2024 年上海高职院校学生技能大赛

信息安全管理与评估

样题

赛项时间

三个模块，共计 4 小时。

模块一

平台搭建与安全设备配置防护

一、 赛项信息

竞赛阶段	任务阶段	竞赛任务	分值
第一阶段 平台搭建与安全设备配置防护	任务 1	网络平台搭建	50
	任务 2	网络安全设备配置与防护	250

二、 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。

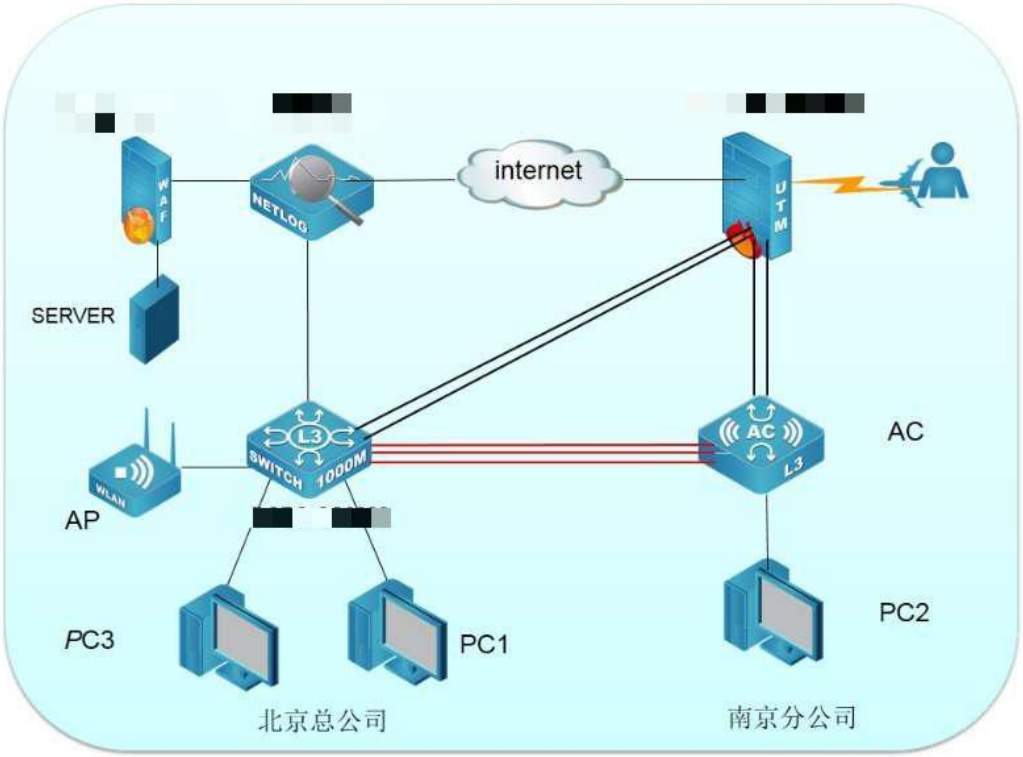
例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

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2024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2024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	192.168.40.1/24		Vlan name

	ETH1/0/8-9	IPV6 2001:DA8:192:168:40::1/96		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	172.16.50.1/24		Vlan name

	Eth1/0/13-14	IPV6 2001:DA8:172:16:60::1/96		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 RS 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“***2024”，密码为明文“***2024”，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 GROUP2024，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 USER2024，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 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；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。
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 ABC2022，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 web2022，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 ***2022，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 GS2024，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.2024skills.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 ***2024，VLAN10，加密模式为 wpa-personal,其口令为 20242024；

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 test2024；

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。

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。

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 350 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

工作任务

第一部分 网络安全事件响应

任务 1 ：操作系统取证

A 集团某 Windows 服务器系统感染恶意程序，导致系统被远程监听，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：操作系统镜像、内存镜像。

请根据赛题环境及任务要求提交正确答案。

任务 1：操作系统取证		
序号	任务要求	答案
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

第二部分 数字取证调查

任务 2： 网络数据包分析

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。

请根据赛题环境及任务要求提交正确答案。

任务 2：网络数据包分析		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

第三部分 应用程序安全

任务 3：代码审计

A 集团发现其发布的 Web 应用程序遭到了恶意攻击，A 集团提供了 Web 应用程序的主要代码，您的团队需要协助 A 集团对该应用程序代码进行分析，找出存在的脆弱点。

本任务素材清单：程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 3：代码审计		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

任务 4：系统恶意程序分析

A 集团发现其网络中蔓延了一种恶意程序，现在已采集到恶意程序的样本，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：恶意程序文件。

请根据赛题环境及任务要求提交正确答案。

任务 4：系统恶意程序分析		
序号	**任务要求**	**答案**
1	任务要求 1	
2	任务要求 2	
3	任务要求 3	
4	.....	

模块三

夺旗挑战 CTF（网络安全渗透）

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：夺旗挑战 CTF（网络安全渗透）。

介绍

夺旗挑战 CTF（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 350。

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。

工作任务

一、 Web 服务器

任务环境说明：

靶机：

服务器场景 1：linux（WEB 服务器）

任务内容：

1. 系统页面中存在隐藏信息，请找出隐藏信息，并将 Flag 值提交；
2. 系统首页图片存在隐藏信息，请找出隐藏信息，并将 Flag 值提交；
3. 设法找到登陆网站后台地址，将可用的帐号作为 FLAG 值提交；
4. 系统后台存在漏洞，请利用漏洞并找到 flag，并将 flag 提交；
5. 根据找到的提示将主目录下 flag 文件的内容作为 flag 提交；

二、 数据库服务器

任务环境说明：

靶机：

服务器场景 1：linux（数据库服务器）

1. 使用 nmap 扫描目标数据库服务器，将目标服务器使用的数据库版本号作为 flag 提交；
2. 利用普通用户 对目标数据库服务器进行爆破，将该普通用户的密码作为 flag 提交；
3. 利用普通用户对目标数据库服务器进行渗透，将具有管理员权限的用户名作为 flag 提交；
4. 设法解密或提权该数据库用户，获得数据库服务器中/root/flag.txt 文件，将该文件内容作为 flag 提交；

三、 FTP 服务器

任务环境说明：

靶机：

服务器场景 1：linux（FTP 服务器）

任务内容：

1. 请获取 FTP 服务器上对应的 F1 文件进行分析，找出其中隐藏的 flag，并将 flag 提交。
2. 请获取 FTP 服务器上对应的 F2 文件进行分析，找出其中隐藏的 flag，并将 flag 提交。

3. 请获取 FTP 服务器上对应的 F3 文件进行分析，找出其中隐藏的 flag，并将 flag 提交。
4. 请获取 FTP 服务器上对应的 F4 文件进行分析，找出其中隐藏的 flag，并将 flag 提交。
5. 请获取 FTP 服务器上对应的 F5 文件进行分析，找出其中隐藏的 flag，并将 flag 提交。

四、 加密服务器

任务环境说明：

靶机：

服务器场景 1：LINUX（版本不详）

1. 通过本地 PC 中渗透测试平台对服务器场景进行渗透测试，在/root 目录下执行./crackme 将显示的第一行字符串通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
2. 设法获得 crackme 进行逆向分析，将程序 crc32 校验码通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
3. 继续分析 crackme，将找到的密文通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
4. 继续分析 crackme，将找到的密钥通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；
5. 继续分析 crackme，将密文解密后的明文通过 MD5 运算后返回哈希值的十六进制结果作为 Flag 值提交（形式：十六进制字符串）；

附录 A

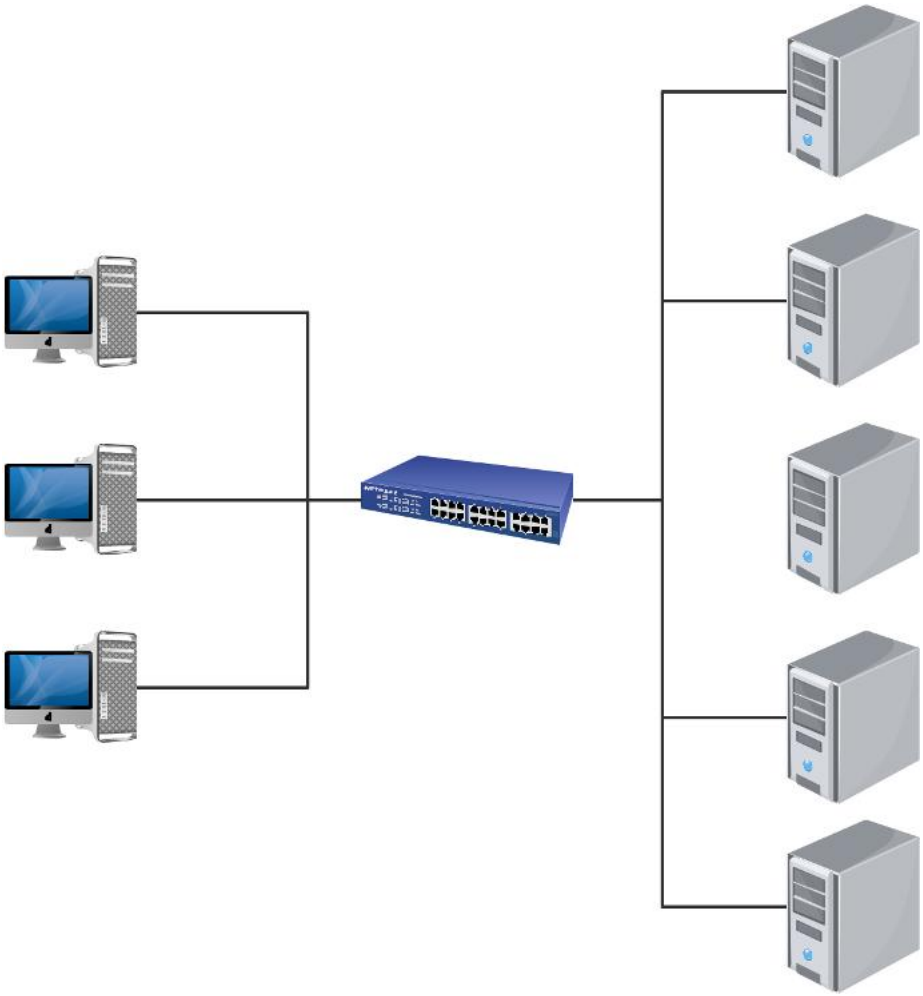


图 1 网络拓扑结构图