上海市“星光计划”第十一届职业院校技能大赛

（高职组）

“信息安全管理与评估”赛项

任务书

一、 赛项时间

共计 4 小时。

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 平台搭建与安全设备配置防护	任务 1	网络平台搭建	240 分钟	50
	任务 2	网络安全设备配置与防护		200
第二阶段 网络安全事件响应、数字取证调查和应用程序安全	任务 1	操作系统取证		250
	任务 2	网络数据包分析		
	任务 3	代码审计		
	任务 4	系统恶意程序分析		
第三阶段 夺旗挑战 CTF（网络安全渗透）	任务 1	Web 服务器		300
	任务 2	协议服务器		
	任务 3	FTP 服务器		
	任务 4	加密服务器		

第一阶段竞赛项目试题

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。

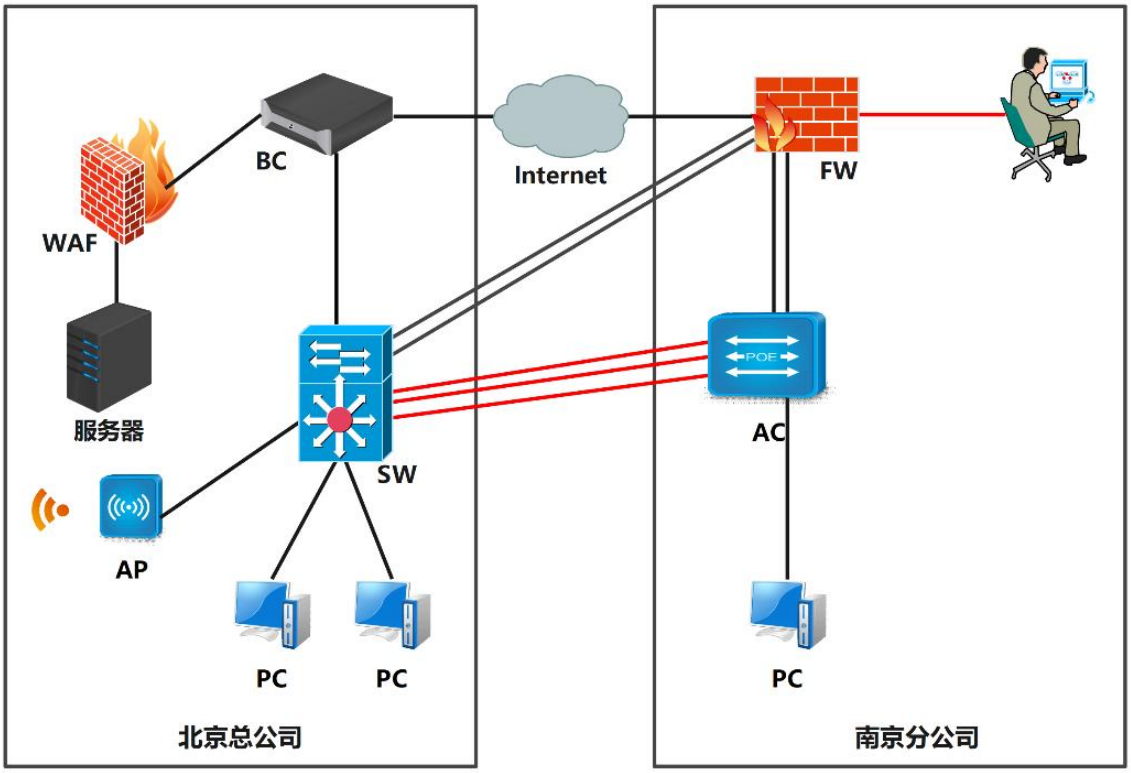
例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

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。

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/Vlan
防火墙 FW	Eth0/1-2	10.0.0.1/30（trust1 安全域）	SW	Eth1/0/1-2
		10.0.1.1/30(untrust1 安全域）	SW	
		222.24.1.1/29（untrust）	SW	
	Eth0/4-5	10.0.0.13/30（trust 安全域）	AC	Eth1/0/21-22
	Loopback1	10.0.0.254/32（trust 安全域） （Router-id）		
	Tunnel1	192.168.10.1/26(VPNHub 安全域） 可用 IP 数量为 20（2-21）		VPN 地址池
三层交换机 SW	Eth1/0/5	trunk	AC	Eth1/0/5
	Eth1/0/6	trunk	AC	Eth1/0/6
	Vlan 21	10.0.0.2/30	FW	Eth1/0/1-

	Eth1/0/1-2			2
	Vlan 22 Eth1/0/1-2	10.0.1.2/30	FW	Eth1/0/1-2
	Vlan 25 Eth 1/0/3	10.0.0.9/30 2001:da8:10:24::1/126	BC	Eth 1
	Vlan 30	10.0.0.5/30	AC	Vlan name TO-CW
	Vlan 31 Eth1/0/10-12	192.168.3.1/25		Vlan name CW
	Vlan 40 Eth1/0/8-9	192.168.40.1/24 2001:da8:20:20::1/64		销售
	Vlan 50 Eth1/0/13-14	192.168.50.1/24 2001:da8:20:21::1/64		产品
	Vlan 60	192.168.60.1/24 2001:da8:10:24::5/126		管理 Native Vlan
	Vlan 100 Eth 1/0/20	Ipv4:需设定	AP	AP-Manage
	Loopback1	10.0.0.253/32(router-id)		
internet	Vlan 222 Eth1/0/1-2	222.24.1.2/29	FW	Eth1/0/1-2
	Vlan 24 Eth1/0/23-24	113.13.1.2/29 240e:3ae:10::1/64	BC	Eth 5
	Loopback2	240e:5a::1/128		IPV6 测试地址
无线控制器 AC	Vlan 30	10.0.0.6/30	SW	Vlan name TO-CW
	Vlan 10 无线 1	Ipv4:需设定 Ipv6:接口 ID: 0:0:0:e::1/64		Vlan name WIFI-Vlan 10
	Vlan 20 无线 2	Ipv4:需设定 Ipv6:接口 ID: 0:0:0:f::1/64		Vlan name WIFI-Vlan 20
	Vlan 31	192.168.3.129/25		Vlan name

	Eth 1/0/9-10			CW
	Vlan 140 Eth1/0/11-12	172.17.40.1/24 Ipv6:接口 ID: 0:0:0:8::1/64		销售
	Vlan 150 Eth1/0/13-14	172.17.50.1/24 Ipv6:接口 ID: 0:0:0:9::1/64		产品
	Vlan 60	192.168.60.2/24 2001:da8:10:24::6/126		管理 Native Vlan
	Vlan 70 Eth1/0/21-22	10.0.0.14/30	FW	Eth1/0/4-5
	Loopback1	10.0.0.252/32(router-id)		
日志服务器 BC	Eth1	10.0.0.10/30（L3-LAN 安全域） 2001:da8:10:24::2/126	SW	Eth1/0/3
	Eth5	113.13.1.1/29(L3-WAN 安全域） 240e:3ae:10::2/64	SW	Eth1/0/23
	Eth3	192.168.218.1/24（L3-DMZ 安全域）	WAF	Eth3
	PPTP-pool	192.168.10.129/26(10 个地址）		
WEB 应用防火墙 WAF	Eth2	192.168.218.2/24	SERVER	
	Eth3		BC	Eth3
AP	Eth		SW	Eth1/0/20

3. 设备初始化信息

设备名称	管理地址	默认管理接口	用户名	密码
防火墙 FW	https://192.168.1.1	Eth0	admin	admin
网络日志系统 BC	https://192.168.0.1:9090	Eth0	admin	admin*PWD
WEB 应用防火墙 WAF	https://192.168.254.1	Eth1	admin	yunke1234!
三层交换机 SW	-	Console 9600	-	-

无线交换机 AC	-	Console 9600	-	-
备注	所有设备的默认管理接口、管理 IP 地址不允许修改; 如果修改对应设备的缺省管理 IP 及管理端口，涉及此设备的题目按 0 分处理。			

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 的各接口 IP 地址进行配置。
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	根据网络拓扑图所示，按照 IP 地址规划表，对 WAF 的名称、各接口 IP 地址进行配置。

注意：为了便于实现题目的测试结果，将 SW、AC 的 Eth1/0/18 端口设置为 trunk 模式，并仅放行业务 Vlan（含财务），连接到 WAF 的空余端口。

任务 2：网络安全设备配置与防护（200 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，禁止使用 trunk 链路。
2. SW 和 AC 开启 telnet 登录功能，telnet 登录账户仅包含“SKILLS2024”，密码为明文“SKILLS2024”，采用 telnet 方式登录设备时需要输入 enable 密码，密码设置为明文“20242024” ，只允许管理 Vlan 通过 telnet 登录设备。

3. 北京总公司和南京分公司租用了运营商两条裸光纤，实现内部办公互通。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，包含 TO-CW Vlan，总公司财务部门和分公司财务部门之间采用 OSPF 路由实现互相访问;OSPF 进程号:2,router-id 为各自 Vlan30 的 IP 地址。
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，TO-CW Vlan、管理 Vlan 关联实例 2，名称为 SKILLS，修订版本为 1，设置 AC 为根交换机，无线用户通过 5 口链路转发,TO-CW Vlan、管理 Vlan 通过 6 口链路转发，同时实现链路备份。除了裸光纤接口，关闭其他接口生成树协议。
5. 总公司 SW 承载了总公司所有内部数据交换，考虑到核心的稳定可靠，计划在总公司增加一台核心作为核心交换备份，现有交换机作为主交换进行转发数据，未来新增加的交换机作为备份交换机，主交换机出现故障时，由备份交换机接替主交换机进行数据转发，实现核心交换机热备。需要在核心交换机上完成相关配置，方便未来实现核心热备。只对销售部门和产品部门做相关配置，销售部门和产品部门最后一个可用 ip 为虚拟网关地址，开启抢占模式。
6. 交换机的端口11不允许转发源MAC地址是00-12-11-23-XX-XX的802.3的数据 报文。
7. 由于总公司出口带宽有限，需要在交换机 13 口对总公司产品部门访问因特网 http 服务做流量控制，访问 http 80 端口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。
8. 配置总公司的交换机策略，检测 other-ipuc 报文，控制报文上 CPU 的速率，每秒最多 30 个包；为减少内部 ARP 广播询问 VLAN 网关地址，在全局下配置 SW 每隔 300S 发送免费 ARP。
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 14 口开启以下安全机制：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；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往反数据流都要经过防火墙，再通过 BC 访问因特网；
12. 总公司今年进行 IPv6 试点，运营商给分配的 IPv6 地址段为 2001:da8:20:20::/60，由于分公司出口没有 IPv6 地址，现将总公司 IPv6 地址段分一半给分公司，实现分公司用户 IPv6 上网需求。要求分公司 AC 可从总公司 SW 处自动获取前缀信息，分公司业务 Vlan 实现自动化分配 IPv6 地址。
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，地址范围：2001:da8:20:20::2-2001:da8:20:20::fffe，排除网关地址。
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,同时为了防止恶意主机发送 RA 欺骗攻击，开启相关安全防护功能。
15. FW-AC、AC-SW、BC-SW 之间配置 OSPF area 0 开启基于链路的 MD5 认证，密钥自定义，SW 和 AC 分别学习到各自网络出口的默认路由，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 10.0.0.254，地址池范围 172.17.40.10-172.17.40.100，dns-server 114.114.114.114。
17. 为分析用户上网行为，需要对交换机连接 BC 的接口进行数据采样，发送到服务器进行分析，交换机采用回环接口 IP 发送数据，接收服务器地址为 172.16.60.100，采样速率为 10000，采样时间间隔为 20。

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 PING，SSH，HTTPS 功能。Loopback 接口除外；
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192.168.60.10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 SSL vpn 方式实现仅允许对分公司内网产品部门的访问，端口号使用 4455，用户名密码均为 SKILLS2024，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 telnet 映射到外网，让外网通过能通过防火墙外网口地址 telnet 到 AC 上，AC 地址为 loopback 地址。外网口地址及 AC 地址禁止采用地址簿形式；
22. 出于安全考虑分公司销售部门通过FW访问因特网时需要在FW上开启web认证，使用 http 方式，采用本地认证，密码账号都为 web2024，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，出口带宽总量为 400M。通过 QoS 配置，实现以下需求：在网络链路使用率达 85%时，将销售部门每个用户使用的最大带宽限制到 100k；当网络链路空闲时，不做限制。系统中 P2P 软件的流量不能超过 200M。 流量的智能化分配：当用户上网时，如果仅用 P2P 软件下载资源，系统将全部流量分配给 P2P 软件；此后，如果用户同时开始浏览网页，则优先保证网页浏览的应用需求，并且使 P2P 应用始终都在下载资源，只是 P2P 下载获得的流量会从早期的占有所有带宽变为只占用少量带宽。注意：安全策略名称设置为“p2p”。
24. 为净化上网环境，要求在防火墙 FW 上实现禁止无线用户周一至周五工作时间 9:00-18:00，对公司员工在网站 www.abc.com 发布包含“X”词汇信 息的行为进行记录。

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 002024,IKE 阶段 1 采用 DH 组 1、3DES 和 MD5 加密方式，IKE 阶段 2 采用 ESP-3DES，MD5 加密方式。
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，让总公司内网用户通过 ip：183.23.1.1/29 访问因特网。
27. 总公司产品部门要求在上班时间周一到周五 9:00 到 18:00 不可以访问外网，而财务部出于安全性的考虑在任何时间段均不允许访问外部网络。
28. 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。
29. 为了提高分公司出口带宽，尽可能加大分公司出口 FW 与 AC 之间带宽，同时设置负载均衡模式为源目 MAC-IP。
30. 在 BC 上开启 IPS 策略，对分公司内网用户访问外网的数据进行 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。开启 IPS 告警，告警条件中危，预警状态，启用日志记录。
31. 对分公司内网用户访问互联网做客户端安全检测，要求满足Windows Defender 不低于 4.18.2210.6 版本的终端可以正常上网，同时禁止隶属于 Administrators组的账户所登录的计算机上网，对于无法检测的终端全部禁止上网。
32. 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下载工具占用大量带宽需要限制内部员工使用下载工具的流量，最大上下行带宽都为50M，以免下载流量占用太多的出口网络带宽，开启P2P抑制技术，启用阻断记录。
33. 通过 BC 设置总公司用户在上班时间周一到周五 9:00 到 18:00 实现阻断内网用户使用流媒体软件或 web 在线看视频等,并启用阻断记录。
34. 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。

35. 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。邮箱服务器 smtp.cn.com，发送邮件地址为 bc@cn.com，接收邮件为 skills2024@cn.com。
36. 总公司内部有一台网站服务器直连到WAF,地址是192.168.218.10,端口是8080,配置将访问日志、DDoS 日志、安全情报日志，以 JSON 格式发送到 syslog 日志服务器，IP 地址是 192.168.60.10，UDP 的 2000 端口。
37. 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。
38. 在 WAF 上针对 HTTP 服务器进行 URL 参数最大个数为 20，Referer 最大长度为 512，Host 最大长度为 1024，Accept-Charset 最大长度为 128，设置严重级别为中级，超出校验数值阻断并发送邮件告警。规则名称“WAF_P1”
39. 对访问 url 为 www.123.com 的 http 访问进行限制，处理动作为拒绝，并记录日志。
40. 开启邮件告警功能，SMTP 地址为 smtp.cn.com，端口号：110，接收邮件地址为 skills2024@cn.com。邮件主题为：告警；攻击触发条件，全部开启。
41. 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。规则名称“WAF_P2”。
42. 在 WAF 上对 www.vcsc.org.cn 开启防跨站请求功能，请求方式为 GET，处理方式拒绝、并记录日志，规则名称“WAF_P3”。建立防护策略，应用所有新建规则。
43. 为了满足网监要求，需要对分公司内网用户访问因特网的流量进行记录，把访问因特网的流量发送到 AC 的 17 口。
44. 由于公司 IP 地址为统一规划，原有无线网段 IP 地址为 172.16.21.0/22,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 30 台；办公无线用户 Vlan 10 预计 300 人，来宾用户 Vlan20 预计不超过 50 人。

45. 总公司 SW 上配置 DHCP，管理 Vlan 为 Vlan100,为 AP 下发管理地址，网段中第十个可用地址为 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；AC 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。
46. 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:da8:20:21::9， SW 上中继地址为 AC loopback1 地址。
47. 在 NETWORK 下配置 SSID,需求如下:NETWORK 1 下设置 SSID SKILLS2024,Vlan10，加密模式为 wpa-personal，版本 2，其口令为 20242024。
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；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，并对接入 GUEST 的用户进行流控，上行 1M，下行 2M；配置所有无线接入用户相互隔离。
49. 配置 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. 为优化无线网络，现需对 AP 做相关调整。把 2.4G 信号工作信道调整到 6，信号发射功率调整到 80%，把 5.0G 信号工作信道调整到 161，信号发射功率调整 90%。

第二阶段任务书

本文件为上海市信息安全管理与评估项目竞赛-第二阶段试题，第二阶段内容包括：网络安全事件响应、数字取证调查和应用程序安全。

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。

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。

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。素材解压密码（********），所有答案提交至竞赛平台。

评分方案

本项目模块分数为 250 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。

工作任务

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。

序号	任务要求
1	请找出内存当中的可疑进程，将可疑进程名称作为 FLAG 进行提交。格式：flag{xxxx}
2	请找出可疑进程的父进程 ID 值作为 FLAG 进行提交。格式：flag{xxx}
3	请将创建此进程的初始恶意执行文件名称作为 FLAG 进行提交。格式：flag{xxx}
4	请将用于删除文件的恶意进程名称作为 FLAG 进行提交。格式：flag{xxx}
5	请将恶意文件首次执行的路径作为 FLAG 进行提交。格式：flag{xxx}
6	请将包含用于加密私钥的勒索软件公钥的文件的文件名作为 FLAG 进行提交。格式：flag{xxx}
7	请将攻击者用于提权操作的函数作为 FLAG 进行提交。格式：flag{xxx}

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。

序号	任务要求
1	数据包中中查找受害者的主机名，将主机名作为 flag 提交；
2	在数据包中中查找受害者的 Windows 用户帐户名。将其作为 flag 提交；
3	找到恶意软件 将恶意软件的文件名作为 flag 提交；
4	分析该恶意软件，将恶意软件感染的协议作为 flag 提交；
5	继续分析该恶意软件，将恶意软件扩散至域控服务器后的文件名作为 flag 提交；

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。

序号	任务要求
1	找到以上代码存在问题，在此基础上封装安全的函数：将 F1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	将F2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	将F3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	将F4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	将F5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）；

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。

序号	任务要求
1	找到逆向用户名密码相关的第一个 flag （形式：abcdbbcc-abcdbbcc-abcdbbcc-abcdbbcc）

2	找到逆向SO中加密函数的密钥 ，将密钥作为flag提交
3	找到逆向SO相关的第二个flag （形式：abcdbbcc-abcdbbcc-abcdbbcc-abcdbbcc）

第三阶段任务书

本文件为上海市信息安全管理与评估项目竞赛-第三阶段试题。根据信息安全管理与评估项目技术文件要求，第三阶段为夺旗挑战 CTF（网络安全渗透）。

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。

介绍

夺旗挑战赛（CTF）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。

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。所有答案提交至竞赛平台。

评分方案

本项目阶段分数为 300 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，请利用你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。

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：

- 信息收集
- 逆向文件分析

- 二进制漏洞利用
- 应用服务漏洞利用
- 杂项与密码学分析

所有设备和服务器的 IP 地址请查看竞赛平台提供的设备列表。

工作任务

任务 1 ：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. 将服务器开放端口从大到小排序作为 flag 值提交。形式：flag{xx/x}
2. 通过漏洞获取服务器用户 daniel 的密码作为 flag 值提交 形式：flag{daniel:pass}
3. 服务器中存在定时任务将每次任务间隔的时间作为 flag 提交。形式：flag{900s}
4. 通过服务器中的提权到 root 所需的工具的绝对路径作为 flag 提交。 形式：flag{}
5. 找到 root 用户下所留下的 flag 值并提交。 形式：flag{}

任务 2：协议服务器

任务环境说明：

靶机：

服务器场景 1：linux（协议服务器）

1. 寻找页面中的隐藏信息将解密后的信息作为提交
2. 寻找页面的隐藏 Flag 将 flag 里的内容提交
3. 寻找解开关键的协议端口， 将端口号作为 flag 提交
4. 寻找隐藏的文件，将被隐藏的文件名作为 flag 提交
5. 获取/root/flag.txt 的信息，将文本里的内容作为 flag 提交

任务 3 ：FTP 服务器

任务环境说明：

靶机：

服务器场景 1：linux（FTP 服务器）

ftp 账号：ftpuser ftp 密码：ftpuser

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。形式：flag{XXXXXX}
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。形式：flag{XXXXXX}
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。形式：flag{XXXXXX}
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。形式：flag{XXXXXX}
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。形式：flag{XXXXXX}

任务 4 ：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 java 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.class 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.class，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.class，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.class，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）;