# 附件1：

# 2021年河北省职业院校技能大赛（高职）网络安全赛项规程

# 一、赛项名称

网络安全（高职组）

# 二、竞赛目的

全面贯彻落实党的十九大提出的“建设知识型、技能型、创新型劳动者大军，弘扬劳模精神和工匠精神，营造劳动光荣的社会风尚和精益求精的敬业风气”要求，通过组织河北省职业院校技能大赛，促进技能竞赛和技能人才培养工作科学有序地发展。参照世界技能大赛的技术要求和规则标准，加深对相关项目技术技能发展趋势的了解与认识，并向社会展示技能、推广技能，促进产教互动、校企融合，增强高职院校学生的新技术学习能力和就业竞争力，助力新一代信息技术产业快速发展。

# 三、竞赛内容

重点考核参赛选手网络系统安全策略部署、信息保护、网络安全的综合实践能力，具体包括：

1.参赛选手能够在赛项提供的设备上配置各种协议和服务，实现网络系统的运行，并根据网络业务需求配置各种安全策略，以满足应用需求。

2.参赛选手能够根据大赛提供的赛项要求，实施网络空间安全防护操作。

3.参赛选手能够根据网络实际运行中面临的安全威胁，确定安全策略并部署实施，防范并制止网络恶意入侵和攻击行为。

4. 参赛选手通过分组混合对抗的形式，能够实时防护自己服务器，抵御外界的攻击，同时能够对目标进行渗透和攻击。

5.竞赛总时长为4个小时，各竞赛阶段安排如下：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **具体内容** | **说明** |
| 第一阶段 | 基础设置和安全强化 | 对目标网络环境进行安全加固与配置 | 主要涉及交换机的登陆安全、密码安全、端口安全、流量镜像、VLAN 划分、网络防环、静态路由、动态路由、路由协议的认证安全、ACL 访问控制、防火墙不同区域配置和对区域间流量的控制策略，以及实现分部私有网络对总部私有网络的有效访问。 |
| 第二阶段 | 单兵模式系统渗透测试 | 密码学和VPN | 密码学、IPSec VPN、IKE：PreShared Key（预共享密钥认证）、IKE：PKI（公钥架构认证）、SSL VPN等。 |
| 操作系统渗透测试及加固 | Windows操作系统渗透测试及加固、Linux操作系统渗透测试及加固等。 |
| Web应用渗透测试及加固 | SQL Injection（SQL注入）漏洞渗透测试及加固、Command Injection（命令注入）漏洞渗透测试及加固、File Upload（文件上传）漏洞渗透测试及加固、Directory Traversing（目录穿越）漏洞渗透测试及加固、XSS（Cross Site Script）漏洞渗透测试及加固、CSRF（Cross Site Request Forgeries）漏洞渗透测试及加固、Session Hijacking（会话劫持）漏洞渗透测试及加固 |
| 网络安全数据分析 | 能够利用日志收集和分析工具对网络流量收集监控，维护网络安全。 |
| 常用渗透扫描工具使用与脚本语言应用 | 能够利用如Nmap、Nessus、metasploit等常用渗透扫描工具进行信息收集及系统渗透；  熟悉shell，Python等脚本语言的应用。 |
| 第三阶段 | 攻防对抗 | 参赛队之间进行对抗演练 | Windows/Linux操作系统安全攻防、Web应用/数据库安全攻防等。 |

7.竞赛分值权重和时间安排

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容模块** | **分值权重** | **阶段时间** |
| 第一阶段 | 基础设置和安全强化 | 30% | 60分钟 |
| 第二阶段 | 单兵模式系统渗透测试 | 40% | 120分钟 |
| 第三阶段 | 攻防对抗 | 30% | 60分钟 |

# 四、竞赛方式

1.本赛项为团体赛，以院校为单位组队参赛，不得跨校组队。

2.每校限报2队。

3.每个参赛队由2名选手组成，每个参赛队限报1-2名指导教师。

# 五、竞赛规则

（一）报名资格

参赛选手须为2021年度河北省在籍全日制高等职业学校学生；五年制全日制高职四至五年级（含五年级）在籍学生可参加比赛。

（二）竞赛工位通过抽签决定，竞赛期间参赛选手不得离开竞赛工位。

（三）竞赛所需的硬件设备、系统软件和辅助工具由组委会统一安排，参赛选手不得自带硬件设备、软件、移动存储、辅助工具、移动通信等进入竞赛现场。

（四）参赛选手自行决定工作程序和时间安排。

（五）参赛选手在赛前10分钟进入竞赛工位并领取竞赛任务，竞赛正式开始后方可展开相关工作。

（六）竞赛过程中，选手须严格遵守操作规程，确保人身及设备安全，并接受裁判员的监督和警示。若因选手因素造成设备故障或损坏，无法继续竞赛，裁判长有权决定终止该队竞赛；若因非参赛选手个人因素造成设备故障，由裁判长视具体情况做出裁决。

（七）竞赛结束（或提前完成）后，参赛选手要确认已成功提交所有竞赛文档，裁判员与参赛选手一起签字确认，参赛选手在确认后不得再进行任何操作。

# 六、竞赛环境

1.竞赛场地。竞赛现场设置竞赛区、裁判区、服务区、技术支持区。现场保证良好的采光、照明和通风；提供稳定的水、电和供电应急设备。同时提供所有指导教师休息室1间。

2.竞赛设备。竞赛设备由执委会和承办校负责提供和保障，竞赛区按照参赛队数量准备比赛所需的软硬件平台，为参赛队提供标准竞赛设备。

3.竞赛工位。竞赛现场各个工作区配备单相220V/3A以上交流电源。每个比赛工位上标明编号。每个比赛间配有工作台，用于摆放计算机和其它调试设备工具等。配备2把工作椅（凳）。

4.技术支持区为参赛选手比赛提供网络环境部署和网络安全防范。

5.服务区提供医疗等服务保障。

6.竞赛工位隔离和抗干扰。竞赛工位之间标有隔离线，每个相邻竞赛赛位隔离线之间间隔不低于1.5米。

# 七、技术规范

该赛项涉及的信息网络安全工程在设计、组建过程中，主要有以下7项国家标准，参赛选手在实施竞赛项目中要求遵循如下规范：

|  |  |  |
| --- | --- | --- |
| **序号** | **标准号** | **中文标准名称** |
| 1 | GB 17859-1999 | 《计算机信息系统安全保护等级划分准则》 |
| 2 | GB/T 20271-2006 | 《信息安全技术信息系统通用安全技术要求》 |
| 3 | GB/T 20270-2006 | 《信息安全技术网络基础安全技术要求》 |
| 4 | GB/T 20272-2006 | 《信息安全技术操作系统安全技术要求》 |
| 5 | GB/T 20273-2006 | 《信息安全技术数据库管理系统安全技术要求》 |
| 6 | GA/T 671-2006 | 《信息安全技术终端计算机系统安全等级技术要求》 |
| 7 | GB/T 20269-2006 | 《信息安全技术信息系统安全管理要求》 |

# 八、技术平台

（一）比赛器材

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **数量** | **设备型号** |
| 1 | 网络空间安全技能评测平台 | 1 | 中科软磐云PY-B7  磐云PY-B7为1U设备，2个千兆以太口， Intel至强处理器，16G内存，120G SSD +1T SATA硬盘。支持多用户并发在线比赛，根据不同的实战任务下发进行自动调度靶机虚拟化模板功能,为学员提供单兵闯关、分组混战和夺旗竞速等实际对战模式，能够提供29种不同级别的攻防场景。 |
| 2 | PC机 | 2 | CPU 主频>=3.5GHZ,>=四核心 八线程；内存>=8G；硬盘>=1T；支持硬件虚拟化；具有串口或者提供USB转串口配置线缆 |

（二）软件技术平台：

比赛的应用系统环境主要以Windows和Linux系统为主，涉及如下版本：

1）物理机安装操作系统：Windows 7。

2）虚拟机安装操作系统：

* Windows系统：Windows XP、Windows 7、Windows2003 Server、Windows2008 Server（根据命题确定）。
* Linux系统：Ubuntu、Debian、CentOS（根据命题确定）。

3）Cisco Packet Tracer7.3模拟器

4）比赛提供Putty作为终端。

# 九、成绩评定

裁判长负责将竞赛三个阶段的分数汇总，产生每赛位号的对应成绩。竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平，成绩产生办法由下表所示产生：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **竞赛阶段** | **阶段名称** | **任务阶段** | **竞赛任务** | **分值** | **评分方式** |
| 第一阶段  权重30% | 基础设置和安全强化 |  | 根据答题卡提交内容 | 300 | 裁判判分 |
| 第二阶段  权重40% | 单兵模式系统渗透测试 | 任务1 | 根据赛题确定内容 | 100 | 机考评分 |
| 任务2 | 根据赛题确定内容 | 100 | 机考评分 |
| 任务3 | 根据赛题确定内容 | 200 | 机考评分 |
| 第二阶段  权重30% | 分组对抗 | 系统攻防 | | 300 | 机考评分 |

参赛选手应体现团队风貌、团队协作与沟通、组织与管理能力和工作计划能力等，并注意相关文档的准确性与规范性。

竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为，由裁判组按照规定扣减相应分数，情节严重的取消竞赛资格。

# 十、奖项设定

本赛项为团体赛，依照实际参赛团队数量确定奖项：一等奖占参赛选手总数的10%，二等奖占参赛选手总数的20%，三等奖占参赛选手总数的30%。

# 十一、竞赛须知

（一）参赛选手须知

1. 各参赛选手要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2．参赛选手应按有关要求如实填报个人信息，否则取消竞赛资格。

3．参赛选手应按照规定时间抵达赛场，凭统一印制的参赛证、有效身份证件检录，按要求入场，不得迟到早退。请勿携带任何电子设备及其他资料、用品进入赛场。

4．参加选手应认真学习领会本次竞赛相关文件，自觉遵守大赛纪律，服从指挥，听从安排，文明参赛。

5．参赛选手应增强角色意识，科学合理做好时间分配。

6. 参赛选手应按有关要求在指定位置就坐。

7.参赛选手须在确认竞赛内容和现场设备等无误后开始竞赛。在竞赛过程中，确因计算机软件或硬件故障，致使操作无法继续的，经项目裁判长确认，予以启用备用计算机。

8. 各参赛选手必须按规范要求操作竞赛设备。一旦出现较严重的安全事故，经总裁判长批准后将立即取消其参赛资格。

9.参赛选手需详细阅读赛题中竞赛文档命名的要求，不得在提交的竞赛文档中标识出任何关于参赛选手地名、校名、姓名、参赛编号等信息，否则取消竞赛成绩。

10. 竞赛时间终了，选手应全体起立，结束操作，将资料和工具整齐摆放在操作平台上，经工作人员清点后可离开赛场。离开赛场时不得带走任何资料。

11.在竞赛期间，未经执委会批准，参赛选手不得接受其他单位和个人进行的与竞赛内容相关的采访。参赛选手不得将竞赛的相关信息私自公布。

12.参赛选手若对竞赛过程有异议，在规定的时间内经由领队向赛项仲裁工作组提出书面报告。

（二）指导教师须知

1.各参赛代表队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。如发现弄虚作假者，取消参赛资格，名次无效。

2.各代表队领队要坚决执行竞赛的各项规定，加强对参赛人员的管理，做好赛前准备工作，督促选手带好证件等竞赛相关材料。

3.竞赛过程中，除参加当场次竞赛的选手、执行裁判员、现场工作人员和经批准的人员外，领队、指导教师及其他人员一律不得进入竞赛现场。

4.指导老师应及时查看大赛专用网页有关赛项的通知和内容，认真研究和掌握本赛项竞赛的规程、技术规范和赛场要求，指导选手做好赛前的一切技术准备和竞赛准备。

5. 参赛选手领队应对本队参赛选手和指导教师的参赛期间安全负责，参赛学校须为参赛选手和指导教师购买意外保险。

（三）工作人员须知

1. 树立服务观念，一切为选手着想，以高度负责的精神、严肃认真的态度和严谨细致的作风，在赛项执委会的领导下，按照各自职责分工和要求认真做好岗位工作。

2. 所有工作人员必须佩带证件，忠于职守，秉公办理，保守秘密。

3. 注意文明礼貌，保持良好形象，熟悉赛项指南。

4. 自觉遵守赛项纪律和规则，服从调配和分工，确保竞赛工作的顺利进行。

5. 提前30分钟到达赛场，严守工作岗位，不迟到，不早退，不得无故离岗，特殊情况需向工作组组长请假。

6. 熟悉竞赛规程，严格按照工作程序和有关规定办事，遇突发事件，按照应急预案，组织指挥人员疏散，确保人员安全。

7. 工作人员在竞赛中若有舞弊行为，立即撤销其工作资格，并严肃处理。

8. 保持通讯畅通，服从统一领导，严格遵守竞赛纪律，加强协作配合，提高工作效率。

# 十二、申诉与仲裁

（一）申诉

参赛队对不符合竞赛规定的软硬件设备，有失公正的评判，以及对工作人员的违规行为等，均可提出申诉。申诉时，应递交由参赛队领队亲笔签字同意的书面报告，报告应对申诉事件的现象、发生的时间、涉及的人员、申诉依据与理由等进行充分、实事求是的叙述。事实依据不充分、仅凭主观臆断的申诉不予受理。申诉人不得无故拒不接受处理结果，不允许采取过激行为刁难、攻击工作人员，否则视为放弃申诉。竞赛结束后1小时内提出，超过时效将不予受理申诉；

2.赛场专设仲裁工作组受理申诉，收到申诉报告之后，根据申诉事由进行审查，3小时内书面通知申诉方，告知申诉处理结果。

（二）仲裁

1.组委会下设仲裁工作组，负责受理竞赛中出现的所有申诉并进行仲裁，以保证竞赛的顺利进行和竞赛结果公平、公正。

2.仲裁工作组的裁决为最终裁决，参赛队不得因申诉或对处理意见不服而停止比赛或滋事，否则按弃权处理。