网络空间安全工程技术人才培养体系指南

（版本**1.0**）

中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟

二〇一九年一月

中国网络空间安全人才教育联盟

网络空间安全工程技术人才培养体系指南

（版本**1.0**）

中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟

二〇一九年一月

© 2019 中国网络空间安全人才教育联盟

联合发布

广州大学

湖南会览网安教育有限公司

湖南合天智汇信息技术有限公司

360 企业安全集团

腾讯安全

版权声明

本指南版权属于中国网络空间安全人才教育联盟、广州大学、湖南会览网安教育有限公司、湖南合天智汇信息技术有限公司、360 企业安全集团、腾讯安全共同所有，受法律保护。转载、摘编或利用其他方式使用白皮书文字或者观点，应注明“来源：中国网络空间安全人才教育联盟”，并书面知会联盟秘书处。违反上述声明者，本指南权利者保留追究其法律责任的权利。

免责声明

本指南仅供参考。对于本文档中的信息，联盟及联合发布单位不作明示、默示保证。本指南基于现状编写。在指南中的信息和意见，均可能会改变，不另行通知。您需自行承担使用风险。

词汇说明

文中“网安人才”特指网络空间安全工程技术人才。

第一次印刷：2019 年 1 月 9 日

引言

网络空间作为人类社会生存和发展的新空间，成为了“陆、海、空、天、网”中的第五维新疆域，党和国家领导人高度重视网络空间安全问题，习近平总书记亲自担任中共中央网络安全和信息化委员会主任，就网络空间安全问题多次作出重要指示。网络空间安全问题进入到国家战略强势介入的全新阶段。

当前我国网安人才需求缺口巨大，人才需求增速不断加快，对有实践经历、实战能力的网络空间安全工程技术人才（以下及正文简称“网安人才”）有特殊需求。针对这一现实情况和特殊需求，本指南提出了我国网安人才培养框架，并就框架中网安人才层次化培养体系、知识技能体系、认证体系等主体部分，进行了论述。首先，针对院校培养体这一主要人才渠道，阐述了如何补充强化其实践化教学和实战化能力培养环节；其次，从从业人员业务标签的角度，参考学科专业体系，梳理并提出了网安人才知识技能体系，突出以“人”为核心、以“知识技能”为业务内容，为工程技术人才培养和考核认证提供参考；最后，在分析国外发达国家网安人才认证体系建设的基础上，结合我国实情和人才渠道现实，提出我国网安人才认证体系建设思路。

本指南主要分四章：第一章论述网络空间安全及其威胁，网安人才的特殊性，并据此提出网安人才培养框架；第二章叙述院校层次化培养体系下，分层、分类的建设目标和培养方式；第三章阐述网安人才知识技能体系；第四章分析国外网安人才认证机制，并探讨如何建立我国的网安人才认证体系。

本指南由中国网络空间安全人才教育联盟联合广州大学、会览

 ©2019 中国网络空间安全人才教育联盟

网安、合天智汇、360企业安全、腾讯安全共同发布。

本指南编写过程中，参考了国家机关、中国工程院等机构研究发布的人才培养数据和观点，得到了（字母序）廖鹏（南瑞集团）、刘宝旭（中科院信工所）、刘建伟（北京航空航天大学）、刘奇旭（中科院信工所）、刘潮歌（中科院信工所）、薛继东（丁牛科技）、杨珉（复旦大学）、杨卿（360集团）等行业专家的帮助指导，在此一并表示感谢。

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

目 录

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

第一章 网安人才培养框架

1.1 网络空间安全及其风险

网络空间是构建在信息通信技术基础设施之上的人造空间，用以支撑人们在该空间中开展各类与信息通信技术相关的活动。信息通信技术基础设施包括互联网、各种通信系统与电信网、各种传播系统与广电网、各种计算机系统和各类关键工业设施中的嵌入式处理器和控制器。信息通信技术活动包括人们对数据的创造、保存、改变、传输、使用、展示等操作过程，及其所带来的对政治、经济、文化、社会、军事等方面的影响。

网络空间安全涉及在网络空间中电磁设备、信息通信系统、运行数据、系统应用中所存在的安全问题，既设备层安全、系统层安全、数据层安全和应用层安全。其中，设备层安全需应对网络空间中信息系统设备所面对的安全问题，包括物理安全、环境安全、设备安全等；系统层安全需应对网络空间中信息系统自身所面对的安全问题，包括网络安全、软件安全等；数据层安全需应对在网络空间中处理数据的同时所带来的安全问题，包括数据安全、身份安全、隐私保护等；应用层安全需应对在信息应用的过程中所形成的安全问题，包括内容安全、应用安全等。

网络空间安全风险包括保护信息通信技术系统及其所承载的数据免受攻击，其属于虚拟世界自身安全风险；也要防止和应对因滥用这些信息通信技术系统而波及到政治安全、经济安全、文化安全、社会安全、国防安全等情况的发生，其属于物理世界衍生安全风险。

针对上述网络空间安全风险，需要采取法律、管理、技术、自律、教育等综合手段来进行应对，确保信息通信技术系统及其所承

 ©2019 中国网络空间安全人才教育联盟

载数据的机密性、可鉴别性（包括完整性、真实性、不可抵赖性）、可用性、可控性。

1.2 网安人才的特殊性

1.安全保障强技能

物理世界中的安保人员追求身强力壮，拼的是体力，物理世界的军人首先要求过硬的身体素质。网络空间的安保人员追求 IT 技能高超，拼的是智力，网络空间的军人首先要求娴熟的网络技术。

这种断崖式的安保人才门槛，导致了网络安全人员的紧缺。

2.攻易防难非对称

物理世界的攻击者段具有鲜明的局域特点，单点攻击只引发局部防范，区域戒备就可以解决问题。网络空间攻击者可以扫描全球，单点攻击会引发全球防范，防御人员的需求规模与系统规模成比例关系，攻击者则与规模无关。

网络攻击者的培养相对简单，重在实践；网络防御者的培养过程复杂，需要理论与实践结合。

3.触及法律高风险

网络攻击技能的培养如同武术技能的传授，受训者的自律程度成为造福人类还是危及社会的分水岭。与武术技能的提高相同，网络攻防的技术能力是建立在不断实践的基础之上，闭门造车无法真正提高实战能力。

如何在不断“挑战高手”的同时避免触及法律红线是难以两全的问题。

4.技能学术弱关联

攻击技能可以通过经验的积累而迅速提高，但防范能力则需要

 ©2019 中国网络空间安全人才教育联盟

深厚的理论积累，尤其是对利用非配置漏洞而发起的攻击的防范，简单的实践不能掌握其要领。

因此，技能型人才不一定依赖学术水平，技能与学术没有直接的强相关性。攻击能力往往呈现实践性，防御人才往往首先呈现学术性，两种人才培养不尽相同。

5.宿主技术后伴生

任何新兴的网络空间技术所对应的安全技术一定是与相应的网络空间技术相伴生的，新兴网络空间安全技术本质上是寄生在新兴宿主网络空间技术之上，不了解所要保护的网络空间技术，就不可能了解相应的网络空间安全技术。

任何新兴网络空间安全技术出现之后，一定会存在相应的安全问题，因此，也一定会伴生出现相应的新型网络空间安全技术。

6.技能水平难鉴别

由于社会上对安全人才需求与供给关系严重失衡，因此存在大量的转行人才。

网络安全技能缺少显式的展现方法，一般机构难以通过简单的方法判断出一名网安人员的技能水平，使得急需网安人才的机构面临两难的境地。

1.3 网安人才培养框架

从网安人才的特殊性和我国网络空间安全的人才需求特点出发，结合国内院校教育、职业培训、自学成才三个网安人才成长主要渠道这一现实，规划设计网安人才培养体系、知识技能体系，以及适应国家发展战略的统一规范的人才出口评价体系。

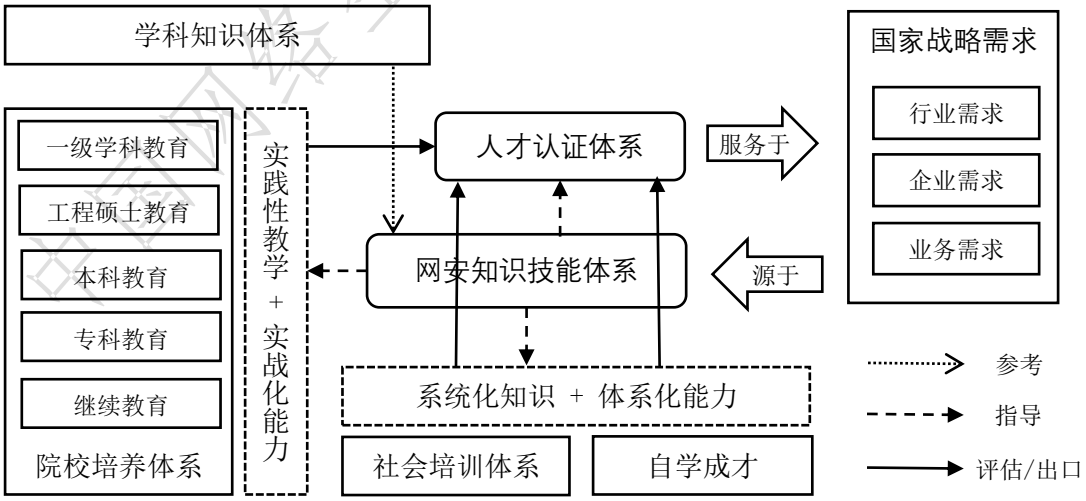
院校培养体系，组织形式上包括普通大学、高职高专、民办高

中国网络空间安全人才教育联盟

校等以学校为单位组织的网安人才培养形式，内涵上包括其培养目标、课程体系和培养模式等。院校培养体系在人才培养路线上一般具有系统化、理论化和学术化等特点，需着重根据网安人才的特殊性和人才需求特点，结合培养机构人才出口、去向等个性情况，强化层次化、方向化的实践教学和实战能力培养。

网安人才知识技能体系，以行业对从业人员知识、技能、素质等的要求为出发点，面向适应网安人才特殊性和满足国家网安人才需求，参考网络空间安全学科知识体系，以“人”为核心，分方向、系统化地描述了不同专业方向网安人才应掌握的知识技能，是衔接人才培养与行业需求间的纽带，为考核评估人才层次、规范人才出口、规划调整岗位设置等提供技术参考。

网安人才认证体系，作为考核评估网安人才层次、规范人才出口的手段，明确并统一了院校教育、职业培训和自学成才等渠道培养的人才的知识、技能和素质，重点强化院校教育渠道的实践性教学和实战化能力培养、职业培训与自学成才渠道的系统化知识学习和体系化能力培养。



 ©2019 中国网络空间安全人才教育联盟

第二章 网安人才层次化培养体系

2.1 层次化培养必要性

院校教育是我国乃至世界先进国家培养网络空间安全从业者、提供网安人才的主要渠道。院校从继续教育、专科和职业教育，到本科、工程硕士和博士教育，具有先天的层次化培养特征。而网安人才从我国当前人才需求现状、网络空间保障从业者分类和具备知识技能层次看，也应该采用层次化的培养体系。

1.从我国网络空间安全的人才需求来看

- 发展网络空间安全继续教育，为计算机初级使用者、IT 行业非计算机专业人士提供快速培训，大量培养基层人才;
- 发展职业教育，快速培养有一定工具使用技巧的网安人才;
- 适应性的调整或补充本科、工程硕士教育，在理论知识和科研学术的基础上，强化实际技能的培养;
- 重视实践、创新和学术能力兼顾的高层次人才培养;
- 重视既有全局综合能力又有具体技术手段、既有管理能力又有学术能力、既文又理的复合型人才培养。

2.网络空间安全保障的参与者来看

- 计算机系统、网络系统和信息系统安全机制的研制者;
- 攻击计算机系统、网络系统和信息系统的组织者;
- 计算机系统、网络系统和信息系统安全隐患的发现者;
- 计算机系统、网络系统和信息系统安全隐患的修复者;
- 计算机系统、网络系统和信息系统安全性的维护者;

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

- 计算机系统、网络系统和信息系统安全性的管理者;
- 计算机系统、网络系统和信息系统安全隐患的利用者。

3.从知识、技能、方法、工具等的掌握程度和运用方式上看

- 专科人才应能熟练运用、维护工具;
- 本科人才应能准确理解方法及其背后的原理且能熟练运用、维护工具，具有运用所学原理理解甚至提出新方法、研制新工具的潜质;
- 研究生人才应能准确理解方法及其背后的原理且能熟练运用、维护工具，并具有运用所学原理理解、提出新方法、研制新工具的能力。

综上，结合网安人才的特殊性，应在不同层次、根据人才不同出口走向，强化实践教学和实战能力培养，从而为国家和社会造就大量急需的工程技术型网安人才和复合型高端人才。

2.2 继续教育层次

通过 1-3 个月的培养，使得计算机专业人才对网络安全有一个具体的认识，从而可以迅速培养百万网安人才。这类型的人才能够知道什么是攻防并知道怎么将现有技术用于网络攻防。

1.建设目标

- 尽快制定网安人才评价标准，用统一、精准的尺度来衡量网络空间安全从业人员的技能水平;
- 为国家储备网安人才，为适应不同需求培养各个方向的专业人才。例如随着政务云的快速建设，市场急需大量的网络空间安全运维人员，而运维人员短时间内可大批量复制培养，以尽快填补国家网安人才的缺口;

 ©2019 中国网络空间安全人才教育联盟

- 整合国内各领域优秀的网络空间安全管理人才、技术人才和学习资源等，汇聚社会各界的力量，建设国家级大型网安人才培养基地，形成良性的安全人才培养、进修生态体系。

2.培养模式

主要通过线上和线下两种方式进行。

- **线上授课方式**，以多媒体技术为主要手段，通过互联网进行跨时空地域、实时非实时并用的交互式教学；利用虚拟化和云计算技术，提供接近实战场景的技能练习平台，强化实战能力。

- **线下授课方式**，可根据参加培训对象的知识水平、能力等进行统一分组分班的培训，讲师可第一时间处理和解答学员遇到的问题，具有更好的互动性和现场感。

不管是线上还是线下授课，都需要依托网安教学实训平台，以课程内容和学员信息为核心，集知识培训、技能训练、仿真演练、管理考核等功能于一体，提供系统化的、持续的人才培养和伴随式人才服务，满足各行业对网安人才的需求。

2.3 专科层次

经过2年培训可以将初高中生培养成安全技工，熟悉常用攻防工具、操作系统和攻防场景，掌握基本的攻防手段。专科层次人才以掌握攻防手段运用为主，在培养阶段应将科学问题剥离，注重操作技能训练。

1.建设目标

面向各类企事业单位、政府机关，培养具有良好的综合素质和网络空间安全专业理论知识，掌握典型网络安全系统的安装与配置、数据库安全管理、网站安全管理、二进制代码行为分析、灾难应急响应、电子取证分析等专业技术的人才，能够胜任网络安全管理员、

 ©2019 中国网络空间安全人才教育联盟

数字取证分析师、灾备工程师、互联网安全工程师、渗透测试工程师等岗位工作。

2.培养模式

采取“CBET”（能力本位的教育和培训）模式，强化学生实践动手能力培养，实施“教师+企业工程师+岗位认证”三位一体的培养方式和“岗位需求驱动、场景项目牵引、实践技能进阶”的实践型教学模式。

2.4 本科层次

在通识大学教育里培养安全专业人才，需要设计论证特殊的培养方案和特殊的教学大纲。本科层次人才不仅要能够熟练运用攻防工具和手段，还需要懂得举一反三。

1.建设目标

定位于熟练运用安全工具，维护网络信息系统安全基础之上，能够准确理解方法及背后的原理，并具有运用所学原理分析甚至提出和研制新方法、新工具的潜质。

- 知识方面：掌握工科基础数学、计算机与网络基本理论和知识；熟悉软件开发语言、操作系统原理、网络安全等相关知识与工具；了解学科前沿领域发展动态。

- 能力方面：具备一定的计算思维和逻辑思维能力；具备一定的计算机系统分析与设计能力；具备一定的独立思考能力和创新能力及自我学习能力；具备很强的实践操作能力；具备较强的表达和沟通能力。

- 素质方面：具有正确的人生观、世界观、公民意识和法律意识；具有良好的职业道德和团队合作精神；具有较强的工程素养及人文精神；具有健全的人格及较强的抗挫折能力。

 ©2019 中国网络空间安全人才教育联盟

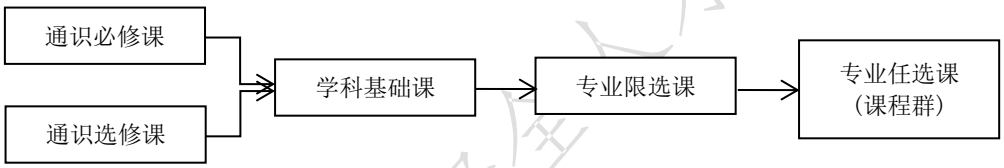
2.培养模式

可以采用“135”培养模式，其中:

“1”是指遵循 1 个人才培养的基本原则，即以“厚基础、强实践、遵法规”的要求作为培养原则;

“3”是指对网安人才培养的三个要求，即要求学生具有扎实的专业理论基础、很强的实践能力、很好的工程技术素养;

“5”是指依照个性化培养的要求，以学生为本，尊重学生的个性差异，设置5个领域特色课程群，适应不同类型安全人才的培养需要，同时也丰富学生对于领域方向课程的选择机会并扩大学生的专业知识面，学生可根据自身情况和兴趣选修。



2.5 工程硕士层次

在通识大学教育的研究生层次培养专业型工程技术人才。与本科层次类似，需要设计论证特殊的培养方案，并突出攻防工具开发和拓展能力，以及运用工具和方法解决复杂工程问题的能力。

1.建设目标

- 掌握马克思主义基本理论，树立正确的世界观和价值观，热爱祖国，遵纪守法，品行端正，学风严谨，具有良好的团结协作意识和积极的进取心;
- 了解网络空间安全学科的基础理论、专业知识和网络空间安全体系结构;
- 熟练运用网络空间安全学科的方法、技术与工具，具有独立

 ©2019 中国网络空间安全人才教育联盟

从事本学科和相关学科领域专业技术工作的能力，可以从事网络空间安全领域的应用研究以及相关设计、开发与管理工作;

- 熟练掌握一门外语，具有良好的写作能力和学术交流能力。

2.培养模式

培养方案设计体现如下原则和特色:

（1）重视政治思想教育和网络空间安全观教育，培养坚定可靠的网安人才;

（2）强化网络攻防训练及演练，夯实学生网络空间安全技能的实操能力；通过竞赛、演练等选拔机制，随时检验培养效果并积极完善方案;

（3）设计灵活的课程体系、选课机制和学分制度，既考虑学生兴趣转变，又兼顾学生知识基础、性格特点，力争个性化培养;

（4）充分利用与安全企业和业务部门的直通培养渠道和资源，紧密面向企业需求，培养适应第一岗位的优秀专业人才;

（5）工程技术研究向网络空间安全大数据分析、物联网及安全、智慧城市及安全、网络攻防对抗与网络靶场等领域聚焦。

2.6 一级学科层次

一级学科层次人才指完成博士阶段理论学习、学术研究和实践训练或获得博士学位的人才，是网络空间安全或相关学科领域具有最高学术、理论与技术创新能力水平的人才。

1.建设目标

网络空间安全学科博士生应深入了解学科的发展现状、趋势和前沿，对相关领域的重要理论、方法与技术有透彻了解和把握，善于发现学科的前沿性问题；在网络空间安全或相关学科领域，用科

 ©2019 中国网络空间安全人才教育联盟

学的方法指导，独立从事高水平的科学研究、理论与技术创新，或开展大型复杂系统的设计、开发与运行管理工作，做出创造性成果。

2.培养模式

一级学科层次人才没有固定的培养模式。需要培养的学生有全面和深厚的理论基础、同时又有高水平的实践动手能力。培养的人才应当掌握网络空间安全领域的深厚的理论、新颖的科学方法和高超的技术，使之具备从事前瞻科学研究与解决网络空间安全复杂系统的设计、开发与运行管理等工作的能力。在培养中要加强理论与实践结合、个性与特色兼顾培养模式，尊重学生的个性差异，采取针对性的特色培养。

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

第三章 网安人才知识技能体系

3.1 体系分类方法

网安人才知识技能分类方法在国际上一直没有公认标准。可参考的相关工作有美国发布的《NICE 网络安全人才框架》、美国国家安全局和国土安全部联合主持成立的国家信息保障/网络防御学术卓越中心（CAE）发布的“基于知识单元的课程体系”、Gartner 近年发布的新兴技术成熟度曲线和信息安全技术列表、国内智联招聘和 360 互联网安全中心联合发布的“2018 网络安全人才市场状况研究报告”等。

鉴于网络空间安全工程技术人才培养的特殊性，在借鉴国内外相关工作的基础上，提出了一种以“网安人才标签”为主维度的分类法及知识技能体系，以满足实战型网安人才培养需求。之所以没有将“网安岗位”作为分类主维度，是因为对每个岗位的理解，因人而异、因用人单位而异、因认证机构而异，存在很大的不确定性。同时，我们注意到一个现象，当问及网安从业人员“做什么方向的工作？”，得到的回答往往既不是自己所在网安岗位，也不是工作所需核心技术，而是从业人员给自己打上的一个标签（如“Web”、“渗透”、“运维”），标签的默认含义也已基本形成共识。

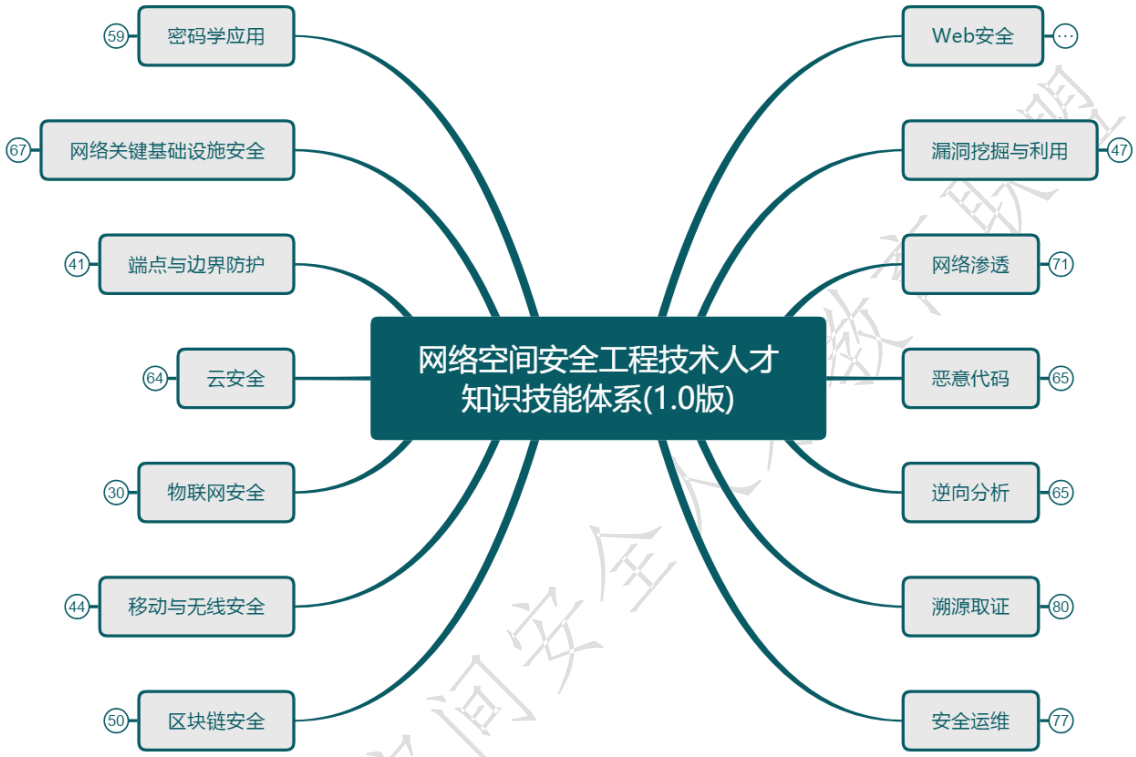
设计一个面向网络空间安全工程技术人才的知识技能体系，为高校授课、网安培训、人才认证、岗位招聘等提供参考依据，是设计本体系的初衷。此外，鉴于面向对象是网安人才，所以，信息安全管理、政策和法律等未列入。

3.2 标签化知识技能体系

本指南将网安人才知识技能体系划分为 14 个子体系（也称为网

 ©2019 中国网络空间安全人才教育联盟

安人才标签或一级节点），分别为 Web 安全、漏洞挖掘与利用、网络渗透、恶意代码、逆向分析、溯源取证、安全运维、密码学应用、网络关键基础设施安全、端点与边界防护、云安全、物联网安全、移动与无线安全、区块链安全。



其中，“Web 安全”关注 Web 服务端和浏览器客户端安全，虽然 Web 安全属于应用安全且与“网络渗透”等一级节点有交集，但因其重要性和标志性而自成一类；漏洞是网络安全中最受关注的技术之一，也常常是攻击者的“先遣部队”，“漏洞挖掘与利用”关注汇编语言、符号执行、二进制插桩和相关工具运用等技术；“网络渗透”关注攻击者综合运用社工和技术手段对特定目标实施渗透以获得远程目标上的代码执行权的行为过程；“恶意代码”关注从自动传播到规避对抗的全生命周期关键技术；“逆向分析”是网络攻防中“变未知为已知”的有效手段，涵盖了文件格式、动态分析、脱壳和相关工具运用等技术；“溯源取证”关注 APT 攻击追踪溯源和网络犯罪取

 ©2019 中国网络空间安全人才教育联盟

证；“安全运维”是信息安全建设不可或缺的一部分，通过安全运维力保 IT 信息系统安全、稳定和可靠运行；密码学是网络安全的重要基础，“密码学应用”关注网络安全中常用的密码算法及应用；“网络关键基础设施安全”关注芯片、操作系统、核心应用软件、域名系统等的安全；“端点与边界防护”关注终端防护平台、端点检测和响应等端点安全技术，入侵检测与防御系统、安全审计系统等边界安全技术，以及威胁猎杀、数据防泄漏等相关防护技术与产品；“云安全”关注数据丢失与泄露、虚拟化安全等云计算平台面临的主要威胁；“物联网安全”关注 IoT 设备安全、通信协议安全和隐私泄露等；“移动与无线安全”关注移动设备安全、无线电安全；“区块链安全”关注矿机与矿池、智能合约和数字钱包等安全技术。

每个子体系（一级节点）又分为多个二级节点，二级节点分类为多个三级节点，最多不超过四级节点。

3.3 体系展开实例

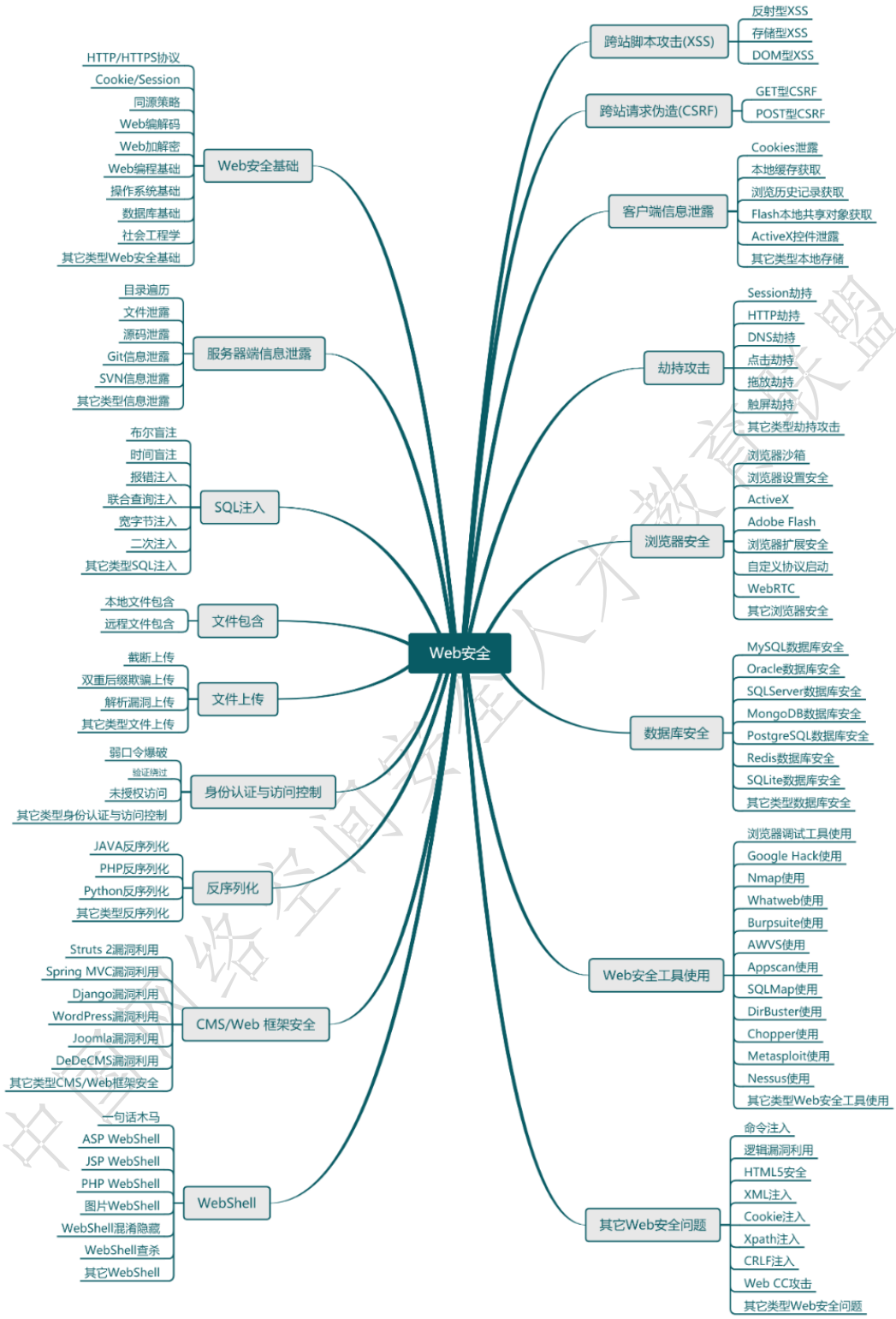
因篇幅有限，本指南只选取 Web 安全、网络渗透、安全运维三个子体系展开描述，并采用思维导图方式简介其三级节点。

1.Web 安全知识技能体系

以电子商务、社交网络为代表的 B/S 架构 Web 应用快速发展，使得 Web 服务成为互联网最重要的服务之一。与此同时，网页篡改、网络钓鱼、用户数据泄露等网络安全事件层出不穷，Web 安全成为亟待解决的焦点问题。Web 安全从知识技能视角可划分为 Web 安全基础、跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、客户端信息泄露、劫持攻击、浏览器安全等客户端安全，和服务端信息泄露、SQL 注入、文件包含、文件上传、身份认证与访问控制、反序列化、CMS/Web 框架安全、数据库安全、Webshell 等服务器端安全。

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟



（1）Web 安全基础。Web 安全基础涵盖了在 Web 安全研究中研究者应掌握的理论知识和实践能力，涉及系统、数据库、协议等理

 ©2019 中国网络空间安全人才教育联盟

论知识，Web 服务端语言及常用编程语言的阅读和编写能力，以及Web服务器的搭建、基础配置、简单运维能力等。Web安全基础主要技术包括 HTTP/HTTPS 协议、Cookie/Session、同源策略、Web 编解码、Web加解密、Web编程基础、操作系统基础、数据库基础、社会工程学等。

（2）跨站脚本攻击（XSS）。跨站脚本攻击(Cross Site Scripting, XSS)是一种常见的 Web 安全漏洞，它允许攻击者将恶意代码植入 Web 客户端，从而影响其他浏览此 Web 页面的用户。攻击者能够利用 XSS 在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户重定向到恶意站点。XSS 主要技术包括反射型 XSS、存储型 XSS 和 DOM 型 XSS。

（3）跨站请求伪造（CSRF）。跨站请求伪造(Cross-site Request Forgery, CSRF)是指伪造成合法用户发起请求，挟持用户在当前已登录的 Web应用程序上执行非本意操作的攻击方法。CSRF 允许攻击者迫使用户浏览器向存在漏洞的应用程序发送请求，而这些请求会被应用程序认为是用户的合法请求。CSRF 主要技术包括 GET 型 CSRF 和 POST 型 CSRF。

（4）客户端信息泄露。客户端信息指存在于客户端的用户数据，包括基本信息、设备信息、账户信息、隐私信息等，此信息若保护不当，一旦被攻击者获取，就会被利用进行网络诈骗、身份仿冒等恶意操作。客户端信息泄露主要技术包括 Cookies 泄露、本地缓存获取、浏览历史记录获取、Flash本地共享对象获取、ActiveX控件泄露等。

（5）劫持攻击。劫持攻击指攻击者通过某些特定的手段，将本该正确返回给用户的数据进行拦截，呈现给用户虚假的信息，主要是通过欺骗的技术将数据转发给攻击者。劫持攻击主要技术包括

 ©2019 中国网络空间安全人才教育联盟

Session 劫持、HTTP 劫持、DNS 劫持、点击劫持、拖放劫持、触屏劫持等。

（6）浏览器安全。浏览器是互联网最大的入口，是大多数网络用户使用互联网的工具，因此浏览器安全是一个极其重要的安全领域。浏览器安全主要技术包括浏览器沙箱、浏览器设置安全、ActiveX、Adobe Flash、浏览器扩展安全、自定义协议启动、WebRTC 等。

（7）服务器端信息泄露。服务器端信息泄露问题指因错误配置或 Web 组件漏洞导致服务器目录、文件等敏感信息遭泄露的问题。敏感信息可能被攻击者利用，进而对服务器发起针对性攻击。服务器端信息泄露主要技术包括目录遍历、文件泄露、源码泄露、Git 信息泄露、SVN 信息泄露等。

（8）SQL 注入。SQL 注入指通过将恶意的 SQL 语句注入正常的 GET 或 POST 方式 HTTP 请求，以改变 Web 服务器后端代码处理请求参数的执行逻辑，从而间接对服务器数据库执行增、删、改、查等操作的行为。SQL 注入主要技术包括布尔盲注、时间盲注、报错注入、联合查询注入、宽字节注入、二次注入等。

（9）文件包含。文件包含的合法用途是在代码中引入其他项目中的包、库等，以实现代码的有效复用。文件包含漏洞指因编程缺陷，导致 Web 服务器在处理时未能对所引用文件严格限制，致使所引用的文件可被攻击者控制的问题。文件包含主要技术包括本地文件包含和远程文件包含。本地文件包含通常通过引用服务器内部的敏感文件（如配置文件、源代码等）以获取服务器的关键信息；远程文件包含通常用于引用攻击者构造的恶意外部文件以在服务器上执行恶意操作。

（10）文件上传。文件上传漏洞指能够通过利用 Web 容器特性

 ©2019 中国网络空间安全人才教育联盟

或 Web 应用逻辑缺陷，向 Web 服务器直接上传恶意脚本、WebShell 等恶意文件的安全问题。文件上传时，通常需要解决文件格式限制绕过、上传路径获取、上传文件正确解析等问题。文件上传主要技术包括截断上传、双重后缀欺骗上传、解析漏洞上传等。

（11）身份认证与访问控制。身份认证与访问控制用于验证访问特定资源的用户身份，并设置访问权限。身份认证的目的在于确保用户身份的真实、合法和唯一性，最常见的认证方式就是用户名与口令，而访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。身份认证与访问控制主要技术包括口令爆破、验证码绕过、未授权访问等。

（12）反序列化。序列化指编程语言将变量、函数等对象转化为字节序列的过程。反之，将字节序列转化为对象的过程称为反序列化。反序列化漏洞指攻击者通过构造字节序列，转化生成恶意对象的安全问题。反序列化主要技术包括 JAVA 反序列化、PHP 反序列化、Python 反序列化等。

（13）CMS/Web 框架安全。CMS（Content Management System，内容管理系统）常用于快速的网站建设，CMS/Web 框架安全问题涉及各类 Web 组件（Struts2、Django、Spring MVC 等）、Web 应用（WordPress、Joomla、DeDeCMS 等）及其各版本具有的漏洞和利用代码。CMS/Web 框架安全主要技术包括 Struts2 漏洞利用、Spring MVC 漏洞利用、Django 漏洞利用、WordPress 漏洞利用、Joomla 漏洞利用、DeDeCMS 漏洞利用等。

（14）数据库安全。数据库系统是 Web 的重要组成部分，使得用户能够通过浏览器端的操作界面以交互的方式经由 Web 服务器来访问数据。数据库安全是指保护数据库以防止非法用户的越权使用、窃取、更改或破坏数据，涉及系统运行安全和系统信息安全两方面。

 ©2019 中国网络空间安全人才教育联盟

数据库安全主要技术包括 MySQL 数据库安全、SQLServer 数据库安全、MongoDB 数据库安全、PostgreSQL 数据库安全、Redis 数据库安全、SQLite 数据库安全等。

（15）WebShell。WebShell 是网站后门的一种形式，通常是以 ASP、PHP、JSP 或者 CGI 等网页文件形式存在于命令执行环境中，以达到控制网站服务器的目的。WebShell 主要技术包括一句话木马、ASP WebShell、JSP WebShell、PHP WebShell、图片 WebShell、WebShell 混淆隐藏、WebShell 查杀等。

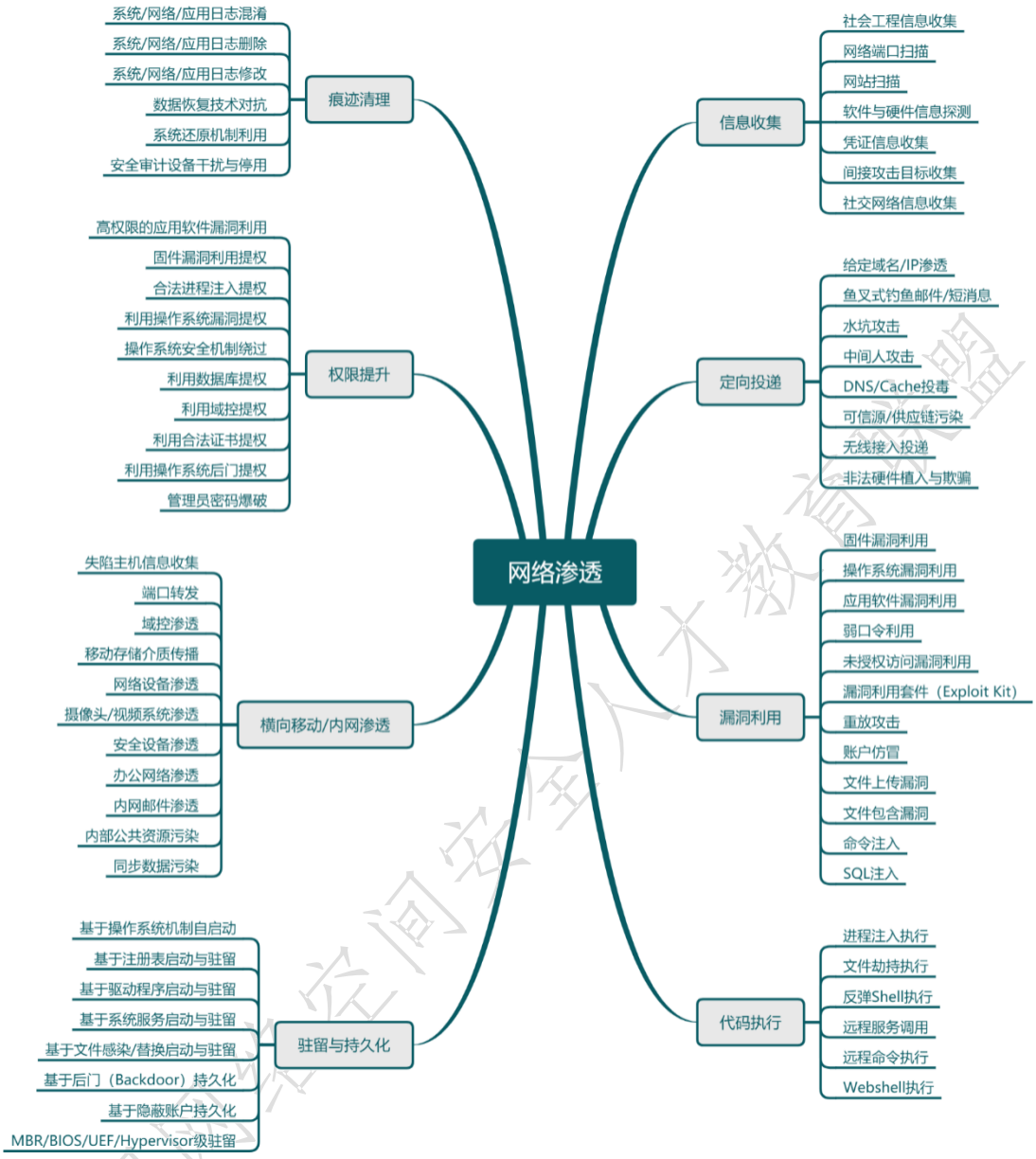
（16）Web 安全工具使用。Web 安全工具的使用能够有效提高工作效率，扩展渗透测试思路，涉及浏览器及其扩展工具，以及代理抓包、敏感文件探测、漏洞扫描、注入探测、目标信息搜集等行为。Web 安全工具主要技术包括浏览器调试工具、Google Hack、Nmap、Whatweb、Burpsuite、AWVS、Appscan、SQLMap、DirBuster、Chopper、Metasploit、Nessus 等工具的使用。

（17）其他 Web 安全问题。其它 Web 安全问题指未包含在上述知识点的其他安全问题。其它 Web 安全问题主要技术包括命令注入、逻辑漏洞利用、HTML5 安全、XML 注入、Cookie 注入、Xpath 注入、CRLF 注入、Web CC 攻击等。

2.网络渗透知识技能体系

网络渗透（Network Penetration）是网络攻防行动中率先开展的、也是最核心的环节，攻击者综合运用社工和技术手段对特定目标实施渗透，获得远程目标上的代码执行权，为进一步植入恶意代码为持久控制目标提供机会。从攻击链视角可将网络渗透技术划分为：信息收集、定向投递、漏洞利用、代码执行、权限提升、横向移动和痕迹清理等。

 ©2019 中国网络空间安全人才教育联盟



（1）信息收集。信息收集（Reconnaissance）主要是攻击者通过各种侦查手段，尽可能全面的获取目标的情报信息，以制定有针对性的行动策略，提高入侵的效率和成功的概率。信息收集主要技术包括社会工程信息收集、网络端口扫描、网站扫描、软件与硬件信息探测、凭证信息收集、间接攻击目标收集和社交网络信息收集等。

 ©2019 中国网络空间安全人才教育联盟

（2）定向投递。定向投递（Targeted Delivery）是将攻击者制作好的恶意程序或代码片段投递到目标系统中的过程。该阶段是攻击者对目标一种攻击尝试的活动，攻击者会尝试多种投递方式。定向投递主要技术包括给定域名/IP 渗透、鱼叉式钓鱼邮件/短消息、水坑攻击、中间人攻击、可信源/供应链污染、无线接入投递、非法硬件植入与欺骗等。

（3）漏洞利用。漏洞利用（Exploitation）主要是综合运用操作系统和应用程序等的漏洞触发代码执行。该阶段使得攻击者投递的恶意程序或代码片段获得执行机会。漏洞利用主要技术包括固件漏洞利用、操作系统漏洞利用、应用软件漏洞利用、弱口令利用、未授权访问漏洞利用、重放攻击、账户仿冒、命令注入和 SQL 注入等。

（4）代码执行。代码执行（Execution）即攻击者投递的恶意程序或代码片段在目标系统上执行的过程。该阶段使得攻击者可获得目标系统的临时或持久控制权限。代码执行主要技术包括进程注入执行、文件劫持执行、反弹 Shell 执行、远程服务调用、远程命令执行和 Webshell 执行等。

（5）驻留与持久化。驻留与持久化（Presence and Persistence）即系统重启后如何让恶意代码自身再次获得执行权而不引起明显异常，实现尽可能长时间生存。当然，也有极少量的恶意代码仅存在于内存之中，断电或重启则会消失。这类恶意代码或者依托快速自动传播能力实现总体规模平衡（如红色代码蠕虫），或者一次性完成特定任务，避免持久化带来的异常。驻留与持久化主要技术包括基于注册表启动与驻留、基于系统服务启动与驻留、基于文件感染启动与驻留、MBR/BIOS/UEFI/Hypervisor 级驻留、基于隐蔽账号持久化、基于后门（Backdoor）持久化等。

（6）权限提升。权限提升（Privilege Escalation）是攻击者为了

 ©2019 中国网络空间安全人才教育联盟

能够在受害主机或网络中获得更多资源时，采取的一种攻击技术，目的是获得管理员权限或系统的执行权限。权限提升主要技术包括高权限的应用软件漏洞利用、固件漏洞利用提权、合法进程注入提权、利用操作系统漏洞提权、操作系统安全机制绕过、利用数据库提权、利用域控提权、利用操作系统后门提权等。

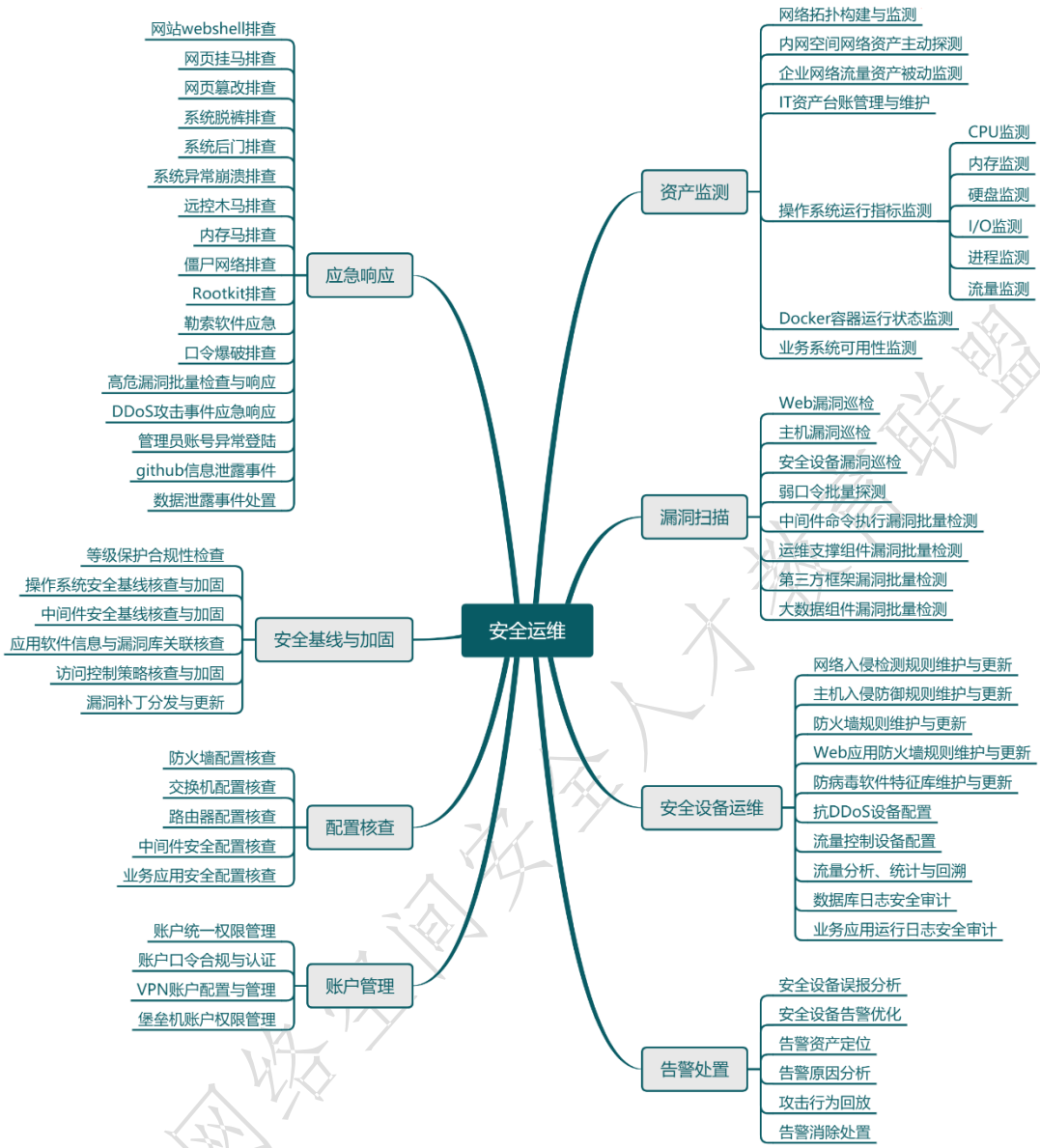
（7）横向移动/内网渗透。横向移动/内网渗透（Lateral Movement）是攻击者进入目标网络后，在目标内网扩散，以获得更高级别目标的执行权限或获取更多有价值的数据。横向移动/内网渗透主要技术包括失陷主机信息收集、端口转发、域控渗透、移动存储介质传播、网络设备渗透、摄像头/视频系统渗透、安全设备渗透、办公网络渗透、内网邮件渗透、内部公共资源污染和同步数据污染等。

（8）痕迹清理。痕迹清理（Trace Erasing）是攻击者为了避免攻击痕迹被电子取证所采取的对抗动作。攻击者需要尽可能的切断取证链，使得攻击现场难以还原。痕迹清理主要技术包括系统/网络/应用日志混淆、系统/网络/应用日志删除、系统/网络/应用日志修改、数据恢复技术对抗、系统还原机制利用、安全审计设备干扰与停用等。

3.安全运维知识技能体系

安全运维是企业信息安全建设不可或缺的一部分。通过安全运维落实企业的安全政策、安全规划和安全体系的建设的保障，确保企业 IT 信息系统安全、稳定和可靠运行。从知识技能视角可划分为资产监测、漏洞扫描、安全设备运维、告警处置、应急响应、安全基线与加固、配置核查和账户管理。如下图所示。

 ©2019 中国网络空间安全人才教育联盟



（1）资产监测。资产监测是安全运维的基础。通过IT资产监测，确保企业运维资产不被遗漏，IT 资产在可见、可控和可管条件下实施。资产监测主要包括网络资产拓扑构建与监测、内网空间网络资产主动探测、企业网络流量资产被动监测、IT 资产台账管理与维护、操作系统运行指标监测、Docker 容器状态运行监测和业务系统可用性监测等。

（2）漏洞扫描。漏洞扫描是安全运维日常主要工作之一。通过

 ©2019 中国网络空间安全人才教育联盟

漏洞扫描与漏洞巡检，能够全面了解企业网络安全风险状况，及时了解新增的高危漏洞和企业暴露的漏洞情况。漏洞扫描工作主要包括 Web 漏洞巡检、主机漏洞巡检、安全设备漏洞巡检、弱口令批量探测、中间件命令执行漏洞批量检测、运维支撑组件漏洞批量检测、第三方框架漏洞批量检测和大数据组件漏洞批量检测等。

（3）安全设备运维。安全设备运维是安全运维日常主要工作之一。通过安全设备运维来保障企业的安全防护体系不被随意打破。安全设备运维工作主要包括网络入侵检测规则维护与更新、主机入侵防御规则维护与更新、防火墙规则维护与更新、Web 应用防火墙规则维护与更新、防病毒软件特征库维护与更新、抗 DDoS 设备配置、流量控制设备配置、流量统计分析与回溯、数据库日志安全审计和业务应用运行日志安全审计等。

（4）告警处置。告警处置是安全运维重要工作之一。通过处置安全设备/系统的告警，保障企业能够有效地检测与防御外部攻击，并且能够及时发现与修复企业自身的安全缺陷。告警处置主要包括安全设备误报分析、安全设备告警优化、告警资产定位、告警原因分析、攻击行为回放和告警消除处置等。

（5）应急响应。应急响应是安全运维重要工作之一。企业需要在各种意外的安全事件发生后采取有效的应对措施，力保将企业因安全事件造成的损失降低到最小。应急响应主要包括网站 webshell 排查、网页挂马排查、网页篡改排查、系统脱库排查、系统后门排查、系统异常崩溃排查、远控木马排查、内存木马排查、僵尸网络排查、Rootkit 排查、勒索软件应急、口令爆破排查、高危漏洞批量检查与响应、DDoS 攻击事件应急响应、管理员账号异常登陆、github 信息泄露事件和数据泄露事件处置等。

（6）安全基线与加固。安全基线与加固是安全运维重要工作之

 ©2019 中国网络空间安全人才教育联盟

一。通过建立安全基线，确保企业安全建设符合国家政策需求和企业自身安全建设的最低要求。安全基线与加固主要包括等级保护合规性检查、操作系统安全基线核查与加固、中间件安全基线核查与加固、应用软件信息与漏洞库关联核查、访问控制策略核查与加固和漏洞补丁分发与更新等。

（7）配置核查。配置核查是安全运维日常工作之一。运维工作人员通过定期核查配置，查缺补漏，确保企业网络安全配置的有效性以及合规性。配置核查主要包括防火墙配置核查、交换机配置核查、路由器配置核查、中间件安全配置核查和业务应用安全配置核查等。

（8）账户管理。账户管理是力图消除企业员工账户使用不规范、不合规带来的安全隐患，避免因员工账户、口令和权限的安全问题给整个企业网络环境带来更大的安全隐患。账户管理主要包括账户统一权限管理、账户口令合规与认证、VPN 账户权限与管理和堡垒机账户权限管理等。

3.4 知识技能体系的应用

1.网安人才培养

- 用于高校网络空间安全和计算机方向教师设置网安课程;
- 用于网安爱好者系统化自学。

2.网安人才训练

- 用于体系化设计网络安全学习型/实操性实验，既可用于学习，也可用于考试;
- 让实验设计者更容易精准打标签，降低对其能力的要求;
- 让实验审核者更容易发现题目重复、分布不均匀等问题;

 ©2019 中国网络空间安全人才教育联盟

- 让学习者更容易掌握进度，建立全局视野。

3.网安人才认证

- 基于体系和题库，建立网安知识图谱;
- 针对特定技能，自动生成考点和难度合理的初始考卷;
- 基于知识图谱和答题情况，动态选题，实现精准评测。

4.网安岗位招聘

- 用人单位更易于选取所需技能并专业化描述需求;
- 围绕技能的面试和笔试，更具针对性。

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

第四章 网安人才认证体系

网络空间安全的认证目的是评判从业人员是否达到网络空间安全专业技术人员独立从事某种网络空间安全专业技术工作知识、技术和能力的要求。建立网络空间安全认证体系有利于加快网安人才培养；有利于指导院校培养体系、社会培训、自学成才等多渠道人才培养/成长活动，促进专业人才队伍素质和业务水平的提高；有利于规范地评价专业人员是否具备相应知识技能，以合理使用专业技术人才。

4.1 发达国家认证情况

美国等发达国家高度重视网络空间安全认证和职业培训，伴随网络空间安全的发展形势和自身实际情况，在国家层面上不断地出台相应的战略计划，以完善其认证体系和培训体系。目前，国际网络空间安全认证和职业培训体系已相对完善，基本形成规模化的认证和培训产业，相关的认证和职业培训认可度高。

2012 年美国正式发布了《NICE 战略计划》，指出由 DHS 负责统一领导制定网安人才框架，以评估工作人员的专业化水平，为预测未来网络空间安全需求推荐最佳的实践活动，为招募和挽留人才制定国家策略。同时，该计划强调关注网安人才培训和职业发展，由 ODNI、DoD、DHS 共同领导，协调学术界、工业界和各级地方政府，共同制定国家网安人才所需的培训和职业发展过程。该计划的目的是建立和维护一个具有全球竞争力的网安人才队伍。2014 年美国发布了最新版本的《NICE 网络安全人才框架》，目前该框架仍在持续更新。

2013 年欧盟发布了《欧盟网络安全战略》，指出网络和信息安全教育和培训工作应从国家层面发起，措施包括：各成员国要在国家

 ©2019 中国网络空间安全人才教育联盟

层面重视网络安全方面的教育与培训；学校要开展网络安全培训，对计算机科学专业学生进行网络安全、网络软件开发以及个人数据保护的培训；对公共部门人员进行网络安全方面的培训。

2013 年日本发布了《网络空间安全战略》，指出将网络与信息安全人才培养作为一项重要举措，措施包括：提出一种可用的社会性的网络安全框架，针对不同需求的技术人员提供不同的专业培训和教育；改进资格/能力评估系统；由政府任命外部信息安全人员，发现和培训专业人才。

2009 年澳大利亚政府发布了《信息安全战略》，提出培养具有网络安全技能的人才，政府协助建立信息安全专业人员认证体系。

4.2 国外主要认证体系

国际网络空间安全认证和职业培训体系建设起步较早，例如，美国白宫早在 1998 年就提出了《信息系统保护的国家计划》，旨在从多方面介入信息系统和网络基础设施安全保障的培训和认证工作，培养更多的信息安全人才。目前，国外主要认证体系涉及到政府、大学研究中心、行业协会和各大公司等几乎行业所有相关实体。主要包括:

- 政府制定政策，倡导开展相关认证和培训;
- 行业协会帮助设定网络空间安全认证和职业培训标准，创立、更新认证项目，开展持续的职业培训活动，组织认证考试，颁发并维持认证证书;
- 高校及科研院所辅助认证和培训体系建设，开展教育和培训活动;
- 企业开展针对内部的非认证职业培训，厂商提供针对自身网络空间安全产品的培训，并颁发相应的培训证书。

中国网络空间安全人才教育联盟

目前，国际网络空间安全认证和培训体系具有较高的权威性和认可度，代表性的有以下几种。

1.美国国家安全局和国土安全部联合主持的国家信息保障/网络防御（IA/CD）学术卓越中心（CAE），简称 CAE 认证。所有在美国地方上认可的两年制、四年制及研究生水平的院校、机构都可以申请成为 IA/CD 学术卓越中心。不同于行业协会和商业机构针对个人技能能力的认证，美国 CAE 认证是一种对教育机构从事网络安全人才培养能力的认证。CAE 认证的目标是通过促进信息保障/网络防御（IA/CD）方面的高等教育和研究，减少美国国家信息基础设施的脆弱性，并培养出越来越多的 IA/CD 学科的专业人士。

2.国际信息系统安全认证联盟（ISC）²（International Information Systems Security Certification Consortium）

- CISSP 认证：注册信息系统安全师
- CSSLP 认证：注册软件生命周期安全师
- CCFP 认证：注册网络取证师
- SSCP 认证：系统安全认证从业者
- CCSP 认证：注册云安全师

3.信息系统审计与管控协会 ISACA（Information System Audit and Control Association）

- CISA 认证：注册信息系统审计师
- CISM 认证：注册信息安全经理
- CGEIT 认证：企业信息科技管治认证
- CRISC 认证：风险及信息系统监控认证

4.国际电子商务顾问局 EC-Council（International Council of E-

 ©2019 中国网络空间安全人才教育联盟

Commerce Consultants）

- CEH 认证：道德骇客
- ECSA 认证：安全分析师
- LPT 认证：授权渗透测试员
- CCISO 认证：首席信息安全官
- CHFI 认证：计算机黑客取证调查人
- ENSA 认证：网络安全管理人
- EDRP 认证：灾难恢复职业人
- ECSP 认证：放心程序员
- ECIH 认证：事故处理人
- CSCU 认证：放心计算机使用者
- ECES 认证：加密专员
- ECSS 认证：安全专员
- CEI 认证：EC-Council 讲师
- CNDA 认证：防卫架构师
- ECVP 认证：VOIP 职业人
- CSE 认证：证书系列教育认证

5.美国计算机行业协会 CompTIA（Computing Technology Industry Association）

- 基础认证级别的信息技术基础认证（IT Fundamentals）
- 专项级的云基础认证（CompTIA Cloud Essentials）
- 医疗信息技术技术员认证（CompTIA Healthcare IT Technician）

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

- 社交媒体安全职业认证（Social Media Security Professional）
- 职业级的安全职业者 CompTIA A+、CompTIA Network+和CompTIA Security+认证
- 大师级的高级安全执业者认证（CompTIA CASP）

6.由联合国训练研究所、网络信息安全管理与服务教育部工程研究中心以及 GPST 全球专业人才认证考试中心联合认证的注册信息安全专员（CISF）认证。

4.3 建设我国网安人才认证体系

网络空间安全认证和职业培训体系是网安人才培养体系的重要组成部分，从网安人才培养的特点和实战化认证体系的必要性看，建立完善的认证体系对网安人才队伍建设有着重要意义。

1.网安人才培养的特点

网安人才的培养具有以下特点:

（1）针对性和实用性，体现在培训目标和课程等根据岗位实际需求和认证标准确定;

（2）灵活性和多样性，体现在培训形式多样，培训时限弹性，培养对象不受限制，教学形式灵活;

（3）技术性和技能性，体现在培训方法强调理论与实践操作相结合;

（4）连续性和持久性，体现在职业培训周期短，能够应对网络空间安全领域不断涌现的新知识、新技术和新产品。

2.建立实战化认证体系的必要性

我国网安人才需求迫切，数量奇缺，但岗位匹配度还很低。随着我国信息化建设的不断推进，网安人才需求将持续增长，并呈逐

 ©2019 中国网络空间安全人才教育联盟

年递增趋势。综合多方数据推测，到 2020 年，我国网安人才需求数量很可能超过百万。

此外，我国网安人才三个主要渠道，高校培养、社会培训、自学成才，在人才出口上均不同程度存在与产业界需求脱节问题。高校网络空间安全毕业生无法快速适应岗位实际工作需求，往往需要用人单位进行一年甚至更长时间的二次培训才能满足实际工作需求；社会培训结业人员，在职业发展、业务能力提升方面，存在知识储备不足、缺少系统性理论能力支撑等问题；自学成才的“奇才”，在职业早期进步很快，但在后期业务拓展、体系性实战能力提升，特别是团队协作、团队管理等方面，存在明显“力不从心”。

综上，迫切需要通过制定规范统一的考核评估方式，发挥认证指挥棒作用，落实实战化网安人才出口标准，解决缺人才、缺合适的人才、缺可持续发展的复合型人才问题。

3.建设我国网安人才认证体系的建议

可借鉴美国 CAE 模式，国内多方通力合作建立完善的网安人才认证和职业培训体系，推进网安人才队伍壮大、质量提升、人尽其才。

实战化网安人才认证体系具有快速壮大网安人才队伍，持续提升网安人才技术水平和实践能力等的优势。具体举措上，包括：

（1）在国家层面上，制定网安人才培养战略计划，强调网络空间安全认证和职业培训的重要地位；

（2）由国家有关机构主导建立“网络空间安全认证体系”，包括专业范畴、职业路径以及岗位能力和资格认证等，突出国家战略、行业需求对人才实战能力的特殊要求；

（3）围绕网络空间安全认证体系配套建立相关政策和法律法规，

 ©2019 中国网络空间安全人才教育联盟

确保认证体系的权威性和有效性。并将网络空间安全认证的协调、执行、监督、管理等权利具体制定给政府和行业的有关部门，共同推动认证体系建设和运行。

中国网络空间安全人才教育联盟

 ©2019 中国网络空间安全人才教育联盟

附 中国网络空间安全人才教育联盟

中国网络空间安全人才教育联盟，是在中国产学研合作促进会的指导下，由从事网络空间安全相关教育、科研、产业、应用的高校、科研学术机构、地方政府、企业单位、社会团体、事业单位和政府机关直（隶）属单位以及热衷于网络空间安全人才教育的个人共同自愿结成的全国性、行业性、非营利性、创新性组织。

联盟旨在发挥桥梁纽带作用，组织和动员全国网安领域顶级高校、企业、事业单位和社会团体，针对人才教育、培养、培训、认证以及就业等环节，探索科学可行的网安人才培养新模式，努力缩小和补齐国家网安人才需求的缺口和短板，为国家网安事业发展提供有力的支撑。

联盟成立于 2018 年 9 月，设理事会、常务理事会和秘书处，共同受会员代表大会监督，在会员代表大会集体授权下，开展工作。联盟下不常设分支机构或分会，根据联盟主旨和当前工作重点，成立了网安人才供需协调工作组、网安人才挖掘发现工作组、网安人才培训培养工作组、网安人才标准认证工作组和网安意识培养提高工作组等主题性工作组。

欢迎有志于网络空间安全人才教育的企业、机构和个人加入！

中国网络空间安全人才教育联盟公众号

 ©2019 中国网络空间安全人才教育联盟