

**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**

**赛题十**

**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。

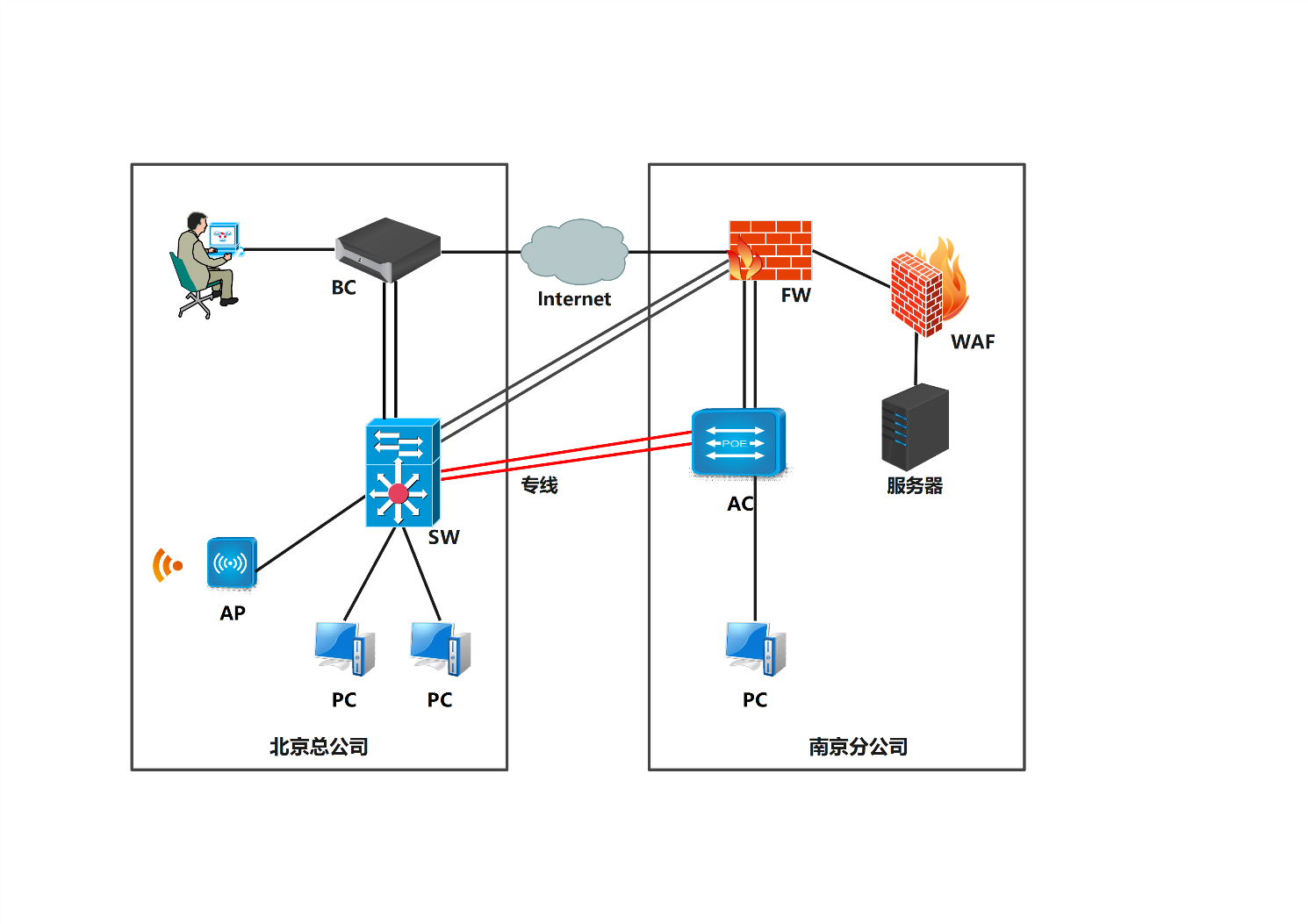
选手首先需要在U盘的根目录下建立一个名为“GWxx”的文件夹（xx用具体的工位号替代），赛题第一阶段所完成的“XXX-答题模板”放置在文件夹中。

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

### 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 |
| 202.22.1.1/29（untrust） | SW |
| ETH0/3 | 20.10.28.1/24(DMZ) | WAF |  |
| Eth0/4-5 | 20.1.0.14/30 | AC | Eth1/0/21-22 |
| Loopback1 | 20.0.0.254/32（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 | 财务专线 | AC ETH1/0/4 |  |
| ETH1/0/5 | 办公专线 | AC ETH1/0/5 |  |
| VLAN21  ETH1/0/1-2 | 20.1.0.2/30 | FW | Vlan name  TO-FW1 |
| VLAN22  ETH1/0/1-2 | 20.1.1.2/30 | FW | Vlan name  TO-FW2 |
| VLAN 23  ETH1/0/1-2 | 202.22.1.2/29 | FW | Vlan name  TO-internet |
| VLAN 24  ETH1/0/24 | 203.23.1.1/29 | BC | Vlan name  TO-BC |
| Vlan 25  Eth 1/0/18-19 | 20.1.0.17/30 | BC | Vlan name  TO-BC-N |
| VLAN 10 | 需设定 | 无线1 | Vlan name  WIFI-vlan10 |
| VLAN 20 | 需设定 | 无线2 | Vlan name  WIFI-vlan20 |
| VLAN 30  ETH1/0/4 | 20.1.0.5/30 | AC  1/0/4 | Vlan name  T0-SW |
| VLAN 31  Eth1/0/10-12 | 20.1.3.1/25 |  | Vlan name  SW |
| VLAN 40  ETH1/0/5 | 20.1.0.9/30 | AC  1/0/5 | Vlan name  TO-IPV6 |
| VLAN 41  ETH1/0/6-9 | 20.1.41.1/24 | PC3 | Vlan name  BG |
| Vlan 50  Eth1/0/13-14 | 20.1.50.1/24  IPV6 2001:DA8:50::1/64 |  | Vlan name  Sales |
| 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  1/0/4 | Vlan name  TO-SW |
| VLAN 31 | 20.1.3.129/25 |  | Vlan name  SW |
| VLAN 40  ETH1/0/5 | 20.1.0.10/30 | SW  1/0/5 | Vlan name  TO-IPV6 |
| Vlan 60  Eth1/0/13-14 | 20.1.60.1/24  IPV6 2001:DA8:60::1/64 |  | Vlan name  sales |
| Vlan 61  Eth1/0/15-18 | 20.1.61.1/24 |  | Vlan name  BG |
| Vlan 100  Eth1/0/21-22 | 20.1.0.13/30 | FW  Eth1/0/4-5 | Vlan name  TO-FW |
| Loopback1 | 20.1.1.254/32(router-id) |  |  |
| 日志服务器BC | LAN2-3 | 20.1.0.18/30 | SW |  |
| WAN2 | 203.23.1.2/29 | SW |  |
| PPTP-pool | 192.168.10.129/26（10个地址） |  |  |
| WEB应用防火墙WAF | ETH2 | 20.10.28.2/24 | SERVER |  |
| ETH3 | FW |  |
| AP | Eth1 |  | SW（20口） |  |
| PC1 | 网卡 | eth1/0/7 | SW |  |
| SERVER | 网卡 | 20.10.28.10/24 |  |  |

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。设备名称根据网络拓扑图所示配置；（8分） |
| 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。设备名称根据网络拓扑图所示配置；（16分） |
| 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。设备名称根据网络拓扑图所示配置；（10） |
| 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。设备名称根据网络拓扑图所示配置；（8分） |
| 5 | 根据网络拓扑图所示，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。设备名称根据网络拓扑图所示配置；（8） |

### 任务2：网络安全设备配置与防护（250分）

1. SW和AC开启telnet登录功能，telnet登录账户仅包含“ABC4321”，密码为明文“ABC4321”，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” 。
2. 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。一条裸光纤承载公司财务部门业务，一条裸光纤承载其他内部业务。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SW 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。
3. 尽可能加大总公司核心和出口BC之间的带宽。
4. 为防止终端产生MAC地址泛洪攻击，请配置端口安全，已划分VLAN41的端口最多学习到5个MAC 地址，发生违规阻止后续违规流量通过，不影响已有流量并产生LOG 日志；连接PC1 的接口为专用接口，限定只允许PC1的MAC 地址可以连接。
5. 总公司核心交换机端口ethernet1/0/6上，将属于网段20.1.41.0内的报文带宽限制为10M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。
6. 在SW上配置将8端口收到的源IP为20.1.41.111的帧重定向到9端口，即从8端口收到的源IP为20.1.41.111的帧通过9端口转发出去。
7. 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。
8. 对SW上VLAN50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欺骗攻击。
9. 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，要求总公司核心交换机9口VLAN41业务的用户访问因特网的流量往反数据流经过防火墙在通过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。
10. 为了防止DOS攻击的发生，在总部交换机vlan50接口下对MAC、ARP、ND表项数量进行限制，具体要求为：最大可以学习20个动态MAC地址、20个动态ARP地址、50个NEIGHBOR表项。
11. 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；AC与SW之间配置静态路由 使VLAN50与VLAN60可以通过IPv6通信；IPv6业务地址规划如下，其它IPv6地址自行规划。

|  |  |
| --- | --- |
| **业务** | **IPV6地址** |
| 总公司VLAN50 | 2001::DA8:50：:1/64 |
| 分公司VLAN60 | 2001::DA8:60：:1/64 |

1. 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:da8:50::2-2001:da8:50::100。
2. 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。
3. SW与AC，AC与FW之间配置OSPF area 0 开启基于链路的MD5认证，密钥自定义，传播访问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；分公司SW和BC之间运行静态路由协议。
4. 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20.1.60.10-20.1.60.100，dns-server 8.8.8.8。
5. 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。
6. 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。
7. 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，复用公网IP： 202.22.1.3、202.22.1.4；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。
8. 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方式实现仅允许对内网VLAN 61的访问，端口号使用4455，用户名密码均为ABC4321，地址池参见地址表。
9. 分公司部署了一台WEB服务器ip为20.10.28.10，接在防火墙的DMZ区域为外网用户提供web服务，要求内网用户能,ping通web服务器和访问服务器上的web服务（端口80）和远程管理服务器（端口3389），外网用户只能访问通过防火墙外网地址访问服务器web服务。
10. 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，采用本地认证，密码账号都为web4321。
11. 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。
12. 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。
13. 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 ABC4321，IKE 阶段 1 采用 DH 组 1、DES 和 MD5 加密方，IKE 阶段 2 采用 ESP-DES，MD5。
14. 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BC外网口ip访问因特网。
15. 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test，密码test23。
16. 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。
17. 在BC上开启上网审计策略，对总公司内网用户启用web全部记录、记录即时通讯的登录信息、记录邮件的全部记录，要求全部审计，记录所有网页访问。
18. 为了防止总公司内网用户私接小路由上网，需要在BC上做相关配置，内网私接小路由进行惩罚，强制下线。
19. 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。
20. 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禁止玩游戏,并启用阻断记录。
21. 限制总公司内网用户访问因特网web视频和即时通信最大带宽为20M，上传为10M，启用阻断记录。
22. 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)。
23. 分公司内部有一台网站服务器直连到WAF，地址是20.10.28.10，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20.10.28.6，UDP的514端口;
24. 在分公司的WAF上配置，阻止常见的WEB攻击数据包访问到公司内网服务器，防止某源IP地址在短时间内发送大量的恶意请求，影响公司网站正常服务，大量请求的确认值是：10秒钟超过1000次请求。
25. 编辑防护策略，定义HTTP请求体的最大长度为256，防止缓冲区溢出攻击。
26. WAF上配置开启爬虫防护功能，当爬虫标识为Spider360，自动阻止该行为；WAF上配置阻止用户上传ZIP、DOC、JPG、RAR格式文件;WAF上配置编辑防护策略，要求客户机访问内部网站时，禁止访问\*.bat的文件;
27. WAF上配置，使用WAF的漏洞立即扫描功能检测服务器（20.10.28.10）的安全漏洞情况，要求包括信息泄露、SQL注入、跨站脚本编制。
28. WAF上配置开启防护策略，将请求报头DATA 自动重写为DATE。
29. WAF上配置开启错误代码屏蔽功能，屏蔽404错误代码。
30. 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 50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。
31. AC 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。
32. 在NETWORK下配置SSID，需求如下：NETWORK 1下设置SSID ABC4321，VLAN10，加密模式为wpa-peSWonal,其口令为43214321。
33. NETWORK 2下设置SSID GUEST，VLAN20不进行认证加密,做相应配置隐藏该SSID。
34. NETWORK 2开启内置portal+本地认证的认证方式，账号为test密码为test4321。
35. 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。
36. 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。
37. 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。
38. SW、AC运行静态组播路由和因特网组管理协议第二版本；总公司办公段和分公司办公段启用组播协议，总公司采用三层组播，使用密集模式，分公司采用二层组播。
39. PC1启用组播，使用VLC工具串流播放视频文件1.mpg，组地址228.10.10.10，端口：1234，实现PC2可以通过组播查看视频播放。



**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 | 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

### 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 | 人力资源管理系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务二 | 人力资源管理系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务三 | 人力资源管理系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

## 邮件系统（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务四 | 邮件系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |
| 任务五 | 邮件系统存在漏洞，请利用漏洞并找到flag，并将flag提交。flag格式flag{<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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，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服务器上对应的文件进行分析，找出其中隐藏的flag，并将flag提交。flag格式flag{<flag值>} |  |  |

## 应用系统服务器（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务十四 | 应用系统服务器10000端口存在漏洞，获取FTP服务器上对应的文件进行分析，请利用漏洞找到flag，并将flag提交。flag格式flag{<flag值>} |  |  |

## 测试系统服务器（30分）

|  |  |  |  |
| --- | --- | --- | --- |
| **任务编号** | **任务描述** | **答案** | **分值** |
| 任务十五 | 应用系统服务器10001端口存在漏洞，获取FTP服务器上对应的文件进行分析，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

2、Open函数中w 参数的作用是？（ ）

A、 读文件内容

B、 写文件内容

C、 删除文件内容

D、 复制文件内容

3、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

4、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

5、通过TCP序号猜测，攻击者可以实施下列哪一种攻击？（ ）

A、 端口扫描攻击

B、 ARP欺骗攻击

C、 网络监听攻击

D、 TCP会话劫持攻击

6、下面不是数据库的基本安全机制的是（ ） 。

A、 用户认证

B、 用户授权

C、 审计功能

D、 电磁屏蔽

7、假设创建了名为f的实例，如何在f中调用类的add\_food函数？（ ）

A、 f(add\_food())

B、 f.[add\_food()]

C、 f.add\_food

D、 f.add\_food()

8、aspx 的网站配置文件一般存放在哪个文件里？（ ）

A、 conn.asp

B、 config.php

C、 web.config

D、 index.aspx

9、一个基于特征的IDS应用程序需要下列选项中的哪一项来对一个攻击做出反应？（ ）

A、 正确配置的DNS

B、 正确配置的规则

C、 特征库

D、 日志

10、完成数据库应用系统的设计并进行实施后，数据库系统进入运行维护阶段。下列工作中不属于数据库运行维护工作的是（ ） 。

A、 恢复数据库数据以核查问题

B、 为了保证安全，定期修改数据库用户的密码

C、 更换数据库服务器以提高应用系统运行速度

D、 使用开发人员提供的SQL语句易始化数据库中的表

11、以下不属入侵检测中要收集的信息的是（ ） 。

A、 系统和网络日志文件

B、 目录和文件的内容

C、 程序执行中不期望的行为

D、 物理形式的入侵信息

12、POP3服务器使用的监听端口是？（ ）

A、 TCP的25端口

B、 TCP的110端口

C、 UDP的25端口

D、 UDP的110端口

13、目标计算机与网关通信失败，更会导致通信重定向的攻击形式是？（ ）

A、 病毒

B、 木马

C、 DOS

D、 ARP欺骗

14、\_\_\_\_\_\_\_\_的目的是发现目标系统中存在的安全隐患，分析所使用的安全机制是否能够保证系统的机密性、完整性和可用性。（ ）

A、 漏洞分析

B、 入侵检测

C、 安全评估

D、 端口扫描

15、以下哪一项描述不正确？（ ）

A、 ARP是地址解析协议

B、 TCP/IP传输层协议有TCP和UDP

C、 UDP协议提供的是可靠传输

D、 IP协议位于TCP/IP网际层

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、MD5的主循环有（ ） 轮。

A、 3

B、 4

C、 5

D、 8

18、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

19、( )是一种架构在公用通信基础设施上的专用数据通信网络，利用 IPSec 等网络层安全协议和建立在 PKI 上的加密与签名技术来获得私有性。（ ）

A、 SET

B、 DDN

C、 VPN

D、 PKIX

20、假设系统中有n个用户，他们使用对称加密体制实现保密通信，那么系统中共需要管理（ n(n-1)/2）个密钥，每个用户需要保存（ ） 个密钥。

A、 n-1

B、 2n

C、 Cn2

D、 n！

21、什么是数据库安全的第一道保障（）。（ ）

A、 操作系统的安全

B、 数据库管理系统层次

C、 网络系统的安全

D、 数据库管理员

22、下列方法中不能用来进行DNS欺骗的是？（ ）

A、 缓存感染

B、 DNS信息劫持

C、 DNS重定向

D、 路由重定向

23、下列选项哪列不属于网络安全机制？（ ）

A、 加密机制

B、 数据签名机制

C、 解密机制

D、 认证机制

24、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

25、现今非常流行的SQL（数据库语言）注入攻击属于下列哪一项漏洞的利用？（ ）

A、 域名服务的欺骗漏洞

B、 邮件服务器的编程漏洞

C、 WWW服务的编程漏洞

D、 FTP服务的编程漏洞

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、如果VPN网络需要运行动态路由协议并提供私网数据加密,通常采用什么技术手段实现（ ） 。

A、 GRE

B、 GRE+IPSEC

C、 L2TP

D、 L2TP+IPSEC

28、过滤所依据的信息来源不包括？（ ）

A、 IP包头

B、 TCP包头

C、 UDP包头

D、 IGMP包头

29、bind9的日志默认保存在？（ ）

A、 /var/log/named.log

B、 /var/log/named/named.log

C、 /var/named/data/named.run

D、 /var/log/data/named.run

30、一个完整的密码体制，不包括以下（ ）要素。

A、 明文空间

B、 密文空间

C、 数字签名

D、 密钥空间

31、Linux系统中，添加用户的命令是？（ ）

A、 net user test /add

B、 user add test

C、 useradd test

D、 test useradd

32、以下关于正则表达式，说法错误的是？（ ）

A、 ‘root’表示匹配包含root字符串的内容

B、 ‘.’表示匹配任意字符

C、 [0-9]表示匹配数字

D、 ‘^root’表示取反

33、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

34、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

35、在常见的安全扫描工具中，以下（ ） 主要用来分析Web站点的漏洞，可以针对数千种常见的网页漏洞或安全风险进行检测。

A、 SuperScan

B、 Fluxay（流光）

C、 Wikto

D、 MBSA

**二、 多选题 （每题3分，共10题，共30分）**

1、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

2、以下关于TCP和UDP协议的说法错误的是？（ ）

A、 没有区别，两者都是在网络上传输数据

B、 TCP是一个定向的可靠的传输层协议，而UDP是一个不可靠的传输层协议

C、 UDP是一个局域网协议，不能用于Interner传输，TCP则相反

D、 TCP协议占用带宽较UDP协议多

3、关于函数中变量的定义，哪些说法是正确的？（ ）

A、 即使函数外已经定义了这个变量，函数内部仍然可以定义

B、 如果一个函数已经定义了name变量，那么其他的函数就不能再定义

C、 函数可以直接引用函数外部定义过的变量

D、 函数内部只能定义一个变量

4、下面标准可用于评估数据库的安全级别的有（ ）

A、 TCSEC

B、 IFTSEC

C、 CC DBMS.PP

D、 GB17859-1999E.TD

5、安全的网络通信必须考虑以下哪些方面？（ ）

A、 加密算法

B、 用于加密算法的秘密信息

C、 秘密信息的分布和共享

D、 使用加密算法和秘密信息以获得安全服务所需的协议

6、RC4加密算法被广.泛应用，包括（ ）

A、 SSL/TLS

B、 WEP协议

C、 WPA协议

D、 数字签名

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、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

9、我国现行的信息安全法律体系框架分为（ ）三个层面。

A、信息安全相关的国家法律

B、信息安全相关的行政法规和部分规章

C、信息安全相关的地方法规/规章和行业规定

D、信息安全相关的个人职业素养

10、信息道德与信息安全问题一直存在的原因有（ ）。

A、信息系统防护水平不高

B、信息安全意识不强

C、信息安全法律法规不完善

D、网络行为道德规范尚未形成