附件 1:

2024 年四川省职业院校技能大赛

高等职业教育组

信息安全管理与评估

任务书

(样题)

模块一：网络平台搭建与设备安全防护

一、 比赛时间

本阶段比赛时长为 180 分钟。

二、 赛项信息

竞赛阶段	任务阶段	竞赛任务	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	400
	任务 2	网络安全设备配置与防护	

三、 赛项内容

本次大赛，各位选手需要完成三个阶段的任务，每个阶段需要按裁判组专门提供的 U 盘中的“信息安全管理与评估竞赛答题卡-模块 X”提交答案。

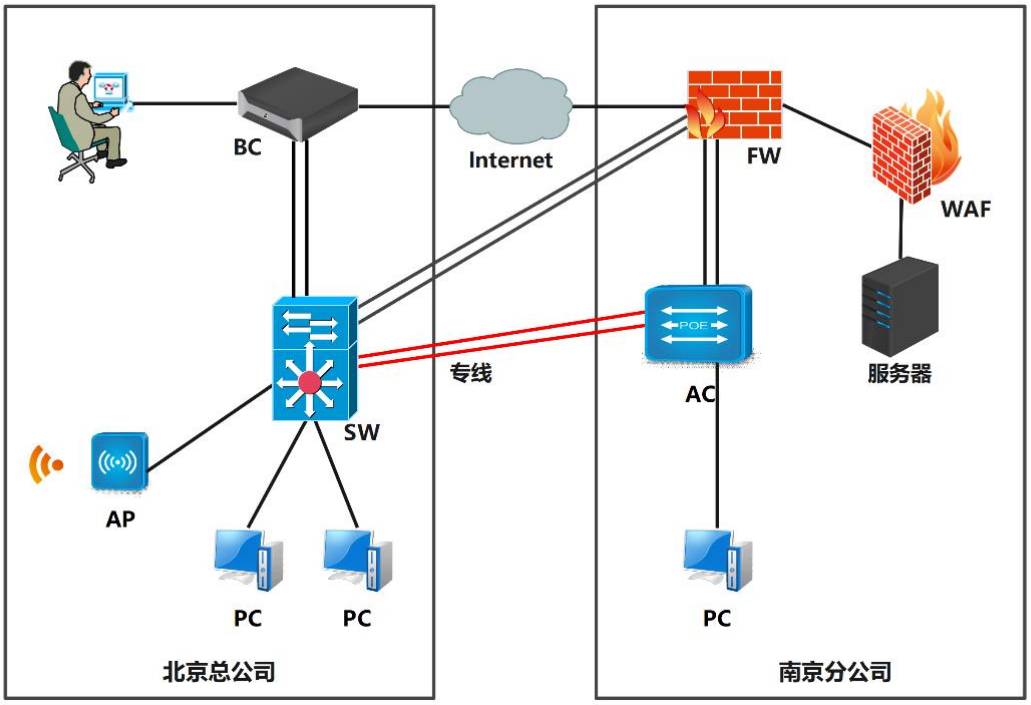
选手首先需要在 U 盘的根目录下建立一个名为“GWxx”的文件夹(xx 用具体的工位号替代)，请将赛题第一阶段所完成的“信息安全管理与评估竞赛答题卡-模块一”答题文档，放置在“GWxx”文件夹中。

例如：08 工位，则需要在 U 盘根目录下建立“GW08”文件夹，请将第一阶段所完成的“信息安全管理与评估竞赛答题卡-模块一”答题文档，放置在“GW08”文件夹中。

【注意事项】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

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	
		202.22.1.1/29(untrust)	SW	
	ETH0/3	20.10.28.1/24(DMZ)	WAF	
	ETH0/4-5	20.1.0.14/30(trust)	AC	ETH1/0/21-22
	Loopback1	20.0.0.254/32(trust) Router-id		
	SSLPool	192.168.10.1/26 可用 IP 数量为 20	SSLVPN 地址池	
三层交换机 SW	ETH1/0/4	财务专线	ACETH1/0/4	
	ETH1/0/5	办公专线	ACETH1/0/5	
	VLAN21 ETH1/0/1-2	20.1.0.2/30	FW	Vlanname TO-FW1
	VLAN22 ETH1/0/1-2	20.1.1.2/30	FW	Vlanname TO-FW2
	VLAN23	202.22.1.2/29	FW	Vlanname

设备名称	接口	IP 地址	对端设备	接口
	ETH1/0/1-2			TO-internet
	VLAN24 ETH1/0/23-24	203.23.1.1/29	BC	Vlanname TO-BC
	VLAN25 ETH1/0/18-19	20.1.0.17/30	BC	Vlanname TO-BC-N
	VLAN10	需设定	无线 1	Vlanname WIFI-vlan10
	VLAN20	需设定	无线 2	Vlanname WIFI-vlan20
	VLAN30 ETH1/0/4	20.1.0.5/30	AC 1/0/4	Vlanname T0-CW
	VLAN31 ETH1/0/10-12 10 口开启 loopback	20.1.3.1/25		Vlanname CW
	VLAN40 ETH1/0/5	20.1.0.9/30	AC 1/0/5	Vlanname TO-IPV6
	VLAN41 ETH1/0/6-9	20.1.41.1/24	PC3	Vlanname BG
	VLAN50 ETH1/0/13-14 13 口开启 loopback	20.1.50.1/24 IPV62001:DA8:50::1/64		Vlanname Sales
	VLAN100 ETH1/0/20	需设定		Vlanname AP-Manage
	Loopback1	20.0.0.253/32(router-id)		
无线 控制器 AC	VLAN30 ETH1/0/4	20.1.0.6/30	SW 1/0/4	Vlanname TO-CW
	VLAN31 ETH1/0/6-9 6 口开启 loopback	20.1.3.129/25		Vlanname CW
	VLAN40 ETH1/0/5	20.1.0.10/30	SW 1/0/5	Vlanname TO-IPV6
	VLAN60 ETH1/0/13-14 13 口开启 loopback	20.1.60.1/24 IPV62001:DA8:60::1/64		Vlanname sales
	VLAN61 ETH1/0/15-18 15 口开启 loopback	20.1.61.1/24		Vlanname BG

设备名称	接口	IP 地址	对端设备	接口
	VLAN100 ETH1/0/21-22	20.1.0.13/30	FW ETH1/0/4-5	Vlanname TO-FW
	Loopback1	20.1.1.254/32(router-id)		
日志 服务器 BC	ETH1-2	20.1.0.18/30	SW	
	ETH3	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		

(二) 第一阶段任务书

1.任务 1：网络平台搭建

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。
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。
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。
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。
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。

2.任务 2：网络安全设备配置与防护

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 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。

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 ETH1/0/6 上，将属于网段 20.1.41.0 内的报文带宽限制为 10Mbps，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 上配置办公用户在上班时间(周一到周五 9:00-17:00)禁止访问外网，内部网络正常访问。

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；14 口启用环路检测，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，同时开启防止 ARP

网关欺骗攻击。

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 untrust1 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 MAARP、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；VLAN40 开启 IPv6，IPv6 业务地址规划如下：

业务	**IPv6 地址**
总公司 VLAN50	2001:DA8:50::1/64
分公司 VLAN60	2001:DA8:60::1/64

12. 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 DHCPSERVER 获取 IPv6 地址，在 SW 上开启 IPv6DHCPserver 功能，IPv6 地址范围 2001:da8:50::2-2001:da8:50::100。

13. 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。

14. SW 与 AC，AC 与 FW 之间配置 OSPFarea0 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；总公司 SW 和 BC 之间运行静态路由协议。

15. 分公司销售部门通过防火墙上的 DHCPSERVER 获取 IP 地址，serverIP 地址为 20.0.0.254，地址池范围 20.1.60.10-20.1.60.100，dns-server8.8.8.8。

16. 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。

17. 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。SNMP 服务器地址：20.10.28.100，团体字：skills。

18. 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:202.22.1.202.22.1.4；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 UDP2000 端口。

19. 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 VLAN61 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。

20. 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)，外网用户只能通过防火墙外网地址访问服务器 Web 服务。

21. 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。

22. 由于分公司到因特网链路带宽比较低，出口只有 200Mbps 带宽，需要在防火墙配置 iQoS，系统中 P2P 总的流量不能超过 100Mbps，同时限制每用户最大下载带宽为 2Mbps，上传为 1Mbps，优先保障 HTTP 应用，为 HTTP 预留 100Mbps 带宽。

23. 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。

24. 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、3DES 和 MD5 加密方式，IKE 阶段 2 采用 ESP-3DES，MD5。

25. 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。

26. 在 BC 上配置 PPTPVPN 让外网用户能够通过 PPTPVPN 访问总公司 SW 上内网地址，用户名为 test，密码 test23。

27. 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。

28. 在 BC 上配置 url 过滤策略，禁止总公司内网用户在周一到周五的早上 8 点到晚上 18 点访问外网 www.skillchina.com。

29. 在 BC 上开启 IPS 策略，对总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. 总公司出口带宽较低，总带宽只有 200Mbps，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 50Mbps，以免 P2P 流量占用太多的出口网络带宽，

启用阻断记录。

31. 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。

32. 限制总公司内网用户访问因特网 Web 视频和即时通信下行最大带宽为 20Mbps，上传为 10Mbps，启用阻断记录。

33. 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。

34. 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、DDOS 日志、攻击日志信息发送 syslog 日志服务器，IP 地址是 20.10.28.6，UDP 的 514 端口。

35. 在分公司的 WAF 上配置，对会话安全进行防护，开启 Cookie 加固和加密。

36. 编辑防护策略，规则名称为“HTTP 协议”，定义 HTTP 请求最大长度为 1024，防止缓冲区溢出攻击。

37. 为防止暴力破解网站服务器，在 WAF 上配置对应的防护策略进行限速防护，名称为“防暴力破解”，限速频率为每秒 1 次，严重级别为高级，记录日志;

38. WAF 上配置阻止用户上传 ZIP、DOJPG、RAR 格式文件，规则名称为“阻止文件上传”。

39. WAF 上配置对应防护规则，规则名称为“HTTP 特征防护”，要求对 SQL 注入、跨站脚本攻击 XSS、信息泄露、防爬虫、恶意攻击等进行防护，一经发现立即阻断并发送邮件报警及记录日志。

40. WAF 上配置对“www.skillchina.com”，开启弱密码检测，名称配置为“弱密码检测”。

41. WAF 上配置防跨站防护功能，规则名称为“防跨站防护”保护“www.skillchina.com”不受攻击,处理动作设置为阻断,请求方法为 GET、POST 方式。

42. 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 AP50 台；办公无线用户 VLAN10 预计 300 人，来宾用户 VLAN20 预计不超过 30 人。

43. 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 DHCPopion43 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。

44. 在 NETWORK 下配置 SSID，需求如下：NETWORK1 下设置 SSIDABC4321,VLAN10,加密模式为 wpa-personal,其口令为 43214321。

45. NETWORK2 下设置 SSIDGUEST，VLAN20 不进行认证加密,做相应配置隐藏该 SSID。

46. NETWORK2 开启内置 portal+本地认证的认证方式，账号为 test 密码为 test4321。

47. 配置 SSIDGUEST 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 1Mbps，下行 2Mbps；配置所有无线接入用户相互隔离。

48. 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。

49. 为了提高 wifi 用户体验感，拒绝弱信号终端接入，设置阈值低于 50 的终端接入无线信号；为防止非法 AP 假冒合法 SSID，开启 AP 威胁检测功能。

50. 通过配置防止多 AP 和 AC 相连时过多的安全认证连接而消耗 CPU 资源，检测到 AP 与 AC 在 10 分钟内建立连接 5 次就不再允许继续连接，两小时后恢复正常。

模块二：网络安全渗透

一、 比赛时间及注意事项

本阶段比赛时长为 180 分钟。

【注意事项】

(1) 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。

(2) 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)，请将赛题第三阶段所完成的“信息安全管理与评估竞赛答题卡-模块三”答题文档，放置在“GWxx”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，请将第三阶段所完成的“信息安全管理与评估竞赛答题卡-模块三”答题文档，放置在“GW08”文件夹中。

二、 竞赛项目赛题

本文件为信息安全管理与评估项目竞赛-第三阶段赛题，内容包括：网络安全渗透。

三、 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。

四、 所需软硬件设备和材料

所有测试项目都可由参赛选手根据基础设施列表中指定的设备和软件完成。

五、 评分方案

本测试项目模块网络安全渗透为 600 分。

六、 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。

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。

七、 工作任务

(一) 人力资源管理系统

任务编号	任务描述	答案	分值
任务一	请对门户网站进行黑盒测试，利用漏洞找到 flag1，并将 flag1 提交。flag1 格式 flag1{<flag 值>}		40
任务二	请对门户网站进行黑盒测试，利用漏洞找到 flag2，并将 flag2 提交。flag2 格式 flag2{<flag 值>}		40
任务三	请对门户网站进行黑盒测试，利用漏洞找到 flag3，并将 flag3 提交。flag3 格式 flag3{<flag 值>}		40

（二） 邮件系统

任务编号	任务描述	答案	分值
任务四	请对办公系统进行黑盒测试，利用漏洞找到 flag1，并将 flag1 提交。flag1 格式 flag1{<flag 值>}		40
任务五	请对办公系统进行黑盒测试，利用漏洞找到 flag2，并将 flag2 提交。flag2 格式 flag2{<flag 值>}		40

（三） FTP 服务器

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>}		40
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>}		40
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>}		40

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>}		40
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>}		40
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>}		40
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>}		40
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>}		40

（四）应用系统服务器

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 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>}		40

（五）运维服务器

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>}		40