广东省通信管理局关于举办广东省信息通信行业第四届网络安全技能大赛的预通知

中国电信股份有限公司广东分公司、中国移动通信集团广东有限公司、中国联合网络通信有限公司广东省分公司、广东省广播电视网络股份有限公司、中国铁塔股份有限公司广东省分公司、广东省通信产业服务有限公司、中移互联网有限公司，各有关互联网企业，网络安全企业：

为深入实施国家网络安全强国战略，大力培养高素质网络安全技术技能人才队伍，加快推进网络安全保障体系建设，服务新型网络基础设施建设，根据《关于做好2022年度广东省职工职业技能大赛工作的通知》（粤工总〔2022〕21号）及《关于做好2022年广东省行业企业职业技能竞赛工作的通知》（粤人社函〔2022〕181号）要求，我局拟于12月牵头举办“广东省信息通信行业第四届网络安全技能大赛”（以下简称大赛），现将有关事项通知如下：

一、大赛基本情况

本届大赛拟由省通信管理局、省总工会、省人力资源和社会保障厅、省工业和信息化厅、省科学技术厅联合主办。自2016年以来，两年一届的大赛吸引了省内通信企业、互联网企业和网络安全企业的广泛参与，大赛持续以提升信息通信行业网络

安全保障能力为目标，以培养网络安全高技术技能人才为主线，着力激发信息通信行业安全创新主体的创新活力，持续培育网络安全人才梯队和领先企业。

二、大赛组织形式

本次大赛分设**个人赛**和**团队赛**。

（一）个人赛

1.参赛对象为我省通信企业，包括广东电信、广东移动、广东联通、广东广电、广东铁塔、广通服和中移互联网的**正式在册工作人员（提供近6个月社保证明）**，参赛人员资格由大赛组委会审核，根据粤人社规〔2022〕12号文，已获得“中华技能大奖”“全国技术能手”等荣誉人员不以选手身份参赛，已获得“广东省技术能手”的选手，不以选手身份参加同一项目同一组别或更低等级的比赛。

2.个人赛分为预赛和决赛两个环节。预赛选拔工作由省内各通信企业自行组织开展，各自选拔产生8至12人进入决赛。根据粤人社规〔2022〕12号文，决赛人数原则上不超过70人。

3.个人赛决赛由大赛组委会统一集中举行，采用**“理论答题30%+CFS综合靶场70%”**的方式，总计3.5小时。

（二）团队赛

1.团队赛采用公开报名和邀请参赛两种方式，面向我省通信企业、互联网企业、网络安全企业。大赛组委会对各企业的团队报名情况进行审核。

2.团队赛分为“通信企业组”、“互联网企业组”和“网络安全企业组”三个组进行。“通信企业组”每家企业选报不超过3支团队，“互联网企业组”、“网络安全企业组”每家企业选报不超过2支团队。每支团队由3名队员组成，参赛团队名单在上报大赛组委会后原则上不得更换。队员应由本企业的**正式在册工作人员中产生（提供近6个月社保证明）**，参赛人员资格由大赛组委会审核。“通信企业组”选派约16支队伍参赛，“互联网企业组”、“网络安全企业组”各选派约8支队伍。

3.团队赛采用**“攻防对抗”模式**，“通信企业组”、“互联网企业组”和“网络安全企业组”三个组同台竞技、分组排名，总计3小时。

三、奖项设置

（一）个人赛

个人奖项设置为特等奖1名、一等奖2名、二等奖4名、三等奖6名。获奖选手经核准后，给予相应奖励，其中特等奖选手按程序推荐为“广东省五一劳动奖章”候选人，根据粤工办〔2017〕86号文，已获得全国或省级“五一劳动奖章”的选手不参与特等奖评选；个人赛成绩前2名选手由省人社厅按程序授予“广东省技术能手”称号。相关获奖人员将由广东通信行业职业技能鉴定中心按相关规定向工信部教育与考试中心申报相应级别的职业资格证书。

（二）团队赛

团队赛依据每个组别团队成绩高低分别依次排名，“通信企业组”设一等奖1名、二等奖4名、三等奖6名；“互联网企业组”、“网络安全企业组”分设一等奖1名、二等奖2名、三等奖3名。获奖选手经核准后，给予相应奖励。

（三）通报表彰

根据粤工总〔2022〕21号文，个人赛的前5名选手将获得省总工会、省人力资源和社会保障厅、省工业和信息化厅、省科学技术厅四部门联合发文通报表彰，个人赛及团队赛获奖人员也将获得大赛组委会颁发的荣誉证书。

四、时间计划

（一）11月15日前由省内各通信企业自行组织完成个人赛的预赛（团体赛不设预赛）。

（二）11月20日前各参赛单位向大赛组委会报送参加个人和团体比赛的人员名单。

（三）初定12月份组织决赛现场比赛。决赛为期一天，上午举行个人赛决赛，下午举行团队赛以及大赛颁奖仪式。

五、工作要求

（一）请各参赛单位于10月25日前上报工作接口人（姓名，职务，联系方式），反馈至gdca_wac@gd.gov.cn邮箱。

（二）为更好开展大赛组织、宣传、会务等各项工作，确保大赛取得圆满成功，鼓励报名参赛的信息通信行业相关企业对本次大赛予以赞助，我局将按规定监督竞赛经费使用，确保

经费全部用于本次大赛。

六、组织要求

（一）加强领导，精心组织

在本次大赛的筹备与举办过程中，各方均应遵循“公开、公平、公正”原则，认真筹备，精心组织，周密实施，确保赛事顺利完成。各参赛单位要积极做好参赛报名的组织、选拔和赛前练兵等工作，组织好个人预赛以及团队报名。

（二）讲求实用，助力发展

各参赛单位要将开展大赛活动与做好日常工作有机结合，将技能大赛与人才培养有机结合，突出网络安全保障意识，切实提高应对信息通信网络常规性问题和应急问题的实战能力，为我省营造安全清朗的网络空间环境，推动信息通信行业健康发展和持续创新。

（三）重视人才，落实待遇

各参赛单位应高度重视本次大赛活动，把大赛作为岗位练兵的重要举措，提升全体人员的网络安全意识和学习热情，促进相关技能提高，同时也作为发现人才和选拔人才的重要依据。各企业单位应有针对性地建立健全激励机制，制订和落实相应待遇，并逐步完善对参赛优胜选手的职位晋升和薪酬奖励制度。

（四）疫情防控，压实责任

各参赛单位要层层压实疫情防控责任，制定周密方案，从严从实抓好各项疫情防控工作，避免人员扎堆和大量流动，并

根据疫情形势变化和防控政策要求调整活动方式和防控措施。

本次大赛最终解释权归竞赛组委会。组委会有权根据实际情况对竞赛相关事项进行调整。

附件：广东省信息通信行业第四届网络安全技能大赛技术方案

广东省通信管理局

2022 年 10 月 19 日

（联系人：陆冠明，电话：020-87626810）

附件

广东省信息通信行业第四届网络安全技能大赛技术方案

一、大赛背景

为深入贯彻习近平总书记“聚天下英才而用之，为网信事业发展提供有力人才支撑”、“网络空间的竞争，归根结底是人才竞争”等论述精神，积极响应国家网络安全强国战略，加快我省网络安全人才培养和队伍建设，充分发挥技能竞赛对高技能人才培养的引领和促进作用，积累网络安全攻防技术，推动我省网络信息产业持续健康发展，广东省通信管理局拟于今年12月份举办“广东省信息通信行业第四届网络安全技能大赛”（以下简称大赛）。

二、大赛赛制及安排

本次大赛分设**个人赛**及**团队赛**。具体要求如下：

（一）个人赛

1、参赛对象为通信企业，包括广东电信、广东移动、广东联通、广东广电、广东铁塔、广通服和中移互联网的**正式在册工作人员（提供近6个月社保证明）**，参赛人员资格由大赛组委会审核。

2、个人赛分为预赛和决赛两个环节。预赛选拔工作由省内各通信企业自行组织开展，各自选拔产生8至12人进入决赛，

决赛人数原则上不超过 70 人。

3、个人赛决赛由大赛组委会统一集中举行，采用**“理论答题 30%+CFS 综合靶场 70%”**的方式，总计 3.5 小时。

（二）团队赛

1、团队赛采用公开报名和邀请参赛两种方式，面向我省通信企业、互联网企业、网络安全企业。大赛组委会对各企业的团队报名情况进行审核。

2、团队赛分为“通信企业组”、“互联网企业组”和“网络安全企业组”三个组进行。“通信企业组”每家企业选报不超过 3 支团队，“互联网企业组”、“网络安全企业组”每家企业选报不超过 2 支团队。每支团队由 3 名队员组成，参赛团队名单在上报大赛组委会后原则上不得更换。队员应由**本企业的正式在册工作人员中产生（提供近 6 个月社保证明）**，参赛人员资格由大赛组委会审核。“通信企业组”选派 16 支队伍参赛，“互联网企业组”、“网络安全企业组”各选派 8 支队伍。

3、团队赛采用“攻防对抗”模式，“通信企业组”、“互联网企业组”和“网络安全企业组”三个组同台竞技、分组排名，总计 3 小时。

（三）比赛内容及评分标准

1、考点范围

理论答题考点主要包括《网络安全法》、《通信网络安全防护管理办法》、数据安全、移动互联网应用安全、5G 安全，工业

互联网安全、《网络通信安全管理员》教材（通信行业职业技能鉴定中心编，北京邮电大学出版社出版）等法律法规和技术理论知识； 实操试题采用 CFS 综合靶场模式，主要包括基础攻击技能、内网渗透攻击技能、权限维持、免杀等。

详见附件一《竞赛大纲》。

2、竞赛评分标准

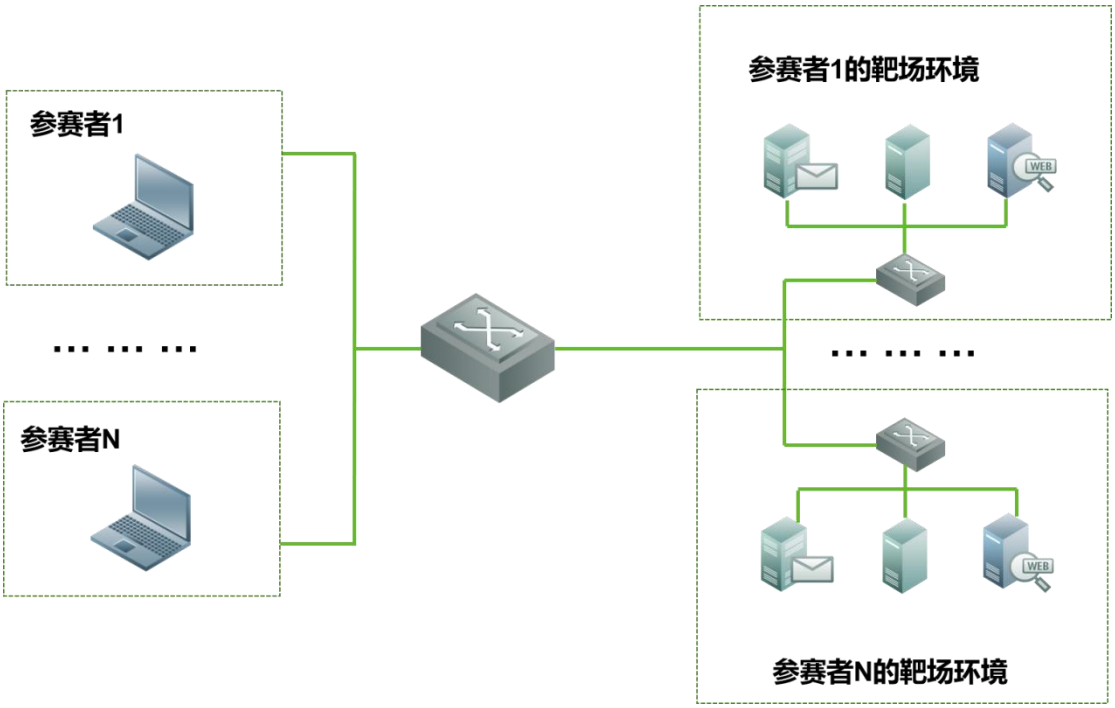
（1）个人赛决赛包含**“理论答题 30%+CFS 综合靶场 70%”**。个人综合靶场模式（CFS）参赛选手在相同比赛环境中根据竞赛系统提示完成相应的关卡考题，通过提交正确答案后获得相应分数。在规定时间内正确完成考题得分最多者获胜，若出现竞赛成绩相同的情况，则根据时间进行排序，即越早达到这一分值的选手排名靠前。

（2）团队赛采用**“攻防对抗”**模式，参赛队伍在竞赛网络空间中互相进行攻击和防守。参赛队伍每队分配一套相同的网络环境，包含若干台防守机，防守机存在若干安全漏洞，参赛队伍需在规定时间内充分挖掘漏洞并利用，提交其他队伍的旗标得分，同时通过修补自身防守机的漏洞进行防御来避免失分。比赛另设置公共夺旗模式的附加题。在规定时间内得分最高的队伍获胜，得分一致则用时最短者获胜。

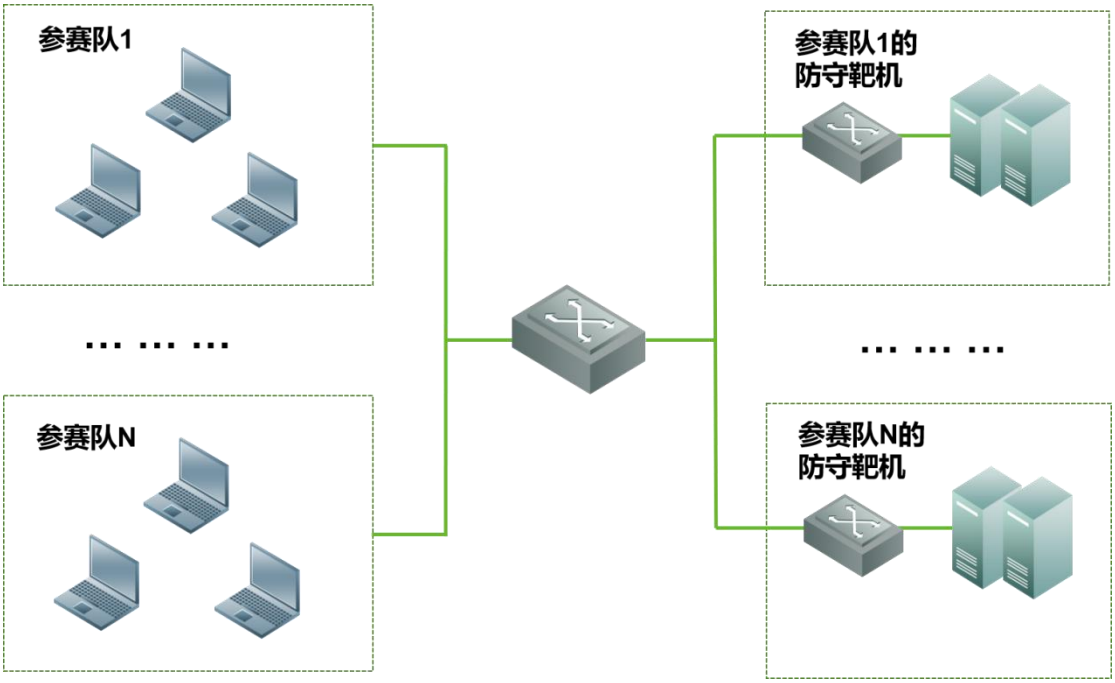
注：任何选手不得通过任何方式扰乱或破坏竞赛环境，一经发现，将直接取消该代表队或选手的参赛资格。

（四）大赛平台系统环境

广东省信息通信行业第四届网络安全大赛使用的系统可全方位模拟真实环境进行个人理论和 CFS 综合靶场、团队攻防对抗实战，并可实时提供参赛人员的比分、排名及相关数据统计分析情况及现场展示。



CFS 综合靶场组网示意图



团队攻防对抗实战组网示意图

各参赛选手需**自带有以太网接口的笔记本电脑（配有线鼠标）**，选手登录大赛系统后，由大赛系统引导进入大赛环境，在大赛环境中通过各种技术手段获得考题答案并提交，答案正确与否系统均会有相应提示。

详见附件二《竞赛样题》。

（五）注意事项

1、选手需要自带电脑、有线鼠标、网络安全类软件工具进入考场；

2、禁止携带网络安全类硬件设备进入考场；

3、禁止根据渗透得到的权限进行特权数据的更改，对赛事环境造成影响；

4、禁止使用 DDOS 攻击考试平台和系统；

5、在竞赛进行期间，需选手填写网络配置确认单进行网络责任归属，由于选手原因造成的网络损坏，后果由选手进行承担；

6、在竞赛进行期间，竞赛场地内将开启信号干扰器、信号屏蔽器等设备，屏蔽现场的手机信号和 WLAN 信号等。

三、本次大赛最终解释权归竞赛组委会。组委会有权根据实际情况对竞赛相关事项进行调整。

附件一:竞赛大纲

（一）政策法规和标准

- 了解中华人民共和国网络安全法的相关内容。掌握安全法所涉及到的角色、应当履行的法律责任与义务。掌握网络安全法在学习、宣传和贯彻实施所涉及的内容;
- 熟悉通信网络等级保护定级范围、评审要求、备案等政策要求;熟知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、定级备案等相关信息;
- 熟悉通信网络安全防护定义、目标、基本原则、体系等内容。熟悉网络单元安全等级划分、定级方法及要素、等级保护原则和实施过程等要求。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;
- 了解安全风险评估工作的国际标准名称(ISO/IEC TR13335、ISOIIEC 17799、ISOIIEC 27001、ISO/IEC TR27103 等),了解《通信网络安全防护管理办法》、《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》等标准和《网络通信安全管理员》教材(通信行业职业技能鉴定指导中心编,

北京邮电大学出版社出版)内容。

(二) 风险评估

- 掌握常规的渗透测试技术。熟练使用各种常见渗透测试工具,渗透测试技术包括:踩点扫描探测、信息收集、暴力破解、常规漏洞利用、Web 权限获取、提权、溢出攻击、植入后门、内网渗透等;
- 熟悉缓冲区溢出、拒绝服务等编码技术,掌握常见安全漏洞的代码审计和代码加固技术,常见漏洞至少包括:缓冲区溢出、拒绝服务、远程命令执行、注入、跨站。

(三) 安全防护

- 熟悉中间件和 Web 应用的安全检测与防护方法。例如框架漏洞、权限绕过、弱口令、注入、跨站、文件包含、文件上传、命令执行、任意文件读取和下载等;了解主流厂商网络设备的调试与配置;
- 了解主流数据库系统的补丁、账号管理、口令强度、有效期检查、远程服务、存储过程、审核层次、备份过程、用户功能和权限控制等基础技术。熟悉数据库库外加密、库内加密、硬件加密等安全措施;深入了解数据库的审计技术、操作系统安全管理、客户端访问控制、入侵检测技术以及数据异地备份等技术实现;

- 掌握主机上操作系统和应用软件的安全配置,主机运行的应用程序、正常运行所必需的端口、服务的正确配置,系统安全风险测试,文件系统、关键数据、配置信息、口令、用户权限等内容的完整性备份。

(四) 应急响应

- 掌握应急响应相关技术。包括:入侵取证分析、日志审计分析等。了解操作系统(Windows、Linux、Unix 等)的常规安全防护技术。能熟练利用系统日志、应用程序日志等溯源攻击途径;掌握系统账号、文件系统、网络参数、服务、日志审计等项目的安全检测与安全加固方法;
- 熟悉有线和无线网络的攻击和防护技术原理和方法。能运用相关工具及技术手段发现并阻断网络层攻击(例如,中间人攻击、DHCP 攻击、DDOS 攻击、无线 DDOS 攻击、无线 WAP jack 攻击等)、验证各种安全防护手段(如,无线网络 WEP WPA 和 WPA2 的密码强度)的有效性和强度;
- 熟悉常见网络设备和安全设备的功能及使用方法。包括:路由器、交换机、防火墙(含 Web 应用防火墙)、入侵检测系统、抗拒绝服务攻击系统、网页防篡改系统、漏洞扫描系统等。

(五) 其他

- 了解密码学的概念、加密体制的分类、常见加密方式与密码

分析工具的利用;

- 掌握隐写术在不同场景下的具体使用;
- 掌握网络攻击原理与常见网络攻击协议;
- 掌握常见 WEB 攻击种类,常见的 WEB 利用方式;
- 掌握注入攻击的类型,注入攻击利用的方式;
- 熟练掌握漏洞产生原因、漏洞的利用与漏洞防护方式;
- 了解物联网安全、无线安全、硬件安全等相关方面的安全问题;
- 熟练掌握恶意代码与逆向技术的常用工具与具体使用方法;
- 熟悉移动互联网恶意程序监测与处置机制,掌握移动应用的逆向分析和代码审计技术、移动应用的安全防护方法等;
- 掌握常见协议分析工具的使用,常见数据包分析方法;
- 熟练使用数据恢复的常用技术等相关知识点内容;
- 熟悉恶意代码的识别方法及防护措施。能运用相关技术发现、隔离、清除常见恶意代码;并能对常见恶意代码进行逆向分析

附件二:竞赛样题

（一）个人赛

理论答题考点主要包括5G安全,工业互联网安全、《网络安全法》、《通信网络安全防护管理办法》、《网络通信安全管理员》教材（通信行业职业技能鉴定中心编，北京邮电大学出版社出版）等法律法规和技术理论知识；实操试题采用CFS综合靶场模式，每个参赛者提供相同的模拟真实企业内部架构的靶场环境，环境由若干存在漏洞的靶机组成，在靶机的关键位置存有Flag文件。参数选手需要按照网络拓扑情况对此环境进行逐层渗透得到Flag并提交,参赛选手需要按照设定的攻击路径完成，并显示最终得分。主要包括基础攻击技能、内网渗透攻击技能、权限维持、免杀等技术。

1. 理论考试样题

例题一：基于哪一项技术的实现也进一步增加了5G网络的灵活性，更好地满足了网络切片灵活构建、上下线的需求(D)

A、 网络切片技术

B、 边缘计算技术

C、 SB技术

D、 NFVSDN虚拟化技术

例题二：以下哪些类别属于工控信息安全产业防护类产品？（D）

A、 边界安全

B、 终端安全

C、 监测审计

D、 以上都是

例题三：根据国际电工委员会制定的工业控制编程语言标准（IEC1131-3），PLC 有五种标准编程语言，请问下面哪一种语言不属于此类？（C）

A、 梯形图语言（LD）

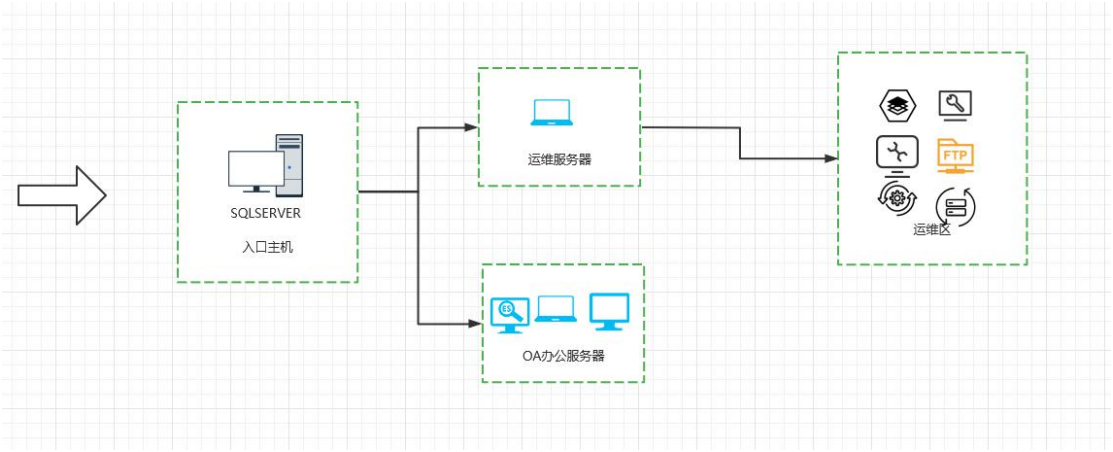
B、 指令表语言（IL）

C、 PHP 语言

D、 功能模块语言（FBD）

2. CFS 实操样题

环境由多个靶机构成，存在多层网络环境。并且靶机中存在一个或多个 flag，每个选手拥有独立的一套环境，选手需要从入口靶机开始渗透，通过一层一层的渗透,获取每个靶机的 flag 进行拿分。



考点一：SQLSEVER 弱口令

nmap 扫描入口主机，发现主机开启 SQLSERVER 服务，随后使用字典爆破 1433 密码，成功登录数据库。并且在数据库表中获取第一个 flag，随后使用 xp_cmdshell 成功获取该主机的低权限。

考点二：权限提升

通过当前 xp_cmdshell 的低权限用户查看进程信息，不存在杀毒软件，使用 CVE-2021-1675 成功提权至 SYSTEM 权限，随后寻找该主机上的敏感文件，最后在 Administrator 用户的桌面 Desktop 中寻找到第二个 flag。

考点三：隧道搭建

查看 SQLSERVER 的网络配置，发现该主机存在两张网卡，并且在查看网络连接情况时发现存在其他网段的主机连接行为，目标主机为办公 OA 系统。因此需要搭建隧道，才能够访问内部办公 OA 系统，进而漏洞利用。使用 ew、iox 等内网代理工具，在 SQLSERVER 主机上开启 socket 隧道，成功将流量代理入办公 OA 端。随后发现该办公 OA 存在漏洞，利用漏洞拿下该主机权限。

考点四：横向移动

在拿下办公 OA 主机权限后，寻找主机上的敏感资料，发现在.ssh 目录中存在 ssh 私钥。扫描当前网段，发现其他主机，并且开启 ssh 端口。接着利用发现的 ssh 私钥成功登录这些主机，并在之上发现了 flag。

考点五：木马免杀

在办公段横向过程中发现部分机器通向运维段，随后搭建隧道，成功访问到运维主机，并通过漏洞利用成功获取该运维主机的

webshell，但权限太低，需要获取交互 shell 进行提权。在查看进程中发现存在杀毒软件，因此需要对木马进行免杀操作。随后使用免杀木马成功获取交互 shell，提权成功后，使用 mimikatz 抓取系统密码，成功获取管理员口令，远程桌面登入，发现打开着笔记软件，上面记录着其他主机的账号密码，随后直接使用运维密码本登录运维段其他主机，成功获取其他 flag。

（二）团队对抗实操样题

第 1 个至第多个混合环境由 N(n 队)个相同环境构成,同时开启,竞赛平台将显示当前团队考题地址,请渗透并对其防御,该团队环境将是其他参赛队的得分环境,本团队提交不得分。提交团队得分,被提交团队扣相应分。竞赛开始前 30 分钟,每个团队只能渗透并加固自己的环境, 30 分钟后可以访问其他团队环境。

考点一：文件上传

漏洞发现：经过测试在会员个人中心中，发现在文章中心存在上

传点。通过抓包工具进行抓包改包，通过绕过文件上传类型限制，从而成功解析，上传成功。

加固：修改程序源码上传类型，限定目录执行权限

考点二：sql 注入

漏洞发现：在首页新闻链接中发现注入点，通过数据库类型判断、后台管理页面查找、表名字段名猜解、数据读取和解密等手段实现后台登录

加固：修改程序源码修复注入漏洞

考点三：命令执行

漏洞发现：登录到后台，发现到函数存在写入权限，通过 getshell 写入一句话木马

加固：修改程序源码修复漏洞