ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.18, No.19, July 2022
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

网络安全学习策略与职业规划的探讨

刘一廷[1],郑立琴[2]

(1.西安邮电大学 网络空间安全学院,陕西 西安 710100;2.西南科技大学 环境与资源学院,四川 绵阳 621010)

摘要:随着国内社会经济快速发展,计算机技术和网络技术行业获得新的发展空间。网络环境安全已经是社会发展的重要保证。个人信息与商业信息、甚至是国家敏感信息与机密等,必然招致来自全球各行各业的攻击(如信息盗取、信息泄密、数据修改、数据破坏及病毒入侵等),引发网络安全人才紧缺。基于此,从计算机网络安全的基本知识着手,分析各网络安全岗位的特点与其所需的特质,对专业课理论知识和实践路线作分类与梳理,分析总结出指导初学者科学合理学习的方法,同时提出学习规划与发展的方向性建议,就网络安全的学习策略与职业规划的关联性进行简要梳理探讨。

关键词:网络安全;信息对抗;课程路线;学习方法;职业规划

中图分类号:TP393 文献标识码:A

文章编号:1009-3044(2022)19-0033-04

开放科学(资源服务)标识码(OSID):

DOI:10.14004/j.cnki.ckt.2022.1316

1 引言

随着《网安法》的落地,越来越多的大众全面深刻认识了网络空间安全,对网络空间安全的学习亦逐渐系统化。

当今计算机技术和网络技术高速发展,人们对网络空间安全问题更加重视与关注,侵害网络安全的因素很多,如各种恶意软件(病毒和木马)。迫使网络安全技术得以快速提升与发展,网络安全人才需求大幅提高。

2 网络空间安全学科课程,社会对人才需求,专业特色及要求情况

2.1 学科课程知识点要求及社会对人才需求状况

网络空间安全学院的网络安全与信息对抗学生是电子信息通信计算类人才,国际化企业对此类人才素质最基本的要求是有过硬的专业知识技能和出色的语言能力。许多进入华为、中兴等有海外市场的电子信息类毕业生,不管是从事研发、测试还是从事产品服务,都需要掌握扎实的专业知识与技能,与海外本土员工的交流更离不开出色的语言能力[1],而在网络空间安全领域需具有坚实的网络信息的获取、入侵检测与应急响应、渗透测试、处理、防御及进攻等方面的基础知识理论和工程实战综合技术能力,才能成为政府、公安、部队、情报及企业等部门急需的高素质网络空间安全工程应用型人才。当代社会需要理论扎实,动手实践能力强的大学生。

因此网络空间安全学院本科生主干学科与课程较多:如网络空间安全、计算机科学与技术、网络空间安全导论、网络攻防技术、高级语言与程序设计、计算机网络、数据结构与算法、Python语言程序设计、大数据技术及应用、操作系统、安全数据库、密码学基础、网络安全编程、网络安全法、移动终端安全、物联网安全、恶意代码检测技术、Web安全实践及渗透测试实践等,以及电子信息工程与通信工程、数字电路与逻辑设计、电子科学与技术、数理基础课程、微机原理与接口技术、电路分析基础、模拟电子技术基础、信号与系统、数字信号处理、通信原理、通信对抗原理、嵌入式系统及安全、软件无线电、FPGA设计、DSP设计、网络攻防技术扩频通信及计算机病毒检测等。

上述科目多知识点繁杂,外界对此新学科与行业不甚了解,基于此,给刚踏入校园的学子进行学习策略梳理,学生可在整体认知后,进一步确认后续专业科目的学习方向及适合自己的人生职业规划,来扩展学习领域。

计算机网络空间安全,从消费者的视角分析会着重关注用户的敏感信息与公司商业信息,或技术信息在网络上的安全,避免被窃取、篡改及伪造等;从网络供应商的角度分析,除在网络传输中信息防护安全外,还注重突发的自然灾害、军事打击、黑客攻击等对网络设备硬件的破坏,以及在网络传输中出现异常时怎样快速恢复网络传输通信的连续性。

本质上计算机网络安全是指:利用计算机网络安全控制及技术安全保护[2],对计算机硬件保护、数据的保密性、完整性、可使用性、不因偶然和恶意的因素而受到破坏、篡改、伪造及泄漏等。而网络安全亦是确保网络系统连续可靠地正常运行及网络服务正常有序。安全的核心是保障信息资产的完整性、可用性与保密性,大致分为网络安全、终端安全及应用安全等。信息系统安全划分为4个层次:设备安全、数据安全、内容安全及行为安全等。

2018年全国网络信息安全人才缺口已大于70万,国内3000所高校仅120所开设相关专业,年培养1万~2万人,加上10~20家社会机构,全国每年相关人才输送量约为3万,距离70万缺口差距达95%。此外,2020年网络安全人才需求量直线增长,预计达140万。2021年上半年,网络安全产业人才需求总量较去年增长39.87%,安全研究、应急响应等岗位需求量很

收稿日期:2022-03-26

作者简介:刘一廷(2001—),男,湖南湘潭人,学士,主要研究方向为网络空间安全与信息对抗技术;郑立琴(1968—),女,贵州遵义人,副教授,学士,主要研究方向为信息用户教育、信息技术教育、双创教育。

高，以下两组数据充分显现需求状况，行业高薪的背后，是巨大的人才缺口。

图1显示网络安全人员就业薪资分布情况。

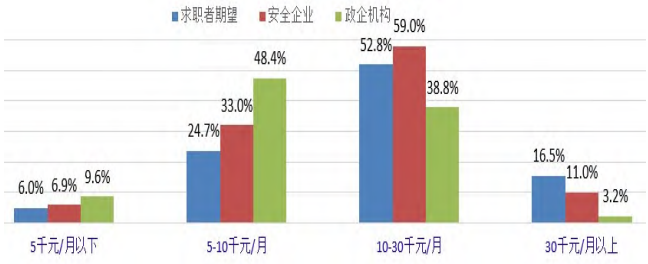

图1　网络安全人才与用人单位的薪资水平对比

工业和信息化部人才交流中心和网络安全产业发展中心发布了《2021网络安全产业人才发展报告》，显示网络安全行业的人才短缺分布方向：

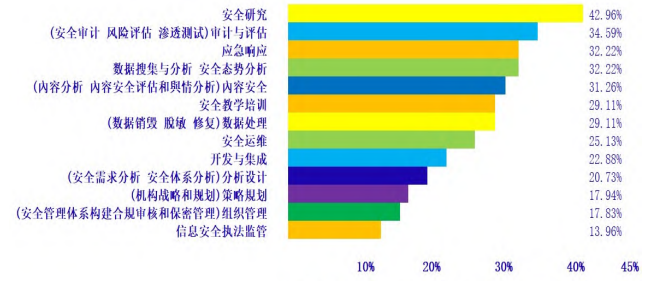

图2　2021年网络安全人才短缺岗位分布[3]

2.2 网络安全专业各门类的特点及要求的技能需求分类

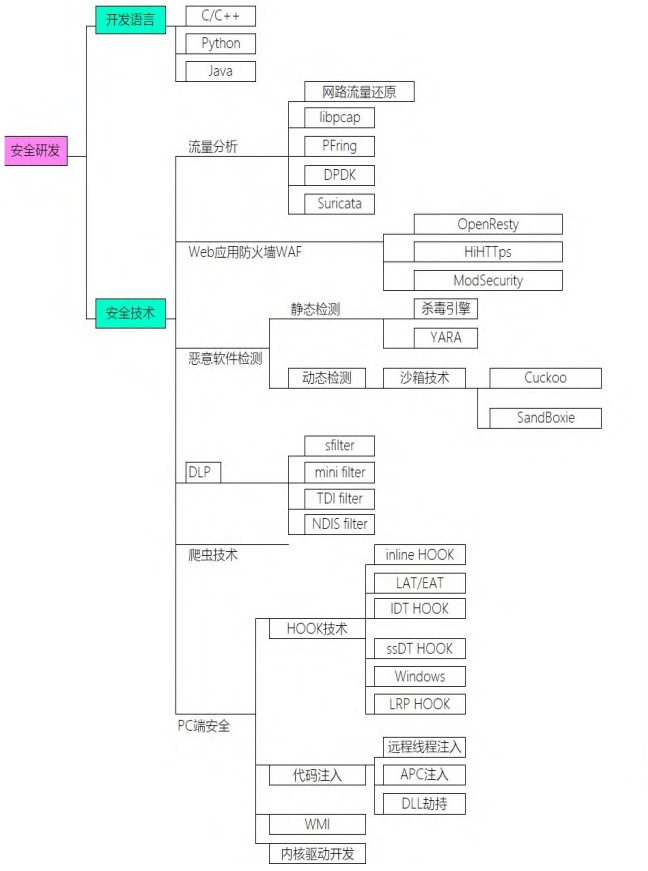

图3　安全研发技术学习思维导图[5]

目前互联网、通信、新能源、房地产、金融证券及电子技术等行业迫切需要网络安全人才，因为网络安全的重要性，每一行业同时又催生出不同的需求方向，初学者可以根据自身的知识结构、能力特点及兴趣来选择学习工作方向。

网络安全岗位有三大类可选：A研发类：网络安全研究工程师、网络安全设备开发及攻防安全研究员等。B安服类：安全服务工程师、渗透测试工程师、反病毒工程师、代码审计工程师、风险评估分析师、网络安全建设工程师及等保测评师等。C运维类：安全运维工程师、技术服务工程师等。

按技术门类分，网络安全工作岗位有以下三类：A安全研发，B安全研究：二进制方向，C安全研究：网络渗透方向[4]。

网络安全有不同的技术门类，学子们可依据各自的主攻的方向，进行系统性学习，并结合实战学习网络安全。注重老师教授的基础学科与专业理论原理外，更重要的是还要自学实用的技巧性知识，把理论知识和实践贯通起来，通过大量的实战累积提升能力。下面按门类方向展开学习策略梳理。

安全研发方向：开发安全产品(如软件+工具)用来检测搜寻发现、防御、攻击终端硬件(手机、桌面PC、NB及网络设施等)及网络方向等[4]，相对安全研究二进制网络渗透岗位，安全技术较浅更容易学成，分为防护(数据库网关等)安全产品开发和攻击(杀毒软件等)的安全工具开发。可借鉴如图3总结的思维导图来快速地学好安全研发技术。

安全研究二进制安全方向：研究二进制安全是安全技术研究领域两方向中的分支。二进制安全需要漏洞挖掘分析、逆向安全开发及木马病毒(或统称为恶意程序)分析等工作[4]，需要Linux内核分析、调试与反调试、病毒识别处理等网络安全技术，如能掌握由Ring0-Ring3进入Ring-1层次那是更上一层楼。因为日常工作是分析处理二进制的数据，技术难度系数和复杂程度更大，要求勤奋努力和更多天分才能应对挑战。可借鉴图4的导图更有效地学习。

安全研究网络渗透方向：容易入门，掌握了部分基本技术，借用业界现有的工具可以攻击手机、PC、NB、网站、服务器及内网等[4]。

初学者要先掌握最简单的基本知识，再去深造完善：掌握HTTP协议的工作机制→Web技术(含前、后端如何协同工作/浏览器如何工作/服务器如何处理一个HTTP请求/一个网站如何搭建等)→再学习使用一些Web漏洞扫描工具，学习网站漏洞的概念，建立“安全”概念。

网络渗透的高阶是成长为一个安全顶尖专家，在广度上提升深度，深度上拓展广度走实，专业上有更深的造诣，拓展自己的知识：从网络硬件(网卡、中继站、集线器、桥连接器、交换机及路由器等)、网络TCP/IP协议、Web服务(Web、E-mail、file及database等)、至OS及攻击方法手段等都需要懂得，涉猎比如二进制漏洞攻击、逆向工程、木马技术、内核安全、移动安全及侧信道攻击等，成为多面手的IT技术专家。初学者可参照下述汇总的思维线路进行。

3 掌握专业课程的理论与实践相结合学习路线及学习方法

3.1 进行专业课程理论与实践相结合的学习

第一步：计算机基础理论的掌握

五大课程：计算机网络、算法与数据结构、计算机组成原

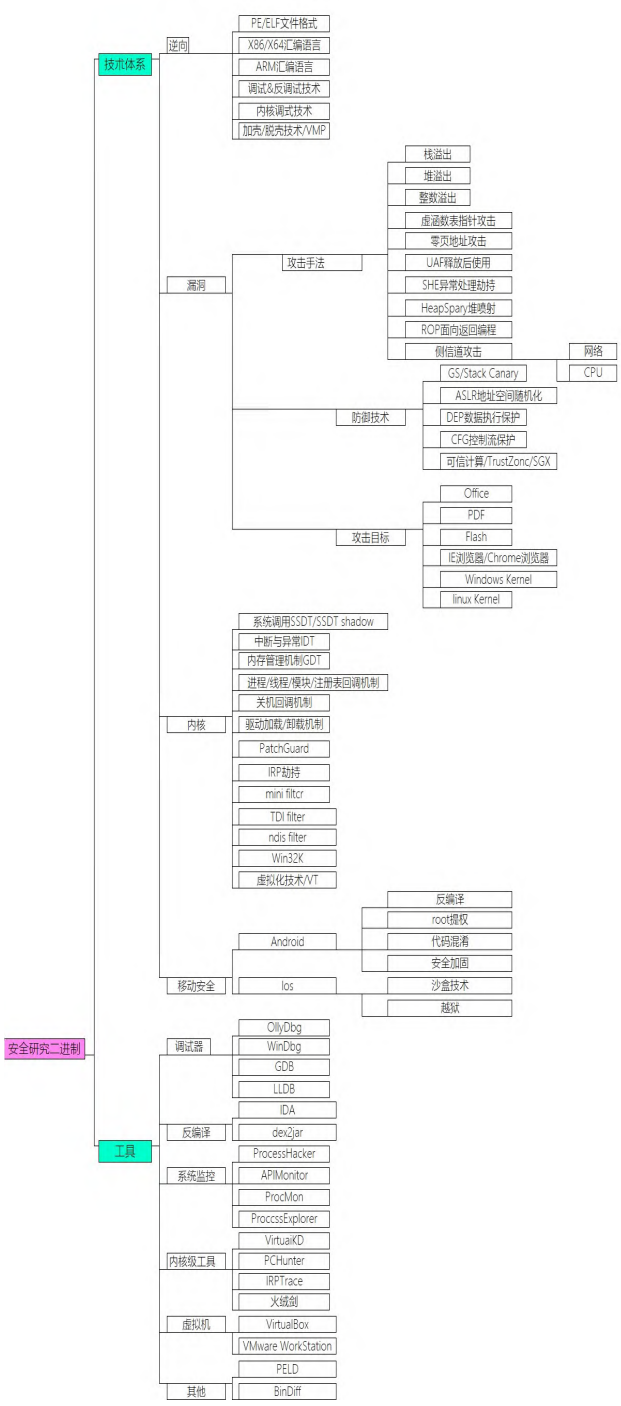

图4　安全研究二进制安全技术学习思维导图[5]

理、操作系统及数据库等。

第二步：编程能力培养

世界上有很多种编程语言，当前排前10名的编程语言是JavaScript、Python、Java、PHP、HTML、C#、SQL、CSS、C++和R。每种语言有不同的优势，众多编程语言其实是非常相似的。虽然编程语言语法不同，外观不同，甚至功能完全不同，然而核心层面的相似程度高。几乎所有的编程语言都会有分支、循环、调用方法或过程以及代码组织方式等。有的甚至相似到精通一门语言后自然会了另一门语言。

网络安全行业最好都能掌握以下三类语言：

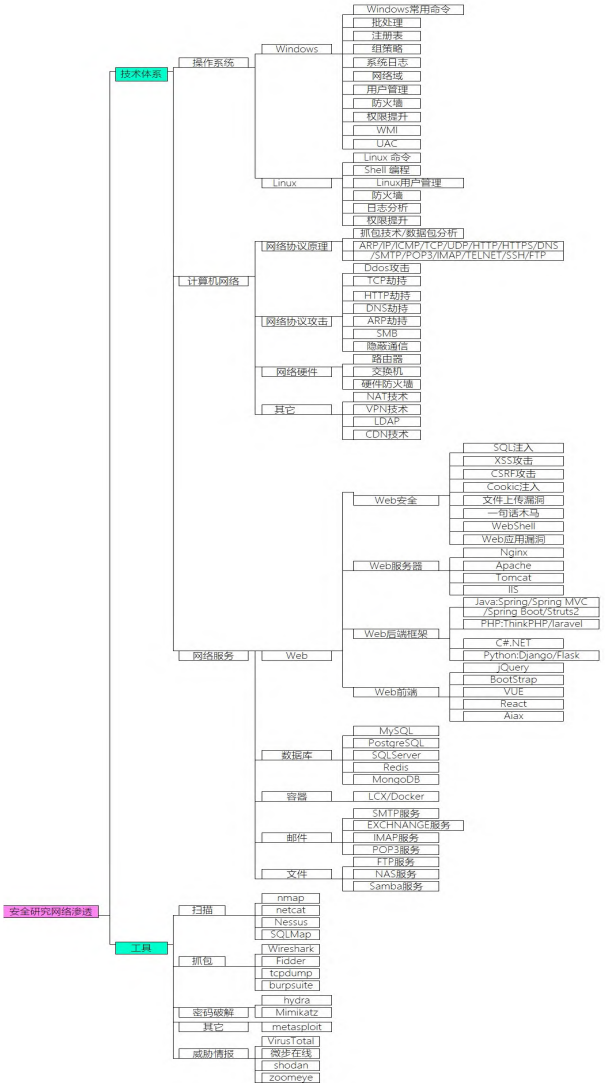

图5　安全研究网络渗透技术学习思维导图[5]

Shell脚本：与Windows/Dos下的批处理相似，它使用了Linux/Unix下的命令，比Windows下的批处理更强大，效率更高于用其他编程程序编辑的程序。只需学会基本的Linux命令，学会编简易Shell脚本，做一些简易的编程。

C语言（C++可选）：是现代编程语言的元祖，是面向过程的，广泛应用于底层开发，抽象化的通用语言。C语言能以简易的方式进行编译和处理低级存储器，有跨平台的特性。掌握C编程语言，结合学习数据结构、数据库及操作系统等能更容易帮助初学者非常透彻领会内存、算法及操作系统等IT知识。

Python程序设计语言：语言简单灵活，有庞大的外部库，使用极方便，具有较高的开发效率；在网络运维中借助其他模块，提升运维的效率；可提供多种开发框架，可用Python代码编写运维脚本，提升网络运维的自动化。Python具备灵活、简单、强大功能及满足脚本处理的优势等，因此被广泛应用到运维领域中，在网络运维过程中使用Python，能够使网络运维工作效率得到提高[6]。

C语言帮助学生们理解底层知识机制，Python能提升编程技能，且可大数据分析、网络蜘蛛、自动化运维、人工智能及识别漏洞并发现如何解决该问题等，在网络安全职业生涯中极具有优势。

第三步:安全技术基础实践

掌握上述的基础理论知识,进一步接触各方面的技术技能,对网络安全技术例如:物理安全分析技术、网络结构安全分析技术、系统安全分析技术、管理安全分析技术,及其他的安全服务和安全机制策略有基本的认知[7]。

掌控网络信息安全技术重要的一点是要多实践且不断挑战与探索,如:网络TCP/IP协议攻击、网站服务器攻击、Web页面安全、浏览器网络安全和浏览器系统安全、漏洞bug攻击、逆向破解(汇编指令→脱壳→修复程序→破解(算法))及防攻工具开发都去实战摸索等,掌握各技术的基本流程步骤与应用,在实践中获得成就感的同时找到自己的优势、兴趣和未来发展方向。

初始实践是要从最基本的接网线、路由、网上截包及扫描漏洞等开始,再到高级一点的搭服务器,制定安全策略,分级权限等都需要摸索。

第四步:分方向发展

在安全技术基础实践中了解并判定自己的特长、优势及兴趣方向(安全产品软件工具开发/二进制安全研究方向涉及操作系统内核分析、调试与反调试、反病毒等技术/网络渗透方向)等,确认了发展方向并拥有了一定知识基础后,可有目的地去各种讲座、社群、网站及技术论坛等猎取技能、知识及技巧等,了解行业最新知识与发展趋势。借鉴学习前人经验至关重要,提高学习效率亦是非常明智的选择。创造条件多阅读相关领域的英文文献,了解前沿知识并寻找适合自己的方向。专注自己的目标领域并在此方向上不断提升自己,将理论和技能进行应用和实践,将成为某一个领域的行家。

3.2 学习方法

阅读是课程学习核心根本的方式。首先是对安全技术的理论基础作系统性全面的了解。

其次是明确学习网络安全的目标方向,以目标为导向按目标重点课程知识合理分配时间与精力:每一门都是大学学习科目,其实用到安全上的只是一部分,毕竟人的精力是有限的。如果在暂时用得不多的课程内容上花费了大量时间,学习效率必然低下,抓不到重点,甚至会打击信心,导致实现目标的时间大大拉长。

网络信息安全学习特别需要注重实践,做技术需要非常多的实践经验,动手实践是学习成效的关键。

安全研发开发方向实践拓展训练实施:需要多练习网络安全系统码,分析前辈的优秀开源代码能学习到实现强大特定模块化的功能、严密的逻辑、提高写代码水平、提升抽象思维能力,阅读代码时粗略浏览它的运作流程整体性与模块之间协作,再关注具体实现模块化细节。

安全研究二进制方向实践拓展训练实施:首先,分析样本,其过程用查壳工具、监测工具及调试工具通过静态分析信息和动态分析信息完成等。其次,实践编写EXP(漏洞利用)其漏洞挖掘,一般先用通用应用程序(挖掘)→发现漏洞(调试)→POC/EXP(编写),POC/EXP是在漏洞挖掘后的最后一个环节,与此同时可挑战使用IDA、GDB逆向调试工具等。

安全研究网络渗透方向实践拓展训练实施:可用测试扫描器找免费开源的用于渗透测试的网站练手(掌握各种漏洞的检测、漏洞利用方法及渗透步骤等)等,打夺旗赛,多参与一些网络安全比赛,接近实战的环境下锻炼动手能力,培养自己的科技实践能力和创新意识。

最后强调下网络安全必备的5个基础的知识,如图6。

图6 基础知识图

4 结束语

根据安全规范、应用场景及技术实现等,网络安全行业可以有很多分类,简单分为网络安全、Web安全、云安全、移动安全(手机等)、桌面安全(电脑)、主机安全(服务器)、工控安全、无线安全及数据安全等不同领域。

岗位划分成:网络安全运维、渗透测试、Web安全、逆向、安全开发、代码审计及安全服务类岗位等。不同的岗位需要具备不同的技术技能。编程能力较好可以从事Web安全、逆向、代码审计及安全开发等岗位。不喜爱代码编程的人员适合从事安全运维、渗透测试、Web安全及网络安全架构等工作。

在学校学习掌握理论基础只是入行起点,要正式踏入网络安全行业需要在大学及后阶段花更多精力去努力学习更深更专业的技能与行业知识,参加相关的比赛来丰富实战技能。必要时亦可参加渗透之类培训。自身能力提升是最重要的一环,提升的途径与方式:数据显示,绝大多数人员都会通过职业培训来提升增强自己的实战能力,占比高达73.89%,其次是工作单位内部培训(49.12%)和自学(46.46%)[8]。

不管学什么技术,选择好后要不遗余力地走下去,坚持下去,细化目标,制定具体的学习内容,才能学有所成,走上技术道路。

参考文献:

[1] 赵波,张志华.创新型国际化人才培养模式初探——以电子信息类高校为视角[J].黑龙江高教研究,2010,28(7):138-140.
[2] 林建红.军事网络信息安全系统的研究与设计[D].长沙:中南大学,2004.
[3] 付京波,色云峰,李学林,等.2021网络安全产业人才发展报告[R].北京:工业和信息化部人才交流中心,网络安全产业发展中心,2021.
[4] 小风.网络安全有哪些职业方向?[EB/OL].(2020-09-09)[2021-10-18].https://www.xf1433.com/4377.html.
[5] 代码熬夜敲.网络安全的学习方向和路线是怎么样的?[EB/OL].(2021-09-29)[2021-10-18].https://www.bilibili.com/read/cv13383009.
[6] 宋焱宏.Python在网络运维中的应用[J].电脑知识与技术,2018,14(19):33-35.
[7] 周刚伟,苏凯.对网络安全技术的浅析[J].数字技术与应用,2009(10):196-197.
[8] 中国信息安全评测中心,杭州安恒信息技术股份有限公司,猎聘网.2018网络安全人才发展白皮书[R].“网络安全人才培养”成都分论坛:中国信息安全测评中心,安恒信息,猎聘网,2018.

【通联编辑:谢媛媛】