**2026年河北省职业院校技能大赛**

**（高职组）**

**“信息安全管理与评估”项目**

**任务书**

# 赛项时间

共计4小时。

# 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 | 240分钟 | 250 |
| 任务2 | 网络安全设备配置与防护 |
| 第二阶段  网络安全事件响应、数字取证调查、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  网络安全渗透、理论技能与职业素养 | 任务1 | Web服务器 | 200 |
| 任务2 | 协议服务器 |
| 任务3 | FTP服务器 |
| 任务4 | 加密服务器 |
| 任务5 | 理论技能与职业素养 | 100 |

# 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。

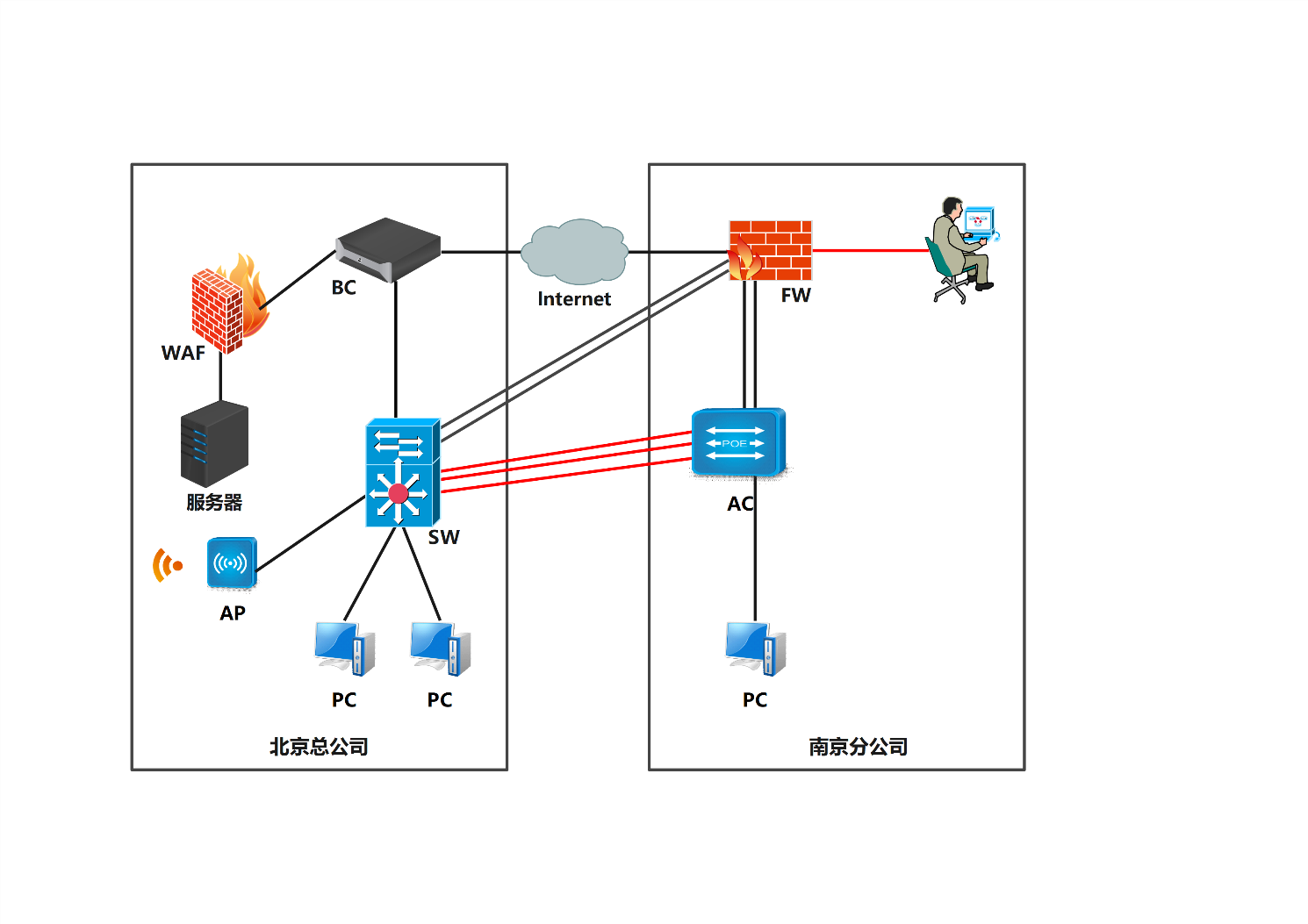
例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

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。

1. 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。

### 网络拓扑图



### 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  Eth1/0/1-2 | 10.0.0.2/30 | FW | Eth1/0/1-2 |
| 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-Vlan10 |
| Vlan 20  无线2 | Ipv4:需设定  Ipv6:接口ID：0:0:0:f::1/64 |  | Vlan name  WIFI-Vlan20 |
| Vlan 31  Eth 1/0/9-10 | 192.168.3.129/25 |  | Vlan name  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 |

### 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。 | | | |

1. **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](http://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%。

# 第二阶段竞赛项目试题

本文件为河北省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） |

# 第三阶段竞赛项目试题

本文件为河北省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

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{}
6. **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
6. **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}
6. **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）；
6. **理论技能与职业素养**

请根据赛题环境及任务要求提交正确答案。