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
样题二

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

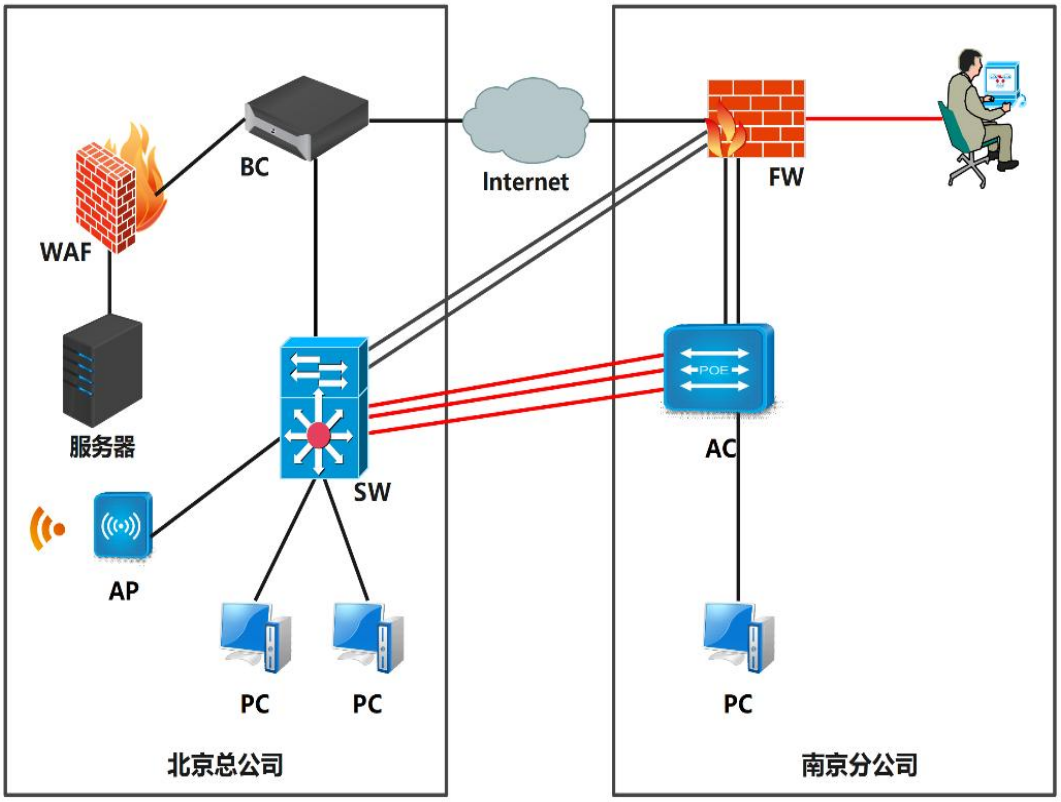

图 1 网络拓扑图

2.IP 地址规划表

设备名称	接口	IP地址	对端设备	接口
防火墙 FW	ETH0/1-2	20.1.0.1/30（trust1安全域）	SW	eth1/0/1-2
		20.1.1.1/30（untrust1安全域）	SW	
		222.22.1.1/29（untrust）	SW	
	ETH0/3	20.10.28.1/24(DMZ)	WAF	

设备名称	接口	IP地址	对端设备	接口
	Eth0/4-5	20.1.0.13/30 2001:da8:192:168:10:1::1/96	AC	Eth1/0/21-22
	Loopback1	20.0.0.254/32（trust） Router-id		
	L2TP Pool	192.168.10.1/26 可用IP数量为20	L2tp VPN地址池	
三层交换机SW	ETH1/0/4	财务专线 VPN CW	AC	ETH1/0/4
	ETH1/0/5	trunk	AC	ETH1/0/5
	ETH1/0/6	trunk	AC	ETH1/0/6
	VLAN21 ETH1/0/1-2	20.1.0.2/30	FW	Eth1/0/1-2
	VLAN22 ETH1/0/1-2	20.1.1.2/30	FW	Eth1/0/1-2
	VLAN 222 ETH1/0/1-2	222.22.1.2/29	FW	Eth1/0/1-2
	VLAN 24 ETH1/0/24	223.23.1.2/29	BC	Eth 5
	Vlan 25 Eth 1/0/3	20.1.0.9/30 Ipv6:2001:da8:20:1:0::1/96	BC	Eth 1
	VLAN 30 ETH1/0/4	20.1.0.5/30	AC 1/0/4	Vlan name CW
	VLAN 31 Eth1/0/10-12 10口配置 Loopback	20.1.3.1/25		Vlan name CW
	VLAN 40 ETH1/0/8-9	192.168.40.1/24 IPV6 2001:DA8:192:168:40::1/96		Vlan name 销售
	VLAN 50 ETH1/0/13-14	192.168.50.1/24 IPV6 2001:DA8:192:168:50::1/96	PC3	Vlan name 产品
	Vlan 60 Eth1/0/15-16	192.168.60.1/24 IPV6 2001:DA8:192:168:60::1/96		Vlan name 信息
	VLAN 100 ETH 1/0/20	需设定		Vlan name AP-Manage
	Loopback1	20.0.0.253/32(router-id)		
无线控制器AC	VLAN 30 ETH1/0/4	20.1.0.6/30	SW	Vlan name TO-CW
	VLAN 10	Ipv4:需设定 2001:da8:172:16:1::1/96	无线1	Vlan name WIFI-vlan10
	VLAN 20	Ipv4:需设定 2001:da8:172:16:2::1/96	无线2	Vlan name WIFI-vlan20
	VLAN 31	20.1.3.129/25		Vlan name CW
	VLAN 140	172.16.40.1/24	SW	Vlan name

设备名称	接口	IP地址	对端设备	接口
	ETH1/0/5		1/0/5	销售
	Vlan 150 Eth1/0/13-14	172.16.50.1/24 IPV6 2001:DA8:172:16:60::1/96		Vlan name 产品
	Vlan 60 Eth1/0/15-18	192.168.60.2/24 IPV6 2001:DA8:192:168:60::2/96		Vlan name 信息
	Vlan 70 Eth1/0/21-22	20.1.0.14/30 2001:da8:192:168:10:1::1/96	FW	Eth1/0/4-5
	Loopback1	20.1.1.254/24(router-id)		
日志服务器BC	Eth1	20.1.0.10/30 Ipv6:2001:da8:20:1:0::2/96	SW	Eth1/0/3
	Eth5	223.23.1.1/29	SW	
	eth3	192.168.28.1/24	WAF	
	PPTP-pool	192.168.10.129/26（10个地址）		
WEB应用防火墙WAF	ETH2	192.168.28.2/24	SERVER	
	ETH3		FW	
AP	Eth1		SW（20口）	
SERVER	网卡	192.168.28.10/24		

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. 北京总公司和南京分公司有两条裸纤采用了骨干链路配置，做必要的配置，只允许必要的 vlan 通过，不允许其他 vlan 信息通过包含 vlan1。
2. SW 和 AC 开启 telnet 登录功能，telnet 登录账户仅包含“***2023”，密码为明文“***2023”，采用 telnet 方式登录设备时需要输入 enable 密码，密码设置为明文“12345” 。
3. 北京总公司和南京分公司租用了运营商三条裸光纤，实现内部办公互通。一条裸光纤承载公司财务部门业务，另外两条裸光纤承载其他内部有业务。使用相关技术实现总公司财务段路由表与公司其它业务网段路由表隔离，财务业务位于 VPN 实例名称 CW 内，总公司财务和分公司财务能够通信，财务部门总公司和分公司之间采用 RIP 路由实现互相访问。
4. SW 和 AC 之间启用 MSTP，实现网络二层负载均衡和冗余备份，要求如下：无线用户关联实例 1，信息部门关联实例 2，名称为 SKILLS，修订版本为 1，设置 AC 为根交换机，走 5 口链路转发、信息部门通过

6 口链路转发，同时实现链路备份。除了骨干接口，关闭其他接口生成树协议。

5. 总公司产品部门启用端口安全功能，最大安全 MAC 地址数为 20，当超过设定 MAC 地址数量的最大值，不学习新的 MAC、丢弃数据包、发 snmp trap、同时在 syslog 日志中记录，端口的老化定时器到期后，在老化周期中没有流量的部分表项老化，有流量的部分依旧保留，恢复时间为 10 分钟；禁止采用访问控制列表，只允许 IP 主机位为 20-50 的数据包进行转发；禁止配置访问控制列表，实现端口间二层流量无法互通，组名称 FW。
6. 由于总公司出口带宽有限，需要在交换机上对总公司销售部门访问因特网 http 服务做流量控制，访问 http 流量最大带宽限制为 20M 比特/秒，突发值设为 4M 字节，超过带宽的该网段内的报文一律丢弃。
7. 在 SW 上配置将 8 端口收到的源 IP 为 10.0.41.111 的帧重定向到 9 端口，即从 8 端口收到的源 IP 为 10.0.41.111 的帧通过 9 端口转发出去。
8. 总公司 SW 交换机模拟因特网交换机，通过某种技术实现本地路由和因特网路由进行隔离，因特网路由实例名 internet。
9. 对 SW 上 VLAN60 开启以下安全机制:
10. 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;开启防止 ARP 网关欺骗；
11. 配置使北京公司内网用户通过总公司出口 BC 访问因特网，分公司内网用户通过分公司出口 FW 访问因特网，要求总公司销售部门的用户访问因特网的流量往反数据流都要经过防火墙，在通过 BC 访问因特网；防火墙 untrust 和 trust1 开启安全防护，参数采用默认参数。

12. 总部核心交换机上配置 SNMP，引擎 id 分别为 1；创建组 GROUP2023，采用最高安全级别，配置组的读、写视图分别为：SKILLS_R、SKILLS_W；创建认证用户为 USER2023，采用 aes 算法进行加密，密钥为 Pass-1234，哈希算法为 sha，密钥为 Pass-1234；当设备有异常时，需要用本地的环回地址 loopback1 发送 v3 Trap 消息至集团网管服务器 20.10.11.99、采用最高安全级别；当财务部门对应的用户接口发生 UP DOWN 事件时，禁止发送 trap 消息至上述集团网管服务器。
13. 总公司和分公司今年进行 IPv6 试点，要求总公司和分公司销售部门用户能够通过 IPV6 相互访问，IPV6 业务通过租用裸纤承载。实现分公司和总公司 ipv6 业务相互访问；FW、AC 与 SW 之间配置动态路由 OSPF V3 使总公司和分公司可以通过 IPv6 通信
14. 在总公司核心交换机 SW 配置 IPv6 地址，开启路由公告功能，路由器公告的生存期为 2 小时，确保销售部门的 IPv6 终端可以通过 DHCP SERVER 获取 IPv6 地址，在 SW 上开启 IPV6 dhcp server 功能。
15. 在南京分公司上配置 IPv6 地址，使用相关特性实现销售部的 IPv6 终端可自动从网关处获得 IPv6 无状态地址
16. FW、SW、AC、BC 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义，SW 与 AC 手动配置 INTERNET 默认路由，让总公司和分公司内网用户能够相互访问包含 AC 上 loopback1 地址。
17. 分公司销售部门通过防火墙上的 DHCP SERVER 获取 IP 地址，server IP 地址为 20.0.0.254，地址池范围 172.16.40.10-172.16.40.100，dns-server 8.8.8.8。
18. 如果 SW 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；为了更好地提高数据转发的性能，SW 交换中的数据包大小指定为 1600 字节；

19. 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，telnet，SNMP 功能，Untrust 安全域开启 SSH、HTTPS 功能；
20. 在分部防火墙上配置，分部 VLAN 业务用户通过防火墙访问 Internet 时，转换为公网 IP： 182.22.1.1/29；保证每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址，当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至 20.10.28.10 的 UDP 2000 端口；
21. 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；
22. 由于总公司无线是通过分公司的无线控制器统一管理，为了防止专线故障导致无线不能使用，总公司和分公司使用互联网作为总公司无线 ap 和 AC 相互访问的备份链路。FW 和 BC 之间通过 IPSEC 技术实现 AP 管理段与无线 AC 之间联通，具体要求为采用预共享密码为 ***2023，IKE 阶段 1 采用 DH 组 1、3DES 和 MD5 加密方，IKE 阶段 2 采用 ESP-3DES，MD5。
23. 总公司用户，通过 BC 访问因特网，BC 采用路由方式，在 BC 上做相关配置，让总公司内网用户（不包含财务）通过 ip：183.23.1.1/29 访问因特网。
24. 在 BC 上配置 PPTP vpn 让外网用户能够通过 PPTP vpn 访问总公司 SW 上内网地址，用户名为 GS2023，密码 123456。
25. 为了提高分公司出口带宽，尽可能加大分公司 AC 和出口 FW 之间带宽。
26. 在 BC 上开启 IPS 策略，对分公司内网用户访问外网数据进行 IPS 防护，保护服务器、客户端和恶意软件检测，检测到攻击后进行拒绝并记录日志。

27. BC 上开启黑名单告警功能，级别为预警状态，并进行邮件告警和记录日志，发现 cpu 使用率大于 80%，内存使用大于 80%时进行邮件告警并记录日志，级别为严重状态。发送邮件地址为 123@163.com，接收邮件为 133139123456@163.com。
28. 分公司内部有一台网站服务器直连到 WAF，地址是 192.168.28.10，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 192.168.28.6，UDP 的 514 端口;
29. 要求能自动识别内网 HTTP 服务器上的 WEB 主机，请求方法采用 GET、POST 方式。
30. 在 WAF 上针对 HTTP 服务器进行 URL 最大个数为 10，Cookies 最大个数为 30，Host 最大长度为 1024，Accept 最大长度 64 等参数校验设置，设置严重级别为中级，超出校验数值阻断并发送邮件告警;
31. 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;
32. 为更好对服务器 192.168.28.10 进行防护，防止信息泄露，禁止美国地区访问服务器;
33. 在 WAF 上配置基础防御功能，建立特征规则“HTTP 防御”，开启 SQL 注入、XSS 攻击、信息泄露等防御功能，要求针对这些攻击阻断并保存日志发送邮件告警;
34. 在 WAF 上配置定期每周六 1 点对服务器的 http://192.168.28.10/进行最大深度的漏洞扫描测试;
35. 为了对分公司用户访问因特网行为进行审计和记录，需要把 AC 连接防火墙的流量镜像到 8 口。

36. 由于公司 IP 地址为统一规划，原有无线网段 IP 地址为 172.16.0.0/22,为了避免地址浪费需要对 ip 地址进行重新分配；要求如下：未来公司预计部署 ap 150 台；办公无线用户 vlan 10 预计 300 人，来宾用户 vlan20 以及不超过 50 人；

37. BC 上配置 DHCP，管理 VLAN 为 VLAN100,为 AP 下发管理地址，网段中第一个可用地址为 AP 管理地址，最后一个可用地址为网关地址，AP 通过 DHCP opion 43 注册，AC 地址为 loopback1 地址；为无线用户 VLAN10,20 下发 IP 地址，最后一个可用地址为网关；AP 上线需要采用 MAC 地址认证。

38. AC 配置 dhcpv4 和 dhcpv6，分别为总公司产品段 vlan50 分配地址；ipv4 地址池名称分别为 POOLv4-50，ipv6 地址池名称分别为 POOLv6-50；ipv6 地址池用网络前缀表示；排除网关；DNS 分别为 114.114.114.114 和 2400:3200::1；为 PC1 保留地址 192.168.50.9 和 2001:da8:192:168:50::9， SW 上中继地址为 AC loopback1 地址。

39. NETWORK 1 下设置 SSID GUEST，VLAN20 不进行认证加密,做相应配置隐藏该 SSID； NETWORK 2 开启内置 portal+本地认证的认证方式，账号为 test 密码为 test2023；

40. 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；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 2 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；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；

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		100
	数字取证调查	任务 2	网络数据包分析		100
	应用程序安全	任务 3	恶意代码分析		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 网络数据包分析（100 分）

A 集团的网络安全监控系统发现有恶意攻击者对集团官方网站进行攻击，并抓取了部分可疑流量包。请您根据捕捉到的流量包，搜寻出网络攻击线索，并分析黑客的恶意行为。

本任务素材清单：捕获的网络数据包文件（***.pcapng**）

请按要求完成该部分的工作任务，答案有多项内容的请用换行分

隔。

任务 2 网络数据包分析		
序号	任务要求	答案
1	提交恶意程序传输协议 （只提交一个协议，两个以上视为无效）	
2	恶意程序对外连接目标 IP	
3	恶意程序加载的 dll 文件名称	
4	解密恶意程序传输内容	
5	分析恶意程序行为	

第三部分 应用程序安全

任务 3 恶意程序分析（100 分）

A 集团发现其发布的应用程序文件遭到非法篡改，您的团队需要协助A 集团对该恶意程序样本进行逆向分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：恶意程序代码

请按要求完成该部分的工作任务。

任务 3 恶意程序分析		
序号	任务内容	答案
1	请提交素材中的恶意应用回传数据的 url 地址	
2	请提交素材中的恶意代码保存数据文件名称 （含路径）	
3	请描述素材中恶意代码的行为	
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

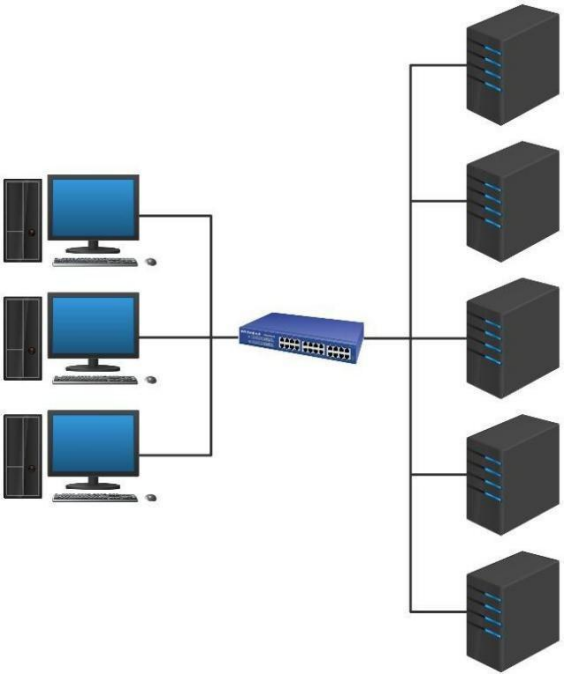

图 2 网络拓扑结构图

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、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

2、在学校或单位如果发现自己的计算机感染了病毒,应首先采取什么措施( )。

A、断开网络

B、告知领导

C、杀毒

D、重启

答案：A

3、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

4、下列哪个不属于密码破解的方式？（　　）

A、 密码学分析

B、 撞库

C、 暴力破解

D、 字典破解

5、下列不属于应用层安全协议的是哪一项？（　　）

A、 Secure shell

B、 超文本传输协议

C、 电子交易安全协议SET

D、 SSL协议

6、\x32\x2E\x68\x74\x6D此加密是几进制加密？（　　）

A、 二进制

B、 八进制

C、 十进制

D、 十六进制

7、下列关于SQL Server 2008中分离和附加数据库的说法，错误的是（　　）

A、 在分离数据库之前，必须先断开所有用户与该数据库的连接

B、 分离数据库只分离数据文件，不会分离日志文件

C、 附加数据库时文件存储位置可以与分离数据库时文件所处的存储位置不同

D、 进行分离数据库操作时不能停止SQL Server服务

8、C语言中的标识符只能由字母、数字和下划线三种字符组成,且第一个字符？（　　）

A、 必须为字母

B、 必须为下划线

C、 必须为字母或下划线

D、 可以是字母,数字和下划线中任一种字符

9、下面那个名称不可以作为自己定义的函数的合法名称？（　　）

A、 print

B、 len

C、 error

D、 Haha

10、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（　　）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

11、.IPSec包括报文验证头协议AH 协议号（ ）和封装安全载荷协议ESP协议号（　　）。

A、 51 50

B、 50 51

C、 47 48

D、 48 47

12、SYN攻击属于DOS攻击的一种，它利用（ ）协议缺陷，通过发送大量的半连接请求，耗费CPU和内存资源？（　　）

A、 UDP

B、 ICMP

C、 TCP

D、 OSPF

13、POP3服务器使用的监听端口是？（　　）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

14、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（　　）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

15、下列工具中可以直接从内存中读取windows 密码的是？（　　）

A、 getpass

B、 QuarkssPwDump

C、 SAMINSIDE

D、 John

16、利用虚假IP地址进行ICMP报文传输的攻击方法称为？（　　）

A、 ICMP泛洪

B、 死亡之ping

C、 LAND攻击

D、 Smurf攻击

17、关于函数，下面哪个说法是错误的？（　　）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

18、在TCP/IP参考模型中，与OSI参考模型的网络层对应的是？（　　）

A、 主机-网络层

B、 传输层

C、 互联网层

D、 应用层

19、MD5的主循环有（　　）轮。

A、 3

B、 4

C、 5

D、 8

20、Open函数中w 参数的作用是？（　　）

A、 读文件内容

B、 写文件内容

C、 删除文件内容

D、 复制文件内容

21、根据工信部明确的公共互联网网络安全突发事件应急预案文件，公共互联网网络突发事件等级最高可标示的颜色是什么？（　　）

A、 红色

B、 黄色

C、 蓝色

D、 橙色

22、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

23、以下选项中，不属于结构化程序设计方法的是哪个选项？（　　）

A、 可封装

B、 自顶向下

C、 逐步求精

D、 模块化

24、关于并行数据库，下列说法错误的是（　　）。

A、 层次结构可以分为两层，顶层是无共享结构，底层是共享内存或共享磁盘结构

B、 无共享结构通过最小化共享资源来降低资源竞争，因此具有很高的可扩展性，适合于OLTP应用

C、 并行数据库系统经常通过负载均衡的方法来提高数据库系统的业务吞吐率

D、 并行数据库系统的主要目的是实现场地自治和数据全局透明共享

25、下面不是 Oracle 数据库支持的备份形式的是（　　）。

A、 冷备份

B、 温备份

C、 热备份

D、 逻辑备份

26、Linux中，通过chmod修改权限设置，正确的是？（　　）

A、 chmod test.jpg +x

B、 chmod u+8 test.jpg

C、 chmod 777 test.jpg

D、 chmod 888 test.jpg

27、windows自带FTP服务器的日志文件后缀为？（　　）

A、 evt或.evtx

B、 log

C、 w3c

D、 txt

28、部署IPSEC VPN时，配置什么样的安全算法可以提供更可靠的数据加密（　　）。

A、 DES

B、 3DES

C、 SHA

D、 128位的MD5

29、如果明文为abc，经恺撒密码-加密后，密文bcd，则密钥为？（　　）

A、 1

B、 2

C、 3

D、 4

30、部署IPSEC VPN 网络时我们需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，其中每条加密ACL将消耗多少IPSEC SA资源（　　）。

A、 1个

B、 2个

C、 3个

D、 4个

31、部署IPSEC VPN 网络时我们需要考虑IP地址的规划，尽量在分支节点使用可以聚合的IP地址段，其中每条加密ACL将消耗多少IPSEC SA资源（　　）。

A、 1个

B、 2个

C、 3个

D、 4个

32、DES的秘钥长度是多少Bit?（　　）

A、 6

B、 56

C、 128

D、 32

33、VIM命令中，用于删除光标所在行的命令是？（　　）

A、 dd

B、 dw

C、 de

D、 db

34、Linux软件管理rpm命令，说法不正确的是？（　　）

A、 -v 显示详细信息

B、 -h: 以#显示进度；每个#表示2%

C、 -q PACKAGE_NAME: 查询指定的包是否已经安装

D、 -e 升级安装包

35、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

二、 多选题（每题 3 分，共 10 题，共 30 分）

1、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

2、以下关于TCP和UDP协议的说法错误的是？（　　）

A、 没有区别，两者都是在网络上传输数据

B、 TCP是一个定向的可靠的传输层协议，而UDP是一个不可靠的传输层协议

C、 UDP是一个局域网协议，不能用于Interner传输，TCP则相反

D、 TCP协议占用带宽较UDP协议多

3、关于函数中变量的定义，哪些说法是正确的？（　　）

A、 即使函数外已经定义了这个变量，函数内部仍然可以定义

B、 如果一个函数已经定义了name变量，那么其他的函数就不能再定义

C、 函数可以直接引用函数外部定义过的变量

D、 函数内部只能定义一个变量

4、下面标准可用于评估数据库的安全级别的有（　　）

A、 TCSEC

B、 IFTSEC

C、 CC DBMS.PP

D、 GB17859-1999E.TD

5、安全的网络通信必须考虑以下哪些方面？（　　）

A、 加密算法

B、 用于加密算法的秘密信息

C、 秘密信息的分布和共享

D、 使用加密算法和秘密信息以获得安全服务所需的协议

6、RC4加密算法被广.泛应用，包括（　　）

A、 SSL/TLS

B、 WEP协议

C、 WPA协议

D、 数字签名

7、VIM的工作模式，包括哪些？（　　）

A、 命令模式

B、 输入模式

C、 高亮模式

D、 底行模式

8、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

9、我国现行的信息安全法律体系框架分为（　）三个层面。

A、信息安全相关的国家法律

B、信息安全相关的行政法规和部分规章

C、信息安全相关的地方法规/规章和行业规定

D、信息安全相关的个人职业素养

10、信息道德与信息安全问题一直存在的原因有（　）。

A、信息系统防护水平不高

B、信息安全意识不强

C、信息安全法律法规不完善

D、网络行为道德规范尚未形成