2024年甘肃省职业院校技能大赛
高职学生组电子与信息大类信息安全管理与评估赛项
样题三

竞赛需要完成三个阶段的任务，分别完成三个模块，总分共计 1000 分。三个模块内容和分值分别是：

1.第一阶段：模块一 网络平台搭建与设备安全防护（180 分钟，300 分）。

2.第二阶段：模块二 网络安全事件响应、数字取证调查、应用程序安全（180 分钟，300 分）。

3.第三阶段：模块三 网络安全渗透、理论技能与职业素养（180 分钟，400 分）。

【注意事项】

1.第一个阶段需要按裁判组专门提供的U 盘中的“XXX-答题模板”提交答案。

第二阶段请根据现场具体题目要求操作。

第三阶段网络安全渗透部分请根据现场具体题目要求操作，理论测试部分根据测试系统说明进行登录测试。

2.所有竞赛任务都可以由参赛选手根据基础设施列表中指定的设备和软件完成。

第一阶段

模块一 网络平台搭建与设备安全防护

一、竞赛内容

第一阶段竞赛内容包括：网络平台搭建、网络安全设备配置与防护，共 2 个子任务。

竞赛阶段	任务阶段	竞赛任务	竞赛时间	分值
第一阶段 网络平台搭建与设备安全防护	任务 1	网络平台搭建	XX:XX-XX:XX	50
	任务 2	网络安全设备配置与防护		250
总分				**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

第一阶段请按裁判组专门提供的 U 盘中的“XXX-答题模板”中的要求提交答案。

选手需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），所完成的“XXX-答题模板”放置在文件夹中作为竞赛结果提交。

例如：08 工位，则需要在 U 盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

【特别提醒】

只允许在根目录下的“GWxx”文件夹中体现一次工位信息，不允许在其它文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

四、赛项环境设置

1.网络拓扑图

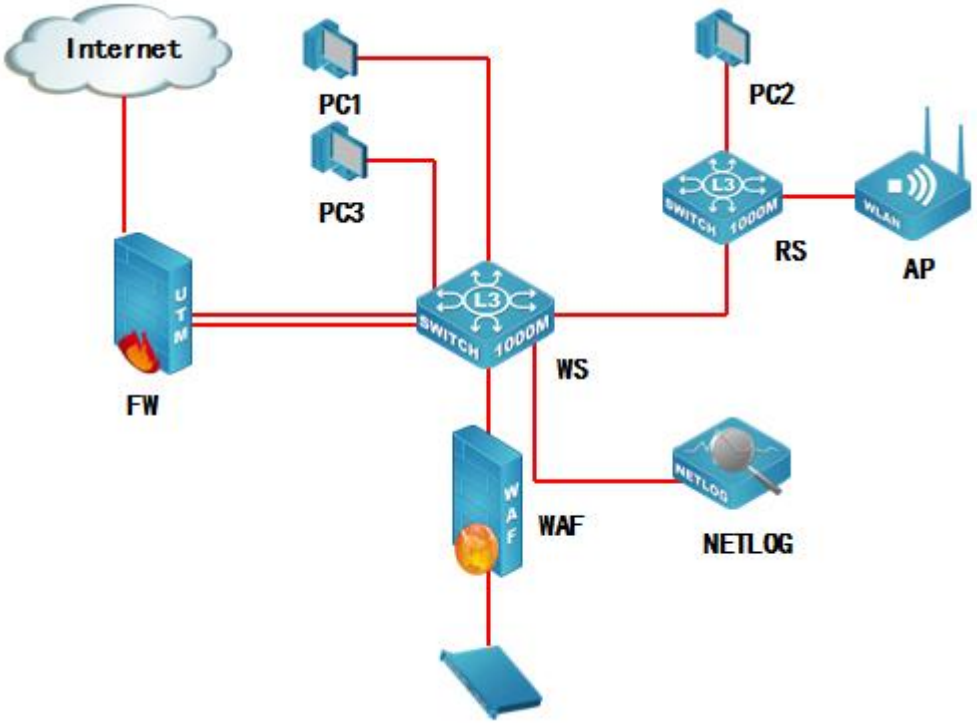

图 1 网络拓扑

2.IP 地址规划表

设备名称	接口	IP地址	对端设备
防火墙FW	ETH0/1	9.0.0.1/30 （Trust安全域）	WS
	ETH0/2	10.0.0.1/30 （untrust安全域）	
	ETH0/3	11.0.0.1/30 （Trust安全域）	WS
	ETH0/4	12.0.0.1/30 （Trust安全域）	WS
	ETH0/5	218.5.18.1/27（untrust安全域）	INTERNET
	SSL Pool	192.168.10.1/24 可用IP数量为20	SSL VPN地址池
三层无线交换机 WS	ETH1/0/1-2	10.0.0.2/30	FW
	VLAN 51 ETH1/0/3	10.0.0.10/30	NETLOG
	VLAN 52 ETH1/0/22	172.16.100.1/24	WAF
	VLAN 10	172.16.10.1/24	无线1
	VLAN 20	172.16.20.1/25	无线2
	VLAN 30 ETH1/0/3	172.16.30.1/26	PC1
	VLAN 50 ETH1/0/5	172.16.50.1/26	PC3
	ETH1/0/20 VLAN 100	192.168.100.1/24	RS
三层交换机 RS	ETH1/0/1 VLAN 100	192.168.100.254/24	WS
	无线管理VLAN	192.168.101.1/24	AP

	VLAN 101 ETH1/0/2		
	VLAN 40 ETH1/0/4	172.16.40.1/26	PC2
日志服务器 NETLOG	ETH2	10.0.0.9/30	WS
WEB应用防火墙 WAF	ETH2	172.16.100.2/24	
	ETH3		RS
堡垒服务器	-	-	WAF

第一阶段 任务书

任务 1 网络平台搭建（50 分）

题号	网络需求
1	按照 IP 地址规划表，对防火墙的名称、各接口 IP 地址进行配置
2	按照 IP 地址规划表，对三层交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN, 对各接口 IP 地址进行配置
3	按照 IP 地址规划表，对无线交换机的名称进行配置，创建 VLAN 并将相应接口划入 VLAN,对接口 IP 地址进行配置
4	按照 IP 地址规划表，对网络日志系统的名称、各接口 IP 地址进行配置
5	按照 IP 地址规划表，对 Web 应用防火墙的名称、各接口 IP 地址进行配置

任务 2 网络安全设备配置与防护（250 分）

1. RS 和 WS 开启 telnet 登录功能，配置使用 telnet 方式登录终端界面前显示如下授权信息: “WARNING!!! Authorised access only, all of your done will be recorded! Disconnected IMMEDIATELY if you are not an authorised user! Otherwise, we retain the right to pursue the legal responsibility”。
2. 总部部署了一套网管系统实现对核心 RS 进行管理，网管系统 IP 为: 172.16.100.21，读团体值为: ABC2022，版本为 V2C， RS Trap 信息实时上报网管，当 MAC 地址发生变化时，也要立即通知网管发生的变化，每 35s 发送一次；
3. RS 出口往返流量发送给 NETLOG，由 NETLOG 对收到的数据进行用户所要求的分析;
4. 对 RS 上 VLAN40 开启以下安全机制:

   业务内部终端相互二层隔离，启用环路检测，环路检测的时间间隔为 10s，发现环路以后关闭该端口，恢复时间为30分钟； 如私设DHCP服务器关闭该端口; 防止ARP欺骗攻击；

5. 配置使总部 VLAN10，30，40 业务的用户访问 INTERNET 往返数据流都经过 FW 进行最严格的安全防护；RS 使用相关 VPN 技术，模拟 INTERNET ，VPN 名称为 INTERNET 地址为 218.5.18.2；
6. WS 与 RS 之间配置 RIPng， 是 VLAN30 与 VLAN50 可以通过 IPv6 通信；

   IPv6业务地址规划如下，其它IPv6地址自行规划:

业务	IPV6 地址
VLAN30	2001::30::254/64
VLAN50	2001::50::254/64

7. FW、RS、WS 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义；
8. 为了有效减低能耗，要求每天晚上 20:00 到早上 07:00 把 RS 端口指示灯全部关闭；如果 RS 的 11 端口的收包速率超过 30000 则关闭此端口，恢复时间 5 分钟，并每隔 10 分钟对端口的速率进行统计；为了更好地提高数据转发的性能，RS 交换中的数据包大小指定为 1600 字节；
9. 为实现对防火墙的安全管理，在防火墙 FW 的 Trust 安全域开启 PING, HTTP，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能;
10. 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP: 218.5.18.9、218.5.18.10；
11. 远程移动办公用户通过专线方式接入总部网络，在防火墙 FW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 ABC2021，地址池参见地址表；
12. 为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行最小带宽设置为 2M，下行最大带宽设置为 4M; 为净化上网环境，要

求在防火墙 FW 做相关配置，禁止无线用户周一至周五工作时间 9：00-18：00 的邮件内容中含有“病毒”、“赌博”的内容，且记录日志；

13. 在公司总部的 NETLOG 上配置，设备部署方式为旁路模式，并配置监控接口与管理接口。增加非 admin 账户 NETLOG2022，密码 NETLOG2022，该账户仅用于用户查询设备的日志信息和统计信息。使 NETLOG 能够通过邮件方式发送告警信息，邮件服务器在服务器区，IP 地址是 172.16.10.200，端口号 25，账号 test，密码 test; NETLOG 上配置 SNMPv3，用户名 admin，MD5 秘钥 adminABC，配置日志服务器与 NTP 服务器，两台服务器地址：172.16.10.200；
14. 在公司总部的 NETLOG 上配置，监控工作日（每周一到周五）期间 PC1 网段访问的 URL 中包含 xunlei 的 HTTP 访问记录，并且邮件发送告警。监控 PC2 网段所在网段用户的即时聊天记录。监控内网所有用户的邮件收发访问记录。
15. NETLOG 配置应用及应用组“P2P 视频下载”，UDP 协议端口号范围 65531-65631，在周一至周五 8：00-20：00 监控内网中所有用户的“P2P 视频下载”访问记录；
16. NETLOG 配置对内网 ARP 数量进行统计，要求 30 分钟为一个周期；NETLOG 配置开启用户识别功能，对内网所有 MAC 地址进行身份识别；
17. NETLOG 配置统计出用户请求站点最多前 20 排名信息，发送到邮箱为 bn2022@chinaskills.com；
18. 公司内部有一台网站服务器直连到 WAF，地址是 RS 上 VLAN10 网段内的第五个可用地址，端口是 8080，配置将服务访问日志、WEB 防护日志、服务监控日志信息发送 syslog 日志服务器， IP 地址是服务器区内第六个可用地址，UDP 的 514 端口;

19. 在公司总部的 WAF 上配置，阻止常见的 WEB 攻击数据包访问到公司内网服务器，防止某源 IP 地址在短时间内发送大量的恶意请求，影响公司网站正常服务。
20. 大量请求的确认值是：10 秒钟超过 3000 次请求;编辑防护策略，定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击;
21. WAF 上配置开启爬虫防护功能，当爬虫标识为 360Spider，自动阻止该行为；WAF 上配置阻止用户上传 ZIP、DOC、JPG、RAR 格式文件;WAF 上配置编辑防护策略，要求客户机访问内部网站时，禁止访问 *. bat 的文件;
22. WAF 上配置，使用 WAF 的漏洞立即扫描功能检测服务器（172.16.10.100）的安全漏洞情况，要求包括信息泄露、SQL 注入、跨站脚本编制;
23. 在公司总部的 WAF 上配置， WAF 设备的内存使用率超过 50%每隔 5 分钟发送邮件和短信给管理，邮箱 bn2022@digitalchina. com，手机 13912345678；在公司总部的 WAF 上配置，将设备状态告警、服务状态告警信息通过邮件（发送到 bn2022@digitalchina. com）及短信方式(发送到 13812345678)发送给管理员;
24. WS 上配置 DHCP，管理 VLAN 为 VLAN101,为 AP 下发管理地址，保证完成 AP 注册； 为无线用户 VLAN10,20, 有线用户 VLAN 30,40 下发 IP 地址；
25. 在 NETWORK 下配置 SSID，需求如下:

    1、NETWORK 1下设置SSID ABC2021，VLAN10，加密模式为wpa-personal,其口令为ABCE2022；

    2、NETWORK 2下设置SSID GUEST，VLAN20不进行认证加密,做相应配置隐藏该SSID；

26. NETWORK 1 开启内置 portal+本地认证的认证方式，账号为 ABC 密码为 ABCE2022；
27. 配置 SSID GUEST 每天早上 0 点到 6 点禁止终端接入；GUSET 最多接入 10 个用户，并对 GUEST 网络进行流控，上行 1M，下行 2M；配置所有无线接入用户相互隔离；
28. 配置当 AP 上线，如果 AC 中储存的 Image 版本和 AP 的 Image 版本号不同时，会触发 AP 自动升级；配置 AP 发送向无线终端表明 AP 存在的帧时间间隔为 1 秒；配置 AP 失败状态超时时间及探测到的客户端状态超时时间都为 2 小时；配置 AP 在脱离 AC 管理时依然可以正常工作；
29. 为防止外部人员蹭网，现需在设置信号值低于 50%的终端禁止连接无线信号；为防止非法 AP 假冒合法 SSID，开启 AP 威胁检测功能；
30. RS、WS 运行静态组播路由和因特网组管理协议第二版本；PC1 启用组播，使用 VLC 工具串流播放视频文件 1.mpg，组地址 228.10.10.9，端口：5678，实现 PC2 可以通过组播查看视频播放。
31. 在公司总部的 BC 上配置，设备部署方式为透明模式。增加非 admin 账户 skills01，密码 skills01，该账户仅用于用户查询设备的日志信息和统计信息；要求对内网访问 Internet 全部应用进行日志记录。
32. 在 BC 上配置激活 NTP，本地时区+8:00，并添加 NTP 服务器名称清华大学，域名为 s1b.time.edu.cn。
33. BC 配置内容管理，对邮件内容包含“比赛答案”字样的邮件， 记录且邮件报警。
34. BI 监控周一至周五工作时间 VLAN40 用户使用“迅雷”的记录， 每天工作时间为 9:00-18:00。
35. 在公司总部的 WAF 上配置，设备部署方式为透明模式。要求对内网 HTTP 服务器 172.16.10.45/32 进行安全防护。

36. 方便日志的保存和查看，需要在把 WAF 上攻击日志、访问日志、DDoS 日志以 JSON 格式发给 IP 地址为 172.16.10.200 的日志服务器上。
37. 在 WAF 上配置基础防御功能，开启 SQL 注入、XXS 攻击、信息泄露等防御功能，要求针对这些攻击阻断并发送邮件告警。
38. 为防止 www.2023skills.com 网站资源被其他网站利用，通过 WAF 对资源链接进行保护，通过 Referer 方式检测，设置严重级别为中级，一经发现阻断并发送邮件告警。
39. 在公司总部的 WAF 上配置，编辑防护策略，定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击。
40. 对公司内网用户访问外网进行网页关键字过滤，网页内容包含“暴力”“赌博”的禁止访问。

第二阶段

模块二 网络安全事件响应、数字取证调查、应用程序安全

一、竞赛内容

第二阶段竞赛内容包括：网络安全事件响应、数字取证调查和应用程序安全。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第二阶段	网络安全事件响应	任务 1	应急响应	XX:XX	100
	数字取证调查	任务 2	计算机单机取证		100
	应用程序安全	任务 3	代码审计		100
总分					**300**

二、竞赛时长

本阶段竞赛时长为 180 分钟，共 300 分。

三、注意事项

1.本部分的所有工作任务素材或环境均已放置在指定的计算机上，参赛选手完成后，填写在电脑桌面上“信息安全管理与评估竞赛-第二阶段答题卷”中。

2.选手的电脑中已经安装好 Office 软件并提供必要的软件工具（Tools 工具包）。

【特别提醒】

竞赛有固定的开始和结束时间，选手必须决定如何有效的分配时间。请阅读以下指引！

1.当竞赛结束，**离开时请不要关机；**

2.所有配置应当在重启后有效；

3.除了 CD-ROM/HDD/NET 驱动器，请不要修改实体机的配置和虚拟机本身的硬件设置。

第二阶段 任务书

任务描述

随着网络和信息化水平的不断发展，网络安全事件也层出不穷，网络恶意代码传播、信息窃取、信息篡改、远程控制等各种网络攻击 行为已严重威胁到信息系统的机密性、完整性和可用性。因此，对抗 网络攻击，组织安全事件应急响应，采集电子证据等技术工作是网络 安全防护的重要部分。现在，A 集团已遭受来自不明组织的非法恶意攻击，您的团队需要帮助 A 集团追踪此网络攻击来源，分析恶意攻击行为的证据线索，找出操作系统和应用程序中的漏洞或者恶意代码， 帮助其巩固网络安全防线。

本模块主要分为以下几个部分：

- 网络安全事件响应；
- 数字取证调查；
- 应用程序安全。

第一部分 网络安全事件响应

任务1 应急响应（100 分）

A 集团的 WebServer 服务器被黑客入侵，该服务器的 Web 应用系统被上传恶意软件，系统文件被恶意软件破坏，您的团队需要帮助该公司追踪此网络攻击的来源，在服务器上进行全面的检查，包括日志信息、进程信息、系统文件、恶意文件等，从而分析黑客的攻击行为，

和残留的关键证据信息。

本任务素材清单：**Server** 服务器虚拟机

受攻击的Server 服务器已整体打包成虚拟机文件保存，请选手自行导入分析。

虚拟机用户名：root，密码：123456，若题目中未明确规定，请使用默认配置。

请按要求完成该部分工作任务，答案有多项内容的请用换行分隔。

任务 1 应急响应		
序号	**任务要求**	**答案**
1	提交攻击者的两个内网 IP 地址	
2	提交网站管理员用户的用户名与密码	
3	提交黑客得到MySQL 服务的root 账号密码的时间（格式：dd/MM/yyyy:hh:mm:ss）	
4	查找黑客在 Web 应用文件中写入的恶意代码，提交文件绝对路径	
5	查找黑客在 Web 应用文件中写入的恶意代码，提交代码的最简形式（格式：<?php xxxx?>）	
6	分析攻击者的提权手法，提交攻击者通过哪一个指令成功提权	
7	服务器内与动态恶意程序相关的三个文件绝对路径	
8	恶意程序对外连接的目的 IP 地址	

第二部分 数字取证调查

任务2 计算机单机取证（100 分）

对给定取证镜像文件进行分析，搜寻证据关键字（线索关键字为“evidence 1”“evidence 2”……“evidence 10”，有文本形式也有图片形式，不区分大小写），请提取和固定比赛要求的标的证据文件，并按样例的格式要求填写相关信息，证据文件在总文件数中所占比例不低于15%。取证的信息可能隐藏在正常的、已删除的或受损的文件中，您

可能需要运用编码转换技术、加解密技术、隐写技术、数据恢复技术，还需要熟悉常用的文件格式（如办公文档、压缩文档、图片等）。

本任务素材清单：取证镜像文件

请根据赛题环境及现场答题卡任务要求提交正确答案。

任务 2 计算机单机取证		
证据编号	**原始文件名（不包含路径）**	**镜像中原文件 Hash 码（MD5，不区分大小写）**
evidence 1		
evidence 2		
evidence 3		
evidence 4		
evidence 5		
evidence 6		
evidence 7		
evidence 8		
evidence 9		
evidence 10		

第三部分 应用程序安全

任务3 代码审计（100 分）

代码审计是指对源代码进行检查，寻找代码存在的脆弱性，这是一项需要多方面技能的技术。作为一项软件安全检查工作，代码安全审查是非常重要的一部分，因为大部分代码从语法和语义上来说是正确的，但存在着可能被利用的安全漏洞，你必须依赖你的知识和经验来完成这项工作。

本任务素材清单：源文件

请按要求完成该部分的工作任务。

任务 3 代码审计		
序号	**任务内容**	**答案**
1	请指出存在安全漏洞的代码行	
2	请指出可能利用该漏洞的威胁名称	
3	请提出加固修改建议	
4	.....	

第三阶段

模块三 网络安全渗透、理论技能与职业素养

一、竞赛内容

第三阶段竞赛内容是：网络安全渗透、理论技能与职业素养。本阶段分为两个部分。第一部分主要是在一个模拟的网络环境中实现网络安全渗透测试工作，要求参赛选手作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等渗透测试技术完成对网络的渗透测试；并且能够通过各种信息安全相关技术分析获取存在的 flag 值。第二部分是在理论测试系统中进行考核。

竞赛阶段	任务阶段		竞赛任务	竞赛时间	分值
第三阶段网络安全渗透、理论技能与职业素养	网络安全渗透	第一部分：网站	任务 1～任务 3	XX:XX-XX:XX	45
		第二部分：应用系统	任务 4～任务 5		30
		第三部分：应用服务器 1	任务 6～任务 13		165
		第四部分：应用服务器 2	任务 14		30
		第五部分：应用服务器 2	任务 15		30
	第六部分：理论技能与职业素养				100

二、竞赛时长

本阶段竞赛时长为 180 分钟，其中网络安全渗透 300 分，理论技能与职业素养 100 分，共 400 分。

三、注意事项

通过找到正确的flag 值来获取得分，flag 统一格式如下所示：

flag{<flag 值 >}

这种格式在某些环境中可能被隐藏甚至混淆。所以，注意一些敏

感信息并利用工具把它找出来。

【特别提醒】部分 flag 可能非统一格式，若存在此情况将会在题目描述中明确指出flag 格式，请注意审题。

第三阶段 任务书

任务描述

在 A 集团的网络中存在几台服务器，各服务器存在着不同业务服务。在网络中存在着一定网络安全隐患，请利用您所掌握的渗透测试技术，通过信息收集、漏洞挖掘等渗透测试技术，完成指定项目的渗透测试，在测试中获取flag 值。网络环境参考样例请查看附录A。

本模块所使用到的渗透测试技术包含但不限于如下技术领域：

- 数据库攻击；
- 枚举攻击；
- 权限提升攻击；
- 基于应用系统的攻击；
- 基于操作系统的攻击；
- 逆向分析；
- 密码学分析；
- 隐写分析。

所有设备和服务器的IP 地址请查看现场提供的设备列表，请根据赛题环境及现场答题卡任务要求提交正确答案。

第一部分 网站（45 分）

任务编号	任务描述	答案	分值
任务 1	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 2	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 3	门户网站存在漏洞，请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第二部分 应用系统（30 分）

任务编号	任务描述	答案	分值
任务 4	应用系统存在漏洞， 请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 5	应用系统存在漏洞， 请利用漏洞并找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第三部分 应用服务器 1（165 分）

任务编号	任务描述	答案	分值
任务 6	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 7	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 8	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 9	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

任务 10	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 11	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 12	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		
任务 13	请获取 FTP 服务器上对应的文件进行分析找出其中隐藏的 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第四部分 应用服务器 2（30 分）

任务编号	任务描述	答案	分值
任务 14	应用系统服务器 10000 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

第五部分 应用服务器 3（30 分）

任务编号	任务描述	答案	分值
任务 15	应用系统服务器 10001 端口存在漏洞，获取 FTP 服务器上对应的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。 flag 格式 flag{<flag 值>}		

附录 A

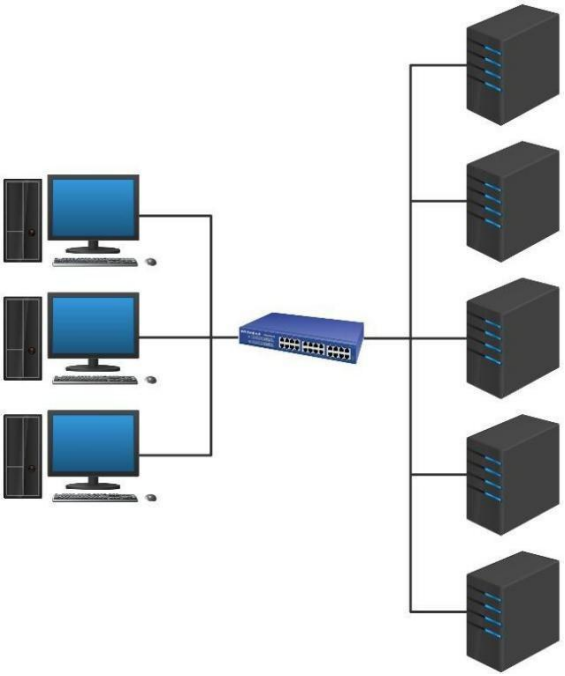

图 2 网络拓扑结构图

第六部分 理论技能与职业素养（100 分）

【注意事项】

1.该部分答题时长包含在第三阶段竞赛时长内，请在临近竞赛结束前提交。

2.参赛团队可根据自身情况，可选择1-3名参赛选手进行作答，参赛队内部可以进行交流，但不得影响其他团队。

一、 单选题（每题 2 分，共 35 题，共 70 分）

1、为了保护计算机信息系统的安全，促进计算机的应用和发展，保障社会主义现代化建设的顺利进行制定的条例。由中华人民共和国国务院于（ ）年2月18日发布实施《中华人民共和国计算机信息系统安全保护条例》，（ ）年1月8日修订。

A、 1994 2010

B、 1995 2011

C、 1994 2011

D、 1995 2010

2、随意下载、使用、传播他人软件或资料属于（ ）信息道德与信息安全失范行为。

A、黑客行为

B、侵犯他人隐私

C、侵犯知识产权

D、信息传播

3、部署大中型 IPSEC VPN 时，从安全性和维护成本考虑，建议采

取什么样的技术手段提供设备间的身份验证。（　　）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

4、针对Windows系统主机，攻击者可以利用文件共享机制上的Netbios“空会话”连接漏洞，获取众多对其攻击有利的敏感信息，获取的信息中不包含下列哪一项信息？（　　）

A、 系统的用户和组信息

B、 系统的共享信息

C、 系统的版本信息

D、 系统的应用服务和软件信息

5、IP数据报分片后的重组通常发生在？（　　）

A、 源主机和数据报经过的路由器上

B、 源主机上

C、 数据报经过的路由器上

D、 目的主机上

6、下面不属于SYN FLOODING攻击的防范方法的是？（　　）

A、 缩短SYN Timeout（连接等待超时）时间

B、 利用防火墙技术

C、 TCP段加密

D、 根据源IP记录SYN连接

7、当数据库系统出现故障时，可以通过数据库日志文件进行恢复。下列关于数据库日志文件的说法，错误的是（　　）。

A、 数据库出现事务故障和系统故障时需使用日志文件进行恢复

B、 使用动态转储机制时，必须使用日志文件才能将数据库恢复到一致状态

C、 在OLTP系统中，数据文件的空间使用量比日志文件大得多，使用日志备份可以降低数据库的备份空间

D、 日志文件的格式主要有以记录为单位的日志文件和以数据块为单位的日志文件两种

8、SQL的GRANT和REVOKE语句可以用来实现（　　）。

A、 自主存取控制

B、 强制存取控制

C、 数据库角色创建

D、 数据库审计

9、下面对于数据库视图的描述正确的是（　　）。

A、 数据库视图也是物理存储的表

B、 可通过视图访问的数据不作为独特的对象存储，数据库内实际存储的是 SELECT语句

C、 数据库视图也可以使用 UPDATE 或 DELETE 语句生成

D、 对数据库视图只能查询数据，不能修改数据

10、有一种攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统显影减慢甚至瘫痪。它影响正常用户的使用，甚至使合法用户被排斥而不能得到服务。这种攻击叫做（　　）。

A、 可用性攻击

B、 拒绝性攻击

C、 保密性攻击

D、 真实性攻击

11、16模20的逆元是？（　　）

A、 3

B、 4

C、 5

D、 不存在

12、PKZIP 算法广泛应用于（　　）程序。

A、 文档数据加密

B、 数据传输加密

C、 数字签名

D、 文档数据压缩

13、下列选项哪列不属于网络安全机制？（　　）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

14、一个C程序的执行是从哪里开始的？（　　）

A、 本程序的main函数开始，到main函数结束

B、 本程序文件的第一个函数开始，到本程序main函数结束

C、 本程序的main函数开始，到本程序文件的最后一个函数结束

D、 本程序文件的第一个函数开始，到本程序文件的最后一个函数结束

15、检查点能减少数据库完全恢复时所必须执行的日志，提高数据库恢复速度。下列有关检查点的说法，错误的是（　　）。

A、 检查点记录的内容包括建立检查点时正在执行的事务清单和这些事务最近一个日志记录的地址

B、 在检查点建立的同时，数据库管理系统会将当前数据缓冲区中的所有数据记录写入数据库中

C、 数据库管理员应定时手动建立检查点，保证数据库系统出现故障时可以快速恢复数据库数据

D、 使用检查点进行恢复时需要从"重新开始文件"中找到最后一个检查点记录在日志文件中的地址

16、下列不属于口令安全威胁的是？（　　）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

17、在远程管理Linux服务器时，以下（　　）方式采用加密的数据传输。

A、 rsh

B、 telnet

C、 ssh

D、 rlogin

18、在C语言中（以16位PC机为例），5种基本数据类型的存储空间长度的排列顺序为?（　　）

A、 char<int<long int<=float<double

B、 char=int<long int<=float<double

C、 char<int<long int=float=double

D、 char=int=long int<=float<double

19、下列方法中不能用来进行DNS欺骗的是？（　　）

A、 缓存感染

B、 DNS信息劫持

C、 DNS重定向

D、 路由重定向

20、以下对DoS攻击的描述，正确的是？（　　）

A、 不需要侵入受攻击的系统

B、 以窃取目标系统上的机密信息为目的

C、 导致目标系统无法正常处理用户的请求

D、 若目标系统没有漏洞，远程攻击就不会成功

21、通过TCP序号猜测，攻击者可以实施下列哪一种攻击？（　　）

A、 端口扫描攻击

B、 ARP欺骗攻击

C、 网络监听攻击

D、 TCP会话劫持攻击

22、下面不是保护数据库安全涉及到的任务是（）。（　　）

A、 确保数据不能被未经过授权的用户执行存取操作

B、 防止未经过授权的人员删除和修改数据

C、 向数据库系统开发商索要源代码，做代码级检查

D、 监视对数据的访问和更改等使用情况

23、下面不是 Oracle 数据库提供的审计形式的是（　　）。

A、 备份审计

B、 语句审计

C、 特权审计

D、 模式对象设计

24、在一下古典密码体制中，属于置换密码的是？（　　）

A、 移位密码

B、 倒叙密码

C、 仿射密码

D、 PlayFair 密码

25、一个基于网络的IDS应用程序利用什么来检测攻击？（　　）

A、 正确配置的DNS

B、 特征库

C、 攻击描述

D、 信息包嗅探器

26、下列工具中可以对web表单进行暴力破解的是?（　　）

A、 Burp suite

B、 Nmap

C、 sqlmap

D、 Appscan

27、在(　　)年，美国国家标准局NBS把IBM的Tuchman-Meyer方案确定数据加密标准，即 DES。（　　）

A、 1949

B、 1972

C、 1977

D、 2001

28、VIM模式切换的说法中，正确的是？（　　）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

29、密码学的目的是?（　　）

A、 研究数据加密

B、 研究数据解密

C、 研究数据保密

D、 研究信息安全

30、能显示TCP和UDP连接信息的命令是？（　　）

A、 netstat -s

B、 netstat -e

C、 netstat -r

D、 netstat -a

31、重合指数法对下面哪种密码算法的破解最有效？（　　）

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

32、Python中哪个占位符表示字符串数据？（　　）

A、 %s

B、 %S

C、 %d

D、 %b

33、关于sed操作命令中，说法错误的是？（　　）

A、 a 命令在行的前面另起一行新增

B、 p 命令打印相关行，配合-n使用

C、 c 命令替换行

D、 d 命令删除行

34、RIP路由协议有RIP v1 和RIP v2两个版本，下面关于这两个版本的说法错误的是（　　）。

A、 RIP v1和RIP v2都具有水平分割功能

B、 RIP v1 是有类路由协议，RIP v2是无类路由协议

C、 RIP v1 和 RIP v2 都是以跳数作为度量值

D、 RIP v1 规定跳数的最大值为15，16跳视为不可达；而RIP v2无此限制

35、在RHEL5系统中，对Postfix邮件服务的配置主要通过修改（　　）文件来进行。

A、 Main.cf

B、 Smtpd.conf

C、 Postfix.cf

D、 Postfix.conf

二、 多选题（每题3分，共10题，共30分）

1、安全业务指安全防护措施，包括（　　）　。

A、 保密业务

B、 认证业务

C、 完整性业务

D、 不可否认业务

2、SQL Server提供了DES、RC2、RC4和AES等加密算法，没有某种算法能适应所有要求，每种算法都有优劣势，但选择算法需要有如下共通之处（　　）　。

A、 强加密通常会比较弱的加密占用更多的CPU资源

B、 长密钥通常会比短密钥生成更强的加密

C、 如果加密大量数据，应使用对称密钥来加密数据，并使用非对称密钥来加密该对称密钥

D、 可以先对数据进行加密，然后再对其进行压缩

3、Python中哪些符号可以包含字符串数据？（　　）

A、 单引号

B、 双引号

C、 两个双引号

D、 三个双引号

4、下面哪些选项是类的属性？（ ）

A、 __doc__

B、 __init__

C、 __module__

D、 __class__

5、下面那些方法可以检测恶意ICMP流量？（ ）

A、 检测同一来源ICMP数据包的数量

B、 注意那些ICMP数据包中payload大于64比特的数据包

C、 寻找那些响应数据包中payload跟请求数据包不一致的ICMP数据包

D、 检查ICMP数据包的协议标签

6、使用os.walk函数可以得到哪些内容？（ ）

A、 目录的路径

B、 子目录的列表

C、 非目录的文件列表

D、 目录中文件的大小

7、VPN设计中常用于提供用户识别功能的是（ ） 。

A、 RADIUS

B、 TOKEN卡

C、 数字证书

D、 802.1xAA.OOcIn.com

8、上传文件夹权限管理方法包括 ？（ ）

A、 取消执行权限

B、 限制上传文件大小

C、 设置用户umask值

D、 在上传目录关闭php解析引擎

9、在反杀伤链中，情报可以分为那几个层次？（ ）

A、 战斗

B、 战略

C、 战区

D、 战术

10、以下后缀中，属于Linux中常见压缩文件后缀的有？（ ）

A、 doc

B、 zip

C、 tar.gz

D、 ppt