中科磐云

2022网络安全赛项总结与技术分析

磐云安全研究院
Pan Yun Safety Research Institute

目录
CONTENTS

01 赛项情况介绍

ChinaSkills

2022年全国职业院校技能大赛

2022 National competition for Skills of Vocational Education

中职组网络安全赛项

主办单位：教育部、天津市人民政府、江苏省人民政府、国家发展和改革委员会、科学技术部、工业和信息化部、国家民族事务委员会、民政部、财政部、人力资源和社会保障部
自然资源部、生态环境部、住房和城乡建设部、交通运输部、水利部、农业农村部商务部、文化和旅游部、国家卫生健康委员会、应急管理部、国务院国有资产监督管理委员会
国家粮食和物资储备局、中国民用航空局、国家中医药管理局、国家乡村振兴局、中华全国总工会共青团中央、中华职业教育社、中国职业技术教育学会、中华全国供销合作总社
中国机械工业联合会、中国有色金属工业协会、中国石油和化学工业联合会、中国物流与采购联合会、中国纺织工业联合会、中国煤炭工业协会

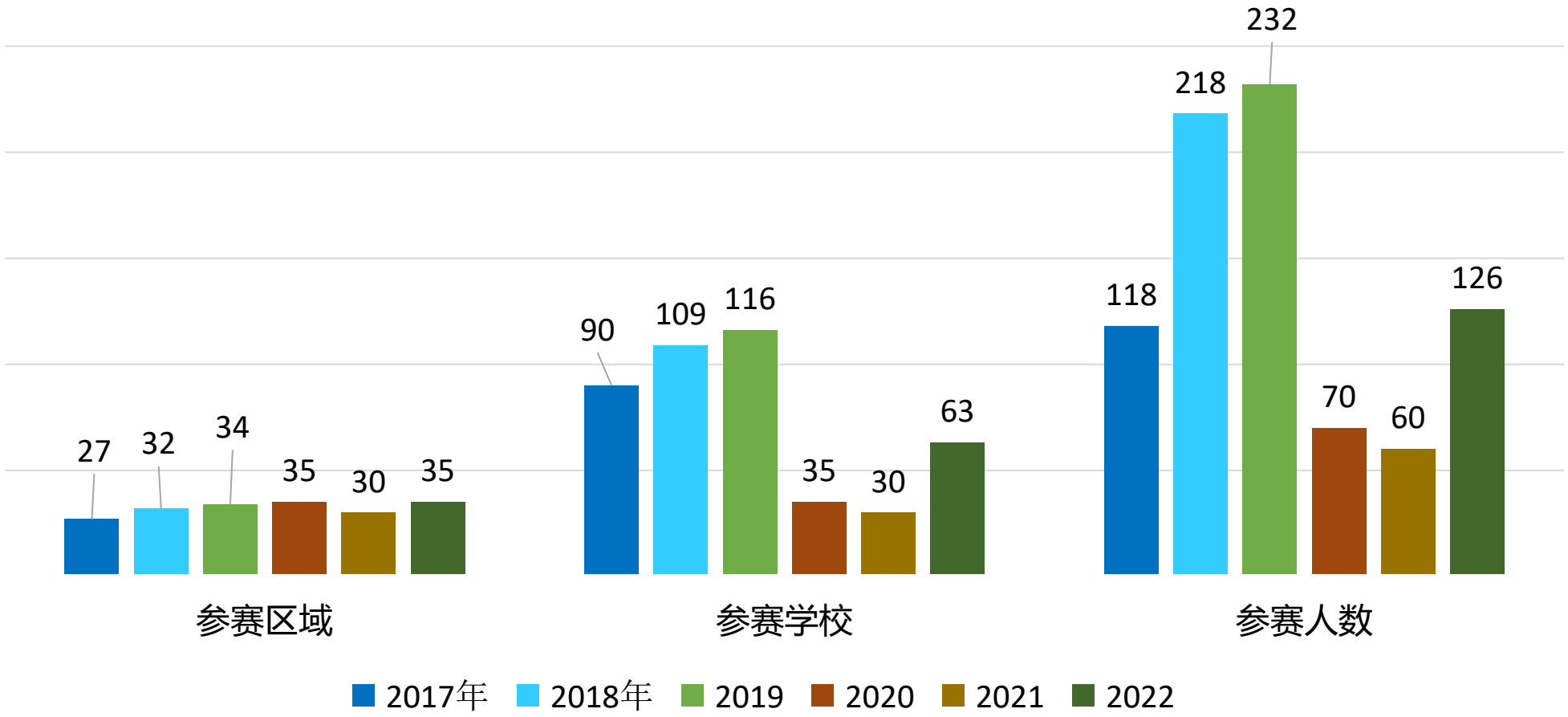
承办单位：江苏省教育厅、南京市人民政府

协办单位：工业和信息化职业教育教学指导委员会、南京市教育局、南京商业学校、中科磐云（北京）科技有限公司

2022年全国职业院校技能大赛江苏分赛区组委会
2022年7月

历年参赛情况

2017-2022中职组“网络安全”赛项各区域参与情况汇总



赛项现场

2017年

2018年

2019年

2020年

2021年

2022年

大赛内容与行业应用的热门技术紧密相关，每年都会加入新的技术内容，同时引领院校教学内容不断更新。

大赛采用系统自动评分，大屏幕公开直播并显示赛场实况和选手即时分数，以确保大赛的公平、公开、公正。

分值权重和时间安排

日程	模块编号	模块名称	时间分配	分值权重	评分方式
Day 1	A	基础设施设置与安全加固	4小时	20%	客观评分
	B	网络安全事件响应、数字调查取证和应用安全		40%	机考评分
Day 2	C	CTF夺旗-攻击	3小时	20%	机考评分
	D	CTF夺旗-防御		20%	客观评分
总计			7小时	100%	

竞赛内容设计

模块	模块名称	考核内容	考核能力
A	基础设施设置与安全加固	登录安全加固、数据库加固（Data）、Web安全加固、流量完整性保护（Web,Data）、事件监控、服务加固、防火墙策略等	考察选手综合运用登录和密码策略、数据库安全策略、流量完整性保护策略、事件监控策略、防火墙策略等多种安全策略来提升服务器系统的网络安全防御能力
B	网络安全事件响应、数字调查取证和应用安全	网络安全事件、数字取证调查和应用安全，主要包括：数据分析、数字取证、内存取证、漏洞扫描与利用、操作系统渗透测试、应急响应等	考察选手对常用操作系统及Web的漏洞进行检测、监控和修复的能力，以及能够对网络安全事件作出应急响应处理，使系统恢复正常运行，并对事件进行调查和追踪的能力
C	CTF夺旗-攻击	寻找企业网络中可能存在的各种问题和漏洞，利用各种攻击手段，攻击特定靶机，了解网络黑客的心态，从而改善服务器的防御策略	考察选手在未知场景下综合运用各种安全技能进行渗透测试的能力
D	CTF夺旗-防御	参赛队拥有专属的堡垒机服务器,通过扫描、渗透测试等手段检测自己堡垒服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能	考察选手通过扫描、渗透测试等手段检测靶机服务器中存在的安全缺陷，进行针对性加固，从而提升系统的安全防御性能并制作系统防御实施报告的能力

模块B任务说明

模块编号	竞赛任务	考核能力
模块B	任务1 主机发现与信息收集	考察选手使用渗透测试常用工具的能力（Nmap、Metasploit、md5sum等工具）
	任务4 漏洞扫描与验证	
	任务6 Telnet弱口令渗透测试	
	任务7 文件MD5校验	
	任务3 数据分析数字取证	考察选手在计算机发生紧急事件后是否能够迅速采取对应的措施，将事件造成的损失危害降低到最少，检查学生是否拥有病毒检测，后门检测、隔离，系统恢复，事件调查与追踪、以及数据分析数据溯源能力
	任务9 操作系统应急响应	
	任务2 Web渗透测试	考察选手对未知操作系统场景的综合渗透能力（掌握各种扫描工具对靶机进行信息收集并进行漏洞验证）
	任务8 Linux系统安全	
	任务10 Windows系统安全	
	任务5 PE Reverse	主要考察选手通过调试器对Windows PE可执行文件进行逆向分析，考察通过Python模糊测试分析缓冲区的参数以及对Python Socket网络编程的掌握

竞赛环境

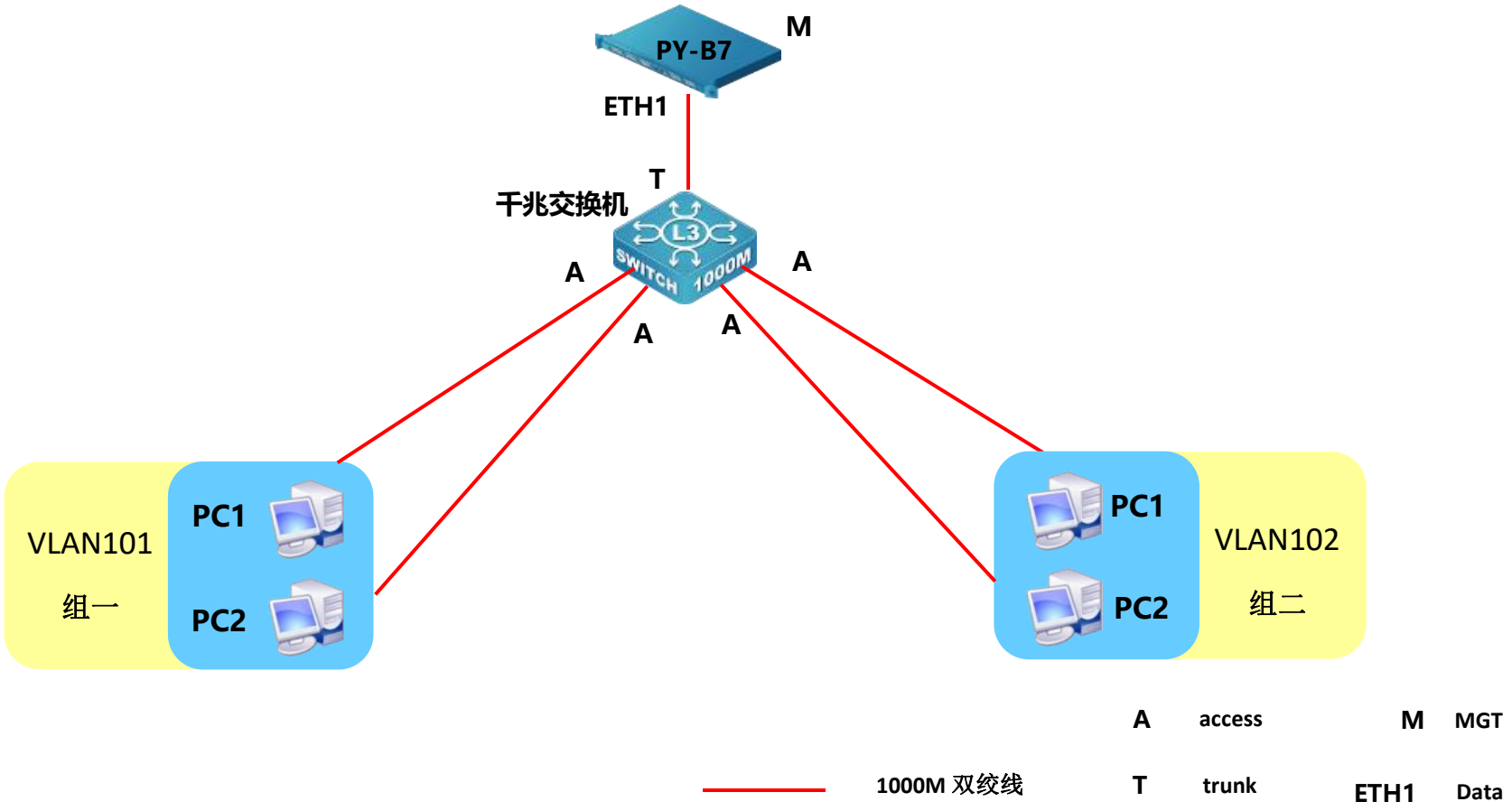
硬件环境

序号	设备名称	设备规格
1	网络安全技能评测平台	竞赛平台（中科磐云）
2	三层交换机	全千兆三层交换机
3	PC机	CPU 主频≥2.8GHZ, ≥四核四线程；内存≥8G；硬盘≥500G；支持硬件虚拟化
4	WAF（保障设备）	企业级 WEB 应用防火墙保障服务器安全
5	UPS电源（保障设备）	满足至少30分钟不间断电源

软件平台

序号	分类	版本型号
1	Windows系统	Windows XP、Windows 7、Windows2003 Server、Windows2008 Server
2	Linux系统	Ubuntu、Debian、CentOS
3	工具软件	Vmware、Chrome、Putty、Office、福昕PDF阅读器、Snipaste、截图工具、搜狗拼音输入法、RAR解压

网络环境



每组两台PC都可以作为渗透机且能提交flag

答题和评分

答题方式

模块A：赛前发放U盘，含有A模块答题模板，按照模板要求进行文档的编辑，比赛结束，将文档另存为PDF格式保存至U盘，等待裁判签收

模块B：根据题目要求，获得唯一“FLAG”值，根据题号在答题平台上进行提交，正确得分，错误0分，系统自动计算分数

模块C：攻击特定靶机，获得“FLAG”值，在答题处提交靶机地址+FLAG，正确得分，错误0分，系统自动计算分数

模块D：赛前发放U盘，含有D模块答题模板，按照模板要求进行文档的编辑，比赛结束，将文档另存为PDF格式保存至U盘，等待裁判签收

评分方式

模块A：分为 N 个任务，每道题的具体分值在赛题中标明，由评分裁判客观评分

模块B：安全事件响应、网络安全数据取证、应用安全等部分，由系统自动评分和排名

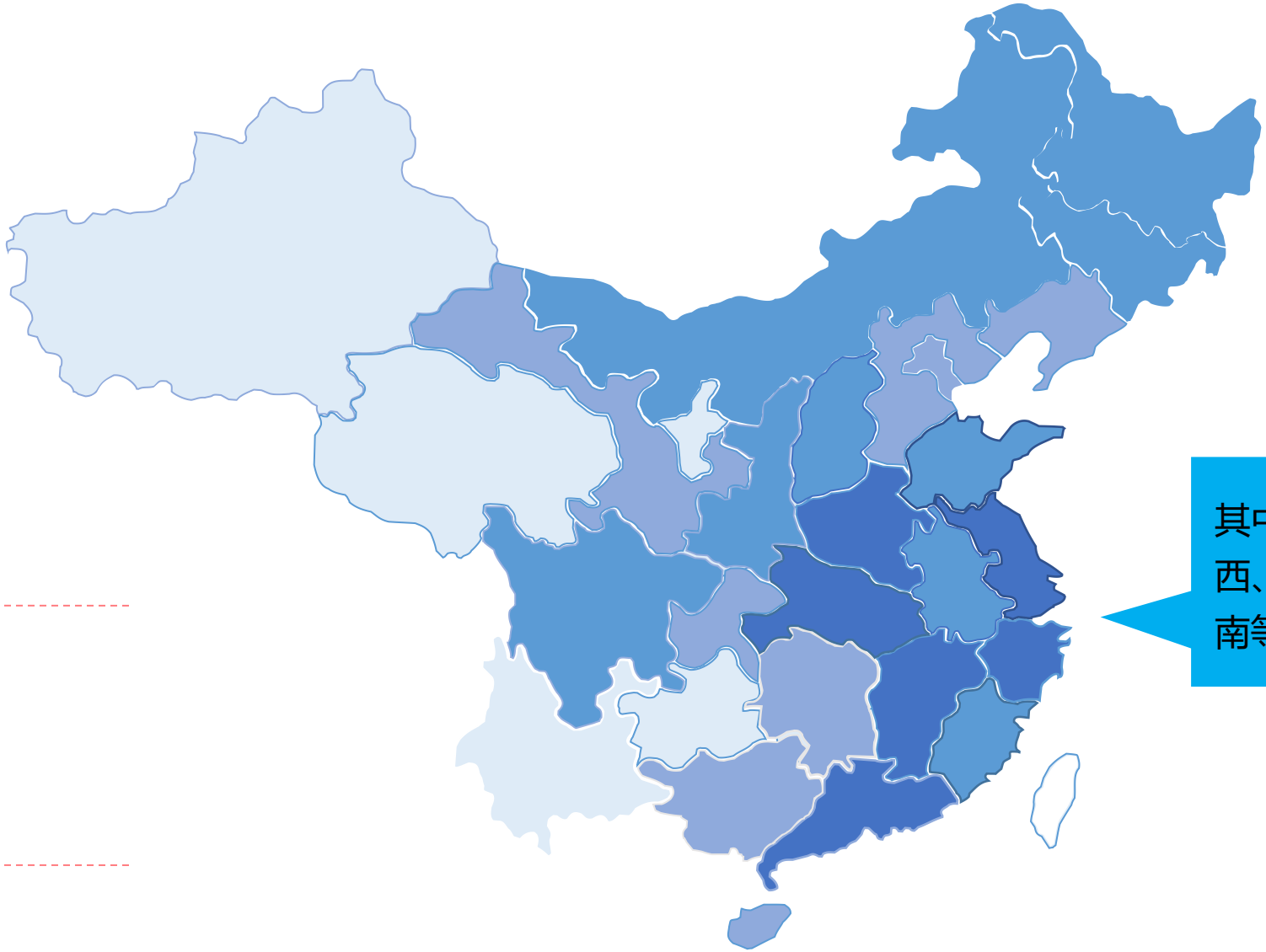
模块C：按照选手获得攻击“FLAG”的值得到相应的分数。由系统自动评分和排名

模块D：按照选手答题内容，由评分裁判进行客观评分

参赛队最后得分为：四个模块分数相加

02 获奖情况统计

获奖区域统计

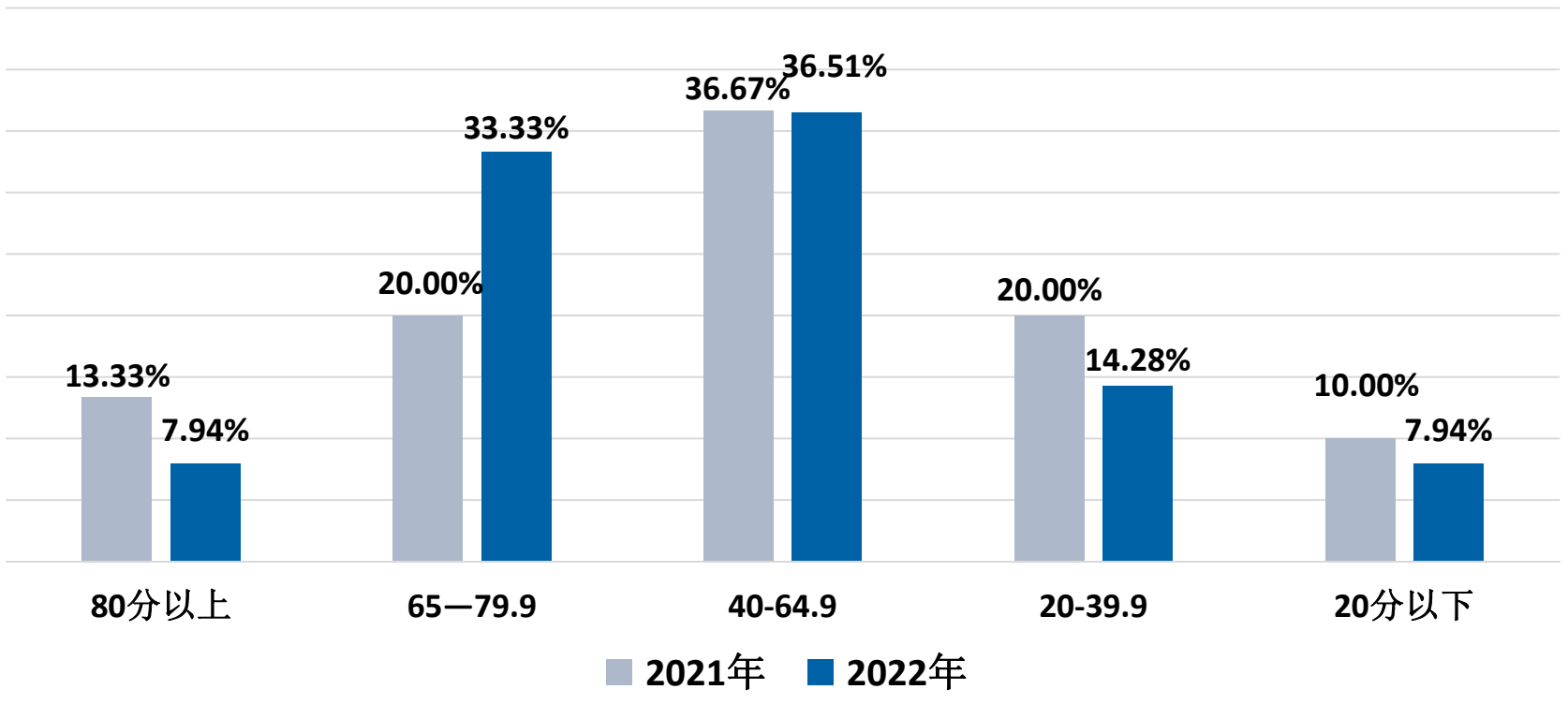


- 一等奖（6个）
- 二等奖（13个）
- 三等奖（19个）

其中，宁波、江苏、江西、湖北、广东以及河南等区域成绩较突出。

总分情况

2022年中职组“网络安全”赛项获奖队伍得分情况



卓越：
80分以上

优秀：
65-79.9

良好：
40-64.9

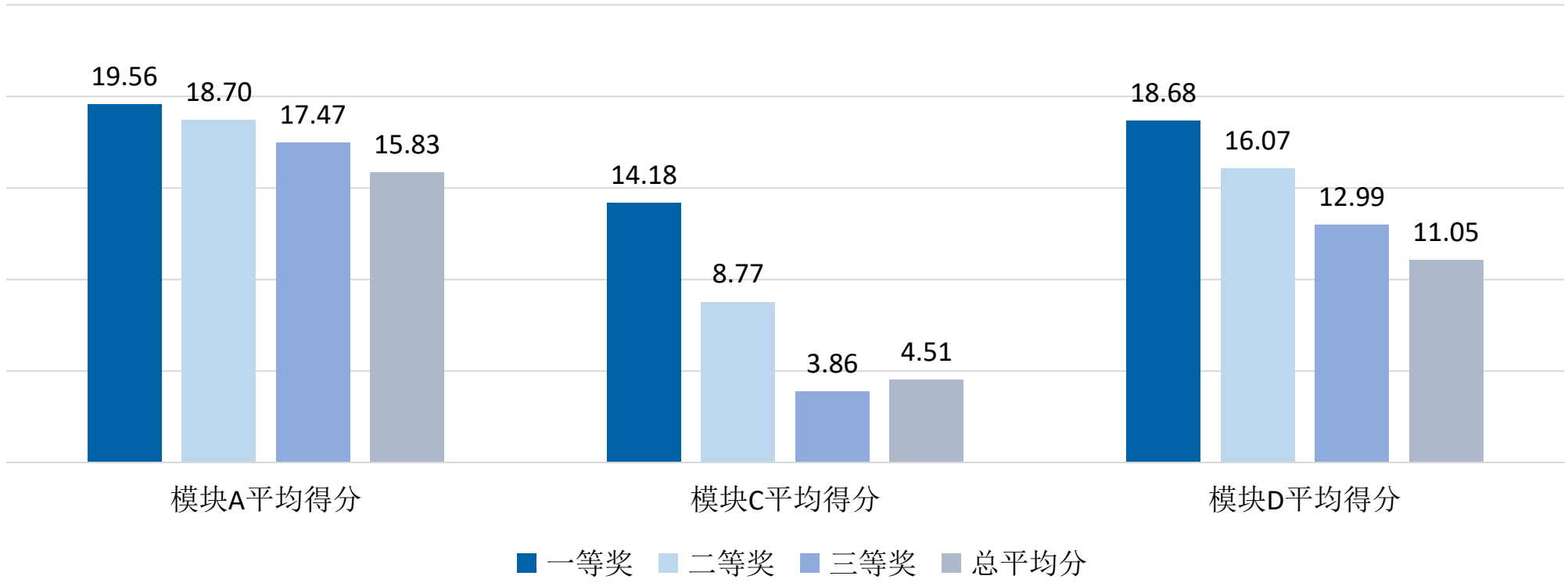
及格：
20-39.9

不及格：
20分以下

03 赛项技术分析

模块分析（模块A、C、D）

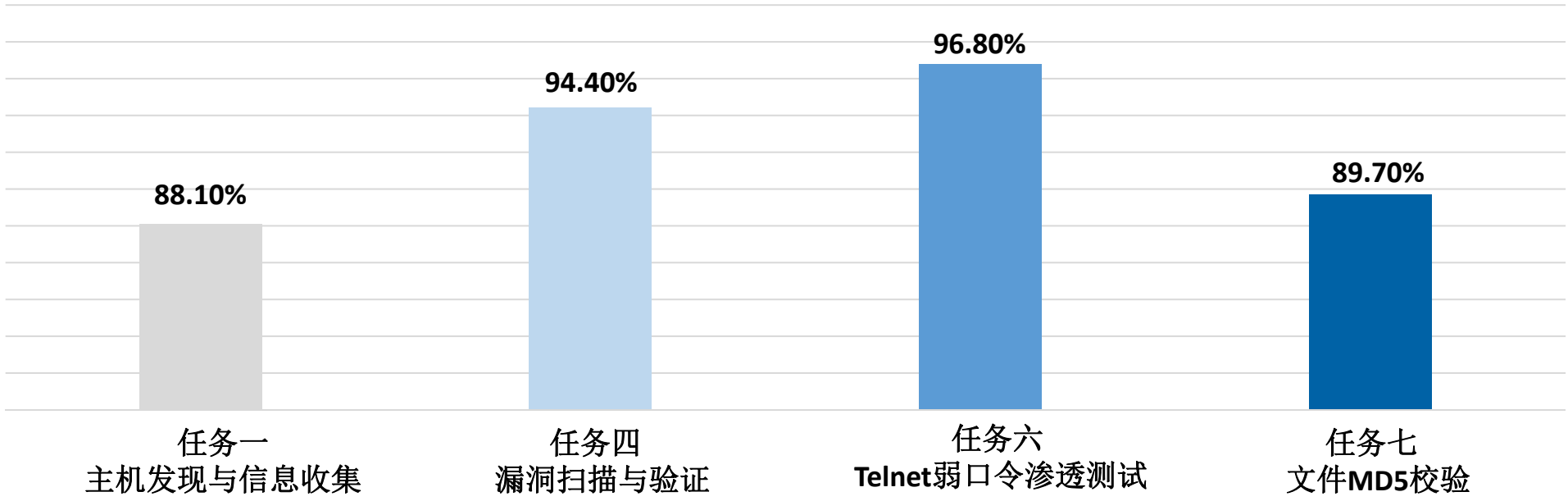
中职组“网络安全”赛项模块A、C、D平均得分统计



一等奖队伍在模块C、D部分取得了大比分领先，大多数选手在模块A上得分都很不错；二、三等奖队伍在系统渗透与加固方面能力较差，提升空间较大。

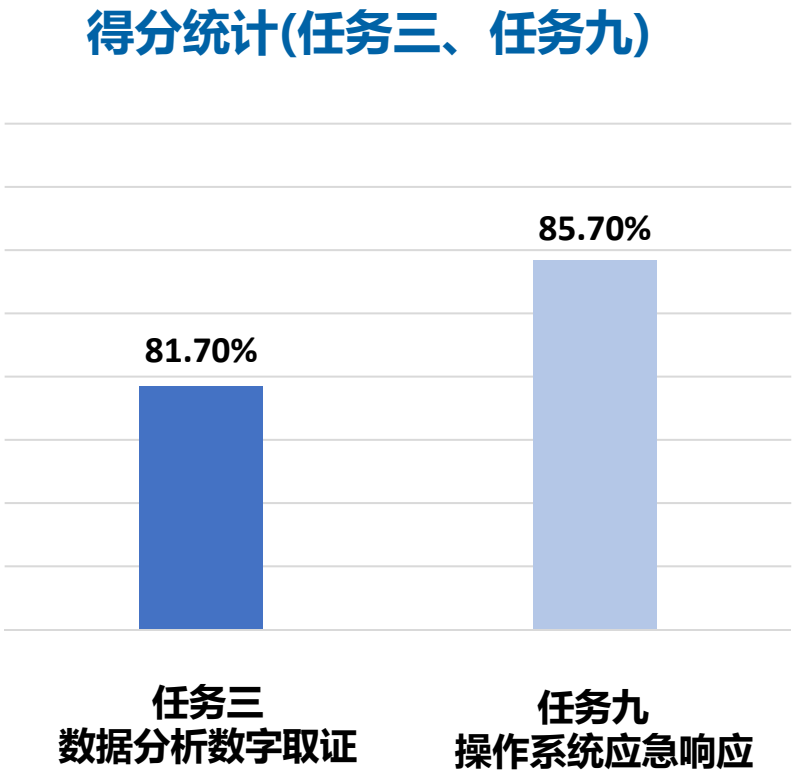
模块分析（模块B）

得分统计(任务一、任务四、任务六、任务七)



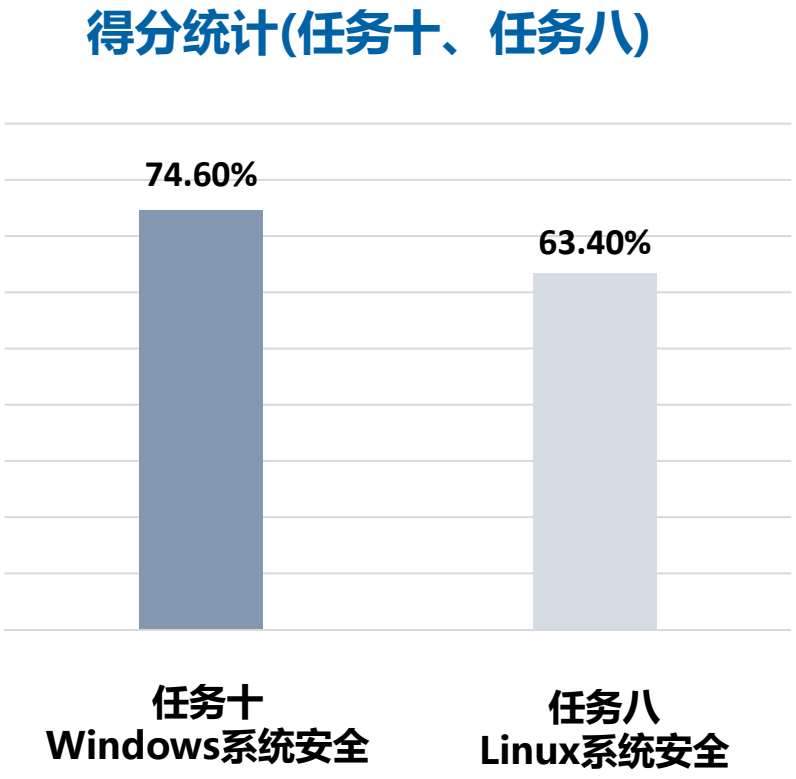
任务一考察选手使用信息收集工具Nmap的能力，任务四、任务六考察选手使用Metasploit工具检测系统漏洞的能力，任务七考察选手md5sum工具的使用能力；这四个任务主要考察选手使用渗透测试常用工具的能力，四个任务的得分率都很高，较去年有较大提升，反映各参赛队对常用渗透测试工具的使用掌握比较熟练。

模块分析（模块B）



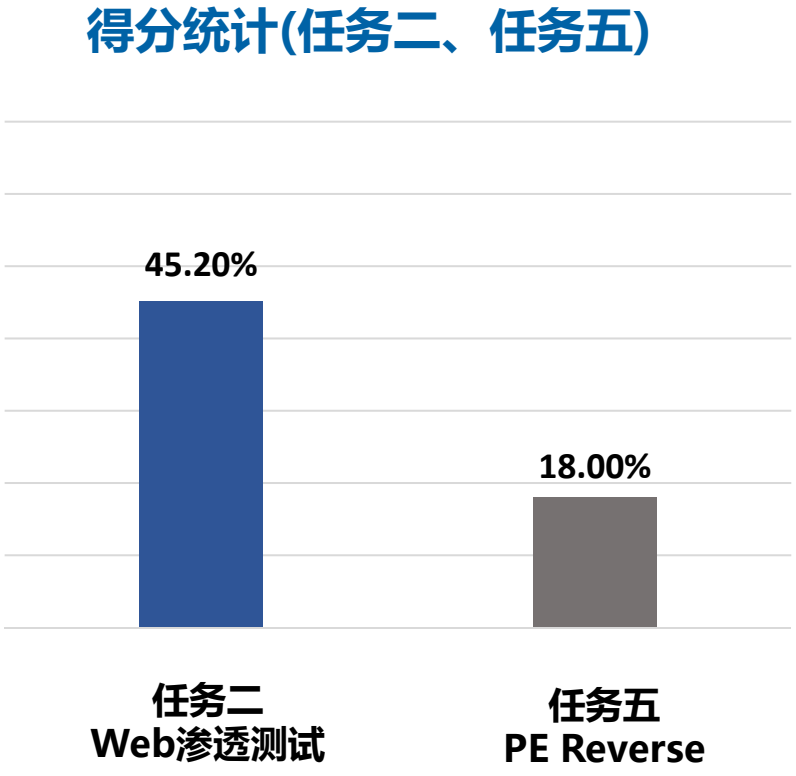
- 任务三考察选手使用Wireshark工具分析数据包的能力，本题首先通过过滤规则，过滤出黑客连接服务器的IP地址，扫描的方式可能为SYN半开连接扫描，最后识别出nmap探测流量的数据包，前面两题相对表简单，后续的内容要能发现网站采取的登录界面的加密方式为Base64加密，这里考察选手加密解密的能力，最后分析黑客上传至服务器中一句话木马的信息，需要通过分析来发现上传木马的文件名及连接密码，由于只抓取到了菜刀木马返回的数据包，所以在过滤时需要分析一句话木马的数据包详情，并分析出木马的连接密码。
- 任务九考察系统发生安全事件时，作为安全人员需要采取措施对操作系统进行安全检测，找出恶意利用者在系统中隐藏的后门，在进行解题的过程中，大多数选手都能够对安全隐患进行加固，但是在完成查找木马病毒这一需求时，有的选手可能发现了木马的源文件，但是无法甄别出该文件是否为木马程序，对完成最后一道题造成一定的麻烦，实际上该木马是由Kali生成的Meterpreter木马文件，运行木马程序后分析网络连接的情况很容易就能够发现木马会向特定的地址发起连接会话，由此可以找到木马文件的位置。

模块分析（模块B）



- 任务十考察选手Windows系统渗透的能力，本题需要通过哈希传递攻击获取Windows操作系统的靶机控制权，再利用Responder结合Hash破解工具（John the Ripper）可以进行自动化的拦截及密码解密，最终获取到数据库用户执行命令的权限，最后进行目录遍历可以发现Flag所在文件夹的位置进行提交完成最后的答题。
- 任务八考察选手Linux系统渗透的能力，这台Linux服务器的root密码就是常规的弱口令123456，也开启了SSH服务，但是大家可能也发现了通过Nmap工具扫描靶机时发现SSH等服务都被防火墙过滤掉了，实际上这里有一个端口敲门的设计，需要先发送UDP包到端口A，再发送UDP包到端口B后SSH服务才会被防火墙规则放行，关于端口敲门以及端口号的提示其实已经在靶机中有体现，大部分队伍都找到了提示信息，对端口敲门有所了解，本任务的整体完成情况还不错。

模块分析（模块B）



- 任务二考察选手Web渗透测试的能力，服务器的网站存在RCE（远程命令执行 Remote Command Execute）漏洞，可以通过phpggc环境来生成Phar反序列化的代码进行利用，通过该漏洞可以将“脏”数据写入至服务器的日志文件中，然后利用Phar协议进行PHP反序列化攻击。攻击成功后将会在服务器中生成远程控制木马，最后使用“蚁剑”工具来连接远程服务器中的木马，并进行遍历操作。
- 任务五考察选手通过调试器对Windows PE可执行文件进行逆向分析，考察通过Python模糊测试分析缓冲区的参数以及对Python Socket网络编程的掌握，通过以上分析的结果，获得靶机的控制权，以及对字符串进行加密的问题，是选手们答题的薄弱环节。

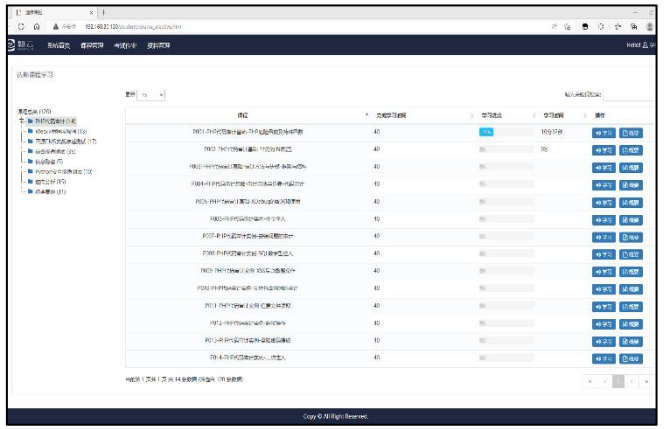
04 赛项总结分享

赛项亮点

赛项设计接轨世界技能大赛

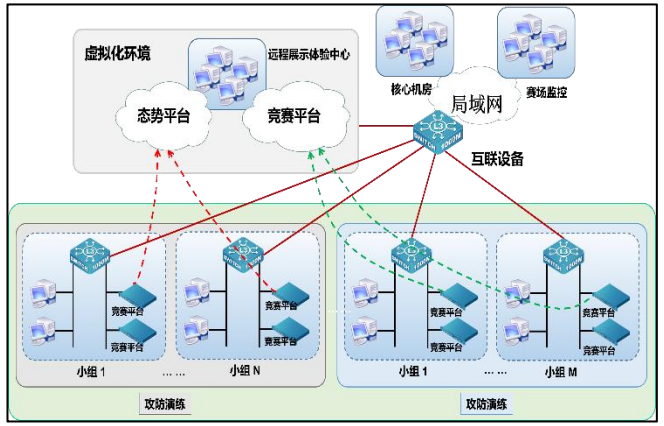
本赛项设计参考**世界技能大赛“网络安全”赛项**，设置A、B、C、D四个模块。在竞赛内容与考核形式上与世赛高度接近，同时结合我国当前中等职业学校网络信息安全技能学习情况在考核的难度上进行优化和调整

先进智能手段保证竞赛公平



网络安全竞赛因其特殊性，竞赛公平性受到广泛质疑，为保证本赛项公平、公正，竞赛平台采用先进的**违规检测机制**，杜绝竞赛过程中的作弊现象（非常规渗透测试、加固手段），保证比赛更公平合理、更真实、更贴近实际

赛项技术方案设计科学全面



基于网络平台的竞赛对网络依赖程度高，网络设施的稳定性直接影响整体比赛的可靠性，是网络安全攻防竞赛环境准备的重要环节。本赛项技术方案从**电力系统、弱电系统、网络设备、攻防平台、PC端**等方面全局设计，保障赛项顺利进行

赛项亮点

故障应急处理预案清晰明确

针对本赛项设计了**科学的处理流程，快速、准确的故障恢复操作步骤**，保障在第一时间恢复业务的正常进行，保证赛事顺利进行。故障应急处理方案为每一位技术人员提供了标准的操作方案，为竞赛提供可靠保障

态势排名赛场监控实时展示

赛项B、C模块采用全新的态势展示系统，实时显示团队排名和选手得分、失分过程及原因，数据详实、内容清晰、画面震撼。赛场监控比赛过程**全程公开，全程零故障、零投诉**

赛项赠书活动助力教学发展

中科磐云在竞赛期间协同机械工业出版社、电子工业出版社开展现场免费赠书活动，为指导教师**提供网络安全专业教材以及网络安全专业建设方案**，助力网络安全专业发展

选手素质体现

从容镇定、认真投入

选手竞赛过程从容镇定、认真投入：表现出较高的分析、解决问题能力和较强的心理调节能力

准备充分、应对自如

选手灵活调整答题顺序:采取先易后难的策略，增强信心的同时也为解决困难问题保证了宽裕的时间

1 2 3

分工明确，团队为赢

团队协作能力是取得致胜的关键：部分参赛队团队分工明确，合理分配任务，在模块C阶段有明显体现

选手能力分析

英文读写能力普遍存不足

网络安全属于综合学科，涉及计算机网络技术、通信技术、密码技术、信息安全技术以及英语等多种领域。选手不仅要具备优秀的网络安全技术，还需要掌握网络安全常见的英文词汇，对学习者相对要求较高。

通过对本次竞赛任务提交历史记录中发现，提交单词的拼写错误现象非常多，导致提交多次失败没有得分。

在现场答题过程中使用渗透测试工具时，选手对工具的英文菜单及屏幕返回的信息不能很好的解读，导致无法操作。

题目阅读理解能力待提高

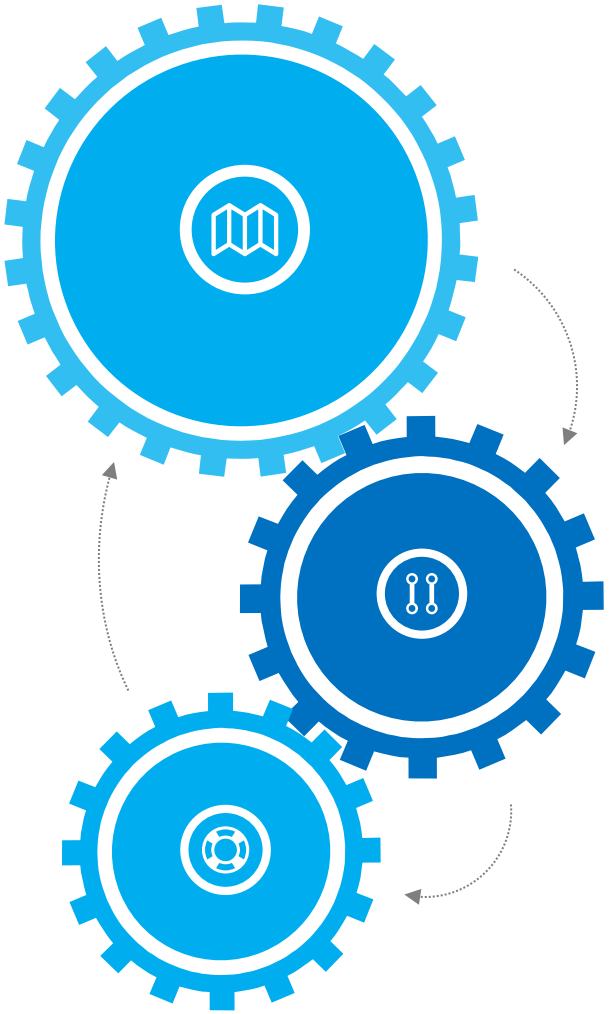
通过各板块的题目得失分统计显示，很多队伍往往在很基础的题目上丢分。

A模块中有一题需要修改SSH服务端口号为2222，使用命令netstat -anltp | grep sshd查看SSH服务端口信息，将回显结果截图。此题为基础题型，主要考察选手对服务安全加固的掌握情况。多数队伍能按照题目要求完成加固，但在提交答案时，部分队伍并未按照题干信息要求进行截图，或是在截图中未体现关键部分，导致最后未能得分。选手们养成细致、认真的阅读习惯，是未来提升自身能力的重点。

对获奖队伍的建议

一等奖队伍

部分队伍在审题方面还有待加强，特别是在模块D，审题越细心，实验的思路越清晰，得分率会更高



二等奖队伍

在单个工具的使用上基本没有问题，在综合多种工具结合使用的时候，不能准确熟练的结合各种模块的特性来做到更深入的渗透

三等奖队伍

对赛题的熟练程度还不够，在模块A、模块B上还要再多下功夫

对所有参赛队的建议

初次参赛的队伍

1.备赛时应多熟悉各操作系统不同漏洞的验证方法：了解各种渗透测试工具的特性,结合各种漏洞来完成渗透测试。

2.加强系统防御实施报告的制作能力：模块D主要考察选手将发现漏洞加固并验证的过程编写为文档的能力。多数队伍在漏洞加固并验证过程完成度很高，但这文档编写时逻辑、思路不完整而导致大量失分。

有一定经验的参赛队伍

在漏洞原理上还要多下功夫，漏洞成因即验证思路，漏洞验证思路是需要大家不断总结深入学习的目标之一。

例如反序列化漏洞的利用，与XSS，SQL注入等十分相似（闭合-构造），以改变原本代码结构来实现漏洞利用，反序列化数据本质上没有危害，但是当反序列化数据是用户可控时就有可能存在危害。

非网络安全专业的参赛队伍

非安全专业的参赛队，在掌握了基本的计算机基础知识后，按照操作系统安全加固、渗透测试工具的应用以及系统服务等安全漏洞的验证的顺序学习，这类知识点与模块A、D的关联性很强。熟练掌握后再系统学习一些Web安全的知识，例如数据库管理与安全维护、网站建设与安全管理等，从而更好的处理Web应用安全问题。

总结

网络安全赛项为广大职业院校搭建了一个良好的学习信息安全技能、拓展信息安全视野、促进信息安全教学的平台。大赛仅仅是个开始，专业建设、资源转化的工作还需要共同努力。希望能以大赛为依托，有效促进中职学校的专业教学改革、人才培养模式创新、为信息安全产业培养大量优秀技能人才！

问题的答案

- 信息安全专业发展前景怎么样？

  信息技术产业发展依然迅速，我国逐步实现自主可控的必然趋势，信息安全技术是建设网络强国的根本与核心。前景是广阔的。

- 中职开设安全专业的必要性？学生能不能学的会？

  中职作为职业教育体系中基础部分，定位是明确的。
  信息安全专业也是信息技术类中少有的，横跨中、高、本全部职教各层级的专业。
  作为传统网络技术专业的衍生专业出现，转型是必然趋势，比如速录专业。
  可以学会，为高职的进阶发展打好专业基础。

- 我校要开设网络安全专业应具备哪些基础，从哪些地方开始准备。

  网络技术专业、计算机应用专业 有大赛的经验，懂得如何通过大赛促进教学。
  师资先行，系统的培训，通过带来学生参加比赛，进一步提升技术水平，建立交流平台。
  教师的意识与意愿。
  区域内有高职的合作。

中科磐云

汇报完毕 感谢您的聆听

磐云安全研究院
Pan Yun Safety Research Institute

400-690-0108