**河南省“天安杯”网络安全技能大赛**

**竞赛手册**

1. 网络安全技能大赛考试大纲
2. 网络安全技能大赛竞赛规则
3. 参考资料和推荐书目

中国信息通信研究院

2018.3.20

**一、网络安全技能大赛考试大纲**

**【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**

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。

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。

熟悉河南省通信网络信息安全相关政策和管理要求。

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**

 熟悉各专业网络单元安全防护标准中技术要求内容。

 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。

 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。

 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。

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。

了解拟态防御基本概念及基本技术原理，了解拟态防御系统的发展情况和应用场景。

**二、网络安全技能大赛竞赛规则**

（一）个人比赛说明

1.环境说明

(1)单骑闯关赛

1. 比赛环境为闯关竞赛平台。
2. 每位参赛选手的答题环境均完全相同且互相隔离，选手通过独立帐户访问答题环境。
3. 闯关竞赛平台由竞赛服务器构建，提供统一的访问ip地址。
4. 闯关竞赛答题需要的电脑终端需参赛选手提前自行准备。

(2)综合靶场赛

1. 比赛环境包括综合靶场场景。其中综合靶场包括多台常规虚拟机。
2. 每位参赛选手的目标环境均完全相同且互相隔离。
3. 参赛选手比赛开始阶段会得到服务器ip地址作为综合靶场环境入口，靶场内部其它服务器需要自行探测；
4. 每个靶场环境中会有多个flag信息。
5. 提交flag信息到评分系统自动判分，并现场实时展示得分榜。
6. 题目涵盖WEB类漏洞、内网渗透、远程溢出、逆向等类型，所有比赛中可能需要的工具需参赛选手提前自行准备。

2.评分说明

(1)单骑闯关赛（40%）

 闯关赛题目总分占决赛个人赛总成绩的40%，包括多道不同难度的关卡，每道关卡的分值根据难度不同有所差别。题目难度比例为较易20%、中等50%、较难30%。

(2)综合靶场赛（60%）

综合靶场赛题目总分占决赛个人赛总成绩的60%，具体如下：

综合靶场内置多个flag，flag分值根据难度不同有所差别，题目难度比例为较易占30%、中等50%、较难20%。

3.评分规则

(1)单骑闯关赛

1)每个flag信息获得后提交评分系统将获得对应分值，提交错误不扣分，可以多次反复提交。

2)flag提交没有先后顺序，成功提交flag后直接获得对应分数。

(2)综合靶场赛

1)综合靶场的flag在综合靶场中提交。

2）每个flag信息获得后提交评分系统将获得对应分值，提交错误不扣分，可以多次反复提交。

3)flag提交有先后顺序，请按照提示提交，成功提交flag后直接获得对应分数。

4.比赛规则和纪律

(1)参赛选手在赛前统一进行竞赛平台连通性测试，签订连通性确认单，一旦签订，在竞赛过程中出现的接入连通性问题均由参赛选手自行解决并承担相关结果。

(2)参赛选手在竞赛开始前15分钟进入考场，并按规定位置就座，不得随意变动。

(3)比赛时间开始后，比赛环节中所有平台同时开放，评分系统开始计分；结束时间到达后，评分系统将自动停止判分，参赛选手停止比赛。

(4)所有比赛环节的题目说明和竞赛方式均在相关竞赛平台中进行了详细展示，请参赛选手仔细阅读并参考。

(5)比赛过程中听从监考人员安排。

(6)严禁使用互联网，严禁携带、使用手机、蓝牙等设备。

(7)严禁通过各种方式访问、使用互联网，严禁使用VPN通道远程接入考试环境参赛，严禁通过互联网交换答案（创建群、传送答案）。

(8)严禁通过自带设备构建考场环境中WLAN或是跨参赛选手的内部局域网络。

(9)严禁干扰他人答题，尤其是通过技术手段对上机操作环境进行攻击。

(10)比赛过程中，不同参赛选手之间不允许以任何形式相互讨论、交流，一经发现，直接判定比赛成绩为0分，立刻终止其比赛资格。

(11)比赛现场配备专业安全设备对所有流量进行监控记录，比赛过程中禁止使用CC/DDOS/ARP等恶意攻击工具，禁止对裁判服务器进行攻击，一经发现，发现一次现场主裁判将做警告处理，同时扣除个人总成绩20分；再次发现相同违规行为将判令参赛选手停止比赛，分数将做清零处理并终止其比赛资格。

(12)严禁修改考试环境中相关主机的网络配置。

(13)参赛选手如果发现竞赛平台故障请及时联系现场裁判进行恢复。

(14)对上机参赛队员的违纪现象以及监考老师的渎职现象，请填写举报表后留在桌子上。查证违纪、渎职属实，违纪选手上机成绩无效，并通报处理；渎职的监考老师将通知其所在单位，并通报处理。

（二）团队混合攻防赛说明

1.环境说明

(1)比赛环境为团队混战靶场，每组参赛队伍拥有2台常规虚拟机服务器。

(2)每组参赛队伍的比赛环境均完全相同。

(3)每组参赛队伍比赛开始阶段会得到自己2台服务器ip地址，其他队伍服务器需要自行探测。

(4)题目涵盖WEB类漏洞、内网渗透、远程溢出等类型，所有比赛中可能需要的工具需参赛人员提前自行准备。

(5)混战靶场评分系统自动判分，并现场实时展示得分榜。

2.评分说明

团队混和攻防赛（100%）

团队混战赛总分占团队赛总成绩的100%，混战平台的服务器中内置多个flag，flag分值根据难度不同有所差别。提交其他参赛队伍服务器的flag得到相应分数；被其他队伍获取并提交本方队伍服务器中flag，扣除相应flag分数。

3.评分规则

(1)团队混战赛在竞赛开始25分钟之内，各参赛队伍完成本方服务器的加固，不会受到其他参赛队伍的攻击。在25分钟后，所有参赛队伍可以展开互相攻击，同时可以持续对本方服务器进行加固。

(2)获得并提交其他参赛队伍flag信息，每个将获得对应分值，提交错误不扣分，可以多次反复提交。

(3)flag提交没有先后顺序，成功提交flag后直接获得对应分数。

(4)本方参赛队伍的flag被其他参赛队伍成功提交后，本方扣除相应flag分数，相同flag反复提交只会一次扣分。

(5)每个flag每半小时会刷新一次，刷新前重复提交正确flag只一次计分，不叠加计分；刷新后再次提交正确flag可以再次计分。

(6)如果被其他参赛队伍攻击导致本方参赛队伍服务器不能继续使用，可向现场裁判申请重置靶机系统。每次重新开机将扣除团队赛总成绩2分。

(7)如果为了避免受到其他参赛队伍攻击而恶意关机，一经发现，在二十分钟内没有开机者，扣除团队赛总成绩10分，若仍不开机，后续按照每延续10分钟不开机扣除团队赛总成绩10分的方式计分。此项不与第6项重复扣分，6项和7项由现场裁判组统一认定。

(8)如果为了避免受到其他参赛队伍攻击而恶意关闭或替换混战平台原有服务者，一经发现，每次扣除团队赛总成绩20分。

4.比赛规则和纪律

(1)参赛选手在赛前统一进行竞赛平台连通性测试，签订连通性确认单，一旦签订，在竞赛过程中出现的接入连通性问题均由参赛选手自行解决并承担相关结果。

(2)参赛选手在竞赛开始前15分钟进入考场，并按规定位置就座，不得随意变动。

(3)比赛过程中听从监考人员安排。

(4)严禁使用互联网，严禁携带、使用手机、无线网卡、蓝牙等设备。

(5)严禁通过各种方式访问、使用互联网，严禁使用VPN通道远程接入考试环境参赛，严禁通过互联网交换答案（创建群、传送答案）。

(3)严禁通过自带设备构建考场环境中WLAN或是跨参赛选手的内部局域网络。

(8)比赛过程中，不同参赛队伍之间不允许以任何形式相互讨论、交流，一经发现，相关队伍立刻停止比赛，分数将做清零处理并终止其比赛资格。

(7)比赛现场配备专业安全设备对所有流量进行监控记录，比赛过程中禁止使用CC/DDOS/ARP等恶意攻击工具，禁止对裁判服务器进行攻击，一经发现，发现一次现场主裁判将做警告处理，同时扣除参赛队伍总成绩20分；再次发现相同违规行为将判令参赛队伍停止比赛，分数将做清零处理并终止其比赛资格。

(8)严禁修改考试环境中相关主机的网络配置。

(9)各组参赛队伍必须保证自有环境中的所有服务器正常运行，如果发现服务器故障或服务故障请及时联系现场裁判进行恢复。

(10)比赛结束时间到达后，评分系统将自动停止判分，参赛队伍停止比赛。

(11)对上机参赛队员的违纪现象以及监考老师的渎职现象，请填写举报表后留在桌子上。查证违纪、渎职属实，违纪选手上机成绩无效，并通报处理；渎职的监考老师将通知其所在单位，并通报处理。

**三、参考资料和推荐书目**

【管理部分】

1. 中华人民共和国网络安全法
2. 通信网络安全防护管理办法（工信部令第11号）
3. 电信和互联网用户个人信息保护规定（工信部令第24号）
4. 工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见（工信部保〔2014〕368号）
5. 电信网和互联网网络安全防护系列标准
6. 通信网络安全管理文件与标准汇编

【技术部分】

1. 黑客攻防技术宝典-Web实战篇
2. 黑客大曝光:Web应用程序安全(原书第3版)
3. 黑客大曝光：恶意软件和Rootkit安全
4. 数据库黑客大曝光——数据库服务器防护术
5. PHP漏洞挖掘与修复（英文版）
6. 数据恢复技术深度揭秘
7. Android安全攻防权威指南
8. Android软件安全与逆向分析
9. Android安全架构深究
10. Android软件安全攻防实例分析
11. Android系统安全和反编译实战
12. iOS 应用安全权威指南
13. iOS 应用逆向工程：分析与实战
14. 无线网络安全攻防实战
15. 云计算安全与隐私
16. 物联网信息安全
17. 大数据时代
18. OWASP: https://www.owasp.org
19. 恶意代码分析实战