网络空间安全认知实习

苑　洁

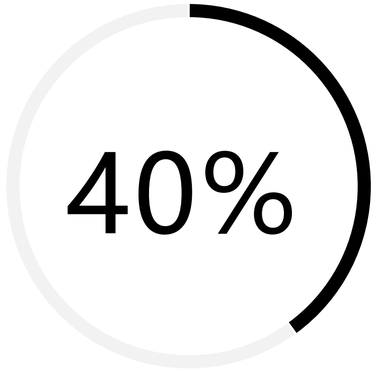
yuanjie@bupt.edu.cn

成绩考核

本课程1学分，考核方式为考察，总成绩100分。

成绩由两部分组成

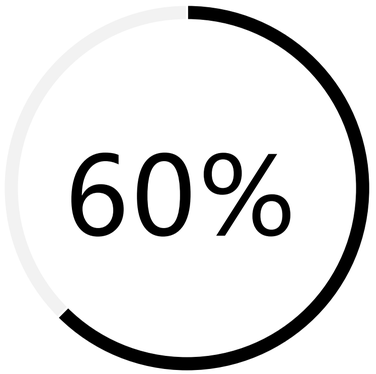
平时表现+报告部分



平时表现

考勤
课堂表现
展示和演示

共计40分



报告部分

通识报告
实验报告
实践报告

共计60分

课程进度安排

周一上午　课程内容讲解、企业专家讲座	周一下午　上机实践、撰写报告
周二上午　上机实践、撰写报告	周二下午　13：00创新创业讲座、撰写报告
周三上午　上机实践、撰写报告	周三下午　13：00汇报展示、填写调查问卷、实习报告、ppt的提交

实习验收

完成实习各部分，按照规定模板完成实习报告、准备5分钟ppt，以学号+姓名的格式命名，

8月30日周五下午六点前在教学云平台提交

扩展阅读

官方网站资料

- Getting Started with Metasploit for Penetration Testing, https://www.metasploit.com/get-started
- Kali Linux Documentation, https://www.kali.org/docs/
- Nmap Security Scanner, https://nmap.org
- The Hacker’s Choice, https://www.thc.org
- https://www.social-engineer.org/
- http://www.xshellcn.com/xsh_column/

扩展阅读

参考书目

- 《网络技术攻防与实践》 作者 诸葛建伟
- 《Kali Linux渗透测试技术详解》作者 杨波
- 《Metasploit渗透测试指南》 作者 David Kennedy等
- 《黑客大曝光：网络安全机密与解决方案（第7版）》 作者Stuart McClure等
- 《白帽子讲web安全》 作者 吴翰清
- 《加密与解密》 作者 段钢
- 《The Art of Intrusion》 作者 Kevin D. Mitnick
- 《社会工程 安全体系中的人性漏洞》 作者 Christopher Hadnagy
- 《CISSP官方学习手册》作者 Mike Chapple

联系方式

get in touch

地点：网安楼529

苑洁 老师

yuanjie@bupt.edu.cn

助教、答疑

junjuntvt@bupt.edu.cn

网络空间安全通识部分

2024全国两会

全国政协委员周鸿祎携三份提案上会聚焦安全和人工智能两件事

提案一 关于深化人工智能多场景应用支持大模型向垂直化、产业化方向发展的提案

相关建议:

1.场景很重要，大模型在垂直领域大有可为，建议政府、央国企率先提供更多应用场景，聚焦“小切口，大纵深”，推动大模型垂直化、产业化落地。知识很重要，基于“暗知识”的垂直大模型能更好。

2.解决企业问题，建议鼓励企业在定制AI前，做好知识管理，将企业大数据平台升级为企业知识平台。

3.业务融合很重要，建议鼓励和引导企业将大模型与数字化业务系统深度结合，同业务流程相结合充分发挥大模型价值。

2024全国两会

全国政协委员周鸿祎携三份提案上会聚焦安全和人工智能两件事

提案二　关于鼓励兼具“安全和AI”能力的企业解决通用大模型安全问题的提案

相关建议:

1.建议国家更加重视通用大模型安全问题，给予兼具“安全A”能力的企业专项扶持政策，更好发挥其解决通用大模型安全问题的重要作用。

2.建议国家研究制定保障通用大模型安全的标准体系，推动通用大模型开展安全评测、接入安全服务，降低通用大模型安全风险

3.建议政府、央国企与兼具“安全和AI”能力的企业在大模型安全领域展开深入合作，发挥此类企业在人工智能安全领域的优势作用。

2024全国两会

全国政协委员周鸿祎携三份提案上会聚焦安全和人工智能两件事

提案三 关于全面建设安全云推广数字安全云化服务的提案

相关建议:

1.统筹建设数字安全公共服务基础设施，集中数字安全能力。

2.改变重建设轻效果的思路，鼓励各单位购买数字安全云化服务，作为传统网络安全建设的升级路径。

3.鼓励网络安全企业积极转型，以“安全即服务方式为国家整体数字安全水平提升做出贡献，尤其是鼓励具备核心技术的被美制裁的龙头企业发挥更大作用。

2024全国两会

全国政协委员齐向东：**创新发展“AI+安全”**

网络和数据安全是数字经济发展的底板工程，建议：针对AI带来的安全威胁、攻防失衡和军事威胁，应大力探索“AI+安全”创新应用，比如鼓励各行业头部企业与专业安全厂商结成创新联合体，并针对“AI+安全”发展设置专项基金。

网络空间安全新态势

- **网络空间安全威胁层出不穷**——全球网络安全战略进入全球部署阶段，各国为了维护本国在网络安全的核心利益，持续加大网络空间的军事投入，网络战威胁日益严重。
- **大规模网络攻击事件持续高发**——大规模网络攻击已经升级为成为全球五大风险之一。软硬件设备安全漏洞频出、关键信息基础设施遭受攻击、个人信息和商业数据遭受噶规模泄露和违规利用。网络安全态势趋向复杂化、网络攻击事件不断增多、影响范围持续加大。
- **个人信息保护与利用深度影响大数据应用发展**——大数据收集、分析、应用发展与信息安全基本是诉求形成重大冲突。

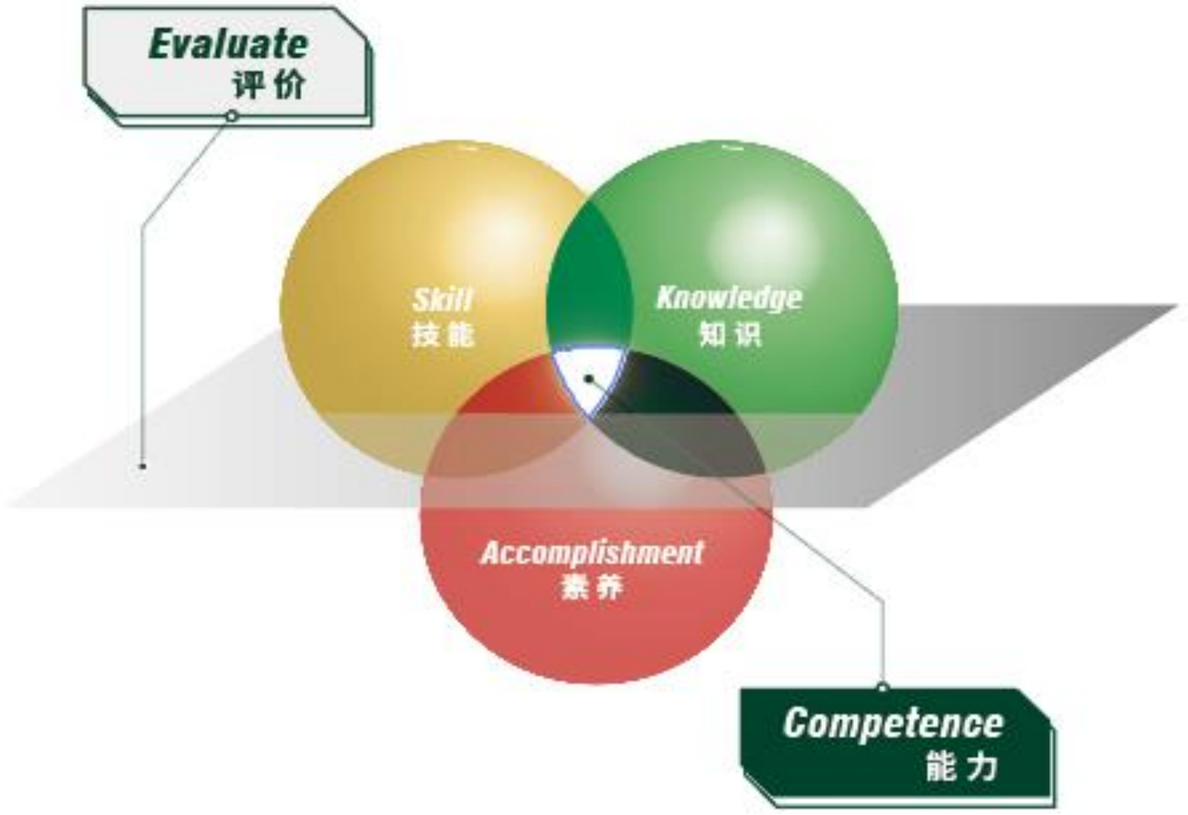
网络空间安全新态势

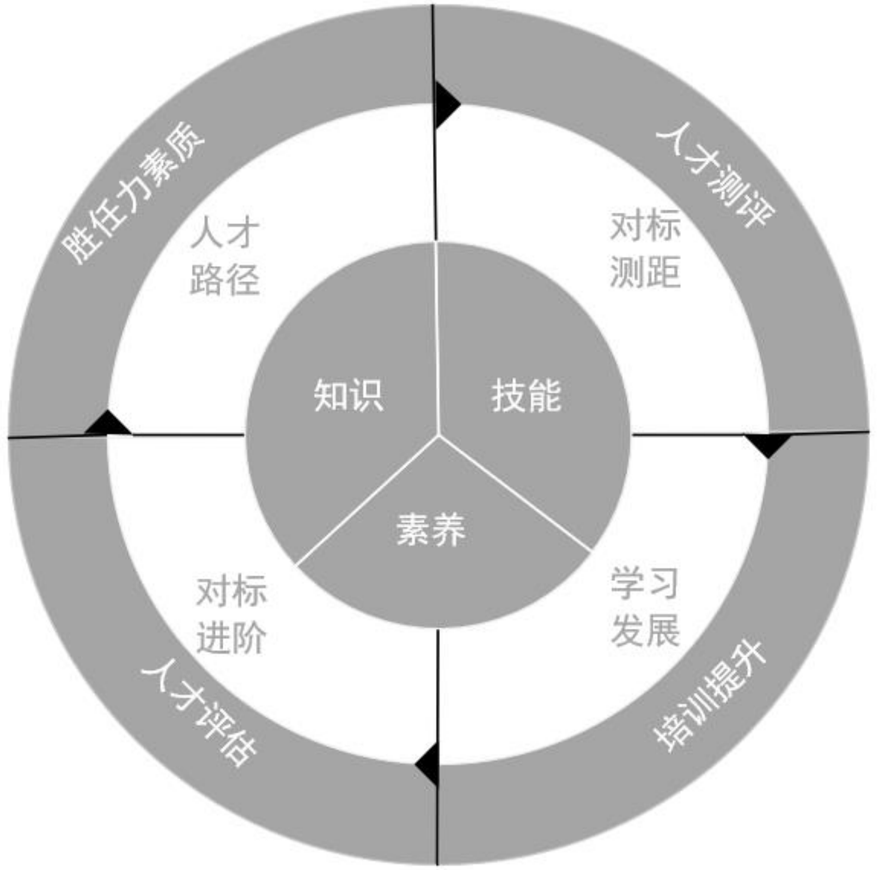
- **体系化协同防御成为网络安全保障新趋势**——在数字化转型、5G 网络覆盖、移动互联网及物联网快速应用的大背景下，政府机关、能源、交通、通信、金融、水利等行业关键信息基础设施暴露在互联网上的情况续增多，攻击者除了利用安全漏洞、口令、拒绝服务等常见方式实施攻击外，通过供应链、云平台、大数据等作为攻击途径的事件也呈上升趋势。大数据背景下的体系化协同防御将成为网络安全保障的发展趋势。
- **网络空间人才培养是关键**——人才短缺依然形势严峻，从业人员在知识储备、技能、职业素养等方面亟待提高。

网络安全人才
是安全保体系的决定因素

- 网络安全的本质是人与人的对抗，网络安全人才能力发展须与组织安全需求相匹配，组织应通过普通高校、职业院校、科研院所及企业联合培养新时期复合型网络安全人才。根据国家网信部门要求，建立政府、企业等安全需求及安全能力大数据，并通过逐步丰富的安全人才大数据，更精细化、自动化、个性化地获得网络安全人才及人才需求， 从而建立社会化的网络安全人才运营体系，支撑我国网络空间安全战略。

网络安全人才能力模型


Evaluate
评价
Skill
技能
Knowledge
知识
Accomplishment
素养
Competence
能力


胜任力素质
人才测评
人才
路径
对标
测距
知识
技能
素养
对标
进阶
学习
发展
人才评估
培训提升

网络安全人才培养体系和组织建设能力架构

- 基于近十几年网络安全发展趋势，以及对国内外网络安全法律法规、人才战略、标准的参考，对于网络安全组织的能力建设进行了初步总结提炼与研究，可以将网络安全组织建设方向分为6大方向，26个专业领域，94个安全任务角色。

网络安全人才培养体系和组织建设能力架构

网络安全组织建设能力框架

6大分类	26个专业领域
监督、管理与合规	网络安全检查、网络安全等级保护、风险治理、法律法规
规划、开发与建设	网络安全架构、网络安全规划、系统开发、安全测试评估
运行、维护与评估	网络安全管理、数据安全、安全运维管理、技术支持
检测、防御与响应	网络安全检测、网络安全防御、实战攻防演练、应急响应
意识、教育与培训	网络安全人才研究、网络安全意识、网络安全培养
创新、支持与促进	创新与研究、新技术研究、服务支撑、产业促进

94个
安全任务角色

599条任务

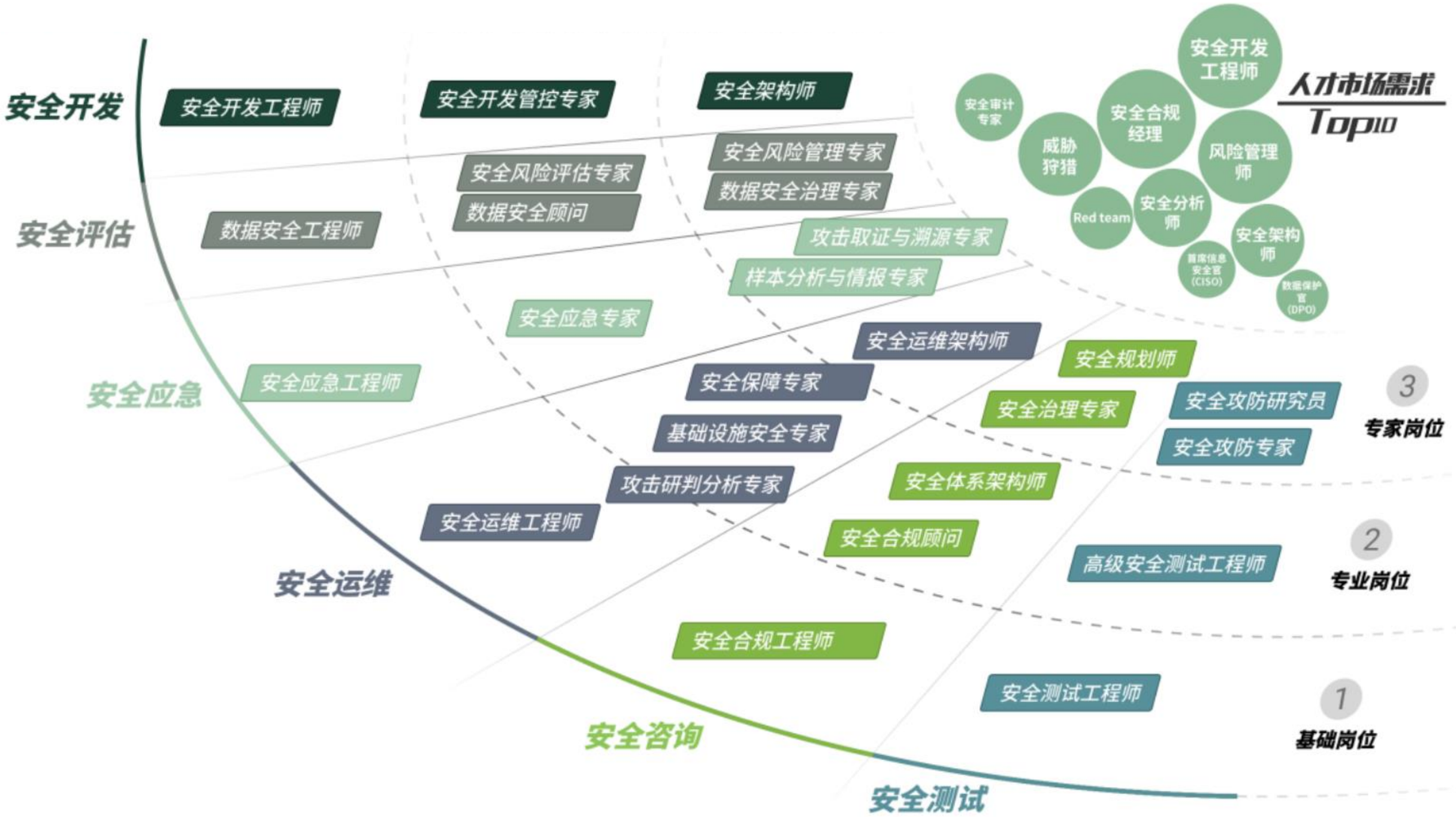
405条知识

619条技能

65条素养

网络安全服务人才成长路线

- 安全岗位是人才发展路线的立足点，岗位的设定和演进关乎着人才的关键发展。
- 基于各类安全能力诉求，提出了**六大岗位方向**（安全评估、安全开发、安全运维、安全应急、安全测试和安全咨询）、**三层岗位级别**（基础岗位、专业岗位和专家岗位）、二十六种岗位设定的安全服务人才发展路线图，细化岗位的关键技能，识别各方向涉及的知识领域和技能特性，帮助个人确认目标达成路径以及发展过程中的技能需求。

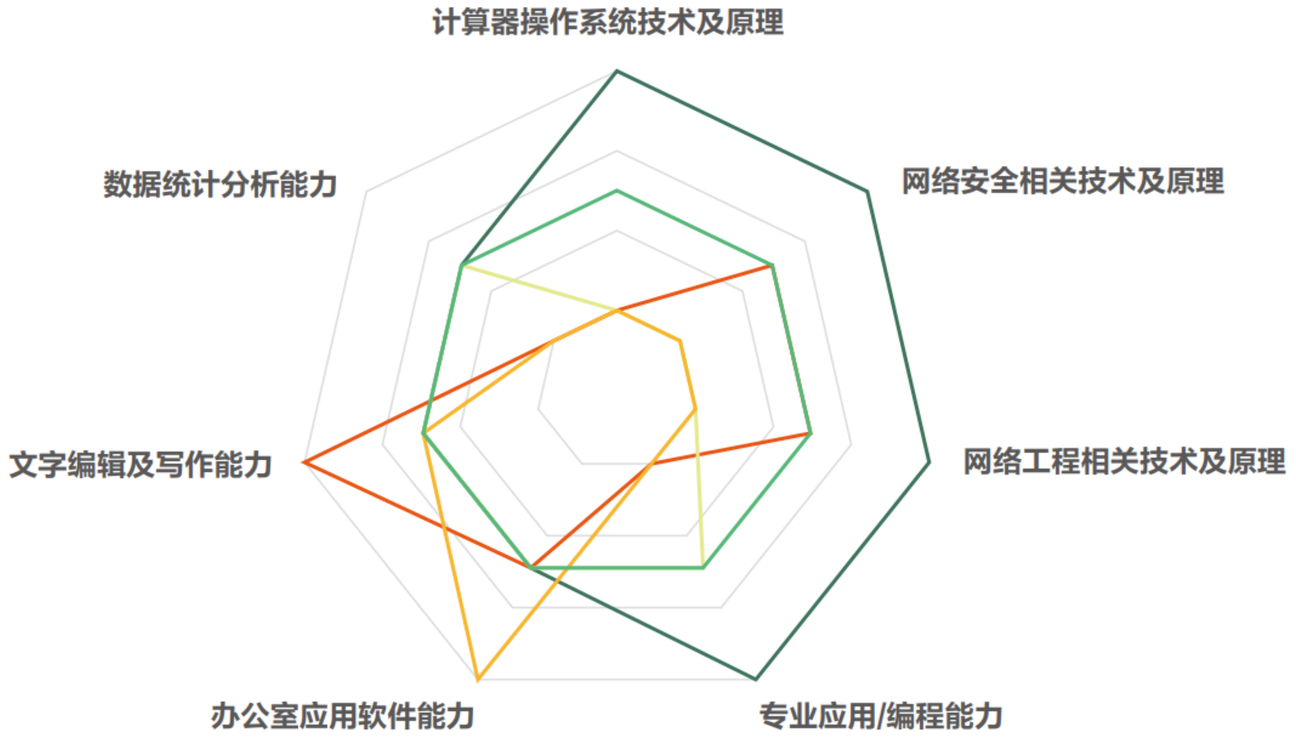


网络空间安全认知实习

网络安全服务岗位关键技能

- 根据六大岗位方向所需的关键技能，结合三层岗位级别，制作了安全服务岗位关键技能图。
- 通过构建安全人才的职业发展通路，解决信息安全服务人才职业发展的根本困惑，指引团队通过技能提升从而创造更多的专业能力。
- 根据工作需要和职责要求，每一个岗位都有关键的工作任务和必备的技能。

网络安全人才不同岗位专业能力分布



不同岗位专业能力分布图

研发岗　销售岗　运营岗　职能岗　产品岗

给网络安全在校生的建议

- 脚踏实地，打好专业基础；
- 积极参与课外实践；
- 尽早完成较清晰的职业规划。

从事科学研究、基础研发、安全服务和安全运维等不同工作岗位，对基础素质、综合能力和专业技术均有不同的要求，多数用人单位选拔的是知识结构优化，基础能力扎实的，值得继续培养的人才，因此实践经验固然重要，基础知识也将决定能力天花板的高低，多参加社团活动和学科竞赛是切实可行的能力提升渠道。

网络空间安全认知实习

通识报告

就以下其中一到两个方向展开思考和探索，记录学习的思考过程和收获，解决问题的过程、方法和收获等，形成报告，不少于1000字。

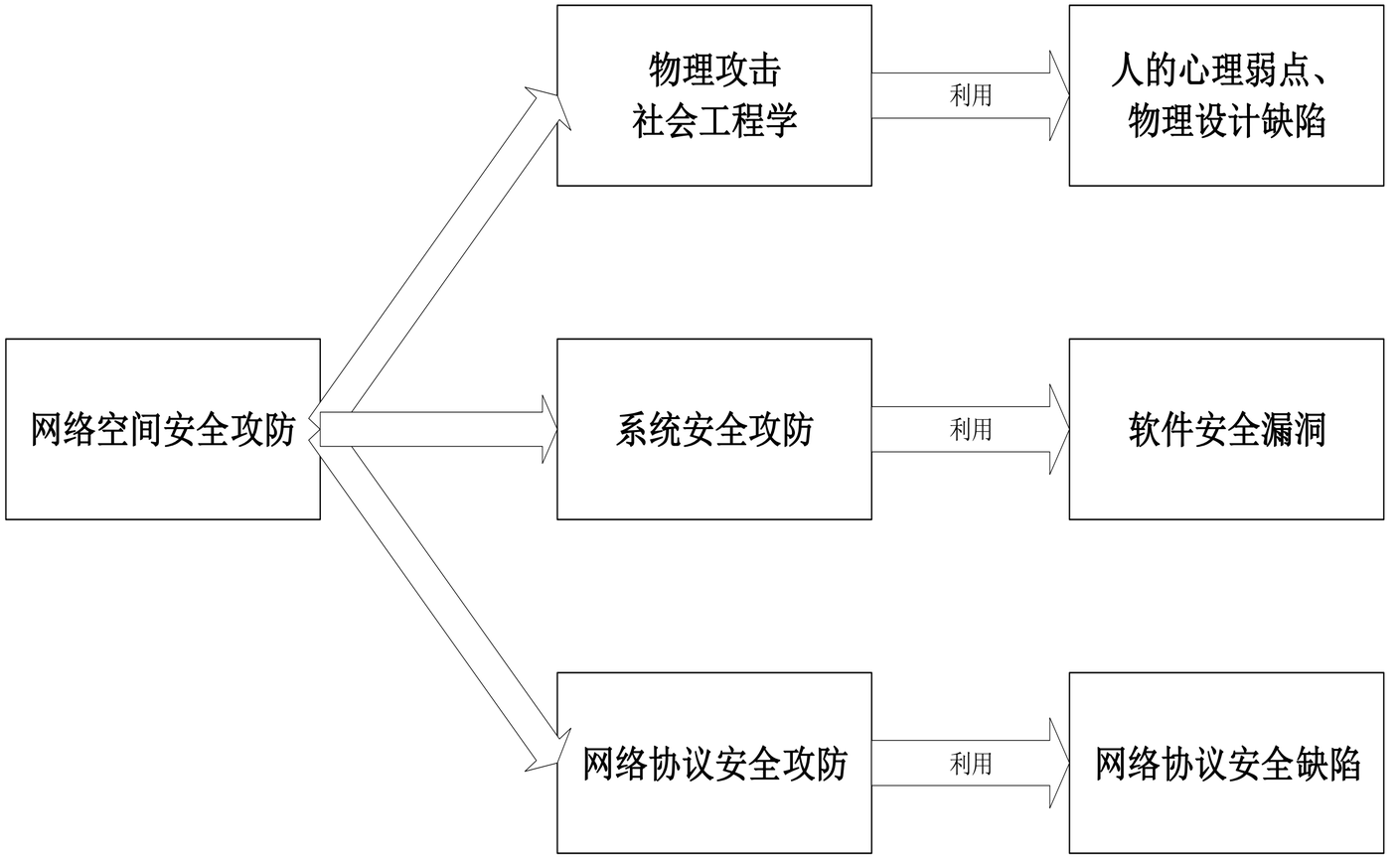
- 洞悉网络空间安全领域态势发展、前沿技术的发展，就此方向展开探讨和分析。
- 从国家、法律、行业、专业知识与技能等多个角度，按照自己的理解形成对网络空间安全综合认知。
- 理解人才是安全保障体系的决定因素，思考如何从知识、技能、素养三方面全面提升自己的能力。
- 了解网络安全服务人才岗位需求、技能要求、成长路线，思考个人职业规划和发展。

网络攻防实验部分

网络攻防技术框架

网络攻击技术的主要内容包括物理与社会工程学、系统安全攻防、网络安全攻防三个部分，分别利用物理缺陷和人性弱点、软件安全漏洞、网络协议安全缺陷进行攻击。

网络攻防的基础技术体系框架



实验环境介绍

01

为什么需要网络攻防实验环境

网络攻防是基础知识和实践技术紧密结合的技术方向。

学习网络攻防技术需要实验环境。

能不能直接用Internet进行网络攻防实验？为什么？

网络攻防实验环境包括哪些组成部分？如何搭建网络攻防实验环境？

实验环境介绍

虚拟化网络攻防环境

01

虚拟化技术能够从有限硬件设备中虚拟出额外的硬件资源，并支持在这些虚拟硬件设备上构建完整的虚拟机系统，此外还提供方便的虚拟机控制功能。利用虚拟化技术可构建功能丰富、易于部署和管理的网络攻防实验环境。

实验环境介绍

01

虚拟化网络攻防环境

对于网络攻防实验来说，实验所需的硬件资源相对集中，并且经常需要根据实验目标的变化而频繁的对实验环境中的网络拓扑、实验主机操作系统、主机上安装的各类系统程序和应用程序等进行重新安装和配置，因此，攻防仿真环境采用服务器虚拟化技术构建，通过虚拟化场景与实际网络安全设备相结合的方式，为用户提供高度接近实际情况的实验环境。目前，服务器虚拟化软件主要有 VMware、Xen、Hyper-V、KVM 等。

实验环境介绍

虚拟化网络攻防环境

01

VMware Workstation是一款功能强大的桌面虚拟计算机软件，用户可在单一的桌面上同时运行不同的操作系统，可在一部实体机器上模拟完整的网络环境、构建支撑网络攻防实验环境的虚拟化平台。利用VMware 虚拟机软件虚拟出多台相互隔离的虚拟主机，并通过虚拟机管理平台对这些虚拟主机进行集中管理。

实验环境介绍

虚拟化网络攻防环境动手实践

01

- 下载并安装VMware Workstation软件
- 查看VMware 的虚拟网卡和虚拟网络设置
- 安装Windows 虚拟机镜像和Kali linux虚拟机镜像

实验环境介绍

01

虚拟化网络攻防环境动手实践

虚拟化网络攻防实验环境组成部分

虚拟机镜像名称	虚拟机镜像类型	基本操作系统	注意事项和思考
Windows 虚拟机	Windows 靶机	Windows 7	未装ms17-010补丁，445端口打开。 思考：防火墙开启和关闭对实验有什么影响？原因是什么？
Kali linux 虚拟机	Linux 攻击机	Kali linux	了解CVE、渗透测试和Kali Linux

渗透测试与Kali Linux

02 Kali Linux

CVE

Common Vulnerabilities & Exposures，即通用漏洞披露，网址http://cve.mitre.org。国际著名的安全漏洞库，也是对已知漏洞和安全缺陷的标准化名称的列表，它是一个由企业界、政府界和学术界综合参与的国际性组织，采取一种非盈利的组织形式，其使命是为了能更加快速而有效地鉴别、发现和修复软件产品的安全漏洞。

渗透测试与Kali Linux

02 Kali Linux

CVE

好比一个字典表，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称。使用一个共同的名字，可以帮助用户在各自独立的各种漏洞数据库中和漏洞评估工具中共享数据，虽然这些工具很难整合在一起。这样就使得CVE成为了安全信息共享的“关键字”。比如在一个漏洞报告中指明的一个漏洞，如果有CVE名称，你就可以快速地在任何其它CVE兼容的数据库中找到相应修补的信息，解决安全问题。

渗透测试与Kali Linux

02 Kali Linux

渗透测试

是通过模拟恶意黑客的攻击技术与方法，挫败目标系统的安全防护措施并获得控制访问权的安全测试方法，以达到评估计算机网络系统安全性的目的。这个过程包括对系统的任何弱点、技术缺陷或漏洞的主动分析。网络渗透测试主要依据CVE已经发现的安全漏洞，模拟入侵者的攻击方法对网站应用、服务器系统和网络设备进行非破坏性的攻击测试。

渗透测试与Kali Linux

02 Kali Linux

Kali Linux

渗透测试的工具种类繁多，涉及广泛；安装这些工具是一个浩大的工程。有人将所有工具都预装在一个Linux系统中，其中最典型的就是Kali Linux。

Kali Linux是非常强大的操作系统，预装了大量能够摧毁计算机、网络基础设施的工具，如果使用不当或者不道德，会导致犯罪行为或者触犯法律。

实验环境搭建

虚拟化网络攻防环境动手实践

- 下载并安装VMware Workstation软件
- 查看VMware 的虚拟网卡和虚拟网络设置
- 安装Windows 虚拟机镜像和Kali linux虚拟机镜像

虚拟化网络攻防实验环境组成部分

虚拟机镜像名称	虚拟机镜像类型	基本操作系统	注意事项和思考
Windows 虚拟机	Windows靶机	Windows 7	未装ms17-010补丁，445端口打开。 思考：防火墙开启和关闭对实验有什么影响？原因是什么？
Kali linux虚拟机	Linux攻击机	Kali linux	了解CVE、渗透测试、Kali linux

实验

漏洞利用

02

02

04

06

知识点与要求

通过本部分学习和实践：

1）掌握Windows网络服务远程渗透攻击基本理论知识；

2）掌握Windows漏洞及漏洞利用方法原理；

3）掌握Windows网络服务远程渗透攻击防范措施；

4）了解渗透测试软件Metasploit并掌握操作使用Metasploit进行Windows远程渗透攻击的方法。

漏洞和漏洞利用

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

漏洞利用是指用户从目标系统中找到容易攻击的漏洞，然后利用漏洞获得权限。

Windows系统的安全漏洞生命周期

系统安全的本质核心在于安全漏洞、渗透攻击及安全检测防御机制之间的攻防博弈与竞赛，安全漏洞从发现、被渗透利用、被大规模扩展并用于恶意代码，以及被修补从而消亡，构成了系统安全攻防中的一个个生命轮回，而黑客们在这些看似一成不变的安全漏洞生命周期中，却不断进行技术突破与创新，推动供给与防御技术的不断更新与发展。

WannaCry勒索病毒

病毒指编制者在计算机程序中插入的破坏计算机功能或者破坏数据、影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。2017年5月爆发的WannaCry病毒，是一种蠕虫式勒索病毒。不法分子利用危险漏洞MS17-010 “永恒之蓝”（Windows操作系统445端口存在过的漏洞）进行网络端口扫描攻击，目标机器被成功攻陷后会从攻击机下载WannaCry病毒进行感染，并作为攻击机再次扫描互联网和局域网其他机器，形成蠕虫感染，大范围超快速扩散。至少150个国家、30万名用户中招，造成损失达80亿美元，已经严重影响到金融、能源、医疗等众多行业。

针对特定目标的渗透测试攻击过程

在互联网用户和普通用户所面临的安全威胁中，绝大部分是由于未能及时修补已公开披露的安全漏洞所导致的渗透攻击和恶意代码传播。

针对一个特定的主机系统目标，典型的渗透测试攻击过程包括漏洞扫描测试、查找针对发现漏洞的渗透代码、实施渗透测试这几个环节。

Metasploit

- Metasploit渗透测试软件是附带数百个已知软件漏洞的专业级漏洞检测和攻击工具，通过它可以很容易地获取、开发并对计算机软件漏洞实施攻击，也可以帮助专业安全人士识别安全性问题、验证漏洞缓解措施。
- Metasploit软件采用开发框架和模块组件的可扩展模型，模块组件是真正实施渗透攻击的代码，比如利用安全漏洞的Exploits模块、进行扫描和查看等其他辅助任务的Auxiliary模块等。
- Metasploit软件提供四种不同的用户交互接口，其中MSF交互终端（MSFCONSOLE）比较常用。MSFCONSOLE可获得用户连接到主机的信息，从而利用漏洞，使得用户能启动渗透攻击目标系统。

MSFCONSOLE 常用命令

- search：搜索一个特定模块
- use：选择使用特定的模块
- run：启动一个非渗透测试模块
- exploit：实施渗透攻击
- set：配置各种类型 模块中的详细参数
- quit/exit：退出终端
- show：查看每种类型模块的详细配置参数

MSFCONSOLE漏洞利用操作步骤

- 启动MSFCONSOLE，执行命令：root@Kalix64:~# msfconsole。输出的信息出现msf>提示符，表示登录成功，可在该命令行运行其他任何命令。
- 搜索漏洞，得到相应扫描模块和渗透代码，使用该模块。
- 设置靶机IP地址，执行扫描，查看靶机是否存在漏洞。
- 若靶机存在漏洞，使用该渗透模块对靶机进行渗透。
- 查看可设置的选项，确认漏洞对应的端口是否可设置。
- 设置靶机的IP地址，并执行渗透攻击，拿到靶机windows系统的使用权。

网络空间安全认知实习

实验报告

就以下其中一个方向展开思考、探索、实验，记录学习的思考过程和收获，解决问题的过程、方法和收获等，形成报告。

- 实验内容一，独立完成，永恒之蓝漏洞利用实验
- 实验内容二，独立完成，技术讲座安排实验

实验内容一

操作使用Metasploit：

1）对Windows靶机上的MS17-010漏洞进行远程渗透攻击，获得目标主机的访问权；

2）了解计算机编码方式，操作修改靶机的编码方式；

3）操作实现对靶机进行屏幕监控、键盘监控、新增用户、重启。

4）（提高部分，选做）编写脚本实现ssh爆破。可使用paramiko、pexpect、pxssh等python模块进行编写。但在ssh服务端将配置加密方式为非常用加密方式3des-cbc，端口为9981端口。

漏洞利用

实验报告

01

02

04

06

独立完成实验内容和实验报告：

独立完成实验报告，根据自己的理解和实验经过，详细说明实验过程（文字加截图）、遇到的问题、以及解决问题的过程、方法和收获等。

实验内容二

10

技术讲座后通知

02

04

06

实践实习部分

实践内容

05

1-5人共同完成实践内容，独立完成实践报告：

- 曾参加一次网安相关的专业竞赛，介绍竞赛、本人的任务和成长、竞赛收获。
- 曾参加、或者正在参加、或者即将参加创新创业活动，包括雏雁计划或者大创，介绍项目背景、设计、实现应用情况、本人任务和收获。（可参考雏燕计划立项申请书格式）
- 其他专业相关的实践或者实习经历。

THANK

感谢

THANK YOU ~