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

赛题八

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。

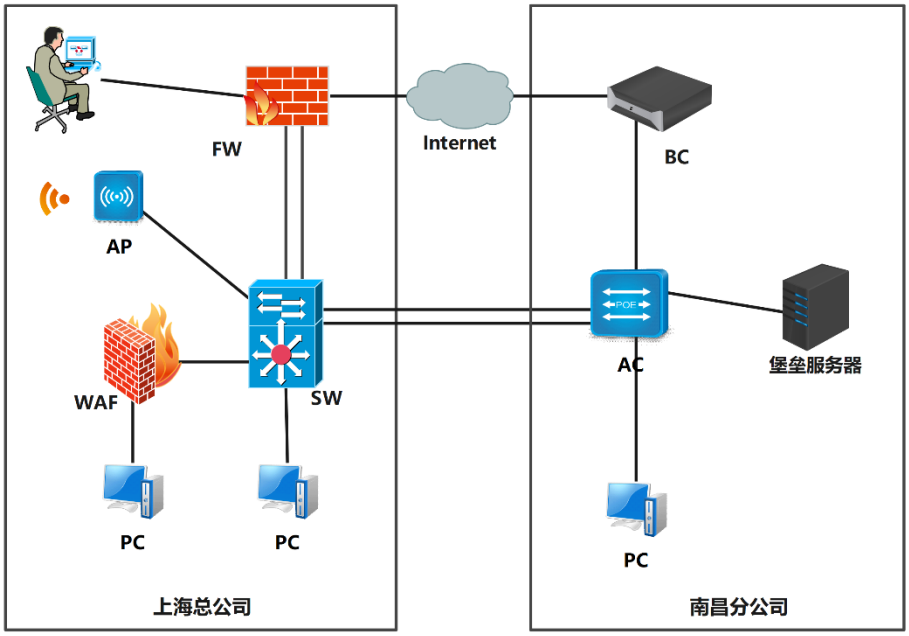
选手首先需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹（xx 用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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

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	10.10.255.1/30（trust 安全域） 2001:DA8:10:10:255::1/127	SW	eth1/0/1-2
		10.10.255.5/30（trust 安全域） 2001:DA8:10:10:255::5/127	SW	
	ETH0/3	20.23.1.1/30（untrust 安全域） 223.20.23.1/29(nat-pool) 2001:DA8:223:20:23::1/64	SW	Eth1/0/23
	Loopback1	10.0.0.254/32（trust） Router-id		
	SSL Pool	192.168.10.1/26 可用 IP 数量为 20	SSL VPN 地址池	
三层交换机 SW	ETH1/0/4	专线	AC ETH1/0/4	
	ETH1/0/5	专线	AC ETH1/0/5	
	VLAN21 ETH1/0/1-2	10.10.255.2/30 2001:DA8:10:10:255::2/127	FW	Vlan name TO-FW1
	VLAN22 ETH1/0/1-2	10.10.255.6/30 2001:DA8:10:10:255::6/127	FW	Vlan name

设备名称	接口	IP 地址	对端设备	接口
				TO-FW2
	VLAN 23 ETH1/0/23	20.23.1.2/30 2001:DA8:223:20:23::2/127	FW	Vlan name TO-internet
	VLAN 24 ETH1/0/24	223.20.23.10/29 2001:DA8:223:20:23::10/127	BC	Vlan name TO-BC
	VLAN 10	172.16.10.1/24	无线 1	Vlan name WIFI-vlan10
	VLAN 20	172.16.20.1/24	无线 2	Vlan name WIFI-vlan20
	VLAN 30 ETH1/0/6-7	192.168.30.1/24 2001:DA8:192:168:30:1::1/96		Vlan name XZ
	VLAN 31 Eth1/0/8-9	192.168.31.1/24 2001:DA8:192:168:31:1::1/96		Vlan name sales
	VLAN 40 ETH1/0/10-11	192.168.40.1/24 2001:DA8:192:168:40:1::1/96		Vlan name CW
	Vlan 50 Eth1/0/13-14	192.168.50.1/24 2001:DA8:192:168:50:1::1/96		Vlan name manage
	Vlan1001	10.10.255.9/30 2001:DA8:10:10:255::9/127		TO-AC1
	Vlan1002	10.10.255.13/30 2001:DA8:10:10:255::13/127		TO-AC2
	VLAN 1000 ETH 1/0/20	172.16.100.1/24		Vlan name AP-Manage
	Loopback1	10.0.0.253/32(router-id)		
无线控制器 AC	VLAN 10	192.168.10.1/24 2001:DA8:192:168:10:1::1/96		Vlan name TO-CW
	VLAN 20	192.168.20.1/24 2001:DA8:192:168:20:1::1/96		Vlan name CW

设备名称	接口	IP 地址	对端设备	接口
	VLAN 1001	10.10.255.10/30 2001:DA8:10:10:255::10/127		
	VLAN 1002	10.10.255.14/30 2001:DA8:10:10:255::14/127		
	Vlan 60 Eth1/0/13-14	192.168.60.1/24 2001:DA8:192:168:60:1::1/96		Vlan name sales
	Vlan 61 Eth1/0/15-18	192.168.61.1/24 2001:DA8:192:168:61:1::1/96		Vlan name BG
	Vlan 100 Eth1/0/21	10.10.255.17/30 2001:DA8:10:10:255::17/127	BC eth2	Vlan name TO-BC
	VLAN 2000 ETH 1/0/19	192.168.100.1/24	沙盒	
	Loopback1	10.1.1.254/32(router-id)		
日志服务器 BC	eth2	10.10.255.18/30 2001:DA8:10:10:255::18/127	AC	
	ETH3	223.20.23.9/29 2001:DA8:223:20:23::9/127	SW	
	PPTP-pool	192.168.10.129/26（10 个地址）		
WEB 应用防火墙 WAF	ETH2	192.168.50.2/24	PC3	
	ETH3		SWEth1/0/13	
AP	Eth1		SW（20 口）	
PC1	网卡	eth1/0/7	SW	
沙盒		192.168.100.10/24	AC ETH1/0/19	

(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. SW 和 AC 开启 SSH 登录功能，SSH 登录账户仅包含“USER-SSH”，密码为明文“123456”，采用 SSH 方式登录设备时需要输入 enable 密码，密码设置为明文“enable” 。
2. 应网监要求，需要对上海总公司用户访问因特网行为进行记录，需要在交换机上做相关配置，把访问因特网的所有数据镜像到交换机 1/0/18 口便于对用户上网行为进行记录。
3. 尽可能加大上海总公司核心和出口之间带宽，端口模式采用 lacp 模式。
4. 上海总公司和南昌分公司租用了运营商两条裸光纤，实现内部办公互通，要求两条链路互为备份，同时实现流量负载均衡，流量负载模式基于 Dst-src-mac 模式。
5. 上海总公司和南昌分公司链路接口只允许必要的 vlan 通过，禁止其它 vlan 包括 vlan1 二层流量通过。
6. 为防止非法用户接入网络，需要在核心交互上开启DOT1X认证，对vlan40用户接入网络进行认证，radius-server 为192.168.100.200。
7. 为了便于管理网络，能够让网管软件实现自动拓朴连线，在总公司核心和分公司 AC 上开启某功能，让设备可以向网络中其他节点公告自身的存在，并保存各个邻近设备的发现信息。
8. ARP 扫描是一种常见的网络攻击方式，攻击源将会产生大量的 ARP 报文在网段内广播，这些广播报文极大的消耗了网络的带宽资源，为了防止该攻击对网络造成影响，需要在总公司交换机上开启防扫描功能，对每端口设置阈值为 40，超过将关闭该端口 20 分钟后自动恢复，设置和分公司互联接口不检查。

9. 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。
10. 对 SW 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;开启防止 ARP 网关欺骗攻击。
11. 配置使上海公司核心交换机 VLAN31 业务的用户访问因特网数据流经过 10.10.255.1 返回数据通过 10.10.255.5。要求有测试结果。
12. 为响应国家号召，公司实行 IPV6 网络升级改造，公司采用双栈模式，同时运行 ipv4 和 ipv6，IPV6 网络运行 OSPF V3 协议，实现内部 ipv6 全网互联互通，要求总公司和分公司之间路由优先走 vlan1001，vlan1002 为备份。
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，ipv6 地址范围 2001:da8:192:168:31:1::2-2001:da8:192:168:31:1::100。
14. 在南昌分公司上配置 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 之间配置 OSPF，实现 ipv4 网络互通。要求如下：区域为 0 同时开启基于链路的 MD5 认证，密钥自定义，传播访问 INTERNET 默认路由，分公司内网用户能够与总公司相互访问包含 loopback 地址；分公司 AC 和 BC 之间运行静态路由。
16. 总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 10.0.0.254，地址池范围 192.168.31.10-192.168.31.100，dns-server 8.8.8.8。

17. 总公司交换机上开启 dhcp server 为无线用户分配 ip 地址，地址租约时间为 10 小时，dns-server 为 114.114.114.114，前 20 个地址不参与分配,第一个地址为网关地址。
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. 交换机的端口 10 不希望用户使用 ftp，也不允许外网 ping 此网段的任何一台主机。
20. 交换机 vlan 30 端口连接的网段 IPV6 的地址为 2001:da8:192:168:30:1::0/96 网段，管理员不希望除了 2001:da8:192:168:30:1:1::0/112 网段用户访问外网。
21. 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 ping、SSH、HTTPS 功能。
22. 在总部防火墙上配置，总部VLAN业务用户通过防火墙访问Internet时，复用公网IP： 223.20.23.1/29，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192.168.100.10 的UDP 2000 端口。
23. 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，端口号使用 4455，用户名密码均为 ABC2023，地址池参见地址表。
24. 总公司部署了一台 WEB 服务器 ip 为 192.168.50.10，为外网用户提供 web 服务，要求外网用户能访问服务器上的 web 服务（端口 80）和远程管理服务器（端口 3389），外网用户只能通过 223.20.23.2 外网地址访问服务器 web 服务和 3389 端口。

25. 为了安全考虑，需要对内网销售部门用户访问因特网进行实名认证，要求在防火墙上开启 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。
26. 由于总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 4M，上传为 2M，http 访问总带宽为 50M。
27. 财务部门和公司账务有关，为了安全考虑，禁止财务部门访问因特网，要求在防火墙 FW 做相关配置。
28. 由于总公司销售和分公司销售部门使用的是同一套 CRM 系统，为了防止专线故障导致系统不能使用，总公司和分公司使用互联网作为总公司销售和分公司销售相互访问的备份链路。FW 和 BC 之间通过 IPSEC 技术实现总公司销售段与分公司销售之间联通，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。
29. 分公司用户，通过 BC 访问因特网，BC 采用路由方式，在 BC 上做相关配置，让分公司内网用户通过 BC 外网口 ip 访问因特网。
30. 在 BC 上配置 PPTP vpn 让外网用户能够通过 PPTP vpn 访问分公司 AC 上内网资源，用户名为 GS01，密码 GS0123。
31. 分公司部署了一台安全攻防平台，用来公司安全攻防演练，为了方便远程办公用户访问安全攻防平台，在 BC 上配置相关功能，让外网用户能通过 BC 的外网口接口 IP，访问内部攻防平台服务器，攻防平台服务器地址为 192.168.100.10 端口：8080。
32. 在 BC 上配置 url 过滤策略，禁止分公司内网用户在周一到周五的早上 8 点到晚上 18 点访问外网 www.skillchina.com。
33. 对分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。

34. 为了安全考虑，无线用户移动性较强，访问因特网时需要实名认证，在BC上开启web认证使用http方式，采用本地认证，密码账号都为web2023。
35. DOS攻击/DDoS 攻击通常是以消耗服务器端资源、迫使服务停止响应为目标，通过伪造超过服务器处理能力的请求数据造成服务器响应阻塞，从而使正常的用户请求得不到应答，以实现其攻击目的，在分公司内网区域开起DOS攻击防护，阻止内网的机器中毒或使用攻击工具发起的 DOS 攻击，检测到攻击进行阻断。
36. 分公司 BC 上配置 NAT64，实现分公司内网 ipv6 用户通过 BC 出口 ipv4 地址访问因特网。
37. 分公司内网攻防平台，对 Internet 提供服务，在 BC 上做相关配置让外网 IPV6 用户能够通过 BC 外网口 IPV6 地址访问攻防平台的 web 服务端口号为 80。
38. BC 上开启病毒防护功能，无线用户在外网下载 exe、rar、bat 文件时对其进行杀毒检测，防止病毒进入内网，协议流量选择 HTTP 杀毒、FTP 杀毒、POP3、SMTP。
39. 公司内部有一台网站服务器直连到 WAF，地址是 192.168.50.10，端口是 8080，配置将访问日志、攻击日志、防篡改日志信息发送 syslog 日志服务器， IP 地址是 192.168.100.6，UDP 的 514 端口。
40. 编辑防护策略，在“专家规则”中定义 HTTP 请求体的最大长度为 256，防止缓冲区溢出攻击。
41. WAF 上配置开启爬虫防护功能，防护规则名称为 http 爬虫，url 为 www.2023skills.com，自动阻止该行为；封禁时间为 3600 秒。

42. WAF 上配置，开启防盗链，名称为 http 盗链，保护 url 为 www.2023skills.com，检测方式 referer+cookie，处理方式为阻断，并记录日志。
43. WAF 上配置开启 IDP 防护策略，采用最高级别防护，出现攻击对攻击进行阻断。
44. WAF 上配置开启 DDOS 防护策略，防护等级高级并记录日志。
45. 在公司总部的 WAF 上配置，内部 web 服务器进行防护安全防护，防护策略名称为 web_p，记录访问日志，防护规则为扫描防护规则采用增强规则、HTTP 协议校验规则采用专家规则、特征防护规则采用专家规则、开启爬虫防护、开启防盗链、开启敏感信息检测。
46. AC 上配置 DHCP，管理 VLAN 为 VLAN1000,为 AP 下发管理地址，AP 通过 DHCP opion 43 注册，AC 地址为 loopback1 地址。
47. 在 NETWORK 下配置 SSID，需求如下：NETWORK 1 下设置 SSID SKILL-WIFI，VLAN10，加密模式为 wpa-peSWonal,其口令为 12345678，开启隔离功能。
48. 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 XXX 密码为 test2023。
49. 为了合理利用 AP 性能，需要在 AP 上开启 5G 优先配置 5G 优先功能的客户端的信号强度门限为 40。
50. 通过配置防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接，两小时后恢复正常；GUSET 最多接入 50 个用户，并对 GUEST 网络进行流控，上行 1M，下行 2M。

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 服务器虚拟机		
序号	任务内容	答案
1	请提交攻击者的 IP 地址	
2	请提交攻击者使用的操作系统	
3	请提交攻击者进入网站后台的密码	
4	请提交攻击者首次攻击成功的时间，格式：DD/MM/YY:hh:mm:ss	

5	请提交攻击者上传的恶意文件名（含路径）	
6	请提交攻击者写入的恶意后门文件的连接密码	
7	请提交攻击者创建的用户账户名称	
8	请提交恶意进程的名称	
9	请提交恶意进程对外连接的 IP 地址	

第二部分 数字取证调查（150 分）

任务 2：基于 Windows Server 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 Windows Server 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(TCP/IP)（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(TCP/IP)		
序号	任务内容	答案
1	请提交攻击者通过什么协议发起的攻击	
2	请提交攻击者第一次攻击成功的时间	
3	请提交攻击者在目标主机上上传的文件名	
4	请解密出上传的文件内容	

任务 4：基于 Linux 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 Linux 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	提交文件名正确得分	
evidence 2	提交文件名正确得分	
evidence 3	提交文件名正确得分	
evidence 4	提交文件名正确得分	
evidence 5	提交文件名正确得分	
evidence 6	提交文件名正确得分	

evidence 7	提交文件名正确得分	
evidence 8	提交文件名正确得分	
evidence 9	提交文件名正确得分	
evidence 10	提交文件名正确得分	

第三部分 应用程序安全（80 分）

任务 5：Windows 恶意程序分析（50 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：Windows 恶意程序

请按要求完成该部分的工作任务。

任务 5：Windows 恶意程序分析		
序号	任务内容	答案
1	请提交恶意程序回传数据的 url 地址	
2	请指出恶意程序会加密哪些类型的文件	
3	请指出恶意程序加密文件的算法	
4	请指出恶意程序创建的子进程名称	

任务 6：JAVA 语言代码审计（30 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：Java 源文件

请按要求完成该部分的工作任务。

任务 6：JAVA 语言代码审计

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、 人力资源管理系统（45 分）

任务编号	任务描述	答案	分值
任务一	请对人力资源管理系统进行黑盒测试，利用漏洞找到 flag1，并将 flag1 提交。flag1 格式 flag1{<flag 值>}		
任务二	请对人力资源管理系统进行黑盒测试，利用漏洞找到 flag2，并将 flag2 提交。flag2 格式 flag2{<flag 值>}		
任务三	请对人力资源管理系统进行黑盒测试，利用漏洞找到 flag3，并将 flag3 提交。flag3 格式 flag3{<flag 值>}		

二、 邮件系统（30 分）

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

任务编号	任务描述	答案	分值
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、 认证服务器（30 分）

任务编号	任务描述	答案	分值
任务十四	认证服务器 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、 运维服务器（30 分）

任务编号	任务描述	答案	分值
任务十五	运维服务器 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

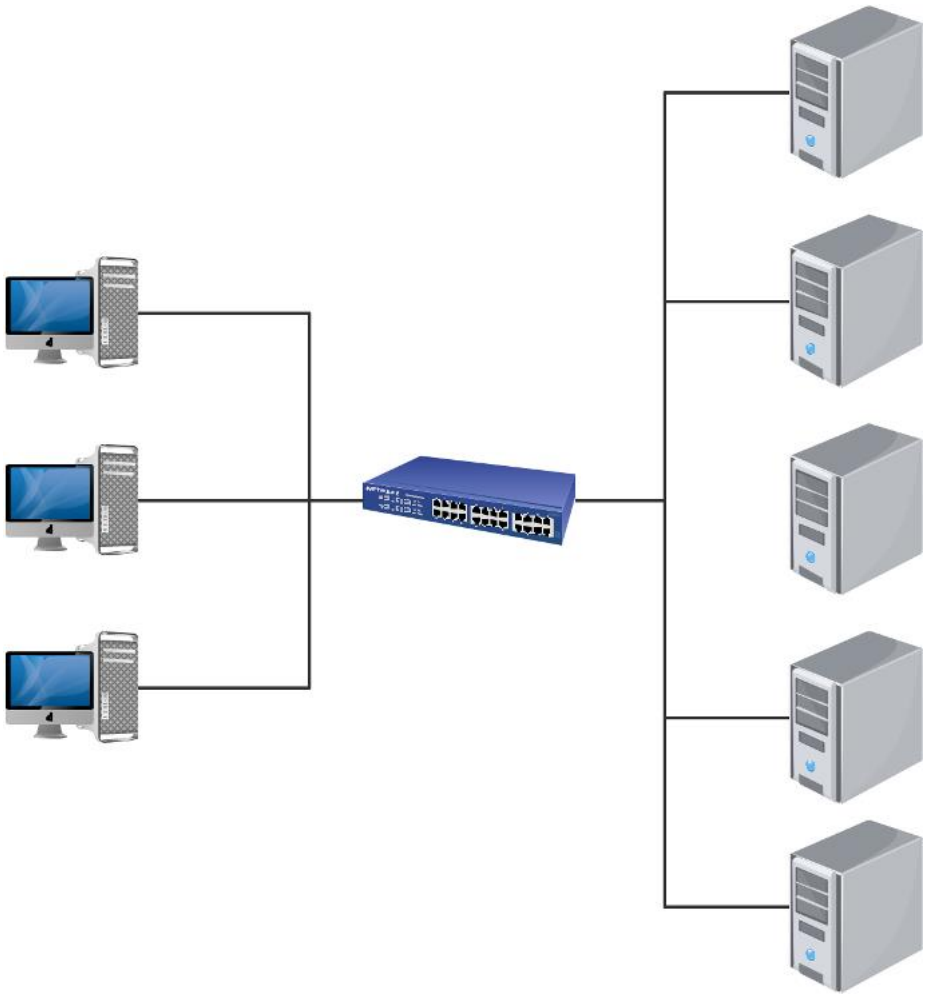


图 1 网络拓扑结构图

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、(　)是指在信息的采集、加工、存储、传播和利用的各个环节中，用来规范期间产生的各种社会关系的道德意识、道德规范和道德行为的总和。

A、信息规范

B、信息规则

C、信息道德

D、信息行为

2、以下能够大幅度提高信息安全的做法是(　)。

A、不再网络条件下使用计算机

B、定期使用安全软件

C、尽量少用计算机

D、多用纸质工具工作

3、以下不属于入侵监测系统的是（　　）　。

A、 AAFID 系统

B、 SNORT 系统

C、 IETF 系统

D、 NETEYE 系统

4、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

5、下面不是 SQL Server 支持的身份认证方式的是（　　）。

A、 Windows NT 集成认证

B、 SQL Server 认证

C、 SQL Server 混合认证

D、 生物认证

6、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

7、SHA-1 接受任何长度的输入消息，并产生长度为（　　）比特的 hash 值。

A、 64

B、 160

C、 128

D、 512

8、下列选项中不是 Hydra 工具中的-e 参数的值是？（　　）

A、 o

B、 n

C、 s

D、 r

9、在 Google Hacking 中，下面哪一个是搜索指定文件类型的语句？（　　）

A、 intext

B、 Intitle

C、 site

D、 filetype

10、以下选项中，对文件的描述错误的是哪个选项？（　　）

A、 文件中可以包含任何数据内容

B、 文本文件和二进制文件都是文件

C、 文本文件不能用二进制文件方式读入

D、 文件是一个存储在辅助存储器上的数据序列

11、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

12、攻击者在使用 nmap 对目标网络进行扫描时发现，某个主机开放了 25 和 110 端口，此主机最有可能是？（　　）

A、 文件服务器

B、 邮件服务器

C、 WEB 服务器

D、 DNS 服务器

13、在数据库系统中,死锁属于（　　） 。

A、 系统故障

B、 事务故障

C、 介质保障

D、 程序故障

14、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

15、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

16、如果想在类中创建私有方法，下面哪个命名是正确的？（　　）

A、 _add_one

B、 add_one

C、 __add_one

D、 add_one__

17、如果想在文件 test.txt 中追加内容，应该使用下列哪个选项？（　　）

A、 a=open('test.txt',"a")

B、 a=open('test.txt',"r")

C、 a=open('test.txt',"d")

D、 a=open('test.txt',"w")

18、当下各大厂商均有相关的应急响应中心部门，奖励均根据漏洞等级来进行划分。根据相应的安全标准，下列哪项不符合该要求？（　　）

A、 警告

B、 中危

C、 低危

D、 超危

19、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

20、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

21、当发现原有的 IDS 不能检测到新的攻击类型时，你应该采取哪种措施？（　　）

A、 购买或更新特征库

B、 配置防火墙

C、 关闭 IDS 直到得到新的 IDS 应用程序

D、 定义一个新的规则来检测攻击

22、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

23、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

24、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

25、os.getcwd()函数的作用是？（　　）

A、 返回当前目录下的文件

B、 返回当前目录的路径

C、 返回上一层目录的路径

D、 返回当前目录下的文件夹列表

26、哪个关键词可以在 python 中进行处理错误操作？（ ）

A、 try

B、 catch

C、 finderror

D、 error

27、下面哪一项不是 hash 函数的主要应用？（ ）

A、 文件校验

B、 数字签名

C、 数据加密

D、 鉴权协议

28、Geffe 发生器使用了（ ） 个 LFSR。

A、 1

B、 2

C、 3

D、 4

29、ELK 日志解决方案中，Elasticsearch 的作用是？（ ）

A、 收集日志并分析

B、 保存日志并搜索日志

C、 收集日志并保存

D、 保存日志并展示日志

30、CVE-2016-8704（ ）

A、 CVE-2016-8704

B、 CVE-2016-8705

C、 CVE-2018-8174

D、 CVE-2016-8706

31、下面哪种密码算法抵抗频率分析攻击能力最强，而对已知明文攻击最弱？（ ）

A、 仿射密码

B、 维吉利亚

C、 轮转密码

D、 希尔密码

32、re.match 函数中参数 Flag 的作用是？（ ）

A、 声明正则表达式的内容

B、 声明正则表达式的名称

C、 控制正则表达式的匹配方式

D、 声明要匹配的字符串

33、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

34、VIM 退出命令中，能强制保存并退出的是？（　　）

A、 x

B、 wq

C、 q

D、 wq!

35、将用户 user123 修改为管理员权限命令是 （　　）。

A、 net user localgroup administrators user123 /add

B、 net use localgroup administrators user123 /add

C、 net localgroup administrators user123 /add

D、 net localgroup administrator user123 /add

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、下列哪些选项属于木马程序？（　　）

A、 X—Scan

B、 流光

C、 BO

D、 冰河

3、关于函数，下面哪些说法是错误的？（　　）

A、 函数必须返回一个结果

B、 函数不能调用自身

C、 函数命名只能以字母或数字开头

D、 在同一个文件中，不应定义重名的函数

4、下面哪些函数的执行结果将返回一个元组？（ ）

A、 os.stat

B、 os.path.split

C、 os.listdir

D、 os.getcwd

5、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

6、数据库的完整性分为以下种类（ ） 。

A、 实体完整性

B、 域完整性

C、 参照完整性

D、 用户定义完整性

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、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、IPSec 的安全联盟与 IKE 的安全联盟的区别是（ ）。

A、 IPSec 的安全联盟是单向的

B、 IPSec 的安全联盟是双向的

C、 IKE 的安全联盟是单向的

D、 IKE 的安全联盟是双向的

10、Bash 环境变量中，常见的环境变量有？（ ）

A、 HOSTNAME

B、 PASS

C、 SHELL

D、 USER