**第6部分**

操作技能考核模拟试卷

注 意 事 项

1．考生根据操作技能考核通知单中所列的试题做好考核准备。

2．请考生仔细阅读试题单中具体考核内容和要求，并按要求完成操作或进行笔答或口答，若有笔答请考生在答题卷上完成。

3．操作技能考核时要遵守考场纪律，服从考场管理人员指挥，以保证考核安全顺利进行。

注：操持技能鉴定试题评分表及答案是考评员对考生考核过程及考核结果的评分记录表，也是评分依据。

职业技能等级认定

信息安全管理员（三级）操作技能考核通知单

姓名：

准考证号：

考核日期：

试题1

试题代码：1.1.1

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

配分：20分

试题2

试题代码：1.3.1

试题名称：配置Windows Server防火墙和远程桌面安全

考核时间：20min

配分：20分

试题3

试题代码：2.1.4

试题名称：无线网络接入安全管理

考核时间：20min

配分：15分

试题4

试题代码：2.2.1

试题名称：配置Linux审计日志

考核时间：20min

配分：15分

试题5

试题代码：3.1.1

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

配分：15分

试题6

试题代码：3.3.1

试题名称：提取WEB服务日志并分析

考核时间：20min

配分：15分

**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：1.1.1

试题名称：配置无线控制器和访问点以增强网络安全

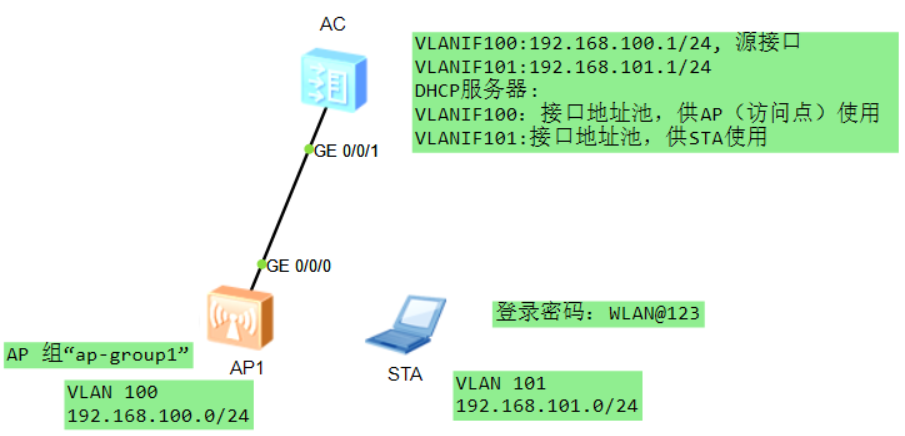
考核时间：20min

**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：1.1.1

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：1.3.1

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：1.3.1

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：2.1.4

试题名称：无线网络接入安全管理

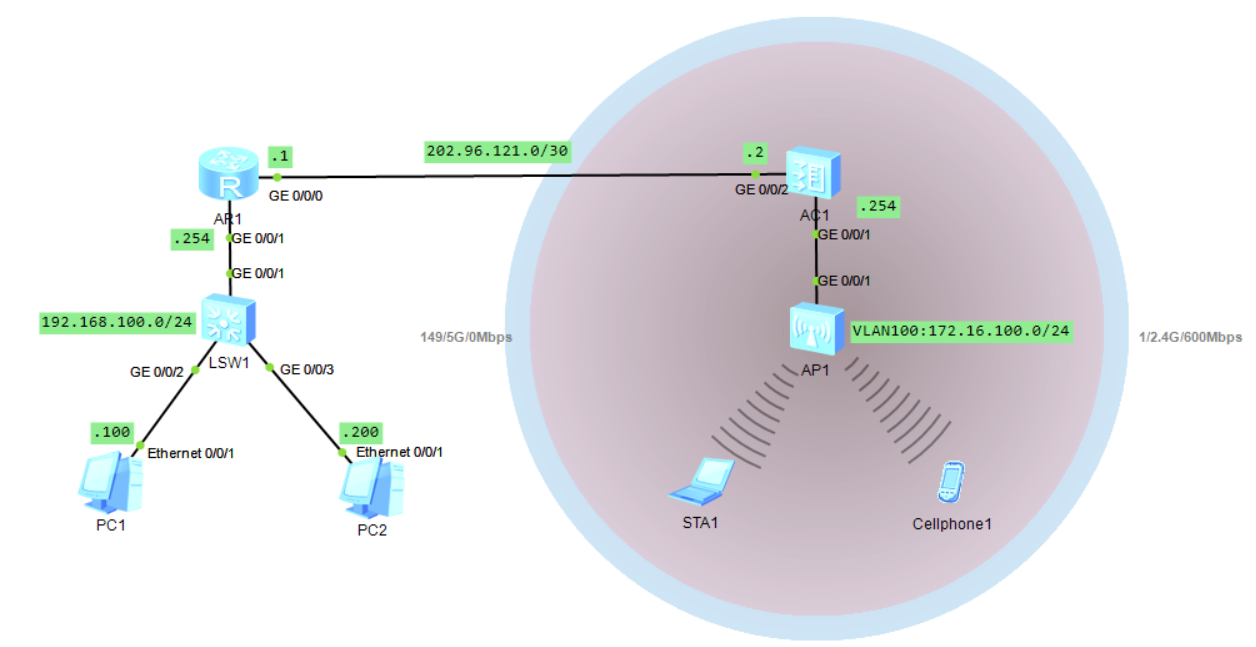
考核时间：20min

**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：2.1.4

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：2.2.1

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：2.2.1

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：3.1.1

试题名称：运用防火墙来监控数据流量、识别攻击特征

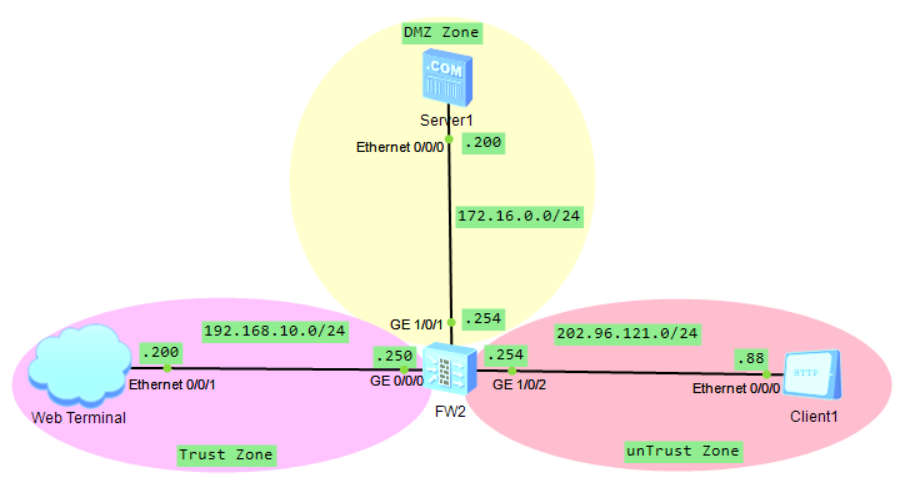
考核时间：20min

**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：3.1.1

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：3.3.1

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：3.3.1

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）