2023

金砖国家职业技能大赛
(金砖国家未来技能挑战赛)

样题 TP(仅供省级选拔赛参考)

BRICS-FS-28-SA_网络安全

2023 年 5 月

一、参加比赛的形式

团队参与，每队 2 名选手（设队长 1 名）。

二、项目项目阶段简介

项目由四个阶段组成，将按顺序完成。向参与者提供答题说明、靶机信息、IP 地址分配表及信息地址分配表。

项目包括以下阶段：

1. 职业素养与理论技能
2. 安全运营
3. 应急响应
4. CTF 夺旗

只有当竞赛环境无法完成并经技能竞赛经理批准时，才能更改项目阶段和标准。

如果竞争对手不遵守要求或使自己和/或其他竞争对手面临危险，则可能会将其从竞争中移除。

阶段项目将根据随机抽签按顺序完成。当参赛者完成模块时，结果将进行评分。

三、项目阶段和所需时间

阶段和时间总结

序号	阶段名称	阶段完成时间
1	第一阶段：职业素养与理论技能	60 分钟
2	第二阶段： 安全运营	90 分钟
3	第三阶段： 应急响应	90 分钟
4	第四阶段： CTF 夺旗	120 分钟

表 1.项目阶段列表

样　题

第一阶段：　职业素养与理论技能

背景：作为信息安全技术人员必须能够掌握操作系统基础、网络基础、数据库基础等相关基础知识，利用这些基础知识进一步学习信息安全技术掌握模糊测试、漏洞挖掘，从而具备成为高水平信息安全人员的基础。

理论阶段题目主要包含职业素养、网络安全、安全运营、应急响应等相关内容，详细内容见下表：

序号	内容模块	说明
第一阶段（理论）	职业素养	网络安全规范意识、安全意识、纪律意识等;
	网络安全	路由器、交换机、防火墙、日志审计、入侵检测等安全组网安全设备管理与安全配置等； 防火墙路由、安全策略、NAT、VPN 等配置和测试； 网络日志系统网络检测、统计、告警等配置； web 应用防火墙防护策略、过滤策略、告警等配置； 无线管理、无线 网络设置、安全策略等配置和测试； 三层交换机路由、 二层安全等配置和测试；
	安全运营	应用系统安全与操作系统安全运营知识点考核；
	应急响应	操作系统和应用系统的日志分析，漏洞分析，系统进程分析，内存分析，系统安全加固，程序逆向分析，编码转换，加解密技术，数据隐写，文件分析取证，网络流量包分析，移动应用程序分析，代码审计等常用渗透与防护管理知识点考核；

项目 1. 职业素养

1. 网页病毒主要通过以下途径传播
   A. 邮件或网盘传送
   B. 文件交换
   C. 网页浏览
   D. 移动媒介
2. 浏览器存在的安全风险主要包含
   A. 网络钓鱼、隐私跟踪
   B. 网络钓鱼 、隐私跟踪 、数据劫持
   C. 隐私跟踪、数据劫持、浏览器的安全漏洞
   D. 网络钓鱼、隐私跟踪、数据劫持、浏览器的安全漏洞
3. 为了防止邮箱邮件爆满而无法正常使用邮箱，您认为应该怎么做
   A. 看完的邮件就立即删除
   B. 期删除邮箱的邮件
   C. 定期备份邮件并删除
   D. 发送附件时压缩附件
4. 可以从哪些方面增强收邮件的安全性
   A. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新防病毒软件
   B. 不断优化垃圾邮件设置、查看邮件数字签名，确认发件人信息、定期更新防病毒软件、邮件传输加密
   C. 全部不是
   D. 查看邮件数字签名，确认发件人信息、定期更新防病毒软件、邮件传输加密
5. 以下说法错误的是
   A. 需要定期更新 QQ 软件
   B. 可以使用非官方提供的 QQ 软件
   C. 不在合作网站轻易输入 QQ 号
   D. 完善保密资料，使用密保工具
6. QQ 密码保护都能使用哪些方式
   A. 密保手机、手机令牌
   B. 密保手机、手机令牌 、QQ 令牌、设置密保问题
   C. 手机令牌、QQ 令牌

D. 密保手机、QQ 令牌、设置密保问题

7. 多久更换一次计算机的密码较为安全
   A. 一个月或一个月以内
   B. 1——3 个月
   C. 3——6 个月
   D. 半年以上或从不更换

8. 以下哪种口令不属于弱口令
   A. 66668888
   B. aabbccdd
   C. 姓名+出生日期
   D. qw@bydp00dwz1.

9. 以下哪个说法是错误的
   A. 随身携带员工卡
   B. 不将员工卡借予其它人
   C. 购买指纹膜，特殊原因时由同事协助打卡
   D. 身份证复印件使用后要销毁

10. 以下哪项是只有你具有的生物特征信息
   A. 指纹、掌纹、手型
   B. 指纹、掌纹、虹膜、视网膜
   C. 指纹、手型、脸型、声音、签名
   D. 指纹、掌纹、手型、虹膜、视网膜、脸型、声音、签名

11. 企业信息安全哪一方面更加重要
   A. 安全设备的采买
   B. 企业人员信息安全意识的提高
   C. 企业安全部门的建立
   D. 企业内部安全制度的建立

12. 发现同事电脑中毒该怎么办
   A. 不关我事，继续办公
   B. 协助同事查找问题
   C. 及时报告给信息安全人员
   D. 用 U 盘把同事电脑里面资料拷到自己电脑里面

13. 第三方公司人员到公司洽谈业务，期间向您要公司无线网络的账号密码，您应该怎么做
   A. 给他一个公用的账号密码。

B. 将自己的账号密码告诉他。

C. 礼貌的告诉他，公司的无线网络使用需要相应审批申请。

D. 让他使用公用电脑上网。

14. 社交网站安全防护建议错误的选项是：(D)

A. 尽量不要填写过于详细的个人资料

B. 不要轻易加社交网站好友

C. 充分利用社交网站的安全机制

D. 信任他人转载的信息

15. 下载安全建议正确的选项是： (D)

A. 选择资源丰富的网站下载

B. 关闭杀毒软件，提高下载速度

C. 下载完成后直接打开下载的文件

D. 下载软件时，最好到软件官方网站或者其他正规软件下载网站下载

项目 2. 网络安全

16. 内网嗅探是主要的内网攻击手段之一，可以利用 Arp 欺骗来在本机上监听同一网段内其余主机的流量包，是比较恶劣且较难防御的攻击手段。一般来说，如果要进行内网嗅探，需要将本机的网卡设置为哪个模式？（ ）

A. 广播模式

B. 组播模式

C. 混杂模式

D. 直接模式

17. 防止用户被冒名所欺骗的方法是（ ）。

A. 对信息源发放进行身份验证

B. 进行数据加密

C. 对访问网络的流量进行过滤和保护

D. 采用防火墙

18. 给电脑设置多道口令，其中进入电脑的第一道口令是（ ）。

A. 系统口令

B. CMOS 口令

C. 文件夹口令

D. 文档密码

19. 攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提

取出信息重新发往 B 称为（ ）。

A. 中间人攻击

B. 口令猜测器和字典攻击

C. 强力攻击

D. 回放攻击

20. 通常黑客扫描目标机的 445 端口是为了( )。

A. 利用 NETBIOS SMB 服务发起 DOS 攻击

B. 发现并获得目标机上的文件及打印机共享

C. 利用 SMB 服务确认 Windows 系统版本

D. 利用 NETBIOS 服务确认 Windows 系统版本

21. 以下哪种攻击可能导致某些系统在重组 IP 分片的过程中宕机或者重新启动？（ ）

A. 分布式拒绝服务攻击

B. Ping of Death

C. NFS 攻击

D. DNS 缓存毒化攻击

22. 下面哪一种攻击方式最常用于破解口令？（ ）

A. 哄骗(spoofing)

B. 字典攻击(dictionary attack)

C. 拒绝服务(DoS)

D. WinNuk

23. Web 应用的认证与会话处理不当，可能被攻击者利用来伪装其他用户身份。强认证手段不包括如下哪种？（ ）

A. 静态密码

B. 短信挑战

C. 指纹认证

D. 图片认证

24. （ ）即攻击者利用网络窃取工具经由网络传输的数据包，通过分析获得重要的信息。

A. 身份假冒

B. 数据篡改

C. 信息窃取

D. 越权访问

25. 以下哪一个最好的描述了数字证书？（ ）

A. 等同于在网络上证明个人和公司身份的身份证

B. 浏览器的一个标准特性，它使得黑客不能得知用户的身份

C. 网站要求用户使用用户名和密码登陆的安全机制

D. 伴随在线交易证明购买的收据

26. TCP SYN Flood 网络攻击时利用了 TCP 建立连接过程需要（ ）次握手的特点而完成对目标进行攻击的。

A. 1

B. 2

C. 3

D. 6

27. 143、有编辑/etc / passwd 文件能力的攻击者可以通过把 UID 变为____就可以成为特权用户。（ ）

A. -1

B. 0

C. 1

D. 2

28. 144、在 windows 系统中，查看本地开放的端口使用的命令是：（ ）

A. net use

B. net share

C. netstat -an

D. arp -a

29. WEB 站点过滤了脚本文件的上传功能，下面哪种文件命名方式可以利用 Apache 的文件解析漏洞( )

A. .php.kzp.rar

B. .php;.gif

C. .php.phpB

D. .phpB;.gif

30. 对于文件名后面有个小点的文件（如 D:\123..），以下说法正确的有：( )

A. 对文件夹删除，需进入 DOS 用 rd 命令删除

B. 双击里面新建文件，均可直接打开

C. 对文件夹可以直接拖到回收站中删除

D. 对于打开文件夹，在 DOS 中 cd 至 D:\盘以后，可以用 start 123..\打开

31. 端口扫描的原理是向目标主机的（ ）端口发送探测数据包，并记录目标主

机的响应。

A. www 服务端口

B. FTP 服务端口

C. UDP 服务端口

D. TCP/IP 服务端口

32. 黑客向受害者发送一封中奖的邮件，要求受害者必须提供银行卡号和对应的密码才能领奖，这种攻击手段属于（）

A. DDOS 攻击

B. 缓存溢出攻击

C. 暗门攻击

D. 钓鱼攻击

33. 下列哪类工具是日常用来扫描 web 漏洞的工具？

A. IBM APPSCAN

B. Nessus

C. NMAPNetwork Mapper

D. X-SCAN

34. 下列哪一项不是黑客在入侵踩点（信息搜集）阶段使用到的技术？

A. 公开信息的合理利用及分析

B. IP 及域名信息收集

C. 主机及系统信息收集

D. 使用 sqlmap 验证 SQL 注入漏洞是否存在

35. 常规端口扫描和半开式扫描的区别是？

A. 没什么区别

B. 没有完成三次握手，缺少 ACK 过程

C. 半开式采用 UDP 方式扫描

D. 扫描准确性不一样

项目 3. 安全运营

36. Bell-LaPadula 安全模型主要关注安全的哪个方面?

A. 可审计

B. 完整性

C. 机密性

D. 可用性

37. 下面哪类控制模型是基于安全标签实现的？

A. 自主访问控制

B. 强制访问控制

C. 基于规则的访问控制

D. 基于身份的访问控制

38. 下面哪个角色对数据的安全负责？

A. 数据拥有者

B. 数据监管人员

C. 用户

D. 安全管理员

39. 系统本身的，可以被黑客利用的安全弱点，被称为？

A. 脆弱性

B. 风险

C. 威胁

D. 弱点

40. 系统的弱点被黑客利用的可能性，被称为？

A. 风险

B. 残留风险

C. 暴露

D. 几率

41. 下列哪一项准确地描述了可信计算基（TCB）？

A. TCB 只作用于固件（Firmware）

B. TCB 描述了一个系统提供的安全级别

C. TCB 描述了一个系统内部的保护机制

D. TCB 通过安全标签来表示数据的敏感性

42. 安全模型明确了安全策略所需的数据结构和技术，下列哪一项最好地描述了安全模型中的“简单安全规则”？

A. Biba 模型中的不允许向上写

B. Biba 模型中的不允许向下读

C. Bell-LaPadula 模型中的不允许向下写

D. Bell-LaPadula 模型中的不允许向上读

43. 为了防止授权用户不会对数据进行未经授权的修改，需要实施对数据的完整性保护，下列哪一项最好地描述了星或（*-）完整性原则？

A. Bell-LaPadula 模型中的不允许向下写

B. Bell-LaPadula 模型中的不允许向上读

C. Biba 模型中的不允许向上写

D. Biba 模型中的不允许向下读

44. 某公司的业务部门用户需要访问业务数据，这些用户不能直接访问业务数据，而只能通过外部程序来操作业务数据，这种情况属于下列哪种安全模型的一部分？

A. Bell-LaPadula 模型

B. Biba 模型

C. 信息流模型

D. Clark-Wilson 模型

45. 作为一名信息安全专业人员，你正在为某公司设计信息资源的访问控制策略。由于该公司的人员流动性较大，你准备根据用户所属的组以及在公司中的职责来确定对信息资源的访问权限，最应该采用下列哪一种访问控制模型？

A. 自主访问控制（DAC）

B. 强制访问控制（MAC）

C. 基于角色访问控制（RBAC）

D. 最小特权（Least Privilege）

46. 下列哪一种访问控制模型是通过访问控制矩阵来控制主体与客体之间的交互？

A. 强制访问控制（MAC）

B. 集中式访问控制（Decentralized Access Control）

C. 分布式访问控制（Distributed Access Control）

D. 自主访问控制（DAC）

47. 下列哪种类型的 IDS 能够监控网络流量中的行为特征，并能够创建新的数据库？

A. 基于特征的 IDS

B. 基于神经网络的 IDS

C. 基于统计的 IDS

D. 基于主机的 IDS

48. 访问控制模型应遵循下列哪一项逻辑流程？

A. 识别，授权，认证

B. 授权，识别，认证

C. 识别，认证，授权

D. 认证，识别，授权

49. 在对生物识别技术中的错误拒绝率（FRR）和错误接收率（FAR）的定义中，下列哪一项的描述是最准确的？

A. FAR 属于类型 I 错误，FRR 属于类型 II 错误

B. FAR 是指授权用户被错误拒绝的比率，FRR 属于类型 I 错误

C. FRR 属于类型 I 错误，FAR 是指冒充者被拒绝的次数

D. FRR 是指授权用户被错误拒绝的比率，FAR 属于类型 II 错误

50. 某单位在评估生物识别系统时，对安全性提出了非常高的要求。据此判断，下列哪一项技术指标对于该单位来说是最重要的？

A. 错误接收率（FAR）

B. 平均错误率（EER）

C. 错误拒绝率（FRR）

D. 错误识别率（FIR）

51. 下列哪种方法最能够满足双因子认证的需求？

A. 智能卡和用户 PIN

B. 用户 ID 与密码

C. 虹膜扫描和指纹扫描

D. 磁卡和用户 PIN

52. 在 Kerberos 结构中，下列哪一项会引起单点故障？

A. E-Mail 服务器

B. 客户工作站

C. 应用服务器

D. 密钥分发中心（KDC）

53. 在下列哪一项访问控制技术中，数据库是基于数据的敏感性来决定谁能够访问数据？

A. 基于角色访问控制

B. 基于内容访问控制

C. 基于上下文访问控制

D. 自主访问控制

54. 数据库管理员在检查数据库时发现数据库的性能不理想，他准备通过对部分数据表实施去除规范化（denormanization）操作来提高数据库性能，这样做将增加下列哪项风险？

A. 访问的不一致

B. 死锁

C. 对数据的非授权访问

D. 数据完整性的损害

55. 下列哪一项不是一种预防性物理控制？

A. 安全警卫

B. 警犬

C. 访问登记表

D. 围栏

56. 对于 Information security 特征,下列说法正确的有()。

A. Information security 是一个系统的安全

B. Information security 是一个动态的安全

C. Information security 是一个无边界的安全

D. Information security 是一个非传统的安全

57. Information security 的对象包括有()。

A. 目标

B. 规则

C. 组织

D. 人员

58. 实施 Information security,需要保证()反映业务目标。

A. 安全策略

B. 目标

C. 活动

D. 安全执行

59. 实施 Information security,需要有一种与组织文化保持一致的(ABCD)Information security 的途 径。

A. 实施

B. 维护

C. 监督

D. 改进

60. 实施 Information security 的关键成功因素包括()。

A. 向所有管理者和员工有效地推广安全意识

B. 向所有管理者、员工及其他伙伴方分发 Information security 策略、指南和标准

C. 为 Information security 管理活动提供资金支持

D. 提供适当的培训和教育

61. National security 组成要素包括()。

A. Information security

B. 政治安全

C. 经济安全

D. 文化安全

62. 下列属于 assets 的有()。

A. 信息

B. 信息载体

C. 人员

D. 公司的形象与名誉

63. Security threats 的特征包括()。

A. 不确定性

B. 确定性

C. 客观性

D. 主观性

64. Manage risk 的方法,具体包括()。

A. 行政方法

B. 技术方法

C. 管理方法

D. 法律方法

65. Manage risk 的基本概念包括()。

A. 资产

B. 脆弱性

C. Security threats

D. 控制措施

66. PDCA 循环的内容包括()。

A. 计划

B. 实施

C. 检查

D. 行动

67. Information security 实施细则中,安全方针的具体内容包括()。

A. 分派责任
B. 约定 Information security 管理的范围
C. 对特定的原则、标准和遵守要求进行说明
D. 对报告可疑安全事件的过程进行说明

68. Information security 实施细则中,Information security 内部组织的具体工作包括()。

A. Information security 的管理承诺
B. Information security 协调
C. Information security 职责的分配
D. 信息处理设备的授权过程

69. Information security 事件分类包括()。

A. 一般事件
B. 较大事件
C. 重大事件
D. 特别重大事件

70. Information security 灾难恢复建设流程包括()。

A. 目标及需求
B. 策略及方案
C. 演练与测评
D. 维护、审核、更新

71. 重要 Information security 管理过程中的技术管理要素包括()。

A. 灾难恢复预案
B. 运行维护管理能力
C. 技术支持能力
D. 备用网络系统

72. Site safety 要考虑的因素有 ()

A. 场地选址
B. 场地防火
C. 场地防水防潮
D. 场地温度控制
E. 场地电源供应

73. 64 Automatic fire alarm 部署应注意()

A. 避开可能招致电磁干扰的区域或设备
B. 具有不间断的专用消防电源
C. 留备用电源
D. 具有自动和子动两种触发装置

74. 为了减小 Lightning loss，可以采取的措施有()

A. 机房内应设等电位连接网络
B. 部署 UPS
C. 设置安全防护地与屏蔽地
D. 根据雷击在不同区域的电磁脉冲强度划分，不同的区域界面进行等电位连接
E. 信号处理电路

75. 会导致 Electromagnetic leakage 的有()

A. 显示器
B. 开关电路及接地系统
C. 计算机系统的电源线
D. 机房内的电话线
E. 信号处理电路

76. Computer information system security 的目标包括（）

A. 信息机密性
B. 信息完整性
C. 服务可用性
D. 可审查性

77. Computer information system security 保护的目标是要保护计算机信息系统的()

A. 实体安全
B. 运行安全
C. Information security
D. 人员安全

78. Computer information system security 包括()

A. 系统风险管理
B. 审计跟踪
C. 备份与恢复
D. 电磁信息泄漏

79. Computer information system security protection 的措施包括()

A. 安全法规
B. 安全管理
C. 组织建设
D. 制度建设

项目 4. 应急响应

80. Computer information system security management 包括()

A. 组织建设
B. 事前检查
C. 制度建设
D. 人员意识

81. Public information network security supervision 工作的性质()

A. 是公安工作的一个重要组成部分
B. 是预防各种危害的重要手段
C. 是行政管理的重要手段

D. 是打击犯罪的重要手段

82. Public information network security supervision 工作的一般原则()

A. 预防与打击相结合的原则
B. 专门机关监管与社会力量相结合的原则
C. 纠正与制裁相结合的原则
D. 教育和处罚相结合的原则

83. Information security officer 应具备的条件:()

A. 具有一定的计算机网络专业技术知识
B. 经过计算机安全员培训，并考试合格
C. 具有大本以上学历
D. 无违法犯罪记录

84. OS 应当提供哪些安全保障()

A. 验证(Authentication)
B. 授权(Authorization)
C. 数据保密性(DataConfidentiality)
D. 数据一致性(DataIntegrity)

85. Windows OS 的"域"控制机制具备哪些安全特性()

A. 用户身份验证
B. 访问控制
C. 审计(Log)
D. 数据通讯的加密

86. 从系统整体看，Security vulnerabilities 包括哪些方面()

A. 技术因素
B. 人的因素
C. 规划，策略和执行过程

87. 从系统整体看，下述那些问题属于系统 Security vulnerabilities()

A. 产品缺少安全功能
B. 产品有 Bugs
C. 缺少足够的安全知识
D. 人为错误

88. 应对操作系统 Security vulnerabilities 的基本方法是什么()

A. 对默认安装进行必要的调整
B. 给所有用户设置严格的口令
C. 及时安装最新的安全补丁
D. 更换到另一种操作系统

89. 造成操作系统 Security vulnerabilities 的原因()

A. 不安全的编程语言
B. 不安全的编程习惯
C. 考虑不周的架构设计

90. 严格的 Password policy 应当包含哪些要素()

A. 满足一定的长度，比如 4 位以上
B. 同时包含数字，字母和特殊字符
C. 系统强制要求定期更改口令
D. 用户可以设置空口令

91. Computer security cases 包括以下几个方面()

A. 重要安全技术的采用
B. 安全标准的贯彻
C. 安全制度措施的建设与实施
D. 重大安全隐患、违法违规的发现，事故的发生

92. Computer security cases 包括以下几个内容()

A. 违反国家法律的行为
B. 违反国家法规的行为
C. 危及、危害计算机信息系统安全的事件

D. 计算机硬件常见机械故障

93. 重大 Computer security accident 可由_____受理()

A. 案发地市级公安机关公共信息网络安全监察部门
B. 案发地当地县级（区、市）公安机关治安部门
C. 案发地当地县级（区、市）公安机关公共信息网络安全监察部门
D. 案发地当地公安派出所

94. Site investigation 主要包括以下几个环节_____()

A. 对遭受破坏的计算机信息系统的软硬件的描述及被破坏程度
B. 现场现有电子数据的复制和修复
C. 电子痕迹的发现和提取，证据的固定与保全
D. 现场采集和扣押与事故或案件有关的物品

95. Computer security accident 原因的认定和计算机案件的数据鉴定,____()

A. 是一项专业性较强的技术工作
B. 必要时可进行相关的验证或侦查实验
C. 可聘请有关方面的专家，组成专家鉴定组进行分析鉴定
D. 可以由发生事故或计算机案件的单位出具鉴定报告

96. 只要选择一种最安全的操作系统，整个系统就可以保障安全。（）

A. 正确
B. 错误

97. Screen saver 的 Password 是需要分大小写的。（）

A. 正确
B. 错误

98. Password 学的基本规则是，你必须让 Password 分析者知道 Encryption 和解密所使用的方法。（）

A. 正确
B. 错误

99. Social engineering，冒充合法用户发送邮件或打电话给管理人员，以骗取用户口令和其他信息；垃圾搜索：Attacker 通过搜索被攻击者的废弃物，得到与系统有关的信息，如果用户将口令写在纸上又随便丢弃，则很容易成为垃圾搜索的 Attack 对象。（）

A. 正确

B. 错误

100. 安全管理从范畴上讲，涉及物理安全策略、访问控制策略、信息 Encryption 策略和 Network security management 策略。（）

A. 正确

B. 错误

第二阶段： 安全运营

背景：作为信息安全技术人员必须能够掌握操作系统加固与安全管控、防火墙一般配置、常见服务配置等相关技能，利用这些技能我们能够进一步保障重要业务平稳运行。

安全运营阶段题目主要包含应用系统安全加固与配置、操作系统安全加固与配置等内容，详细内容见下表：

序号	内容模块	说明
第二阶段（实操）	应用系统安全运营管理	中间件安全运营、数据库安全运营、应用软件安全运营、安全设备运营;
	操作系统安全运营管理	系统安全策略、系统日志、系统帐户安全、系统事件监控、系统应用运营

项目 1. 操作系统安全配置与加固

任务一 Linux 加固

你作为 A 公司的安全运营人员，当前有一部 Linux 系统电脑需要加固，请按照下面要求完成相关操作，保障系统安全运行。

1. Linux 操作系统中修改本地登录显示信息的文件路径为；
2. Linux 操作系统中锁定 user 用户的命令为；
3. Linux 操作系统新建用户的密码最长使用天数需要修改的配置是；
4. Linux 操作系统 SSH 服务禁止空密码登陆需要修改的配置是；
5. Linux 操作系统 SSH 服务允许密码错误次数需要修改的配置是；
6. 查看此 Linux 操作系统中/file/目录下哪个文件既有不可更改属性，又有 SUID 权限，将文件名作为 Flag 进行提交。

项目 2.　应用服务安全

任务二 MySQL 数据库配置

你作为 A 公司的安全运营人员，当前有一部 MySQL 的数据库服务器的需要配置，请按照下面要求完成相关操作，保障系统安全运行。

1. 通过分析数据库服务器的配置，获得 MySQL 当前配置的错误日志路径，将获得的完整错误日志路径作为 flag 值提交，提交格式：flag{******}；
2. 将当前 MySQL 服务器设置为只允许本机访问，将需要修改的配置参数和配置内容作为 flag 值提交，配置参数和配置内容用=分隔，提交格式：flag{***=***}；
3. 当前 MySQL 服务器的密码被遗忘了，现需要通过其他的方式登录到 MySQL 中，获取 flag 数据库中的 flag 值作为 flag 值提交，提交格式：flag{******}；
4. 黑客经常通过 SQL 注入的方式获取系统核心文件，mysql 对本地文件的存取主要通过 LoadDATA LOCAL INFILE 等 SQL 语句实现，对当前的 MySQL 服务进行安全配置，禁止黑客通过数据库获取到系统文件，将需要修改的配置参数和配置内容作为 flag 值提交，配置参数和配置内容用=分隔，提交格式：flag{***=***}；
5. 为了防止弱口令爆破，数据库的密码长应该设有复杂度要求，查看当前 MySQL 配置，将当前 MySQL 密码最少长度要求的值作为 flag 进行提交，提交格式：flag{******}
6. MySQL 安全策略中需要启用登录失败处理功能，查看当前 MySQL 配置，获取登录失败次数限制与登录发生延迟时，延迟的最小时间(单位为毫秒)，将两个值通过/进行分隔，然后作为 flag 进行提交，提交格式：flag{***/***}

第三阶段：　应急响应

背景：作为信息安全技术人员必须能够掌握内容镜像分析、重要数据恢复、恶意文件分析等相关技能，利用这些技能我们能够第一时间分析相关恶意文件、分析蛛丝马迹帮助我们更好的完成应急响应工作。

应急响应阶段题目主要包含安全事件应急响应及数字取证与调查等内容，详细内容见下表：

序号	内容模块	说明
第三阶段（实操）	安全事件应急响应	系统日志分析、进程分析、内存文件分析、木马病毒分析、程序逆向分析、恶意脚本分析、追踪溯源;
	数字取证与调查	网络流量分析、协议流量分析、文件分析取证、编码转换、加解密、数据恢复、数据隐写

项目 1. 安全事件应急响应

任务一 数据泄露应急响应事件

某台服务器由于存在 SQL 注入漏洞，被不法分析获取到了网站的某个管理员的账号和密码，现需要您通过登入到服务器中进行研判分析。（SSH 账号：user，口令：toor）

1. 找到服务器中记录到此次攻击事件的日志文件，将此日志文件的文件名（包括后缀）作为 flag 进行提交；
2. 上一步中找到的日志分析中发现有多个 IP 地址对此服务器进行了访问或者攻击，找到访问或攻击次数最多的 IP 地址，将该 IP 地址字符串通过 SHA256 运算后返回哈希值的十六进制结果作为 Flag 值（形式：十六进制字符串）提交；
3. 找到访问或攻击次数最多的 IP 地址，将此 IP 地址访问和攻击的总次数作为 Flag 进行提交；
4. 哪一个 IP 地址对此服务器发起了 SQL 注入攻击，并最终获取到了 Web 应用中 admin 用户的密码，将该 IP 地址字符串通过 SHA256 运算后返回哈希值的十六进制结果作为 Flag 值（形式：十六进制字符串）提交；
5. 通过日志分析找到被泄露的 Web 应用中 admin 用户的密码，并使用浏览器访问此 Web 应用，使用被泄露的用户名和密码进行登录，获得 Flag 值进行提交。

任务二 漏洞利用应急响应事件

某服务器由于存在漏洞导致黑客可以访问到不该访问的机密文件，现需要你登入到服务器中，通过分析找到此漏洞，并对存在的漏洞进行修复（SSH 账号：user，口令：toor）

1. 找到存在漏洞的应用服务，将此应用服务的名称作为 Flag 进行提交；
2. 黑客利用此漏洞获取了某个机密文件，此机密文件中存在机密信息，将此机密信息解密后作为 Flag 进行提交；
3. 找到存在漏洞的配置文件，将此配置文件在服务器中的绝对路径通过 SHA256 运算后返回哈希值的十六进制结果作为 Flag 值（形式：十六进制字符串）提交
4. 对此漏洞进行修复，靶机中存在自动检测脚本，脚本每 5 分钟运行一次，修复完成后，选手可以到/tmp/secret 文件中查看修复结果。如：Result：Fail（表示失败），Result：Success（表示成功，并会给出 flag 字符串）

项目 2. 电子取证分析

任务三 磁盘分析取证

1. 分析磁盘文件，并对磁盘进行挂载，挂载成功后，在磁盘的 file/目录下获取 Flag 进行提交；
2. 修复磁盘中 img/目录下被损坏的图片文件，并获取 Flag 进行提交；
3. 磁盘的 file/目录下存在被隐藏的文件，找到此隐藏文件并进行恢复，在恢复后的文件中找到 Flag 进行提交；
4. 磁盘中的一些文件已经被删除，将其恢复，并将文件中的机密字符串解密后作为 Flag 进行提交。

第四阶段： CTF 夺旗

背景：作为信息安全技术人员，除了要掌握安全运营、应急响应这些方面安全内容还应该经常参与 CTF 夺旗实战，通过夺旗赛能够进一步提升实战技术能力，磨练选手的耐心，增强选手的学习能力。

CTF 夺旗阶段题目主要包含：Misc 综合、Crypto 加解密、Reverse 逆向、Web 安全、PWN 溢出。

项目 1. Misc 综合

任务一 文件隐写

1. 对压缩包 filezip1.zip 进行破解，获得 Flag 进行提交；
2. 对压缩包 filezip2.zip 进行破解，获得 Flag 进行提交；
3. 对压缩包中包含的文件进行修复，获得 Flag 进行提交。

项目 2. Crypto 加解密

任务二 Crypto1

1. 对题目中给出的密文进行解码与解密，获得 Flag 进行提交

任务三 Crypto2

1. 分析题目附件，使用广播攻击，并编写脚本进行爆破公钥，获得明文 Flag 进行提交

项目 3. Reverse 逆向

任务四 Reverse1

对文件中涉及到的算法进行分析，通过逆推加密过程并解密获得 Flag 进行提交；

项目 4. Web 安全

任务五 Web1

1. 分析题目给出的源代码，并利用源代码中存在的漏洞读取 Flag 进行提交；

任务六 Web2

1. 获取题目源代码，在源代码中找到 Flag 进行提交；
2. 利用题目环境中存在的漏洞，成功登陆到 Web 应用，在登录成功的提示框中获得 Flag 进行提交；
3. 利用题目环境中存在的任意文件漏洞，读取靶机网站根目录下的机密文件内容，将文件内容作为 Flag 进行提交；
4. 利用题目环境中存在的反序列化漏洞，获得靶机服务器权限，并读取靶机服务器根目录下的机密文件内容，将文件内容作为 Flag 进行提交；

项目 5. PWN 溢出

任务七 PWN1

1. 利用栈溢出漏洞，得到服务器运行权限，获取 flag；

任务八 PWN2

1. 利用堆溢出漏洞，得到服务器运行权限，获取 flag；

2023

金砖国家职业技能大赛
（金砖国家未来技能挑战赛）

金砖职赛微信号