网络安全（线下决赛）

BRICS-FS-28_网络安全

2022 年金砖国家职业技能大赛

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	Windows Server 系统与 Linux 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. 以下命令中会哪条会对 Linux 系统造成致命破坏

   A. rm -f *
   B. rm /tmp
   C. yum update
   D. cat /dev/null > /etc/fstab

2. 密钥管理的主要内容包括密钥的那些内容？

   A. 生成、分配、使用、存储、备份、恢复和销毁
   B. 生成、检验、使用、存储、备份、恢复和销毁
   C. 生成、分配、使用、下载、备份、恢复和销毁
   D. 生成、验证、使用、存储、备份、恢复和销毁

3. 常规加密密钥的分配方案，以下描述正确的是？

   A. 使费用减到最小与灾难恢复相结合
   B. 提供足够的能力满足业务需求
   C. 提供合理的担保满足对客户的责任
   D. 及时地生成性能报告

4. 使用 openssl 工具查看证书信息的命令正确的是？

   A. openssl x509 -noout -text -in cert.pem
   B. openssl x509 -noout -text -key cert.pem
   C. openssl genrsa -noout -text -in cert.pem
   D. openssl cert -noout -text -in cert.pem

5. 利用 cfssl 生成证书时可以查看的默认参数正确的是？

   A. config,pem
   B. config,csr
   C. csr,pem
   D. csr,configs

6. 当一个关键文件服务器的存储增长没有被合理管理时，以下哪一项是最大的

风险？

A. 备份时间会稳定增长

B. 备份成本会快速增长

C. 存储成本会快速增长

D. 服务器恢复工作不能满足恢复时间目标（RTO）的要求

7. 在 CMM 标准中，哪一个等级表明组织在软件开发过程中已经建立了定量的质量指标？

A. 可重复级

B. 已定义级

C. 已管理级

D. 优化级

8. 在软件开发过程中，为了让程序内部接口错误能够被尽早发现，下列哪一种测试方法是最有效的？

A. 自底向上测试

B. 白盒测试

C. 自顶向下测试

D. 黑盒测试

9. 在可信计算机系统评估准则（TCSEC）中，下列哪一项是满足强制保护要求的最低级别？

A. C2

B. C1

C. B2

D. B1

10. Clark-Wilson 模型可以满足所有三个完整性安全目标，哪一个是错误的？

A. 防止授权用户不适当的修改

B. 防止非授权用户进行篡改

C. 维持内部和外部的一致性

D. 保障数据和程序安全

11. 在 linux 系统中用哪个命令可以查看文件和目录，显示文件的属性？

A. cat
B. mkdir
C. ls
D. ls －l

12. 在 linux 系统中磁盘分区用哪个命令？

A. parted
B. mv
C. du
D. df

13. 当实施 IT 治理时，决定实施对象的优先级时,下列哪一项是最重要的考虑因素？

A. 过程成熟度
B. 性能指标
C. 商业风险
D. 保证报告

14. 下列措施中哪项不是登录访问控制措施？

A. 审计登录者信息
B. 密码失效时间
C. 密码长度
D. 登录失败次数限制

15. 下列项目中，哪个是专门用于用户身份识别的？

A. PIN
B. 电话号码
C. IP 地址
D. MAC 地址

项目 2. 网络安全

16. 以下哪一种 Data Backup 方式在时间上最快？

A. 增量 Data Backup
B. 差异 Data Backup
C. 完全 Data Backup
D. 磁盘镜像

17. 下面哪项不是 Electromagnetic radiation leakage 防护手段？

A. 红黑电源
B. 屏蔽机房
C. 视频干扰器
D. 防静电服

18. 下面哪类恶意程序可以不接触任何介质，自主传播？

A. 木马
B. 病毒
C. 蠕虫
D. 钓鱼程序

19. 下面那类设备常用于风险分析？

A. Firewall
B. IDS
C. 漏洞扫描器
D. UTM

20. Windows 操作系统的注册表运行命令是：

A. Regsvr32
B. Regegit
C. Regedit.msc
D. Regedit.mmc

21. 安装活动目录时会同时创建 DNS 的主要区域，区域记录不全会导致目录服务

异常，可通过重启 Windows 的（）来重写 DNS 区域？

A. Server 服务
B. NetLogon 服务
C. Messenger 服务
D. NetworkDDE 服务

22. 关闭 Windows 网络共享功能需要关闭（）服务？

A. Server
B. Workstation
C. ServiceLayer
D. Terminal Services

23. AD 中的组策略不可以应用到？

A. 域
B. OU
C. 站点
D. 组

24. EFS encryption 文件系统使用的 encryption 技术是（）。

A. DES
B. 3DES
C. IDEA
D. RSA

25. 下列哪种 IDS 将最有可能对正常网络活动产生错误警报？

A. 基于统计
B. 基于数字 Signature
C. 神经网络
D. 基于主机

26. 一个长期的雇员具有很强的技术背景和管理经验，申请审计部门的一个职位。是否聘用他，应基于个人的经验和____?

A. 服务年限的长短，因为这将有助于确保技术能力。

B. 年龄，（年纪太大的话）在审计技术培训时可能不切实际。

C. 信息系统知识，因为这将加强审计的可信度

D. 能力，作为信息系统审计师，将独立于现有的信息系统

27. 一个组织使用 ERP，下列哪个是有效的访问控制？

A. 用户级权限

B. 基于角色

C. 细粒度

D. 自主访问控制

28. 下列哪一项是预防 CC 攻击的有效手段?

A. 删除可能存在 CC 攻击的页面

B. 提高服务器性能

C. 限制单个 IP 地址每秒访问服务器的次数

D. 使用 IDS 设备

29. 下列针对 Windows 主机安全说法最准确的是

A. 系统重新安装后最安全

B. 系统安装了防病毒和 Firewall 就安全了

C. 把管理员密码长度修改的比较复杂安全

D. 经过专业的安全服务人员根据业务系统的需要进行评估，然后根据评估结果进行安全加固后比较安全

30. 下列哪一项安全机制是一个抽象机，不但确保主体拥有必要的访问权限，而且确保对客体不会有未经授权的访问以及破坏性的修改行为？

A. 安全核心

B. 可信计算基

C. 引用监视器

D. 安全域

31. 下列对安全审计涉及的基本要素说法正确的是？

A. 安全审计可分为实时入侵安全审计和事后审计检测两种

B. 安全审的基本要素是控制目标、安全漏洞、控制措施和控制测试

C. 安全审的基本要素是控制目标、安全漏洞、控制措施和检测

D. 安全审计可分为控制措施和检测控制

32. 下列对安全审计描述最完整的是？

A. 安全审计系统可以对所有明文数据进行审计

B. 安全审计只能审计网站系统

C. 安全审计可以审计数据库

D. 安全审计可以审计网站论坛

33. 某公司在执行灾难恢复测试时，Information security professionals 注意到灾难恢复站点的服务器的运行速度缓慢，为了找到根本原因，他应该首先检查：

A. 灾难恢复站点的错误事件报告

B. 灾难恢复测试计划

C. 灾难恢复计划(DRP)

D. 主站点和灾难恢复站点的配置文件

34. 为了达到组织灾难恢复的要求，备份时间间隔不能超过：

A. 服务水平目标(SLO)

B. 恢复时间目标 (RTO)

C. 恢复点目标 (RPO)

D. 停用的最大可接受程度 (MAO)

35. 某公司正在进行 IT 系统灾难恢复测试，下列问题中的哪个最应该引起关注?

A. 由于有限的测试时间窗，仅仅测试了最必须的系统，其他系统在今年的剩余时间里陆续单独测试

B. 在测试过程中，有些备份系统有缺陷或者不能正常工作，从而导致这些系统的测试失败

C. 在开启备份站点之前关闭和保护原生产站点的过程比计划需要多得多的时间

D. 每年都是由相同的员工执行此测试，由于所有的参与者都很熟悉每一个恢复步骤，因而没有使用灾难恢复计划（DRP）文档

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：操作系统安全加固，iptables 防火墙配置，应用服务安全配置等内容。

项目 1. 系统安全管控

任务一 Windows 加固

你作为 A 公司的安全运营人员，当前有一部 Windows 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. 通过 wmic 工具将当前系统服务简要信息列出，并存储为 html 格式使用的命令是；
2. 通过 wmic 工具将当前系统用户详细信息列出，使用的命令是；
3. 通过 sc 工具管理服务，启动 mysql 服务的命令是；
4. 通过命令行 CMD 管理 Windows 防火墙，允许 192.168.1.100 连接所有端口的命令是；
5. 通过命令行 CMD 配置 Windows 防火墙，阻断 tcp/3389 端口连接的命令是；
6. 通过命令行 CMD 管理 Windows 用户，添加 skill 用户至 administrators 组的命令是。

任务二 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 操作系统中存储实时内存信息文件的路径是；
2. Linux 操作系统中存储开机自动挂载磁盘信息的文件路径是；
3. Linux 操作系统 SSH 服务禁用 root 用户登陆要修改的配置是；
4. Linux 操作系统 SSH 服务开机端口网关需要修改的配置是；
5. Linux 操作系统 VSFTPD 服务默认的匿名用户名是；
6. Linux 操作系统 VSFTPD 服务禁用匿名需要进行的配置是。

项目 2. 防火墙安全管控

任务三 工作站防火墙配置

你作为 A 公司的安全运营人员，当前有一部 Linux 系统的工作站防火墙需要配置，请按照下面要求完成相关操作，保障系统安全运行。

1. 使用 iptables 防火墙控制流量转发，需要操作的链是哪条；
2. 使用 iptables 防火墙控制流量进入，限制进入流量 IP 地址使用的选项是；
3. 使用 iptables 防火墙控制默认规则拒绝所有进入流量，需使用的命令是；
4. 使用 iptables 防火墙配置工作站类型防火墙，出口方向一般执行什么操作；
5. 使用 iptables 防火墙配置 tcp/22 端新建连接速度，需使用的命令是什么；
6. 使用 iptables 防护墙配置 nat 地址转换需要操作哪张表；
7. 使用 iptables 防火墙配置放行从 192.168.1.100 至 192.168.3.100 需使用的命令是；
8. 使用 iptables 防火墙配置工作站类型防火墙时，哪一接口流量应全部放行；
9. 使用 iptables 防火墙配置工作站类型防火墙时，执行什么命令可以清除所有规则。

项目 3. 应用服务安全

任务四 VSFTPD 服务配置

你作为 A 公司的安全运营人员，当前有一部 Linux 系统的 VSFTPD 服务需要配置，请按照下面要求完成相关操作，保障系统安全运行。

1. 配置启用 VSFTPD 虚拟用户的配置是；
2. 配置启用 VSFTPD 虚拟用户文件，用户名 admin 密码 admin 用户文件中如何表示；
3. 配置修改 VSFTPD 服务端口为 2200，firewalld 防火墙需要进行的操作是；
4. 配置修改 VSFTPD 服务端口为 2200，selinux 需要进行的操作是；
5. 配置修改 VSFTPD 服务公共文件夹至/srv/ftp/share，selinux 需要进行的配置是；
6. 使用 hdyra 工具破解 vsftpd 服务密码的命令（用户名：admin 密码字典：password.txt ）是；
7. 使用 medusa 工具破解 vsftpd 服务密码的命令（用户名：admin 密码字典：password.txt ）是。

任务五 文件共享服务配置

你作为 A 公司的安全运营人员，当前有一部 Linux 系统的文件共享服务需要

配置，请按照下面要求完成相关操作，保障文件共享系统安全运行。

1. Linux 操作系统使用 yum 包管理器安装文件共享服务的命令是；
2. Linux 操作系统配置文件共享目录在/srv/samba，selinux 需要进行的配置是；
3. Linux 操作系统配置文件共享服务用户的命令是；
4. Linux 操作系统配置文件共享服务用户，创建新用户 share 的命令是；
5. Linux 操作系统配置文件共享服务匿名用户访问配置是；
6. Linux 操作系统配置文件共享服务共享打印机，默认共享名是；
7. smbclient 工具查看服务器 192.168.1.100 下存在哪些共享目录使用的命令是。

任务六 证书管理服务配置

你作为 A 公司的安全运营人员，当前有一部 Linux 系统的证书管理服务需要配置，请按照下面要求完成相关操作，保障证书分发系统安全运行。

1. 使用 cfssl 工具查看默认请求配置信息使用的命令是
2. 使用 cfssl 工具初始化 CA 证书使用的命令是；
3. 使用 cfssl 工具初始化服务器证书使用的命令是；
4. 使用 cfssl 工具吊销 test 证书使用命令是；
5. 使用 openssl 工具生成 rsa 密钥的命令是；
6. 使用 openssl 工具查看证书信息的命令是。

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：Windows 内存镜像分析，Linux 内存镜像分析，磁盘文件恢复，恶意程序分析等内容。

项目 1. 内存镜像分析

任务一 Windows 内存镜像分析

你作为 A 公司的应急响应人员，请分析提供的内存文件按照下面的要求找到相关关键信息，完成应急响应事件。

1. 从内存中获取到用户 admin 的密码并且破解密码，以 Flag{admin,password}形式提交(密码为 6 位)；
2. 获取当前系统 ip 地址及主机名，以 Flag{ip:主机名}形式提交；
3. 获取当前系统浏览器搜索过的关键词，作为 Flag 提交；
4. 当前系统中存在挖矿进程，请获取指向的矿池地址，以 Flag{ip:端口}形式提交；
5. 恶意进程在系统中注册了服务，请将服务名以 Flag{服务名}形式提交。

项目 2. 机密数据恢复

任务二 财务数据恢复

你作为 A 公司的应急响应人员，请分析提供的磁盘文件按照下面的要求找到相关关键信息，完成应急响应事件。

1. 分析磁盘镜像中的文件系统，找到关键财务证据一
2. 分析磁盘镜像中的文件系统，找到关键财务证据二
3. 分析磁盘镜像中的文件系统，找到关键财务证据三
4. 分析磁盘镜像中的文件系统，找到关键财务证据四
5. 分析磁盘镜像中的文件系统，找到关键财务证据五
6. 分析磁盘镜像中的文件系统，找到关键财务证据六
7. 分析磁盘镜像中的文件系统，找到关键财务证据五
8. 分析磁盘镜像中的文件系统，找到关键财务证据六

任务三 快递运单信息恢复

你作为 A 公司的应急响应人员，请分析提供的流量包文件按照下面的要求找到相关关键信息，完成应急响应事件。

1. 分析提供的流量包，找到系统运单信息相关数据一
2. 分析提供的流量包，找到系统运单信息相关数据二
3. 分析提供的流量包，找到系统运单信息相关数据三
4. 分析提供的流量包，找到系统运单信息相关数据四
5. 分析找到的运单系统管理员的密码库，尝试破解密码一
6. 分析找到的运单系统管理员的密码库，尝试破解密码二
7. 分析找到的运单系统管理数据，找到关键运单记录一
8. 分析找到的运单系统管理数据，找到关键运单记录二

任务四 加密系统破解

你作为 A 公司的应急响应人员，请分析提供的残缺脚步文件按照下面的要求找到相关关键信息，完成应急响应事件。

1. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F1 字符串，将该字符串通过 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；
2. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F2 字符串，将该字符串通过 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. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F3 字符串，将该字符串通过 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；
4. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F4 字符串，将该字符串通过 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. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F5 字符串，将该字符串通过 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；
6. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F6 字符串，将该字符串通过 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；
7. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F7 字符串，将该字符串通过 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；

8. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F8 字符串，将该字符串通过 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；
9. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，填写该文件当中空缺的 F9 字符串，将该字符串通过 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；
10. 编辑 Python 程序 ssh_brute_force.py 文件，利用 superdic.txt 密码字典文件，使该程序实现暴力破解服务器场景 SSH 服务登录密码的功能，运行该程序，将程序运行后得到的正确密码通过 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。

项目 3. APT 攻击溯源

任务五 攻击流量溯源

你作为 A 公司的应急响应人员，公司内某重要部门操作 APT 攻击，现捕获到相关流量请你按照下面的要求找到关键信息，完成应急响应事件。

1. 使用 Wireshark 查看并分析服务器场景桌面下的 login.pcapng 数据包文件，通过分析数据包 login.pcapng 的第 130 号报文，找出黑客提交的有效命令，并将该有效命令作为 FLAG（形式：[命令]）提交；
2. 继续查看数据包文件 login.pacapng，分析出黑客又执行了什么命令，并将该有效命令作为 FLAG（形式：[命令]）提交；
3. 继续查看数据包文件 login.pacapng 分析出黑客执行上述命令后，得到的结果中的多个 IP 地址作为 FLAG（形式：[IP 地址 1:IP 地址 2:IP 地址 n]）提交；
4. 继续查看数据包文件 login.pacapng 分析出黑客执行上述命令后，得到的结果中的最后 1 个物理地址作为 FLAG（形式：[物理地址]）提交；
5. 继续查看数据包文件 login.pacapng 分析出黑客建立映射使用的有效命令，并将该命令中的 IP 地址作为 FLAG（形式：[IP 地址]）提交；
6. 继续查看数据包文件 login.pacapng 分析出黑客建立映射使用的有效命令，并将该命令中的用户名作为 FLAG（形式：[用户名]）提交；
7. 继续查看数据包文件 login.pacapng 分析出黑客建立映射使用的有效命令，并将该命令中的密码作为 FLAG（形式：[密码]）提交。

任务六 服务器日志分析

你作为 A 公司的应急响应人员，公司内一重要服务器遭到攻击，被攻击时捕获到该流量包请按照下面的要求获取关键信息，完成应急响应事件。

1. 使用 Wireshark 查看并分析服务器场景桌面下的 logs.pcapng 数据包文件，通过分析数据包 logs.pcapng 找出恶意用户目录扫描的第 9 个文件，并将该文件名作为 FLAG（形式：[robots.txt]）提交；

2. 继续查看数据包文件 logs.pcapng，分析出恶意用户扫描了哪些端口，并将全部的端口作为 FLAG（形式：[端口名 1，端口名 2，端口名 3…，端口名 n]）从低到高提交；
3. 继续查看数据包文件 logs.pcapng 分析出恶意用户读取服务器的文件名是什么，并将该文件名作为 FLAG（形式：[robots.txt]）提交；
4. 继续查看数据包文件 logs.pcapng 分析出恶意用户写入一句话木马的路径是什么，并将该路径作为 FLAG（形式：[/root/whoami/]）提交；
5. 继续查看数据包文件 logs.pcapng 分析出恶意用户连接一句话木马的密码是什么，并将一句话密码作为 FLAG（形式：[一句话密码]）提交；
6. 继续查看数据包文件 logs.pcapng 分析出恶意用户下载了什么文件，并将文件名及后缀作为 FLAG（形式：[文件名.后缀名]）提交；
7. 继续查看数包文件 logs.pcapng 将恶意用户下载的文件里面的内容作为 FLAG（形式：[文件内容]）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：注入攻击，模版逃逸，序列化漏洞，服务漏洞等相关内容。

项目 1. 注入攻击

任务一 命令注入

1. 打开渗透机上的火狐浏览器，在地址栏输入靶机服务器的 IP 地址访问网页，使用默认用户名 admin 密码 password 登录，在登陆后的 DVWA 页面点击左边导航栏的“DVWA Security”按钮，修改难易程度为“low”，然后点击“Submit” 提交。点击“Command Injection”输入靶机服务器 IP，可以看到正常返回数据，将返回数据的最后一行的第 1 个单词作为 Flag 值提交。
2. 构造语句用于显示操作系统中的用户，将构造语句中除 IP 地址以外的部分作为 Flag 值提交。
3. 在 DVWA 页面点击“DVWA Security” 选择难易程度为“medium”，然后点击“Submit” 提交，再次利用上述构造语句用于显示系统中的用户，发现报错，将返回结果的倒数第 2 个单词作为 Flag 值提交。
4. 点击“view_source”查看源代码，将源码中用于防御注入的过滤内容以 F1.F2 形式作为 Flag 值提交。
5. 重新构造语句用于显示操作系统中的用户，可以看到正常返回数据，将重新构造语句中除 IP 地址以外的部分作为 Flag 值提交。
6. 在 DVWA 页面点击“DVWA Security” 选择难易程度为“high”，然后点击“Submit”提交，将上一步中重新构造的语句重新进行提交，发现报错，点击“view_source”查看源代码，发现服务器端对 IP 参数进一步做了一定过滤，将源码中第 3 个过滤的内容作为 Flag 值提交。
7. 再次构造语句用于显示操作系统中的用户，可以看到正常返回数据，将再次构造语句中除 IP 地址以外的部分作为 Flag 值提交。
8. 再次构造语句用于显示操作系统中的用户，可以看到正常返回数据，将返回的用户列表中的最后一个用户名作为 Flag 值提交。

任务二 SQL 注入

1. 该系统存在漏洞，登陆系统找到隐藏信息，并将 flag 提交;
2. 该系统存在漏洞，找到当前 WEB 系统所使用的数据库用户名;

3. 该系统存在漏洞，找到数据库中的隐藏信息，并将 flag 提交。

项目 2. 序列化漏洞

任务三 序列化链式利用

1. 访问靶机地址，将靶机 PHP 环境中的 PHP_SHA256 值作为 flag 提交；
2. 访问靶机地址，将完成题目需要提交的通过 GET 方式发送的变量 content 前 6 位作为 flag 提交；
3. 访问靶机地址，将完成题目需要配置的特殊 HTTP 头变量的名字做为 flag 提交；
4. 访问靶机地址，将完成题目需要绕过的函数名作为 flag 提交；
5. 访问靶机地址，将完成题目需要使用的请求方式作为 flag 提交；
6. 访问靶机地址，利用题目中的反序列化漏洞将靶机环境中的 flag 提交。

任务四 序列化字符串逃逸

1. 访问靶机 8081 端口，将通过伪协议查看 index.php 文件的 payload 作为 flag 提交；
2. 将完成发序列化字符串逃逸所得到的结果作为 flag 提交；
3. 完成 POP 链式反序列化并将得到的文件名作为 flag 提交；
4. 破解上一题目找到的文件，将找到的文件名作为 flag 提交；
5. 破解上一题目找到的文件，将找到的文件名作为 flag 并提交；
6. 利用找到的信息登录系统完成提权，获得最终 flag 并提交。

项目 3. 服务漏洞

任务五 文件上传

访问靶机地址 9000 端口并将页面中用户显示代码的函数名称，作为 flag 提交；

将程序中 session 的类型作为 flag 提交；

将获得 admin 用户权限需要设置的 PHPSSID 作为 flag 提价；

将完成题目需要上传的文件名前四位作为 flag 提交；

将题目环境中 session 文件保存位置作为 flag 提交；

将下载到的 session 文件的最后 9 位最为 flag 提交；

将/app/session/success.txt 类型作为 flag 提交；

完成题目，将最后获得的 flag 值作为 flag 提交。

任务六 缓冲区溢出漏洞

1. 从靶机服务器的 FTP 上下载 flag0001.exe，分析该文件，请提交程序使用的加密函数；
2. 请提交程序正常运行使用的 Key 值；
3. 请提交溢出点地址；
4. 请提交加密算法使用的秘钥；
5. 请提交最终 flag 的值。