ICS 35.240.01
I6440

T/WHCSAxxx—2024

团　体　标　准

网络安全人才实战化训练环境建设

Construction of a Practical Training Environment for Network Security Talents

2024-xx-xx 发布　　2024-10-1 实施

武汉市网络安全协会　发布

目　次

前　言

本文件按照GB/T 1.1-2020《标准化工作导则第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由奇安信科技集团股份有限公司、湖北经济学院共同提出。

本文件由武汉市网络安全协会归口。

本文件起草单位：奇安信科技集团股份有限公司、湖北经济学院、武汉市网络安全协会、湖北省教育装备行业协会、武汉职业技术学院、武汉软件工程职业学院、湖北科技职业学院、武汉商贸职业学院、武汉交通职业学院、湖北国土资源职业学院、鄂州职业大学、长江职业学院、湖北职业技术学院、武汉东西湖职业技术学校、武汉同德兴信息技术有限公司、武汉铁路职业技术学院、江汉大学、武汉商学院、汉口学院、湖北华育智远信息科技有限公司、武汉科云信息技术有限公司等。

本文件主要起草人：孙宝林、张宇、张玉印、刘悦恒、乔奇、邓小飞、骆泓玮、涂家海、谢日星、宋莺、李彤亚、胡迎九、潘志安、李强、赵小娜、赵新、陈浩亮、官灵芳、何新洲、易鹤健、卢力、刘媛、丰婉伊、连进、陈新文、蒋方园、郭浩平、吴鹏、周盛飞、姜明哲、邓太勇等。

本文件为首次发布。

引　言

培养网络安全人才的网络安全体系规划能力、信息系统安全防护保障能力、数据库安全与管理能力、数据备份与恢复能力、网络协议分析能力、网络安全技术应用能力、网络安全设备部署配置、移动网络与云安全技术、攻防实战、应急响应及运维综合能力等，以建立网络安全实战化的人才培养体系。

培养具备扎实的专业基础知识和实战化网络安全能力，可以根据业务需求制定信息系统和网络的安全策略和防御措施，能够较快解决本专业领域实际工作中出现的各种安全问题，能保障信息系统安全稳定运行，能够在网络空间安全领域及相关产业从事安全运维、攻防对抗、应急处理和综合应用的优秀工程实战化人才。

通过网络安全实战化实训室的建设，提升对网络安全攻防实战和专业安全人员培养、人员实操、人员实战、多维度数据分析等多方面的能力培养。在实战方面，建立一体化的业务综合仿真系统与虚拟化业务平台，完善网络安全事件流程，建立起队伍管理、任务管理、资源管理、安全事件应急、安全防护等一体化业务体系，充分整合各类资源，固化安全隐蔽技术措施，以建立高效、实用、信息化的指挥与业务平台，形成业务的一整套信息化管理体系；在专业安全人员培养与实训方面，通过培训与演练相结合的实训靶场系统，建立完善的学习、演练、实训、考核一体化平台。

网络安全人才实战化训练环境建设

1 范围

本文件规定了网络安全人才实战化训练环境建设的基本要求，包括网络安全人才实战化训练环境建设框架、实训设施、训练环境建设、实训管理等方面的要求。

本文件适用于应用型本科院校、高职院校、校企合作网络安全公司等信息安全类专业实训室的规划设计、建设和运营。网络安全公司、中等职业学校及其他类型学校可参考执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款，其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JY/T 0595-2019 基础教育装备 分类与代码

T/CAS 375-2019 网络安全服务机构等级评定规范

GA/T 1717.1-2020 信息安全技术 网络安全事件通报预警 第1部分：术语

GB/T 25069-2022 信息安全技术 术语

GB/T 29264-2012 信息技术服务 分类与代码

GB/T 32921-2016 信息安全技术 信息技术产品供应方行为安全准则

GB/T 20984-2022 信息安全技术 信息安全风险评估方法

GB/T 22240-2020 信息安全技术 信息系统安全等级保护定级指南

GB/T 25058-2019 信息安全技术 信息系统安全等级保护实施指南

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

GB/T 20275-2021 信息安全技术 网络入侵检测系统技术要求和测试评价方法

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 40652-2021 信息安全技术 恶意软件事件预防和处理指南

GB/T 39680-2020 信息安全技术 服务器安全技术要求和测评准则

GB/T 37932-2019 信息安全技术 数据交易服务安全要求

GB/T 28450-2020 信息技术 安全技术 信息安全管理体系审核指南

GB/T 36342-2018 智慧校园总体框架

3 术语和定义

GB/T 20984、GB/T 20986、GB/T 25069-2022、GB/T 30279、GB/T 36643界定的以及下列术语和定义适用于本文件。

3.1

安全监控 Security monitoring

安全监控是指对计算机系统、网络、应用程序和数据进行实时监控、识别、跟踪和统计分析等，以发现安全威胁、防止安全威胁以及安全攻击的过程。

3.2

安全评估　Security assessment

按安全标准及相应方法，验证特定功能的工作系统（或交付件）与适用标准的符合程度、安全程度等所进行的分析与评估。

注：安全评估通常是产品评价过程的最后阶段。

[来源：GB/T25069-2022, 3.19]

3.3

安全审计　Security audit

安全审计是指由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对相关网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价，并在控制、安全策略和过程等方面提出改进建议。

[来源：GB/T25069-2022, 3.24]

3.4

对抗双方　Antagonistic parties

在网络安全领域中，对抗双方通常指的是黑客（攻击者）和防御者（如企业、组织或个人用户）。

3.5

防火墙 Firewall

设置在网络环境之间的一种安全屏障，它由一台专用设备或若干组件和技术的组合组成。网络环境之间两个方向的所有通信流均通过此屏障，并且只有按照本地安全策略定义的、已授权的数据流才允许通过。

[来源：GB/T 25068.1-2020, 3.12]

3.6

防御 Defense

从网络安全的角度来看，防御是为了保护己方信息网络系统和信息安全而进行的防御，是网络战的组成部分。

3.7

访问控制 Access control

一种确保数据处理系统的资源只能由经授权实体以授权方式进行访问的手段。

[来源：GB/T25069-2022, 3.147]

3.8

非法控制 Illegal control

使系统或网络按非法控制者意愿运行的行为。

[来源：GB/T25069-2022, 3.153]

3.9

非入侵式攻击 Non-intrusive attack

一种针对密码模块，对其边界内的组件不直接物理接触，也不更改其状态的攻击。

[来源：GB/T25069-2022, 3.155]

3.10

分布式拒绝服务攻击 Distributed denial-of-service attack

分布式拒绝服务攻击是指处于不同位置的多个攻击者同时向一个或数个目标发动攻击，或者一个攻击者控制了位于不同位置的多台机器并利用这些机器对受害者同时实施攻击。由于攻击的发出点是分布在不同地方的，这类攻击称为分布式拒绝服务攻击，其中的攻击者可以有多个。

3.11

风险 Risk

风险就是人们所期望的目标与实际结果之间的不确定性影响。

注 1：影响是指与期望的偏离（正向的或反向的）。

注 2：不确定性是对事态及其结果或可能性的相关信息、解或知识缺乏的状态(即使是部分的)。

注 3：风险常被表征为潜在的事态和后果,或者它们的组合。

注 4：风险常被表示为事态的后果（包括情形的改变）和其发生可能性的组合。

注 5：在信息安全管理体系的语境下，信息安全风险可被表示为对信息安全目标的不确定性影响。

注 6：信息安全风险与威胁利用信息资产或信息资产组的脆弱性对组织造成危害的潜力相关。

[来源：GB/T25069-2022, 3.164]

3.12

风险分析 Risk analysis

理解风险本质和确定风险级别的过程。

注 1：风险分析提供风险评价和风险处置决策的基础。

注 2：风险分析包括风险估算。

[来源：GB/T25069-2022, 3.166]

3.13

风险管理 Risk management

指导和控制组织相关风险的协调活动。

[来源：GB/T25069-2022, 3.168]

3.14

攻防混战 Attack-defensive melee

在网络安全领域，攻防混战则表现为黑客（攻击方）与网络安全防御团队（防御方）之间的较量。

3.15

攻防模式 Offensive and defensive mode

攻防模式是指在网络安全对抗赛中，参赛队伍在网络空间互相进行攻击和防守的一种比赛模式。

3.16

攻击 Attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[来源：GB/T25069-2022, 3.218]

3.17

攻击检测 Attack detection

攻击检测是一种网络安全技术，用于识别、分析和响应针对计算机网络或系统的恶意行为或攻击。

3.18

攻击特征 Attack signature

预先界定的据以能发现一次攻击事件正在发生的特定信息。

[来源：GB/T25069-2022, 3.220]

3.19

攻击者 Attacker

故意利用技术和非技术安全控制的脆弱性，以窃取或损害信息系统和网络，或者损害合法用户对信息系统和网络资源可用性为目的的任何人。

[来源：GB/T25069-2022, 3.221]

3.20

缓冲区溢出 Buffer overflow

当程序试图将数据写入一个固定大小的缓冲区时，如果数据的大小超过了缓冲区的大小，就会发生缓冲区溢出。这可能会导致程序崩溃、数据损坏或执行恶意代码。

3.21

漏洞扫描 Vulnerability scanning

漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，以发现可利用漏洞的一种安全检测行为。

3.22

认证方式 Authentication

在网络安全中，认证是确保只有授权用户才能访问系统或资源的重要机制。这是验证用户、进程或设备的身份或其他属性的过程。

3.23

入侵检测 Intrusion detection

入侵检测是指通过对行为、安全日志或审计数据或其他网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图。

3.24

渗透测试 Penetration test

渗透测试旨在检测应用程序、网络或系统的安全弱点，通过模拟攻击者的行为来发现潜在的安全漏洞。

3.25

数据备份 Data backup

数据备份是指为防止系统出现操作错误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。

3.26

网络安全对抗赛 Cyber security challenge

网络安全对抗赛是指通过模拟真实的网络攻击和防御行为，来评估和提升网络安全能力的比赛。

3.27

网络安全事件 Cybersecurity incident

与可能危害组织资产或损害其运行相关、单个或多个被识别的信息安全事态。

[来源：GB/T 43557-2023, 3.5]

3.28

网络安全态势 Cybersecurity situation

对一定范围网络中脆弱性、网络安全威胁、网络安全事态、网络安全事件，以及与网络安全相关的其他情况的整体描述。

[来源：GB/T 43557-2023, 3.6]

3.29

网络安全信息 Cyber security information

描述网络安全（即网络空间安全）相关情况的信息。

注：网络安全信息主要包括威胁信息、脆弱性信息、网络安全事件信息、网络安全态势信息等。

[来源：GB/Z 42885-2023, 3.1]

3.30

网络防御 Network defense

网络防御是指通过采取一系列的技术和管理措施，保护计算机网络系统及其中的数据免受潜在的威胁、攻击和损害的过程。

3.31

网络攻击 Network attack

网络攻击是指针对计算机信息系统、基础设施、计算机网络或个人计算机设备的任何类型的进攻动作。

3.32

网页木马 Web trojan horse

一种恶意软件，通常伪装成普通的网页文件或将恶意代码直接插入到正常的网页文件中。当有人访问这些网页时，网页木马就会利用系统或浏览器的漏洞自动下载并执行恶意代码。

3.33

网络威胁 Network threat

网络威胁是指任何可能危害计算机网络、系统或数据的机密性、完整性、可用性或可控性的行为、事件或状况等。

3.34

威胁分析 Threat analysis

威胁分析可以帮助组织识别网络系统中的安全薄弱环节，并采取相应的安全措施来预防和应对威胁。

3.35

信息安全 Information security

对信息的保密性、完整性和可用性的保持。

注：另外，也可包括诸如真实性、可核查性、抗抵赖和可靠性等其他性质。

[来源：GB/T25069-2022, 3.673]

3.36

信息安全保障能力 Capability of information security assurance

被保障实体安全防御、响应和恢复等特性的体现。

[来源：GB/T25069-2022, 3.676]

3.37

信息安全保障评价 Evaluation of information security assurance

收集信息安全保障证据，并获得信息安全保障值的过程和途径。

[来源：GB/T25069-2022, 3.677]

3.38

信息安全风险 Information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注：它以事态的可能性及其后果的组合来度量。

[来源：GB/T25069-2022, 3.681]

3.39

信息安全竞技系统 Information security competitive system

信息安全竞技系统可用于竞赛活动比拼中漏洞环境及各类实训环境的搭建。安全竞技系统目的主要用于行业、高校及社会组织中各大技能CTF竞赛活动（Capture The Flag）、攻防混战、攻防技能竞赛专业的网络安全竞赛活动。该系统使用主流的安全竞技平台设备及实训环境，可用于竞赛活动比拼中漏洞环境及各类实训环境的搭建。

3.40

信息安全实训系统 Information security training system

信息安全实训系统是面向应用型本科以及高职类院校信息安全实训需求的实训类系列产品，致力于解决人才培养问题，通过先进的平台化架构，提供从教学方案制定--理论学习--仿真实训--项目实训--能力评估--教学跟踪的一体化人才培养方案，提供专业的信息安全教学方案，帮助学校教师进行课程理论体系的建设，实现复合型人才培养的目标。

3.41

信息安全意识 Information security awareness

人们面对有可能对信息本身或信息所处的介质造成损害的外在条件的一种戒备和警觉的心理状态。

[来源：GB/T25069-2022, 3.688]

3.42

行为监控 Behaviour monitoring

行为监控是观察用户、信息系统和流程的活动的过程。通过行为监控，可以发现异常行为或潜在的安全威胁。

3.43

嗅探 Sniffing

嗅探是指对局域网中流经的数据包进行截取及分析，从中获取有效信息。黑客可以使用嗅探技术来窃取用户的敏感信息，如用户名、密码等。

3.44

应急事件 Emergency

应急事件是指突发自然灾害、事故灾难、社会安全事件等，在一定时间和空间范围内造成或可能造成较大的生命财产损失，危及公共安全、社会稳定等的事件。

3.45

应急响应 Emergency response

应急响应主要是为了应对各种网络安全事件，包括计算机或网络所存储、传输、处理的信息的安全事件。

3.46

应急演练 Emergency drill

应急演练是在预设的情景条件下，通过各级组织按照应急预案和既定程序，组织相关人员进行的一种模拟应对过程。

4 网络安全人才实战化培养定位

网络安全人才实战化培养定位是指针对网络安全领域,以培养具备实际操作能力和应对真实威胁能力的网络安全人才为目标，通过整合教育培训、实践演练、企业实训和国际交流等多种方式，全面提升网络安全人才的实战能力和综合素质。网络安全人才实战化的岗位要求框架如图1所示，网络安全人才实战化的知识结构如图2所示。

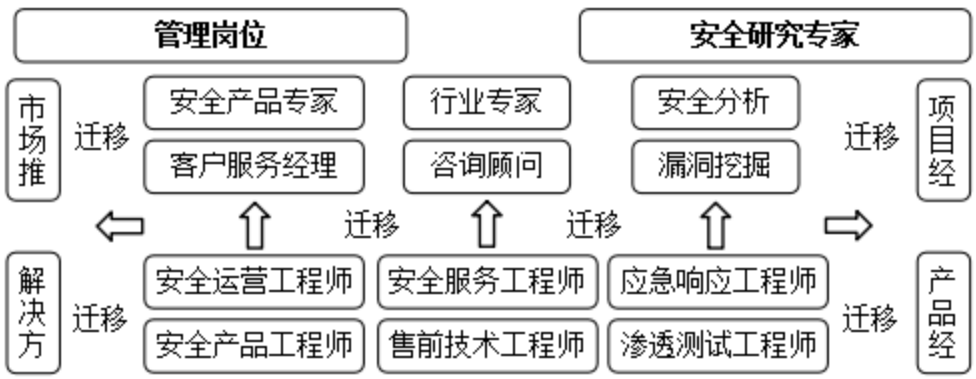

图 1 网络安全人才实战化的岗位要求框架

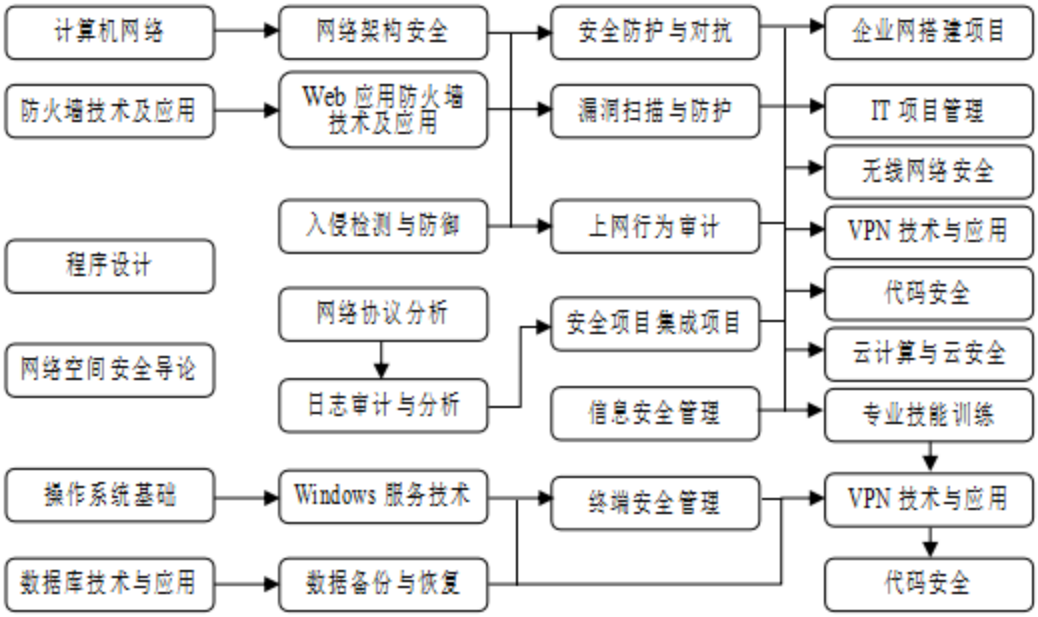

图 2　网络安全人才实战化的知识结构图

4.1 网络安全人才实战化培养的基本要求

1）培养定位的基本要求主要有：

a) 实战导向。培养过程注重实际操作和应对真实威胁的能力训练，使学员能够在真实或模拟的网络环境中进行安全监测、风险评估、渗透测试、应急响应等实战操作。

b) 综合素质。除了网络安全技术和工具的使用能力外，还注重培养学员的团队协作能力、沟通能力、创新能力等综合素质，以适应复杂的网络安全环境。

c) 终身学习。网络安全技术和威胁环境在不断变化，应具备终身学习的能力，不断更新自己的知识和技能，以应对新的挑战。

以上培养定位仅是基于一般的理解和描述，具体的培养定位可能会根据国家标准、行业需求和实际情况进行调整和完善。在实际应用中，建议参考相关的国家标准、行业标准和最佳实践，以确保网络安全人才实战化培养的有效性和针对性。

2）培养方式的基本要求主要有：

a) 实训平台。建立网络安全实训平台，为学员提供实战演练的场所和工具，让学员在真实环境中进行学习和实践。

b) 校企合作。高校与企业合作，共同制定培养方案，开展实习实训，将理论与实践相结合，提高学员的实战能力。

c) 竞赛活动。组织网络安全竞赛活动，激发学员的学习兴趣和热情，提高学员的实战能力和团队协作能力。

3）培养标准的基本要求主要有：

网络安全人才实战化培养应遵循国家标准和网络安全要求，确保培养出的网络安全人才具备高度实战能力和综合素质。同时，还应根据行业发展和市场需求，不断更新和完善培养方案和标准，确保培养出的网络安全人才能够适应行业发展和市场需求。

4）培养效果评估的基本要求主要有：

为了确保网络安全人才实战化培养的效果，应建立科学、全面的评估体系。通过定期对学员的理论知识、技能掌握程度、实战能力等方面进行评估，及时发现问题并进行改进。确保培养出的网络安全人

才掌握网络安全基本理论和前沿技术，熟悉网络安全攻防策略和方法，提升网络安全事件应急响应和处置能力，培养团队协作和沟通能力，形成网络安全防护综合素质。

4.2 网络安全人才实战化岗位的基本要求

通过对专业岗位的分析，信息安全人才类的目标岗位有：网络安全运营工程师、安全产品工程师、售前技术工程师、渗透测试工程师、应急响应工程师、安全服务工程师。发展岗位有：产品专家、咨询顾问、漏洞挖掘；迁移岗位有产品经理、项目经理等。

基于一般的网络安全实践和对人才能力的普遍要求，以下是一些网络安全人才实战化岗位的要求：

1）技术能力的基本要求主要有：

a) 熟练掌握网络安全基础知识，如 TCP/IP 协议、操作系统安全、数据加密等。

b) 熟悉常见的网络安全威胁和攻击手段，具备对安全事件进行快速响应和处置的能力。

c) 熟练使用各种网络安全工具和技术，如渗透测试工具、漏洞扫描工具、防火墙、入侵检测系统等。

2）实战经验的基本要求主要有：

a) 具备丰富的网络安全实战经验，能够独立完成安全事件的调查、分析和处置工作。

b) 参与过实际的网络安全项目或攻防演练，具备在复杂环境中解决安全问题的能力。

3）沟通能力的基本要求主要有：

a) 具备良好的沟通能力，能够与技术团队、业务部门和管理层进行有效的沟通，传达安全信息和风险。

b) 具备撰写安全报告、安全策略、安全培训等文档的能力。

4）团队协作能力的基本要求主要有：

a) 能够与团队成员协作，共同完成安全任务，分享安全知识和经验。

b) 在团队中扮演不同的角色，如安全分析师、安全顾问、安全管理员等。

5）持续学习的基本要求主要有：

a) 具备持续学习的能力，能够跟踪最新的网络安全技术和威胁动态，不断提升自己的安全能力。

b) 积极参加安全培训、研讨会等活动，与同行交流学习。

6）职业操守的基本要求主要有：

a) 遵守职业道德和法律法规，保护客户隐私和敏感信息。

b) 遵循安全最佳实践，确保网络系统和数据的安全性。

7）认证与资质的基本要求主要有：

a) 持有相关的网络安全认证证书，如 CISP、CISSP、PMP 等。

b) 具备特定的技术资质或认证，如渗透测试工程师、安全分析师等。

4.3 网络安全人才实战化知识结构的要求

网络安全人才实战化知识结构的要求通常涵盖多个方面，以确保他们具备全面的网络安全知识和能力。其基本要求为：

1）基础理论知识的基本要求主要有：

a) 深入理解计算机网络原理、TCP/IP 协议族、操作系统原理等基础知识。

b) 掌握数据加密、身份认证、访问控制等安全机制的基本原理。

2）网络安全技术知识的基本要求主要有：

a) 精通防火墙、入侵检测系统（IDS/IPS）、安全信息和事件管理（SIEM）等安全设备的工作原理和配置方法。

b) 熟悉网络攻击技术和防御策略，包括漏洞利用、恶意软件分析、网络钓鱼等。

c) 掌握安全漏洞评估、渗透测试、代码审计等安全评估技术。

3）安全管理与策略的基本要求主要有：

a) 理解网络安全管理框架和最佳实践，如 ISO 27001、NIST 网络安全框架等。

b) 掌握制定和执行安全策略、安全标准和安全流程的方法。

c) 了解风险管理和业务连续性规划的基本概念。

4）安全管理与策略的基本要求主要有：

a) 熟悉国内外网络安全法律法规，如《网络安全法》、《数据安全法》等。

b) 了解隐私保护、数据出境安全评估等合规要求。

5）编程与脚本能力的基本要求主要有：

a) 至少熟悉一门编程语言，如 Python、C/C++、Java 等，能够编写安全相关的脚本和工具。

b) 理解自动化和脚本化在网络安全领域的应用。

6）实战经验与案例分析的基本要求主要有：

a) 具备网络安全事件响应、安全漏洞管理、渗透测试等实战经验。

b) 了解和分析网络安全事件的案例，学习攻击者的手法和防御策略。

7）持续学习与自我提升的基本要求主要有：

a) 跟踪网络安全领域的最新动态和技术发展，如新的攻击手法、新的防御技术等。

b) 参加网络安全培训和研讨会，不断提升自己的专业能力和技术水平。

5 网络安全人才实战化训练环境建设的基本要求

5.1 总则

网络安全人才实战化训练环境建设的准则（以下简称：训练环境建设）的安全准则应遵守《信息安全技术 信息技术产品供应方行为安全准则》（GB/T 32921-2016），还应具备如下基本要求。

5.2 基本要求

网络安全人才实战化训练环境建设旨在通过构建真实、高效、可持续的训练环境，提升网络安全人才的实战能力，为应对日益复杂的网络安全挑战提供有力支持。本标准的制定遵循团体标准的编制要求，确保客观性、适用性、可操作性、可验证性、法律合规性、可持续性、可信度和透明度的原则。网络安全人才实战化训练环境建设基本要求有：

a) 实战性要求。训练环境应能够模拟真实的网络安全场景，包括网络攻击、入侵检测、应急处置等环节，使参训人员能够在实践中学习和掌握网络安全技能。

b) 先进性要求。训练环境应采用最新的网络安全技术和工具，确保训练内容与行业前沿保持同步。同时，应支持多种训练模式和场景，以满足不同层次和需求的网络安全人才培养。

c) 安全性要求。训练环境应具备完善的安全保障机制，确保参训人员在训练过程中不会泄露敏感信息或造成实际损害。此外，训练环境应定期进行安全检查和漏洞修复，以确保其安全性得到持续保障。

d) 可扩展性要求。训练环境应具备良好的可扩展性，能够随着网络安全技术的发展和人才培养需求的变化进行升级和扩展。这包括硬件设备的升级、软件系统的更新以及训练场景的增加等。

e) 规范性要求。训练环境的建设应符合国家和行业的相关标准和规范，确保训练过程的合规性和规范性。同时，应建立健全的管理制度和操作流程，以确保训练环境的有序运行和高效利用。

f) 协作性要求。训练环境应支持多人协作和团队作战，促进参训人员之间的交流和合作。通过团队协作训练，提升参训人员的团队协作能力和整体战斗力。

5.3 网络安全人才实战化训练环境建设框架

网络安全人才实战化训练环境建设管理框架，首先应确定实战化训练环境建设内容；其次应明确实战化训练环境建设的要求；第三应明确实战化训练环境建设的安全准则；最后应有高效的实战化训练环境建设管理的组织结构。网络安全人才实战化训练环境管理建设框架如图3所示。网络安全人才实战化训练环境技术建设框架如图4所示。

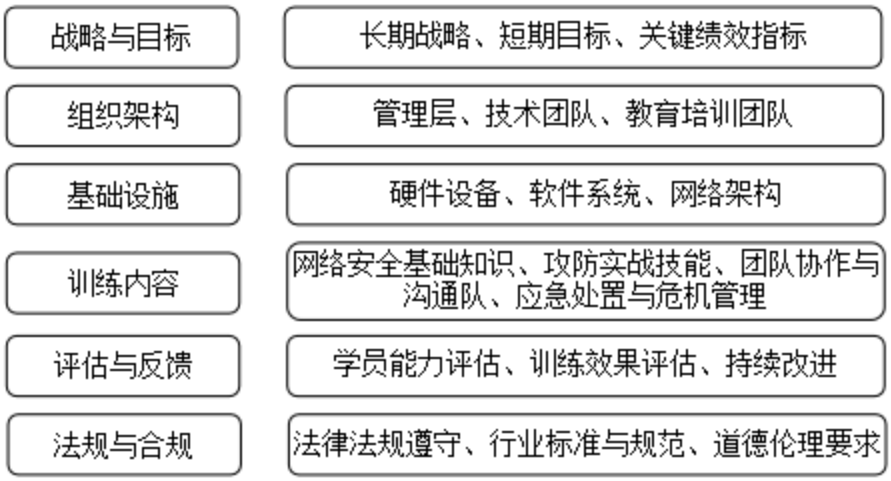

图 3　网络安全人才实战化训练环境管理建设框架

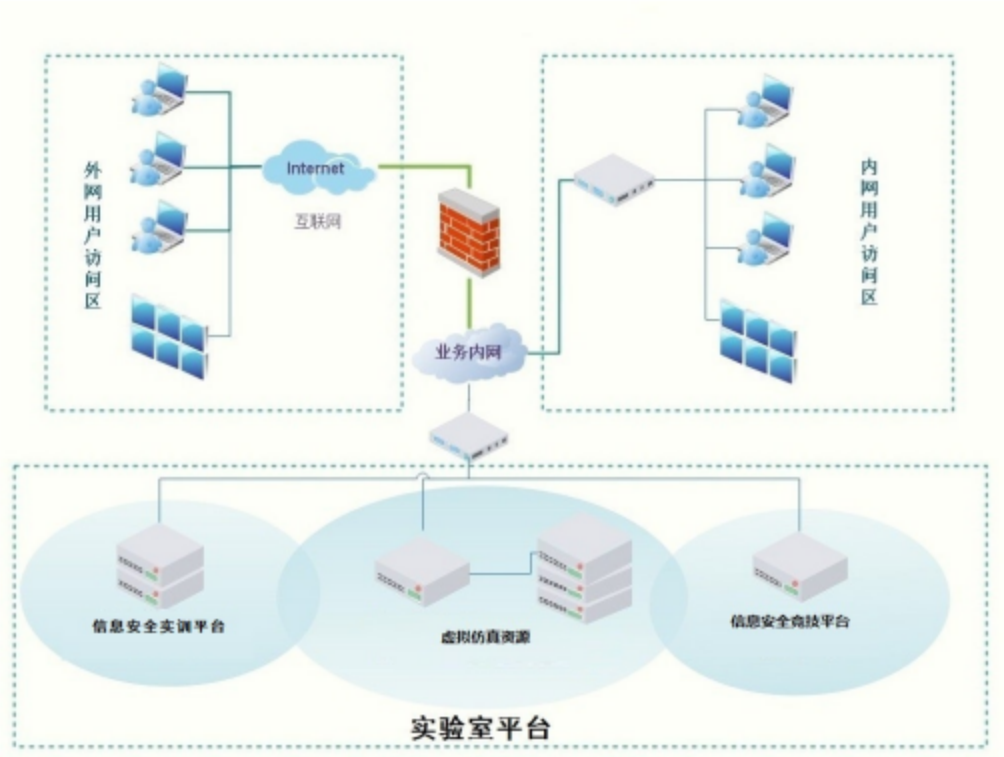

图4　网络安全人才实战化训练环境技术建设框架

5.4　网络安全人才实战化训练环境建设内容

网络安全人才实战化训练活动中的教学应用和系统运行情况进行训练环境建设，环境建设的选取应参考《信息技术服务 分类与代码》（GB/T 29264-2012）、《信息安全技术　信息系统安全等级保护实施指南》(GB/T 25058-2019)、《信息技术　安全技术　信息安全管理体系审核指南》(GB/T 28450-2020)

中适用于网络安全人才实战化训练活动的内容，环境建设的内容包括：实训设施建设、教学内容设计、师资队伍建设、教学资源建设、管理机制建设等。

1）实训设施建设：

a) 网络攻防实训室。建设专门用于网络安全攻防实战演练的实训室，包括高性能服务器、网络设备（如防火墙、交换机、路由器等）、安全设备（如入侵检测系统、安全审计系统等）等。

b) 虚拟网络环境。构建与真实网络环境相似的虚拟网络环境，用于模拟各种网络安全场景和攻击行为，让学员在虚拟环境中进行实战化训练。

c) 实训终端和工作站。提供一定数量的高性能实训终端和工作站，供学员进行实训操作、模拟攻防、日志分析等。

2）教学内容设计：

a) 网络安全基础知识。包括网络协议、操作系统安全、密码学基础、网络安全法律法规等。

b) 攻防实战技能。包括网络扫描、漏洞挖掘、渗透测试、恶意代码分析、应急响应等实战技能。

c) 团队协作与沟通。培养学员在网络安全领域的团队协作能力和沟通技巧，如项目分工、进度管理、信息共享等。

d) 应急处置与危机管理。教授学员如何快速响应网络安全事件，制定应急预案，进行危机管理和恢复工作。

3）师资队伍建设：

a) 对教师进行定期培训和考核，更新其知识和技能，保持与行业发展同步。

b) 鼓励教师参与网络安全领域的科研项目和实践活动，提高其专业素养和实践能力。

4）教学资源建设：

a) 教材与教辅材料。编写或选用符合实战化训练要求的教材和教辅材料，包括理论教学资源、实训手册、案例库等。

b) 在线课程与资源。开发或引入优质的在线课程和资源，供学员自主学习和补充知识。

c) 实训案例库。建立实训案例库，收录各种典型的网络安全案例和攻防实战场景，供学员参考和学习。

5）管理机制建设：

a) 制定实训环境的管理制度和使用规范，确保实训环境的正常运行和有效管理。

b) 建立实训效果的评估机制，对学员的实训成果进行定期评估和反馈，指导其改进和提高。

c) 加强与企业和行业的合作与交流，了解行业需求和动态，及时调整和优化实训环境建设内容和方案。

6 网络安全人才实战化训练环境设施的基本要求

6.1 总则

网络安全人才实战化训练环境设施主要有：实训场所面积、硬件设施要求、软件设施要求、实训内容要求、其他要求等。

6.2 实训场所的基本要求

网络安全人才实战化训练场所的基本要求有：

a) 应确保实训场所的物理安全，如安装门禁系统、监控摄像头等，防止未经授权的人员进入实训场所。

b) 应对实训场所的网络环境进行隔离和保护，防止外部攻击和恶意入侵。

c) 应制定严格的安全管理制度和操作规程，确保实训过程中的安全可控。

d) 实训室面积和布局。实训室面积应保证教学基本要求、或满足多小组同时使用的需求，保证学生的技能训练效果。实训室布局应合理、宽敞、明亮，便于学生操作和交流。如：学生可以以岛形台的形式成组学习，两侧墙壁挂有显示器，用于同步显示教师教学内容，标准配置可容纳40人同时上课。

e) 实训室环境。实训室环境应整洁、安静、舒适，确保学生在实训过程中能够保持良好的学习状态。同时，实训室应具备良好的通风和照明条件，保障学生的健康和安全。

6.3 实训室平面布局要求

实训室平面布局可根据实训室的设计进行，确保教学的正常开展。如实训室平面布局结构图如图5所示。

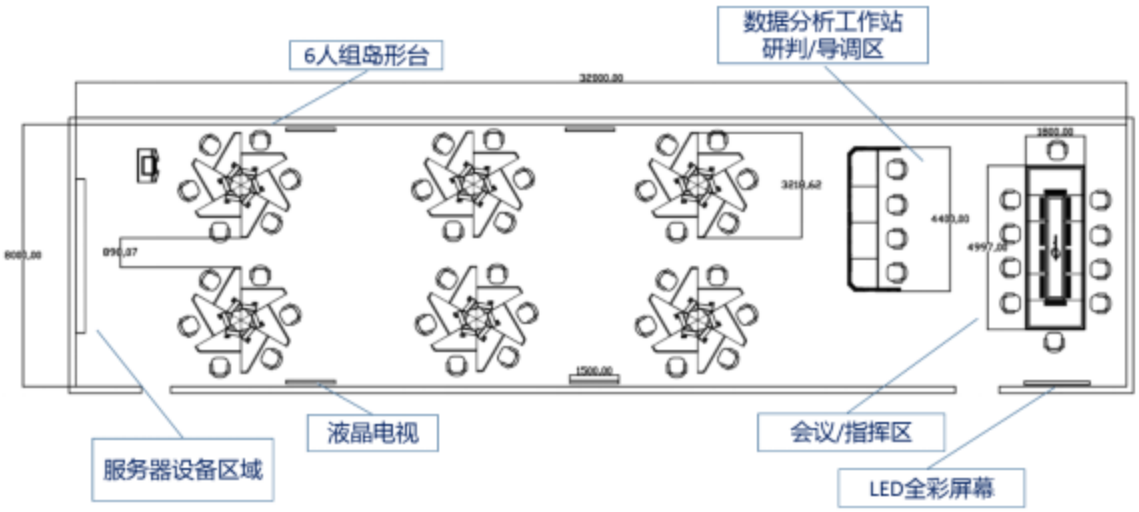

图5 实训室平面布局结构图

6.4 实训室网络逻辑布局要求

网络安全人才实战化的实训环境均为B/S结构。实训室连线布局时，只需保证网络通畅即可。只需学生在客户端使用浏览器访问，无特殊访问需求和特殊协议支持需求。

为了实训逻辑清晰，每一组岛台配备一个机柜。机柜中主要包含安全硬件设备、数通连接设备和管理控制设备。如实训室网络逻辑布局结构图如图6所示。

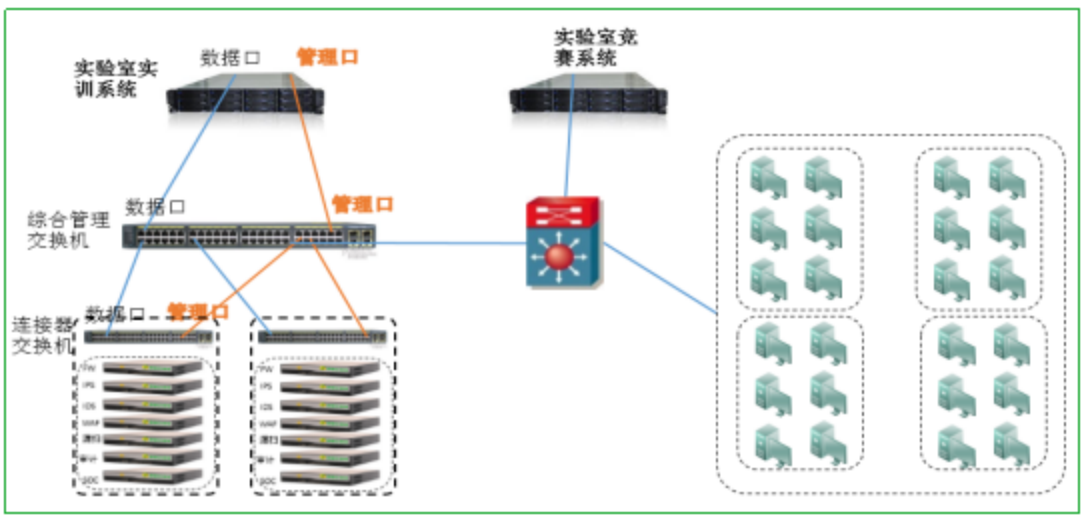

图6 实训室网络逻辑布局结构图

6.5 实训室硬件设施的基本要求

网络安全人才实战化实训室硬件设施的基本要求有：

a) 计算机设备。购置高性能计算机，配置主流的操作系统和网络安全软件，确保实训环境的稳定性和高效性。同时，应考虑到未来技术的升级和扩展需求，计算机设备应具有良好的可扩展性和兼容性。

b) 网络设备。建设完整的网络环境，包括交换机、路由器、防火墙等关键网络设备。网络设备应能够反映当前主流网络技术，配置灵活、可扩展性好、支持协议类型丰富，满足最新网络安全技术的攻防演练需求。

c) 实训工具。购置网络安全实训器材，如网络流量分析仪、安全扫描仪等，用于进行网络安全实训和演练。这些工具应能够模拟真实网络环境中的各种攻击和防范手段，帮助学生熟悉和掌握网络安全技能。

6.6 实训室软件平台的基本要求

网络安全人才实战化实训室软件平台的基本要求有：

a) 操作系统。安装多个常用的操作系统，如 Windows、Linux、鸿蒙、麒麟、Mac OS 等操作系数，以便学员能够熟悉不同平台下的网络安全操作。同时，应确保软件平台的稳定性和安全性，避免因为软件漏洞导致实训环境受到攻击。

b) 虚拟化技术。使用虚拟化技术建立虚拟网络环境，以提供更多的网络安全演练机会。虚拟化技术应具有良好的性能和可靠性，支持多种操作系统和应用软件的部署和管理。

6.7 实训内容的基本要求

网络安全人才实战化实训内容的基本要求有：

a) 网络安全基础理论与技术。网络安全概念与原理，加密与解密技术，网络安全协议与标准，操作系统与网络安全，网络攻击与防御技术。

b) 网络安全攻防实战。网络扫描与漏洞发现，渗透测试与漏洞利用，恶意代码分析与防护，拒绝服务攻击与防御，社交工程与网络钓鱼防范。

c) 网络安全事件应急响应。网络安全事件分类与识别，应急响应流程与策略，数据备份与恢复技术，网络安全事件报告与处置，网络安全事件后评估与总结。

d) 网络安全管理与法律法规。网络安全管理体系与标准，网络安全风险评估与控制，网络安全法律法规与政策，网络安全合规性检查与审计，网络安全伦理与职业道德。

e) 网络安全团队协作与沟通。网络安全团队组织与建设，网络安全情报收集与分析，网络安全攻防演练与协作，网络安全沟通与报告技巧，网络安全文化建设与推广。

6.8 实训室训练的基本方法

网络安全人才实战化实训室训练的基本要求有：

a) 理论教学。通过讲座、课程、教材等方式，传授网络安全基础理论与技术；

b) 实战演练。组织网络安全攻防实战、应急响应等模拟演练，提升实战能力；

c) 案例分析。分析典型网络安全事件案例，总结经验教训，提高防范意识；

d) 团队协作。加强网络安全团队协作与沟通训练，提升整体防护能力；

e) 竞赛与创新。组织网络安全竞赛、沙龙及相关的创新创业等活动，激发学习兴趣和创新精神。

6.9 实训室其他要求

网络安全人才实战化实训室的其他要求有：

a) 实训室面积和布局。实训室面积应满足多小组同时使用的需求，保证学生的技能训练效果。实训室布局应合理、宽敞、明亮，便于学生操作和交流。
b) 实训室环境。实训室环境应整洁、安静、舒适，确保学生在实训过程中能够保持良好的学习状态。同时，实训室应具备良好的通风和照明条件，保障学生的健康和安全。
c) 实训室管理。实训室应建立完善的管理制度和安全规定，确保实训设施的正常运行和实训过程的安全有序。同时，实训室应配备专业的管理人员和技术支持人员，为学生提供及时的技术指导和帮助。

7 网络安全人才实战化训练平台系统的基本要求

7.1 总则

网络安全人才实战化训练平台系统应满足功能要求、技术要求、用户体验要求以及管理与安全要求。这些要求有助于构建一个高效、稳定、安全、易用的实战化训练平台，为网络安全人才的培养提供有力支持。

7.2 平台系统的结构图

网络安全人才实战化训练平台系统的结构图如图7所示。

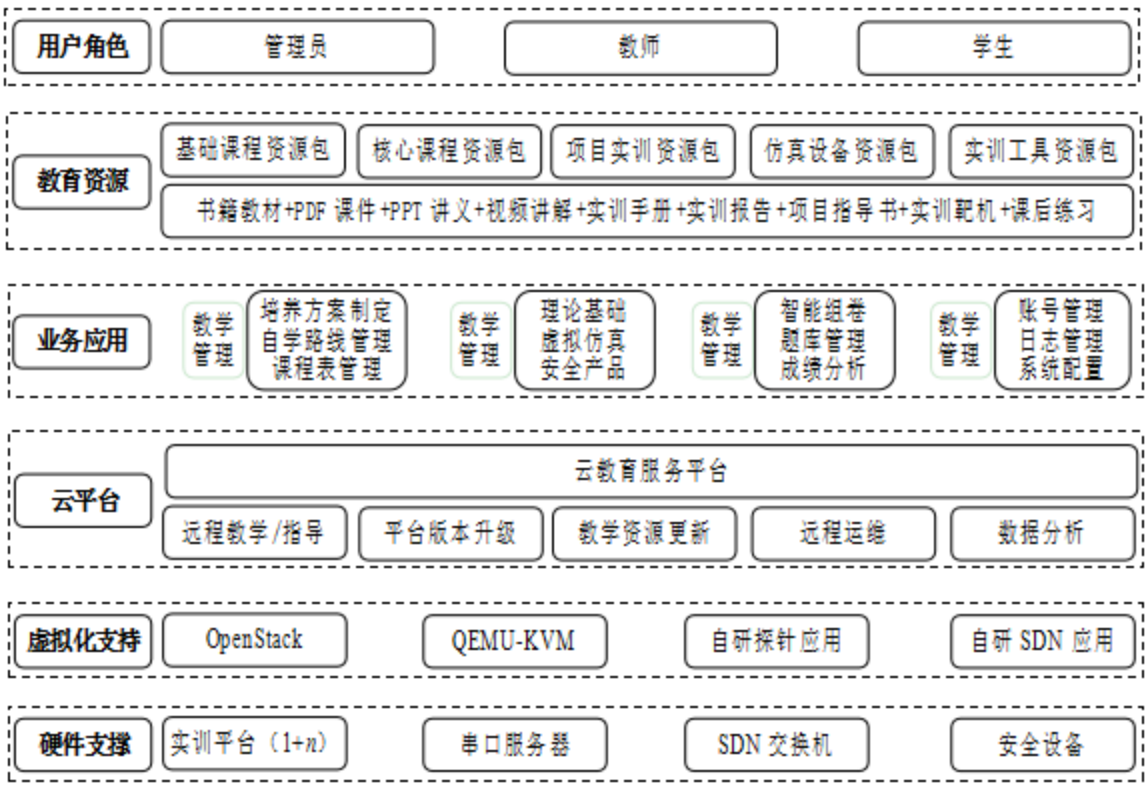

图7 实训室平台系统结构图

7.3 实战化训练平台系统的功能要求

网络安全人才实战化训练平台系统的功能要求有：

a) 仿真环境。平台应提供高度仿真的网络环境，模拟真实世界中的网络架构、设备、应用和服务。这种仿真环境应能够支持各种网络攻击和防御手段的模拟，包括但不限于 DDoS 攻击、SQL 注入、跨站脚本攻击等。
b) 实战演练。平台应支持实战化的网络攻防演练，包括个人和团队的训练模式。在演练中，学员应能够模拟攻击者进行渗透测试，或者作为防御者进行安全加固和应急响应。
c) 自动化评估。平台应能够对学员的实战演练进行自动化评估，包括评估学员的攻击能力、防御能力和团队协作能力等。评估结果应能够及时反馈给学员，帮助他们了解自己的优点和不足。

7.3 技术要求

网络安全人才实战化训练平台系统的技术要求有：

a) 稳定性。平台应具备高度的稳定性，能够支持长时间的实战演练和大量用户的同时访问。在运行过程中，平台应能够自动检测和修复故障，确保服务的连续性。
b) 安全性。平台应确保自身的安全性，防止被攻击者利用漏洞进行攻击。同时，平台应能够监控和记录学员的实战演练过程，防止恶意行为的发生。
c) 可扩展性。平台应具备良好的可扩展性，能够根据实际需求进行功能扩展和性能提升。例如，可以增加新的仿真环境、攻击手段和防御手段等。

7.4 用户体验要求

网络安全人才实战化训练平台系统的用户体验要求有：

a) 易用性。平台应具备简洁明了的用户界面和操作流程，方便学员快速上手和使用。同时，平台应提供详细的帮助文档和技术支持，帮助学员解决在使用过程中遇到的问题。
b) 互动性。平台应支持学员之间的交流和互动，例如在线讨论、分享经验等。这种互动性有助于学员之间的学习和成长，提高实战训练的效果。
c) 反馈机制。平台应建立有效的反馈机制，收集学员对平台的意见和建议。这些反馈可以帮助平台不断完善和优化功能和服务，提高用户体验和满意度。

7.5 管理与安全要求

网络安全人才实战化训练平台系统的管理与安全要求有：

a) 权限管理。平台应建立完善的权限管理机制，确保不同用户只能访问其权限范围内的功能和数据。这有助于保护平台的敏感信息和防止未经授权的访问。
b) 数据安全。平台应确保学员数据的安全性，防止数据泄露和非法获取。在数据存储和传输过程中，应采取加密等安全措施来保护数据的机密性和完整性。
c) 监控与审计。平台应建立监控和审计机制，对学员的实战演练过程进行实时监控和记录。这有助于发现潜在的安全问题和违规行为，并采取相应的处理措施。

8 网络安全人才实战化对抗赛的基本要求

网络安全人才实战化对抗赛系统结构图如图 8 所示。

8.1 对抗赛管理的基本要求

竞赛管理层作为平台竞赛管理核心，负责平台中竞赛功能化管理。包含题库管理、竞赛组织、比赛监控、防作弊及成绩管理五个部分。其中：

a) 题库管理。主要针对竞技系统中的题目录入、题目增、删、改、查等操作，完成竞技系统中的题目管理功能。

图8　网络安全人才实战化对抗赛系统结构图

b) 竞赛组织。主要进行竞赛系统的赛事添加、赛事组织管理、队伍组织等竞赛组织相关功能。
c) 比赛监控。主要针对赛事情况进行全方位的监控，同时具备一系列比赛监控管理功能，做到赛事情况一览便知，清晰化赛事情况。
d) 防作弊。赛事作弊情况监控，防止发生参赛人员作弊问题（如恶意关闭靶机操作）。
e) 成绩管理。针对赛事情况进行成绩统计、成绩排名等成绩管理操作。
f) 用户管理。平台全方位管理：管理监测安全竞技系统整体的运行状态，节点管理，和登陆日志。
g) 人员及队伍管理。多维度人员管及竞技队伍理方式，管控操作更便捷灵活。

8.2 竞赛管理的基本要求

竞赛管理功能位于产品架构中的竞赛管理层，主要用于赛事中，裁判人员对赛事的管理及控制，竞赛管理主要分为四个模块：竞赛设置、竞赛题目、竞赛监控、竞赛管理。网络安全人才实战化训练对抗赛竞赛管理的基本要求有：

a) 竞赛设置。主要针对赛事的开始时间及结束时间进行设置，提供开始、暂停设置功能，以及加减分设置及公告设置。
b) 竞赛题目。主要针对赛事中的题目进行设置，裁判人员可针对本场比赛情况，对赛事题库进行题目的管理操作。
c) 竞赛监控。针对赛事防作弊、竞赛情况进行监控操作。
d) 竞赛报表。可查看目前赛事排名情况、得失分情况一览表、赛事系统运行报表等竞赛报表信息。

8.3 场景仿真的基本要求

采用基于内核的虚拟化技术作为底层，自主研发了虚拟化管理平台软件。管理引擎向计算资源发送控制指令，存储中的信息按需调入计算资源的内存中运算。计算资源被看做是统一的虚拟资源池，随着使用用户数的提升，只需增加计算资源便可满足更高人数和要求的攻防演练。通过先进的架构，进行场景仿真模式底层设计，支持虚拟机管理（虚机上传及仿真等操作）、网络划分（赛事实训场景网络拓扑划分）、访问控制（赛事环境访问控制）、拓扑生成、拓扑监控（赛事拓扑情况监控）一系列功能操作。

8.4 竞赛展示的基本要求

针对信息安全竞技赛事特点，竞赛展示层提供赛事的 3D 大屏展示及直播。运用先进的科技风竞赛展示设计，使赛事更具参与感及沉浸感。

同时，基于赛事风格定制，网络安全人才实战化训练具有专业团队，可为用户量身定制赛事风格、赛事展示、赛事设计等一条龙赛事定制化服务。

8.5 初赛的基本要求

以团队或个人方式在线上进行，共分为两个部分，分别为选择题、渗透攻防题。

1）选择题内容的要求

选择题主要根据企业日常运维及工作需要，考察选手日常的安全意识、安全运维及安全攻防等技能，分为单选题、多选题，涉及安全管理、安全体系模型、安全设计运维、物理安全、网络安全、系统安全、应用安全、数据安全、密码学、恶意代码、移动终端安全、安全工具等多个方向，网络安全竞技平台内置题目1400多道。

2）渗透攻防题内容的要求

渗透攻防题以实战为主，包含常见的SQL注入、跨站脚本攻击（XSS）、文件包含、上传漏洞、解析漏洞、弱口令、命令执行漏洞、数据库提权、操作系统远程溢出漏洞等，每个类型设置X道题。

8.6 决赛的基本要求

经过线上选拔赛（初赛），选拔出多支队伍进行决赛，决赛设计和混战模式。

决赛设计

设置好比赛时间和靶机环境，每支队伍有各自的靶机，比赛开始后可预先对自己的靶机进行加固，加固完成后进入混战模式（还可以继续加固）。

混战模式

在攻防兼备混战比赛中，选手需要加固自己防守的靶机，同时攻击对方的靶机。如比赛初始分值为X，攻陷对方一台靶机并获得KEY值提交得X分，被对方攻破丢失X分。比赛KEY值每10分钟变换一次。

8.7 题库管理的基本要求

题库管理提供丰富的题目数量展示，及题库的综合化管理。

题目分类清晰多样。题目类型丰富，多类型题目展示分类明确清晰，同时支持管理员自定义题目分类设定。分类中，适用者分类通常按照题目对参考人员的难易度划分，默认的包括基础知识、基础技能、专业技术和专业管理。

系统内置的题库，应支持攻防题、公共题、CTF（Capture the Flag）题、选择题等四种类型，并支持用户自行增删改查。

1）基础知识竞赛资源。内置1000个选择题，包含基本能力测评、安全工具、安全模型体系、安全管理、安全设计运维、密码学、应用安全、恶意代码、数据安全、法律法规、渗透Web、物理安全、系统安全、终端安全、网络安全等相关知识，适用于海选比赛。

2）CTF夺旗竞赛赛题资源。如至少内置150道CFT题目，应包含CRYPTO、Stega、MISC、WEB、PWN、Reverse等相关题目。

3）攻防混战（Attack-Defensive Melee）赛题资源。如至少内置20道攻防混战赛题，主要用于组织攻防混战竞赛，可以多个队伍互相攻防渗透，分别统计各队成绩。

4）目前各类赛事题目支持根据用户需求进行定制。

9 网络安全人才实战化师资队伍的基本要求

9.1 总则

为满足国家网络安全战略需求，提升网络安全人才的实战能力，培养具备高度专业素养和实战经验的网络安全师资队伍至关重要。该基本要求根据国家相关标准和政策，明确了网络安全人才实战化师资队伍的基本条件和能力要求。网络安全人才实战化师资队伍的能力结构如图9所示。

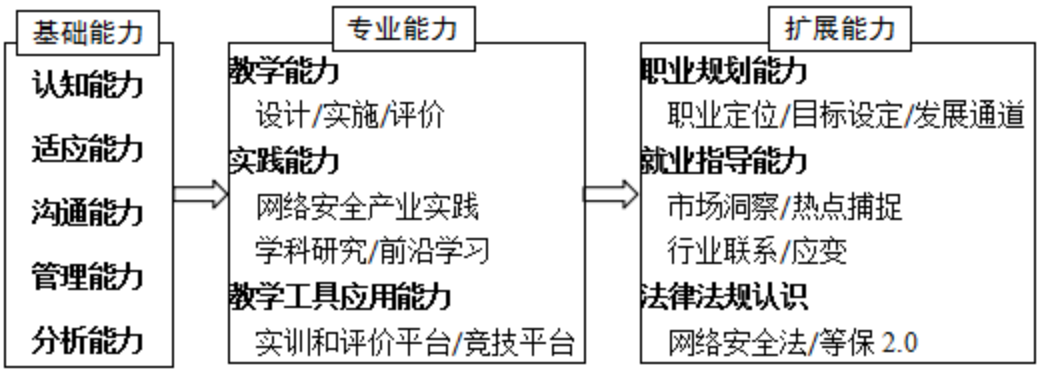

图9　网络安全人才实战化师资队伍的能力结构图

9.2　基本要求

网络安全人才实战化师资队伍的基本要求有：

a) 专业知识与技能。具备深厚的网络安全理论基础，熟悉网络安全前沿技术和发展趋势，熟练掌握网络安全攻防技术，包括网络扫描、渗透测试、恶意代码分析、应急响应等，具备网络安全事件分析、处置和报告的能力，能够独立或带领团队应对网络安全威胁。

b) 实战经验。具有丰富的网络安全实战经验，包括参与网络安全攻防演练、应急响应、安全评估等实际项目，了解网络安全行业的最新动态和最佳实践，能够将实战经验融入教学之中。

c) 教学能力。具备良好的教学能力和教学方法，能够针对不同学员的特点和需求，制定个性化的教学计划和教学方案；善于运用多种教学手段和工具，提高教学效果和学员的学习兴趣；能够进行课程开发和教材编写，不断更新和完善教学内容。

d) 团队协作与沟通能力。具备良好的团队协作和沟通能力，能够与团队成员有效合作，共同完成任务；能够与学员建立良好的师生关系，有效沟通和指导学员的学习和实践；能够与行业内外专家、企业和机构建立联系，促进知识交流和资源共享。

e) 职业道德与操守。遵守职业道德规范，保守国家和企业的机密信息，维护网络安全和信息安全；秉持公正、客观、诚实的原则，不参与任何违法违规的网络活动；尊重知识产权，不侵犯他人的知识产权和利益。

f) 持续学习与自我提升。具备持续学习和自我提升的意识，关注网络安全领域的最新技术和研究成果；积极参加专业培训、学术交流等活动，不断提升自身的专业素养和实战能力；鼓励学员进行自主学习和实践，引导学员树立正确的网络安全观念和价值观。

10　网络安全人才实战化训练环境建设的考核体系

10.1　总则

为全面评估网络安全人才的实战能力，确保网络安全人才符合行业要求，应满足网络安全人才实战化考核原则。考核原则旨在明确考核的目标、内容、方法和标准，确保考核的公正性、客观性和有效性。

10.2 网络安全人才实战化考核原则

网络安全人才实战化考核原则主要有：

a) 全面性与实战性相结合。考核内容应全面涵盖网络安全人才的理论知识、技能操作和实战经验，突出实战性，确保网络安全人才具备解决实际问题的能力。

b) 理论与实践相结合。考核不仅要关注理论知识的掌握程度，更要注重实际操作能力和实践经验的考核，确保网络安全人才能够将理论知识应用于实际工作中。
c) 客观性与公正性。考核过程应客观公正，采用标准化的考核方法和评分标准，确保考核结果的准确性和可靠性。同时，应建立监督机制，防止任何形式的作弊和违规行为。
d) 注重过程与结果相结合。考核不仅要关注最终结果的达成情况，还要注重过程中的表现和努力程度。对于在考核过程中表现出色但结果稍有欠缺的网络安全人才，应给予适当的肯定和鼓励。
e) 持续改进与适应性。考核标准和内容应根据国家标准、行业发展和技术进步的要求进行持续改进和更新。同时，考核应具有一定的灵活性，能够适应不同领域、不同岗位的网络安全人才需求。
f) 安全性与保密性。在考核过程中，应严格遵守网络安全相关法律法规和保密要求，确保考核过程的安全性和保密性。对于涉及敏感信息和核心技术的考核内容，应采取相应的安全措施和保密措施。

10.2 网络安全人才实战化考核内容与方法

网络安全人才实战化考核内容与方法主要有：

a) 理论知识考核。通过考试、测试等方式，考核网络安全人才的网络安全基础理论知识掌握程度；
b) 技能操作考核。通过模拟环境、实训平台等方式考核网络安全人才的技能操作能力，包括网络扫描、渗透测试、恶意代码分析、应急响应等。
c) 实战经验考核。通过项目实践、案例分析等方式考核网络安全人才的实战经验，包括参与网络安全攻防演练、应急响应等实际项目的表现。
d) 团队协作与沟通能力考核。通过团队协作任务、沟通汇报等方式考核网络安全人才的团队协作与沟通能力，包括与团队成员的协作配合、与上级和客户的沟通汇报等。
e) 综合素质评价。综合考虑网络安全人才的理论知识、实战能力、团队协作与沟通能力等方面，进行综合评价。

10.3 网络安全人才实战化考核标准与结果

a) 考核标准。根据国家标准和行业要求，制定明确的考核标准和评分标准，确保考核结果的准确性和可靠性。
b) 考核结果。根据考核标准和评分标准，对网络安全人才的各项考核内容进行评分和综合评价，形成最终的考核结果。考核结果应作为人才选拔、培训和晋升的重要依据。

10.4 网络安全人才实战化评审组织机制

为规范网络安全人才实战化的评审工作，确保评审的公正性、客观性和有效性，特制定网络安全人才实战化评审组织机制。评审组织机制旨在明确评审的目标、组织架构、评审流程以及监督管理等方面，为网络安全人才实战化评审提供指导和支持。

1）评审目标

网络安全人才实战化评审旨在全面评估网络安全人才的实战能力，包括理论知识、技能操作、实战经验以及团队协作与沟通能力等方面，确保网络安全人才符合国家标准和行业要求。

2）组织架构

a) 评审委员会。设立评审委员会，负责网络安全人才实战化评审的组织、指导和监督工作。评审委员会成员应具备丰富的网络安全经验和专业知识，并具备高度的公正性和客观性。
b) 评审专家组。根据评审需求，组建由网络安全领域专家组成的评审专家组，负责具体的评审工作。评审专家组应根据评审标准和要求，对网络安全人才的各项能力进行客观、公正的评审。

c) 评审工作组。设立评审工作组，负责评审工作的具体实施和协调。评审工作组应确保评审过程的顺利进行，并及时处理评审过程中出现的问题。

3）评审流程

a) 提交申请。网络安全人才向评审组织提交实战化评审申请，包括个人简历、实战经历、成果展示等相关材料。

b) 资格审查。评审工作组对提交的申请进行初步资格审查，确保申请人符合评审的基本条件。

c) 评审准备。评审专家组根据评审标准和要求，制定具体的评审方案和评分标准，并准备相应的评审工具和材料。

d) 实战评审。评审专家组对网络安全人才进行实战评审，包括理论知识测试、技能操作考核、实战经验评估以及团队协作与沟通能力考核等方面。评审过程中，评审专家组应确保评审的公正性、客观性和有效性。

e) 结果公示。评审结果经过审核后，向申请人公示，并接受社会监督。如有异议，申请人可在规定时间内提出申诉。

f) 颁发证书。经公示无异议的申请人，将获得网络安全人才实战化证书，作为其实战能力的证明。

4）监督管理

a) 评审过程监督。评审委员会应对评审过程进行全程监督，确保评审的公正性、客观性和有效性。对于发现的违规行为，应及时进行处理并追究责任。

b) 评审结果复核。评审结果应经过复核程序，确保评审结果的准确性和可靠性。对于存在争议的评审结果，应组织专家进行再次评审或仲裁。

c) 评审信息公示。评审过程、评审结果以及申诉处理情况等信息应及时公示，接受社会监督。对于社会关注的热点问题或重大事件，应主动回应并说明情况。

11 网络安全人才实战化实训室管理的基本要求

为确保网络安全人才实战化实训室的正常运行，提升网络安全人才的实战能力，依据国家标准和行业规范，特制定网络安全人才实战化实训室管理的基本要求。

11.1 实训室管理目标

实训室管理旨在创造一个安全、高效、规范的实训环境，为网络安全人才提供实战化训练的场所和条件，保障实训教学的质量和效果。

11.2 实训室管理的基本要求

a) 安全管理。实训室应建立严格的安全管理制度，明确安全责任人和安全操作流程；定期对实训室进行安全检查，确保设备、网络、电力等方面的安全稳定；对进入实训室的人员进行安全教育，增强安全意识，防止安全事故的发生。

b) 设备管理。实训室设备应按照国家相关标准进行配置，满足网络安全实战化训练的需求；建立设备台账，对设备进行编号、登记和维护，确保设备的完好率和可用性；定期对设备进行维护和保养，保持设备的正常运行状态。

c) 环境管理。实训室应保持整洁、安静、舒适的环境，确保实训人员能够集中精力进行实战化训练；控制实训室内的温度、湿度和光照等环境条件，以满足设备运行和人员实训的需求；对实训室进行定期清洁和消毒，防止细菌滋生和疾病传播。

d) 教学管理。制定实训教学计划，明确实训目标、内容、方法和考核标准；配备具有丰富教学经验和专业知识的实训教师，确保实训教学的质量和效果；建立实训教学档案，记录实训人员的实训情况、成绩和反馈等信息。

e) 实训过程管理。实训过程中应严格遵守实训操作规程和安全要求，确保实训过程的安全和顺利；实训教师应密切关注实训人员的实训情况，及时给予指导和帮助；实训结束后，实训人员应按照规定完成实训报告和成果展示等任务。
f) 资源管理。实训室应充分利用现有的资源，包括设备、软件、数据等，提高资源利用效率；鼓励实训人员积极参与资源开发和共享，促进实训资源的丰富和完善；定期对实训资源进行评估和更新，确保实训资源的时效性和实用性。
g) 保密与知识产权保护。实训室应建立严格的保密制度，保护实训过程中涉及的国家机密、商业机密和个人隐私等敏感信息；尊重知识产权，不得擅自复制、传播或使用他人的知识产权成果；鼓励实训人员进行创新研究和技术开发，保护其知识产权成果。

11.3 管理组织机构

管理的基本要求，由学校、二级学院（或专业）等共同参与及共同成立相应的组织结构。包括但不限于以下几个方面：

a) 依据工作的需要，建立学校、二级学院（或专业）的两级工作小组，其相关责任人为组长、专业负责人为副组长、专业教师以及组员若干名；
b) 制定事件的处理流程，并参照事件处理流程对工作小组成员分配不同的角色；
c) 建立学校、二级学院（或专业）的两级管理组织制度和沟通协调机制；
d) 建立完善的保障体系；开展网络安全人才实战化实训室巡查工作。

11.4 评价管理

1）评价目标

评价管理旨在确保实训室能够提供高质量、实战化的网络安全培训，提高学员的网络安全技能和综合素质，满足国家和社会对网络安全人才的需求。

2）评价标准

a) 硬件设施评价。评价实训室计算机设备、网络设备、实训工具等硬件设施的完善程度和先进性，确保能够满足网络安全实训和模拟演练的需求。
b) 软件平台评价。评价实训室安装的操作系统、安全工具、虚拟化技术等软件平台的稳定性和功能性，确保学员能够充分利用这些平台进行网络安全学习和实践。
c) 实训内容评价。评价实训内容的针对性、实用性和挑战性，确保实训内容能够紧密结合国家标准和网络安全要求，提高学员的实战能力。
d) 师资力量评价。评价教师团队的教学水平、实践经验和创新能力，确保教师团队能够为学员提供专业的指导和帮助。
e) 学员满意度评价。通过问卷调查、访谈等方式收集学员对实训室的意见和建议，了解学员对实训室的满意度和期望，为改进实训室提供依据。

3）评价方法

a) 定期检查。定期对实训室的硬件设施、软件平台、实训内容等进行检查，确保各项指标符合要求。
b) 专项评估。针对实训室的某个方面或某个环节进行专项评估，深入了解实训室的运行情况和存在的问题。
c) 学员反馈。通过学员的反馈了解实训室的教学效果和学员的满意度，及时调整和改进实训室的工作。

4）评价结果处理

a) 针对评价结果，及时制定改进措施，并明确责任人和完成时间。
b) 对改进措施进行跟踪和督查，确保各项措施得到有效执行。

c) 将评价结果和改进措施纳入实训室的管理档案，为今后的管理提供依据。

11.5 改进措施

评价管理是一个持续改进的过程，应根据评价结果和学员反馈不断调整和优化实训室的管理策略和工作流程，确保实训室始终保持高水平的教学质量和服务水平。至少应：

a) 建立管理监测改进机制；
b) 对不符合策划要求的行为进行总结分析；
c) 对未达成的指标进行调查分析；

参考文献

[1]《教育行业信息系统安全等级保护定级工作指南（试行）》的通知. 教育部，（教技厅函〔2014〕74号），2014年10月27日. http://www.moe.gov.cn/srcsite/A16/s3342/201410/t20141029_178343.html

[2] 中华人民共和国计算机信息系统安全保护条例. 国务院第147号令，2020年12月25日. http://www.gov.cn/zhengce/2020-12/25/content_5575080.htm

[3] 教育信息化2.0行动计划. 教育部，2018年4月13日. https://www.csdp.edu.cn/article/3838.html

[4] 中国教育现代化2035. 中共中央、国务院，2019年2月23日. http://www.gov.cn/xinwen/2019-02/23/content_5367987.htm

附　录：网络安全人才实战化训练环境建设的配置要求

序号	类别	设备名称	描述	备注
1	信息安全实训系统	计算设备	为实训系统提供虚机资源调度与分配,支持虚拟化安全设备的授权统一维护及管理。	
2		基础教学模块	提供对基础课程资源的统一管理与维护，支持课程的新建、修改以及分类管理功能，提供课程的类型标识，可以对课程公开程度进行设定。	
3		教学方案模块	支持教学方案的建设，支持用户以学期为主线，设置规划各学期的课程内容以及课程属性,支持以列表方式及时序图形式显示教学方案。系统的课程类型包含基础实训课程以及项目实训课程，均可以用于教学方案的组织。	
4		考试测评模块	提供基础题库，题库包含 WEB 安全、终端安全等多个方向的内容，同时系统支持用户自定义导入题目。系统支持智能组卷及手动组卷两种方式对试卷进行组织，题目选择从题库中选取。	
5		教学管理模块	提供课程表管理、教学事务查看、课程及成绩数据分析功能，提供系统日志查看功能。	
6		系统管理模块	支持学生账号及班级管理，支持逐个及批量导入，支持对用户状态的设置。	
7		用户授权	满足整个专业的用户数教学需求	
8	信息安全竞技系统	计算设备	内置虚拟化资源池服务环境以及资源调度算法,为竞技系统提供虚机计算资源。	
9		系统管理模块	提供账号、队伍、角色权限管理，并提供系统配置、审计日志、系统版本管理；	
10		竞赛管理模块	系统提供竞赛创建、竞赛中管理、竞赛结果导出、题库管理、工具管理、竞赛展屏。可支撑个人赛、团体赛 2 种参赛方式；理论赛、解题赛、攻防赛 3 种竞赛形式，并配有选择类题目。	
11		CTF 竞赛题库	题库题目包含 CRYPTO、MISC、WEB、PWN、Revers 方向，含 2CTF 题目，有详细解题思路;含攻防题目，有详细解题思路;	
12		训练管理模块	可支撑用户自主刷题，查看解题思路，并统计训练人次、通过率、训练题目分类、题目占比等数据。	
13	信息安全实训设施	防火墙课程资源包+实训设施	智慧防火墙系统及智慧防火墙课程资源包，包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
14		上网行为管理课程资源包+实训设施	上网行为管理系统及上网行为管理课程资源包 包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
15		终端安全课程资源包+实	终端安全管理系统及终端安全课程资源包 包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可	

		训设施	满足高校一个学期的理论和实训教学需求。	
16		WAF 课程资源包+实训设施	Web 应用防火墙系统及 WEB 应用防火墙（WAF）课程资源包包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
17		漏扫课程资源包+实训设施	漏洞扫描与防护系统及漏洞扫描课程资源包 包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
18		IPS 课程资源包+实训设施	入侵防御系统及入侵防御（IPS）课程资源包 包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
19		代码安全课程资源包+安全设备	代码卫士系统及代码安全课程资源包 包含课程大纲、教学 ppt、实训指导书、实训设施等丰富的教学及实操资源，可满足高校一个学期的理论和实训教学需求。	
20	虚实结合网络设备	SDN 交换机	48 口千兆三层 SDN 交换机	
21		串口服务器	串口服务器 8 口 RS232/422/485 机架式 220V	
22		二层接入交换机	48 口千兆二层可管理交换机	
23	计算机设备	台式机	各类台式计算机设备	
24		便携式计算机	各类笔记本、平板电脑等便携式相关设备	
25	各种教学应用设备	交互式一体机	具有显示、操作、触控交互、批注、绘画、网络接入机制及相关教学软件等信息化终端	
26		电子班牌	含班牌终端、智慧班牌综合管理平台、家长/教师 APP 等相关设备和软件	
27		学科信息化教学设备	包含各学科进行信息化教学的相关设备总称	
28	其它软硬件设备		中小学信息化教学、数字化教学发展过程中产生新的软硬件教学设备	