全国职业院校技能大赛

高等职业教育组

信息安全管理与评估

赛题一

模块一

网络平台搭建与设备安全防护

一、 赛项时间

共计 180 分钟。

二、 赛项信息

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

三、 赛项内容

本次大赛，各位选手需要完成三个阶段的任务，其中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、三阶段请根据现场具体题目要求操作。

选手首先需要在 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），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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。

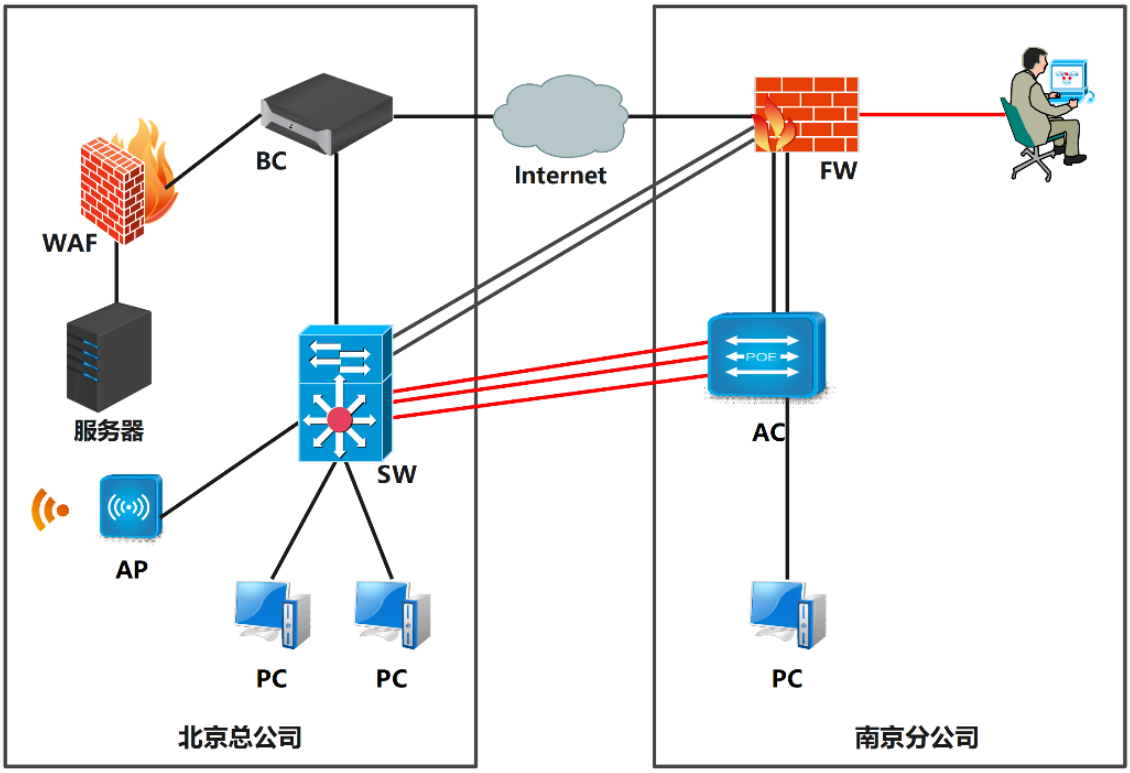
特别说明：只允许在根目录下的“GWxx”文件夹中体现一次工位信息，不允许在其他文件夹名称或文件名称中再次体现工位信息，否则按作弊处理。

(一) 赛项环境设置

某集团公司原在北京建立了总部，在南京设立了分公司。总部设有销售、产品、财务、信息技术 4 个部门，分公司设有销售、产品、财务 3 个部门，统一进行 IP 及业务资源的规划和分配，全网采用 OSPF 动态路由协议和静态路由协

议进行互连互通。公司规模在 2023 年快速发展，业务数据量和公司访问量增长巨大。为了更好管理数据，提供服务，集团决定建立自己的中型数据中心及业务服务平台，以达到快速、可靠交换数据，以及增强业务部署弹性的目的。集团、分公司的网络结构详见拓扑图。其中总公司使用一台 SW 交换机用于总部核心和终端高速接入，采用一台 BC 作为总公司因特网出口；分公司采用一台 FW 防火墙作为因特网出口设备，一台 AC 作为分公司核心，同时作为集团有线无线智能一体化控制器，通过与 AP 高性能企业级 AP 配合实现集团无线覆盖，总部有一台 WEB 服务器，为了安全考虑总公司部署了一台 WAF 对服务器进行 web 防护。在 2023 年公司进行 IPV6 网络改造，内部网络采用双栈模式。Ipv6 网络采用 ospf V3 实现互通。

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	
	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 ETH1/0/5	172.16.40.1/24	SW 1/0/5	Vlan name 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		

(二) 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	根据网络拓扑图所示，按照 IP 地址参数表，对 FW 的名称、各接口 IP 地址进行配置。
2	根据网络拓扑图所示，按照 IP 地址参数表，对 SW 的名称进行配置，创建 VLAN 并将相应接口划入 VLAN。
3	根据网络拓扑图所示，按照 IP 地址参数表，对 AC 的各接口 IP 地址进行配置。
4	根据网络拓扑图所示，按照 IP 地址参数表，对 BC 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：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。
10. 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。
11. 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。
12. 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。

13. 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。
14. 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。
15. 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。
16. 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。
17. 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。
18. 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。
19. 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。
20. 远程移动办公用户通过专线方式接入分公司网络，在防火墙 FW 上配置，采用 L2TP 方式实现仅允许对内网信息部门的访问，端口号使用 4455，用户名密码均为 ABC2023，地址池参见地址表。

21. 分公司部署了一台 AC 为了便于远程管理，需要把 AC 的 web 映射到外网，让外网通过能通过防火墙外网口地址访问 AC 的 web 服务，AC 地址为 loopback 地址。
22. 为了安全考虑，无线用户移动性较强，访问因特网时需要在 BC 上开启 web 认证使用 https 方式，采用本地认证，密码账号都为 web2023，同一用户名只能在一个客户端登录，设置超时时间为 30 分钟。
23. 由于分公司到因特网链路带宽比较低，出口只有 200M 带宽，需要在防火墙配置 iQOS，系统中 P2P 总的流量不能超过 100M ，同时限制每用户最大下载带宽为 2M，上传为 1M，优先保障 HTTP 应用，为 http 预留 100M 带宽。
24. 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。
25. 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。
26. 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。
27. 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。
28. 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。

29. 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。
30. 对分公司内网用户访问外网数据进行防病毒防护，检查协议类型包含 HTTP、FTP、POP3、SMTP，文件类型包含exe、bat、vbs、txt，检测到攻击后进行记录日志并阻断。
31. 总公司出口带宽较低，总带宽只有200M，为了防止内网用户使用p2p迅雷下载占用大量带宽需要限制内部员工使用P2P工具下载的流量，最大上下行带宽都为50M，以免P2P流量占用太多的出口网络带宽，启用阻断记录。
32. 通过 BC 设置分公司用户在上班时间周一到周五 9:00 到 18:00 禁止玩游戏，并启用阻断记录。
33. 限制总公司内网用户访问因特网 web 视频和即时通信上传最大带宽为 10M，启用阻断记录。
34. 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。
35. 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。
36. 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。
37. 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。

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. 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。
40. 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。
41. 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。
42. 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。
43. 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。
44. 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。
45. 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。

46. 在 NETWORK 下配置 SSID，需求如下：NETWORK 1 下设置 SSID ***2023，VLAN10，加密模式为 wpa-personal,其口令为 20232023。
47. NETWORK 2 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。
48. 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。
49. 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。
50. 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。

全国职业院校技能大赛

高等职业教育组

信息安全管理与评估

模块二

网络安全事件响应、数字取证调查、应用程序安全

竞赛项目赛题

本文件为信息安全管理与评估项目竞赛-第二阶段样题，内容包括：网络安全事件响应、数字取证调查、应用程序安全。

本次比赛时间为 180 分钟。

介绍

竞赛有固定的开始和结束时间，参赛队伍必须决定如何有效的分配时间。请认真阅读以下指引！

（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）请不要修改实体机的配置和虚拟机本身的硬件设置。

所需的设备、机械、装置和材料

所有测试项目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。

评分方案

本阶段总分数为 300 分。

项目和任务描述

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

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-答题卷”中，竞赛结束时每组将答案整合到一份 PDF 文档提交。选手的电脑中已经安装好 Office 软件并提供必要的软件工具。

工作任务

第一部分 网络安全事件响应（70 分）

任务 1：Windows 服务器应急响应（70 分）

A 集团的 Windows 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，发现系统中的漏洞，并对发现的漏洞进行修复。

本任务素材清单：Windows 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。

注意：Server 服务器的基本配置参见附录，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的工作任务。

任务 1：Windows 服务器应急响应		
序号	任务内容	答案
1	请提交攻击者攻击成功的第一时间，格式：YY:MM:DD hh:mm:ss	
2	请提交攻击者的浏览器版本	

3	请提交攻击者目录扫描所使用的工具名称	
4	找到攻击者写入的恶意后门文件，提交文件名（完整路径）	
5	找到攻击者隐藏在正常 web 应用代码中的恶意代码，提交该文件名（完整路径）	
6	请提交内存中可疑进程的 PID	
7	请提交攻击者执行过几次修改文件访问权限的命令	
8	请指出可疑进程采用的自动启动的方式	

第二部分 数字取证调查（150 分）

任务 2 ：基于 Linux 的内存取证（40 分）

A 集团某服务器系统感染恶意程序，导致系统关键文件被破坏，请分析 A 集团提供的系统镜像和内存镜像，找到系统镜像中的恶意软件，分析恶意软件行为。

本任务素材清单：存储镜像、内存镜像。

请按要求完成该部分的工作任务。

任务 2：基于 Linux 的内存取证		
序号	任务内容	答案
1	请提交用户目录下压缩包的解压密码	
2	请提交 root 账户的登录密码	
3	请指出攻击者通过什么命令实现提权操作	
4	请指出内存中恶意进程的 PID	
5	请指出恶意进程加密文件的文件类型	

任务 3：通信数据分析取证（USB）（50 分）

A 集团的网络安全监控系统发现恶意份子正在实施高级可持续攻击（APT），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，分解出隐藏的恶意程序，并分析恶意程序的行为。

本任务素材清单：捕获的通信数据文件。

请按要求完成该部分的工作任务。

任务 3：通信数据分析取证（USB）		
序号	任务内容	答案
1	请提交攻击者一共上传了几个文件	
2	请提交攻击者上传的木马文件的 MD5 值	
3	请写出攻击者运行木马文件的命令（含参数）	
4	攻击者获取主机权限之后，进行了回连操作，请提交回连的 IP 地址	

任务 4： 基于 MacOS 计算机单机取证（60 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。

请按要求完成该部分的工作任务。

任务 4：基于 MacOS 计算机单机取证		
证据编号	在取证镜像中的文件名	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（80 分）

任务 5：Android 恶意程序分析（50 分）

A 集团发现其发布的 Android 移动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：Android 的 apk 文件。

请按要求完成该部分的工作任务。

任务 5：Android 恶意程序分析		
序号	**任务内容**	**答案**
1	请提交恶意应用回传数据的 url 地址	提交正确 flag 值得分
2	请提交恶意应用保存数据文件名称（含路径）	提交正确 flag 值得分
3	请提交恶意应用解密数据的密钥	提交正确 flag 值得分
4	请描述恶意应用的行为	提交正确 flag 值得分

任务 6：PHP 代码审计（30 分）

A 集团发现其发布的 web 应用程序中被黑客种植了 webshell，文件遭到非法篡改，您的团队需要协助 A 集团对该恶意脚本程序样本进行分析、对其攻击/破坏的行为进行调查取证。

本任务素材清单：PHP 文件。

请按要求完成该部分的工作任务。

任务 6：PHP 代码审计		
序号	**任务内容**	**答案**
1	请提交存在安全漏洞的代码行	
2	请指出安全漏洞的名称	
3	请修改该代码行使其变得安全	

全国职业院校技能大赛

高等职业教育组

信息安全管理与评估

模块三

网络安全渗透、理论技能与职业素养

竞赛项目赛题

本文件为信息安全管理与评估项目竞赛-第三阶段样题，内容包括：网络安全渗透、理论技能与职业素养。

本次比赛时间为 180 分钟。

介绍

网络安全渗透的目标是作为一名网络安全专业人员在一个模拟的网络环境中实现网络安全渗透测试工作。

本模块要求参赛者作为攻击方，运用所学的信息收集、漏洞发现、漏洞利用等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。

所需的设施设备和材料

所有测试项目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。

评分方案

本测试项目模块分数为 400 分，其中，网络安全渗透 300 分，理论技能与职业素养 100 分。

项目和任务描述

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。

特别提醒

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。

注：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。

工作任务

一、 门户网站（45 分）

任务编号	任务描述	答案	分值
任务一	请对门户网站进行黑盒测试，利用漏洞找到 flag1，并将 flag1 提交。flag1 格式 flag1{<flag 值>}		
任务二	请对门户网站进行黑盒测试，利用漏洞找到 flag2，并将 flag2 提交。flag2 格式 flag2{<flag 值>}		

任务三	请对门户网站进行黑盒测试，利用漏洞找到 flag3，并将 flag3 提交。flag3 格式 flag3{<flag 值>}		

二、 办公系统（30 分）

任务编号	任务描述	答案	分值
任务四	请对办公系统进行黑盒测试，利用漏洞找到 flag1，并将 flag1 提交。flag1 格式 flag1{<flag 值>}		
任务五	请对办公系统进行黑盒测试，利用漏洞找到 flag2，并将 flag2 提交。flag2 格式 flag2{<flag 值>}		

三、 FTP 服务器（165 分）

任务编号	任务描述	答案	分值
任务六	请获取 FTP 服务器上 task6 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务七	请获取 FTP 服务器上 task7 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务八	请获取 FTP 服务器上 task8 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务九	请获取 FTP 服务器上 task9 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务十	请获取 FTP 服务器上 task10 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

任务十一	请获取 FTP 服务器上 task11 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务十二	请获取 FTP 服务器上 task12 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		
任务十三	请获取 FTP 服务器上 task13 目录下的文件进行分析，找出其中隐藏的 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

四、 应用系统服务器（30 分）

任务编号	任务描述	答案	分值
任务十四	应用系统服务器 10000 端口存在漏洞，获取 FTP 服务器上 task14 目录下的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

五、 测试系统服务器（30 分）

任务编号	任务描述	答案	分值
任务十五	应用系统服务器 10001 端口存在漏洞，获取 FTP 服务器上 task15 目录下的文件进行分析，请利用漏洞找到 flag，并将 flag 提交。flag 格式 flag{<flag 值>}		

附录 A

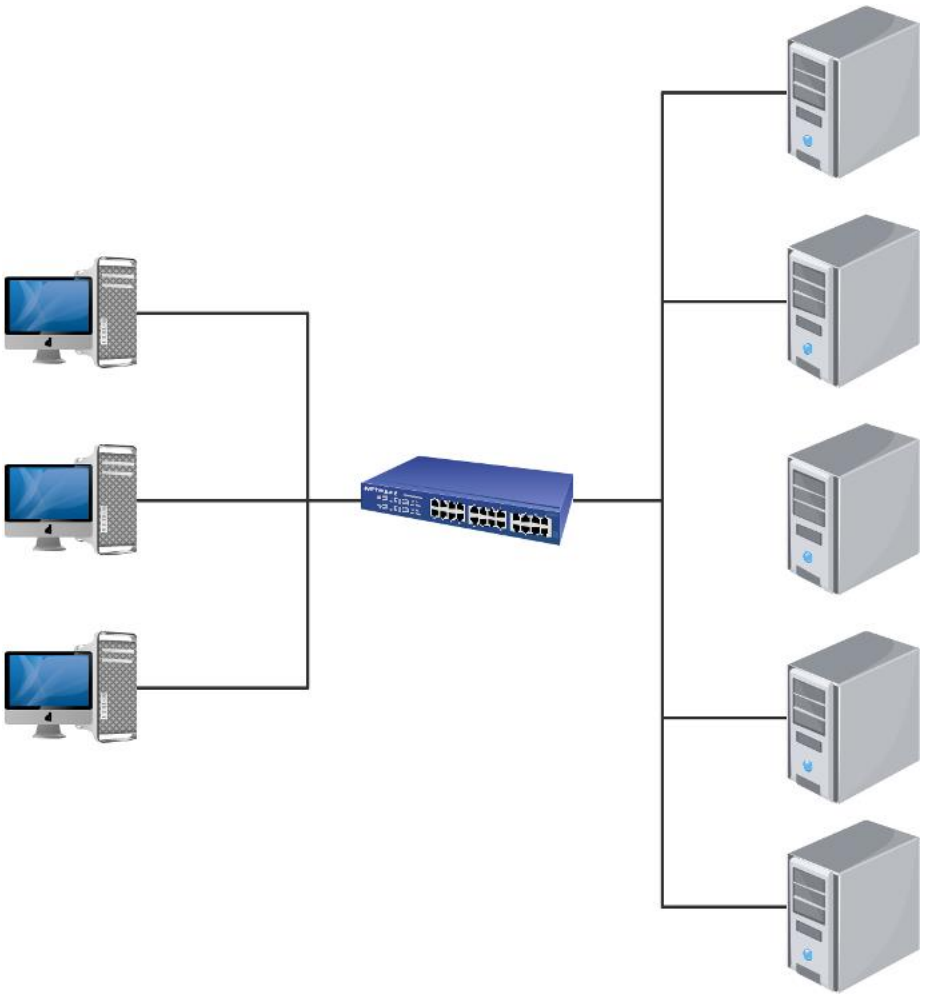


图 1 网络拓扑结构图

六、 理论技能与职业素养（100 分）

2023 年全国职业院校技能大赛（高等职业教育组）

“信息安全管理与评估”测试题（样题）

【注意事项】

1.理论测试前请仔细阅读测试系统使用说明文档，按提供的账号和密码登录测试系统进行测试，账号只限 1 人登录。

2.该部分答题时长包含在第三阶段比赛时长内，请在临近竞赛结束前提交。

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

一、 单选题 （每题 2 分，共 35 题，共 70 分）

1、《中华人民共和国数据安全法》已由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议通过，现予公布，自（ ）起施行。

A、2020 年 9 月 1 日

B、2021 年 9 月 1 日

C、2020 年 1 月 1 日

D、2021 年 1 月 1 日

2、下列( )方式属于对学生进行信息道德与信息安全教育。

A、用计算机播放影片

B、用计算机为某活动搜索素材

C、用计算机处理班级照片

D、播放计算机犯罪新闻专题片

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、下面程序的运行结果是： #i nclude<stdio.h> { int k=0; char c='A'; do {switch(c++) {case 'A':k++;break; case 'B':k--; case 'C':k+=2;break; case 'D':k=k%2;continue。

A、 k=0

B、 k=2

C、 k=3

D、 k=4

5、大学遭遇到DDOS攻击，那么根据网络安全应急预案，启动应急响应方案时，可以将应急预案定为哪个等级？（ ）

A、 3级

B、 4级

C、 2级

D、 1级

6、以下不属入侵检测中要收集的信息的是（ ）。

A、 系统和网络日志文件

B、 目录和文件的内容

C、 程序执行中不期望的行为

D、 物理形式的入侵信息

7、外部数据包过滤路由器只能阻止一种类型的 IP 欺骗，即（ ），而不能阻止 DNS 欺骗？

A、 内部主机伪装成外部主机的 IP

B、 内部主机伪装成内部主机的 IP

C、 外部主机伪装成外部主机的 IP

D、 外部主机伪装成内部主机的 IP

8、部署全网状或部分网状 IPSEC VPN 时为减小配置工作量可以使用哪种技术。（ ）

A、 L2tp+IPSEC

B、 DVPN

C、 IPSEC over GRE

D、 动态路由协议

9、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

10、数据库管理员应该定期对数据库进行重组，以保证数据库性能。下列有关数据库重组工作的说法，错误的是（ ）。

A、 重组工作中可能会对数据库数据的磁盘分区方法和存储空间进行调整

B、 重组工作一般会修改数据库的内模式和模式，一般不改变数据库外模式

C、 重组工作一般在数据库运行一段时间后进行，不应频繁进行数据库重组

D、 重组工作中应尤其注意频繁修改数据的表，因为这些表很容易出现存储碎片，导致效率下降

11、Skipjack 是一个密钥长度为( )位。

A、 56

B、 64

C、 80

D、 128

12、m-序列本身是适宜的伪随机序列产生器，但只有在（ ）下，破译者才不能破解这个伪随机序列。

A、 唯密文攻击

B、 已知明文攻击

C、 选择明文攻击

D、 选择密文攻击

13、小李在使用 nmap 对目标网络进行扫描时发现，某一个主机开放了 25 和 110 端口，此主机最有可能是什么？（ ）

A、 文件服务器

B、 邮件服务器

C、 WEB 服务器

D、 DNS 服务器

14、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

15、以下关于 TCP 和 UDP 协议的描述中，正确的是？（ ）

A、 TCP 是端到端的协议，UDP 是点到点的协议

B、 TCP 是点到点的协议，UDP 是端到端的协议

C、 TCP 和 UDP 都是端到端的协议

D、 TCP 和 UDP 都是点到点的协议

16、下面不是计算机网络面临的主要威胁的是?（ ）

A、 恶意程序威胁

B、 计算机软件面临威胁

C、 计算机网络实体面临威胁

D、 计算机网络系统面临威胁

17、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

18、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

19、Str='heiheihei' print str[3:]将输出？（　）

A、 hei

B、 heihei

C、 eih

D、 ihe

20、包过滤型防火墙工作在?（　）

A、 会话层

B、 应用层

C、 网络层

D、 数据链路层

21、下面是个人防火墙的优点的是?（　）

A、 运行时占用资源

B、 对公共网络只有一个物理接口

C、 只能保护单机，不能保护网络系统

D、 增加保护级别

22、关于 IP 提供的服务，下列哪种说法是正确的？（ ）

A、 IP 提供不可靠的数据投递服务，因此数据包投递不能受到保障

B、 IP 提供不可靠的数据投递服务，因此它可以随意丢弃报文

C、 IP 提供可靠的数据投递服务，因此数据报投递可以受到保障

D、 IP 提供可靠的数据投递服务，因此它不能随意丢弃报文

23、print type(2.0)将输出？（ ）

A、<type 'long'>

B、<type 'str'>

C、<type 'int'>

D、<type 'float'>

24、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

25、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

26、在 RHEL5 服务器中，查看用户 vanzk 密码记录的操作及输出如下所示：[root@pc05~]#grep vanzk /etc/shadow vanzk:!!1fKuFV9X8$VxFk0Ergj4uzP9UZGnleb.:15771:0:99999:7::: 则据此可判断用户 vanzk 的账号（ ）。

A、 每次设置新的密码后，有效期为 7 天，过期后必须重设

B、 其 uid 为 0，具有与 root 用户一样的权限

C、 因密码被锁定而无法登录

D、 使用的密码长度超过 8 位，安全性较高

27、Shell 编程条件判断中，文件权限判断说法错误的是？

A、 -r 判断该文件是否存在，并且该文件是否拥有读写权限

B、 -w 判断该文件是否存在，并且该文件是否拥有写权限

C、 -x 判断该文件是否存在，并且该文件是否拥有执行权限

D、 -u 判断该文件是否存在，并且该文件是否拥有 SUID 权限

28、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

29、VIM 光标操作说法中错误的是？（ ）

A、 h 光标向左移动一位

B、 2j 光标向下移动两行

C、 w 跳到下一个单词的词尾

D、 G 跳到文档的最后一行

30、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

31、部署 IPSEC VPN 时，配置什么安全算法可以提供更可靠的数据验证().

A、 DES

B、 3DES

C、 SHA

D、 128 位的 MD5

32、指数积分法（Index Calculus）针对下面那种密码算法的分析方法？

A、 背包密码体制

B、 RSA

C、 ElGamal

D、 ECC

33、Linux 的基本命令 ls，其选项-l 代表的是？

A、 显示详细信息

B、 查看目录属性

C、 人性化显示文件大小

D、 显示文件索引号

34、VIM 命令中，用于撤销的命令是？

A、 a

B、 x

C、 p

D、 u

35、你想发送到达目标网络需要经过那些路由器，你应该使用什么命令？

A、 Ping

B、 Nslookup

C、 Traceroute

D、 Ipconfig

二、 多选题 （每题 3 分，共 10 题，共 30 分）

1、数据库系统可能的潜在安全风险包括（）。

A、 操作系统安全风险，包括软件的缺陷、未进行软件安全漏洞修补工作、脆弱的服务和选择不安全的默认配置

B、 数据库系统中可用的但并未正确使用的安全选项、危险的默认设置、给用户不适当的权限、对系统配置的未经授权的改动等

C、 不及时更改登录密码或密码太过简单，存在对重要数据的非法访问以及

窃取数据库内容或恶意破坏等

D、 数据库系统的内部风险，如内部用户的恶意操作等

2、SQL Server 中的预定义服务器角色有（）。

A、 Sysadmin

B、 Serveradmm

C、 Setupadmin

D、 Securityadmin

3、想使用 python 输出 im happy 下面哪些写法是正确的?

A、 print (im happy)

B、 print 'im happy'

C、 echo 'im happy'

D、 print '''im happy'''

4、以下属于多表代换的密码是?

A、 Playfair

B、 Polybius

C、 Vigenere

D、 Hill 密码

5、下列关于 SQL Server 2008 身份验证模式的说法，正确的是（）。

A、 在"Windows 身份验证模式"下，不允许 sa 登录到 SQL Server 服务器

B、 在"Windows 身份验证模式"下,所有 Windows 用户都自动具有登录到 SQL Server 服务器的权限

C、 不管是哪种身份验证模式，Windows 中的 Administrator 无需授权就可登录到 SQL Server 服务器

D、 安装好 SQL Server 之后，可以根据需要随时更改身份验证模式

6、数据库访问控制的粒度可能有（）。

A、 数据库级

B、 表级

C、 记录级（ 行级 ）

D、 属性级

7、操作系统安全主要包括（ ）等方面 。

A、 账户密码安全和文件共享安全

B、 文件权限管理和用户权限管理

C、 日志审计和远程访问权限管理

D、 文件夹选项和安全选项

8、IPSec 可以提供哪些安全服务 ()

A、 数据机密性

B、 数据完整性

C、 数据来源认证

D、 防重放攻击

9、关于类的说法，下面哪些是错误的?

A、 私有方法和私有变量只能在类的内部使用

B、 一个类只能创建一个实例

C、 两个不同的类中的方法不能重名

D、 创建类的实例时，传入的变量类型要和类中定义的一致

10、IKE 的主要功能包括()

A、 建立 IPSec 安全联盟

B、 防御重放攻击

C、 数据源验证

D、 自动协商交换密钥