC汇报了Dasher蠕虫的爆发，定位用于传播的Shell、FTP服务器**
- **2005年12月16日北京时间19:30， 协助CNCERT/CC关闭FTP，Dasher蠕虫感染上万台主机**
- **2005年12月16日北京时间19:45， 发布黛蛇蠕虫分析报告**
- **2005年12月17日协助CNCERT/CC对相关主机进行取证分析，定位蠕虫编写和投放者为河南南阳某ADSL用户，上报相关部门**
- **2005年12月18日北京时间15:00，协助CNCERT/CC发布“黛蛇”(Dasher)蠕虫公告**

黛蛇蠕虫CNCERT/CC公告



国家计算机网络应急技术处理协调中心
National Computer network Emergency Response technical Team /Coordination Center of China

ENGLISH >> | 首页 | 即时信息 | 安全资源 | 事件专栏 | 关于我们 | 搜索 | 搜

报告安全事件

请您进入事件提交表单

当前位置：/安全公告

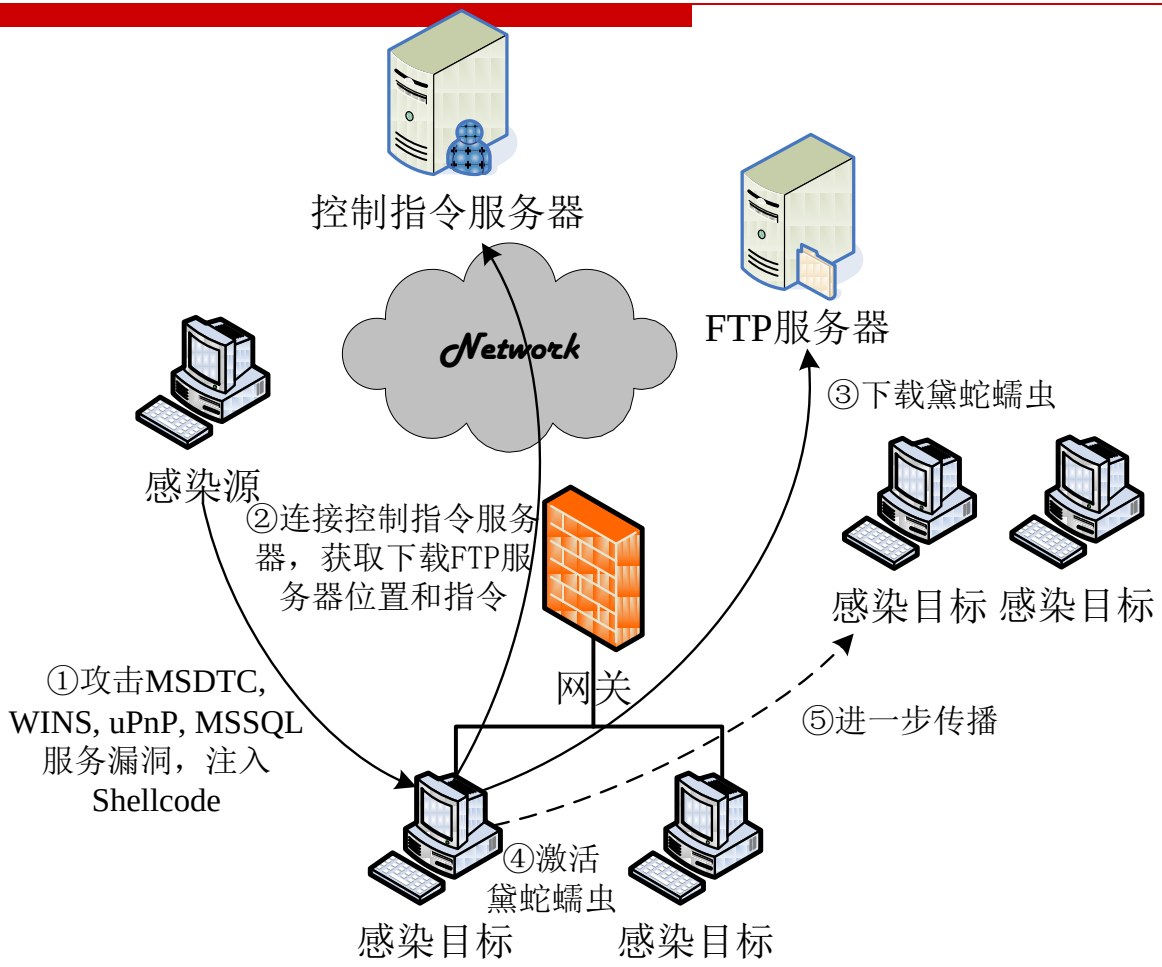
“黛蛇（Dasher）”蠕虫公告

来源：CNCERT/CC　　2005-12-18

安全公告：CN-SA05-20
发布日期：2005-12-18
安全等级：三级
公开程度：公共

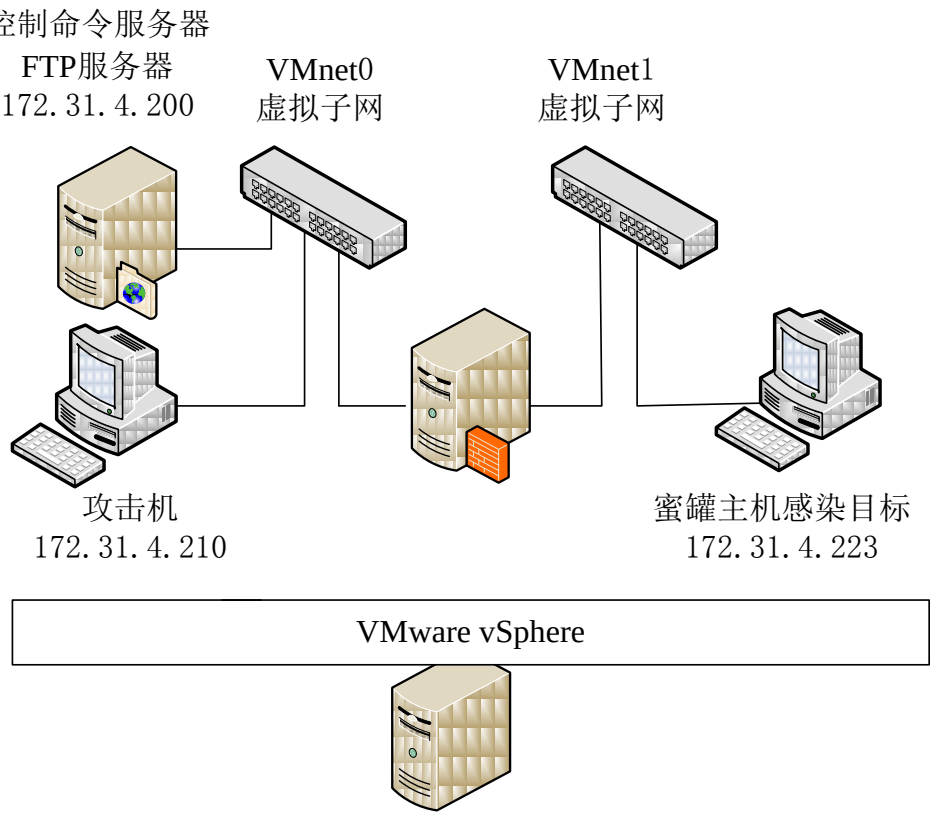
CNCERT/CC的支持单位北京大学狩猎女神项目组（中国蜜网项目组）于12月15日截获一个可利用微软视窗操作系统最新高危漏洞——微软MS05-051传播的名为“黛蛇”（Dasher.B）的蠕虫。该蠕虫主要针对Windows 2000操作系统、部分Windows XP系统和部分WindowsServer2003操作系统，通过攻击TCP/1025端口获得远程执行命令的权限；此外，该蠕虫还可以针对微软MS04-045、MS04-039漏洞或利用SQL溢出工具进行攻击。蠕虫感染成功后将安装键盘记录程序暗中记录用户的按键操作，从而使用户面临泄密的危险。

黛蛇蠕虫机理图示



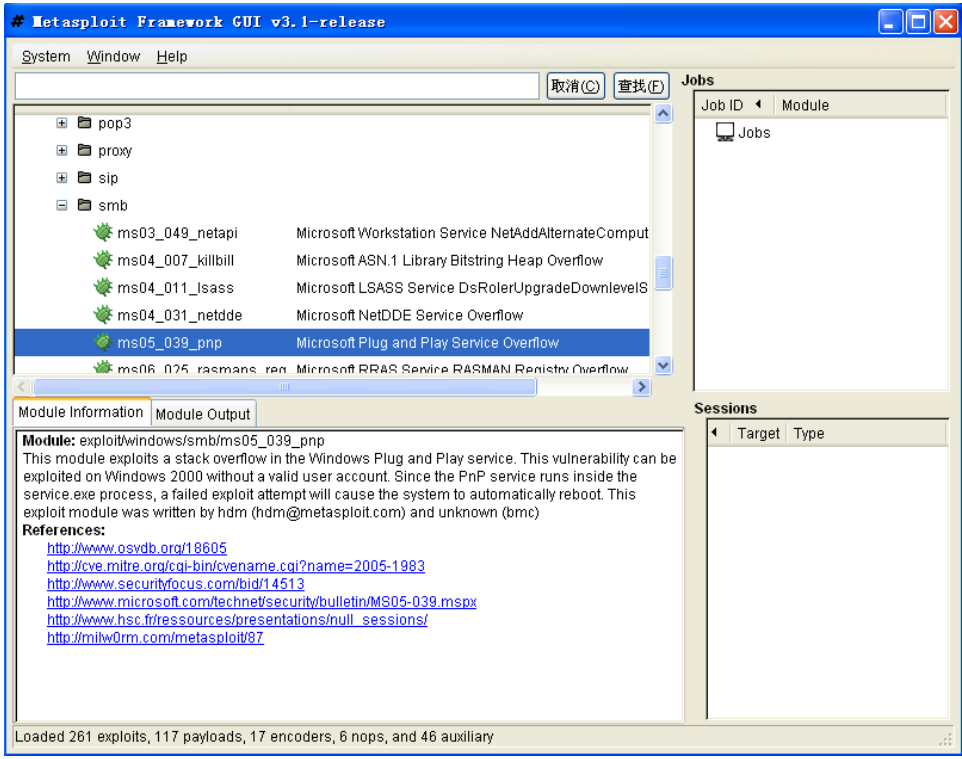
黛蛇蠕虫案例演示环境

- 虚拟蜜网攻防实验环境
  - 一台高性能服务器
  - 如何构建: 第二堂课主要内容
- 黛蛇蠕虫攻击源-攻击机
- 控制命令/FTP服务器
- 虚拟蜜网
  - 虚拟机软件：**VMware vSphere**
  - 蜜网网关: **ROO V1.4**
  - 虚拟机蜜罐(靶机): **Windows 2K SVR**



Metasploit渗透攻击软件

- **Metasploit渗透攻击代码**
  - **http://www.metasploit.org/**
  - **H.D.Moore**
  - 渗透攻击代码和工具的开发平台
  - **2004年发布稳定版本2.1版，目前为3.4.x**
  - 与商业渗透测试软件**CANVAS、IMPACT**构成竞争



黛蛇蠕虫案例演示过程

- 黛蛇蠕虫攻击漏洞检测和渗透攻击
  - 利用**Metasploit**进行**uPnP**漏洞的渗透攻击
  - 展示**Walleye**上的攻击数据捕获和分析结果
- 黛蛇蠕虫的模拟感染过程
  - **1)**启动**FTP**服务器**Serv-U**，提供黛蛇样本下载
  - **2)**启动控制命令服务器**NetCat**，提供批处理命令
  - **3)**执行黛蛇蠕虫中包含的**uPnP**漏洞渗透攻击脚本
  - **4)** 查看感染目标蜜罐主机的文件系统、任务运行列表和系统状态
  - **5)** 利用**Walleye**分析由蜜网网关、**Sebek**捕获的黛蛇蠕虫攻击场景数据

黛蛇蠕虫演示视频

黛蛇蠕虫事件的取证过程

- **IP追踪定位**
  - **FTP服务器**
    - 样本文件上载时间
  - 控制命令服务器
    - 控制脚本上载时间
  - **Web服务器虚拟目录(样本尝试连接的)**
    - **Web访问日志**
  - 确认蠕虫投放时间，及该段时间内可疑的**Web**访问**IP**地址
  - 河南南阳**ADSL**用户
- **Profiling**
  - **FTP banner: [Evil_Security_Team]**
  - 网络搜索及线索追踪: **sdbot.blog.edu.cn**

网名<Primary Identity>	Evil[xiaoyu]
团队<team>	N/A
国家/地区<Nationality>	中国大陆
族群< Colony >	恶意程序编写者
	自我满足/经济利益(Ego，Money)
其他名<second Identity>	慕容雨
姓名<real identity>	不详
性别<gender>	男
出生年<birth year>	1986年
联系方式<primary contact>	x140yu@hotmail.com
其他联系方式<second contact>	QQ：75951371
blog	http://sdbot.blog.edu.cn
居住地<location>	河南南阳
毕业学校<school>	不详
	2005-12编写了"黛蛇"病毒并在互联网上投放
黑客历程<career>	我对 Worm.Dasher.B 的分析!!!
	2006-5-18: VBS 批量挂马脚本(Modify by Evil[xiaoyu])
	2006-9-20: NameLess Eternity Version僵尸程序
恶意代码<Malware>	"黛蛇"病毒
媒体报道<media reports>	"黛蛇（Dasher）"蠕虫公告

黛蛇蠕虫案例小结

- 涉及攻防技术术语
  - 蠕虫: 恶意代码
  - 安全漏洞
  - 渗透攻击
  - 蜜罐(样本捕获)，恶意代码分析，取证分析
- 涉及人物/组织
  - 病毒编写&投放者: 黑帽子
  - 安全研究&维护人员: 白帽子
  - 安全应急处理组织
- 故事摘要：一个黑帽子"黑客"写了个蹩脚的蠕虫，投放到了互联网上，一个白帽子帮助应急组织进行了及时处理，挽救了无辜百姓和黑帽子，但被黑帽子骂了SB。

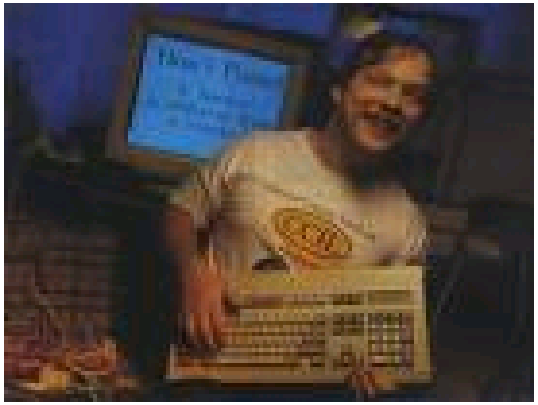
内容

1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

“黑客帝国”是由黑客英雄们创造的

黑客-Hacker

- 黑客(hacker) ≠ “黑客”
  - “黑客”：黑帽子(black hat) - 骇客(cracker)



- Hacker?
  - “:hacker: /n./ 原意:用斧头做家具的能工巧匠
  - 《黑客词典》—Jargon File, by E.S.R (Eric S. Raymond)

黑客的定义-Jargon File

- 1. 享受探索系统的实现细节，拓展系统能力的人
- 2. 编程狂热者，甚至编程强迫症患者
- 3. 能够欣赏黑客能力和价值的人
- 4. 能够快速提升编程能力的人
- 5. 在某种编程语言和系统上的专家和高手
- 6. 在任意特定领域上的专家和技术狂热者
- 7. 以创造性突破极限的智力挑战为追求和享受的人
- 8. [偏见]通过到处刺探尝试发现敏感信息的恶意攻击者，他们应该被称为骇客。

黑客道-史前时代

- **E.S.R五部曲之A Brief History of Hackerdom**
  - 黑客道起源实际上就是计算机技术和社区的起源

- **45-70s: 黑客道“史前时代” - 真程序师文化**
  - **1945: Eckert & Mauchly ENIAC**
  - 真程序师**Real Programmer:** 通过硬件器件搭建系统，使用原始编程语言甚至机器码编程，通过打卡机**punch**到卡片上，通过读卡机输入电脑并执行
  - 代表人物：西摩·克雷**(Seymour Cray)**
  - 打卡计算机与“大铁块”巨型机**(mainframes)**流行的年代 -伟大的真程序师们主宰着计算机文化

黑客道-远古时代之ITS文化

- 1961: MIT TMRC实验室出现第一台大型机DEC PDP-1
  - 黑客道的起源: MIT/1961
- 1969: ARPANET，进入网络时代
- 黑客道三大重镇
  - 中心MIT AI Lab, SAIL, CMU
- 机器-大型机(DEC公司的PDP)
- 操作系统
  - ITS: MIT AI Lab操作系统，汇编+LISP
  - 1964: Multics操作系统- MIT, GE, AT&T

黑客道-近古时代之Unix与微电脑文化

- **1969-8x: 黑客“近古时代”-Unix文化兴起**
  - **1969: AT&T Bell Lab, Ken Thompson发明Unix, Dennis Ritchie发明C语言**
  - **1980: UUCP, Usenet**
  - **1983: ARPANET – TCP/IP**
- **1975-8x: 黑客“近古时代”微电脑文化新潮**
  - **1975: 第一台PC IBM5150出现**
  - **1975: Bill Gates创建MS, 1981: MS-DOS**
  - **1977: 苹果电脑, 1984: Mac OS**
  - **1978: Intel 8086, x86 architecture**

黑客道近代史-开源软件与Wintel的对决

- 80-83: ITS、Unix和微电脑文化同时存在
- 1983: DEC停止PDP-10生产, 集中在PDP-11和VAX, ITS过于复杂,无法移植至其他机器
  - ITS文化被Unix取代
- 私有Unix时代: 1984年AT&T拆分, Unix成为商品
  - Unix社区分裂为Berkley Unix (BSD)和AT&T Unix两大阵营，长达十年的诉讼
- 黑客道近代史开启-WIntel与开源软件对决

黑客道近代史-开源软件与Wintel的对决

- **WIntel商业垄断联盟**
  - **MS: Windows操作系统**
  - **Intel: x86芯片**
- 开源软件社群
  - **R.M.S建立FSF: Free Software Foundation**
  - **GNU: GNU is Not Unix**
  - 直至**1996**年，**R.M.S**承诺的**GNU**操作系统**- HURD**并没有如期出现
  - 互联网时代**: 1988-1995**全球互联网，**1991: WWW – Tim Berners-Lee**
  - **1992: Linux Kernel**在互联网上发布**-**芬兰学生**Linus Torvalds, 1993**年底趋于稳定
  - **E.S.R**五部曲之《大教堂与市集》

黑客道的分化

- 随着计算机技术发展和衍生，黑客社区逐步缩减至安全领域
- 黑客道的分化
  - **Whitehats, Blackhats, Grayhats**
  - **Kevin Mitnick:** 频繁攻击军方, **FBI,** 商业公司网络，被**FBI**通缉，多年流亡**+3**次入狱，成为世界最著名黑客
  - 俄罗斯、东欧剧变后，追求经济利益的黑帽子大量出现
  - 僵尸网络、**DDoS**攻击和敲诈成为在线服务的重要威胁
  - 垃圾邮件、网站钓鱼、信用卡盗用、网站挂马等针对互联网用户的攻击日益猖獗
- 人们逐渐将黑客等同于骇客，或计算机犯罪者
  - 骇客总是自称为黑客
  - 媒体报道：**Computer hacker = criminal**

Kevin Mitnick

- Kevin Mitnick (凯文·米特尼克)
  - “世界头号黑客”-最具传奇色彩的黑客人物
- Kevin的传奇人生经历
  - 1964年出生洛杉矶，父母离异，没人管
  - 4岁：“滑铁卢的拿破仑”，13岁：业余无线电
  - 攻破洛杉矶的公交卡系统坐霸王车
  - 1979(15岁)：闯入了“北美空中防务指挥系统”
    - 1983年好莱坞大片“战争游戏”故事蓝本
  - 1980(16岁)：“太平洋电话公司” 、联邦调查局
    - 被FBI捕获，“少年犯管教所”，第一名“电脑网络少年犯”
  - 1980-1988：5家大公司/全美数据装配系统
    - 1988: 再次被执法当局逮捕

Kevin Mitnick (2)

- **1993:** 非法侵入电话网, **FBI,** 在**FBI**发布逮捕令前开始流亡
- **1994:** 攻击圣迭戈超级计算机中心，激怒日籍安全专家下村勉，**1995**年下村勉协助**FBI**追踪并抓捕**Kevin**
  - **TakeDown: The Pursuit and Capture of Americas most wanted computer outlaw.**
- **1995-2000:** 入狱**4**年半，被禁止使用任何电子设备，尝试改造收音机联网
- **2000**年**1**月出狱，改过自新，从事安全咨询工作**(http://www.kevinmitnick.com/)**
- 出版畅销书：欺骗的艺术、入侵的艺术

黑客道“现代史”

- 1988年Morris蠕虫爆发 - RTM: Robert Tappan Morris
  - 分水岭事件
  - 催生CERT机构/FIRST组织
- 缓冲区溢出攻击技术广泛传播
  - 1996: Phrack 49, Alphe One, Smashing The Stack For Fun And Profit
  - 1998: Dildog, The Tao of Windows Buffer Overflows
- 2000: Yahoo、亚马逊、CNN、ebay等门户网站被DDoS攻击
- 2001-2004: Windows平台上的蠕虫频繁: Code Red, Blaster, Slammer, Sasser, etc.
- 2005-: 经济利益驱动的黑客行为盛行
- 1990s: 计算机安全产业的形成
  - FW: DEC(FW product 1991), CheckPoint(1993)
  - IDS: Wheel Group(1994, ->Cisco), ISS(1994, ->IBM)
  - AV: Norton (mid-80s, ->Symantec), McAfee (1987), Kaspersky(1997)

中国的黑客道发展史-史前期

- 漫长的史前期(1956-1994)
  - **1956-1965:** 电子计算机研制
  - **1974.8: 748**工程，汉字进入信息化时代，北大计算机所王选教授—激光照排
  - **70s-80s:** 微机、汉字显示处理**(CCDOS**、五笔输入法、汉王汉字识别、**UCDOS**、清华**OCR**、金山**WPS)**
  - 计算机核心技术的缺失和落后：芯片、操作系统等
  - **1987**年北京计算机应用技术研究所实施的中国学术网，钱天白教授中国第一封电子邮件”越过长城，走向世界”
  - **1992**年中国台湾、香港联入全球互联网
  - **1994**年中国大陆正式联入全球互联网**:** 中科院高能物理所 许榕生研究员

中国的黑客道-萌芽期

- 萌芽期(1994-1998)
  - 中国刚刚联入全球互联网
  - 窃客－破解软件、注册码…
  - 初级黑客: 学习初步技术，使用国外黑客工具，追随精神领袖－Kevin Mitnick
  - 台湾地区Coolfire黑客入门教程系列(1995-96年编写)
  - 1998年台湾地区陈盈豪 CIH病毒
  - 1998年美国“死牛崇拜” 黑客团队发布BO，掀起特洛伊木马热潮，国内黑客开发NetSpy, 冰河等
  - 国内黑客软件：小榕软件、天行、谢朝霞、PP(彭泉)等
  - 1998年7-8月：针对印尼排华事件的网络攻击→绿色兵团

中国的黑客道-混沌发展期

- 混沌发展期(1999-2001)
  - 1999年5月大使馆被炸事件: 对美黑客攻击
  - 1999年7月台湾省两国论事件: 对台黑客攻击
  - 第一代黑客的商业化: 绿色兵团→中联绿盟、安络科技、补天和瑞
  - 2000年初东史郎南京大屠杀败诉事件: 对日黑客攻击
  - 2001年三菱事件、日航事件、教科书事件和《台湾论》事件: 对日黑客攻击
  - 2001年4-5月中美撞机事件: 中美黑客大战
    - 中国红客联盟、中国鹰派、中国黑客联盟、…
  - 中国红客的出现和发展

中国的黑客道-成熟发展期

- 成熟发展期(2002-Now)
  - 传统黑客团队专注于技术研发: 安全焦点、看雪学院、白细胞、**Ph4nt0m**、...
  - 大量传统黑客创办或进入安全公司: 绿盟、启明星辰、安天、大成天下、知道创宇、...
    - **XCon**安全焦点峰会 **since 2002**
    - 安全漏洞研究和发现: **nsfocus**等
    - **Phrack**黑客杂志和知名黑客会议出现国人身影
    - 大量技术书籍与著作涌现
  - 黑客培训商业化：黑客基地、华夏黑客同盟、第八军团
  - 黑帽子日趋猖獗：证券大盗、灰鸽子、熊猫烧香、**DDoS**、网络虚拟资产地下经济链...

黑客道文化精髓:
ESR五部曲之《黑客道: 如何成为一名黑客》

- 搞清楚黑客和骇客的区别
  - 根本的区别是：黑客搞建设，骇客搞破坏
  - 骇客往往自称为黑客，黑客往往是由**community**所认可
- 如何成为一名黑客
  - **To follow the path: (沿着这样一条道路:)**
  - **look to the master, (寻找大师,)**
  - **follow the master, (跟随大师,)**
  - **walk with the master, (与大师同行,)**
  - **see through the master, (洞察大师,)**
  - **become the master. (成为大师.)**

黑客应有的态度

- **1.** 世界充满了待解决的迷人问题。
  - 做一名黑客会有很多乐趣，但却是要费很多气力方能得到的乐趣。
  - 做黑客，你得能从解决问题，磨练技术及锻炼智力中得到基本的乐趣。
- **2.** 一个问题不应该被解决两次。
  - 聪明的脑袋是宝贵的有限的资源。
  - 解决问题并发布结果给其他黑客几乎是一种道义。

黑客应有的态度(2)

- **3.** 无聊和乏味的工作是罪恶。
  - 无聊和乏味的工作不仅仅是令人不舒服而已，而且是罪恶。
  - 作为一个黑客，你必须坚信这点并尽可能多地将乏味的工作自动化，不仅为你自己，也为了其他人（尤其是其他黑客们）。
- **4.** 自由万岁。
  - 黑客们是天生的反独裁主义者。
  - 作为一个黑客， 你得对审查、保密，以及使用武力或欺骗去压迫有行为能力的人们的做法有一种本能的敌意。
- **5.** 态度不能替代能力。
  - 成为一名黑客需要智力，实践，奉献精神和辛苦工作。
  - 你必须学会怀疑，并尊重各种各样的能力。

黑客道德

- 传统黑客道德 – **Old Hacker Ethics (Levy - <Hackers: Heroes of the Computer Revolution>)**
  - **Hands On Imperative (首要诫令：对计算机和硬件的访问应是彻底和完全的)**
  - **Information Wants to Be Free (自由、没有知识产权、免费)**
  - **Mistrust Authority (不信任权威，促进分权)**
  - **No Bogus Criteria (黑客只以技术能力和成就进行评价，没有其他“伪造的标准”)**
  - **You can create truth and beauty on a computer (Hacking=艺术和创新)**
  - **Computers can change your life for the better (计算机能改善生活，黑客应为之奋斗)**

黑客道德(2)

- “90年代新黑客道德” – New Hacker Ethics (Steven Mizrach, Is there a Hacker Ethic for 90s Hackers?)
  - Above all else, do no harm (无论如何，不要作恶)
  - Protect Privacy (保护隐私)
  - Waste not, want not (浪费可耻; 无欲无求)
  - Exceed Limitations (超越限制)
  - The Communicational Imperative (通讯自由)
  - Leave No Traces(不要留下任何踪迹)
  - Share! (共享！)
  - Self Defense (自我防御)
  - Hacking Helps Security (投身帮助提高安全性)
  - Trust, but Test! (只有通过渗透测试才能信任！)

法律法规

- 黑客道德 **VS.** 法律法规
- 各国均有相关法律法规，成熟程度和侧重面不同
- 我国信息安全相关立法情况
  - 基本法律、民法: 宪法、商标法、专利法、保守国家秘密法、反不正当竞争法等在数字网络空间仍适用
  - 刑法: 普遍条款，专门针对打击计算机犯罪的**285-287**条款
  - 国家条例与管理办法
    - 计算机软件保护条例**(1991.6.4)**
    - 计算机系统安全保护条例**(1994.2.18)** → 计算机信息系统安全保护等级划分准则**(1999.10)**
    - 商用密码管理条例**(1999.10.7)**,计算机信息系统国际联网保密管理规定**(2000.1.1)**
    - 计算机病毒防治管理办法**(2000.4.6)**
    - 互联网信息服务管理办法**(2000.9.20)**
    - …

刑法中关于计算机犯罪相关条款

- 第285条－(非法侵入计算机信息系统罪)
  - 违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
- 第286条－(破坏计算机信息系统罪)
  - (1) 违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。
  - (2) 违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。
  - (3) 故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。
- 第287条－(利用计算机实施的各类犯罪)
  - 利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

刑法修正案-285条

- 2009年2月刑法修正案(七)，十号主席令
- 285条增加两款
  - 侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。
  - 提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚
  - 拓展法律保护的范围，加强了惩罚力度

相关案例

- **2004年证券大盗案件**
  - 盗取股票帐号，盗买、盗卖股票价值**1141.9**万元，非法获利**38.6**万元
  - 刑法第**264**条盗窃罪 + 刑法第**287**条利用计算机实施的各类犯罪：主犯无期徒刑
- **2006年1月首宗盗卖QQ号码案**
  - 腾讯内部人员盗取**QQ**号保护信息，联合外部人员盗取并出售，获利**6**万多元
  - 刑法第**252**条侵犯通信自由罪 +《人大常委会关于维护互联网安全的决定》：拘役六个月
- **2007年“熊猫烧香”案件**
  - 故意制作和传播计算机病毒，主犯李俊获利**14.5**万元
  - 刑法第**286**条破坏计算机信息系统罪：主犯有期徒刑**4**年

相关案例(2)

- **2009年2月“大小姐”系列木马团伙网络犯罪案**
  - 占据我国木马盗号程序市场**60%?**，经王业供述，他生意最好的时候，曾经**3**个月就挣了**3000**万？！
  - 全国首例提供程序工具“非法侵入计算机信息系统罪”**285**条补充条款第**3**条

- **2009年8月“温柔”系列木马团伙网络犯罪案**
  - 占据中国木马市场份额约一半，该案涉案金额逾三千万元
  - **286**条涉嫌破坏计算机信息系统罪

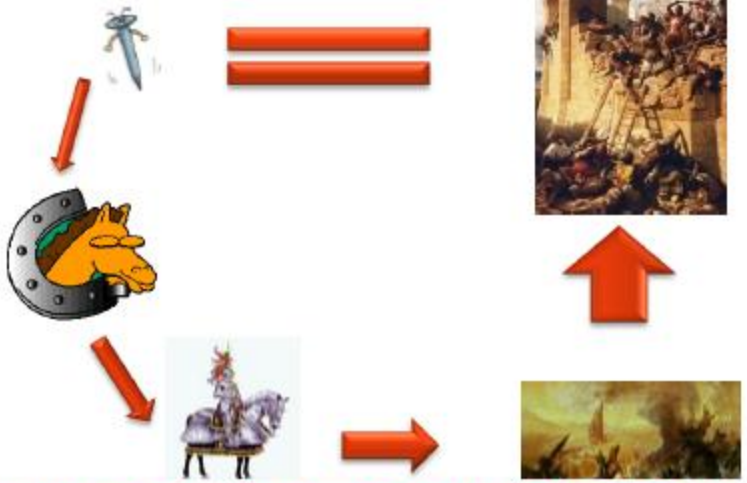
蝴蝶效应 – “小事件也能有大影响”

蝴蝶效应：1963年 美国气象学家洛伦兹提出来

大意：一只南美亚马逊河流域热带雨林中的蝴蝶，偶尔扇动几下翅膀，可能在两周后引起美国德克萨斯的一场龙卷风。

一个民谣：

丢失一个钉子，坏了一只蹄铁；
坏了一只蹄铁，折了一匹战马；
折了一匹战马，伤了一位骑士；
伤了一位骑士，输了一场战斗；
输了一场战斗，亡了一个帝国。



事物发展的结果对初始条件具有极为敏感的依赖性。
初始条件的极小偏差，将会引起结果的极大差异。

5.19断网事件的蝴蝶效应

DNSPOD.COM被人恶意大流量攻击，承担DNSPOD.COM网络接入的电信运营商断掉了其网络服务。

因暴风影音软件网络服务的需要和缺陷，使得安装有暴风影音的电脑不断发起域名解析请求，导致网络瘫痪。

由于DNSPOD网络服务被中断，诸多采用DNSPOD服务的网站无法访问。采用DNSPOD服务的暴风影音网站受到影响。

519断网案告破

您所在的位置： 腾讯首页 > 科技频道 > 互联网新闻 > 正文

5.19断网案告破：当事人称对互联网影响深远

http://tech.QQ.com 2009年06月02日18:13 腾讯科技 京东 我要评论(4)

腾讯科技讯 6月2日下午消息，导致5.19日南方6省断网事故案的4名嫌疑犯终于被公安

519断网案告破：少年花28万租81台私服发起攻击

2009年07月15日10:40 [我来说两句(53)] [字号：大 中 小]

买变频 选美的

来源：常州晚报

5月19日晚19点左右，江苏、安徽、浙江、广西、海南、甘肃六省区出现严重网络故障，很多网民在登陆互联网时发现，新浪、搜狐、网易等各大门户网站均不能访问。5月20日，广东省也出现类似故障。

0 519断网案嫌犯被抓：最高学历仅为

引用

8月20日，广东佛山警方向社会公布，该局破获

永嘉籍青年男子徐某。该案由网络"私服"攻击所

市公安局天宁分局，并被天宁区检察院批准逮捕

后遇到这类攻击案件，他将毫不犹豫选择报案。（文/京东）

- 架设私服，对竞争对手网站使用的域名服务器**DNSPod**实施攻击

内容

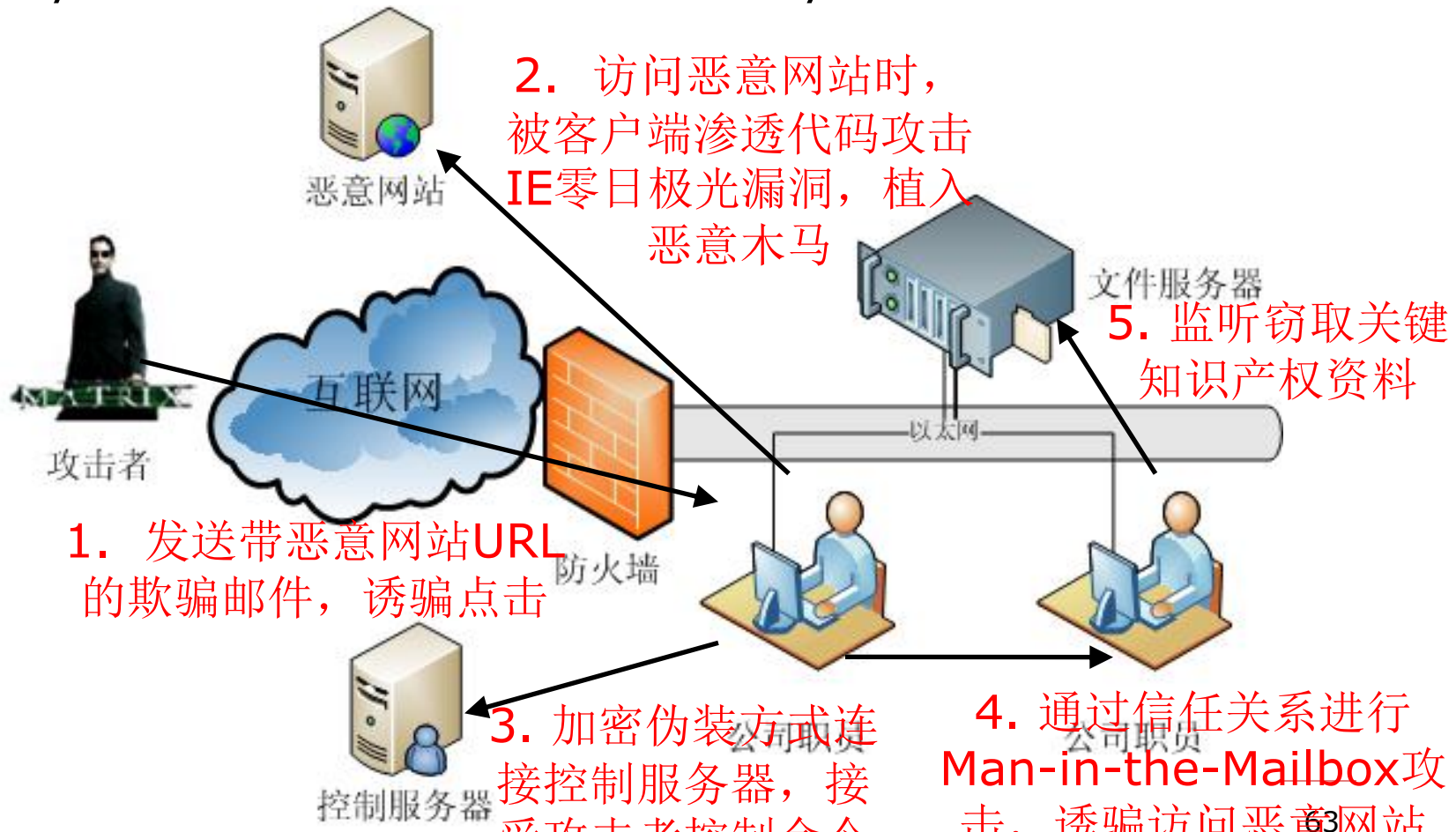
1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

“极光”攻击事件

- 今年年初**Google**退出中国市场的导火索
  - 美国二十多家大型企业遭受“极光”攻击
  - 窃取企业知识产权
- **IE**浏览器“极光”**0 day**安全漏洞
  - 意外公开披露，引发国内挂马攻击狂潮
  - 《中国教育网络》**2010**年**2**月期**:** 微软“极光”漏洞殃及谷歌和中国网民
- “源自中国”？→ 中国黑客威胁论
  - 一段中国特色的生成**CRC**校验和的代码**?**
  - 上海交通大学 **&** 山东蓝翔高级技工学校**?**

“极光”攻击技术内幕

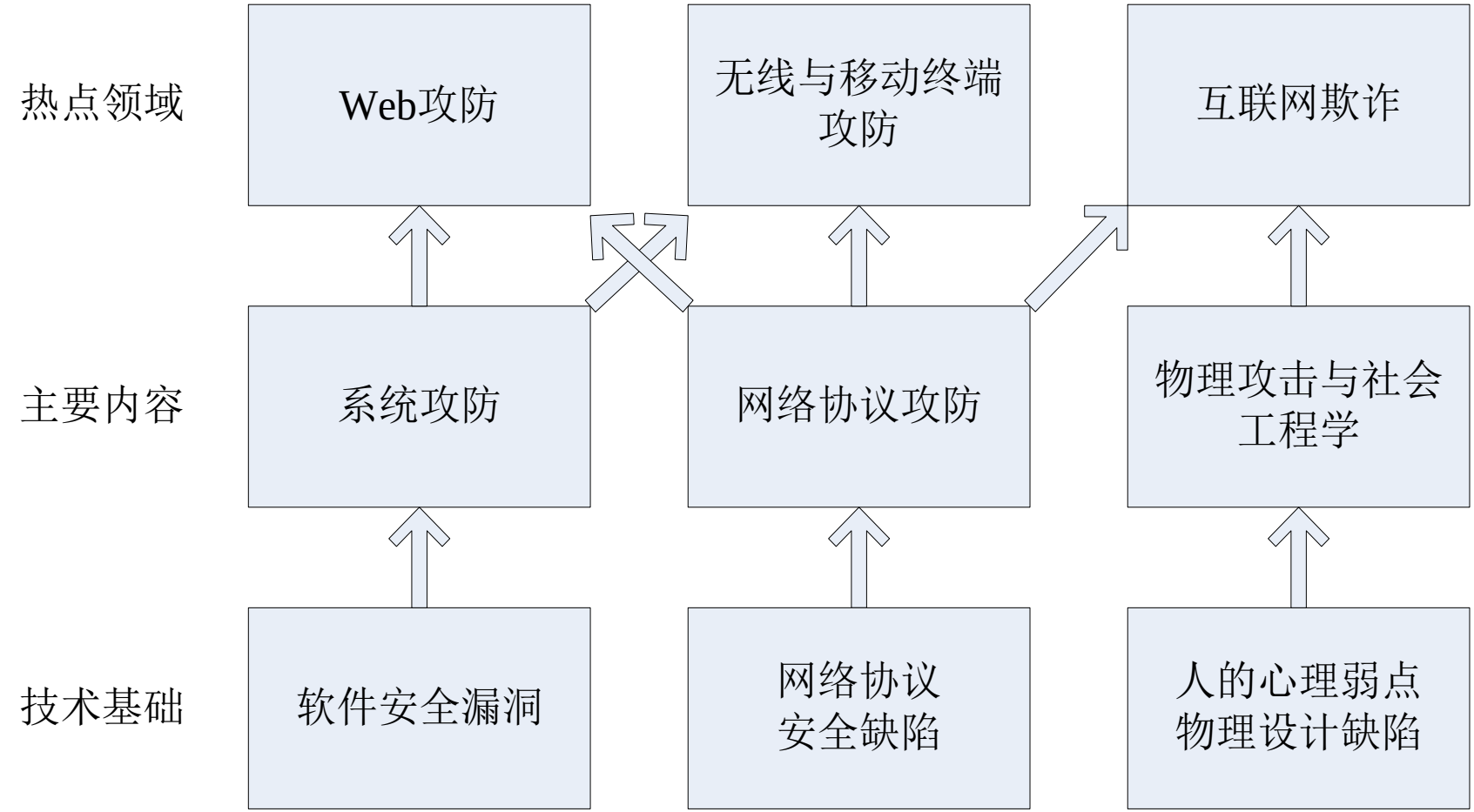
美国Symantec、SecureWorks、HBGary等安全公司受委托进行调查



从“极光”事件看攻击形态

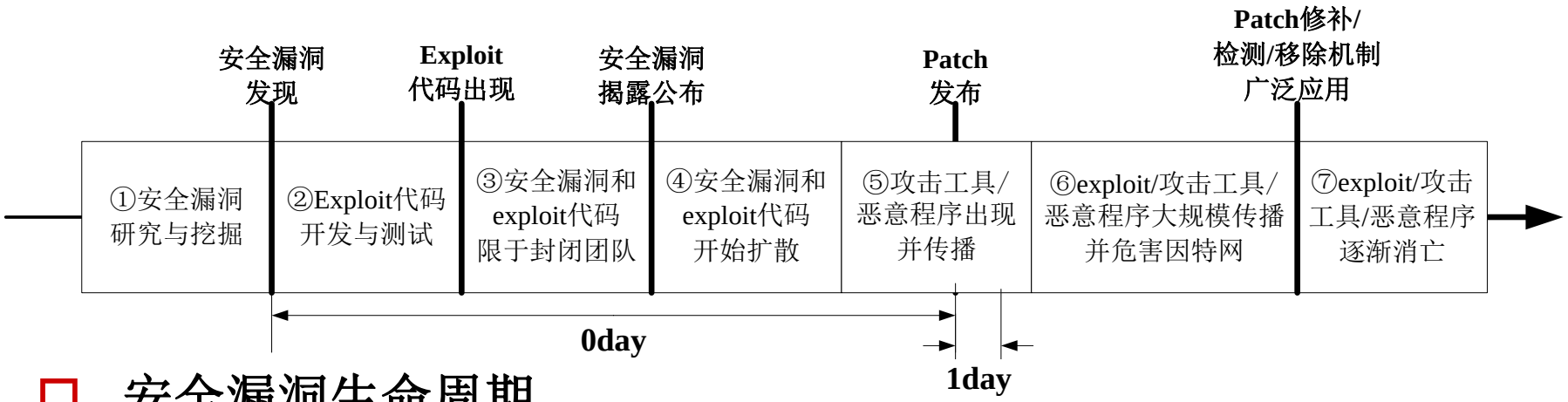
- 计算机系统
  - 硬件、操作系统、网络服务/应用程序
  - 系统安全攻击：利用安全漏洞的渗透攻击和恶意代码感染
  - **IE**“极光”网页木马渗透攻击：利用**IE**安全漏洞
- 网络
  - 网络**(network of computers)**→互联网**(network of networks)**
  - 网络协议攻击与滥用：设计缺陷**&**滥用**(**源地址欺骗、**DDoS)**
  - **Man-in-the-Mailbox**攻击：电子邮件缺乏身份认证
- 人
  - 计算机和互联网的使用者
  - 物理攻击/社会工程学：环境与人性弱点
  - 欺骗邮件：诱骗点击邮件中的链接

网络攻防技术框架



系统攻防

- 系统攻防的基础 – 安全漏洞



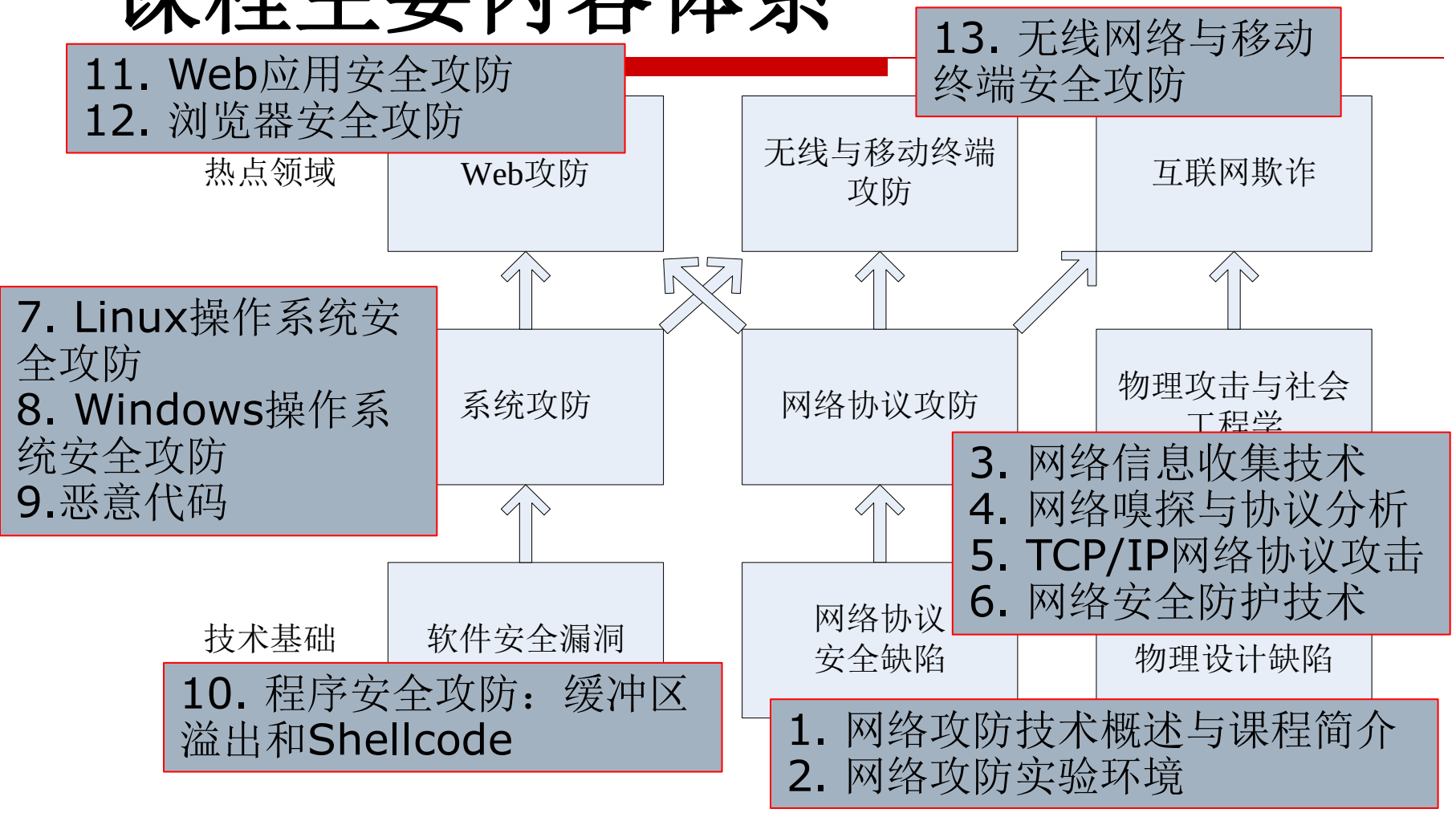
- 安全漏洞生命周期

- 系统攻防的核心：安全漏洞、Exploit(渗透攻击)/恶意代码、安全防御与检测机制三者之间的技术博弈

网络协议攻防

- **TCP/IP**网络协议在设计时存在的安全缺陷或不安全因素。
- 网络信息收集
- 网络接口层：网络嗅探
- 网络互连层：**IP**源地址欺骗、**ARP**欺骗、**ICMP**协议攻击
- 传输层：**TCP**重置攻击、会话劫持、**SYN**洪泛、**UDP**洪泛
- 应用层：敏感信息窃听、篡改与身份假冒

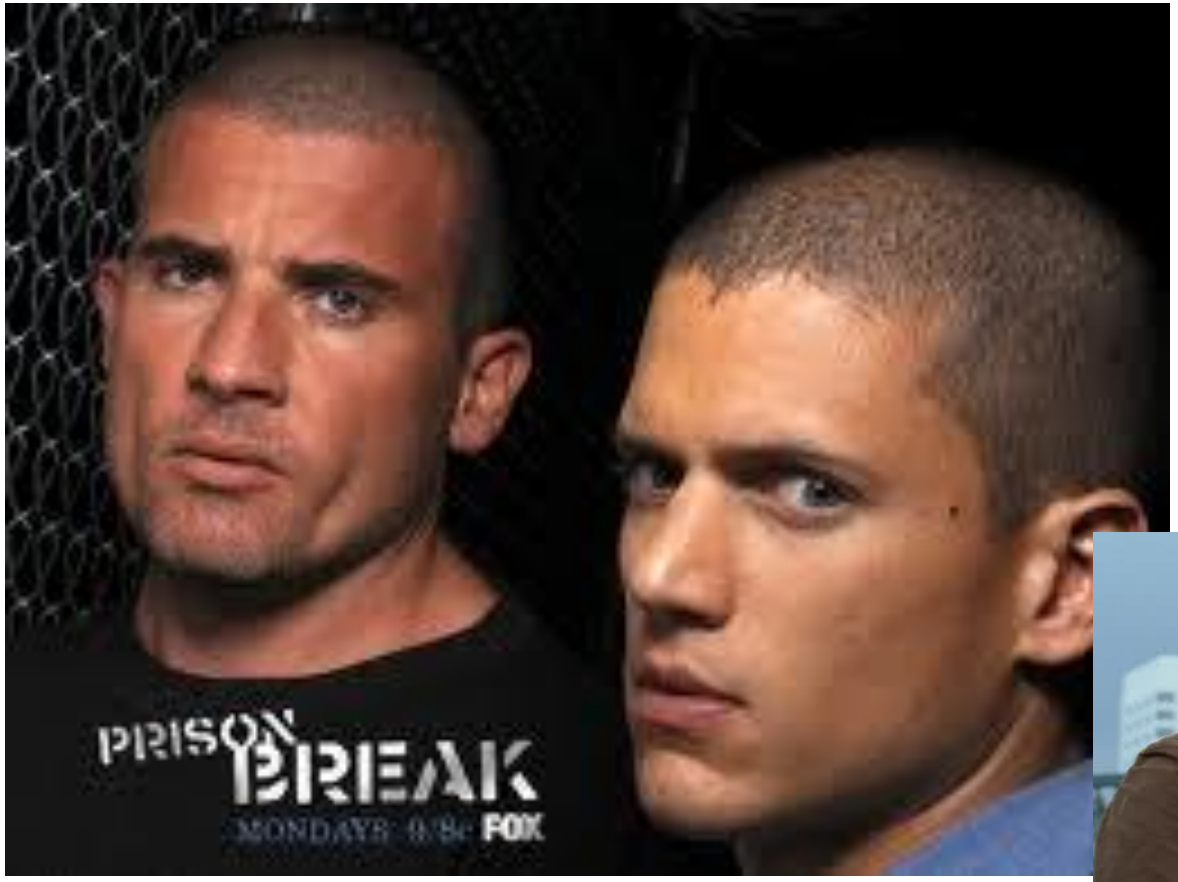
课程主要内容体系

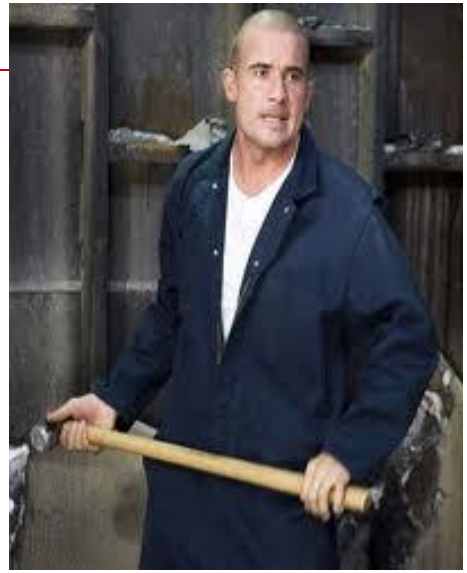


内容

1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

物理攻击与社会工程学





物理攻击

- 物理攻击定义
  - 通过各种技术手段绕开物理安全防护体系，从而进入受保护的设施场所或设备资源内，获取或破坏信息系统物理媒体中受保护信息的攻击方式
- 经典物理攻击场景
  - 《碟中谍1》之潜入中央情报局偷取 NOC名单
  - 《越狱》之闯入Company总部偷取Scylla
- 物理攻击并非遥不可及
  - 宾馆的锁并不安全
  - 《战争游戏》便贴纸上窥视到教务系统登录口令
  - 1978年“最大的计算机诈骗案”
  - 实验室中笔记本电脑被盗

物理攻击防御措施

物理攻击防范Checklist

- 笔记本/手机防盗：寝室、食堂、实验室
  - 必要时使用笔记本锁
- 注意真正的桌面安全
  - 高价值财物，重要资料文档
  - 有价值信息：口令便贴纸，随手记的密码，财务信息，移动硬盘/U盘等
  - 离开时电脑锁定，尽量不让不可信的他人使用自己的电脑/U盘等
- 门禁安全
  - 确保门禁关闭，拒绝陌生人(开门、尾随)

看看这台ATM机有什么问题?

社会工程学

- “只有两种事物是无穷尽的——宇宙和人类的愚蠢，但对于前者我不敢确定。” ——爱因斯坦
- 社会工程学攻击
  - 利用人类的愚蠢，操纵他人执行预期的动作或泄漏机密信息的一门艺术与学问。
- 社会工程学技巧
  - 不引人关注的职业，攻击新员工，伪装身份，正面攻击，构造陷阱施以援手，制造陷阱骗取同情与帮助，奉承改善自我感觉，施以小恩小惠，垃圾搜寻，结合多种技术手段
- 知名社会工程师
  - **Kevin Mitnick: Book-The Art of Deception, The Art of Intrusion, ..**
  - **Frank Abagnale: Movie/Book-Catch Me if You Can**

《Catch me if you can》中的经典社会工程学片段

- 1.采访、电话获取信息
- 2.兑现支票
- 3.第一次抓捕

社会工程学防御措施

- 尽可能不要使用真名上网，将真实世界与网络世界划清明确的界限；
- 不要轻易相信别人，尤其是未曾谋面或未建立起信任关系的陌生人；
- 别把自己的电脑或移动终端轻易留给别人使用，必要时刻(如维修电脑时)务必清理上面的个人隐私信息，否则结果可能会很惨；
- 单位应建立起规范的安全操作规程，包括门禁和人员控制，不同分类资料数据的访问机制，规范的垃圾回收和处理机制等；
- 单位应对员工进行安全意识和操作规程培训，使其具备基础的社会工程学抵御能力。
- 涉密信息与计算机系统的处理有着相应更加严格的保密流程与规范。

内容

1. 课程简介
2. 网络攻击和取证分析案例演示
3. 黑客与黑客道
4. 网络攻防技术概述
5. 物理攻击与社会工程学
6. 作业1

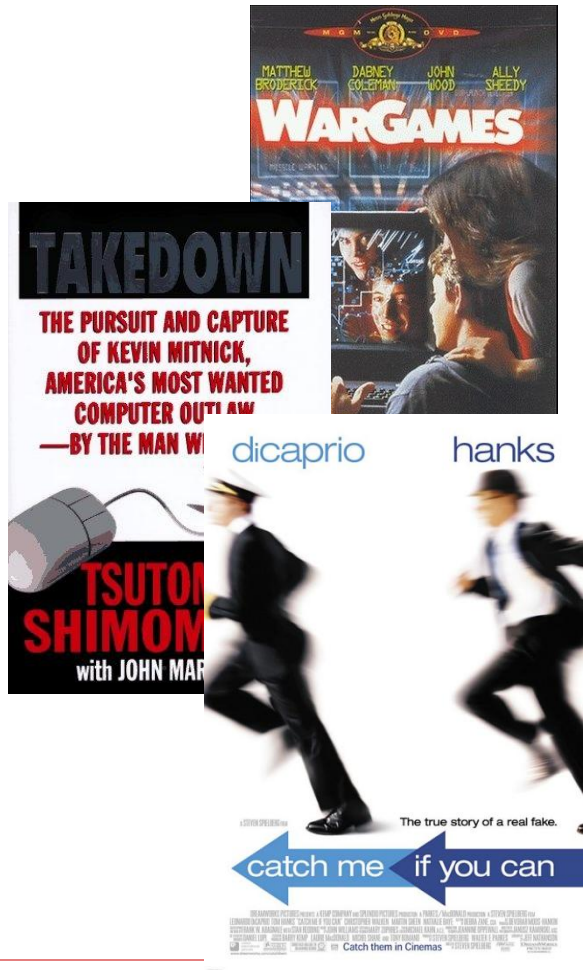
作业1

- 作业1（10分+2分bonus）- 团队作业
  - 作业1.1—黑客电影鉴赏或黑客影视片断剪辑说明(5分)
  - 作业1.2—通过社会工程学手段尝试获知异性同学的 a)生肖 b)星座 c)出生日期 d)生辰八字(bonus: 2分)，并详述你的社会工程学攻击过程，包括成功的和失败的。 (5分)

- 提交deadline
  - 发布至HackingExposed版面，注意作业1.2的匿名化
  - 发邮件给助教登记, zhanghuilin@icst.pku.edu.cn
  - 2009年9月29日

作业1.1－黑客电影鉴赏

- 观看下列四部好莱坞大片之一或其他自选黑客电影，观看后写影评或观后感，发到BBS课程版面，并通知助教
- 《战争游戏》
  - **1983年 War Games**
  - 导演：约翰·班德汉姆；主演：马修·布鲁德里克, 迈克尔·麦德逊
- 《骇客追缉令》
  - **2000年 Take Down**
  - 导演：乔·查派尔； 主演：斯基特·奥里奇, 汤姆·贝伦杰
- 《逍遥法外》
  - **2002年 Catch Me If You Can**
  - 导演：斯蒂文·斯皮尔伯格； 主演：汤姆·汉克斯, 莱昂纳多·迪卡普里奥
- 《战争游戏2：死亡代码》
  - **2008年 War Game 2: The Dead Code**
- **…**



作业1.1－黑客影视片断剪辑和说明

- 从某部黑客相关影视作品中剪辑出一个主题视频，如社会工程学，物理攻击等，说明利用了何种攻击手段，加以具体评述
- 如
  - 《PB:越狱》中的社会工程学技巧案例
  - 007中的物理攻击经典片段
  - …
- 视频剪辑软件
  - 格式工厂软件简介(FTP/materials/)
  - Google其他你所喜欢的视频剪辑软件
- 发布至BBS或课程FTP, 通知助教

作业1.2－社会工程学攻击尝试

- 通过社会工程学手段尝试获知异性同学的
- a)生肖
- b)星座
- c)出生日期
- d)生辰八字(bonus 2分)

- 详述你的社会工程学攻击过程，包括成功的和失败的。

Thanks

诸葛建伟

zhugejianwei@icst.pku.edu.cn

请向助教登记选课学生信息

学号，学院/专业，年级，**Email**地址