**第4部分**

操作技能复习题

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置无线控制器和访问点以增强网络安全

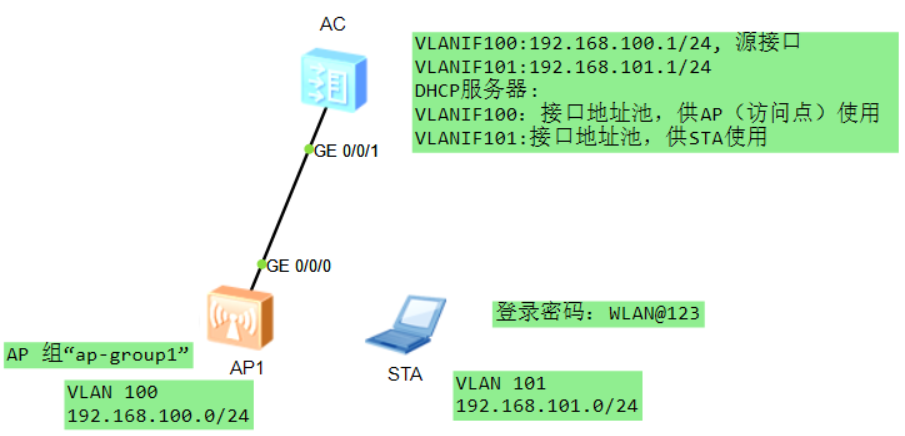
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

随着业务扩展，信息安全成为公司管理层的重点关注对象。为了实施集中管理公司的无线网络环境，如图1所示，现在需要对无线控制器AC进行配置，打开考题1.1.1.paper，完成以下任务：  
（1）设定无线控制器名称与VLAN划分：配置无线控制器（AC，无线控制器）的名称为AC，在无线控制器AC上创建VLAN100到VLAN101，将接口G0/0/1配置为Trunk模式,配置接口G0/0/1的PVID为100，配置接口G0/0/1允许所有VLAN通过。  
（2）配置DHCP服务：在AC上启动DHCP服务，配置VLANIF100接口的IP地址为192.168.100.1/24，采用接口的DHCP功能，供AP（访问点）使用，配置VLANIF101接口的IP地址为192.168.101.1/24，采用接口的DHCP功能，供STA使用。  
（3）配置AC的AP组并导入AP：配置建立CAPWAP隧道的源接口为VLANIF100，创建名为“ap-group1”的AP组,在 AC 上使用MAC认证离线导入 AP（AP的MAC地址为00e0-fc46-1aa0）；将图中AP命名为“AP1”，将 AP 加入 AP 组“ap-group1” 中。  
（4）配置无线业务参数：创建并配置以下模板：  
创建安全模板“WLAN-SEC”，配置WPA2+PSK+AES的安全策略，密钥使用字符串形式，设置密码为“WLAN@123”。  
创建SSID模板“WLAN-SSID”，配置SSID名称设为“WLAN-INSPC”。  
创建VAP模板“WLAN-VAP”，配置业务数据转发模式为隧道转发，配置业务VLAN为101，并引用前述安全模板“WLAN-SEC”和SSID模板“WLAN-SSID”。  
（5）配置AP组引用VAP模板：AP组上射频0和射频1都使用VAP模板“WLAN-VAP”的配置。  
（6）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能配置无线AC控制器；   
（2）能保存配置文件。

**4.**质量指标

（1）无线AC名称配置正确，接口划入VLAN正确；   
（2）无线AC的DHCP服务配置正确；   
（3）AC 的源接口配置正确；   
（4）AC的AP组并导入AP正确；   
（5）WLAN无线参数配置正确；   
（6）VAP模版引用正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置无线控制器和访问点以增强网络安全

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 无线AC名称配置正确； | 根据数据 |  |  |
| M2 | 1 | 无线AC创建VLAN正确； | 根据数据 |  |  |
| M3 | 1 | 接口trunk设置正确； | 根据数据 |  |  |
| M4 | 1 | 接口pvid设置正确； | 根据数据 |  |  |
| M5 | 1 | Trunk设置允许vlan正确； | 根据数据 |  |  |
| M6 | 1 | 无线AC的DHCP服务启动正确； | 根据数据 |  |  |
| M7 | 1 | Vlan100接口启用DHCP正确； | 根据数据 |  |  |
| M8 | 1 | 接口IP地址配置正确； | 根据数据 |  |  |
| M9 | 1 | Vlan101接口启用DHCP正确； | 根据数据 |  |  |
| M10 | 1 | 接口IP地址配置正确； | 根据数据 |  |  |
| M11 | 1 | AC的AP组配置正确，AP命名正确； | 根据数据 |  |  |
| M12 | 1 | AP导入正确； | 根据数据 |  |  |
| M13 | 1 | 安全模板创建正确，WLAN无线密码设置正确； | 根据数据 |  |  |
| M14 | 1 | SSID模版创建正确，SSID命名正确； | 根据数据 |  |  |
| M15 | 1 | VAP模板创建正确，业务数据转发模式配置正确； | 根据数据 |  |  |
| M16 | 1 | 业务VLAN配置正确； | 根据数据 |  |  |
| M17 | 1 | 引用安全模板正确； | 根据数据 |  |  |
| M18 | 1 | 引用SSID模板正确； | 根据数据 |  |  |
| M19 | 1 | Radio0的VAP模版引用正确； | 根据数据 |  |  |
| M20 | 1 | Radio1的VAP模版引用正确。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置交换机和路由器安全策略

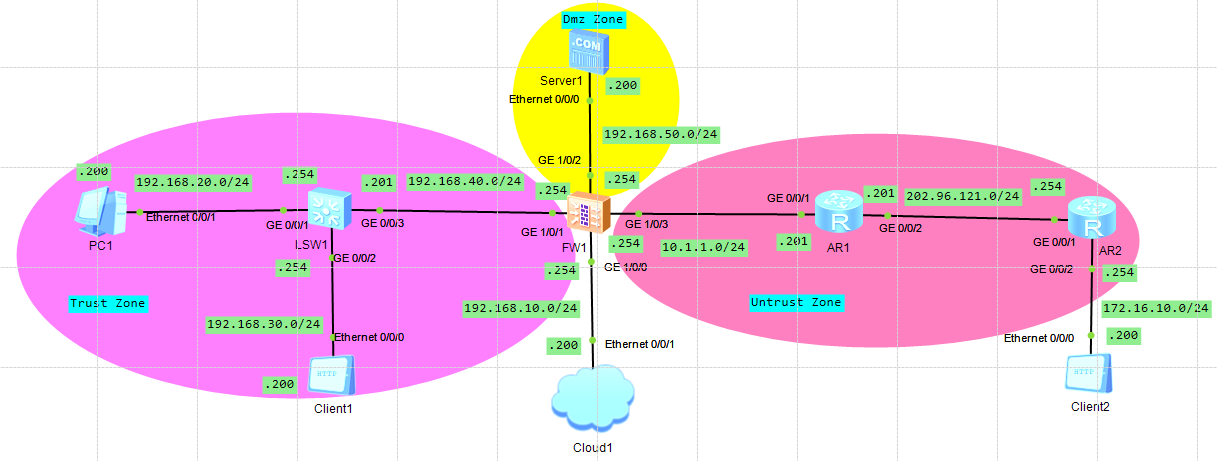
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，AR1路由器作为接入Internet的网关，Server1对公网和私网用户提供WWW服务，公司为Server1申请了公网地址202.96.121.200。现在需要对图中LSW1交换机和AR1路由器配置安全策略，打开三级-1.1.2.paper，完成以下任务：  
（1）配置设备名称：设置交换机（LSW1，交换机）的名称为“LSW1”，设置路由器（AR1，路由器）的名称为“AR1”。  
（2）配置交换机Console口用户认证：设置LSW1交换机Console口用户认证方式为AAA认证，且用户名为admin123，密码为Admin@1234（请不要修改为其他密码），设置admin123用户仅为Console口登录用户。  
（3）配置交换机telnet登录：设置LSW1交换机telnet登录认证方式为AAA认证，且用户名为admin456，密码为admin@456（请不要修改为其他密码），设置admin456用户仅为telnet登录用户。  
（4）配置交换机端口安全：对LSW1交换机的G0/0/1，设置为：限制不能连入除图1 之外的其他主机，且一旦发现非法接入设备，直接关闭端口。  
（5）配置路由器Console口用户认证：设置AR1路由器Console口用户认证方式为AAA认证，且用户名为admin123，密码为Admin@1234（请不要修改为其他密码），设置admin123用户仅为Console口登录用户。  
（6）限制路由器telnet登录：禁用AR1路由器的telnet服务。  
（7）根据图1配置AR1路由器端口G0/0/2的IP地址。  
（8）配置路由器NAT策略：在AR1路由器上配置公网地址池1，地址池范围是202.96.121.202--202.96.121.207；配置ACL规则2000,使得局域网内192.168.0.0/16网段主机可以访问公网；在端口G0/0/2处配置动态NAT转换，使得局域网内192.168.0.0/16网段主机访问公网的数据包源地址能够转换为地址池中的公网地址；在端口G0/0/2处配置静态NAT转换，使得公网主机可以通过公网地址202.96.121.200访问内网WWW服务器Server1提供的WWW服务。  
（9）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能配置交换机安全策略；   
（2）能配置路由器安全策略；   
（3）能保存配置文件。

**4.**质量指标

（1）交换机名称配置正确，路由器名称配置正确；   
（2）交换机Console口用户认证方式配置正确，Console口登录用户配置正确；   
（3）禁用交换机的telnet服务配置正确；   
（4）交换机端口安全配置正确；   
（5）路由器Console口用户认证方式配置正确，Console口登录用户配置正确；   
（6）禁用路由器的telnet服务配置正确；   
（7）路由器NAT策略配置正确；   
（8）配置文件保存正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置交换机和路由器安全策略

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | LSW1交换机名称配置正确； | 根据数据 |  |  |
| M2 | 1 | AR1路由器名称配置正确； | 根据数据 |  |  |
| M3 | 1 | LSW1交换机Console口用户认证方式配置正确； | 根据数据 |  |  |
| M4 | 1 | LSW1交换机Console口登录用户名和密码配置正确； | 根据数据 |  |  |
| M5 | 1 | 配置admin123用户仅为Console口登录用户正确； | 根据数据 |  |  |
| M6 | 1 | LSW1交换机telnet用户认证方式配置正确； | 根据数据 |  |  |
| M7 | 1 | LSW1交换机telnet登录用户名和密码配置正确； | 根据数据 |  |  |
| M8 | 1 | 配置admin456用户仅为telnet登录用户正确； | 根据数据 |  |  |
| M9 | 1 | 交换机G0/0/1端口安全使能配置正确； | 根据数据 |  |  |
| M10 | 1 | 交换机G0/0/1端口与MAC地址绑定配置正确； | 根据数据 |  |  |
| M11 | 1 | 交换机G0/0/1端口异常情况关闭配置正确； | 根据数据 |  |  |
| M12 | 1 | AR1路由器Console口用户认证方式配置正确； | 根据数据 |  |  |
| M13 | 1 | AR1路由器Console口用户认证方式配置正确； | 根据数据 |  |  |
| M14 | 1 | AR1路由器Console口用户认证方式配置正确； | 根据数据 |  |  |
| M15 | 1 | 禁用AR1路由器的telnet服务配置正确； | 根据数据 |  |  |
| M16 | 1 | AR1路由器G0/0/2端口IP地址配置正确； | 根据数据 |  |  |
| M17 | 1 | AR1路由器地址池配置正确； | 根据数据 |  |  |
| M18 | 1 | AR1路由器ACL规则配置正确； | 根据数据 |  |  |
| M19 | 1 | AR1路由器动态NAT配置正确； | 根据数据 |  |  |
| M20 | 1 | AR1路由器静态NAT配置正确. | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置防火墙安全防护功能

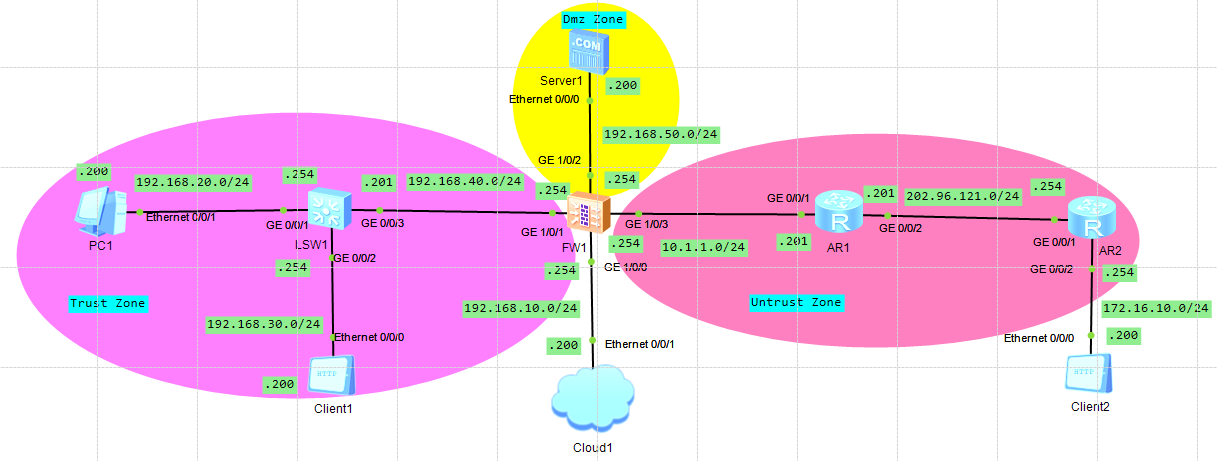
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，AR1路由器作为接入Internet的网关，Server1对公网和私网用户提供WWW服务，公司为Server1申请了公网地址202.96.121.200。现在需要对图中防火墙FW1进行适当安全防护配置，打开三级-1.1.3.paper，完成以下任务：  
（1）启动所有设备，登录防火墙FW1命令行界面（登录用户admin，密码Admin@1234,请勿修改密码）,完成防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置，具体信息如图1所示；  
（2）配置防火墙接口G1/0/1、G1/0/2、G1/0/3所属安全区域，具体信息如图1所示；  
（3）配置防火墙安全策略，使得192.168.0.0/16网段主机可以访问Internet，公网主机和内网主机都可以访问内网WWW服务器Server1；  
（4）在防火墙FW1上做适当配置，使得公网主机和内网主机都可以使用公网地址202.96.121.200访问WWW服务器Server1；  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能配置防火墙接口IP；   
（2）能配置防火墙接口安全区域；   
（3）能配置防火墙安全策略；   
（4）能配置防火墙NAT策略。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）防火墙接口安全区域配置正确；   
（3）防火墙安全策略配置正确；   
（4）防火墙NAT策略配置正确；   
（5）配置文件保存正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置防火墙安全防护功能

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | FW1防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置正确; | 根据数据 |  |  |
| M2 | 3 | FW1防火墙接口G1/0/1、G1/0/2、G1/0/3所属安全区域配置正确; | 根据数据 |  |  |
| M3 | 2 | FW1防火墙安全策略（从trust到untrust），源区域和目的区域配置正确； | 根据数据 |  |  |
| M4 | 2 | FW1防火墙安全策略（从trust到untrust），源地址范围和动作类型配置正确； | 根据数据 |  |  |
| M5 | 2 | FW1防火墙安全策略（从untrust到dmz），源区域和目的区域配置正确； | 根据数据 |  |  |
| M6 | 3 | FW1防火墙安全策略（从untrust到dmz），源地址范围、定义的服务类型和动作类型untrust），目的地址范围、定义的服务类型和动作类型配置正确； | 根据数据 |  |  |
| M7 | 2 | FW1防火墙安全策略（从trust到dmz），源区域和目的区域配置正确； | 根据数据 |  |  |
| M8 | 2 | FW1防火墙安全策略（从trust到dmz），目的地址范围、定义的服务类型和动作类型配置正确； | 根据数据 |  |  |
| M9 | 1 | FW1防火墙静态NAT策略配置正确。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用防火墙实现入侵防御

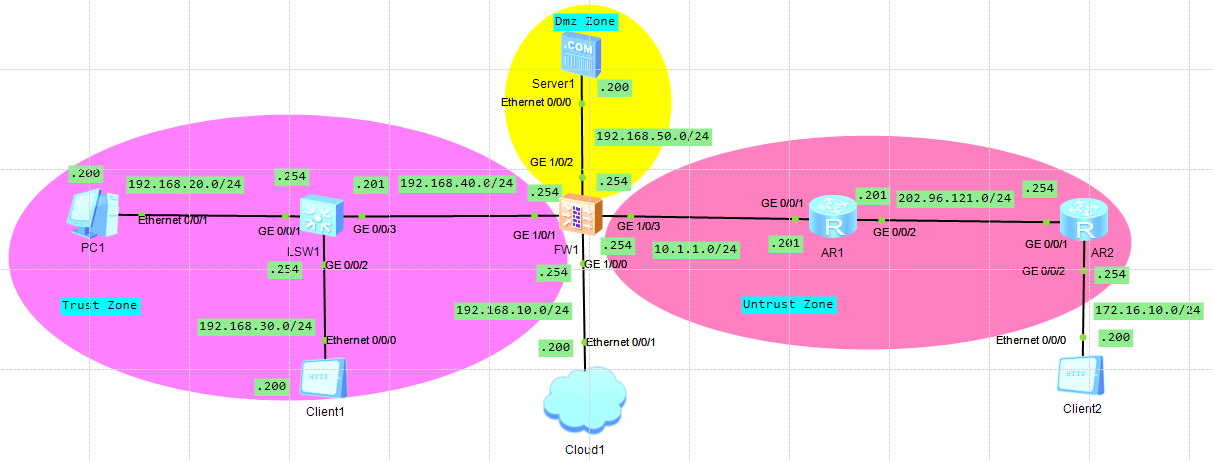
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，AR1路由器作为接入Internet的网关，内网服务器Server1对公网和私网用户均提供WWW服务，公司为Server1申请了公网地址202.96.121.200。现在需要在防火墙FW1进行入侵防御配置，打开三级-1.1.4.paper，完成以下任务：  
（1）启动所有设备，登录防火墙FW1的web界面（登录用户admin，密码Admin@1234,请勿修改密码）,完成防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置，具体信息如图1所示；  
（2）配置防火墙接口G1/0/1、G1/0/2、G1/0/3所属安全区域，具体信息如图1所示；  
（3）在防火墙上新建入侵防御配置文件，文件名称为anti\_untrust，签名过滤器名为filter\_www，过滤器的对象、严重性、操作系统、应用程序、协议、威胁类别默认全部选中，动作设置为:采用签名的缺省动作；  
（4）在防火墙上新建入侵防御配置文件，文件名称为anti\_trust，签名过滤器名为filter\_www，过滤器的对象、严重性、操作系统、应用程序、协议、威胁类别默认全部选中，动作设置为:采用签名的缺省动作；  
（5）配置防火墙安全策略，策略名称为untrust2dmz，使得公网主机可以访问内网WWW服务器Server1；该安全策略调用配置文件anti\_untrust；  
（6）配置防火墙安全策略，策略名称为trust2dmz，使得内网主机可以访问内网WWW服务器Server1；该安全策略调用配置文件anti\_trust；  
（7）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能配置防火墙接口IP；   
（2）能配置防火墙接口安全区域；   
（3）能配置防火墙安全策略；   
（4）能配置防火墙入侵防御策略。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）防火墙接口安全区域配置正确；   
（3）防火墙安全策略配置正确；   
（4）防火墙入侵防御策略配置正确；   
（5）配置文件保存正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用防火墙实现入侵防御

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | FW1防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置正确; | 根据数据 |  |  |
| M2 | 1 | FW1防火墙接口G1/0/2所属安全区域配置正确; | 根据数据 |  |  |
| M3 | 2 | 入侵防御文件anti\_untrust添加成功；其中签名过滤器filter\_www添加成功； | 根据数据 |  |  |
| M4 | 2 | 入侵防御文件anti\_trust添加成功；其中签名过滤器filter\_www添加成功； | 根据数据 |  |  |
| M5 | 3 | 配置FW1防火墙安全策略（从untrust到dmz）untrust2dmz，源区域、目的区域、目的地址配置正确； | 根据数据 |  |  |
| M6 | 3 | 配置FW1防火墙安全策略（从untrust到dmz）untrust2dmz，允许的服务类型，调用的入侵防御配置文件名，动作类型配置正确； | 根据数据 |  |  |
| M7 | 3 | 配置FW1防火墙安全策略（从trust到dmz）trust2dmz，源区域、目的区域、目的地址配置正确； | 根据数据 |  |  |
| M8 | 3 | 配置FW1防火墙安全策略（从trust到dmz）trust2dmz，允许的服务类型，调用的入侵防御配置文件名，动作类型配置正确。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用防火墙控制用户行为

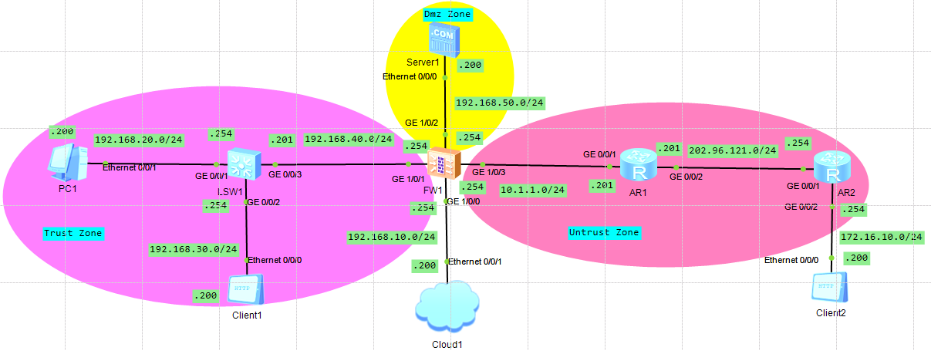
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络拓扑规划如图1所示，AR1路由器作为接入Internet的网关，内网主机（包括研发部门和销售部门）可以访问Internet，现在需要对研发部门和销售部门使用企业云应用“钉钉”分别进行行为控制，打开三级-1.1.5.paper，完成以下任务：  
（1）启动所有设备，登录防火墙FW1的web界面（登录用户admin，密码Admin@1234,请勿修改密码）,完成防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置，具体信息如图1所示；  
（2）配置防火墙接口G1/0/1、G1/0/2、G1/0/3所属安全区域，具体信息如图1所示；  
（3）假定已经在FW1防火墙的default认证域下，创建了用户组research和sales，分别对应研发员工和销售员工，而且完成了认证配置，现在要求针对“研发员工只允许使用钉钉进行即时通信，不能传输文件和浏览”的需求，新建云接入安全感知配置文件，文件名为file\_research；针对“销售员工可以使用钉钉进行即时通信和浏览，但是不能进行文件传输”的需求，新建云接入安全感知配置文件，文件名为file\_sales；  
（4）为研发员工配置防火墙安全策略，策略名为rule\_research，源区域为trust，目的区域为untrust，源地址范围为192.168.0.0/16，该策略调用云接入安全感知配置文件file\_research，用来控制研发员工行为；  
（5）为销售员工配置防火墙安全策略，策略名为rule\_sales，源区域为trust，目的区域为untrust，源地址范围为192.168.0.0/16，该策略调用云接入安全感知配置文件file\_sales，用来控制销售员工行为；  
（6）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
  
  
图1



**3.**技能要求

（1）能配置防火墙接口IP；   
（2）能配置防火墙接口安全区域；   
（3）能配置用户行为控制；   
（4）能配置防火墙安全策略。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）防火墙接口安全区域配置正确；   
（3）防火墙用户行为控制配置正确；   
（4）防火墙安全策略配置正确；   
（5）配置文件保存正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用防火墙控制用户行为

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | FW1防火墙接口G1/0/1、G1/0/2、G1/0/3的IP配置正确; | 根据数据 |  |  |
| M2 | 3 | FW1防火墙接口G1/0/1、G1/0/2、G1/0/3所属安全区域配置正确; | 根据数据 |  |  |
| M3 | 3 | 云接入安全感知配置文件file\_research和file\_sales配置正确； | 根据数据 |  |  |
| M4 | 3 | 防火墙安全策略rule\_research，源区域、目的区域、源地址范围配置正确； | 根据数据 |  |  |
| M5 | 3 | 防火墙安全策略rule\_research，用户主体、调用的云接入安全感知配置文件、动作类型配置正确； | 根据数据 |  |  |
| M6 | 3 | 防火墙安全策略rule\_sales，源区域、目的区域、源地址范围配置正确； | 根据数据 |  |  |
| M7 | 2 | 防火墙安全策略rule\_sales，用户主体、调用的云接入安全感知配置文件、动作类型配置正确。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows Server的安全策略

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Windows服务器进行一些安全事件的审核和安全策略的优化设置，具体包括：  
（1）对备份和还原权限的使用进行审核；  
（2）审核策略更改设置成功与失败；  
（3）对账户锁定策略的成功与失败进行审核；  
（4）用户可以通过可移动硬盘读取外部资料，用户禁止通过可移动磁盘向外写入数据；  
（5）阻止用户在登录时显示账户详细信息；  
（6）删除超过7天的用户配置文件；  
（7）用户在进行远程桌面连接时始终要求提示输入密码。

**3.**技能要求

（1）能配置Windows各种审核策略；   
（2）能配置Windows各种安全策略。

**4.**质量指标

（1）启用备份和还原权限审核策略配置正确；   
（2）审核策略配置正确；   
（3）账户锁定安全策略配置正确；   
（4）账户登录安全策略配置正确；   
（5）可移动存储访问策略配置正确；   
（6）用户配置文件策略配置正确；   
（7）远程桌面连接客户端策略配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows Server的安全策略

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确设置“启用对备份和还原权限的使用进行审核”； | 根据数据 |  |  |
| M2 | 2 | 正确设置“修改审核策略为成功” | 根据数据 |  |  |
| M3 | 2 | 正确设置“修改审核策略为失败” | 根据数据 |  |  |
| M4 | 2 | 正确设置“审核账户锁定策略为成功”； | 根据数据 |  |  |
| M5 | 2 | 正确设置“审核账户锁定策略为失败”； | 根据数据 |  |  |
| M6 | 2 | 正确设置“阻止用户在登录时显示账户详细信息”； | 根据数据 |  |  |
| M7 | 2 | 正确设置“可以通过移动硬盘读取外部资料； | 根据数据 |  |  |
| M8 | 2 | 正确设置“禁止通过可移动磁盘向外写入数据”； | 根据数据 |  |  |
| M9 | 2 | 正确设置“删除超过7天的用户配置文件”； | 根据数据 |  |  |
| M10 | 2 | 正确设置“在进行远程桌面连接时始终要求提示输入密码” | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows Server系统加固

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Windows Server服务器进行基础的安全加固，要求完成以下目标：  
（1）启用本地安全策略的审核策略更改，成功和失败操作都需要审核；启用本地安全策略的审核对象访问，成功和失败操作都需要审核；启用本地安全策略的审核目录服务访问，仅失败操作需要审核；  
（2）修改windows日志中应用程序日志存档策略，使得日志存满的时候进行存档，不覆盖事件；  
（3）禁用TCP/IP NetBIOS Helper服务；网卡1取消LMHOSTS查找，禁用TCP/IP上的NetBIOS；  
（4）修改本地安全策略，不会在登录屏幕中显示最后成功登录的用户的名称，关机时清除系统页面文件，不希望允许 SAM 帐户和共享的匿名枚举；

**3.**技能要求

（1）能配置Windows各种审核策略；   
（2）能配置Windows各种日志存档策略；   
（3）能配置Windows各种安全策略。

**4.**质量指标

（1）审核策略配置正确；   
（2）日志存档策略配置正确；   
（3）服务安全策略配置正确；   
（4）本地安全策略配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows Server系统加固

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确设置审核策略更改； | 根据数据 |  |  |
| M2 | 2 | 正确设置审核对象访问； | 根据数据 |  |  |
| M3 | 2 | 正确设置审核目录服务访问； | 根据数据 |  |  |
| M4 | 4 | 正确设置应用程序日志达到最大大小时的策略； | 根据数据 |  |  |
| M5 | 4 | 正确设置服务禁用TCP/IP上的NetBIOS得2分，正确设置网卡不启用LMHOSTS查找得1分，正确设置网卡禁用TCP/IP上得NetBIOS得1分； | 根据数据 |  |  |
| M6 | 2 | 正确设置启用“不显示最后的用户名”选项； | 根据数据 |  |  |
| M7 | 2 | 正确设置启用“关机：清除虚拟内存页面文件”选项； | 根据数据 |  |  |
| M8 | 2 | 正确设置启用“网络访问：不允许SAM账户和共享的匿名枚举”选项。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux系统安全加固

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Linux服务器进行基础的安全加固，使用root用户登录，要求完成以下目标：  
（1）锁定不需要登录的账户：锁定daemon账户，不允许其登录；  
（2）设置新建用户密码策略：在文件login.defs中设置“新建用户的密码最长使用天数”为90，“新建用户的最短密码使用天数”为0，“最小密码长度“为9，“新建用户的密码到期提前提醒天数”为7；  
（3）用默认参数方式创建用户组group1，创建用户user1，user1密码为Admin@1234，将user1加入group1组；  
（4）设置文件权限：在/root下创建文本文件file1，将file1文件的权限设置为所有者可读可写可执行，同组用户可读可执行，其他用户可读可执行；将file1所属组改为group1；  
（5）启动防火墙，将防火墙设置为开机自启动；  
（6）永久禁止7554端口通过防火墙，并立即生效；  
（7）永久开启7557端口通过防火墙，并立即生效。

**3.**技能要求

（1）能配置Linux各种账户管理策略；   
（2）能配置Linux各种密码策略；   
（3）能配置Linux各种文件权限策略；   
（4）能配置Linux防火墙规则。

**4.**质量指标

（1）账户管理策略配置正确；   
（2）密码策略配置正确；   
（3）文件权限配置正确；   
（4）防火墙规则配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux系统安全加固

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确配置锁定daemon账户； | 根据数据 |  |  |
| M2 | 3 | 配置新建用户的密码策略，配置文件名正确得1分，“新建用户的密码最长使用天数”得1分、“新建用户的最短密码使用天数”配置正确得1分； | 根据数据 |  |  |
| M3 | 2 | 配置新建用户的密码策略，“最小密码长度”配置正确得1分、“新建用户的密码到期提前提醒天数”配置正确得1分； | 根据数据 |  |  |
| M4 | 1 | 正确创建用户组group1； | 根据数据 |  |  |
| M5 | 1 | 正确创建用户user1； | 根据数据 |  |  |
| M6 | 2 | 正确配置将用户user1加入group1组； | 根据数据 |  |  |
| M7 | 2 | 创建文件正确得1分，设置文件权限正确得1分； | 根据数据 |  |  |
| M8 | 1 | 设置文件所属组正确； | 根据数据 |  |  |
| M9 | 2 | 正确设置启动防火墙得1分，正确设置防火墙开机自启动得1分； | 根据数据 |  |  |
| M10 | 2 | 正确设置在防火墙上永久禁止7554端口得1分，正确设置立即生效得1分。 | 根据数据 |  |  |
| M11 | 2 | 正确设置在防火墙上永久开启7557端口得1分，正确设置立即生效得1分。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows Server服务器安全配置

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Windows Server服务器进行安全配置，要求完成以下目标：  
（1）配置账号密码策略：启用“密码必须符合复杂性要求”，“密码长度最小值”为10，“密码最短使用期限”为0天，“密码最长使用期限”为90天，“强制密码历史”为3个，禁用“用可还原的加密来储存密码”；  
（2）配置账户锁定策略：设置“账户锁定阈值”为5次，“账户锁定时间”为30分钟，“重置账户锁定计数器”为30分钟之后；  
（3）配置本地安全策略：在“本地策略”的“安全选项”中，启用“网络访问：不允许SAM账户和共享的匿名枚举”选项；  
（4）配置日志策略：修改windows日志中系统日志存档策略，使得系统日志存满的时候进行存档，不覆盖事件；  
（5）配置审核策略：启用本地安全策略的审核策略更改，成功和失败操作都需要审核；启用本地安全策略的审核目录服务访问，仅失败操作需要审核。

**3.**技能要求

（1）能配置Windows各种账号密码策略；   
（2）能配置Windows各种账户锁定策略；   
（3）能配置Windows各种本地策略；   
（4）能配置Windows各种日志策略；   
（5）能配置Windows各种审核策略。

**4.**质量指标

（1）账号密码策略配置正确；   
（2）账户锁定策略配置正确；   
（3）本地策略配置正确；   
（4）日志策略配置正确；   
（5）审核策略配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows Server服务器安全配置

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确配置账户密码策略,“密码必须符合复杂性要求”策略得1分、“密码长度最小值”得1分、“密码最短使用期限”得1分； | 根据数据 |  |  |
| M2 | 3 | 正确配置账户密码策略,“密码最长使用期限”得1分、“强制密码历史”策略得1分、“用可还原的加密来储存密码”得1分； | 根据数据 |  |  |
| M3 | 3 | 正确配置账户锁定策略，“账户锁定阈值”为5次得1分，“账户锁定时间”为30分钟得1分，“重置账户锁定计数器”为30分钟得1分； | 根据数据 |  |  |
| M4 | 3 | 正确配置本地安全策略； | 根据数据 |  |  |
| M5 | 4 | 正确配置日志策略； | 根据数据 |  |  |
| M6 | 4 | 正确配置审核策略，启用本地安全策略的审核策略更改得2分，启用本地安全策略的审核目录服务访问得2分。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Linux系统安全防护

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司需要网络安全防护人员对公司的Linux服务器进行安全防护配置，要求完成以下目标：  
（1）给以下文件加上不可更改属性，防止未经授权的删除或更改，文件包括：/etc/test/passwd、/etc/test/shadow、/etc/test/group、/etc/test/gshadow、/etc/test/services、/etc/test/su、/etc/test/config；  
（2）配置服务器端SSH安全：修改/etc/ssh/sshd\_config这个配置文件，将SSH默认端口22，修改为2222；配置不允许root用户远程SSH登录；禁止使用空白密码用户访问SSH服务器；限制允许密码尝试次数为3；关闭tcp端口转发；关闭X11转发；  
（3）添加防火墙规则，允许防火墙放行2222端口；防火墙重新加载使配置生效；  
（4）配置限制重要目录权限：对重要日志目录/var/log递归设置权限为640。  
（5）配置umask值：在/etc/profile设置umask值为027，使得新建目录默认权限为750，新建普通文件默认权限为640。

**3.**技能要求

（1）能配置Linux系统各种文件属性；   
（2）能配置Linux系统各种服务安全策略；   
（3）能配置Linux各种防火墙规则；   
（4）能配置Linux系统各种目录权限；   
（5）能配置Linux系统umask值。

**4.**质量指标

（1）文件属性配置正确；   
（2）SSH服务安全配置正确；   
（3）防火墙规则配置正确；   
（4）重要目录权限配置正确；   
（5）umask值配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Linux系统安全防护

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 正确操作给/etc/test/passwd 加上不可更改属性； | 根据数据 |  |  |
| M2 | 1 | 正确操作给/etc/test/shadow 加上不可更改属性； | 根据数据 |  |  |
| M3 | 1 | 正确操作给/etc/test/group 加上不可更改属性； | 根据数据 |  |  |
| M4 | 1 | 正确操作给/etc/test/gshadow 加上不可更改属性； | 根据数据 |  |  |
| M5 | 1 | 正确操作给/etc/test/services 加上不可更改属性； | 根据数据 |  |  |
| M6 | 1 | 正确操作给/etc/test/su 加上不可更改属性； | 根据数据 |  |  |
| M7 | 1 | 正确操作给/etc/test/config 加上不可更改属性； | 根据数据 |  |  |
| M8 | 3 | 配置SSH安全，更改SSH端口号正确得1分、设置禁止root用户SSH远程登录正确得2分； | 根据数据 |  |  |
| M9 | 3 | 配置SSH安全，设置禁止空白密码用户访问SSH服务器正确得1分、设置允许密码尝试次数正确得1分、配置关闭tcp端口转发正确得1分； | 根据数据 |  |  |
| M10 | 2 | 配置SSH安全，配置关闭X11转发正确得2分； | 根据数据 |  |  |
| M11 | 2 | 正确配置防火墙允许开放2222端口得1分；防火墙重新加载使配置生效得1分； | 根据数据 |  |  |
| M12 | 1 | 正确配置重要日志目录/var/log及子目录的权限； | 根据数据 |  |  |
| M13 | 2 | 正确配置umask值，使得新建目录默认权限为750得1分，新建普通文件默认权限为640得1分。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Windows Server防火墙和远程桌面安全

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司的一台服务器开放了远程桌面服务，方便对它进行远程管理，作为网络安全防护人员，需要对该服务器进行安全配置，要求：  
（1）创建普通用户user1,设置密码为Pass@123，禁止该用户本地登录，授权其可以进行远程桌面连接，但不能远程关机，并设置远程桌面连接的时间限制为10分钟。  
（2）改变远程桌面连接服务的端口为6666，并配置Windows系统自带防火墙，建立入站规则(以端口号命名规则)，允许通过该端口进行远程桌面连接。

**3.**技能要求

（1） 能配置远程桌面服务；   
（2） 能配置远程桌面安全策略；   
（3） 能配置防火墙端口出入站规则。

**4.**质量指标

（1） 远程桌面用户配置正确；   
（2） 远程桌面服务开启正确；   
（3） 远程桌面安全策略配置正确；   
（4） 防火墙端口出入站规则配置正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Windows Server防火墙和远程桌面安全

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确创建用户user1 | 根据数据 |  |  |
| M2 | 2 | 正确设置user1隶属于Remote Desktop Users组 | 根据数据 |  |  |
| M3 | 2 | 配置组策略，禁止账户本地登录； | 根据数据 |  |  |
| M4 | 2 | 取消账户远程关机权限； | 根据数据 |  |  |
| M5 | 2 | 设置远程桌面连接的时间限制为10分钟； | 根据数据 |  |  |
| M6 | 2 | 远程桌面连接服务的端口设置为6666 | 根据数据 |  |  |
| M7 | 2 | 存在防火墙规则，规则名为6666； | 根据数据 |  |  |
| M8 | 2 | 正确配置入站规则； | 根据数据 |  |  |
| M9 | 2 | 正确配置规则允许的端口是6666； | 根据数据 |  |  |
| M10 | 2 | 正确配置规则是Tcp协议 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：SSH基于密钥的登录

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

利用Windows Server系统中的PuTTY产生密钥，并将公钥分发至Centos系统，实现root用户从Windows Server系统到Centos系统的基于密钥的登录。请将主要操作流程截图保存至Windows Server系统的D:\kaoshi\_3\。（主要操作流程至少包括密钥生成，公钥分发、公钥权限修改，私钥保存以及基于密钥登录）。

**3.**技能要求

（1）能生成密钥对；   
（2）能进行公钥分发和私钥保存；   
（3）能实现密钥身份验证登录。

**4.**质量指标

（1）正确生成密钥对；   
（2）正确进行公钥分发和私钥保存；   
（3）成功实现基于密钥的身份验证登录。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：SSH基于密钥的登录

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 4 | 正确生成密钥对 | 根据数据 |  |  |
| M2 | 4 | 正确进行公钥分发，在Linux服务器的/root/.ssh下有 authorized\_key文件 | 根据数据 |  |  |
| M3 | 4 | authorized\_key文件文件的权限为644或600或640 | 根据数据 |  |  |
| M4 | 4 | 私钥保存在本地 | 根据数据 |  |  |
| M5 | 4 | 成功实现root用户基于密钥的身份验证登录 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Web 服务日志审计

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

公司在Centos系统中使用Nginx部署web服务器,现需要企业安全技术人员对Nginx的日志进行提取与筛选分析，使用shell命令对如下要求进行操作（Nginx的配置文件在etc/test/nginx/下）：  
（1）分别提取Nginx的访问日志和错误日志存放至“/tmp/access.log”和“/tmp/error.log”；  
（2）筛选error.log中所有包含“MSJ/1.0”信息的日志保存至“/tmp/abnormal.log”；  
（3）筛选access.log，过滤HTTP状态码404的行后，将剩余POST方法的记录保存至“/tmp/post.log”。

**3.**技能要求

（1）能提取Web服务器日志；   
（2）能筛选日志中的指定信息。

**4.**质量指标

（1）正确提取Web访问日志和错误日志并保存；   
（2）正确筛选Web日志中的信息并保存。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Web 服务日志审计

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确找到Nginx访问日志的存储位置； | 根据数据 |  |  |
| M2 | 2 | 正确找到Nginx错误日志的存储位置； | 根据数据 |  |  |
| M3 | 1 | 正确新建/tmp/access.log； | 根据数据 |  |  |
| M4 | 2 | 正确提取访问日志存放至/tmp/access.log； | 根据数据 |  |  |
| M5 | 1 | 正确新建/tmp/error.log； | 根据数据 |  |  |
| M6 | 2 | 正确提取错误日志存放至/tmp/error.log； | 根据数据 |  |  |
| M7 | 1 | 正确新建/tmp/abnormal.log； | 根据数据 |  |  |
| M8 | 3 | 正确筛选error.log，筛选包含MSJ/1.0的信息得2分，筛选后的信息保存至/tmp/abnormal.log得1分； | 根据数据 |  |  |
| M9 | 1 | 正确新建/tmp/post.log； | 根据数据 |  |  |
| M10 | 5 | 正确筛选access.log，过滤状态码404得2分，保留POST方法得2分，筛选后的信息保存至/tmp/post.log得1分。 | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：web应用日志策略配置

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

企业使用Windows 系统的IIS部署web服务器，在服务器运维阶段需要通过日志来分析网站的运行状况，及时对网站的访问进行审计，因此需要对web服务器的日志进行配置。  
要求：  
（1）检查并启动IIS服务（如果未启动）；  
（2）每个站点配置一个日志文件，日志文件格式为W3C；  
（3）日志文件默认保存在D:\kaoshi\_3\iis\_log\，日志记录字段设置成日期、时间、服务名称、服务器名称；  
（4）日志能使用本地时间进行文件命名，并每小时滚动更新；  
（5）打开Chrome浏览器，访问默认网站后，查看最近一次访问日志。

**3.**技能要求

（1）能对IIS日志进行安全配置。

**4.**质量指标

（1）正确配置IIS日志格式；   
（2）正确配置IIS日志记录字段策略；   
（3）正确配置IIS日志更新策略

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：web应用日志策略配置

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确启动IIS； | 根据数据 |  |  |
| M2 | 3 | 正确配置IIS日志格式为W3C； | 根据数据 |  |  |
| M3 | 3 | 设置每个站点配置一个日志文件； | 根据数据 |  |  |
| M4 | 4 | 正确设置IIS日志记录字段，设置成日期得1分、时间得1分、服务名称得1分、服务器名称得1分； | 根据数据 |  |  |
| M5 | 3 | 日志能使用本地时间进行文件命名； | 根据数据 |  |  |
| M6 | 3 | 日志每天滚动更新； | 根据数据 |  |  |
| M7 | 2 | 浏览默认站点后，正确访问网站日志，显示日志结果； | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：FTP应用日志策略配置

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

企业使用Windows 系统的IIS部署FTP服务器，在FTP服务器运维阶段需要通过日志来分析其运行状况，及时对服务器的访问进行审计，因此需要对FTP服务器的日志进行配置。  
要求：  
（1）检查并启动IIS服务（如果未启动）；  
（2）每个服务器配置一个日志文件，日志文件默认保存在D:\kaoshi\_3\ftp\_log\；  
（3）需能记录日志的字段包括日期、时间、服务器名称、 发送的字节数、接收的字节数、所用时间；  
（4）FTP日志能使用本地时间进行文件命名，并每月滚动更新。

**3.**技能要求

（1）对 FTP 日志进行安全配置

**4.**质量指标

（1）正确配置FTP日志格式；   
（2）正确配置FTP日志记录字段策略；   
（3）正确配置FTP日志更新策略

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：FTP应用日志策略配置

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确启用IIS； | 根据数据 |  |  |
| M2 | 3 | 日志文件默认保存在D:\kaoshi\_3\ftp\_log\； | 根据数据 |  |  |
| M3 | 3 | 每个服务器配置一个日志文件； | 根据数据 |  |  |
| M4 | 6 | 日志字段设置日期得1分、时间得1分、服务器名称得1分、 发送的字节数得1分、接收的字节数得1分、所用时间得1分； | 根据数据 |  |  |
| M5 | 3 | 日志能使用本地时间进行文件命名； | 根据数据 |  |  |
| M6 | 3 | 日志每月滚动更新； | 根据数据 |  |  |
| 合计配分 | 20 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置堡垒机以控制Linux资产文件传输

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）JumpServer系统。

**2.**工作任务

某公司希望通过堡垒机统一管理内网的服务器，实现运维操作和文件传输等管控，并对这些操作进行审计。JumpServer已经安装在CentOS虚拟机上，作为堡垒机服务器。具体操作要求如下：  
（1）启动JumpServer服务，登陆JumpServer，用户名admin密码Sjtu@1896；  
（2）创建堡垒机用户，用户名为“ops01”格式命名,邮箱以为“ops01@jumpserver.cn”,使用密码“admin@123”，角色为“用户”，其他保持默认；  
（3）创建1个centos主机资产，ip同jumpserver服务器ip，名称centos1，资产账号jumper，密码jumper；  
（4）将上述的资产授权给ops01用户，授权连接、文件上传权限，其他权限禁止；  
（5）用ops01用户登陆堡垒机，并向资产传输一个文件；  
（6）使用“admin”账户登录审计台，查看上述会话记录，并获取到“ops01”用户登录资产的时间点以及执行的所有操作。

**3.**技能要求

（1）能通过堡垒机控制用户对资产的登陆和文件传输权限；   
（2）能通过堡垒机审计到用户对资产的历史操作；

**4.**质量指标

（1）堡垒机初始化启动正确；   
（2）堡垒机用户创建正确；   
（3）堡垒机资产添加正确；   
（4）堡垒机授权规则配置正确；   
（5）堡垒机文件传输操作正确；   
（6）堡垒机审计操作使用正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置堡垒机以控制Linux资产文件传输

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确启动堡垒机； | 根据数据 |  |  |
| M2 | 2 | 堡垒机用户创建正确，用户名正确得1分，密码选项正确得1分； | 根据数据 |  |  |
| M3 | 2 | 堡垒机资产添加正确，ip正确得1分，名称正确得1分 | 根据数据 |  |  |
| M4 | 1 | 堡垒机资产账号添加正确 | 根据数据 |  |  |
| M5 | 2 | 堡垒机授权规则配置正确，资产授权ops01正确得1分，文件上传权限正确得1分； | 根据数据 |  |  |
| M6 | 1 | 堡垒机子用户ops01能登陆； | 根据数据 |  |  |
| M7 | 2 | 堡垒机子用户ops01文件传输操作正确，； | 根据数据 |  |  |
| M8 | 2 | 堡垒机审计操作使用正确。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：通过堡垒机实现资产运维命令过滤和审计

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）JumpSeryer系统。

**2.**工作任务

某公司为了加强登陆和运维管控，引入JumpServer堡垒机，配置通过堡垒机登录，限制登录的账号、操作的命令，并在会话结束后，对操作命令进行审计。JumpServer已经安装在CentOS虚拟机上，作为堡垒机服务器。具体操作要求如下：  
（1）启动JumpServer服务，登陆JumpServer，用户名admin密码Sjtu@1896；  
（2）创建堡垒机用户，用户名为“ops02”,邮箱为“ops02@jumpserver.cn”,使用密码“admin@123”，角色为“用户”，其他保持默认；  
（3）创建1个centos主机资产，ip同jumpserver服务器ip，名称centos2，资产账号jumper，密码jumper，其他保持默认；  
（4）添加命令过滤规则，并配置不允许jumper账号执行rm命令实现文件删除；  
（5）将资产“centos2”分配给“ops02”用户，并将此规则命名为“centos2规则”，  
（6）使用“ops02”用户登录堡垒机，并使用Web Terminal登录该“centos2”资产，尝试用“rm”命令去删除，查看结果；  
（7）使用“admin”账户登录审计台，查看上述会话记录，并获取到“ops02”用户登录“centos2”资产的时间点以及执行的所有命令。

**3.**技能要求

（1）能通过堡垒机限制用户远程登录资产执行命令；   
（2）能通过堡垒机审计到用户对资产的历史操作命令；

**4.**质量指标

（1）正确启动堡垒机；   
（2）正确添加堡垒机账号；   
（3）正确添加资产；   
（4）正确关联资产与堡垒机账号；   
（5）堡垒机命令过滤规则配置正确；   
（6）堡垒机资产登陆和审计操作正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：通过堡垒机实现资产运维命令过滤和审计

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确启动堡垒机； | 根据数据 |  |  |
| M2 | 2 | 普通用户创建正确，用户名正确得1分，密码选项正确得1分； | 根据数据 |  |  |
| M3 | 2 | 堡垒机资产添加正确，ip正确得1分，名称正确得1分； | 根据数据 |  |  |
| M4 | 2 | 堡垒机资产账号添加； | 根据数据 |  |  |
| M5 | 2 | 堡垒机授权规则配置正确； | 根据数据 |  |  |
| M6 | 2 | 堡垒机命令过滤规则配置正确，指定账号正确得0.5分，过滤类型正确得0.5分，过滤内容正确得1分； | 根据数据 |  |  |
| M7 | 2 | 堡垒机资产登陆和审计操作正确，使用ops02登陆centos2资产得0.5分，使用rm命令得0.5分，审计后台得到上述操作记录得1分; | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置堡垒机以控制Windows资产文件传输

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）JumpSeryer系统。

**2.**工作任务

在某公司内网中有一系列的服务器，Windows服务器居多。现希望通过堡垒机统一管理这些服务器，实现运维操作和文件传输管控，并对这些操作进行审计。JumpServer已经安装在CentOS虚拟机上，作为堡垒机服务器。具体操作要求如下：  
（1）启动JumpServer服务，登陆JumpServer，用户名admin密码Sjtu@1896；  
（2）创建堡垒机用户，用户名为“ops03”,邮箱为“ops03@jumpserver.cn”,使用密码“admin@123”，角色为“用户”，其他保持默认；  
（3）创建1个windows2016主机资产，ip同当前浏览器ip，名称windows2016，资产账号jumper，密码jumper，协议组仅保留远程桌面；  
（4）将资产“windows2016”分配给“ops03”用户，并将此规则命名为“windows2016规则”，  
（5）使用“ops03”用户登录堡垒机，并向Windows资产传输一个文件；  
（6）使用“admin”账户登录审计台，查看上述会话记录，并获取到“ops03”用户登录“windows2016”资产的时间点以及所有操作。

**3.**技能要求

（1）能通过堡垒机控制用户对资产的登陆和文件传输权限；   
（2）能通过堡垒机审计到用户对资产的历史操作；

**4.**质量指标

（1）堡垒机初始化启动正确；   
（2）堡垒机用户创建正确；   
（3）堡垒机资产添加正确；   
（4）堡垒机授权规则配置正确；   
（5）堡垒机文件传输操作正确；   
（6）堡垒机审计操作使用正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置堡垒机以控制Windows资产文件传输

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确启动堡垒机； | 根据数据 |  |  |
| M2 | 2 | 堡垒机用户创建正确，用户名正确得1分，密码选项正确得1分； | 根据数据 |  |  |
| M3 | 3 | 堡垒机资产添加正确，ip正确得1分，名称正确得1分，协议组正确得1分； | 根据数据 |  |  |
| M4 | 1 | 堡垒机资产账号添加正确； | 根据数据 |  |  |
| M5 | 2 | 堡垒机授权规则添加正确； | 根据数据 |  |  |
| M6 | 1 | ops03账号远程登陆windows； | 根据数据 |  |  |
| M7 | 1 | ops03账号传输一个文件； | 根据数据 |  |  |
| M8 | 2 | 堡垒机审计操作使用正确； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：无线网络接入安全管理

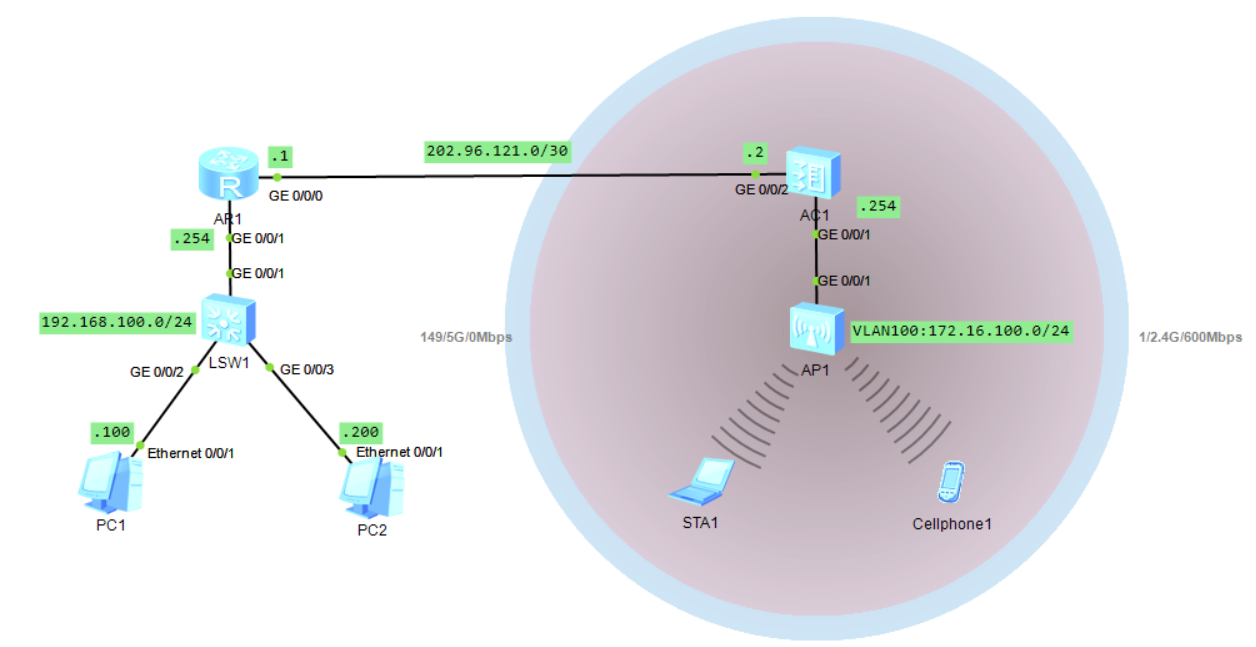
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络架构图如图1所示，因安全需求，对无线接入设备做安全管理。作为公司的IT工程师，请打开考题三级-2.1.4.paper，完成以下任务：  
（1）按图1信息配置AR1到右侧网络和AC1到左侧网络的缺省路由；  
（2）配置无线AC的攻击检测功能，开启WPA2-PSK认证方式的暴力破解密钥攻击检测功能和泛洪攻击检测功能；  
（3）配置无线AC的配置WPA2-PSK认证方式的暴力破解密钥攻击检测的检测周期为70秒，检测周期内允许密钥错误的次数为25次，静默时间为700秒（此处的wids profile文件名为wlan-wids）。  
（4）配置泛洪攻击检测的检测周期为70秒，泛洪攻击检测阈值为350个，静默时间为700秒。  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。



**3.**技能要求

（1）能配置路由器和无线设备的路由信息；   
（2）能配置无线设备的攻击检测功能。

**4.**质量指标

（1）路由器和无线AC的路由信息正确；   
（2）无线AC的暴力破解密钥攻击检测功能配置正确；   
（3）无线AC的泛洪攻击检测功能配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：无线网络接入安全管理

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 路由器的缺省路由正确； | 根据数据 |  |  |
| M2 | 2 | 无线AC的缺省路由配置正确； | 根据数据 |  |  |
| M3 | 2 | 无线AC的射频0上启用WPA2-PSK认证方式的暴力破解密钥攻击检测功能正确； | 根据数据 |  |  |
| M4 | 1 | 无线AC的射频0上启用泛洪攻击检测功能正确； | 根据数据 |  |  |
| M5 | 1 | 无线AC的射频1上启用WPA2-PSK认证方式的暴力破解密钥攻击检测功能正确； | 根据数据 |  |  |
| M6 | 1 | 无线AC的射频1上启用泛洪攻击检测功能正确； | 根据数据 |  |  |
| M7 | 1 | WPA2-PSK认证方式的暴力破解密钥攻击检测的检测周期配置正确； | 根据数据 |  |  |
| M8 | 1 | 检测周期内允许密钥错误的次数配置正确； | 根据数据 |  |  |
| M9 | 1 | 静默时间配置正确； | 根据数据 |  |  |
| M10 | 1 | 泛洪攻击检测的检测周期配置正确； | 根据数据 |  |  |
| M11 | 1 | 泛洪攻击检测阈值正确； | 根据数据 |  |  |
| M12 | 1 | 泛洪攻击检测静默时间配置正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：防火墙远程访问安全管理

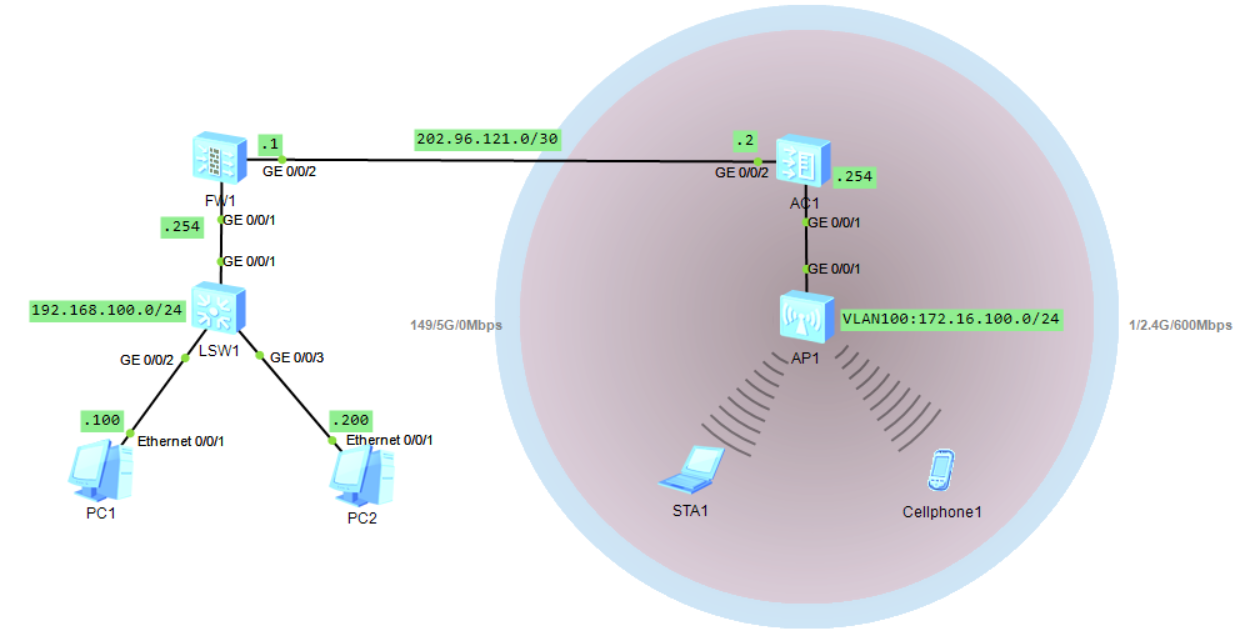
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）eNSP仿真软件。

**2.**工作任务

某公司的网络架构图如图1所示，因安全需求，利用防火墙（登录用户admin，密码Admin@1234）对接入设备做安全管理。作为公司的IT工程师，请打开考题三级-2.1.5.paper，完成以下任务：  
（1）按图1信息配置FW1到右侧网络和AC1到左侧网络的缺省路由；  
（2）配置FW1的每IP新建连接限速功能，用于内网防护，配置源会话限制为500，目标会话限制为1000，源会话防护模式为丢弃模式，目标会话防护模式也为丢弃模式；  
（3）在FW1的两个接口上启用会话限制；  
（4）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1  
注意：各设备的IP基础信息请保持跟图1一致，请勿修改网络设备的密码。



**3.**技能要求

（1）能配置路由器和无线设备的路由信息；   
（2）能配置无线设备的攻击检测功能。

**4.**质量指标

（1）路由器和无线AC的路由信息正确；   
（2）无线AC的暴力破解密钥攻击检测功能配置正确；   
（3）无线AC的泛洪攻击检测功能配置正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：防火墙远程访问安全管理

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 防火墙的缺省路由正确； | 根据数据 |  |  |
| M2 | 2 | 无线AC的缺省路由配置正确； | 根据数据 |  |  |
| M3 | 2 | FW1的内网防护源会话限制正确； | 根据数据 |  |  |
| M4 | 2 | 目标会话限制正确； | 根据数据 |  |  |
| M5 | 2 | 源会话防护模式正确； | 根据数据 |  |  |
| M6 | 2 | 目标会话防护模式正确； | 根据数据 |  |  |
| M7 | 2 | G0/0/0接口会话限制启用正确； | 根据数据 |  |  |
| M8 | 1 | G1/0/0接口会话限制启用正确。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：配置Linux审计日志

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

假设你正在管理一台 CentOS 服务器，需要确保服务器的安全性。作为安全措施的一部分，你需要配置 Auditd 来监控特定的系统活动，以便及时发现任何可疑行为。  
任务：  
（1）启动 Auditd 服务并设置其开机自启；  
（2）创建一个规则来监控 /etc/test/auditd\_test 文件上的所有写入操作，并给这些审计记录加上标签 file\_access；  
（3）设置审计日志保存在/etc/test/audit/audit.log；  
（4）设置审计日志的滚动机制，日志文件数目10，当文件大小超过 5MB 时进行滚动；  
（5）尝试修改/etc/test/auditd\_test，搜索审计日志，验证上述操作是否被正确记录。

**3.**技能要求

（1）能启动Centos审计服务Auditd；   
（2）能添加Centos审计规则；   
（3）能修改Centos审计配置；   
（4）能查询Centos审计结果。

**4.**质量指标

（1） 正确启动Centos审计工具Auditd；   
（2） 正确添加Centos审计规则；   
（3） 正确修改Centos审计配置；   
（4）正确查询Centos审计结果。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：配置Linux审计日志

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 正确启动 Auditd 服务并设置开机自启，启动Auditd得1分，开机自启得1分； | 根据数据 |  |  |
| M2 | 3 | 正确创建一个规则来监控 /etc/test/auditd\_test 文件上的所有写入操作，监视目录正确得1分，监视权限正确得1分，关键字标签正确得1分； | 根据数据 |  |  |
| M3 | 2 | 正确设置审计日志保存位置； | 根据数据 |  |  |
| M4 | 6 | 正确配置审计日志的滚动机制，设置滚动正确得2分，设置日志最大文件正确得2分，设置最多保留日志文件数得2分； | 根据数据 |  |  |
| M5 | 2 | 验证审计日志得2分； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows远程桌面访问安全配置

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司正在管理一台Windows服务器，这台服务器上运行着远程桌面服务，用于方便管理员进行远程管理。为了增强安全性并遵循最佳实践，  
决定对远程桌面服务进行一系列的安全配置。  
（1）创建一个新的管理员组用户：名为zg，该用户具有管理员权限。修改本地策略，zg的组不允许执行远程关机或重启系统的操作；  
（2）设置远程桌面会话主机安全：要求使用TLS1.0对会话主机服务器进行身份验证，客户端与服务器之间传送的数据使用128位强加密，远程桌面服务是否始终提示客户端连接时需要密码；  
（3）用命令行方式，更改特定文件的权限：将C:\Windows\System32\compmgmt.msc文件的所有权更改为Administrators。

**3.**技能要求

（1） 能创建用户，隶属于管理员组；   
（2） 能设置安全策略，使用户不能远程关机或重启系统；   
（3） 能配置桌面主机会话的安全层协议；   
（4） 能更改控制面板类文件所有者。

**4.**质量指标

（1）正确创建管理员组用户；   
（2）正确设置安全策略，使用户不能远程关机或重启系统；   
（3）正确设置远程桌面主机会话的安全层协议配置为 SSL，加密级别为高；   
（4）正确修改控制面板类文件所有者。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows远程桌面访问安全配置

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确创建用户zg得1分，隶属管理员组得2分； | 根据数据 |  |  |
| M2 | 3 | 正确设置安全策略，使zg用户不能远程关机或重启系统； | 根据数据 |  |  |
| M3 | 2 | 正确设置远程桌面主机会话的安全层协议配置为SSL； | 根据数据 |  |  |
| M4 | 2 | 正确设置远程桌面主机会话的安全始终在连接时提示输入密码； | 根据数据 |  |  |
| M5 | 2 | 设置客户端连接加密级别高等级； | 根据数据 |  |  |
| M6 | 3 | 正确修改c:\windows\system32\compmgmt.msc文件的所有者为Administrator | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows系统数据备份和还原

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某企业为了防止文件意外丢失，使用Windows备份服务对数据进行备份。要求企业安全技术人员能够安装Windows Server Backup服务，并完成以下备份和还原任务：  
（1）安装Windows Server Backup；  
（2）对D:\documents文件夹做一次完整备份，保存在C盘。以上操作在确认页，截图保存至d:\kaoshi\_3\2.2.3-1.png；  
（3）设置每天20：00对D:\documents文件夹进行一次完整备份,保存在C盘。以上操作在确认页，截图保存至d:\kaoshi\_3\2.2.3-2.png  
（4）通过任务计划把上述每天20：00备份改成每周六10：00进行备份。截图保存至d:\kaoshi\_3\2.2.3-3.png  
（5）利用之前C盘生成的备份文件恢复D:\documents文件夹中的内容，并生成副本保存在原来的位置。在恢复确认页，截图保存至d:\kaoshi\_3\2.2.3-4.png；

**3.**技能要求

（1） 能对要求的文件进行一次性完整备份；   
（2） 能对要求的文件进行计划备份；   
（3） 能根据备份文件进行文件还原。

**4.**质量指标

（1）正确配置一次性完整备份；   
（2）正确配置每天的计划备份；   
（3）正确配置每周的计划备份；   
（4）正确配置文件还原。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows系统数据备份和还原

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | 正确安装Windows Server Backup； | 根据数据 |  |  |
| M2 | 3 | 设置一次完整备份，正确设置备份项目得1分，正确设置备份目标得1分，正确设置备份类型为完整得1分； | 根据数据 |  |  |
| M3 | 4 | 设置备份计划，正确设置备份项目得1分，正确设置备份目标得1分，正确设置备份类型为完整得1分，正确设置备份时间得1分； | 根据数据 |  |  |
| M4 | 2 | 修改备份计划，正确设置每周六得1分，正确设置10点得1分； | 根据数据 |  |  |
| M5 | 3 | 备份恢复，正确设置备份来源得1分，正确设置恢复项目得1分，正确设置恢复目标得1分； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Linux 系统日志管理

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

在一个大型企业内部，使用CentOS中的rsyslog作为主要的日志处理工具，负责收集、过滤和转发来自各个系统和应用程序的日志信息。随着业务规模的不断扩大和系统环境的日益复杂，公司对日志管理的效率和安全性提出了更高的要求。希望通过修改配置文件rsyslog.conf和logrotate.conf实现以下任务：  
（1）统一日志记录：将用户程序产生的error级别日志、邮件系统产生的alert级别日志以及内核产生的debug级别日志统一记录到/var/log/secure文件中，以便于集中管理和分析；  
（2）日志保留策略：为了合理利用存储资源并满足合规性要求，公司规定日志文件的保留时间不得超过50天，轮转后的旧日志文件将被压缩以节省空间，如果日志文件不存在不会产生错误信息；  
（3）安全日志同步：为了确保日志数据在传输过程中的完整性和保密性，公司决定采用TCP协议进行日志同步，并将日志实时转发到位于内网中的另一台日志服务器（IP地址为192.168.1.100），以便进行进一步的分析和备份。

**3.**技能要求

（1）能对Linux系统中不同设备不同级别的日志进行记录；   
（2）能设置日志的留存时间；   
（3）能进行日志同步。

**4.**质量指标

（1）正确配置日志服务；   
（4）正确设置日志留存时间；   
（5）正确配置日志同步。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Linux 系统日志管理

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 3 | rsyslog.conf配置，user.error路径配置正确得1分，mail.alert路径配置正确得1分，kern.debug路径配置正确得1分； | 根据数据 |  |  |
| M2 | 2 | logrotate.conf文件存在日志保留策略/var/log/secure； | 根据数据 |  |  |
| M3 | 6 | 日志保留策略配置正确，包含daily得2分、 rotate 50得2分、 compress得2分 、missingok得2分； | 根据数据 |  |  |
| M4 | 2 | rsyslog.conf配置启用TCP协议； | 根据数据 |  |  |
| M5 | 2 | rsyslog.conf配置日志服务器； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows系统日志管理

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

企业安全技术人员需要对Windows Server系统中的日志进行管理和分析，具体要求如下：   
（1）在计算机策略中，启用安装程序的日志记录，并且配置日志大小最大10M，日志存储位置为D:\kaoshi\_3\2.2.5\；  
（2）查询安全日志中登录失败的日志信息，并导出保存在D:\kaoshi\_3\2.2.5\fail.txt文件中；  
（3）查询应用程序日志中事件级别为“警告”的日志信息，并导出保存在D:\kaoshi\_3\2.2.5\app\_warning.txt文件中。

**3.**技能要求

（1）能设置日志安全策略；   
（2）能根据要求筛选不同类别的日志中的事件；   
（3）能保存筛选出的日志。

**4.**质量指标

（1）正确启用日志记录；   
（2）正确设置日志最大大小；   
（3）正确查询安全日志中登录失败的日志信息；   
（4）正确查询应用程序日志中事件级别为“警告”的日志；   
（5）正确保存筛选出的日志

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows系统日志管理

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 启用安装程序的日志记录； | 根据数据 |  |  |
| M2 | 4 | 正确配置日志大小得2分，正确日志存储位置得2分； | 根据数据 |  |  |
| M3 | 3 | 在事件查看器中，筛选安全日志中登录失败的日志信息； | 根据数据 |  |  |
| M4 | 2 | 登录失败的日志信息保存为D:\kaoshi\_3\2.2.5\fail.txt； | 根据数据 |  |  |
| M5 | 2 | 在事件查看器中，筛选应用程序日志中事件级别为“警告”的日志； | 根据数据 |  |  |
| M6 | 2 | 应用程序日志中事件级别为“警告”的日志,全选保存为D:\kaoshi\_3\2.2.5\app\_warning.txt； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Nginx Web服务器安全加固

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

Nginx是Centos上常用的web服务软件，为增强 Nginx Web 服务器的安全性，防止版本号、项目代码编写语言等信息泄露，需要对其进行安全管理，具体要求如下：  
（1）启动Nginx服务，确保NGINX服务能够在CentOS系统上正常启动并运行；  
（2）隐藏站点 Response Header 里的Web服务版本信息；  
（3）隐藏站点 Response Header 里的X-Powered-By 字段；  
（4）Nginx访问日志存放位置修改为/opt/bak/access.log；  
（5）屏蔽IP为192.168.X.X网段的访问请求；  
（6）启用SSL/TLS，为站点配置HTTPS访问。假设SSL证书路径为/etc/nginx/ssl/site.crt，SSL私钥路径为/etc/nginx/ssl/site.key；  
完成所有配置后，提交NGINX配置文件nginx.conf。

**3.**技能要求

（1）能基本操作Nginx；   
（2）能对Nginx进行安全管理；   
（3）能对Nginx进行日志管理。   
（4）能配置IP访问限制；   
（5）能为Nginx站点启用SSL/TLS。

**4.**质量指标

（1）正确启动Nginx服务；   
（2）正确隐藏Nginx的关键信息；   
（3）访问日志正确备份至指定目录。   
（4）正确配置IP访问限制；   
（5）正确启用SSL/TLS，并确保站点能通过HTTPS访问。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Nginx Web服务器安全加固

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Nginx服务已启动； | 根据数据 |  |  |
| M2 | 4 | 正确隐藏站点Response Header，隐藏Web服务版本信息得2分，隐藏X-Powered-By 字段得2分； | 根据数据 |  |  |
| M3 | 2 | 正确配置在Nginx访问日志存放路径； | 根据数据 |  |  |
| M4 | 2 | 正确屏蔽IP段； | 根据数据 |  |  |
| M5 | 1 | 正确配置HTTPS监听443端口； | 根据数据 |  |  |
| M6 | 4 | 正确配置SSL证书和私钥位置，证书位置正确得2分；私钥位置正确得2分； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Nginx Web 防攻击消息过滤

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

在公司网络中，Nginx作为常用的Web服务器软件，需要对其进行安全加固，以防止恶意请求和攻击行为，确保服务器稳定运行并有效记录访问日志。为此，需要对Nginx服务器的访问消息进行过滤和日志管理。具体要求如下：  
（1）启动Nginx服务，确保NGINX服务能够在CentOS系统上正常启动并运行；  
（2）仅允许 Get 和 Post 通过，拒绝其它类型的请求，返回错误代码405；  
（3）屏蔽固定IP（192.168.6.12）的访问请求，返回错误代码403；  
（4）Nginx访问日志存放位置修改为/opt/bak/access.log；  
（5）配置Nginx限制访问频率，防止DoS攻击。定义一个名称为one，大小为10m的存储区域，用于存储请求速率信息。每个IP地址每秒最多允许1个请求。允许在短时间内超过速率限制的请求个数为5。当请求超过速率限制时，立即返回错误，而不是延迟处理；  
（6）设置一个自定义的404错误页面，假设错误页面路径为/usr/share/nginx/html/error.html；  
完成所有配置后，提交NGINX配置文件nginx.conf。

**3.**技能要求

（1）能基本操作Nginx；   
（2）能对Nginx进行消息屏蔽操作；   
（3）能对Nginx进行日志管理。   
（4）能配置访问频率限制；   
（5）能设置自定义错误页面。

**4.**质量指标

（1）正确启动Nginx服务；   
（2）仅允许GET和POST请求通过；   
（3）屏蔽固定IP（192.168.6.12）的访问请求；   
（4）访问日志正确备份至指定目录。   
（5）正确配置访问频率限制；   
（6）设置自定义404错误页面并能正确显示。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Nginx Web 防攻击消息过滤

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Nginx服务已启动； | 根据数据 |  |  |
| M2 | 2 | 正确设置允许Get通过得1分，正确设置允许Post通过得1分； | 根据数据 |  |  |
| M3 | 3 | 正确屏蔽IP得2分，返回错误代码得1分； | 根据数据 |  |  |
| M4 | 2 | 正确配置在Nginx访问日志存放路径； | 根据数据 |  |  |
| M5 | 4 | 限制访问频率，防止DoS攻击。正确配置存储区域得1分，每个IP每秒请求数得1分，短时间内超过速率得请求个数得1分，超过速率限制时不延时处理得1分； | 根据数据 |  |  |
| M6 | 2 | 正确配置404错误页面； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Nginx Web服务器SSL/TLS加密

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

Nginx是Linux上常用的web服务软件，为增强 Nginx Web 服务器的安全性，提升通信隐私保护能力，需要修改nginx.conf对其进行安全加密配置，具体要求如下：  
（1）启动Nginx服务，确保NGINX服务能够在CentOS系统上正常启动并运行；  
（2）Nginx访问日志存放位置修改为/opt/bak/access.log；  
（3）配置NGINX使用SSL/TLS（安全套接层/传输层安全）加密。假设SSL证书路径为/etc/nginx/ssl/site.crt，SSL私钥路径为/etc/nginx/ssl/site.key；  
（4）配置SSL支持的协议版本为TLSv1.2 TLSv1.3，加密算法为HIGH:!aNULL:!MD5，Nginx优先使用服务器提供的加密套件列表中的选项，配置SSL会话缓存大小10M，会话缓存的有效期为20分钟；  
（5）配置HTTP访问跳转到HTTPS访问,返回响应码301；  
完成所有配置后，提交NGINX配置文件nginx.conf。

**3.**技能要求

（1）能基本操作Nginx；   
（2）能对Nginx进行安全加密管理；   
（3）能对Nginx进行日志管理；   
（4）能配置HTTP跳转到HTTPS；   
（5）能配置HSTS策略。

**4.**质量指标

（1）正确启动Nginx服务；   
（2）SSL/TLS加密正确配置；   
（3）访问日志正确备份至指定目录；   
（4）配置HTTP跳转到HTTPS。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Nginx Web服务器SSL/TLS加密

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Nginx服务已启动； | 根据数据 |  |  |
| M2 | 2 | 正确配置在Nginx访问日志存放路径； | 根据数据 |  |  |
| M3 | 2 | 正确配置SSL证书和私钥位置，证书位置正确得1分；私钥位置正确得1分； | 根据数据 |  |  |
| M4 | 2 | 正确配置HTTPS监听443端口； | 根据数据 |  |  |
| M5 | 5 | 正确配置SSL，配置SSL版本得1分，配置加密算法得1分，配置使用服务器提供的加密套件列表中的选项得1分，配置SSL会话缓存得1分，配置缓存有效期得1分； | 根据数据 |  |  |
| M6 | 2 | 正确配置HTTP转向HTTPS，响应码正确得1分，跳转正确得1分； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：邮件服务器配置垃圾邮件过滤

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

假设您正在负责配置一个hMailServer实例以处理垃圾邮件。请根据以下要求完成配置：  
（1）配置在垃圾邮件消息中添加自定义头，以便其他邮件服务器或客户端可以识别这些消息。配置在垃圾邮件消息中添加一个头，用来标记设为垃圾邮件的原因。设置一个阈值，当垃圾邮件的得分达到此阈值时，将自动删除该邮件，阈值设置为40。配置仅扫描小于或等于特定大小的邮件以查找垃圾邮件特征。请将最大邮件大小设置为4096KB；  
（2）启用SPF检查，以验证发件人的IP地址是否与其域名允许的IP地址匹配。检查发件人电子邮件地址中的域名是否具有DNS-MX记录。验证DKIM签名头，以确保邮件来自可信的发件人；  
（3）启用灰名单功能，暂时拒绝首次尝试向服务器发送的邮件。首次尝试发送邮件的服务器将被暂时拒绝60分钟。设置一个天数，对于已经成功通过灰名单检查的邮件，其灰名单记录将在36天后由 hMailServer 自动移除。对于未被确认为有效发件人的记录，这些记录将在10天后由 hMailServer 自动移除；  
（4）启用DNS黑名单功能，设置DNS黑名单服务器的地址为111.111.111.111；

**3.**技能要求

（1）能对邮件服务器的反垃圾邮件功能做配置；   
（2）能配置邮件服务器中的DNS黑名单；   
（3）能配置邮件服务器的灰名单功能。

**4.**质量指标

（1）正确配置邮件服务器的反垃圾邮件功能；   
（2）正确配置邮件服务器的DNS黑名单功能；   
（3）正确配置邮件服务器的灰名单功能

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：邮件服务器配置垃圾邮件过滤

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 添加自定义垃圾邮件头； | 根据数据 |  |  |
| M2 | 1 | 添加拒绝原因头； | 根据数据 |  |  |
| M3 | 1 | 设置垃圾邮件删除阈值40； | 根据数据 |  |  |
| M4 | 1 | 设置扫描的最大邮件大小4096； | 根据数据 |  |  |
| M5 | 1 | 启用SPF检查； | 根据数据 |  |  |
| M6 | 1 | 启用检查发件人具有DNS-MX记录； | 根据数据 |  |  |
| M7 | 1 | 启用验证DKIM签名头； | 根据数据 |  |  |
| M8 | 2 | 启用灰名单功能； | 根据数据 |  |  |
| M9 | 1 | 设置邮件传递延迟时间； | 根据数据 |  |  |
| M10 | 1 | 设置移除已使用记录的天数； | 根据数据 |  |  |
| M11 | 1 | 设置移除未使用记录的天数； | 根据数据 |  |  |
| M12 | 2 | 启用DNS黑名单功能； | 根据数据 |  |  |
| M13 | 1 | 设置DNS主机111.111.111.111； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：vsftp日志管理审计

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

作为一名系统管理员，你需要配置/etc/vsftpd/vsftpd.conf文件，增加vsftpd的日志功能，以便追踪和监控FTP服务器的活动。  
（1）启用传输日志，确保vsftpd记录所有传输的详细信息，传输日志存储在/log/vsftpd.log；  
（2）为了确保日志的一致性和可读性，请使用标准的日志格式记录传输信息；  
（3）为了调试和安全目的，请记录FTP协议的所有活动；  
（4）为了增加日志的冗余性，请同时启用标准传输日志和安全日志；  
（5）请确保vsftpd不使用系统日志记录FTP事件；  
（6）请禁用日志锁定功能，以避免在高并发情况下可能出现的日志锁定问题；  
（7）对已经存在的/etc/test/vsftpd.log日志文件进行筛选操作，筛选出Failed password事件存入/log/failed.log。

**3.**技能要求

（1）能启用vsftpd的日志功能；   
（2）能对vsftpd的日志进行管理配置；   
（3）能对vsftpd日志进行筛选审计；

**4.**质量指标

（1）正确启用vsftpd的日志功能；   
（2）正确设置vsftpd的日志配置项；   
（3）日志结果筛选正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：vsftp日志管理审计

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 正确启用传输日志； | 根据数据 |  |  |
| M2 | 2 | 正确配置传输日志文件的位置； | 根据数据 |  |  |
| M3 | 2 | 正确配置标准的日志格式； | 根据数据 |  |  |
| M4 | 2 | 正确配置记录FTP协议的所有活动； | 根据数据 |  |  |
| M5 | 2 | 正确配置启用双重日志记录； | 根据数据 |  |  |
| M6 | 2 | 正确配置不使用系统日志记录FTP事件； | 根据数据 |  |  |
| M7 | 2 | 正确配置禁用日志锁定功能； | 根据数据 |  |  |
| M8 | 2 | 正确筛选出Failed password事件存入/log/failed.log； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：运用防火墙来监控数据流量、识别攻击特征

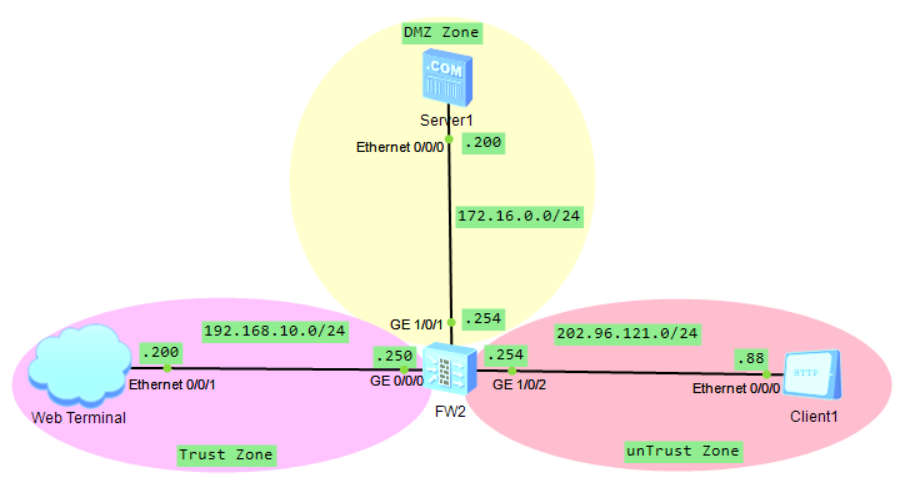
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

某公司因业务扩大，公司管理层越来越重视信息安全，决定对公司的内外交互数据中的DNS恶意行为实施监控管理，如图1所示，作为公司的IT安全工程师，打开3.1.1.paper后需要完成以下任务：  
（1）启动图中所有设备，并登录FW2的web管理界面（登录用户admin，密码Admin@1234,请勿修改密码），完成防火墙接口的IP配置，具体信息如图所示；  
（2）为了保护内部服务器Server1的数据安全，请在防火墙上添加安全策略，该策略能够保证数据的正常通信和监控；（策略名为untrust2dmz，源安全区域为untrust，目的安全区域为dmz，动作为允许，启用记录流量日志、记录命中策略日志、记录会话日志三项功能，其它设置默认；）  
（3）为了预防针对DNS协议的恶意行为，请在防火墙的安全策略里调用入侵防御的安全配置文件；（配置文件名为anti1，签名过滤器名为filter1，过滤器的对象、严重性、操作系统、应用程序、协议、威胁类别默认全部选中，动作设置为阻断；协议异常检测中针对DNS协议做相应的限制，防止DNS的恶意请求，DNS域名最大检测长度为6，DNS会话最大请求次数为3；）  
（4）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能通过web页面管理防火墙；   
（2）能配置防火墙的安全策略；   
（3）能配置防火墙的入侵防御功能；

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）防火墙安全策略配置正确；   
（3）防火墙安全配置文件添加并引用正确；   
（4）服务器的服务启动正确；   
（5）配置文件保存正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：运用防火墙来监控数据流量、识别攻击特征

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | 防火墙GE1/0/1接口IP为172.16.0.254/24； | 根据数据 |  |  |
| M2 | 2 | 防火墙GE1/0/2接口IP为202.96.121.254/24； | 根据数据 |  |  |
| M3 | 1 | 安全策略untrust2dmz添加成功，源安全区域为untrust； | 根据数据 |  |  |
| M4 | 1 | 目的安全区域为dmz； | 根据数据 |  |  |
| M5 | 1 | 记录流量日志； | 根据数据 |  |  |
| M6 | 1 | 命中策略日志； | 根据数据 |  |  |
| M7 | 1 | 会话日志功能打开； | 根据数据 |  |  |
| M8 | 1 | 签名过滤器filter1添加成功，操作系统全部选中； | 根据数据 |  |  |
| M9 | 1 | 签名过滤器filter1的对象、严重性、操作系统、应用程序、协议、威胁类别全部选中； | 根据数据 |  |  |
| M10 | 1 | 动作为阻断； | 根据数据 |  |  |
| M11 | 1 | Dns协议异常检测中域名最大检测长度为6； | 根据数据 |  |  |
| M12 | 1 | Dns协议异常检测中会话最大请求次数为3； | 根据数据 |  |  |
| M13 | 1 | 安全策略untrust2dmz的内容安全部分调用anti1 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：网络流量监控与信息过滤

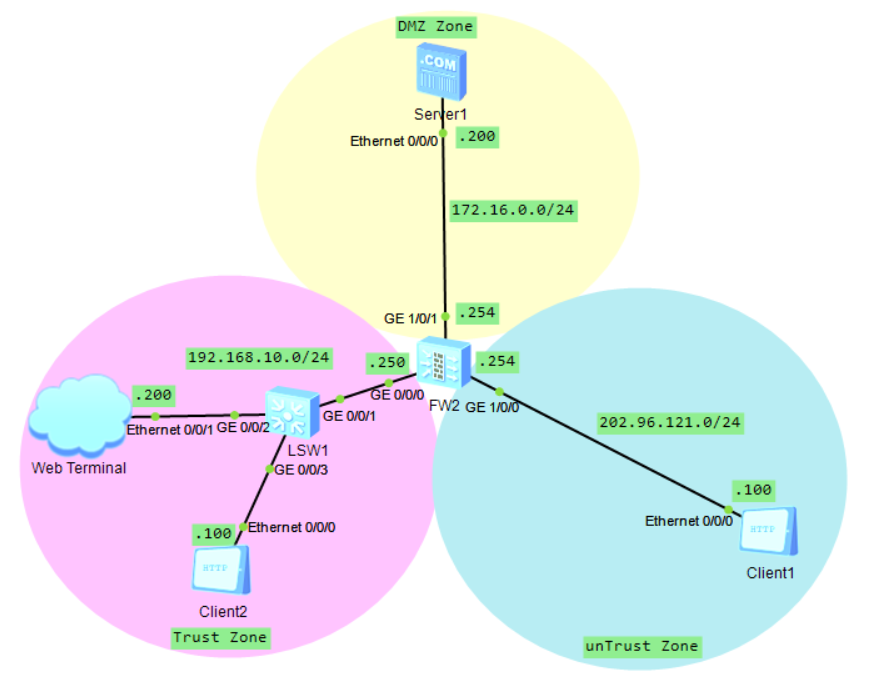
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

某公司因业务扩大，公司管理层越来越重视信息安全，决定对公司的内外交互数据中的数据流量实施监控管理，以及时发现攻击行为并阻止，如图1所示，作为公司的IT安全工程师，请打开3.1.2.paper后需要完成以下任务：  
（1）使用web界面登录FW2（登录用户admin，密码Admin@1234,请勿修改密码），完成防火墙G1/0/0和G1/0/1接口的IP配置，具体信息如图所示；  
（2）在FW2上创建安全策略Block\_Host，阻断IP地址为192.168.10.100/24的主机所有出站流量，同时再创建安全策略Permit\_Host允许该网段内的其它主机；  
（3）在安全策略Permit\_Host中调用反病毒、URL过滤、DNS过滤三项内容安全配置文件，三项内容安全使用默认配置文件，以此来监控并过滤指定的受限流量；  
（4）在FW2的G0/0/0接口上启动数据抓包功能，将来自192.168.10.100主机到Server1的ping包流量导出到D:\kaoshi\_3\，保存类型默认。  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能通过web页面管理防火墙；   
（2）能配置防火墙接口IP地址；   
（3）能创建并应用安全策略；   
（4）能配置入侵检测规则；   
（5）能利用工具进行抓包分析。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）安全策略正确创建并生效；   
（3）配置文件调用正确；   
（4）抓包结果导出正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：网络流量监控与信息过滤

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 防火墙GE1/0/1接口IP为172.16.0.254/24； | 根据数据 |  |  |
| M2 | 1 | 防火墙GE1/0/0接口IP为202.96.121.254/24； | 根据数据 |  |  |
| M3 | 1 | G1/0/0接口加入untrust区域； | 根据数据 |  |  |
| M4 | 1 | G1/0/1接口加入dmz区域； | 根据数据 |  |  |
| M5 | 2 | 安全策略Block\_Host创建正确，源IP地址为192.168.10.100，目标IP地址为所有，动作为禁止； | 根据数据 |  |  |
| M6 | 2 | 安全策略Permit\_Host创建正确，源IP地址为192.168.10.0/24网段，目前IP地址为所有，动作为允许； | 根据数据 |  |  |
| M7 | 1 | 安全策略Permit\_Host调用了默认的反病毒配置文件； | 根据数据 |  |  |
| M8 | 2 | 安全策略Permit\_Host调用了默认的URL过滤配置文件； | 根据数据 |  |  |
| M9 | 2 | 安全策略Permit\_Host调用了默认的DNS过滤配置文件； | 根据数据 |  |  |
| M10 | 2 | 192.168.10.100到server1的ping包正确抓包并导出到D:\。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：网络安全策略部署与APT防御

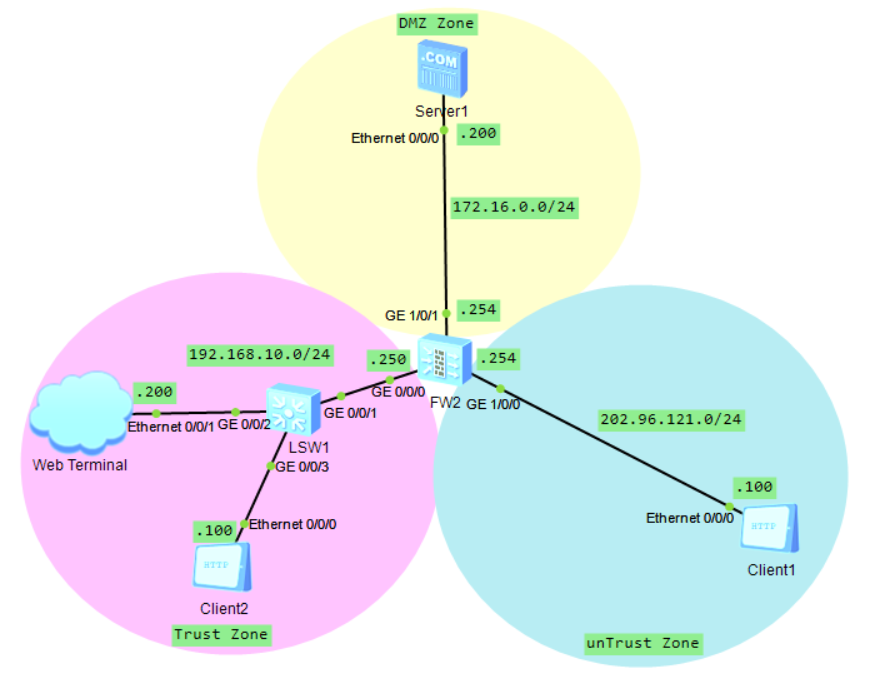
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

某公司近期遭受了多次网络攻击，为了提高网络安全防护能力，公司管理层决定加强网络安全策略的部署和审计工作。作为公司的IT安全工程师，请打开3.1.3.paper后需要完成以下任务：  
（1）使用web界面登录FW2（登录用户admin，密码Admin@1234,请勿修改密码），完成防火墙G1/0/0和G1/0/1接口的IP配置，具体信息如图所示；  
（2）在FW2上创建安全策略Block\_External，阻断来自特定IP地址202.96.121.100的所有入站流量到trust区域；  
（3）创建安全策略Permit\_Internal，允许公司内部网段192.168.10.0/24的所有出站流量，并记录详细流量和会话日志；  
（4）在安全策略Permit\_Internal中调用反病毒、APT防御两项内容安全的配置文件（反病毒、APT调用默认配置），确保这些策略能够正确应用并审计；  
（5）利用抓包工具对FW2的G1/0/0接口进行实时监控，审计并分析来自202.96.121.100的流量，生成审计报告（报告中必须包含流量内容、分析、建议三部分内容），并保存至D:\kaoshi\_3\审计报告.txt。  
（6）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能通过web页面管理防火墙；   
（2）能配置防火墙接口IP地址；   
（3）能创建并应用安全策略；   
（4）能配置内容安全策略；   
（5）能进行网络安全审计和分析。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）安全策略正确创建并生效；   
（3）内容安全策略正确调用并审计；   
（4）日志审计报告完整，分析准确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：网络安全策略部署与APT防御

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 防火墙GE1/0/1接口IP为172.16.0.254/24； | 根据数据 |  |  |
| M2 | 1 | 防火墙GE1/0/0接口IP为202.96.121.254/24； | 根据数据 |  |  |
| M3 | 1 | G1/0/0接口加入untrust区域； | 根据数据 |  |  |
| M4 | 1 | G1/0/1接口加入dmz区域； | 根据数据 |  |  |
| M5 | 2 | 安全策略Block\_External创建正确，源IP地址为202.96.121.100，目标IP地址为所有，动作为禁止； | 根据数据 |  |  |
| M6 | 2 | 安全策略Permit\_Internal创建正确，源IP地址为192.168.10.0/24网段，目前IP地址为所有，动作为允许； | 根据数据 |  |  |
| M7 | 1 | 安全策略Permit\_Internal启用了记录流量日志功能； | 根据数据 |  |  |
| M8 | 1 | 安全策略Permit\_Internal启用了记录会话日志功能； | 根据数据 |  |  |
| M9 | 2 | 安全策略Permit\_Internal调用了默认的反病毒配置文件； | 根据数据 |  |  |
| M10 | 2 | 安全策略Permit\_Internal调用了默认的APT防御配置文件； | 根据数据 |  |  |
| M11 | 1 | 来自202.96.121.100的审计报告正确，包含流量内容、分析和建议三部分。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：网络安全策略部署与DDoS攻击防范

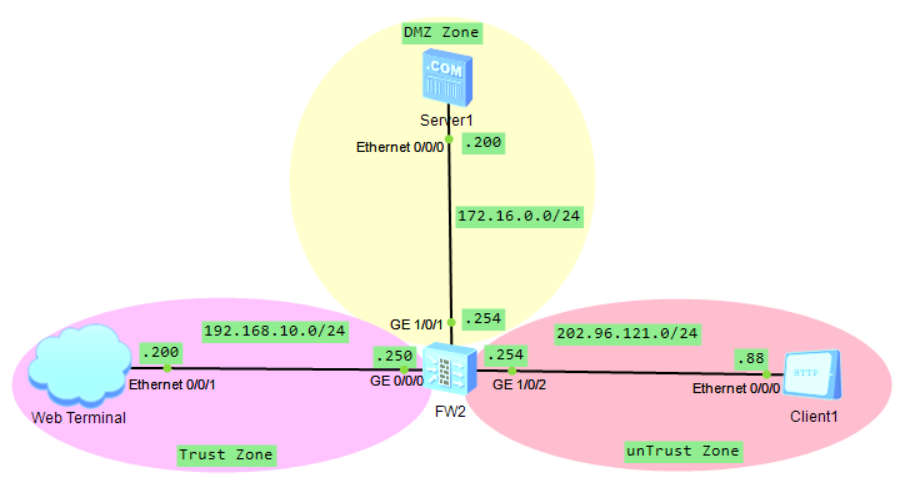
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

某公司因业务扩大，公司管理层越来越重视信息安全，决定对公司的内外交互数据中的DNS恶意行为实施监控管理，如图1所示，作为公司的IT安全工程师，打开3.1.4.paper后需要完成以下任务：  
（1）启动图中所有设备，并登录FW2的web管理界面（登录用户admin，密码Admin@1234,请勿修改密码），完成防火墙接口的IP配置，具体信息如图所示；  
（2）为了保护内部服务器Server1的数据安全，请在防火墙上添加安全策略，该策略能够保证数据的正常通信和监控；（策略名为untrust2dmz，源安全区域为untrust，目的安全区域为dmz，动作为允许，启用记录流量日志、记录命中策略日志、记录会话日志三项功能，其它设置默认；）  
（3）配置FW2的攻击防范，将IP地址和端口的最大扫描速率提高50%，黑名单的老化时间增加25%；将超大ICMP报文的最大长度降低50%；  
（4）在FW2的G1/0/2接口上启动数据抓包功能，将来自Client1到Server1的ping包流量导出到D:\kaoshi\_3\，保存类型默认；  
（5）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能通过web页面管理防火墙；   
（2）能配置防火墙的安全策略；   
（3）能配置防火墙的入侵防御功能；   
（4）能利用工具进行抓包分析。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）防火墙安全策略配置正确；   
（3）防火墙攻击防范设置正确；   
（4）抓包的结果导出正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：网络安全策略部署与DDoS攻击防范

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 防火墙GE1/0/1接口IP为172.16.0.254/24； | 根据数据 |  |  |
| M2 | 1 | 防火墙GE1/0/2接口IP为202.96.121.254/24； | 根据数据 |  |  |
| M3 | 1 | GE1/0/1加入dmz区域； | 根据数据 |  |  |
| M4 | 1 | GE1/0/2加入untrust区域； | 根据数据 |  |  |
| M5 | 1 | 安全策略添加成功，源安全区域为untrust； | 根据数据 |  |  |
| M6 | 1 | 目的安全区域为dmz； | 根据数据 |  |  |
| M7 | 1 | 记录流量日志； | 根据数据 |  |  |
| M8 | 1 | 命中策略日志； | 根据数据 |  |  |
| M9 | 1 | 会话日志功能打开； | 根据数据 |  |  |
| M10 | 1 | 攻击防范的IP地址扫描最大速率为6000包/秒； | 根据数据 |  |  |
| M11 | 1 | 黑名单老化时间为25分钟； | 根据数据 |  |  |
| M12 | 1 | 攻击防范的端口扫描最大速率为6000包/秒； | 根据数据 |  |  |
| M13 | 1 | 黑名单老化时间为25分钟； | 根据数据 |  |  |
| M14 | 1 | 超大ICMP报文的最大长度为2000字节； | 根据数据 |  |  |
| M15 | 1 | Client1到server1的ping包正确抓包并导出到D:\kaoshi\_3\； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：网络安全策略部署与邮件防护

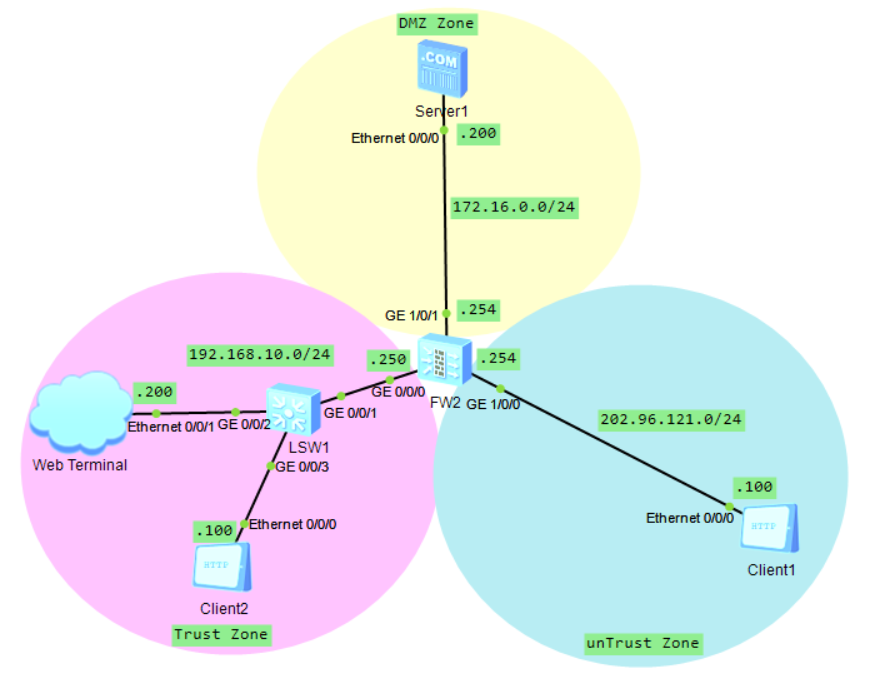
考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统；   
（4）eNSP仿真软件。

**2.**工作任务

某公司近期遭受了多次网络攻击，为了提高网络安全防护能力，公司管理层决定加强网络安全策略的部署和审计工作。作为公司的IT安全工程师，请打开3.1.5.paper后需要完成以下任务：  
（1）使用web界面登录FW2（登录用户admin，密码Admin@1234,请勿修改密码），完成防火墙G1/0/0和G1/0/1接口的IP配置，具体信息如图所示；  
（2）在FW2上创建安全策略Block\_External，阻断来自特定IP地址202.96.121.100的所有入站流量到trust区域；  
（3）创建安全策略Permit\_Internal，允许公司内部网段192.168.10.0/24的所有出站流量，并记录详细会话日志；  
（4）在安全策略Permit\_Internal中调用默认的反病毒和入侵防御内容安全的配置文件（mail\_server），确保这些策略能够正确应用并审计；  
（5）利用抓包工具对FW2的G1/0/1接口进行实时监控，审计并分析来自202.96.121.100的流量，生成审计报告（报告中必须包含流量内容、分析、建议三部分内容），并保存至D:\kaoshi\_3\审计报告.txt；  
（6）保存所有设备的配置，点击paper里的“交卷”，输入考生ID为“准考证号”，保存路径为“D:\kaoshi\_3\”，并生成答案文件。  
  
图1



**3.**技能要求

（1）能通过web页面管理防火墙；   
（2）能配置防火墙接口IP地址；   
（3）能创建并应用安全策略；   
（4）能配置内容安全策略；   
（5）能进行网络安全审计和分析。

**4.**质量指标

（1）防火墙接口IP配置正确；   
（2）安全策略正确创建并生效；   
（3）内容安全策略正确调用并审计；   
（4）日志审计报告完整，分析准确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：网络安全策略部署与邮件防护

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | 防火墙GE1/0/1接口IP为172.16.0.254/24； | 根据数据 |  |  |
| M2 | 1 | 防火墙GE1/0/0接口IP为202.96.121.254/24； | 根据数据 |  |  |
| M3 | 1 | G1/0/0接口加入untrust区域； | 根据数据 |  |  |
| M4 | 1 | G1/0/1接口加入dmz区域； | 根据数据 |  |  |
| M5 | 2 | 安全策略Block\_External创建正确，源IP地址为202.96.121.100，目标IP地址为所有，动作为禁止； | 根据数据 |  |  |
| M6 | 2 | 安全策略Permit\_Internal创建正确，源IP地址为192.168.10.0/24网段，目前IP地址为所有，动作为允许； | 根据数据 |  |  |
| M7 | 1 | 安全策略Permit\_Internal启用了记录会话日志功能； | 根据数据 |  |  |
| M8 | 2 | 安全策略Permit\_Internal调用了反病毒的内容安全配置文件； | 根据数据 |  |  |
| M9 | 2 | 安全策略Permit\_Internal调用了mail\_server的入侵防御配置文件； | 根据数据 |  |  |
| M10 | 2 | 来自202.96.121.100的审计报告正确，包含流量内容、分析和建议三部分。 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：识别系统异常状态并进行恢复

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；

**2.**工作任务

某公司的文件服务器疑似被恶意访问，导致服务器Server1目前处于性能和安全的不稳定状态，作为公司的IT安全工程师，需要完成以下任务来解决问题：  
（1）打开服务器的windows defender，对服务器进行快速扫描，如发现异常文件，执行隔离操作，并将隔离文件的信息存放至D:/kaoshi\_3/隔离记录.txt中；  
（2）调整服务器的用户账户控制级别为最高级别，确保所有设置更改会发出通知；  
（3）建立服务器的连接安全规则，保障数据通信安全，针对文件和打印共享（SMB-in）服务的入站访问，只允许安全连接，同时设置仅允许sales组、manager用户连接。

**3.**技能要求

（1）能使用系统的病毒与威胁防护功能；   
（2）能设置系统的账户控制功能；   
（3）能设置系统防火墙。

**4.**质量指标

（1）系统的病毒与威胁防护扫描正确；   
（2）用户账户控制设置正确；   
（3）防火墙入站规则设置正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：识别系统异常状态并进行恢复

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | windows defender快速扫描后的隔离记录D:\kaoshi\_3\隔离记录.txt存在； | 根据数据 |  |  |
| M2 | 2 | D:\kaoshi\_3\隔离记录.txt中的内容正确； | 根据数据 |  |  |
| M3 | 3 | 用户账户控制设置为最高级别； | 根据数据 |  |  |
| M4 | 2 | 防火墙高级设置里显示文件和打印共享（SMB-In）规则已启用； | 根据数据 |  |  |
| M5 | 2 | 规则的属性常规选项卡显示只允许安全连接被选中。且规则的属性远程用户选项卡里显示仅允许来自下列用户的连接已打勾； | 根据数据 |  |  |
| M6 | 2 | 用户组sales已存在； | 根据数据 |  |  |
| M7 | 2 | 用户manager已存在； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：CentOS系统安全检测与应急响应

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）ClamAV扫描软件。

**2.**工作任务

某公司的文件服务器疑似被恶意访问，导致服务器Server1目前处于性能和安全的不稳定状态，作为公司的IT安全工程师，需要完成以下任务来解决问题：  
（1）使用ClamAV对系统关键目录进行病毒扫描，并将结果记录到/var/log/virus\_scan.log；   
（2）配置iptables防火墙规则，禁止所有出站连接，仅允许22端口的SSH服务，并将规则记录至/var/log/iptables.txt；   
（3）检查系统用户列表和crontab任务，记录任何可疑的新增用户或定时任务到/var/log/security\_check.log。

**3.**技能要求

（1）能执行系统关键目录的病毒扫描；   
（2）能设置iptables防火墙规则进行流量控制；   
（3）能检查系统用户和计划任务，识别可疑活动；

**4.**质量指标

（1）病毒扫描准确记录；   
（2）防火墙规则正确设置，符合安全策略；   
（3）系统用户和crontab检查无误，可疑活动得到记录。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：CentOS系统安全检测与应急响应

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | /var/log/virus\_scan.log文件存在 | 根据数据 |  |  |
| M2 | 3 | /var/log/virus\_scan.log存在病毒扫描记录 | 根据数据 |  |  |
| M3 | 2 | /var/log/iptables.txt文件存在 | 根据数据 |  |  |
| M4 | 2 | /var/log/iptables.txt里的规则正确 | 根据数据 |  |  |
| M5 | 2 | /var/log/security\_check.log文件存在 | 根据数据 |  |  |
| M6 | 3 | /var/log/security\_check.log存在可疑活动记录 | 根据数据 |  |  |
| M7 | 1 | 病毒扫描和安全检查记录文件格式正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：CentOS系统安全加固与日志审查

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）ClamAV扫描软件。

**2.**工作任务

某公司的文件服务器疑似被恶意访问，导致服务器Server1目前处于性能和安全的不稳定状态，作为公司的IT安全工程师，需要完成以下任务来解决问题：  
（1）使用ClamAV对系统关键目录进行病毒扫描，并将结果记录到/var/log/virus\_scan.log；  
（2）配置SELinux策略，确保所有关键服务都在严格监控下运行，并记录状态到/var/log/selinux\_status.log；   
（3）检查系统用户列表和crontab任务，记录任何可疑的新增用户或定时任务到/var/log/security\_check.log。

**3.**技能要求

（1）能执行系统关键目录的病毒扫描；   
（2）能配置SELinux策略并检查其状态；   
（3）能检查系统用户和计划任务，识别可疑活动；

**4.**质量指标

（1）病毒扫描准确记录；   
（2）SELinux策略正确配置并记录；   
（3）系统用户和crontab检查无误，可疑活动得到记录.

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：CentOS系统安全加固与日志审查

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | /var/log/virus\_scan.log文件存在 | 根据数据 |  |  |
| M2 | 3 | /var/log/virus\_scan.log存在病毒扫描记录 | 根据数据 |  |  |
| M3 | 2 | /var/log/selinux\_status.log文件存在 | 根据数据 |  |  |
| M4 | 2 | /var/log/selinux\_status.log里的状态记录正确 | 根据数据 |  |  |
| M5 | 2 | /var/log/security\_check.log文件存在 | 根据数据 |  |  |
| M6 | 3 | /var/log/security\_check.log存在可疑活动记录 | 根据数据 |  |  |
| M7 | 1 | 病毒扫描和安全检查记录文件格式正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows系统安全审计与日志审核

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机；   
（2）Windows Server系统；   
（3）CentOS系统。

**2.**工作任务

某公司的文件服务器疑似被恶意访问，导致服务器Server1目前处于性能和安全的不稳定状态，作为公司的IT安全工程师，需要完成以下任务来解决问题：  
（1）打开服务器的windows defender，对服务器进行快速扫描，如发现异常文件，执行隔离操作，并将隔离文件的信息存放至D:\kaoshi\_3\隔离记录.txt中；  
（2）审核系统日志文件，如事件查看器中的安全日志，以查找异常登录尝试和系统警告，并记录到D:\kaoshi\_3\system\_audit.log;  
（3）配置Windows防火墙规则（规则名为deny\_app），禁止文件共享和WEB服务的出站连接，并导出规则至D:\kaoshi\_3\wf.txt。

**3.**技能要求

（1）能使用Windows Defender执行系统扫描；   
（2）能审核系统日志文件，识别异常事件；   
（3）能配置Windows防火墙规则；

**4.**质量指标

（1）病毒扫描准确记录；   
（2）系统日志审核准确，异常事件得到记录；   
（3）防火墙规则正确设置，符合安全策略

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows系统安全审计与日志审核

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | windows defender快速扫描后的隔离记录D:\kaoshi\_3\隔离记录.txt存在； | 根据数据 |  |  |
| M2 | 2 | D:\kaoshi\_3\隔离记录.txt中的内容正确； | 根据数据 |  |  |
| M3 | 2 | D:\kaoshi\_3\system\_audit.log文件存在 | 根据数据 |  |  |
| M4 | 3 | D:\kaoshi\_3\system\_audit.log里的状态记录正确 | 根据数据 |  |  |
| M5 | 2 | 防火墙规则存在，名称为deny\_app | 根据数据 |  |  |
| M6 | 2 | D:\kaoshi\_3\wf.txt文件存在 | 根据数据 |  |  |
| M7 | 2 | D:\kaoshi\_3\wf.txt文件里的规则正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：CentOS系统安全优化与监控

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）ClamAV扫描软件。

**2.**工作任务

某公司的文件服务器疑似被恶意访问，导致服务器Server1目前处于性能和安全的不稳定状态，作为公司的IT安全工程师，需要完成以下任务来解决问题：  
（1）优化系统性能，调整关键内核参数以提高系统响应速度（调整页面缓存大小为80%），并记录优化结果到/var/log/system\_optimization.log；   
（2）使用ClamAV对系统关键目录进行病毒扫描，并将结果记录到/var/log/virus\_scan.log;  
（3）配置iptables防火墙规则，禁止所有出站连接，仅允许22端口的SSH服务，并记录规则至/var/log/iptables.txt。

**3.**技能要求

（1）能优化系统性能并调整内核参数；   
（2）能执行系统关键目录的病毒扫描；   
（3）能配置iptables防火墙规则；

**4.**质量指标

（1）系统性能优化得当，内核参数调整合理，优化结果记录完整；   
（2）病毒扫描准确记录；   
（3）防火墙规则正确设置，符合安全策略.

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：CentOS系统安全优化与监控

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 1 | /var/log/system\_optimization.log文件存在 | 根据数据 |  |  |
| M2 | 2 | /var/log/system\_optimization.log存在内存优化参数 | 根据数据 |  |  |
| M3 | 2 | /var/log/system\_optimization.log存在文件系统缓存优化参数 | 根据数据 |  |  |
| M4 | 2 | /var/log/virus\_scan.log文件存在 | 根据数据 |  |  |
| M5 | 3 | /var/log/virus\_scan.log存在病毒扫描记录 | 根据数据 |  |  |
| M6 | 2 | /var/log/iptables.txt文件存在 | 根据数据 |  |  |
| M7 | 3 | /var/log/iptables.txt里的规则正确 | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：提取WEB服务日志并分析

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）Splunk enterprise。

**2.**工作任务

某公司的网站服务器最近访问量波动较大，IT主管推测可能有可疑流量，作为公司的IT安全工程师，请完成以下任务来获取相关日志并进行分析。  
（1）安装Splunk软件（安装源在D盘，安装的用户名admin，密码Admin@12345），然后添加一个新用户operator，权限为power用户，供以后分析日志备用；  
（2）将提供的日志文件（位于D盘），导入到Splunk平台，新建索引appiis，索引数据类型默认，直至完成；  
（4）在搜索页面，编写spl语句（Splunk搜索语言）将日志时间范围定位到当前日期的前24小时；  
（5）新建仪表板，标题为iis，仪表板ID任意，生成后并设置为主页仪表板。  
（6）针对WEB服务的日志分析报告，导出到D:\kaoshi\_3\3.3.1.pdf文件。

**3.**技能要求

（1）能安装日志分析工具并添加用户；   
（2）能导入日志文件；   
（3）能配置日志分析的搜索功能；   
（4）能配置日志数据可视化。

**4.**质量指标

（1）系统用户添加正确；   
（2）IIS日志导入和索引创建正确；   
（3）spl语句正确；   
（4）数据可视化正确；   
（5）日志分析报告导出正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：提取WEB服务日志并分析

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Splunk安装成功； | 根据数据 |  |  |
| M2 | 2 | 管理员账号admin存在； | 根据数据 |  |  |
| M3 | 2 | 设置的用户中存在Operator用户，角色为power； | 根据数据 |  |  |
| M4 | 3 | WEB服务器日志导入正确； | 根据数据 |  |  |
| M5 | 2 | 在搜索框中输入index=appiis host=Server1语句，可以搜出对应的日志信息； | 根据数据 |  |  |
| M6 | 2 | 在首页的仪表板中出现名为iis的仪表板; | 根据数据 |  |  |
| M7 | 2 | 日志报告导出路径为D:\kaoshi\_3\3.3.1.pdf； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：SQL Server数据库服务日志分析

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）Splunk enterprise。

**2.**工作任务

某公司的网站服务器最近访问量波动较大，IT主管推测可能有可疑流量，作为公司的IT安全工程师，请完成以下任务来获取相关日志并进行分析。  
（1）安装Splunk软件（安装源在D盘，安装的用户名admin，密码Admin@12345），然后添加一个新用户operator，权限为power用户，供以后分析日志备用；  
（2）将SQL Server日志文件（在D盘）导入到Splunk平台，新建索引sql\_server，索引数据类型默认，直至完成；  
（4）在搜索页面，编写spl语句（Splunk搜索语言）将时间范围定位到日志时间段的最近24小时；  
（5）针对SQL Server服务的日志分析报告，导出到D:\kaoshi\_3\3.3.2.pdf文件。

**3.**技能要求

（1）能安装日志分析工具并添加用户；   
（2）能导入日志文件；   
（3）能配置日志分析的搜索功能；   
（4）能导出日志分析报告。

**4.**质量指标

（1）系统用户添加正确；   
（2）日志导入正确；   
（3）spl语句正确；   
（4）日志分析报告导出正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：SQL Server数据库服务日志分析

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Splunk安装成功； | 根据数据 |  |  |
| M2 | 2 | 管理员账号admin存在； | 根据数据 |  |  |
| M3 | 2 | 设置的用户中存在Operator用户，角色为power；（2分） | 根据数据 |  |  |
| M4 | 2 | SQLserver日志导入成功；（2分） | 根据数据 |  |  |
| M5 | 2 | Splunk索引创建正确；（2分） | 根据数据 |  |  |
| M6 | 2 | Splunk搜索语句正确，能定位到前24小时；（2分） | 根据数据 |  |  |
| M7 | 1 | 日志报告导出路径为D:\kaoshi\_3\3.3.2.pdf；（1分） | 根据数据 |  |  |
| M8 | 2 | 日志报告中存在警告信息；（2分） | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：邮件服务日志分析

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）Splunk enterprise。

**2.**工作任务

某公司的网站服务器最近访问量波动较大，IT主管推测可能有可疑流量，作为公司的IT安全工程师，请完成以下任务来获取相关日志并进行分析。  
（1）安装Splunk软件（安装源在D盘，安装的用户名admin，密码Admin@12345），然后添加一个新用户operator，权限为power用户，供以后分析日志备用；  
（2）将Winmail邮件日志文件（在D盘）导入到Splunk平台，新建索引winmail\_server，索引数据类型默认，直至完成；  
（3）在搜索页面，编写spl语句（Splunk搜索语言）将时间范围定位到日志时间段的最近24小时；  
（4）特别关注可能表明垃圾邮件的日志条目，并在报告中进行标记，将邮件服务的日志分析报告，导出到D:\kaoshi\_3\3.3.3.pdf文件。

**3.**技能要求

（1）能安装日志分析工具并添加用户；   
（2）能导入日志文件；   
（3）能配置日志分析的搜索功能；   
（4）能导出日志分析报告。

**4.**质量指标

（1）系统用户添加正确；   
（2）日志导入及索引正确；   
（3）spl语句正确；   
（4）日志分析报告导出正确

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：邮件服务日志分析

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Splunk安装成功； | 根据数据 |  |  |
| M2 | 2 | 管理员admin存在； | 根据数据 |  |  |
| M3 | 2 | 设置的用户中存在Operator用户，角色为power； | 根据数据 |  |  |
| M4 | 2 | 日志文件导入Splunk正确； | 根据数据 |  |  |
| M5 | 2 | 索引创建正确； | 根据数据 |  |  |
| M6 | 2 | Splunk搜索语句正确，能定位到前24小时；（2分） | 根据数据 |  |  |
| M7 | 1 | 日志报告导出路径为D:\kaoshi\_3\3.3.3.pdf；（1分） | 根据数据 |  |  |
| M8 | 2 | 日志报告中存在垃圾邮件的警告信息；（2分） | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Apache HTTP服务日志分析

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）Splunk enterprise。

**2.**工作任务

某公司的网站服务器最近访问量波动较大，IT主管推测可能有可疑流量，作为公司的IT安全工程师，请完成以下任务来获取相关日志并进行分析。  
（1）安装Splunk软件（安装源在D盘，安装的用户名admin，密码Admin@12345），然后添加一个新用户operator，权限为power用户，供以后分析日志备用；  
（2）将Apache日志文件（在D盘）导入到Splunk平台，新建索引apache，索引数据类型默认，直至完成；  
（3）在搜索页面，编写spl语句（Splunk搜索语言）将时间范围定位到日志时间段的最近48小时；  
（4）特别关注HTTP的所有404和500错误，并在报告中进行标记，将HTTP服务的日志分析报告，导出到D:\kaoshi\_3\3.3.4.pdf文件。

**3.**技能要求

（1）能安装日志分析工具并添加用户；   
（2）能导入日志文件；   
（3）能配置日志分析的搜索功能；   
（4）能导出日志分析报告。

**4.**质量指标

（1）系统用户添加正确；   
（2）apache日志导入及索引正确；   
（3）spl语句正确；   
（4）日志分析报告导出正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Apache HTTP服务日志分析

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Splunk安装成功； | 根据数据 |  |  |
| M2 | 2 | 管理员admin存在； | 根据数据 |  |  |
| M3 | 2 | 设置的用户中存在Operator用户，角色为power； | 根据数据 |  |  |
| M4 | 2 | 日志文件导入正确； | 根据数据 |  |  |
| M5 | 2 | 索引创建正确； | 根据数据 |  |  |
| M6 | 2 | Splunk搜索语句正确，能定位到前48小时； | 根据数据 |  |  |
| M7 | 1 | 日志报告导出路径为D:\kaoshi\_3\3.3.4.pdf； | 根据数据 |  |  |
| M8 | 2 | 日志报告中存在404和500的HTTP错误的警告信息； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）

**信息安全管理员（三级）操作技能考核**

**试题单**

准考证号：

试题代码：

试题名称：Windows应用安全日志分析

考核时间：20min

**1.**场地设备要求

（1）VMware虚拟机   
（2）Windows Server系统   
（3）CentOS系统；   
（4）Splunk enterprise。

**2.**工作任务

某公司的网站服务器最近访问量波动较大，IT主管推测可能有可疑流量，作为公司的IT安全工程师，请完成以下任务来获取相关日志并进行分析。  
（1）安装Splunk软件（安装源在D盘，安装的用户名admin，密码Admin@12345），然后添加一个新用户operator，权限为power用户，供以后分析日志备用；  
（2）将Windows应用安全日志文件（在D盘）导入到Splunk平台，新建索引win\_sec，索引数据类型默认，直至完成；  
（3）在搜索页面，编写spl语句（Splunk搜索语言）将时间范围定位到日志时间段的最近48小时；  
（5）特别关注包含“登录失败”关键字的日志条目，并在报告中进行标记，将安全日志分析报告导出到D:\kaoshi\_3\3.3.5.pdf文件。

**3.**技能要求

（1）能登录日志分析工具并添加用户；   
（2）能导出Windows安全日志；   
（3）能导入日志文件；   
（4）能配置日志分析的搜索功能；   
（5）能导出日志分析报告。

**4.**质量指标

（1）系统用户添加正确；   
（2）windows应用安全日志导入及索引正确；   
（3）spl语句正确；   
（4）日志分析报告导出正确。

**信息安全管理员（三级）操作技能考核**

**试题评分表及答案（主客观评分方式）**

准考证号：

试题代码：

试题名称：Windows应用安全日志分析

考核时间：20min

测量分评分表

| 细则编号 | 配分 | 评分细则描述 | 规定或  标称值 | 结果或  实际值 | 得分 |
| --- | --- | --- | --- | --- | --- |
| M1 | 2 | Splunk安装成功； | 根据数据 |  |  |
| M2 | 2 | 管理员admin存在； | 根据数据 |  |  |
| M3 | 2 | 设置的用户中存在Operator用户，角色为power； | 根据数据 |  |  |
| M4 | 2 | 日志文件导入Splunk正确； | 根据数据 |  |  |
| M5 | 2 | 索引创建正确； | 根据数据 |  |  |
| M6 | 2 | Splunk搜索语句正确，能定位到前48小时； | 根据数据 |  |  |
| M7 | 1 | 日志报告导出路径为D:\kaoshi\_3\3.3.5.pdf； | 根据数据 |  |  |
| M8 | 2 | 日志报告中存在登录失败的警告信息； | 根据数据 |  |  |
| 合计配分 | 15 | 合计得分 | |  |  |

考评员： 日期：

**参考答案**（尽量将细则内容写在上面的表格内，写不下可另写，但要具体可评判）