《信息系统安全运维》

培训课程标准

2020 年 9 月

目　录

《信息系统安全运维》培训课程标准

一、培训说明

1. 课程名称

信息系统安全运维

2. 标准定义

信息系统安全运维是在指对已建立好的信息系统的运行进行维护,并采用各种手段确保信息系统免受各种安全威胁所采取的一系列预先定义的活动。

3. 培训对象

具有高中（或同等学力）以上学历，身体健康、年龄在18岁以上，45岁以下有意于从事信息系统安全运维相关工作的人员。

二、培训目标

通过培训，掌握安全运维服务体系的流程和方法，掌握网络管理与运维中各类知识、技巧和故障处理及最佳安全运维实践方法，能够胜任信息系统安全运维员岗位上的各项工作。

1.职业素养目标

1) 培养学生对信息系统安全运维的综合知识能力和职业素质；

2) 培养学生的实际动手能力和自主学习能力；

3) 培养学生的分析问题、解决问题的能力；

4) 培养学生开拓创新能力，逐步积累信息系统安全运维经验；

5) 培养学生的自我管理和组织能力、与人交往和表达能力、团队协作、爱岗敬业的精神。

2. 专业能力目标

1) 能够了解信息想系统安全运维的主要工作内容和实施步骤；

2) 能够通过分析用户需求选择合适的运维服务体系；

3) 能够根据用户信息系统状况选择合适的安全运维策略；

4) 能够根据用户需求编写运维方案；

5) 能够理解和掌握日程运维工作内容；

6) 理解网络协议、网络模型和 IP 地址；

6）能够安装和连接网络软硬件设备；

7) 能够搭建与配置服务器；

8) 能够安装和配置无线网络；

9) 能够组建办公网络；

10) 掌握网络常见故障排查；

11) 能够根据网络特点选择网络安全技术,实现网络安全运维。

3. 方法能力目标

1) 制定工作计划能力；

2）对信息系统安全运维方案设计以及评价能力；

3）能够有效地获取、利用、传递资料信息进行自主学习；

4）通过独立学习，不断获取新的知识和技能，能够在工作中寻求发现问题、解决问题的途径；

5）具备应急响应和处置能力；

6）具备应对复杂情况的能力和开拓创新能力。

三、课时分配

总培训课时：120 课时，其中理论 32 课时，实操 84 课时，考核评价 4 学时。

具体培训课时分配见下：

培训课时分配表

培训内容	课程类型	培训课时	总课时
模块一：安全运维服务体系			116
1. 安全运维框架 2. 合规要求	理论教学	4	
模块二： 安全运维策略			
1. 安全策略 2. 案例分析	理论教学	4	
模块三： 安全运维准备			
1. 安全运维需求分析 2. 安全运维策划 3. 安全运维服务预算 4. 案例分析 5. 任务 1：编写安全运维需求报告 6. 任务 2：编写安全运维服务方案	理论教学	8	
模块四： 运维实施			

培训内容	课程类型	培训课时	总课时
1. 日常运维 2. 网络协议、网络模型和 IP 地址 3. 网络硬件设备的安装和连接 4. 组建办公网络 5. 局域网资源共享 6. 服务器搭建与配置 7. 无线网络应用 8. 常见故障排查	理论 8 学时+实操 64 学时	72	
模块五： 运维安全			
1．运维安全概述 2．资产管理 3．日志管理 4．访问控制 5．密码管理 6．漏洞管理 7．备份 8．安全事件管理及响应 9.任务：利用工具扫描信息系统，并对漏洞进行加固，编写分析报告。	理论教学 8 学时+ 实操 20 学时	28	
考核评价			
理论考核 实操考核	理论考核 1 学时 +实操考核 3 学时	4	

四、培训内容

课程模块	课程名称	培训内容	培训建议

课程模块	课程名称	培训内容	培训建议
模块一 **安全运维服务体系**	一、安全运维框架 二、合规要求	一、安全运维框架 1. 安全运维主体 2. 安全运维对象 3. 安全运维流程 4. 安全运维支撑平台 5. 安全运维活动 二、合规要求 1. 法律法规要求 2. 信息安全标准 3. 运维服务标准	重点： 1. 安全运维流程 2. 运维服务标准
模块二 **安全运维策略**	一、安全策略 二、案例分析	一、安全策略 1. 安全策略概述 2. 制定安全策略方法 3. 安全策略内容 二、案例分析 1. 信息安全运维策略框架 2. 信息安全策略的执行和维护	重点： 1. 制定安全策略方 2. 信息安全运维策略框架
模块三 **安全运维准备**	一、安全运维需求分析 二、安全运维策划 三、安全运维服务预算 四、案例分析 五、任务 1：编写安全运维需求报告 六、任务 2：编写安全运维服务方案	一、安全运维需求分析 1. 服务需求确认 2. 服务需求说明 3. 服务需求管理 二、安全运维策划 1. 安全运维架构 2. 安全运维活动 3. 安全运维团队 4. 安全运维平台 三、安全运维服务范围 1. 安全运维资产梳理 2. 安全运维业务梳理 四、案例分析 1. 运维服务用户需求	重点： 1.安全运维需求分析 2.编写安全运维服务方案

课程模块	课程名称	培训内容	培训建议
		2. 安全运维预算管理 3. 安全运维组织 4. 运维服务范围及内容 五、任务 1：编写安全运维需求报告 六、任务 2：编写安全运维服务方案	
模块四 **运维实施**	一、日常运维 二、网络协议、网络模型和 IP 地址 三、网络硬件设备的安装和连接 四、组建办公网络 五、局域网资源共享 六、服务器搭建与配置 七、无线网络应用 八、常见故障排查	**一、日常运维** 1. 日常运维内容 2. 日常运维组织保障 3. 日常运维处理流程 4. 日常安全运维建议 **二、网络协议、网络模型和 IP 地址** 1. 网络基础模型，数据封装 2. IP 寻址方式，地址转换 3. 子网掩码、VLSM 与子网划分 4. TCP/IP 协议 5. IP 路由选择（static route） 6. 任务 1： 查看局域网中的某台主机是否在线 7. 任务 2： 查看 ADSL 上网获取到的 IP 地址 **三、网络硬件设备的安装和连接** 1. 客户机和服务器电脑 2. 网络传输介质 3. 网络传输设备 4. 辅助设备 5. 网络连接 （1）网络连接示意图 （2）任务 1： 动手制作网线 （3）任务 2： 网线通断测试 6. 网卡的安装与连接	重点： 1. 网络硬件设备的安装和连接； 2. 服务器搭建与配置； 3. 安装和配置无线网络； 4. 常见故障排查

课程模块	课程名称	培训内容	培训建议
		（1）任务 1： 动手安装网卡 （2）任务 2：动手连接网线与网卡 7. 交换机的连接 (1)动手连接交换机与相关网络设备 8. 路由器的安装与连接 9. 网络扩展方案 (1) 交换机的级联 (2) 交换机的堆栈 (3) 机柜和网络设备的安装 (4) 任务：动手安装和连接路由器 **四、组建办公网络** 1. 办公网络设计 2. 办公网络的设计原则 3. 网络结构与网络类型的选择 4. 网络设备的选择 5. 组网方案的选择 6. 水晶头、网线和网卡的选择 7. 交换机的选择 8. 路由器的选择 9. 防火墙的选择 10. 办公网络的连接 11. 任务 1：动手组建办公网络 12. 任务 2：RJ-45 信息模块的安装 **五、局域网资源共享** 1. 共享文件至局域网中 2. 共享硬件设备至局域网中 3. 连接网络打印机 4. 任务 1：解决不同系统间共享打印机的问题 5. 局域网共享宽带上网 6. 光纤接入网 7. 共享上网 8. 局域网路由器共享上网配置	

课程模块	课程名称	培训内容	培训建议
		9. 任务 1： 静态 IP 配置 10. 任务 2： 动态 IP 配置 11. 任务 3：DHCP 服务器和客户机配置 **六、服务器搭建与配置** 1. 服务器操作系统的安装 2. 服务器操作系统管理 （1）任务 1： 设置账户所在的组 （2）任务 2：设置用户或组的权限 （3） 多个用户同时远程登录或同一用户多个远程登录 4. 网络服务的搭建与管理 （1） WWW 服务器的搭建与管理 （2）任务 3： 通过修改默认网站来添加网 （3） DHCP 服务器的搭建与管理 5. DNS 服务器的搭建与管理 6. 任务 4： 备份和还原 DNS 服务 7. FTP 服务器的搭建与管理 8. 任务 5： FTP 服务器不能访问的解决办法 9. 流媒体服务器的搭建与管理 10. 任务 6： 查看 CPU 是否支持虚拟化技术 11. 任务 7： 开启 CPU 虚拟化功能 **七、无线网络应用** 1. 无线局域网基础 2. 无线网络设备的分类与选择策略 3. 无线局域网典型应用方案 4. 无线局域网设备的安装 5. 配置 SOHO 无线网络 6. 任务 1： 安装无线网络控制器 7. 任务 2：安装室内无线 AP 8. 任务 3：安装无线路由器	

课程模块	课程名称	培训内容	培训建议
		9. 任务 4：安装无线天线 **八、常见故障排查**	
模块五 **运维安全**	一、运维安全概述 二、资产管理 三、日志管理 四、访问控制 五、密码管理 六、漏洞管理 七、备份 八、安全事件管理及响应 九、任务：利用工具扫描信息系统，并对漏洞进行加固，编写分析报告。	一、运维安全概述 二、资产管理 1. 资产识别 2. 资产管理 三、日志管理 四、访问控制 五、密码管理 六、漏洞管理 1. 漏洞扫描 2. 安全加固 七、备份 八、安全事件管理及响应 九、任务 1：利用工具扫描信息系统，并对漏洞进行加固，编写分析报告。	重点： 1. 日志管理； 2. 漏洞管理； 3. 密码管理； 4. 备份。

五、推荐教材

《网络系统建设与运维》华为技术有限公司主编，人民邮电出版社出版，2020-09-01 出版，ISBN：9787115544872。

六、培训实施

1.培训师资

培训师资要求本科以上学历，在 IT 行业工作 5 年以上，中级以上职称，具有较强的理论基础与实战经验的行业精英。

2.培训场地

（1）能满足30人以上学习的的理论课室，配备人手一台电脑、投影、白板、音响设备等教学设备；

（2）能满足30人以上实操训练的场地，配备网络设备、安全设备、应用系统、安防系统、建筑智能化系统等实训设备。

3.实训设备

技能培训的实习工具与设备表

序号	设备及用品名称	型号/软件版本	数量	备注
1.	教师电脑	联想M415-i5 7500/8GB/128GB+1TB/Win 10专业版	1	一套完整多媒体电脑
2.	投影仪	明基MS527-教育投影机	1	
3.	学生电脑	联想M420-i3 8100/8GB/1TB/集显 /Win10专业版	30	完整多媒体电脑
4.	白板	-	1	用于板书
5.	投影幕布	-	1	
6.	音响功放	JSL B-300	1台	可联无线麦
7.	无线麦	谭师傅 F-1	2只	一只备用
8.	音箱	JSL S350	2台	悬挂或落地
9.	无线WiFi路由	TP-link TL-WR2041N	1个	带千兆有线网口
10.	课件遥控笔	/		1个

序号	设备及用品名称		型号/软件版本	数量	备注
11.	服务器		联想 ThinkSystem SR550-Xeon 银牌 4110/16GB/2TB/550W	5	实训室内搭建一个模拟环境
12.	网络配套设备	路由器	H3C ER5200G2	5 套	
		交换机	H3C S5130S-28P-EI、ADSL		
		调制解调器	B-Link UM03A		
		防火墙	华为 USG6530/深信服 NGAF-1000-A400		
13.	网络安全工具	嗅探器	Sniffer Pro V 4.7.5	5 套	
		漏洞扫描	Nessus V8.13.1		
		渗透测试工具	burpsuite V2.1		
		端口扫描	ZeNmap v7.91		
		发包工具	xcap v1.0.3		
		入侵检测/日志审计系统	sauditor Network Security Auditor 网络安全审计软件/V3.1.4.0		

七、 考核评价

1.考核方式

考核形式采用理论与实操相结合，理论考核采用闭卷笔试，操作考核采用现场实际操作方式进行。考核成绩均实行百分制，其中理论考试成绩 100 分满分，60分及格，考核时间为90分钟；实操成绩 100 分满分，60 分及格，考核时间为 180 分钟。

考核形式	满分	及格	考核时间

理论	100	60	1 小时
操作	100	60	3 小时

培训课程结束后立即进行考核，先进行理论考核，再进行操作考核，两项考核均达考核标准，才核算为考核通过，颁发相应的证书。未参加考核或考核未通过者不发证书。

2. 考核内容

（1）理论考核

理论考核主要围绕所学过的知识,考查学员的基本掌握情况及融会贯通以及综合应用能力，主要的考核内容以及比重如下：

序号	考核内容		比重
1	职业素养	从事信息系统安全运维工作必备的职业素养	5
2	合规性要求	1. 信息安全法律法规 2. 等保、关保制度、标准 3. 监管部门要求	10
3	安全运维策略	1. 安全策略概述 2. 制定安全策略方法 3. 安全策略内容	10
4	网络协议、网络模型和IP地址	1. 网络基础模型，数据封装 2. IP 寻址方式，地址转换 3. 子网掩码、VLSM 与子网划分 4. TCP/IP 协议 5. IP 路由选择	15
5	交换机、路由器管理、VLAN等网络设置的配置和管理	1. 交换机和路由器的组成 2. IOS CLI 命令行功能 3. 交换机和路由器的启动过程 4. 交换机或路由器的基本配置 5. 交换机或路由器的管理方式	10

序号	考核内容		比重
6		1.交换机工作原理 2.交换机端口基本配置命令 3.VLAN 技术 4.基于 Access 口 VLAN 配置命令 5.VLAN 汇聚链接(Tmnk) 6.VLAN 数据帧的透传 7.基于 Trunk 口 VLAN 配置命令 8.VLAN 间的路由 9.VLAN 的部署与规划	15
7		1.交换网络中的环路问题 2.生成树协议的基本概念 3. RSTP 4.MSTP 5.以太网链路聚合 6.网关的备份和负载分担	10
8	网络故障排查	常见网络故障排查	10
9	运维安全	1.运维安全概述 2.资产管理 3.日志管理 4.访问控制 5.密码管理 6.漏洞管理 7.备份 8.安全事件管理及响应	15
合计			100

（2）操作考核

操作考核主要围绕所学过的知识，全面考查学员的理论基础、实际动手操作能力以及综合应用能力，实际场景应用能力。主要的考核内容以及比重如下：

序号	考核内容	比重
1	网线通断测试	5

2	连接网线与网卡	5
3	连接交换机与相关网络设备	10
4	安装和连接路由器	10
5	配置 静态 IP、 动态 IP、DHCP 服务器和客户机	20
6	备份和还原 DNS 服务	20
7	安装无线局域网设备	20
8	配置 SOHO 无线网络	10
合计		100

3.考核设施

（1）理论考核可以在教室，30 人标准位，隔位座，采用纸质试卷。也可以在机房采用考试系统进行无低化考试。

（2）机房搭建模拟化环境。

八 、联系方式

本标准的起草单位为广东省网络空间安全协会，联系人：成珍苑，

联 系 电 话 ： 020-83609433 、 15360402627 邮 箱 ： 896229800@qq.com。