

**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**

**赛题五**

**模块一**

网络平台搭建与设备安全防护

# 赛项时间

共计180分钟。

# 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 |

# 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。

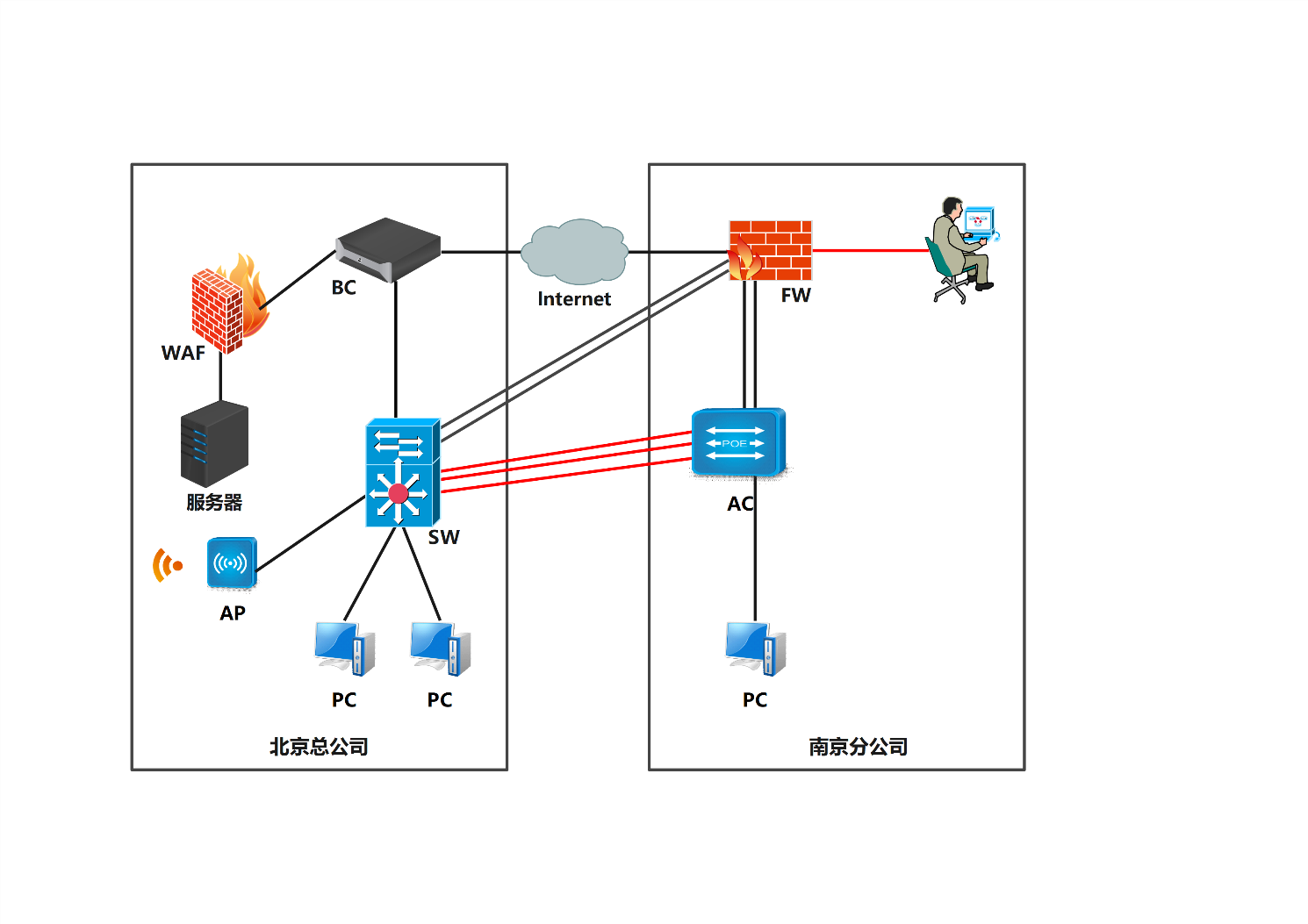
例如：08工位，则需要在U盘根目录下建立“GW08”文件夹，并在“GW08”文件夹下直接放置第一个阶段的所有“XXX-答题模板”文件。

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。

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。

### 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** |
| --- | --- | --- | --- | --- |
| 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 |  |  |

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。

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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。
8. 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。
9. 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。
10. 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。
11. 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。
12. 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。
13. 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。
14. 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。
15. 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。
16. 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。
17. 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。
18. 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。
19. 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。
20. 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。
21. 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。
22. 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。
23. 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。
24. 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；
25. 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](mailto:邮件地址为123@163.com，接收邮件为133139123456@163.com)。
26. 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;
27. 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。
28. 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。
29. 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。
30. 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。
31. 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。
32. 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。
33. 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。
34. 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。
35. 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。
36. 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。
37. 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。

1. 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。
2. 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。
3. 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。
4. 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

### 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 server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

### 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

### 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 |  |
| 2 | 请提交恶意应用保存数据文件名称（含路径） |  |
| 3 | 请提交恶意应用解密数据的密钥 |  |
| 4 | 请描述恶意应用的行为 |  |

### 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

## 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>} |  |  |

## 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>} |  |  |

## 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>} |  |  |

## 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>} |  |  |

## 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

## 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、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1、《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议通过，自（ ）起施行。

A、 2019年6月1日

B、 2018年6月1日

C、 2017年6月1日

D、 2016年6月1日

2、传播计算机病毒属于以下（ ）问题行为。

A、信息道德与信息安全失范行为

B、侵害他人财产

C、危害国家安全

D、传播有害文件

3、一个基于网络的IDS应用程序利用什么来检测攻击？（ ）

A、 正确配置的DNS

B、 特征库

C、 攻击描述

D、 信息包嗅探器

4、你检测到一次针对你的网络的攻击，你的服务器日志显示了攻击的源IP地址，但是你需要确定这个地址来自哪个域，你应该？（ ）

A、 Ping根服务器

B、 进行反向DNS查找

C、 检查你的DNS服务器的A记录

D、 请你的互联网服务供应商为你寻找需要的信息

5、扫描器之王NMAP中，全面扫描的命令是什么？（ ）

A、 -o

B、 -SV

C、 -sP

D、 -a

6、根据网络安全应急处理流程，应急启动后，应该进行哪一步（ ） 。

A、 归类&定级

B、 应急处置

C、 信息通报

D、 后期处理

7、能修改系统引导扇区，在计算机系统启动时首先取得控制权的病毒属于（ ） 。

A、 文件病毒

B、 引导型病毒

C、 混合型病毒

D、 恶意代码

8、你有一个共享文件夹，你将它的NTFS权限设置为sam用户可以修改，共享权限设置为sam用户可以读取，当sam从网络访问这个共享文件夹的时候，他有什么样的权限？（ ）

A、 读取

B、 写入

C、 修改

D、 完全控制

9、通过设置网络接口（网卡）的（），可以使其接受目的地址并不指向自己的网络数据包，从而达到网络嗅探攻击的目的？（ ）

A、 共享模式

B、 交换模式

C、 混杂模式

D、 随机模式

10、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

11、下列有关数据库系统及相关内容的说法中，错误的是（ ） 。

A、 数据库系统是由计算机软硬件组成的复杂系统，其体系结构与系统硬件平台密切相关

B、 数据库管理系统提供了查询、插入、删除、更新等通用数据操作，但没有提供各种面向具体应用领域的业务处理

C、 数据库中的数据是按照一定的数据模型组织和存储的、可供多个用户共享的、具有最小冗余度的相关数据集合

D、 数据字典记录数据库系统运行时数据库操作情况的日志信息，通常由数据库管理员管理和维护

12、下列对计算机网络的攻击方式中，属于被动攻击的是？（ ）

A、 口令嗅探

B、 重放

C、 拒绝服务

D、 物理破坏

13、关于分布式数据库，下列说法正确的是（ ） 。

A、 分布式数据库的事务管理包括恢复控制和并发控制，恢复控制一般采用的策略是基于两阶段提交协议

B、 在分布式数据库查询中，导致数据传输通信代价大的主要原因是各个站点分片的连接和并操作

C、 分布式数据库中的分布透明性包括分片透明性、位置透明性、局部数据模型透明性，其中分片透明性是最高层次的透明性

D、 分布式数据库的目标是本地自治、非集中式管理、高可用性、位置独立性、数据分片独立性等

14、MD5算法以（ ）位分组来处理输入文本。

A、 64

B、 128

C、 256

D、 512

15、关于函数，下面哪个说法是错误的？（ ）

A、 函数必须有参数

B、 函数可以有多个函数

C、 函数可以调用本身

D、 函数内可以定义其他函数

16、根据我国网络安全应急响应的法律法规，网络安全事件可以分为7类，下列哪项不属于有害程序事件。（ ）

A、 蠕虫事件

B、 特洛伊事件

C、 信息泄露事件

D、 混合程序攻击事件

17、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

18、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

19、ICMP泛洪利用了？（ ）

A、 ARP命令的功能

B、 traceroute命令的功能

C、 ping命令的功能

D、 route命令的功能

20、根据工信部明确的公共互联网网络安全突发事件应急预案文件，公共互联网网络突发事件等级最高可标示的颜色是什么？（ ）

A、 红色

B、 黄色

C、 蓝色

D、 橙色

21、黑客利用IP地址进行攻击的方法有？（ ）

A、 IP欺骗

B、 解密

C、 窃取口令

D、 发送病毒

22、在强制存取控制机制中，当主体的许可证级别等于客体的密级时，主体可以对客体进行如下操作（）。（ ）

A、 读取

B、 写入

C、 不可操作

D、 读取、写入

23、ARP欺骗的实质是？（ ）

A、 提供虚拟的MAC与IP地址的组合

B、 让其他计算机知道自己的存在

C、 窃取用户在网络中的传输的数据

D、 扰乱网络的正常运行

24、函数的\_\_doc\_\_属性表示？（ ）

A、 函数的名称

B、 函数中的说明

C、 函数中定义的变量

D、 函数的返回值

25、下列不属于口令安全威胁的是？（ ）

A、 弱口令

B、 明文传输

C、 MD5加密

D、 多账户共用一个密码

26、维吉利亚(Vigenere)密码是古典密码体制比较有代表性的一种密码，其密码体制采用的是（ ） 。

A、 置换密码

B、 单表代换密码

C、 多表代换密码

D、 序列密码

27、DES的秘钥长度是多少Bit?（ ）

A、 6

B、 56

C、 128

D、 32

28、MD5散列算法具有（ ） 位摘要值。

A、 56

B、 128

C、 160

D、 168

29、VIM模式切换的说法中，正确的是？（ ）

A、 命令模式通过i命令进入输入模式

B、 输入模式通过:切换到末行模式

C、 命令模式通过ESC键进入末行模式

D、 末行模式通过i进入输入模式

30、Shell编程条件判断中，说法错误的是？（ ）

A、 -b 判断文件是否存在，并且是否为块设备文件

B、 -c 判断文件是否存在，并且是否为字符设备文件

C、 -d 判断文件是否存在，并且是否为目录文件

D、 -e 判断文件是否存在，并且是否为普通文件

31、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

32、关于sed操作命令中，说法错误的是？（ ）

A、 a 命令在行的前面另起一行新增

B、 p 命令打印相关行，配合-n使用

C、 c 命令替换行

D、 d 命令删除行

33、部署大中型IPSEC VPN 时，从安全性和维护成本考虑，建议采取什么样的技术手段提供设备间的身份验证?（ ）

A、 预共享密钥

B、 数字证书

C、 路由协议验证

D、 802.1x

34、Jennings 发生器用了一个复合器来组合（ ）个LFSR。

A、 1

B、 2

C、 3

D、 4

35、vim命令中，用于查找并替换的命令，正确的是？（ ）

A、 xw

B、 1,$s/test/360/g

C、 cw

D、 p

###### **二、 多选题 （共每题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、SQL Server提供了DES、RC2、RC4和AES等加密算法，没有某种算法能适应所有要求，每种算法都有优劣势，但选择算法需要有如下共通之处（ ） 。

A、 强加密通常会比较弱的加密占用更多的CPU资源

B、 长密钥通常会比短密钥生成更强的加密

C、 如果加密大量数据，应使用对称密钥来加密数据，并使用非对称密钥来加密该对称密钥

D、 可以先对数据进行加密，然后再对其进行压缩

3、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

4、下面哪些选项是类的属性？（ ）

A、 \_\_doc\_\_

B、 \_\_init\_\_

C、 \_\_module\_\_

D、 \_\_class\_\_

5、下面那些方法可以检测恶意ICMP流量？（ ）

A、 检测同一来源ICMP数据包的数量

B、 注意那些ICMP数据包中payload大于64比特的数据包

C、 寻找那些响应数据包中payload跟请求数据包不一致的ICMP数据包

D、 检查ICMP数据包的协议标签

6、使用os.walk函数可以得到哪些内容？（ ）

A、 目录的路径

B、 子目录的列表

C、 非目录的文件列表

D、 目录中文件的大小

7、VPN设计中常用于提供用户识别功能的是（ ） 。

A、 RADIUS

B、 TOKEN卡

C、 数字证书

D、 8O2.1xAA.OOcIn.com

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、在反杀伤链中，情报可以分为那几个层次？（ ）

A、 战斗

B、 战略

C、 战区

D、 战术

10、以下后缀中，属于Linux中常见压缩文件后缀的有？（ ）

A、 doc

B、 zip

C、 tar.gz

D、 ppt