中国通信企业协会
通信网络安全专业委员会

网安专〔2020〕9号

关于举办“2020年全国电信和互联网行业网络安全管理职业技能竞赛（第九届）”选拔赛安排的通知

各省、自治区、直辖市通信管理局，信息通信行业（企业）协会，基础电信企业，互联网企业，网络安全企业,相关高等院校、职业院校（含技工院校）及有关单位：

按照中国通信企业协会和中国国防邮电工会全国委员会联合发布的《关于举办2020年全国电信和互联网行业网络安全管理职业技能竞赛（第九届）的通知》（通企〔2020〕62号文件）的相关要求，“2020年全国电信和互联网行业网络安全管理职业技能竞赛（第九届）”（以下简称“竞赛”）选拔赛将于11月6日举办。目前，中国通信企业协会通信网络安全专业委员会（以下简称“网络安全专委会”）正在积极推进选拔赛相关工作，现将选拔赛有关事项通知如下：

一、选拔赛安排

（一） 基础电信运营企业由各集团公司自行安排选拔赛；

（二） 各省、自治区和直辖市根据实际情况自行安排选拔赛；

（三） 对于未参加各省组织选拔赛的职工和在校学生可参加

由竞赛办公室统一组织的线上选拔赛，具体如下：

1. 报名时间：2020 年 10 月 23 日 09:00-11 月 3 日 18:00

2. 报名网站：https://cacenssc.bjbochum.com/

3. 选拔赛时间：2020 年 11 月 6 日 13:00-18:00

4. 选拔赛形式：采用团队线上模式，每个队伍 1 个账号，三名参赛队员共用 1 个账号。主要考察 5G 安全、云安全、AI 安全、IPv6 安全、IOT 安全、APP 安全、逆向、溢出、密码、取证、隐写、编程、代码审计、web 安全、应急等知识点，重点考核每支队伍整体的安全技术水平和能力，相关计分和比赛规则请见比赛考试网站。

二、参赛须知

1. 所有参赛人员须拥有唯一中国国籍（不含港澳台地区）

2. 职工类参赛选手须为企业正式合同制人员并连续工作六个月以上；

3. 已获得往届竞赛前 5 名且为职工身份的人员，不得以选手身份参赛；

4. 每支队伍需由三人组成，参赛队伍自行命名；

5. 结果公布：晋级结果将在安全专委会网站上（www.cace-ns.org.cn）进行公布。

三、联系方式：

竞赛办公室联系人：

王牧风 010-68094555

郝　强 010-68094558

竞赛QQ交流群：1158431411

邮箱：cacenssc@163.com

附件：竞赛大纲

中国通信企业协会通信网络安全专业委员会

2020年10月22日

附件：

竞赛大纲

【管理部分】

1. 法律

了解《网络安全法》主要内容，包括：网络运行安全、关键信息基础设施安全、网络信息安全、监测预警与应急处置等要求。

2. 法规

1) 了解《通信网络安全防护管理办法》（工信部令第 11 号）主要内容，包括：通信网络安全防护范围、管理主体、责任主体、同步要求、分级备案要求、符合性评测要求、风险评估要求、应急演练要求等内容。

2) 了解《电信和互联网用户个人信息保护规定》（工信部令第 24 号）主要内容，包括：用户个人信息的收集和使用规范要求、安全保障措施、责任和义务等内容。

3. 政策文件

1) 了解通信网络安全防护工作总体思路、基本原则、主要任务、实施及监督检查要求、安全服务机构管理等政策文件。

2) 熟悉通信网络安全防护定级范围、评审要求、备案等政策要求，熟悉通信网络单元安全防护定级方法、定级对象命名规则、定级报告内容、定级备案相关信息等。

3) 了解通信行业网络信息安全管理体系相关工作。

4. 通信网络安全防护标准

1) 熟悉各专业网络单元安全防护标准中技术要求内容。

2) 了解安全风险评估要素及关系、工作形式、不同生命周期要求和实施要点等要求。

3) 了解灾难备份原则、灾难备份资源要素、实施过程、灾难恢复预案等要求。

4) 了解安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等内容。

5) 了解安全风险评估工作的国际标准名称（ISO/IEC TR 13335、ISO/IEC 17799、ISO/IEC 27001 等），了解《信息系统安全等级保护定级指南》、《信息系统安全等级保护实施指南》等国家标准总体情况。

【技术部分】

1. 操作系统安全检测与防护

了解操作系统（Windows、Linux、Unix 等）的常规安全防护机制。熟悉系统日志、应用程序日志等溯源攻击途径。掌握系统账号、权限、文件系统、文件共享、网络参数、端口和服务、日志审计、漏洞补丁等项目的安全检测与安全加固方法；掌握系统加密、系统防火墙、安全策略、杀毒软件的安装和配置方法。

2. 数据库安全检测与防护

了解数据库（Mssql、Mysql、Oracle、MongoDB）的库表管理、数据访问、权限控制等基础安全防护机制。熟悉数据存储加密不当、数据库访问与权限管理配置不当、SQL 注入攻击、数据库漏洞攻击等常见安全问题。

掌握数据库运维管控、数据存储加密、数据脱敏、风险发现、日志审计等安全防护方法。

3. 网络层攻击与防护

了解网络层的网络架构、传输方式、传输协议和控制措施；了解针对有线和无线的攻击方式和安全防护机制。熟悉常见的网络层攻击，包括：DoS 和 DDoS、窃听、假冒/伪装、重放攻击、篡改、针对 DNS 的工具（欺骗、投毒和劫持）、ARP 攻击、DHCP 攻击以及无线攻击等。掌握通过使用网络层安全工具和设备（如：NMAP、防火墙、Web 防火墙、IDS/IPS、抗拒绝服务攻击系统、网络扫描器等）发现和阻断网络层攻击的方法和技术；掌握对网络层设备（如：路由器、交换机等）的安全配置和加固技术；掌握验证各种安全防护手段（如密码强度、访问控制）有效性和强度的方法。

4. Web 应用安全

了解 Web 应用安全架构，风险分析及常规防护思路。熟悉框架和组件漏洞、权限绕过、弱口令、注入、跨站、文件包含、非法上传、非法命令执行、任意文件读取和下载等常见安全问题。掌握常见 Web 环境的安全配置方法和检测方法和安全防护手段。

5. 渗透测试技术

熟悉渗透基本思路、方法和流程，熟悉各种常见渗透测试工具。掌握常规的渗透测试技术，包括：信息收集、漏洞发掘、常规漏洞利用、常见应用入侵、服务器提权、远程溢出攻击、内网渗透、身份隐藏、暗网挖掘等。

6. 应急响应与恢复

熟悉应急响应与恢复的基本方法和流程。掌握应急响应和恢复的调查、取证、恢复等相关技术，包括：入侵取证分析、日志审计分析、反取证技术、文件删除恢复、中毒文件恢复等。

7. 软件开发安全

了解软件安全开发生命周期、软件安全架构和设计、软件威胁建模原理和方法；了解常见编程环境（C/C++、JAVA、PHP、JSP 等）的构建以及语言的编写。熟悉常见的软件安全漏洞的产生原理和加固方法；熟悉软件安全开发过程中有关参数化查询、输入验证、输出编码、访问控制、身份验证、安全日志、API 接口安全、使用安全的第三方组件等安全开发规范；熟悉代码审计（包括人工审计和工具审计）和代码加固技术。

8. 恶意代码与逆向

熟悉恶意代码的分类、特点和运行机制，熟悉常见的恶意代码，包括：后门、僵尸网络、启动器、感染病毒、远程控制木马、Rootkit 等。熟悉发现、隔离、清除常见恶意代码的相关工具及技术手段。熟悉常见的恶意代码保护措施以及清除手段。熟悉对常见恶意代码进行静态与动态的分析、源定位以及修复的方法。

9. 移动应用安全

了解智能终端操作系统（安卓系统、苹果 IOS）的安全机制；了解移动应用软件的安全机制和调试分析、代码审计技术。熟悉移动互联网联网应用和应用商店的架构组成与技术实现；熟悉移动应用软件的越权访问、信息泄露、上传漏洞、业务逻辑错误等安全问题的检测与处理技术；熟悉针对移动应用程序的安全防护技术。掌握移动互联网恶意程序的监测与处

置方法。

10. 新技术应用安全

了解云计算的基本概念及特征。熟悉云计算常见的安全问题，包括：虚拟机安全、应用程序安全、数据安全、网络隔离、接口安全等。

了解大数据的基本概念及特征。熟悉利用大数据分析技术提升网络系统安全隐患发现和防护能力。

了解物联网的基本概念及相关基础技术，了解智能摄像头、ID/IC 卡、智能卡、智能家居、可穿戴智能设备等常见安全威胁，熟悉物联网应用环境中典型的安全攻击，如 RFID 攻击等。